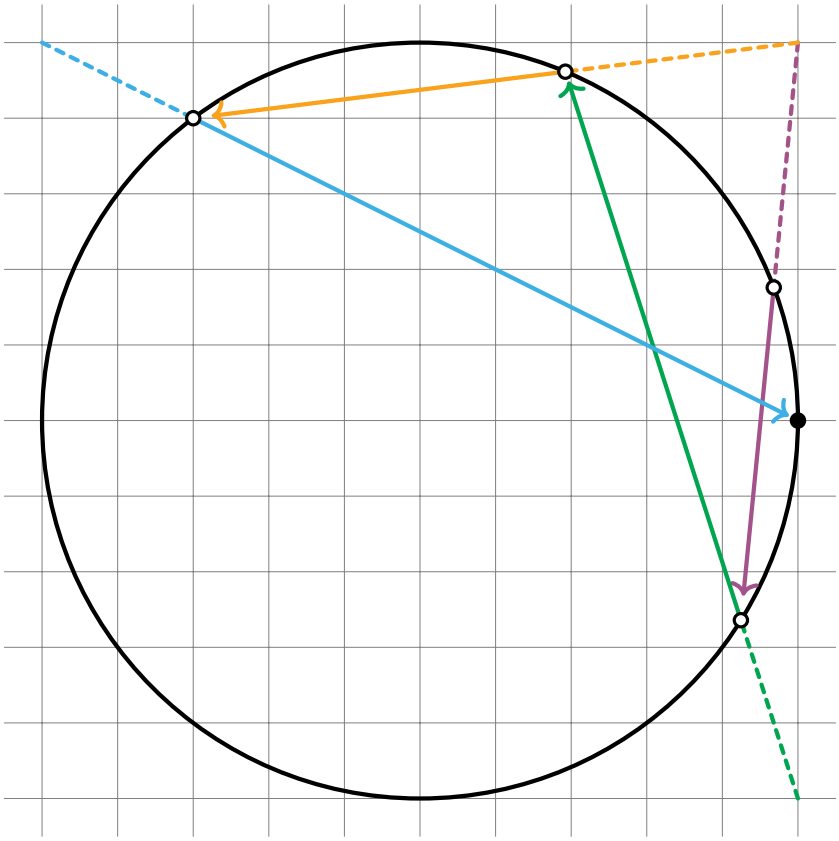
Johns Hopkins University

Egbert Rijke



The Great Story of Numbers

Version: 0.261124
Primary font: Libertinus
Supporting fonts: EB Garamond, GFS Artemisia, Noto Sans Cuneiform, STIX Two Math, Theano Didot
TeX engine: LuaHBTeX, Version 1.24.0 (TeX Live 2026); development id 7724
LaTeX format: LaTeX2e 2026-11-01
Document language: en-US
PDF version: 2.0
Accessibility standard: PDF/UA-2
Archival standard: PDF/A-4f
Tagging setup: MathML structure elements (math/setup=mathml-SE)

© 2025 Egbert Rijke.
All rights reserved.

Citing this work:

```
@book{rijke-0.261124,
  author = {Egbert Rijke},
  title = {The Great Story of Numbers},
  year = {2026},
  month = nov,
  note = {Version 0.261124},
  url = {https://egbertrijke.github.io/notes/number-theory/}
}
```

Cover image: Vieta jumps between the rational points on the unit circle eventually reach one of the points $(1, 0)$, $(0, 1)$, $(-1, 0)$, or $(0, -1)$. See §11.5 for a full explanation.

To those on Earth whom Līlāvatī keeps in her embrace,
Of noble birth, her form with virtues pure adorned,
Who hearken to her speech, instinct with grace,
Increased be their joy, for evermore.

Bhāskarācārya, from *Līlāvatī*

Contents

Introduction · xiii

I **The Nature of Numbers · 1**

1 The Nature of Mathematical Inquiry · 3
1.1 Brief Remarks on the History of Number Theory · 3
1.1.1 The Ancient Greek Scholars · 3
1.1.2 Mathematics, Astronomy, and Poetry in Ancient India · 5
1.1.3 Pierre de Fermat · 5
1.1.4 Leonhard Euler · 9
1.1.5 Johannes Carl Friedrich Gauss · 11
1.1.6 Contemporary Mathematics · 11
1.2 The Concept of Number Through History · 12
1.3 Mathematical Language · 17

2 Mathematical Induction · 19
2.1 Recursion and Induction · 19
2.2 Addition of Natural Numbers · 22
2.3 Arithmetic of Natural Numbers · 24
2.4 Relations on the Natural Numbers · 25
2.5 Finite Sums and Products · 27
2.6 Hemachandra's Counting Problem · 29
Exercises · 31

3 Counting · 37
3.1 Hume's Principle · 37

3.2 Equivalent Ways of Defining Bijections · 42
3.3 Counting Bijections · 44
3.4 Counting Subsets · 46
3.5 The Binomial Theorem · 50
3.6 The Inclusion–Exclusion Principle · 51
3.7 The Stars-and-Bars Problem · 54
Exercises · 60

4 The Integers · 65
4.1 Cyclic Sets · 65
4.2 Maps Preserving Cyclic Structure · 67
4.3 A Structural Definition of the Integers · 70
4.4 Constructing the Integers from the Natural Numbers · 73
4.5 Integer Arithmetic · 75
Exercises · 79

5 Notation for Numbers · 81
5.1 Some Remarks on the History of Written Numbers · 81
5.2 The Well-Ordering Principle of the Natural Numbers · 83
5.3 Euclidean Division · 84
5.4 The Representability Theorem · 86
5.5 Combinatorial Applications · 88
Exercises · 90

6 Divisibility · 93
6.1 The Condition of Divisibility · 93
6.2 The Ordering by Divisibility · 95
6.3 Ideals of Integers · 97
Exercises · 99

7 Linear Diophantine Equations · 101
7.1 Greatest Common Divisors · 101
7.2 Euclid's Algorithm · 103
7.3 Linear Diophantine Equations in Multiple Variables · 106
7.4 Āryabhaṭa's Computations of the Positions of Planets · 108
Exercises · 109

8 Congruences · 111
8.1 The Congruence Relations · 111
8.2 Equivalence Relations · 116
8.3 Equivalence Classes and Residue Systems · 119
8.4 Modular Arithmetic · 121
8.5 The Multiplicative Order of an Integer Modulo n · 124
Exercises · 128

9 Systems of Linear Congruences · 131
9.1 Solving Linear Congruences · 131
9.2 Solving Multiple Linear Congruences Simultaneously · 133
9.3 The Chinese Remainder Theorem · 135
9.4 A Method Suggested by Gauss · 136
9.5 Lifting Invertible Congruence Classes · 137
Exercises · 139

10 The Rational Numbers · 141
10.1 Integer Fractions · 141
10.2 The Irrationality of Square Roots · 144
10.3 Continued Fractions · 144
10.4 Farey's Series of Fractions · 150
10.5 A Structural Definition of the Rational Numbers · 152
Exercises · 155

11 Pythagorean Triples · 157
11.1 The Pythagorean Theorem · 157
11.2 Euclid's Parametrization of the Pythagorean Triples · 161
11.3 Rational Points on the Unit Circle · 166
11.4 Vieta Jumping · 167
11.5 The Tree of Primitive Pythagorean Triples · 169
11.6 Squares in Arithmetic Progressions · 177
Exercises · 184

12 Infinite Descent · 187
12.1 The Method of Infinite Descent · 187
12.2 The Area of a Pythagorean Triangle is not a Square · 189
12.3 The Unsolvability of $x^4 + y^4 = z^4$ · 190
12.4 Aubry's Theorem · 192
12.5 The Nonexistence of Four Squares in an Arithmetic Progression · 194
12.6 The Congruent Number Problem · 197
Exercises · 203

II **The Multiplicative Nature of Numbers · 207**

13 Prime Numbers · 209
13.1 The Fundamental Theorem of Arithmetic · 209
13.2 The Infinitude of Primes · 214
13.2.1 Euclid's Proof · 214
13.2.2 Saidak's Proof · 215
13.2.3 Furstenberg's Proof, Following Cass–Wildenberg · 215
13.2.4 Erdős's Proof · 216



13.2.5 A Proof via the Stars-and-Bars Method · 217
13.3 Fermat Primes · 218
13.4 Legendre's Formula and Kummer's Theorem · 220
13.5 Bertrand's Postulate · 226
Exercises · 229

14 Multiplicative Functions · 233
14.1 Perfect Numbers · 233
14.2 Euler's Totient Function · 237
14.3 Multiplicative Functions · 239
14.4 The Möbius Function · 241
14.5 Dirichlet Convolution · 243
14.6 Dirichlet Inverses · 245
Exercises · 247

15 Cyclic Counting · 251
15.1 Hemachandra Wheels · 251
15.2 The Prime–Fixed Point Congruence · 253
15.3 Lucas's Theorem · 254
15.4 The Orbit–Counting Formula · 255
15.5 The Divisor Sum of the Totient Function · 257
15.6 Arithmetic Functions of Orbits and Fixed Points · 259
Exercises · 262

16 Fermat's Little Theorem and its Consequences · 265
16.1 Fermat's Little Theorem · 265
16.2 Euler's Theorem · 268
16.3 Wilson's Theorem · 270
16.4 Concerning Strong Divisibility Sequences · 271
16.5 The Quadratic Character of -1 · 273
16.6 The Infinitude of Primes Congruent to 1 Modulo Powers of 2 · 276
Exercises · 278

17 Fermat's Two-Squares Theorem · 281
17.1 Numbers Representable as a Sum of Two Squares · 281
17.2 Euler's Proof by Infinite Descent · 287
Exercises · 289

18 The Gaussian Integers · 291
18.1 Definition and Basic Properties of the Gaussian Integers · 291
18.2 Euclidean Division of Gaussian Integers · 292
18.3 The Greatest Common Divisor of Gaussian Integers · 293
18.4 Primes in the Gaussian Integers · 293
18.5 Fermat's Two-Square Theorem · 293

18.6 The Biquadratic Character of −1 · 293
Exercises · 294

19 Strong Divisibility Sequences · 295
19.1 Lucas Sequences · 295
19.2 The Rank of Apparition · 300
19.3 Primitive Sequences · 304
19.4 LCM-sequences · 305
19.5 The Lifting the Exponent Lemma · 306
Exercises · 308

20 Polynomials · 311
20.1 Polynomials with Abstract Coefficients · 311
20.2 The Factor Theorem · 314
20.3 Polynomial Congruences of Prime Moduli · 315
20.4 Lagrange's Interpolation Theorem · 318
20.5 Fixed Divisors of Integer Polynomials · 322
Exercises · 324

21 Primitive Roots · 327
21.1 Counting Elements of a Given Order Modulo a Prime · 327
21.2 Primitive Roots · 330
21.3 The Discrete Logarithm · 331
21.4 A Criterion for Congruences of Degree n · 332
Exercises · 335

22 The Moduli with Primitive Roots · 337
22.1 Primitive Roots Modulo Odd Prime Powers · 337
22.2 The Complete Characterization of Moduli with Primitive Roots · 338
22.3 Carmichael's Function · 339

23 Polynomial Congruences · 341
23.1 Polynomial Congruences of Composite Moduli · 341
23.2 Derivatives of Polynomials · 342
23.3 Hensel's Lemma · 344
23.4 The Elementary Symmetric Polynomials · 345
23.5 Reduced Polynomials Modulo a Prime · 346

24 Divisibility and Irreducibility of Polynomials · 347
24.1 Primitive Polynomials and Gauss's Lemma · 347
24.2 Euclid's Algorithm for Polynomials · 349
24.3 Irreducible Polynomials · 350
24.4 Eisenstein's Criterion · 352
Exercises · 355



25 Cyclotomic Polynomials · 357
25.1 The Primitive Factors of $x^n - 1$ · 357
25.2 The Möbius Inversion Formula for the Cyclotomic Polynomials · 360
25.3 Irreducibility of the Cyclotomic Polynomials · 360
25.4 Zsigmondy's Theorem · 361
25.5 The Infinitude of Primes Congruent to 1 Modulo n · 364
25.6 Vantieghem's Theorem · 365
Exercises · 368

26 Integer Factorizations of Polynomial Values · 369
26.1 The Reducibility of $x^n - a$ · 369
26.2 Aurifeuillean Factorizations · 369
26.3 Obstructions to the Infinitude of Primes in Lucas Sequences · 369

III **The Arithmetic of Quadratic Forms · 373**

27 Quadratic Residues · 375
27.1 Quadratic Congruences · 375
27.2 Quadratic Residues · 377
27.3 Legendre Symbols · 378
27.4 Euler's Criterion · 380
27.5 Euler's Prime-Generating Polynomial · 381
Exercises · 384

28 Quadratic Reciprocity · 389
28.1 The Quadratic Character of 2 · 389
28.2 The Statement of Quadratic Reciprocity · 394
28.3 Gauss's Lemma · 398
28.4 Eisenstein's Proof · 402
Exercises · 406

29 Primality Testing · 409
29.1 Pépin's Primality Test for the Fermat Numbers · 409
29.2 The Carmichael Numbers · 409
29.3 The Lucas–Lehmer Primality Test · 413
29.4 Pocklington's Criteria · 413
29.5 Mersenne Primes · 414
Exercises · 416

A Conjectures in Elementary Number Theory · 417
A.1 Conjectures About the Infinitude of Certain Classes of Primes · 417
A.2 Conjectures About Exceptional Primes · 419
A.3 Conjectures About Gaps Between the Primes · 420

A.4 Conjectures About Conditions for Primality · 420
A.5 Conjectures About Prime Decompositions · 420
A.6 Conjectures About Arithmetic Functions · 421
A.7 Conjectures About Diophantine Problems · 422
A.8 Conjectures About Representations of Numbers · 423
A.9 Conjectures About Iterative and Dynamical Processes · 424

References · 425

Illustrations

1.1 Euclid of Alexandria · 4
1.2 Pierre de Fermat · 6
1.3 Leonhard Euler · 8
1.4 Carl Friedrich Gauss · 10

2.1 Some Hemachandra tilings of a 1-by-19 grid · 29
2.2 Hemachandra tilings of a 1-by-5 grid · 30

3.1 A bijection · 38
3.2 Not a bijection · 39
3.3 Not a bijection · 39
3.4 Composition of bijections · 40
3.5 A bijection and its inverse · 43
3.6 Pascal's triangle · 48
3.7 The inclusion-exclusion principle · 52
3.8 Examples of stars-and-bars configurations · 54
3.9 A placement of 8 bars between 5 stars · 55
3.10 Transposition of lattice walks · 58
3.11 The Chu–Vandermonde identity · 61
3.12 Parity in Pascal's triangle · 63

4.1 A bijection on a 12-element set · 66
4.2 A cyclic set with 12 elements · 67
4.3 A cyclic-structure map from a 14-element set to a 7-element set · 68
4.4 Cyclic-structure maps · 69
4.5 The infinite cyclic set of integers · 70
4.6 The set of integers along the axis of the positive quadrant · 73



5.1 The sexagesimal notation in cuneiform script · 82

6.1 The Hasse diagram of the divisors of 120. · 97

8.1 The 12-hour clock · 112
8.2 Weaving patterns modulo 13 · 127

9.1 The Chinese Remainder Theorem · 135
9.2 Surjectivity of the map $(\mathbb{Z}/12)^\times \to (\mathbb{Z}/4)^\times$ · 138

10.1 Lattice points in a parallelogram · 142
10.2 The Farey fractions with their adjacency relation · 152
10.3 The Stern–Brocot path from 1 to $\frac{13}{18}$. · 154

11.1 A diagram in the Jackson–Johnson proof · 160
11.2 The Babylonian tablet Plimpton 322 · 162
11.3 The unit circle · 166
11.4 Stereographic projection · 168
11.5 Vieta jumps between rational points on the unit circle · 171
11.6 A forest · 174
11.7 The forest of rational points on the unit circle · 176
11.8 The tree of primitive Pythagorean triples · 178
11.9 Leonardo Pisano · 179
11.10 Differences of squares congruent to 1 modulo 24 · 180

12.1 Aubry's Theorem · 192
12.2 The curve $y^2 = x^3 - 49x$ · 201
12.3 Aubry's theorem for $x^2 + 2y^2 = 11$ and $x^2 - xy + y^2 = 7$ · 204

13.1 The sieve of Eratosthenes · 210
13.2 The 2-adic valuations of the numbers up to 15 · 221

15.1 Hemachandra wheels · 252
15.2 A bijection on a 12-element set · 255
15.3 Hemachandra wheels of order 7 · 262

16.1 Carl Friedrich Gauss · 274

17.1 Sums of two squares · 282
17.2 Thue's Lemma · 285
17.3 Thue's lemma in Lucas' weaving patterns · 286

18.1 The Gaussian integers · 292

20.1 Example polynomial obtained by Lagrange interpolation · 319

21.1 Doubling integers modulo 13 · 328

28.1 Quadratic residues and nonresidues · 391
28.2 The least absolute residue bijection · 400
28.3 Gauss's lemma · 401
28.4 Eisenstein's proof of quadratic reciprocity · 404

Introduction

Number theory is the study of numbers, particularly the natural numbers

$$0, 1, 2, \ldots$$

increasing indefinitely in increments of 1, the integers

$$\ldots, -2, -1, 0, 1, 2, \ldots,$$

and occasionally the rational numbers (fractions of integers). Its central themes include questions about divisibility, modular arithmetic, prime numbers, arithmetic functions, and finding integer solutions to equations. Additionally, number theory explores the question whether numbers can be represented in a certain form, such as a sum of two, three, or four squares, as a product or sum of primes, or as the area of a Pythagorean triangle. Paired with such representability questions is the combinatorial question of determining the number of ways a number can be so represented. More advanced branches of number theory are occasionally also concerned with obtaining quantitative bounds or other forms of approximation of certain aspects of numbers, which naturally leads to the use of other number systems, such as the real numbers, complex numbers, or p-adic numbers. However, in *elementary number theory* these explorations are primarily motivated by how these number systems relate back to the integers.

The diversity of the kinds of questions described above has led to a wealth of mathematical techniques, methods of proof, and advanced concepts, and number theory remains a very active field of study to this day. The aim of these books is to introduce some of the most fundamental ideas upon which number theory is built. Some of these ideas you might already know or have heard about: prime numbers are the building blocks of numbers; mathematical induction is a proof technique to formally prove properties of all natural numbers; and the idea that some of the most frequently occurring numbers can be arranged geometrically such as in triangles, squares, pentagons, and



so on. By asking the very simple question *How can we know or determine properties that hold for all such numbers?*, we will start our journey through the mathematical world of proof, theory building, and learn to recognize abstract mathematical concepts and witness the emergence of mathematical structures and theories that naturally flow from our basic questions about the counting numbers.

The theory of numbers is a marvelous achievement of the human mind, and so we set out on this journey with the intention to travel slowly and be amazed at every turn. We advance through the theory of numbers by asking questions. Starting with the question *What is a number?* leads us to discover that the most fruitful mode of discourse about numbers begins by specifying the *set of natural numbers*. By moving the question away from what a number is in isolation to what the set of counting numbers is, we are granted the primary method of proof for numbers, *mathematical induction*. Again, when we ask the question *What is counting?* we discover that the answer entails mathematical methods of counting. By asking the question *What are whole numbers, including negative numbers?* we discover the concept of cyclicity, which will return over and over again as the theory develops. And as before, we will be granted the principle of integer induction, by which to prove properties for all integers.

We will inspect number-theoretic phenomena from multiple perspectives. The idea of divisibility can be introduced on its own, or be studied order-theoretically or algebraically. Euclid's algorithm is a method to compute greatest common divisors, but also to solve linear equations or to even to find representations of rational numbers as continued fractions. We will follow a 19th century clockmaker from Paris in asking the very questions by which he was able to recognize that the methods leading from Euclid's algorithm to continued fractions allowed him to find gear rations best approximationg planetary periods.

The Pythagorean triples, which are integer solutions to the equation $x^2 + y^2 = z^2$, correspond to rational points on the unit circle. This correspondence relates an algebraic concept to a geometric concept. This geometry can be used to discover that there is a way of stepping from each rational point on the unit circle to one with smaller denominators. Doing so, a tree emerges which spans all the Pythagorean triples! The method by which we obtain this tree is one of which Pierre de Fermat was truly fond, the method of infinite descent. Some of the most delightful theorems can be proven with infinite descent. One example is the impossibility of solving $x^4 + y^4 = z^4$ within the positive integers. Another is a theorem of Aubry, asserting that on any circle $x^2 + y^2 = n$ on which there is a rational point, there is an integer point.

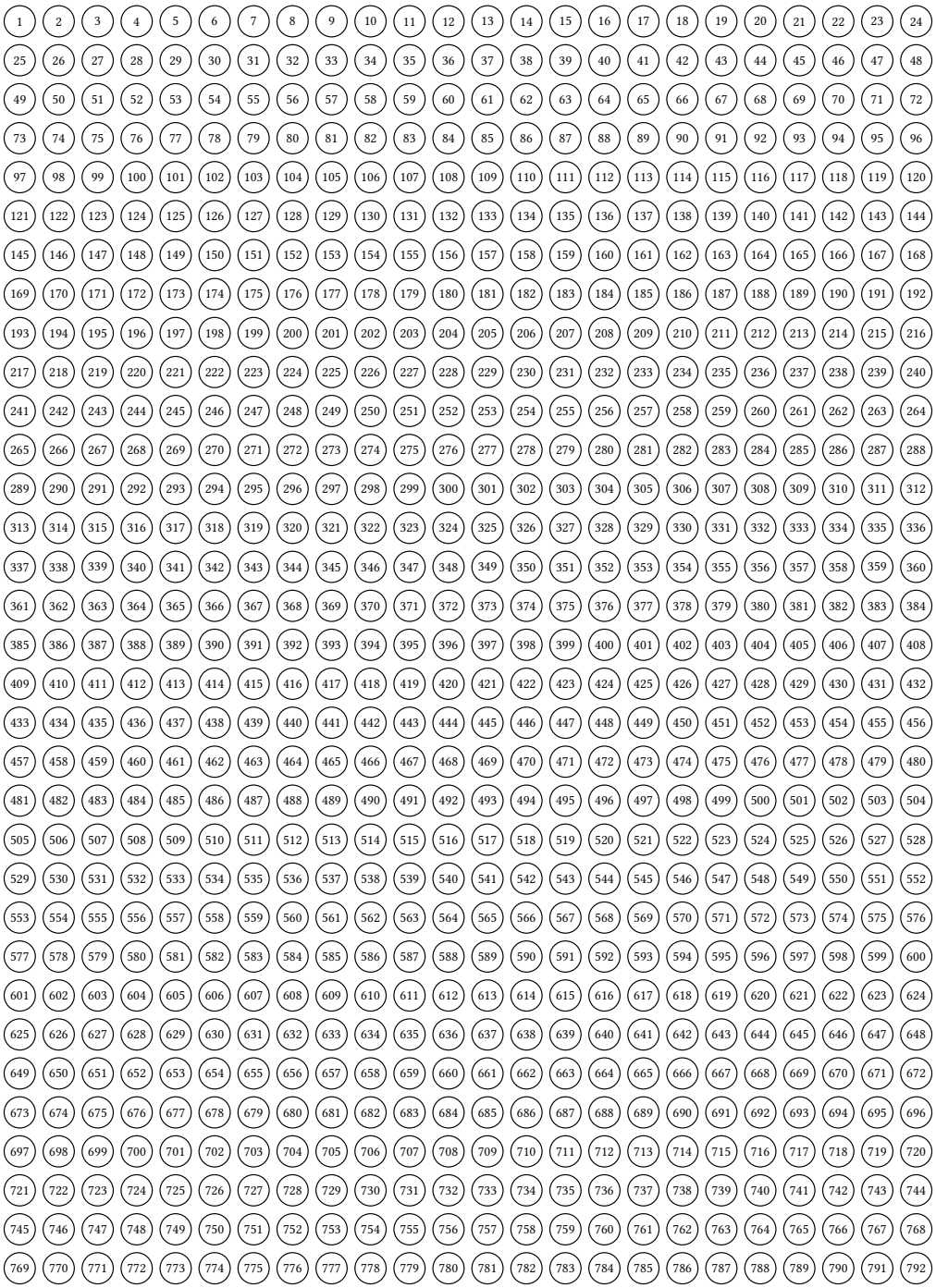
Literature

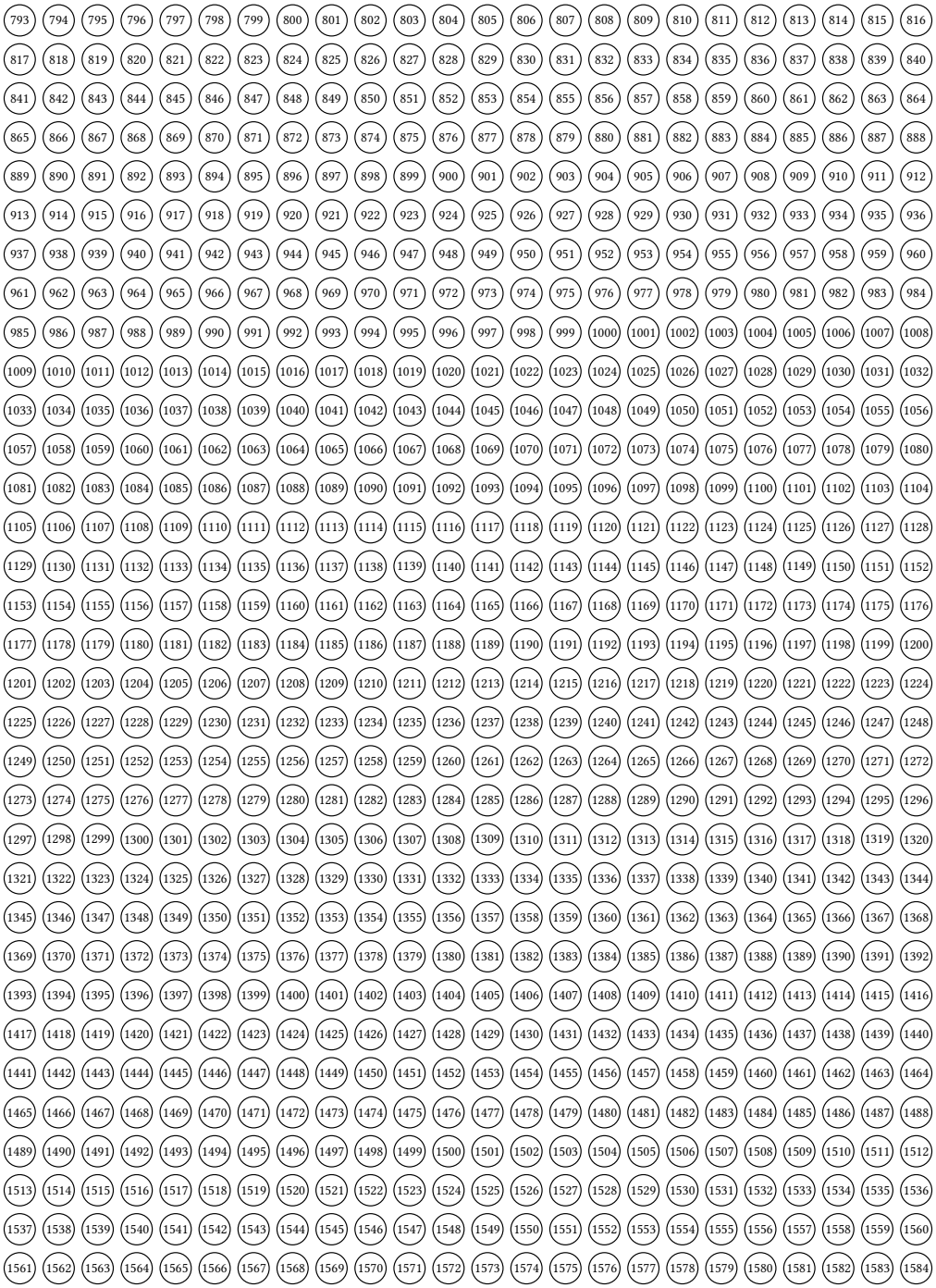
This course was originally designed to follow [AND1994] fairly closely. One distinctive feature of this book is that it presents many of the most important theorems from two perspectives: a combinatorial one and an abstract one. This dual approach helps to clarify not only why these results are true but also appreciate why they are natural and inevitable within the broader framework of mathematics.

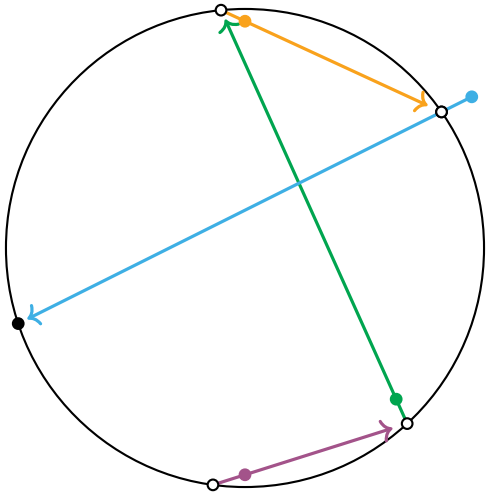
From the Fall semester of 2025 onwards, the course was redesigned to follow [Sil2012]. Silverman's book encourages the reader to explore numbers, hypothesize their properties and relations, and effectively teaches students how to generate ideas towards proving number-theoretic theorems. It is written a very accessible, conversational style, with practical examples and exercises.

There are many further excellent sources to learn number theory from. One of my personal favorites for its clarity and accessibility is LeVeque's Topics in Number Theory [LeV1956a; LeV1956b]. Both Andrews', Silverman's, and LeVeque's textbooks contain plenty of exercises, most of which are very fun.

The undisputed classic textbook on number theory, which is warmly recommended for any aspiring number theorist, is Hardy and Wright's Introduction to the Theory of Numbers [Har+2008]. This book covers all the essential topics in number theory, including elementary number theory and analytical number theory. It is more comprehensive and also provides more historical notes. The textbook of Hardy and Wright does not provide exercises, but it contains the proofs of many important facts in number theory that are stated as exercises elsewhere.


1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72
73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96
97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120
121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144
145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168
169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192
193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216
217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240
241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264
265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288
289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312
313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336
337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360
361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384
385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408
409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432
433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456
457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480
481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504
505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528
529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552
553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576
577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600
601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624
625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648
649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672
673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696
697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720
721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744
745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768
769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792


793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816
817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840
841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864
865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888
889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912
913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936
937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960
961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984
985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008
1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032
1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056
1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080
1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104
1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128
1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152
1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176
1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200
1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224
1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248
1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272
1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296
1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320
1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344
1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368
1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392
1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416
1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440
1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464
1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488
1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512
1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536
1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560
1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584



Book I

The Nature of Numbers

Chapter 1

The Nature of Mathematical Inquiry

1.1 Brief Remarks on the History of Number Theory

1.1.1 The Ancient Greek Scholars

Number theory has a long history that dates back to antiquity. While a more complete history of mathematics would include findings about earlier civilizations [BM2011], we begin our story in the Hellenistic city of Alexandria, which was founded by Alexander the Great in 331 BCE on the Mediterranean coast of Egypt. After the death of Alexander the Great in 323 BCE, Egypt came under the control of his general Ptolemy, who first ruled as satrap and became king of Egypt in 305/304 BCE [Fra1972; Höl2001]. During the early Ptolemaic period, the city of Alexandria saw great development, such as the founding of the Mouseion, a state-supported research and teaching institution in which also the Library of Alexandria was housed [Cas2001]. This is the intellectual milieu in which Euclid of Alexandria likely lived, taught, and wrote one of the most influential manuscripts in the history of mathematics, the Elements [Euc2015; Hea1981]. In this monumental work, which is conventionally dated to around 300 BCE, Euclid systematically derived several key results in geometry and number theory from a small number of postulates. These include the infinitude of primes and the algorithm for finding the greatest common divisor, which bears his name. The 5th-century mathematical commentator Proclus reports in his commentary



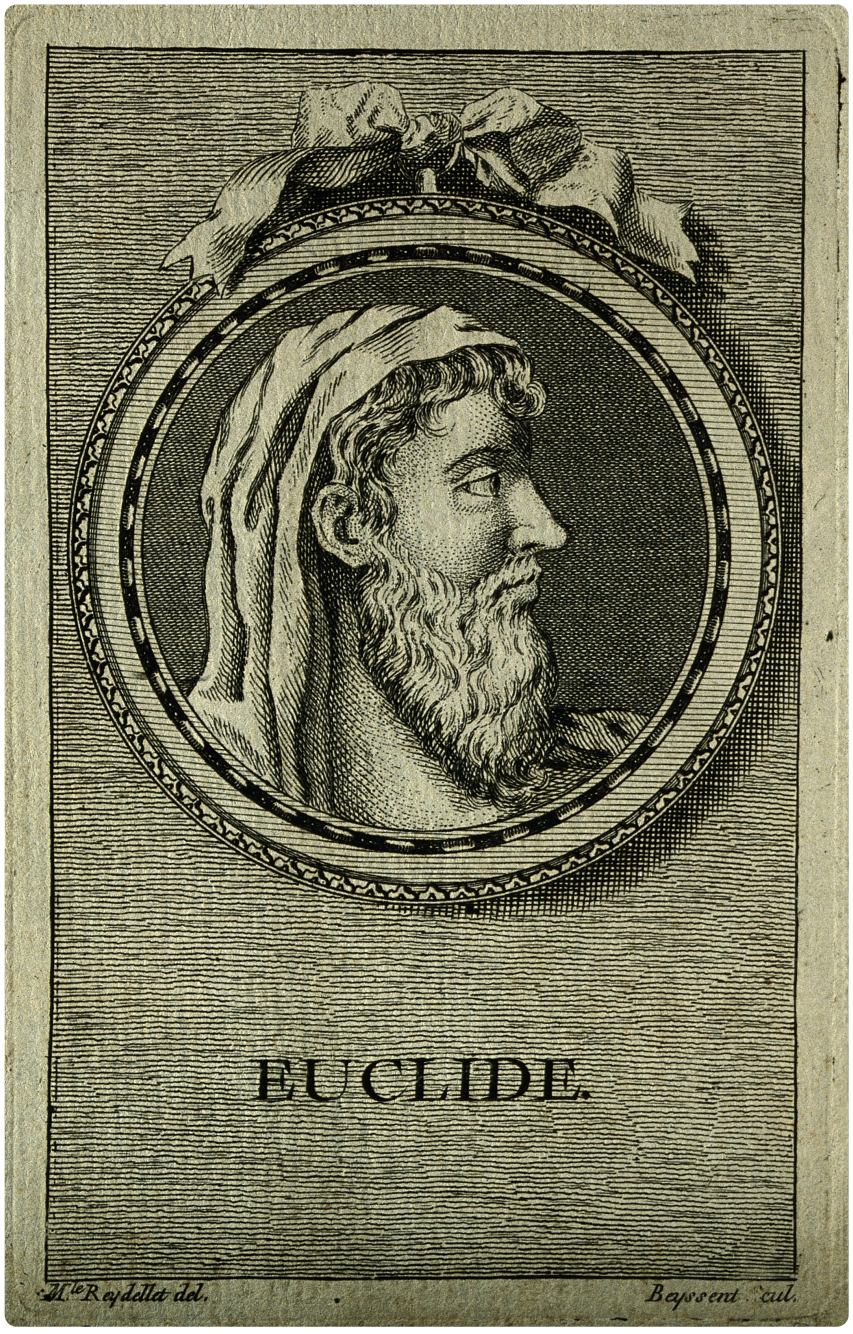


Figure 1.1: Euclid of Alexandria. Line engraving by S. Beyssent after Mlle. C. Reydell.

on Euclid's Elements that king Ptolemy came to Euclid with the question whether there is a quicker way of learning geometry [Pro1992]. We can easily imagine the king recognizing the importance of Euclid's axiomatic approach but struggling with Euclid's careful derivations, and surely his royalty should not have to work through all thirteen books of the Elements. To which Euclid replied with the famous apothegm: *"There are no royal roads to geometry."*

Around 250 CE, the Greek mathematician Diophantus of Alexandria wrote his Arithmetica [Dio1910], which focused on solving equations with integer coefficients in one or multiple unknowns. This 13-volume work is often considered the first comprehensive treatment of algebra, though Diophantus relied on rhetorical descriptions rather than modern algebraic notation. Only six of the original volumes have survived, but they profoundly influenced later mathematicians.

The works of Euclid and Diophantus were preserved and studied by scholars in the Byzantine Empire, such as Theon of Alexandria and his daughter Hypatia. They added commentaries that clarified and expanded upon the original text.

During the Islamic Golden Age, scholars like Al-Khwarizmi, Ibn al-Haytham, and Omar Khayyam preserved and expanded upon the works of Euclid and Diophantus. Al-Khwarizmi's work, especially his Kitab al-Mukhtasar fi Hisab al-Jabr wal-Muqabala from which the term "algebra" originates, introduced systematic methods for solving linear and quadratic equations. He used rhetorical algebra, like Diophantus, but began a transition toward symbolic representation by relying on consistent terminology for operations and equations.

After the invention of the printing press, Erhard Ratdolt, a German printer based in Venice, produced the first printed edition of the Elements in 1482. This edition included mathematical diagrams and marked an important step in the dissemination of Euclid's work. The first printed edition of Diophantus' Arithmetica was published in 1575 by Wilhelm Xylander, a German mathematician. The printing was done in Basel, Switzerland, which was a major hub for academic publishing at the time. By the time of Pierre de Fermat in the 17th century, both the Elements and Arithmetica had become essential texts for mathematicians across Europe, influencing the development of number theory and inspiring Fermat's pioneering discoveries.

1.1.2 Mathematics, Astronomy, and Poetry in Ancient India

We could not move forward with the story of the greatest mathematical achievements without first turning our attention to the scholarly traditions of ancient India.

1.1.3 Pierre de Fermat

Pierre de Fermat (1607–1665) is often considered the founder of modern number theory [Mah1994; Wei1984]. He was a contemporary of Blaise Pascal and Father Marin Mersenne, both of whom he corresponded with, and also of Galileo Galilei. He wrote a manuscript titled Éléments de Géométrie, which served as an extension and commentary on Euclid's Elements. In this work, he sought to modernize Euclid's geom-





Figure 1.2: Pierre de Fermat. Engraving in Oeuvres Mathématiques Diverses.

etry by applying the emerging methods of algebra and analytic geometry to classical geometric problems.

Fermat made many groundbreaking discoveries in the theory of numbers. Among his most influential discoveries is *Fermat's Little Theorem*, which states that if p is a prime number, then

$$a^p \equiv a \pmod{p}.$$

This theorem is key to many further results in modular arithmetic, and has modern applications in RSA encryption. Fermat also came up with the method of *infinite descent*, which allows one to show that a certain equation or proposition cannot hold by showing that it would lead to an infinite descending sequence of positive integers. Fermat was very fond of this method, and used it brilliantly to prove some of his most profound claims. For instance, the case $n = 4$ of *Fermat's Last Theorem*, which states that there are no positive integers x, y, and z such that $x^4 + y^4 = z^4$ is proven using infinite descent. In order to prove this fact, Fermat also showed that the area of a Pythagorean triangle is never a perfect square. Fermat is furthermore famous for the *Two-Squares Theorem*, which states that any prime $p \equiv 1 \pmod{4}$ can be written uniquely as a sum of two squares, up to ordering of the summands, and that primes $p \equiv 3 \pmod{4}$ cannot be written as a sum of two squares. Fermat also claimed that any number can be written as the sum of at most three triangular numbers, as the sum of four squares, as the sum of five pentagonal numbers, and so on, but he did not indicate how these claims might be proven. The case of the triangular numbers is now known as Gauss's *Eureka Theorem*, the *Four-Squares* theorem was proven by Lagrange, and Cauchy proved the general theorem asserting that any number can be expressed as the sum of at most n n-gonal numbers.

Fermat also made several famous conjectures. He conjectured that the equation $x^2 - Ny^2 = 1$ has infinitely many solutions for any positive non-square integer N. Euler made a significant advance to this problem by proving it for specific values of N. The general form of the solution to equations of the form $x^2 - Ny^2 = 1$ was found later by Legendre and Lagrange.

Finally, Fermat famously asserted that there could be no three positive integers x, y, and z such that the equation

$$x^n + y^n = z^n$$

holds, when $n \geq 3$. This statement is now known as *Fermat's Last Theorem*. He claimed to have a "truly marvelous proof", but that the margin of his copy of Arithmetica was too small to contain it. His assertion, known as *Fermat's Last Theorem*, captivated mathematicians for centuries. It was finally proven in 1995 by Andrew Wiles, about 350 years after Fermat made his famous note in the margin, using advanced techniques from algebraic geometry and modular forms. Wiles's achievement is considered one of the most remarkable milestones in the history of mathematics.



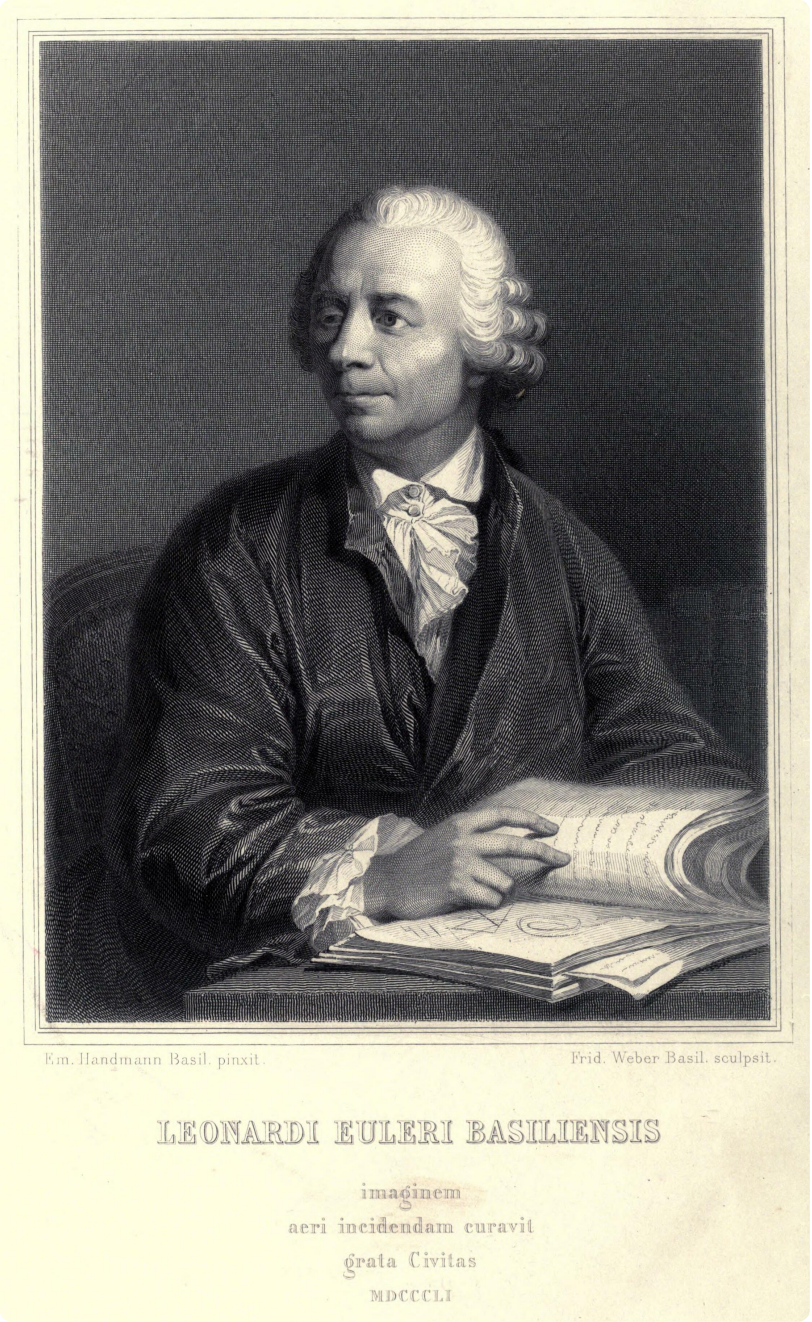


Figure 1.3: Leonhard Euler. Engraving by Friedrich Weber.

1.1.4 Leonhard Euler

While Fermat laid the groundwork for modern number theory, we should mention that the concept of *function* hasn't been crystallized until Leibniz coined the term in 1673, using it to describe quantities related to curves, such as slopes, tangents, and areas. Bernoulli played a significant role in expanding the idea of functions. He used the term explicitly in 1718, describing it as a quantity dependent on another variable. Euler provided the first modern definition of a function in his Introductio in Analysin Infinitorum (1748) [Eul1988]. He emphasized that functions could include both algebraic (e.g., polynomials) and transcendental forms (e.g., trigonometric and exponential functions). Peter Gustav Lejeune Dirichlet was the first to define functions abstractly as a correspondence between two sets, removing the requirement for expressions or formulas. This abstraction was a key insight for the theorem that we now know as *Dirichlet's theorem*: Every arithmetic progression

$$a,\ a+b,\ a+2b,\ a+3b,\ \ldots$$

in which $b > 0$ and a is coprime to b, contains an infinitude of primes. Dirichlet proved his theorem in 1837, more than 150 years after Leibniz first coined the term of function.

Euler's Introductio in Analysin Infinitorum marked the beginning of *analytical number theory*. As we mentioned before, Euler defined functions here and established the notation $f(x)$ of a function applied to its variable, which we still use today. He derived the famous formula for complex exponentials

$$e^{ix} = \cos(x) + i\sin(x).$$

This identity connects the exponential function, trigonometric functions, and the imaginary unit. The Riemann zeta function $\zeta(s)$ makes its first appearance here in a complex variable s, and he derived the celebrated *product formula*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\,\text{prime}} \frac{1}{1-p^{-s}},$$

which holds when $\mathrm{Re}(s) > 1$. More generally, Euler explored infinite series and products. The *Basel summation formula*

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

was first proven here, which was one of Euler's most celebrated achievements. Euler was keen to explore the connection between geometry and analysis, and in Introductio in Analysin Infinitorum, he advanced the idea that the study of functions and infinite series could provide new insights into geometric problems. He showed how techniques from analysis could be used to solve problems in geometry and vice versa, fostering the development of applied mathematics.





Figure 1.4: Carl Friedrich Gauss. Painting by Christian Albrecht Jensen.

1.1.5 Johannes Carl Friedrich Gauss

Building on the work of Euler, Gauss began using the properties of the zeta function and other analytic methods to investigate the distribution of the primes. His seminal work Disquisitiones Arithmeticae [Gau1986] is often considered the starting point of the study of the distribution of primes, ultimately leading up to the *Prime Number Theorem*. Gauss conjectured that the number $\pi(n)$ of primes below a number n satisfies the asymptotic law

$$\pi(n) \sim \frac{n}{\log(n)}.$$

This conjecture was proved independently by Jacques Hadamard and Charles Jean de la Vallée Poussin. Furthermore, Gauss laid the foundation for modular arithmetic, and proved the celebrated law of quadratic reciprocity, which tells us when a quadratic equation modulo an odd prime number is solvable. More precisely, it states that for odd primes p and q, if $q \equiv 1 \pmod 4$ then the congruence $x^2 \equiv p \pmod q$ is solvable if and only if the congruence $x^2 \equiv q \pmod p$ is solvable.

A brief remark on the interesting etymology of the word theorem is in order. The English word *theorem* ultimately derives from the Ancient Greek θεώρημα (theōrēma), literally "that which is seen", and by usage in classical philosophy as an "object of contemplation". The verb θεωρεῖν (*theōreîn*, "to observe, examine") and the agent noun θεωρός (*theōrós*, "spectator") are close relatives, and ultimately give us both 'theorem' and 'theory'.

In Euclid's Elements, specifically through the careful editorial work and commentaries of the Byzantine scribes, we start seeing the label *theōrēma* for statements that require deductive proof, in contrast to the "givens" (ὑπόθεσις, hypóthesis) and "proof" (ἀπόδειξις, apódeixis). However, the fixed label *Theōrēma* for such statements emerges more clearly in Medieval translations into Late Latin and Middle French of the Elements, through the editorial adjustments made by his copyists. The Late Latin word *theorema* and the Middle French word *théorème* both retained the meaning "proposition that is to be proved".

Euclid's Elements was first translated into English by Sir Henry Billingsley in 1570, who was mayor of London at the time, with a preface written by John Dee. This Billingsley–Dee edition of Euclid's Elements established *theorem* in the English language as a word meaning "proposition that is to be proved". Over the ensuing centuries, the word theorem came to mean exclusively a mathematical assertion proven from axioms, definitions, and previously established theorems.

1.1.6 Contemporary Mathematics

So far, we have covered some of the most celebrated advances in humanity's understanding of numbers up to the early 19th century. Mathematics has made rapid progress since then. Bertrand's postulate, which asserts that there is always at least one prime p between n and $2n$, for any $n > 1$, was proven by Pafnuty Chebyshev in 1852, and Ben



Green and Terence Tao proved in 2004 that the sequence of prime numbers contains arbitrarily long arithmetic progressions.

The 20th century saw the emergence of the Langlands program, a far-reaching research program that aims to connect number theory, representation theory, and algebraic geometry. With the contributions of mathematicians like André Weil, Robert Langlands, and many others, the program has shaped much of the direction of modern research in number theory and its applications to other branches of mathematics.

Even today fundamental concepts such as sets and functions continue to evolve. We live in an era of digital computation, with tools far beyond the reach of Fermat, Euler, and Gauss, where essentially all recorded knowledge is readily available to almost anyone. This computational revolution has also given rise to powerful tools like proof assistants; that is, computer programs designed to construct and formally verify mathematical proofs. Since proof assistants are programming languages, they are often based on type theory rather than set theory, slightly changing the way mathematics is done. Functions in type theory are even more general than Leibniz, Euler, and Dirichlet envisioned: unlike in set theory where functions are a specific kind of relations between sets, functions in type theory are primitive entities satisfying certain rules for evaluation, and they have an extra dependency built in, allowing types of their outputs to depend on the input. Proof assistants are being used with great success to formally verify advanced mathematical theorems. Georges Gonthier formally verified the Four Color Theorem and the Odd Order Theorem, and Tom Hales verified Kepler's conjecture about sphere packings. An effort led by Kevin Buzzard aims to formally verify Fermat's Last Theorem. Meanwhile, through rapid advances in the field of artificial intelligence, an eager AI company has outpowered his team and was able to generate such a formal verification.

Number theory continues to be one of the most active and fruitful areas of mathematical research, all of which started simply with counting on ten fingers.

1.2 The Concept of Number Through History

Many people are familiar with numbers through everyday experiences like counting, measuring, or comparing quantities. From a young age, we develop an intuition about how numbers behave. For example, one of the things we quickly learn about numbers is that it does not matter in which order we add them. Given two numbers a and b it is always true that $a + b = b + a$. Truths such as this one seem so self-evident that we might be tempted to just accept them. However, for a rigorous mathematical theory we need to be more careful. Mathematicians require proofs. Checking a property for every number up to a hundred, a million, or even 10^{27} might confirm a pattern, but infinitely many numbers remain beyond such finite checks. Mathematical proofs, on the other hand, are logical arguments that establish beyond any possibility of doubt why certain properties hold universally for all numbers, or at least for precisely defined sets of numbers. To reason about all natural numbers at once, we need formal principles that extend beyond empirical observation and anecdotal evidence. In order to discover

such reasoning principles, we need to find out first what the natural numbers really are, a question with a rich and very interesting history.

Although natural numbers arise from counting, the notion of number is not inherently linked to any particular collection of entities being counted. Scholars in the Pythagorean tradition were among the first to articulate this insight. Nicomachus emphasized in his Introduction to Arithmetic the concepts of *monad* and *dyad* for the totality of all things that come in one or two units [Nic1926]. Nicomachus ascribed divine properties to the monad, or unity: "*It generates itself without beginning, without end, and appears to be the cause of enduring, as God in the realm of physical actualities is in such manner perceived of as a preserving and guarding agent of nature*". Nicomachus drew strong parallels between the monad and the concept of sameness, and dually between the dyad and the concept of otherness. He also emphasized that numbers were composed of monads. In other words, the monad is the source of all numbers. Although mathematicians do not ascribe divine properties to numbers anymore, we see here the emergence of some important ideas. The first is that all numbers are generated from the monad, that is, unity. The second idea is to connect unity with sameness. The idea that all things equal to a given object form a unit, or a singleton, anticipates a fundamental principle of equality. However, we shall forego the interesting digressions that we could make about equality and focus our attention on the concept of number.

Euclid takes a more abstract point of view, in which the concept of number is defined without relating it to the divine conception of the monad. For Euclid, a *unit* is the conceptual principle by which an individual object is identified as one, and a *number* is a multitude composed of such units in a discrete fashion [Euc2015]. In other words, the concept of unit captures the notion of oneness, but this is distinct of the number 1 itself. Both Nicomachus's and Euclid's views on the concept of number were highly influential throughout late antiquity and the Middle Ages, particularly through Boethius's Latin rendition of Nicomachus's Introduction to Arithmetic [KP2012] and Adelard of Bath's translation of Euclid's Elements [Cla1953].

While Pierre de Fermat is regarded the founder of modern number theory, he did not write extensively on the philosophy of mathematics. Nevertheless, certain themes in his correspondence and work show a clear orientation. For him, mathematics is about truths intrinsic to numbers. Numbers were the object of exact reasoning. He emphasized that *induction*, by which mathematicians up to the early 19th century understood experimental verification, was insufficient to establish universal truths of numbers. Nowadays, this historical use of the word induction is sometimes called *empirical induction*. Among Fermat's lasting contributions was his method of infinite descent, a method of proof by contradiction in which one shows that any supposed solution would lead to an ever-decreasing sequence of natural numbers, which is impossible.

With Euler, we witness a significant conceptual expansion. In his Elements of Algebra, Euler extended the notion of number beyond the natural and rational to encompass negative numbers, irrationals, complex numbers, and even infinite series. He was among the first to conjecture that constants like e and π are transcendental;

that is, not the roots of any algebraic equation with rational coefficients. For Euler, numbers were entities governed by formal laws, irrespective of whether they corresponded to geometric magnitudes. Euler's broadening of the concept of numbers, and his use of analytic methods would eventually spark debates about the foundations of mathematics and the logical principles underlying mathematical truth.

In the 19th century, the nature of mathematics itself began to change. The emergence of non-Euclidean geometry was a challenge to the status of Euclid's Elements as the de facto foundation of mathematics, and Weierstrass's discovery of continuous, nowhere differentiable functions meant that one could not simply rely on intuition in the study of calculus and analytics. Furthermore, with Galois's use of symmetries in order to show that there are quintic equations had no solutions expressible in terms of radicals, abstract algebra became a prominent subject of mathematics with algebraic objects that have little in common with numbers except for a few formal laws. These discoveries underscored the need for a more solid foundation of mathematics, ultimately resulting in the emergence of Frege's logicism and set theory.

Nevertheless, the question of formally defining the set of natural numbers was left mostly unexplored until the second half of the 19th century. Even as late as 1886, Kronecker is quoted as proclaiming that "God created the integers, all else is human work" [WEB1893], not helping the cause of finding a definition of the natural numbers. In *Was sind und sollen die Zahlen?* (translated to English as *What are numbers and what should they be?*), Dedekind was the first to formally define the set of natural numbers. His idea was that the number zero and the successor function together should be sufficient to describe all the natural numbers. He formalized this idea in 1888 by specifying that the set of natural numbers is a *simply infinite set*, meaning that there is a one-to-one function $S : \mathbb{N} \to \mathbb{N}$ such that every element of $\mathbb{N}$ can be reached by iteratively applying S to a distinguished element 0, which is not itself a value of S [DED1888]. Dedekind showed furthermore that all simply infinite sets are similar to each other; in modern termimology, he showed that all simply infinite sets are *isomorphic*. Thus, Dedekind's definition was structural in nature, in the sense that it captured the structure a set must possess in order for it to be considered a set of natural numbers.

Not much later, Giuseppe Peano arrives at a very similar definition of the set of natural numbers. In ARITHMETICES PRINCIPIA NOVA METHODO EXPOSITA he established the set of natural numbers as a set satisfying a small number of axioms, the celebrated *Peano axioms* [PEA1889]:

(i) For any two natural numbers x and y we have

$$(x = y) \Leftrightarrow (S(x) = S(y)).$$

(ii) There is no natural number x such that $S(x) = 0$.

(iii) For any set A, if $0 \in A$ and if for any natural number x we have $(x \in A) \Rightarrow (S(x) \in A)$, then every natural number is in A.

The first axiom establishes that the successor function S is one-to-one. This means that every natural number is the successor of at most one natural number. The number 0 itself is, in the setup of Dedekind and Peano, not a successor by the second axiom. The third axiom encodes *mathematical induction*. The notation $x \in A$ means that x is an element of A, or in other words that A contains the element x. Thus, Peano's third axiom asserts that if A is a set containing 0 and containing the successor of every element it contains, then it contains all the natural numbers. While the similarity between Dedekind's and Peano's approach is clear, we note Dedekind's approach was structural, set-theoretic, and intended for a philosophical audience, Peano's approach was formal, logical, and symbolic.

A common alternative way of formulating mathematical induction is as follows. Given any property $P(n)$ expressing a condition of an arbitrary natural number n, in order to prove that $P(n)$ is true for all n it suffices to prove that:

(i) The property $P(0)$ is true.

(ii) For all n, if the property $P(n)$ holds then the property $P(n+1)$ holds.

Mathematical induction formalizes the idea that every natural number is either 0 or it is the successor of a previous natural number, and that no proper subset of the natural numbers that contains 0 is closed under successors. Proving a property for all natural numbers therefore breaks down in two cases: The **base case** in which we prove that $P(0)$ is true, and the **inductive step** where we prove that $P(n+1)$ is true provided that $P(n)$ is true.

While proofs by mathematical induction go back to antiquity, the first to formulate the mathematical induction abstractly as a method of proof was Blaise Pascal in his Traité du triangle arithmétique [Pas1665]. In this work, he studied the triangle of numbers now named after him. In a passage on the ratios of two horizontally adjacent binomial coefficients he wrote:

> *Quoy que cette proposition ait une infinité de cas, j'en donneray une démonstration bien courte, en supposant deux lemmes.*
>
> *Le 1. qui est évident de soy-mesme, que cette proportion se rencontre dans la seconde base; car il est bien visible que φ est à σ comme 1 à 1.*
>
> *Le 2. que si cette proportion se trouve dans une base quelconque, elle se trouvera nécessairement dans la base suivante.*

Notice, however, that Pascal did not yet use the term *induction* for this method of proof. As we mentioned earlier, mathematicians of his time understood the word induction to refer to the empirical method of extrapolating patterns from finite data. Augustus De Morgan was the first to coin the term *mathematical induction* in 1838, albeit somewhat incidentally [Caj1918]. In his article on this topic in the Penny Cyclopedia he coined the term *successive induction*, but he used the phrase *mathematical induction* in a concluding remark [De 1838]. Through the efforts of Dedekind and Peano, the induction principle has evolved from a method of proof to a defining principle for the set of natural numbers.



By the turn of the 20th century, set theory, as pioneered by Georg Cantor and developed further by Richard Dedekind and others, was increasingly seen as a promising foundation for mathematics. However, the emergence of paradoxes around 1900 prompted efforts to axiomatize set theory. Beginning with Zermelo's axioms in 1908 and refined into the Zermelo–Fraenkel system in the 1920s, set theory gradually became the de facto foundational framework for modern mathematics. This raises the question whether the natural numbers can be defined within Zermelo–Fraenkel's set theory. Von Neumann gave an elegant set-theoretic definition of the natural numbers: The number 0 was defined as the empty set $\emptyset$, the number 1 was defined as the set $\{0\}$ containing the empty set, the number 2 was defined as the set $\{0, 1\}$, and so on:

$$0 := \emptyset, \quad 1 := \{\emptyset\}, \quad 2 := \{\emptyset, \{\emptyset\}\} \quad 3 := \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \quad \dots$$

However, Von Neumann's definition is not the only possible definition. One can also define

$$0 := \emptyset, \quad 1 = \{\emptyset\}, \quad 2 := \{\{\emptyset\}\}, \quad 3 := \{\{\{\emptyset\}\}\}, \quad \dots$$

These two definitions are clearly distinct, since $0 \in 2$ is true in Von Neumann's definition but false in the latter definition. This raises the question, if Zermelo–Fraenkel set theory is to be the foundation of mathematics, then what is *the* set of natural numbers? Paul Benacerraf argued in his famous essay *What numbers could not be?* that the essence of the set of natural numbers is its structure, much like Dedekind had already argued almost a century before him [BEN1965].

While mathematicians often prefer to work with sets, computer scientists might prefer to work with types. The distinction is merely that of the logical framework being used: Most mathematicians rely on the Zermelo–Fraenkel set theory, while computer scientist rely on programming languages that often have a type theory in its foundation. Theorem proving in computer programs called *proof assistants* is rapidly becoming a more essential mathematical activity for students and researchers alike. However, many of the most popular proof assistants are based on type theory, in which collections of mathematical objects are called types.

Modern mathematics is increasingly formalized in computer programs called *proof assistants*. There are many libraries of formalized mathematics in active current development, containing vast amounts of mathematics from a wide variety of mathematical subjects. However, the foundation of most such systems is not set-theoretic. Instead, many proof assistants use *dependent type theory* as their foundational language, which was developed in the 1970s and 80s by Per Martin-Löf. Both sets and types are collections of abstract objects often referred to as **elements**, but the formalisms by which they are studied are different in character, thus justifying the different names *sets* and *types*. The way the natural numbers are introduced in type theory is also slightly different. Whereas the induction principles of Dedekind and Peano establish the inclusion of the set of natural numbers into other sets, the natural numbers in type theory come equipped with a *structural induction principle* that allows one to define functions out of the natural numbers. Similar to the previous definitions, the type of natural numbers comes equipped with a distinguished element 0 and a successor function. The

structural induction principle states that in order to define a function $f(n)$ taking as input a natural number n and as output an element of a set A_n, possibly depending on n, one has to specify:

(i) an element $a_0 \in A_0$, and

(ii) a function $h_n : A_n \to A_{n+1}$ for every natural number n.

The function f obtained in this manner satisfies the equations

$$f(0) = a_0,$$
$$f(n+1) = h_n(f(n)).$$

From a type-theoretic perspective, there is no need to assume that the successor function is a one-to-one function or that 0 is not a successor. Indeed, these two axioms can be derived from structural induction.

We have thus seen that the concept of number has evolved over thousands of years of mathematical effort and underwent refinements up to the second half of the 20th century. We will follow the type-theoretic approach, and take a structural approach to the subject. Thus, the set of natural numbers contains an element 0 and a successor function, and together they generate all the natural numbers in the sense that functions out of the natural numbers can be uniquely specified with recursive definitions. Similarly, we will give in this course structural accounts of the set $\mathbb{Z}$ of all integers, and the set $\mathbb{Q}$ of rational numbers. In the remainder of this chapter, we will explore from a practical perspective what induction and recursion mean, and how to use them.

1.3 Mathematical Language



Chapter 2

Mathematical Induction

2.1 Recursion and Induction

When we say that the natural numbers are the numbers 0, 1, 2, ..., we really mean that they are generated from 0 and the successor function S given by $n \mapsto n + 1$.

As we saw in §1.2 on the history of the concept of number, the definition of the set of natural numbers centers on precisely expressing the idea that all numbers are generated from 0 and a successor function. Several ways of expressing this idea have been proposed through history: Dedekind's simply infinite sets, Peano's axioms, and the structural induction principle of type theory. We will follow the type-theoretic approach.

Definition 2.1.1. The set $\mathbb{N}$ of **natural numbers** is a set equipped with a distinguished element 0 called **zero** and a **successor function** $S : \mathbb{N} \to \mathbb{N}$, which we also denote by the map $n \mapsto n + 1$, satisfying the following principle of **structural induction**: For any family of sets A_n indexed by the natural numbers, equipped with

(i) an element $a_0 \in A_0$, and

(ii) for each n, a function $h_n : A_n \to A_{n+1}$,

there is a function f taking a natural number n as input and returning a value $f(n)$ in the set A_n, satisfying the following two equations:

$$f(0) = a_0,$$
$$f(n + 1) = h_n(f(n)).$$

REMARK 2.1.2 (The method of structural induction). When defining a function by structural induction, there are two subtasks: First, we have to specify the value of $f(0)$ by specifying an element of the set A_0, and second, we have to specify how each potential value of f at n can be used to obtain the value of f at $n+1$. This second task is performed by defining a function h_n from A_n to A_{n+1}, so that if $f(n)$ is determined, then we can determine $f(n+1)$ by applying h_n to $f(n)$.

The two equations that the function f in the structural induction principle satisfies are called the **computation rules**. By these computation rules we can present definitions by structural induction in the following shorthand form:

$$\begin{aligned} f(0) &:= a_0, \\ f(n+1) &:= h_n(f(n)). \end{aligned}$$

An important special case of structural induction, which will serve as our first example and by which we will obtain many further examples of recursively defined functions, is to iterate a function $f : X \to X$ acting on a set X. The family of sets (A_n) used in this application of structural induction is defined by $A_n := X$ for each n (so it is not dependent on n), and we define the function $h_n : X \to X$ by $h_n := f$ (again, not dependent on n).

DEFINITION 2.1.3. Consider a function $f : X \to X$. For each natural number n, we define the nth **iteration** f^n of f by

$$\begin{aligned} f^0(x) &:= x, \\ f^{n+1}(x) &:= f(f^n(x)). \end{aligned}$$

In other words, the 0th iteration of f is the **identity function**, which leaves all elements untouched, and the $(n+1)^{\text{st}}$ iteration of f is obtained by applying f once more to the values of the nth iteration of f.

REMARK 2.1.4 (A choice made in the definition of iterates). Notice that we made a choice in the definition of the $(n+1)^{\text{st}}$ iteration of f. We could have defined it alternatively by $f^{n+1}(x) := f^n(f(x))$. In order to prove that the identity

$$f^{n+1}(x) = f^n(f(x))$$

indeed holds we will need mathematical induction, which can be derived from structural induction.

DEFINITION 2.1.5. The principle of **mathematical induction** asserts that for any predicate $P(n)$—that is, for any property of numbers depending on n—if

(i) the proposition $P(0)$ holds, and

(ii) for any n, if the proposition $P(n)$ holds then the proposition $P(n+1)$ holds,

then $P(n)$ is true for all n.

Remark 2.1.6 (The method of mathematical induction). Proofs by induction proceed in the following steps, each of which is a necessary aspect of an inductive proof:

(i) First, announce that your proof proceeds by induction and identify the property $P(n)$ that you are about to prove. The goal of an induction proof is always to prove that $P(n)$ is true for all n.

(ii) Next, prove the **base case**. In other words, show that $P(0)$ is a true proposition. While this step is often trivial, it is a necessary and essential part of an induction proof.

(iii) Finally, for the **inductive step**, write down the exact **induction hypothesis**, namely the property $P(n)$, and the exact goal of the inductive step, namely the property $P(n+1)$. Then use the induction hypothesis to prove that $P(n+1)$ then also holds.

After these steps the proof that $P(n)$ holds is complete. Using induction we can prove, for example, that the identity $f^{n+1}(x) = f^n(f(x))$ holds for every n.

Proposition 2.1.7. *Consider a function $f : X \to X$ on a set X, and let n be a natural number. Then we have*

$$f^{n+1}(x) = f^n(f(x))$$

for all $x \in X$.

Proof. The proof is by induction on n. In the base case, we must show that

$$f^1(x) = f^0(f(x)).$$

By our definition of $f^n(x)$, we have that $f^1(x) = f(f^0(x))$, and we have $f^0(x) = x$, so that

$$f^1(x) = f(f^0(x)) = f(x).$$

Likewise, we have $f^0(f(x)) = f(x)$. Therefore, it follows that both $f^1(x) = f(x)$ and $f^0(f(x)) = f(x)$, which proves the base case.

In the inductive step, we assume as our inductive hypothesis that the equality

$$f^{n+1}(x) = f^n(f(x))$$

holds for every $x \in X$. Our goal is then to show that

$$f^{n+2}(x) = f^{n+1}(f(x)).$$

Recall from the definition of iteration that $f^{n+2}(x) = f(f^{n+1}(x))$. Since we have assumed as our inductive hypothesis that the equality $f^{n+1}(x) = f^n(f(x))$ holds, we can continue our calculation as follows:

$$f^{n+2}(x) = f(f^{n+1}(x)) = f(f^n(f(x))).$$

To finish the proof, we note that $f^{n+1}(y) = f(f^n(y))$. Choosing $y := f(x)$, we obtain that $f^{n+1}(f(x)) = f(f^n(f(x)))$. Thus we have shown the two equalities

$$f^{n+2}(x) = f(f^n(f(x))) \qquad \text{and} \qquad f^{n+1}(f(x)) = f(f^n(f(x))),$$

so the inductive step is complete. □

2.2 Addition of Natural Numbers

Iteration of functions is a basic operation that can be used to define many further operations. Here we will define addition by iteratively adding 1 to a number m. For example, the number $2+3$ can be defined as the third successor of 2, so that the equality $2 + 3 = S(S(S(2)))$ holds, which is equal to $S(S(3))$, which is equal to $S(4)$, which is equal to 5.

DEFINITION 2.2.1. The **addition operation** $+ : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$ is a binary operation defined by iterating the successor function S:

$$m + n := S^n(m).$$

In other words, $m + n$ is the nth successor of m.

REMARK 2.2.2. Since we defined addition in terms of iterated successor, and the iterated successor function itself is defined by structural induction, the addition function satisfies two computation rules:

$$m + 0 = m,$$
$$m + (n + 1) = (m + n) + 1.$$

These are the only equalities given to us. Other equalities, such as the equalities

$$0 + n = n,$$
$$(m + 1) + n = (m + n) + 1,$$

and other familiar laws of addition are also true, but require proof.

PROPOSITION 2.2.3. *For any two natural numbers m and n we have*

$$0 + n = n,$$
$$(m + 1) + n = (m + n) + 1.$$

PROOF. Both equalities are proven by induction on n. For the base case of the first equality, note that the equality $0 + 0 = 0$ holds by definition. For the inductive step, assume that $0 + n = n$. Then we have

$$0 + (n + 1) = (0 + n) + 1 = n + 1.$$

For the base case of the second equality, note that the equalities $(m + 1) + 0 = m + 1 = (m+0)+1$ hold by definition. For the inductive step, assume that $(m+1)+n = (m+n)+1$. Then we have

$$(m + 1) + (n + 1) = ((m + 1) + n) + 1 = ((m + n) + 1) + 1 = (m + (n + 1)) + 1. \quad \square$$

Proposition 2.2.4. *For any function $f : X \to X$, we have*

$$f^{m+n}(x) = f^n(f^m(x)).$$

Proof. The proof is by induction on n. In the base case, we have $m + 0 = m$ and

$$f^{m+0}(x) = f^m(x) = f^0(f(x)).$$

For the inductive step, assume that for every element $x \in X$, we have $f^{m+n}(x) = f^n(f^m(x))$. Our goal is to show that

$$f^{n+1}(f^m(x)) = f^{m+(n+1)}(x).$$

Here, we use that the equalities $m+(n+1) = (m+n)+1$ and $f^{n+1}(y) = f(f^n(y))$ hold by definition. These identities give:

$$f^{m+(n+1)}(x) = f(f^{m+n}(x)) = f(f^n(f^m(x))) = f^{n+1}(f^m(x)).$$ □

Corollary 2.2.5. *Addition of natural numbers is **associative**: For any three natural numbers l, m, and n we have*

$$(l + m) + n = l + (m + n).$$

Proof. By definition, we have $(l + m) + n = S^n(S^m(l))$ and $l + (m + n) = S^{m+n}(l)$. Combining these identities with Proposition 2.2.4, we obtain

$$(l + m) + n = S^n(S^m(l)) = S^{m+n}(l) = l + (m + n).$$ □

Proposition 2.2.6. *Addition of natural numbers is **commutative**: For any two natural numbers m and n, we have*

$$m + n = n + m.$$

Proof. The proof is by induction on n. In the base case, we use Proposition 2.2.3

$$m + 0 = m = 0 + m.$$

For the inductive step, assume that $m+n = n+m$. Then we use Proposition 2.2.3 again to obtain:

$$\begin{aligned} m + (n + 1) &= (m + n) + 1 \\ &= (n + m) + 1 \\ &= (n + 1) + m. \end{aligned}$$

This completes the induction step. □



Some further useful identifications of addition, which follow from the associativity and commutativity laws, are:

$$(l+m)+n = (l+n)+m,$$
$$l+(m+n) = m+(l+n),$$
$$(k+l)+(m+n) = (k+m)+(l+n).$$

The last identification is called the **interchange law** for addition. The first one follows from the second, and the second and third are proven by a short calculation:

$$\begin{aligned} l+(m+n) &= (l+m)+n \\ &= (m+l)+n \\ &= m+(l+n), \end{aligned} \qquad \begin{aligned} (k+l)+(m+n) &= k+(l+(m+n)) \\ &= k+(m+(l+n)) \\ &= (k+m)+(l+n). \end{aligned}$$

2.3 Arithmetic of Natural Numbers

DEFINITION 2.3.1. The **multiplication function** $m,n \mapsto mn$ on the natural numbers is defined recursively by

$$m0 := 0,$$
$$m(n+1) := mn+m.$$

PROPOSITION 2.3.2. *Multiplication of natural numbers satisfies the following laws:*

$$0n = 0, \qquad m0 = 0,$$
$$(m+1)n = mn+n, \qquad m(n+1) = mn+m,$$
$$1m = m, \qquad m1 = m,$$
$$l(m+n) = lm+ln, \qquad (l+m)n = ln+mn,$$
$$(lm)n = l(mn), \qquad mn = nm.$$

PROOF. We prove that $0n = 0$ by induction on n. In the base case, we have the equality $00 = 0$. For the inductive step, assume that $0n = 0$. Then $0(n+1) = 0n+0 = 0n = 0$, completing the proof of the first identity. The identity $m0 = 0$ holds by definition.

The proof that $(m+1)n = mn+n$ is again by induction on n. In the base case, we have the equalities $(m+1)0 = 0 = m0 = m0+0$. For the inductive step, assume that $(m+1)n = mn+n$. Then we have

$$\begin{aligned} (m+1)(n+1) &= (m+1)n+(m+1) \\ &= (mn+n)+(m+1) \\ &= (mn+m)+(n+1) \\ &= m(n+1)+(n+1). \end{aligned}$$

The identity $m(n+1) = mn + m$ holds by definition.

Next, we prove first that $mn = nm$, by induction on n. In the base case, we have the equalities $m0 = 0 = 0m$. For the inductive step, assume that $mn = nm$. Then we have that

$$m(n+1) = mn + m = nm + m = (n+1)m.$$

Now we prove that $l(m+n) = lm + ln$. We prove it by induction on n. In the base case, we have that $l(m+0) = lm = lm + 0 = lm + l0$. For the inductive step, assume that $l(m+n) = lm + ln$. Then we have that

$$\begin{aligned} l(m + (n+1)) &= l((m+n)+1) \\ &= l(m+n) + l \\ &= (lm + ln) + l \\ &= lm + (ln + l) \\ &= lm + l(n+1). \end{aligned}$$

The identification $(l+m)n = ln + mn$ follows from the previous identification, using the fact that $mn = nm$.

Finally, the proof that $(lm)n = l(mn)$ is by induction on n. In the base case, we have the equalities $(lm)0 = 0 = l0 = l(m0)$. For the inductive step, assume that $(lm)n = l(mn)$. Then we have that

$$(lm)(n+1) = (lm)n + lm = l(mn) + lm = l(mn+m) = l(m(n+1)).$$

This completes the inductive step. □

2.4 Relations on the Natural Numbers

Among Peano's axioms are the axioms stating that 0 is not a successor and that the successor function is injective. Recall that a function $f : X \to Y$ is called **injective** if the following implication holds:

$$f(x) = f(y) \quad \Rightarrow \quad x = y.$$

As the reader may have duly noted, we have neither postulated that 0 is not a successor and that the successor function is injective. Our goal is to prove them.

Example 2.4.1. We define the binary relation E on $\mathbb{N}$ by

$$\begin{aligned} E(0,0) &:= \top, & E(0,n+1) &:= \bot, \\ E(m+1,0) &:= \bot, & E(m+1,n+1) &:= E(m,n). \end{aligned}$$

We can prove by induction that the proposition $E(m,n)$ is true if and only if $m = n$. For the forward direction, we have to show that if $E(m,n)$ is true, then $m = n$. This is

proven by double induction: the proposition $E(0,0)$ is true by definition, and indeed we have $0 = 0$; the propositions $E(0, n+1)$ and $E(m+1, 0)$ are both false by definition; and if $E(m+1, n+1)$ is true, then $m = n$ by the inductive hypothesis, which implies that $m + 1 = n + 1$.

For the converse, we have to show that if $m = n$, then $E(m, n)$ is true. In other words, we need to show that $E(n, n)$ is true for all natural numbers n. Indeed, the proposition $E(0,0)$ is true by definition, and the proposition $E(n+1, n+1)$ is by definition equal to the proposition $E(n, n)$, which is true by the inductive hypothesis.

This simple example allows us to prove the two properties Peano postulated as axioms.

THEOREM 2.4.2. *The natural number* 0 *is not a successor.*

PROOF. Suppose that $0 = n + 1$ for some natural number n. This equality implies that

$$E(0,0) = E(0, n+1).$$

Since $E(0,0) = \top$ and $E(0, n+1) = \bot$, we conclude that $\top = \bot$, which is a contradiction. □

THEOREM 2.4.3. *The successor function is injective.*

PROOF. Suppose that $m + 1 = n + 1$. Then the proposition $E(m+1, n+1)$ is true, and consequently we find that the proposition $E(m, n)$ is true. This shows that $m = n$. □

EXAMPLE 2.4.4. Likewise, we can define the binary relations $\leq$ and $<$ recursively on the natural numbers. Their recursive definitions are given by

$$\begin{aligned} 0 \leq 0 &:= \top, & 0 \leq n+1 &:= \top, \\ m+1 \leq 0 &:= \bot & m+1 \leq n+1 &:= m \leq n. \end{aligned}$$

and

$$\begin{aligned} 0 < 0 &:= \bot, & 0 < n+1 &:= \top, \\ m+1 < 0 &:= \bot & m+1 < n+1 &:= m < n. \end{aligned}$$

REMARK 2.4.5. We have an obligation to mention why Peano postulated these two properties as axioms. Peano was working in a logical framework that was much weaker than set theory. In particular, the system in which he formulated the axioms for the natural numbers contained no powersets. The **powerset** $\mathscr{P}(A)$ of a set A is a set whose elements are subsets $U \subseteq A$.

For example, let $\mathbf{1} := \{*\}$ be the singleton set containing only the element $*$. Then the powerset $\mathscr{P}(\mathbf{1})$ contains the empty subset $\emptyset \subseteq \mathbf{1}$ and the full subset $\mathbf{1} \subseteq \mathbf{1}$. More generally, for every proposition P, we have the subset

$$\{* \mid P\} \subseteq \{*\},$$

which contains the element $*$ only when the proposition P holds. For example, when $P :\equiv \bot$ is the false proposition, then the subset $\{* \mid \bot\}$ is empty, and when $P :\equiv \top$ is the true proposition, then the subset $\{* \mid \top\}$ contains the element $*$.

Our reason for considering the powerset $\mathscr{P}(\mathbf{1})$ is that we can define relations on the natural numbers by recursively defining maps

$$\mathbb{N} \to (\mathbb{N} \to \mathscr{P}(\mathbf{1})).$$

2.5 Finite Sums and Products

Definition 2.5.1. The **finite summation operation** $\sum$ is defined by specifying a finite subset $I \subseteq \mathbb{N}$ and a family of natural numbers a_i where i ranges over the elements of I. We will write

$$\sum_{i \in I} a_i$$

for the sum over all the natural numbers a_i, with i ranging over I. This sum is defined by recursion over the number of elements in I. If I has no elements (that is, I is empty), then we define

$$\sum_{i \in I} a_i :\equiv 0.$$

If I has at least one element i_0, then we write $J :\equiv I \setminus \{i_0\}$, allowing us to define

$$\sum_{i \in I} a_i :\equiv a_{i_0} + \sum_{i \in J} a_j.$$

Theorem 2.5.2. *For any natural number n we have*

$$0 + \cdots + n = \frac{n(n+1)}{2}.$$

Proof. Let $S_n :\equiv 0 + \cdots + n$, and let $P(n)$ be the property that $S_n = \frac{n(n+1)}{2}$. We will prove that $P(n)$ is true for all n by induction. In the base case, we have to show that $P(0)$ holds, that is, that the identity

$$0 = \frac{0 \cdot 1}{2}$$

is true. This is indeed true, because the numerator in the fraction on the right-hand side is 0.

For the induction step, let n be a natural number and assume as our inductive hypothesis that $P(n)$ is true. Our goal is now to prove $P(n+1)$, that is, that the identity

$$S_{n+1} = \frac{(n+1)(n+2)}{2}.$$



Note that $S_{n+1} = S_n + (n+1)$. By the inductive hypothesis we have that $S_n = \frac{n(n+1)}{2}$, which we may now use to rewrite

$$S_n + (n+1) = \frac{n(n+1)}{2} + (n+1).$$

Observe that $(n+1) = \frac{2(n+1)}{2}$. Therefore we can make the following computation:

$$\begin{aligned}\frac{n(n+1)}{2} + (n+1) &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+2)(n+1)}{2}.\end{aligned}$$

Since $(n+2)(n+1) = (n+1)(n+2)$ it follows that $S_{n+1} = \frac{(n+1)(n+2)}{2}$ as desired. □

We illustrate induction with another example, the **formula for the geometric series**.

THEOREM 2.5.3. *For any real number x not equal to 1, the identity*

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}.$$

PROOF. The proof is by induction on n. In the case $n = 0$ the sum

$$\sum_{k=0}^{-1} x^k$$

is an empty sum, because it sums over all elements $0 \leq k \leq -1$ of which there are none. In empty sums, nothing is being added, so they are always 0. On the right hand side, we also see that

$$\frac{x^0 - 1}{x - 1} = \frac{1 - 1}{x - 1} = 0,$$

and hence the base case holds.

For the inductive step, assume that $\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}$. Our goal is to show that

$$\sum_{k=0}^{n} x^k = \frac{x^{n+1} - 1}{x - 1}.$$

Note that $\sum_{k=0}^{n} x^k = (\sum_{k=0}^{n-1} x^k) + x^n$. By applying the induction hypothesis we therefore find that

$$\sum_{k=0}^{n} x^k = \frac{x^n - 1}{x - 1} + x^n.$$

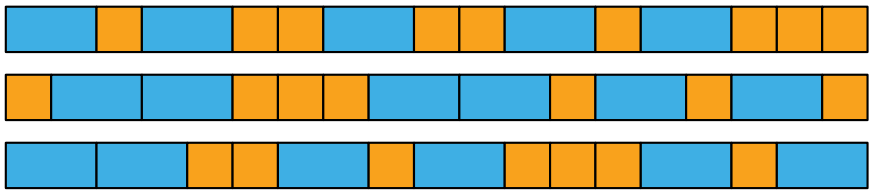


Figure 2.1: Three example tilings of a 1-by-19 grid using monominoes (1-by-1 tiles) and dominoes (1-by-2 tiles).

Note that $x^n = \frac{(x-1)x^n}{x-1}$. Therefore we can bring the two summands under one fraction as follows:

$$\frac{x^n-1}{x-1} + x^n = \frac{x^n-1}{x-1} + \frac{(x-1)x^n}{x-1} = \frac{x^n-1+x^{n+1}-x^n}{x-1} = \frac{x^{n+1}-1}{x-1}.$$

This completes the inductive step, and therefore the proof. □

2.6 Hemachandra's Counting Problem

In the 12th century, the Indian scholars Gopāla and Hemachandra studied the number of rhythmic patterns formed by combining short and long syllables in Sanskrit prosody. Hemachandra, around the year 1150, found a systematic way of counting the number of rhythmic patterns that can occur for any number of beats.

In order to rediscover Hemachandra's method, it might be helpful to think of the patterns of short and long syllables in terms of tilings one can make on a 1-by-n grid using monominoes (1-by-1 tiles) and dominoes (1-by-2 tiles). We have displayed some arbitrary examples of such tilings in Figure 2.1. The question is thus: How many such patterns are there?

In order to count them, let H_n be the number of such tilings. One way of finding the number H_n, which works when a specific n is given, is to simply list all the tilings of a 1-by-n grid. Doing so for small values of n is a great way to get a feeling for the problem. In Figure 2.2 we have listed all the possible tilings of the 1-by-5 grid.

For the first few numbers it is easy to determine the value of H_n. For example, the number H_1 is just 1, since the only way of tiling a 1-by-1 grid using monominoes and dominoes is to use a single monomino. Likewise, the number H_2 is 2, since we can either use two monominoes or one domino as a tiling of a 1-by-2 grid. However, listing all such tilings gets elaborate for larger n quite quickly, and furthermore doing so by hand is quite error-prone. The problem is therefore to find a clever way of counting all possible patterns for all n.

Notice that the last tile is either a monomino or a domino, so there are two cases to consider. The number of tilings ending in a monomino is exactly the number H_{n-1}, and the number of tilings ending in a domino is exactly the number H_{n-2}. This can be seen in Figure 2.2, where we listed all the tilings of the 1-by-5 grid. There are five

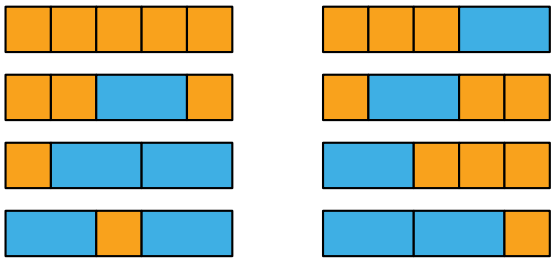


Figure 2.2: A list of all the possible tilings of a 1-by-5 grid using monominoes and dominoes.

tilings ending in a monomino, corresponding to each of the five different tilings of the 1-by-4 grid. Similarly, there are three tilings ending in a domino, corresponding to the three different tilings of the 1-by-3 grid. Thus, the total number of tilings of a 1-by-n grid is the sum of these two numbers:

$$H_n = H_{n-1} + H_{n-2}.$$

This recursive rule is very famous: It is the rule that generates the Fibonacci numbers.

DEFINITION 2.6.1. The sequence F_n of **Fibonacci numbers** is defined by

$$F_0 := 0, \qquad F_1 := 1, \qquad \text{and} \qquad F_{n+2} = F_{n+1} + F_n.$$

Since the numbers H_n start with $H_1 = 1$ and $H_2 = 2$, we find that

$$H_n = F_{n+1}.$$

Hemachandra applied this recurrence to list the initial values of the sequence H_n: 1, 2, 3, 5, 8, 13, 21. His results appear in his treatise on metrics, the CHANDONUŚĀSANA [HEM1961], composed several decades before Fibonacci's LIBER ABACI (1202). Nevertheless, in most of the world this sequence of numbers is called the Fibonacci numbers, even though it might be more appropriate to call them the Hemachandra–Fibonacci numbers.

The tiling interpretation of the Fibonacci numbers also appears in [BRI+1996]. The delightful book PROOFS THAT REALLY COUNT: THE ART OF COMBINATORIAL PROOF by Arthur Benjamin and Jennifer Quinn uses the tiling interpretation of the Fibonacci numbers to derive many Fibonacci identities combinatorially, and it contains many further examples of beautiful counting constructions [BQ2003].

Exercises

Starter Exercises

2.1 Prove that the sum of the first n odd numbers is a perfect square. That is, prove that

$$\sum_{k=0}^{n-1} 2k+1 = n^2.$$

Note: This summation formula is the starting point from which Fibonacci derived much of his work in his book Liber Quadratorum [FS1987].

2.2 (a) Prove that

$$\sum_{k=0}^{n} F_k = F_{n+2} - 1.$$

(b) Prove that

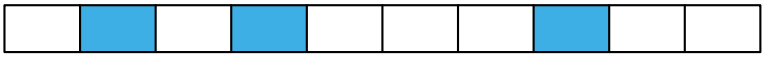
$$\sum_{k=0}^{n-1} F_{2k+1} = F_{2n}.$$

(c) Prove that

$$\sum_{k=0}^{n} F_{2k} = F_{2n+1} - 1.$$

2.3 Just as in Hemachandra's counting problem, suppose we have a metre of n beats composed of long (2 beats) and short syllables (1 beat). This time, the short syllables are distinguished between strong or soft beats. Write down the recursive formula for the number of rhythmic patterns of n beats, and use it to determine the correct values for $1 \leq n \leq 10$.

2.4 Consider strips subdivided into n blocks, in which some blocks are colored blue, so that no two colored blocks are adjacent. For example, the following is a valid coloring of the strip with 10 blocks:



Let c_n be the number of such colorings. Find c_1 and c_2, and express c_{n+2} in terms of c_{n+1} and c_n.

Routine-Building Exercises

2.5 Prove the **formula for the difference of nth powers**

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^k y^{n-1-k}.$$

Note that this formula generalizes the **formula for the difference of squares**

$$x^2 - y^2 = (x-y)(x+y)$$

as well as the **formula for the geometric series**

$$x^n - 1 = (x-1)\sum_{k=0}^{n-1} x^k.$$

2.6 Write T_n for the nth triangular number.

(a) For $0 \leq m < n$, show that

$$T_n - T_m = \frac{(n-m)(n+m+1)}{2}.$$

(b) For any two natural numbers m and n, show that

$$T_{m+n} = T_m + T_n + mn.$$

(c) Show that

$$T_{2n} = 4T_n - n.$$

(d) Show that

$$8T_n + 1 = (2n+1)^2.$$

Conclude that a natural number m is a triangular number if and only if $8m+1$ is a perfect square.

2.7 Write T_n for the nth triangular number, and define the nth **tetrahedral number** S_n by

$$S_n := \sum_{k=0}^{n} T_k.$$

(a) Give a geometric interpretation of these numbers justifying their name.

(b) Prove that

$$S_n = \frac{n(n+1)(n+2)}{6}.$$

(c) Prove that

$$S_{m+n} = S_m + S_n + \frac{mn(m+n+2)}{2}.$$

2.8 (a) Prove the **formula for the square pyramidal numbers**

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}.$$

Can you explain why the numbers of the form $\sum_{k=0}^{n} k^2$ are called square pyramidal numbers?

(b) Prove that

$$\sum_{k=0}^{n-1} (2k+1)^2 = \frac{n(4n^2-1)}{3}.$$

2.9 (a) Prove **Nicomachus's Theorem**

$$\sum_{k=0}^{n} k^3 = \left(\sum_{k=0}^{n} k\right)^2.$$

(b) Prove that

$$\sum_{k=0}^{n-1} (2k+1)^3 = n^2(2n^2-1).$$

2.10 Prove that

$$\sum_{k=0}^{n} k(k+1)(k+2) = \frac{n(n+1)(n+2)(n+3)}{4}.$$

2.11 Prove that

$$\sum_{k=0}^{n} F_k^2 = F_n F_{n+1}.$$

2.12 Consider the sequence (F_n) defined by

$$F_0 := 3 \qquad \text{and} \qquad F_{n+1} = F_n^2 - 2F_n + 2.$$

Show that $F_n = 2^{2^n} + 1$ for each $n \geq 0$. That is, show that (F_n) is the sequence of **Fermat numbers**.

Foundational Exercises

2.13 Consider a function $f : X \to X$. Show that for any $x \in X$ the following equality holds:

$$f^n(f^m(x)) = f^m(f^n(x)).$$

2.14 Consider a function $f : X \to X$. Show that for any $x \in X$, the following equality holds:

$$f^{mn}(x) = (f^m)^n(x).$$

2.15 For any natural number m, consider the function

$$I_m : (X \to X) \to (X \to X)$$

defined by $I_m(f) := f^m$. We can iterate this function too! Prove that for any function $f : X \to X$ and any $x \in X$, the following equality holds:

$$f^{m^n}(x) = (I_m)^n(f)(x).$$

2.16 Show that the function $x \mapsto x + n$ is injective, meaning that the following implication holds:

$$x + n = y + n \quad \Rightarrow \quad x = y.$$

2.17 Show that for $n \geq 1$, the function $x \mapsto nx$ is injective, meaning that the following implication holds:

$$nx = ny \quad \Rightarrow \quad x = y.$$

2.18 Show that if $xy = 1$, then $x = 1$ and $y = 1$.



Challenge Exercises

2.19 Let a_n be the number of ways to write a natural number n as an ordered sum $m_1 + \cdots + m_k = n$ of natural numbers $m_i \geq 2$. For example,

$$2 + 6 = 8, \qquad 2 + 3 + 3 = 8, \qquad \text{and} \qquad 3 + 2 + 3 = 8$$

are three distinct ways of writing the number 8 as an ordered sum of natural numbers ≥ 2. Find a_1 and a_2, and express a_{n+2} in terms of a_{n+1} and a_n [CAY1876].

2.20 (a) Prove **Cassini's identity**:

$$F_{n+1}^2 - F_n F_{n+2} = (-1)^n.$$

(b) Prove the following generalization of Cassini's identity:

$$F_{n+k}^2 - F_n F_{n+2k} = (-1)^n F_k^2.$$

2.21 Consider two nonzero natural numbers a and b satisfying $a(a+b) < b^2$. Prove that the strict inequality

$$F_n < \left(\frac{b}{a}\right)^n$$

holds for all n. Use Cassini's identity to give some examples of natural numbers a and b that satisfy this inequality.

2.22 Show that

$$F_{2n+1}^2 + F_{2n+3}^2 + 1 = 3F_{2n+1}F_{2n+3}.$$

2.23 Define

$$\begin{aligned} a_n &:= F_n F_{n+1} - (-1)^n, \\ b_n &:= F_n^2 + F_{n+1}^2, \\ c_n &:= 3F_n F_{n+1} + (-1)^n. \end{aligned}$$

Show that (a_n^2, b_n^2, c_n^2) is an **arithmetic progression of squares**; that is, show that

$$b_n^2 - a_n^2 = c_n^2 - b_n^2.$$

2.24 A 3-**term arithmetic progression** (a, b, c) is a triple of numbers $a \leq b \leq c$ with common increment, so that $b - a = c - b$. Show that every 3-term arithmetic progression of distinct positive Fibonacci numbers is of the form

$$(F_n, F_{n+2}, F_{n+3}).$$

Conclude that there are no 4-term arithmetic progressions of distinct positive Fibonacci numbers.

2.25 Let A_n be the number of maps $f : \{1, \ldots, n\} \to \{1, 2, 3\}$ satisfying the condition that

$$\min(f(i), f(j)) \leq |i - j|$$

for any two distinct elements $1 \leq i, j \leq n$.

(a) Compute the numbers A_1, A_2, A_3, and A_4.
(b) Find a recursive expression for A_{n+4}.

2.26 Consider the numbers s_n given by

$$s_0 := 0, \qquad s_1 := 1, \qquad \text{and} \qquad s_{n+2} = 34\, s_{n+1} - s_n + 2.$$

The first few numbers in this sequence are 0, 1, 36, 1225, 41616, 1413721, and 48024900.

(a) Show that s_n is a square number for each n.
(b) Show that s_n is a triangular number for each n.



Chapter 3

Counting

3.1 Hume's Principle

Combinatorics, or discrete mathematics, is the mathematics of finite structures. A central theme in combinatorics is counting, establishing a closed form for the number of objects of a certain kind. Such counting methods can sometimes be used to obtain results in number theory. For instance, we will use a counting argument to show that the product

$$n(n-1)\cdots(n-k+1)$$

of any k consecutive natural numbers is always divisible by $k!$.

What do mathematicians mean by counting? How do we establish that a certain set of objects contain a certain number of objects? Or, more generally, how do we establish that two sets of objects have the same number of objects?

These questions take us back to the 18th-century Scottish philosopher David Hume. He sheds light on this very question in his Treatise of Human Nature, a philosphical work in which he set out to found a general "science of man" by applying empirical methods to understanding, the passions, and morals [Hum1978, Part III, Book I]. In discussing the idea of number, he observes that equality of numbers can be determined whenever there is a one-to-one correspondence between their constituents:

> *We are possest of a precise standard, by which we can judge of the equality and proportion of numbers; and according as they correspond or not to that standard, we determine their relations, without any possibility of error. When two numbers are so combin'd, as that the one has always an unite answering to every unite of the other, we pronounce them equal; and 'tis for want of such*

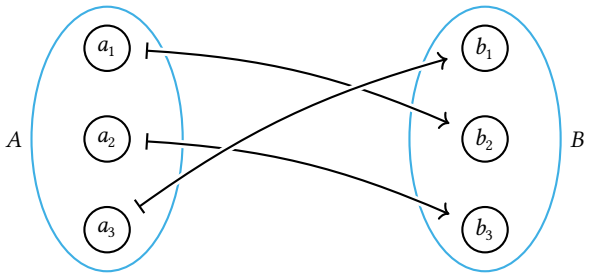


Figure 3.1: A bijection between two 3-element sets.

> *a standard of equality in extension, that geometry can scarce be esteem'd a perfect and infallible science.*

We note here that Hume relies on the Euclidean conception of number, where a number is a multitude of units: the number n is the collection of n units. By contrast, in modern mathematics we treat the natural numbers as an inductively generated set. To recover Hume's insight in our setting, we introduce the notion of a standard n-element set, which is to be a fixed set with exactly n elements playing the role of Euclid's collection of n units.

DEFINITION 3.1.1. The **standard finite set** $[n]$ with n elements is defined by

$$[n] := \{0, \dots, n-1\} = \{x \in \mathbb{N} \mid x < n\}.$$

The standard 0-element set $[0]$ is the empty set, since there are no natural numbers strictly smaller than 0. The standard 1-element set is the set $\{0\}$, since 0 is the only element strictly smaller than 1. The standard 2-element set is the set $\{0, 1\}$, since the only two elements strictly smaller than 2 are 0 and 1, and so forth.

Suppose now that we are given an arbitrary set A, and we wish to count its elements. What does it mean when we say that the set A has n elements? It means that we can, at least in principle, label each element of A with a number $0 \leq i < n$ in such a way that every label $0 \leq i < n$ is used *exactly once*. By making sure that all labels are used at least once, we make sure that there are indeed at least n elements in A, and by making sure that all labels are used at most once, we make sure not to overcount the elements of A. Thus, in order to show that the set A has n elements, we have to create what is called a **bijective correspondence** between the elements of the standard finite set $[n]$ and the set A.

DEFINITION 3.1.2. A function $f : X \to Y$ is said to be a **bijection** if for every $y \in Y$ there is exactly one element $x \in X$ such that $f(x) = y$. The set of bijections from X to Y is denoted by

$$X \cong Y.$$

Furthermore, we say that X **is an n-element set** if there exists a bijection $[n] \cong X$.

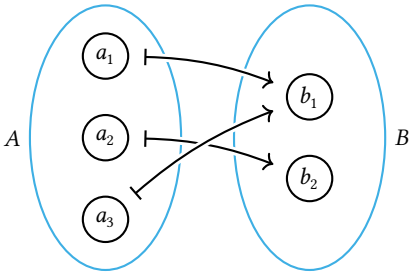


Figure 3.2: This function is not a bijection since the distinct elements a_1 and a_3 are both sent to b_1.

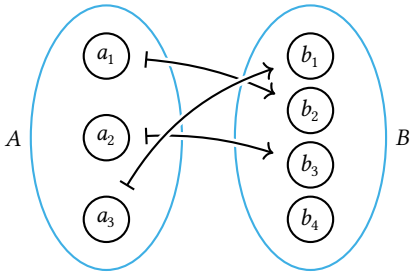


Figure 3.3: This function is not a bijection since b_4 is not the value of any element in A.

In Figure 3.1 we displayed an example of a bijection between two 3-element sets. Note that such a bijection would not exist between A and B if the number of elements in B was different from three. If B had fewer than 3 elements, as shown in Figure 3.2, then any function $f : A \to B$ would necessarily repeat a value, while if B had more than 3 elements, as shown in Figure 3.3, then no function $f : A \to B$ could have all the elements of B in its range.

This is precisely the reason why we are interested in bijections: If there is a bijection between A and B, then they must have the same number of elements. The principle that any two finite sets have the same number of elements if and only if there is a bijection between them is **Hume's Principle**.

In order to prove Hume's principle more formally, we need two lemmas. The first is an abstract lemma that asserts that two bijections $f : A \cong B$ and $g : B \cong C$ can be composed into a bijection $g \circ f : A \cong C$. The second is a self-evident looking lemma that establishes that if A is an $(n+1)$-element set and $a \in A$, then the set $A \setminus \{a\}$ consisting of all elements of A except a is an n-element set. Indeed, such a lemma also requires proof.

Before we state the composability of bijections, a few comments about how to prove that a function is a bijection and how to use the assumption that a function is a bijection are in order.

Proving that $f : X \to Y$ is a bijection. The condition that a function $f : X \to Y$ is a bijection states that for every element $y \in Y$ there is a unique element $x \in X$ such that $f(x) = y$. Such unique existence properties have two parts: first we have to show that there indeed exists at least one such x, and second we have to show that it is unique. For the second part, we assume that if both x satisfies $f(x) = y$ and x' satisfies $f(x') = y$, then we must have $x = x'$.

Using the condition that $f : X \to Y$ is a bijection. If we assume that $f : X \to Y$ is a bijection, then we have for every $y \in Y$ access to an element $x \in X$ such that $f(x) = y$. Furthermore, for every $x' \in X$ such that $f(x') = y$ we know that the equality $x = x'$ must hold, which we may use if it helps us in our proof.

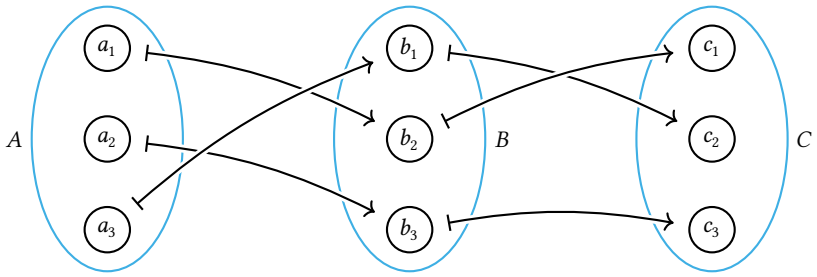


Figure 3.4: Composition of bijections between 3-element sets.

LEMMA 3.1.3. *Consider two bijections $f : A \cong B$ and $g : B \cong C$. Then the* ***composite*** *function $g \circ f$ defined by $a \mapsto g(f(a))$, as illustrated in Figure 3.4, is also a bijection.*

PROOF. We have to show that for every element $z \in C$ there is exactly one element $x \in A$ such that $g(f(x)) = z$.

Since g is assumed to be a bijection, there is exactly one element $y \in B$ such that $g(y) = z$. Furthermore, since f is assumed to be a bijection there is exactly one element $x \in A$ such that $f(x) = y$. For such x, we have

$$g(f(x)) = g(y) = z.$$

Thus we have shown that there is at least one such element x.

To see that there is at most one, let $x' \in A$ be such that $g(f(x')) = z$. Since both $g(f(x)) = z$ and $g(f(x')) = z$, it follows from the assumption that g is a bijection that $f(x) = f(x')$. Now, since f is a bijection, it follows that $x = x'$. This completes the proof that x is the unique element of A mapping to z. □

LEMMA 3.1.4. *Consider an $(n+1)$-element set A equipped with a distinguished element a. Then the set*

$$A \setminus \{a\} := \{x \in A \mid x \neq a\}$$

is an n-element set.

PROOF. Suppose $f : [n+1] \to A$ is a bijection. Then there is a unique element $x < n+1$ such that $f(x) = a$. We will first construct a bijection $h : [n+1] \to [n+1]$ such that $h(n) = x$. Once we have such a bijection, it follows that $f \circ h : [n+1] \to A$ is a bijection such that $f(h(n)) = a$, which will allow us to make progress.

The bijection h is defined by swapping the elements n and x:

$$h(y) := \begin{cases} x & \text{if } y = n, \\ n & \text{if } y = x, \\ y & \text{otherwise.} \end{cases}$$

The fact that h is a bijection follows by case analysis on y: If $y = n$ then the only element mapping to y is x; if $y = x$ then the only element mapping to y is n, and otherwise the only element mapping to y is y itself.

Now, since we have a bijection $g := f \circ h : [n+1] \to [n+1]$ such that $g(n) = a$, it follows that the restriction of g to the set $[n]$ is a bijection from $[n]$ to $A \setminus \{a\}$. □

Theorem 3.1.5 (Hume's Principle). *Consider an m-element set A and an n-element set B. Then there exists a bijection between A and B if and only if $m = n$.*

Proof. The claim has two directions. In the forward direction, we have to show that if there is a bijection $A \cong B$, then $m = n$. In the reverse direction we have to show that if $m = n$, then there is a bijection $A \cong B$. The reverse direction is most immediate, so we do it first.

Suppose that $m = n$. This implies that $[m] = [n]$, which in particular implies that there is a bijection $[m] \cong [n]$. Since A is an m-element set, there exists a bijection $[m] \cong A$, and since B is an n-element set, there is a bijection $[n] \cong B$. Chaining these bijections gives

$$A \cong [m] \cong [n] \cong B.$$

In other words, the composite of all these bijections results in a bijection $A \cong B$. This completes the reverse direction of the claim.

The proof of the forward direction is by induction on m. For the base case, if $m = 0$ it follows that A is empty. This implies that n is not nonzero. Indeed, if n were nonzero, then B would have an element, which would correspond to a unique element in A, which does not exist. Thus we conclude that $n = 0$, and hence that $m = n$.

Now assume that for any m-element set A with a bijection into an n-element set B, we have $m = n$. Our goal is to show that if A is an $(m+1)$-element set with a bijection into an n-element set B, then $m + 1 = n$. Note that $n > 0$, since A has at least one element. Thus, we can write $n = n' + 1$. Furthermore, given an element $a \in A$, we obtain $f(a) \in B$. Then the bijection f restricts to a bijection

$$(A \setminus \{a\}) \cong (B \setminus \{f(a)\})$$

between an m-element set and an n'-element set. By the inductive hypothesis, this implies that $m = n'$ and thus we conclude that $m + 1 = n' + 1 = n$. □

Example 3.1.6. We claim that the number of functions $f : [m] \to [n]$ is n^m. The proof is by induction on m.

In the base case, we have to show that there is exactly one function $[0] \to [n]$. Indeed this is the case, as the set $[0]$ is empty, and since functions are specified by specifying the values for all its elements, the empty specification is a specification of the empty function.

For the inductive step, we observe that there is a bijection

$$([m+1] \to [n]) \cong ([m] \to [n]) \times [n].$$



Indeed, since any function is uniquely determined by its values, a function $f : [m+1] \to [n]$ is uniquely determined by its restriction $[m] \to [n]$, which determines the values of f for $0 \leq i < m$, and a value for $f(m)$. By the inductive hypothesis, there are n^m functions in the set $[m] \to [n]$, so the number of elements of the set $([m] \to [n]) \times [n]$ is $n^m \cdot n = n^{m+1}$. By Theorem 3.1.5 (Hume's Principle) it follows that ther are n^{m+1} functions in the set $[m+1] \to [n]$.

3.2 Equivalent Ways of Defining Bijections

We have defined bijections to be functions $f : X \to Y$ such that for every $y \in Y$ there exists exactly one element $x \in X$ such that $f(x) = y$. The unique existence of such an element x can be broken down in two parts: existence and uniqueness. This suggests that also the definition of bijectivity can be broken down in two parts. This is indeed the case, and both concepts turn out to be useful.

DEFINITION 3.2.1. A function $f : X \to Y$ is said to be **surjective** if for every $y \in Y$ there exists an element $x \in X$ such that $f(x) = y$. When f is a surjective function from X to Y, it is common to write

$$f : X \twoheadrightarrow Y.$$

A function $f : X \to Y$ is said to be **injective** if for every $y \in Y$ there is at most one element $x \in X$ such that $f(x) = y$. When f is an injective function from X to Y, it is common to write

$$f : X \hookrightarrow Y.$$

Thus, a function $f : X \to Y$ is surjective if every element of Y is a value of f. The function shown in Figure 3.2 is an example of a surjective function.

Likewise, a function $f : X \to Y$ is injective if the function f does not repeat values. Another way of stating the condition that f is injective is by the condition

$$f(x) = f(y) \quad \Rightarrow \quad x = y,$$

which states that if two elements x and y have the same value under f, then they must be the same. The function shown in Figure 3.3 is an example of an injective function.

An immediate corollary of these definitions is that a function is a bijection if and only if it is both surjective and injective. Indeed, many authors take this as the definition of bijections.

PROPOSITION 3.2.2. *A function is a bijection if and only if it is both surjective and injective.* □

Suppose that $f : X \to Y$ is a bijection. Since for every $y \in Y$ there exists a unique element $x \in X$ such that $f(x) = y$, we can define a new function $g : Y \to X$ so that $g(y)$ is this unique element of X such that $f(g(y)) = y$, as illustrated in Figure 3.5. The function g reverses all the value-assignments of the function f, so we call it the *inverse* of f. This leads us to the concept of *invertible functions*.

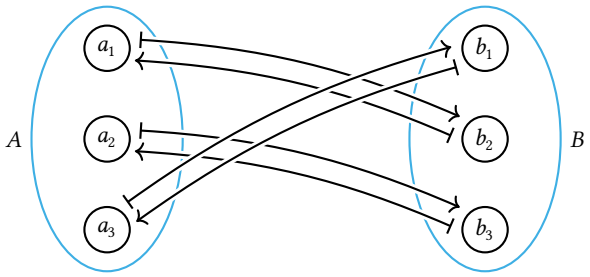


Figure 3.5: A bijection between two 3-element sets, together with its inverse.

Definition 3.2.3. A function $f : X \to Y$ is said to be **invertible** if there is a function $g : Y \to X$ such that

$$f(g(y)) = y \qquad \text{and} \qquad g(f(x)) = x$$

for every $x \in X$ and $y \in Y$. Such a function g is called an **inverse** of f.

The idea behind the concept of invertible functions is that mapping an element via an invertible function can be undone by means of a function in the reverse direction. Thus, if $f : X \to Y$ is an invertible function with inverse $g : Y \to X$, then if we map an element $x \in X$ to $f(x) \in Y$, we can undo this by mapping it back to $g(f(x)) \in X$, which is equal to x. Furthermore, the function f is also inverse to the function g so that if we map an element $y \in Y$ to $g(y) \in X$, we can undo this by mapping it back to $f(g(y)) \in Y$, which is equal to y.

Theorem 3.2.4. *A function $f : X \to Y$ is a bijection if and only if it is invertible.*

Proof. Suppose first that f is a bijection. To construct its inverse g, we must assign to each element $y \in Y$ an element $x \in X$. By the assumption that f is a bijection, we are given that the set

$$\{x \in X \mid f(x) = y\}$$

has exactly one element. Thus, we let $g(y)$ be the unique element of this set. By definition, we have $f(g(y)) = y$. To see that $g(f(x)) = x$, note that x is the unique element in the set

$$\{x' \in X \mid f(x') = f(x)\}.$$

Thus, if we can show that $g(f(x))$ is also in this set, then it follows that $g(f(x)) = x$. In other words, our plan is to show that $f(g(f(x))) = f(x)$. However, this follows at once from the definition of g, using the element $y := f(x)$. This shows that f is invertible.

For the converse, assume that f is invertible with inverse g, and consider the set

$$\{x \in X \mid f(x) = y\}.$$

Observe that $g(y)$ is in this set, since $f(g(y)) = y$ by the assumption that g is an inverse of f. Thus, the set has at least one element. It remains to show that it has at

most one element. To see this, consider two elements x and x' such that $f(x) = y$ and $f(x') = y$. Then we obtain that

$$x = g(f(x)) = g(y) = g(f(x')) = x'.$$

This shows that any two elements in the set $\{x \in X \mid f(x) = y\}$ must be equal, so it has at most one element. □

3.3 Counting Bijections

Recall that the set $[n]$ consists of all natural numbers strictly smaller than n. That is, the set $[n]$ is the set $\{0, \ldots, n-1\}$. If $n = 0$ this set is understood to be empty. Assuming that $n > 0$, the largest element of $[n]$ is therefore $n - 1$.

Intuitively, a bijection from $[n]$ to $[n]$ is determined, at least for $n > 0$, by first specifying the value of the largest element $n-1$, which may be any element $x < n$, and second by picking a bijection $[n-1] \cong [n] \setminus \{x\}$. In other words, bijections between finite sets are determined recursively! This suggests that the number of bijections $[n] \cong [n]$ is also determined by a recursive function.

DEFINITION 3.3.1. The **factorial function** $n \mapsto n!$ is defined recursively by

$$0! := 1,$$
$$(n+1)! := n!(n+1).$$

In the following proposition we prove the number of bijections $[n] \cong [n]$ on the standard n-element set is the number $n!$. In other words, the factorial function counts the number of bijections on the standard n-element set.

PROPOSITION 3.3.2. *The number of bijections $[n] \cong [n]$ from the standard n-element set to itself is exactly $n!$.*

PROOF. The proof is by induction on n. For the base case, let $n = 0$. Then $[n]$ is an empty set, and there is exactly one function $[n] \to [n]$, the empty function. This function is a bijection, because assuming an element of an empty set is an inherent contradiction from which we can conclude anything.

Now suppose that the number of bijections $[n] \cong [n]$ is $n!$. We claim that for each $y \in [n+1]$ there are exactly $n!$ bijections $f : [n+1] \cong [n+1]$ such that $f(n) = y$.

To see this, we first define the **transposition function** $s_{y,n}$ defined by

$$s_{y,n}(x) = \begin{cases} n & \text{if } x = y, \\ y & \text{if } x = n, \\ x & \text{otherwise.} \end{cases}$$

In other words, the function $s_{y,n}$ swaps the elements n and y, and leaves the other elements fixed. This function is a bijection by Theorem 3.2.4, because $s_{y,n}(s_{y,n}(x)) = x$

for all $x \in [n+1]$; that is, swapping two elements and swapping them right back is the same as doing nothing.

Now we observe that the function

$$([n+1] \cong [n+1]) \to ([n+1] \cong [n+1])$$

given by $g \mapsto s \circ g$ is itself a bijection, because it is an invertible function. Indeed, it is its own inverse, because $s \circ s \circ g = g$ for any bijection g.

Thus, if $f : [n+1] \cong [n+1]$ is a bijection such that $f(n) = y$, then $s \circ f$ is a bijection satisfying $s(f(n)) = n$. In other words, every bijection satisfying $f(n) = y$ corresponds uniquely to a bijection satisfying $f(n) = n$.

Now we observe that there are exactly $n!$ bijections $f : [n+1] \cong [n+1]$ satisfying $f(n) = n$. Indeed, such bijections are uniquely determined by their restriction to the set $[n]$, and by the induction hypothesis there are $n!$ such bijections. Since there are $n+1$ possible choices of a value y, we conclude that there are $n!(n+1)$ bijections altogether from $[n+1]$ to $[n+1]$. □

Remark 3.3.3. It is useful to have a simple lower bound for the factorial $n!$. Recall that the **exponential function** is defined by the infinite series

$$e^x := \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Here, the quantity $e := \sum_{n=0}^{\infty} \frac{1}{n!}$ is Euler's number, of which the first few terms are

$$\frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \frac{1}{5!} + \cdots = 1 + 1 + \frac{1}{2} + \frac{1}{6} + \frac{1}{24} + \frac{1}{120} + \cdots.$$

The terms from $1/0!$ to $1/5!$ add up to $2 + \frac{86}{120} \approx 2.71\cdots$, which correctly estimates the value of e up to two decimal digits.

We claim that for any positive natural number n, we have the strict inequality

$$\left(\frac{n}{e}\right)^n < n!.$$

To see this, observe that when x is positive, then every term $\frac{x^n}{n!}$ contributes a positive amount to the exponential function. This gives the strict inequality

$$\frac{x^n}{n!} < e^x.$$

We may simply take $x = n$ to obtain

$$\frac{n^n}{n!} < e^n,$$

and the claim is proven by rearranging.



The strict lower bound for $n!$ given here is not the best known estimate of the factorial function. Nevertheless, its proof is elementary, and it can be used in basic number-theoretic estimates. The most famous approximation to the factorial function is given by **Stirling's approximation formula**:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

This means that the ratio of the quantities $n!$ and $\sqrt{2\pi n}(n/e)^n$ tends to 1 as n becomes arbitrarily large. While Stirling's approximation formula is certainly applicable in number theory, we shall have no need for it in the present introduction to the subject and therefore we will omit the proof.

3.4 Counting Subsets

A **subset** A of a set X is a set consisting entirely of elements of X. Subsets may be empty, they may contain some elements of X, or they may also contain all elements of X. When A is a subset of X, we write

$$A \subseteq X.$$

Subsets of X can be formed using predicates over the elements of X. A **predicate** is a proposition about or condition on indeterminate elements. For example, the condition that n is an even natural number is a predicate with the indeterminate natural number n. This predicate determines the subset of all even natural numbers

$$\{0, 2, 4, 6, \ldots\} \subseteq \mathbb{N}.$$

Often, we write $P(x)$ for a predicate on the indeterminate element x. The subset determined by this predicate is the set of all the elements x that satisfy the condition $P(x)$. Such subsets are conveniently defined by **set-builder notation**:

$$\{x \in X \mid P(x)\} \subseteq X.$$

For example, the subset of even natural numbers can be written in set-builder notation as follows:

$$\{n \in \mathbb{N} \mid n \text{ is even}\} \subseteq \mathbb{N}.$$

Here, the condition that n is even could also be expressed through the logical formula

$$\exists_{(k \in \mathbb{N})} 2k = n,$$

asserting that there exists a natural number k such that the number $2k$ is equal to the number n. Nevertheless, we often find ourself preferring expressions in natural language that convey the intended meaning more easily.

Subsets of a set X are determined by a function $X \to \{0,1\}$. Indeed, given a subset A of X, we define its **characteristic function** χ_A by

$$\chi_A(x) := \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{otherwise.} \end{cases}$$

Conversely, any function $f : X \to \{0,1\}$ determines the subset

$$\{x \in X \mid f(x) = 1\}.$$

Thus, we can go back and forth between (1) subsets of a set, (2) predicates on a set, and (3) functions from a set into $\{0,1\}$. All of these are equivalent descriptions of the concept of subset.

Since subsets of X are equivalently described as functions from X into the set $\{0,1\}$, it follows that the number of subsets of an n-element set X is 2^n. Indeed, for each element x there are two options: Either it is in the subset or it isn't. Given that X has n elements, there are thus 2^n specifications of subsets of X.

Less trivial is the question: *How many k-element subsets are there of an n-element set?* For example, there are six 2-element subsets of the set $\{1,2,3,4\}$:

$$\{1,2\},\ \{1,3\},\ \{1,4\},\ \{2,3\},\ \{2,4\},\ \text{and } \{3,4\}.$$

Let us write

$$\mathscr{P}_k(X) := \{S \subseteq X \mid \#S = k\}.$$

Assuming that both n and k are positive natural numbers, so that in particular X contains at least one element x_0, we can approach this question by distinguishing two classes of k-element subsets of X: Those that contain x_0 and those that don't contain x_0. Note that a k-element subset of X that contains x_0 is uniquely determined by a $(k-1)$-element subset of the set $X \setminus \{x_0\}$. Likewise, a k-element subset of X that doesn't contain x_0 is uniquely determined by a k-element subset of $X \setminus \{x_0\}$. Thus we find that

$$\#\mathscr{P}_k(X) = \#\mathscr{P}_k(X \setminus \{x_0\}) + \#\mathscr{P}_{k-1}(X \setminus \{x_0\}).$$

This formula suggests a recursive method of determining the number of k-element subsets.

Definition 3.4.1. The **binomial coefficients** $\binom{n}{k}$ are defined recursively by

$$\binom{0}{0} := 1 \qquad \binom{0}{k+1} := 0$$

$$\binom{n+1}{0} := 1 \qquad \binom{n+1}{k+1} := \binom{n}{k} + \binom{n}{k+1}.$$

The binomial coefficients can be arranged in **Pascal's triangle**, where each entry is the sum of the two directly above it. At the top of the triangle we find the binomial coefficient $\binom{0}{0}$. This is 0th row of Pascal's triangle. In the nth row from the top, we find the binomial coefficients $\binom{n}{k}$ for $0 \leq k \leq n$.



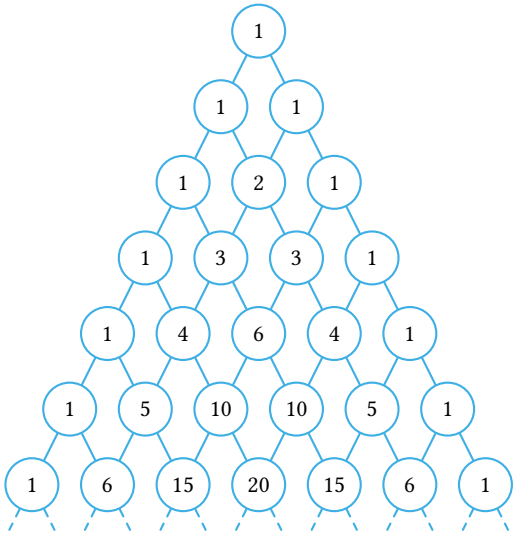


Figure 3.6: Pascal's triangle. Counting from 0 from the top, the kth entry in the nth row is the binomial coefficient $\binom{n}{k}$.

THEOREM 3.4.2. *Consider an n-element set X, and a natural number k. Then the number of k-element subsets of X is the binomial coefficient $\binom{n}{k}$.*

PROOF. We will proof the theorem by induction on both variables. There are four cases to consider.

There is always exactly one 0-element subset of any set, the empty subset. In particular, we find that the number of 0-element subsets of a 0-element set is $\binom{0}{0}$, and the number of 0-element subsets of a $(n+1)$-element set is $\binom{n+1}{0}$.

If X has no elements, then X doesn't contain any subsets with a positive number of elements, so we conclude that the number of $(k+1)$-element subsets of X is $\binom{0}{k+1}$.

Finally, we consider the case of $(k+1)$-element subsets of an $(n+1)$-element set X. Since X has a positive number of elements, we may pick one and call it x_0. As we have already found in the discussion leading up to this theorem, the number of $(k+1)$-element subsets is given by the formula

$$\#\mathscr{P}_{k+1}(X) = \#\mathscr{P}_k(X \setminus \{x_0\}) + \#\mathscr{P}_{k+1}(X \setminus \{x_0\}).$$

By the inductive hypothesis, we have that $\#\mathscr{P}_k(X \setminus \{x_0\}) = \binom{n}{k}$ and $\#\mathscr{P}_{k+1}(X \setminus \{x_0\}) = \binom{n}{k+1}$, so that the number of $(k+1)$-element subsets of X is

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}. \qquad \square$$

Next, we turn our attention to the closed form for the binomial coefficients

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Equivalent formulas and computational rules were studied in several mathematical traditions over many centuries. Indian mathematicians had studied problems of permutations and combinations since antiquity, and by the ninth century Mahāvīra had given general arithmetical rules for their calculation [Mah1912]. In the Līlāvatī, written around 1150 CE, the Indian mathematician Bhāskara II dedicated an entire chapter to combinatorics and provided rules for calculating combinations and permutations [BB1817]. In Maaseh Hoshev, completed in 1321 CE, the French mathematician Levi ben Gerson stated the closed form for both combinations and permutations [Ger1909]. Furthermore, his proofs are among the earliest surviving clear uses of mathematical induction. The Italian mathematician Girolamo Cardano published the closed form in [Car1570].

We will prove the formula for the binomial coefficients via a counting argument, by showing that

$$\binom{n}{k} \cdot k! = n(n-1)\cdots(n-k+1)$$

Products of successive natural numbers such as the one on the right-hand side of this equation are called *falling factorials*.

Definition 3.4.3. Let k and n be natural numbers. The kth **falling factorial** of n is the number

$$n_k := n(n-1)\cdots(n-k+1),$$

where we take $n_k = 0$ for $k > n$.

The 0th falling factorial requires some explanation. It is the product of 0 consecutive integers going down from n. The product of no numbers is an empty product, which is 1 by definition. Thus, we have

$$n_0 = 1.$$

From here on, the falling factorials are less tricky: The first falling factorial of n is $n_1 = n$, the second falling factorial of n is $n_2 = n(n-1)$, the third falling factorial of n is $n_3 = n(n-1)(n-2)$, and so on.

Theorem 3.4.4. *The number of injective functions $f : [k] \hookrightarrow [n]$ is n_k.*

Theorem 3.4.5 (Formula for binomial coefficients.) *For any two natural numbers n and k such that $k \leq n$, we have*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$



PROOF. We will show that for each k-element subset $S \subseteq [n]$, there are exactly $k!$ injective functions $f : [k] \to [n]$ such that $\mathrm{im}(f) = S$. By this claim we obtain the identity

$$n_k = \binom{n}{k} \cdot k!,$$

from which the theorem follows. □

3.5 The Binomial Theorem

If we expand the exponent $(x + y)^3$, we get

$$\begin{aligned}(x+y)^3 &= (x+y)^2(x+y)\\ &= (x^2 + 2xy + y^2)(x+y)\\ &= x^3 + 2x^2y + xy^2 + x^2y + 2xy^2 + y^3\\ &= x^3 + 3x^2y + 3xy^2 + y^3.\end{aligned}$$

Going further, if we expand the exponent $(x + y)^4$, we get

$$\begin{aligned}(x+y)^4 &= (x^3 + 3x^2y + 3xy^2 + y^3)(x+y)\\ &= x^4 + 3x^3y + 3x^2y^2 + xy^3 + x^3y + 3x^2y^2 + 3xy^3 + y^4\\ &= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4.\end{aligned}$$

Now we might recognize an emerging pattern in the coefficients of these polynomials: they are all binomial coefficients! The binomial theorem generalizes this observation to all exponents n.

The binomial theorem has many proofs, including combinatorial proofs and algebraic proofs. All these proofs have their own merits. We will present here an algebraic proof, using induction, since it is the most easily applicable to settings other than the integers.

THEOREM 3.5.1 (The Binomial Theorem). The binomial theorem. *In any number system, such as the natural numbers, the integers, the rational numbers, the reals, the complex numbers,*[1] *we have*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

PROOF. We prove the statement by induction on n. In the base case, we find that both sides of the equation

$$(x+y)^0 = \sum_{k=0}^{0} \binom{n}{k} x^k y^{0-k}$$

[1] More generally, the binomial theorem applies to any semiring, conditional on the assumption that $xy = yx$.

evaluate to 1, so the equation is true. In the inductive step, we have that

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} \\
&= \sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k+1} \\
&= x^{n+1} + \sum_{k=0}^{n-1}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=1}^{n}\binom{n}{k}x^k y^{n-k+1} + y^{n+1} \\
&= x^{n+1} + \sum_{k=1}^{n}\binom{n}{k-1}x^k y^{n-k+1} + \sum_{k=1}^{n}\binom{n}{k}x^k y^{n-k+1} + y^{n+1} \\
&= x^{n+1} + \sum_{k=1}^{n}\left(\binom{n}{k-1} + \binom{n}{k}\right)x^k y^{n-k+1} + y^{n+1} \\
&= \sum_{k=0}^{n+1}\binom{n+1}{k}x^k y^{(n+1)-k}.
\end{aligned}$$

□

The binomial theorem has a long history. The earliest known references to aspects of the binomial theorem are found in the Chinese mathematical text Jiuzhang Suanshu (Nine Chapters on the Mathematical Art), from approximately the 2nd century BCE. Around the 11th century CE, the Chinese mathematician Jia Xian described a method for calculating binomial coefficients, which corresponds to what we now refer to as Pascal's triangle. This method was popularized by Yang Hui in the 13th century CE, and thus Pascal's triangle is sometimes called the **Yang Hui triangle** in China. Isaac Newton was the first to generalize the binomial theorem to non-integer number systems, in 1687 in his Principia Mathematica.

3.6 The Inclusion–Exclusion Principle

Consider two subsets A and B of a set X. The **union** of A and B is the set

$$A \cup B := \{x \in X \mid x \in A \text{ or } x \in B\}.$$

Given that X is a finite set, we may wish to determine the number of elements in $A \cup B$. Note, however, that in general the answer is not found by simply adding up the number of elements of A and the number of elements in B. Indeed, some elements might be contained in both subsets, and they would therefore be counted double. Since every element in the intersection $A \cap B$ is counted twice, the correct formula for the number of elements in $A \cup B$ is:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$



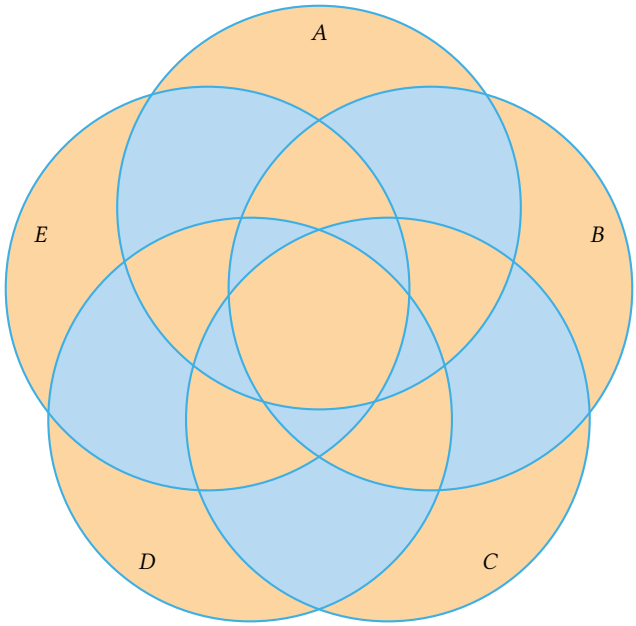


Figure 3.7: Five overlapping sets, with their intersections shaded in orange and blue according to the parity of sets they are contained in.

EXAMPLE 3.6.1. Consider the set $X = \{1, \dots, 100\}$, and our goal is to find the number of integers in X that are neither divisible by 2 nor by 3. This problem can be solved with the inclusion–exclusion principle.

Let A and B be the subsets of X consisting of numbers divisible by 2 and by 3, respectively. The set $A \cap B$ then consists of all the numbers divisible by both 2 and 3; that is, the numbers divisible by 6.

There are 50 numbers in X divisible by 2, there are 33 numbers in X divisible by 3, and there are 16 numbers in X divisible by 6. Thus, the total count of numbers in X not divisible by either 2 or 3 is

$$100 - 50 - 33 + 16 = 33.$$

The inclusion–exclusion principle is a generalization of the formula for the number of elements of $A \cup B$ to any finite number of subsets of a set X. To see the pattern, let us consider the case with three subsets A, B, and C of a set X. Now, if we wish to determine the number of elements in $A \cup B \cup C$, we can again start by adding the numbers $|A|$, $|B|$, and $|C|$. Every element that was in exactly one of the three subsets is correctly accounted for, but we have overcounted the elements in $A \cap B$, $A \cap C$, and $B \cap C$. If we subtract the numbers $|A \cap B|$, $|A \cap C|$, and $|B \cap C|$ from our total, then we

have correctly accounted for every element that was in at most two subsets. However, now we have subtracted every element in $A \cap B \cap C$ three times from our count, so we must add them again to arrive at the correct number:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Thus, we see an alternating pattern emerging: Single sets are added, intersections of two sets are subtracted, triple intersections are added again, and so on. The inclusion–exclusion principle is stated with this alternating pattern.

Theorem 3.6.2 (The Inclusion–Exclusion Principle). *Consider a finite set X and a finite family of subsets $A_i \subset X$ indexed by $1 \leq i \leq n$. Then the number of elements in the union of the subsets A_i is given by*

$$|A_1 \cup \cdots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{1 \leq i_1 < \cdots < i_k \leq n} |A_{i_1} \cap \cdots \cap A_{i_k}| \right).$$

Proof. Without loss of generality, we may assume that $X = A_1 \cup \cdots \cup A_n$. For any subset $B \subseteq X$ and any element $x \in X$, let us define the number

$$[x \in B] := \begin{cases} 1 & \text{if } x \in B, \\ 0 & \text{if } x \notin B. \end{cases}$$

The numbers thus defined satisfy the identity $\sum_{x \in X} [x \in B] = |B|$, which is useful for algebraic manipulations. The inclusion–exclusion principle is then asserted equivalently as the identity

$$\sum_{k=0}^{n} (-1)^k \left(\sum_{1 \leq i_1 < \cdots < i_k \leq n} \sum_{x \in X} [x \in A_{i_1} \cap \cdots \cap A_{i_k}] \right) = 0$$

Here we assume the convention that for $k = 0$ we have $A_{i_1} \cap \cdots \cap A_{i_k} = X = A_1 \cup \cdots \cup A_n$. By rearranging the equation, we see that the inclusion–exclusion principle is equivalent to the identity

$$\sum_{x \in X} \sum_{k=0}^{n} (-1)^k \left(\sum_{1 \leq i_1 < \cdots < i_k \leq n} [x \in A_{i_1} \cap \cdots \cap A_{i_k}] \right) = 0$$

Therefore it suffices to show that

$$\sum_{k=0}^{n} (-1)^k \left(\sum_{1 \leq i_1 < \cdots < i_k \leq n} [x \in A_{i_1} \cap \cdots \cap A_{i_k}] \right) = 0$$

for each $x \in X$.

Observe that the sum $\sum_{1 \leq i_1 < \cdots < i_k \leq n} [x \in A_{i_1} \cap \cdots \cap A_{i_k}]$ is a count of the number of strictly increasing sequences $i_1 < \cdots < i_k$ such that $x \in A_{i_j}$ for all $1 \leq j \leq k$. If the total





Figure 3.8: Four example configurations with five stars and three bars.

number of indices i such that $x \in A_i$ is m, then the number of such strictly increasing sequences is $\binom{m}{k}$. This shows that

$$\sum_{k=0}^{n}(-1)^k\left(\sum_{1\le i_1<\cdots<i_k\le n}[x\in A_{i_1}\cap\cdots\cap A_{i_k}]\right)=\sum_{k=0}^{n}(-1)^k\binom{m}{k}$$
$$=\sum_{k=0}^{m}(-1)^k\binom{m}{k}.$$

By the binomial theorem, the latter sum equals $(1-1)^m$. Since $m \geq 1$ for each $x \in X$, we conclude that this sum is 0. This concludes the proof. □

3.7 The Stars-and-Bars Problem

The **stars-and-bars problem** is a classic counting exercise which asks in how many ways it is possible to place a linear arrangement of n bars between or at the ends of a linear arrangement of m stars. In the stars-and-bars problem it is allowed to place multiple bars successively at any valid position. In Figure 3.8 we displayed some example configurations for the stars-and-bars problem.

While the statement of the stars-and-bars problem is intuitively clear, it is good practice to precisely define stars-and-bars configurations so that there can be no ambiguity as to what is being counted. There are of course many equivalent ways of thinking about this problem, and indeed it is fruitful to try to think of a couple of them. For, if we have found two equivalent ways of thinking about a problem there must be a bijective correspondence between their representations. Furthermore, once we have found a bijection it follows by Theorem 3.1.5 (Hume's Principle) that they are equinumerous.

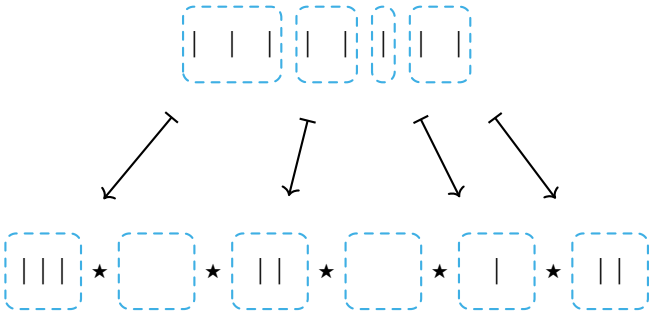


Figure 3.9: A placement of 8 bars between 5 stars.

For our definition of stars-and-bars configurations, we need to think about what it means "to place a linear arrangement of n bars between or at the ends of a linear arrangement of m stars". Since the stars and the bars are both supposed to be in linear arrangements, they can be numbered 1 through m and 1 through n, respectively. The stars separate the $m+1$ spaces in which the bars can go, so we label them 0 through m. Then, the bars are placed in those spaces, in such a way as to preserve their ordering. An example of such a placement is displayed in Figure 3.9. We observe now that all there is to a stars-and-bars configuration is an *order-preserving map* from the set $\{1, \dots, n\}$ of bars to the set $\{0, \dots, m\}$ of spaces separated by the stars.

Definition 3.7.1. A **stars-and-bars configuration** with m stars and n bars is an order-preserving map $f : \{1, \dots, n\} \to \{0, \dots, m\}$, where f is said to be **order-preserving** if it satisfies the implication

$$i \leq j \quad \Rightarrow \quad f(i) \leq f(j)$$

for all $i, j \in \{1, \dots, n\}$.

Another way of thinking about the stars-and-bars problem is that a stars-and-bars configuration is entirely determined by the number of stars between successive bars. That is, a stars-and-bars configuration is represented by a list $(s_0, \dots, s_n)$ of natural numbers, such that the total number of stars is

$$s_0 + \cdots + s_n = m.$$

Listing the number of stars in each of the four configurations displayed in Figure 3.8 gives us $(0, 0, 3, 2)$ for the first example, $(1, 3, 1, 0)$ for the second, $(2, 0, 2, 1)$ for the third, and $(0, 2, 2, 1)$ for the fourth.

Yet another way of thinking about the stars-and-bars problem is that the bars mark an n-element subset $B \subseteq \{1, \dots, m+n\}$, and the elements not in S are the bars. Now, it does not suffice to merely appreciate that each of these ways indeed model the stars-and-bars problem. We need to prove their equivalence.

THEOREM 3.7.2. *There are bijections between the following sets:*

(i) *The set of stars-and-bars configurations with m stars and n bars; that is, the set of order-preserving maps from $\{1, \dots, n\}$ to $\{0, \dots, m\}$.*

(ii) *The set of ordered $(n+1)$-tuples $(s_0, \dots, s_n)$ of natural numbers such that*

$$s_0 + \cdots + s_n = m.$$

(iii) *The set of n-element subsets of the set $\{1, \dots, m+n\}$.*

PROOF. In a stars-and-bars configuration f, the value $f(k)$ counts the stars preceding the kth bar. Successive differences therefore count the stars in the groups separated by the bars.

More precisely, put $f(0) = 0$ and $f(n+1) = m$, and define

$$s_k = f(k+1) - f(k)$$

for each $0 \leq k \leq n$. Since f is order-preserving we have $0 \leq s_k \leq m$ for each k, and their sum is

$$\sum_{k=0}^{n} s_k = f(n+1) - f(0) = m.$$

Conversely, from any such tuple we recover an order-preserving map by taking partial sums:

$$f(k) = s_0 + \cdots + s_{k-1} \qquad (1 \leq k \leq n).$$

Since successive differences and partial sums are mutual inverse operations, this gives the first bijection.

For the second, the idea is that each stars-and-bars configuration f determines the subset B_f of bar-positions in the set $\{1, \dots, m+n\}$. Observe that k^{th} bar is preceeded by $f(k)$ stars and $k-1$ bars, so we define

$$B_f := \{f(k) + k \mid 1 \leq k \leq n\}.$$

The positions $f(k) + k$ are indeed strictly increasing, since

$$f(k) + k \leq f(l) + k < f(l) + l$$

for any $1 \leq k < l \leq n$. Furthermore we have $f(n) + n \leq m + n$, so the set B_f is indeed an n-element subset of $\{1, \dots, m+n\}$, as required.

Conversely, by listing the elements of an n-element subset B of $\{1, \dots, m+n\}$ in order, we obtain a strictly increasing sequence $b_1 < \dots < b_n$. Then the map $f : \{1, \dots, n\} \to \{0, \dots, m\}$ given by

$$f(k) = b_k - k$$

is order-preserving, since

$$b_k - k \leq b_l - (l-k) - k = b_l - l$$

for every $1 \leq k \leq l \leq n$, and takes values between $0 \leq b_1 - 1$ and $b_n - n \leq (m+n) - n$. Since $(f(k) + k) - k = f(k)$ and $(b_k - k) + k = b_k$, it follows that the map $f \mapsto B_f$ is a bijection. □

The attentive reader may have already observed that stars and bars play dual roles in the stars-and-bars problem. This is most clearly seen in the last interpretation of Theorem 3.7.2 (The Stars-and-Bars Problem): An n-element subset of an $(m+n)$-element set is equivalently described by its m-element *complement*.

The **complement** of a subset A of a set X is the subset $A^c \subseteq X$ consisting of all the elements of X not in the subset A. For any two subsets A and B of X, the complement satisfies the logical equivalence

$$A \subseteq B^c \Leftrightarrow A \cap B = \emptyset.$$

That is, a subset A is contained in the complement of B if and only if A and B have no elements in common. Now observe that the complement of an n-element subset of an $(m+n)$-element set is an m-element subset. Furthermore, the operation of taking complements is a bijection

$$\{A \subseteq X \mid \#A = m\} \cong \{B \subseteq X \mid \#B = n\}.$$

Indeed, the inverse operation is again taking the complement. This bijection proves the identity

$$\binom{m+n}{m} = \binom{m+n}{n}.$$

In light of this observation, we can reverse the roles of m and n in the third statement of Theorem 3.7.2 and retain sets with the same number of elements. Now we get to the point: We can also reverse the roles of m and n in any of the other statements! We obtain the following corollaries:

Corollary 3.7.3. *There is a bijection*

$$\{(a_0, \ldots, a_m) \mid a_0 + \cdots + a_m = n\} \cong \{(b_0, \ldots, b_n) \mid b_0 + \cdots + b_n = m\}.$$

Remark 3.7.4. The previous corollary has a natural interpretation in walks on the two-dimensional integer lattice. The points on this lattice are vectors (x, y) in which each coordinate is an integer. A lattice walk starts at the origin $(0, 0)$ and each step either increases the x-coordinate by exactly 1 or increases the y-coordinate by exactly 1. The question is then, in how many ways can we walk to the point (m, n)?

Notice that a lattice walk is completely determined by specifying for each of the integers 0 through m, how many steps upwards the path should travel. For example, the first lattice walk of Figure 3.10 steps upwards 0 steps at x-coordinate 0, 2 steps at x-coordinate 1, 0 steps at x-coordinate 2, 1 step at x-coordinate 3, and 0 steps at x-coordinate 4. The total number of steps traveled upwards must be $n = 3$, so we have written n as the sum $0 + 2 + 0 + 1 + 0 = 3$. Thus we see that lattice walks from $(0, 0)$

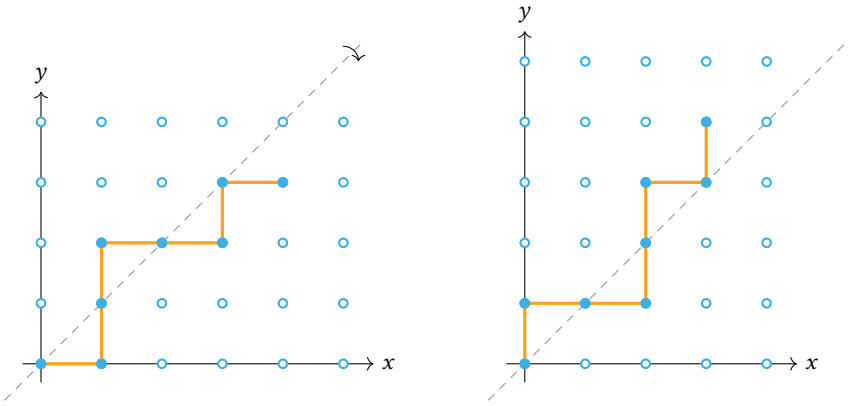


Figure 3.10: By reflecting a lattice walk through the diagonal we obtain a bijective correspondence between lattice walks to (m, n) and lattice walks to (n, m).

to (m, n) are uniquely determined by lists $(a_0, ..., a_m)$ of nonnegative integers such that $a_0 + \cdots + \cdots a_m = n$. Of such lists, there are $\binom{m+n}{n}$, as we have seen in Theorem 3.7.2.

Now, we could also flip the lattice walk about the diagonal axis, as indicated in Figure 3.10. This operation is a bijection between lattice walks from $(0, 0)$ to (m, n) and lattice walks from $(0, 0)$ to (n, m). By the previous reasoning, there are $\binom{m+n}{n}$ such lattice walks. This bijection, which is induced by the symmetry about the diagonal axis, corresponds to the bijection of Corollary 3.7.3 which was obtained via taking complements.

It also follows from Theorem 3.7.2 (The Stars-and-Bars Problem) that there is a bijection between the set of order-preserving maps

$$f : \{1, \dots, n\} \to \{0, \dots, m\}$$

and the set of order-preserving maps

$$g : \{1, \dots, m\} \to \{0, \dots, n\}.$$

This bijection has some nice properties, but they are best expressed if we extend the domain of f to include 0 and set $f(0) = 0$, and the domain of g to include 0 and set $g(m) = n$.

THEOREM 3.7.5. *There is a bijective correspondence between order-perserving maps*

$$f : \{0, \dots, n\} \to \{0, \dots, m\}, \qquad f(0) = 0$$

and order-preserving maps

$$g : \{0, \dots, m\} \to \{0, \dots, n\}, \qquad g(m) = n,$$

characterized by the logical equivalence

$$f(x) \leq y \quad \Leftrightarrow \quad x \leq g(y) \tag{$*$}$$

for all $0 \leq x \leq n$ *and* $0 \leq y \leq m$.

Proof. We begin the proof by showing that for any order-preserving map f satisfying $f(0) = 0$, there is at most one map g satisfying $*$. Indeed, if g' is another such map, we get

$$g(y) \leq g(y) \quad \Rightarrow \quad f(g(y)) \leq y \quad \Rightarrow \quad g(y) \leq g'(y),$$

showing that $g(y) \leq g'(y)$. Interchanging g and g' gives the reverse inequality, so we conclude that $g(y) = g'(y)$. Any map g satisfying $*$ is order-preserving. Indeed, given $y \leq z$, we obtain the implication $f(x) \leq y \Rightarrow f(x) \leq z$, which gives $x \leq g(y) \Rightarrow x \leq g(z)$. By choosing $x = g(y)$ we conclude that $g(y) \leq g(z)$. Moreover, the map g satisfies $g(m) = n$ since $f(n) \leq m$ holds.

By the same argument, it follows that for any order-preserving map g satisfying $g(m) = n$, there is at most one map f satisfying $*$, which is necessarily order-preserving and satisfies $f(0) = 0$.

Let $f : \{0, \dots, n\} \to \{0, \dots, m\}$ be an order-preserving map satisfying $f(0) = 0$. For any $0 \leq y \leq m$, we define

$$g(y) := \max\{0 \leq x \leq n \mid f(x) \leq y\}.$$

This maximum is always attained, since $f(0) = 0$. By its very definition, the function g satisfies the logical equivalence $*$.

Conversely, for any order-preserving map $g : \{0, \dots, m\} \to \{0, \dots, n\}$ satisfying $g(m) = n$ the function f given by

$$f(x) := \min\{0 \leq y \leq m \mid x \leq g(y)\}$$

is well-defined since $g(m) = n$, and also satisfies the logical equivalence $*$ by its very definition. □

Remark 3.7.6. The Canadian mathematician André Joyal observed that duality between order-preserving maps $\{1, \dots, n\} \to \{0, \dots, m\}$ and order-preserving maps $\{1, \dots, m\} \to \{0, \dots, n\}$ can be generalized to a duality between planar trees and a combinatorial structure called disks [Joy1997].

Exercises

Starter Exercises

3.1 In the empty copy of Pascal's triangle at the end of this chapter, shade all the positions of the odd binomial coefficients. It is not necessary to compute them all.

3.2 Prove that $2^n < n!$ for all $n \geq 4$.

3.3 Prove that

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

in three different ways: using the binomial theorem, by a direct proof by induction, and by a combinatorial proof.

3.4 Consider an n-element set X. We call a bijection $f : X \cong X$ **transitive** if X is inhabited and for every two elements $x, y \in X$, there exists a natural number k such that $f^k(x) = y$. How many transitive bijections are there on X?

3.5 Find the first 20 positive integers that are not divisible by any Fibonacci number other than 1.

Routine-Building Exercises

3.6 Show that the strict inequalities

$$\frac{4^n}{2n+1} < \binom{2n}{n} < 4^n$$

hold for all $n \geq 1$.

3.7 For $n \geq 1$, prove that

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0.$$

Conclude that

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} = \sum_{k=0}^{\lfloor (n-1)/2 \rfloor} \binom{n}{2k+1}.$$

In this formula, the floor $\lfloor x \rfloor$ of a number x is the largest integer below or equal to x.

3.8 *The hockey-stick identity.* Show that

$$\sum_{i=k}^{m} \binom{i}{k} = \binom{m+1}{k+1}.$$

3.9 *The Chu–Vandermonde identity.* The **Chu–Vandermonde identity** asserts that

$$\binom{m+n}{k} = \sum_{i=0}^{k} \binom{m}{i} \binom{n}{k-i}.$$

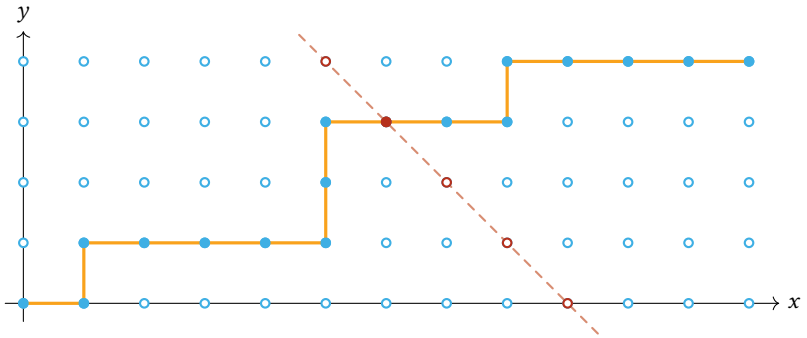


Figure 3.11: Every lattice walk from $(0, 0)$ to $(12, 4)$ must pass through exactly one of the lattice points on the line $x + y = 9$.

(a) Use the binomial theorem at the polynomial $(x + 1)^m(x + 1)^n$ to prove the Chu–Vandermonde identity.
(b) Use the suggestion of Figure 3.11 to give a lattice-walk interpretation of the Chu–Vandermonde identity.

3.10 Show that

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

The binomial coefficient $\binom{2n}{n}$ is also called the **central binomial coefficient**.

3.11 Define a bijection between ordered triples (a, b, c) of positive integers such that $a + b + c = n$ and the set of 2-element subsets of $\{1, \dots, n - 1\}$, and use this to determine the number of such ordered triples.

3.12 Consider an arbitrary subset A of the natural numbers, and let the sets $\mathscr{P}_{\text{even}}(A)$ and $\mathscr{P}_{\text{odd}}(A)$ be defined as follows:

$$\mathscr{P}_{\text{even}}(A) := \left\{S \subseteq A \;\middle|\; S \text{ is finite and } \textstyle\sum_{s\in S} s \text{ is even}\right\},$$
$$\mathscr{P}_{\text{odd}}(A) := \left\{S \subseteq A \;\middle|\; S \text{ is finite and } \textstyle\sum_{s\in S} s \text{ is odd}\right\}.$$

Show that there is a bijection bijection $f : \mathscr{P}_{\text{even}}(A) \to \mathscr{P}_{\text{odd}}(A)$ if and only if the set A contains an odd number. Use this bijection to conclude that for $n \geq 1$, there are exactly 2^{n-1} subsets $S \subseteq \{1, \dots, n\}$ whose sum of elements is even.

Challenge Exercises

3.13 Show that

$$\sum_{k=0}^{n} \prod_{i=0}^{m} (k + i) = (m + 1)! \binom{n + m + 1}{m + 2}.$$

3.14 (a) Show that in the nth row of Pascal's triangle all the entries are odd precisely when $n = 2^k - 1$ for some k.

(b) Show that in each row of Pascal's triangle, the number of odd entries is always a power of 2.

3.15 A **derangement** is a bijection $f : A \to A$ such that $f(x) \neq x$ for every $x \in A$. We define the **derangement number** $!n$ to be the number of derangements on an n-element set.

(a) Compute $!n$ for $0 \leq n \leq 6$.

(b) Show that the derangement numbers satisfy the following recurrence relation:

$$!(n+2) = (n+1)(!(n+1) + !n).$$

(c) Use the principle of inclusion–exclusion to show that

$$!n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

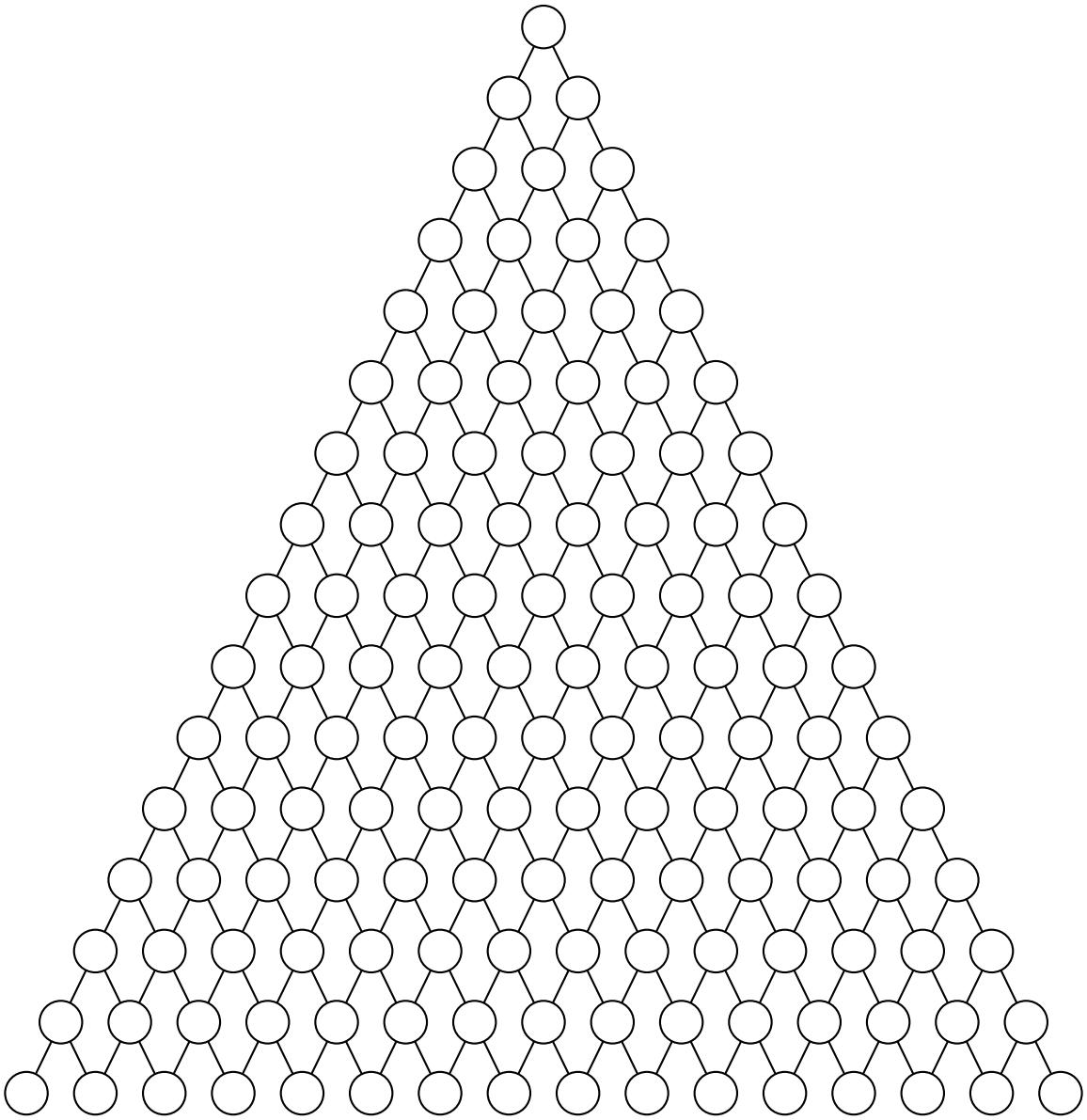


Figure 3.12: Shade all the circles in which the binomial coefficient is odd.

Chapter 4

The Integers

4.1 Cyclic Sets

Natural numbers count elements of finite sets. The empty set has zero elements, the set of solutions to the equation $3x - 3 = 0$ has exactly one element, the booleans have exactly two elements, true and false, and so on.

Natural numbers have been around for at least as long as humans count. But what do negative numbers count? Surely, there are no sets with -5 elements! One explanation of negative numbers is that they represent deficits. In other words, integers can be thought of as *differences* between natural numbers. This point of view is completely valid, and we will come back to it. There is, however, a more structural and conceptually compelling way of thinking about integers, using cyclic sets. Cyclic sets are an often recurring structure in mathematics. Some of the prettiest proofs of Theorem 16.1.1 (Fermat's Little Theorem) and Theorem 16.3.1 (Wilson's Theorem) use them.

When we map out a bijection $f : A \to A$ from a finite set A to itself by displaying an arrow between each element and its value under f, as we did in Figure 4.1, we discover that the finite set A gets partitioned into cycles. The iterated action of f on an element a is mapped out by tracing along the arrows, which eventually loops back to itself. An intuitive reason for this phenomenon is that by iterating f often enough, we obtain a sequence

$$a,\ f(a),\ f^2(a),\ \ldots$$

which must eventually have repeated values since the set A was assumed to be finite. If $f^n(a)$ is the first n such that $f^n(a) = f^m(a)$ for a later value of m, then we must have

$n = 0$. Indeed, if $n > 0$ then we find that

$$f(f^{n-1}(a)) = f(f^{m-1}(a)),$$

which implies by the assumption that f is a bijection that $f^{n-1}(a) = f^{m-1}(a)$. This is impossible by the minimality of n, so we must have $n = 0$. We conclude that the iterations of f trace out cycles. Such cycles are called *orbits*.

DEFINITION 4.1.1. Consider a bijection $f : X \cong X$. We say that $x, y \in X$ are **in the same orbit** of f if there exists a natural number k such that $f^k(x) = y$ or $f^k(y) = x$.

A subset $U \subseteq X$ is an **orbit** of f if there exists an element $x \in X$, such that U consists of exactly the elements in the same orbit as x.

The bijection on the 12-element set in Figure 4.1, for example, has four such orbits. Since bijections on a set partition the set into cyclic orbits, we can now define a *cyclic set* to be a set equipped with a bijection that has exactly one orbit, so that all the elements of the set fit in the same cycle. In Figure 4.2 we displayed an example of a cyclic set.

DEFINITION 4.1.2. A **cyclic set** is a pair (X, s) consisting of a set X and a bijection $s : X \cong X$ that has exactly one orbit.

REMARK 4.1.3. Since orbits are assumed to be inhabited—that is, nonempty—subsets of a set X, it follows that cyclic sets are always inhabited. Indeed, if U is the unique orbit of a cyclic set, and U is inhabited by an element $x \in U$, then we have $x \in X$. Thus, empty sets are not considered to be cyclically structured.

EXAMPLE 4.1.4. Every inhabited standard finite set can be given the structure of a cyclic set. The cyclic structure on the standard finite set $[n+1]$ is given by

$$0 \mapsto 1 \mapsto 2 \mapsto \cdots \mapsto n \mapsto 0.$$

To define this function precisely, observe that there are two functions $\iota, \sigma : [n] \to [n+1]$ given by

$$\iota(x) = x \qquad \text{and} \qquad \sigma(x) = x + 1.$$

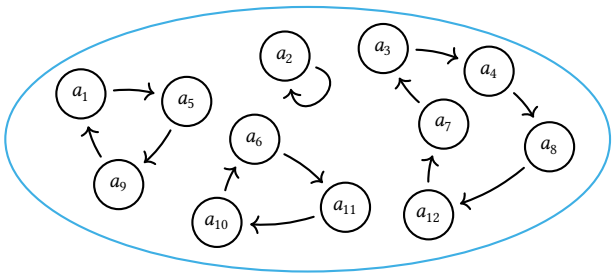


Figure 4.1: A bijection on a 12-element set.

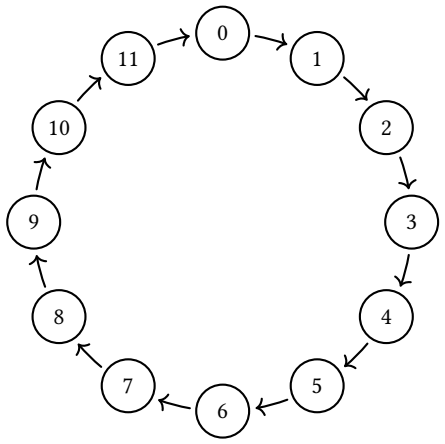


Figure 4.2: A cyclic set with 12 elements.

These allow us to define the successor function S and its inverse T as follows:

$$S(x) = \begin{cases} \sigma(y) & \text{if } x = \iota(y), \\ 0 & \text{if } x = n, \end{cases} \qquad T(x) = \begin{cases} \iota(y) & \text{if } x = \sigma(y), \\ n & \text{if } x = 0. \end{cases}$$

Thus, we obtain a cyclic set $([n+1], 0, S)$ for each n.

4.2 Maps Preserving Cyclic Structure

An important organizational principle of structural mathematics is that when we define a certain kind of structured sets, such as cyclic sets in our case, then it is good practice to also define the *structure-preserving maps* between them. Doing so allows us to learn more about how such structured sets relate to each other. Thus, we will now introduce cyclic-structure maps. As we will see shortly, maps preserving the cyclic structure on a set have some interesting properties, and they feature prominently in our structural definition of the set of integers.

Definition 4.2.1. Consider two cyclic sets (X, s) and (Y, t). A map $f : X \to Y$ is said to be a **cyclic-structure map** if

$$f(s(x)) = t(f(x))$$

for every $x \in X$. We will write $\hom((X, s), (Y, t))$ for the set of all cyclic-structure maps from (X, s) to (Y, t).

For example, if (X, s) is a cyclic set, then s is always a cyclic-structure map onto itself. To see this, we simply note that the equality

$$s(s(x)) = s(s(x))$$



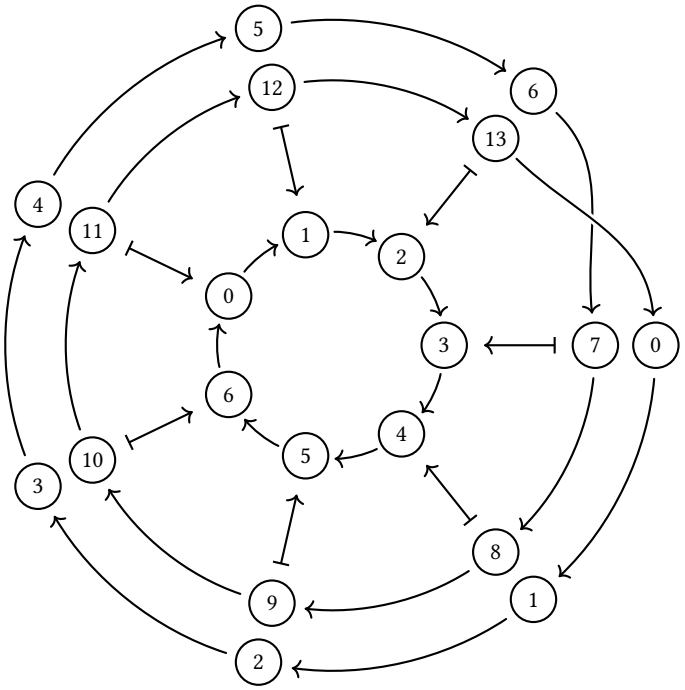


Figure 4.3: A cyclic-structure map from a 14-element set to a 7-element set.

holds trivially. In Figure 4.3 we displayed an example of a cyclic-structure map from a 14-element set to a 7-element set. More generally, the idea of a cyclic-structure map is that we can overlay the elements of a cyclic set X onto the elements of a cyclic set Y so that the cyclic structure of the overlay matches the cyclic structure of Y. This means that in a cyclic-structure map, we can't skip any elements.

THEOREM 4.2.2. *Consider two cyclic sets (X, s) and (Y, t) with a cyclic-structure map $f : X \to Y$ between them. If X is an m-element set and Y is an n-element set, then m is a multiple of n.*

PROOF. For each $y \in Y$ consider the set

$$f^{-1}(y) := \{x \in X \mid f(x) = y\}$$

consisting of all the elements in X that have the value y under f. Then the bijection $s : X \to X$ restricts to a bijection

$$s : f^{-1}(y) \to f^{-1}(s(y)).$$

Thus it follows that all the sets of the form $f^{-1}(y)$ have the same size. Since X is the union of these sets, it follows that the size of X is n times the size of the set $f^{-1}(y)$. □

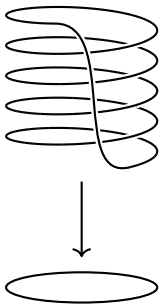


Figure 4.4: Cyclic-structure maps are defined by "winding" the source cyclic set around the target cyclic set.

Cyclic-structure maps have the special property that if they share an equal value for a given input, then they are equal everywhere. Indeed, suppose that $f, g : X \to Y$ are two cyclic-structure maps between cyclic sets (X, s) and (Y, t) such that $f(x) = g(x)$ for some $x \in X$. By the cyclic structure of X, it follows that for every $x' \in X$, there exists a natural number k such that $s^k(x) = x'$ or $s^k(x') = x$. Thus there are two cases to consider. If $s^k(x) = x'$ then it follows that

$$f(x') = f(s^k(x)) = s^k(f(x)) = s^k(g(x)) = g(s^k(x)) = g(x').$$

On the other hand, if $s^k(x') = x$ then it follows that $f(x') = g(x')$ if and only if $s^k(f(x')) = s^k(g(x'))$, which follows from the calculation

$$s^k(f(x')) = f(s^k(x')) = f(x) = g(x) = g(s^k(x')) = s^k(g(x')).$$

The previous observation can be used to prove the following theorem:

Theorem 4.2.3. *Consider two cyclic sets (X, s) and (Y, t). If the set*

$$\hom((X, s), (Y, t))$$

of cyclic-structure maps from (X, s) to (Y, t) is inhabited, then it is itself a cyclic set.

Proof. The function $h \mapsto t \circ h$ is a bijection from $\hom((X, s), (Y, t))$ to itself. To see that it has exactly one orbit, consider two cyclic-structure maps $f, g : X \to Y$, and let $x_0 \in X$. Then there exists an integer k such that

$$t^k(f(x_0)) = g(x_0) \qquad \text{or} \qquad t^k(g(x_0)) = f(x_0).$$

In the first case it follows that $t^k \circ f = g$, while in the second case it follows that $t^k \circ g = f$. Thus it follows that f and g are in the same orbit of the map $h \mapsto t \circ h$. □

The organizational principle of defining structured sets along with their structure-preserving maps comes from *category theory*, a mathematical discipline which emphasizes structural mathematics. What we have defined here is the category of cyclic

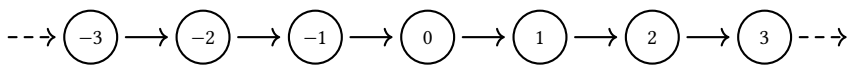


Figure 4.5: The infinite cyclic set of integers.

sets. In this course we won't rely on category theory, but the curious reader might find Emily Riehl's book *Category Theory in Context* of interest [RIE2016]. Riehl is a world-famous professor in our department.

4.3 A Structural Definition of the Integers

Although the examples we have discussed so far are finite, the definition of cyclic sets isn't restricted to finite sets. We could indeed imagine a very large cyclic set that extends infinitely in both directions, as in Figure 4.5. If such a set has a designated zero element, we could use it as the starting point to describe the other elements as the iterated successors and the iterated predecessors. This way, we would expect to find one element for each integer. Alternatively, as we are about to do now, we could take the infinite cyclic set as the definition of the set of integers!

DEFINITION 4.3.1. The set of **integers** is specified to be a set $\mathbb{Z}$ equipped with a distinguished **zero** element $0 \in \mathbb{Z}$ and a **successor** bijection $S : \mathbb{Z} \cong \mathbb{Z}$ such that for every set X, every element x_0 and every bijection $h : X \cong X$ uniquely determine a function $f : \mathbb{Z} \to X$ such that

(i) $f(0) = x_0$, and

(ii) $f(S(a)) = h(f(a))$ for every $a \in \mathbb{Z}$.

Such functions are said to be defined by **integer recursion**. We will commonly write $a \mapsto a + 1$ for the successor function S, and $a \mapsto a - 1$ for its inverse.

For example, integer recursion can be used to define *iterated bijections* $f^k : A \cong A$ for any bijection $f : A \cong A$. The idea is entirely analogous to the idea of iterated functions, where a function $f : A \to A$ could be iterated any natural number of times. For iterated bijections, we restrict to the case of a bijection $f : A \cong A$, which allows us to also consider the *negative iterations* of f by using the inverse of f. In order to formally define iterated bijections, we need the following theorem:

THEOREM 4.3.2. *For any bijection $f : A \cong B$ and any set X, there are bijections*

$$- \circ f : (B \cong X) \cong (A \cong X)$$
$$f \circ - : (X \cong A) \cong (X \cong B).$$

PROOF. Suppose $f : A \cong B$ is a bijection with inverse f^{-1}. Then for any bijection $g : B \cong X$ we have

$$g \circ f \circ f^{-1} = g,$$

and for any $h : A \cong B$ we have

$$h \circ f^{-1} \circ f = h.$$

This shows that the function $- \circ f^{-1}$ is inverse to the function $- \circ f$. Similarly $f^{-1} \circ -$ is inverse to the function $f \circ -$. □

Definition 4.3.3. Consider a set X equipped with a bijection $f : X \cong X$. Then we define for each integer k the kth **iteration** of f by

$$f^0 := \mathrm{id}$$
$$f^{k+1} := f \circ f^k.$$

This definition is possible, since composing with f on the left is a bijection $(X \cong X) \cong (X \cong X)$.

The specification of the set of integers with integer recursion also allows us to formulate an induction principle for the integers. This induction principle states what one should do in order to show that a proposition $P(x)$ is true for all integers x. The induction principle for the integers was first formulated by Angelo Margaris [Mar1961].

Theorem 4.3.4 (Integer Induction Principle). *Consider a property $P(a)$ parametrized by an integer a. In order to prove that $P(a)$ is true for all a, it suffices to prove:*

(i) *The property $P(0)$ is true.*

(ii) *The logical equivalence $P(a) \Leftrightarrow P(a+1)$ holds for all $a \in \mathbb{Z}$.*

Note the similarity with the induction principle of the natural numbers: We have to prove a base case and an inductive step. However, in the inductive step we have to prove two directions:

$$P(a) \Rightarrow P(a+1) \qquad \text{and} \qquad P(a+1) \Rightarrow P(a).$$

In other words, there are two steps in the inductive step: the *forward step* and the *backward step*. In the forward step, you will assume $P(a)$ as the inductive hypothesis as usual, and the task is to prove that $P(a+1)$ holds. In the backward step, you will assume $P(a+1)$ is true, and the task is to prove that $P(a)$ holds. In §4.5 we will use the integer induction principle to prove the laws for integer arithmetic.

Proof. Consider a property $P(a)$ of the integers, such that $P(0)$ is true and for which the logical equivalence

$$P(a) \Leftrightarrow P(a+1)$$

holds. In order to show that $P(a)$ is true for every integer a, we will use the recursion principle for $\mathbb{Z}$. Thus, we have to construct a set A equipped with an element $a_0 \in A$ and a bijection $s : A \cong A$. We define the set A by

$$A := \{a \in \mathbb{Z} \mid P(a)\},$$

so that A consists of exactly those integers a for which $P(a)$ holds. Clearly, we have $0 \in A$, so we choose $a_0 := 0$. In order to define a function $s : A \to A$, observe that for $a \in A$, the property $P(a)$ holds by assumption, which implies $P(a+1)$ so that $a+1 \in A$. Thus, we simply define $s(a) := a + 1$.

To see that s is a bijection, we define an inverse t. For any $a \in A$, observe that the logical equivalence $P(a-1) \Leftrightarrow P(a)$ holds, since $(a-1)+1 = a$, so it follows that $P(a-1)$ holds. This allows us to define $t(a) := a - 1$. It follows immediately from the definition of t that the identities $s(t(a)) = a$ and $t(s(a)) = a$ hold. Thus we see that t is an inverse of s, which concludes the proof that s is a bijection on A.

By the specification of $\mathbb{Z}$, it follows that there is a unique function $f : \mathbb{Z} \to A$ such that

$$f(0) = 0 \qquad \text{and} \qquad f(S(a)) = S(f(a)).$$

Now we claim that $f(a) = a$ for all $a \in \mathbb{Z}$. To see this, note that by the inclusion of $A \subseteq \mathbb{Z}$ we may regard f as a function $\mathbb{Z} \to \mathbb{Z}$ satisfying the equations

$$f(0) = 0 \qquad \text{and} \qquad f(a+1) = s(f(a)) = f(a) + 1.$$

However, there is a known function satisfying these equations: the *identity function* $x \mapsto x$, which is often denoted by id. Since f is uniquely determined by its equations, which are also satisfied by the identity function, it follows that f and the identity function must be the same. Thus it follows that $f(a) = a$ for all $a \in \mathbb{Z}$. Furthermore, since we have $f(a) \in A$ by definition, we obtain that $a \in A$ for every integer a. Thus we conclude that the property $P(a)$ holds for all $a \in \mathbb{Z}$. □

The induction principle for the integers may be used, for instance, to prove that the integers form a cyclic set.

THEOREM 4.3.5. *The pair $(\mathbb{Z}, S)$ consisting of the set $\mathbb{Z}$ of integers and the successor bijection S is a cyclic set. Furthermore, for any cyclic set (Y, t) with a distinguished element y_0, there is a unique cyclic-structure preserving map f from $(\mathbb{Z}, S)$ to (Y, t) satisfying $f(0) = y_0$.*

PROOF. We show by integer induction that every integer is in the orbit of 0. Clearly 0 is in its own orbit, so the base case is trivial. For the inductive step, we have to show that x is in the orbit of 0 if and only if $S(x)$ is.

Suppose first that x is in the orbit of 0. If $S^k(0) = x$ for some natural number k, then $S^{k+1}(0) = S(x)$. Otherwise, $S^k(x) = 0$ for some natural number k. The case $k = 0$ gives $x = 0$ and is already covered. We may therefore write $k = k' + 1$, and we obtain $S^{k'}(S(x)) = 0$. In either case, $S(x)$ is in the orbit of 0.

Conversely, suppose that $S(x)$ is in the orbit of 0. If $S^k(0) = S(x)$ for some natural number k, we distinguish two cases. If $k = 0$, then $S(x) = 0$, so x is in the orbit of 0. If $k = k' + 1$, injectivity of S gives $S^{k'}(0) = x$. Alternatively, if $S^k(S(x)) = 0$ for some natural number k, then $S^{k+1}(x) = 0$. Thus x is in the orbit of 0, completing the induction.

The final claim follows from the integer recursion principle. □

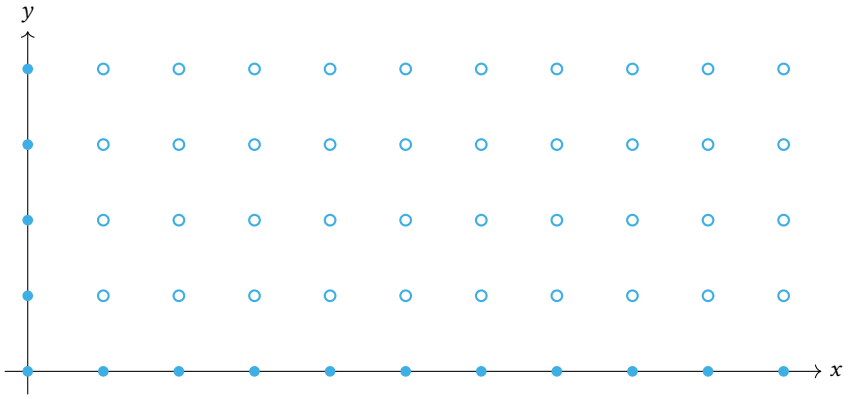


Figure 4.6: The set Z consists of the lattice points on the coordinate axes whose coordinates are natural numbers. Along the axis of abscissas we find the nonnegative integers in their usual positions, while along the axis of ordinates we find the nonpositive integers.

Theorem 4.3.6. *Let the inclusion of the naturals into the integers $i : \mathbb{N} \to \mathbb{Z}$ be defined by*

$$\begin{aligned} i(0) &:= 0, \\ i(n+1) &:= S(i(n)). \end{aligned}$$

Then 0 is not of the form $S(i(n))$, for any natural number n.

Proof. Suppose that $0 = S(i(n)) = i(n+1)$ for some natural number n. Recall from Example 4.1.4 that the set $\{0, \dots, n+1\}$ has the structure of a cyclic set with successor map S. Integer recursion therefore gives us a function $f : \mathbb{Z} \to \{0, \dots, n+1\}$ satisfying the equations

$$f(0) = 0 \qquad \text{and} \qquad f(a+1) = S(f(a)).$$

Since $S(x) = x+1$ for each $0 \leq x \leq n$, it follows that $f(i(x)) = x$ for each $0 \leq x \leq n+1$. Now we obtain a contradiction with Theorem 2.4.2:

$$0 = f(0) = f(i(n+1)) = n+1. \qquad \square$$

4.4 Constructing the Integers from the Natural Numbers

We have given a structural definition of the set of integers as the universal cyclic set. We think of this as the *specification* of the integers. In this section we will construct a set that meets this specification.

DEFINITION 4.4.1. We define the set $\mathbb{Z}_C$ of **cartesian integers** by

$$\mathbb{Z}_C := \{(a,b) \in \mathbb{N} \times \mathbb{N} \mid ab = 0\}.$$

The **zero-element** of $\mathbb{Z}_C$ is defined to be the element $(0,0)$. We define the **successor function** $s : \mathbb{Z}_C \to \mathbb{Z}_C$ recursively on b by

$$\begin{aligned} s(a,0) &:= (a+1,0) \\ s(a,b+1) &:= (a,b). \end{aligned}$$

THEOREM 4.4.2. *The successor function $s : \mathbb{Z}_C \to \mathbb{Z}_C$ is a bijection.*

PROOF. We prove that it is a bijection by constructing its inverse $t : \mathbb{Z}_C \to \mathbb{Z}_C$. The function t is defined recursively on a by

$$\begin{aligned} t(0,b) &:= (0,b+1) \\ t(a+1,b) &:= (a,b). \end{aligned}$$

The proof that $s \circ t = \mathrm{id}$ is by induction on a. We have $s(t(0,b)) = s(0,b+1) = (0,b)$ proving the base case, and we have

$$s(t(a+1,b)) = s(a,b) = (a+1,b)$$

since $b = 0$ in this case.

Similarly, the proof that $t \circ s = \mathrm{id}$ is by induction on b. We have $t(s(a,0)) = t(a+1,0) = (a,0)$ proving the base case, and we have

$$t(s(a,b+1)) = t(a,b) = (a,b+1)$$

since $a = 0$ in this case. This completes the proof that t is an inverse of s, and hence s is a bijection. □

THEOREM 4.4.3. *The set $\mathbb{Z}_C$ equipped with the distinguished zero element $(0,0)$ and the successor function s satisfies the specification of the integers in Definition 4.3.1.*

PROOF. Consider a set X equipped with a point $x_0 \in X$ and a bijection $h : X \cong X$. Then we define a function $f : \mathbb{Z}_C \to X$ by recursion on a and b:

$$\begin{aligned} f(0,0) &:= x_0 \\ f(a+1,0) &:= h(f(a,0)) \\ f(0,b+1) &:= h^{-1}(f(0,b)). \end{aligned}$$

This function satisfies $f(0,0) = x_0$ by definition. We claim that

$$f(s(a,b)) = h(f(a,b))$$

for every $(a, b) \in \mathbb{Z}_C$. The proof is by induction on b. For the base case, observe that the equalities $f(s(a,0)) = f(a+1,0) = h(f(a,0))$ hold by definition. For the inductive step, note that the equality $f(0, b+1) = h^{-1}(f(0,b))$ implies that $h(f(0,b+1)) = f(0,b)$. Using this, we obtain

$$f(s(0,b+1)) = f(0,b) = h(f(0,b+1)).$$

Thus far, we have proven that there exists a function $f : \mathbb{Z}_C \to X$ satisfying

$$f(0,0) = x_0 \qquad \text{and} \qquad f(s(a,b)) = h(f(a,b)).$$

It remains to show that this function f is unique. □

Knowing that there is a set that meets the specification in Definition 4.3.1, we shall now abandon the set $\mathbb{Z}_C$ again, and we will consider $\mathbb{Z}$ to be an arbitrary set as specified in Definition 4.3.1.

4.5 Integer Arithmetic

We can now define addition of two integers, just as we did for the natural numbers, by using the iterated successor bijection. Furthermore, since iterated bijections are again bijections, we obtain something that we didn't get for the natural numbers: For every integer y there is a unique integer x such that $x + a = y$. In other words, we can define differences of integers.

Definition 4.5.1. We will define **addition** of two integers and the **additive inverse** of an integer:

(i) For any two integers a and b, we define

$$a + b := S^b(a),$$

where S^b is the bth iteration of the successor function $S : \mathbb{Z} \cong \mathbb{Z}$. Henceforth, we will write $a + 1$ for $S(a)$.

(ii) For any integer a, we define $-a$ to be the unique element in the set

$$\{x \in \mathbb{Z} \mid x + a = 0\}.$$

Such an element is indeed uniquely determined, since S^a is a bijection.

Before we start proving the laws of addition and the additive inverse of the integers, we will show how addition interacts with iteration.

Theorem 4.5.2. *For any bijection $f : X \cong X$ with inverse f^{-1}, and for any $x \in X$, we have*

$$f^{a+b}(x) = f^b(f^a(x))$$
$$f^{-a}(x) = (f^{-1})^a(x).$$

PROOF. For the first identity, we will use Theorem 4.3.4 (Integer Induction Principle) on b. It is clear that

$$f^{a+0}(x) = f^a(x) = f^0(f^a(x)),$$

so the base case holds. To see that

$$f^{a+b}(x) = f^b(f^a(x)) \quad \Leftrightarrow \quad f^{a+(b+1)}(x) = f^{b+1}(f^a(x))$$

note that $f^{a+(b+1)}(x) = f(f^{a+b}(x))$ and $f^{b+1}(f^a(x)) = f(f^b(f^a(x)))$. Furthermore, since f is a bijection, it follows that $f(y) = f(z)$ if and only if $y = z$. In our case we get:

$$\begin{aligned} f^{a+b}(x) = f^b(f^a(x)) &\Leftrightarrow f(f^{a+b}(x)) = f(f^b(f^a(x))) \\ &\Leftrightarrow f^{a+(b+1)}(x) = f^{b+1}(f^a(x)). \end{aligned}$$

This completes the proof of the first identity. The second identity is proven by integer induction on a. Since $-0 = 0$, it follows that

$$f^{-0}(x) = f^0(x) = x = (f^{-1})^0(x).$$

For the inductive step, we calculate in similar fashion:

$$\begin{aligned} f^{-a}(x) = (f^{-1})^a(x) &\Leftrightarrow f^{-(a+1)+1}(x) = f(f^{-1}((f^{-1})^a(x))) \\ &\Leftrightarrow f(f^{-(a+1)}(x)) = f((f^{-1})^{a+1}(x)) \\ &\Leftrightarrow f^{-(a+1)} = (f^{-1})^{a+1}(x). \end{aligned}$$

□

THEOREM 4.5.3. *Addition of integers satisfies the following laws:*

$$\begin{aligned} (a+b)+c &= a+(b+c), & a+(b+1) &= (a+b)+1, \\ a+0 &= a, & (a+1)+b &= (a+b)+1, \\ 0+a &= a, & a+b &= b+a. \\ a-a &= 0, \end{aligned}$$

PROOF. By the previous theorem, we calculate:

$$(a+b)+c = S^c(S^b(a)) = S^{b+c}(a) = a+(b+c).$$

Next, note that the unit law $a+0=a$ holds because

$$a+0 = S^0(a) = a$$

Similarly, we note that $0+a=a$ by induction on a. The base case is covered in the previous step. For the inductive step, we have to show that

$$0+a=a \quad \Leftrightarrow \quad 0+(a+1)=a+1.$$

This can be seen by chaining the injectivity of the successor function and associativity:

$$\begin{aligned} 0 + a = a &\Leftrightarrow (0 + a) + 1 = a + 1 \\ &\Leftrightarrow 0 + (a + 1) = a + 1. \end{aligned}$$

The fact that $a - a = 0$ follows from the observation that

$$a - a = (0 + a) - a = S^{-a}(S^a(0)) = 0.$$

The right successor law $a + (b + 1) = (a + b) + 1$ is an instance of the associativity law, which we have already shown. On the other hand, the left successor law $(a + 1) + b = (a + b) + 1$ is proven by induction on b.

The two unit laws $a + 0 = a$ and $0 + a = a$ combined settle the base case for the inductive proof that $a + b = b + a$. For the inductive step, we have to show that

$$a + b = b + a \quad \Leftrightarrow \quad a + (b + 1) = (b + 1) + a.$$

This follows from the injectivity of the successor function and the left and right successor laws that we have previously shown. □

Next, we define multiplication of integers.

Definition 4.5.4. We define the **multiplication operation** $a, b \mapsto ab$ on the integers by

$$\begin{aligned} a0 &:= 0 \\ a(b + 1) &:= ab + a \end{aligned}$$

This well-defined, since for any integer a, the function $x \mapsto x + a$ is a bijection.

Theorem 4.5.5. *Multiplication of integers distributes from both sides over addition: For any three integers a, b, and c we have*

$$a(b + c) = ab + ac \qquad \text{and} \qquad (a + b)c = ac + bc.$$

Proof. We will prove only the first equation, leaving the other equation as an exercise. To show that multiplication of the integers distributes from the left over addition, we will use integer induction on c to show that for any two integers a and b we have $a(b + c) = ab + ac$.

In the base case, we simply note that

$$a(b + 0) = ab = ab + 0 = ab + a0.$$

For the inductive step, we have to show that

$$\forall_{a,b\in\mathbb{Z}} a(b + c) = ab + ac \quad \Leftrightarrow \quad \forall_{a,b\in\mathbb{Z}} a(b + (c + 1)) = ab + a(c + 1).$$

For the forward implication, assume that $a(b+c) = ab+ac$ is true for any two integers a and b. Then we have

$$a(b + (c + 1)) = a((b + 1) + c) = a(b + 1) + ac = ab + a + ac = ab + a(c + 1).$$

For the reverse implication, assume that $a(b + (c + 1)) = ab + a(c + 1)$ is true for any two integers a and b. Then we have

$$a(b + c) = a((b - 1) + (c + 1)) = a(b - 1) + a(c + 1) = ab - a + ac + a = ab + ac. \quad \square$$

Exercises

Routine-Building Exercises

4.1 Show that multiplication of integers is associative: For any three integers a, b, and c we have

$$(ab)c = a(bc).$$

4.2 Show that multiplication of integers is commutative: For any two integers a and b we have

$$ab = ba.$$

4.3 Show that multiplication with a nonzero integer a satisfies the cancellation law

$$ax = ay \quad \Rightarrow \quad x = y.$$

4.4 Prove that for any two integers a and b, either $b \leq a$ or $a \leq b$.

Foundational Exercises

4.5 Consider a bijection $f : X \cong X$, and let $x \in X$. Show that a subset $U \subseteq X$ is the orbit of x if and only if U is the intersection of all subsets $V \subseteq X$ containing x, such that $f(V) = V$.

4.6 Consider a bijection $f : X \cong X$, and let $x \in X$. Show that the image of the unique map $h : \mathbb{Z} \to X$ determined by x and f is a cyclic set.



Chapter 5

Notation for Numbers

5.1 Some Remarks on the History of Written Numbers

The *decimal representation* of integers is well-embedded in our culture: Any integer can be uniquely represented as a sequence of digits from 0 to 9, where the leading digit is nonzero. When we write a number such as 231, it represents the number two hundred and thirty-one, which consists of two lots of hundred, three lots of ten and one unit. Similar representations exists in binary (using only the digits 0 and 1), and in hexadecimal notation (using the digits 0 to 9 and the letters A to F representing digits of values 10 through 15). The binary representation of the number 231 is $(11100111)_2$, while the hexadecimal representation of this number is $(E7)_{16}$. In each of these representations of the number 231, the position of the digits relative to each other is significant for its value. Such ways of writing numbers are therefore called **positional**. Positional number systems have a long history, going back to the Sumerians in ancient Mesopotamia. The Sumerians were known for using a *sexagesimal* system, which is in base 60. They used cuneiform script, which was also the earliest form of writing.

On the other side of the world, the Mayans developed roughly between 400 BCE and 150 CE a *vigesimal* numerical system; that is, a system base 20. Notably, there was no contact between the Mayans in Mesoamerica and civilizations in Africa, Asia, or Europe. They had thus developed their number system entirely independently, and conversely their number system did not influence the Indian and Arabic developments which would eventually make its way into the modern mathematical tradition. The Mayans were the first known civilization to have notation for the number 0.

Although zero was conceived independently by the Mayans, the modern digit 0 has



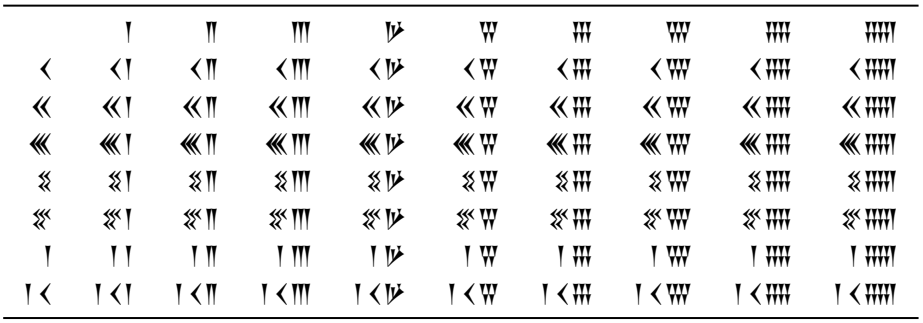


Figure 5.1: The sexagesimal system in cuneiform script was developed by the ancient Sumerians in Mesopotamia, around 3200 BCE, and continued to be used by the Babylonians. Note that there was no notation for the number 0 in cuneiform script. Consequently, there was no visual distinction between the numbers 1, 60, and 3600, and so on.

its roots in the Indian mathematical tradition. One of the earliest known occurrences appears in the Bakhshali manuscript, a collection of around seventy birch-bark leaves, many of which are fragmentary. It was discovered by a farmer in 1881 near Bakhshali in present-day Pakistan. The text was written in an early form of the Śāradā script, and the number 0 was denoted by a dot. Radiocarbon analysis shows that different leaves date from between the 3rd and 9th centuries CE, which suggests a long process of compilation and copying. Nevertheless, instances of the number 0 occur on leaves dating from the 3rd or 4th century CE, making this one of the earliest surviving records of the modern number 0 in written form.

The earliest surviving stone inscription of the number 0 was found in the ruins of a temple in Mekong, Cambodia, by the French archaeologist George Cœdès. He catalogued this stone tablet as K-127. It mentions the year in which the temple was built, the year 605 of the Śāka era, which corresponds to the year 683 CE. The number 0 again appeared as a dot.

Another famous early inscription of the number 0 can be found in the Chaturbhuj temple in Gwalior, India, from 876 CE. The numerals were written in an early Nāgarī script, in which the number 0 already had its modern, circular form. The inscription tells of the temple built on a piece of land 270 hastas in length and 187 hastas in breadth. Since the 0 is used at the last digit of a number, as opposed to a placeholder in the middle of a number, this is considered to be the earliest occurrence of 0 as a numeral.

We saw that throughout the history of human civilization, we have seen numerical systems with various bases. The decimal system is most common nowadays, a sexagesimal system was used by the Sumerians and Babylonians, a vigesimal system was used by the Mayans, and other systems such as the binary and hexadecimal systems are used by computers. On account of these number systems with various distinct bases, it may not come as a surprise that any number $k > 1$ can serve as the basis of a numerical system. We will prove this theorem using Theorem 5.4.1 (The Representabil-

ity Theorem), which itself rests on Theorem 5.2.1 (The Well-Ordering Principle of the Natural Numbers).

5.2 The Well-Ordering Principle of the Natural Numbers

The induction principle of the natural numbers implies other important reasoning principles. One of them is the **well-ordering principle**. The well-ordering principle has many practical implications. For example, in the next section we will apply a variation of the well-ordering principle, which we will describe below, to construct division with remainder.

Theorem 5.2.1 (The Well-Ordering Principle of the Natural Numbers). *Any inhabited subset of the natural numbers has a least element.*

Proof. We will prove, by induction on n, that every subset $A \subseteq \mathbb{N}$ with $n \in A$ has a least element.

In the base case we have to show that every subset $A \subseteq \mathbb{N}$ containing 0 has a least element. Since 0 is the least natural number, it follows that any subset containing 0 must have a least element.

For the inductive step assume that every subset $A \subseteq \mathbb{N}$ containing n has a least element. Our goal is to show that every subset $A \subseteq \mathbb{N}$ containing $n+1$ has a least element. There are two cases to consider: either $0 \in A$ or $0 \notin A$. In the first case, where $0 \in A$ is assumed, then A clearly has a least element. In the second case, define the subset $B \subseteq \mathbb{N}$ to be

$$\{x \in \mathbb{N} \mid x + 1 \in A\}.$$

In other words, B is the set of all natural numbers x such that $x+1$ is in A. Since $n+1$ is in A by assumption, it follows that $n \in B$. However, note that we are in position to apply the induction hypothesis now: The set B must have a least element m.

We claim that $m+1$ must be the least element of A. First of all, we know that $m+1 \in A$ because $m \in B$. Second of all, if $x \in A$ then we know that x is nonzero. This means that $x = x' + 1$ for some natural number x'. In other words, we have $x' + 1 \in A$, which means that $x' \in B$. Since m is the least element of B it follows that $m \leq x'$. This implies that $m + 1 \leq x' + 1$, so $m + 1 \leq x$ follows. This shows that any element of A must be greater than or equal to $m+1$. In other words, $m+1$ is the least element of A. □

We also have some variations of the well-ordering principle that apply to subsets of the integers. For the following theorem, we say that a subset $A \subseteq \mathbb{Z}$ is **bounded from below** if there is an integer b such that $b \leq x$ for every element $x \in A$. Similarly, we say that a subset $A \subseteq \mathbb{Z}$ is **bounded from above** if there is an integer b such that $x \leq b$ for every element $x \in A$.

Theorem 5.2.2. *Let A be a subset of the integers. We make the following two claims:*



(i) *If A is inhabited and bounded from below, then A has a least element.*

(ii) *If A is inhabited and bounded from above, then A has a largest element.*

PROOF. For the first claim, assume that A is inhabited and suppose that $b \leq x$ for every element $x \in A$. Then we define the subset

$$B := \{x \in \mathbb{Z} \mid x + b \in A\}.$$

The subset B is inhabited and it is bounded from below by 0. This means that B is in fact a subset of the natural numbers, and so it has a least element by the well-ordering principle, Theorem 5.2.1. Observe that $x \in B$ if and only if $x + b \in A$, so if x is the least element of B then $x + b$ is the least element of A. This proves the first claim.

The second claim follows from the first, because if A is inhabited and bounded from above, then the set

$$B := \{x \in \mathbb{Z} \mid -x \in A\}$$

is inhabited and bounded from below. Since the set B has a least element by the previous claim, it follows that the set A has a largest element. □

5.3 Euclidean Division

The Euclidean division operation with a divisor $d > 0$ is the operation that returns for each integer a the division with remainder of a by d. More specifically, the Euclidean division operation of a by an integer d returns two integers, the **quotient** q and the **remainder** r, such that $0 \leq r < d$ and such that

$$a = q \cdot d + r$$

For example, if $a := 23$ and $d := 5$, then the Euclidean division operation returns $q := 4$ for the quotient, and $r := 3$ for the remainder. Note that we have $0 \leq 3 < 5$, and the identity

$$23 = 4 \cdot 5 + 3$$

holds. We will prove that for every $d > 0$ there is always a unique such pair (q, r) of integers satisfying the two constraints for Euclidean division. Before we do so, we first explain in more detail how to go about **unique existence** proofs.

Suppose X is a set and $P(x)$ is a property of the elements of the set X. For a concrete example, which we will work out below, take X to be the set $\mathbb{N}$ of natural numbers and $P(x)$ to be the property that $x = 0$. Now suppose someone asks you to prove that there is a unique element x that satisfies $P(x)$. Then your task splits up in two parts:

(i) First, you have to prove existence. Here, your task is to find a concrete element $a \in X$ and prove that it satisfies the property $P(a)$.

(ii) Second, you have to prove uniqueness. This means that you have to show for any two elements x and y, if both $P(x)$ and $P(y)$ hold then we must have $x = y$. In other words, in the uniqueness part of the proof you are tasked with showing that there is *at most one* element satisfying P.

The existence part of the proof ensures that at least one solution exists, while the uniqueness part of the proof ensures that there is at most one solution. Both steps combined allow us to conclude that there exists exactly one element of x such that $P(x)$ holds. In a logical formula, it is customary to write $\exists!_{(x\in X)}P(x)$ for the unique existence property.

The example where we take $X := \mathbb{N}$ and $P(x) := x = 0$ is simple, but it captures the essence of unique existence proofs. To show that there is a unique natural number equal to 0, we first have to give an example of a natural number that is equal to 0. We simply take the number 0 itself. For the uniqueness part of the proof, we have to show that any two numbers that are equal to 0 are equal to each other. This is evident, because they are both equal to 0. Thus we conclude that

$$\exists!_{(n\in\mathbb{N})} n = 0.$$

Theorem 5.3.1 (The Euclidean Division Theorem). *Consider an integer a and an integer $d > 0$. Then there exists a unique pair of integers (q, r) such that $0 \leq r < d$ satisfying the identity*

$$a = q \cdot d + r.$$

Proof. Consider the set

$$A := \{x \in \mathbb{Z} \mid xd \leq a\}$$

of integers x whose product with d is at most a. We will show that A is bounded from above and that A is inhabited. Together, this will imply by Theorem 5.2.2 that A has a largest element, which will be our quotient q.

First, we show that the set A has an upper bound. There are two cases to consider: either $a \geq 0$ or $a < 0$. If $a \geq 0$, the integer a is an upper bound because for any $x \in A$ we have $x \leq \max(0, xd) \leq a$. If $a < 0$ then the integer 0 is an upper bound because $xd \leq a < 0$ implies that x must be negative.

Next, we observe that the integer $-|a|$ is always in the set A, because $-|a|d \leq -|a| \leq a$. Therefore it follows that the set A has a largest element, which we will call q.

By definition, q satisfies $qd \leq a$ and q is the largest such element. By maximality of q it follows that $a < (q+1)d = qd + d$. Now we take $r := a - qd$. Since $qd \leq a$ it follows that $0 \leq r$, and since $a < qd + d$ it follows that $r < d$. This completes the existence of q and r.

It remains to prove uniqueness. Suppose that (q, r) and (q', r') are two pairs of integers satisfying $0 \leq r < d$, $0 \leq r' < d$, and the equations

$$a = qd + r, \qquad \text{and} \qquad a = q'd + r'.$$

It follows that

$$(q - q')d = r' - r.$$

However, the integer $r' - r$ satisfies the strict inequalities $-d < r' - r < d$ and it is divisible by d. This implies that $r' - r = 0$, so it follows that $r = r'$. Now it also follows that $(q - q')d = 0$. Since d was assumed to be positive, this implies that $q - q' = 0$, from which it follows that $q = q'$. This completes the proof of uniqueness. □

5.4 The Representability Theorem

THEOREM 5.4.1 (The Representability Theorem). *Consider a natural number $k > 1$. Then there exists for every natural number n a unique list ℓ of digits $d_0, \dots, d_{l-1}$ of length l, such that the inequalities $0 \leq d_i < k$ hold for each $i < l$, such that the **leading digit** $d_{l-1} \neq 0$, and satisfying the equation*

$$n = \sum_{i=0}^{l-1} d_i k^i.$$

Before proving the theorem, let's first discuss the main idea behind the proof. Since we assumed that $k > 0$, it follows from the Euclidean division theorem, Theorem 5.3.1, that there is a unique pair (q, r) of numbers such that $n = qk + r$ and $0 \leq r < k$. This gives us the first digit in the representation theorem[1]: the number $d_0 := r$.

The representability theorem would now follow if we already knew that q has a unique representation. If $d_0 = r$ and if $d_1, \dots, d_{l-1}$ is the unique representation of q, then the list $d_0, \dots, d_{l-1}$ is a unique representation of n. However, the usual induction principle doesn't allow us to make this step, because n is not necessarily the successor of q. Therefore we need something stronger: the **strong induction principle**.

THEOREM 5.4.2. *Consider a property $P(n)$ of the natural numbers, and assume that the following two conditions hold:*

(i) *The property $P(0)$ is true.*

(ii) *If the property $P(k)$ is true for all $k \leq n$, then the property $P(n+1)$ is true.*

Then $P(n)$ is true for all n.

The strong induction principle can be formulated more succinctly using the **universal quantifier**. The universal quantifier $\forall$ is used to express that a property is true for all elements in a domain of discourse. In other words, when we say that a property $P(n)$ is true for all natural numbers n, we can write that as the logical formula

$$\forall_{(n \in \mathbb{N})} P(n).$$

Using universal quantification, we can state the strong induction principle as follows. Suppose that the following two conditions hold:

[1] It should be noted that this digit appears last in the actual representation. It is the "ones digit" of the representation.

(i) The property $P(0)$ is true.

(ii) If the property $\forall_{k \leq n} P(k)$ is true, then the property $P(n+1)$ is true.

Then $P(n)$ is true for all n. The universal quantifier is helpful in the proof of the strong induction principle.

Proof. Let $P(n)$ be a property of an arbitrary natural number n, and define

$$Q(n) := \forall_{(m \leq n)} P(m)$$

Note that in order to prove that $P(n)$ is true for all n, it suffices to prove that $Q(n)$ is true for all n. Indeed, if $Q(n)$ is true for all n, that just means that $P(m)$ is true for all $m \leq n$, for all n. In particular $P(n)$ is true for all n.

With that out of the way, assume that $P(0)$ is true, and that $Q(n)$ implies $P(n+1)$ as in the induction step of the strong induction principle. Our goal is to show that $P(n)$ is true for all n, and we have already shown that it suffices to show that $Q(n)$ is true for all n. We proceed by induction on n.

For the base case we need to prove that $Q(0)$ is true, meaning that $P(m)$ is true for all $m \leq 0$. Note that $m \leq 0$ implies $m = 0$, so the base case follows from the assumption that $P(0)$ is true.

For the inductive step, assume that $Q(n)$ is true. Our goal is to show that $Q(n+1)$ is true. However, we have assumed that $Q(n)$ implies $P(n+1)$. Now notice that if $Q(n)$ is true, meaning that if $P(m)$ is true for all $m \leq n$, and if $P(n+1)$ is true, then $P(m)$ is true for all $m \leq n+1$. In other words, $Q(n+1)$ is true. This completes the inductive step and therefore the proof. □

Our earlier idea to prove the representability theorem can finally be made into a proof.

Proof of Theorem 5.4.1. We prove the theorem by strong induction. For the base case, note that the empty list satisfies the requirements vacuously since there are no digits in the empty list and empty sums are set to be 0. Thus the empty list is a representation of 0. Now suppose that $\ell = (d_0, \ldots, d_{l-1})$ is a representation of 0 and ℓ is a list of nonzero length l. By the requirement that the leading digit d_{l-1} is nonzero it follows that the sum

$$\sum_{i=0}^{l-1} d_i k^i$$

is nonzero. Such a list is therefore not a representation of 0. The only representation of 0 is therefore the empty list.

Now suppose that every number $m \leq n$ has a unique representation. To show that the number $n+1$ has a unique representation, first note that there is a unique pair (q, r) of numbers q and $0 \leq r < k$ such that

$$n + 1 = qk + r.$$

There are two cases to consider: either $q = 0$ or $q \neq 0$. In the first case we find that $n + 1 = r < k$. We let ℓ be the list (d_0) of length 1 with $d_0 := r$. Its leading digit is nonzero because $n + 1$ is nonzero, and clearly we have

$$\sum_{i=0}^{0} d_i k^i = d_0 = n + 1.$$

Furthermore, this representation is unique because any representation of $n + 1$ must be a list of digits of length 1, which fixes its digit d_0 to $n + 1$.

If $q \neq 0$, then we have the inequalities

$$q + 1 \leq 2q \leq qk \leq qk + r = n + 1.$$

The second inequality follows from the assumption that $k > 1$. Since $q + 1 \leq n + 1$ it follows that $q \leq n$. This puts us in position to apply the induction hypothesis of the strong induction principle: The number q has a unique representation $(e_0, \ldots, e_{l-1})$. Now we define the representation of $n+1$ to be $(d_0, \ldots, d_l)$, where $d_0 := r$ and $d_{i+1} := e_i$ for $0 \leq i < l$.

This representation of $n + 1$ is unique, because for any representation of $n + 1$, its d_0 must be equal to r, and the list $(d_1, \ldots, d_{l-1})$ must be a representation of q, which is unique, thus completing the proof. □

5.5 Some Combinatorial Applications of the Euclidean Division Theorem

Theorem 5.3.1 (The Euclidean Division Theorem) can be used to obtain some elementary combinatorial application. We will make use of the pigeonhole principle, which is commonly attributed to Gustav Lejeune Dirichlet, who used this principle brilliantly in his approximation theorem. The idea of the pigeonhole principle is that if we place n objects in m boxes, and m is strictly smaller than n, then there is a box containing more than one object. The pigeonhole principle underlies a remarkable array of existence results across number theory and combinatorics. Among classical number-theoretic applications, one finds the aforementioned approximation theorem of Dirichlet, the Erdős–Ginzburg–Ziv zero-sum theorem, and the Chevalley–Warning theorem on solutions of systems of polynomial congruences. The pigeonhole principle is stated formally as follows:

THEOREM 5.5.1 (The Pigeonhole Principle). *Consider two natural numbers $m < n$, and a function $f : X \to Y$ from a set X with n elements into a set Y with m elements. Then there exists an element y such that $f(x) = y$ for more than one element x.*

In the present chapter, we will be content with some very elementary applications of the pigeonhole principle in combination with Theorem 5.3.1 (The Euclidean Division Theorem).

Theorem 5.5.2. *Consider two positive integers $m < n$. In any set of n integers, there is a pair of distinct integers such that their difference is divisible by m.*

Proof. Consider a set A of size n of integers, and list, for every integer in A its remainder after division by m. Since the remainder is a number between 0 and $m-1$, it follows from the pigeonhole principle that there must be at least two distinct integers x and y with the same remainder. It follows that $x - y$ is divisible by m. □

Theorem 5.5.3. *Consider two positive integers $m \leq n$. In any set of n integers, there is a nonempty subset such that the sum of its elements is divisible by m.*

Proof. Consider the n integers $a_1, \dots, a_n$, and consider the sums

$$0,\ a_1,\ a_1 + a_2,\ \dots,\ a_1 + \cdots + a_n.$$

By Theorem 5.5.2 it follows that at there are at least two of these sums that differ by a multiple of m. Notice that the difference of two such sums is of the form $a_k + \cdots + a_l$, so the theorem is proven. □

Theorem 5.5.4. *Consider positive integers m and n such that $m < 2^n - 1$, and consider a set of integers S of size n. Then there are two distinct nonempty subsets of S such that the difference of the sums of their elements is divisible by m.*

Proof. There are 2^k subsets of S, of which $2^k - 1$ are nonempty. By Theorem 5.5.2 it follows that there are two distinct nonempty subsets of S such that the difference of their sums is divisible by m. □

Exercises

Routine-Building Exercises

5.1 Prove that among any choice of $n+1$ numbers from the set $\{1, \ldots, 2n\}$, there will be two distinct numbers that sum to $2n+1$.

5.2 Show that a number written as $d_{l-1} \cdots d_0$ in its decimal representation is divisible by 11 if and only if the alternating sum

$$\sum_{i=0}^{l-1} (-1)^i d_i$$

is divisible by 11. For example, the number 2541 is divisible by 11 because $-2 + 5 - 4 + 1 = 0$ is divisible by 11.

5.3 Show that for any natural number $n > 0$ there is a unique pair of numbers (m, r) such that the only square dividing r is 1, and

$$n = m^2 r.$$

This is called the **square-free decomposition** of n.

5.4 Show that for any natural number $n > 0$ there is a unique pair of numbers (k, m) such that

$$n = 2^k(2m+1).$$

This is called the 2-**adic decomposition** of n.

5.5 Show that any natural number n can be written uniquely in the form

$$\sum_{k=1}^{m} d_k k!,$$

where $0 \le d_k \le k$ and $d_m \neq 0$. This is called the **factoradic expansion** of n. For example, the number 629 has factoradic expansion $(5, 1, 0, 2, 1)_!$, since

$$629 = 5 \cdot 5! + 1 \cdot 4! + 0 \cdot 3! + 2 \cdot 2! + 1 \cdot 1!.$$

5.6 Show that for any m, any natural number n can be written uniquely in the form

$$\sum_{k=1}^{m} \binom{c_k}{k},$$

where $0 \le c_1 < c_2 < \cdots < c_m$ is a strictly increasing sequence of natural numbers. This is called the **combinatoradic expansion** of n of degree m. For example, the 2nd, 3rd, and 4th degree combinatoracic expansions of 629 are

$$\binom{35}{2} + \binom{34}{1}, \quad \binom{16}{3} + \binom{12}{2} + \binom{3}{1}, \quad \text{and} \quad \binom{12}{4} + \binom{10}{3} + \binom{5}{2} + \binom{4}{1},$$

so we can write $629 = (35, 34)_{\text{c}}$, $629 = (16, 12, 3)_{\text{c}}$, and $629 = (12, 10, 5, 4)_{\text{c}}$.

Challenge Exercises

5.7 *Zeckendorf's representation theorem.* Show that every natural number has a unique **Zeckondorf representation**: For any natural number n there is a unique list $\ell = (d_0, \dots, d_{l-1})$ of digits 0 and 1, such that its leading digit d_{l-1} is nonzero, no two consecutive digits are both 1, and satisfying the identity

$$n = \sum_{i=0}^{l-1} d_i F_{i+2},$$

where F_j is the jth Fibonacci number. Zeckendorf representations have some fun applications:

(i) The Zeckendorf representation theorem can be used in the design of any document to get meaningful relative font sizes: If $d_{l-1} \cdots d_0$ is the Zeckendorf representation of a font size n, then adding an extra zero at the end gives the Zeckendorf representation $d_{l-1} \cdots d_0 0$ of a good next font size. If you are working with font size 12, what is the next sensible font size?

(ii) Zeckendorf representations can also be used to convert miles to kilometers with a fair degree of accuracy. Again, given a number n of miles, with Zeckendorf representation $d_{l-1} \cdots d_0$, add a 0 at the end to get the Zeckendorf representation $d_{l-1} \cdots d_0 0$ of the number of kilometers. How fast is 65 mph in kph according to this conversion?

5.8 (Erdős–Szekeres) Show that any sequence $a_1, \dots, a_{mn+1}$ of real numbers contains either an increasing subsequence of length $m+1$ or a decreasing subsequence of length $n+1$.



Chapter 6

Divisibility

6.1 The Condition of Divisibility

The simplest Diophantine equation is the equation $ax = b$ in one variable x. The condition of its solvability leads to the concept of *divisibility*.

Definition 6.1.1. We say that an integer a **divides** an integer b if there exists an integer x such that the equation

$$ax = b$$

holds. When a divides b, we write $a \mid b$ and we say that a is a **divisor** of b. Sometimes we also refer to b as the **dividend**. When a does not divide b, we write $a \nmid b$. An integer a is called **even** if $2 \mid a$ and is called **odd** if $2 \nmid a$.

Example 6.1.2. The integers -1, 0, and 1 have special properties with respect to divisibility:

(i) The integers 1 and -1 divide any integer b. Indeed, the integer b itself is a solution to the equation $1x = b$, and the integer $-b$ is a solution to the equation $-1x = b$.

(ii) Every integer a divides 0. Indeed, $x = 0$ is a solution to the equation $ax = 0$.

(iii) If $0 \mid b$ for some integer b, then it follows that $b = 0$. Indeed, if $0x = b$ has a solution, then $b = 0$ because $0x = 0$. Furthermore, we observe that *every* integer is a solution to the equation $0x = 0$. It follows that $0 \nmid 1$, and indeed that $0 \nmid b$ for any nonzero integer b.

(iv) Similarly, if $a \mid 1$ for some integer a, then it follows that $a = \pm 1$. Indeed, if $ax = 1$ has a solution, then the absolute value $|a|$ of a cannot be greater than 1, because

its nonzero multiples would be of absolute value greater than 1. Therefore it follows that $|a| = 1$, which proves the claim. In the situation where $a \mid 1$, we say that a is **invertible**, or that it is a **multiplicative unit**, because the solution to the equation $ax = 1$ is a multiplicative inverse of a.

LEMMA 6.1.3. *Suppose that $a \mid b$, where a is a nonzero integer. Then there is a unique integer x satisfying the equation $ax = b$. We will write b/a for this unique integer, which is called the **quotient** of b divided by a.*

PROOF. By the assumption that $a \neq 0$, it follows that the function $x \mapsto ax$ is *injective* [needs reference or proof]. This means that $ax = ay$ implies $x = y$. Consequently, there can be at most one integer x such that $ax = b$. □

REMARK 6.1.4. While we have given a definition of divisibility in natural language, the formal definition of divisibility features the *existential quantifier* $\exists$. When we write the logical formula $\exists_{(x \in X)} P(x)$, this means that there exists an element $x \in X$ for which $P(x)$ holds. The definition of divisibility translates to the following logical formula:

$$a \mid b \ := \exists_{(x \in \mathbb{Z})} ax = b.$$

In order to use existential quantification in proofs, it is useful to know how to break them down systematically. There are two cases to consider: (1) How to *prove* an existence claim, and (2) how to *use* an existence claim as an assumption to prove something else.

(i) The principal way to prove that there exists an element $x \in X$ such that $P(x)$ holds, is to construct an element x of X and prove that the property $P(x)$ holds.

(ii) To use that there exists an $x \in X$ such that $P(x)$ holds in the proof of another property Q, you may assume to have an element x and you may assume that the property $P(x)$ holds. However, in this scenario we may not assume anything else about x unless that is otherwise warranted.

In the case of divisibility, in order to prove that $a \mid b$ holds we must find a solution to the equation $ax = b$, and in order to use that $a \mid b$ holds as an assumption, we may assume x is an integer for which the equation $ax = b$ holds.

PROPOSITION 6.1.5. *If d divides a and b, then d divides $ax + by$ for any two integers x and y.*

PROOF. Suppose that d divides both a and b. Let u and v be integers such that $du = a$ and $dv = b$. Then we have

$$ax + by = dux + dvy = d(ux + vy),$$

which shows that $ax + by$ is a multiple of d. □

Sometimes, the hardest thing is to figure out how to rigorously prove a property that looks completely self-evident. The following proposition, for instance, asserts that in any set of k consecutive integers, exactly one of them is divisible by k.

There are, as is commonly the case in mathematics, several ways to approach this problem, but the question is how to generate ideas towards a full proof. One good way of generating ideas is by looking at special cases. In our problem at hand, a special case of interest is the set $\{0, 1, \dots, k-1\}$. There should be exactly one element in the set $\{0, 1, \dots, k-1\}$ divisible by k.

Indeed, this is a direct consequence of the Euclidean division theorem: The only element in this set that has remainder 0 after division by k is the integer 0. This suggests using the Euclidean division theorem for the general claim as well. Furthermore, we will also use the common proof technique of assuming something *without loss of generality*.

Proposition 6.1.6. *In any set of $k > 0$ consecutive integers*

$$\{a, a+1, \dots, a+k-1\}$$

there is exactly one element divisible by k.

Proof. First, consider the function

$$r : \{a, a+1, \dots, a+k-1\} \to \{0, 1, \dots, k-1\},$$

where $r(x)$ is defined to be the remainder of x after division by k. We claim that this map is injective, meaning that if $r(x) = r(y)$ for two elements x and y, then $x = y$. To see this, consider two elements x and y in the set $\{a, \dots, a+k-1\}$. Without loss of generality we may assume that $x \leq y$. Indeed, either $x \leq y$ or $y \leq x$ holds, and these situations are completely similar, so nothing is lost if we just assume that $x \leq y$.

We have the equalities $x = q(x)k + r(x)$ and $y = q(y)k + r(y)$, where $q(x)$ and $q(y)$ are the quotients of x and y after division by k, respectively. Since we assumed that $r(x) = r(y)$, it follows that $y - x = (q(y) - q(x))k$. In other words, $y - x$ is divisible by k. Furthermore, we have $0 \leq y - x < k$ because both x and y are in the set $\{a, \dots, a+k-1\}$. It follows from Euclidean division theorem that the only integer $0 \leq z < k$ divisible by k is 0, so we find that $y - x = 0$. We conclude that $x = y$.

It now follows that every element $y \in \{0, 1, \dots, k-1\}$ is the value of r of exactly one element $x \in \{a, a+1, \dots, a+k-1\}$, because both sets have k elements and the map r doesn't take any value more than once. In particular, there is exactly one element $x \in \{a, a+1, \dots, a+k-1\}$ whose remainder after division by k is 0. In other words, exactly one element of this set is divisible by k. □

6.2 The Ordering by Divisibility

The divisibility relation equips the sets of integers and natural numbers with a useful extra structure, a *partial ordering* of their elements. The set of natural numbers

equipped with the divisibility relation is a poset, while the set of integers equipped with the divisibility relation is a preorder, a slightly weaker structure.

DEFINITION 6.2.1. A **preorder** consists of a set X and an ordering $\leq$ of the elements of X, such that

(i) The ordering is **reflexive**. This means that $x \leq x$ holds for every x.

(ii) The ordering is **transitive**. This means that if $x \leq y$ and $y \leq z$ both hold, then $x \leq z$ also holds.

A **poset**, or **partially ordered set** in full, is a preorder $(X, \leq)$ satisfying additionally the condition:

(iii) The ordering is **antisymmetric**. This means that if both $x \leq y$ and $y \leq x$ hold, then $x = y$.

THEOREM 6.2.2. *The set of integers equipped with the divisibility relation $\mid$ is a preorder, and the set of natural numbers equipped with the divisibility relation $\mid$ is a poset.*

PROOF. We first show that the set of integers with divisibility is a preorder. To see that the divisibility relation is reflexive, note that $x = 1$ is a solution of the equation

$$ax = a.$$

Therefore, it follows that $a \mid a$ for every integer a. To see that the divisibility relation is transitive, assume that $a \mid b$ and $b \mid c$. That is, assume that we have integers x and y such that $ax = b$ and $by = c$. Then it follows that

$$a(xy) = (ax)y = by = c.$$

In other words, c is divisible by a. This completes the proof that $\mathbb{Z}$ equipped with the divisibility relation is a preorder.

To see that the natural numbers equipped with divisibility forms a poset, it remains to show that the divisibility relation is antisymmetric on the natural numbers. Suppose that $m \mid n$ and $n \mid m$; that is, that there are natural numbers x and y so that $mx = n$ and $ny = m$. By transitivity of divisibility it follows that $m(xy) = m$. □

The diagram displayed in Figure 6.1 is the *Hasse diagram* of the positive divisors of the number 120, a fragment of the poset of the natural numbers ordered by divisibility.

Despite lacking antisymmetry, the preorder of the integers with divisibility is essentially equivalent to the poset of natural numbers with divisibility. For every integer a there is a unique natural number n satisfying $n \mid a$ and $a \mid n$. This unique number is of course the absolute value of a. The absolute value function $x \mapsto |x|$ preserves divisibility, which means that $a \mid b$ implies $|a| \mid |b|$, and it satisfies the logical equivalence

$$(a \mid b) \wedge (b \mid a) \Leftrightarrow |a| = |b|$$

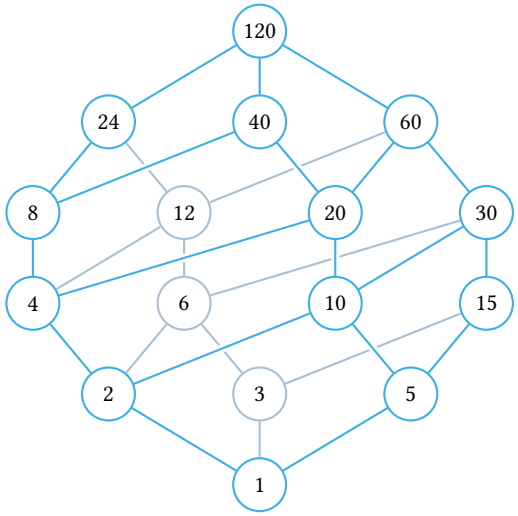


Figure 6.1: The Hasse diagram of the divisors of 120.

for any integer a and any natural number n. Order preserving maps $f : (P, \leq_P) \to (Q, \leq_Q)$ from a preorder $(P, \leq_P)$ to a poset $(Q, \leq_Q)$ that satisfy the logical equivalence $(x \leq_P y) \wedge (y \leq_P x) \Leftrightarrow f(x) = f(y)$ for every $x, y \in P$ are also called *poset reflections*. Every preorder has a poset refection, but we will not need to go into that aspect of order theory in this course.

6.3 Ideals of Integers

A fruitful way of studying the divisibility relation is by studying the set of *all* integers divisible by a given integer. That is, instead of focusing on one instance of divisibility, we turn our attention to the totality of all integers divisible by a given integer, and we ask questions such as: What properties does the set of all integers divisible by an integer a have? This abstraction leads us to the concept of *ideal*, which was first defined and studied by Richard Dedekind [Ded1871; Kle1998].

Definition 6.3.1. An **ideal of integers** is a subset $I \subseteq \mathbb{Z}$ that contains 0, and contains the linear combination $kx + ly$ for any $x, y \in I$, and any $k, l \in \mathbb{Z}$.

Example 6.3.2. The subset $\{0\} \subseteq \mathbb{Z}$ satisfies the conditions of being an ideal in a trivial way; this ideal is called the **zero ideal**.

Example 6.3.3. The subset $(a) := \{ka \mid k \in \mathbb{Z}\}$ also satisfies the conditions of being an ideal; ideals of this form are called **principal ideals**, since they are generated by a single integer.

In the following theorem we show that every ideal of integers is a principal ideal. By virtue of this properties, we also call $\mathbb{Z}$ a **principal ideal domain**.

THEOREM 6.3.4. *For every ideal $I \subseteq \mathbb{Z}$ there is a unique natural number n such that $I = (n)$.*

PROOF. There are two cases to consider: Either I is the zero ideal, or I contains a nonzero integer. In the first case it is clear that $I = (0)$, and that 0 is the unique natural number n such that $I = (n)$. Thus we focus on the nonzero case.

Suppose that I contains a nonzero integer x. Then I contains the integer $|x|$, because $|x| = \pm x$. In particular, I contains a positive integer. Therefore it follows that I contains a least positive integer n. To see that $I = (n)$, consider an element $x \in I$. By the Euclidean division theorem, it follows that $x = qn + r$, where $0 \leq r < n$. Notice that $r \in I$, since it is the difference $x - qn$ of two elements in I. Since r is nonnegative and n is the least positive integer in I, it follows that $r = 0$, which gives us that $x = qn$. Thus, every element in I is a multiple of n.

Now suppose that $I = (n)$ and $I = (m)$ for two nonzero natural numbers n and m. Then it follows that $m = qn$ and $n = pm$. Thus, we see that $m = (pq)m$, which implies that $pq = 1$. Furthermore, both p and q are positive integers, so we have $p = 1$ and $q = 1$. This shows that $m = 1n = n$, establishing uniqueness. □

The set of ideals of $\mathbb{Z}$ is ordered by inclusion: We write $I \subseteq J$ for two ideals I and J, if every element of I is an element of J. Note that $(b) \subseteq (a)$ holds if and only if $a \mid b$. The theory of ideals of integers is therefore closely related to the theory of divisibility of integers.

Exercises

Starter Exercises

6.1 Draw the Hasse diagrams for the posets of positive divisors of the following numbers: 360, 900, 1024, 1296, and 2310.

6.2 Show that $a^n - 1$ is divisible by $a - 1$ for every integer a.

6.3 Show that $a^n + b^n$ is divisible by $a + b$ for any odd natural number n.

6.4 Suppose that $a \mid b$, where a is assumed to be nonzero.

(a) Show that $d \mid b/a$ if and only if $ad \mid b$.

(b) Show that for any integer ideal I, $b/a \in I$ if and only if $b \in aI$, where $aI = \{ax \mid x \in I\}$.

6.5 Suppose that $a \mid b$ and $b \mid c$, where $a \neq 0$.

(a) Show that if $d \mid b/a$ then $d \mid c/a$.

(b) Show that for any integer ideal I, if $b/a \in I$ then $c/a \in I$.

6.6 Show that if a and ab are n^{th} powers, with $a \neq 0$, then so is b.

6.7 Suppose that $a \neq 0$. Show that if ab and ac are squares, then so is bc.

Routine-Building Exercises

6.8 (a) Show that $a^2 - b^2$ is divisible by 8 for any two odd integers a and b.

(b) Show that $(a^2 - 1)/8$ is a triangular number for any odd integer a.

6.9 (a) Show that $a^3 - a$ is divisible by 6 for every integer a.

(b) Show that

$$\sum_{k=1}^{a-1} \binom{k+1}{2} = \frac{a^3 - a}{6}$$

for every $a \geq 0$.

(c) Use the previous identity to give a geometric interpretation of the numbers $(a^3 - a)/6$.

6.10 Show that $a^5 - a$ is divisible by 30 for every integer a.

6.11 Show that for any two positive integers $a \leq b$ there is a unique integer $a \leq x \leq b$ satisfying the logical equivalence

$$2^k \mid x \quad \Leftrightarrow \quad 2^k \mid \operatorname{lcm}(a, \ldots, b)$$

for every $k \geq 0$.

Challenge Exercises

6.12 (a) Prove the **Fibonacci addition formula** $F_{m+n+1} = F_{m+1}F_{n+1} + F_m F_n$.

(b) For any integer d and any two natural numbers m and n, show that if two of the three following conditions hold, then so does the third:

(i) $d \mid F_m$.



(ii) $d \mid F_n$.

(iii) $d \mid F_{n+m}$.

6.13 Show that if x and y are positive integers such that xy divides x^2+y^2, then $x = y$.

6.14 Show that in any subset of $n+1$ integers from the set $\{1, \ldots, 2n\}$, there is a pair of distinct integers such that one divides the other. Does the claim still hold for every subset of n integers from the set $\{1, \ldots, 2n\}$?

6.15 Consider two relatively prime positive integers m and n, and define a sequence (a_k) of natural numbers by

$$a_0 = m + n \qquad \text{and} \qquad a_{i+1} = a_i^2 - na_i + n$$

Show that $\gcd(a_i, a_j) = 1$ for all $i \neq j$ [MOH1978].

6.16 Show that for $n > 1$ there are no solutions in the positive integers to the equation

$$a(a+1)(a+2) = b^n.$$

More generally, Paul Erdős and John Lewis Selfridge showed that no product of at least two consecutive integers can be an nth power for $n > 1$ [ES1975].

6.17 Find all solutions to the equation

$$3^m - 2^n = 1.$$

Chapter 7

Linear Diophantine Equations

In this section we study *linear Diophantine equations*. These are equations of the form

$$a_0x_0 + \cdots + a_kx_k = b,$$

with integer coefficients $a_0, \ldots, a_k$. The objective of a linear Diophantine equation such as the one above is to find integers $x_0, \ldots, x_k$ for which the equation holds, to study conditions under which the equation has integer solutions, and ultimately to characterize all solutions.

7.1 Greatest Common Divisors

Some preorders $(P, \leq)$ satisfy the property that for any two elements $a, b \in P$ there is a greatest element below both of them. This property can be formulated succinctly as follows: An element d is a greatest element below a and b if it satisfies the logical equivalence

$$(x \leq a) \wedge (x \leq b) \Leftrightarrow (x \leq d)$$

for every element $x \in P$. If d satisfies this property, we also say that d is the *meet* of a and b. It is common to write $a \wedge b$ for the meet of a and b, if P is a poset in which any two elements have a meet.

The definition of meets needs some explanation. It uses the *conjunction* ($\wedge$) and it uses *logical equivalence* ($\Leftrightarrow$). The conjunction $p \wedge q$ of two propositions p and q is the proposition that both p and q are true. The logical equivalence $p \Leftrightarrow q$ is the proposition that p is true if and only if q is true. In other words, it is the conjunction of the proposition that p implies q and the proposition that q implies p.



If d is the meet of a and b, then the logical equivalence gives two implications back and forth:

(i) Any element x that is below both a and b, must be below d.

(ii) Any element x that is below d, must be below both a and b. In particular, d itself satisfies $d \leq d$, so it follows that $d \leq a$ and $d \leq b$. That is, d itself is below both a and b, and by the first property it is the greatest such element.

We wouldn't have this discussion if it didn't apply for us. Indeed, we will show that the preorder of integers with divisibility has meets. In the case of the integers, we will call such meets *greatest common divisors*.

DEFINITION 7.1.1. Consider two integers a and b. An integer d is said to be a **greatest common divisor** of a and b if it satisfies the following logical equivalence

$$(x \mid a) \wedge (x \mid b) \Leftrightarrow (x \mid d)$$

for every integer x.

Thus, a greatest common divisor of a and b is an integer d that divides both a and b, and any integer that divides both a and b is a divisor of d. In other words, the signifier "greatest" refers to the divisibility ordering of the integers.

EXAMPLE 7.1.2. The greatest common divisor of 0 and 0 is 0. To see this, simply note that the proposition

$$(x \mid 0) \wedge (x \mid 0) \Leftrightarrow (x \mid 0)$$

is true because any proposition is logically equivalent to the conjunction with itself. Here we see why it was relevant to note that the word "greatest" refers to the divisibility ordering: Any integer is a divisor of 0, but none of them are the greatest in the standard ordering $\leq$.

THEOREM 7.1.3. *Any two integers a and b have a greatest common divisor, for which we write* $\gcd(a, b)$. *Furthermore, there are integers k and l satisfying* ***Bézout's identity***

$$ax + by = \gcd(a, b).$$

PROOF. Consider two integers a and b, and let $I := (a)$ and $J := (b)$ be the principal ideals generated by a and b. Now consider the set

$$I + J := \{x + y \mid x \in I,\ y \in J\}$$

of all sums of elements of I and elements of J. We claim that the set $I + J$ is again an ideal. It contains 0, because $0 = 0 + 0$ is a sum of elements in I and J. Furthermore, to see that $I + J$ is closed under linear combinations of its elements, consider two elements $u, v \in I + J$. If $u = x_u + y_u$ and $v = x_v + y_v$, then we can write any linear combination $ku + lv$ of u and v in the form

$$ku + lv = (kx_u + lx_v) + (ky_u + ly_v),$$

which is the sum of an element in I and an element in J. Thus, it follows that $I + J$ is an ideal.

Now let d be the unique natural number such that $I + J = (d)$, which exists by Theorem 6.3.4. We claim that d is the greatest common divisor of a and b. Notice that $a = a + 0 \in I + J$, so a must be a multiple of d. Similarly, we have $b = 0 + b \in I + J$, so b must be a multiple of d. In other words, d is a common divisor of a and b. Furthermore, if e is any common divisor of a and b, then e is a divisor of any element in $I + J$. In particular, we must have $e \mid d$, allowing us to conclude that d is the greatest common divisor.

The last claim follows, because d is an element of $I + J$, which consists elements of the form $ax + by$. □

A very important condition on pairs of integers a and b, which occurs as an assumption in many lemmas, propositions, and theorems, is the condition that $\gcd(a, b) = 1$. In other words, that any nonnegative common divisor of a and b must be 1. Such numbers are called *relatively prime* or *coprime*.

Definition 7.1.4. Two integers a and b are said to be **relatively prime** or **coprime** if

$$\gcd(a, b) = 1.$$

The following proposition is a must-know fact about the integers.

Proposition 7.1.5. *Consider two relatively prime integers a and b, and an arbitrary integer c. Then we have*

$$a \mid bc \Leftrightarrow a \mid c.$$

Proof. The fact that $a \mid c$ implies $a \mid bc$ is obvious, since if c is a multiple of a, then so is bc. This establishes the converse direction of the logical equivalence.

For the forward direction, assume that $a \mid bc$. Since we have assumed that a and b are relatively prime, there is a solution to the equation

$$ax + by = 1.$$

Consequently, there is a solution to the equation $cax + cby = c$. However, both cax and cby are divisible by a, so c must be divisible by a. □

7.2 Euclid's Algorithm

Theorem 7.1.3 shows that any two integers a and b have a greatest common divisor $\gcd(a, b)$, and that there are integers k and l such that

$$ka + lb = \gcd(a, b),$$

but it doesn't reveal much about how the integers k and l can be found, or even how to find the greatest common divisor in the first place. This problem is solved by *Euclid's*



Algorithm, which provides an efficient way to compute the greatest common divisor of two integers and to find integers k and l establishing the greatest common divisor as a linear combination. The algorithm relies on the following proposition.

PROPOSITION 7.2.1. *Suppose a and b are two integers and $b = qa + r$. Then we have*

$$\gcd(b, a) = \gcd(a, r).$$

PROOF. Suppose that d is a divisor of a. Then we claim that $d \mid b$ if and only if $d \mid r$. Indeed, since $b = qa + r$ it follows that b is a linear combination of a and r, and also that r is a linear combination of a and b. Thus, any divisor of a and b is also a divisor of r, and any divisor of a and r is also a divisor of b. In other words, we have

$$d \mid b \Leftrightarrow d \mid r.$$

It follows that d is a common divisor of a and b if and only if d is a common divisor of a and r. This implies that their greatest common divisors coincide. □

As an immediate corollary, we obtain:

COROLLARY 7.2.2. *If b is of the form $ka + 1$, then a and b are always relatively prime.*

Euclid's algorithm works by repeatedly using Proposition 7.2.1. For any pair (a, b) of integers, if $b \neq 0$ then there is a unique pair (q, r) such that $0 \leq r < |b_0|$ and such that the equality

$$a = qb + r$$

holds. This determines a new pair $(a', b') := (b, r)$ and $\gcd(a, b) = \gcd(b, r)$. Note that $\gcd(b, r)$ is somewhat easier to compute, since the numbers involved are smaller. Repeating this procedure, we obtain a list of equalities

$$\begin{aligned} a_1 &= q_1 b_1 + r_1, \\ a_2 &= q_2 b_2 + r_2, \\ &\vdots \\ a_N &= q_N b_N + r_N, \end{aligned}$$

in which $a_1 = a$, $b_1 = b$, $a_{i+1} = b_i$, $b_{i+1} = r_i$, and $0 \leq r_i < |b_i|$. This procedure results in a decreasing sequence $r_1 > r_2 > \cdots > r_N$ of nonnegative integers, so it terminates when $r_N = 0$. Indeed, the Euclidean division theorem cannot be applied to the pair (b_N, r_N) any further when $r_N = 0$. Since Proposition 7.2.1 implies that

$$\gcd(a, b) = \gcd(b_1, r_1) = \gcd(b_2, r_2) = \cdots = \gcd(b_N, r_N),$$

we see that b_N is the greatest common divisor of a and b.

Example 7.2.3. We will illustrate Euclid's algorithm by an example. Suppose we want to calculate the greatest common divisor of 578 and 732. Then we write 732 in the form $q \cdot 578 + r$; that is, we write

$$732 = 1 \cdot 578 + 154.$$

By Proposition 7.2.1, it follows that $\gcd(732, 578) = \gcd(578, 154)$. We now proceed in the same manner, by writing

$$578 = 3 \cdot 154 + 116,$$

and we observe that $\gcd(732, 578) = \gcd(154, 116)$. We proceed with this process until we find that $\gcd(732, 578) = \gcd(d, 0)$ for some number d. Once we reach this stage, we conclude that $\gcd(732, 578) = d$. Putting words to action:

$$\begin{aligned} 154 &= 1 \cdot 116 + 38 && \gcd(732, 578) = \gcd(116, 38), \\ 116 &= 3 \cdot 38 + 2 && \gcd(732, 578) = \gcd(38, 2), \\ 38 &= 19 \cdot 2 + 0 && \gcd(732, 578) = \gcd(2, 0). \end{aligned}$$

Thus, we conclude that $\gcd(732, 578) = 2$.

A few further remarks about the sequence of equations

$$a_i = q_i b_i + r_i$$

produced by Euclid's algorithm are in order. Since each r_i can be written as a linear combination of a_i and b_i, it follows by induction that each r_i can be written as a linear combination of a and b. In other words, for each $1 \leq i \leq N$, there are integers k_i and l_i such that

$$r_i = k_i a + l_i b.$$

These linear coefficients can be determined recursively, by what is called the *extended Euclidean algorithm*. Notice that $k_1 = 1$ and $l_1 = q_1$. We also set $k_0 := 0$ and $l_0 := 1$. Then k_{i+1} and l_{i+1} are recursively determined by the rule:

$$\begin{aligned} k_{i+1} &= k_{i-1} - q_{i+1} k_i, \\ l_{i+1} &= l_{i-1} - q_{i+1} l_i. \end{aligned}$$

To see this, simply note that

$$r_{i+1} = a_{i+1} - q_{i+1} b_{i+1} = r_{i-1} - q_{i+1} r_i.$$

Example 7.2.4. In the previous example, Euclid's algorithm has given us that

$$\gcd(732, 578) = 2.$$



We will now express 2 as a linear combination of 732 and 578. We start with the first equation, $732 = 1 \cdot 578 + 154$ to write

$$154 = 732 - 1 \cdot 578.$$

Next, we use the equation $578 = 3 \cdot 154 + 116$ to write

$$116 = 578 - 3 \cdot 154 = 578 - 3 \cdot (732 - 1 \cdot 578) = 4 \cdot 578 - 3 \cdot 732.$$

Continuing this way, we find that

$$38 = 154 - 1 \cdot 116 = (732 - 1 \cdot 578) - 1 \cdot (4 \cdot 578 - 3 \cdot 732) = 4 \cdot 732 - 5 \cdot 578$$

and

$$2 = 116 - 3 \cdot 38 = (4 \cdot 578 - 3 \cdot 732) - 3 \cdot (4 \cdot 732 - 5 \cdot 578) = 19 \cdot 578 - 15 \cdot 732.$$

In the second to last equation, we find that 2 is a linear combination of 38 and 116; that is,

$$2 = 116 - 3 \cdot 38.$$

However, by the equation before that we see that 38 itself is a linear combination of 154 and 116. This can be used to express 2 as a linear combination of 154 and 116; that is,

$$2 = 116 - 3 \cdot (154 - 116) \qquad \Rightarrow \qquad 2 = 4 \cdot 116 - 3 \cdot 154.$$

Furthermore, 116 is a linear combination of 154 and 578, giving us that

$$2 = 4 \cdot (578 - 3 \cdot 154) - 3 \cdot 154 \qquad \Rightarrow \qquad 2 = 4 \cdot 578 - 15 \cdot 154.$$

In the final step, we use that 154 is a linear combination of 732 and 578 to find

$$2 = 4 \cdot 578 - 15 \cdot (732 - 578) \qquad \Rightarrow \qquad 2 = -15 \cdot 732 + 19 \cdot 578.$$

THEOREM 7.2.5. *Every nonempty list $(q_0, \ldots, q_N)$ of positive integers uniquely determines a pair (a, b) of relatively prime positive integers such that $a > b$. In other words, there is a bijection*

$$\{(q_0, \ldots, q_N) \mid q_i \geq 1 \text{ for all } 0 \leq i \leq N\} \cong \{(a, b) \mid \gcd(a, b) = 1 \text{ and } a > b > 0\}.$$

7.3 Linear Diophantine Equations in Multiple Variables

In this section we turn our attention to linear Diophantine equations in two variables, that is, integer equations of the form

$$ax + by = c.$$

We begin by applying the theory of ideals to establish that this equation has a solution if and only if $\gcd(a, b) \mid c$.

Theorem 7.3.1. *Consider integers a, b, and c, and let $d = \gcd(a, b)$. The linear Diophantine equation*

$$ax + by = c$$

is solvable with integers x and y if and only if $d \mid c$.

Proof. The first part of the claim is equivalent to the claim that we have an equality of ideals

$$(a) + (b) = (\gcd(a, b)).$$

We recall that the ideal $I + J$ consists of sums $x + y$ of $x \in I$ and $y \in J$. Furthermore, the ideals (a) and (b) consist of multiples of a and b, respectively. Thus the ideal $(a) + (b)$ consists of all the linear combinations of a and b; in other words, all the possible integers c for which there is a solution to the equation $ax + by = c$.

In Theorem 7.1.3 we defined $\gcd(a, b)$ to be the unique natural number d such that $(a) + (b) = (d)$. Such a natural number exists by Theorem 6.3.4. Now we observe that the equality

$$(a) + (b) = (\gcd(a, b))$$

tells us exactly that the set of integers c for which there exists a solution of the equation $ax + by = c$ has the same elements as the set of multiples of $\gcd(a, b)$. In other words, a solution to $ax + by = c$ exists if and only if c is a multiple of the greatest common divisor of a and b. □

As an immediate corollary of the previous theorem, we note that:

Corollary 7.3.2. *If a and b are relatively prime integers, then the linear Diophantine equation*

$$ax + by = c$$

is solvable for any c.

Now that we have established a necessary and sufficient condition for its solvability, it remains to describe a way of finding all solutions, if there are any. Notice that we have already collected quite a bit of useful information. Euclid's algorithm allows find a solution to the equation

$$ax + by = d,$$

where $d = \gcd(a, b)$. Thus, if $c = kd$, then we can solve

$$ax + by = c$$

by first finding a solution $ax_0 + by_0 = d$ by Euclid's algorithm. Then we find that

$$a(kx_0) + b(ky_0) = kd = c.$$

In other words, we can use Euclid's algorithm to find a solution to the equation $ax + by = c$ if it has any.

PROPOSITION 7.3.3. *Consider integers a, b, and c, and assume that a and b are relatively prime. If $ax_0 + by_0 = c$ is a solution to the Diophantine equation*

$$ax + by = c,$$

then every solution is of the form

$$x = x_0 + bk, \qquad \text{and} \qquad y = y_0 - ak.$$

PROOF. Suppose that $ax + by = c$ is another solution. Then it follows that

$$a(x - x_0) + b(y - y_0) = 0.$$

In other words, we have $a(x - x_0) = -b(y - y_0)$. Thus we see that $b(y - y_0)$ is divisible by a. Since a and b are relatively prime, this implies that $a \mid y - y_0$. Similarly, $a(x - x_0)$ is divisible by b, and therefore it follows that $b \mid x - x_0$. Furthermore, if $ka = y - y_0$ and $lb = x - x_0$. Then the equation

$$lab - kab = 0$$

implies that $k = l$. In other words, $x = x_0 + bk$ and $y = y_0 - ak$. □

THEOREM 7.3.4. *Suppose that $ax_0, by_0 = c$ is a solution to the Diophantine equation*

$$ax + by = c.$$

Then every solution is of the form

$$x = x_0 + \frac{b}{d}k, \qquad \text{and} \qquad y = y_0 - \frac{a}{d}k.$$

PROOF. This theorem follows from the previous proposition. If $d = \gcd(a, b)$, then we find that

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}.$$

The integers $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime, so we find that $x = x_0 + \frac{b}{d}k$ and $y = y_0 - \frac{a}{d}k$ for some integer k. □

7.4 Āryabhaṭa's Computations of the Positions of Planets

Exercises

Starter Exercises

7.1 Suppose that d is a common divisor of two nonzero integers a and b.

(a) Show that the greatest common divisor of a/d and b/d is $\gcd(a,b)/d$.
(b) Show that d is a greatest common divisor of a and b if and only if a/d and b/d are relatively prime.

7.2 Show that $a \mid bc$ if and only if $a/\gcd(a,b) \mid c$.
7.3 Show that if $\gcd(a,b) = 1$ and both $a \mid c$ and $b \mid c$, then $ab \mid c$.
7.4 Show that $\gcd(a^n, b^n) = \gcd(a,b)^n$.
7.5 Show that if $d \mid a+b$, then $\gcd(d,a) \mid \gcd(a,b)$ and $\gcd(d,b) \mid \gcd(a,b)$. Conclude that if a and b are relatively prime, then d is relatively prime to both a and b.
7.6 Consider three integers a, b, and c. Show that the following are equivalent:

(i) The integers a and b are both relatively prime to c.

(ii) The integer ab is relatively prime to c.

Routine-Building Exercises

7.7 Show that $a \mid b$ implies $ac \mid bc$. Furthermore, show that if c is nonzero, then $ac \mid bc$ implies $a \mid b$. Conclude that $a^n \mid b^n$ if and only if $a \mid b$ for any nonzero natural number n.
7.8 (a) Show that any three consecutive Fibonacci numbers are pairwise relatively prime.
(b) Find all n for which the five consecutive Fibonacci numbers $F_n, ..., F_{n+4}$ are pairwise relatively prime.
7.9 Show that $n! + 1$ and $(n+1)! + 1$ are relatively prime for all nonzero n.

Challenge Exercises

7.10 (a) Show that if a and b are both relatively prime to 24, then $a^2 - b^2$ is divisible by 24.
(b) A *generalized pentagonal number* is a number of the form

$$\frac{3k^2 \pm k}{2}.$$

Show that if a is the nth integer relatively prime to 24, then the number

$$\frac{a^2 - 1}{24}.$$

is the nth generalized pentagonal number.



(c) Let $0 \le a \le b \le c$ be integers such that their squares form an arithmetic progression; that is, the numbers a^2, b^2, and c^2 listed in increasing order have a common increment:

$$\Delta := b^2 - a^2 = c^2 - b^2.$$

Show that Δ is a multiple of 24 [FS1987].

(d) Find five examples of triples (a, b, c) as described in part (a), and explain how you found them.

7.11 (a) Consider two positive integers a and n such that $\gcd(a, n) = 1$. Prove that there is a natural number m such that

$$n \;\Big|\; \sum_{k=0}^{m} a^k.$$

Hint: Apply the pigeonhole principle.

(b) Find the least positive integer m such that

$$7 \;\Big|\; \sum_{k=0}^{m-1} 10^k = \underbrace{11\cdots1}_{m}.$$

7.12 Show that $2^m - 1$ and $2^n + 1$ are relatively prime, provided that m is odd.

7.13 Show that

$$\binom{a+k}{k} \;\Big|\; \operatorname{lcm}(a, a+1, \ldots, a+k).$$

7.14 (Erdős) Show that any set of $n+1$ integers chosen from an interval $a, \ldots, a+2n-1$ must contain a pair of relatively prime integers.

7.15 An interval $a, \ldots, a+n-1$ of consecutive positive integers is said to be *stapled* if it does not contain any integer that is relatively prime to all the others [EVA1969]. The sequence A090318 of the OEIS lists for each n the first positive integer a such that the interval $a, \ldots, a+n-1$ is stapled, or 0 if no such number exists. This sequence starts to show nonzero values from $n = 17$ onwards, with the value 2184 at $n = 17$.

(a) Check that the interval $2184, \ldots, 2200$ is stapled.

(b) Show that in every interval of ten consecutive digits there is an integer that is relatively prime to all the others. In other words, no interval of ten consecutive digits is stapled.

Chapter 8

Congruences

8.1 The Congruence Relations

Carl Friedrich Gauss introduced the congruence relations in his *Disquisitiones Arithmeticae* [Gau1986], which stands as the first systematic treatise on number theory. By introducing the congruence relations, he simplified the study of the classes of numbers that differ by a multiple of a given modulus. In doing so, proofs involving these classes became more transparent and insightful.

Definition 8.1.1. We say that a is **congruent to** b **modulo** c, written

$$a \equiv b \pmod{c},$$

if $c \mid a - b$. The number c is called the **modulus** of the congruence.

Example 8.1.2. We have

$$17 \equiv 2 \pmod{3}$$

because $17 - 2 = 15$ and 15 is divisible by 3. Similarly, we have

$$28 \equiv 3 \pmod{5}$$

because $28 - 3 = 25$ and 25 is divisible by 5.

Example 8.1.3. The most well-known system for modular arithmetic is the 12-hour clock. If a typical 8-hour workday starts at 9 in the morning, then it ends at

$$9 + 8 \equiv 5 \pmod{12},$$





Figure 8.1: The 12-hour clock contains two systems of modular arithmetic: A system with modulus 12 to mark the hours and a system with modulus 60 to mark the minutes.

that is, at 5 in the afternoon. Analog clocks also display a modular system with base 60 to mark the minutes.

Since the clock is the most well-known system of modular arithmetic, some people use the term *clock arithmetic* for modular arithmetic.

EXAMPLE 8.1.4. A classic application of modular arithmetic is to compute the day of the week it is on any given date. Various people, including Gauss, Zeller, and Conway, have found algorithms for this purpose. We will present here Zeller's algorithm to compute which day of the week it is on day d of month m in year y.

In essence, the weekday algorithm proceeds by separately computing the number $Y(y)$ of days in all the prior years, the number $M(m)$ in all the prior months of the current year, and the number $D(d)$ of all the days in the current month. The number

$$Y(y) + M(m) + D(d)$$

thus obtained is then reduced modulo 7 and calibrated to obtain the following corre-

spondence between residues modulo 7 and days of the week:

$$\begin{aligned} 0 &\mapsto \text{Sunday}, \\ 1 &\mapsto \text{Monday}, \\ &\vdots \\ 6 &\mapsto \text{Saturday}. \end{aligned}$$

The main difficulty is obtaining the right correction terms for leap days. Since leap days are added at the end of February, it is therefore customary to consider the days in January and February to belong to the prior year. That is, we will be working with the values

$$m' := \begin{cases} m+12 & \text{if } m = 1 \text{ or } m = 2, \\ m & \text{otherwise,} \end{cases}$$

$$y' := \begin{cases} y-1 & \text{if } m = 1 \text{ or } m = 2, \\ y & \text{otherwise.} \end{cases}$$

Every year has 365 days, except in a leap year, which has an extra day at the end of February. In the Gregorian calendar, every fourth year is a leap year, except every hundredth year, in which the leap day is skipped, except every four hundredth year, in which skipping the leap day is skipped. Thus, the exact number of days in all years prior to the given date is

$$Y(y') := 365y' + \left\lfloor \frac{y'}{4} \right\rfloor - \left\lfloor \frac{y'}{100} \right\rfloor + \left\lfloor \frac{y'}{400} \right\rfloor.$$

Furthermore, since we are only interested in the quantity $Y(y')$ modulo 7, we observe that $365 \equiv 1 \pmod 7$ so that the factor 365 can be dropped from the first term.

The quantity $M(m')$ returns the number of days in all full months in the given year y', from March to the given month m'. The standard length of one month is 30 days, so that $M(m')$ is $30(m'-3)$ and a correction term for the months having a 31st day. The months from March to January having a 31st day follow the following pattern:

$$1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1.$$

Note that there is a recurring pattern of $1, 0, 1, 0, 1$, which is truncated after eleven steps. The function that makes increments of 1 according to this pattern is given by

$$\left\lfloor \frac{3x+2}{5} \right\rfloor.$$

Thus, the number $M(m')$ of days in the year from March 1st onwards is

$$M(m') := 30(m'-3) + \left\lfloor \frac{3(m'-3)+2}{5} \right\rfloor.$$

We note that $30 \equiv 2 \pmod{7}$, so the factor 30 in the first term may be replaced by 2. Furthermore, we will drop any constants such as $2 \cdot (-3)$ since we will be recalibrating the function towards the end.

Finally, we add the number d of the given day in the month plus a given calibration constant c. The formula that calculates the correct day in the week is thus

$$y' + \left\lfloor \frac{y'}{4} \right\rfloor - \left\lfloor \frac{y'}{100} \right\rfloor + \left\lfloor \frac{y'}{400} \right\rfloor + 2m' + \left\lfloor \frac{3m'-2}{5} \right\rfloor + d + 2 \pmod{7},$$

where m' and y' are determined as previously specified.

The lecture in which this example is presented was on September 23rd, 2025. For this date, we have $d := 23$, $m' := 9$, and $y' = 2025$. Then $Y(y') = 2025 + 506 - 20 + 5 = 2516$, $M(m') = 2 \cdot 9 + 5 = 23$ and $D(d) = 23 + 2 = 25$, so that the day of the week comes out to be

$$2516 + 23 + 25 \equiv 2 \pmod{7},$$

a Tuesday.

We note that our formula for the day of the week does not take into account some rare oddities, most of which have occurred during the process of switching from the Julian calendar to the Gregorian calendar. Italy, Poland, Portugal, and Spain skipped 10 days between Thursday, October 4th, and Friday, October 15th; Sweden and Finland had a February 30th in 1712; Britain and its colonies skipped 11 days from Wednesday, September 2nd, 1752 to Thursday, September 14th, 1752; and Greece skipped 13 days between February 14th, 1923 and March 1st, 1923. In 1867, when the US bought Alaska from Russia and Alaska switched from the Julian calendar to the Gregorian calendar, Friday, October 6th was followed by Friday, October 18th, thus having two consecutive Fridays.

REMARK 8.1.5. Congruence modulo 0 is equality, because $0 \mid b - a$ holds if and only if $b - a = 0$. Congruence modulo 1, on the other hand, is true for any two integers a and b, because $1 \mid b - a$ is always true.

Also, we note that $a \equiv b \pmod{c}$ holds if and only if $a \equiv b \pmod{-c}$ holds. For this reason, the modulus is usually taken to be a natural number n.

In the following lemma we establish that a and b are congruent modulo n if and only if they have the same remainder after division by n.

LEMMA 8.1.6. *Consider integers a and b, and a positive natural number n, and suppose that $a = qn + r$ and $b = pn + s$, where $0 \leq r, s < n$. Then the congruence*

$$a \equiv b \pmod{n}$$

holds if and only if $r = s$.

PROOF. By definition, the congruence $a \equiv b \pmod{n}$ holds if and only if $n \mid a - b$. Since $a = qn + r$ and $b = pn + s$, where $0 \leq r, s < n$ we see that $n \mid a - b$ holds if and only if $n \mid (qn + r) - (pn + s)$. Rewriting the expressing $(qn + r) - (pn + s)$, we see that

$$n \mid (qn + r) - (pn + s) \qquad \text{if and only if} \qquad n \mid (q - p)n + (r - s).$$

Now we note that the number $(q-p)n$ is divisible by n, so we find that $n \mid (q-p)n+(r-s)$ holds if and only if $n \mid r-s$. However, the number $r-s$ satisfies the strict inequalities

$$-n < r-s < n,$$

and the only integer in this range that is divisible by n is the integer 0. Thus we see that $n \mid r-s$ holds if and only if $r = s$, completing the chain of logical equivalences. □

Example 8.1.7. Recall from Theorem 5.4.1 that any number n can be written as

$$n = \sum_{i=0}^{l-1} d_i b^i$$

in base $b > 1$. Given that n is written in this way, we have $n \equiv d_0 \pmod{b}$. Indeed, the digit d_0 was constructed using Theorem 5.3.1 (The Euclidean Division Theorem) as the remainder of n after division by b. For example, the congruence $37 \equiv 7 \pmod{10}$ holds.

An important property of the congruence relations, which makes them so useful in the study of the integers, is that they are compatible with the arithmetic operations of addition and multiplication.

Proposition 8.1.8. *Suppose that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. Then the following congruences hold:*

$$a + b \equiv a' + b' \pmod{n},$$

$$ab \equiv a'b' \pmod{n}.$$

Consequently, for any integers x and y,

$$ax + by \equiv a'x + b'y \pmod{n}.$$

Proof. By assumption we have that $n \mid a - a'$ and $n \mid b - b'$. Thus it follows that n divides the sum

$$n \mid (a - a') + (b - b') = (a + b) - (a' + b'),$$

which shows that $a+b \equiv a'+b' \pmod{n}$. Moreover, n divides any linear combination of $a - a'$ and $b - b'$, so in particular we have

$$n \mid (a - a')b + a'(b - b') = ab - a'b + a'b - a'b' = ab - a'b'.$$

This shows that $ab \equiv a'b' \pmod{n}$. □

One way of thinking about the following corollary, is that every polynomial is periodic modulo n. In other words, every polynomial repeats itself modulo n after every n steps.

COROLLARY 8.1.9. *If* $x \equiv y \pmod{n}$, *then we have*

$$\sum_{k=0}^{l-1} a_k x^k \equiv \sum_{k=0}^{l-1} a_k y^k \pmod{n}.$$

The power of modular arithmetic is effectively demonstrated with divisibility tests. Consider a number n written in base 10 as

$$n = \sum_{k=0}^{l-1} d_k 10^k.$$

Then n is divisible by 9 if and only if the sum of its digits is divisible by 9. Indeed, since $10 \equiv 1 \pmod{9}$, it follows that

$$\sum_{k=0}^{l-1} d_k 10^k \equiv \sum_{k=0}^{l-1} d_k 1^k \pmod{9},$$

and we recognize that the right-hand side is just the sum of the digits of n. For example, the number $34,524$ is divisible by 9 because $3+4+5+2+4 = 18$ and the number 18 is divisible by 9 because $1+8=9$.

REMARK 8.1.10. One might wonder whether congruence relations are also preserved by operations like the greatest common divisor. However, this is not the case. For a counter example, consider the congruences $6 \equiv 16 \pmod{10}$ and $15 \equiv 25 \pmod{10}$. The greatest common divisor of 6 and 15 is 3, while the greatest common divisor of 16 and 25 is 1. Thus we see that, even though $6 \equiv 16$ and $15 \equiv 25$ modulo 10, we have

$$\gcd(6,15) \not\equiv \gcd(16,25) \pmod{10}.$$

8.2 Equivalence Relations

The congruence relations are examples of equivalence relations, which we will now define.

DEFINITION 8.2.1. An **equivalence relation** on a set A is a binary relation $\sim$ satisfying the following three conditions:

(i) **Reflexivity.** For any element $a \in A$, we have

$$a \sim a.$$

(ii) **Symmetry.** For any two elements $a, b \in A$, we have

$$(a \sim b) \Rightarrow (b \sim a).$$

(iii) **Transitivity.** For any three elements $a, b, c \in A$, we have

$$(a \sim b) \wedge (b \sim c) \Rightarrow (a \sim c).$$

Thus, where the ordering relation of a poset is reflexive, *antisymmetric* and transitive, an equivalence relation is reflexive, *symmetric* and transitive. The standard example of an equivalence relation is equality itself, which is indeed reflexive, symmetric and transitive.

Proposition 8.2.2. *For any natural number n, the congruence relation $\equiv$ modulo n is an equivalence relation.*

Proof. To see that the congruence relation modulo n is reflexive, note that $a - a = 0$ and any number divides 0. Thus the congruence $a \equiv a \pmod{n}$ always holds. To see that the congruence relation modulo n is symmetric, note that if $n \mid a - b$ then $n \mid -(a-b) = b-a$. This shows that $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$. To see that the congruence relation modulo n is transitive, assume that $n \mid a - b$ and that $n \mid b - c$. Then it follows that

$$n \mid (a - b) + (b - c) = a - c,$$

showing that $a \equiv c \pmod{n}$. □

Proposition 8.2.3. *For any two integer fractions $\frac{a}{b}$ and $\frac{c}{d}$, the sameness relation given by*

$$\frac{a}{b} = \frac{c}{d} := (ad - bc = 0)$$

is an equivalence relation.

Proof. Reflexivity follows from the fact that $ab - ba = 0$. Symmetry follows from the fact that if $ad - bc = 0$, then $cb - da = 0$. To prove transitivity, suppose that $ad - bc = 0$ and $cf - de = 0$. Then we have

$$d(af - be) = (da)f - b(de) = (bc)f - b(cf) = 0.$$

Since denominators of integer fractions are assumed to be nonzero, it follows that $d \neq 0$, so that $af - be = 0$. □

Equivalence relations come about in many forms, and one can get quite creative in defining them. We illustrate the generality of equivalence relations with some examples.

A common way in which equivalence relations come about is via a function. Given a function $f : A \to B$, there is an equivalence relation $\sim_f$ on the set A, given by

$$x \sim_f y \qquad \text{if and only if} \qquad f(x) = f(y).$$

This relation is also called the **kernel** of f.

Proposition 8.2.4. *For any function $f : A \to B$, the relation $\sim_f$ is an equivalence relation.*



PROOF. To see that any relation of the form $\sim_f$ is an equivalence relation, we need to check reflexivity, symmetry, and transitivity. Note that we have reflexivity because $f(x) = f(x)$ for any $x \in A$. The relation $\sim_f$ is symmetric because $f(y) = f(x)$ holds whenever $f(x) = f(y)$ holds. Finally, the relation $\sim_f$ is transitive because $f(x) = f(z)$ holds whenever both $f(x) = f(y)$ and $f(y) = f(z)$ hold. □

EXAMPLE 8.2.5. Consider the function $r : \mathbb{Z} \to \{0, \dots, n-1\}$, defined via Theorem 5.3.1 (The Euclidean Division Theorem) so that $r(x)$ is the unique integer $0 \leq r(x) < n$ such that $x - r(x)$ is divisible by n. Then the equivalence relation $\sim_r$ is such that $x \sim_r y$ if and only if x and y have the same remainder after division by n. In other words,

$$x \sim_r y \Leftrightarrow x \equiv y \pmod{n}.$$

Another way in which equivalence relations come about is by looking at iterations of an operation $T : X \to X$. We illustrate this by an example first.

EXAMPLE 8.2.6. Recall from Exercise 5.7 that Zeckendorf's representation theorem established that any natural number n can be written uniquely as a sum

$$n = \sum_{k=0}^{l_n - 1} d_{n,k} F_{k+2}$$

of nonconsecutive Fibonacci numbers with index at least 2. Now we define an equivalence relation $\sim_F$ by declaring that two natural numbers m and n are equivalent, if one can be obtained from the other by shifting their Zeckendorf representation. More precisely, we define $m \sim_F n$ to hold if and only if there exist natural numbers s and t such that

$$\sum_{k=0}^{l_m - 1} d_{m,k} F_{k+s+2} = \sum_{k=0}^{l_n - 1} d_{n,k} F_{k+t+2}.$$

For example, the number 17 is written $(100101)_F$ in the Zeckendorf notation, and its shifts are the numbers $(1001010)_F = 28$, $(10010100)_F = 45$, and so on. Thus we have

$$17 \sim_F 28 \sim_F 45 \sim_F \cdots.$$

The general method of obtaining equivalence relations of this kind assumes an arbitrary operation $T : A \to A$. Given such an operation, we define the equivalence relation $\sim_T$ by declaring that

$$x \sim_T y \qquad \text{if and only if} \qquad \exists_{(s,t \in \mathbb{N})} T^s(x) = T^t(y).$$

In technical terminology, the set A equipped with the operation T form a *dynamical system*, and when $x \sim_T y$ holds we say that x and y have the same *eventual orbit*. The operation T in the equivalence relation $\sim_F$ of the previous example is the shift operation on the Zeckendorf representation, which simply appends a digit 0.

Proposition 8.2.7. *For any operation T on a set A, the relation $\sim_T$ is an equivalence relation.*

Proof. To see that the relation $\sim_T$ is indeed an equivalence relation, we need to verify reflexivity, symmetry, and transitivity.

The relation $\sim_T$ is reflexive, because $T^0(x) = x = T^0(x)$, and the relation $\sim_T$ is symmetric because the condition that $\exists_{(s,t\in\mathbb{N})}(T^s(x) = T^t(y))$ is symmetric in x and y. To see that $\sim_T$ is transitive, consider s, t, u, v such that $T^s(x) = T^t(y)$ and $T^u(y) = T^v(z)$. Then we have

$$T^{u+s}(x) = T^u(T^s(x)) = T^u(T^t(y)) = T^t(T^u(y)) = T^t(T^v(z)) = T^{t+v}(z),$$

showing that $x \sim_T z$. □

Perhaps one of the most famous dynamical systems on the set of positive integers is due to Collatz, whose function T is defined by

$$T(n) := \begin{cases} n/2 & \text{if } n \text{ is even,} \\ 3n+1 & \text{otherwise.} \end{cases}$$

For example, starting at the number 3, repeated application of the Collatz function produces the sequence:

$$3,\ 10,\ 5,\ 16,\ 8,\ 4,\ 2,\ 1,\ 4, \cdots.$$

Once the sequence reaches 1, it enters the cycle

$$1 \mapsto 4 \mapsto 2 \mapsto 1 \mapsto \cdots$$

The famous and elusive *Collatz conjecture* states that for every positive integer n, the sequence

$$n,\ T(n),\ T^2(n),\ \ldots$$

eventually reaches the value 1. In our notation, the Collatz conjecture asserts that $n \sim_T 1$ for every positive natural number n.

8.3 Equivalence Classes and Residue Systems

Definition 8.3.1. Consider an equivalence relation $\sim$ on a set A. Then the **equivalence class** of an element $a \in A$ is the set

$$[a] := \{x \in A \mid a \sim x\}.$$

Example 8.3.2. In the case where the equivalence relation under consideration is a congruence relation with modulus n, then the equivalence classes are called **congruence classes**. For any positive integer n, there are exactly n distinct congruence classes modulo n, corresponding to the n possible residues $0 \leq r < n$ after division by n with remainder.



The congruence class modulo 2 of any even integer consists precisely of all the even integers, and the congruence class of any odd integer consists precisely of all the odd integers.

To see this, suppose that a is an even integer. Then $a \equiv x \pmod 2$ holds if and only if a and x have the same remainder after division by 2. Since the remainder of a divided by 2 is 0, it follows that a is congruent to x precisely when x is divisible by 2; that is, when x is even. This shows that for an even integer a, the congruence class

$$[a] := \{x \in A \mid a \equiv x \pmod 2\}$$

is the set of even numbers.

Similarly, if a is an odd integer, then $a \equiv x \pmod 2$ holds if and only if x is also odd, because $a \equiv x \pmod 2$ holds if and only if x divided by 2 has remainder 1, which means that x is odd.

The equivalence classes of an equivalence relation $\sim$ on a set A form a set

$$A/\sim := \{U \subseteq A \mid \exists_{(a \in A)} U = [a]\}$$

In other words, the set of equivalence classes of $\sim$ is the set of subsets $U \subseteq A$ such that $U = [a]$ for some $a \in A$. The set $A/\sim$ is called the **quotient** of A by the equivalence relation $\sim$. Furthermore, the function

$$a \mapsto [a] : A \to A/\sim$$

sending an element to its equivalence class is called the **quotient map**. We often write q for the quotient map.

PROPOSITION 8.3.3. *For any equivalence relation $\sim$ on a set A, the quotient map*

$$a \mapsto [a] : A \to A/\sim$$

satisfies the following two conditions:

(i) *The quotient map is surjective. This means that for any equivalence class $U \subseteq A$ there is an element $a \in A$ such that $U = [a]$.*

(ii) *The quotient map is **effective**. This means that for any two elements $a, b \in A$ we have*

$$[a] = [b] \qquad \textit{if and only if} \qquad a \sim b.$$

PROOF. The first claim is true by definition: the set of equivalence classes is defined as

$$\{U \subseteq A \mid \exists_{(a \in A)} U = [a]\}.$$

In other words, the set of equivalence classes is the set of subsets of A of the form $[a]$ for some $a \in A$.

For the second claim, let $a, b \in A$. If we have the equality $[a] = [b]$, then it follows that $b \in [a]$, so that $a \sim b$. For the converse, if $a \sim b$ holds, and $x \in A$, then we have $a \sim x$ if and only if $b \sim x$ by symmetry and transitivity of the relation $\sim$. This shows that $x \in [a]$ if and only if $x \in [b]$. Thus, the subsets $[a]$ and $[b]$ contain the same elements, so they must be the same. □

Definition 8.3.4. A **complete residue system** modulo n is a choice of exactly one element from each congruence class modulo n. In other words, a complete residue system is a set

$$\{r_1, \dots, r_n\}$$

satisfying the condition that for every integer a there is a exactly one index $1 \leq i \leq n$ such that

$$a \equiv r_i \pmod{n}.$$

Example 8.3.5. For every nonnegative integer n, the set

$$\{0, \dots, n-1\}$$

forms a complete residue system modulo n. Similarly, any set

$$\{a, \dots, a+n-1\}$$

of n consecutive integers is a complete residue system modulo n.

Remark 8.3.6. Since complete residue systems contain a unique element in every congruence class, there is for every complete residue system $\{r_0, \dots, r_{n-1}\}$ a bijection

$$\mathbb{N}/(\equiv \pmod{n}) \cong \{r_0, \dots, r_{n-1}\}.$$

8.4 Modular Arithmetic

We have seen that the congruence relations modulo a natural number n form equivalence relations that are compatible with the arithmetic operations of addition and multiplication. We have also seen that equivalence relations give rise to equivalence classes, and that the set of all equivalence classes for a given equivalence relation is called the **quotient**. Quotients are important mathematical constructions, which are used to simplify mathematical problems and constructions by treating similar or equivalent elements of a set as the same.

Definition 8.4.1. We define the set $\mathbb{Z}/n\mathbb{Z}$ of **integers modulo** n as the set of congruence classes modulo n.

The set of integers modulo n can be equipped with addition and multiplication in the following way:

$$[a] + [b] := [a+b]$$
$$[a][b] := [ab]$$



Notice that the result of these operations depends only on the equivalence classes, not on the particular integers a and b chosen to represent the equivalence classes $[a]$ and $[b]$. Recall from Proposition 8.3.3 that we have $[a] = [a']$ if and only if $a \equiv a' \pmod{n}$, and similarly we have $[b] = [b']$ if and only if $b \equiv b' \pmod{n}$. Thus, for any $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, it follows from Proposition 8.1.8 that $a + b \equiv a' + b' \pmod{n}$ and $ab \equiv a'b' \pmod{n}$. In other words, if $[a] = [a']$ and $[b] = [b']$, then we have

$$[a] + [b] = [a'] + [b']$$
$$[a][b] = [a'][b'].$$

This ensures that the definitions of addition and multiplication on the integers modulo n is *well-defined* on the congruence classes modulo n.

REMARK 8.4.2. The definitions of addition and multiplication on the integers modulo n follow a general pattern of defining functions $f : A/\sim \to B$ out of quotient sets. Given a function $g : A \to B$, a function $f : A/\sim \to B$ is said to be **defined by descent** from g if f is defined by

$$f([a]) := g(a).$$

For this definition to make sense, the values of f must depend only on the equivalence classes. In other words, if a and a' represent the same equivalence class, so that $a \sim a'$, then we must have that $f([a]) = f([a'])$. In other words, we must have that

$$g(a) = g(a').$$

By verifying that $a \sim a'$ implies $f([a]) = f([a'])$, we ensure that f is **well-defined**. The well-definedness condition ensures that f returns the same output for all elements of the same equivalence class.

EXAMPLE 8.4.3. The well-definedness condition is important to verify, because not all functions are well-defined with respect to the congruence relations modulo n.

Take, for example, the absolute value function $a \mapsto |a|$ on the integers. Then the operation

$$[a] \mapsto |a|$$

is not well-defined on the integers modulo 3, because $2 \equiv -1 \pmod{3}$ while

$$|2| \not\equiv |-1| \pmod{3}.$$

Typical functions that *are* well defined on congruence classes modulo n, include functions that are entirely built up from arithmetic operations, such as polynomials.

Theorem 8.4.4. *The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n satisfies the following laws of arithmetic:*

$$\begin{aligned} (x+y)+z &= x+(y+z) & (xy)z &= x(yz) \\ 0+x &= x & 1x &= x \\ x+0 &= x & x1 &= x \\ x-x &= 0 & x(y+z) &= xy+xz \\ -x+x &= 0 & (x+y)z &= xz+yz \\ x+y &= y+x & xy &= yx. \end{aligned}$$

In proper mathematical parlance: the set $\mathbb{Z}/n\mathbb{Z}$ equipped with the operations of addition and multiplication form a commutative ring.

Proof. To see that $(x+y)+z = x+(y+z)$, we first note that the variables x, y, and z represent congruence classes of integers modulo n. Since for every congruence class there is an integer representing it, it suffices to prove that

$$([a]+[b])+[c] = [a]+([b]+[c]).$$

By unfolding the definitions, this equation reduces to

$$[(a+b)+c] = [a+(b+c)].$$

However, the integers $(a+b)+c$ and $a+(b+c)$ are equal, so their equivalence classes are the same.

The proofs of the other properties follow a very similar pattern. We will give the proofs of commutativity of addition and distributivity of multiplication over addition from the left, but leave the other proofs to the reader.

To see that $x+y = y+x$, it suffices to show that

$$[a]+[b] = [b]+[a].$$

By unfolding the definitions, this equation reduces to

$$[a+b] = [b+a],$$

and indeed those equivalence classes are the same, because $a+b = b+a$ holds for any two integers a and b.

To see that $x(y+z) = xy+xz$, it suffices to show that

$$[a]([b]+[c]) = [a][b]+[a][c].$$

By unfolding the definitions, this equation reduces to

$$[a(b+c)] = [ab+ac].$$

Again, this identification of equivalence classes holds, because we have the equality $a(b+c) = ab+ac$. □



8.5 The Multiplicative Order of an Integer Modulo n

Expanding a fraction such as $1/7$ in decimal notation amounts to writing

$$\frac{1}{7} = \sum_{k=0}^{\infty} \frac{d_k}{10^k},$$

where each digit d_k is an integer from 0 to 9 except possibly the number d_0, which can be any integer. In the case of $1/7$, the integer d_0 is 0. The digits d_1, d_2, d_3 are called the tenth's digit, the hundredth's digit, the thousandth's digit, and so on.

We see from the above expression that the tenth's digit of $1/7$ can be computed as the integer part of the number $10/7$, which has all the decimal digits of $1/7$ shifted by one position to the left. It also follows that the remainder of the digits coincide with the digits of $3/7$, where the numerator is the remainder of 10 after division by 7. The first digit of the fractional part of $3/7$ is the integer part of $30/7$, which is 4. For the next digit after that, we take the remainder of 30 after division by 7, which is 2, and we compute the integer part of the fraction $20/7$. If we keep going in this manner, we find that

$$d_1 = \left\lfloor \frac{10}{7} \right\rfloor, \qquad d_2 = \left\lfloor \frac{30}{7} \right\rfloor, \qquad d_3 = \left\lfloor \frac{20}{7} \right\rfloor, \qquad d_4 = \left\lfloor \frac{60}{7} \right\rfloor,$$
$$d_5 = \left\lfloor \frac{40}{7} \right\rfloor, \qquad d_6 = \left\lfloor \frac{50}{7} \right\rfloor, \qquad d_7 = \left\lfloor \frac{10}{7} \right\rfloor.$$

Here we see that our task at hand begins to repeat itself. We have already computed the integer part of $10/7$ in the first step, which led us to compute the integer part of $30/7$, and so on. Thus, we find that the decimal expansion of $1/7$ is given by

$$\frac{1}{7} = 0.142857142857142857\ldots$$

This satisfies the property that, after shifting the decimal expansion for $1/7$ by 6 places, the decimal digits will line up exactly. A mathematically precise way of expressing that decimal expansion of the fraction $1/7$ repeats with period 6, is by the property that

$$\frac{10^6}{7} - \frac{1}{7} \in \mathbb{Z}.$$

Note that this difference of fractions is only an integer if 7 divides the number $10^6 - 1$. In other words,

$$10^6 \equiv 1 \pmod{7}.$$

Since 6 is the first positive integer for which $10^k \equiv 1 \pmod{7}$, we say that the *multiplicative order* of 10 modulo 7 is 6.

For the general definition of the multiplicative order of an element a modulo n, note that if $\gcd(a, n) = 1$, then we can simply define the multiplicative order of a to be the least positive integer k such that

$$a^k \equiv 1 \pmod{n}.$$

However, if $\gcd(a,n) \neq 1$ then there will not be such a positive integer. In this case we set the multiplicative order of a modulo n to be 0. At first glance, this may look quite arbitrary. However, there is a natural way of looking at it.

Definition 8.5.1. Consider an integer a and a natural number n. We define the **multiplicative order** of a modulo n to be the unique natural number m such that the ideal

$$I_{a,n} := \{k \in \mathbb{Z} \mid a^{|k|} \equiv 1 \pmod{n}\}$$

is the ideal (m) generated by m.

Using this definition, we see that if $\gcd(a,n) = 1$, then indeed the order $\mathrm{ord}_n(a)$ of a modulo n is the least positive integer k such that $a^k \equiv 1 \pmod{n}$. If $\gcd(a,n) \neq 1$, then the ideal $I_{a,n}$ is the zero ideal (0), which implies that $\mathrm{ord}_n(a) = 0$.

In the following theorem, which is also known as the *Order Theorem*, we will see that by setting the value of the order of a modulo n to be 0 when $\gcd(a,n) \neq 1$, we prove a powerful duality principle between multiples of $\mathrm{ord}_n(a)$ and numbers dividing $a^k - 1$.

Theorem 8.5.2 (Order Theorem). *The multiplicative order of an integer a modulo n satisfies the logical equivalence*

$$\mathrm{ord}_n(a) \mid k \Leftrightarrow n \mid a^k - 1.$$

Proof. We have two cases to consider: either $\gcd(a,n) = 1$ or $\gcd(a,n) \neq 1$. In the first case, $\mathrm{ord}_n(a)$ is the least positive integer m such that

$$a^m \equiv 1 \pmod{n}.$$

It is immediate from this condition that if $m \mid k$, then it follows that $a^k \equiv 1 \pmod{n}$. Conversely, if $a^k \equiv 1 \pmod{n}$, then we can write $k = qm + r$ by Theorem 5.3.1 (The Euclidean Division Theorem), where $0 \leq r < m$. It follows that

$$a^r \equiv a^{qm} a^r \equiv a^{qm+r} \equiv a^k \equiv 1 \pmod{n}.$$

Since r is strictly less than m and m is the least positive integer such that $a^m \equiv 1 \pmod{n}$, it follows that $r = 0$. Thus we conclude that $\mathrm{ord}_n(a) \mid k$. This proves the claim in the first case.

In the second case we have $\mathrm{ord}_n(a) = 0$. Then the condition that $\mathrm{ord}_n(a) \mid k$ is equivalent to the condition that $k = 0$. Thus, our task is to show that $n \mid a^k - 1$ if and only if $k = 0$. If $k = 0$, then we have $a^k - 1 = 0$ so that $n \mid a^k - 1$. This proves the reverse direction.

For the forward direction, assume that $n \mid a^k - 1$, and consider a common divisor $d > 1$ of a and n. Then we have $d \mid a^k - 1$. The assumption that $d > 1$ then implies that $d \nmid a^k$. On the other hand, we have assumed that $d \mid a$. Therefore, we must have $k = 0$. □



The Order Theorem can be used to show that the digits in the fractional part of a reduced integer fraction $\frac{a}{b}$ such that b is relatively prime to 10 are periodic. The case where b is not relatively prime can be dealt with from the relatively prime case, since we can multiply $\frac{a}{b}$ with a sufficiently high power of 10, so that after bringing it to lowest terms, the denominator becomes relatively prime to 10. This leads us to conclude that every rational number has an *eventually periodic* decimal expansion.

THEOREM 8.5.3. *Consider a reduced integer fraction $\frac{a}{b}$ with $\gcd(b, 10) = 1$. Then there exists a positive integer k such that*

$$10^k \frac{a}{b} - \frac{a}{b}$$

is an integer. Furthermore, the least such k is $\operatorname{ord}_b(10)$.

PROOF. The number $10^k \frac{a}{b} - \frac{a}{b}$ is an integer if and only if $b \mid 10^k a - a$, which is another way of expressing the condition

$$10^k a \equiv a \pmod{b}.$$

Furthermore, since a is assumed to be relatively prime to b, this is equivalent to the congruence

$$10^k \equiv 1 \pmod{b}.$$

By Theorem 8.5.2 (Order Theorem) it follows that this congruence holds if and only if $\operatorname{ord}_b(10) \mid k$. □

The logical equivalence in Theorem 8.5.2 (Order Theorem) can also be used effectively to compute the order of a power of an element in terms of the order of that element.

THEOREM 8.5.4. *For any integer a of order $k = \operatorname{ord}_n(a)$, we have*

$$\operatorname{ord}_n(a^m) = \frac{k}{\gcd(m, k)}.$$

In particular, we have $\operatorname{ord}_n(a^m) = k$ if and only if m and k are relatively prime.

PROOF. We have the following chain of logical equivalences:

$$\operatorname{ord}_n(a^m) \mid l \;\Leftrightarrow\; n \mid (a^m)^l - 1 \;\Leftrightarrow\; \operatorname{ord}_n(a) \mid ml \;\Leftrightarrow\; \frac{\operatorname{ord}_n(a)}{\gcd(m, \operatorname{ord}_n(a))} \mid l.$$

Thus, we see that $\operatorname{ord}_n(a^m)$ and $k/\gcd(m, k)$ divide the same numbers, so they must be equal. □

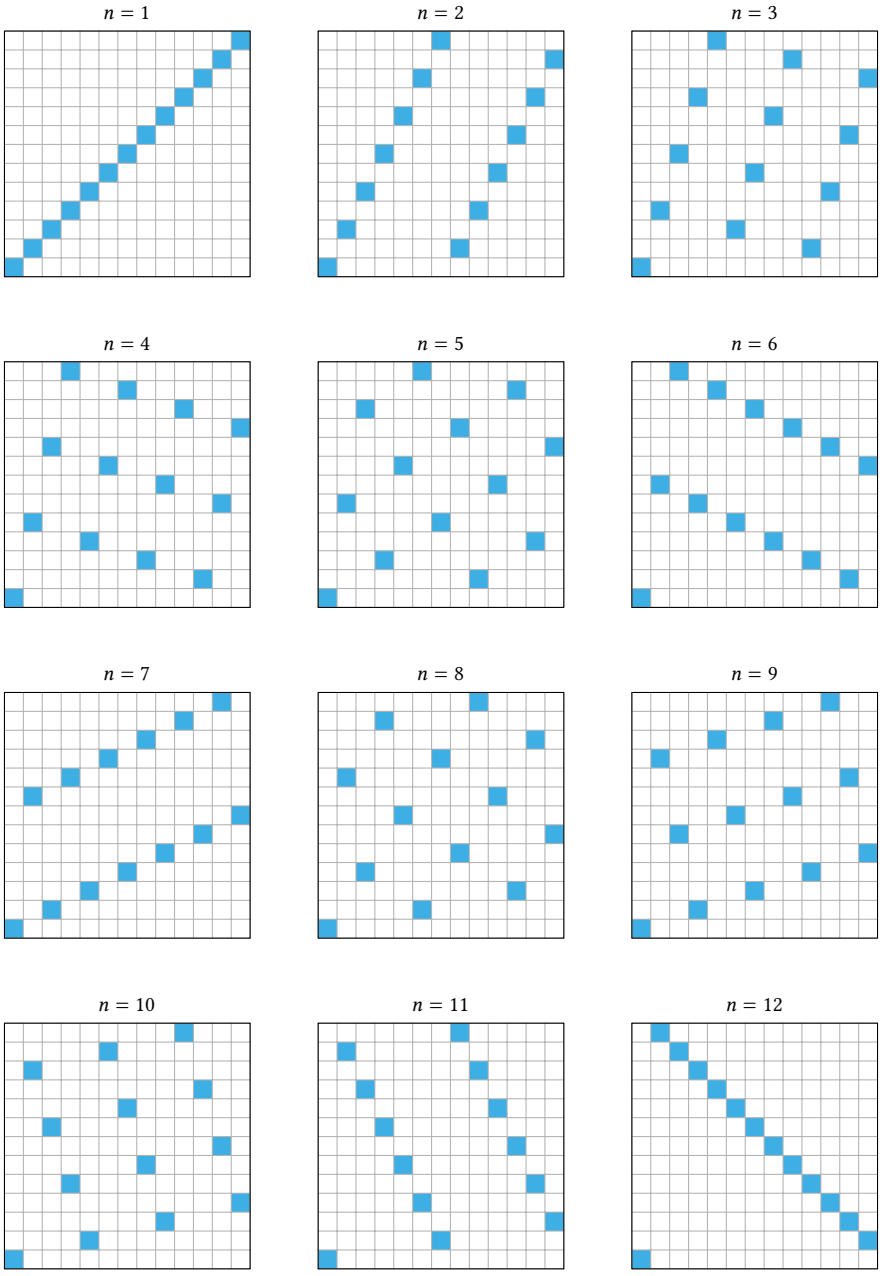


Figure 8.2: In the nth grid, the square (x, y) is colored blue if $y \equiv nx \pmod{13}$.

Exercises

Starter Exercises

8.1 Describe a complete residue system modulo 7 consisting entirely of multiples of 3.

8.2 List all the numbers $0 \leq a < 6$ such that $a \equiv x^2 \pmod{6}$ for some x, and all the numbers $0 \leq a < 8$ such that $a \equiv x^2 \pmod{8}$ for some x.

8.3 Find the multiplicative inverses of 1, 2, 3, 4, 5, and 6 modulo 7.

8.4 Find the multiplicative inverses of 1, 3, 7, 9, 11, 13, 17, and 19 modulo 20.

8.5 Show that $\operatorname{ord}_{a^k-1}(a) = k$.

8.6 Show that for any divisor $d \mid 1 + a + a^2 + \cdots + a^k$, we have

$$\operatorname{ord}_d(a) \mid k + 1.$$

Routine-Building Exercises

8.7 (a) Show that no century ever starts on a Sunday.
(b) Show that any seven consecutive leap days within a century run through all weekdays.

8.8 Show that the following are equivalent for any $n > 0$ and any integer a:

(i) $\gcd(a, n) = 1$.

(ii) There exists an integer b such that $ab \equiv 1 \pmod{n}$.

8.9 (a) Find integers k, a, and b such that

$$ka \equiv kb \pmod{4}, \qquad \text{but} \qquad a \not\equiv b \pmod{4}.$$

(b) Prove that if $\gcd(k, n) = d$, then we have

$$ka \equiv kb \pmod{n} \qquad \text{if and only if} \qquad a \equiv b \left(\mod \frac{n}{d}\right).$$

8.10 Show that if $a \equiv b \pmod{m}$, then we have

$$\gcd(a, m) = \gcd(b, m).$$

8.11 Show that for any modulus n, the number of integers $x \pmod{n}$ such that $x^2 \equiv 1 \pmod{n}$ is a power of 2.

8.12 Show that if $ab \equiv 1 \pmod{n}$, then

$$\operatorname{ord}_n(a) = \operatorname{ord}_n(b).$$

8.13 Consider an integer a. Show that if

$$a^m - 1 \mid a^n - 1,$$

then $m \mid n$.

8.14 Consider a bijection $f : X \to X$ on a finite set X, and let d be the number of elements in the orbit of an element x.

(a) Show that
$$f^k(x) = x \quad \Leftrightarrow \quad d \mid k.$$

(b) Which finite set X and which bijection $f : X \to X$ can be used to see that the previous part generalizes Theorem 8.5.2 (Order Theorem)?

Foundational Exercises

8.15 Consider a finite set X and a map $f : X \to X$. We say that two elements x and y of X lie **in the same orbit** of f if there exist natural numbers k and l such that
$$f^k(x) = f^l(y).$$

(a) Show that the relation $\sim$ is an equivalence relation.

Challenge Exercises

8.16 Let $F_n = 2^{2^n} + 1$ be the nth Fermat number. Show that $F_n \equiv 17 \pmod{24}$ for $n \geq 2$.

8.17 Prove that for any $n > 1$ and any k, we have
$$(n-1)^2 \mid n^k - 1 \qquad \text{if and only if} \qquad n - 1 \mid k.$$

Chapter 9

Systems of Linear Congruences

9.1 Solving Linear Congruences

The simplest linear congruence is the linear congruence

$$ax \equiv b \pmod{n}.$$

To solve this linear congruence, we are tasked with finding an integer x for which the congruence $ax \equiv b \pmod{n}$ holds. However, we may immediately observe that if $x \equiv x' \bmod n$, then the congruence $ax \equiv b \pmod{n}$ holds if and only if the congruence $ax' \equiv b \pmod{n}$ holds. Thus, we are really interested in solving such congruences in $\mathbb{Z}/n\mathbb{Z}$, i.e., in finding a congruence class $[x]$ modulo n for which the congruence $ax \equiv b \pmod{n}$ holds.

A complete solution to the linear congruence $ax \equiv b \pmod{n}$ is a description of the set of all congruence classes $[x]$ modulo n that satisfy the linear congruence. We typically list these solutions by listing the numbers $0 \leq x < n$ for which the congruence holds. For example, the linear congruence

$$4x \equiv 2 \pmod{6}$$

has two incongruent solutions modulo 6, the congruence classes of 2 and 5 modulo 6.

Definition 9.1.1. We say that a **divides** b modulo n if there exists an integer x for which the congruence

$$ax \equiv b \pmod{n}.$$

By the definition of congruence relations, the congruence $ax \equiv b \pmod{n}$ holds if and only if $n \mid ax - b$, which is equivalent to the problem of finding an integer y such that the equation

$$ax + ny = b$$

holds. By Theorem 7.3.4 we have an exact description of the set of solutions of this equation: Given a solution $ax_0 + ny_0 = b$, every solution is of the form

$$x = x_0 + k\frac{n}{d}, \qquad \text{and} \qquad y = y_0 - k\frac{a}{d},$$

where $d = \gcd(a, n)$. Furthermore, a solution can be found if and only if $d \mid b$, and in this case we can find x_0 and y_0 through Euclid's algorithm for finding the greatest common divisor.

Now, observe that there are exactly d incongruent solutions of the equation $ax + ny = b$ modulo n. Thus, we can reformulate Theorem 7.3.4 in modular arithmetic as follows.

THEOREM 9.1.2. *Consider two integers a and b, and a natural number n with $d = \gcd(a, n)$. The linear congruence*

$$ax \equiv b \pmod{n}$$

is solvable if and only if $d \mid b$, and in this case the number of incongruent solutions is exactly d. Furthermore, if we have one solution $ax_0 \equiv b \pmod{n}$, then all the solutions are of the form

$$x \equiv x_0 + k\frac{n}{d}$$

for $0 \leq k < d$.

EXAMPLE 9.1.3. Consider the linear congruence

$$6x \equiv 15 \pmod{21}.$$

The greatest common divisor of 6 and 21 is $\gcd(6, 21) = 3$. Since 15 is divisible by 3, we expect to find exactly 3 incongruent solutions modulo 21.

To find one solution, we first express 3 as a linear combination of 6 and 21. Normally, we would use Euclid's algorithm to do this, but the numbers here are small enough to immediately see that

$$3 = 4 \cdot 6 - 21.$$

From this expression we find that

$$15 = 20 \cdot 6 - 5 \cdot 21.$$

This gives us the solution $6 \cdot 20 \equiv 15 \pmod{21}$. The remaining solutions are now of the form

$$x \equiv 20 + k \cdot 7$$

for $0 \leq k < 3$. In other words, the full set of incongruent solutions of the equation $6x \equiv 15 \pmod{21}$ is

$$\{6, 13, 20\}.$$

Corollary 9.1.4. *The linear congruence* $ax \equiv 1 \pmod{n}$ *has at most one solution, and it is solvable if and only if* $\gcd(a, n) = 1$.

The previous corollary connects integers relatively prime to n to the integers that are *invertible* modulo n. Indeed, if $ax \equiv 1 \pmod{n}$ has a solution, then its solution x also guarantees that the equality

$$[a][x] = [1]$$

holds in $\mathbb{Z}/n\mathbb{Z}$. In other words, the integer a represents an invertible congruence class modulo n.

Example 9.1.5. The invertible congruence classes modulo 5 are the congruence classes of 1, 2, 3, and 4. Indeed, one can verify that

$$1 \cdot 1 \equiv 1 \pmod{5} \qquad 2 \cdot 3 \equiv 1 \pmod{5}$$
$$3 \cdot 2 \equiv 1 \pmod{5} \qquad 4 \cdot 4 \equiv 1 \pmod{5}.$$

Corollary 9.1.6. *Consider an integer* a *relatively prime to* n. *Then the operation* $x \mapsto [a]x$ *is a bijection on* $\mathbb{Z}/n\mathbb{Z}$.

9.2 Solving Multiple Linear Congruences Simultaneously

Consider the linear congruences

$$10x \equiv 4 \pmod{12}$$
$$15x \equiv 6 \pmod{21},$$

and suppose our goal is to find a single solution x that simultaneously solves both of them. To start off, we observe that if we can find such a solution, then each individual congruence must be solvable in its own right. By Theorem 9.1.2, this is the case if and only if $\gcd(10, 12) \mid 4$ and $\gcd(15, 21) \mid 6$. Indeed, $\gcd(10, 12) = 2$ and $\gcd(15, 21) = 3$, so the divisibility requirements are satisfied.

By dividing through with $\gcd(10, 12)$, we see that the linear congruence $10x \equiv 4 \pmod{12}$ has the same set of solutions as the linear congruence $5x \equiv 2 \pmod{6}$, which we can work out to be $x \equiv 4 \pmod{6}$. Similarly the linear congruence $15x \equiv 6 \pmod{21}$ has the same set of solutions as the linear congruence $5x \equiv 2 \pmod{7}$, which we can work out to be $x \equiv 6 \pmod{7}$. Thus, the original system of linear congruences has the same set of solutions as the system of linear congruences

$$x \equiv 4 \pmod{6}$$
$$x \equiv 6 \pmod{7}.$$



In other words, x is simultaneously of the form $6y + 4$ and of the form $7z + 6$. We can find such y and z by solving the linear Diophantine equation

$$6y + 4 = 7z + 6,$$

which reduces to $6y - 7z = 2$. By Theorem 7.3.1, it follows that this equation solves if and only if $\gcd(6, 7) \mid 2$, which is indeed the case since 6 and 7 are relatively prime. Using the extended Euclid's algorithm, we find that $y = 5$ and $z = 4$ gives a solution. In this case, we have $x = 34$. Note that any integer in the congruence class of 34 modulo 42 is also a solution, so we see that

$$x \equiv 34 \pmod{42}$$

is a solution to our original system of linear congruences. Indeed, we can check that $10 \cdot 34 = 28 \cdot 12 + 4$ and $15 \cdot 34 = 24 \cdot 21 + 6$.

To summarize the method by which we found this solution, we first reduced each individual linear congruence by dividing through by the greatest common divisor of the scalar and the modulus. This way we obtained a system of linear congruences that were individually uniquely solvable. Their solutions gave two expressions for the variable x, which combined into a single linear Diophantine equation, which we solved by Theorem 7.3.1 and Euclid's algorithm. As the saying goes, any good method in mathematics begs to become a theorem. The essential theorem to solve systems of linear congruences is Theorem 9.3.1 (Chinese Remainder Theorem), which we will state and prove in the next section.

We also note that the methods we used to solve two linear congruences simultaneously can be used to solve three or more linear congruences simultaneously. Suppose our original problem included a third linear congruence

$$\begin{aligned} 10x &\equiv 4 \pmod{12} \\ 15x &\equiv 6 \pmod{21} \\ 6x &\equiv 3 \pmod{15}. \end{aligned}$$

Then we'd simply solve the first two as before, and continue solving the system of two linear congruences

$$\begin{aligned} x &\equiv 34 \pmod{42} \\ x &\equiv 3 \pmod{5}. \end{aligned}$$

This system of linear congruences has solution $x \equiv 118 \pmod{210}$.

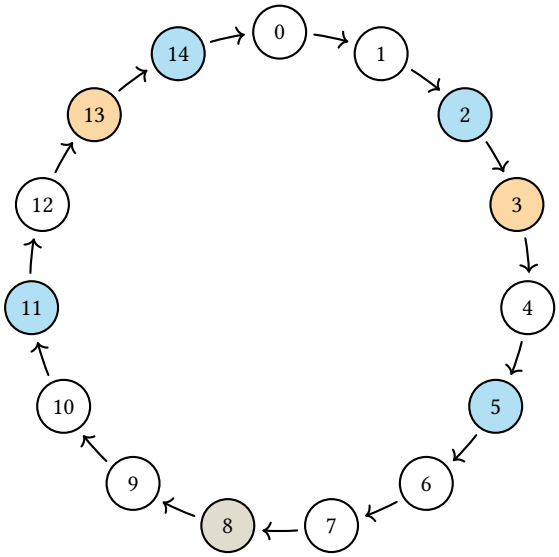


Figure 9.1: The cyclic set with 15 elements admits maps to the cyclic sets with 3 and 5 elements. Every third element of C_{15} starting from 2 is colored blue, while every fifth element starting from 3 is colored orange. Exactly one element is colored both blue and orange. In this case, the number 8 is both orange and blue.

9.3 The Chinese Remainder Theorem

An essential step in the previous example was the reduction of a system of linear congruences, to a system of congruences of the form

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}.$$

In the following theorem we will prove that this system of congruences is uniquely solvable modulo mn, provided that m and n are relatively prime.

Theorem 9.3.1 (Chinese Remainder Theorem). *Consider two linear congruences*

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n},$$

where m and n are relatively prime. Then there is a unique solution x modulo mn that solves both linear congruences simultaneously.

Proof. By the first linear congruence, we find that $x = my + a$ for some integer y. Substituting this into the second linear congruence, we obtain that

$$my \equiv b - a \pmod{n}.$$

This linear congruence has a unique solution modulo n, since $\gcd(m,n) = 1$. Therefore, there is exactly one integer $0 \leq y_0 < n$ such that $x = my_0 + a$. Consequently, there is exactly one $0 \leq x < mn$ that solves both linear congruences simultaneously. □

9.4 A Method Suggested by Gauss

Gauss mentions in his *Disquisitiones Arithmeticae* [GAU1986, Article 36] that he sometimes prefers the following method of solving systems

$$x \equiv a_1 \pmod{m_1}, \ \ldots, \ x \equiv a_n \pmod{m_n}$$

of linear congruences, where $m_1, \ldots, m_n$ are pairwise relatively prime. First, we are to find numbers e_i such that

$$e_i \equiv \begin{cases} 1 \pmod{m_j} & \text{if } j = i, \\ 0 \pmod{m_j} & \text{if } j \neq i. \end{cases} \tag{9.1}$$

Having found such numbers, the solution to the original system of linear congruences is given by

$$\sum_{j=1}^{n} a_j e_j.$$

Indeed, by the given specification of e_i it follows that

$$\sum_{j=1}^{n} a_j e_j \equiv a_i \pmod{m_i}$$

for every $1 \leq i \leq n$.

In order to find e_i as specified, we need to find a multiple of $M_i := \prod_{j \neq i} m_j$ which leaves a remainder of 1 after division by m_i. That is, the number e_i is determined to be the number $M_i u_i$, where u_i is the unique solution to the linear congruence

$$M_i u_i \equiv 1 \pmod{m_i}.$$

In other words, the number u_i is the inverse of M_i modulo m_i.

EXAMPLE 9.4.1. To illustrate Gauss's preferred method, consider the system of linear congruences

$$7x \equiv 2 \pmod{15}, \ 11x \equiv 1 \pmod{14}, \ 5x \equiv 3 \pmod{11}.$$

Before we can apply Gauss's method, we should bring each congruence to the form $x \equiv a_i \pmod{m_i}$. By inverting 7 modulo 15, 11 modulo 14, and 5 modulo 11, we see that the given system of linear congruences is equivalent to the system

$$x \equiv 7 \pmod{15}, \qquad x \equiv 9 \pmod{14}, \qquad \text{and} \qquad x \equiv 5 \pmod{11}.$$

In order to find e_i as specified in Equation (9.1), we need to separately solve the linear congruences

$$154u_1 \equiv 1 \pmod{15}, \qquad 165u_2 \equiv 1 \pmod{14}, \qquad \text{and} \qquad 210x \equiv 1 \pmod{11}.$$

These simplify as follows:

$$4u_1 \equiv 1 \pmod{15}, \qquad 11u_2 \equiv 1 \pmod{14}, \qquad \text{and} \qquad u_3 \equiv 1 \pmod{11}.$$

Using the methods described in §9.1, we find the following solutions:

$$u_1 \equiv 4 \pmod{15}, \qquad u_2 \equiv 9 \pmod{14}, \qquad \text{and} \qquad u_3 \equiv 1 \pmod{11}.$$

This gives us $e_1 := 4 \cdot 154$, $e_2 := 9 \cdot 165$, and $e_3 := 1 \cdot 210$, from which we obtain the final solution that

$$x \equiv 7 \cdot 4 \cdot 154 + 9 \cdot 9 \cdot 165 + 5 \cdot 1 \cdot 210 \equiv 247 \pmod{2310}$$

9.5 Lifting Invertible Congruence Classes

Example 9.5.1. Let us compare the invertible numbers modulo 4 and modulo 12, with the moduli being chosen so that $4 \mid 12$. The invertible numbers modulo 4 are 1 and 3, while the invertible numbers modulo 12 are 1, 5, 7, and 11. Thus, 3 is invertible modulo 4, but not modulo 12. The question is whether we can find an integer congruent to 3 modulo 4 that is also invertible modulo 12. In other words, if we color every fourth integer starting from 3 blue, as indicated in Figure 9.2, will we find one that is relatively prime to 12?

Indeed, there are two such numbers: 7 and 11. In other words, the invertible congruence class of 3 modulo 4 can be *lifted* to an invertible congruence class modulo 12. The following theorem shows that this observation holds whenever one modulus divides another.

Theorem 9.5.2. *Suppose that $m \mid n$, and $\gcd(a, m) = 1$. Then there is an integer b such that*

$$a \equiv b \pmod{m} \qquad \textit{and} \qquad \gcd(b, n) = 1.$$

Proof. Let s be the greatest divisor of n such that $\gcd(s, m) = 1$, so that

$$d \mid s \quad \Leftrightarrow \quad d \mid n \text{ and } \gcd(d, m) = 1,$$

and set $t = n/s$, giving $n = st$. Since $m \mid st$ and m is relatively prime to s, it follows that $m \mid t$. By Theorem 9.3.1 there exists an integer b satisfying

$$b \equiv 1 \pmod{s},$$
$$b \equiv a \pmod{t}.$$



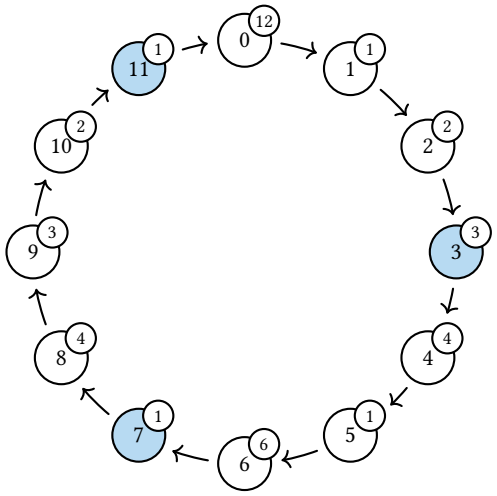


Figure 9.2: The cyclic set with 12 elements, with at each node k a smaller node with the value $\gcd(12, k)$. Every fourth node is shaded blue, starting from the node 3. The number 3 is relatively prime to 4, and among the blue nodes we find some that are relatively prime to 12.

Since $m \mid t$, the second congruence implies that $b \equiv a \pmod{m}$. The first congruence gives us that $\gcd(b, s) = 1$. Therefore it remains to show that $\gcd(b, t) = 1$. Since $b \equiv a \pmod{t}$, we know that $\gcd(b, t) = \gcd(a, t)$. Set $d = \gcd(a, t)$. Then $\gcd(d, m) = 1$ and $d \mid n$, so that $d \mid s$ by the defining property of s. It follows that $d \mid \gcd(s, t) = 1$. □

REMARK 9.5.3. It is common to write $(\mathbb{Z}/n)^\times$ for the set of invertible numbers modulo n. Using this notation, we can rephrase Theorem 9.5.2 as follows: *If $m \mid n$, then the reduction map*

$$(\mathbb{Z}/n)^\times \to (\mathbb{Z}/m)^\times$$

is surjective.

Exercises

Starter Exercises

9.1 Solve Master Sun's mathematical problem, which he stated in *Sunzi Suanjing*, written between the 3rd and 5th century CE: Find all integers x satisfying the linear congruences

$$x \equiv 2 \pmod{3},$$
$$x \equiv 3 \pmod{5},$$
$$x \equiv 2 \pmod{7}.$$

9.2 Three musicians perform a piece of percussion music. The first musician plays on the first of every four beats, the second plays on the third of every five beats, and the third plays on the second of every third beat. The performance concludes when all three musicians play on the same beat for the first time. How many beats does the performance last?

Routine-Building Exercises

9.3 Find all integers x satisfying the linear congruences

$$x \equiv 4 \pmod{9},$$
$$x \equiv 3 \pmod{10},$$
$$x \equiv 2 \pmod{11}.$$

9.4 Find all integers x satisfying the linear congruences

$$x \equiv 3 \pmod{5},$$
$$x \equiv 6 \pmod{11},$$
$$x \equiv 9 \pmod{17}.$$

9.5 Consider the congruence

$$xy + 7x + 4y \equiv 10 \pmod{13}.$$

Compute the congruence class of y modulo 13 for $x \equiv 2, 5, 8 \pmod{13}$.

9.6 Show that Theorem 9.5.2 can be extended to the folling more general statement: If $m \mid n$ and $\gcd(a, m) = g$, then there is an integer b such that

$$a \equiv b \pmod{m} \qquad \text{and} \qquad \gcd(b, n) = g.$$

9.7 For any natural number n, and any two integers a and b, show that the following are equivalent:

(i) $\gcd(a, n) = \gcd(b, n)$,

(ii) There is an invertible integer k modulo n such that

$$ka \equiv b \pmod{n}.$$

Challenge Exercises

9.8 *(The Bass stable-range-one property).* Show that for any two integers a and b, and any positive integer n, there is an integer t such that the following identity holds [BAS1964, Corollary 6.5]:

$$\gcd(a + tb, n) = \gcd(a, b, n).$$

Chapter 10

The Rational Numbers

On the integers we have the arithmetic operations of addition, subtraction, and multiplication, but we generally can't divide integers and expect the result to be another integer. Instead, we have Theorem 5.3.1 (The Euclidean Division Theorem) which establishes division with remainder, and in the previous chapters we introduced the basics of the theory of integer divisibility and modulo arithmetic. Nevertheless, there is a clear sense of ratios of integers, even if such ratios are not necessarily integers. It is thus natural to introduce the concepts of *integer fractions* and the *rational numbers*.

10.1 Integer Fractions

Definition 10.1.1. An **integer fraction** is an expression of the form

$$\frac{a}{b}$$

in which a is an integer and b is a positive integer. In such an integer fraction, the integer a is called the **numerator** and the positive integer b is called the **denominator**. Furthermore:

(i) An integer fraction $\frac{a}{b}$ is said to be **reduced** or **in lowest terms** if a and b are relatively prime.

(ii) An integer a can be presented as an integer fraction by $\frac{a}{1}$.

(iii) An integer fraction of the form $\frac{1}{b}$ is called a **unit fraction**.

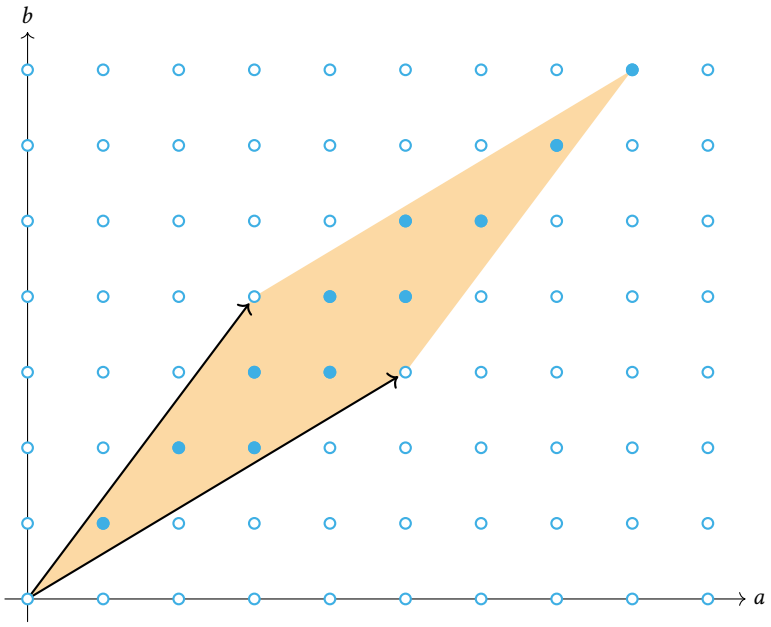


Figure 10.1: There are 11 lattice points in the parallelogram spanned by $(3,4)$ and $(5,3)$, not including the points $(0,0)$, $(3,4)$, and $(5,3)$. This number is equal to the Farey determinant $4 \cdot 5 - 3 \cdot 3$.

While it is common to think of rational numbers as integer fractions, there is a subtle distinction between the concepts of integer fractions and rational numbers. For example, the two integer fractions $\frac{4}{3}$ and $\frac{8}{6}$ have different expressions in terms of their numerators and denominators, but we think of them as representing the *same* rational number. The rational sameness relation on integer fractions is defined as follows.

DEFINITION 10.1.2. Two integer fractions $\frac{a}{b}$ and $\frac{c}{d}$ are considered the **same** if

$$ad - bc = 0.$$

The set $\mathbb{Q}$ of **rational numbers** is defined according to the following rules:

(i) To construct a rational number, one has to construct an integer fraction.

(ii) To prove that two rational numbers $\frac{a}{b}$ and $\frac{c}{d}$ are equal, one has to prove that $ad - bc = 0$.

REMARK 10.1.3. More generally, the quantity $|bc - ad|$ is a measure for how far apart the fractions a/b and c/d are. The quantity $k = |bc - ad|$ is the area of the parallelogram spanned by (a,b) and (c,d), as indicated by Figure 10.1. Moreover, there are exactly k lattice points in this parallelogram, excluding multiples of (a,b) and (c,d).

Theorem 10.1.4. *For any integer fraction $\frac{a}{b}$ there is a unique reduced integer fraction $\frac{c}{d}$ such that $\frac{a}{b} \sim \frac{c}{d}$. Consequently, two integer fractions are the same if and only if they have the same reduced integer fraction.*

Proof. The reduced integer fraction $\frac{a'}{b'}$ associated to an integer fraction $\frac{a}{b}$ is defined by the integers

$$a' := \frac{a}{\gcd(a,b)} \qquad \text{and} \qquad b' := \frac{b}{\gcd(a,b)}.$$

This definition makes sense within the integers, since a and b are both divisible by the greatest common divisor $\gcd(a,b)$. To see that the fractions $\frac{a}{b}$ and $\frac{a'}{b'}$ are the same, we compute

$$ab' - ba' = a\frac{b}{\gcd(a,b)} - b\frac{a}{\gcd a,b} = 0.$$

This shows that for every integer fraction is the same to at least one reduced integer fraction. For the uniqueness claim, we will show that any two reduced integer fractions that are the same, have the same numerator and denominator. Let $\frac{a}{b}$ and $\frac{c}{d}$ be two reduced integer fractions such that

$$ad - bc = 0,$$

so that the equation $ad = bc$ holds. Then we have $d \mid bc$, from which it follows that $d \mid b$ by Proposition 7.1.5. Conversely, we have $b \mid ad$ so that $b \mid d$. Since b and d are positive integers mutually dividing each other, it follows that $b = d$. Consequently, we obtain that $ab = bc$, which gives that $a = c$. □

Definition 10.1.5. Integer fractions can be added, subtracted, and multiplied according to the following rules:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}, \qquad \text{and} \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Furthermore, if the numerator of $\frac{a}{b}$ is nonzero, then we can invert $\frac{a}{b}$ by:

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

Theorem 10.1.6. *Addition, subtraction, multiplication and inversion of integer fractions satisfies the axioms of a field:*

$$\begin{aligned} (x+y)+z &= x+y+z & (xy)z &= x(yz) \\ x+y &= y+x & xy &= yx \\ 0+x &= x & 1x &= x \\ x-x &= 0 & xx^{-1} &= 1 \\ & & x(y+z) &= xy+xz. \end{aligned}$$

Furthermore, adding, subtracting, multiplying or inverting integer fractions preserves the sameness relation on integer fraction, in the sense that if we substitute each integer fraction in a sum, difference, product, or inversion by one that is the same to the original, the result will be the same.

THEOREM 10.1.7. *Every pair of reduced integer fractions $\frac{a}{b}$ and $\frac{c}{d}$ such that $bc - ad = 1$ is uniquely determined by the triple (b, d, q) satisfying $\gcd(b, d) = 1$ and $0 \leq a - qb < b$.*

10.2 The Irrationality of Square Roots

THEOREM 10.2.1. *If a natural number n is not a perfect square, then its square root $\sqrt{n}$ is irrational.*

PROOF. We will prove the theorem by deriving a contradiction under the assumption that there is a reduced integer fraction $\frac{a}{b}$ such that

$$\frac{a^2}{b^2} = n.$$

This equation is equivalent to the equation $a^2 = nb^2$. Furthermore, we may assume without loss of generality that a and b are relatively prime, because we can always divide both sides of the equation $a^2 = nb^2$ by $\gcd(a, b)^2$. By this very equation, it follows that $b^2 \mid a^2$. Thus we have

$$b^2 = \gcd(a^2, b^2) = \gcd(a, b)^2 = 1,$$

and we see that $b = 1$. However, this implies that $n = a^2$ is a perfect square, contradicting our assumtion that n is not a perfect square. □

10.3 Continued Fractions

Consider the numbers $a = 193$ and $b = 71$. Running Euclid's algorithm on these numbers to find their greatest common divisor, we obtain:

$$\begin{aligned}
193 &= 2 \cdot 71 + 51, \\
71 &= 1 \cdot 51 + 20, \\
51 &= 2 \cdot 20 + 11, \\
20 &= 1 \cdot 11 + 9, \\
11 &= 1 \cdot 9 + 2, \\
9 &= 4 \cdot 2 + 1, \\
2 &= 2 \cdot 1 + 0.
\end{aligned}$$

If we divide the top equation through by 71, we obtain the equation

$$\frac{193}{71} = 2 + \frac{51}{71}.$$

Similarly, we have $\frac{71}{51} = 1 + \frac{20}{51}$, and so on. Rewriting $\frac{51}{71}$ to the fraction $1/\frac{71}{51}$ then allows us to obtain:

$$\frac{193}{71} = 2 + \cfrac{1}{1 + \frac{20}{51}}.$$

Continuing this way, we find that

$$\frac{193}{71} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{2}}}}}}.$$

Such iterated fractions are called **continued fractions**. The fraction $\frac{193}{71}$ is a famously accurate approximation of Euler's number e, being correct to within a distance of $1/71^2$, and its continued fraction is the start of the continued fraction expansion of e. As we just saw, continued fractions are closely related to Euclid's algorithm, and indeed they are used for rational approximations of real numbers.

Definition 10.3.1. A **finite (simple) continued fraction** is an expression of the form

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\cdots + \frac{1}{q_n}}}},$$

where q_0 is an arbitrary integer, each q_i with $i > 0$ is a positive integer, and furthermore $q_n > 1$. The adjective *simple* refers to the fact that only the number 1 is ever used as a numerator. We will generally assume that continued fractions are simple, so we will omit this disambiguation. A commonly used compact notation for finite simple continued fractions is $[q_0, q_1, q_2, \ldots, q_n]$.

Infinite continued fractions are infinite expressions of the form

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \frac{1}{\cdots}}}.$$

A more compact notation for infinite continued fractions is $[q_0, q_1, \ldots]$. The numbers q_i in a continued fraction $[q_0, q_1, \ldots]$ are called the **partial quotients**.

Carl Friedrich Gauss had the following elegant notation for continued fractions, which is not widely used anymore:

$$q_0 + \operatorname*{K}_{i=1}^{\infty} \frac{1}{q_i} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots}}}.$$

Here, the letter K stands for *Kettenbruch*, the German word for continued fraction. In the present chapter we will mostly focus our attention on finite continued fractions. Infinite continued fractions are an important way of uniquely representing arbitrary real numbers, and they have applications in Pells equations, or more generally the study of quadratic fields, the theory of Diophantine approximations, and the theorems establishing the transcendence of numbers like π and e.

THEOREM 10.3.2. *Every reduced integer fraction can be uniquely represented as a finite continued fraction.*

PROOF. Consider two relatively prime integers a and b with $b > 0$. The proof is by strong induction on b. In the base case, where $b = 1$, the unique finite continued fraction representing $\frac{a}{b}$ is the continued fraction $[a]$, which has no fractional part.

By Theorem 5.3.1 (The Euclidean Division Theorem) there is a uniqe pair (q, r) of integers with $0 \leq r < b$ such that $a = qb + r$. In the case where $r = 0$, we obtain that $\frac{a}{b} = q$, from which it follows that $[q]$ is the unique finite continued fraction representing $\frac{a}{b}$. In case $r > 0$ we write

$$\frac{a}{b} = q + \frac{1}{\frac{b}{r}}.$$

The integers b and r are relatively prime with $r < b$. By the strong induction hypothesis, it follows that $\frac{b}{r}$ is uniquely represented as a continued fraction $[q_1, q_2, \ldots, q_n]$. It follows that $[q, q_1, \ldots, q_n]$ is a continued fraction representing $\frac{a}{b}$. Furthermore, it is the unique such representation, since the integer part of a continued fraction is uniquely determined as the largest integer below $\frac{a}{b}$. □

DEFINITION 10.3.3. Consider a continued fraction $[q_0, \ldots, q_n]$ or $[q_0, q_1, \ldots]$. The continued fractions

$$\frac{a_i}{b_i} := [q_0, \ldots, q_i]$$

are called the **convergents** of the continued fraction.

The first few convergents of a continued fraction $[q_0, q_1, \ldots]$ are

$$\frac{a_0}{b_0} = \frac{q_0}{1}, \qquad \frac{a_1}{b_1} = \frac{q_0 q_1 + 1}{q_1}, \qquad \frac{a_2}{b_2} = \frac{q_0 q_1 q_2 + q_0 + q_2}{q_1 q_2 + 1}, \qquad \ldots$$

so that $a_0 = q_0$, $b_0 = 1$, $a_1 = q_0 q_1 + 1$, $b_1 = q_1$, and so on. For example, consider the continued fraction $[2, 1, 2, 1, 1, 4, 2]$, which we used at the beginning of this section to motivate the definition of continued fractions. Its convergents are:

$$\frac{a_0}{b_0} = \frac{2}{1}, \quad \frac{a_1}{b_1} = \frac{3}{1}, \quad \frac{a_2}{b_2} = \frac{8}{3}, \quad \frac{a_3}{b_3} = \frac{11}{4}, \quad \frac{a_4}{b_4} = \frac{19}{7}, \ldots$$

This sequence of fractions provides increasingly better rational approximations of Euler's number e. Notice that the numerators and denominators are increasing. In fact, one can check that the fraction $\frac{19}{7}$ is the best approximation of e using a denominator not exceeding 7, and the distance from $\frac{19}{7}$ to e does not exceed $\frac{1}{7^2}$.

We are thus naturally led to the question of determining the value of a finite continued fraction $[q_0, \ldots, q_n, x]$, provided that we know the previous values. Note that the variable x occurs deeply nested in the continued fraction. At first sight, computing the value for $[q_0, \ldots, q_n, x]$ thus seems increasingly complicated as n gets larger. Euler faced the same problem in 1744, and he discovered a nice pattern [Eul1744, art. 7]. He recognized that if we recursively define the sequences a_n and b_n by

$$\begin{aligned} a_0 &:= q_0, & a_1 &:= q_1 q_0 + 1, & a_{n+2} &:= q_{n+2} a_{n+1} + a_n, \\ b_0 &:= 1, & b_1 &:= q_1, & b_{n+2} &:= q_{n+2} b_{n+1} + b_n, \end{aligned}$$

then the fraction $\frac{a_n}{b_n}$ is the nth convergent of the continued fration $[q_0, q_1, \ldots]$. This observation works even if the partial quotients q_i aren't integers, which Euler took advantage of in order to express some functions as continued fractions.

A key ingredient of Euler's inductive proof is the identity

$$[q_0, \ldots, q_n, r] = [q_0, \ldots, q_n + \tfrac{1}{r}].$$

Thus, we will need to distinguish in notation for the numerators and denominators of different continued fractions with the same value. A good way to do this, is to explicity use the list of numbers $q_0, \ldots, q_n$ in our notation for the numerator and denominator of $[q_0, \ldots, q_n]$: They will be denoted by

$$a_{q_0,\ldots,q_n} \qquad \text{and} \qquad b_{q_0,\ldots,q_n}.$$

Or, to establish a more compact notation, if we write $\mathbf{q} = q_0, \ldots, q_n$, then we can write $a_{\mathbf{q}}$ and $b_{\mathbf{q}}$ for the numerator and denominator of the continued fraction $[\mathbf{q}] = [q_0, \ldots, q_n]$.

Theorem 10.3.4 (Recurrence Theorem for Convergents). *Define the numbers $a_{\mathbf{q}}$ and $b_{\mathbf{q}}$ for every finite continued fraction $[\mathbf{q}] := [q_0, \ldots, q_n]$ by list recursion as follows:*

$$\begin{aligned} a_q &:= q & a_{q,r} &:= rq + 1, & a_{\mathbf{q},r,s} &:= s a_{\mathbf{q},r} + a_{\mathbf{q}}, \\ b_q &:= 1 & b_{q,r} &:= r, & b_{\mathbf{q},r,s} &:= s b_{\mathbf{q},r} + b_{\mathbf{q}}. \end{aligned}$$



Then we have $\frac{a_{\mathbf{q}}}{b_{\mathbf{q}}} = [\mathbf{q}]$.

PROOF. Since the numbers $a_{\mathbf{q}}$ and $b_{\mathbf{q}}$ are defined by list recursion, we will prove the claim with list induction. Note that $a_q = q$ and $b_q = 1$, so that

$$\frac{a_q}{b_q} = [q].$$

Similarly, we have $a_{q,r} = rq + 1$ and $b_{q,r} = r$, so that

$$\frac{a_{q,r}}{b_{q,r}} = \frac{rq+1}{r} = q + \frac{1}{r} = [q, r].$$

We will do one more base case. Note that $a_{q,r,s} = srq + q + s$ and $b_{q,r,s} = sr + 1$. Then we have that

$$\frac{a_{q,r,s}}{b_{q,r,s}} = \frac{srq+q+s}{sr+1} = q + \frac{s}{sr+1} = q + \frac{1}{r+\frac{1}{s}} = [q, r, s].$$

For the inductive step, consider an arbitrary list $[\mathbf{q}] = [q_0, \ldots, q_n]$ and three more numbers r, s, and t. Using the recursive definition of a and b as well as the inductive hypothesis in the final equality, we note that

$$\frac{a_{\mathbf{q},r,s,t}}{b_{\mathbf{q},r,s,t}} = \frac{ta_{\mathbf{q},r,s} + a_{\mathbf{q},r}}{tb_{\mathbf{q},r,s} + b_{\mathbf{q},r}} = \frac{a_{\mathbf{q},r,s} + \frac{a_{\mathbf{q},r}}{t}}{b_{\mathbf{q},r,s} + \frac{b_{\mathbf{q},r}}{t}} = \frac{(s+\frac{1}{t})a_{\mathbf{q},r} + a_{\mathbf{q}}}{(s+\frac{1}{t})b_{\mathbf{q},r} + b_{\mathbf{q}}} = \frac{a_{\mathbf{q},r,s+\frac{1}{t}}}{b_{\mathbf{q},r,s+\frac{1}{t}}} = [\mathbf{q}, r, s+\tfrac{1}{t}].$$

This completes the proof, since $[\mathbf{q}, r, s + \frac{1}{t}] = [\mathbf{q}, r, s, t]$. □

THEOREM 10.3.5 (Determinant Identity for Convergents). *For any continued fraction* $[\mathbf{q}, r] = [q_0, \ldots, q_n, r]$ *of length* $n + 2$*, we have*

$$a_{\mathbf{q},r}b_{\mathbf{q}} - b_{\mathbf{q},r}a_{\mathbf{q}} = (-1)^n.$$

PROOF. In the base case we have

$$a_{q,r}b_q - b_{q,r}a_q = (rq+1) - rq = 1.$$

For the inductive step, assume that $a_{\mathbf{q},r}b_{\mathbf{q}} - b_{\mathbf{q},r}a_{\mathbf{q}} = (-1)^n$. Then we compute:

$$\begin{aligned} a_{\mathbf{q},r,s}b_{\mathbf{q},r} - b_{\mathbf{q},r,s}a_{\mathbf{q},r} &= (sa_{\mathbf{q},r} + a_{\mathbf{q}})b_{\mathbf{q},r} - (sb_{\mathbf{q},r} + b_{\mathbf{q}})a_{\mathbf{q},r} \\ &= a_{\mathbf{q}}b_{\mathbf{q},r} - b_{\mathbf{q}}a_{\mathbf{q},r} \\ &= -(-1)^n. \end{aligned}$$

□

Theorem 10.3.6. *Consider a continued fraction* $[\mathbf{q}] = [q_0, \dots, q_n]$ *with integer partial quotients* q_i*. Then the convergent*

$$\frac{a_{\mathbf{q}}}{b_{\mathbf{q}}} = [\mathbf{q}]$$

is an integer fraction in lowest terms.

Proof. If each q_i is an integer, then $a_{\mathbf{q}}$ and $b_{\mathbf{q}}$ are determined by recursively adding and multiplying integers, so they are integers. Furthermore, the determinant identity

$$a_{\mathbf{q},r} b_{\mathbf{q}} - b_{\mathbf{q},r} a_{\mathbf{q}} = (-1)^n.$$

shows that $\gcd(a_{\mathbf{q}}, b_{\mathbf{q}}) \mid (-1)^n$, so $a_{\mathbf{q}}$ and $b_{\mathbf{q}}$ are relatively prime. □

We summarize the above results for infinite continued fractions.

Corollary 10.3.7. *Consider an infinite continued fraction* $[q_0, q_1, \dots]$ *and define the sequences* a_n *and* b_n *recursively by*

$$\begin{aligned} a_0 &:= q_0, & a_1 &:= q_1 q_0 + 1, & a_{n+2} &:= q_{n+2} a_{n+1} + a_n, \\ b_0 &:= 1, & b_1 &:= q_1, & b_{n+2} &:= q_{n+2} b_{n+1} + b_n. \end{aligned}$$

Then the fraction $\frac{a_n}{b_n}$ *is the* n^{th} *convergent of* $[q_0, q_1, \dots]$*, it is in lowest terms for every* n*, and we have* $a_{n+1} b_n - b_{n+1} a_n = (-1)^n$*.*

Furthermore, the numerators a_n *and denominators* b_n *of the convergents of an infinite continued fraction form strictly increasing sequences of integers for* $n > 0$*, and*

$$\frac{a_{n+1}}{b_{n+1}} - \frac{a_n}{b_n} = \frac{(-1)^n}{b_n b_{n+1}}.$$

Example 10.3.8. Consider, for example, the continued fraction $\varphi := [1, 1, \dots]$ in which each partial quotient is 1. Then the numerators and denominators of the convergents are determined recursively by

$$\begin{aligned} a_0 &:= 1, & a_1 &:= 2, & a_{n+2} &:= a_{n+1} + a_n, \\ b_0 &:= 1, & b_1 &:= 1, & b_{n+2} &:= b_{n+1} + b_n. \end{aligned}$$

In other words, $a_n = F_{n+2}$ is the $(n+2)^{\text{nd}}$ Fibonacci number and $b_n = F_{n+1}$ is the $(n+1)^{\text{st}}$ Fibonacci number. The recurrence theorem furthermore implies that the Fibonacci numbers satisfy the identity

$$F_{n+2} F_n - F_{n+1} F_{n+1} = (-1)^{n+1}.$$

This identity is known as *Cassini's identity*.

Furthermore, we can compute the exact value of the continued fraction $\varphi := [1, 1, \dots]$. Notice that

$$\varphi = [1, 1, \dots] = 1 + \frac{1}{[1, 1, \dots]} = 1 + \frac{1}{\varphi}.$$

By rewriting this equation, we see that $\varphi^2 = \varphi + 1$. The quadratic forumal now gives us that

$$\varphi = \frac{1+\sqrt{5}}{2}.$$

This number is known as the **golden ratio**. The continued fraction $[1, 1, \ldots]$ shows that the convergents

$$\frac{F_{n+1}}{F_n}$$

determine increasingly accurate approximations of the golden ratio.

10.4 Farey's Series of Fractions

The geologist John Farey Sr. observed in a letter to the British periodical *The Philosophical Magazine and Journal* [FAR1816] that for any three consecutive fractions $\frac{a}{b}$, $\frac{s}{t}$, and $\frac{c}{d}$ in the series $\mathscr{F}_n$, we must have

$$\frac{s}{t} = \frac{a+c}{b+d}.$$

DEFINITION 10.4.1. The **mediant** of two reduced integer fractions $\frac{a}{b}$ and $\frac{c}{d}$ is the integer fraction

$$\frac{a}{b} \triangledown \frac{c}{d} := \frac{a+c}{b+d}.$$

We stress that this definition of the mediant makes essential use of the assumption that the input integer fractions are in reduced form. If not, the value of the mediant could be skewed by common factors.

We can think of the mediant of two reduced integer fractions as the *weighted average*, where the weights are assigned according to the ratio of their denominators:

$$\frac{a}{b} \triangledown \frac{c}{d} = \frac{b}{b+d}\frac{a}{b} + \frac{d}{b+d}\frac{c}{d}.$$

PROPOSITION 10.4.2. *The mediant satisfies the following laws:*

$$x \triangledown y = y \triangledown x,$$
$$x \triangledown x = x,$$
$$\lambda x \triangledown \lambda y = \lambda(x \triangledown y).$$

Furthermore, we have

$$x \leq x \triangledown y \leq y \qquad \text{and} \qquad x < x \triangledown y < y$$

if $x \leq y$ or $x < y$, respectively. However, the mediant is nonunital and nonassociative, meaning that there does not exist an element e such that $x \triangledown e = x$ and there are integer fractions x, y, and z such that $(x \triangledown y) \triangledown z = x \triangledown (y \triangledown z)$.

Proof. To prove the interchange law, consider the integer fractions $\frac{a}{b}$, $\frac{c}{d}$, $\frac{e}{f}$, and $\frac{g}{h}$. Then we calculate

$$\left(\frac{a}{b} \triangledown \frac{c}{d}\right) \triangledown \left(\frac{e}{f} \triangledown \frac{g}{h}\right) = \frac{a+c}{b+d} \triangledown \frac{e+g}{f+h}$$ □

Theorem 10.4.3. *Consider two reduced fractions $\frac{a}{b} < \frac{c}{d}$ such that*

$$bc - ad = 1.$$

Then there is a unique Farey fraction of order $b+d$ strictly between $\frac{a}{b}$ and $\frac{c}{d}$: the mediant

$$\frac{a+b}{c+d}.$$

Proof. Suppose that $\frac{a}{b} < \frac{p}{q} < \frac{c}{d}$, with $q > 0$, so that the numbers $bp - aq$ and $cq - pd$ are positive integers. Then it follows that

$$q = (bc - ad)q = b(cq - pd) + d(bp - aq) \geq b + d.$$

Here we have an equality if and only if $cq - pd = 1$ and $bp - aq = 1$. In this case, it follows that the numerator p is also uniquely determined, for we have

$$p = (bc - ad)p = a(cq - dp) + c(bp - aq) = a + c.$$ □

The previous theorem shows that if $\frac{a}{b}$ and $\frac{c}{d}$ are adjacent Farey fractions, then there is a unique rational number strictly between them whose denominator is $\leq b+d$, namely their mediant. The observation that there is a unique rational number with minimal denominator in the interval of rational numbers strictly between $\frac{a}{b}$ and $\frac{c}{d}$ generalizes to arbitrary intervals $I \subseteq (0,1)$ that contain at least one rational number.

Definition 10.4.4. An **interval** of rational numbers is a subset $I \subseteq \mathbb{Q}$ such that if $q, r \in I$, then $x \in I$ for all $q \leq x \leq r$. For any two rational numbers q and r, the **closed interval** $[q,r]$ is defined as

$$[q,r] := \{x \in \mathbb{Q} \mid q \leq x \leq r\};$$

the **open interval** (q,r) is defined as

$$(q,r) := \{x \in \mathbb{Q} \mid q < x < r\};$$

and the **half-open intervals** $[q,r)$ and $(q,r]$ are defined as

$$[q,r) := \{x \in \mathbb{Q} \mid q \leq x < r\},$$
$$(q,r] := \{x \in \mathbb{Q} \mid q < x \leq r\}.$$

Theorem 10.4.5. *Any interval $I \subseteq (0,1) \subseteq \mathbb{Q}$ containing at least one rational number, contains a unique rational number with minimal denominator.*



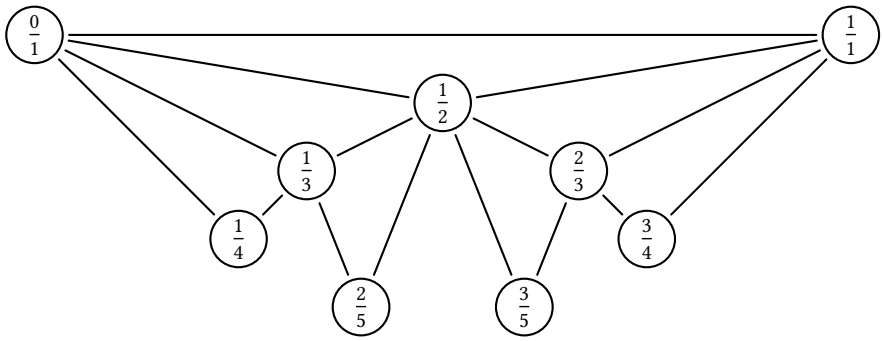


Figure 10.2: The Farey fractions with their adjacency relation.

PROOF. Suppose I is an interval of rational numbers containing reduced fractions $\frac{a}{q}$ and $\frac{b}{q}$, where $0 < a < b < q$. We claim that

$$\frac{a}{q} < \frac{a}{q-1} < \frac{b}{q},$$

so that $\frac{a}{q-1} \in I$. This claim indeed proves the theorem, since it shows that any denominator which occurs more than once in I cannot be minimal.

It is clear that $\frac{a}{q} < \frac{a}{q-1}$, since $q - 1 < q$. To see that $\frac{a}{q-1} < \frac{b}{q}$, it suffices to show that $aq < b(q-1)$, or equivalently,

$$aq + b < bq.$$

Since $a < b < q$, it follows that $aq + b < aq + q = (a+1)q \leq bq$. □

10.5 A Structural Definition of the Rational Numbers

DEFINITION 10.5.1. Consider a set Q equipped with a binary relation $q, r \mapsto (q \sim r)$. A **Farey structure** on the pair $(Q, \sim)$ consist of:

(i) a map $i : \mathbb{Z} \to Q$,

(ii) a partial binary operation

$$m : \{(x, y) \in Q \mid x \sim y\} \to Q$$

called the **mediant**,

such that

(i) for any integer a, the relation $i(a) \sim i(a+1)$ holds,

(ii) for any two elements $x, y \in Q$ such that $x \sim y$ holds, the relations

$$x \sim m(x,y) \qquad \text{and} \qquad m(x,y) \sim y$$

hold.

Definition 10.5.2. The set Q equipped with the adjacency relation $\sim$ and a Farey structure (i,m) is a set of rational numbers if for every set Q' with an adjacency relation $\sim$ and Farey structure (i',m'), there is a unique map $f : Q \to Q'$ such that $x \sim y$ implies $f(x) \sim f(y)$, such that

$$f(i(a)) = i'(a)$$
$$f(m(x,y)) = m'(f(x), f(y)).$$

The set $\mathbb{Q}$ is specified to be a set of rational numbers in this sense.

Example 10.5.3. We can use the specification of $\mathbb{Q}$ as a universal Farey structure to define a map

$$f : \mathbb{Q} \to X$$

into any set X equipped with a map $i : \mathbb{Z} \to X$ and a binary operation $m : X \times X \to X$. Indeed, in order to do so we define the relation $x \sim y$ on X to always hold. This can be used to define the numerator and the denominator of any rational number:

$$\begin{aligned} \operatorname{num}(i(a)) &:= a, & \operatorname{denom}(i(a)) &:= 1, \\ \operatorname{num}(m(x,y)) &:= \operatorname{num}(x) + \operatorname{num}(y), & \operatorname{denom}(m(x,y)) &:= \operatorname{denom}(x) + \operatorname{denom}(y). \end{aligned}$$

Thus, any rational number q determines an integer fraction $\frac{a}{b}$.

Conversely, we can ask whether any reduced integer fraction $\frac{a}{b}$ uniquely determines a rational number. To see this,

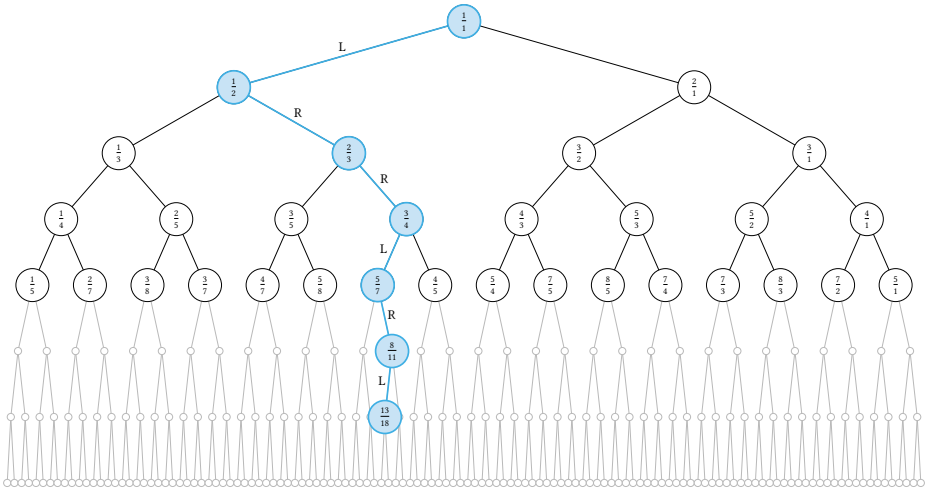


Figure 10.3: The Stern–Brocot tree, with the path *LRRLRL* from $\frac{1}{1}$ to $\frac{13}{18}$ highlighted. The Euclidean algorithm for the pair $(13, 18)$ traces the same left-right pattern, when marking the side of the smaller number at each stage:

$$(13, 18) \mapsto (13, 5) \mapsto (8, 5) \mapsto (3, 5) \mapsto (3, 2) \mapsto (1, 2) \mapsto (1, 1).$$

Exercises

Starter Exercises

10.1 In each of the following intervals, find the unique rational number with minimal denominator:

(a) $\frac{9}{20} < x < \frac{7}{15}$,

(b) $\frac{8}{23} < x < \frac{11}{31}$,

(c) $\frac{333}{106} < x < \frac{22}{7}$.

Routine-Building Exercises

10.2 For every integer a, show that there are infinitely many pairs of rational numbers x and y satisfying the equation

$$x^2 - y^2 = a.$$

10.3 Find all the integers of the form $x + \frac{1}{x}$, where x is a rational number.

10.4 Prove that

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}.$$

10.5 Prove that

$$\prod_{k=2}^{n} \left(1 - \frac{1}{k}\right) = \frac{1}{n}.$$

10.6 Prove that

$$\prod_{k=1}^{n} \left(1 - \frac{1}{k^2}\right) = \frac{n+1}{2n}.$$

10.7 Consider a positive integer $n = 3k + 2$. Show that there are positive integers a, b, and c such that

$$\frac{4}{n} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}.$$

This is a special case of the famous Erdős–Straus conjecture, which asserts that this equation has a solution in the positive integers for all $n > 0$.

10.8 Consider four integers a, b, c, and d. Prove that the following are equivalent:

(i) The integers $cx + a$ and $dx + b$ are relatively prime for every x.

(ii) For any nonnegative divisor t of $\Delta := ad - bc$ such that $\gcd(c, t) \mid a$ and $\gcd(d, t) \mid b$, we have $t = 1$.

Conclude that if $ad - bc = \pm 1$, then the integer fraction

$$\frac{cx + a}{dx + b}$$

is reduced for any integer x.



10.9 Consider the binary operation D on the reduced integer fractions, defined by

$$D\Big(\frac{a}{b}, \frac{c}{d}\Big) := |bc - ad|.$$

Show that D satisfies the axioms of a **metric**:

(i) D is **positive definite**: $D(\frac{a}{b}, \frac{c}{d}) = 0$ if and only if $\frac{a}{b} = \frac{c}{d}$.

(ii) D is **symmetric**: $D(\frac{a}{b}, \frac{c}{d}) = D(\frac{c}{d}, \frac{a}{b})$.

(iii) D satisfies the **triangle inequality**:

$$D\Big(\frac{a}{b}, \frac{e}{f}\Big) \leq D\Big(\frac{a}{b}, \frac{c}{d}\Big) + D\Big(\frac{c}{d}, \frac{e}{f}\Big).$$

10.10 (a) Consider two square-free integers a and c, both dividing an integer b. Show that if $x = \frac{u}{s}$ and $y = \frac{v}{t}$ are rational numbers in lowest terms with $s, t > 0$ such that

$$ax^2 + bxy + cy^2 \in \mathbb{Z},$$

then $s = t$.

(b) Consider a form $f(x, y)$ of degree n given by

$$f(x, y) = \sum_{i=0}^{n} a_i x^{n-i} y^i,$$

where we assume that a_0 and a_n are square-free and $a_0 \mid a_1$ and $a_n \mid a_{n-1}$. Show that if $f(x, y) \in \mathbb{Z}$ for two rational numbers $x = \frac{u}{s}$ and $y = \frac{v}{t}$ in lowest terms with $s, t > 0$, then $s = t$.

10.11 Show that for any two positive rational numbers $r \leq s$, there is a unique rational number $r \leq \frac{a}{b} \leq s$ such that $a + b$ is minimal.

10.12 Consider three reduced fractions

$$\frac{a}{b} < \frac{p}{q} < \frac{c}{d}$$

with positive denominators. Show that any two of the following three conditions imply the third:

(i) $bp - aq = 1$,

(ii) $qc - pd = 1$,

(iii) $\frac{p}{q} = \frac{a+c}{b+d}$.

Chapter 11

Pythagorean Triples

Pythagorean triples have been studied since antiquity. While this topic is very accessible, many aspects of the theory Pythagorean triples are natural entry points for more advanced concepts in number theory. First of all, the very definition of Pythagorean triples connects a geometric idea with a number-theoretic concept. Euclid's parametrization of the Pythagorean triples provides a complete description of the exact nature of Pythagorean triples. We will prove that there is an equivalence between Pythagorean triples and rational points on the circle, thus connecting the integer solutions to the diophantine equation

$$a^2 + b^2 = c^2$$

with the rational points on an algebraic curve, a topic which is important in more advanced branches of number theory. We will also show that Pythagorean triples can be equivalently described as arithmetic triples of squares. This is an elementary example of the concept of *equivalence of quadratic forms*. Moreover, the correspondence between Pythagorean triples and arithmetic triples of squares leads us to an important open problem, which we will describe in more detail in §12.6: the congruent number problem.

11.1 The Pythagorean Theorem

Recall that a right triangle is a triangle in which one of the angles is a right angle; that is, it is exactly 90°. Theorem 11.1.1 (Pythagorean Theorem) relates the lengths of the sides of a right triangle to the length of its hypotenuse. There are many ways to prove this theorem. We will present the *Chinese proof*, *Euclid's proof*, and the proof

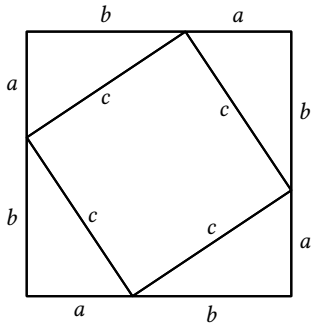


of Ne'Kiya Jackson and Calcea Johnson, who made headlines in 2023 as high school students with their remarkable discovery of a trigonometric proof [THE2023].

THEOREM 11.1.1 (Pythagorean Theorem). *Consider a right triangle with side lengths a and b, and a hypotenuse of length c. Then*

$$a^2 + b^2 = c^2.$$

THE CHINESE PROOF. Consider a square with side lengths $a+b$, and include four right triangles with side lengths a and b in the square, so that their right angles coincide with the four right angles of the square.

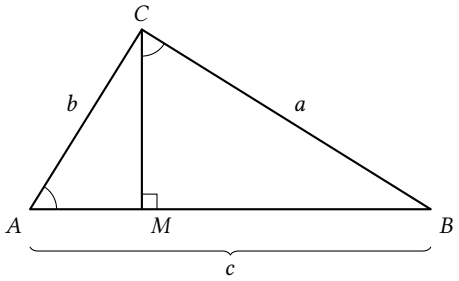


The area of the square is $(a+b)^2$. On the other hand, the area of each triangle is $ab/2$. Combined with the area of the inner square, whose sides are the hypotenuses of the four triangles, we obtain that

$$(a+b)^2 = c^2 + 4\frac{ab}{2} = c^2 + 2ab.$$

Since $(a+b)^2 = a^2 + 2ab + b^2$, we find that $a^2 + b^2 = c^2$. □

EUCLID'S PROOF. Consider a right triangle ACB with hypotenuse AB, and draw a line from C through AB at a right angle. The intersection point is called M.

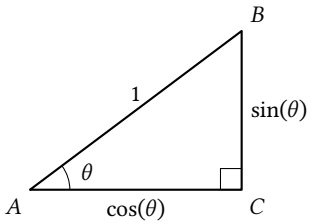


Let x be the length of the line segment AM, and let y be the length of the line segment BM, so that $x+y=c$. The line CM divides the triangle ACB into two triangles CMA and CMB, both of which are similar to the original triangle ACB. Thus, the ratio $a : c$ is the same as the ratio $y : a$, and the ratio $b : c$ is the same as the ratio $x : b$. This gives us the equalities

$$a^2 = cy \qquad \text{and} \qquad b^2 = cx.$$

Since $x + y = c$, we find that $a^2 + b^2 = c^2$. □

Our third proof and final proof in this section, which is due to Ne'Kiya Jackson and Calcea Johnson, is remarkable because it makes essential use of trigonometric functions sine and cosine and the addition law, which can be derived trigonometrically, rather than on calculations involving areas of shapes. Besides its use of trigonometry, it is also remarkable because Ne'Kiya Jackson and Calcea Johnson were still in high school when they found their proof, and it stands out for its inventive creativity.



Recall that the sine and cosine functions are defined to be the lengths of the vertical and horizontal sides of a right triangle, as indicated in the diagram on the side. This means that if ACB is a right triangle with side BC of length a, side AC of length b, hypotenuse AB of length c, and angle $\theta := \angle CAB$, then we have

$$\sin(\theta) = \frac{a}{c} \qquad \text{and} \qquad \cos(\theta) = \frac{b}{c}.$$

In the proof of Theorem 11.1.1 (Pythagorean Theorem), we will make use of the addition formulas for sine and cosine:

$$\sin(\theta + \phi) = \sin(\theta)\cos(\phi) + \cos(\theta)\sin(\phi)$$
$$\cos(\theta + \phi) = \sin(\theta)\sin(\phi) - \cos(\theta)\cos(\phi).$$

In particular, $\sin(2\theta) = 2\sin(\theta)\cos(\theta)$, and $\cos(2\theta) = \sin^2(\theta) - \cos^2(\theta)$. These laws can be derived geometrically if $\theta + \phi$ is an acute angle; that is, if it is strictly less than 90°.

The Jackson–Johnson proof [JJ2024]. Consider a right triangle ACB with the right angle at C, and label the sides $a = BC$, $b = AC$, and $c = AB$ so c is the hypotenuse.

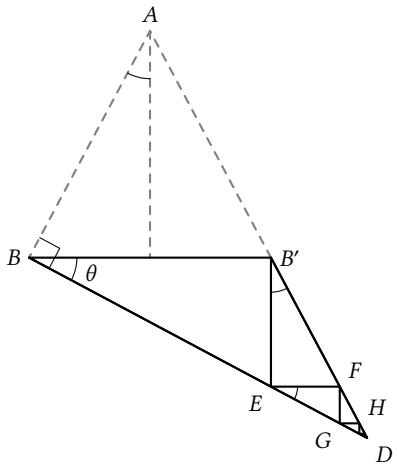
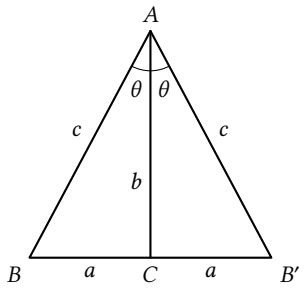


Figure 11.1: The recursive subdivision of the triangle BDB'.

In the special case where ACB is isosceles, meaning that $a = b$, the hypotenuse is the diagonal of an a-by-a square, which gives us that $c^2 = 2a^2$. Hence, we may assume that ACB is nonisosceles.

Without loss of generality, we will assume that $a < b$, so that BC is the shorter side. We reflect the triangle along the longer side AC, as indicated in the diagram below:



Observe that the angle $\theta := \angle BAC$ is strictly less than 45°, so that the angle $2\theta = \angle BAB'$ is still an acute angle.

Using this combined triangle, we draw a line from B perpendicular to the line AB, and we extend the line AB' until they meet in an intersection point, which we call D. This construction yields a new right triangle ABD with the right angle at B, as in Figure 11.1.

We will now subdivide the triangle BDB' by first dropping a line down from B' at a right angle from the line BB', creating a new right triangle BEB'. Since this triangle also has an angle θ, it is similar to the original triangle ACB. Its sides have lengths $2a$

and $2a^2/b$.

We continue subdividing the triangle BDB' into ever smaller right triangles, as indicated in the figure. The successive triangles in this sequence are all right triangles with an angle θ, so they are all similar. Corresponding sides in these successive triangles have a ratio of a/b. The hypotenuses of these triangles therefore have length

$$2c\left(\frac{a}{b}\right)^n$$

This allows us to calculate the length of the side $B'D$ via the formula for the geometric series, which we proved in Theorem 2.5.3:

$$|B'D| = \sum_{k=0}^{\infty} 2c\left(\frac{a}{b}\right)^{2k+2} = 2c\left(\frac{a}{b}\right)^2 \sum_{k=0}^{\infty}\left(\frac{a}{b}\right)^{2k} = \frac{2c\left(\frac{a}{b}\right)^2}{1-\left(\frac{a}{b}\right)^2} = \frac{2ca^2}{b^2-a^2}.$$

Now we can find two expressions for the length of the line AD. First, it consists of the lines AB' and $B'D$, so it is of length $c+|B'D|$, which we calculated above. On the other hand, by trigonometry we have that $c/|AD| = \cos(2\theta)$, which gives us that $|AD| = c/\cos(2\theta)$. Since both expressions give the length of the line AD, both involving a factor of c which we can factor out, we obtain the following equation:

$$1 + \frac{2a^2}{b^2-a^2} = \frac{1}{\cos(2\theta)}.$$

Furthermore, the addition formula for cosines gives us that $\cos(2\theta) = \sin^2(\theta) - \cos^2(\theta)$. Since $\sin(\theta) = \frac{b}{c}$ and $\cos(\theta) = \frac{a}{c}$, we find that

$$1 + \frac{2a^2}{b^2-a^2} = \frac{c^2}{b^2-a^2}.$$

Rearranging this equation gives us that $(b^2-a^2)+2a^2 = c^2$, which yields

$$a^2 + b^2 = c^2.$$

□

11.2 Euclid's Parametrization of the Pythagorean Triples

Our goal in this section is to describe all the solutions of the quadratic Diophantine equation

$$a^2 + b^2 = c^2,$$

where c is a nonzero integer. By Theorem 11.1.1 (Pythagorean Theorem), any such triple (a,b,c) describes the lengths of the sides and hypotenuse of a right triangle. Such a triple is therefore called a **Pythagorean triple**. Notice that if (a,b,c) is a Pythagorean triple, then so is (ka,kb,kc), and their corresponding triangles are of the



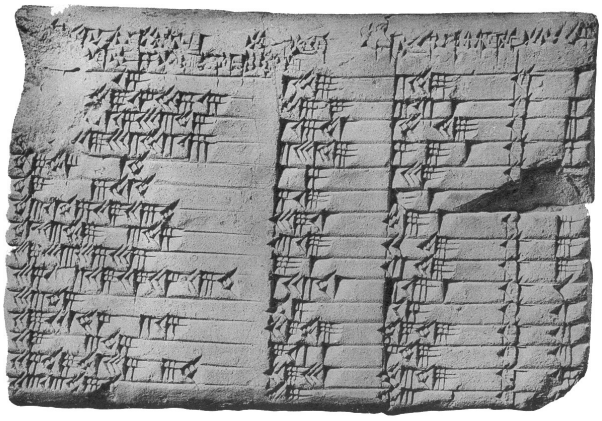
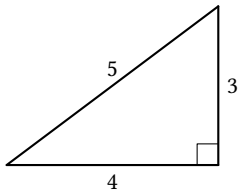


Figure 11.2: The Babylonian tablet Plimpton 322, listing Pythagorean triples.

same shape. Such Pythagorean triples are therefore called **similar**, and we are interested in the Pythagorean triples up to similarity.



The trivial solutions are $(0, 1, 1)$ and $(1, 0, 1)$. The simplest nontrivial solution is the famous equation

$$3^2 + 4^2 = 5^2.$$

The triangle with side lengths 3 and 4 and a hypotenuse of length 5 is sometimes called the **Egyptian triangle**, since it is believed that the ancient Egyptians used this triangle for practical applications. Some further Pythagorean triples include

$$(5, 12, 13), \qquad (21, 20, 29), \qquad \text{and} \qquad (15, 8, 17).$$

The oldest surviving table of Pythagorean triples was created by the Babylonians, in what is now known as the tablet *Plimpton 322*. This clay tablet, which is estimated to date from 1800 BCE, contains a mathematical table written in cuneiform script, where each row describes a Pythagorean triple in sexagesimal notation; that is, in base 60.

Fibonacci devised in his book *Liber Quadratorum (The Book of Squares)* [FS1987] a clever way to quickly show that there are infinitely many Pythagorean triples. If an

odd square a^2 is the nth odd number, so that $a^2 = 2n+1$, then by Exercise 2.1 there are positive integers b and c such that

$$b^2 = \sum_{i=0}^{n-1}(2i+1), \qquad \text{and} \qquad c^2 = \sum_{i=0}^{n}(2i+1)$$

For this choice of a, b, and c, we have

$$a^2 + b^2 = c^2.$$

Proposition 11.2.1. *There are infinitely many Pythagorean triples (a,b,c) such that $c = b+1$.*

Note that while Fibonacci used the sum of odd numbers to find a triple (a,b,c) of integers such that $a^2+b^2=c^2$, these Fibonacci triples follow the pattern

$$(2b+1) + b^2 = (b+1)^2.$$

Here we immediately see that if $2b+1$ is a square number a^2, and indeed any odd square is of this form, then we obtain a Pythagorean triple of the form $(a,b,b+1)$. Rewriting $a = 2k+1$, we see that Fibonacci's Pythagorean triples are of the form

$$(2k+1,\ 2k^2+2k,\ 2k^2+2k+1).$$

The Pythagorean triples (a,b,c) generated by Fibonacci's method always satisfy $c = b+1$. However, we have already seen that $(21,20,29)$ is a Pythagorean triple that is not of this form. Therefore we see that, even though Fibonacci's method can be used to see that there are infinitely many Pythagorean triples, it does not generate all of them.

In the remainder of this section we will derive the classic formula that describes all the Pythagorean triples. The method leading to this formula was described by Euclid in Book X, Proposition 29 and Book 6, Proposition 21 of the Elements.

Definition 11.2.2. A **primitive Pythagorean triple** is a triple (a,b,c) satisfying

$$a^2 + b^2 = c^2$$

such that $\gcd(a,b) = 1$.

Example 11.2.3. All the Pythagorean triples generated by Fibonacci's method are primitive, since $\gcd(2b+1, b) = 1$.

Lemma 11.2.4. *For any Pythagorean triple (a,b,c) there is a unique primitive Pythagorean triple (a',b',c') consisting of positive integers for which there is an integer k such that $(ka', kb', kc') = (a,b,c)$.*



PROOF. Given a Pythagorean triple (a, b, c), let $k := \gcd(a, b)$. Since $k \mid a$ and $k \mid b$, it follows from the equation $a^2 + b^2 = c^2$ that $k \mid c$. Thus, we define

$$a' := a/k, \qquad b' := b/k, \qquad \text{and} \qquad c' := c/k.$$

Then a' and b' are relatively prime, and we have

$$a'^2 + b'^2 = \frac{a^2 + b^2}{k^2} = \frac{c^2}{k^2} = c'^2.$$

The triple (a', b', c') is therefore a primitive Pythagorean triple such that

$$(ka', kb', kc') = (a, b, c).$$

For uniqueness, suppose that (a'', b'', c'') is an other such primitive Pythagorean triple, satisfying $(la'', lb'', lc'') = (a, b, c)$. Since $\gcd(a'', b'') = 1$, it follows that

$$k = \gcd(a, b) = \gcd(la'', lb'') = l$$

Furthermore, since at least one of a or b is nonzero, it follows both k and l are nonzero. Thus we get $a' = a''$ from the equation $ka' = ka''$, and we get $b' = b''$ from the equation $kb' = kb''$. We conclude that $(a', b', c') = (a'', b'', c'')$. □

By the previous lemma we can restrict our attention to primitive Pythagorean triples. Next, we do a parity analysis of the components of a primitive Pythagorean triple to show that exactly one of the components of (a, b, c) in a Pythagorean triple is divisible by 4. In Exercise 11.3 we make the similar claims that exactly one of the components of a Pythagorean triple is divisible by 3, and exactly one divisible by 5.

LEMMA 11.2.5. *Consider a primitive Pythagorean triple (a, b, c). Then c is odd, exactly one of a and b is divisible by 4, and the other is odd.*

PROOF. Since (a, b, c) is a primitive Pythagorean triple, it is clearly impossible for both a and b to be even. It is also impossible for both of them to be odd, since in that case c^2 would be of the form $4k + 2$, which is impossible since every square is of the form $4k$ or $4k + 1$. Thus, one of a and b is even and the other is odd. This gives us that c^2 is odd, which is onlb possible if c is odd.

It remains to show that the even component among a and b is in fact divisible by 4. To this end, recall that every square is of the form $8k$, $8k+1$, or $8k+4$. Since $a^2+b^2 = c^2$ is of the form $8k + 1$, it is impossible for one of the squares a^2 or b^2 to be of the form $8k + 4$. It follows that the even square is of the form $8k$. If a^2 is divisible by 8, then clearly a is divisible by 4, and likewise if b^2 is divisible by 8 then b is divisible by 4. □

By the previous lemma we may assume, without loss of generality, that in a primitive Pythagorean triple (a, b, c), the integer a is odd and the integer b is even. Under this assumption, we can show that both $c - a$ and $c + a$ are twice a square, which leads us directly to Euclid's parametrization of the Pythagorean triples.

Lemma 11.2.6. *Consider a primitive Pythagorean triple (a, b, c) in which b is even, so that a is odd. Then there are two relatively prime positive integers $s < t$ of opposite parity, such that*

$$c - a = 2s^2 \qquad \text{and} \qquad c + a = 2t^2.$$

Proof. By the assumption that b is even, we can write $b = 2u$. Then we have

$$(c - a)(c + a) = c^2 - a^2 = b^2 = 4u^2.$$

Any common divisor d of $c - a$ and $c + a$ must divide their sum $2c$ and their difference $2a$. However, since a and c are relatively prime, it follows that $d \mid 2$. On the other hand, since both a and c are odd it follows that $c \pm a$ is even, which implies that $d = 2$. Thus we see that

$$\left(\frac{c-a}{2}\right)\left(\frac{c+a}{2}\right) = u^2$$

is a decomposition of a square into relatively prime factors. This implies that each factor is itself a square. More precisely, there are two relatively prime positive integers $s < t$ such that

$$\frac{c-a}{2} = s^2 \qquad \text{and} \qquad \frac{c+a}{2} = t^2.$$

Furthermore, observe that since c and a are both odd, it follows that one of $c - a$ and $c + a$ is divisible by 4 and the other is of the form $4k + 2$. This implies that one of s and t is even and the other is odd. □

Theorem 11.2.7 (Euclid's Parametrization of the Primitive Pythagorean Triples). *For every primitive Pythagorean triple (a, b, c) with b even, we can uniquely determine two relatively prime positive integers $s < t$ of opposite parity such that*

$$a = t^2 - s^2, \qquad b = 2st, \qquad \text{and} \qquad c = t^2 + s^2.$$

Proof. To prove that two relatively prime integers $0 < s < t$ exist as specified, we will use s and t as determined in Lemma 11.2.6, where

$$\frac{c-a}{2} = s^2, \qquad \text{and} \qquad \frac{c+a}{2} = t^2.$$

A simple calculation shows that $t^2 - s^2 = a$, and $t^2 + s^2 = c$. To see that $b = 2st$, it suffices to show that $b^2 = 4s^2t^2$. This follows from the following short calculation:

$$4s^2t^2 = (c - a)(c + a) = c^2 - a^2 = b^2.$$

In order to show that s and t are uniquely determined as specified, consider additionally two relatively prime positive integers $u < v$ of opposite parity such that

$$a = v^2 - u^2, \qquad b = 2uv, \qquad \text{and} \qquad c = v^2 + u^2.$$

then $c - a = 2u^2$ and $c + a = 2v^2$, while at the same time we have $c - a = 2s^2$ and $c + a = 2t^2$. This implies $s^2 = u^2$ and $t^2 = v^2$. Since all the numbers involved are positive, we obtain that $s = u$ and $t = v$. □

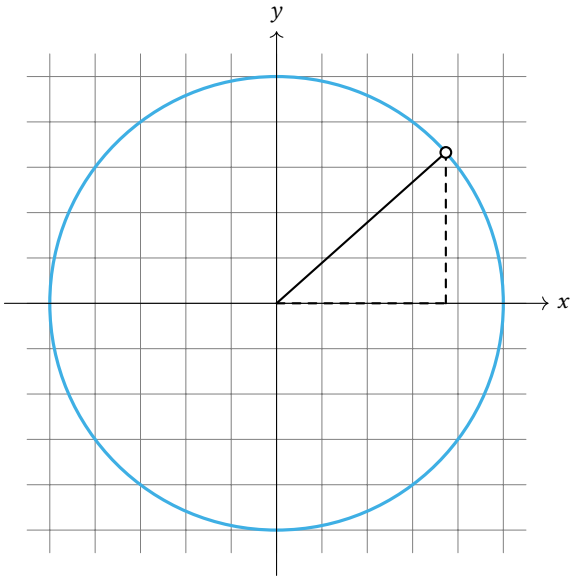


Figure 11.3: The unit circle consists of all points (x, y) for which the distance to the origin $\sqrt{x^2 + y^2}$ is equal to 1.

11.3 Rational Points on the Unit Circle

The **unit circle** consists of all points (x, y) that are a unit distance from the origin. In other words, a point (x, y) in the plane with real number coordinates lies on the unit circle if it satisfies the equation

$$x^2 + y^2 = 1.$$

When both coordinates x and y are rational numbers, we say that (x, y) is a **rational point** on the unit circle. Primitive Pythagorean triples can be used to obtain such rational points on the unit circle. Every primitive Pythagorean triple (a, c, b) determines the point

$$\left(\frac{a}{c}, \frac{b}{c}\right),$$

which satisfies $(a/c)^2 + (b/c)^2 = (a^2 + b^2)/c^2 = 1$. Thus we see that if (a, b, c) is a primitive Pythagorean triple, then $(a/c, b/c)$ is a rational point on the unit circle. We will show that *every* rational point on the unit circle arises in this way.

THEOREM 11.3.1. *There is a bijection between the set of primitive Pythagorean triples (a, b, c), where we allow a and b to be any integer but we maintain the requirement that c is positive, and rational points on the unit circle.*

Proof. We begin by observing that the map

$$(a, b, c) \mapsto \left(\frac{a}{c}, \frac{b}{c}\right)$$

is an injective function from primitive Pythagorean triples to rational points on the unit circle, since the fractions a/c and b/c are in lowest terms. Therefore, it suffices to show that this map is surjective, meaning that every rational point on the unit circle is of this form.

We first claim that if (x, y) is a rational point on the unit circle with $x = a/c$ and $y = b/d$ in lowest terms, then we must have $c = d$. This is a special case of Exercise 10.10, so the reader who has already solved that exercise may skip ahead.

The equation $x^2 + y^2 = 1$ can be rearranged to the equation

$$a^2d^2 + b^2c^2 = c^2d^2.$$

It follows that $c^2 \mid a^2d^2$ and $d^2 \mid b^2c^2$. However, since $\gcd(a, c) = 1$ and $\gcd(b, d) = 1$, we conclude that $c^2 \mid d^2$ and $d^2 \mid c^2$, which implies the claim.

To finish the proof, consider a rational point (x, y) on the unit circle with $x = a/c$ and $y = b/d$. Then we have $c = d$ by the previous claim. It follows that

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = \left(\frac{a}{c}\right)^2 + \left(\frac{b}{d}\right)^2 = 1,$$

and we conclude that (a, b, c) is a primitive Pythagorean triple satisfying $(a/c, b/c) = (x, y)$. □

11.4 Vieta Jumping Between Rational Points on the Unit Circle

The unit circle is a 1-dimensional curve through the plane. This suggests that there should be a way of parametrizing all the (rational) points on the unit circle using one rational number as a parameter. We will use a parametrization called the **stereographic projection** (see Figure 11.3). The idea of the stereographic projection is to take one particularly simple rational point on the unit circle as our base point—we take the point $(-1, 0)$ as our base point—and characterize all the other rational points (x, y) by the slope of the line through the base point $(-1, 0)$ and (x, y). Surely, if (x, y) is a rational point on the circle, then the line through $(-1, 0)$ and (x, y) will have a rational slope. The question that thus arises is: Does every line through $(-1, 0)$ with a rational slope intersect the unit circle in a rational point?

At first consideration, it might not be so clear that this should indeed be the case. The key insights are obtained through Vieta's formulas for the roots of a (quadratic) polynomial, named after the 16th century French mathematician François Viète. He was one of the first to use letters as parameters in his study of algebraic equations. Vieta's formulas are the essential ingredient in a problem-solving technique called **Vieta jumping**.



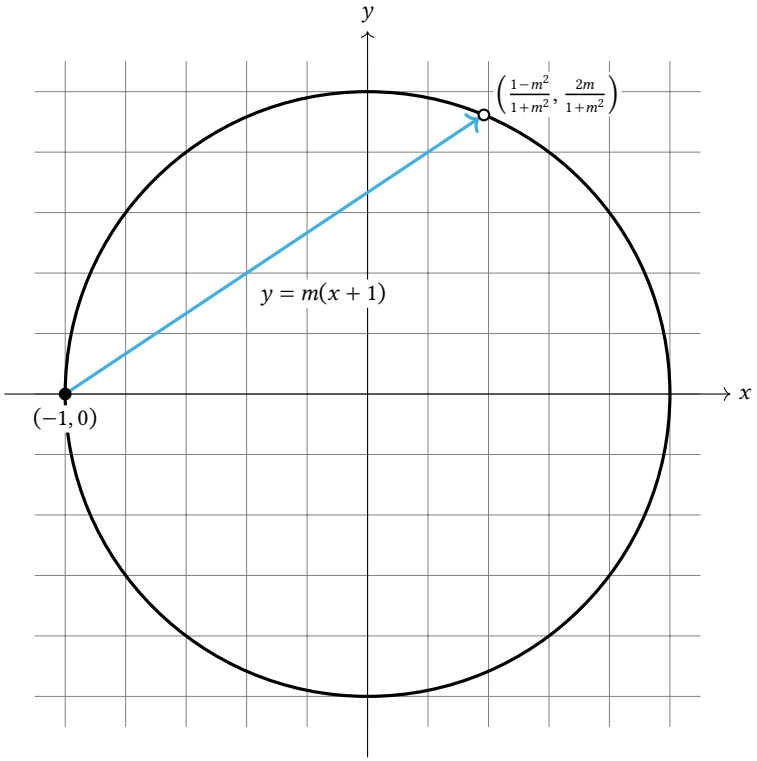


Figure 11.4: A point (x, y) on the unit circle is rational if and only if the line through $(-1, 0)$ and (x, y) has a rational slope.

THEOREM 11.4.1 (Vieta's Formulas for the Roots of a Quadratic Polynomial). *Consider a polynomial of the form $t^2 - Bt + C$ and suppose that r is a root of this polynomial. Then the other root s satisfies the relations*

$$r + s = B \qquad \text{and} \qquad rs = C.$$

PROOF. The two roots of a quadratic polynomial $f(t) = t^2 - Bt + C$ are r and s if and only if we can write $f(t)$ in the form

$$f(t) = (t - r)(t - s).$$

However, if this equation holds, then we find that

$$t^2 - (r + s)t + rs = t^2 - Bt + C.$$

The asserted relations now follow by comparing coefficients. □

A corollary of the previous theorem is that if B and C are rational numbers and r is a rational root of the polynomial $t^2 - Bt + C$, then the other root s is also rational.

Theorem 11.4.2. *Consider the line given by the equation $y = m(x+1)$, which has slope m and passes through the point $(-1, 0)$. This line intersects the unit circle at the point*

$$\left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right).$$

Consequently, the line $y = m(x+1)$ intersects the unit circle at a rational point other than $(-1, 0)$ if and only if the slope m is rational.

Proof. In order to find the two points (x, y) on the intersection of the line $y = m(x+1)$ and the unit circle, we must solve the equation

$$x^2 + m^2(x+1)^2 = 1.$$

By rearranging, we find that it is equivalent to solve the equation

$$x^2 + \frac{2m^2}{1+m^2}x + \frac{m^2-1}{1+m^2} = 0.$$

Since we already know that there is one root at -1, we can find the other root by Vieta's formulas given in Theorem 11.4.1: The other intersection point is at (x, y), where

$$x = \frac{1-m^2}{1+m^2} \qquad \text{and} \qquad y = \frac{2m}{1+m^2}.$$

For the final claim, it is clear that if $m \in \mathbb{Q}$, then both x and y are rational numbers. Conversely, if (x, y) is a rational point on the unit circle distinct from $(-1, 0)$, then we have $-1 < x \leq 1$ and $m = \frac{y}{x+1}$, which is a quotient of rational numbers and thus rational. □

Remark 11.4.3. If (a, b, c) is a primitive Pythagorean triple, then the corresponding rational point on the unit circle is $(a/c, b/c)$, and the slope of the line through $(-1, 0)$ and this point is

$$\frac{b}{a+c}.$$

11.5 The Tree of Primitive Pythagorean Triples

In 1934, the Swedish senior high school teacher B. Berggren discovered that the primitive Pythagorean triples can naturally be given the structure of a ternary tree [Ber1934]. More precisely, he discovered that all primitive Pythagorean triples can be obtained by iterated application of three linear operations, starting with the triple $(3, 4, 5)$. The three linear operations found by Berggren are the three matrices

$$A = \begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}, \qquad \text{and} \qquad C = \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{pmatrix}.$$



To rediscover Berggren's matrices and his ternary tree, we will use the technique of Vieta jumping, which we have already used in the previous section to establish a correspondence between primitive Pythagorean triples and rational points on the unit circle. We begin with a generalization of Theorem 11.4.2, where we established the stereographic projection of the (rational) points on the unit circle.

THEOREM 11.5.1 (Vieta Jumping for Rational Points on the Unit Circle). *Consider a rational point (x, y) on the unit circle. For any point (u, v) with rational coordinates such that $u \neq x$, consider the line through (u, v) and (x, y), whose slope is*

$$m := \frac{y - v}{x - u}.$$

This line intersects the unit circle in a second rational point (x', y'). Moreover, x and x' satisfy the relation

$$xx' = \frac{(mu - v)^2 - 1}{1 + m^2}.$$

PROOF. First, we parametrize the line through (u, v) and (x, y) as a function of t given by

$$s(t) := m(t - u) + v,$$

where the slope m is defined by $m := \frac{y-v}{x-u}$. In order to find the intersection points of this line with the unit circle, we have to solve the equation $t^2 + s(t)^2 = 1$. We can simplify this equation as follows:

$$\begin{aligned} 0 &= t^2 + (v + m(t - u))^2 - 1 \\ &= t^2 + v^2 + 2vm(t - u) + m^2(t^2 - 2ut + u^2) - 1 \\ &= (1 + m^2)t^2 + (2vm - 2um^2)t + (mu - v)^2 - 1. \end{aligned}$$

Dividing through by $1+m^2$, we see that x and x' are the roots of the quadratic equation

$$t^2 + \frac{2vm - 2um^2}{1 + m^2}t + \frac{(mu - v)^2 - 1}{1 + m^2} = 0.$$

We have thus reached a quadratic equation of the form $t^2 + Bt + C$, which has by assumption one rational solution at $t = x$. It follows from Theorem 11.4.1 that the second solution x' satisfies the Vieta relation

$$xx' = \frac{(mu - v)^2 - 1}{1 + m^2}.$$ □

By making a suitable choice for the rational point (u, v), the previous theorem can be used to find, for each rational point (x, y) on the unit circle corresponding to a primitive Pythagorean triple (a, b, c) with $0 < c$, which we assume to be nontrivial in the sense that $ab \neq 0$, a new rational point (x', y') on the unit circle corresponding to

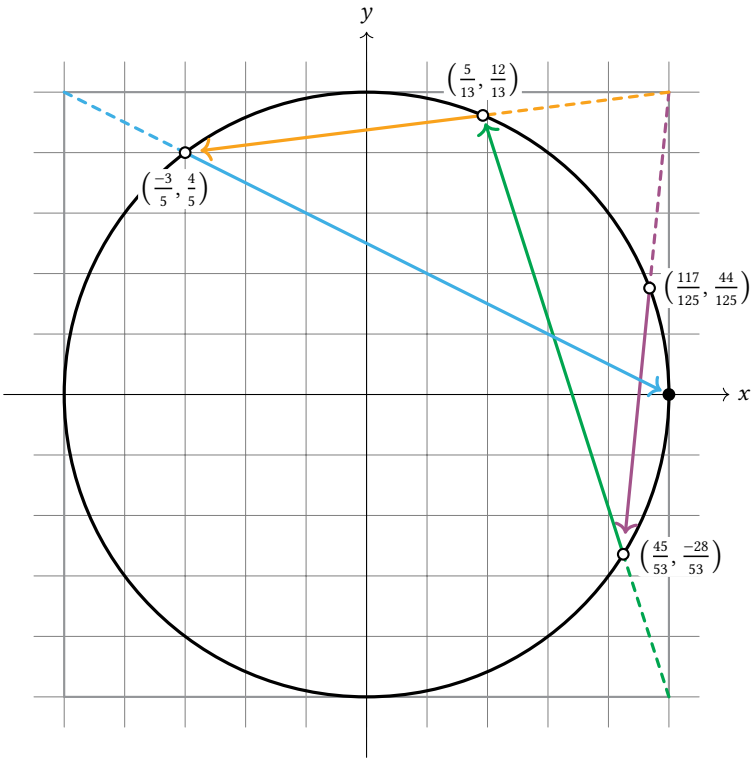


Figure 11.5: For any rational point (x, y) on the unit circle apart from $(0, \pm 1)$ and $(\pm 1, 0)$, draw a straight line through it from the outer corner of its quadrant to find a new rational point (x', y') on the unit circle. The common denominator of the fractions x' and y', when brought to lowest terms, is strictly smaller than that of x and y, so that this process eventually terminates at $(0, \pm 1)$ or $(\pm 1, 0)$.

a primitive Pythagorean triple (a', b', c') satisfying $0 < c' < c$. That is, we will find a procedure to step from a primitive Pythagorean triple to a new Pythagorean triple with a smaller hypotenuse.

The suitable choice of (u, v) that we just alluded is given by

$$u := \operatorname{sgn}(a) \qquad \text{and} \qquad v := \operatorname{sgn}(b).$$

In other words, the point (u, v) is the nearest corner of the 2-by-2 square centered at the origin to the rational point (x, y) on the unit circle. The procedure $(a, b, c) \mapsto (a', b', c')$ of stepping from one Pythagorean triple to a new one with a smaller hypotenuse is illustrated in the following example, which is accompanied by Figure 11.5.

EXAMPLE 11.5.2. Consider the Pythagorean triple $(a, b, c) := (117, 44, 125)$, which corresponds to the rational point $(x, y) := (117/125, 44/125)$ on the unit circle. Since both a and b are positive, we have $u = v = 1$, and the new point (x', y') the unit circle and on the line through (u, v) and (x, y) satisfies

$$xx' = \frac{(m-1)^2 - 1}{1 + m^2},$$

where $m = \frac{y-1}{x-1}$. Since $x = a/c$ and $y = b/c$, we can rearrange the previous Vieta relation to obtain that

$$xx' = \frac{(b-a)^2 - (a-c)^2}{(a-c)^2 + (b-c)^2} = \frac{73^2 - 8^2}{8^2 + 81^2}.$$

From these calculations, we obtain that $x' = 45/53$ and $y' = -28/53$, which corresponds to the primitive Pythagorean triple $(45, -28, 53)$, which indeed has a hypotenuse satisfying $53 < 125$.

Recall that for each rational point (x, y) on the unit circle, we can write $x = a/c$ and $y = b/c$ in lowest terms with identical denominators, which we always take to be positive. This observation is a direct consequence of Theorem 11.3.1. Thus, we can unambiguously refer to the *common denominator* of any rational point on the unit circle. We also recall that for any two positive integers a and b, we have

$$2ab \leq a^2 + b^2. \tag{$*$}$$

This inequality, which is an instance of the AM–GM inequality, follows from the observation that $(a - b)^2 = a^2 - 2ab + b^2 \geq 0$.

THEOREM 11.5.3 (Pythagorean Descent). *Consider a primitive Pythagorean triple (a, b, c) with $c > 1$, corresponding to the rational point (x, y) on the unit circle given by*

$$x = \frac{a}{c} \qquad \textit{and} \qquad y = \frac{b}{c}.$$

Furthermore, consider one of the corner points $(u, v) = (\pm 1, \pm 1)$ *of the* 2*-by-*2 *square centered at the origin. Then the second intersection point* (x', y') *of the line through* (u, v) *and* (x, y) *and the unit circle, as determined by Theorem 11.5.1, corresponds to the primitive Pythagorean triple* (a', b', c') *given by*

$$\begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = \begin{pmatrix} -1 & -2uv & 2u \\ -2uv & -1 & 2v \\ -2u & -2v & 3 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

Moreover, when $u = \operatorname{sgn}(x)$ *and* $v = \operatorname{sgn}(y)$*, then we have* $0 < c' < c$.

Proof. The rational point (x', y') obtained from Theorem 11.5.1 satisfies the relation

$$xx' = \frac{(mu - v)^2 - 1}{1 + m^2},$$

where $m := \frac{y-v}{x-u}$ is the slope of the line through (u, v) and (x, y). Given that $x = a/c$ and $y = b/c$, we see that

$$m = \frac{b - vc}{a - uc}.$$

We use this to rewrite Vieta's relation between x and x' as follows:

$$xx' = \frac{(bu - av)^2 - (a - uc)^2}{(a - uc)^2 + (b - vc)^2}.$$

Given that $u^2 = v^2 = 1$ and $a^2 + b^2 = c^2$, we compute this quantity as follows:

$$\begin{aligned} xx' &= \frac{(bu - av)^2 - (a - uc)^2}{(a - uc)^2 + (b - vc)^2} \\ &= \frac{b^2 - c^2 - 2uvab + 2uac}{-2uac - 2vbc + a^2 + b^2 + 2c^2} \\ &= \frac{a}{c} \frac{-a - 2uvb + 2uc}{-2ua - 2vb + 3c}. \end{aligned}$$

Thus, we obtain the following expressions for a' and c', so that $x' = a'/c'$:

$$\begin{aligned} a' &= -a - 2uvb + 2uc, \\ c' &= -2ua - 2vb + 3c. \end{aligned}$$

Now we can verify that $b' = -2uva - b + 2vc$ by checking that, taking this as our definition for b', we have $a'^2 + b'^2 = c'^2$ and

$$\frac{b' - b}{a' - a} = m.$$

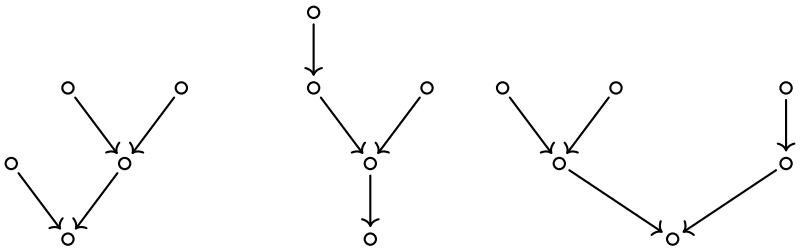


Figure 11.6: A forest.

Both of these identities are verified by a quick calculation, which we leave to the reader. It follows that, given a primitive Pythagorean triple (a, b, c), the Pythagorean triple (a', b', c') is determined by the matrix multiplication

$$\begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = \begin{pmatrix} -1 & -2uv & 2u \\ -2uv & -1 & 2v \\ -2u & -2v & 3 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

If M is the matrix in the above equation, it is immediate from the construction of M that $M^2 = I$, the identity matrix. Indeed, jumping from (x, y) to (x', y') using the point (u, v), and jumping again from (x', y') using the same point (u, v) reverses the process and lands us back at (x, y). This implies that any common divisors of (a', b', c') are also common divisors of (a, b, c). Since (a, b, c) is primitive, it follows that (a', b', c') is also primitive.

The final claim is that $c' := 3c - 2|a| - 2|b|$ satisfies $0 < c' < c$. By rearranging the terms, we see that these strict inequalities are equivalent to the strict inequalities

$$2c < 2|a| + 2|b| < 3c.$$

We can prove these strict inequalities by proving that they hold for the squares:

$$4c^2 < 4(|a| + |b|)^2 < 9c^2.$$

To see this, we note that $(|a|+|b|)^2 = a^2 + 2|a||b|+b^2 = c^2 + 2|a||b|$. This immediately implies that $c^2 \leq (|a|+|b|)^2$. Furthermore, we have the inequality $2|a||b| \leq a^2+b^2 = c^2$ by the inequality stated in Equation $(*)$. Thus we obtain that

$$4c^2 < 4(|a| + |b|)^2 = 4c^2 + 8|a||b| \leq 4c^2 + 4c^2 < 9c^2. \qquad \square$$

Theorem 11.5.3 (Pythagorean Descent) can be used to determine a ternary tree structure on the set of primitive Pythagorean triples. We will define trees to be forests consisting of a single tree. Mathematically, a **forest** is defined as a set F equipped with a **height function** $h : F \to \mathbb{N}$, and for each height n a **parent function**

$$p : \{x \in F \mid h(x) = n + 1\} \to \{x \in F \mid h(x) = n\}.$$

Given a forest F, an element $x \in F$ is called a **node**; a node x of height 0 is called a **root**; the node $p(x)$ is called the **parent** of x; and for any node y, all the nodes x whose parent is y are called the **children** of y. A forest is said to be a **tree** if it contains exactly one root. We note that a forest can contain nodes of arbitrary height; that is, mathematical trees can be infinitely tall. In Figure 11.6 we have drawn an example of a forest.

Example 11.5.4 (The forest of rational points on the unit circle). In Theorem 11.5.3 (Pythagorean Descent), we showed that for each rational point on the unit circle other than $(\pm 1, 0)$ or $(0, \pm 1)$, we can jump to another rational point whose positive common denominator is strictly smaller than that of the original point. If the new point is not one of the points $(\pm 1, 0)$ or $(0, \pm 1)$, we can jump again to yet another rational point whose common denominator is still smaller. Starting at $(x_0, y_0) := (x, y)$, repeating this process results in a sequence of rational points (x_n, y_n) on the unit circle, whose common denominators strictly decrease as the sequence progresses. Since a sequence of positive integers cannot be infinitely long, we see that this sequence must terminate. That is, in a finite number of jumps we must reach one of the points $(\pm 1, 0)$ or $(0, \pm 1)$.

For any rational point (x, y) on the unit circle, let $h(x, y)$ be the least number of jumps required to reach one of the points $(\pm 1, 0)$ or $(0, \pm 1)$. Furthermore, if (x, y) is of height $n + 1$, so that it is neither $(\pm 1, 0)$ nor $(0, \pm 1)$, let $p(x, y) := (x', y')$ be the target of the jump from (x, y). This height and parent function gives the set of rational points on the unit circle the structure of a forest with four roots, the points $(\pm 1, 0)$ and $(0, \pm 1)$. In Figure 11.7 we displayed one branching point in this forest, along with the path to its root.

We observe that in this forest, each root $(\pm 1, 0)$ or $(0, \pm 1)$ has two children. These are the eight points $(\pm 3/5, \pm 4/5)$ and $(\pm 4/5, \pm 3/5)$. Any rational point on the unit circle other than a root has exactly three children, one in each quadrant other than its own.

We also observe that the forest of rational points on the unit circle possesses some important symmetries. Each rotation by 90° and each reflection along the axis of abscissas, the line $y = x$, the axis of ordinates, and the line $y = -x$ maps rational points on the unit circle to rational points on the unit circle in such a way that the height and parent functions are preserved. To see this, observe that each of those symmetries reflects a point (x, y) on the unit circle to one of the points $(\pm x, \pm y)$ or $(\pm y, \pm x)$.

Example 11.5.5 (The tree of primitive Pythagorean triples). We will now use the forest of rational points on the unit circle to construct the tree of primitive Pythagorean triples, and derive Berggren's matrices.

The matrix we used in Theorem 11.5.3 (Pythagorean Descent) to jump from a primitive Pythagorean triple (a, b, c) with $1 < c$ to a new primitive Pythagorean triple (a', b', c') was defined as

$$M_{u,v} := \begin{pmatrix} -1 & -2uv & 2u \\ -2uv & -1 & 2v \\ -2u & -2v & 3 \end{pmatrix}.$$

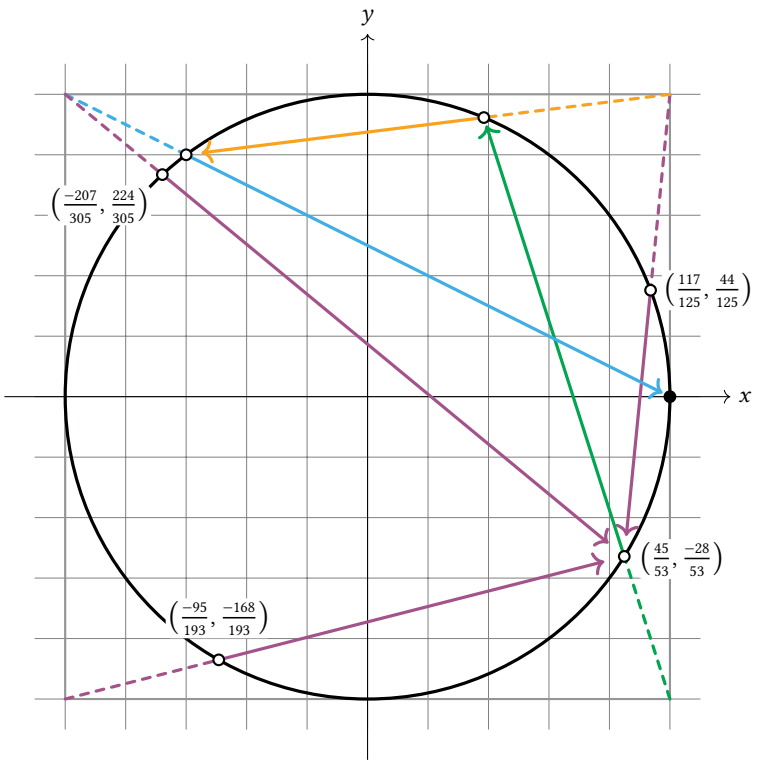


Figure 11.7: Each rational point on the unit circle other than $(\pm 1, 0)$ or $(0, \pm 1)$ is the target of a Vieta jump from three rational points on the unit circle with larger common denominator, one for each quadrant other than its own. Here, the purple, green, and orange jumps are drawn exactly as in Figure 11.5. The point $(45/53, -28/53)$ is the target of three jumps, each drawn in blue. Since each rational point is the target of three Vieta jumps that decrease the common denominator, we see that the rational points on the unit circle can be organized in a forest consisting of four trees, where the four nodes at height 0 are the points $(\pm 1, 0)$ and $(0, \pm 1)$.

When $u := \operatorname{sgn}(a)$ and $v := \operatorname{sgn}(b)$, then the new Pythagorean triple satisfies $0 < c' < c$. This implies that for any of the three other choices of (u, v), the new Pythagorean triple satisfies $c < c'$.

From now on, we will assume that (a, b, c) is a primitive Pythagorean triple in which all of a, b, and c are positive integers, and furthermore b is even. To step upwards along the tree, we set $u = \pm 1$ and $v = \pm 1$ so that at least one of u and v is -1. This results in a new Pythagorean triple corresponding to a rational point on the unit circle in the quadrant of the point (u, v). To reflect this rational point back to the quadrant with positive x- and y-cordinates, we compose the matrix $M_{u,v}$ with one further linear operation as follows:

$$\begin{pmatrix} u & 0 & 0 \\ 0 & v & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & -2uv & 2u \\ -2uv & -1 & 2v \\ -2u & -2v & 3 \end{pmatrix} = \begin{pmatrix} -u & -2v & 2 \\ -2u & -v & 2 \\ -2u & -2v & 3 \end{pmatrix}$$

Instantiating these matrices at $(u, v) = (-1, 1)$, $(1, -1)$, and $(-1, -1)$ gives the matrices that Berggren discovered in 1934:

$$A = \begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}, \qquad \text{and} \qquad C = \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{pmatrix}$$

By Theorem 11.5.3 (Pythagorean Descent) it follows that all primitive Pythagorean triples can be obtained by iteratively applying the matrices A, B, and C given above. This tree is displayed in Figure 11.8.

11.6 Squares in Arithmetic Progressions

The Euclidean parametrization of the Pythagorean triples has some further applications, but in order to get there we must make a short excursion to the city of Pisa in the 13th century, where Frederick II reigned as the Holy Roman Emperor, and King of Sicily, Jerusalem, and Apulia. When Leonardo Pisano, more commonly known as Fibonacci, was summoned to the court of Frederick II, he met with Master John of Palermo who challenged him with mathematical problems.

One of the challenges of Master John is stated as follows: Find a rational number q such that the numbers

$$q^2 - 5 \qquad \text{and} \qquad q^2 + 5$$

are both squares of rational numbers. Fibonacci's investigations into this problem would eventually lead him to write his *Liber Quadratorum* [FS1987]. The Liber Quadratorum covers topics such as Pythagorean triples, a method of generating infinitely many of them, and arithmetic progressions of squares. There were no known remaining copies of the Liber Quadratorum until a 15th century copy was rediscovered in the Biblioteca Ambrosiana in Milan, which was republished in print in 1857 by the



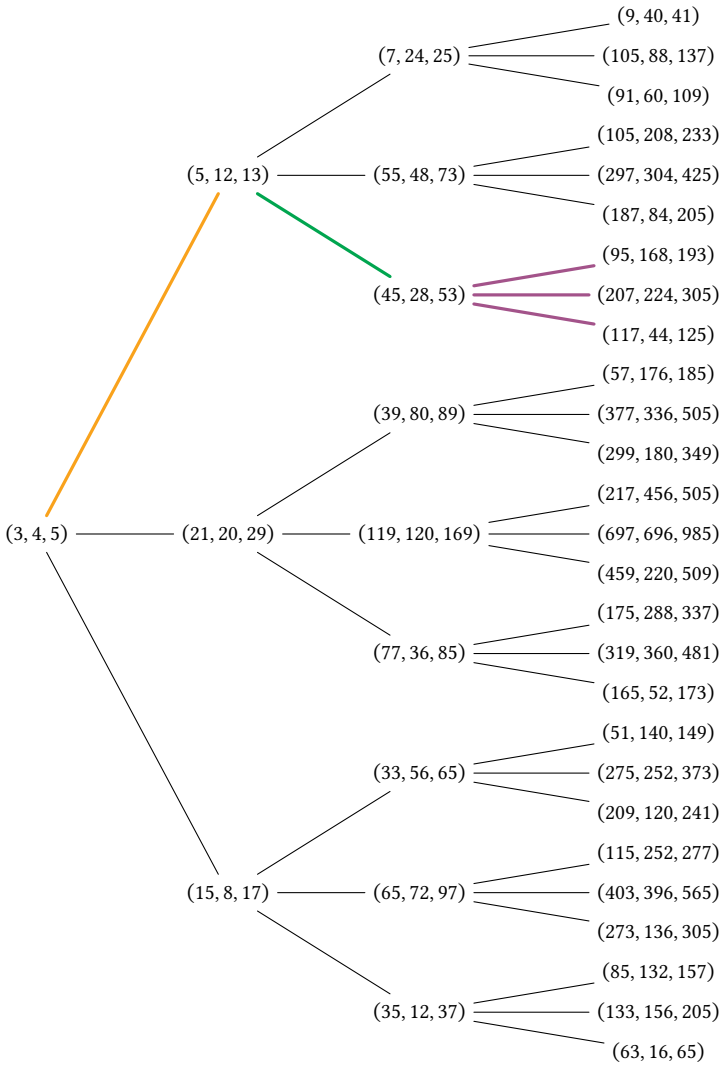


Figure 11.8: The tree of primitive Pythagorean triples. The edges that were drawn in orange, green, or purple in Figure 11.7 have been drawn here in the same color.



Figure 11.9: Leonardo Pisano.

Italian historian and mathematician Baldassarre Boncompagni Ludovisi. Today, the work available in an English translation by Laurence E. Sigler as *The Book of Squares* [FS1987].

Master John's challenge is equivalently formulated as the question of finding four integers a, b, c, and t such that

$$b^2 - a^2 = 5t^2 \qquad \text{and} \qquad c^2 - b^2 = 5t^2.$$

Thus, we are looking for three squares a^2, b^2, and c^2 increasing in increments of $5t^2$. Thus we see that we can conveniently state the problem in terms of arithmetic triples of squares.

Definition 11.6.1. An **arithmetic triple of squares** is a triple (a^2, b^2, c^2) consisting of integer squares such that

$$b^2 - a^2 = c^2 - b^2.$$

This common increment is called the **congruum** and is denoted by $\Delta_{a,b,c}$, or simply Δ. An arithmetic triple of squares (a^2, b^2, c^2) is said to be **primitive** if $\gcd(a, b, c) = 1$.

It follows immediately from the definition that if (a^2, b^2, c^2) is a primitive arithmetic triple of squares, then a, b, and c are also pairwise relatively prime.

We are thus looking for an arithmetic triple of squares, with a congruum of the form $\Delta := 5t^2$. In Exercise 7.10 you were asked to show that the congruum Δ of an arithmetic triple of squares is always divisible by 24, which Fibonacci also reported on in Liber Quadratorum. We conclude from this observation that if Δ is of the form $5t^2$ then Δ must be a multiple of $2 \cdot 3 \cdot 5 \cdot 24 = 720$.

The fact that the congruum in an arithmetic triple of squares is always a multiple of 24 implies that primitive arithmetic triples of squares consist entirely of integers of the form $(6m \pm 1)^2$. Any such square exceeds a multiple of 24 by one. This significantly

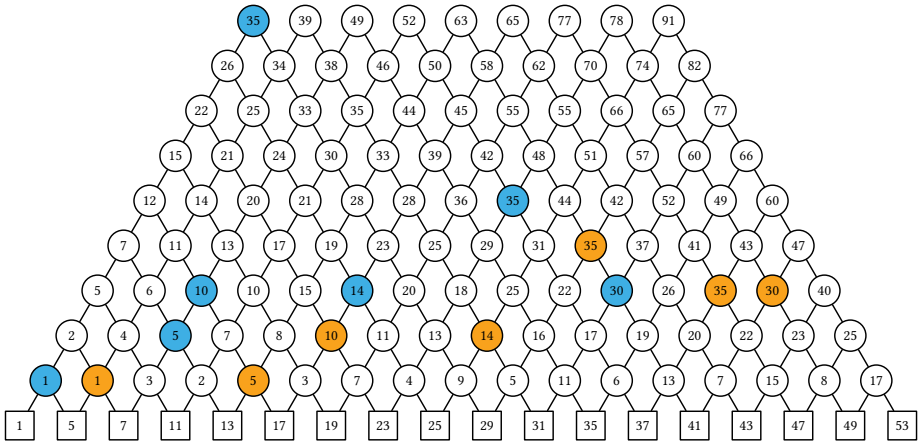


Figure 11.10: The numbers in squares at the base of the grid are the numbers of the form $6m \pm 1$, which correspond exactly to all the numbers n such that $n^2 - 1$ is divisible by 24. If x and y are two numbers in squares at the base of the grid, then the number k at the apex of the triangle spanned by x and y satisfies $y^2 - x^2 = k \cdot 24$. For each primitive arithmetic triple (x^2, y^2, z^2) of squares, the apex of the triangle spanned by x and y is marked in blue, and the apex of the triangle spanned by y and z is marked in orange.

reduces the search space for arithmetic triples of squares. If a_n is the nth positive integer of the form $(6k \pm 1)^2$, then

$$d_n := \frac{a_{n+1} - a_n}{24} = \begin{cases} n & \text{if } n \text{ is odd,} \\ n/2 & \text{if } n \text{ is even.} \end{cases}$$

In order to determine the number of units of 24 in the difference between two arbitrary numbers of the form $(6m \pm 1)^2$, we simply sum the numbers d_n: We define

$$s_{n,m} := \sum_{i=0}^{m} d_{n+i} = \frac{a_{n+m+1} - a_n}{24}.$$

Alternatively, the numbers $s_{n,m}$ are determined by the recursive rule $s_{n,m} = s_{n+1,m-1} + s_{n,m-1} - s_{n+1,m-2}$. The numbers $s_{n,m}$ are displayed in Figure 11.10, from which we

determine that:

$$\begin{aligned}
5^2 - 1^2 = 7^2 - 5^2 &= 1 \cdot 24,\\
13^2 - 7^2 = 17^2 - 13^2 &= 5 \cdot 24,\\
17^2 - 7^2 = 23^2 - 17^2 &= 10 \cdot 24,\\
25^2 - 17^2 = 31^2 - 25^2 &= 14 \cdot 24,\\
29^2 - 1^2 = 41^2 - 29^2 &= 35 \cdot 24,\\
37^2 - 23^2 = 47^2 - 37^2 &= 35 \cdot 24,\\
41^2 - 31^2 = 49^2 - 41^2 &= 30 \cdot 24.
\end{aligned}$$

The solution to Master John's problem to Fibonacci, which Fibonacci reported in Proposition 17 of *Liber Quadratorum*, thus corresponds to the last listed arithmetic triple of squares, which gives

$$\left(\frac{41}{12}\right)^2 - \left(\frac{31}{12}\right)^2 = \left(\frac{49}{12}\right)^2 - \left(\frac{41}{12}\right)^2 = 5.$$

Arithmetic triples of squares are closely related to Pythagorean triples. Given an arithmetic triple of squares (a^2, b^2, c^2), we can write b^2 as a sum of two squares written in terms of a and c. The crucial identity that leads to the construction of a Pythagorean triple using the integers a, b, and c is

$$c^2 + a^2 = 2b^2.$$

Using this identity, we see that

$$\frac{(c-a)^2}{4} + \frac{(c+a)^2}{4} = \frac{c^2 - 2ac + a^2}{4} + \frac{c^2 + 2ac + a^2}{4} = \frac{c^2 + a^2}{2} = b^2.$$

Thus, if (a^2, b^2, c^2) is an arithmetic progression of squares, then the integers

$$x := \frac{c-a}{2}, \qquad y := \frac{c+a}{2}, \qquad \text{and} \qquad z := b$$

determine a Pythagorean triple (x, y, z). Conversely, if (x, y, z) is a Pythagorean triple, then we define

$$a := |y - x|, \qquad b := z, \qquad \text{and} \qquad c := y + x,$$

so that (a^2, b^2, c^2) is easily seen to be an arithmetic triple of squares. Here, we defined a to be the *distance* between y and x in order to ensure that a is positive. The congruum of this arithmetic triple is given by

$$z^2 - (y - x)^2 = 2xy,$$



which is four times the area of the Pythagorean triangle described by the Pythagorean triple (x, y, z). The operations thus described create the following correspondence between some of the most familiar arithmetic triples of squares and Pythagorean triples:

$$(1^2, 5^2, 7^2) \leftrightarrows (3, 4, 5),$$
$$(7^2, 13^2, 17^2) \leftrightarrows (5, 12, 13),$$
$$(1^2, 29^2, 41^2) \leftrightarrows (21, 20, 29),$$
$$(7^2, 17^2, 23^2) \leftrightarrows (15, 8, 17).$$

The fact that these operations mapping arithmetic triples of squares to Pythagorean triples and back are mutually inverse to each other is easily verified by a few quick computations, which we leave to the reader. Thus, we have established:

THEOREM 11.6.2. *Arithmetic triples (a^2, b^2, c^2) of squares are in bijective correspondence with Pythagorean triples (x, y, z), so that primitive arithmetic triples of squares correspond to primitive Pythagorean triples.*

PROOF. We only prove that (a^2, b^2, c^2) is a primitive arithmetic triple of squares if and only if the Pythagorean triple

$$\left(\frac{c-a}{2}, \frac{c+a}{2}, b\right)$$

is primitive.

For the forward direction, assume that $\gcd(a, b, c) = 1$. To see that $(c - a)/2$ and $(c + a)/2$ are relatively prime, it suffices to show that any common divisor d of $c - a$ and $c + a$ is a divisor of 2. Indeed, if d is a common divisor of $c - a$ and $c + a$, then it is also a common divisor of $2a = (c + a) - (c - a)$ and $2c = (c + a) + (c - a)$. Since a and c are relatively prime, it follows that d is a divisor of 2.

Likewise, to show that $(c - a)/2$ and b are relatively prime, we note that since b is odd it suffices to show that $c - a$ and b are relatively prime, which is only the case if $(c - a)^2$ and b^2 are relatively prime. This follows from

$$(c - a)^2 = c^2 + a^2 - 2ac = 2b^2 - 2ac,$$

since any common divisor of $(c - a)^2$ and b^2 is also a common divisor of b^2 and $2ac$, which are relatively prime by assumption. The proof that $(c + a)/2$ and b are relatively prime is similar.

For the reverse direction, assume that

$$\left(\frac{c-a}{2}, \frac{c+a}{2}, b\right)$$

is a primitive Pythagorean triple, so that b is odd, and thus b, $(c-a)/2$, and $(c+a)/2$ are all pairwise relatively prime. Then any common divisor d of a and c is also a common divisor of $(c - a)/2$ and $(c + a)/2$, so that a and c are seen to be relatively prime.

We will prove that (x, y, z) is a primitive Pythagorean triple if and only if

$$((y-x)^2, z^2, (y+x)^2)$$

is a primitive arithmetic triple of squares. By Euclid's parametrization of Pythagorean triples, it suffices to show that for any two □

The previous theorem raises an interesting point. Since the primitive Pythagorean triples are precisely described by Euclid's parametrization, there must similarly be a parametrization of the arithmetic triples of squares.

Corollary 11.6.3. *For any primitive arithmetic triple of squares (a^2, b^2, c^2), we can uniquely determine two relatively prime positive integers $s < t$ of opposite parity such that*

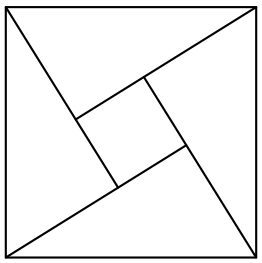
$$a = 2st - t^2 + s^2, \qquad b = t^2 + s^2, \qquad \text{and} \qquad c = 2st + t^2 - s^2$$

with common difference $d = 2st(t-s)^2$.

Exercises

Starter Exercises

11.1 *Bhaskara's proof of the Pythagorean Theorem.* Use the following diagram to give a proof of Theorem 11.1.1 (Pythagorean Theorem):



Routine-Building Exercises

11.2 *The Brahmagupta–Fibonacci identity.* Show that

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2.$$

Conclude that if m and n are two integers that can be written as the sum of two squares, then their product mn can also be written as the sum of two squares.

11.3 Consider a primitive Pythagorean triple (x, y, z).

(a) Prove that exactly one of x, y, and z is divisible by 3.
(b) Prove that exactly one of x, y, and z is divisible by 5.
(c) Find all Pythagorean triples (x, y, z) in which $x = 30$ or $y = 30$. Can any of them be primitive?
(d) Find all relatively prime positive integers x and z such that

$$x^2 + 60^2 = z^2,$$

showing that the components divisible by 3, 4, or 5 might all coincide.

11.4 Find three distinct triangular numbers in an arithmetic progression.

11.5 Find three distinct tetrahedral numbers, that is, numbers of the form $\binom{n+2}{3}$, in an arithmetic progression.

11.6 Define an **Egyptian triple** to be a triple (a, b, c) of integers such that

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c}.$$

Such an Egyptian triple is called **primitive** if $\gcd(a, b) = 1$.

(i) Show that if (a, b, c) is a primitive Egyptian triple, then $\gcd(a, c) = \gcd(b, c) = 1$.

(ii) Show that for any primitive Egyptian triple (a, b, c) with $a \leq b$, we can uniquely determine two relatively prime positive integers $s \leq t$ such that

$$a = s(s+t), \qquad b = t(s+t), \qquad c = st.$$

Challenge Exercises

11.7 Find a parametrization of all pairs (m, n) of natural numbers such that $n^2 - m^2$ is a number of the form 2^k, and prove that your parametrization is a bijection.

11.8 Find a complete parametrization of all triples (a, b, c) satisfying $\gcd(a, b, c) = 1$ such that

$$\frac{1}{a^2} + \frac{1}{b^2} = \frac{1}{c^2}.$$

Note: The condition $\gcd(a, b, c) = 1$ does not imply that a, b, and c are pairwise relatively prime.

11.9 Show that for every positive integer y divisible by 4, there is a primitive Pythagorean triple (a, b, c) with $b = y$.

11.10 Show that every odd positive integer $x \geq 3$ can be written in the form $t^2 - s^2$, where $s < t$ are relatively prime positive integers of opposite parity. Conclude that every odd integer $x \geq 3$ occurs in a Pythagorean triple (a, b, c) with $a = x$.

11.11 Define

$$\begin{aligned} x_n &:= F_n F_{n+1} + (-1)^n, \\ y_n &:= 2F_n F_{n+1}, \\ z_n &:= F_n^2 + F_{n+1}^2, \end{aligned}$$

where F_k is the kth Fibonacci number. Show that (x_n, y_n, z_n) is a Pythagorean triple for each n.

11.12 Let

$$\begin{aligned} a_n &:= F_n F_{n+1} - (-1)^n, \\ b_n &:= F_n^2 + F_{n+1}^2, \\ c_n &:= 3F_n F_{n+1} + (-1)^n. \end{aligned}$$

be defined as in Exercise 2.23, so that (a_n^2, b_n^2, c_n^2) is an arithmetic triple of squares. Show that

$$\gcd(a_n, b_n, c_n) = \begin{cases} 2 & \text{if } n \equiv 1 \pmod 3, \\ 1 & \text{otherwise.} \end{cases}$$

11.13 Consider three squares a^2, b^2, and c^2 in an arithmetic progression in increasing order.



(a) Show that at least one of

$$c-b,\ c-a,\ \text{and}\ b-a$$

is divisible by 3.

(b) Show that at least one of

$$c-b,\ c-a,\ \text{and}\ b-a$$

is divisible by 4.

(c) Show that at least one of

$$b \text{ and } c-a$$

is divisible by 5.

(d) Find all arithmetic progressions (a^2, b^2, c^2) such that $c-a=60$, where only a is allowed to be negative. Are there any such triples with $\gcd(a,b,c)=1$?

(e) Find all *primitive* arithmetic progressions (a^2, b^2, c^2) such that $c-a=120$, where only a is allowed to be negative. Hint: There are four such triples.

11.14 Find all solutions to the equation $x^2-2y^2=1$.

11.15 *Master Theodore's problem for Leonardo Pisano* [FS1987, Proposition 24]. Find three positive integers x, y, and z such that the numbers

$$x+y+z+x^2, \qquad x+y+z+x^2+y^2, \qquad \text{and} \qquad x+y+z+x^2+y^2+z^2$$

are all squares.

11.16 Consider a quadruple (a,b,c,d) such that $\gcd(a,b,c,d)=1$ and

$$a^2+b^2+c^2=d^2.$$

Prove that there is a unique quadruple (s,t,u,v) such that $\gcd(s,t,u,v)=1$, the numbers s^2+t^2 and u^2+v^2 have opposite parity, and

$$\begin{aligned} a &= 2(su-tv),\\ b &= 2(sv+tu),\\ c &= s^2+t^2-u^2-v^2,\\ d &= s^2+t^2+u^2+v^2. \end{aligned}$$

Chapter 12

Infinite Descent

12.1 The Method of Infinite Descent

The method of infinite descent was invented by Fermat. He used this method effectively to solve various problems, including that there are no solutions to $x^4 + y^4 = z^4$ in the positive integers, and that the area of a right triangle is not a perfect square. The method of infinite descent is used to show that certain properties or identities are impossible, by showing that if they do hold then an infinitely descending sequence of natural numbers can be constructed. The following theorem shows that there is no such sequence.

Proposition 12.1.1. *There is no infinite descending sequence*

$$a_0 > a_1 > a_2 > \cdots$$

of natural numbers.

Proof. Suppose, by way of contradiction, that there is such a sequence

$$a_0 > a_1 > a_2 > \cdots .$$

Then the set

$$A := \{a_0, a_1, a_2, \ldots\}$$

is a nonempty subset of the natural numbers, and by Theorem 5.2.1 (The Well-Ordering Principle of the Natural Numbers) it follows that this set has a least element. However, all the elements in A are of the form a_n for some natural number $\mathbb{N}$, and none of these elements are minimal, since we have assumed that $a_n > a_{n+1}$. This contradiction shows

that our assumption that there exists an infinite descending sequence must be false, and thus there is no such sequence. □

The previous proposition leads to Fermat's method of infinite descent. Fermat observed that if an assumption H leads to an infinite descending sequence, then the assumption H must be false.

THEOREM 12.1.2 (Method of Infinite Descent). *Consider a set A equipped with a function $f : A \to A$ and a function $h : A \to \mathbb{N}$. If $h(f(a)) < h(a)$ for all a, then A is empty.*

PROOF. Suppose, by way of contradiction, that the set A is inhabited by an element $a \in A$. By iterating f, we define a sequence of elements a_i by

$$\begin{aligned} a_0 &:= a \\ a_{i+1} &:= f(a_i). \end{aligned}$$

Then we have $h(a_0) > h(a_i) > h(a_2) > \cdots$, which is an infinite descending sequence of natural numbers. Thus, the assumption that A is inhabited was false. □

In §11.4 we used Vieta jumping to jump between rational points on the unit circle in such a way that the common denominators formed a decreasing sequence of positive integers. Necessarily, this process terminates once an integral point on the unit circle is reached. Vieta jumping can also be used with the method of infinite descend.

Recall that the basic idea of Vieta jumping is to use Viète's formulas for the roots of a quadratic formula

$$(x - r)(x - s) = x^2 - (r + s)x + rs$$

in order to jump to the other root once one is known. We saw in Theorem 11.4.1 that if r is a root of a monic polynomial $x^2 - Bx + C$, then the other root s satisfies

$$s = B - r = \frac{C}{s}.$$

Thus, if we know one root of a quadratic polynomial then we can easily 'jump' to the other root using one the above formulas. Vieta jumping became a popular problem-solving technique for international contests such as the International Mathematics Olympiad.

EXAMPLE 12.1.3. In Exercise 6.13 you were asked to show that for any two positive integers x and y such that $xy \mid x^2 + y^2$, we must have $x = y$. The expected solution was to observe that the discriminant of the quadratic equation $x^2 - kxy + y^2 = 0$ seen as an equation in one variable x and a parameter y is $(ky)^2 - 4y^2$, which is a square if and only if $k = 2$. Although this problem can readily be solved directly, we will use it here to illustrate Vieta jumping.

We first observe that the quadratic equation

$$x^2 - kxy + y^2 = 0$$

arising from the divisibility condition $xy \mid x^2 + y^2$ is *homogeneous* in the sense that each of the three terms have the same degree in x and y combined. Thus, if x an y satisfy this polynomial equation, then so must

$$x' := \frac{x}{\gcd(x,y)} \qquad \text{and} \qquad y' := \frac{y}{\gcd(x,y)}.$$

We can therefore solve the problem by showing that the only pair of coprime positive integers x and y satisfying the polynomial equation must satisfy $x = y = 1$.

To see this, we may assume without loss of generality that $0 < y < x$. Given that x is a solution of the quadratic equation $t^2 - kty + y^2$ in the variable t, it follows that the other solution is $x' := ky - x$. Notice that $\gcd(ky - x, y) = 1$, so that $x' := ky - x$ and y are again relatively prime. Furthermore, since $xx' = y^2$ it follows that

$$0 < x' = \frac{y^2}{x} < y.$$

We have thus found a new solution with $x' < y$. Now we can swap the roles for x' and y and repeat the process, obtaining every smaller solutions in the positive integers. Since this is clearly impossible, it must have been impossible for there to be a pair of relatively prime positive integers x and y such that $xy \mid x^2 + y^2$.

12.2 The Area of a Pythagorean Triangle is not a Square

A classic application of Fermat's infinite descent gives us that the area of a Pythagorean triangle is never a square number. Recall that the area of a triangle is half the base times the height, so that every Pythagorean triple (a, b, c) determines a Pythagorean triangle with area

$$\frac{1}{2}ab.$$

Theorem 12.2.1. *The area of a Pythagorean triangle is not a square number.*

Proof. It suffices to prove the statement for primitive Pythagorean triangles; that is, a triangle whose sides (a, b, c) form a primitive Pythagorean triple. By Theorem 11.2.7 (Euclid's Parametrization of the Primitive Pythagorean Triples), we can find two relatively prime integers $s < t$ of opposite parity, such that

$$a = t^2 - s^2, \qquad b = 2st, \qquad \text{and} \qquad c = t^2 + s^2.$$

The area of the triangle is given in terms of this parametrization by the nonzero quantity

$$st(t^2 - s^2) = st(t - s)(t + s).$$

Now observe that all of these factors are relatively prime to one another; indeed, given that s and t are relatively prime, it follows at once from Proposition 7.2.1 that both s

and t are relatively prime to both $s - t$ and $s + t$. Furthermore, any common divisor of $s - t$ and $s + t$ must be a common divisor of $2s$ and $2t$, which implies that it must divide 2. However, $s - t$ and $s + t$ are odd since s and t are of opposite parity, so that $s - t$ and $s + t$ are seen to be relatively prime. Thus we conclude that if the area of the Pythagorean triangle is a square, then each of these factors must also be a square. This allows us to write

$$s = u^2, \quad t = v^2, \quad t - s = x^2, \quad \text{and} \quad t + s = y^2.$$

Since s and t are of opposite parity, it follows that x and y are both odd. Now notice that the triple of integers

$$\left(\frac{y-x}{2}, \frac{y+x}{2}, v\right)$$

is a Pythagorean triple, since

$$\left(\frac{y-x}{2}\right)^2 + \left(\frac{y+x}{2}\right)^2 = \frac{y^2+x^2}{2} = v^2.$$

Furthermore, the area of the corresponding Pythagorean triangle is given by

$$\frac{1}{2}\left(\frac{y-x}{2}\right)\left(\frac{y+x}{2}\right) = \frac{y^2-x^2}{8} = \frac{u^2}{4}.$$

The quantity $u^2/4$ must therefore be an integer strictly less than s, which in turn is strictly less than the area $\frac{1}{2}ab$. Thus, we have constructed a Pythagorean triangle whose area is a strictly smaller nonzero square number, which leads to a contradiction by infinite descent. □

12.3 The Unsolvability of $x^4 + y^4 = z^4$

THEOREM 12.3.1. *There are no three positive integers x, y, and z for which the equation*

$$x^4 + y^4 = z^2$$

holds.

PROOF. Consider the set

$$A := \{(x, y, z) \in \mathbb{Z}_{>0} \mid x^4 + y^4 = z^2\}$$

with $h(x, y, z) := z$. We will construct a function $f : A \to A$ such that $h(f(x, y, z)) < h(x, y, z)$ for every $(x, y, z) \in A$.

First, we notice that if (x, y, z) is a triple of positive integers satisfying the equation $x^4 + y^4 = z^2$, then (x^2, y^2, z) is a Pythagorean triple. Since we can always divide out any common factors, we may assume that x and y are relatively prime. Furthermore,

we may assume that y is even, so that by Euclid's parametrization there are relatively prime positive integers $s < t$ of opposite parity such that

$$x^2 = t^2 - s^2,$$
$$y^2 = 2st,$$
$$z = t^2 + s^2.$$

The key observation is now in the first equation: We obtain a new Pythagorean triple $x^2 + s^2 = t^2$, allowing us to apply Euclid's parametrization of Pythagorean triples once more. Since x is odd it follows that s is even, so we find relatively prime positive integers $u < v$ such that

$$x = v^2 - u^2$$
$$s = 2uv$$
$$t = v^2 + u^2.$$

Now it follows that $y^2 = 4uv(v^2 + u^2)$. We claim that the numbers uv and $v^2 + u^2$ are relatively prime. To see this, note that both u and v are relatively prime to $v^2 + u^2$ since

$$\gcd(u, v^2 + u^2) = \gcd(u, v^2) = 1 \qquad \text{and} \qquad \gcd(v, v^2 + u^2) = \gcd(v, u^2) = 1,$$

and hence their product uv is also relatively prime to $v^2 + u^2$.

Since uv and $v^2 + u^2$ are relatively prime, the fact that $4uv(v^2 + u^2)$ is a square implies that both uv and $v^2 + u^2$ are squares. Given that u and v are relatively prime, this implies that u and v are squares. It follows that there are integers a and b such that $u = a^2$ and $v = b^2$, and thus we see that

$$v^2 + u^2 = a^4 + b^4$$

is a square, say c^2. We have therefore shown that any triple of positive integers x, y, and z such that $x^4 + y^4 = z^2$ we can construct positive integers a, b, and c such that

$$a^4 + b^4 = c^2.$$

This finishes the construction of the function $f : A \to A$. Furthermore, the strict inequality $c^2 = s < s^2 + t^2 = z^2$ shows that $h(f(x, y, z)) < h(x, y, z)$, so we conclude by Theorem 12.1.2 (Method of Infinite Descent) that the set A must be empty. □

Corollary 12.3.2. *There is no solution to the equation*

$$x^4 + y^4 = z^4,$$

where x, y, and z are positive integers.

Proof. Given such a solution, set $a = x$, $b = y$, and $c = z^2$. Then we have

$$a^4 + b^4 = c^2,$$

which is impossible. □

12.4 Aubry's Theorem

The following theorem is due the the French winemaker and amateur mathematician Léon Aubry [AUB1912]. The idea of the proof is illustrated in Figure 12.1.

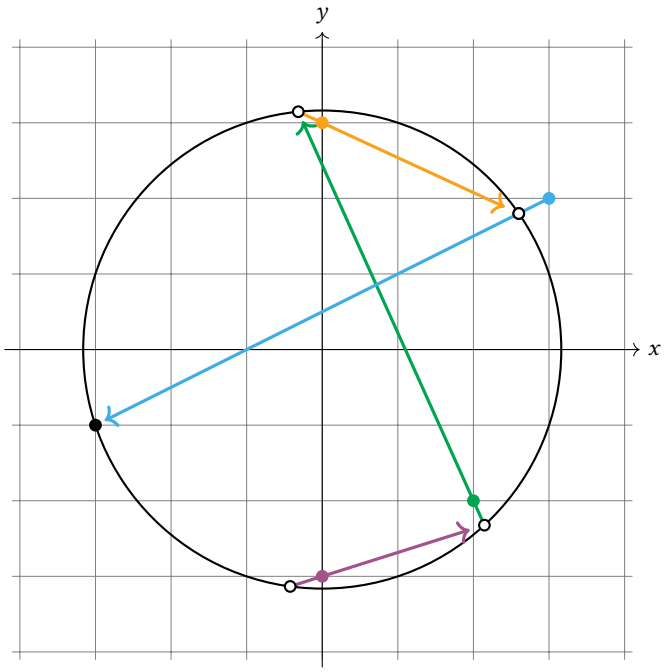


Figure 12.1: By repeated Vieta jumping between rational points on the circle of radius $\sqrt{10}$, we always reach a point with integer coordinates. The idea of the proof is that, starting from a rational point on the circle with radius $\sqrt{n}$, if we draw a line through it and the nearest point with integer coordinates, then we find a new point on the circle with smaller common denominator. Here, we started at the point $(-1401/3305, -10357/3305)$ on the circle with radius $\sqrt{10}$. The nearest point with integer coordinates is $(0, -3)$, and the line through it intersects the circle at $(1401/653, -1517/653)$. Its nearest point with integer coordinates is $(2, -2)$. Continuing this process leads to the sequence of points

$$\left(-\frac{1401}{3305}, -\frac{10357}{3305}\right) \mapsto \left(\frac{1401}{653}, -\frac{1517}{653}\right) \mapsto \left(-\frac{13}{41}, \frac{129}{41}\right) \mapsto \left(\frac{13}{5}, \frac{9}{5}\right) \mapsto (-3, -1),$$

at which the process terminates, since we have reached an integer point on the circle with radius $\sqrt{10}$.

THEOREM 12.4.1 (Aubry's Theorem). *For any natural number n, the following are equivalent:*

(i) *There are rational numbers x and y such that*

$$x^2 + y^2 = n.$$

(ii) *There are integers a and b such that*

$$a^2 + b^2 = n.$$

In the proof, it will be convenient to view pairs of rational numbers (x_1, x_2) as vectors. Recall that if $x = (x_1, x_2)$ and $y = (y_1, y_2)$ are vectors, then their *inner product* $x \cdot y$ is defined as

$$x \cdot y := x_1 y_1 + x_2 y_2.$$

In particular, $x \cdot x = x_1^2 + x_2^2$ is a sum of two squares, and the equation $x \cdot x = n$ tells us that the vector x lies on the circle with radius $\sqrt{n}$.

Proof. Consider two rational numbers x and y such that $x^2 + y^2 = n$, and let d be the least positive integer such that both dx and dy are integers; that is, d is the least common multiple of the denominators of x and y. If $d = 1$, then both x and y are integers, which implies that we can choose $a = x$ and $b = y$. For the remainder of the proof, we assume that $d > 1$.

We choose two integer vectors $q := (q_1, q_2)$ and $r := (r_1, r_2)$ such that

$$dx = dq_1 + r_1, \qquad dy = dq_2 + r_2, \qquad \text{and} \qquad |r_i| \le \frac{d}{2}.$$

In other words, we have chosen q and r such that

$$(x, y) = q + \frac{1}{d} r.$$

Observe that if $r_1 = 0$, then the equation $dx = dq_1$ implies that $x = q_1$, so we see that the rational number x is an integer if and only if $r_1 = 0$. Likewise, the rational number y is an integer if and only if $r_2 = 0$. Since we have assumed that $d > 1$, it follows that at least one of r_1 and r_2 is nonzero; that is, the vector r is nonzero.

Thus, (x, y) is one of the intersection points of the line $q + tr$ with the circle of radius $\sqrt{n}$. Both intersection points satisfies the equation

$$(r \cdot r)t^2 + 2(q \cdot r)t + (q \cdot q) - n = 0.$$

Recall that the vector r is nonzero, so we can divide through by $r \cdot r$:

$$t^2 + 2\frac{q \cdot r}{r \cdot r} t + \frac{q \cdot q - n}{r \cdot r} = 0.$$

Since we have one of the intersection points at $t = 1/d$, the other intersection point can now be found by the Vieta relations:

$$t = d\frac{q \cdot q - n}{r \cdot r}.$$

We conclude that the vector

$$w := q + d\frac{q \cdot q - n}{r \cdot r} r$$

lies on the circle with radius $\sqrt{n}$. It remains to show that the least positive integer e such that ew is a vector with integer coordinates satisfies $e < d$.

Here, we observe that the denominator $q \cdot q - n$ is an integer. So it suffices to show that $d \mid r \cdot r$, and that the integer

$$e := \frac{r \cdot r}{d}$$

satisfies $e < d$.

To see that $d \mid r \cdot r$, we observe that

$$d^2 n = (dx)^2 + (dy)^2 = (dq_1 + r_1)^2 + (dq_2 + r_2)^2 = d^2(q \cdot q) + 2d(q \cdot r) + (r \cdot r).$$

Since all the terms but the term $r \cdot r$ are divisible by d, it follows that $r \cdot r$ is divisible by d. Define e as suggested above. Then we have that

$$e = \frac{r \cdot r}{d} = \frac{r_1^2}{d} + \frac{r_2^2}{d} \leq \frac{d}{4} + \frac{d}{4} = \frac{d}{2} < d. \qquad \square$$

12.5 The Nonexistence of Four Squares in an Arithmetic Progression

We have shown in Theorem 11.6.2 that there is a bijective correspondence between arithmetic triples of squares and Pythagorean triples. It is natural to wonder whether there are any longer arithmetic progressions of squares. Fermat posed this problem in his correspondence with Bernard Frénicle de Bessy in 1640, and noted that it was impossible to find four such squares. The first publicly known proof is due to Euler. Here we will follow a proof of Alf van der Poorten [POO2007], who observed that any four pairwise relatively prime squares a^2, b^2, c^2, and d^2 in an arithmetic progression determine, besides the Pythagorean triples corresponding to (a^2, b^2, c^2) and (b^2, c^2, d^2), a third Pythagorean triple. To see this, assume that the common increment of the arithmetic progression (a^2, b^2, c^2, d^2) is a number of the form $2n$, where indeed it follows from Exercise 7.10 that n is divisible by 12, and let x be the average of b^2 and c^2 so that $b^2 = x - n$ and $c^2 = x + n$. Then the number $y := abcd$ satisfies

$$y^2 = a^2b^2c^2d^2 = (x - 3n)(x - n)(x + n)(x + 3n) = (x^2 - n^2)(x^2 - 9n^2).$$

Now we use the identity

$$XY + \left(\frac{X - Y}{2}\right)^2 = \left(\frac{X + Y}{2}\right)^2$$

with $X = x^2 - n^2$ and $Y = x^2 - 9n^2$ to obtain the Pythagorean triple

$$y^2 + (4n^2)^2 = (x^2 - 5n^2)^2.$$

Since a, b, c, and d are assumed to be relatively prime, the number y is relatively prime to $4n$ and thus to x and $x^2 - 5n^2$. This implies that our newly obtained Pythagorean triple is primitive. Crucially, the even leg of this new Pythagorean triple is a square, which allows us to extract two further Pythagorean triples that can be used to derive a contradiction.

Lemma 12.5.1. *For every four pairwise relatively prime squares a^2, b^2, c^2, and d^2 in an arithmetic progression we can uniquely determine a pair of relatively prime positive integers u and v such that $4u^2 + v^2$ and $u^2 + v^2$ are both squares, and the step size in the arithmetic progression of squares is $2uv$.*

Proof. Consider four pairwise relatively prime squares a^2, b^2, c^2, and d^2 in an arithmetic progression, where a, b, c, and d are assumed to be relatively prime numbers of the form $6k \pm 1$, and the step size is a number of the form $2n$ so that n is divisible by 12. As previously shown, we obtain a primitive Pythagorean triple

$$y^2 + (4n^2)^2 = (x^2 - 5n^2)^2,$$

where $y = abcd$ and x is the average of b^2 and c^2. Since the Pythagorean triple $(y, 4n^2, x)$ is primitive, there are relatively prime positive integers $2s$ and t such that

$$y = |t^2 - 4s^2|, \qquad 4n^2 = 4st, \qquad \text{and} \qquad x^2 - 5n^2 = t^2 + 4s^2.$$

Since $n^2 = st$ and s and t are relatively prime, it follows that $s = u^2$, $t = v^2$, and $uv = n$. We obtain that

$$\begin{aligned} y &= |v^4 - 4u^4|, \\ 4n^2 &= 4u^2v^2, \\ x^2 &= v^4 + 5u^2v^2 + 4u^4 = (4u^2 + v^2)(u^2 + v^2). \end{aligned}$$

Finally, we prove that the factors $4u^2 + v^2$ and $u^2 + v^2$ of x^2 are perfect squares by showing that $4u^2 + v^2$ and $u^2 + v^2$ are relatively prime for any two relatively prime integers u and v. To see this, note that any common divisor k of $4u^2 + v^2$ and $u^2 + v^2$ must satisfy the following divisiblity relations:

$$\begin{aligned} k \mid (4u^2 + v^2) - (u^2 + v^2) = 3u^2, \\ k \mid 4(u^2 + v^2) - (4u^2 + v^2) = 3v^2. \end{aligned}$$

Since u and v are relatively prime, these relations imply that $k \mid 3$. Moreover, observe that $u^2 + v^2$ is divisible by 3 if and only if both u and v are, since every perfect squares is congruent to 0 or 1 modulo 3. Since 3 does not divide both u and v by the assumption that u and v are relatively prime, we find that $k = 1$. □

The following lemma is an observation of Euler.



LEMMA 12.5.2. *There does not exist a pair of positive integers (u, v) such that both u^2+v^2 and $4u^2+v^2$ are perfect squares.*

PROOF. First, we observe that if such pair of positive integers exist, then the pair obtained by factoring out any common divisors is again of the same type. Thus, we may assume that u and v are relatively prime. Suppose that

$$u^2 + v^2 = \alpha^2 \qquad \text{and} \qquad 4u^2 + v^2 = \beta^2$$

By our assumption that u and v are relatively prime, it follows that (u, v, α) is a primitive Pythagorean triple.

As for the parity of u and v, there are two cases to consider: Either u is odd or u is even. Assuming the first case, so that u is odd and v is even, we can write $v = 2k$, so that

$$(2u)^2 + (2k)^2 = \beta^2.$$

Setting $\beta = 2\gamma$ and dividing this equation through by 4, we obtain the equations

$$u^2 + k^2 = \gamma^2, \qquad \text{and} \qquad u^2 + (2k)^2 = \alpha^2.$$

Observe that the first equation, with u being odd, implies that k is even. Thus we have reduced the first case to the second case. From now on, we assume that u is even, so that v is odd.

Setting $u = 2w$, we assume that w and v are relatively prime positive integers satisfying the equations

$$4w^2 + v^2 = \alpha^2 \qquad \text{and} \qquad 16w^2 + v^2 = \beta^2.$$

Under these assumptions, both $(2w, v, \alpha)$ and $(4w, v, \beta)$ are primitive Pythagorean triples. By Theorem 11.2.7 (Euclid's Parametrization of the Primitive Pythagorean Triples), there exist positive integers $s < t$ and $q < r$ such that

$$v = t^2 - s^2, \qquad v = r^2 - q^2,$$
$$2w = 2st, \qquad 4w = 2qr.$$

There are again two cases to consider, of which we will prove one and leave the other to the reader: Either q is even or r is even. In the first case, where $q = 2q'$ for some integer q', it follows that

$$st = w = q'r,$$

where $\gcd(s, t) = 1$ and $\gcd(q', r) = 1$. This implies that we can write $s = ab$, $t = cd$, $q' = ac$, and $r = bd$. The equations for v can now be written as follows:

$$c^2d^2 - a^2b^2 = v = b^2d^2 - 4a^2c^2.$$

Rearranging this equation, we see that $b^2(d^2 + a^2) = c^2(d^2 + 4a^2)$. Since a and d are relatively prime, it follows from the proof of Lemma 12.5.1 that $d^2 + a^2$ and $d^2 + 4a^2$ are relatively prime, and therefore both $d^2 + a^2$ and $d^2 + 4a^2$ are perfect squares. We have thus constructed a strictly smaller pair (a, d) of positive integers of the type of (u, v). By the method of infinite descent, we conclude that no such pair exists. □

Theorem 12.5.3 (Fermat–Euler). *Every arithmetic progression of length four of the integer squares is constant.*

Proof. We saw in Lemma 12.5.1 that if (a^2, b^2, c^2, d^2) is an arithmetic progression of integer squares with step size $2n$, then we can find relatively prime integers u and v such that $n = uv$ and both $4u^2 + v^2$ and $u^2 + v^2$ are perfect squares. However, we saw in Lemma 12.5.2 that there does not exist a pair of positive integers (u, v) such that both $4u^2 + v^2$ and $u^2 + v^2$ are perfect squares. Hence we conclude that any arithmetic progression of length four of integer squares must be constant. □

12.6 The Congruent Number Problem

Recall from §11.6 the challenge that Master John posed in the early 13th century to Leonardo Fibonacci: To find a rational number q such that both

$$q^2 - 5, \qquad \text{and} \qquad q^2 + 5$$

are both rational squares. Or equivalently, to find a Pythagorean triangle whose area is five times a square. Master John must somehow have known that the number 5 in his challenge was special: It is the smallest positive integer for which his challenge has a solution.

Definition 12.6.1. A **rational Pythagorean triple** is a triple (a, b, c) consisting of rational numbers satisfying

$$a^2 + b^2 = c^2,$$

corresponding to the sides and hypothenuse of a right triangle. A positive integer n is said to be a **congruent number** if there exists a rational Pythagorean triangle whose area is exactly n. That is, n is congruent if there exists a rational Pythagorean triple (a, b, c) such that

$$n = \frac{ab}{2}.$$

From Fibonacci's solution to Master John's challenge we thus conclude that 5 is a congruent number: The area of the rational right triangle with sides

$$a = \frac{3}{2}, \qquad b = \frac{20}{3}, \qquad \text{and} \qquad c = \frac{41}{6}.$$

is 5. The number 6 is also congruent since it is the area of the $(3, 4, 5)$-triangle. The following lemma rephrases the condition of being a congruent number in terms of Pythagorean triangles. Given the connection between Pythagorean triangles and arithmetic triples of squares, the concept of congruent number can be formulated in the following equivalent ways.

Lemma 12.6.2. *Consider a number n. The following are equivalent:*



(i) *The number n is congruent.*

(ii) *There is a primitive Pythagorean triple (a, b, c) whose area $\frac{1}{2}ab$ is n times a square.*

(iii) *There is an arithmetic triple of rational squares (x^2, y^2, z^2) with congruum n.*

(iv) *There is a primitive arithmetic triple of squares (a^2, b^2, c^2) whose congruum is n times a square.*

PROOF. Consider three rational numbers a, b, and c such that

$$a^2 + b^2 = c^2, \qquad \text{and} \qquad \frac{ab}{2} = n,$$

so that n is presented as the area of a right triangle with rational sides and hypotenuse. By multiplying a, b, and c with m, which we define to be the least common multiple of the denominators of a and b, we obtain integers $A := ma$, $B := mb$, and $C := mc$ such that

$$A^2 + B^2 = C^2, \qquad \text{and} \qquad \frac{AB}{2} = nm^2$$

so that (A, B, C) constitutes a Pythagorean triple whose area is n times a square. By dividing out any common divisors, we obtain a primitive such Pythagorean triangle. Since this process is clearly reversible, this proves that i is logically equivalent to ii. The fact that ii is logically equivalent to iii follows from Theorem 11.6.2. □

The previous theorem can be used to show that some numbers are not congruent. For example, the following theorem is merely a rephrasing of Fermat's Theorem 12.2.1, which states that the area of a Pythagorean theorem cannot be a square.

THEOREM 12.6.3. *No positive square integer is a congruent number.* □

We will show in the following theorem that the number 2 is not congruent. The noncongruence of the number 3 is stated as an exercise. Having the integers 1, 2, 3, and 4 ruled out as congruent numbers, we see indeed that 5 is the least congruent number.

THEOREM 12.6.4. *The number 2 is not congruent.*

PROOF. It suffices to show that there is no primitive Pythagorean triple (a, b, c) such that

$$\frac{1}{2}ab = 2d^2.$$

Using Theorem 11.2.7 (Euclid's Parametrization of the Primitive Pythagorean Triples), we suppose that there are relatively prime positive integers $s < t$ of opposite parity, such that

$$st(t^2 - s^2) = 2d^2.$$

We recall that s, t, $t - s$, and $t + s$ are all relatively prime. Since one of s and t is assumed to be even and the other odd, it follows that $t - s$ and $t + s$ are odd perfect squares. There are two cases to consider: we have either $s = 2u^2$ and $t = v^2$ or $s = u^2$ and

$t = 2v^2$. We will show that in the first case we can construct a smaller Pythagorean triple whose area is 2 times a perfect square. The argument we are about to give may also be applied to the second case, which we leave to the reader.

Consider integers u, v, x, and y such that

$$s = 2u^2, \qquad t = v^2, \qquad t - s = x^2, \qquad \text{and} \qquad t + s = y^2.$$

Then we define

$$a' := \frac{y - x}{2}, \qquad b' := \frac{y + x}{2}, \qquad \text{and} \qquad c' := v.$$

Then we have $a'^2 + b'^2 = t = v^2$, so that (a', b', c') is a Pythagorean triple satisfying the strict inequality $c' = v \leq t < c$. Furthermore, we have

$$\frac{1}{2}a'b' = \frac{(y - x)(y + x)}{8} = \frac{y^2 - x^2}{8} = \frac{2s}{8} = \frac{u^2}{2}.$$

Since the area of a Pythagorean triple is always an integer, it follows that u is even. It follows that $\frac{1}{2}a'b' = 2d'^2$ for some integer d'. We have thus constructed a strictly smaller Pythagorean triple whose area is twice a square, which is impossible by infinite descent. □

Using a very similar argument, we will also show that 3 is not congruent.

Theorem 12.6.5. *The number* 3 *is not congruent.*

Proof. It suffices to show that there is no primitive Pythagorean triple (a, b, c) such that

$$\frac{1}{2}ab = 3d^2.$$

Using Theorem 11.2.7 (Euclid's Parametrization of the Primitive Pythagorean Triples), we suppose that there are relatively prime positive integers $s < t$ of opposite parity, such that

$$st(t^2 - s^2) = 3d^2.$$

We recall that s, t, $t - s$, and $t + s$ are all relatively prime, so that exactly one of them is of the form $3k^2$ and the others are perfect squares not divisible by 3.

Suppose that $3 \nmid s$, so that s is a perfect square and hence we must have $s \equiv 1 \pmod 3$. Then the numbers $t - s$ and $t + s$ are incongruent modulo 3. Since the numbers $t - s$ and $t + s$ are either perfect squares or divisible by 3, we conclude that one of them is divisible by 3 and the other a perfect square $\equiv 1 \pmod 3$. It follows that t is also a perfect square $\equiv 1 \pmod 3$. However, this implies that $t + s \equiv 2 \pmod 3$, which is therefore neither a perfect square nor divisible by 3. We conclude from this contradiction that $3 \mid s$, and thus we have thus shown that there are integers u, v, x, and y such that

$$s = 3u^2, \qquad t = v^2, \qquad t - s = x^2, \qquad \text{and} \qquad t + s = y^2.$$



Now observe that $x^2 + y^2 = 2v^2$. Since x and y are relatively prime, it follows from this equation that both x and y are odd. Thus we define

$$a' := \frac{y-x}{2}, \qquad b' := \frac{y+x}{2}, \qquad \text{and} \qquad c' := v.$$

It follows that $a'^2 + b'^2 = v^2$, so that the triple (a', b', c') is again a Pythagorean triple. This triple satisfies the strict inequalities $c' = v < t < c$. Furthermore, we have

$$\frac{1}{2}a'b' = \frac{y^2 - x^2}{2} = \frac{(t+s) - (t-s)}{2} = s = 3u^2.$$

Thus we have constructed a strictly smaller Pythagorean triangle whose area is 3 times a square. By the method of infinite descent, we conclude that there cannot be any Pythagorean triangles whose area is 3 times a square. □

Having shown that the numbers 1, 2, 3, and 4 are not congruent, while the numbers 5 and 6 are congruent, we now focus on proving that 7 is congruent. Before we do so, we will reformulate the condition of n being congruent to an equivalent condition.

Suppose we are given the task of showing that a positive integer n is a congruent number. In order to construct a Pythagorean triangle with rational sides and hypotenuse, we observe that any such Pythagorean triangle can be obtained by scaling with a rational factor a Pythagorean triangle described by a rational point on the unit circle. Using the stereographic projection of Theorem 11.4.2, we see that all rational Pythagorean triangles are described by pairs

$$\left(\frac{r(1-m^2)}{1+m^2}, \frac{2rm}{1+m^2}\right),$$

where r and m are rational numbers. A simpler parametrization of all rational Pythagorean triangles can be obtained by substituting $s = r/(1+m^2)$:

$$(s(1-m^2), 2sm).$$

Thus, our task is to find rational numbers s and m satisfying $n = s^2 m(1-m^2)$, which is equivalent to

$$\frac{n^4}{s^2} = n^3 m - (nm)^3.$$

Substituting $x = -nm$ and $y = n^2/s$ in this equation, we find that our original problem is equivalent to finding a rational solution to the problem

$$y^2 = x^3 - n^2 x.$$

We have thus proven the following theorem:

THEOREM 12.6.6. *Consider a number n. The following are equivalent:*

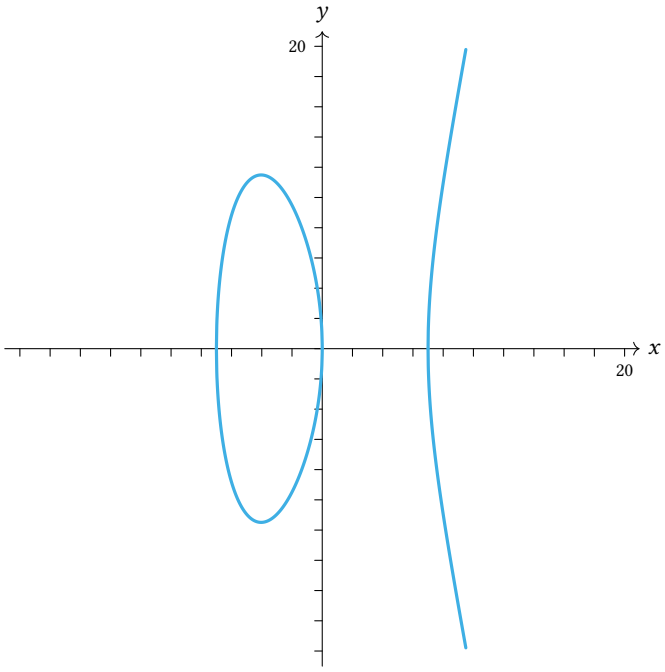


Figure 12.2: The curve $y^2 = x^3 - 49x$.

(i) *The number n is congruent.*

(ii) *There is a rational solution to the equation*

$$y^2 = x^3 - n^2 x$$

such that $y \neq 0$.

Example 12.6.7. The number 7 is a congruent number. We will prove this by finding an integer solution to the Diophantine equation

$$y^2 = x^3 - 49x.$$

We emphasize that the problem of proving that 7 is congruent is equivalent to showing the existence of a *rational* solution to the above equation. Nevertheless, luck turns out to be on our side in this special case and an integer solution can be found.

Note that if $x^3 - 49x$ is a square, then $7 \nmid x$. Indeed, if 7 were to divide x, we would have an integer solution to $y^2 = x^3 - x$ with $y \neq 0$, showing that 1 is a congruent number. It follows that x and $x^2 - 49$ are relatively prime. Consequently, in order for $x^3 - 49x$ to be a square, we need x and $x^2 - 49$ to be perfect squares. Set

$$x := u^2 \qquad \text{and} \qquad x^2 - 49 := v^2.$$

Then we have $u^4 - v^2 = 49$, which we can rewrite as $(u^2 - v)(u^2 + v) = 49$. Since $49 = 7^2$, this implies that $u^2 - v = 1$ and $u^2 + v = 49$. We find that

$$2v = (u^2 + v) - (u^2 - v) = 48$$

so that $v = 24$. Furthermore, since $u^2 - 24 = 1$, we find that $u = 5$. It follows that

$$120^2 = 25^3 - 49 \cdot 25.$$

Determining which numbers are congruent turns out to be an incredibly difficult problem, which is still unsolved. This problem is called the *congruent number problem*, and via Tunnell's theorem it has connections to the famous Birch and Swinnerton-Dyer conjecture.

Exercises

Starter Exercises

12.1 Use the method of infinite descent to show that there are no integer solutions to the equation

$$x^2 + y^2 = 3t^2$$

such that $t > 0$.

12.2 Let x and y be positive integers satisfying the equation

$$x^2 - xy + y^2 = 1.$$

(a) Use the discriminant $y^2 - 4(y^2 - 1)$ to give a direct proof that the only solution is $x = y = 1$.

(b) Find a second proof by Vieta jumping that $x = y = 1$.

Routine-Building Exercises

12.3 Use the method of infinite descent to show that if a and b are relatively prime and the product ab is a square, then both a and b are squares.

12.4 Show that there are no positive integer squares of the form

$$2x^2 + 2xy + 2y^2.$$

12.5 Use the method of infinite descent to show that there are no integer solutions to the equation

$$x^2 + y^2 + z^2 = 7t^2$$

such that $t > 0$.

12.6 Prove that the area of a Pythagorean triangle cannot be twice a square.

12.7 Consider a natural number n. Use a descent construction similar to that in Theorem 12.4.1 (Aubry's Theorem) to show that the equation

$$x^2 + 2y^2 = n$$

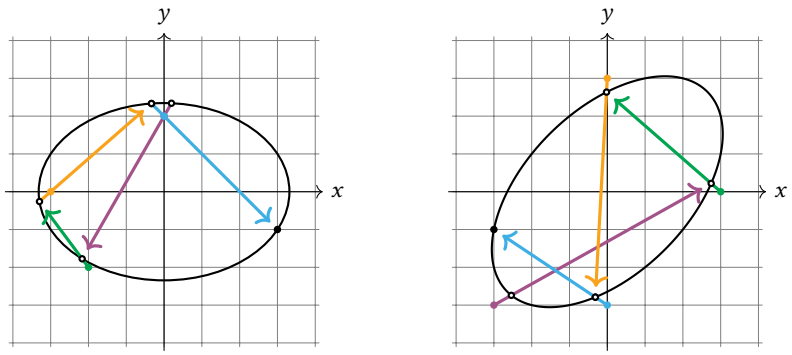
has a solution in the rational numbers if and only if it has a solution in the integers. See Figure 12.2 (a) for an illustration.

12.8 Consider a natural number n. Use a descent construction similar to that in Theorem 12.4.1 (Aubry's Theorem) to show that the equation

$$x^2 - xy + y^2 = n$$

has a solution in the rational numbers if and only if it has a solution in the integers. See Figure 12.3 (b) for an illustration.





(a) (b)

Figure 12.3: On each of the curves (a) $x^2 + 2y^2 = 11$ and (b) $x^2 - xy + y^2 = 7$, by repeated Vieta jumping between rational points we eventually reach a point with integer coordinates.
In case (a), we started with the point $(151/771, 1805/771)$. The sequence of rational points obtained by Vieta jumping is in this case:

$$\left(\frac{151}{771}, \frac{1805}{771}\right) \mapsto \left(-\frac{453}{209}, -\frac{371}{209}\right) \mapsto \left(-\frac{89}{27}, -\frac{7}{27}\right) \mapsto \left(-\frac{1}{3}, \frac{7}{3}\right) \mapsto (3, -1).$$

In case (b), we started with the point $(-14334/5647, -15481/5647)$. The sequence of rational points obtained by Vieta jumping is in this case:

$$\left(-\frac{14334}{5647}, -\frac{15481}{5647}\right) \mapsto \left(\frac{2493}{907}, \frac{199}{907}\right) \mapsto \left(-\frac{3}{151}, \frac{398}{151}\right) \mapsto \left(-\frac{6}{19}, -\frac{53}{19}\right) \mapsto (-3, -1).$$

There are 8 binary quadratic forms and a total of 70 quadratic forms (with up to 8 variables) to which this argument applies [NEB2003]. Such quadratic forms are called *positive definite Euclidean*.

Challenge Exercises

12.9 Prove that the Diophantine equation

$$x^4 - y^4 = z^2$$

has no solutions in the positive integers.

12.10 Show that if x and y are positive integers such that xy divides $x^2 + y^2 + 1$, then

$$\frac{x^2 + y^2 + 1}{xy} = 3.$$

12.11 Let x, y, and z be positive integers such that $xy + yz + zx$ divides $x^2 + y^2 + z^2$. Prove that

$$\frac{x^2 + y^2 + z^2}{xy + yz + zx}$$

is a perfect square.

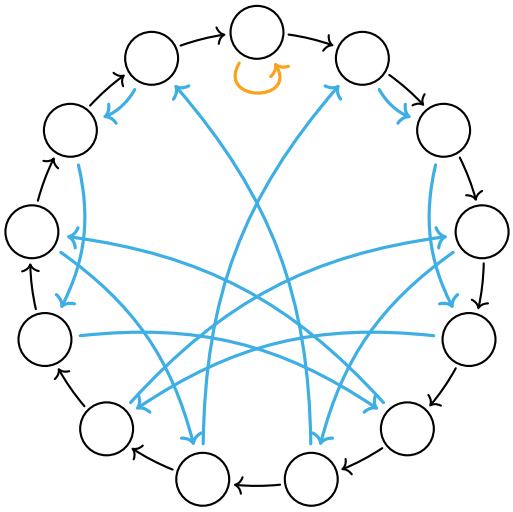
12.12 Show that the only triangular number which is also a fourth power is 1.

12.13 Show that the equation

$$x^4 - x^2y^2 + y^4 = z^2$$

has no solutions in the positive integers.





Book II

The Multiplicative Nature of Numbers

Chapter 13

Prime Numbers

13.1 The Fundamental Theorem of Arithmetic

Definition 13.1.1. An integer a is said to be **prime** if it has exactly one positive proper divisor. Any integer $a \neq \pm 1$ that is not prime is said to be a **composite number**.

The numbers 0 and 1 are not prime. To see that 0 isn't prime, simply note that any positive integer is a proper divisor of 0. To see that 1 isn't prime, note that 1 doesn't have any proper divisors. Indeed, it has exactly one positive divisor, namely 1 itself, but this divisor isn't proper. We also note that if $a > 1$ is prime, then the number 1 is always a positive proper divisor. Thus we see that $a > 1$ is prime if and only if the number 1 is its unique positive proper divisor. We note that older literature often uses the name *aliquot divisors* for what we have called proper divisors.

To see that the number 2 is prime, note that its positive divisors are a subset of the set $\{1, 2\}$ consisting of all the positive integers below 2. Its proper divisors are therefore a subset of $\{1\}$. The integer 1 is indeed a positive divisor, so we see that 2 has exactly one positive proper divisor.

To see that the number 3 is prime, note that its positive divisors are a subset of the set $\{1, 2, 3\}$ consisting of all positive integers below 3. The number 1 is a proper divisor, the number 2 doesn't divide 3, and 3 itself is a divisor but it isn't proper. Therefore we see that the number 3 has exactly one positive proper divisor.

The number 4 isn't prime, because the numbers 1 and 2 are two distinct proper divisors of 4. This process of finding all primes up to a desired bound is formalized in the **sieve of Eratosthenes**, which we will now describe. Figure 13.1 displays the sieve of Eratosthenes up to 1120.

The sieve of Eratosthenes is an iterative process that generates at stage n a set P_n



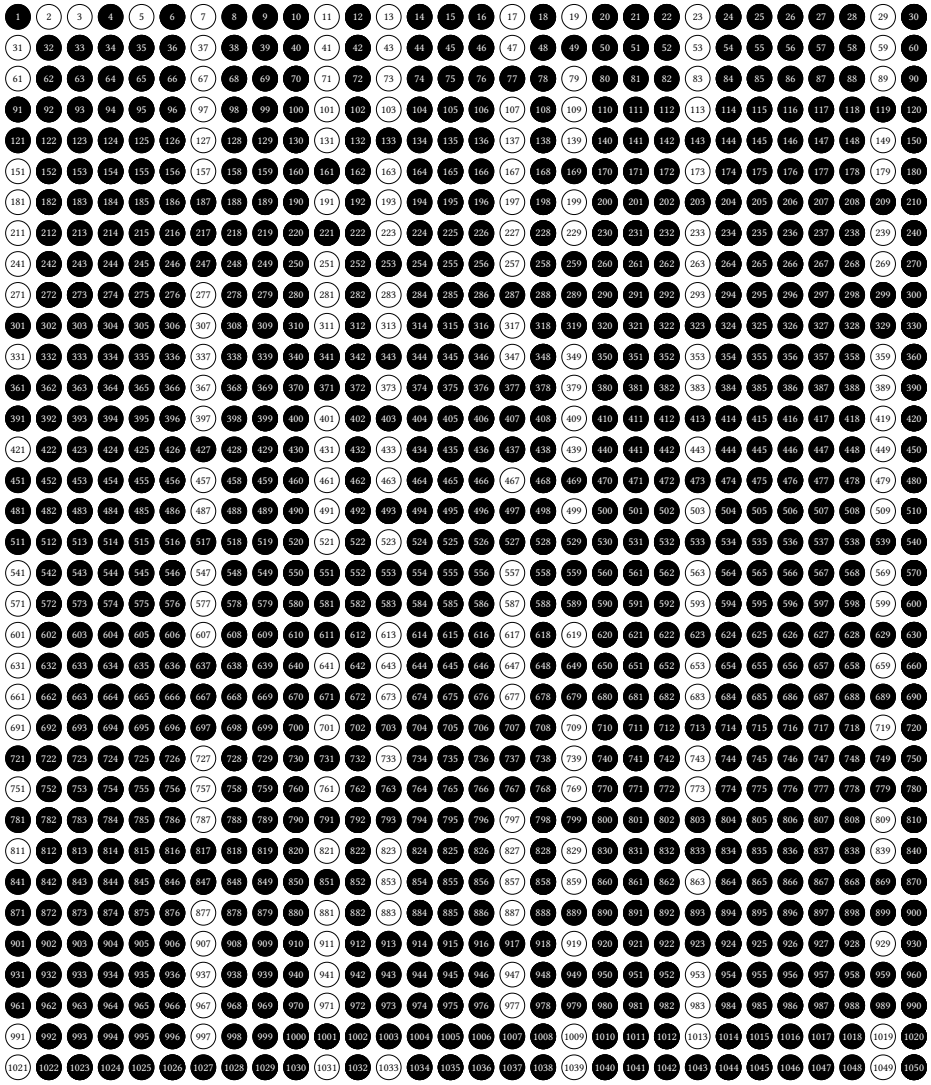


Figure 13.1: The sieve of Eratosthenes up to 1050: The number 1 and every composite number are marked in black, leaving just the primes in white circles.

of numbers known to be prime at stage n, and a set Q_n of prime candidates. In other words, the sets P_n form an increasing sequence

$$P_0 \subseteq P_1 \subseteq P_2 \subseteq \cdots$$

of sets of numbers known to be prime, where at each higher stage the set of known primes becomes larger, and the sets Q_n form a decreasing sequence

$$Q_0 \supseteq Q_1 \supseteq Q_2 \supseteq \cdots$$

of candidates, from which we pick our next prime. We will define the sets P_n and Q_n by a recursive process. Initially, the set P_0 is empty and $Q_0 = \{n \in \mathbb{N} \mid n \geq 2\}$ is the set of all numbers ≥ 2. Now we define P_{n+1} to be $P_n \cup \{p(n)\}$, where $p(n) := \min(Q_n)$, and we define

$$Q_{n+1} := Q_n \setminus \{kp(n) \mid k \geq 1\}.$$

In other words, the nth prime $p(n)$ is the minimal element of $Q(n)$, and the set Q_{n+1} of candidates is the set Q_n minus all the multiples of $p(n)$. In the first five stages, these sets look as follows:

n	P_n	Q_n
0	$\emptyset$	$\{2, 3, 4, 5, 6, 7, 8, \ldots\}$
1	$\{2\}$	$\{3, 5, 7, 9, 11, 13, 15, \ldots\}$
2	$\{2, 3\}$	$\{5, 7, 11, 13, 17, 19, 23, \ldots\}$
3	$\{2, 3, 5\}$	$\{7, 11, 13, 17, 19, 23, 29, \ldots\}$
4	$\{2, 3, 5, 7\}$	$\{11, 13, 17, 19, 23, 29, 31, \ldots\}$
5	$\{2, 3, 5, 7, 11\}$	$\{13, 17, 19, 23, 29, 31, 37, \ldots\}$

Notice that not only the minimal element of Q_n is prime, but every element $q \in Q_n$ such that $q < (\max(P_n))^2$ is prime. This is because if $q < (\max(P_n))^2$ is composite, then its lowest factor must be a prime number $p < \max(P_n)$, i.e., it must be a prime number in P_n. However, all the multiples of the primes in P_n have been removed from Q_n, so there are no such composite numbers.

We can use this observation to obtain the list of all primes below 100, at stage 5 in the sieve of Eratosthenes. The list of primes below 100 is

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

The sieve of Eratosthenes either terminates, i.e., it reaches a stage for which Q_n is empty, or there are infinitely many primes. We will now show that there are infinitely many primes. In the following lemma we use the concept of **nontrivial divisors**, which are divisors d of a natural number n such that $d \neq 1$. The concept of nontrivial divisors should not be confused with the concept of proper divisors, which are divisors d of a natural number n such that $d \neq n$.



THEOREM 13.1.2. *Any natural number $n > 1$ has a least nontrivial divisor, and this divisor is prime.*

PROOF. Suppose that $n > 1$. Then the set of nontrivial divisors $d \neq 1$ of n contains the number n, so it has a least element p by Theorem 5.2.1 (The Well-Ordering Principle of the Natural Numbers) of the natural numbers. Then the set of divisors of p itself is the set $\{1, p\}$, because any divisor of p also divides n, and p is assumed to be the least nontrivial divisor. This shows that p has exactly one proper divisor, and therefore p is prime. □

The following proposition is due to Euclid, who has included it as proposition 30 of book VII of the *Elements*.

LEMMA 13.1.3. *Suppose that p is prime, and that a is an integer. Then either $p \mid a$ or* $\gcd(p, a) = 1$.

PROOF. The greatest common divisor of p and a is in particular a divisor of p, so it is either 1 or p. If $\gcd(p, a) = p$, then we have $p \mid a$. □

PROPOSITION 13.1.4. *Consider a positive integer a. The following are equivalent:*

(i) *The integer a is prime.*

(ii) *We have $a > 1$, and for any two integers b and c such that $a \mid bc$, we have that $a \mid b$ or $a \mid c$.*

PROOF. Suppose first that a is prime. Since 0 and 1 aren't prime, it follows that $a > 1$. Now consider two integers b and c such that $a \mid bc$. There are two cases to consider: either $a \mid b$, in which case we are done immediately, or $a \nmid b$. In the case where $a \nmid b$, it follows from Lemma 13.1.3 that a and b are relatively prime. This allows us to apply Proposition 7.1.5, by which we conclude that $a \mid c$.

For the converse, suppose that for any two integers b and c such that $a \mid bc$, we have $a \mid b$ or $a \mid c$, and let d be a proper divisor of a. Now consider any positive proper divisor d of a, and write $a = dk$. Then it follows in particular that $a \mid dk$, so by assumption we have either $a \mid d$ or $a \mid k$. The first condition can be ruled out, because d is assumed to be a proper divisor and therefore $a \nmid d$. Thus we find ourselves in the second case, where $a \mid k$ and $k \mid a$. The integer k is also positive, since a and d are positive, so it follows that $a = k$. This implies that $d = 1$, and hence we conclude that a is prime. □

The fundamental theorem of arithmetic asserts that every positive integer can be written uniquely, up to reordering, as a product of primes. Gauss is often credited for being the first to state this fact as a theorem. He did so in Article 16 of his *Disquisitiones Arithmeticae* [GAU1986], where he has mentioned that prior authors often assumed it or gave inadequate reasons for its truth.

Theorem 13.1.5. *For any natural number $n > 0$, there is a unique list $\ell = (p_0, \dots, p_{l-1})$ of length l, consisting of primes $p_0 \leq p_1 \leq \cdots \leq p_{l-1}$ such that*

$$n = \prod_{i=0}^{l-1} p_i.$$

This unique list of primes is called the ***prime decomposition of*** *n.*

Proof. We apply strong induction on n, with base case 1. In the base case, we let ℓ be the empty list. The empty list satisfies the increasing primes condition vacuously, and empty products are 1 by definition, so the empty list is indeed a prime decomposition of 1.

For the inductive step, recall that any natural number $n + 1 > 1$ has a least prime divisor. If p is the least prime divisor of $n + 1$, then it follows that $(n + 1)/p \leq n$. By the strong induction hypothesis we have a unique prime decomposition $(q_0, \dots, q_{l-1})$ of $(n + 1)/p$. Now define the list $\ell := (p_0, p_1, \dots, p_l)$ by $p_0 := p$ and $p_{i+1} := q_i$. Then each p_i is a prime divisor of $n + 1$, and since p_0 is the least prime divisor of $n + 1$ we have the inequalities

$$p_0 \leq p_1 \leq \cdots \leq p_l.$$

Furthermore, we have

$$n + 1 = p \cdot ((n + 1)/p) = p_0 \cdot \prod_{i=1}^{l} p_i = \prod_{i=0}^{l} p_i.$$

This proves that the prime decomposition of $n + 1$ exists.

To show that the prime decomposition of $n + 1$ is unique, let $(r_0, \cdots, r_k)$ be a prime decomposition of $n + 1$. The smallest prime divisor p of $n + 1$ then divides the product

$$p \mid \prod_{i=0}^{k} r_i.$$

This implies that $p \mid r_i$ for some $0 \leq i \leq k$, i.e., that $p = r_i$. However, p is assumed to be the smallest prime factor of $n + 1$, so it follows that $p = r_0$. Now it follows that $(r_1, \dots, r_k)$ is a prime decomposition of $(n + 1)/p$, which is unique, and therefore we conclude that $n + 1$ has a unique prime factorization. □

Corollary 13.1.6. *For any positive integer n with prime factorization $n = p_1^{m_1} \cdots p_k^{m_k}$, the map*

$$x \mapsto \left(x \mod p_1^{m_1}, \dots, x \mod p_k^{m_k}\right)$$

is a bijection

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_k \mathbb{Z}/p_k^{m_k}\mathbb{Z}.$$

REMARK 13.1.7. Although the prime factorization of arbitrary large numbers can be an arduous task, numbers of special forms can sometimes be factorized more easily. For instance, using the formula for the difference of squares we see that

$$\begin{aligned} 2^{16} - 1 &= (2^8 - 1)(2^8 + 1) \\ &= (2^4 - 1)(2^4 + 1)(2^8 + 1) \\ &= (2^2 - 1)(2^2 + 1)(2^4 + 1)(2^8 + 1) \\ &= 3 \cdot 5 \cdot 17 \cdot 257. \end{aligned}$$

Even though $2^{16} - 1 = 65535$ is a fairly large number, finding its prime factorization was fairly effortless.

13.2 The Infinitude of Primes

13.2.1 Euclid's Proof

The theorem asserting the infinitude of primes asserts that no finite set of primes is the set of all primes. Many proofs of the infinitude of primes require the following lemma:

LEMMA 13.2.1. *If a and b are relatively prime integers, then any prime divisors of a are distinct from any prime divisors of b.*

PROOF. Suppose that a and b are relatively prime, and that p and q are prime divisors of a and b, respectively. By the assumption that a and b are relatively prime, it follows that $p \nmid b$ and that $q \nmid a$. Therefore it follows that p and q cannot be the same. □

THEOREM 13.2.2. *There are infinitely many prime numbers.*

EUCLID'S PROOF OF THEOREM 13.2.2. We will prove that there are infinitely many prime numbers by showing that for any finite set of prime numbers, there is a prime number not belonging to the finite set.

Consider a finite set $\{p_0, \dots, p_k\}$ of primes, and define

$$n := 1 + \prod_{i=0}^{k} p_i.$$

Then there exists, for each $0 \leq i \leq k$, a natural number q_i such that $n = q_i p_i + 1$. Indeed, we can simply define

$$q_i := \prod_{j=0, j \neq i}^{k} p_j.$$

Since n can be written in this way, it follows that n is relatively prime to each p_i. Consequently, the least prime divisor of n is relatively prime to each p_i. In other words, the least prime divisor of n is not in the set of primes $\{p_0, \dots, p_k\}$. □

13.2.2 Saidak's Proof

There are many proofs of the infinitude of primes. The following is due to Filip Saidak [Sai2006], who has published his proof in 2006, based on the idea that if $n = ab$ is the product of two numbers that are relatively prime and both at least 2, then n must have two prime factors.

Saidak's proof of Theorem 13.2.2. Let $N_0 := 1$, and define

$$N_{n+1} := N_n(N_n + 1).$$

We claim that N_n has at least n prime factors. In the base case, we note that it is indeed true that 1 has at least zero prime factors. For the inductive step, suppose that N_n has at least n prime factors. The number $N_n + 1$ is relatively prime to N_n, so its prime factors are all distinct from the prime factors of N_n. Furthermore, we have $1 < N_n + 1$, so $N_n + 1$ indeed has at least one prime factor. Thus it follows that N_{n+1} has at least $n + 1$ prime factors, and therefore there must be infinitely many primes. □

13.2.3 Furstenberg's Proof, Following Cass–Wildenberg

The following proof of the infinitude of primes is, in its essence, due to Hillel Furstenberg [Fur1955]. In its original formulation, this proof makes clever use of a topology on $\mathbb{Z}$. Although topologies are not hard to define, motivating them is beyond the scope of this course. We will therefore present a revised version of Furstenberg's proof, following Daniel Cass and Gerald Wildenberg [CW2003].

The Cass–Wildenberg approach to prove the infinitude of primes makes use of the concept of a periodic subset of $\mathbb{Z}$. A subset $A \subseteq \mathbb{Z}$ is said to be **periodic with period** n, or simply **periodic** if we merely assume such a natural number n to exist, if we have

$$x \in A \quad \Leftrightarrow \quad x + n \in A.$$

Thus, if A is a periodic subset of $\mathbb{Z}$ with period n, and $x \in A$, then

$$x + kn \in A$$

for all $k \in \mathbb{Z}$. In particular, all inhabited periodic subsets of $\mathbb{Z}$ are infinite. We note two basic facts about periodic subsets of $\mathbb{Z}$, which we leave to the reader to verify:

(i) If $A_1, \ldots, A_m$ is a finite family of periodic subsets of $\mathbb{Z}$, each with their own periods, then the union

$$A_1 \cup \cdots \cup A_m$$

is again a periodic subset of $\mathbb{Z}$. The period of the union is the least common multiple of the periods of the subsets A_i.

(ii) If A is a periodic subset of $\mathbb{Z}$, then its complement $A^c := \{x \in \mathbb{Z} \mid x \notin A\}$ is periodic with the same period.



FURSTENBERG'S PROOF OF THEOREM 13.2.2, FOLLOWING CASS–WILDENBERG. Consider the subsets

$$S_p := \{kp \mid k \in \mathbb{Z}\},$$

where p is a prime number, and define

$$S := \bigcup_{p \text{ prime}} S_p.$$

Since every integer besides ± 1 is divisible by a prime, it follows that S consists of all the integers besides ± 1. The complement of S is therefore the set $\{-1, 1\}$. Note that the subset $\{-1, 1\}$ of $\mathbb{Z}$ cannot be periodic, since is inhabited and finite. This allows us to conclude that the subset S of $\mathbb{Z}$ is not periodic. However, if there were only finitely many primes, then S would be periodic because it would be a finite union of periodic subsets of $\mathbb{Z}$. Thus we conclude that there must be infinitely many primes. □

13.2.4 Erdős's Proof

DEFINITION 13.2.3. A natural number n is said to be **square-free** if the only square dividing n is 1. In other words, n is square-free if

$$k^2 \mid n \quad \Rightarrow \quad k = 1$$

for every natural number k.

By Theorem 13.1.5 (The Fundamental Theorem of Arithmetic) it follows that square-free numbers are those numbers of which the prime decomposition

$$n = p_1 \cdots p_n$$

is a product of distinct primes. In particular, if n is square free then the exponents in the prime factorization of n do not exceed 1. For instance, the numbers $3 \cdot 5 \cdot 17$ and $2 \cdot 11 \cdot 37$ are square-free, while the numbers $3^3 \cdot 5 \cdot 31$ and $2^5 \cdot 5^{11} \cdot 61$ aren't.

THEOREM 13.2.4. *Every natural number n can be written uniquely in the form*

$$n = k^2 m,$$

*where m is a square-free number. This is called the **square-free decomposition** of n, and the number m is called the **square-free part** of n.*

PROOF. Consider the set of natural numbers

$$S := \{d \in \mathbb{N} \mid \text{There exists a } k \in \mathbb{N} \text{ such that } k^2 d = n\}.$$

Clearly, this set contains the element n itself, since $n/n = 1$ is a perfect square. By Theorem 5.2.1 (The Well-Ordering Principle of the Natural Numbers), it follows that

S has a least element, which we call m. By definition, n/m is a perfect square, so there is a natural number k such that

$$n = k^2 m.$$

Next, we need to show that m is square-free. Suppose $d^2 \mid m$ is a positive divisor of m. Then the quotient $q = m/d^2$ is a divisor of n such that n/q is the perfect square $(kd)^2$. Since $q \leq m$ it follows by minimality that $q = m$ and hence that $d^2 = 1$. This implies that $d = 1$.

To finish the proof, we need to show that the square-free decomposition of n is unique. To this end, suppose that $n = l^2 d$, where d is square-free. We claim that any prime divisor of k is a prime divisor of l and conversely that any prime divisor of l is a prime divisor of k. To see this, note that for any prime $p \mid k$ we have $p^2 \mid k^2$ and consequently $p^2 \mid l^2 d$. Since d is square-free, this implies that $p \mid l^2$ and hence that $p \mid l$. The same argument applies the other way around, so it follows that $k = l$ and consequently $m = d$. □

Now that we have established that every natural number has a unique square-free decomposition, we are able to give Erdős's proof of the infinitude of primes. This proof was originally published in [Erd1938].

Erdős's proof of Theorem 13.2.2. Consider a finite list of primes $p_1, \dots, p_n$. We claim that for any x, there are at most

$$\sqrt{x} 2^n$$

numbers below x with all prime factors from the list $p_1, \dots, p_n$. To see this, recall from Theorem 13.2.4 that any number can be written in the form $k^2 m$ where m is square free. Then we have $k \leq \sqrt{x}$, leaving at most $\sqrt{x}$ choices for the number k. Furthermore, there are only 2^n square-free numbers m whose prime factors are from the list $p_1, \dots, p_n$, leaving at most 2^n choices for the value of m.

If all the numbers below x are products of powers of primes from the list $p_1, \dots, p_n$, we find that $x \leq \sqrt{x} 2^n$, or equivalently that

$$\sqrt{x} \leq 2^n.$$

However, this inequality clearly fails when x exceeds 2^{2n}, so there must be primes other than $p_1, \dots, p_n$. □

13.2.5 A Proof via the Stars-and-Bars Method

In Theorem 3.7.2 we have shown that the number of n-tuples $(m_1, \dots, m_n)$ such that $m_1 + \cdots + m_n = k$ is

$$\binom{k+n-1}{n-1}.$$



Making use of Theorem 13.1.5 (The Fundamental Theorem of Arithmetic), we consequently find that for any list $p_1, \dots, p_n$ of distinct primes there are $\binom{k+n-1}{n}$ distinct natural numbers that can be written in the form

$$p_1^{m_1} \cdots p_n^{m_n},$$

where $m_1 + \cdots + m_n = k$. Furthermore, there are $\binom{k+n}{n}$ distinct numbers that can be written in the form

$$p_1^{m_1} \cdots p_n^{m_n},$$

where $m_1 + \cdots + m_n \leq k$. We will use this observation to obtain a bound on numbers N such that the prime factors of all positive integers $\leq N$ are among the primes $p_1, \dots, p_n$, which yields another proof of the infinitude of primes.

PROOF OF THEOREM 13.2.2. Consider a set $p_1, \dots, p_n$ of distinct primes, where $n \geq 5$, and let N be such that all the numbers $1 \leq x \leq N$ can be written as products of the primes $p_1, \dots, p_n$.

For any $x = p_1^{m_1} \cdots p_n^{m_n} \leq N$, we have $2^{m_1 + \cdots + m_n} \leq x \leq N$, so that

$$m_1 + \cdots + m_n \leq \log_2 N.$$

The set of ordered tuples $(m_1, \dots, m_n)$ with sum $\leq \log_2$ is in bijection with the set of ordered tuples $(m_0, \dots, m_n)$ satisfying

$$m_0 + m_1 + \cdots + m_n = \log_2 N.$$

The number of such ordered $(n+1)$-tuples is determined in Theorem 3.7.2, by which it follows that

$$N \leq \binom{\lfloor \log_2 N \rfloor + n}{n} \leq \frac{(\log_2 N + n)^n}{n!} \leq (\log_2 N + n)^n$$

Note that if $p_1, \dots, p_n$ were indeed a list of all the primes, then N would always satisfy this inequality. It remains to find a number N for which this inequality fails. We are permitted to pick a large number of a suitable form so as to reach a quick contradiction. Let us choose $N = 2^{2^n}$. Then we have

$$2^{2^n} \leq (2^n + n)^n < (2^n + 2^n)^n = 2^{n(n+1)}.$$

Now observe that for $n \geq 5$, as we have assumed at the start of the proof, we have $n(n+1) < 2^n$, which shows that $2^{n(n+1)} < 2^{2^n}$. Thus we have reached a contradiction, and we conclude that there must be infinitely many primes. □

13.3 Fermat Primes

During the 17th century, when computational resources were limited to human cognitive capacity aided with pen and paper, it was a significant challenge to come up with

large prime numbers. The hunt for large primes was focused primes of the form $2^n - 1$ and $2^n + 1$, since such numbers have a simple form yet grow very fast. Fermat observed that if $2^n + 1$ is a prime, then n cannot have any odd divisors.

Theorem 13.3.1. *If a number of the form $2^n + 1$ is prime, then $n = 2^k$ for some natural number k.*

Proof. Write $n = 2^k m$, where m is odd. Recall that when m is odd, then we have the following algebraic identity:

$$a^m + b^m = (a + b) \sum_{i=0}^{m-1} (-1)^i a^i b^{m-i-1}$$

By this formula for the sum of odd powers, we obtain the factorization

$$2^{2^k m} + 1 = (2^{2^k})^m + 1 = (2^{2^k} + 1) \sum_{i=0}^{m-1} (-1)^i 2^{2^k i}.$$

Thus, if $2^{2^k m} + 1$ is prime, then we must have $m = 1$. □

In other words, all primes of the form $2^n + 1$ are in fact of the form $2^{2^k} + 1$. Such numbers are called **Fermat numbers**: The nth Fermat number is given by

$$F_n := 2^{2^n} + 1.$$

The first few Fermat numbers are:

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65537.$$

Of these numbers, F_0 through F_3 are easily seen to be prime. The number F_4 is also prime, but to prove this in a clean manner requires us to develop some more theory. Fermat famously conjectured that all Fermat numbers are prime. Goldbach brought this claim to Euler's attention in his letter, who was sceptical. A little later, Euler was able to prove that F_5 is indeed composite. Fermat had an extremely strong record of correct mathematical claims and conjectures, but this was one of the very few he got wrong. We will prove in Corollaries 16.1.5 and 16.1.6 that F_4 is prime and that F_5 is composite, once we have developed a bit more theory to help us reduce the search for prime factors.

Our next proof of the infinitude of primes is due to Goldbach, from 1730. In the 18th century, it was customary among mathematicians to share their findings private correspondences. In July of 1730, Goldbach wrote a letter to Euler, in which he established that all distinct Fermat numbers are relatively prime, and that hence there must be infinitely many primes. Recall that the Fermat numbers F_n are defined by

$$F_n := 2^{2^n} + 1.$$



THEOREM 13.3.2 (Product formula for the Fermat numbers). *The nth Fermat number satisfies the identity*

$$F_n - 2 = \prod_{0 \le k < n} F_k.$$

PROOF. We will prove the claim by strong induction. In the base case, we have

$$F_0 - 2 = 2^{2^0} - 1 = 1 = \prod_{0 \le k < 0} F_k,$$

since the product on the right-hand side is empty.

For the inductive step, we use the formula for the difference of squares:

$$(F_{n+1} - 2) = 2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1) = F_n \cdot \prod_{0 \le k < n} F_k = \prod_{0 \le k < n+1} F_k. \qquad \square$$

THEOREM 13.3.3 (Goldbach's Theorem). *Any two distinct Fermat numbers are relatively prime.*

PROOF. Consider two distinct natural numbers m and n, and assume that $m < n$. Using Theorem 13.3.2 (Product formula for the Fermat numbers), we see that $F_m \mid F_n - 2$. It follows that any common divisor d of F_m and F_n is also a divisor of 2, i.e., $d = 1$ or $d = 2$. However, all Fermat numbers are clearly odd, and this implies that any common divisor of F_m and F_n is 1. In other words, F_m and F_n are relatively prime. $\square$

GOLDBACH'S PROOF OF THEOREM 13.2.2. Since any two distinct Fermat numbers are relatively prime, and since any number ≥ 2 has a prime divisor, it follows that choosing a prime divisor for each Fermat number F_n yields infinitely many distinct primes. $\square$

13.4 Legendre's Formula and Kummer's Theorem

In some cases we can give precise expressions of the prime factorization of a number. We will describe here two such cases: The prime factorization of the factorial $n!$, which is due to Adrien-Marie Legendre, and the prime factorization of the binomial coefficients $\binom{n}{m}$, which is due to Ernst Kummer. We will use a corollary to Kummer's theorem in the proof of Bertrand's Postulate.

DEFINITION 13.4.1. The **p-adic valuation** of a positive integer n is the largest exponent m such that $p^m \mid n$. That is, the p-adic valuation $v_p(n)$ of n satisfies the logical equivalence

$$p^k \mid n \quad \Leftrightarrow \quad k \le v_p(n)$$

for every natural number k.

In other words, the p-adic valuation of n is the exponent of p in the prime factorization of n. For example, the 2-adic valuation of 24 is $v_2(24) = 3$ because the exponent of 2 in $24 = 2^3 \cdot 3$ is 3, and its 3-adic valuation is $v_3(24) = 1$ because the exponent

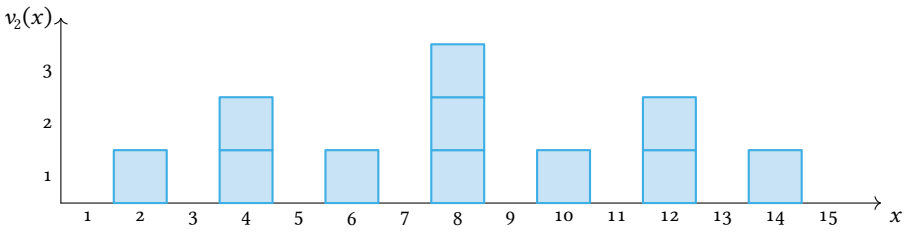


Figure 13.2: The 2-adic valuations of the numbers up to 15.

of 3 in $2^3 \cdot 3$ is 1. On the other hand, the 5-adic valuation of 24 is $v_5(24) = 0$ since 24 is not divisible by 5. The 2-adic valuations of the numbers up to 15 are displayed in Figure 13.2.

Example 13.4.2. A useful application of p-adic valuations is that the p-adic valuation of the greatest common divisor of two numbers is the minimum of their respective p-adic valuations. More generally, if the greatest common divisor is taken of multiple natural numbers we obtain

$$v_p(\gcd(n_1, \dots, n_k)) = \min(v_p(n_1), \dots, v_p(n_k)).$$

Likewise, the p-adic valuation of the least common multiple of $n_1, \dots, n_k$ is

$$v_p(\operatorname{lcm}(n_1, \dots, n_k)) = \max(v_p(n_1), \dots, v_p(n_k)).$$

For example the greatest common divisor and the least common multiple of $60 = 2^2 \cdot 3 \cdot 5$ and $525 = 3 \cdot 5^2 \cdot 7$ are

$$\gcd(60, 525) = 3 \cdot 5 = 15 \qquad \text{and} \qquad \operatorname{lcm}(60, 525) = 2^2 \cdot 3 \cdot 5^2 \cdot 7 = 2100.$$

An immediate consequence of the definition of p-adic valuations is the following proposition:

Proposition 13.4.3. *For any two positive integes a and b, the following are equivalent:*

(i) $a \mid b$.

(ii) $v_p(a) \leq v_p(b)$ *for every prime* p.

Example 13.4.4. The prime factorization of 15! can be obtained by computing the prime factorization of the numbers 1 through 15 individually, which are:

$$1, 2, 3, 2^2, 5, 2 \cdot 3, 7, 2^3, 3^2, 2 \cdot 5, 11, 2^2 \cdot 3, 13, 2 \cdot 7, 3 \cdot 5.$$

Thus, we obtain

$$15! = 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13.$$



THEOREM 13.4.5 (Legendre's formula). *For any natural number n, we have*

$$n! = \prod_{p \leq n} p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots}.$$

PROOF. Another way of stating Legendre's formula for $n!$ is that the p-adic valuation of $n!$ is given by

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

To see this, note that each integer $1 \leq x \leq n$ divisible by p contributes a factor p to $n!$. Each integer $1 \leq x \leq n$ divisible by p^2 contributes a second factor of p to $n!$, and more generally, each integer $1 \leq x \leq n$ divisible by p^k contributes a kth factor of p.

Since there are $\left\lfloor \frac{n}{p^k} \right\rfloor$ integers from 1 to n divisible by p^k, it follows that the number of factors of p in $n!$ is

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor. \qquad \square$$

Incidentally, Legendre's formula can be used to give yet another proof of the infinitude of primes, due to Junho Peter Whang [WHA2010].

WHANG'S PROOF OF THEOREM 13.2.2. The p-adic valuation of $n!$ is bounded from above by

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \leq \sum_{k=1}^{\infty} \frac{n}{p^k} = \frac{n}{p-1}.$$

Now suppose that n is a natural number so that all the primes below n are from the list $p_1, \ldots, p_m$, and define

$$M := \prod_{i=1}^{m} p_i^{\frac{1}{p_i - 1}}.$$

Then it follows from Legendre's formula that

$$n! \leq M^n.$$

To give a quick lower bound for $n!$, note that for $1 \leq k \leq n$ we have $n \leq k(n+1-k)$. This gives the inequalities

$$n^{\frac{n}{2}} \leq n! \leq M^n.$$

However, this inequality fails when n exceeds M^2, so it follows that for $n > M^2$ there must be a prime not in the list $p_1, \ldots, p_m$. $\square$

In the following theorem we give a useful alternative expression for the p-adic valuation of $n!$.

Theorem 13.4.6 (de Polignac's formula). *Consider a natural number $n \geq 1$ written in its base p representation*

$$\sum_{i=0}^{l} a_i p^i,$$

where we have $0 \leq a_i < p$ for each i. Then p-adic valuation of $n!$ is

$$v_p(n!) = \frac{n - \sum_{i=0}^{l} a_i}{p-1}.$$

Proof. Given the base-p representation of n, the base-p representation of $\lfloor \frac{n}{p^k} \rfloor$ is given by dropping the digits first k digits in the base-p representation of n:

$$\left\lfloor \frac{n}{p^k} \right\rfloor = a_k + a_{k+1} p + \cdots + a_l p^{l-k}.$$

Using this observation, we obtain:

$$\sum_{k=1}^{l} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{l} \sum_{j=k}^{l} a_j p^{j-k} = \sum_{j=1}^{l} a_j \sum_{k=1}^{j} p^{j-k} = \sum_{j=1}^{l} a_j \frac{p^j - 1}{p-1}.$$

On the other hand, we have

$$n - \sum_{j=0}^{l} a_j = \sum_{j=0}^{l} a_j p^j - a_j = \sum_{j=0}^{l} a_j (p^j - 1).$$

This gives

$$\frac{n - \sum_{j=0}^{l} a_j}{p-1} = \sum_{j=0}^{l} a_j \frac{p^j - 1}{p-1} = \sum_{k=1}^{l} \left\lfloor \frac{n}{p^k} \right\rfloor. \qquad \square$$

Example 13.4.7. We can use Legendre's formula and de Polignac's formula to compute the prime factorizations of binomial coefficients. For example, it follows immediately from Legendre's formula that all the prime factors of the central binomial coefficient

$$\binom{64}{32}$$

are bounded from above by 64. Moreover, every prime $32 < p \leq 64$ occurs with p-adic valuation 1. Furthermore, the central binomial coefficient $\binom{64}{32}$ is not divisible by any prime $\frac{2}{3}32 < p \leq 32$, showing that the 23-, 29-, and 31-adic valuations of $\binom{64}{32}$ are 0. To compute the p-adic valuations for the lower primes, we use de Polignac's formula, for which it is necessary to write 32 and 64 in base p. Using letters A, B, C, and so forth for digits representing values of 10 and higher, we gather all the calculations for de Polignac's formula in the following table:

p	32 base p	64 base p	$\frac{2s_p(32)-s_p(64)}{p-1}$
2	$(100000)_2$	$(1000000)_2$	1
3	$(1012)_3$	$(2101)_3$	2
5	$(112)_5$	$(224)_5$	0
7	$(44)_7$	$(121)_7$	2
11	$(2A)_{11}$	$(59)_{11}$	1
13	$(26)_{13}$	$(4C)_{13}$	0
17	$(1F)_{17}$	$(3D)_{17}$	1
19	$(1D)_{19}$	$(37)_{19}$	1

Thus, we see that

$$\binom{64}{32} = 2 \cdot 3^2 \cdot 7^2 \cdot 11 \cdot 17 \cdot 19 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61.$$

Even though the binomial coefficient $\binom{64}{32}$ is a fairly large number with 19 decimal digits, we didn't need to evaluate it in order to obtain its prime factorization. In fact, without fully evaluating it, we can now determine the last decimal digit of $\binom{64}{32}$ by the following procedure: Start with $d_0 := 1$ and let d_{i+1} be the remainder of the product $d_i p_i^{m_i}$ after division by 10, where $p_i^{m_i}$ is the ith prime power in the prime factorization of $\binom{64}{32}$. This gives:

$$d_1 = 2,\ d_2 = 8,\ d_3 = 2,\ d_4 = 2,\ \ldots,\ d_{13} = 4.$$

The last decimal digit of $\binom{64}{32}$ is therefore a 4.

In the following theorem, which is due to Ernst Kummer [KUM1852], we will compute the p-adic valuation of the binomial coefficients in full generality. Before we do this, we need to recall addition of two natural numbers written in base p. Suppose that

$$m = \sum_{i=0}^{l_m} a_i p^i \qquad \text{and} \qquad n = \sum_{i=0}^{l_n} b_i p^i.$$

Then their sum $m + n$ has base-p representation

$$m + n = \sum_{i=0}^{l_n} c_i p^i,$$

where c_i is obtained by the following recursive procedure, simultaneously with a number $u(m,n)_i \in \{0,1\}$ recording whether a 1 needs to be carried over to the next digit: Set $u(m,n)_0 = 0$ and define

$$(c_i, u(m,n)_{i+1}) := \begin{cases} (a_i + b_i + u(m,n)_i, 0) & \text{if } a_i + b_i + u(m,n)_i < p, \\ (a_i + b_i + u(m,n)_i - p, 1) & \text{if } a_i + b_i + u(m,n)_i \geq p. \end{cases}$$

Theorem 13.4.8 (Kummer's Theorem). *Consider two natural numbers m and n. The p-adic valuation of the binomial coefficient $\binom{m+n}{m}$ is the number of carries in the addition of m and n in base p: If m and n have base p-representations*

$$m = \sum_{i=0}^{l_m} a_i p^i \qquad \text{and} \qquad n = \sum_{i=0}^{l_n} b_i p^i,$$

then

$$v_p\binom{m+n}{m} = \#\{0 \leq i \leq l_n \mid u(m,n)_i = 1\}.$$

Proof. Write $s_p(x)$ for the sum of the digits of the p-adic representation of a natural number x. By de Polignac's formula for the p-adic valuation of $(m+n)!$ we find that

$$v_p\binom{m+n}{m} = v_p((m+n)!) - v_p(m!) - v_p(n!) = \frac{s_p(m) + s_p(n) - s_p(m+n)}{p-1}.$$

The p-adic representation of $m+n$ is given by

$$m+n = \sum_{i=0}^{l_{m+n}} c_i p^i,$$

where

$$c_i = \begin{cases} a_i + b_i + u(m,n)_i & \text{if } a_i + b_i + u(m,n)_i < p, \\ a_i + b_i + u(m,n)_i - p & \text{otherwise.} \end{cases}$$

We therefore find that the numerator in de Polignac's expression for $v_p\binom{m+n}{m}$ contains a term $p - u(m,n)_{i+1}$ for every time $u(m,n)_{i+1} = 1$. That is, the numerator is of the form $C(p-1)$ where C is the number of carries. This proves the theorem. □

Example 13.4.9. Consider two natural numbers m and n such that

$$m = \sum_{i=0}^{k} a_i 2^i \qquad \text{and} \qquad n - m = \sum_{i=0}^{k} b_i 2^i,$$

where $0 \leq a_i, b_i < 2$ for every i. Then the binomial coefficient $\binom{n}{m}$ is odd if and only if $a_i b_i = 0$ for every $0 \leq i \leq k$, since only in this situation there are no carries when m and n are added in base 2.

Kummer's theorem can be used to show that the binomial coefficient $\binom{n}{k}$ always divides the least common multiple of $1, 2, \ldots, n$. In order to prove this result, note that the largest exponent m such that $p^m \leq n$ is the number

$$m = \lfloor \log_p(n) \rfloor.$$

In other words, if m is the largest integer not exceeding $\log_p(n)$, then the leading digit in the base-p representation of n belongs to p^m.



COROLLARY 13.4.10. *For any $0 \leq k \leq n$ we have*

$$\binom{n}{k} \Big| \operatorname{lcm}(1, \ldots, n).$$

PROOF. Suppose that the base-p representation of n is

$$n = \sum_{i=0}^{l} a_i p^i.$$

Then there are clearly at most l carries when we add k to $n-k$. Since $p^l \leq n$, it follows that

$$p^{\nu_p\binom{n}{k}} \mid \operatorname{lcm}(1, \ldots, n).$$

Since this is true for every prime $p \leq n$, and $\binom{n}{k}$ contains only prime divisors up to n, the claim follows. □

13.5 Bertrand's Postulate

In 1845, Joseph Bertrand observed that for any $1 \leq n \leq 3,000,000$ there is always a prime between n and $2n$, and conjectured that this must be true for all n [BER1845]. Nowadays on a computer, it is really easy to generate lists of primes p_i so that the prime p_{i+1} is strictly below $2p_i$ for each i. Taking each time the largest possible prime satisfying this requirement, we obtain the list

2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259,

2503, 5003, 9973, 19937, 39869, 79699, 159389,

318751, 637499, 1274989, 2549951, 5099893, ...

The primes in this list are sometimes called the **Bertrand primes**, and they are listed as A006992 in the On-Line Encyclopedia of Integer Sequences [OEI2025]. Bertrand's conjecture was proven five years later by Pafnuty Chebyshev, who contributed many more results about the distribution of the primes using analytical methods [CHE1852]. We will give a proof by Paul Erdős [ERD1932], which can be obtained through the methods of the previous section.

LEMMA 13.5.1 (Chebyshev's primorial bound). *For any positive integer n, we have*

$$\prod_{p \leq n} p < 4^n.$$

PROOF. The proof is by induction on n. For $n = 1$, there are no primes $p \leq 1$, so the product over all the primes $p \leq 1$ is just 1, which is indeed strictly below 4. Likewise, the theorem holds for $n = 2$, because $2 < 4^2$.

For the inductive step, assume that $n \geq 2$ and that $\prod_{p \leq n} p < 4^n$. In order to show that

$$\prod_{p \leq n+1} p < 4^{n+1},$$

there are two cases to consider: Either $n+1$ is even or $n+1$ is odd. The even case is immediate: We have

$$\prod_{p \leq n+1} p = \prod_{p \leq n} p < 4^n < 4^{n+1}.$$

In the odd case, there is an m such that $2m+1 = n+1$. Since every prime $m+2 \leq p \leq 2m+1$ divides the binomial coefficient $\binom{2m+1}{m}$, it follows that

$$\prod_{p \leq 2m+1} p \leq \binom{2m+1}{m} \cdot \prod_{p \leq m+1} p < \binom{2m+1}{m} 4^{m+1}.$$

To finish the proof, it suffices to show that $\binom{2m+1}{m} \leq 4^m$. This follows, since the binomial coefficients $\binom{2m+1}{m}$ and $\binom{2m+1}{m+1}$ occur separately in the expansion of $(1+1)^{2m+1}$. However, they are equal, so neither of them can exceed $\frac{1}{2} 2^{2m+1} = 4^m$, which proves the lemma. □

Theorem 13.5.2. *For any positive integer n, there is a prime $n < p \leq 2n$.*

Proof. Consider an integer $n \geq 2$ for which there is no prime $n < p < 2n$, and let p be a prime divisor of the central binomial coefficient $\binom{2n}{n}$. Such a prime divisor must then be less than or equal to $\frac{2}{3}n$, since $q^3 \nmid (2n)!$ for any prime $\frac{2}{3}n < q \leq n$, while $q^2 \mid (n!)^2$.

Now, recall from Corollary 13.4.10 that any prime power $p^m \mid \binom{2n}{n}$ must satisfy $p^m \leq 2n$. In particular, the number of primes p such that $p^2 \mid \binom{2n}{n}$ is bound from above by the inequality

$$p \leq \sqrt{2n}.$$

This shows that there are at most $\sqrt{2n}$ primes in the prime factorization of $\binom{2n}{n}$, of which the exponent is larger than 1. Furthermore, it follows that

$$\prod_{p^2 \mid \binom{2n}{n}} p^{v_p\binom{2n}{n}} \leq (2n)^{\sqrt{2n}}.$$

Combined with the fact that the prime factors of $\binom{2n}{n}$ don't exceed $\frac{2n}{3}$, we obtain the following estimates:

$$\frac{4^n}{2n+1} < \binom{2n}{n} \leq (2n)^{\sqrt{2n}} \cdot \prod_{p \leq 2n/3} p < (2n)^{\sqrt{2n}} \cdot 4^{\frac{2n}{3}}.$$

Here, the first inequality was established in Exercise 3.6, and the last inequality follows from Lemma 13.5.1. Rearranging this strict inequality, we obtain

$$4^{\frac{n}{3}} < (2n+1)(2n)^{\sqrt{2n}} < 2(2n)^{\sqrt{2n}+1}.$$



Taking logarithms base 2 on both sides, we find that

$$\frac{2n}{3} < (\sqrt{2n} + 1)\log_2(2n) + 1.$$

We see that this strict inequality fails for $n \geq 2^9 = 512$, since

$$341 \leq \frac{2^{10}}{3} \not< 331 = (2^5 + 1) \cdot 10 + 1.$$

We have thus proven that if there does not exist a prime $n < p \leq 2n$, then we must have $p < 512$. However, using the Bertrand primes up to 631, we see that for every $n < 512$ there exists a prime $n < p \leq 2n$. Thus Bertrand's postulate is proven for all n. □

Exercises

Starter Exercises

13.1 In the number grid provided at the end of the introduction, shade the numbered cells in two colors:

(i) Leave all the prime numbers unshaded.

(ii) Shade the number 1 and all square-free composite numbers in one color.

(iii) Shade all non-square-free numbers in the other color.

Explain your method.

13.2 Find the first ten primes of the form $n^2 + 1$. The first of Laundau's four open problems about primes asks whether there are infinitely many such primes [Lan1912].

13.3 Find the first ten primes p such that $2p - 1$ is also prime. It is unknown whether there are infinitely many such primes.

13.4 Given a prime $p > 3$, show that $p^2 \equiv 1 \pmod{24}$.

13.5 By computing its prime factorization, show that

$$\binom{50}{3}$$

is a square number.

13.6 Show that

$$a^2 \equiv 1 \pmod{p} \Leftrightarrow a \equiv \pm 1 \pmod{p}.$$

13.7 Show that

$$\sum_{k=1}^{n} k^3 \,\Big|\, \prod_{k=1}^{n} k^3$$

holds for every n, except when $n + 1$ is an odd prime.

Routine-Building Exercises

13.8 Find the longest arithmetic progression of primes under 1000. Hint: Use congruences to constrain the step size.

13.9 Compute the prime factorizations of the following numbers:

(a) $5^{15} - 1$.
(b) $3^{18} - 1$.
(c) $2^{48} - 1$.

13.10 Show that there are no primes p such that $p + 8$ and $p + 22$ are also prime.

13.11 A pair of **twin primes** is a pair of primes p and q such that $q - p = 2$. Consider a pair of twin primes p and q strictly greater than 3.

(a) Show that $p + q \equiv 0 \pmod{12}$.



(b) Show that $pq \equiv -1 \pmod 9$.

13.12 A **Sophie Germain prime** is a prime p such that $2p+1$ is also prime. Show that if $p > 3$ is a Sophie Germain prime, then

$$p(2p+1) \equiv 1 \pmod{18}.$$

13.13 (a) Show that any odd prime of the form $x^2 + y^2$ must be congruent to $1 \pmod 4$, and find the first ten primes of this form.

(b) Show that any prime $p > 3$ of the form $x^2 + 3y^2$ must be congruent to $1 \pmod 6$, and find the first ten primes of this form.

(c) Show that any prime $p \neq 5$ of the form $x^2 + 5y^2$ must satisfy

$$p \equiv 1 \text{ or } 9 \pmod{20}$$

and find the first ten primes of this form.

(d) Show that any prime p of the form $x^2 + 6y^2$ must satisfy

$$p \equiv 1 \text{ or } 7 \pmod{24}$$

and find the first ten primes of this form.

The book [Cox1989] contains a beautiful exposition of the theory of primes of the form $x^2 + ny^2$, and serves as a wonderful introduction to class field theory.

13.14 Determine the number of trailing zeros in the decimal representations of $100!$ and $2^{10}!$.

13.15 Show that the inequality

$$2^{v_2\binom{2n}{n}} - 1 \leq n$$

holds for all $n \geq 0$.

13.16 (a) In Figure 13.2 we saw that $v_2((2^4-1)!) = 11$. More generally, prove that

$$v_p((p^k-1)!) = \frac{p^k-1}{p-1} - k$$

(b) Show that

$$v_p\left(\binom{p^n-1}{p^m-1}\right) = 0$$

for any $0 \leq m \leq n$.

13.17 Show that

$$\binom{42}{6} \,\Big|\, \binom{42}{12} \qquad \text{and} \qquad \binom{42}{6} \,\Big|\, \binom{42}{18}.$$

13.18 (a) Show that

$$\binom{30}{2} \,\Big|\, \binom{30}{2k}$$

for every $1 \leq k \leq 14$.

(b) Show that if p is a prime such that $q = 2p - 1$ is also a prime, then

$$\binom{2p}{2} \mid \binom{2p}{2k}$$

for every $1 \leq k \leq p - 1$.

13.19 (a) Show that

$$\frac{\operatorname{lcm}(1, \ldots, n)}{\operatorname{lcm}(1, \ldots, m)} = \prod_{k \geq 1} \prod_{\substack{p \text{ prime} \\ m < p^k \leq n}} p.$$

Use this formula to conclude that

$$\frac{\operatorname{lcm}(1, \ldots, n)}{\operatorname{lcm}(1, \ldots, n-1)} = \begin{cases} p & \text{if } n = p^k \text{ for some prime } p \text{ and } k \geq 1, \\ 1 & \text{otherwise.} \end{cases}$$

(b) Show that

$$\frac{\operatorname{lcm}(1, \ldots, n)}{\operatorname{lcm}(1, \ldots, m)}$$

is square-free for every $m \leq n$ such that $n \leq 2m$.

(c) Show that

$$\frac{\operatorname{lcm}(1, \ldots, n)}{\operatorname{lcm}(1, \ldots, m)} \mid \binom{n}{m}.$$

for every $m \leq n$ such that $n \leq 2m$.

Challenge Exercises

13.20 Show that for any prime p, if $p^2 + 2$ is prime then $p + 2$ is prime.

13.21 Consider $n \geq 1$. Prove that among any 2^n integers all of whose prime factors are less than or equal to n, there are two distinct integers such that their product is a square.

13.22 Consider a prime $p \equiv 3 \pmod 4$, and suppose that $v_p(n)$ is odd. Show that there is a bijection between the set of divisors $d \equiv 1 \pmod 4$ of n and the set of divisors $d \equiv 3 \pmod 4$ of n.

13.23 For any n, let $\omega(n)$ be the number of its prime divisors. Show that the number of integers $0 < x < n$ such that $x^2 \equiv x \pmod n$ is $2^{\omega(n)}$. Hint: Use the Chinese Remainder Theorem to show that there is a bijection between the integers x such that $x^2 \equiv x \pmod n$ and the subsets of the set of prime divisors of n.

13.24 Show that there is exactly one positive integer k such that both $2^k - 1$ and $2^k + 1$ are prime.

13.25 In this exercise F_n denotes the nth Fibonacci number. Show that a prime p divides F_{p-1} if and only if $p \equiv \pm 1 \pmod 5$ and p divides F_{p+1} if and only if $p \equiv \pm 2 \pmod 5$.

13.26 Prove the following identity of Bakir Farhi [FAR2009]:

$$\operatorname{lcm}\left(\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}\right) = \frac{\operatorname{lcm}(1, \ldots, n+1)}{n+1}.$$

13.27 Show that there are infinitely many numbers not divisible by any Fibonacci numbers other than 1.

13.28 Use Bertrand's Postulate to show that

$$\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}$$

is never an integer.

Chapter 14

Multiplicative Functions

14.1 Perfect Numbers

The number 6 satisfies the curious property that the sum of its proper divisors $1+2+3$ is equal to the number 6 itself. This property of a number being equal to the sum of its own proper divisors, which is also called the *aliquot sum*, was deemed so special in ancient times, that these numbers were called *perfect*.

Definition 14.1.1. Consider a positive natural number n. The **aliquot sum** $s(n)$ of n is defined by

$$s(n) := \sum_{d \mid n,\ d<n} d$$

(i) The number n is called **perfect** if $s(n) = n$.

(ii) The number n is called **deficient** if $s(n) < n$.

(iii) The number n is called **abundant** if $s(n) > n$.

Example 14.1.2. The number 6 is perfect, since $6 = 1+2+3$; the number 8 is deficient, since $1+2+4 = 7 < 8$, and the number 12 is abundant, since $1+2+3+4+6 = 16 > 12$.

Euclid observed that if $2^m - 1$ is prime, then we can always find a number k such that

$$2^k(2^m - 1)$$

is perfect. Indeed, since the divisors of 2^k are precisely the numbers 2^i with $0 \le i \le k$, it follows that the divisors of $2^k(2^m-1)$ are exactly

$$1,\ 2, \dots,\ 2^k, \qquad \text{and} \qquad (2^m-1),\ 2(2^m-1), \dots,\ 2^k(2^m-1).$$

The sum of the divisors of $2^k(2^m-1)$ is therefore

$$(2^{k+1}-1)+(2^{k+1}-1)(2^m-1)=(2^{k+1}-1)2^m.$$

The equation

$$(2^{k+1}-1)2^m = 2\cdot 2^k(2^m-1)$$

now implies that $m=k+1$. Thus, we have proven the following proposition, which Euclid recorded as Proposition 36 in Book IX of the Elements.

PROPOSITION 14.1.3 (Euclid). *If the number 2^m-1 is prime, then the number $2^{m-1}(2^m-1)$, which is indeed the $(2^m-1)^{th}$ triangular number, is perfect.*

Using Euclid's method, we can find the first few perfect numbers. Table 14.1 displays the prime factorization of the *Mersenne number* 2^m-1 for $2\le m\le 11$.

m	2	3	4	5	6	7	8	9	10	11
2^m-1	**3**	7	3·5	**31**	3^2·7	**127**	3·5·17	7·73	3·11·31	23·89

Table 14.1: The Mersenne numbers M_m for $2\le m\le 11$.

We see that M_2, M_3, M_5, and M_7 are prime, and thus we obtain the following perfect numbers:

$$\begin{aligned} 6 &= 2^1(2^2-1),\\ 28 &= 2^2(2^3-1),\\ 496 &= 2^4(2^5-1),\\ 8128 &= 2^6(2^7-1). \end{aligned}$$

Prime numbers of the form $M_m=2^m-1$ are called Mersenne primes, after Father Marin Mersenne who studied them more deeply in the 17th century. An elementary property of Mersenne primes is that if M_m is prime, then m must be prime.

PROPOSITION 14.1.4. *If the mth Mersenne number $M_m=2^m-1$ is prime, then m is prime.*

PROOF. We prove the contrapositive: If m is composite, so that $m=ab$ for some $a,b>1$, then M_m is composite. This follows directly from the formula for the difference of powers:

$$2^{ab}-1=(2^a)^b-1^b=(2^a-1)\sum_{k=0}^{b-1}(2^a)^k. \qquad \square$$

Mersenne numbers which are prime are called **Mersenne primes**. They are used in the search for extremely large prime numbers. Note, however, that not every Mersenne number M_p with p prime is a prime number. For example, $M_{11}=23\cdot 89$.

No perfect numbers other than the ones described by Euclid have been found, so it is natural to wonder whether Euclid described all of them. This leads us to Euler, who was able to prove in the 18th century that every *even* perfect number is of Euclid's form. Euler did so by analyzing the function σ, which returns for each n the sum of its divisors. Euler's proof marks the beginning of the theory of *arithmetic functions*.

Definition 14.1.5. We define the **sum-of-divisors** function σ by

$$\sigma(n) := \sum_{d|n} d.$$

Thus, a number n is perfect if $\sigma(n) = 2n$. Notice that a number n is prime if and only if $\sigma(n) = n+1$. The next easiest sum of divisors to calculate is the sum of divisors of a prime power. For any prime p we have

$$\sigma(p^m) = \sum_{k=0}^{m} p^k = \frac{p^{m+1}-1}{p-1}.$$

Indeed, $d \mid p^m$ if and only if $d = p^k$ for some $0 \le k \le m$, so the sum of the divisors of p^m is the finite geometric series $1 + p + p^2 + \cdots + p^m$.

Proposition 14.1.6. *Suppose m and n are relatively prime. Then*

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Proof. We first claim that the operation $u, v \mapsto uv$, which takes a pair of numbers $u \mid m$ and $v \mid n$ and returns their product, which is a divisor of mn, defines a bijection

$$\{u \mid u \mid m\} \times \{v \mid v \mid n\} \cong \{d \mid d \mid mn\}$$

To see this, we need to define an inverse function. That is, given a divisor $d \mid mn$ we need to construct divisors of m and n. Observe that, since m and n are relatively prime, it follows that $d = \gcd(d,m)\gcd(d,n)$. Thus, we define $u_d := \gcd(d,m)$ and $v_d := \gcd(d,n)$. Furthermore, when $u \mid m$ and $v \mid n$ are arbitrary, then we have $\gcd(uv,m) = u$ and $\gcd(uv,n) = v$. These equations show that the map $d \mapsto (u_d, v_d)$ is indeed inverse to the function $u, v \mapsto uv$.

Using the bijection we just constructed, we see that

$$\left(\sum_{u|m} u\right)\left(\sum_{v|n} v\right) = \sum_{u|m}\sum_{v|n} uv = \sum_{d|mn} d. \qquad \square$$

The multiplicative property of the sum-of-divisors function along with the expressions for $\sum(p^m)$ completely determine the values of the function σ for any positive integer of which the prime factorization is known.

Corollary 14.1.7. *Suppose that $n = p_1^{m_1} \cdots p_k^{m_k}$, where all the primes p_i are distinct. Then*

$$\sigma(n) = \frac{p_1^{m_1+1}-1}{p_1-1} \cdots \frac{p_k^{m_k+1}-1}{p_k-1}.$$



EXAMPLE 14.1.8. We saw in Example 13.4.4 that $15! = 2^{11}\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13$. It follows that

$$\sigma(15!) = (2^{12}-1)\cdot\frac{3^7-1}{2}\cdot\frac{5^4-1}{4}\cdot\frac{7^3-1}{6}\cdot 12\cdot 14 = 2^5\cdot 3^5\cdot 5\cdot 7^2\cdot 13^2\cdot 19\cdot 1093.$$

THEOREM 14.1.9 (Euclid–Euler). *An even number n is perfect if and only if it is of the form*

$$2^{p-1}(2^p-1)$$

for some prime p, where the number 2^p-1 is prime.

PROOF. We have already seen that n is perfect if $n = 2^{p-1}(2^p-1)$, provided that 2^p-1 is prime. Furthermore, since the condition that 2^p-1 is prime implies that p is prime, and hence that 2^{p-1} is divisible by 2, it follows that numbers of the form $2^{p-1}(2^p-1)$ are even.

For the converse, assume that n is an even perfect number, so that $\sigma(n) = 2n$. Using the 2-adic decomposition, we can write $n = 2^k m$ where m is odd. Since odd numbers are relatively prime to powers of 2, it follows that

$$\sigma(2^k m) = \sigma(2^k)\sigma(m) = (2^{k+1}-1)\sigma(m).$$

By the assumption that $2^k m$ is perfect, we obtain that

$$(2^{k+1}-1)\sigma(m) = 2^{k+1}m.$$

Since the number $s := 2^{k+1}-1$ is relatively prime to 2^{k+1}, it follows that $s \mid m$. If we write $m = st$, then the displayed equation simplifies to

$$\sigma(m) = 2^{k+1}t = (s+1)t = t + st.$$

Now observe that both t and st are divisors of m. They are distinct, since n is assumed to be even and thus we have $s > 1$. Since $\sigma(m) = t + st$ is the sum of all the divisors of m, it follows that t and st are the only divisors of m. We conclude that $t = 1$ and $s = m$. Furthermore, we obtain that $\sigma(m) = m + 1$, which implies that m is prime. We have thus shown that

$$n = 2^k(2^{k+1}-1),$$

and that $2^{k+1}-1$ is prime. This last property implies that $k+1$ is prime, which completes the proof. □

The Euclid–Euler theorem completely characterizes even perfect numbers. However, it doesn't tell us anything about odd perfect numbers. No odd perfect numbers have ever been found, and it is conjectured that none exist. It has been shown that any odd perfect number must be greater than 10^{1500} [OR2012].

14.2 Euler's Totient Function

Before we introduce reduced residue systems, let us prove a lemma.

Lemma 14.2.1. *Suppose that* $a \equiv b \pmod{n}$. *Then* $\gcd(a,n) = \gcd(b,n)$. *Consequently, we have* $\gcd(a,n) = 1$ *if and only if* $\gcd(b,n) = 1$.

Proof. By the assumption that a and b are congruent modulo n, it follows that they have the same remainder after division by n. Let r be this remainder. Since $\gcd(a,n) = \gcd(r,n)$ and $\gcd(b,n) = \gcd(r,n)$ we see that

$$\gcd(a,n) = \gcd(b,n).$$

This equality implies that the left hand side equals 1 if and only if the right hand side equals 1. □

By the previous lemma, we can test whether an integer is relatively prime to n by testing any element in its congruence class. This allows us to make the following definition.

Definition 14.2.2. A **reduced residue system** modulo n is a set

$$\{r_1, \dots, r_k\}$$

of integers satisfying the condition that for every integer a relatively prime to n, there is exactly one index $1 \leq i \leq k$ such that

$$a \equiv r_i \pmod{n}.$$

Corollary 14.2.3. *Any two reduced residue systems modulo* n *have the same size, for which we write* $\phi(n)$. *The function* ϕ *is called* ***Euler's totient function****.*

Proof. Reduced residue systems are choices of representatives of the congruence classes in which all elements are relatively prime to n. Thus, the size of a reduced residue system is always equal to the number of such congruence classes. □

Theorem 14.2.4. *Euler's totient function* ϕ *is multiplicative: For any two relatively prime numbers* m *and* n *we have*

$$\phi(mn) = \phi(m)\phi(n).$$

Proof. We prove the claim by a counting argument: We claim that the bijection of Theorem 9.3.1 (Chinese Remainder Theorem)

$$\{0 \leq x < mn\} \cong \{0 \leq a < m\} \times \{0 \leq b < n\},$$

given by $x \mapsto (x \pmod{m}, x \pmod{n})$, restricts to a bijection

$$\{0 \leq x < mn \mid \gcd(x, mn) = 1\} \cong \{0 \leq a < m \mid \gcd(a,m) = 1\} \times \{0 \leq b < n \mid \gcd(b,n) = 1\}.$$

To see this, note that x is relatively prime to a number k if and only if $x \pmod{k}$ is relatively prime to k. Thus, we have to show that

$$\gcd(x, mn) = 1 \quad \Leftrightarrow \quad \gcd(x, m) = 1 \text{ and } \gcd(x, n) = 1.$$

For the forward direction, suppose that $\gcd(x, mn) = 1$. In this case, any d dividing both x and m is also a common divisor of x and mn so it must be 1. Thus, it is clear that if $\gcd(x, mn) = 1$, then $\gcd(x, m) = \gcd(x, n) = 1$.

For the converse, suppose that $\gcd(x, m) = \gcd(x, n) = 1$, and suppose that $d \mid x$ and $d \mid mn$. Since m and n are relatively prime, we can uniquely determine two numbers a and b satisfying $d = ab$, such that $a \mid m$ and $b \mid n$. For these numbers, we obtain that $a \mid \gcd(x, m) = 1$ and $b \mid \gcd(x, n) = 1$ so that both $a = 1$ and $b = 1$. This shows that $d = 1$. □

Since multiplicative functions are fully determined by their values on prime powers, we obtain the following important expression for Euler's totient function.

THEOREM 14.2.5. *Consider a positive integer n with prime factorization $n = p_1^{m_1} \cdots p_k^{m_k}$. Then*

$$\phi(n) = \prod_{i=1}^{k} (p_i^{m_i} - p_i^{m_i - 1}) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

COROLLARY 14.2.6. *The value $\phi(n)$ of Euler's totient function is even for $n > 2$.*

PROOF. For $k \geq 2$ we have $\phi(2^k) = 2^{k-1}$, which is even. Furthermore, every odd prime factor p contributes an even factor $p - 1$ to $\phi(n)$. □

Since $\phi(p^k) = p^{k-1}(p - 1)$, it follows that if $k \leq l$, then $\phi(p^k) \mid \phi(p^l)$. Since Euler's totient function is multiplicative by theorem:multiplicative-totient, we obtain the following corollary:

COROLLARY 14.2.7. *The function $n \mapsto \phi(n)$ is a divisibility sequence: For any two natural numbers m and n, we have*

$$m \mid n \quad \Rightarrow \quad \phi(m) \mid \phi(n).$$

EXAMPLE 14.2.8. We will use Theorem 14.2.5 to determine all n for which $\phi(n) = 2^k$ for some k.

If p is an odd prime so that $p^a - p^{a-1} = p^{a-1}(p-1)$ is a power of 2, then it follows that $a - 1 = 0$. In other words, in order for $p^a - p^{a-1}$ to be a power of 2, we must have $a = 1$. This shows that if $\phi(n)$ is a power of 2, then n must be of the form

$$n = 2^a \prod_{p \in S} p,$$

where S is a subset of the **Fermat primes**; that is, every prime in S is the form $2^b + 1$. The only known such primes are

$$3,\ 5,\ 17,\ 257,\ \text{and } 65537.$$

2^k	Fermat primes $p \leq 2^k + 1$	n such that $\phi(n) = 2^k$
1	none	1, 2
2	3	3, 4, 6
4	3, 5	5, 8, 10, 12
8	3, 5	15, 16, 20, 24, 30
16	3, 5, 17	17, 32, 34, 40, 48, 60
32	3, 5, 17	51, 64, 68, 80, 96, 102, 120
64	3, 5, 17	85, 128, 136, 160, 170, 192, 204, 240
128	3, 5, 17	255, 256, 272, 320, 340, 384, 408, 480, 510

Table 14.2: Lists of numbers n for which $\phi(n) = 2^k$

We conclude that the only numbers n for which $\phi(n) = 4$ are 5, 8, 10, and 12, and the only numbers n for which $\phi(n) = 8$ are 15, 16, 20, 24, and 30. Table 14.2 lists the numbers n for which $\phi(n) = 2^k$ up to $2^k = 128$.

14.3 Multiplicative Functions

A function f defined on the positive integers with output in any number system, such as the integers, real numbers, or complex numbers, is called an **arithmetic function**. For example, Euler's totient function ϕ, which returns for each n the number of elements $0 < k < n$ relatively prime to n, is an arithmetic function. Some other important arithmetic functions include the **number of divisors function** τ and the **sum of divisors function** σ:

$$\tau(n) := \sum_{d|n} 1 \qquad \text{and} \qquad \sigma(n) := \sum_{d|n} d.$$

Note that the number of divisors and the sum of divisors are not defined for $n = 0$. Arithmetic functions are typically only defined on the positive integers $\{1, 2, 3, \ldots\}$. Even for functions which are defined on 0, such as Euler's totient function, when we consider them as arithmetic functions we will consider their domain of definition to be the positive integers.

Other functions, which are worth naming are the **constant function** $n \mapsto 1$, which we will simply denote by 1, and the **identity function** $n \mapsto n$, which we will denote by id. In the pages that follow, we shall encounter two more arithmetic functions: the *unit function* ε and the *Möbius function* μ.

Definition 14.3.1. An arithmetic function f is said to be **multiplicative** if for any two relatively prime natural numbers m and n we have

$$f(mn) = f(m)f(n).$$

Proposition 14.3.2. *If f is a nonzero multiplicative function, then $f(1) = 1$.*



PROOF. Since f is assumed to be nonzero, there is a natural number n such that $f(n) \neq 0$. Thus,

$$f(n) = f(1n) = f(1)f(n)$$

by the assumption that f is multiplicative. Since multiplication by a nonzero number is injective, it follows that $f(1) = 1$. □

It follows that the constant function 1 is the only constant multiplicative function. By the following proposition, we see that any multiplicative function is determined by its values on prime powers.

PROPOSITION 14.3.3. *If f is a multiplicative function and $n = p_1^{m_1} \cdots p_k^{m_k}$, where the primes $p_1, \ldots, p_k$ are distinct, then*

$$f(n) = f(p_1^{m_1}) \cdots f(p_k^{m_k}).$$

PROOF. Since the primes $p_1, \ldots, p_k$ are assumed to be distinct, it follows that the prime powers $p_1^{m_1}, \ldots, p_k^{m_k}$ are pairwise relatively prime, hence the claim follows by induction on k. □

The following theorem provides a useful way of proving that a function is multiplicative.

THEOREM 14.3.4. *Suppose f is a multiplicative function, and define the function F by*

$$F(n) := \sum_{d \mid n} f(d).$$

PROOF. Consider two relatively prime natural numbers m and n. Then there is a bijection $(c, d) \mapsto cd$ from the set

$$\{c \mid c \text{ divides } m\} \times \{d \mid d \text{ divides n}\}$$

to the set of divisors of mn. For the inverse function, define the function

$$e \mapsto (\gcd(e, m), \gcd(e, n)),$$

which sends a divisor e of mn to a pair of divisors of m and n. To see that this is indeed an inverse, note that if $c \mid m$ and $d \mid n$, then $\gcd(d, m) = 1$ so that

$$c = \gcd(cd, m).$$

Similarly, we have that $\gcd(c, n) = 1$ so that $d = \gcd(cd, n)$. This shows that

$$(c, d) = (\gcd(cd, m), \gcd(cd, n)).$$

We also have to show that $\gcd(e, m)\gcd(e, n) = e$ for any divisor e of mn. Write $c = \gcd(e, m)$ and $d = \gcd(e, n)$. Since c and d are relatively prime and since both are divisors of e, it follows that $cd \mid e$. Now, suppose that $kcd = e$. Since $\gcd(kcd, m) = c$ it

follows that $\gcd(k,m) = 1$. Similarly, $\gcd(k,n) = 1$. However, if p is any prime divisor of k, which divides mn, it follows that $p \mid m$ or $p \mid n$. Since this is impossible, it follows that $k = 1$. This completes the proof that the map $(c,d) \mapsto cd$ is a bijection.

Using this bijection, we find that

$$\begin{aligned} F(mn) = \sum_{e \mid mn} f(e) &= \sum_{c \mid m} \sum_{d \mid n} f(cd) \\ &= \sum_{c \mid m} \sum_{d \mid n} f(c)f(d) = \sum_{c \mid m} f(c) \sum_{d \mid n} f(d) = F(m)F(n). \end{aligned}$$ □

Theorem 14.3.5. *The functions τ and σ are multiplicative.*

Proof. The functions τ and σ are defined by

$$\tau(n) := \sum_{d \mid n} 1, \qquad \text{and} \qquad \sigma(n) := \sum_{d \mid n} d.$$

Clearly the constant function $n \mapsto 1$ and the identity function $n \mapsto n$ are multiplicative, so it follows from Theorem 14.3.4 that τ and σ are multiplicative. □

The previous theorem implies that if $n = p_1^{m_1} \cdots p_k^{m_k}$ is a product of distinct primes, then

$$\tau(n) = \prod_{i=1}^{k} (m_i + 1), \qquad \text{and} \qquad \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{m_1+1} - 1}{p_i - 1}.$$

Indeed, for any prime power p^m, the divisors of p^m are the prime powers p^i where $0 \le i \le m$. There are $m+1$ powers of p in this range, and their sum is computed by the formula for the geometric series

$$1 + p + \cdots + p^m = \frac{p^{m+1} - 1}{p - 1}.$$

Remark 14.3.6. Many identities of arithmetic functions involve reindexing double sums such as in the proof of Theorem 14.3.4. Another reindexing identity that is occasionally helpful is:

$$\sum_{c \mid n} \sum_{d \mid c} f(c,d) = \sum_{d \mid n} \sum_{e \mid \frac{n}{d}} f(de, d).$$

14.4 The Möbius Function

Definition 14.4.1. The **Möbius function** μ is defined by

$$\mu(n) := \begin{cases} (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes,} \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p. \end{cases}$$



For example, $\mu(3 \cdot 7 \cdot 17^3) = 0$ because the input is divisible by 17^2. On the other hand, $\mu(3 \cdot 7 \cdot 17) = (-1)^3 = -1$ because the input is the product of three distinct primes. The following table lists the values of $\mu(n)$ for the first 15 natural numbers

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(n)$	0	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1

It is immediate from the definition that the Möbius function is multiplicative. We will give two proofs of the following theorem: a combinatorial and an arithmetic proof.

THEOREM 14.4.2. *The Möbius function is multiplicative, and it satisfies*

$$\sum_{d \mid n} \mu(d) = \varepsilon(n).$$

In other words, $\mu * 1 = \varepsilon$.

COMBINATORIAL PROOF. It is clear that the formula holds for $n = 1$. For $n > 1$, we prove the formula by showing that there is a bijection

$$\{d \mid n \mid \mu(d) = 1\} \cong \{d \mid n \mid \mu(d) = -1\}$$

To describe such a bijection, let $p \mid n$ be a prime divisor of n, and define the map on a square-free divisor of n by

$$\theta_p(d) := \begin{cases} pd & \text{if } p \nmid d \\ \frac{d}{p} & \text{if } p \mid d. \end{cases}$$

In other words, θ_p is defined by "toggling" the prime p in a square-free divisor d of n. Note that $\theta_p(d)$ is again square-free, and that

$$\mu(\theta_p(d)) = -\mu(d).$$

Furthermore, the equality $\theta_p(\theta_p(d)) = d$ holds for every d, so we conclude that θ_p defines a bijection between the set of divisors d of n such that $\mu(d) = 1$ and the set of divisors d of n such that $\mu(d) = -1$. □

ARITHMETIC PROOF. Likewise, the arithmetic function

$$F(n) := \sum_{d \mid n} \mu(d)$$

is multiplicative by Theorem 14.3.4. Since multiplicative functions are completely determined by their values on prime powers, and ε is the multiplicative function given by

$$\varepsilon(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise,} \end{cases}$$

it suffices to show that $F(p^k) = 0$ for any $k \geq 1$. To see this, we simply evaluate

$$\sum_{d \mid p^k} \mu(p^k) = \mu(p^0) + \mu(p^1) + 0 = 1 - 1 = 0.$$ □

Remark 14.4.3. The previous theorem could be viewed as a recurrence relation that is satisfied by the Möbius function:

$$\mu(n) = -\sum_{\substack{d \mid n \\ d \neq n}} \mu(d)$$

Gian-Carlo Rota used this perspective to make the theory of arithmetic functions and the Möbius function applicable to a wide class of partially ordered sets [Rot1964].

14.5 Dirichlet Convolution

The set of arithmetic functions with values in a fixed number system such as the integers, the real numbers, or the complex numbers, possesses algebraic structure that can be used to obtain number-theoretic properties such as identities or divisibility results. The fundamental operation on arithmetic functions is *Dirichlet convolution*, a way of combining two arithmetic functions into a new one.

Definition 14.5.1. Consider two arithmetic functions f and g. We define their **Dirichlet convolution** $f * g$ by

$$(f * g)(n) := \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right).$$

Example 14.5.2. Let 1 be the constant arithmetic function given by $1(n) = 1$. Then we have

$$(1 * f)(n) = \sum_{d \mid n} 1(d) f\left(\frac{n}{d}\right) = \sum_{d \mid n} f\left(\frac{n}{d}\right) = \sum_{d \mid n} f(d).$$

Recall that the arithmetic function F given by $F(n) = \sum_{d \mid n} f(d)$ is the subject of Theorem 14.3.4, where we have established that if f is multiplicative, then so is F. We also note that

$$(1 * 1)(n) = \sum_{d \mid n} 1 = \tau(n).$$

Thus, we have the identity of arithmetic functions $1 * 1 = \tau$.

Example 14.5.3. Define the arithmetic function d_k by

$$d_k(n) := \#\{(a_1, \ldots, a_k) \mid a_1 \cdots a_k = n\}.$$

That is, $d_k(n)$ is the number of ways of writing n as an ordered product of k positive integers. For example, we have $d_2(n) = \tau(n)$ since every divisor $d \mid n$ uniquely determines an ordered pair (d, e) such that $de = n$. Thus, it follows from Example 14.5.2 that $1 * 1 = d_2$.

Next, observe that we can define 1^{*k} by iteratively convolving with the arithmetic function 1. That is, 1^{*1} is defined to be the arithmetic function 1, and $1^{*(k+1)}$ is defined to be the arithmetic function $1 * 1^{*k}$. We claim that

$$1^{*k} = d_k.$$



The proof is by induction on $k \geq 1$. Note that $d_1(n)$ is the number of ways of writing n as a single number. There is of course exactly one such way, so we have $d_1(n) = 1$ for all n. That is, we have $d_1 = 1$.

We have already seen that $1 * 1 = d_2$. For the inductive step, assume that $1^{*k} = d_k$. Then we have

$$1^{*(k+1)}(n) = (1 * 1^{*k})(n) = \sum_{d|n} 1(d) \cdot d_k\left(\frac{n}{d}\right) = \sum_{d|n} \#\{(a_1, \dots, a_k) \mid a_1 \cdots a_k = \tfrac{n}{d}\}.$$

Note that the data of d along with $(a_1, \dots, a_k)$ such that $a_1 \cdots a_k = \frac{n}{d}$ is equivalent to the data of $(d, a_1, \dots, a_k)$ such that $da_1 \cdots a_k = n$. The number of such $(k+1)$-tuples is $d_{k+1}(n)$, which completes the inductive step.

Using Theorem 14.3.4 repeatedly along with the fact that 1 is a multiplicative function, we obtain as a consequence of the identity $1^{*k} = d_k$ that d_k is a multiplicative function for each k. It follows that the values of d_k are determined by the values $d_k(p^a)$ at the prime powers p^a. Since each divisor of p^a is itself a power of p, it follows that $d_k(p^a)$ is equal to the number of ways of writing a as an ordered sum with k terms:

$$m_1 + \cdots + m_k = a.$$

Thus, it follows by Theorem 3.7.2 that $d_k(p^a) = \binom{a+k-1}{a}$. For $n = p_1^{a_1} \cdots p_m^{a_m}$ we therefore conclude:

$$d_k(n) = \prod_{1 \leq i \leq m} \binom{a_i + k - 1}{a_i}.$$

In the previous example, one might wonder whether it matters whether we define $1^{*k} = 1 * (1 * (\cdots * 1))$ or $1^{*k} = ((1 * \cdots) * 1) * 1$. Indeed, this shouldn't make a difference, as we prove in the following theorem.

THEOREM 14.5.4. *Dirichlet convolution is associative and commutative, meaning that*

$$(f * g) * h = f * (g * h), \qquad \textit{and} \qquad f * g = g * f,$$

respectively.

PROOF. Another way of writing the Dirichlet convolution of f and g is

$$(f * g)(n) = \sum_{\substack{c,d \\ cd=n}} f(c)g(d).$$

Since this expression is symmetric in f and g, we see immediately that the Dirichlet convolution is commutative. Furthermore, to see that the Dirichlet convolution is

associative we make the following two calculations:

$$\begin{aligned}((f*g)*h)(n) &= \sum_{\substack{c,d\\cd=n}} (f*g)(c)h(d) & (f*(g*h))(n) &= \sum_{\substack{a,e\\ae=n}} f(a)(g*h)(e)\\ &= \sum_{\substack{c,d\\cd=n}} \sum_{\substack{a,b\\ab=c}} f(a)g(b)h(d) & &= \sum_{\substack{a,e\\ae=n}} \sum_{\substack{b,d\\bd=e}} f(a)g(b)h(d)\\ &= \sum_{\substack{a,b,d\\abd=n}} f(a)g(b)h(d), & &= \sum_{\substack{a,b,d\\abd=n}} f(a)g(b)h(d). \qquad \square\end{aligned}$$

Example 14.5.5. By associativity of Dirichlet convolution, it follows that $1^{*k} * 1^{*l} = 1^{*(k+l)}$. Since $1^{*k} = d_k$ for each k by Example 14.5.3, it follows that $d_k * d_l = d_{k+l}$.

Theorem 14.5.6. *Let ε be the function given by*

$$\varepsilon(n) := \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Then $\varepsilon * f = f$ and $f * \varepsilon = f$ for any arithmetic function f.

Proof. Consider an arithmetic function f. Then

$$(\varepsilon * f)(n) = \sum_{d|n} \varepsilon(d) f\left(\frac{n}{d}\right) = f(n),$$

since the only term contributing to the sum is $d = 1$. The fact that $f * \varepsilon = f$ follows by commutativity of the Dirichlet convolution. $\square$

14.6 Dirichlet Inverses

Definition 14.6.1. Consider an arithmetic function f such that $f(1)$ is nonzero. Then we define the **Dirichlet inverse** f^{-1} of f by

$$f^{-1}(1) := \frac{1}{f(1)} \qquad \text{and} \qquad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n\\d\neq n}} f^{-1}(d) f\left(\frac{n}{d}\right) \qquad (\text{for } n > 1).$$

Theorem 14.6.2. *For every arithmetic function f such that $f(1)$ is nonzero, the arithmetic function f^{-1} is the inverse of f with respect to Dirichlet involution, in the sense that*

$$f^{-1} * f = \varepsilon \qquad \text{and} \qquad f * f^{-1} = \varepsilon.$$

Furthermore, f^{-1} is the unique such arithmetic function.



PROOF. To show that $(f * f^{-1})(n) = \varepsilon(n)$ for every $n \geq 1$, there are two cases to consider. In the case where $n = 1$, we have

$$(f * f^{-1})(1) = f(1)f^{-1}(1) = f(1)\frac{1}{f(1)} = 1 = \varepsilon(1).$$

In the case where $n > 1$, we have

$$(f * f^{-1})(n) = \sum_{d|n} f(d)f^{-1}\left(\frac{n}{d}\right) = f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d \neq n}} f(d)f^{-1}\left(\frac{n}{d}\right),$$

which is 0 by the definition of f^{-1}. This completes the proof that $f * f^{-1} = \varepsilon$. The equality $f^{-1} * f = \varepsilon$ follows by commutativity of Dirichlet convolution.

Uniqueness of the inverse follows from a purely algebraic argument. Suppose that g is another arithmetic function such that $f * g = \varepsilon$. Then we obtain

$$f^{-1} = f^{-1} * \varepsilon = f^{-1} * (f * g) = (f^{-1} * f) * g = \varepsilon * g = g. \qquad \square$$

EXAMPLE 14.6.3. The Dirichlet inverse of the constant function 1 is the Möbius function μ. Indeed, we saw in Theorem 14.4.2 that $\mu * 1 = \varepsilon$.

REMARK 14.6.4. If $f^{-1} = g$ for some arithmetic functions f and g, then it follows that $g^{-1} = f$. Indeed, the equations

$$f * g = \varepsilon \qquad \text{and} \qquad g * f = \varepsilon$$

simultaneously imply that g is the inverse of f and f is the inverse of g. Thus, we have that $1^{-1} = \mu$ and $\mu^{-1} = 1$.

THEOREM 14.6.5 (The Möbius Inversion Formula). *Consider two arithmetic functions f and g. Then we have*

$$g(n) = \sum_{d|n} f(d) \quad \Leftrightarrow \quad f(n) = \sum_{d|n} \mu(d)g\left(\frac{n}{d}\right).$$

In other words, if $g = 1 * f$ then $f = \mu * g$.

PROOF. If $g = 1 * f$, then

$$\begin{aligned} \mu * g &= \mu * (1 * f) \\ &= (\mu * 1) * f \\ &= \varepsilon * f \\ &= f. \end{aligned}$$

Conversely, if $f = \mu * g$, then

$$\begin{aligned} 1 * f &= 1 * (\mu * g) \\ &= (1 * \mu) * g \\ &= \varepsilon * g \\ &= g. \end{aligned}$$

$\square$

Exercises

Starter Exercises

14.1 Show that every even perfect number is congruent to 6 or 8 modulo 10.

14.2 Show that every even perfect number other than 28 is congruent to ±1 modulo 7.

14.3 Show that the Mersenne numbers M_n satisfy the recurrence relation

$$M_{n+2} = 3M_{n+1} - 2M_n.$$

14.4 Compute $\phi(n)$ for $n = 1, \ldots, 12$.

14.5 Show that the number $\tau(n)$ of divisors of n is odd if and only if n is a square number.

14.6 Compute $\mu * \sigma$.

Routine-Building Exercises

14.7 Let $M_n := 2^n - 1$ be the nth Mersenne number.

(a) Show that if n is even, then $3 \mid M_n$.
(b) Show that if $3 \mid n$, then $7 \mid M_n$.

14.8 Show that any Mersenne prime $M_p = 2^p - 1$ with p an odd prime satisfies the congruence

$$M_p \equiv 7 \pmod{24}.$$

14.9 Suppose that p is an odd prime, and that q is a prime divisor of the Mersenne number $M_p = 2^p - 1$. Show that

$$q \equiv 1 \pmod{2p}.$$

Conclude that $\gcd(k, M_p) = 1$ for all $1 \leq k \leq 2p$. Also use this congruence to give yet another proof of the infinitude of primes. Hint: Apply Theorem 8.5.2 (Order Theorem).

14.10 Prove the following identity, first found by Joseph Liouville [Lio1857]:

$$\sum_{d \mid n} \tau(d)^3 = \left(\sum_{d \mid n} \tau(d) \right)^2.$$

14.11 (a) Show that

$$\sigma(p^m) \mid \sigma(p^n) \quad \Leftrightarrow \quad m+1 \mid n+1.$$

(b) Let $d := \gcd(m+1, n+1)$. Show that

$$\gcd(\sigma(p^m), \sigma(p^n)) = \sigma(p^{d-1}).$$



14.12 (a) Prove that if $\gcd(a,b) = d$, then

$$\phi(ab) = \frac{d\phi(a)\phi(b)}{\phi(d)}.$$

(b) For any $n > 1$, prove that

$$\sum_{\substack{a<n \\ \gcd(a,n)=1}} a = \frac{n\phi(n)}{2}.$$

14.13 Prove that there is no positive integer $n < 2^{65}$ such that $\phi(n) = 2^{64}$.

14.14 For any $d \mid \phi(n)$ such that $d > 2$, prove that

$$\prod_{\substack{0<x<n \\ \mathrm{ord}_n(x)=d}} x \equiv 1 \pmod{n}.$$

14.15 (a) Show that

$$\frac{\phi(n)}{2} \equiv 1 \pmod{2}$$

if and only if

$$n = 4, \qquad \text{or} \qquad n = p^k, \qquad \text{or} \qquad n = 2p^k,$$

where $p \equiv 3 \pmod{4}$ is a prime.

(b) Show that

$$\frac{\phi(n)}{2} \equiv 1 \pmod{4}$$

if and only if

$$n = 4, \qquad \text{or} \qquad n = p^k, \qquad \text{or} \qquad n = 2p^k,$$

where either $p \equiv 3 \pmod{8}$ and k is odd or $p \equiv 7 \pmod{8}$ and k is even.

14.16 Compute $\mu * \mu$.

14.17 (a) Show that if two out of three arithmetic functions f, g, and $f * g$ are multiplicative, then so is the third.

(b) Show that if f is an arithmetic function such that $f(1)$ is nonzero, then f is multiplicative if and only if f^{-1} is multiplicative.

14.18 Let f be a multiplicative function.

(a) Show that

$$f^{-1}(n) = \mu(n)f(n)$$

for every square-free natural number n.

(b) Show that

$$f^{-1}(p) = -f(p) \qquad \text{and} \qquad f^{-1}(p^2) = f(p^2) - f(p)^2$$

for every prime number p.

(c) Show that

$$f^{-1}(p^m) = \sum_{k=1}^{m} (-1)^k \left(\sum_{\substack{i_1+\cdots+i_k=m \\ i_1,\ldots,i_k \geq 1}} f(p^{i_1}) \cdots f(p^{i_k}) \right).$$

14.19 Consider a prime p. Show that

$$\sum_{\substack{0<n<p-1 \\ \gcd(n,p-1)=1}} a^n \equiv \mu(\operatorname{ord}_p(a)) \frac{\phi(p-1)}{\phi(\operatorname{ord}_p(a))} \pmod{p}.$$

14.20 Write $R_n(k)$ for the number of integers $0 \leq x < n$ such that

$$x^k \equiv 1 \pmod{n}.$$

(a) Show that the function $n \mapsto R_n(k)$ is multiplicative, for each $k > 0$.
(b) Show that the number of integers $0 \leq x < n$ of order k is given by the quantity

$$A_n(k) := \sum_{d \mid k} \mu\left(\frac{k}{d}\right) R_n(k).$$

14.21 Consider a natural number of the form $n = 2^k p$, where p is an odd prime. Show that the following are equivalent:

(i) n is perfect,
(ii) $2n \mid \binom{2n}{n}$.

Hint: Use Theorem 13.4.8 (Kummer's Theorem). The forward direction was discovered by Hoon Balakram [Bal1929].

Challenge Exercises

14.22 Determine the number of reduced fractions $\frac{a}{b}$, where $0 \leq a \leq b \leq n$.

14.23 Consider the nth Fermat number $F_n = 2^{2^n} + 1$ and the mth Mersenne number $M_m = 2^m - 1$. Show that

$$\gcd(F_n, M_m) = \begin{cases} F_n & \text{if } 2^{n+1} \mid m, \\ 1 & \text{otherwise.} \end{cases}$$

14.24 For any two natural numbers $0 \leq d \leq n$, determine the number of ordered pairs (a, b) of nonnegative integers a and b such that $a + b = n$ and $\gcd(a, b) = d$.

14.25 For how many congruence classes $b \pmod{n}$ is the linear congruence

$$ax \equiv b \pmod{n}$$

solvable?

14.26 (a) Find all primes p and exponents m such that

$$v_2\left(\frac{p^{m+1}-1}{p-1}\right) = 0.$$

(b) Find all primes p and exponents m such that

$$v_2\left(\frac{p^{m+1}-1}{p-1}\right) = 1.$$

(c) (Euler) Show that if n is an odd perfect number, then n is of the form

$$p^\alpha m^2$$

where p is a prime such that $p \equiv \alpha \equiv 1 \pmod 4$ and $p \nmid m$.

14.27 Show that

$$\sigma(2^n - 1) = \prod_{\substack{p \text{ odd prime} \\ d := \operatorname{ord}_p(2) \mid n}} \frac{p^{v_p(2^d-1)+v_p(n/d)+1} - 1}{p-1}.$$

14.28 Let Ω be the arithmetic function given by

$$\Omega(m) = m_1 + \cdots + m_n$$

for any $m = p_1^{m_1} \cdots p_n^{m_n}$, where the prime factors $p_1, \ldots, p_n$ are assumed to be distinct. Thus, Ω returns the number of prime factors, counted with multiplicity. Show that

$$\Omega(m) \leq \frac{\log m}{\log\left(\frac{1}{n}\sum_{i=1}^n p_i\right)}.$$

Hint: Use Jensen's inequality.

Chapter 15

Cyclic Counting

15.1 Hemachandra Wheels

In §2.6 we considered the problem of counting the number H_n of ways we can subdivide a strip of n blocks into squares and dominoes. An equivalent formulation of this problem was stated Exercise 2.4, where the task was to find a recursive expression for the number of ways in which we could color some squares along a strip of length n blue, so that no two blue squares are adjacent; this number is H_{n+1}. How do these counts change, if instead we ask for the number of Hemachandra colorings of a cyclic strip? And how do we determine the number of those Hemachandra colorings that are rotationally distinct?

Definition 15.1.1. A **Hemachandra wheel** of order n is an n-element cyclic set in which the elements are colored white and blue, so that no two adjacent elements are both colored blue. Two Hemachandra wheels are considered to be the same when one can be obtained from the other by rotation. Elements of Hemachandra wheels will be called **segments**.

A Hemachandra wheel is said to be **labeled** if its n segments are labeled 0 through $n-1$ in cyclic ordering. Two labeled Hemachandra wheels of order n are considered to be the same if segments with matching labels have the same color.

We write W_n for the number of labeled Hemachandra wheels of order n, and we write $\tilde{W}_n$ for the number of (unlabeled) Hemachandra wheels of order n.

Remark 15.1.2. The number W_n of labeled Hemachandra wheels can be determined by considering two cases: Either the element labeled 0 is white or it is blue. In the first case, the remaining elements of the Hemachandra wheel form a strip of elements labeled 1



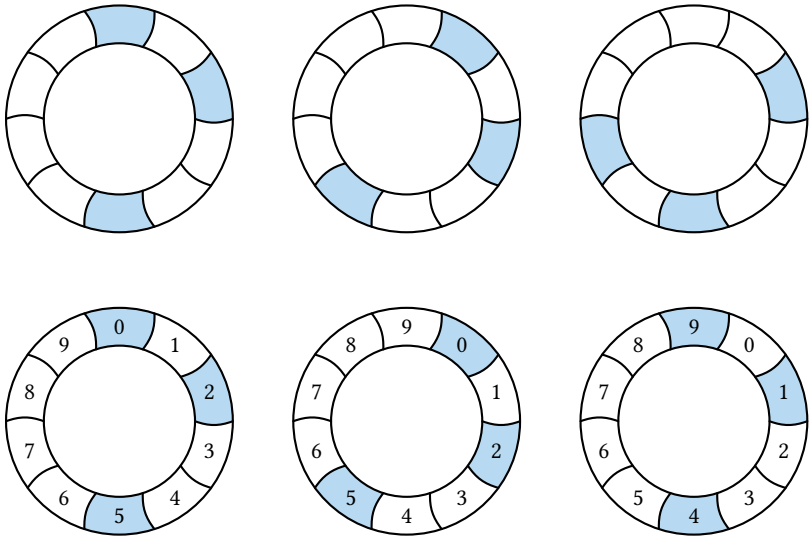


Figure 15.1: The top row displays three unlabeled Hemachandra wheels. The first and second are the same up to rotation, while the third is distinct from the other two. The bottom row displays three labeled Hemachandra wheels. The first two are the same, since their colorings match the labeling. The third is distinct from the first two since it is the only wheel among the three with a blue segment labeled 9.

through $n-1$, and the number of colorings of this strip is the Fibonacci number F_{n+1}. In the second case, the blue element labeled 0 cannot have an adjacent blue element, so the coloring of the remaining strip is determined by the coloring of the elements 2 through $n-2$. Their number is F_{n-1}. Therefore, we conclude that

$$W_n = F_{n+1} + F_{n-1}.$$

Since $F_{n+1} + F_{n-1}$ is the nth Lucas number L_n, we find that $W_n = L_n$.

THEOREM 15.1.3. *The number $\tilde{W}_p$ of unlabeled Hemachandra wheels of prime order p is*

$$\tilde{W}_p = \frac{1}{p}(F_{p+1} + F_{p-1} + p - 1),$$

where F_i denotes the ith Fibonacci number.

PROOF. All labelings of the entirely white Hemachandra wheel are the same, so it corresponds to exactly one labeled wheel. Every wheel with at least one blue segment has p distinct labelings. Indeed, if this were not so then its coloring would be preserved by a rotation through k positions for some $0 < k < p$. Since p is prime, the positions $0, k, 2k, \ldots, (p-1)k$ exhaust the wheel. Every position would therefore have the same color, a contradiction. Consequently, we have

$$W_p = 1 + p(\tilde{W}_p - 1),$$

and the result follows. □

Corollary 15.1.4. *For any prime number p we have the congruence*

$$F_{p-1} + F_{p+1} \equiv 1 \pmod{p}.$$

Proof. The number $\tilde{W}_p$ is an integer, so $p \mid F_{p+1} + F_{p-1} - 1$. □

In many cases, our main method to prove congruences is by algebraic manipulation. In the previous theorem we found a new source of congruences: *rotational symmetry!* In the present chapter we will refine this method and find many congruences that can be proven naturally with rotational symmetry.

15.2 The Prime–Fixed Point Congruence

Definition 15.2.1. We define the set of **fixed points** of a map $f : X \to X$ by

$$\mathrm{Fix}(f) := \{x \in X \mid f(x) = x\}.$$

Theorem 15.2.2 (The Prime–Fixed Point Congruence). *Consider a finite set X and a map $f : X \to X$ such that $f^p(x) = x$ for all $x \in X$, where p is a prime number. Then we have*

$$\#X \equiv \#\mathrm{Fix}(f) \pmod{p}.$$

In particular, if $\#X \not\equiv 0 \pmod{p}$, then f has a fixed point.

Proof. If $f(x) \neq x$, then the least positive n for which $f^n(x) = x$ is p. Indeed, by the assumption that p is prime, if $1 < n < p$ then there is an integer k such that $kn \equiv 1 \pmod{p}$. For such k we find that $f(x) = f^{kn}(x) = x$, contradicting our assumption on x. Thus we see that X is partitioned into orbits of size 1 and of size p, and the claim follows. □

Example 15.2.3. The congruence of Corollary 15.1.4 is an instance of Theorem 15.2.2 (The Prime–Fixed Point Congruence), since the total number of Hemachandra wheels of order p is

$$F_{p-1} + F_{p+1},$$

and the only fixed point under rotation is the entirely white Hemachandra wheel.

Example 15.2.4. Consider a set A with a elements, and a cyclic set C with p elements, where p is a prime number. Then there are a^p functions from C to A, which we view as A-colorings of the elements of C. The fixed points under rotation are precisely the colorings defined by a constant function $C \to A$. The number of such constant functions is a. Therefore we obtain from Theorem 15.2.2 (The Prime–Fixed Point Congruence) the congruence

$$a^p \equiv a \pmod{p}.$$

That is, we have proven *Fermat's Little Theorem*. This theorem is of such great consequence in the theory of numbers, that we will devote the entire next chapter to it and its consequences. The proof given here was found by Solomon Golomb [Gol1956].



15.3 Lucas's Theorem

Our next application of Theorem 15.2.2 is a theorem due to Édouard Lucas [LUC1878b], which allows us to compute the residue class of binomial coefficients modulo a prime. This theorem is complementary to Theorem 13.4.8 (Kummer's Theorem), which gives a complete description of the prime factorization of binomial coefficients. The proof we present below is due to Bruce Sagan [SAG2020, Theorem 6.5.6].

THEOREM 15.3.1 (Lucas's Theorem). *Consider a prime number p, and natural numbers m and n written in base p as*

$$m = \sum_{i=0}^{k} a_i p^i \qquad \text{and} \qquad n = \sum_{i=0}^{k} b_i p^i.$$

Then the congruence

$$\binom{n}{m} \equiv \prod_{i=0}^{k} \binom{b_i}{a_i} \pmod{p}$$

holds. In particular, if $b_i < a_i$ for some i, then $\binom{n}{m}$ is divisible by p.

PROOF. By Euclidean division, write $m = m'p + a_0$ and $n = n'p + b_0$, so that

$$m' = \sum_{i=0}^{k-1} a_{i+1} p^i \qquad \text{and} \qquad n' = \sum_{i=0}^{k-1} b_{i+1} p^i$$

It suffices to show that

$$\binom{n}{m} \equiv \binom{n'}{m'}\binom{b_0}{a_0} \pmod{p},$$

since the claim follows by iterating this congruence. Consider an n-element set X and a map $f : X \to X$ so that the number of p-cycles is n' and the number of fixed points is b_0. Then we can define a map φ on the set of m-element subsets of X by

$$\varphi(U) := \{f(x) \mid x \in U\}.$$

The image of an m-element subset U under f is indeed again an m-element subset. Furthermore, since f satisfies $f^p(x) = x$ for all $x \in X$, it also follows that $\varphi^p(U) = U$ for every m-element subset of X. Therefore it follows by Theorem 15.2.2 that

$$\binom{n}{m} \equiv \#\mathrm{Fix}(\varphi) \pmod{p}.$$

Now observe that $\varphi(U) = U$ if and only if for every $x \in U$ we have $f(x) \in U$. This means that for every $x \in U$, the entire orbit under f is contained in U. As we have seen in Theorem 15.2.2, these orbits have either p elements or 1 element. Since the number of fixed points of f is $0 \leq b_0 < p$, it follows that every m-element subset contains

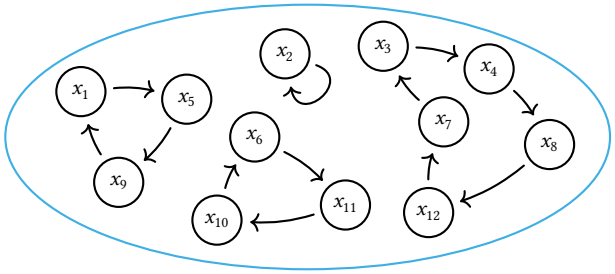


Figure 15.2: A bijection on a 12-element set.

of a number t of orbits with p elements, and a number $0 \leq c < p$ of fixed points, which allows us to write $m = tp + c$. By the uniqueness property of Theorem 5.3.1 (The Euclidean Division Theorem), it follows that $t = m'$ and $c = a_0$. We conclude that a fixed point U of φ consists of a choice of m' orbits with p elements and a choice of a_0 fixed points of f, so that

$$\#\mathrm{Fix}(\varphi) = \binom{n'}{m'}\binom{b_0}{a_0}. \qquad \square$$

15.4 The Orbit–Counting Formula

Recall from Exercise 8.14 that if the orbit of x under a bijection $f : X \to X$ contains exactly t elements, then

$$f^k(x) = x \quad \Leftrightarrow \quad t \mid k. \tag{$*$}$$

That is, x is a *fixed point* of the map $f^k : X \to X$ if and only if k is a multiple of the number of elements in the orbit of x.

Example 15.4.1. Consider the bijection f displayed in Figure 15.2. Since x_1 is in a 3-element orbit, it follows that x_1 is a fixed point for f^k if and only if k is a multiple of 3. Likewise, x_3 is in a 5-element orbit so it is a fixed point for f^k if and only if k is a multiple of 5. The element x_2 is a fixed point of f, so it is a fixed point of f^k for every $k \geq 0$.

The bijection displayed in Figure 15.2 satisfies $f^{15}(x) = x$ for all $x \in X$, since the length of every orbit is a divisor of 15. Running through all $0 \leq k < 15$, we see that the orbit of length 1 contributes a fixed point for every k; each orbit of length 3 contributes 3 fixed points every third k; and the orbit of length 5 contributes 5 fixed points every fifth k. Indeed, listing out the number of fixed points for f^k we get the following table

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\#\mathrm{Fix}(f^k)$	12	1	1	7	1	6	7	1	1	7	6	1	7	1	1

Adding up all these totals gives us $60 = 4 \cdot 15$. We therefore see that the average number of fixed points of f^k over $0 \leq k < 15$ is exactly the number of orbits. We note also

that $\#\mathrm{Fix}(f^k) = 1$ precisely when $\gcd(k, 15) = 1$; that $\#\mathrm{Fix}(f^k) = 7$ precisely when $\gcd(k, 15) = 3$; and that $\#\mathrm{Fix}(f^k) = 6$ precisely when $\gcd(k, 15) = 5$. Since for any $k \mid l$ we have $\gcd(l, n) = k$ if and only if $\gcd(l/k, n/k) = 1$, the number of which are determined by Euler's totient function ϕ, these observations suggest that

$$\frac{1}{15} \sum_{k|15} \phi(15/k)\, \#\mathrm{Fix}(f^k) = 4.$$

That is, the average number of fixed points of f^k, being equal to the number of orbits, can be organized as a divisor-sum. We establish this relation between orbits and fixed points in the following theorem.

THEOREM 15.4.2 (The Orbit–Counting Formula). *Consider a bijection $f : X \to X$ on a finite set X, and suppose that $f^n(x) = x$ for all $x \in X$, where n is a positive integer. Let N be the number of orbits of f. Then we have*

$$N = \frac{1}{n} \sum_{k|n} \phi(n/k)\, \#\mathrm{Fix}(f^k).$$

PROOF. For each divisor $k \mid n$ and each $1 \leq l \leq n$ such that $\gcd(l, n) = k$, we have $\#\mathrm{Fix}(f^l) = \#\mathrm{Fix}(f^k)$. To see this, consider an element x in an orbit of length t. Since t is a divisor of n, it follows that $t \mid l$ if and only if $t \mid k$, which implies the claim. The number of integers $1 \leq l \leq n$ such that $\gcd(l, n) = k$ is $\phi(n/k)$, so we obtain that

$$\frac{1}{n} \sum_{k|n} \phi(n/k)\, \#\mathrm{Fix}(f^k) = \frac{1}{n} \sum_{k=1}^{n} \#\mathrm{Fix}(f^k) = \frac{1}{n} \sum_{k=0}^{n-1} \#\mathrm{Fix}(f^k).$$

Now label the orbits of f with indices 1 through N, and let f_i be the restriction of f to the ith orbit. Then it follows that

$$\#\mathrm{Fix}(f^k) = \sum_{i=1}^{N} \#\mathrm{Fix}(f_i^k).$$

Consequently, we have

$$\sum_{k=0}^{n-1} \#\mathrm{Fix}(f^k) = \sum_{k=0}^{n-1} \sum_{i=1}^{N} \#\mathrm{Fix}(f_i^k) = \sum_{i=1}^{N} \sum_{k=0}^{n-1} \#\mathrm{Fix}(f_i^k).$$

Therefore it suffices to prove that

$$\frac{1}{n} \sum_{k=0}^{n-1} \#\mathrm{Fix}(f_i^k) = 1$$

for all $1 \leq i \leq N$.

For each $1 \leq i \leq N$, write t_i for the number of elements in the ith orbit. By the logical equivalence Equation $(*)$, which was shown in Exercise 8.14, it follows that

$$\#\mathrm{Fix}(f_i^k) = \begin{cases} t_i & \text{if } t_i \mid k, \\ 0 & \text{otherwise.} \end{cases}$$

Since the number of multiples of t_i among the integers 0 through $n-1$ is n/t_i, we conclude that

$$\sum_{k=0}^{n-1} \#\mathrm{Fix}(f_i^k) = \frac{n}{t_i} t_i = n,$$

and the claim follows. □

Remark 15.4.3. Theorem 15.4.2 (The Orbit–Counting Formula) is a special case of a more general theorem of group theory, called *Burnside's Lemma*.

Example 15.4.4. Let B be a cyclic set consisting of n beads, with one-step rotation $r : B \to B$, and let C be a set of c colors. Then a C-coloring of B is a function $B \to C$, and we obtain a bijection f on the C-colorings of B by the rotation on B. Two C-colorings are considered the same if one can be obtained from the other by rotation; that is, if they are in the same orbit under f.

For each $k \mid n$, the colorings fixed under the k-step rotation f^k are precisely the colorings that are constant on the orbits of r^k on B, of which there are k. Therefore we have

$$\#\mathrm{Fix}(f^k) = c^k.$$

Now it follows by Theorem 15.4.2 (The Orbit–Counting Formula) that the number of rotationally distinct ways to color the cyclic set B is

$$\frac{1}{n} \sum_{k \mid n} \phi(n/k) \cdot c^k.$$

For example, the number of 3-colored necklaces with 10 beads is

$$\frac{1}{10}(\phi(10) \cdot 3^1 + \phi(5) \cdot 3^2 + \phi(2) \cdot 3^5 + \phi(1) \cdot 3^{10}) = 5934.$$

15.5 The Divisor Sum of the Totient Function

The orbit–counting theorem implies an important identity, which is sometimes known as **Gauss's theorem**.

Theorem 15.5.1. *Euler's totient function ϕ satisfies the following divisor-sum identity:*

$$\sum_{k \mid n} \phi(k) = n.$$



PROOF VIA THE ORBIT–COUNTING THEOREM. Consider the singleton set $X = \{\star\}$ and let $f : X \to X$ be the identity function. Then f has one orbit. Furthermore, $\#\mathrm{Fix}(f^k) = 1$ for every k, so we obtain by Theorem 15.4.2

$$1 = \frac{1}{n} \sum_{k|n} \phi(k). \qquad \square$$

Of an identity so fair as the one obtained in Theorem 15.5.1 it is only appropriate to admire and treasure it. What better way is there to savor a theorem than to prove it again, to established it on its own, and then yet again?

COMBINATORIAL PROOF. The sum suggests that there is a way of partitioning the set $\{1, \dots, n\}$ into sets A_d of size $\phi(d)$, and this is indeed how this theorem is proven. For each positive divisor d of n, define the map

$$f_k : \{1 \leq x \leq k \mid \gcd(x, k) = 1\} \to \{1, \dots, n\}$$

by $x \mapsto \frac{n}{k} x$, and define the set A_k to be the image of f_k. Since $\frac{n}{k}$ is a positive integer, it follows that the map f_k is injective, and therefore each set A_k has exactly $\phi(k)$ elements. Now notice that

$$y \in A_k \quad \Leftrightarrow \quad \gcd(y, n) = \frac{n}{k},$$

since if $x = y/\gcd(y, n)$, then $\gcd(x, k) = \gcd(y/\gcd(y, n), n/\gcd(y, n)) = 1$. Therefore, it follows that for every $1 \leq y \leq n$ there is exactly one $k \mid n$ such that $y \in A_k$, so it follows that the sets A_k partition the set $\{1, \dots, n\}$. The sum of the numbers of elements of each A_k is therefore n. $\square$

ARITHMETIC PROOF. Recall from Theorem 14.2.4 that ϕ is a multiplicative function, which implies by Theorem 14.3.4 that the function

$$n \mapsto \sum_{k|n} \phi(k)$$

is multiplicative. Since multiplicative functions are completely determined by their values on prime powers, it suffices to show that

$$\sum_{k|p^m} \phi(k) = p^m.$$

The only divisors of p^m are p^k for $0 \leq k \leq m$, and for any $k \geq 1$ we have $\phi(p^k) = p^k - p^{k-1}$. Thus, it follows that

$$\sum_{k|p^m} \phi(k) = \sum_{k=0}^{m} \phi(p^k) = 1 + \sum_{k=1}^{m} p^k - p^{k-1} = 1 + (p^m - 1) = p^m. \qquad \square$$

In terms of Dirichlet convolution, the identity in Theorem 15.5.1 can be stated as follows:

$$\phi * 1 = \mathrm{id}.$$

Corollary 15.5.2. *Euler's totient function satisfies the identity*

$$\phi(n) = \sum_{k|n} \mu(k)\frac{n}{k}$$

In other words, $\phi = \mu * \mathrm{id}$.

Proof. By Theorem 15.5.1 we have $\mathrm{id} = 1 * \phi$, so we have $\phi = \mu * \mathrm{id}$ by the Möbius inversion formula. □

We also give a direct proof of Corollary 15.5.2.

Direct proof of Corollary 15.5.2. Note that Euler's totient function ϕ can be written in the form

$$\phi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{\gcd(k,n)} \right\rfloor.$$

Then it follows from Theorem 14.4.2 that

$$\phi(n) = \sum_{k=1}^{n} \sum_{d\,|\,\gcd(k,n)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d) = \sum_{d|n} \sum_{\substack{k=1 \\ d|k}}^{n} \mu(d) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

The last step follows, since there are exactly $\frac{n}{d}$ multiples of d among the numbers from 1 to n. □

15.6 Arithmetic Functions of Orbits and Fixed Points

The formula

$$\frac{1}{n}\sum_{k|n} \phi(n/k)\,\#\mathrm{Fix}(f^k)$$

for the number of orbits of a bijection $f : X \to X$ satisfying $f^n(x) = x$ for all x suggests that we can treat of orbits and fixed points in terms of arithmetic functions and their Dirichlet convolution.

Definition 15.6.1. Consider a map $f : X \to X$ on a finite set X. We write

$$\nu_f(n) := \#\mathrm{Fix}(f^n) \qquad \text{and} \qquad \gamma_f(n) := \#\{f\text{-orbits of length } n\}.$$

Since x is a fixed point for f^n if and only if the length of the orbit of x divides n, we obtain the formula

$$\nu_f(n) = \sum_{k|n} k\,\gamma_f(k). \tag{15.1}$$



We will write $f \cdot g$ for the *pointwise multiplication* of f and g and we will write f/g for the *pointwise division* of f by g; that is,

$$(f \cdot g)(n) = f(n)g(n) \qquad \text{and} \qquad (f/g)(n) = f(n)/g(n).$$

Using these conventions, we see that the arithmetic functions ν_f and γ_f are related to each other by the following identities.

PROPOSITION 15.6.2. *Consider a bijection $f : X \to X$ on a finite set X. Then*

$$\nu_f = 1 * (\mathrm{id} \cdot \gamma_f) \qquad \textit{and} \qquad \gamma_f = \frac{\mu * \nu_f}{\mathrm{id}}.$$

The following corollary generalizes the Theorem 15.2.2 (The Prime–Fixed Point Congruence).

COROLLARY 15.6.3 (The Gauss congruence). *For any bijection $f : X \to X$ on a finite set X, we have*

$$\sum_{d|n} \mu(d)\nu_f(n/d) \equiv 0 \pmod{n}.$$

In particular, we have

$$\nu_f(p^m) \equiv \nu_f(p^{m-1}) \pmod{p^m}.$$

PROOF. Since the quantity

$$\gamma_f(n) = \frac{1}{n} \sum_{d|n} \mu(d)\nu_f(n/d)$$

is the integer, determining the number of f-orbits of length n, it follows that the sum is an integer divisible by n. □

Defining

$$\omega_f := (\nu_f * \phi)/\mathrm{id},$$

Theorem 15.4.2 asserts that $\omega_f(n)$ is the number of orbits of f if $f^n(x) = x$ for all $x \in X$.

THEOREM 15.6.4. *Consider a bijection f on a finite set X. Then*

$$\omega_f = 1 * \gamma_f.$$

Consequently, the quantity

$$\frac{1}{n} \sum_{k|n} \phi(n/k)\, \#\mathrm{Fix}(f^k) = \sum_{k|n} \gamma_f(k)$$

is an integer for every n, and counts the number of orbits whose length divides n.

Proof. Since $\nu_f = (\mathrm{id} \cdot \gamma_f) * 1$, it follows that

$$\nu_f * \phi = \nu_f * \mu * \mathrm{id} = (\mathrm{id} \cdot \gamma_f) * \mathrm{id} = \mathrm{id} \cdot (\gamma_f * 1). \qquad \square$$

Example 15.6.5. Consider an n-element cyclic set C with one-step rotation r. For each $k \mid n$, the k-step rotation r^k by partitions C into k orbits of size n/k. An m-element subset of C is then fixed under r^k precisely when it is a union of r^k-orbits. More conveniently, an m-element subset of C is fixed under $r^{n/k}$ precisely when it is a union of $r^{n/k}$-orbits, of which there are k. Therefore, it follows that

$$\nu_f(n/k) = \begin{cases} \binom{n/k}{m/k} & \text{if } k \mid m, \\ 0 & \text{otherwise.} \end{cases}$$

This implies that

$$\gamma_r(n) = \frac{1}{n} \sum_{k \mid \gcd(m,n)} \mu(k) \binom{n/k}{m/k}.$$

Gauss's congruence in this case asserts that

$$\sum_{k \mid \gcd(m,n)} \mu(k) \binom{n/k}{m/k} \equiv 0 \pmod{n}.$$

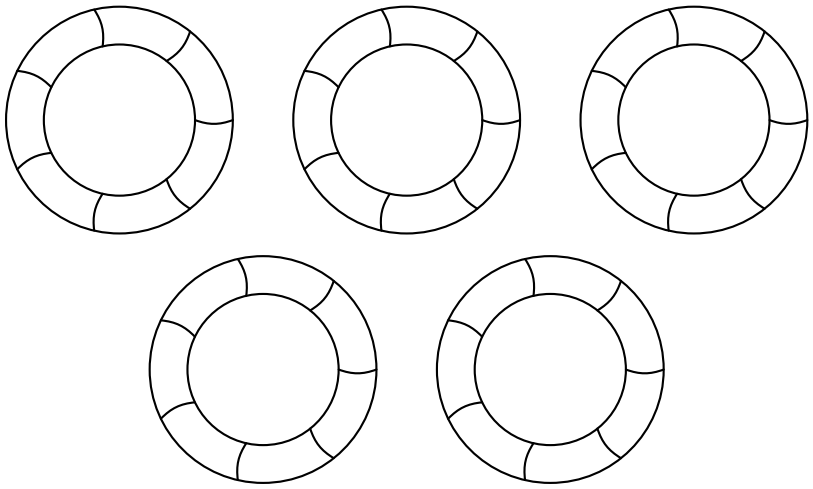


Figure 15.3: Shade the segments of these wheels so as to find all Hemachandra wheels of order 7.

Exercises

Starter Exercises

15.1 Find all the distinct unlabeled Hemachandra wheels of order 7.

Routine-Building Exercises

15.2 Let $n = mp^k$, where p is a prime such that $p \nmid m$, and let F be the sequence of Fibonacci numbers. Prove the **Gauss congruence** for Lucas numbers

$$F_{n-1} + F_{n+1} \equiv F_{n/p-1} + F_{n/p+1} \pmod{p^k}.$$

15.3 Consider a prime p. Show that

$$\binom{n}{m} \equiv \binom{n-p}{m-p} + \binom{n-p}{m} \pmod{p}.$$

15.4 Determine the number of labeled and unlabeled bicolored wheels with n segments in which no three adjacent segments all have the same color.

15.5 Prove that

$$\sum_{k=1}^{n} \gcd(k,n)\mu(\gcd(k,n)) = \mu(n).$$

Challenge Exercises

15.6 Define **Jordan's totient function** $J_k(n)$ by

$$J_k(n) = \#\{(x_1, \dots, x_k) \mid 1 \le x_1, \dots, x_k \le n \text{ and } \gcd(x_1, \dots, x_k, n) = 1\}.$$

In other words, Jordan's totient function counts the number of k-tuples $(x_1, \dots, x_k)$ of positive integers not exceeding n such that if d simultaneously divides all the integers $x_1, \dots, x_k$ and n, then $d = 1$. Note that $J_1(n)$ is just Euler's totient function ϕ.

(a) Find $J_2(n)$ for $1 \le n \le 12$.

(b) Show that for any divisor d of n, the number of elements in the set

$$\left\{(x_1, \dots, x_k) \,\middle|\, 1 \le x_1, \dots, x_k \le n \text{ and } \gcd(x_1, \dots, x_k, n) = \frac{n}{d}\right\}$$

is exactly $J_k(d)$.

(c) Show that

$$\sum_{d \mid n} J_k(d) = n^k \qquad \text{and} \qquad \sum_{d \mid n} \mu(d) \left(\frac{n}{d}\right)^k = J_k(n).$$

(d) Show that J_k is a multiplicative function.

(e) Show that

$$J_k(p^m) = p^{km} - p^{k(m-1)}$$

for any prime p and any exponent $m \ge 1$.

(f) Show that

$$J_k(n) = n^k \prod_{p \mid n} \left(1 - \frac{1}{p^k}\right).$$

Chapter 16

Fermat's Little Theorem and its Consequences

16.1 Fermat's Little Theorem

Theorem 16.1.1 (Fermat's Little Theorem). *Consider a prime number p and an integer a. Then the congruence*

$$a^p \equiv a \pmod{p}$$

holds.

Remark 16.1.2. Note that the congruence $(-a)^p \equiv -a^p \pmod{p}$ holds for all primes p, so it suffices to prove the claim for the nonnegative integers.

We already saw a proof of Fermat's Little Theorem in Example 15.2.4. The following proof, which proceeds by mathematical induction and makes use of the Theorem 3.5.1 (The Binomial Theorem), was first published by Leonhard Euler. Euler, however, was not the first to discover it [Dic1919, p. 59]. Several decades prior, this proof was discovered by Gottfried Wilhelm Leibniz, which was only published posthumously in [Lei1863].

The additive proof. This proof is by induction on a. The base case $0^p \equiv 0 \pmod{p}$ clearly holds. For the inductive step, assume that $a^p \equiv a \pmod{p}$. Theorem 3.5.1 (The Binomial Theorem) then gives us that

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k$$

However, note that $p \mid \binom{p}{k}$ for any $0 < k < p$. We therefore find that

$$(a+1)^p \equiv a^p + 1 \pmod{p}.$$

Since $a^p \equiv a \pmod{p}$ holds by the induction hypothesis, the claim follows. □

COROLLARY 16.1.3. *Consider a prime number p and an integer a not divisible by p. Then the congruence*

$$a^{p-1} \equiv 1 \pmod{p}$$

holds.

PROOF. Since a is not divisible by p, it follows that a is relatively prime to p, and therefore the claim follows from the cancellation law

$$ax \equiv ay \pmod{p} \quad \Rightarrow \quad x \equiv y \pmod{p}.$$ □

Fermat's Little Theorem can be used to analyze the prime divisors of special numbers such as Fermat numbers or Mersenne numbers. Regarding Fermat numbers, we have the following theorem, which is of great help when trying to prove or disprove that a Fermat number is prime.

THEOREM 16.1.4. *If p is a prime divisor of a Fermat number $F_n := 2^{2^n} + 1$, then*

$$p \equiv 1 \pmod{2^{n+1}}.$$

PROOF. If p is a prime divisor of $2^{2^n} + 1$, then it follows that

$$2^{2^n} \equiv -1 \pmod{p}.$$

This implies via Theorem 8.5.2 (Order Theorem) that $\mathrm{ord}_p(2) \mid 2^{n+1}$. In particular, $\mathrm{ord}_p(2) = 2^k$ for some number $k \leq n+1$. However, note that

$$2^{2^k} \equiv 1 \pmod{p} \qquad \text{implies} \qquad 2^{2^{k+1}} = (2^{2^k})^2 \equiv 1 \pmod{p}.$$

Since $2^{2^n} \equiv -1 \pmod{p}$, it follows that the order of 2 modulo p cannot divide 2^n. Thus, it follows that $\mathrm{ord}_p(2) = 2^{n+1}$. By Theorem 16.1.1 (Fermat's Little Theorem), we conclude that

$$2^{n+1} \mid p - 1.$$ □

COROLLARY 16.1.5. *The fourth Fermat number $2^{2^4} + 1 = 65537$ is prime.*

PROOF. Any prime divisor of $F_4 = 2^{2^4} + 1$ must satisfy the congruence $p \equiv 1 \pmod{33}$. If F_4 is composite, then it must have a prime divisor below $\sqrt{F_4}$, and thus below $2^8 = 256$. The sieve of Eratosthenes displayed in Figure 13.1 reveals that the only two primes $p \equiv 1 \pmod{33}$ below 256 are 97 and 193. A quick computation gives that

$$F_4 \equiv 62 \pmod{97} \qquad \text{and} \qquad F_4 \equiv 110 \pmod{193},$$

so that neither 97 nor 193 is a prime divisor of F_4, and therefore we conclude that F_4 is prime. □

Corollary 16.1.6. *The fifth Fermat number* $2^{2^5}+1 = 4,294,967,297$ *is composite, and its smallest prime factor is* 641.

Proof. By Theorem 16.1.4 it follows that any prime divisor of $2^{2^5}+1$ must satisfy

$$p \equiv 1 \pmod{2^6}.$$

The prime numbers of the form $64k+1$ below one thousand are 193, 257, 449, 577, and 641, as can be read off of Figure 13.1. We will prove that 193, 257, 449, and 577 do not divide F_5, and that 641 does.

(i) First, we note that $3 \cdot 2^6 \equiv -1 \pmod{193}$, which implies that

$$3 \equiv -2^{-6} \pmod{193}.$$

A quick computation shows that $3^2 = 9$, $3^4 = 81 = 2^6 + 2^4 + 1$, and $3^8 = 6561 = 34 \cdot 193 - 1$, so that

$$3^8 \equiv -1 \pmod{193}$$

and thus $\operatorname{ord}_{193}(3) = 16$. It follows that

$$1 \equiv 3^{16} \equiv (-2)^{6\cdot 16} \equiv 2^{96} \pmod{193},$$

which allows us to conclude that $\operatorname{ord}_{193}(2) \mid 96$. Now observe that if $193 \mid F_5$ so that $2^{32} \equiv -1 \pmod{193}$, then we'd have $\operatorname{ord}_{193}(2) = 64 \nmid 96$, a contradiction.

(ii) Note that 257 is itself a Fermat number. In Theorem 13.3.3 (Goldbach's Theorem) we showed that any two distinct Fermat numbers are relatively prime, so that $257 \nmid F_5$.

(iii) To show that $449 \nmid 2^{32}+1$, we will simply compute $2^{32} \pmod{449}$. Note that $2^9 \equiv 2^6 - 1 \pmod{449}$. This allows us to compute

$$\begin{aligned} 2^{16} &\equiv 2^7(2^6-1) \\ &\equiv 2^{13} - 2^7 \\ &\equiv 2^4(2^6-1) - 2^7 \\ &\equiv 2^{10} - 2^7 - 2^4 \\ &\equiv 2(2^6-1) - 2^7 - 2^4 \\ &\equiv -2^4 - 2 \pmod{449}. \end{aligned}$$

It follows that $2^{32} \equiv (-2^4-2)^2 \equiv 2^8 + 2^6 + 2^2 \equiv 324 \pmod{449}$, so we see that $2^{32} \not\equiv -1 \pmod{449}$.

(iv) Here we note that $2^9 \equiv -(2^6+1) \pmod{577}$. By a similar calculation as above, we compute that

$$2^{32} \equiv -2^8 - 2^5 - 2 \equiv 287 \pmod{577}.$$

Since $2^{32} \not\equiv -1 \pmod{577}$, it follows that $577 \nmid F_5$.

(v) Finally, we prove that $641 \mid F_5$. Euler's insight was that $641 = 5^4 + 2^4$, so that

$$5^4 \equiv -2^4 \pmod{641}.$$

Furthermore, we have $641 = 5 \cdot 2^7 + 1$, so that $5 \equiv -2^{-7} \pmod{641}$. It follows that

$$2^{32} \equiv 2^4 \cdot 2^{7\cdot 4} \equiv -5^4 \cdot 2^{7\cdot 4} \equiv -(5 \cdot 2^7)^4 \equiv -(-1)^4 \equiv -1 \pmod{641}.$$

We conclude that $641 \mid 2^{32} + 1$. □

REMARK 16.1.7. Édouard Lucas showed that any prime divisor $p \mid F_n$ of the nth Fermat number F_n, where $n \geq 2$, must in fact be of the form $k2^{n+2} + 1$. Had Euler known this stronger restriction on the prime divisors of the Fermat numbers, he wouldn't even have to cover the cases 193, 449, and 577!

16.2 Euler's Theorem

Euler figured out a way to generalize Fermat's Little Theorem to the composite moduli. He made use of his totient function ϕ, which counts for each n the number of $0 \leq m < n$ relatively prime to n.

THEOREM 16.2.1 (Euler's Theorem). *Consider a natural number n and an integer a such that $\gcd(a, n) = 1$. The congruence*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

holds

We present two proofs of Euler's Theorem. The first is the standard proof, and the other is inspired by methods of group theory.

FIRST PROOF OF EULER'S THEOREM. Consider an integer a relatively prime to n, and consider a reduced residue system $r_1, \ldots, r_{\phi(n)}$ modulo n. We claim that

$$ar_1, \ldots, ar_{\phi(n)}$$

is again a reduced residue system modulo n. Indeed, since multiplying by a induces a bijection on $\mathbb{Z}/n\mathbb{Z}$, we see that all integers $ar_1, \ldots, ar_{\phi(n)}$ are incongruent. Furthermore, the product of any two integers relatively prime to n is again relatively prime to n, so all the integers ar_i are relatively prime to n. Since any set of $\phi(n)$ incongruent integers relatively prime to n form a reduced residue system, the claim follows.

Using that the integers $ar_1, \ldots, ar_{\phi(n)}$ form a reduced residue system, it follows that

$$\prod_{i=1}^{\phi(n)} r_i \equiv \prod_{i=1}^{\phi(n)} ar_i = a^{\phi(n)} \prod_{i=1}^{\phi(n)} r_i \pmod{n}$$

Since $\prod_{i=1}^{\phi(n)} r_i$ is relatively prime to n, it follows that $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Second proof of Euler's theorem. Consider the least positive integer k such that $a^k \equiv 1 \pmod{n}$, and consider the relation $\sim$ on the set of integers $0 \leq b < n$ relatively prime to n, where

$$b \sim c \qquad \text{if and only if} \qquad \exists_{0 \leq i < k} ba^i \equiv c \pmod{n}.$$

This relation is reflexive, because $ba^0 \equiv b \pmod{n}$. It is symmetric, because if $ba^i \equiv c \pmod{n}$ for some nonzero i, then $ca^{k-i} \equiv ba^i a^{k-i} \equiv b \pmod{n}$. Furthermore, it is transitive, because if $ba^i \equiv c$ and $ca^j \equiv d$, then $ba^{i+j} \equiv d$. If $k \leq i + j$, then we find that also $ba^{i+j-k} \equiv d$. Thus, the relation $\sim$ is an equivalence relation.

We claim that each equivalence class has size k. Indeed, for each b, the set

$$\{b, ba, ba^2, \ldots, ba^{k-1}\}$$

consists of k distinct elements, because multiplying with b is a bijection. Thus we have partitioned the set of all numbers $0 \leq b < n$ relatively prime to n into equivalence classes of size k. On the other hand, the total number of elements $0 \leq b < n$ relatively prime to n is the number $\phi(n)$. This shows that $k \mid \phi(n)$, so it follows that $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Remark 16.2.2. The second proof of Euler's theorem can be simplified using the language of group theory. A **group** is a set G equipped with a binary operation $x, y \mapsto xy$, a unary operation $x \mapsto x^{-1}$, and a unit element 1, satisfying the axioms

$$\begin{aligned} (xy)z &= x(yz) \\ x1 &= x \\ 1x &= x \\ xx^{-1} &= 1 \\ x^{-1}x &= 1. \end{aligned}$$

One can show that the set of integers modulo n relatively prime to n forms a group, where the binary operation is multiplication, the unit element is the integer 1, and the inverse x^{-1} of an integer x modulo n is the unique solution to the equation $xy \equiv 1 \pmod{n}$. The number of elements in this group is $\phi(n)$. For any integer a modulo n relatively prime to n such that $a^k \equiv 1 \pmod{n}$, the set $\{1, a, a^2, \ldots, a^{k-1}\}$ is a subgroup, which means that it is closed under the group operations. The argument where we introduced an equivalence relation $\sim$ to partition the set of all integers modulo n relatively prime to n into equivalence classes of size k is an instance of a much more general result, Lagrange's Theorem, which asserts that the size of any subgroup of a finite group divides the size of the entire group.

Since $\phi(p) = p - 1$, it follows that Theorem 16.1.1 (Fermat's Little Theorem) is also a direct corollary of Theorem 16.2.1 (Euler's Theorem).



REMARK 16.2.3. We saw the multiplicative order featuring in the second proof of Theorem 16.2.1 (Euler's Theorem). Thus, using the second proof of Euler's theorem we immediately observe that

$$\mathrm{ord}_n(a) \mid \phi(n),$$

for any a and n such that $\gcd(a, n) = 1$.

Some questions about Euler's totient function remain unresolved. While we have seen that $\phi(p) = p - 1$ for any prime number p, Lehmer asked whether there is any composite number n such that

$$\phi(n) \mid n - 1.$$

This open problem is now known as **Lehmer's problem** [LEH1933].

16.3 Wilson's Theorem

The following theorem is a factorial criterion by which to decide whether a number is prime. It states that n is prime if and only if the congruence

$$(n-1)! \equiv -1 \pmod{n}$$

holds.

In the European mathematical tradition, it was first published by Edward Waring, who attributed it as follows to John Wilson [WAR1782, p. 380] along with high praise: *This most elegant property of prime numbers was discovered by the most illustrious and most skilled mathematician, John Wilson, Esquire.* However, neither Wilson nor Waring were able to rigorously prove this property of the prime numbers. The first to give a proof was Joseph–Louis Lagrange [LAG1771]. Euler, and later Gauss, gave separate proofs of this fact.

THEOREM 16.3.1 (Wilson's Theorem). *A natural number $n \geq 2$ is prime if and only if*

$$(n-1)! \equiv -1 \pmod{n}.$$

PROOF. First, we observe that the claim holds for $n = 2$, since $1 \equiv -1 \pmod{2}$.

Suppose that n is prime strictly greater than 2. Then every integer $0 < a < n$ has a multiplicative inverse modulo n, meaning that for every integer a there is an integer a^{-1} such that

$$aa^{-1} \equiv 1.$$

Now we group the integers $1 \leq a < n$ into pairs with their inverses. By Exercise 13.6 and the assumption that $n \neq 2$, there are exactly two integers that would pair up with themselves because they are their own inverses: The integers 1 and -1 are the only two integers a modulo n for which the congruence $a^2 \equiv 1 \pmod{n}$ holds. The other integers come in proper pairs (a, a^{-1}). Therefore, we have

$$(n-1)! \equiv 1(n-1) \equiv -1 \pmod{n}.$$

Conversely, suppose that the congruence $(n-1)! \equiv -1 \pmod{n}$ holds. Since any $0 < a < n$ is a divisor of $(n-1)!$, it follows that for any such a there is a solution to the linear congruence

$$ax \equiv -1 \pmod{n}.$$

This implies that any $0 < a < n$ is invertible modulo n, so it follows that $\gcd(a, n) = 1$ for all $0 < a < n$. We conclude that the only proper divisor of n is 1, and therefore n is prime. □

Second proof of the forward direction of Theorem 16.3.1 (Wilson's Theorem). Consider a prime p, and consider the monic polynomial

$$f(x) = \prod_{k=0}^{p-1}(x-k).$$

Since every element is a root of $f(x)$ modulo p, it follows by Theorem 16.1.1 (Fermat's Little Theorem) that $f(x) \equiv x^p - x \pmod{p}$. Since $f(x) = xg(x)$, where $g(x) := \prod_{k=1}^{p-1}(x-k)$, it follows by the product rule for differentiation that

$$f'(x) = xg'(x) + g(x).$$

This shows that $f'(0) = g(0)$. On the other hand the derivative of $x^p - x$ is $px^{p-1} - 1$. Thus, we conclude that

$$k! = \prod_{k=1}^{p-1}(0-k) \equiv -1 \pmod{p}.$$ □

16.4 Some Theorems Concerning Strong Divisibility Sequences

Example 16.4.1. Consider the pth Mersenne number $M_p = 2^p - 1$, where p is an odd prime. We claim that the following congruence holds:

$$\prod_{k=1}^{p-1}(2^k + 1) \equiv 1 \pmod{M_p}.$$

To see this, set $A := \prod_{k=1}^{p-1}(2^k - 1)$ and $B := \prod_{k=1}^{p-1}(2^k + 1)$. Then we have

$$AB = \prod_{k=1}^{p-1}(2^{2k} - 1).$$

The order of 2 modulo M_p is p. It follows that $2^k - 1 \equiv 2^l - 1 \pmod{M_p}$ if and only if $k \equiv l \pmod{p}$. Since p was assumed to be odd, multiplication by 2 is a bijection modulo p, so we conclude that

$$\prod_{k=1}^{p-1}(2^{2k} - 1) \equiv \prod_{k=1}^{p-1}(2^k - 1) \pmod{M_p},$$



since both products have the same factors modulo M_p. This shows that $AB \equiv A \pmod{M_p}$. Moreover, A is invertible modulo M_p, since A is a product of invertible numbers:

$$\gcd(2^k - 1, 2^p - 1) = 2^{\gcd(k,p)} - 1 = 1.$$

Therefore, we cancel A on both sides to obtain $B \equiv 1 \pmod{M_p}$.

This example relies on having a bijection which rearranges the order of the factors in a product. This idea is generalizable; particularly to the setting of strong divisibility sequences.

THEOREM 16.4.2. *Let (u_m) be a strong divisibility sequence. Furthermore, suppose there is a natural number n and an integer c such that*

$$u_{m+n} \equiv cu_m \pmod{u_n}$$

for all m. Then the congruence

$$\prod_{\substack{k=1 \\ \gcd(n,k)=1}}^{n-1} \frac{u_{rk}}{u_k} \equiv c^{(r-1)\varphi(n)/2} \pmod{u_n}$$

holds for every r relatively prime to n.

PROOF. For each k relatively prime to n, write $rk = q_k n + s_k$, where $1 \leq s_k < n$. Since $\gcd(r, n) = 1$, multiplying by r is a bijection on reduced residue classes modulo n, so that the map $k \mapsto s_k$ is also bijection on reduced residue classes modulo n.

By the congruence $u_{m+n} \equiv cu_m \pmod{u_n}$, it follows that

$$u_{rk} \equiv c^{q_k} u_{s_k} \pmod{u_n}.$$

Consequently, we obtain the congruence

$$\prod_{\substack{1 \leq k < n \\ \gcd(n,k)=1}} u_{rk} \equiv c^{\sum_k q_k} \prod_{\substack{1 \leq k < n \\ \gcd(n,k)=1}} u_k \pmod{u_n}.$$

By the assumption that (u_m) is a strong divisibility sequence, it follows that $\gcd(u_n, u_k) = u_{\gcd(n,k)} = 1$, so that $\prod_k u_k$ is invertible modulo u_n.

It remains to evaluate the sum $\sum_k q_k$. Observe that

$$n \sum_k q_k = \sum_k (rk - s_k) = \sum_k (r-1)k = n(r-1)\varphi(n)/2. \qquad \square$$

COROLLARY 16.4.3. *For every Lucas sequence (u_n) with $u_{n+2} = au_{n+1} - bu_n$, where $\gcd(a, b) = 1$, and every r relatively prime to n, we have the following congruence:*

$$\prod_{\substack{1 \leq k \leq n-1 \\ \gcd(n,k)=1}} \frac{u_{rk}}{u_k} \equiv u_{n+1}^{(r-1)\varphi(n)/2} \pmod{u_n}.$$

Proof. The Lucas sequence (u_n) is strongly divisible by Theorem 19.1.12. Moreover, (u_n) satisfies the following addition formula by Proposition 19.1.8:

$$u_{m+n} = u_{n+1}u_m - bu_nu_{m-1}.$$

This implies the congruence

$$u_{m+n} \equiv u_{n+1}u_m \pmod{u_n}.$$

Thus, the claim follows from Theorem 16.4.2 with $c := u_{n+1}$. □

Example 16.4.4. Consider the Lucas sequence given by $u_n = n$, which satisfies the recurrence relation $u_{n+2} = 2u_{n+1} - u_n$. Then we have $u_{n+1} \equiv 1 \pmod{u_n}$. Assuming r relatively prime to n, the congruence of Corollary 16.4.3 is therefore exactly Theorem 16.2.1 (Euler's Theorem):

$$r^{\varphi(n)} \equiv 1 \pmod{n}.$$

Example 16.4.5. Consider the Lucas sequence given by $u_n = 1 + a + \cdots + a^{n-1}$, which satisfies the recurrence relation $u_{n+2} = (a+1)u_{n+1} - au_n$. Since $u_{n+1} = 1 + au_n$, it follows that $u_{n+1} \equiv 1 \pmod{u_n}$. Moreover, note that

$$\frac{u_{rk}}{u_k} = \frac{a^{rk}-1}{a^k-1} = 1 + a^k + \cdots + a^{k(r-1)}.$$

Assuming r relatively prime to n, the congruence of Corollary 16.4.3 is therefore:

$$\prod_{\substack{1\le k\le n-1\\ \gcd(n,k)=1}} 1 + a^k + \cdots + a^{k(r-1)} \equiv 1 \pmod{u_n}.$$

This is Hao Pan's q-analogue of Euler's Theorem [Pan2007].

Example 16.4.6. Consider the Fibonacci numbers F_n, and set $r = 2$. Since $F_{2k} = F_kL_k$, it follows from the congruence of Corollary 16.4.3 that

$$\prod_{k=1}^{p-1} L_k \equiv F_{p+1}^{\frac{p-1}{2}} \pmod{F_p}$$

for any odd prime p.

16.5 The Quadratic Character of −1

Theorem 16.3.1 (Wilson's Theorem) can be used to prove a historically important result in the development of modular arithmetic: that −1 is congruent to a square modulo an odd prime p if and only if $p \equiv 1 \pmod 4$. In his *Disquisitiones Arithmeticae* [Gau1986],



Figure 16.1: Carl Friedrich Gauss. Pastel painting by Johann Christian August Schwartz, 1803.

Gauss writes of this result that when he encountered it in 1795—he was 19 at the time—he considered it to be a result of rare beauty and suspected deep connections with even more profound results, that he concentrated all his efforts into understanding its underlying principles. He became so attracted by the questions of this nature, that he could not let them be. Ultimately, Gauss's investigations into higher arithmetic, as he preferred to call it, led him to prove the celebrated Theorem 28.2.1 (The Law of Quadratic Reciprocity).

While the law of quadratic reciprocity is certainly the central theorem of our subject, the quadratic character of -1 modulo a prime is a key result on its own. In this section we will show that it can be used to show that there are infinitely many primes congruent to 1 modulo 4. Furthermore, we will use the fact that -1 is congruent to a square modulo p when $p \equiv 1 \pmod 4$ in the next chapter to prove Fermat's *Two-Square Theorem*, which asserts that every such prime is the sum of two squares. Questions similar to the quadratic character of -1 modulo a prime will be investigated more fully in Chapters 27 and 28.

THEOREM 16.5.1 (The Quadratic Character of -1). *Consider an odd prime p. Then there exists an integer a such that*

$$a^2 \equiv -1 \pmod p$$

if and only if $p \equiv 1 \pmod 4$.

PROOF. First, we show that if there is an integer a such that $a^2 \equiv -1 \pmod p$, then we must have $p \equiv 1 \pmod 4$. By Theorem 16.1.1 (Fermat's Little Theorem) it follows that

$$(-1)^{\frac{p-1}{2}} \equiv (a^2)^{\frac{p-1}{2}} \equiv a^{p-1} \equiv 1 \pmod p$$

This shows that $\frac{p-1}{2}$ must be even, which is equivalent to the congruence $p \equiv 1 \pmod 4$.

For the converse, assume that $p \equiv 1 \pmod 4$. By Theorem 16.3.1 (Wilson's Theorem) we know that $(p-1)! \equiv -1 \pmod p$. Now, observe that the integers $1, \dots, p-1$ can be arranged in pairs, where each i is paired with $p-i$, which is always distinct from i because $p-1$ is even. Since $i(p-i) \equiv -i^2 \pmod p$, we obtain the congruences

$$-1 \equiv (p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p.$$

The last congruence holds, because $(p-1)/2$ is even by the assumption that $p \equiv 1 \pmod 4$. Thus, we have presented -1 as a square modulo p. □

The previous theorem describing the quadratic character of -1 modulo an odd prime p can be used to show that there are infinitely many primes congruent to 1 modulo 4. The first fifteen primes congruent to 1 modulo 4 are:

$$5,\ 13,\ 17,\ 29,\ 37,\ 41,\ 53,\ 61,\ 73,\ 89,\ 97,\ 101,\ 109,\ 113,\ \text{and } 137.$$

Theorem 16.5.2. *There are infinitely many primes congruent to* 1 *modulo* 4.

Proof. Consider a finite set of primes $p_1, \dots, p_k$ that are all congruent to 1 modulo 4, and define

$$n = (2p_1 \cdots p_k)^2 + 1.$$

Notice that $n \equiv 1 \pmod 4$ is greater than 1, and $p_i \nmid n$ for any $1 \le i \le k$. It follows that for any prime divisor q of n, we have

$$(2p_1 \cdots p_k)^2 \equiv -1 \pmod q,$$

showing that -1 is a quadratic residue modulo q. Since -1 is a quadratic residue modulo q if and only if $q \equiv 1 \pmod 4$, it follows that any prime divisor q of n is congruent to 1 modulo 4. Since none of the prime divisors of n are among the primes p_i we started out with, the primes p_i could not have listed all the primes congruent to 1 modulo 4. □

Theorem 16.5.1 and its proof can be generalized to arbitrary exponents. For example, the following theorem implies that the congruence $x^4 \equiv -1 \pmod p$ is solvable if and only if $p \equiv 1 \pmod 8$, that the congruence $x^8 \equiv -1 \pmod p$ is solvable if and only if $p \equiv 1 \pmod{16}$, and so on.

Theorem 16.5.3. *Consider an odd prime p and consider a natural number n with 2-adic decomposition $n = 2^k m$. Then the congruence*

$$x^n \equiv -1 \pmod p$$

is solvable if and only if $p \equiv 1 \pmod{2^{k+1}}$.

PROOF. The proof is by induction on k. For $k = 0$, the statement is trivial, and for $k = 1$, the proof was given in Theorem 16.5.1. For the inductive step, assume that for any number n with 2-adic decomposition $n = 2^k m$, the congruence $x^n \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{2^{k+1}}$, and consider a number n with 2-adic decomposition $n = 2^{k+1}m$.

For the forward direction, assume that a is an integer such that $a^n \equiv -1 \pmod{p}$. Then $b := a^{2m}$ is an integer such that

$$b^{2^k} \equiv -1 \pmod{p},$$

so we see that $p \equiv 1 \pmod{2^{k+1}}$. Consequently, the fraction

$$\frac{p-1}{2^{k+1}}$$

is an integer. By Theorem 16.1.1 (Fermat's Little Theorem) it follows that

$$(-1)^{\frac{p-1}{2^{k+1}}} \equiv (a^{2^{k+1}m})^{\frac{p-1}{2^{k+1}}} \equiv (a^m)^{p-1} \equiv 1 \pmod{p}.$$

This implies that $\frac{p-1}{2^{k+1}}$ is even, so that $p \equiv 1 \pmod{2^{k+2}}$.

For the converse, suppose that $p \equiv 1 \pmod{2^{k+2}}$ and consider an integer a such that $a^{2^k} \equiv -1 \pmod{p}$. Such an integer exists by the inductive hypothesis. Now partition the set of numbers $\{1, \ldots, p-1\}$ into classes of 2^{k+1} numbers of the form $\{x, ax, \ldots, a^{2^{k+1}-1}x\}$. We will write c for the number of such classes. Then we have $p = 2^{k+1}c + 1$, so we see that c is even.

Since the number of classes is c, we can label them by C_i for each $1 \leq i \leq c$, and we can pick a representative $x_i \in C_i$ for each i. Now it follows by Theorem 16.3.1 (Wilson's Theorem) that

$$-1 \equiv (p-1)! \equiv \prod_{i=1}^{c} \prod_{j=0}^{2^{k+1}-1} a^j x_i \equiv \prod_{i=1}^{c} (-1) x_i^{2^{k+1}} \equiv (-1)^c \prod_{i=1}^{c} x_i^{2^{k+1}} \equiv \left(\prod_{i=1}^{c} x_i \right)^{2^{k+1}} \pmod{p}.$$

□

16.6 The Infinitude of Primes Congruent to 1 Modulo Powers of 2

One way to show that a prime p is congruent to 1 modulo n is by finding an integer a such that

$$\operatorname{ord}_p(a) = n.$$

By Theorem 8.5.2 (Order Theorem) and Theorem 16.1.1 (Fermat's Little Theorem), this implies that $n \mid p-1$. We will use this idea to show that there are infinitely many primes congruent to 1 modulo any power of 2. In particular, there are infinitely many primes congruent to 1 modulo 4, modulo 8, modulo 16, and so on.

Theorem 16.6.1. *For any positive natural number n, there are infinitely many primes congruent to 1 modulo 2^n.*

Proof. Since $p \equiv 1 \pmod{2^{n+1}}$ implies that $p \equiv 1 \pmod{2^n}$, it suffices to show that for any finite list $p_1, \ldots, p_k$ of primes congruent to 1 modulo 2^{n+1}, there is a prime $q \equiv 1 \pmod{2^{n+1}}$ which is not among the primes p_i.

Given such a list of primes p_i, let

$$a := 2p_1 \cdots p_k,$$

and let q be a prime divisor of the integer $b := a^{2^n} + 1$. Note that q is necessarily an odd prime, since a is even and hence b is odd. Since $p_i \nmid b$ for any i, it follows that q is not among the primes p_i. Furthermore, we observe that

$$a^{2^n} \equiv -1 \pmod{q}.$$

This implies that $\mathrm{ord}_q(a) \mid 2^{n+1}$, while clearly $\mathrm{ord}_q(a) \nmid 2^n$. Thus, we must have $\mathrm{ord}_q(a) = 2^{n+1}$, and this allows us to conclude that $q \equiv 1 \pmod{2^{n+1}}$. □

The previous theorem is a special case of a deep theorem in analytic number theory: *Dirichlet's Theorem*. Dirichlet's Theorem shows that for any integer a relatively prime to n, there are infinitely many primes

$$p \equiv a \pmod{n}.$$

The techniques of proving Dirichlet's Theorem are beyond the scope of this course. However, having taken this course, you are well equipped to read LeVeque's excellent *Topics in Number Theory* [LeV1956a; LeV1956b], a two-volume work that contains well-explained proofs of Dirichlet's Theorem as well as the Prime Number Theorem.

Exercises

Starter Exercises

16.1 For every prime $p \equiv 1 \pmod 4$ below 100, find the least positive integer a such that $a^2 \equiv -1 \pmod p$.

16.2 (a) Consider two integers a and b, and a prime number p. Prove, without using Fermat's Little Theorem, that

$$(a+b)^p \equiv a^p + b^p \pmod p.$$

(b) Suppose that $a \geq 0$. Use the previous congruence and the fact that $a = \sum_{i=1}^{a} 1$ to give your own proof of Fermat's Little Theorem.

16.3 (a) Prove that

$$5^{5^5} \equiv 5^5 \pmod{31}.$$

(b) Prove that

$$7^{7^7} \equiv 7^7 \pmod{43}.$$

Routine-Building Exercises

16.4 Show that

$$2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \pmod p$$

for any prime number $p \neq 3$.

16.5 For any positive integer n we define the **Euler quotient**

$$q_n(x) := \frac{x^{\phi(n)} - 1}{n},$$

where x is assumed to be relatively prime to n. In the special case where n is a prime, $q_n(x)$ is called the **Fermat quotient**.

(a) Show that

$$q_n(ab) \equiv q_n(a) + q_n(b) \pmod n$$

for any two integers a and b relatively prime to n, and conclude that $q_n(a^k) \equiv kq_n(a) \pmod n$ for a relatively prime to n.

(b) For any prime p, define the **Wilson quotient** W_p by

$$W_p := \frac{(p-1)! + 1}{p}.$$

Prove **Lerch's formula** [LER1905], which asserts that

$$\sum_{k=1}^{p-1} q_p(k) \equiv W_p \pmod p.$$

16.6 Show that

$$3^{3^{3^3}} \equiv 3^{3^3} \pmod{97}.$$

16.7 (a) Show that any number of the form

$$m^5 n - n^5 m$$

is divisible by 30.

(b) Show that for any two odd primes p and q, the number

$$p^5 q - q^5 p$$

is divisible by 240.

16.8 Prove that if

$$a^n \equiv a \pmod{n}$$

for every integer a, then $n = 2$ or n is odd.

16.9 Consider two distinct primes p and q, and an integer $a \geq 0$. Prove that

$$a^{pq} + a \equiv a^p + a^q \pmod{pq}$$

16.10 Consider an odd prime $p = 2n + 1$. Show that

$$\binom{2n}{n} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

16.11 Consider a prime p and two numbers m and n. Prove that

$$\binom{p^k n}{p^k m} \equiv \binom{n}{m} \pmod{p}.$$

16.12 Show that the congruence

$$\sum_{k=1}^{n} k^n \equiv 0 \pmod{n}$$

holds if and only if n is odd.

16.13 (a) Consider a prime p and an integer $p \nmid a$. Show that

$$a^p \equiv a \pmod{p^2} \quad \Leftrightarrow \quad a^{p^2} \equiv a \pmod{p^2}.$$

(b) A prime satisfying $a^p \equiv a \pmod{p^2}$ is called a **Wieferich prime base** a. Wieferich encountered this condition by showing that if $x^p + y^p = z^p$ with $p \nmid xyz$, then p must be a Wieferich prime base 2 [Wie1909]. The only known Wieferich primes base 2 are $p = 1093$ and $p = 3511$, and there are no smaller Wieferich primes base 2.
In bases larger than 2 there are smaller Wieferich primes, although they are still rare. The only known Wieferich primes base 3 are $p = 11$ and $p = 1006003$. Show that 5 is a Wieferich prime base 32.

Challenge Exercises

16.14 Find the least integer $k > 1$ such that every integer of the form $x^k - x$ is divisible by 47 and 89.

16.15 Find a prime $p > 3$ such that

$$3^{3^3} \equiv 3^3 \pmod{p}.$$

16.16 For any integer a and any prime number p, show that

$$a^{p^k} \equiv a^{p^{k-1}} \pmod{p^k}.$$

16.17 Find all the solutions to the equation

$$p^q - q^p = p + q,$$

where p and q are prime numbers.

16.18 Consider two primes p and q. Show that

$$pq \mid (13^p - 5^p)(13^q - 5^q) \quad \Leftrightarrow \quad pq \mid 12.$$

16.19 (a) Show that the number $6481 = 3^8 - 3^4 + 1$ is prime. Hint: In order to avoid trying out all the primes below 80, show first that every prime factor p of 6481 satisfies $p \equiv 1 \pmod{24}$.

(b) Compute the prime factorization of the number

$$3^{24} - 1.$$

16.20 Consider the function $f(n) = 2n + 1$. Show for every prime p, the sequence

$$k \mapsto f^k(p)$$

obtained by iterating the function f, contains composite numbers.

16.21 (a) Consider an odd prime q. Show that the numbers

$$2^q - 1 \qquad \text{and} \qquad q + 1.$$

are relatively prime.

(b) Consider two distinct primes p and q, and let r be a common prime divisor of the numbers

$$\frac{p^q - 1}{p - 1} \qquad \text{and} \qquad \frac{q^p - 1}{q - 1}.$$

Show that $r \equiv 1 \pmod{2pq}$.

16.22 Let F_n be the nth Fibonacci number. Show that if p is prime, then

$$F_{p-1} + F_{p+1} \equiv 1 \pmod{p}.$$

Chapter 17

Fermat's Two-Squares Theorem

17.1 Numbers Representable as a Sum of Two Squares

In this chapter we are concerned with the question which numbers are representable as a sum of two squares. In other words, our goal is to find a precise characterization of the numbers n that can be written in the form

$$n = a^2 + b^2.$$

Here, we permit ourselves to pick $a = 0$ or $b = 0$, so that any perfect square is trivially representable as a sum of two squares. The problem of finding those numbers n that can be written as the sum of two squares is equivalent to the problem of finding integer lattice points on the circle of radius $\sqrt{n}$, as illustrated in Figure 17.1.

Using modular arithmetic, we can find some basic obstructions to the possibility of representing a number as a sum of two squares. Recall that the square of an even number is always divisible by 4, and the square of an odd number is always of the form $4k + 1$. As a direct consequence we see that if n is of the form $4k + 3$ then it is not representable as a sum of two squares. This observation leads to the following lemma.

Lemma 17.1.1. *Suppose that $n = a^2 + b^2$ and consider a prime $p \equiv 3 \pmod 4$ such that $p \mid n$. Then $p \mid a$ and $p \mid b$.*

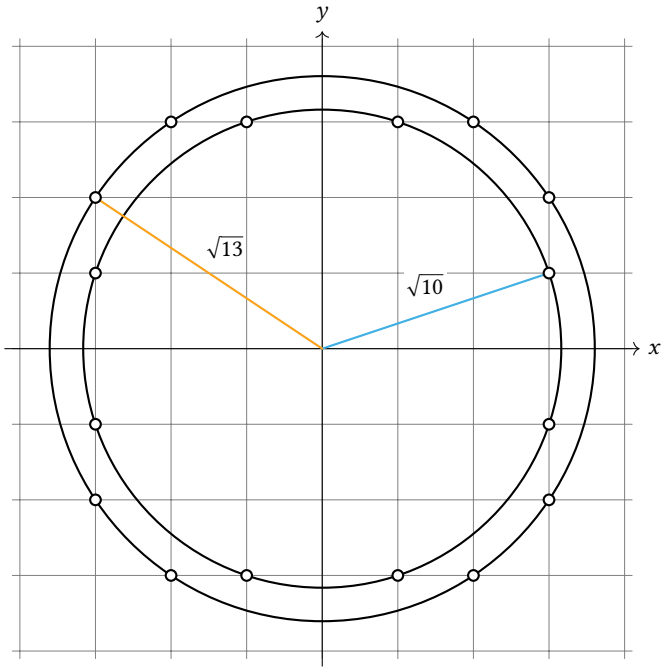


Figure 17.1: Representing a number as a sum of two squares is equivalent to finding an integer lattice point on the circle of radius $\sqrt{n}$. Here we displayed the integer lattice points on the circles of radii $\sqrt{10}$ and $\sqrt{13}$.

PROOF. If $p \nmid a$, then the integer a is invertible modulo p. Then the congruence $a^2+b^2 \equiv 0 \pmod{p}$ implies that

$$(a^{-1}b)^2 \equiv -1 \pmod{p}.$$

This is a contradiction, since the congruence $x^2 \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{4}$. Thus, it follows that $p \mid a$ and consequently we also obtain $p \mid b$. □

The previous lemma can be used to find an obstruction to numbers being representble as a sum of two squares.

COROLLARY 17.1.2. *If the square-free part of a natural number n is divisible by a prime $p \equiv 3 \pmod{4}$, then n is not representable as a sum of two squares.*

PROOF. By Lemma 17.1.1 it follows that if n is divisible by a prime $p \equiv 3 \pmod{4}$, then we also have $p^2 \mid n$. Writing $n = p^2n'$, $a = pa'$ and $b = pb'$, we find that

$$n' = a'^2 + b'^2.$$

By iterating this process, we see that the p-adic valuation of n is even. Thus, if the p-adic valuation of n is odd, which is equivalent to the condition that the square-free part of n is divisible by p, then n is not representable as a sum of two squares. □

One of Fermat's most remarkable discoveries was that the statement in Corollary 17.1.2 is sharp: A number is representable as a sum of two squares if and only if its square-free part is not divisible by any primes congruent to $3 \pmod 4$. The first published proof of this claim was due to Euler. Fermat's discovery is now known as *Fermat's Two-Squares Theorem*. We will give Euler's proof in the next section. Another classic proof is Don Zagier's, who famously wrote it up in a single—rather complicated—sentence.

A commonality between all these proofs is a reduction to the primes, which we will also perform here. Just as we did for the Pythagorean triples, we will consider numbers that are representable as a sum of two squares, which are relatively prime to each other. Such representations will be called **primitive**.

Definition 17.1.3. We say that a number n is **primitively representable** as a sum of two squares if there are relatively prime positive integers a and b such that

$$a^2 + b^2 = n.$$

By Corollary 17.1.2 it follows immediately that numbers divisible by a prime $p \equiv 3 \pmod 4$ are never primitively representable as a sum of two squares: Either they are not representable at all, or they are representable as the sum of two squares of numbers, each of which is divisible by p. Likewise, any number divisible by 4 is not primitively representable, since two squares only sum to a number divisible by 4 if they are both even. Thus, we obtain the following corollary.

Corollary 17.1.4. *Any number divisible by 4 or by any prime $p \equiv 3 \pmod 4$ is not primitively representable as a sum of two squares.*

We can thus formulate the Two-Squares Theorem for primitive representations as sums of two squares as follows: A number n has a primitive representation as a sum of two squares if and only if n is a product of primes congruent to $1 \pmod 4$ or n is twice such a product.

In order to reduce the Two-Squares Theorem to the primes $p \equiv 1 \pmod 4$, we first recall the **Brahmagupta–Fibonacci identity**, from which it follows that products of numbers representable as sums of two squares are again so representable. While this identity might appear to come out of thin air, it has a natural interpretation in the Gaussian integers, which we will discuss in Chapter 18.

Lemma 17.1.5 (The Brahmagupta–Fibonacci Identity). *For an integers a, b, c, and d, we have*

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2.$$

Proof. This identity can be verified by a simple calculation:

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= a^2c^2 \pm 2abcd + b^2d^2 + a^2d^2 \mp 2abcd + b^2c^2 \\ &= (ac \pm bd)^2 + (ad \mp bc)^2.\end{aligned}$$

□

By the Brahmagupta–Fibonacci identity it is easy to note that the number 65 can be represented as a sum of two squares in two distinct ways:

$$65 = 1^2 + 8^2 \qquad \text{and} \qquad 65 = 4^2 + 7^2.$$

Indeed, the Brahmagupta–Fibonacci identity gives that

$$65 = 13 \cdot 5 = (2^2 + 3^2)(1^2 + 2^2) = (6 \pm 2)^2 + (4 \mp 3)^2.$$

We have thus reduced the Two-Squares Theorem to the following statement: Every prime $p \equiv 1 \pmod 4$ can be represented as a sum of two squares. In fact, somthing stronger is true: Every prime $p \equiv 1 \pmod 4$ can be *uniquely* represented as a sum of two squares.

PROPOSITION 17.1.6. *Any prime number p can be represented in at most one way as a sum of two squares.*

PROOF. We have already seen that primes of the form $p \equiv 3 \pmod 4$ are not representable as the sum of two squares, which means that the claim is indeed true for such primes. The only way to represent 2 as a sum of two squares is

$$2 = 1^2 + 1^2.$$

The only remaining case is $p \equiv 1 \pmod 4$.

Consider a prime $p \equiv 1 \pmod 4$, and suppose that $p = x^2 + y^2$ and $p = u^2 + v^2$ are two distinct representations of p as a sum of two squares with $x < y$ and $u < v$. Any such representations are automatically primitive, since p is prime. It follows that y and v are invertible modulo p, so we have

$$(xy^{-1})^2 \equiv -1 \pmod p \qquad \text{and} \qquad (uv^{-1})^2 \equiv -1 \pmod p.$$

This implies that $xy^{-1} \equiv \pm uv^{-1} \pmod p$. By changing the sign of u, which doesn't affect the equation $u^2 + v^2 = p$, we may assume that $xy^{-1} \equiv uv^{-1} \pmod p$, which is equivalent to

$$xv \equiv yu \pmod p.$$

However, note that all of x, y, u, and v are strictly below $\sqrt{p}$. Hence it follows that $xv = yu$. This implies that the fractions $\frac{x}{y}$ and $\frac{u}{v}$ are equal. Since they are in lowest terms, we must have $x = u$ and $y = v$. □

In order to prove this claim, suppose that $a^2 \equiv -1 \pmod p$. Such a solution indeed exists, since $p \equiv 1 \pmod 4$. We will now analyze the multiples of a

$$0,\ a,\ 2a,\ 3a, \ldots, ma$$

modulo p, up to some bound $m < p$ which is yet to be determined. At first sight, we don't know much about the distribution of these residues, except that they are all distinct since the integer a is invertible modulo p.

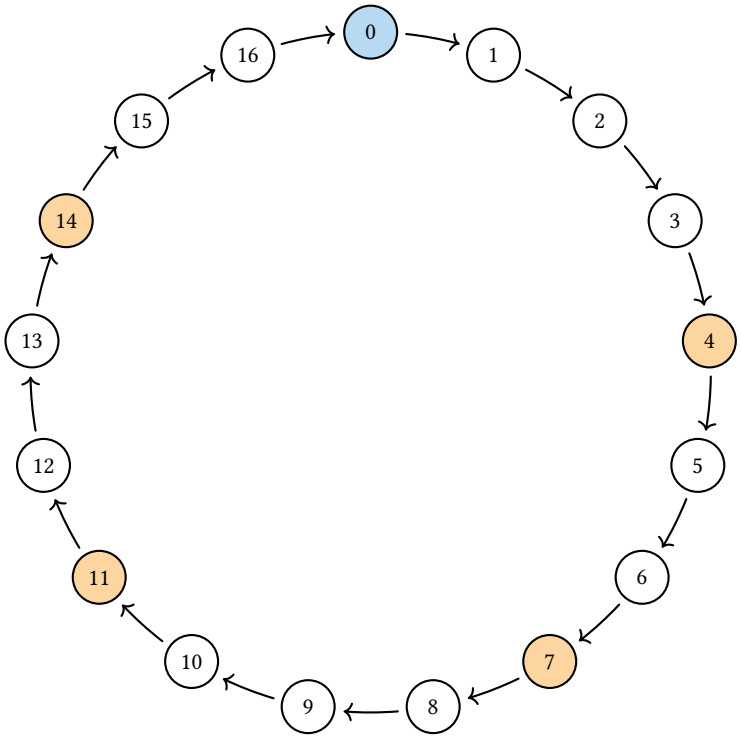


Figure 17.2: By Thue's lemma, in any set of m multiples $\{a, 2a, \dots, ma\}$ modulo any prime p, there is one multiple whose cyclic distance to 0 does not exceed $\frac{p}{m+1}$. Here we see that there is a number of the form $k \cdot 7$, for $1 \le k \le 4$, whose cyclic distance to 0 is 3, which is indeed below $\frac{17}{5}$.

In order to analyze them further, write $|x|_p$ for the least distance to a multiple of p. The least distance from any number to a multiple of p is always at most $p/2$. For example, $|13|_5 = 2$ and $|39|_7 = 3$. The following lemma, which is due to Axel Thue, will be of use.

Lemma 17.1.7 (Thue's Lemma). *Consider two positive integers a and n such that $\gcd(a, n) = 1$. For any natural number m, there is some $1 \le k \le m$ such that*

$$|ka|_n \le \frac{n}{m+1}.$$

Proof. We will assume that $m < n$, for if m is greater then we find $|na|_n = 0$. For each $0 \le i, j \le m$, write $d_{i,j} := |(i-j)a|_n$ be the distance to the nearest multiple of n from the difference between ia and ja. Since i ranges over $m+1$ numbers, the shortest such distance can be no longer than $n/(m+1)$. In other words, we can find distinct numbers $0 \le i, j \le m$ such that

$$d_{i,j} = |(i-j)a|_n \le \frac{n}{m+1}.$$

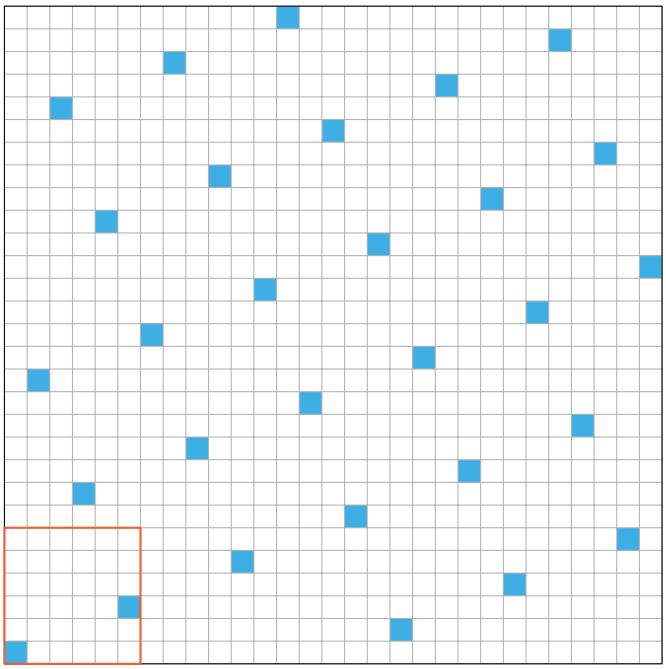


Figure 17.3: Thue's lemma in Lucas' weaving patterns. Here we displayed the points (x, y) satisfying $y \equiv 12x \pmod{29}$.

Now define $k := j - i$. Then we clearly have $0 < k \leq m$, and we have

$$|ka|_n = |(i-j)a|_n \leq \frac{n}{m+1}. \qquad \square$$

Another way of looking at Thue's lemma is by the weaving patterns of Lucas, as illustrated in Figure 17.3. If $\gcd(a, n) = 1$ and $m = \lfloor \sqrt{n} \rfloor$, then there must be a nonzero square with coordinates (x, y) with $0 \leq x, y \leq m$ satisfying $y \equiv ax \pmod{n}$.

THEOREM 17.1.8. *Any prime $p \equiv 1 \pmod{4}$ has a unique primitive representation as a sum of two squares.*

PROOF. Consider a prime $p \equiv 1 \pmod{4}$. We have already seen that there is at most one way to represent p as a sum of two squares, so it remains to prove existence.

Consider an integer $0 \leq a < p$ such that $a^2 \equiv -1 \pmod{p}$. Such an integer exists, since $p \equiv 1 \pmod{4}$. By Lemma 17.1.7 (Thue's Lemma) with $m := \lfloor \sqrt{p} \rfloor$, we find that there is some $1 \leq k < \sqrt{p}$ such that

$$|ka|_p \leq \frac{p}{\sqrt{p}+1} < \sqrt{p}.$$

If we define $r := |ka|_p$, then it follows that $0 < r^2 + k^2 < 2p$. On the other hand, since $a^2 \equiv -1 \pmod{p}$ we have $r^2 + k^2 \equiv (ka)^2 + k^2 \equiv -k^2 + k^2 \equiv 0 \pmod{p}$. Thus, $r^2 + k^2$ is a multiple of p strictly between 0 and $2p$, so we conclude that $r^2 + k^2 = p$. This shows that p can be represented as the sum of two squares. □

Theorem 17.1.9 (Fermat's Two-Squares Theorem). *A natural number n is presentable as the sum of two squares if and only if the prime divisors of its square-free part are either 2 or congruent to $1 \pmod{4}$.*

We will give three more proofs of Fermat's Two-Squares Theorem in remainder of this chapter.

17.2 Euler's Proof by Infinite Descent

Euler proved that every prime $p \equiv 1 \pmod{4}$ can be written as a sum of two squares by using the Brahmagupta–Fibonacci identity in a clever descent argument.

Proof of Theorem 17.1.8. Consider a prime $p \equiv 1 \pmod{4}$. First we observe that there are integers a and b such that

$$p \mid a^2 + b^2.$$

Indeed, it follows from Theorem 16.5.1 that -1 is congruent to a square modulo p, which shows that $p \mid a^2 + 1^2$ for some integer a.

Now assume that a and b are integers such that $p \mid a^2 + b^2$. We claim that if $a^2 + b^2 = rp$ for some $r > 1$, then we can find integers x and y such that $x^2 + y^2 = sp$ for some $s < r$. The theorem then follows at once, since we can keep writing smaller multiples of p as sums of two squares until we have written p itself as a sum of two squares.

To prove the claim, consider let u and v be two integers satisfying the conditions

$$u \equiv a \pmod{r}, \qquad v \equiv b \pmod{r}, \qquad \text{and} \qquad |u|, |v| \leq \frac{r}{2}.$$

Then $u^2 + v^2 \equiv a^2 + b^2 \equiv 0 \pmod{r}$, so that $u^2 + v^2 = rs$. We also observe that it is not possible for both u and v to be congruent to $0 \pmod{r}$. Indeed, if this were the case, then a and b would be divisible by r, which would make the prime p divisible by r. The inequality $u^2 + v^2 \leq \frac{r^2}{2}$ implies that $s \leq \frac{r}{2}$.

Multiplying a^2+b^2 with u^2+v^2 gives $(a^2+b^2)(u^2+v^2) = r^2sp$. By the Brahmagupta–Fibonacci identity, we can write this as

$$(a^2 + b^2)(c^2 + d^2) = (au + bv)^2 + (av - bu)^2.$$

Now we observe that $au + bv \equiv a^2 + b^2 \equiv 0 \pmod{r}$, and that $av - bu \equiv ab - ab \equiv 0 \pmod{r}$. This shows that both $au + bv$ and $av - bu$ are divisible by r, so we obtain the identity

$$\left(\frac{au + bv}{r}\right)^2 + \left(\frac{av - bu}{r}\right)^2 = sp.$$

Thus we have written a smaller multiple of p as a sum of two squares, so the theorem is proven. □

Exercises

Starter Exercises

17.1 For every prime $p \equiv 1 \pmod 4$ below 100, write p as a sum of two squares.

17.2 Show that no odd prime p can be written as a sum of two cubes.

Routine-Building Exercises

17.3 Show that a natural number n can be written as the sum of two triangular numbers if and only if $8n + 2$ can be written as the sum of two squares. Hint: Use one of the identities stated in Exercise 2.6.

Chapter 18

The Gaussian Integers

18.1 Definition and Basic Properties of the Gaussian Integers

Definition 18.1.1. A **Gaussian integer** is an expression of the form

$$a + bi$$

in which a and b are integers. We say that the **real part** of $a + bi$ is the integer a, and the **complex part** of $a + bi$ is the integer b.

We will write $\mathbb{Z}[i]$ for the set of Gaussian integers. Gaussian integers are added, subtracted, and multiplied according to the following rules:

$$(a + ib) + (c + id) = (a + c) + i(b + d)$$
$$(a + ib) - (c + id) = (a - c) + i(b - d)$$
$$(a + ib)(c + id) = (ac - bd) + i(ad + bc).$$

Definition 18.1.2. The **norm** of a Gaussian integer $\alpha = a + bi$ is given by

$$N(\alpha) = a^2 + b^2.$$

Proposition 18.1.3 (The Brahmagupta–Fibonacci identity). *The norm function N is completely multiplicative in the sense that*

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

for any two Gaussian integers α and β.



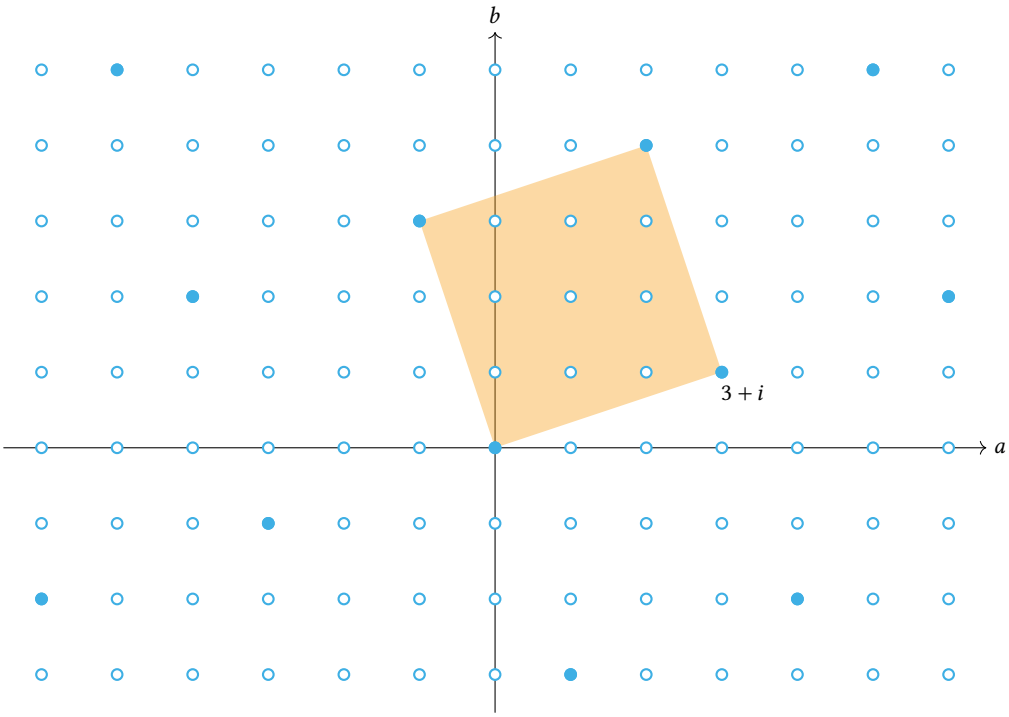


Figure 18.1: The set of Gaussian integers. All the multiples of $3 + i$ are marked with solid dots, and all the nonmultiples are marked with open dots. The norm of $3 + i$ is the area of the square shaded in orange.

DEFINITION 18.1.4. A Gaussian integer α is said to **divide** a Gaussian integer β if there exists a Gaussian integer κ such that

$$\kappa\alpha = \beta.$$

Any Gaussian integer dividing 1 is called a **unit**.

THEOREM 18.1.5. *The only units among the Gaussian integers are* ± 1 *and* $\pm i$.

18.2 Euclidean Division of Gaussian Integers

EXAMPLE 18.2.1. The following choices of α and β show that there can be multiple pairs of Gaussian integers κ and ρ with $N(\rho) < N(\beta)$ such that

$$\alpha = \kappa\beta + \rho.$$

(i) Consider $\alpha := 8 + 11i$ and $\beta = 3 + i$, so that $N(\beta) = 10$. Then

$$\frac{\alpha}{\beta} = \frac{(8+11i)(3-i)}{3^2+1^2} = \frac{35+25i}{10} = (3+2i) + \frac{1+i}{2}.$$

This shows that $\alpha = (3+2i)\beta + (1+2i)$. Note that $N(1+2i) = 5 < 10$. However, we can also write

$$\begin{aligned} \alpha &= (4+2i)\beta + (-2+i), & N(-2+i) &= 5, \\ \alpha &= (3+3i)\beta + (2-i), & N(2-i) &= 5, \\ \alpha &= (4+3i)\beta + (-2-i), & N(-2-i) &= 5. \end{aligned}$$

(ii) Consider $\alpha := 2 + 3i$ and $\beta = 4$, so that $N(\beta) = 16$. Then we can write

$$\begin{aligned} \alpha &= i\beta + (2-i), & N(2-i) &= 5, \\ \alpha &= (1+i)\beta + (-2-i), & N(-2-i) &= 5. \end{aligned}$$

Define the half-open fundamental square to be the following subset of $\mathbb{C}$:

$$\mathcal{S} := \{x + yi \in \mathbb{C} \mid -\tfrac{1}{2} < x, y \leq \tfrac{1}{2}\}.$$

Theorem 18.2.2. *Consider two Gaussian integers α and β with $N(\alpha) > N(\beta)$. Then there exist unique Gaussian integers κ and ρ with $N(\rho) < N(\beta)$, such that*

$$\alpha = \kappa\beta + \rho$$

and $\frac{\rho}{\beta} \in \mathcal{S}$.

18.3 The Greatest Common Divisor of Gaussian Integers

The definition of a greatest common divisor carries over directly from the integers to the Gaussian integers.

Definition 18.3.1. Consider two Gaussian integers α and β. A Gaussian integer δ is said to be the **greatest common divisor** of α and β if it satisfies the following logical equivalence for every Gaussian integer ξ:

$$(\xi \mid \alpha) \wedge (\xi \mid \beta) \Leftrightarrow (\xi \mid \delta).$$

18.4 Primes in the Gaussian Integers

18.5 Fermat's Two-Square Theorem

18.6 The Biquadratic Character of -1



Exercises

Challenge Exercises

18.1 (a) Consider a Gaussian integer $\alpha = a+bi$ such that $\gcd(a,b) = 1$. Show that the number of Gaussian integers in the interior (that is, not on the boundary) of the square spanned by the Gaussian integers 0, α, $i\alpha$, and $(1+i)\alpha$ is $N(\alpha)-1$. See Figure 18.1 for such a square with $\alpha = 3+i$.

(b) For any Gaussian integer $\alpha = a+bi$, determine the number of Gaussian integers in the interior of the square spanned by the Gaussian integers 0, α, $i\alpha$, and $(1+i)\alpha$.

Chapter 19

Strong Divisibility Sequences

19.1 Lucas Sequences

The French mathematician Édouard Lucas observed that the familiar Fibonacci sequence was just a single instance of a larger family of recursively defined sequences that all share similar properties.

Definition 19.1.1. Consider two integers a and b. The **Lucas sequence** u_n at a and b is defined by

$$u_0 := 0, \qquad u_1 := 1, \qquad \text{and} \qquad u_{n+2} := au_{n+1} - bu_n.$$

If the parameters a and b are not clear from the context, we will write $u(a,b)_n$ for u_n. When a and b are relatively prime, we say that the Lucas sequence (u_n) is **reduced**.

Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = au_{n+1} - bu_n$. The **characteristic polynomial** of this Lucas sequence is the polynomial

$$x^2 - ax + b,$$

and its **characteristic form** is the binary quadratic form

$$x^2 - axy + y^2.$$

The roots $\alpha := \frac{a+\sqrt{a^2-4b}}{2}$ and $\beta := \frac{a-\sqrt{a^2-4b}}{2}$ of the characteristic polynomial are called the **characteristic roots**. By the Vieta relations, the characteristic roots satisfy the identites

$$\alpha + \beta = a \qquad \text{and} \qquad \alpha\beta = b.$$



EXAMPLE 19.1.2. Some special cases of Lucas sequences are famous:

(i) When $a = 1$ and $b = -1$, then the sequence (u_n) is the Fibonacci sequence

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

The characteristic polynomial of the Fibonacci sequence is $x^2 - x - 1$ and its characteristic roots are

$$\alpha = \frac{1+\sqrt{5}}{2} \qquad \text{and} \qquad \beta = \frac{1-\sqrt{5}}{2}.$$

(ii) When $a = 2$ and $b = -1$, then the sequence (u_n) is the **Pell sequence**

$$0, 1, 2, 5, 12, 29, 70, 169, 408, 985, \ldots$$

The characteristic polynomial of the Pell sequence is $x^2 - 2x - 1$ and its characteristic roots are

$$\alpha = 1 + \sqrt{2} \qquad \text{and} \qquad \beta = 1 - \sqrt{2}.$$

(iii) In Exercise 14.3 we saw that the sequence (M_n) of Mersenne numbers satisfies the recurrence

$$M_{n+2} = 3M_{n+1} - 2M_n.$$

Thus, the Mersenne numbers also form an example of a Lucas sequence. The characteristic polynomial of the Mersenne numbers is $x^2 - 3x + 4$ and its characteristic roots are

$$\alpha = 4 \qquad \text{and} \qquad \beta = -1.$$

(iv) More generally, for any two distinct integers a and b, the sequence defined by

$$u_n := \frac{a^n - b^n}{a - b}$$

is a Lucas sequence satisfying

$$u_0 = 0, \qquad u_1 = 1, \qquad \text{and} \qquad u_{n+2} = (a+b)u_{n+1} + abu_n.$$

(v) The Lucas sequence (u_n) given by

$$u_0 = 0, \qquad u_1 = 1, \qquad \text{and} \qquad u_{n+2} = 2u_{n+1} - u_n$$

is the sequence of nonnegative integers: For each $n \geq 0$ we have $u_n = n$.

In the following theorem we establish two fundamental identities for a Lucas sequence.

Theorem 19.1.3. *Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = au_{n+1} - bu_n$ and characteristic roots α and β. Then we have the identities*

$$u_{n+1} - \alpha u_n = \beta^n \qquad \text{and} \qquad u_{n+1} - \beta u_n = \alpha^n.$$

Proof. We prove the first identity by induction on n. The second identity can be proven similarly. For the base case, we note that $u_1 - \alpha u_0 = 1 = \beta^0$. For the inductive step, we use that $a = \alpha + \beta$ and $b = \alpha\beta$ to compute

$$u_{n+2} - \alpha u_{n+1} = au_{n+1} - bu_n = (\alpha+\beta)u_{n+1} - \alpha\beta u_n - \alpha u_{n+1} = \beta(u_{n+1} - \alpha u_n) = \beta^{n+1}. \quad \square$$

Theorem 19.1.4 (Binet's Formula). *Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = au_{n+1} - bu_n$ and characteristic roots α and β. Then α and β are distinct, and*

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Proof. By the identities $u_{n+1} - \alpha u_n = \beta^n$ and $u_{n+1} - \beta u_n = \alpha^n$ established in Theorem 19.1.3, it follows that

$$(\alpha - \beta)u_n = (u_{n+1} - \beta u_n) - (u_{n+1} - \alpha u_n) = \alpha^n - \beta^n. \quad \square$$

Binet's formula can be used to show that if $m \mid n$, then $u_m \mid u_n$. Sequences with this property are called *divisibility sequences*. We will additionally assume that divisibility sequences (a_n) satisfy $a_0 = 0$ and $a_1 = 1$. Such divisibility sequences are sometimes called *normalized*.

Definition 19.1.5. An integer sequence (a_n) is said to be a **divisibility sequence** if $a_0 = 0$, $a_1 = 1$, and it preserves the divisibility relation, meaning that it satisfies the condition

$$m \mid n \Rightarrow a_m \mid a_n$$

for all m and n.

Theorem 19.1.6. *Consider two integers a and b such that $a^2 - 4b \neq 0$. Then the Lucas sequence (u_n) at a and b is a divisibility sequence.*

Proof. Suppose that $n = km$. Then we have

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{(\alpha^m - \beta^m)\sum_{i=0}^{k}(\alpha^m)^i(\beta^m)^{k-i}}{\alpha - \beta} = u_m \sum_{i=0}^{k}(\alpha^m)^i(\beta^m)^{k-i}$$

by the formula for the difference of mth powers. This shows that if $m \mid n$, then $u_m \mid u_n$. $\square$

When the parameters a and b in the recursive law of a Lucas sequence (u_n) are relatively prime, the Lucas sequence has the further property of preserving greatest common divisors. Divisibility sequences that preserve greatest common divisors are called *strong divisibility sequences*.



DEFINITION 19.1.7. A divisibility sequence (a_n) is said to be a **strong divisibility sequence** if (a_n) preserves greatest common divisors, meaning that it satisfies the equation

$$a_{\gcd(m,n)} = \gcd(a_m, a_n)$$

for all m and n.

Our first target is to prove an addition formula for Lucas sequences. This law generalizes the addition formula for the Fibonacci numbers, which we stated in Exercise 6.12.

PROPOSITION 19.1.8 (Addition formula for Lucas sequences). *For any two natural numbers m and n, we have*

$$u_{m+n+1} = u_{m+1}u_{n+1} - bu_m u_n$$

INDUCTIVE PROOF. The proof is by induction on n. In the base case, we calculate

$$u_{m+1} = u_{m+1} \cdot 1 - 0 = u_{m+1}u_1 - bu_m u_0.$$

For the inductive step, assume that the identity $u_{m+n+1} = u_{m+1}u_{n+1} - bu_m u_n$ holds for all m. Then we calculate

$$\begin{aligned} u_{m+1}u_{n+2} - bu_m u_{n+1} &= u_{m+1}(au_{n+1} - bu_n) - bu_m u_{n+1} \\ &= (au_{m+1} - bu_m)u_{n+1} - bu_{m+1}u_n \\ &= u_{m+2}u_{n+1} - bu_{m+1}u_n \\ &= u_{(m+1)+n+1} \\ &= u_{m+n+2}. \end{aligned}$$

□

We give a second proof of the addition law, making use of the fundamental identities stated in Theorem 19.1.3. Even though our previous inductive proof is perfectly legitimate, our second proof illustrates something important: Numbers of the form $x + \alpha y$ form their own domain of arithmetic. We will address this point more fully when we study quadratic fields.

PROOF BY THE FUNDAMENTAL IDENTITIES. In this proof, we will assume that α and β are distinct, or equivalently, that $a^2 - 4b \neq 0$.

Given the identity $u_{n+1} - \beta u_n = \alpha^n$ established in Theorem 19.1.3, it follows that

$$\alpha^{m+n} = \alpha^m \alpha^n = (u_{m+1} - \beta u_m)(u_{n+1} - \beta u_n) = u_{m+1}u_{n+1} - \beta(u_m u_{n+1} + u_{m+1}u_n) + \beta^2 u_m u_n.$$

Since β is a root of the equation $x^2 - ax + b$, it follows that $\beta^2 = a\beta - b$. This implies that

$$\alpha^{m+n} = u_{m+1}u_{n+1} - bu_m u_n - \beta(u_m u_{n+1} + u_{m+1}u_n - au_m u_n).$$

Similarly, using the identity $u_{n+1} - \alpha u_n = \beta^n$, we find that

$$\beta^{m+n} = u_{m+1}u_{n+1} - bu_m u_n - \alpha(u_m u_{n+1} + u_{m+1}u_n - au_m u_n).$$

Combining these equations, it follows that

$$u_{m+n} = \frac{\alpha^{m+n} - \beta^{m+n}}{\alpha - \beta} = u_m u_{n+1} + u_{m+1} u_n - a u_m u_n.$$

Using this expression for u_{m+n} in our earlier identity for α^{m+n}, we find that

$$\alpha^{m+n} = u_{m+1} u_{n+1} - b u_m u_n - \beta u_{m+n}.$$

On the other hand, we have $\alpha^{m+n} = u_{m+n+1} - \beta u_{m+n}$. Combining these identities gives us

$$u_{m+n+1} = u_{m+1} u_{n+1} - b u_m u_n. \qquad \square$$

Corollary 19.1.9. *For any Lucas sequence (u_n) with recurrence relation $u_{n+2} = a u_{n+1} - b u_n$ we have the identities*

$$u_{2n+1} = u_{n+1}^2 - b u_n^2 \qquad \text{and} \qquad u_{2n+2} = u_{n+1}(u_{n+2} - b u_n).$$

Proposition 19.1.10 (Cassini's identity). *Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = a u_{n+1} - b u_n$. Then we have*

$$u_{n+2} u_n - u_{n+1}^2 = -b^n.$$

Proof. The proof is by induction on n. In the base case, we have

$$u_2 u_0 - u_1^2 = -1.$$

For the inductive step, we have

$$\begin{aligned} u_{n+3} u_{n+1} - u_{n+2}^2 &= (a u_{n+2} - b u_{n+1}) u_{n+1} - (a u_{n+1} - b u_n) u_{n+2} \\ &= b u_{n+2} u_n - b u_{n+1}^2 \\ &= b(u_{n+2} u_n - u_{n+1}^2) \\ &= -b^{n+1}. \end{aligned}$$

$\square$

Corollary 19.1.11. *Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = a u_{n+1} - b u_n$. Then any two consecutive terms u_n and u_{n+1} are relatively prime.*

Proof. By Proposition 19.1.10 (Cassini's identity) it follows that $\gcd(u_n, u_{n+1})$ divides b^n. However, modulo b we see that (u_n) satisfies the recurrence

$$u_{n+2} \equiv a u_{n+1} \pmod{b}.$$

Since $u_1 = 1$ and a is invertible modulo b, it follows that u_n is relatively prime to b for every n. Thus we conclude that $\gcd(u_n, u_{n+1}) = 1$. $\square$

Theorem 19.1.12. *Consider the Lucas sequence (u_n) with recurrence $u_{n+2} = a u_{n+1} - b u_n$. If a and b are relatively prime, then (u_n) is a strong divisibility sequence.*

PROOF. First, we show that if $n = qm + r$ with $0 \leq r < m$, then

$$\gcd(u_n, u_m) = \gcd(u_m, u_r).$$

The identity $n = qm + r$ implies that

$$u_n = u_{qm+1}u_r - bu_{qm}u_{r-1}$$

Since $u_m \mid u_{qm}$, it follows that $u_n \equiv u_{qm+1}u_r \pmod{u_m}$. However, u_{qm+1} is relatively prime to u_{qm} and hence to u_m. Thus, any common divisor d of u_n and u_m must also be a divisor of u_r. This shows that

$$\gcd(u_n, u_m) \mid \gcd(u_m, u_r).$$

On the other hand, we see that u_n can be written as a linear combination of u_m and u_r, so that $\gcd(u_n, u_m) \mid u_n$. This implies that

$$\gcd(u_m, u_r) \mid \gcd(u_n, u_m).$$

□

EXAMPLE 19.1.13. There are many examples of strong divisibility sequences beyond the class of Lucas sequences. A particularly self-evident example is the sequence

$$u_n := n^2.$$

To see that this is not a Lucas sequence, we show that the equations

$$4 = a \cdot 1 - b \cdot 0$$
$$9 = a \cdot 4 - b \cdot 1$$
$$16 = a \cdot 9 - b \cdot 4$$

has no solutions. The first equation implies that $a = 4$. Given this constraint, the second equation gives that $b = 7$. However, $4 \cdot 9 - 7 \cdot 4 = 8 \neq 16$. Thus we conclude that the sequence (n^2) is not a Lucas sequence for any choice of integers a and b.

An important further class of strong divisibility sequences is the class of *elliptic divisibility sequences* of Morgan Ward [WAR1948].

19.2 The Rank of Apparition

EXAMPLE 19.2.1.

(i) When we look at the Fibonacci sequence modulo a prime p, we see clear patterns emerging:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F_n \pmod 2$	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
$F_n \pmod 3$	0	1	1	2	0	2	2	1	0	1	1	2	0	2	2	1
$F_n \pmod 5$	0	1	1	2	3	0	3	3	1	4	0	4	4	3	2	0
$F_n \pmod 7$	0	1	1	2	3	5	1	6	0	6	6	5	4	2	6	1

(ii) When we look at the Pell sequence modulo a prime p, we again see clear patterns emerging:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_n \pmod 2$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$P_n \pmod 3$	0	1	2	2	0	2	1	1	0	1	2	2	0	2	1	1
$P_n \pmod 5$	0	1	2	0	2	4	0	4	3	0	3	1	0	1	2	0
$P_n \pmod 7$	0	1	2	5	5	1	0	1	2	5	5	1	0	1	2	5

(iii) When we look at the Mersenne numbers modulo a prime p, we obtain the following:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$M_n \pmod 2$	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$M_n \pmod 3$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$M_n \pmod 5$	0	1	3	2	0	1	3	2	0	1	3	2	0	1	3	2
$M_n \pmod 7$	0	1	3	0	1	3	0	1	3	0	1	3	0	1	3	0

Definition 19.2.2. Consider an integer sequence (a_n) and a positive integer m. The **rank of apparition** $\rho_a(m)$ of m is the least positive integer n such that $m \mid a_n$.

Theorem 19.2.3 (Rank of Apparition Theorem). *Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a divisibility sequence. Then the following are equivalent:*

(i) *There is a function $g : \mathbb{N} \to \mathbb{N}$ satisfying the logical equivalence*

$$g(m) \mid n \quad \Leftrightarrow \quad m \mid f(n).$$

(ii) *The divisibility sequence f is a strong divisibility sequence.*

If the first condition holds, then the function g is equal to the rank of apparition function; that is, $g(m) = \rho_f(m)$ for every natural number m.

Proof. Suppose first that there exists a function g satisfying the logical equivalence

$$g(m) \mid n \quad \Leftrightarrow \quad m \mid f(n).$$



Then it follows that

$$\begin{aligned} d \mid f(\gcd(m,n)) &\Leftrightarrow g(d) \mid \gcd(m,n) \\ &\Leftrightarrow g(d) \mid m \wedge g(d) \mid n \\ &\Leftrightarrow d \mid f(m) \wedge d \mid f(n) \\ &\Leftrightarrow d \mid \gcd(f(m), f(n)). \end{aligned}$$

Since $f(\gcd(m,n))$ and $\gcd(f(m), f(n))$ have the exact same set of divisors, they must be equal.

For the converse, suppose that $f(0) = 0$ and that f preserves greatest common divisors. More generally, we will have for any finite list of natural numbers

$$f(\gcd_i(n_i)) = \gcd_i(f(n_i)).$$

Here, the expression $gcd_i(n_i)$ means that the greatest common divisor is taken over all the numbers n_i in the list. Now consider for any natural number m the ideal

$$I_m := \left\{ k_1 n_1 + \cdots + k_r n_r \,\middle|\, m \mid f(n_i) \text{ for all } i \right\}$$

and define the function g by letting $g(m)$ be the unique natural number such that $I_m = (g(m))$.

To see that g is a divisibility sequence, suppose that $m \mid m'$. Then any linear combination of natural numbers n such that $m' \mid f(n)$ is also a linear combination of natural numbers n such that $m \mid f(n)$. In particular $g(m')$ is in the ideal $(g(m))$, which means that $g(m) \mid g(m')$.

We claim that the function g satisfies the logical equivalence

$$g(m) \mid n \quad \Leftrightarrow \quad m \mid f(n).$$

If $m \mid f(n)$, then it follows that $n \in I_m$ so that $g(m) \mid n$. This proves the reverse direction.

For the forward direction, suppose that $g(m) \mid n$. Then it also follows that $n \in I_m$, so that we can write

$$n = \sum_i k_i n_i$$

for some finite list of natural numbers n_i satisfying $m \mid f(n_i)$. By the assumption that $m \mid f(n_i)$, it follows that $m \mid \gcd_i(f(n_i))$. Furthermore, since $\gcd_i(n_i) \mid n$ it follows that

$$f(\gcd_i(n_i)) \mid f(n).$$

Combined with the fact that $m \mid \gcd_i(f(n_i))$ and the assumption that f preserves greatest common divisors, we conclude that

$$m \mid f(n).$$

□

By Theorem 8.5.2 (Order Theorem), it follows that the function g defined by $g(m) := \mathrm{ord}_m(a)$ satisfies the logical equivalence in the first condition of Theorem 19.2.3 (Rank of Apparition Theorem). Thus we obtain the following corollary:

Corollary 19.2.4. *The function $n \mapsto a^n - 1$ is a strong divisibility sequence. Thus, for any integer $a > 1$ and any two natural numbers m and n we have*

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1.$$

Proof. Note that the function $k \mapsto a^k - 1$ is a divisibility sequence, since for $qm = n$ we have the identity

$$a^n - 1 = (a^m)^q - 1^q = (a^m - 1) \sum_{k=0}^{q-1} a^{km}$$

by the formula for the difference of qth powers (Exercise 2.5). The fact that it is a strong divisibility sequence now follows directly from Theorem 19.2.3 and Theorem 8.5.2 (Order Theorem). □

Example 19.2.5. Consider two relatively prime integers a and b with $b < a$, and consider the Lucas sequence (u_n) with recurrence $u_{n+2} = (a + b)u_{n+1} - abu_n$. By Binet's formula, we have

$$u_n = \frac{a^n - b^n}{a - b}.$$

By the assumption that a and b are relatively prime it follows that the sequence u_n is a strong divisiblity sequence. Thus, the rank-of-apparition function ρ satisfies

$$\rho(m) \mid n \quad \Leftrightarrow \quad m \mid u_n.$$

We make a more detailed analysis of the rank of apparition of a prime, depending on whether it divides $a - b$, a, b, or none of these numbers.

First, we will assume that $p \nmid ab(a - b)$. In this case, we have

$$p \mid u_n \Leftrightarrow p \mid a^n - b^n \Leftrightarrow a^n \equiv b^n \pmod{p}.$$

Since a and b are invertible modulo p, it follows that $(a/b)^n \equiv 1 \pmod{p}$, which is equivalent to the condition that $\mathrm{ord}_p(a/b) \mid n$. Thus, we conclude that

$$\mathrm{ord}_p(a/b) \mid n \quad \Leftrightarrow \quad p \mid u_n.$$

It follows that $\rho(p) = \mathrm{ord}_p(a/b)$. We can extend these observation to moduli m with $\gcd(m, ab(a - b)) = 1$. Here again, a and b are invertible modulo m, from which it follows that

$$p \mid u_n \Leftrightarrow a^n \equiv b^n \pmod{p} \Leftrightarrow \mathrm{ord}_m(a/b) \mid n.$$

Thus we find that $\rho(m) = \mathrm{ord}_m(a/b)$. Moreover, one can show that

$$\rho(m_1 m_2) = \mathrm{lcm}(\rho(m_1), \rho(m_2))$$



when m_1 and m_2 are relatively prime integers, both relatively prime to $ab(a-b)$.

Next, we will assume that $p \mid a-b$. Since $a-b$ is relatively prime to both a and b, it follows again that both a and b are invertible modulo p. Then we can rewrite u_n using the formula for the difference of nth powers, and subsequently use the congruence $a \equiv b \pmod{p}$ to obtain:

$$u_n = \frac{a^n - b^n}{a-b} = \sum_{k=0}^{n-1} a^{n-1-k}b^k \equiv \sum_{k=0}^{n-1} a^{n-1-k}a^k = na^{n-1} \pmod{p}.$$

Given that $p \nmid a$, it follows that

$$p \mid n \quad \Leftrightarrow \quad p \mid u_n.$$

In other words, the rank of apparition of p is $\rho(p) = p$.

Finally, we show that $\rho(p) = 0$ when $p \mid a$ and $p \nmid b(a-b)$, from which we also obtain that $\rho(p) = 0$ in the symmetric case where $p \mid b$ and $p \nmid a(a-b)$. Recall that $\rho(p) = 0$ means that $p \nmid u_n$ for all $n > 1$. Note that if $p \mid a$, then we have

$$u_n \equiv b^{n-1} \pmod{p}$$

whenever $n \geq 1$. Since we assumed that $p \nmid b$, this shows that $p \nmid u_n$.

REMARK 19.2.6. More generally, if $(P, \leq_P)$ and $(Q, \leq_Q)$ are two posets, a **Galois connection** between P and Q consists of order preserving maps $f : P \to Q$ and $g : Q \to P$ satisfying the logical equivalence

$$g(x) \leq_P y \quad \Leftrightarrow \quad x \leq_Q f(y)$$

for any $x \in Q$ and $y \in P$. In this case, the map f is said to be the **upper adjoint**, and the map g is said to be the **lower adjoint** of the Galois connection. Thus we have proven in this section that the function $n \mapsto a^n - 1$ is the upper adjoint of a Galois connection, and we have used this fact to show that f preserves greatest common divisors. Theorem 19.2.3 generalizes to the setting of arbitrary posets, and indeed, some readers may recognize it as a special case of the *Adjoint Functor Theorem*.

Another famous Galois connection on the natural numbers ordered by divisibility is the Fibonacci sequence. We will give the full statement of this fact in the exercises.

19.3 Primitive Sequences

DEFINITION 19.3.1. Consider a divisibility sequence $n \mapsto a_n$ indexed by the natural numbers, with $a_1 = 1$. The **primitive sequence** of a_n is the sequence (u_n) of rational numbers defined by

$$u_n := \prod_{d \mid n} a_d^{\mu(n/d)}.$$

THEOREM 19.3.2. *The primitive sequence (u_n) of a divisibility sequence (a_n) satisfies the identity*

$$a_n = \prod_{d|n} u_d.$$

PROOF. By interchanging the product, we find that

$$\prod_{e|n}\prod_{d|e} a_d^{\mu(e/d)} = \prod_{d|n}\prod_{c|\frac{n}{d}} a_d^{\mu(c)} = \prod_{d|n} a_d^{\sum_{c|\frac{n}{d}}\mu(c)} = \prod_{d|n} a_d^{\varepsilon(n/d)} = a_n. \qquad \square$$

19.4 LCM-sequences

DEFINITION 19.4.1. The **lcm-sequence** (m_n) of an integer sequence (a_n) is given by $m_1 := 1$ and

$$m_n := \frac{\operatorname{lcm}(a_1, \dots, a_n)}{\operatorname{lcm}(a_1, \dots, a_{n-1})} \qquad \text{for } n \geq 2.$$

THEOREM 19.4.2. *Consider a divisibility sequence (a_n) indexed by the natural numbers, with $a_1 = 1$. Then the following are equivalent:*

(i) *The sequence (a_n) is a strong divisibility sequence; that is,*

$$a_{\gcd(m,n)} = \gcd(a_m, a_n)$$

for every m and n.

(ii) [WAR1936] *For each prime p, we have $p^k \mid a_n$ if and only if $\rho_k(p) \mid n$, where $\rho_k(p)$ is the rank of apparition of p^k.*

(iii) *Each u_n in the primitive sequence (u_n) of (a_n) is an integer, and furthermore u_m and u_n are relatively prime when $m \nmid n$ and $n \nmid m$.*

(iv) [NOW2015] *The sequence (a_n) satisfies the following divisor-product formula, where (m_n) is the lcm-sequence of (a_n):*

$$a_n = \prod_{d|n} m_d.$$

The following corollary, due to Morgan Ward [WAR1936], is a generalization of a theorem of Édouard Lucas [LUC1878a].

COROLLARY 19.4.3. *If (a_n) is a strong divisibility sequence, then*

$$\prod_{i=1}^{k} a_i \,\Big|\, \prod_{i=n+1}^{n+k} a_i.$$

19.5 The Lifting the Exponent Lemma

For the following lemma, recall that $v_p(a-b) = m$ if and only if $a \equiv b \pmod{p^m}$ but $a \not\equiv b \pmod{p^{m+1}}$. We also recall that for any prime p and any $0 < i < p$, the binomial coefficient $\binom{p}{i}$ is divisible by p.

LEMMA 19.5.1. *Consider an odd prime p, and two integers $a \equiv b \pmod{p}$ such that neither a nor b is divisible by p. Then*

$$v_p(a^p - b^p) = v_p(a-b) + 1.$$

PROOF. Write $s := v_p(a-b)$, so that $s \geq 1$ by the assumption that $a \equiv b \pmod{p}$. Then we have $a \equiv b \pmod{p^s}$, so we can write $b = a + tp^s$, where $p \nmid t$. The value of b^p can therefore be computed using Theorem 3.5.1 (The Binomial Theorem) by

$$b^p = (a+tp^s)^p = \sum_{i=0}^{p} \binom{p}{i} a^i (tp^s)^{p-i} \equiv a^p + a^{p-1}tp^{s+1} \pmod{p^{s+2}}.$$

Since neither a nor t is divisible by p, it follows that $a^p \not\equiv b^p \pmod{p^{s+2}}$. On the other hand, we see from the binomial expansion of b^p that $a^p \equiv b^p \pmod{p^{s+1}}$. Therefore we conclude that

$$v_p(a^p - b^p) = s + 1. \qquad \square$$

The previous lemma can be iterated to obtain a general lemma called the *Lifting the Exponent Lemma*. This lemma was popularized by the Romanian mathematician Mihai Manea [MAN2006].

THEOREM 19.5.2 (Lifting the Exponent). *Consider an odd prime p, and let $x \equiv y \pmod{p}$, where neither x nor y is divisible by p. Then for any natural number $n \geq 1$, we have*

$$v_p(x^n - y^n) = v_p(x-y) + v_p(n).$$

PROOF. Write $n = p^k m$ with $p \nmid m$, so that $v_p(n) = k$, and write $s = v_p(x-y)$. Since we have assumed that $x \equiv y \pmod{p}$, we have $s \geq 1$. We will prove the claim by induction on k.

In the base case, where $k = 0$, the claim is simply that

$$v_p(x^m - y^m) = s.$$

To see this, write $y = x + tp^s$, where $p \nmid t$. Then we have

$$y^m = (x+tp^s)^m \equiv x^m + mx^{m-1}tp^s \pmod{p^{s+1}}.$$

Now observe that m, x, and t are not divisible by p by assumption, so it follows that $mx^{m-1}t$ is not divisible by p. This implies that $y^m \not\equiv x^m \pmod{p^{s+1}}$. On the other hand, the congruence $x \equiv y \pmod{p^s}$ clearly implies that $x^m \equiv y^m \pmod{p^s}$, so we conclude that

$$v_p(x^m - y^m) = s.$$

The inductive step is a direct consequence of Lemma 19.5.1. $\square$

Example 19.5.3. In Example 19.2.5 we saw that for $p \mid a - b$ with a and b relatively prime, the rank of apparition of p in the Lucas sequence given by

$$u_n = \frac{a^n - b^n}{a - b}$$

is $\rho(p) = p$. Now we claim that $\rho(p^k) = p^k$. Using Theorem 19.5.2 (Lifting the Exponent), we see that

$$v_p(u_n) = v_p(a^n - b^n) - v_p(a - b) = v_p(n).$$

This shows that $p^k \mid u_n$ if and only if $p^k \mid n$, and the claim follows.

Definition 19.5.4. A strong divisibility sequence is said to satisfy the **law of repetition** if for any prime p, we have

$$v_p(a_{n\rho_a(p)}) = v_p(a_{\rho_a(p)}) + v_p(n).$$

Theorem 19.5.5. *Consider a strong divisibility sequence (a_n), such that for each prime p we have*

$$\rho_a(p^k) = \rho_a(p)p^{k-1}.$$

Then (a_n) satisfies the law of repetition.

Example 19.5.6. For any two relatively prime integers a and b, the sequence

$$(a^n - b^n)$$

satisfies the law of repetition.

Example 19.5.7. Any Lucas sequence satisfies the law of repetition.



Exercises

Starter Exercises

19.1 Show that consecutive terms of a Lucas sequence (u_n) with characteristic form $x^2 - axy + by^2$ satisfy

$$u_{n+1}^2 - au_{n+1}u_n + bu_n^2 = b^n.$$

Routine-Building Exercises

19.2 Show that

$$\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(m,n)} - b^{\gcd(m,n)}.$$

19.3 Consider a positive integer a, and write $S_m := \sum_{k=0}^{m} a^k$. Prove that

$$\gcd(S_m, S_n) = S_{\gcd(m+1,n+1)-1}.$$

19.4 Consider a Lucas sequence (u_n) with recursion $u_{n+2} = au_{n+1} - bu_n$. Show that

$$u_{n+1}^2 \equiv b^n \pmod{u_n}.$$

19.5 Consider a Lucas sequence (u_n) and let m be such that $u_m \neq 0$. Define the **cofactor sequence** $(\tilde{u}_k)$ by

$$\tilde{u}_k := u_{km}/u_m.$$

Show that $(\tilde{u}_k)$ is again a Lucas sequence.

Challenge Exercises

19.6 Show that for any odd prime p the following congruence holds:

$$\prod_{k=1}^{p-1} L_k \equiv F_{p+1}^{\frac{p-1}{2}} \pmod{F_p}$$

19.7 (a) Show that the function $(x, y) \mapsto (y, x + y)$ is a bijection on the set of pairs of elements $x, y \in \mathbb{Z}/n\mathbb{Z}$.

(b) Show that for any m, the Fibonacci sequence is periodic modulo m. Its period is called the **Pisano period**.

(c) Show that for any natural number m, there is a least positive number n such that

$$m \mid F_n.$$

We will call this number G_m. By virtue of its duality to the Fibonacci sequence, we will call the sequence G the **cofibonacci sequence**.

(d) Show that $G(m)$ satisfies the following logical equivalence

$$G_m \mid n \quad \Leftrightarrow \quad m \mid F_n.$$

Conclude that the Fibonacci sequence is a strong divisibility sequence.

19.8 Use methods similar to the previous exercise to show that the sequence of Pell numbers P_n, which are defined by

$$P_0 := 0, \qquad P_1 := 1, \qquad \text{and} \qquad P_{n+2} = 2P_{n+1} + P_n,$$

forms a strong divisibility sequence.

19.9 Define a **Mersenne integer** to be any integer that can be written in the form

$$\frac{M_{i_1} \cdots M_{i_m}}{M_{j_1} \cdots M_{j_n}}.$$

Show that the number 23 is not a Mersenne integer.

19.10 Define a **Fibonacci integer** to be any integer that can be written in the form

$$\frac{F_{i_1} \cdots F_{i_m}}{F_{j_1} \cdots F_{j_n}}.$$

Show that the number 37 is not a Fibonacci integer [LP2003].

19.11 (The Dickson–Lucas polynomial) Consider a Lucas sequence (u_n) with associated sequence (v_n) given by

$$v_0 := 2, \qquad v_1 := a, \qquad \text{and} \qquad v_{n+2} = av_{n+1} - bv_n.$$

Show that

$$v_m = \sum_{j=0}^{\lfloor m/2 \rfloor} (-1)^j \frac{m}{m-j} \binom{m-j}{j} a^{m-2j} b^j.$$



Chapter 20

Polynomials

20.1 Polynomials with Abstract Coefficients

Definition 20.1.1. A **polynomial** in one variable x is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

in which we require that the **leading coefficient** a_n is nonzero, unless $n = 0$. A polynomial $f(x)$ as above with leading coefficient a_n is said to be of **degree** n. The numbers a_k are called the **coefficients** of $f(x)$. The **zero polynomial** is the constant polynomial $f(x) = 0$.

The coefficients of a polynomial may be taken from any number system. When we wish to specify that the coefficients are integers, rational, or real numbers, we speak of **polynomials with integer coefficients**, **polynomials with rational coefficients**, or **polynomials with real coefficients**. Other number systems from which we will occasionally take coefficients include the rings $\mathbb{Z}/n$ of modular arithmetic. Since there is such a large variety of number systems which will eventually play a role one way or another in number theory, it will be useful to us to develop methods general enough so as to cover all these cases at once.



DEFINITION 20.1.2. A **commutative ring** is a set R equipped with constants 0 and 1 and operations + for addition, − for subtraction, and · for multiplication, satisfying the following laws of arithmetic:

$$\begin{aligned} (x+y)+z &= x+(y+z), & (xy)z &= x(yz), \\ x+y &= y+x, & xy &= yx, \\ 0+x &= x, & 1x &= x, \\ x+(-x) &= 0, & x(y+z) &= xy+xz. \end{aligned}$$

The adjective **commutative** refers to the law asserting that $xy = yx$. A commutative ring with $0 \neq 1$ is said to be a **integral domain** if it satisfies the following condition:

$$xy = 0 \Rightarrow x = 0 \vee y = 0.$$

A commutative ring with $0 \neq 1$ is said to be a **field** if it comes equipped with a further operation $(-)^{-1}$ defined on all nonzero elements, such that

$$xx^{-1} = 1.$$

Examples of commutative rings include most number systems we have encountered so far: $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{Z}/n$ for any n. The Gaussian integers $\mathbb{Z}[i]$ are another important example of a ring. There is one important omission: The set of natural numbers with the usual operations of addition and multiplication is not a ring because it lacks subtraction.

The sharp reader may have observed that some laws of arithmetic, such as $0x = 0$, are not stated in the definition of a (commutative) ring. Indeed, this law can be proven:

$$0x = 0x + 0 = 0x + (0x - 0x) = (0x + 0x) - 0x = (0+0)x - 0x = 0x - 0x = 0.$$

Most rings satisfy the condition that $0 \neq 1$. Indeed, if $0 = 1$ in a ring R, then any element equals 0 because

$$x = 1x = 0x = 0.$$

Thus, only the ring $\mathbb{Z}/1$ satisfies $0 = 1$. This ring is called the **trivial ring** for understandable reasons.

The condition of being an integral domain is quite innocent-looking: It guarantees that the product of any two nonzero numbers is nonzero. This condition is true in familiar number systems such as $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}$, and $\mathbb{R}$, which are therefore integral domains. However, the ring $\mathbb{Z}/n$ is only an integral domain when n is prime. For composite n, we can find examples of nonzero numbers that multiply to 0. For instance, we have $2 \cdot 2 \equiv 0 \pmod 4$ in $\mathbb{Z}/4$, and we have $2 \cdot 3 \equiv 0 \pmod 6$ in $\mathbb{Z}/6$. Having such examples shows that the condition of being an integral domain is not provable from the laws of arithmetic stated in the definition of a ring.

Of the examples we have seen so far, only $\mathbb{Q}$ and $\mathbb{Z}/p$ are fields. Other familiar fields include the field $\mathbb{R}$ of real numbers and the field $\mathbb{C}$ of complex numbers. We note

that any field is an integral domain: If $xy = 0$ and $x \neq 0$, then x has a multiplicative inverse. This allows us to calculate as follows and find that

$$y = 1y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0 = 0.$$

The previous definitions of rings, integral domains, and fields are extremely general. There are many examples of rings that have little to do with numbers, except that they satisfy the laws of arithmetic. We stress here that our goal is not to develop the general theory of rings, where we would have to be concerned with the vast scope of the subject. Instead, our goal is simply to avoid having to reprove essentially the same theorems about polynomials separately for polynomials with integer coefficients, rational coefficients, real coefficients, and so on. By stating them in terms of polynomials with coefficients in a ring or integral domain, we cover all those cases at once.

Remark 20.1.3. There is another subtle, yet important aspect of polynomials which needs to be emphasized: The distinction between polynomials and the functions they describe. This distinction comes to light when considering equality of polynomials. Two polynomials

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \qquad \text{and} \qquad b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$$

are said to be equal if their coefficients are equal, meaning that $a_i = b_i$ for all $0 \leq i \leq n$, while functions are considered equal if their values are equal. This is an important distinction, because for some number systems such as the integers modulo n, polynomials aren't necessarily equal as polynomials when they are equal as functions. For instance, by Theorem 16.1.1 (Fermat's Little Theorem) we have that

$$x^p \equiv x \pmod{p},$$

while the polynomials x^p and x clearly can be distinguished by their coefficients. Nevertheless, we will show in Corollary 20.4.3 that two polynomials with integer coefficients have equal coefficients if and only if they define equal functions.

Definition 20.1.4. Consider a ring R. A function $f : R \to R$ is said to be **polynomial in** R if there exists a polynomial with coefficients in R such as the above, such that

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

for all $x \in R$.

Remark 20.1.5. Polynomials can be added, subtracted, and multiplied in the same way as integers. To add two polynomials, we add their corresponding coefficients, taking missing coefficients as zero when necessary. Polynomials are multiplied by the formula

$$\begin{aligned}\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j x^{i+j} \\ &= \sum_{k=0}^{n+m}\sum_{i=0}^{n} a_i b_{k-i} x^k.\end{aligned}$$



These operations of addition, subtraction, and multiplication of polynomials satisfy the laws of arithmetic. More precisely, the polynomials with coefficients in a commutative ring form itself a commutative ring.

20.2 The Factor Theorem

DEFINITION 20.2.1. Consider a polynomial $f(x)$ with coefficients in a ring R. A **root** of $f(x)$ is an element $r \in R$ such that

$$f(r) = 0.$$

Sometimes we will write $N(f)$ for the set of roots of f.

In the following theorem we will prove that if r is a root of the polynomial $f(x)$, then we can factor $f(x)$ as $(x-r)g(x)$. This theorem applies for polynomials in any commutative ring.

THEOREM 20.2.2 (Factor Theorem). *Consider a ring R, and a nonzero polynomial $f(x)$ of degree n with coefficients in R. An element $r \in R$ is a root of $f(x)$ if and only if there is a polynomial $g(x)$ of degree $n-1$ with coefficients in R such that $f(x) = (x-r)g(x)$.*

PROOF. We will prove the claim by induction on n. In the base case $f(x)$ is a nonzero constant polynomial, so it has no roots and there is nothing to prove.

For the inductive step, it is clear that if there is a polynomial $g(x)$ such that $f(x) = (x-r)g(x)$, then r is a root of the polynomial $f(x)$. For the converse, suppose that r is a root of $f(x)$. Then

$$f(x) = f(x) - f(r) = a_n(x^n - r^n) + \cdots + a_1(x-r).$$

By the formula for the difference of kth powers, which was stated in Exercise 2.5 and which holds in any ring, we can factor $x^k - r^k$ as

$$x^k - r^k = (x-r)q_k(x), \qquad \text{where} \qquad q_k(x) = \sum_{i=0}^{k-1} x^i r^{k-1-i}$$

is a polynomial of degree $k-1$. Now define $g(x) := \sum_{k=1}^{n} a_k q_k(x)$. Then we compute

$$(x-r)g(x) = \sum_{k=1}^{n} a_k(x-r)q_k(x) = \sum_{k=1}^{n} a_k(x^k - r^k) = f(x) - f(r) = f(x). \qquad \square$$

Theorem 20.2.2 (Factor Theorem) has some important corollaries. One of them states that in an integral domain, where the product of any two nonzero numbers is guaranteed to be nonzero, any polynomial of degree n has at most n roots.

COROLLARY 20.2.3. *Consider an integral domain R. A polynomial of degree n with coefficients in R has at most n roots.*

Proof. The proof is by induction on the degree n. If $f(x)$ is a constant polynomial of degree 0 and its leading coefficient is nonzero, then $f(x)$ is always nonzero and so $f(x)$ has no roots.

For the inductive step, assume that all polynomials of degree n have at most n roots, and consider a polynomial $f(x)$ of degree $n+1$. Then either $f(x)$ has no roots, in which case we are done immediately, or $f(x)$ has a root r, in which case $f(x)$ factors as

$$f(x) = (x - r)g(x)$$

by Theorem 20.2.2 (Factor Theorem), where $g(x)$ is a polynomial of degree n. Since we assumed that R is an integral domain, it follows that for any element $x \in R$, the identity $(x - r)g(x) = 0$ holds in R if and only if one of the identities $x - r = 0$ or $g(x) = 0$ holds in R. Thus we see that x is a root of the polynomial $f(x)$ if and only if $x = r$ or x is a root of the polynomial $g(x)$. We conclude that the polynomial $f(x)$ has at most $n + 1$ roots. □

The Factor Theorem also raises an immediate question of uniqueness. If $f(x)$ and $g(x)$ are two polynomials, is there always at most one way in which we can write

$$f(x) = g(x)h(x)?$$

Proposition 20.2.4 (Cancellation Law for Polynomials). *Let $f(x)$ be a nonzero polynomial with coefficients in an integral domain. Consider two polynomials $h(x)$ and $k(x)$ satisfying the identity of polynomials*

$$f(x)h(x) = f(x)k(x).$$

Then $h(x) = k(x)$.

Proof. By the assumption that $f(x)h(x) = f(x)k(x)$, it follows that

$$f(x)(h(x) - k(x)) = 0.$$

Write $g(x) := h(x) - k(x)$. Note that all the coefficients of the polynomial $f(x)g(x)$ are 0. However $f(x)$ is a nonzero polynomial, so it has a leading coefficient a_n. Now, suppose for a contradiction that $g(x)$ is nonzero, with leading coefficient b_m. Their product $f(x)g(x)$ has leading coefficient $a_n b_m$, which is nonzero since it is a product of nonzero elements of an integral domain. Hence $f(x)g(x)$ is nonzero, which is a contradiction. □

20.3 Polynomial Congruences of Prime Moduli

Even though a polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$



has at most n roots in the integers, the same is not true in modular arithmetic. A fairly easy example, the quadratic congruence

$$x^2 \equiv 1 \pmod{8}$$

has four solutions, the numbers 1, 3, 5, and 7. On the other hand, we will prove in this section that the number of solutions of a polynomial congruence modulo a prime is, just as in the integer case, at most the degree of the polynomial.

THEOREM 20.3.1 (Factor Theorem in Modular Arithmetic). *An integer r is a solution to the polynomial congruence*

$$f(x) \equiv 0 \pmod{n},$$

if and only if

$$f(x) \equiv (x - r)g(x) \pmod{n}$$

for some polynomial $g(x)$.

PROOF. The proof is very similar to the proof of Theorem 20.2.2. First, we note that the converse direction is trivial, so we focus on the forward direction. Suppose that

$$f(r) \equiv 0 \pmod{n}$$

and consider the polynomial $f(x) - f(r)$. Then we have

$$f(x) \equiv f(x) - f(r) \pmod{n},$$

and the factorization of $f(x) - f(r)$ as $(x - r)g(x)$ follows in the same way as for Theorem 20.2.2. □

THEOREM 20.3.2 (Lagrange's Theorem). *Consider a polynomial*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

and a prime p such that $p \nmid a_n$. Then the polynomial congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n solutions.

PROOF. We prove the claim by induction on the degree n of the polynomial f. If f has degree zero, then $f(x) = a_0$, and since the leading term of f is assumed to be not divisible by p, it follows that $a_0 \not\equiv 0 \pmod{p}$. Thus, the polynomial f has no solutions modulo p.

Now suppose that any polynomial congruence modulo p of degree n has at most n solutions, and consider a polynomial congruence $f(x) \equiv 0 \pmod{p}$ of degree $n + 1$. If this congruence has no roots, then the number of solutions is certainly below $n + 1$.

On the other hand, if $f(r) \equiv 0 \pmod{p}$ is a solution, then by Theorem 20.3.1 (Factor Theorem in Modular Arithmetic) we can find a polynomial $g(x)$ of degree n such that

$$f(x) \equiv (x-r)g(x) \pmod{p}.$$

It follows that the polynomial congruences $f(x) \equiv 0 \pmod{p}$ and

$$(x-r)g(x) \equiv 0 \pmod{p}$$

have the same sets of solutions. Since p is prime, we have by Proposition 13.1.4 that $ab \equiv 0 \pmod{p}$ if and only if $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. Any solution x of the congruence $(x-r)g(x) \equiv 0 \pmod{p}$ must therefore satisfy $x - r \equiv 0 \pmod{p}$ or $g(x) \equiv 0 \pmod{p}$. There are at most d solutions of the polynomial congruence $g(x) \equiv 0 \pmod{p}$, so we conclude that there are at most $d+1$ solutions to the polynomial congruence $f(x) \equiv 0 \pmod{p}$. □

The previous theorem is due to Joseph-Louis Lagrange, published in 1770 in *Réflexions sur la résolution algébrique des équations* [Lag1770]. Lagrange demonstrated that the roots of polynomials can be studied by their permutations. His ideas would eventually lead to the emergence of group theory (the study of symmetry), and Galois theory.

While Theorem 20.3.2 (Lagrange's Theorem) establishes an upper bound for the number of incongruent solutions of a polynomial congruence modulo a prime, we can use Theorem 16.1.1 (Fermat's Little Theorem) to find examples of polynomial congruences that have the maximum allowable number of solutions.

Theorem 20.3.3. *Consider a prime p and a positive integer n such that $n \mid p-1$. Then the polynomial congruence*

$$x^n \equiv 1 \pmod{p}$$

has exactly n incongruent solutions.

Proof. Note that the polynomial congruence $x^{p-1} - 1 \equiv 0 \pmod{p}$ has exactly $p-1$ solutions. By the formula for the difference of powers, we have

$$(x^{p-1} - 1) \equiv (x^n - 1)q(x) \pmod{p}$$

for some polynomial q of degree $p - 1 - n$. Now we observe that the polynomial congruences

$$x^n - 1 \equiv 0 \pmod{p} \qquad \text{and} \qquad q(x) \equiv 0 \pmod{p}$$

have at most n and $p - 1 - n$ solutions, respectively. Since their product has $p - 1$ solutions, it follows that the polynomial congruence $x^n - 1 \equiv 0 \pmod{p}$ must have exactly n solutions. □

Theorem 20.3.2 (Lagrange's Theorem) can also be used to give another proof of Theorem 16.5.1, which states that for an odd prime p, the quadratic congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.



PROOF OF THEOREM 16.5.1. We prove that if $p \equiv 1 \pmod 4$, then there is a square root of -1 modulo p. Consider a prime p of the form $4k + 1$. Then Theorem 16.1.1 (Fermat's Little Theorem) implies that

$$(x^{2k} + 1)(x^{2k} - 1) = x^{4k} - 1 \equiv 0 \pmod p.$$

Since p is prime, this implies that $x^{2k} + 1 \equiv 0 \pmod p$ or $x^{2k} - 1 \equiv 0 \pmod p$ for every integer x. However, the polynomial congruence

$$x^{2k} - 1 \equiv 0 \pmod p$$

has at most $2k$ solutions modulo p, which is strictly fewer than p. Thus, there must exist an integer x such that

$$x^{2k} + 1 \equiv 0 \pmod p.$$

Given such an integer x, we see that $y := x^k$ is a square root of -1 modulo p. □

20.4 Lagrange's Interpolation Theorem

Lagrange's Interpolation Theorem establishes that for any set of data points, as illustrated in Figure 20.1, there is always a way of defining a polynomial that exactly matches the data. Moreover, it gives the unique way of defining such a polynomial in the lowest degree. Interpolation theorems such as Lagrange's or Newton's addressed a practical need for geometers of the 17th and 18th centuries: It allowed them to estimate intermediate values of a function from a finite amount of data such as tables of planetary positions or values of trigonometric functions.

Lagrange's Interpolation Theorem has the important consequence that any polynomial of degree n is uniquely determined by any $n + 1$ of its values. We will also use Lagrange's Interpolation Theorem in the next section to derive a divisibility property of polynomials due to Kurt Hensel.

The idea underlying Lagrange's Interpolation Theorem is to break the problem into several subproblems: For each data point (x_i, y_i), we create a polynomial that has roots at x_j for all the other data points (x_j, y_j). This is very easy to do: we just take the product

$$g_i(x) = (x - x_0) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_j).$$

Then we have that $g_i(x_j) = 0$ for all $j \neq i$ and $g_i(x_i) \neq 0$. Thus there is some constant c_i such that $c_i g_i(x_i) = y_i$. Adding them all up gives the Lagrange Interpolation Theorem.

EXAMPLE 20.4.1. In Figure 20.1, we started with the set of points

$$(0, 1),\ (1, -2),\ (2, 0),\ (3, 1).$$

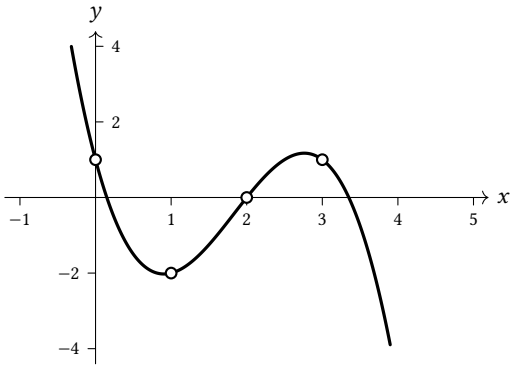


Figure 20.1: A polynomial of degree 3 obtained by Lagrange interpolation.

Then we define the polynomials

$$\begin{aligned} g_0 &:= \tfrac{1}{6}(x-1)(x-2)(x-3) \\ g_1 &:= -x(x-2)(x-3) \\ g_2 &:= 0 \\ g_3 &:= \tfrac{1}{6}x(x-1)(x-2), \end{aligned}$$

which we have already rescaled so that $g_0(0) = 1$, $g_1(1) = -2$, $g_2(2) = 0$, and $g_3(3) = 1$. Adding them up gives the polynomial

$$f(x) := \frac{1}{6}(x-1)(x-2)(x-3) - x(x-2)(x-3) + \frac{1}{6}x(x-1)(x-2),$$

which exactly matches the values specified in the initial data set.

Theorem 20.4.2 (Lagrange's Interpolation Theorem). *For any choice of $n+1$ points (x_i, y_i) such that the x_i are pairwise distinct, there is a unique polynomial $f(x)$ of degree at most n such that*

$$f(x_i) = y_i$$

for all $0 \le i \le n$.

Proof. For any $0 \le i \le n$, define the **basis polynomial** for Lagrange interpolation $g_i(x)$ by

$$g_i(x) := \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j}.$$

Then $g_i(x)$ is a polynomial of degree n, whose n roots are the points x_j for $j \neq i$. Furthermore, we have defined g_i in such a way that $g_i(x_i) = 1$. Now we define the polynomial $f(x)$ of degree n by

$$f(x) = \sum_{i=0}^{n} y_i g_i(x).$$

Then $f(x_i) = y_i$ since $g_j(x_i) = 0$ for $j \neq i$ and $g_i(x_i) = 1$. Thus f satisfies the criteria of the theorem.

To see that the polynomial $f(x)$ is the unique polynomial of degree at most n that satisfies $f(x_i) = y_i$, consider a second polynomial $g(x)$ of degree at most n that satisfies the same requirement. Then the polynomial

$$f(x) - g(x)$$

is a polynomial of degree at most n with $n + 1$ roots. By virtue of Corollary 20.2.3 this is only possible if $f(x) - g(x)$ is the zero polynomial, that is, if $f(x) = g(x)$. □

COROLLARY 20.4.3. *Consider two polynomials $f(x)$ and $g(x)$. Then the following are equivalent:*

(i) *The polynomials $f(x)$ and $g(x)$ have equal coefficients; that is, they are equal as polynomials.*

(ii) *The polynomials $f(x)$ and $g(x)$ have equal values; that is, they are equal as functions.*

(iii) *The polynomials $f(x)$ and $g(x)$ have equal values of any set of $n + 1$ inputs.*

In particular, any polynomial $f(x)$ is uniquely determined by the values

$$f(0), \ldots, f(n).$$

Even though the basis polynomials of Lagrange's Interpolation Theorem don't always have integer coefficients, we can use Lagrange's Interpolation Theorem to show that for any polynomial f with real coefficients, if

$$f(0), \ldots, f(n)$$

are integers, then $f(x)$ is an integer for every integer x.

DEFINITION 20.4.4. A polynomial $f(x)$ with real coefficients is said to be **integer valued** if $f(x)$ is an integer for every integer x.

A simple example of an integer valued polynomial that doesn't have integer coefficients is the polynomial

$$\frac{x(x+1)}{2},$$

which returns the triangular numbers.

Lagrange's Interpolation Theorem establishes a polynomial $f(x)$ as a linear combination of the basis polynomials, thus obtaining

$$f(x) = \sum_{k=0}^{n} f(k) g_i(x).$$

However, we can turn this perspective around. Each value $f(x)$ can be written as a linear combination of the values $f(k)$ for $0 \leq k \leq n$. This observation is important enough that we establish it in its own lemma, which is a direct corollary of Lagrange's Interpolation Theorem.

Lemma 20.4.5. *Consider a polynomial $f(x)$. Then each value $f(x)$ can be written as a linear combination of the values $f(0)$, ..., $f(n)$; that is, there are coefficients $a_i(x)$ for each $0 \leq i \leq n$ depending on x such that*

$$f(x) = \sum_{i=0}^{n} a_i(x) f(i).$$

Proof. The coefficients $a_k(x)$ are given by the basis polynomials $g_k(x)$. □

Equipped with this change of perspective, we can prove that a polynomial of degree n is integer values as soon as its values $f(0)$, ..., $f(n)$ are integers.

Theorem 20.4.6. *Consider a polynomial $f(x)$ of degree n with real coefficients. If the values*

$$f(0), \dots, f(n)$$

are integers, then $f(x)$ is an integer for every integer x.

Proof. The basis polynomials of f are

$$g_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x-j}{i-j}.$$

We can express $g_i(x)$ using binomial coefficients as

$$g_i(x) = \prod_{j=0}^{i-1} \frac{x-j}{i-j} \prod_{j=i+1}^{n} \frac{x-j}{i-j} = (-1)^{n-i} \binom{x}{i} \binom{x-i-1}{n-i},$$

which is an integer for every integer x. Therefore it follows by Theorem 20.4.2 (Lagrange's Interpolation Theorem) that every value $f(x)$ can be written as an integer linear combination of the integers $f(0), \dots, f(n)$, which proves the theorem. □

20.5 Fixed Divisors of Integer Polynomials

In Chapter 7, we have done a few exercises which asked us to show that integers in certain polynomial forms satisfy a divisibility property. For example, we showed that $a^3 - a$ is always divisible by 6, and that $a^5 - a$ is always divisible by 30. We also showed that the product of any n consecutive integers is always divisible by $n!$. In this section we will establish a vast generalization of these facts.

DEFINITION 20.5.1. The **fixed divisor** of a function $f : X \to \mathbb{Z}$ into the integers is the greatest common divisor of all values of f, i.e.,

$$\gcd(\{f(x) \mid x \in X\}).$$

Theorem 20.4.2 (Lagrange's Interpolation Theorem) can be used to determine the greatest common divisor of all the values of a polynomial, by examining only one more value than its degree. This observation is due to Kurt Hensel, who was a student of Leopold Kronecker.

THEOREM 20.5.2 (Hensel's Fixed Divisor Theorem [HEN1896]). *Consider a polynomial $f(x)$ of degree n, with integer coefficients. Then the fixed divisor of f is the greatest common divisor*

$$\gcd(f(a), \dots, f(a+n))$$

of any $n+1$ values of consecutive inputs of f.

PROOF. First, we note that by translating the polynomial along the axis of abscissas, which we can do by considering the polynomial $f(a)$, it suffices to show that for any polynomial $f(x)$ of degree n with integer coefficients, the fixed divisor of f is the greatest common divisor of the integers

$$f(0), \dots, f(n).$$

Now recall from Theorem 20.4.6 that the values $f(x)$ are integer linear combinations of the values $f(0), \dots, f(n)$:

$$f(x) = \sum_{i=0}^{n} f(i) g_i(x).$$

It follows that

$$\gcd(f(0), \dots, f(n)) \mid f(x).$$

Since the fixed divisor of f divides this greatest common divisor, this establishes the theorem. □

EXAMPLE 20.5.3. Consider the polynomial

$$f(x) = x^n - x.$$

When n is even, then f is an **even function**, which means that $f(-x) = f(x)$, and when n is odd, then f is an **odd function** which means that $f(-x) = -f(x)$. In either

case, this implies that the fixed divisor of $x^n - x$ is equal to the greatest common divisor of the elements

$$f(0), \ldots, f(m),$$

where m is the largest integer such that $2m \leq n + 1$. In other words, to compute the fixed divisor of $x^n - x$, we only have to inspect about half the amount of values of Hensel's Fixed Divisor Theorem. Furthermore, the polynomial $f(x) = x^n - x$ always satisfies $f(0) = 0$ and $f(1) = 0$, reducing the amount of cases even further. Thus, the fixed divisor of $x^n - x$ is

$$\gcd(\{f(k) \mid 2 \leq k \leq (n+1)/2\}).$$

(i) For $n = 3$, the only number $2 \leq k \leq (n+1)/2$ is the number 2. The polynomial $f(x) = x^3 - x$ from Exercise 6.9 has the value

$$f(2) = 6,$$

so the fixed divisor of $x^3 - x$ is 6, which is $2 \cdot 3$.

(ii) For $n = 5$, the only two numbers $2 \leq k \leq (n+1)/2$ are the numbers 2 and 3. The polynomial $f(x) = x^5 - x$ from Exercise 6.10 has the values

$$f(2) = 30 \qquad \text{and} \qquad f(3) = 240.$$

Since 240 is divisible by 30 it follows that the fixed divisor of $x^5 - x$ is 30, which is $2 \cdot 3 \cdot 5$.

(iii) For $n = 7$, the only three numbers $2 \leq k \leq (n+1)/2$ are the numbers 2, 3, and 4. The polynomial $f(x) = x^7 - x$ has the values

$$f(2) = 126 \qquad \text{and} \qquad f(3) = 2184.$$

Furthermore, using that $4^7 = (2^7)^2$ we see that $f(4)$ factors as $(2^7 - 2)(2^7 + 2)$ by the formula for the difference of squares. Therefore it follows that the fixed divisor of $f(x)$ is the greatest common divisor of $f(2)$, $f(3)$, and $f(4)$, which is just the greatest common divisor of $f(2)$ and $f(3)$, which is

$$\gcd(126, 2184) = 42 = 2 \cdot 3 \cdot 7.$$

We will generalize these examples in Theorem 29.2.2.



Exercises

Starter Exercises

20.1 Find two integers a and b such that

$$a + b = 150 \qquad \text{and} \qquad ab = 2025.$$

Hint: To avoid guessing, use that a and b are roots of the polynomial $x^2 - (a + b)x + ab$ by Vieta's relations.

20.2 Find a polynomial $f(x)$ such that

$$(x + 1)(x + 2)(x + 3)(x + 4) + 1 = f(x)^2.$$

Routine-Building Exercises

20.3 Show that $x^{13} - x$ has fixed divisor

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13.$$

20.4 *The rational root theorem.* Show that if the polynomial equation

$$a_n x^n + \cdots a_1 x + a_0 = 0$$

with integer coefficients has a rational solution $x_0 = \frac{s}{t}$ with $\gcd(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$. Conclude that if the polynomial is monic, meaning that $a_n = 1$, then any rational root is an integer. Also conclude that $\sqrt[3]{7}$ is irrational.

20.5 (a) (Sophie Germain's identity) Write

$$x^4 + 4y^4$$

as a difference of two squares.

(b) Compute the fixed divisor of the polynomial $f(x) = x^4 + 4$.

(c) Compute the polynomial $g(x) = \gcd(x^4 + 4, (x + 2)^4 + 4)$, and show that $g(x) > 1$ for every integer x.

(d) Find all positive integers x and y for which $x^4 + 4y^4$ is prime.

20.6 (Gauss's Gem) Write

$$f(x, y, z) := x^3 + y^3 + z^3 - 3xyz$$

in the form $\frac{1}{2}d(a^2 + b^2 + c^2)$ for some quadruple of integers a, b, c, d depending on x, y, and z. Hint: For $x + y + z = 0$, evaluate $f(x, y, z)$.

20.7 Show that a number n is square-free if and only if the only integer x satisfying the congruence $x^2 \equiv 0 \pmod{n}$ is $x = 0$.

20.8 Show that there are only two polynomials f such that any two values $f(x)$ and $f(y)$ are relatively prime for distinct inputs x and y.

20.9 Consider a prime number p. Construct for every integer $0 \leq a < p$ a polynomial $f(x)$ of degree $< p$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$ such that

$$f(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{otherwise.} \end{cases}$$

Use these polynomials similarly to the basis polynomials in Theorem 20.4.2 (Lagrange's Interpolation Theorem) to show that every function $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is polynomial.

20.10 Define the kth **power sum**

$$p_k(a_1, \ldots, a_n) := a_1^k + \cdots + a_n^k.$$

We will simply write p_k for $p_k(a_1, \ldots, a_n)$ and e_k for $e_k(a_1, \ldots, a_n)$.

(a) *The Newton-Girard identities.* Show that for all k we have

$$p_k = e_1 p_{k-1} - e_2 p_{k-2} + \cdots + (-1)^{k-1} e_{k-1} p_1 + (-1)^{k-1} k e_k.$$

Hint: This looks more complicated than it is.

(b) Prove that the congruence

$$1^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$$

holds for every $0 < k < p - 1$, and every prime number p.

Challenge Exercises

20.11 (Pólya [Pól1919]) Consider a polynomial $f(x)$ of degree n with rational coefficients. Show that if there exists $n + 1$ distinct integers $x_0, \ldots, x_n$ such that

$$\sum_{i=0}^{n} |f(x_i)| < \frac{n!}{2^n},$$

then $f(x)$ cannot be a polynomial with integer coefficients.



Chapter 21

Primitive Roots

21.1 Counting Elements of a Given Order Modulo a Prime

Theorem 16.2.1 (Euler's Theorem) tells us that

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

for every integer a such that $\gcd(a, n) = 1$. By Theorem 8.5.2 (Order Theorem), this implies that

$$\mathrm{ord}_n(a) \mid \phi(n).$$

Euler's theorem therefore gives an upper bound for the order of any element modulo n. For example, since 13 is a prime number, we have $\phi(13) = 12$, so all integers relatively prime to 13 have an order dividing the number 12. Computing the powers of 2, for instance, we see that $\mathrm{ord}_{13}(2) = 12$:

m	0	1	2	3	4	5	6	7	8	9	10	11
$2^m \pmod{13}$	1	2	4	8	3	6	12	11	9	5	10	7.

The process of doubling integers modulo 13 is illustrated in Figure 21.1. Using Theorem 8.5.4, we can use this table to compute the orders of all the nonzero integers modulo 13. Recall that Theorem 8.5.4 states that

$$\mathrm{ord}_n(a^m) = \frac{\mathrm{ord}_n(a)}{\gcd(m, \mathrm{ord}_n(a))}.$$

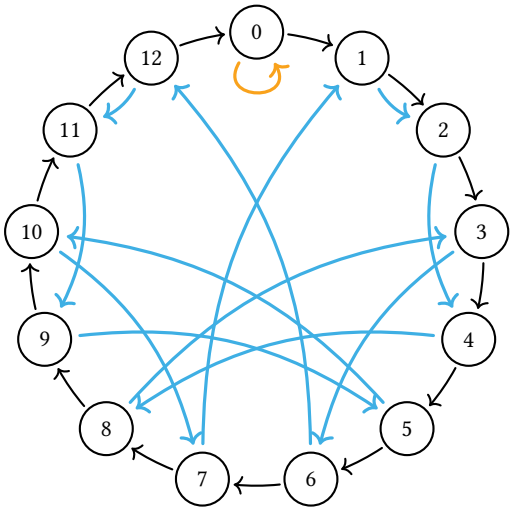


Figure 21.1: Doubling integers modulo 13.

For example, since $3 \equiv 2^4 \pmod{13}$, it follows that the order of 3 modulo 13 is 3. Similarly, since $5 \equiv 2^9 \pmod{13}$, it follows that

$$5^4 \equiv (2^9)^4 \equiv (2^{12})^3 \equiv 1 \pmod{13}.$$

Computing the orders of all the elements from 1 to 12 modulo 13 this way, we obtain:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ord}_{13}(a)$	1	12	3	6	4	12	12	4	3	6	12	2.

While the orders of the integers modulo 13 might at first glance appear to be somewhat unwieldy, Theorem 8.5.4 is the key to some important patterns. For example, given an integer $a \pmod{p}$ with $\operatorname{ord}_p(a) = p - 1$ such as $2 \pmod{13}$, Theorem 8.5.4 tells us that

$$\operatorname{ord}_p(a^m) = k \quad \Leftrightarrow \quad \frac{p-1}{\gcd(m, p-1)} = k$$

In particular, $\operatorname{ord}_p(a^m) = p - 1$ if and only if $\gcd(m, p - 1) = 1$. Indeed, we see that there are four integers modulo 13 of order 12, corresponding to the powers of 2 with exponents 1, 5, 7, and 11.

However, we can go further: There are two integers that have order 6 modulo 13, and indeed $\phi(6) = 2$ as well. Similarly, we find that there are $\phi(1)$, $\phi(2)$, $\phi(3)$, and $\phi(4)$ integers of order 1, 2, 3, and 4, respectively. The following theorem tells us that modulo a prime p, the number of integers of order k modulo p is either 0 or $\phi(k)$. This suggests that for any prime number p and any $k \mid p - 1$, it should be true that the number of elements of order k is exactly $\phi(k)$.

Theorem 21.1.1. *Consider a prime number p. Then there are for every $k \mid p-1$ exactly $\phi(k)$ integers of order k modulo p.*

The proof of this theorem makes essential use of the fact that any polynomial congruence of the form

$$x^d \equiv 1 \pmod{p}$$

has at most d solutions. This was established in Theorem 20.3.3. To emphasize this observation, we will prove Theorem 21.1.1 as a consequence of the following more general theorem.

Theorem 21.1.2. *Consider a number n with the property that every polynomial congruence of the form*

$$x^d \equiv 1 \pmod{n}$$

has at most d solutions. Then there are for every $k \mid \phi(n)$ exactly $\phi(k)$ integers of order k modulo n.

Proof. In this proof, let us write $\psi(k)$ for the number of integers of order k modulo n. We claim that

$$\psi(k) = \begin{cases} \phi(k) & \text{if } k \mid \phi(n), \\ 0 & \text{otherwise.} \end{cases}$$

The fact that if $k \nmid \phi(n)$ then $\psi(k) = 0$ follows immediately from Theorem 8.5.2 (Order Theorem) and Theorem 16.1.1 (Fermat's Little Theorem). Thus, it remains to show that $\psi(k) = \phi(k)$ for any $k \mid \phi(n)$.

Consider an integer a of order k modulo n. By definition, every integer of order k modulo n is a solution to the polynomial congruence

$$x^k \equiv 1 \pmod{n}.$$

This polynomial congruence has at most k solutions. Given that the integer a has order k modulo n, we see that the set of solutions can be described exactly as the following set of numbers:

$$1,\ a,\ \ldots,\ a^{k-1}.$$

Thus, we see that every solution is congruent to a power of a. In particular, it follows that every integer of order k modulo n is itself a power of a. Recall from Theorem 8.5.4 that an integer of the form a^m has order k if and only if $\gcd(m,k) = 1$. Thus we conclude that, given an element of order k, there are exactly $\phi(k)$ integers of order k. In other words, $\psi(k)$ is either 0 or $\phi(k)$, and certainly we have that $\psi(k) \leq \phi(k)$.

To finish the proof, observe that, since every element $1 \leq x < n$ relatively prime to n has an order modulo n, we have

$$\phi(n) = \sum_{k \mid \phi(n)} \psi(k) \leq \sum_{k \mid \phi(n)} \phi(k) = \phi(n).$$

It follows that the inequality is in fact an equality, and since $\psi(k) \leq \phi(k)$ for every $k \mid \phi(n)$ it follows that $\psi(k) = \phi(k)$ for every $k \mid \phi(n)$. □

21.2 Primitive Roots

We saw in the previous section that there are exactly $\phi(k)$ integers of order k modulo p, for every $k \mid p-1$. It follows that there are

$$\phi(p-1)$$

integers of order $p-1$. Since $\phi(p-1) > 0$, it follows that for every prime number p, there is an integer g such that the integers

$$1, g, g^2, \dots, g^{p-2}$$

form a reduced residue system modulo p. That is, there is an integer g such that every integer a relatively prime to p is congruent to exactly one power g^k, where $0 \leq k < p-1$. Such integers are called *primitive roots*. In the previous section we saw that 2 is a primitive root of the prime 13.

DEFINITION 21.2.1. A **primitive root** modulo a natural number n is an integer g such that

$$\operatorname{ord}_n(g) = \phi(n).$$

THEOREM 21.2.2. *Consider a natural number n. The following are equivalent:*

(i) *The number n admits a primitive root modulo n.*

(ii) *Any polynomial congruence of the form*

$$x^d \equiv 1 \pmod{n}$$

has at most d solutions.

Furthermore, if the first condition holds then there are $\phi(\phi(n))$ primitive roots, and if the last condition holds and the polynomial congruence $x^d \equiv 1 \pmod{n}$ has a solution, then it has exactly $\gcd(d, \phi(n))$ solutions.

PROOF. We have already proven that ii implies i in Theorem 21.1.2. To prove that i implies ii, consider a primitive root g modulo n, and consider the polynomial congruence

$$x^d \equiv 1 \pmod{n}.$$

An integer $a \equiv g^m \pmod{n}$ is a solution if and only if $g^{dm} \equiv 1 \pmod{n}$. Since we assumed that $\operatorname{ord}_n(g) = \phi(n)$, it follows from Theorem 8.5.2 (Order Theorem) that the congruence $g^{dm} \equiv 1 \pmod{n}$ holds if and only if $\phi(n) \mid dm$. The number of $0 \leq m < \phi(n)$ such that $\phi(n) \mid dm$ is exactly $\gcd(d, \phi(n))$, which is at most d. Therefore, it follows that there are at most d solutions to the congruence $x^d \equiv 1 \pmod{n}$. □

COROLLARY 21.2.3. *The number of primitive roots of a prime number p is $\phi(p-1)$. In particular, every prime p admits a primitive root.*

Example 21.2.4. The number 9 has the primitive root 2. Indeed $\phi(9) = 6$, and $2^3 \equiv -1 \pmod 9$ so that $\operatorname{ord}_9(2) = 6$. Thus, by the previous theorem it follows that the congruence $x^d \equiv 1 \pmod 9$ has at most d solutions.

Nevertheless, there are polynomials $f(x)$ of degree 2 that are not of this form that have more than two solutions among the integers relatively prime to 9. For example, the polynomial congruence

$$x^2 + x + 7 \equiv 0 \pmod 9,$$

has the three solutions $x \equiv 1$, 4, and 7 $\pmod 9$.

Some further composite numbers with primitive roots include 4 and 6: The number 3 is a primitive root of 4, and 5 is a primitive root of 6.

The number 8, on the other hand, does not have primitive roots because $\phi(8) = 4$ while the odd integers 3, 5, and 7 all have order 2. In fact, it is possible to precisely classify all the natural numbers that have primitive roots. We will do so in Theorem 22.2.1.

21.3 The Discrete Logarithm

It is useful to have access to primitive roots, if they exist, because if g is a primitive root modulo n, then the integers

$$1, g, g^2, \dots, g^{\phi(n)-1}$$

form a reduced residue system modulo n. This means that every number relatively prime to n is congruent to exactly one of the integers g^i, for $0 \le i < \phi(n)$. Having a primitive root therefore gives a convenient way of representing all the elements of a reduced residue system.

Definition 21.3.1. Suppose g is a primitive root modulo n, and let a be an integer relatively prime to n. Then we define the **discrete logarithm** or **index**

$$\operatorname{ind}_g(a)$$

of a base g to be the unique integer k modulo $\phi(n)$ such that $g^k = a$.

Theorem 21.3.2. *Consider a natural number n with a primitive root g.*

(i) *For any two integers a and b relatively prime to n, we have*

$$a \equiv b \pmod n \quad \Leftrightarrow \quad \operatorname{ind}_g(a) \equiv \operatorname{ind}_g(b) \pmod{\phi(n)}.$$

(ii) *Furthermore, we have*

$$\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g(a) + \operatorname{ind}_g(b) \pmod{\phi(n)}$$
$$\operatorname{ind}_g(a^m) \equiv m \operatorname{ind}_g(a) \pmod{\phi(n)}.$$



EXAMPLE 21.3.3. Solving linear congruences becomes quite a straightforward task when a primitive root is known. For example, the congruence

$$14x \equiv 6 \pmod{26}$$

is solvable if and only if $7x \equiv 3 \pmod{13}$ is. By the previous theorem, this linear congruence is equivalent to the linear congruence

$$\operatorname{ind}_2(7) + \operatorname{ind}_2(x) \equiv \operatorname{ind}_2(3) \pmod{12}.$$

Since $\operatorname{ind}_2(7) = 11$ and $\operatorname{ind}_2(3) = 4$, we find that $\operatorname{ind}_2(x) \equiv 5 \pmod{12}$. Thus, we conclude that

$$x \equiv 6 \pmod{13}$$

is a solution of the original linear congruence.

21.4 A Criterion for Congruences of Degree n

While we are primarily interested in the quadratic congruence

$$x^2 \equiv a \pmod{p}$$

in this introductory course on elementary number theory, the techniques that we have developed so far perfectly allow us to cover the nth degree congruence

$$x^n \equiv a \pmod{p}.$$

The following theorem is a significant generalization of Theorem 27.4.1 (Euler's Criterion).

THEOREM 21.4.1. *Consider an integer a and a prime p so that $p \nmid a$. The following are equivalent:*

(i) *The congruence*

$$x^n \equiv a \pmod{p}$$

has a solution.

(ii) *The congruence*

$$\frac{p-1}{\operatorname{ord}_p(a)} \equiv 0 \pmod{\gcd(n, p-1)}$$

holds.

(iii) *The congruence*

$$a^{\frac{p-1}{\gcd(n,p-1)}} \equiv 1 \pmod{p}$$

holds.

If the first condition holds, then the congruence $x^n \equiv a$ has exactly $d := \gcd(n, p-1)$ solutions.

Proof by primitive roots. Let $m := (p-1)/\operatorname{ord}_p(a)$, and consider a primitive root g modulo p such that

$$g^m \equiv a \pmod{p}.$$

Then the congruence

$$x^n \equiv a \pmod{p}$$

is solvable if there exists an integer t such that

$$g^{tn} \equiv g^m \pmod{p}.$$

In other words, the first congruence is solvable if and only if the congruence

$$tn \equiv m \pmod{p-1}$$

is solvable. It follows from Theorem 9.1.2 that this congruence is solvable if and only if $d := \gcd(n, p-1) \mid m$, and in this case there are exactly d solutions. Thus we have shown that *1.* is equivalent to *2.*

To show that *3.* is equivalent to *2.*, consider the condition that

$$a^{\frac{p-1}{\gcd(n,p-1)}} \equiv 1 \pmod{p}.$$

This holds if and only if $\frac{m(p-1)}{\gcd(n,p-1)}$ is an integer multiple of $p-1$, which is equivalent to the condition that $\gcd(n, p-1) \mid m$. □

Proof by Lagrange's theorem. For both directions of the proof, we will write $d := \gcd(n, p-1)$, so that there are integers k and l such that $kd = p-1$ and $ld = n$. It follows that k and l are relatively prime, so that there are integers u and v such that

$$ku + lv = 1.$$

To prove the forward implication, assume that x is an integer such that $x^n \equiv a \pmod{p}$. Then we have by Theorem 16.1.1 (Fermat's Little Theorem)

$$a^k \equiv x^{kn} = x^{kld} = (x^{p-1})^l \equiv 1^l = 1 \pmod{p}.$$

Since $k = (p-1)/\gcd(n, p-1)$, we have proven the forward implication.

For the converse, assume that $a^k \equiv 1 \pmod{p}$. Now we can use the formula for the difference of kth powers to write

$$x^{p-1} - 1 = x^{kd} - 1 \equiv x^{kd} - a^k = (x^d - a) \sum_{i=0}^{k-1} x^{di} a^{k-1-i}.$$

Since the polynomial $x^{p-1}-1$ has exactly $p-1$ roots modulo p, it follows that the number of roots of each factor on the right-hand side is equal to its degree. In other words, the polynomial

$$x^d - a$$

has d roots. Given a root $x^d \equiv a \pmod{p}$, we define $y := x^v$ where $ku + lv = 1$. Then we have

$$y^n = x^{vld} \equiv a^{lv} \equiv a^{1-ku} \equiv a(a^k)^{-u} \equiv a1^{-u} \equiv a \pmod{p}. \qquad \square$$

COROLLARY 21.4.2. *Consider an integer a such that $\operatorname{ord}_p(a) \mid n$. Then the congruence*

$$x^n \equiv a \pmod{p}$$

is solvable if and only if

$$p \equiv 1 \pmod{\operatorname{ord}_p(a) \cdot \gcd(n, p-1)}.$$

COROLLARY 21.4.3. *Consider a prime p and a natural number n relatively prime to $p-1$. Then every nth degree congruence*

$$x^n \equiv a \pmod{p}$$

has a unique solution. In other words, the map $x \mapsto x^n$ is a bijection on $\mathbb{Z}/p\mathbb{Z}$.

In the following corollary, we show that the congruence $x^n \equiv -1 \pmod{p}$ is solvable if and only if the 2-adic valuation of n is strictly smaller than the 2-adic valuation of $p-1$. In other words, for any number $n = 2^k m$ with m odd, the congruence

$$x^n \equiv -1 \mod p$$

is solvable if and only if $p \equiv 1 \pmod{2^{k+1}}$.

COROLLARY 21.4.4. *The congruence*

$$x^n \equiv -1 \pmod{p}$$

is solvable if and only if $v_2(n) < v_2(p-1)$.

PROOF. Since the congruence $x^n \equiv -1 \pmod{p}$ is solvable if and only if

$$(-1)^{\frac{p-1}{\gcd(n,p-1)}} \equiv 1 \pmod{p},$$

it suffices to show that the exponent $\frac{p-1}{\gcd(n,p-1)}$ is an even integer if and only if $v_2(n) < v_2(p-1)$. Indeed, this exponent is even if and only if $\min(v_2(n), v_2(p-1)) = v_2(\gcd(n, p-1)) < v_2(p-1)$. This strict inequality holds if and only if $v_2(n) < v_2(p-1)$. $\square$

Exercises

Starter Exercises

21.1 (a) Find the least primitive root g modulo 23, and give a table of the congruence classes of its powers.
(b) Find all primitive roots modulo 23.
(c) For each $k \mid \phi(23)$, find all elements of order k modulo 23.
(d) For each integer $1, \ldots, 22$, find its index base g modulo 23.
(e) Solve the linear congruence

$$8x \equiv 9 \pmod{23}$$

using indices.

21.2 (a) Show that the number of solutions to the congruence

$$x^n \equiv a \pmod{p}$$

is either $\gcd(n, p-1)$ or 0.
(b) Find, as Gauss did in article 60 of *Disquisitiones Arithmeticae* [Gau1986], all the solutions to the congruence

$$x^{15} \equiv 11 \pmod{19}.$$

Routine-Building Exercises

21.3 In article 55 of *Disquisitiones Arithmeticae* [Gau1986], Gauss gives a second, more explicit construction of primitive roots. In this exercise we will follow this method.
Consider a prime p and suppose that the prime factorization of $p-1$ is

$$p - 1 = q_1^{\alpha_1} \cdots q_n^{\alpha_n}.$$

(a) By Theorem 20.3.2 (Lagrange's Theorem) it follows that for each prime q_i, the congruence

$$x^{\frac{p-1}{q_i}} \equiv 1 \pmod{p}$$

has strictly fewer than $p-1$ solutions, so there must exist a residue x which is not a solution. Using such x, construct an element a_i such that

$$\operatorname{ord}_p(a_i) = q_i^{\alpha_i}.$$

(b) Show that

$$\operatorname{ord}_p(a_1 \cdots a_n) = p - 1$$

and conclude that the product $a_1 \cdots a_n$ is a primitive root.



(c) Use this method to find a primitive root modulo 67.

21.4 Consider a prime $p \neq 3$. Prove that the product of all primitive roots modulo p is congruent to 1 modulo p.

21.5 (a) Consider a prime number p. Show that the following are equivalent:

(i) There is a solution to the congruence

$$x^n \equiv a \pmod{p}$$

of the form $x = a^k$.

(ii) The exponent n is relatively prime to $\operatorname{ord}_p(a)$.

(b) Find a solution to the congruence

$$x^3 \equiv 5 \pmod{13}$$

of the form $x = 5^k$.

21.6 Consider a prime p with a primitive root g, and let $d \mid p-1$. Prove the congruence

$$\sum_{\substack{0 \leq m < p-1 \\ m \equiv 0 \pmod{d}}} g^m \equiv \left\lfloor \frac{d}{p-1} \right\rfloor \pmod{p}.$$

Challenge Exercises

21.7 For any prime p and any integer a not divisible by p, show that the number of primitive roots g modulo p such that

$$g^{\frac{p-1}{\operatorname{ord}_p(a)}} \equiv a \pmod{p}.$$

is $\phi(p-1)/\phi(\operatorname{ord}_p(a))$. Conclude that such a primitive root always exists.

21.8 Consider a prime $p > 2$ and an odd number m. Show that the congruence $x^{2^n m} \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{2^{n+1}}$.

21.9 Consider a prime p of the form $n^2 + 1$. Show that

$$x^n \equiv a \pmod{p} \text{ is solvable} \quad \Leftrightarrow \quad a^n \equiv 1 \pmod{p}.$$

21.10 [GAU1986, art. 81] Consider a prime p. Prove that the sum of all primitive roots satisfies the following property:

$$\sum_{g \text{ primitive root } \pmod{p}} g \equiv \mu(p-1) \pmod{p}.$$

21.11 [GAU1986, art. 78] For any positive integer n, show that

$$\prod_{\substack{0 < x < n \\ \gcd(x,n) = 1}} x \equiv \begin{cases} -1 \pmod{n} & \text{if there is a primitive root modulo } n, \\ 1 \pmod{n} & \text{otherwise.} \end{cases}$$

Hint: Use Theorem 9.3.1 (Chinese Remainder Theorem) to show that the number of integers $0 \leq x < n$ such that $x^2 \equiv 1 \pmod{n}$ is a power of 2.

Chapter 22

The Moduli with Primitive Roots

We have established the existence of primitive roots modulo any prime. In this section, we will give a complete characterization of those moduli for which a primitive root exists.

22.1 Primitive Roots Modulo Odd Prime Powers

Our first target is to show that any odd prime power p^k has a primitive root. Our approach to this problem is of an arithmetic nature, based on an analysis of the p-valuations of differences of powers.

Recall that for any integer a not divisible by p, the integer $a^{p-1}-1$ is divisible by p by Theorem 16.1.1. Therefore, its p-adic valuation $\alpha := v_p(a^{p-1}-1)$ is at least 1. In the following lemma we will establish that the order of a modulo p^k can be determined in terms of α.

Lemma 22.1.1. *Consider an odd prime p and a primitive root g modulo p. Furthermore, let*

$$m := v_p(g^{p-1}-1).$$

Then the order of g modulo p^k is $p^{\max(0,k-m)}(p-1)$.



PROOF. First, we observe that $\operatorname{ord}_p(g) \mid \operatorname{ord}_{p^k}(g)$, so the order of g modulo p^k must be a multiple of $p-1$. Write $g^{p-1} = kp^m + 1$, so that $p \nmid k$. By Theorem 19.5.2 (Lifting the Exponent) it follows that

$$v_p(g^{p^t(p-1)} - 1) = m + t.$$

Consequently, for any integer s not divisible by p we have

$$g^{p^t s(p-1)} = (kp^{m+t} + 1)^s \equiv 1 + skp^{m+t} \pmod{p^{m+t+1}}.$$

This shows that $v_p(g^{p^t s(p-1)} - 1) = m + t$ for such s. The first exponent r such that $g^r \equiv 1 \pmod{p^k}$ is therefore $r = p^{\max(0,k-m)}(p-1)$. □

THEOREM 22.1.2. *Any prime power p^k with $k \geq 1$ admits a primitive root.*

PROOF. By Lemma 22.1.1 it suffices to construct a primitive root h modulo p such that $v_p(h^{p-1} - 1) = 1$.

Consider a primitive root g modulo p. Write $g^{p-1} = kp+1$, and define $h_t := g+tp$. Then we have

$$h_t^{p-1} = (g + tp)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}tp \equiv 1 + p(k - g^{p-2}t) \pmod{p^2}.$$

Thus we see that $h_t^{p-1} \equiv 1 \pmod{p^2}$ if and only if

$$k \equiv g^{p-2}t \pmod{p}.$$

This linear congruence has the unique solution $t \equiv kg \pmod{p}$. Thus we see that for any $t \not\equiv kg \pmod{p}$, we have $h_t^{p-1} \not\equiv 1 \pmod{p^2}$ and hence

$$v_p(h_t^{p-1} - 1) = 1.$$ □

22.2 The Complete Characterization of Moduli with Primitive Roots

THEOREM 22.2.1. *Consider a positive integer n. The following are equivalent:*

(i) *The number n admits a primitive root.*

(ii) *Either $n = 2$, or there is a unique element of order 2 modulo n.*

(iii) *We have*

$$n = 2,\ 4,\ p^k,\ \text{or}\ 2p^k,$$

where p is an odd prime.

Proof. We saw in Theorem 21.2.2 that if n admits a primitive root, then the congruence

$$x^d \equiv 1 \pmod{n}$$

had at most d solutions, for any $d \geq 0$. In particular, there are at most two solutions to the congruence $x^2 \equiv 1 \pmod{n}$. One of them is the number 1, which is of order 1. The other is -1, which is of order 2. Since any element of order 2 is a solution to the congruence $x^2 \equiv 1 \pmod{n}$, we see that i implies ii.

Next, assume that there is a unique element of order 2 modulo n. The case $n = 4$ is swiftly dealt with, since -1 is the unique integer of order 2 modulo 4. If $n = 2^k$ for some $k \geq 3$, then there are three integers of order 2 modulo 2^k:

$$x = -1 \qquad \text{and} \qquad x = 2^{k-1} \pm 1.$$

Thus we see that if $n = 2^k$ for some $k \geq 3$, then n does not satisfy the hypothesis in ii.

Now suppose that $n = km$, where $\gcd(k, m) = 1$ and m is odd and strictly greater than 1. By Theorem 9.3.1 (Chinese Remainder Theorem), it follows that any pair of solutions

$$x^2 \equiv 1 \pmod{k},$$
$$y^2 \equiv 1 \pmod{m},$$

determines a unique solution to the congruence $z^2 \equiv 1 \pmod{km}$. It follows that one of them can have only one nontrivial solution. Since we assumed that $m > 1$ is odd, and thus has two distinct solutions, it follows that there is only one solution to the congruence $x^2 \equiv 1 \pmod{k}$. Observe that there is only one such solution if and only if $k = 1$ or $k = 2$. Furthermore, the previous observation implies that m cannot have distinct prime factors, so we conclude that m must be of the form $m = p^k$ for some odd prime p. Thus we have proven that ii implies iii.

Finally, we have to show that any number of the form $n = 2, 4, p^k$, or $2p^k$, where p is an odd prime, admits a primitive root. The number 1 is a primitive root modulo 2, and the number -1 is a primitive root modulo 4. The fact that any odd prime power p^k admits primitive roots was established in Theorem 22.1.2. To finish the proof that iii implies i, it therefore remains to show that each number of the form $n = 2p^k$, where p is an odd prime, has a primitive root. To see this, observe that the integers relatively prime to $2p^k$ are exactly the odd integers $1 \leq x < 2p^k$ relatively prime to p^k. Among those odd integers is a primitive root g modulo p^k. Its order modulo $2p^k$ is

$$\operatorname{ord}_{2p^k}(g) = \operatorname{ord}_{p^k}(g) = p^{k-1}(p-1) = \phi(2p^k),$$

so we see that g is also a primitive root of $2p^k$. □

22.3 Carmichael's Function

Chapter 23

Polynomial Congruences

23.1 Polynomial Congruences of Composite Moduli

In the following theorem we generalize Theorem 9.3.1 (Chinese Remainder Theorem) to polynomial congruences.

Theorem 23.1.1. *Consider an integer polynomial f and consider two relatively prime integers m and n. Then any solution of the system*

$$f(x) \equiv 0 \pmod{m}$$
$$f(x) \equiv 0 \pmod{n}$$

of polynomial congruences corresponds uniquely to a solution of the polynomial congruence

$$f(x) \equiv 0 \pmod{mn}.$$

Proof. First note that if $f(x) \equiv 0 \pmod{mn}$, then it follows that $f(x) \equiv 0 \pmod{m}$ and $f(x) \equiv 0 \pmod{n}$, simply because divisibility is transitive. Consequently, if y is the unique nonnegative integer strictly below m such that $x \equiv y \pmod{m}$, then $f(y) \equiv \pmod{m}$ is also a solution, and similar for the modulus n. Thus if we write $N_{mn}(f)$ for the set of roots of f modulo mn, and $N_m(f)$ and $N_n(f)$ for the sets of roots of f modulo m and n, respectively, then we define a map

$$\pi : N_{mn}(f) \to N_m(f) \times N_n(f)$$

by $x \mapsto (x \pmod{m}, x \pmod{n})$. We claim that the map π is a bijection.

To see that the map π is a bijection, consider $0 \leq y < m$ and $0 \leq z < n$ such that

$$f(y) \equiv 0 \pmod{m}$$
$$f(z) \equiv 0 \pmod{n}.$$

By the assumption that $\gcd(m, n) = 1$, we obtain from Theorem 9.3.1 (Chinese Remainder Theorem) there a unique $0 \leq x < mn$ such that

$$x \equiv y \pmod{m}$$
$$x \equiv z \pmod{n}.$$

Consequently, we have that $f(x) \equiv 0 \pmod{m}$ and $f(x) \equiv 0 \pmod{n}$. Applying the Chinese Remainder Theorem once more to the number $f(x)$, using that 0 is the only integer u modulo mn such that $u \equiv 0 \pmod{m}$ and $u \equiv 0 \pmod{n}$, we find that $f(x) \equiv 0 \pmod{mn}$. □

COROLLARY 23.1.2. *Consider $n = p_1^{k_1} \cdots p_m^{k_m}$, where all the primes p_i are distinct. A polynomial congruence*

$$f(x) \equiv 0 \pmod{n}$$

is solvable if and only if the polynomial congruence

$$f(x) \equiv 0 \pmod{p_i^{k_i}}$$

is solvable for each i.

PROOF. By induction on the number of prime factors of n. □

23.2 Derivatives of Polynomials

The derivative of a function f at a point x, if it exists, measures the rate of change of f in close vicinity of x. It is formally defined as the limit

$$f'(x) := \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

Intuitively, such a limit exists if we can determine a unique value $y = f'(x)$ so that the quanitity $(f(x+h) - f(x))/h$ gets arbitrarily close to y as h gets arbitrarily close to 0. When such a limit exists for every x, we say that f is **differentiable**. Many of the most common functions are differentiable, except at obvious points of discontinuity as seen, for instance, in step functions, or functions with sudden change of direction such as the absolute value function. In this short section we will prove that all polynomials are differentiable. There is an important theorem in number theory that require knowledge of the derivatives of polynomials: In our proof of Theorem 23.3.1 (Hensel's Lemma) we will make use of Theorem 23.2.3 (Taylor Expansion Theorem for Polynomials) proven below.

The following theorem is not only useful when h approaches 0. For example, in the case where h is a prime p it tells us that $f(x+p) - f(x)$ is always a multiple of p.

Theorem 23.2.1. *Consider the polynomial*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Then the polynomial $f(x+h) - f(x)$ is divisible by h, with quotient

$$\frac{f(x+h)-f(x)}{h} = \sum_{k=1}^{n} \sum_{i=0}^{k-1} a_k x^i (x+h)^{k-1-i}.$$

Proof. By the formula for the difference of kth powers, which was stated in Exercise 2.5, we can write

$$(x+h)^k - x^k = h \sum_{i=0}^{k-1} x^i (x+h)^{k-1-i}$$

In particular, since each of these differences of kth powers is divisible by h, we see that the polynomial $f(x+h) - f(x)$ is divisible by h. It follows that

$$f(x+h) - f(x) = \sum_{k=0}^{n} a_k ((x+h)^k - x^k) = h \sum_{k=1}^{n} a_k \sum_{i=0}^{k-1} x^i (x+h)^{k-1-i}. \qquad \square$$

Theorem 23.2.2. *Consider the polynomial $f(x) = a_n x^n + \cdots + a_0$. Then f is differentiable at every x, and the derivative can be computed by the formula*

$$f'(x) = \sum_{k=1}^{n} k a_k x^{k-1}.$$

Proof. Since polynomials are continuous functions, we can compute the limit as $h \to 0$ simply by evaluating the quotient of $f(x+h) - f(x)$ divided by h at 0:

$$f'(x) = \sum_{k=1}^{n} \sum_{i=0}^{k-1} a_k x^i (x+0)^{k-1-i} = \sum_{k=1}^{n} \sum_{i=0}^{k-1} a_k x^{k-1} = \sum_{k=1}^{n} k a_k x^{k-1}$$

In the last equality we used that the summands in the inner summation do not depend on the summation index i. $\square$

The derivative of any polynomial $f(x)$ is again a polynomial. An immediate consequence of the previous theorem is that if $h(x) = af(x) + bg(x)$ is a linear combination of the polynomials $f(x)$ and $g(x)$, then the derivative of h can be written as the linear combination

$$h'(x) = af'(x) + bg'(x).$$

It also follows that, since the derivative is again a polynomial, it is again differentiable. Thus we have iterated derivatives of polynomials. We will write $\frac{d^k}{dx^k} f(x)$ or $f^{(k)}(x)$ for the kth deriviative of $f(x)$. A straightforward induction argument shows that

$$\frac{d^k}{dx^k} x^n = n(n-1)\cdots(n-k+1)x^{n-k}.$$



We can phrase this identity equivalently as:

$$\frac{1}{k!}\frac{d^k}{dx^k}x^n = \binom{n}{k}x^{n-k}.$$

This leads to the following theorem by Brook Taylor, who stated the result more generally in terms of *fluent quantities* in his work *Methodus incrementorum directa et inversa* [TAY1715]. Although Taylor was the first to prove the series expansion that now bears his name, the method was discovered first without proof by James Gregory, who shared his insight in a letter to John Collins in 1671 [GRE1671]. More on the history of Taylor series can be found in [FEI1985].

THEOREM 23.2.3 (Taylor Expansion Theorem for Polynomials). *Consider the polynomial*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Then we have for each y, the identity

$$f(x+y) = \sum_{k=0}^{n} \frac{f^{(k)}(x)}{k!}y^k.$$

In particular, there is a polynomial $g(x,y)$ in the variables x and y, such that

$$f(x+y) = f(x) + yf'(x) + y^2 g(x,y).$$

PROOF. We will first prove the theorem for $f(x) := x^n$. By Theorem 3.5.1 (The Binomial Theorem) and our earlier observation that $\frac{1}{k!}\frac{d^k}{dx^k}x^n = \binom{n}{k}x^{n-k}$, it follows that

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k = \sum_{k=0}^{n}\frac{1}{k!}\frac{d^k x^n}{dx^k}y^k.$$

This shows that the Taylor expansion formula holds for $f(x) = x^n$. The general claim follows, since every polynomial is a linear combination of polynomials of the form x^i and differentiation preserves linear combinations. Finally, observe that

$$f(x+y) = f(x) + yf'(x) + y^2\sum_{k=2}^{n}\frac{f^{(k)}(x)}{k!}y^{k-2}.$$

This completes the proof of the final claim. □

23.3 Hensel's Lemma

THEOREM 23.3.1 (Hensel's Lemma). *Consider a prime number p and a polynomial $f(x)$ with integer coefficients. Furthermore, consider an integer a such that*

$$f(a) \equiv 0 \pmod{p} \qquad \textit{and} \qquad f'(a) \not\equiv 0 \pmod{p},$$

where $f'(x)$ is the derivative of f. Then there exists for every $k \geq 1$ a unique integer a_k modulo p^k with $a_1 \equiv a \pmod{p}$ such that the congruences

$$a_{k+1} \equiv a_k \pmod{p^k}, \qquad \text{and} \qquad f(a_k) \equiv 0 \pmod{p^k}$$

hold for all k.

Proof. We prove the claim by induction. That is, we prove by induction that for each $k \geq 1$ and every integer $a_k \equiv a \pmod{p}$ satisfying

$$f(a_k) \equiv 0 \pmod{p^k} \qquad \text{and} \qquad f'(a_k) \not\equiv 0 \pmod{p^k},$$

there is a unique integer $a_{k+1} \pmod{p^{k+1}}$ satisfying

$$f(a_{k+1}) \equiv 0 \pmod{p^{k+1}} \qquad \text{and} \qquad f'(a_{k+1}) \not\equiv 0 \pmod{p^{k+1}}.$$

Our goal is to obtain an integer $a_{k+1} = a_k + tp^k$ for some $0 \leq t < p$. Observe that by Theorem 23.2.3 (Taylor Expansion Theorem for Polynomials), we have the congruence

$$f(a_k + tp^k) \equiv f(a_k) + tp^k f'(a_k) \pmod{p^{k+1}}.$$

Since $f(a_k) \equiv 0 \pmod{p^k}$ and $f'(a_k) \not\equiv 0 \pmod{p^k}$, it follows that there is a unique integer t_0 such that

$$f(a_k) + t_0 p^k f'(a_k) \equiv 0 \pmod{p^{k+1}}.$$

We define $a_{k+1} := a_k + t_0 p^k$. Then we have $f(a_{k+1}) \equiv 0 \pmod{p^{k+1}}$ by definition. Furthermore, we have $a_{k+1} \equiv a_k \equiv a \pmod{p}$. This implies that $f'(a_{k+1}) \equiv f'(a) \not\equiv 0 \pmod{p}$. Therefore it follows that $f'(a_{k+1}) \not\equiv 0 \pmod{p^{k+1}}$, completing the proof. □

23.4 The Elementary Symmetric Polynomials

Using the fact that equivalent reduced polynomials must be congruent, we obtain the following factorization of the polynomial $x^{p-1} - 1$ in $\mathbb{Z}/p\mathbb{Z}$, which has roots at the numbers $1, \ldots, p-1$.

Theorem 23.4.1. *Consider a prime p. Then we have*

$$x^{p-1} - 1 \equiv (x-1)\cdots(x-p+1) \pmod{p}$$

for every x. Hence their coefficients are congruent.

Proof. Both polynomials are equivalent and reduced, so they must be congruent. □

The previous theorem provides another way of proving Theorem 16.3.1 (Wilson's Theorem). This proof is due to Lagrange, who was the first to publish a proof of Wilson's theorem.



PROOF OF THEOREM 16.3.1 (WILSON'S THEOREM). The integer $(p-1)!$ is the constant coefficient of the polynomial $(x-1)\cdots(x-p+1)$, which is congruent to the polynomial $x^{p-1}-1$ with constant coefficient -1. □

Using the elementary symmetric polynomials, we find another way of stating Theorem 23.4.1:

THEOREM 23.4.2. *For each prime p and each $1 \leq k < p-1$ we have*

$$e_k(1,\ldots,p-1) \equiv 0 \pmod{p}.$$

23.5 Reduced Polynomials Modulo a Prime

DEFINITION 23.5.1. Two polynomials $f(x)$ and $g(x)$ are said to be **congruent** modulo a prime p if their coefficients are congruent modulo p.

DEFINITION 23.5.2. Two polynomials $f(x)$ and $g(x)$ are said to be **equivalent** modulo a prime p if for each integer x the polynomial congruence

$$f(x) \equiv g(x) \pmod{p}$$

holds.

DEFINITION 23.5.3. A polynomial $f(x)$ is said to be **reduced** modulo p if it is of degree less than p.

THEOREM 23.5.4. *Any two equivalent reduced polynomials modulo p are congruent.*

PROOF. Consider two equivalent reduced polynomials $f(x)$ and $g(x)$. Then $f(x)-g(x)$ is a reduced polynomial equivalent to 0. However, if $f(x)-g(x)$ were nonzero then its number of roots would be strictly less than p. Since the number of roots is p, it follows that $f(x)-g(x)$ is congruent to the zero polynomial. □

THEOREM 23.5.5. *For every polynomial $f(x)$ there is a unique reduced polynomial $g(x)$ equivalent to $f(x)$.*

Chapter 24

Divisibility and Irreducibility of Polynomials

24.1 Primitive Polynomials and Gauss's Lemma

In Theorem 10.2.1 we showed that unless n is a perfect square, the square root of n is irrational. In other words, the roots of the polynomial

$$x^2 - n$$

are either integers or irrational numbers. Theorem 24.1.3 (Gauss's Lemma for Polynomials) is a generalization of this observation, with the consequence that the roots of a polynomial such as

$$f(x) = x^3 - 3x^2 + 3x - 2$$

are either integers or irrational. The crucial property, besides f having integer coefficients, is that the leading coefficient is 1. Such polynomials are called **monic**. Note that the polynomial $x^2 - n$ of our previous example is also monic.

Before we can proceed to stating and proving Gauss's Lemma, we introduce Gauss's concept of primitive polynomials and prove a key property about them.

Definition 24.1.1. A polynomial $f(x)$ with integer coefficients is said to be **primitive** if the greatest common divisor of its coefficients is 1.

Theorem 24.1.2. *The product of two primitive polynomials is primitive.*



PROOF. Consider two primitive polynomials

$$g(x) := \sum_{i=0}^{m} b_i x^i \qquad \text{and} \qquad h(x) := \sum_{j=0}^{n} c_j x^j,$$

and let $f(x) := g(x)h(x)$ be their product. The coefficients for $f(x)$ are given by

$$a_n := \sum_{k=0}^{n} b_{n-k} c_k.$$

If f is not primitive, then there is a prime p such that $p \mid a_n$ for each coefficient a_n. However, since $g(x)$ and $h(x)$ are primitive, there are least indices i_0 and j_0 such that $p \nmid b_{i_0}$ and $p \nmid c_{j_0}$. Now observe that

$$a_{i_0+j_0} = \sum_{k=0}^{i_0+j_0} b_{i_0+j_0-k} c_k \equiv b_{i_0} c_{j_0} \not\equiv 0 \pmod{p},$$

where the first congruence holds because $p \mid c_k$ for $k < j_0$ and $p \mid b_{i_0+j_0-k}$ for $k > j_0$. This is a contradiction, since we have assumed that $p \mid a_{i_0+j_0}$. We conclude that f is primitive. □

THEOREM 24.1.3 (Gauss's Lemma for Polynomials). *Consider a monic polynomial $f(x)$ with integer coefficients, and let $g(x)$ and $h(x)$ be two polynomials with rational coefficients satisfying the polynomial identity*

$$f(x) = g(x)h(x).$$

Then the coefficients of both $g(x)$ and $h(x)$ are integers.

PROOF. Since $g(x)$ and $h(x)$ are polynomials with rational coefficients, there are least positive integers c and d such that $cg(x)$ and $dh(x)$ are polynomials with integer coefficients. Note that $cg(x)$ and $dh(x)$ are primitive polynomials, hence their product

$$cd\,f(x) = (cg(x))(dh(x))$$

is again primitive. Since the integer cd divides each coefficient of $cd\,f(x)$, it follows that $cd = 1$. We conclude that $c = d = 1$. In other words, $g(x)$ and $h(x)$ had integer coefficients to start with. □

COROLLARY 24.1.4. *Suppose $f(x)$ is a monic polynomial with integer coefficients. Then any rational root r is an integer.*

PROOF. If r is a rational root, then it follows from Theorem 20.2.2 (Factor Theorem) that $f(x)$ factors as

$$f(x) = (x - r)g(x),$$

where $g(x)$ is a polynomial with rational coefficients. By Theorem 24.1.3 (Gauss's Lemma for Polynomials) it follows that $x - r$ is a polynomial with integer coefficients; that is, r is an integer. □

24.2 Euclid's Algorithm for Polynomials

Example 24.2.1. Consider the polynomials $f(x) = x^4 + x^2 + 1$ and $g(x) = x^2 + x + 1$. We can apply the ideas behind Theorem 5.3.1 (The Euclidean Division Theorem) to divide out $g(x)$ from $f(x)$ as best we can. To do this, we first write

$$x^4 + x^2 + 1 = x^2(x^2 + x + 1) - x^3 + 1.$$

In the same manner, we can divide out $x^2 + x + 1$ from $-x^3 + 1$:

$$-x^3 + 1 = -x(x^2 + x + 1) + x^2 + x + 1.$$

Finally, we note that the remainder $x^2 + x + 1$ is equal to $g(x)$. For completeness sake, we write the final step:

$$x^2 + x + 1 = 1(x^2 + x + 1) + 0.$$

Having reached 0, the process terminates here. As a parenthetical remark, we note that the process could also have terminated by reaching in the remainder a polynomial of strictly smaller degree than the degree of $g(x)$. Combining the previous calculations, we obtain the polynomial identity

$$x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1).$$

The process we have exhibited here is called **Euclidean division** or **long division** for polynomials.

Definition 24.2.2. We say that a polynomial $g(x)$ **divides** a polynomial $f(x)$ if there is a polynomial $h(x)$ such that

$$f(x) = g(x)h(x).$$

Theorem 24.2.3 (Euclidean Division for Polynomials). *Consider two polynomials $f(x)$ and $g(x)$ with coefficients in an integral domain, and assume that $g(x)$ is a monic polynomial of degree m. Then we can determine unique polynomials $q(x)$ and $r(x)$ satisfying the polynomial identity*

$$f(x) = q(x)g(x) + r(x),$$

such that $\deg(r(x)) < m$.

Proof. The proof is by induction on the degree of $f(x)$. If $\deg(f(x)) < m$, then we simply choose $q(x) = 0$ and $r(x) = f(x)$. These choices are forced, since the degree of any nonzero multiple of $g(x)$ is at least the degree of $g(x)$.

Now suppose that the claim holds for any polynomial of degree $< m + n$, and let $f(x)$ be of degree $m + n$ with leading coefficient a. Then

$$h(x) = f(x) - ax^n g(x)$$



has degree $< m+n$. Consequently, there are unique polynomials $q(x)$ and $r(x)$ of degree $< m$ satisfying the polynomial identity

$$h(x) = q(x)g(x) + r(x).$$

It follows that

$$f(x) = (ax^n + q(x))g(x) + r(x).$$

It remains to show that this choice of polynomials is uniquely determined. Let $p(x)$ and $s(x)$ be polynomials with $\deg(s(x)) < m$ satisfying the polynomial identity $f(x) = p(x)g(x) + s(x)$. Let b be the leading coefficient of $p(x)$. Since $g(x)$ was assumed to be monic, it follows that b is then the leading coefficient of $p(x)g(x)$. Moreover, since $\deg(s(x)) < m$ we see that the leading coefficient of $p(x)g(x)+s(x)$ is b, so we conclude that $a = b$. It also follows by these same considerations that $\deg(p(x)) = n$. Now we see that

$$(p(x) - ax^n)g(x) + s(x) = f(x) - ax^n g(x) = h(x) = q(x)g(x) + r(x).$$

This shows that $s(x) = r(x)$ and $ax^n + q(x) = p(x)$, completing the proof of uniqueness. □

24.3 Irreducible Polynomials

DEFINITION 24.3.1. A polynomial $f(x)$ with coefficients in R is said to be **irreducible** if it cannot be written in the form

$$f(x) = g(x)h(x)$$

where neither $g(x)$ nor $h(x)$ are constant at an invertible element of R.

Theorem 24.1.3 (Gauss's Lemma for Polynomials) can be stated in the form of an irreducibility criterion:

COROLLARY 24.3.2. *Consider a monic polynomial $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is irreducible as a polynomial with integer coefficients, then it is also irreducible as a polynomial with rational coefficients.*

COROLLARY 24.3.3. *Consider a primitive polynomial $f(x)$ with integer coefficients, and consider a prime p such that the leading coefficient of $f(x)$ is not divisible by p. Let $\bar{f}(x) \in (\mathbb{Z}/p)[x]$ be the reduction of $f(x)$ to $\mathbb{Z}/p$. If $\bar{f}(x)$ is irreducible in $(\mathbb{Z}/p)[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

EXAMPLE 24.3.4. Consider the polynomial $f(x) = x^2 - x + 1$. This is a quadratic polynomial, so it is only reducible in $\mathbb{Q}[x]$ if it has rational roots. Note that any root would have to be a root modulo 5 as well. However, a quick calculation shows that $f(a) \not\equiv 0 \pmod 5$ for each integer $0 \leq a < 5$. Therefore, it follows that $f(x)$ is irreducible modulo 5, and this is sufficient to conclude that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example 24.3.5. Our next example is due to Georg Pólya, who showed that the polynomial

$$P_n(x) := (x+1)\cdots(x+n)+1$$

is irreducible in $\mathbb{Z}[x]$ for all $n \neq 4$ [Pól1919]. In the case $n = 4$ we have the factorization

$$(x+1)(x+2)(x+3)(x+4)+1 = (x^2+5x+5)^2.$$

Knowing that the polynomial $P_n(x)$ is irreducible for $n \neq 4$ is consistent with the conjecture that infinitely many numbers of the form $n!+1$ are prime. Primes of the form $n! \pm 1$ are called **factorial primes**. Even though it is still a long way to proving the conjecture, Pólya's observation rules out the simplest algebraic obstruction: The number $P_n(0) = n!+1$ is not automatically composite for purely polynomial reasons.

Note that a polynomial $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if every translation $f(x+a)$ is also irreducible. In other words, translations have no effect on the irreducibility of a polynomial. We use this to bring Pólya's polynomial to slightly more convenient form. We define

$$H_n(x) := (x-1)\cdots(x-n)+1,$$

so that $P_n(x) = H_n(x+n+1)$.

Suppose that $H_n(x) = f(x)g(x)$ for two integer polynomials $f(x)$ and $g(x)$ of degree ≥ 1. Since $H_n(k) = 1$ for every $1 \leq k \leq n$, it follows that

$$f(k)g(k) = 1$$

for every $1 \leq k \leq n$. This implies that either $f(k) = 1$ and $g(k) = 1$, or $f(k) = -1$ and $g(k) = -1$. In particular, we find that $f(k) = g(k)$ for each $1 \leq k \leq n$. Since $\deg(f), \deg(g) < n$, we conclude by Theorem 20.4.2 (Lagrange's Interpolation Theorem) that the polynomial identity $f(x) = g(x)$ holds. Therefore, it follows that

$$H_n(x) = f(x)^2,$$

and $n = 2m$, where m is the degree of f.

Now define the sets

$$I := \{1 \leq k \leq 2m \mid f(k) = 1\} \qquad \text{and} \qquad J := \{1 \leq k \leq 2m \mid f(k) = -1\}.$$

Note that I consists of the integer roots of $f(x)-1$, and J consists of the integer roots of $f(x)+1$. In particular, since the degree of $f(x)$ is m, it follows that $|I| \leq m$ and $|J| \leq m$. On the other hand, the union $I \cup J$ consists of all the numbers $1, \ldots, 2m$, so that $|I| + |J| = 2m$. This allows us to conclude that both I and J consist of exactly m elements, that I consists of all the roots of $f(x)-1$, and that J consists of all the roots of $f(x)+1$. Consequently, we have the polynomial identities

$$f(x)-1 = \prod_{i \in I}(x-i) \qquad \text{and} \qquad f(x)+1 = \prod_{j \in J}(x-j).$$

It follows that for each $i_0 \in I$, we have

$$\prod_{j \in J}(i_0 - j) = \prod_{j \in J}(i_0 - j) - \prod_{i \in I}(i_0 - i) = 2.$$

This integer factorization of 2 shows that the distance $|i_0 - j| \leq 2$ for every integer $j \in J$. Now observe that when J contains at least three integers, then there is at most one integer distinct from all the integers in J such that $|x - j| \leq 2$ for all $j \in J$. However, since I and J contain the same number of elements, this shows that J cannot contain 3 or more integers. We conclude that $m \leq 2$.

We have shown so far that if $P_n(x)$ factors as a product of two polynomials, then $n = 2m$ for $1 \leq m \leq 2$. To finish the proof of Pólya's claim, it remains to show that $P_2(x)$ is irreducible. Reducing Pólya's polynomial $P_2(x)$ modulo 2 gives

$$(x+1)(x+2)+1 \equiv x^2 + x + 1 \pmod{2}.$$

Since quadratic polynomials are only reducible if they have roots, and this polynomial has no roots modulo 2, this immediately implies that $P_2(x)$ cannot have roots and is therefore irreducible.

24.4 Eisenstein's Criterion

THEOREM 24.4.1 (Eisenstein's Criterion). *Consider a polynomial $f(x) = a_n x^n + \cdots + a_0$ with integer coefficients. Suppose that there is a prime number p such that:*

(i) *The prime p is a prime divisor of a_i for every $0 \leq i < n$,*

(ii) *The coefficient a_n is not divisible by p,*

(iii) *The coefficient a_0 is not divisible by p^2.*

Then the polynomial f is irreducible in $\mathbb{Q}[x]$.

PROOF. First, we note that $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $\lambda f(x)$ is irreducible in $\mathbb{Q}[x]$, for any nonzero rational number λ. Taking $d := \gcd(a_0, \ldots, a_n)$ and $\lambda := 1/d$, then the polynomial $\lambda f(x)$ is primitive. Furthermore, $\lambda f(x)$ still satisfies the conditions of Eisenstein's criterion, since $p \nmid d$. Thus, we may assume that $f(x)$ is primitive. By Theorem 24.1.3 (Gauss's Lemma for Polynomials) it suffices to show that $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Suppose that $f(x)$ is reducible in $\mathbb{Z}[x]$, so that $f(x) = g(x)h(x)$ for two polynomials

$$g(x) = b_r x^r + \cdots + b_0 \qquad \text{and} \qquad h(x) = c_s x^s + \cdots + c_0$$

with integer coefficients, where r and s are positive integers such that $r + s = n$. Then we have

$$a_i = \sum_{\substack{j,k \\ i=j+k}} b_j c_k.$$

Since $a_0 = b_0c_0$ is divisible by p but not by p^2, it follows that exactly one of b_0 and c_0 is divisible by p. We will assume without loss of generality that p divides b_0. We claim that every coefficient of $g(x)$ is divisible by p. Using the identity

$$a_i = \sum_{\substack{j,k \\ i=j+k}} b_j c_k = (b_0c_j + \cdots + b_{i-1}c_1) + b_ic_0,$$

this claim follows by induction. Indeed, if $p \mid b_j$ for each $j < i$ and $p \mid a_i$, then we must have $p \mid b_ic_0$. Since we assumed that $p \nmid c_0$, we must have $p \mid b_i$.

However, it follows that $a_n = b_rc_s$ is divisible by p, which is in contradiction with the assumption that $p \nmid a_n$. □

Example 24.4.2. Consider two distinct integers a and b. We claim that the polynomial

$$f(x) = (x+a)^n - (x+b)^n$$

is irreducible if and only if n is prime.

If n is composite, say $n = km$, then we can factor $f(x)$ using the formula for the difference of mth powers:

$$f(x) = ((x+a)^k - (x+b)^k) \sum_{i=0}^{m-1} (x+a)^i (x+b)^{m-1-i}.$$

This shows that for composite n, the polynomial $f(x)$ is reducible.

It remains to show that $f(x)$ is irreducible if $n = p$, where p is prime. To see this, consider $c = a - b$ and the polynomial

$$g(x) = (x+c)^p - x^p.$$

Then we have $f(x) = g(x+b)$, so it follows that $f(x)$ is irreducible if and only if $g(x)$ is. Furthermore, we observe that rescaling also doesn't affect irreducibility in $\mathbb{Q}[x]$: A polynomial $F(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if the polynomial $F(qx)$ is irreducible, where q is a nonzero rational number. Note that

$$g(x) = c^p((x/c)+1)^p - (x/c)^p.$$

It follows that $g(x)$ is irreducible if and only if the polynomial

$$h(x) = (x+1)^p - x^p$$

is irreducible. Thus, it remains to show that the polynomial $h(x)$ is irreducible.

Example 24.4.3. For every prime p, the polynomial

$$f(x) := 1 + x + x^2 + \cdots x^{p-1}$$



is irreducible. Indeed, if we substitute $x = y + 1$ in

$$f(x) = \frac{x^p - 1}{x - 1},$$

we obtain

$$f(y+1) = \frac{(y+1)^p - 1}{y} = \sum_{i=0}^{p-1} \binom{p}{i+1} y^i.$$

This polynomial has coefficients $a_i = \binom{p}{i+1}$. Thus we see that

(i) The binomial coefficient $\binom{p}{i+1}$ is divisible by p for every $0 \leq i < p - 1$.

(ii) The binomial coefficient $\binom{p}{p} = 1$ is not divisible by p.

(iii) The binomial coefficient $\binom{p}{1} = p$ is not divisible by p^2.

Thus it follows from Eisenstein's criterion that $f(y + 1)$ is irreducible, which implies that $f(x)$ is irreducible.

EXAMPLE 24.4.4.

(i) Consider a prime p and an even integer $2 \leq n < p - 1$ such that $p \nmid B_n$. Then the polynomial

$$(x+1)^n + \cdots + (x+p-1)^n$$

is irreducible over $\mathbb{Q}$.

(ii) Show that the polynomial

$$x^6 + 3x^5 + 6x^4 + 9x^3 + 6x^2 + 3x^1 + 1$$

is irreducible over $\mathbb{Q}$.

(iii) Show that the polynomial

$$\frac{(x+2)^n - x^n - 2^n}{x}$$

is irreducible over $\mathbb{Q}$.

Exercises

Starter Exercises

24.1 Show that the following polynomials are irreducible in $\mathbb{Q}[x]$:

(a) $x^2 - x + 3$,
(b) $x^2 + 2x + 3$,
(c) $x^3 - x + 1$,
(d) $x^3 + 2x + 2$,
(e) $x^4 + 3x + 3$.

Routine-Building Exercises

24.2 Suppose that $f(x)$ is an irreducible polynomial of degree n, and consider a, b, c, d with $ad - bc \neq 0$. Show that the polynomial

$$g(x) = (cx + d)^n f\left(\frac{ax + b}{cx + d}\right)$$

is again irreducible.



Chapter 25

Cyclotomic Polynomials

25.1 The Primitive Factors of $x^n - 1$

Consider a prime factor p of $a^n - 1$. Since $p \mid a^n - 1$, it follows that $a^n \equiv 1 \pmod{p}$. By the Theorem 8.5.2 (Order Theorem) it follows that $\mathrm{ord}_p(a) \mid n$. By Theorem 16.1.1 (Fermat's Little Theorem) it follows that the order of a modulo p is itself a divisor of $p - 1$.

Definition 25.1.1. The nth **cyclotomic polynomial** Φ_n is defined by

$$\Phi_n(x) := \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - e^{2\pi i k/n}).$$

Example 25.1.2. Another way of expressing the defining identity of the cyclotomic polynomial $\Phi_{pq}(x)$ is

$$x^{pq} - 1 = \frac{(x^p - 1)(x^q - 1)}{x - 1} \Phi_{pq}(x).$$

In other words, $\Phi_{pq}(x)$ can be expressed as the following fraction of polynomials:

$$\frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)} = \Phi_{pq}(x).$$

The idea is now to write $(x^{pq} - 1)(x - 1)$ as a combination of polynomials of the form $(x^{up} - 1)(x^{vq} - 1)$. Note first that p is invertible modulo q and q is invertible modulo



p. Thus, there are integers $0 \leq s < q$ and $0 \leq t < p$ such that $sp \equiv 1 \pmod{q}$ and $tq \equiv 1 \pmod{p}$. Combining these congruences, we obtain

$$sp + tq \equiv 1 \pmod{pq}.$$

Moreover, we have $0 \leq sp + tq < pq + pq$, so that in fact the identity

$$sp + tq = pq + 1$$

holds. With this choice of s and t, we calculate

$$\begin{aligned}(x^{pq}-1)(x-1) - (x^{sp}-1)(x^{tq}-1) &= x^{pq+1} - x^{pq} - x + 1 - x^{sp+tq} + x^{sp} + x^{tq} - 1 \\ &= -x(x^{pq-1} - x^{sp-1} - x^{tq-1} + 1) \\ &= -x(x^{sp-1}-1)(x^{tq-1}-1) \\ &= -x(x^{(q-s)p}-1)(x^{(p-t)q}-1).\end{aligned}$$

This shows that

$$(x^{pq}-1)(x-1) = (x^{sp}-1)(x^{tq}-1) - x(x^{(q-s)p}-1)(x^{(p-t)q}-1).$$

This shows that

$$\Phi_{pq}(x) = \frac{(x^{sp}-1)(x^{tq}-1)}{(x^p-1)(x^q-1)} - x\frac{(x^{(q-s)p}-1)(x^{(p-t)q}-1)}{(x^p-1)(x^q-1)}.$$

In other words, we find that

$$\Phi_{pq}(x) = \left(\sum_{i=0}^{s-1} x^{ip}\right)\left(\sum_{j=0}^{t-1} x^{jq}\right) - x\left(\sum_{i=0}^{q-s-1} x^{ip}\right)\left(\sum_{j=0}^{p-t-1} x^{jq}\right).$$

THEOREM 25.1.3. *For any natural number n we have the identity*

$$\Phi_n(x) = \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x).$$

THEOREM 25.1.4. *The cyclotomic polynomials $\Phi_n(x)$ have integer coefficients*

In the following theorem we will establish that the coefficients of the cyclotomic polynomials are palindromic, meaning that they read the same forward and back.

THEOREM 25.1.5. *The cyclotomic polynomials $\Phi_n(x)$ are **reciprocal** in the sense that*

$$\Phi_n\left(\tfrac{1}{x}\right) x^{\phi(n)} = \Phi_n(x).$$

Theorem 25.1.6. *Consider a cyclotomic polynomial $\Phi_n(x)$ and a prime p. Then we have*

$$\Phi_n(x) \equiv 0 \pmod{p} \text{ is solvable} \quad \Leftrightarrow \quad n \mid p-1.$$

Furthermore, if $\Phi_n(x) \equiv 0 \pmod{p}$ is solvable, then $\Phi_n(x)$ has exactly $\phi(n)$ roots modulo p.

Definition 25.1.7. We define

$$\Phi_n(x,y) := y^{\phi(n)}\Phi_n\left(\frac{x}{y}\right).$$

Proposition 25.1.8. *For any x, y, and n, we have:*

$$x^n - y^n = \prod_{d \mid n} \Phi_d(x,y).$$

Lemma 25.1.9. *Consider integers a, b, and c, and a prime p such that $p \nmid ab$ and $c \equiv a/b \pmod{p}$. If $\operatorname{ord}_p(c) = k$, then*

$$\Phi_k(c) \equiv 0 \pmod{p} \quad \Leftrightarrow \quad p \mid \Phi_k(a,b)$$

Lemma 25.1.10. *If $p \nmid m$, then $\Phi_m(x^p) = \Phi_{mp}(x)\Phi_m(x)$.*

Lemma 25.1.11. *Consider a prime p, and let $n = p^\alpha m$, where $\alpha \geq 1$ and $p \nmid m$. Then we have*

$$\Phi_n(x) \equiv \Phi_m(x)^{\phi(p^\alpha)} \pmod{p}.$$

Consequently, if $p \mid \Phi_n(a,b)$ then $p \mid \Phi_m(a,b)$.

Proposition 25.1.12. *Consider a prime $p \nmid n$. Then*

$$\operatorname{ord}_p(a) = n \quad \Leftrightarrow \quad p \mid \Phi_n(a)$$

Recall from Theorem 19.5.2 (Lifting the Exponent) that for any odd prime p and any $n = p^\alpha m$ with $p \nmid m$, we have

$$v_p(a^n - b^n) - v_p(a^m - b^m) = \alpha.$$

Since we have expressed $a^n - b^n$ as a product in terms of the homogenized cyclotomic polynomials $\Phi_n(a,b)$, we can thus compute the p-adic valuation of $\Phi_n(a,b)$.

Proposition 25.1.13. *Consider an odd prime p such that $p \nmid ab$. Let $k = \rho(p)$ be the rank of apparition of p in $(a^n - b^n)$. Then we have*

$$v_p(\Phi_n(a,b)) = \begin{cases} v_p(a^k - b^k) & \text{if } n = k, \\ 1 & \text{if } n = p^\alpha k \text{ for some } \alpha \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. □

25.2 The Möbius Inversion Formula for the Cyclotomic Polynomials

THEOREM 25.2.1. *For any n, we have the identity*

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

EXAMPLE 25.2.2. Theorem 25.2.1 can be used effectively to compute the coefficients of a cyclotomic polynomial. For example, in order to compute $\Phi_{12}(x)$, we note that the values $\mu(12/d)$ of the Möbius function are as follows:

$$\mu(12/1) = 0,\ \mu(12/2) = 1,\ \mu(12/3) = 0,\ \mu(12/4) = -1,\ \mu(12/6) = -1,\ \mu(12/12) = 1.$$

This shows that

$$\Phi_{12}(x) = (x^2 - 1)(x^4 - 1)^{-1}(x^6 - 1)^{-1}(x^{12} - 1) = x^4 - x^2 + 1.$$

25.3 Irreducibility of the Cyclotomic Polynomials

DEFINITION 25.3.1. We say that a polynomial $f(x)$ is **square-free** if $r(x)^2 \mid x^n - 1$ implies that $r(x)$ is constant, for every polynomial $r(x)$. Furthermore, we say that $f(x)$ is **square-free modulo** p if $r(x)^2 \mid x^n - 1 \pmod{p}$ implies that $r(x)$ is constant modulo p, for every polynomial $r(x)$.

The polynomial $x^n - 1$ is square-free in the ordinary sense, since it does not have repeated roots. In the following lemma we will prove the stronger property that $x^n - 1$ is square-free modulo primes p not dividing n.

LEMMA 25.3.2. *The polynomial $x^n - 1$ is square-free modulo p for every prime $p \nmid n$.*

PROOF. It suffices that there cannot be an irreducible polynomial $r(x)$ such that

$$x^n - 1 = r(x)^2 s(x) \pmod{p}.$$

By taking derivatives, we see that

$$nx^{n-1} = 2r(x)r'(x)s(x) + r(x)^2 s(x) \pmod{p}.$$

In particular, we see that $r(x) \mid nx^{n-1}$ in $\mathbb{F}_p[x]$. By the assumption that $p \nmid n$ it follows that n is invertible, and hence we obtain

$$r(x) \mid x^{n-1}.$$

Since $r(x)$ is assumed to be irreducible, it follows that $r(x) \mid x$. That is, $x \mid r(x)$. This leads to a contradiction, however, since

$$x \nmid x^n - 1.$$

□

Theorem 25.3.3. *The nth cyclotomic polynomial $\Phi_n(x)$ is irreducible for every $n \geq 1$.*

Proof. Let $\zeta = e^{2\pi i/n}$. We claim that if $f(x)$ is an irreducible polynomial such that $f(\zeta) = 0$, then $f(\zeta^a) = 0$ for every integer a coprime to n. To prove this claim, it suffices to show that $f(\zeta^p) = 0$ for every prime $p \nmid n$.

We observe first that ζ^p is a primitive root of unity, since $(\zeta^p)^m = 1$ implies $n \mid pm$, which implies $n \mid m$ since $p \nmid n$. Now, since we have assumed that $f(\zeta) = 0$ it follows that

$$\Phi_n(x) = f(x)g(x).$$

Therefore, if $f(\zeta^p) \neq 0$, it follows that $g(\zeta^p) = 0$. This shows that ζ is a root of the polynomial $g(x^p)$. Since $f(x)$ is an irreducible polynomial with root ζ, it follows that $f(x) \mid g(x^p)$.

As a consequence of the fact that ζ^a is a root of every irreducible polynomial $f(x)$ such that $f(\zeta) = 0$, for every integer a relatively prime to n, every such polynomial is of degree $\varphi(n)$. It follows that the polynomial $\Phi_n(x)$ is of minimal degree such that $\Phi_n(\zeta) = 0$, and therefore must be irreducible. □

25.4 Zsigmondy's Theorem

Definition 25.4.1. Consider a sequence (a_n) of integers. A prime p is said to be a **primitive prime divisor** of a_n if the rank of apparition of p satisfies $\rho(p) = n$.

Proposition 25.4.2. *Consider two relatively prime integers a and b, and a prime p such that $p \mid \Phi_n(a, b)$, where $n \geq 1$. Then there are two mutually exclusive possibilities:*

(i) *Either $p \equiv 1 \pmod{n}$, in which case p is a primitive prime divisor of $a^n - b^n$, or*

(ii) *$p \mid n$, in which case p is the largest prime factor of n, and provided that $n > 2$ we have furthermore $p^2 \nmid \Phi_n(a, b)$.*

Proof. Since $a^n - b^n = \prod_{d \mid n} \Phi_d(a, b)$, it follows that $a^n \equiv b^n \pmod{p}$. Furthermore a and b are assumed to be relatively prime, the congruence $a^n \equiv b^n \pmod{p}$ implies that neither a nor b is divisible by p. We find that

$$(a/b)^n \equiv 1 \pmod{p},$$

and hence $k := \operatorname{ord}_p(a/b)$ is a divisor of n by Theorem 8.5.2 (Order Theorem). There are two cases to consider: Either $k = n$ or k is a proper divisor of n.

If $k = n$, then it follows by Theorem 16.1.1 (Fermat's Little Theorem) that $n \mid p - 1$, which is another way of saying that $p \equiv 1 \pmod{n}$. Since $k \mid m$ for any m such that $p \mid a^m - b^m$, it follows that p is a primitive divisor of $a^n - b^n$.

For the second case, suppose that k is a proper divisor of n. Since $p \mid \Phi_k(a, b)$ and $p \mid \Phi_n(a, b)$ both hold, it follows that the polynomial congruence

$$x^n - 1 \pmod{p}$$



has roots of multiplicity > 1. It follows that

$$\gcd(x^n - 1, nx^{n-1}) \neq 1,$$

from which we conclude that $p \mid n$.

To show that p is the largest prime factor of n, write $n = p^\alpha m$, where $p \nmid m$. By the implication

$$p \mid \Phi_n(a,b) \Rightarrow p \mid \Phi_m(a,b)$$

it follows that $p \mid \Phi_m(a,b)$. However, since $p \nmid m$ this brings us back to the first case with the exponent m, so we conclude that $m \mid p-1$. In particular, any prime divisor of m is a prime divisor of $p-1$, which implies that p must have been the largest prime divisor of n.

Finally, we have to show that $v_p(\Phi_n(a,b)) = 1$. We consider two cases: Either $p = 2$ or p is odd. If $p = 2$, write $n = 2^\alpha m$. As before, it follows that $m \mid p-1$, so we have $m = 1$ and $n = 2^\alpha$. By the assumption that $n > 2$ it follows that $\alpha \geq 2$. Since a and b are both odd, it follows that

$$\Phi_n(a,b) = a^{2^{\alpha-1}} + b^{2^{\alpha-1}} \equiv 2 \pmod 4,$$

from which we conclude that $v_2(\Phi_n(a,b)) = 1$.

For the case where p is odd, write $n = p^\alpha m$ as before. Then we obtain from Theorem 19.5.2 (Lifting the Exponent) that

$$v_p(a^n - b^n) - v_p(a^m - b^m) = \alpha.$$

The right-hand side can be evaluated using the formula $a^n - b^n = \prod_{d \mid n} \Phi_d(a,b)$. Note that for any divisor d of n, we have $p \mid \Phi_d(a,b)$ if and only if $d = p^i m$ for some $0 \leq i \leq \alpha$. Thus we obtain:

$$\sum_{i=1}^{\alpha} v_p(\Phi_{p^i m}(a,b)) = \alpha.$$

Since $p \mid \Phi_{p^i m}(a,b)$, this implies that

$$v_p(\Phi_{p^i m}(a,b)) = 1$$

for every $1 \leq i \leq \alpha$. The case $i = \alpha$ proves the claim. □

THEOREM 25.4.3 (Zsigmondy's Theorem). *Consider two integers $1 \leq b < a$ with $\gcd(a,b) = 1$ and let $n \geq 1$. Then the number $a^n - b^n$ has a primitive prime divisor, except in the following three cases:*

(i) *$n = 1$ and $a - b = 1$,*

(ii) *$n = 2$ and $a + b$ is a power of 2,*

(iii) *$n = 6$, $a = 2$, and $b = 1$.*

Proof. In order to dispose of the first case, note that if $n = 1$, then any prime divisor of $a - b$ is primitive. Thus, the only case where $a - b$ does not have primitive prime divisors is when $a - b = 1$.

Next, we deal with the case $n = 2$. Suppose that $a^2 - b^2$ does not have primitive prime divisors. An equivalent way of saying this is that any prime divisor $p \mid \Phi_2(a, b) = a + b$ is also a prime divisor of $a - b$. However, we observe that $\gcd(a + b, a - b)$ divides both $2a$ and $2b$, which implies that the only prime possible prime divisor of $a + b$ is 2. In other words, $a + b$ is a power of 2.

For the remainder of the proof we suppose that $n > 2$. We will show that if $a^n - b^n$ has no primitive prime divisors, then $n = 6$, $a = 2$, and $b = 1$. By Proposition 25.4.2 it follows that if $a^n - b^n$ has no primitive prime divisors, then

$$\Phi_n(a, b) = p,$$

where p is the largest prime divisor of n and moreover p is odd. Write $n = p^\alpha m$, where $p \nmid m$.

We claim that $m = 1$ is impossible. To see this, note that

$$\Phi_{p^\alpha}(a, b) = \frac{a^{p^\alpha} - b^{p^\alpha}}{a^{p^{\alpha-1}} - b^{p^{\alpha-1}}} = a^{p^{\alpha-1}(p-1)} + \cdots + b^{p^{\alpha-1}(p-1)}.$$

It follows immediately from this description that $\Phi_{p^\alpha}(a, b) > p$, which contradicts the fact that $\Phi_n(a, b) = p$.

Next, we claim that $m \geq 3$ is impossible, so that only the case $m = 2$ remains. Suppose to the contrary that $m \geq 3$, and define $A := a^{p^{\alpha-1}}$ and $B := b^{p^{\alpha-1}}$, so that $\Phi_n(a, b) = \Phi_{pm}(A, B)$. Since $p \nmid m$, we have the identity

$$\Phi_{pm}(A, B) = \frac{\Phi_m(A^p, B^p)}{\Phi_m(A, B)}.$$

We estimate the magnitude of the numerator and denominator separately. Recall that $\Phi_m(x, y) = \prod(x - \zeta y)$ where the product runs over the numbers of the form $\zeta = e^{2\pi i k/n}$ where $\gcd(k, m) = 1$. Since $m \geq 3$, we note that $\zeta \neq 1$ for every such k. Thus, for every such ζ, we have the strict inequalities $|A^p - \zeta B^p| > A^p - B^p$ and $|A - \zeta B| < A + B$. It follows that

$$\Phi_{pm}(A, B) > \frac{(A^p - B^p)^{\phi(m)}}{(A + B)^{\phi(m)}} = \left(\frac{A^p - B^p}{A + B}\right)^{\phi(m)}.$$

Since $a > b \geq 1$, we have $A \geq 2$ and $B \geq 1$. Furthermore, p is the largest prime factor of n, so p is odd, implying $p \geq 3$. The function $f(x) = (x^p - 1)/(x + 1)$ is increasing for $x \geq 2$, so the term in the parentheses is at least $(2^p - 1)/3$. Combining this with the fact that $\phi(m) \geq 2$ for $m \geq 3$, we obtain

$$\Phi_{pm}(A, B) > \left(\frac{2^p - 1}{3}\right)^2.$$



For $p = 3$, the right-hand side is $(7/3)^2 > 5 > p$. For $p \geq 5$, the inequality holds even more strongly. In all cases we have $\Phi_n(a, b) > p$, which is a contradiction.

By the previous eliminations, we conclude that $m = 2$; that is, $n = 2p^\alpha$. It follows that

$$p = \Phi_{2p^\alpha}(a, b) = \frac{A^p + B^p}{A + B}.$$

Note that $p(A + B) = A^p + B^p \geq 2(\frac{A+B}{2})^p = \frac{(A+B)^p}{2^{p-1}}$, from which we obtain

$$\left(\frac{3}{2}\right)^{p-1} \leq \left(\frac{A+B}{2}\right)^{p-1} \leq p.$$

Since this inequality fails for $p \geq 4$, it follows that $p = 3$. We find that

$$\left(\frac{A+B}{2}\right)^2 \leq 3,$$

which implies that $(A + B)^2 \leq 12$, and consequently $A + B \leq 3$. It follows that $a^{p^{\alpha-1}} = A = 2$ and $B = 1$, which gives us that $\alpha = 1$, so that $n = 6$, $a = 2$, and $b = 1$. □

25.5 The Infinitude of Primes Congruent to 1 Modulo n

THEOREM 25.5.1. *For each $n \geq 1$, there are infinitely many primes $p \equiv 1 \pmod{n}$.*

PROOF. The statement is self-evident for $n \leq 2$, so we will assume that $n > 2$. Consider a finite set $p_1, \ldots, p_k$ of distinct primes such that

$$p_i \equiv 1 \pmod{n}$$

for each $1 \leq i \leq k$, let $a := n \cdot p_1 \cdots p_k$, and define

$$N := \Phi_n(a).$$

Observe that the number N has at least one prime factor. Indeed, this follows directly from Theorem 25.4.3 (Zsigmondy's Theorem), since $n, a \geq 3$.

We claim that any prime factor $q \mid N$ satisfies $q \equiv 1 \pmod{n}$ and is distinct from the primes p_i. Since the constant term of $\Phi_n(x)$ is 1, it follows that $N \equiv 1 \pmod{p_i}$. This immediately implies that $q \neq p_i$ for each $1 \leq i \leq k$. We also observe that the congruence $N \equiv 1 \pmod{n}$ holds, for the same reason. This shows that any prime factor $q \mid N$ is of the first kind in Proposition 25.4.2, which shows that $q \equiv 1 \pmod{n}$. □

25.6 Vantieghem's Theorem

Emmanuel Vantieghem provided a characterization of the prime numbers in terms of the Mersenne numbers [Van1991]. More precisely, he showed that a natural number $n \geq 3$ is prime if and only if

$$\prod_{k=1}^{n-1} M_k \equiv n \pmod{M_n}.$$

Recall that the nth Mersenne number is given by $M_n := 2^n - 1$. The sequence (M_n) of Mersenne numbers is a strong divisibility sequence. There are some analogies between Vantieghem's theorem and Theorem 16.3.1 (Wilson's Theorem). In Wilson's theorem, we make use of the congruence

$$x^p \equiv x \pmod{p},$$

which holds by Theorem 16.1.1 (Fermat's Little Theorem). For instance, in the second proof of Wilson's theorem, this congruence was used to observe that

$$\prod_{k=0}^{p-1}(x-k) \equiv x^p - x \pmod{p}.$$

Similarly, in the proof of Vantieghem's theorem, we will use the congruence $2^p \equiv 1 \pmod{M_p}$ to observe that

$$\prod_{k=1}^{p-1}(x-2^k) \equiv x^p - 1 \pmod{M_p}.$$

We will prove this congruence in the following proposition.

Proposition 25.6.1. *Consider the monic polynomial*

$$f(x) = \prod_{k=0}^{p-1}(x-2^k)$$

Then we have $f(x) \equiv x^p - 1 \pmod{M_p}$.

Proof. To start the proof, we first note that

$$f(0) \equiv \prod_{k=0}^{p-1}(0-2^k) \equiv -2^{\frac{p(p-1)}{2}} \equiv -1 \pmod{M_p}.$$

This shows that the constant term of $f(x)$ is indeed congruent to -1 modulo M_p. Since $f(x)$ is a monic polynomial, it therefore suffices to show that its coefficients of degree $0 < k < p$ are all 0.



To see this, we first claim that $f(2x) \equiv f(x) \pmod{M_p}$. Indeed, using that $2^p \equiv 1 \pmod{M_p}$, which implies that $2^{-1} \equiv 2^{p-1} \pmod{M_p}$, we see that

$$f(2x) = \prod_{k=0}^{p-1}(2x - 2^k) = (2x-1)2^{p-1}\prod_{k=1}^{p-1}(x - 2^{k-1}) \equiv \prod_{k=0}^{p-1}(x-2^k) \pmod{M_p}.$$

Writing $f = a_p x^p + \cdots + a_0$, it follows that

$$0 \equiv f(2x) - f(x) \equiv \sum_{k=0}^{p} a_k(2^k - 1)x^k \pmod{M_p}.$$

Since $2^k \equiv 1 \pmod{M_p}$ implies $p \mid k$, it follows that $a_k \equiv 0 \pmod{M_p}$ for $0 < k < p$, which completes the proof. □

Recall from the second proof of Theorem 16.3.1 (Wilson's Theorem), that after having established that $\prod_k (x-k) \equiv x^p - x \pmod{p}$, we proceeded by taking derivatives on both sides. This strategy again works in the proof of the forward direction of Vantieghem's theorem. For the converse direction, we will make use of Theorem 25.4.3 (Zsigmondy's Theorem).

THEOREM 25.6.2 (Vantieghem's Theorem). *A natural number $n \geq 3$ is prime if and only if*

$$\prod_{k=1}^{n-1} M_k \equiv n \pmod{M_n}$$

PROOF. First, suppose that $n = p$, where p is a prime. Consider the polynomial

$$f(x) = \prod_{k=0}^{p-1}(x - 2^k)$$

which satisfies the congruence $f(x) \equiv x^p - 1 \pmod{M_p}$ by Proposition 25.6.1. It follows that $f'(1) \equiv p \pmod{M_p}$. On the other hand, writing $f(x) = (x-1)g(x)$, where $g(x) = \prod_{k=1}^{p-1}(x-2^k)$, we find that $f'(x) = (x-1)g'(x) + g(x)$. Evaluating at 1 gives taht

$$\prod_{k=1}^{p-1}(1-2^k) = g(1) = f'(1) \equiv p \pmod{M_p}.$$

Since $p-1$ is even, we can multiply each factor with -1 to conclude that $\prod_{k=1}^{p-1} M_k \equiv p \pmod{M_p}$. This completes the proof of the forward direction.

For the converse, assume that the congruence $\prod_{k=1}^{n-1} M_k \equiv n \pmod{M_n}$ holds. Let p be the largest prime divisor of n, so that $M_p \mid M_n$. Then we have the congruence

$$\prod_{k=1}^{n-1} M_k \equiv n \pmod{M_p}$$

We will use this congruence to show that if p is a proper divisor of n, then there is a prime divisor $q > p$ of n. Clearly, such q is again a proper divisor, so there would be by the same argument another prime divisor $r > q$ of n, and so on. Since any natural number has only finitely many prime divisors, this shows that $p = n$.

Suppose, as we announced, that p is a proper divisor of n. Then M_p is among the factors on the left-hand side, which shows that $0 \equiv n \pmod{M_p}$. Thus, we find that $M_p \mid n$. By Theorem 25.4.3 (Zsigmondy's Theorem) it follows that the Mersenne number M_p has a primitive prime divisor $q \mid M_p$. Indeed, p is an odd prime, so we are not in any of the exceptional cases of Zsigmondy's theorem. Since $q \nmid p$, it follows from Proposition 25.4.2 that $q \equiv 1 \pmod{p}$. In particular, we must have $q > p$. □

Exercises

Routine-Building Exercises

25.1 Let $M_n = 2^n - 1$ be the nth Mersenne number. Show that if $d \mid n$, then

$$\Phi_d(2) \mid M_n.$$

25.2 Compute the prime factorization of the Mersenne number $M_{60} = 2^{60} - 1$.

25.3 (a) Show that

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1, \\ p & \text{if } n = p^k \text{ for some prime } p \text{ and } k \geq 1, \\ 1 & \text{if two distinct primes divide } n. \end{cases}$$

(b) Show that for $n \geq 2$ we have

$$\Phi_n(1) = \frac{\operatorname{lcm}(1, \ldots, n)}{\operatorname{lcm}(1, \ldots, n-1)}.$$

25.4 Let $\sigma(n)$ be the sum of the divisors of a natural number n. Show that

$$\sigma(p^m) = \prod_{\substack{d \mid m+1 \\ d>1}} \Phi_d(p).$$

25.5 Suppose that a and b are relatively prime. Show that

$$\frac{2^{ab} - 1}{(2^a - 1)(2^b - 1)} = \prod_{\substack{c \mid a \\ c>1}} \prod_{\substack{d \mid b \\ d>1}} \Phi_{cd}(2).$$

Chapter 26

Integer Factorizations of Polynomial Values

26.1 The Reducibility of $x^n - a$

Theorem 26.1.1 (Vahlen–Capelli). *Consider a rational number a. The polynomial $x^n - a$ is reducible over $\mathbb{Q}$ if and only if either $a = b^k$ for some divisor $k \mid n$, or $n \equiv 0 \pmod 4$ and $a = -4b^4$ for some rational number b.*

26.2 Aurifeuillean Factorizations

26.3 Obstructions to the Infinitude of Primes in Lucas Sequences

In this section, we consider two relatively prime integers a and b, and the associated Lucas sequence (u_n) defined by

$$u_0 = 0, \qquad u_1 = 1, \qquad \text{and} \qquad u_{n+2} = au_{n+1} - bu_n.$$

The central question we are concerned with here, is to determine some conditions on a and b for which all but finitely many numbers u_n are composite. That is, we wish to determine a list of conditions that rule out the possibility of having infinitely many primes of the form u_n, with the goal to better understand restrictions a Lucas sequence must satisfy in order for it to contain infinitely many primes. Some famous conjectures

state that there are infinitely many Mersenne primes and infinitely many Fibonacci primes.

THEOREM 26.3.1 (First obstruction). *Consider two relatively prime integers a and b. Furthermore, assume that $b = k^2$ for some positive integer k, and that $a \geq 3$ as well as $a \geq 2k$. Let (u_n) be the Lucas sequence given by*

$$u_0 = 0, \qquad u_1 = 1, \qquad \text{and} \qquad u_{n+2} = au_{n+1} - bu_n.$$

Then u_n is composite for every $n \geq 3$.

PROOF. Recall from Corollary 19.1.9 that the Lucas sequence (u_n) satisfies the following identities:

$$u_{2n+1} = u_{n+1}^2 - bu_n^2 \qquad \text{and} \qquad u_{2n+2} = u_{n+1}(u_{n+2} - bu_n).$$

By the assumption that $b = k^2$, the first identity shows that any odd idexed entry satisfies the identity

$$u_{2n+1} = (u_{n+1} - ku_n)(u_{n+1} + ku_n).$$

We claim that both factors are ≥ 2, for $n \geq 1$. To see this, it suffices to prove that $u_{n+1} > ku_n + 1$ for $n \geq 1$. This claim is proven by induction. In the base case, there are two cases to consider: Either $k = 1$ or $k > 1$. If $k = 1$, then $u_2 = a \geq 3 > ku_1 + 1$. If $k > 1$, then $u_2 = a \geq 2k > k + 1$. For the inductive step, note that

$$u_{n+2} = au_{n+1} - k^2u_n > 2ku_{n+1} - ku_{n+1} - ku_{n+1}.$$

□

THEOREM 26.3.2 (Second obstruction). *Let α and β be the two roots of the polynomial $x^2 - ax + b$. If $\frac{\alpha}{\beta}$ is a root of unity, then all but finitely many numbers of the form u_n are composite.*

EXAMPLE 26.3.3. The first and second obstructions do not cover all Lucas sequences that are known to have only finitely many primes. To construct a Lucas sequence that is composite for all but finitely many entries outside of the domain of the two obstructions we have so far, we will use Sophie Germain's identity

$$x^4 + 4y^4 = (x^2 - 2xy + 2y^2)(x^2 + 2xy + 2y^2).$$

The only pair of positive integers x and y for which $x^4 + 4y^4$ is prime consists of $x = 1$ and $y = 1$, where we have $1^4 + 4 \cdot 1^4 = 5$. It follows from Sophie Germain's identity that

$$4^{2n+1} + 1 = 2^{4n+2} + 1 = (1 - 2^{n+1} + 2^{2n+1})(1 + 2^{n+1} + 2^{2n+1})$$

is composite except when $n = 0$. Now consider the sequence

$$u_n = \frac{4^n - (-1)^n}{5},$$

which is the Lucas sequence satisfying the recurrence $u_{n+2} = 3u_{n+1} + 4u_n$. The first few values of u_n are $0, 1, 3, 13, 51, 205, 819, \ldots$.

At even exponents, we find the factorization

$$u_{2n} = \frac{4^{2n} - 1}{5} = \frac{(4^n - 1)(4^n + 1)}{5},$$

which shows that u_{2n} is not prime for $n \geq 2$. At odd exponents, we find

$$u_{2n+1} = \frac{4^{2n+1} + 1}{5} = \frac{(1 - 2^{n+1} + 2^{2n+1})(1 + 2^{n+1} + 2^{2n+1})}{5}.$$

Both factors in the numerator are strictly greater than 5 when $n \geq 2$, implying that the denominator 5 is at best a proper divisor of either factor. This shows that u_{2n+1} is composite for $n \geq 2$. Combined with the previous observation about the compositeness of u_{2n}, we find that u_n is composite for all $n \geq 4$. The Lucas sequence (u_n) constructed in this example was discovered in [Ism+2025].

Theorem 26.3.4 (Aurifeuillian obstruction). *Consider a squarefree integer $t > 1$, and set*

$$\mu(t) := \begin{cases} t & \text{if } t \equiv 1 \pmod 4, \\ 2t & \text{if } t \equiv 2, 3 \pmod 4. \end{cases}$$

Consider an integer B of the form $B = s^2 t$, and let (u_n) be the Lucas sequence with characteristic roots

$$\alpha = B^r \qquad \text{and} \qquad \beta = \varepsilon,$$

where $r \geq 1$ is an integer such that $\mu(t) \mid 2r$, and where $\varepsilon = \pm 1$ is chosen such that $\alpha^n - \beta^n$ contains the cyclotomic factor $\Phi_{\mu(t)}(B^n)$ for all odd n. Then the sequence (u_n) contains only finitely many primes.

Definition 26.3.5. A Lucas sequence (u_n) with recurrence relation $u_{n+2} = au_{n+1} - bu_n$ is said to be **regular** if $\gcd(a, b) = 1$.

Definition 26.3.6. A Lucas sequence (u_n) with recurrence relation $u_{n+2} = au_{n+1} - bu_n$ and characteristic roots α and β is said to be **degenerate** if α/β is a root of unity, meaning that there exists an exponent k such that

$$(\alpha/\beta)^k = 1.$$

Theorem 26.3.7. *A Lucas sequence (u_n) with distinct characteristic roots is degenerate if and only if there exists an $n > 0$ such that $u_n = 0$.*

In the following theorem, we give a characterization of the condition that a Lucas sequence *reflects* divisibility. The usual condition for divisibility sequences is that if $m \mid n$, then $u_m \mid u_n$. The property that (u_n) reflects divisibility is the reverse: If $u_m \mid u_n$, then it must be the case that $m \mid n$. A special instance of this condition is that if $u_m = 0$, then $m = 0$.



THEOREM 26.3.8. *Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = au_{n+1} - bu_n$ and characteristic roots α and β. Assume that (u_n) is regular and nondegenerate. Then the following are equivalent:*

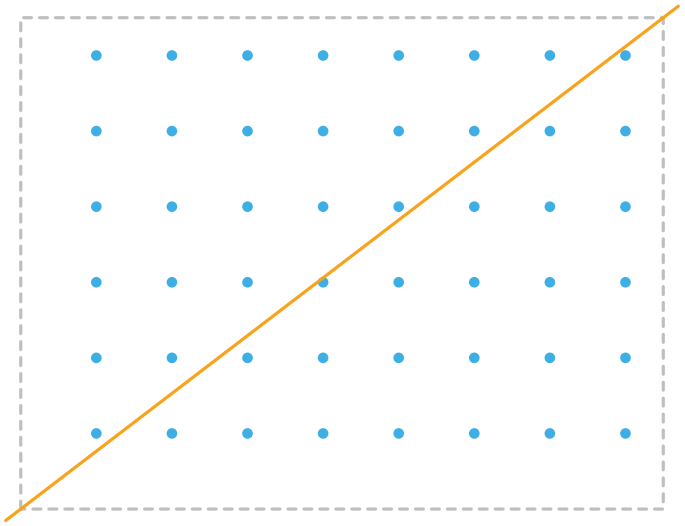
(i) *The Lucas sequence (u_n) reflects divisibility, in the sense that*

$$u_m \mid u_n \quad \Rightarrow \quad m \mid n.$$

(ii) *We have $|u_n| > 1$ for all $n \geq 2$.*

A Lucas sequence which reflects divisibility will be called a ***reflecting Lucas sequence****.*

PROOF. Suppose that m and n are natural numbers such that $u_m \mid u_n$. □



Book III

The Arithmetic of Quadratic Forms

Chapter 27

Quadratic Residues

27.1 Quadratic Congruences

A *quadratic congruence* is a congruence of the form

$$ax^2 + bx + c \equiv 0 \pmod{n},$$

where a is assumed to be relatively prime to n. To build intuition for such quadratic congruences, let's first recall how to solve a quadratic equation

$$ax^2 + bx + c = 0,$$

where $a \neq 0$. Since we have assumed that a is nonzero, we may divide through by a to obtain the equation

$$x^2 + \frac{b}{a}x = -\frac{c}{a}.$$

Completing the square, gives us the equation

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a^2} - \frac{c}{a} = \frac{b^2 - 4ac}{4a^2}.$$

This equation has the familiar solutions

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

The number $\Delta := b^2 - 4ac$ is called the *discriminant* of the quadratic equation $ax^2 + bx + c = 0$. For example, the quadratic equation $x^2 - x - 1$ has discriminant 5, and therefore its solutions are

$$x = \frac{1 \pm \sqrt{5}}{2}.$$

Since the square root $\sqrt{k}$ of an integer k is an integer if and only if k is a perfect square, we obtain the following theorem:

THEOREM 27.1.1. *Consider the quadratic equation with integer coefficients*

$$ax^2 + bx + c = 0,$$

where $a \neq 0$. This equation has a rational solution if and only if the discriminant $\Delta = b^2 - 4ac$ is a perfect square.

Now consider an odd prime p. Recall from Theorem 20.3.2 (Lagrange's Theorem) that a polynomial congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n solutions, where n is the degree of f. It follows that a quadratic congruence modulo a prime has at most two solutions. In the following theorem, which is analogous to the previous theorem, we show that a quadratic congruence modulo an odd prime is solvable if and only if its discriminant is a perfect square.

The situation is slightly different for the prime $p = 2$, since the quadratic congruence

$$x^2 + x + 1 \equiv 0 \pmod{2}$$

has no solutions, even though the discriminant is a perfect square. Indeed, as we will see in the proof below, we will rely on the invertibility of 2 modulo p to solve general quadratic congruences modulo p, which is not possible if $p = 2$.

THEOREM 27.1.2. *Consider a quadratic congruence*

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

modulo an odd prime p, where $a \not\equiv 0 \pmod{p}$. This quadratic congruence is solvable if and only if the discriminant $\Delta = b^2 - 4ac$ is congruent to a square modulo p.

PROOF. Given that p is an odd prime and that $a \not\equiv 0 \pmod{p}$, it follows that $4a$ is invertible modulo p. The quadratic congruence in the statement of the theorem is therefore solvable if and only if the quadratic congruence

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$

is solvable. Given a solution of this quadratic congruence, we calculate

$$\begin{aligned}(2ax + b)^2 &= 4a^2x^2 + 4abx + b^2 \\ &= 4a^2x^2 + 4abx + 4ac + b^2 - 4ac \\ &\equiv b^2 - 4ac\end{aligned}$$

modulo p. This shows that the discriminant is congruent to a square modulo p.

On the other hand, if the discriminant is congruent to a square modulo p, as in

$$y^2 \equiv b^2 - 4ac \pmod{p},$$

then we find, entirely analogous to the case of quadratic equations, that

$$x = \frac{-b \pm y}{2a}$$

solves the quadratic congruence modulo p. We leave the verification that such x is indeed a solution to the reader. □

27.2 Quadratic Residues

We have seen in the previous section that in order to solve a quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

modulo an odd prime p, we need to determine whether the discriminant $\Delta = b^2 - 4ac$ is congruent to a square modulo p. In other words, we need to determine whether the discriminant is a quadratic residue modulo p, which is defined as follows:

Definition 27.2.1. An integer a is said to be a *quadratic residue* modulo n if there is an integer x such that the congruence

$$x^2 \equiv a \pmod{n}$$

holds. If no such x exists, we say that a is a *quadratic nonresidue* modulo n.

For example, 0 and 1 are always quadratic residues modulo any natural number n. The number 0 is called the *trivial quadratic residue*, and we will mostly be interested in the nontrivial quadratic residues.

Modulo 3, the only quadratic residues are 0 and 1, since the quadratic congruence $x^2 \equiv 2 \pmod{3}$ does not have solutions. In other words, every square is either divisible by 3 or congruent to 1 modulo 3.

Similarly, 0 and 1 are the only quadratic residues modulo 4; that is, no square number can be congruent to 2 or 3 modulo 4. Indeed, the square of an even number is divisible by 4 and the square of an odd number is congruent to 1 modulo 4.

Modulo 5 we find that 0, 1, and 4 are quadratic residues, and we can similarly list all the quadratic. The following table lists the nontrivial quadratic residues modulo n from 4 to 10, where 0 is included as a quadratic residue if it is the square of a nonzero integer modulo n:

n	4	5	6	7	8	9	10
quadratic residues	0, 1	1, 4	1, 3, 4	1, 2, 4	0, 1, 4	0, 1, 4, 7	1, 4, 5, 6, 9

If we have access to a primitive root g of a prime p, then it is easy to characterize the nontrivial quadratic residues of p as the even powers of g. This has the immediate corollary that exactly half of the nonzero integers modulo p are quadratic residues.

PROPOSITION 27.2.2. *Consider a prime p with a primitive root g. An integer $a \not\equiv 0 \pmod{p}$ is a nontrivial quadratic residue modulo a p if and only if it is an even power of g.*

PROOF. Consider a primitive root g modulo p. If $a \equiv g^{2k} \pmod{p}$, then a is clearly a quadratic residue modulo p. On the other hand, if $x^2 \equiv a \pmod{p}$, and $x \equiv g^k \pmod{p}$, then we have $a \equiv g^{2k} \pmod{p}$. □

COROLLARY 27.2.3. *There are exactly $(p-1)/2$ nontrivial quadratic residues modulo p in the set $\{1, \ldots, p-1\}$, and exactly $(p-1)/2$ quadratic nonresidues.*

We now turn our attention to the quadratic congruence $x^2 \equiv 1 \pmod{n}$. When n is not a prime number, this congruence can have more solutions than its degree. For example, the quadratic congruence $x^2 \equiv 1 \pmod{8}$ has four distinct solutions. Similarly, the quadratic congruence $x^2 \equiv 1 \pmod{15}$ we have the four solutions

$$1^2 \equiv 1 \pmod{15}, \quad 4^2 \equiv 1 \pmod{15}, \quad 11^2 \equiv 1 \pmod{15}, \quad \text{and} \quad 14^2 \equiv 1 \pmod{15}.$$

In the following theorem we give a precise count of the number of solutions to this quadratic congruence.

THEOREM 27.2.4. *Consider a positive integer n, and let $\omega(n)$ be the number of its prime divisors. Then the number of integers $0 < x < n$ such that $x^2 \equiv 1 \pmod{n}$ is $2^{\omega(n)+\varepsilon(n)}$, where*

$$\varepsilon(n) := \begin{cases} 0 & \text{if } n \text{ is odd,} \\ -1 & \text{if } n \text{ is even but not divisible by } 4, \\ 0 & \text{if } n \text{ is divisible by } 4 \text{ but not by } 8, \\ 1 & \text{if } n \text{ is divisible by } 8. \end{cases}$$

27.3 Legendre Symbols

The fact that the integers $1, 2, \ldots, p-1$ can be split into the sets of quadratic residues and quadratic nonresidues, which are both of size $(p-1)/2$, suggests there is an interesting dichotomy between them. We can explore this further using primitive roots. If g is a primitive root modulo p, then the quadratic residues are precisely those integers modulo p that can be written as an even power of g, and the quadratic nonresidues are precisely those integers modulo p that can be written as an odd power of g. Now recall that

$$g^m g^k = g^{m+k},$$

and that the parity of the sum of two integers can be expressed in terms of the parity of the summands: The summands m and k have the same parity if and only if $m + k$ is

even, and likewise they have distinct parity if and only if $m + k$ is odd. This leads to the following multiplication rule of quadratic residues:

Proposition 27.3.1. *Consider two integers a and b modulo a prime p, both not divisible by p. Then we have*

(i) *If both a and b are quadratic residues, or both are quadratic nonresidues, then ab is a quadratic residue.*

(ii) *If one of a and b is a quadratic residue and the other is a quadratic nonresidue, then ab is a quadratic nonresidue.*

The previous proposition was also observed by Adrien-Marie Legendre, who published his findings in *Essai sur la théorie des nombres* in 1798 [Leg1798]. In this work, he also formulated the quadratic reciprocity theorem, and attempted to prove it. His approach, however, relied on unproven assumptions about certain functions, and was therefore incomplete.

Definition 27.3.2. The *Legendre symbol* of an integer a modulo a prime p, such that $p \nmid a$, is defined by

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

An immediate consequence of Proposition 27.2.2 is that

$$\left(\frac{a}{p}\right) = (-1)^{\operatorname{ind}_g(a)}$$

for any primitive root g modulo p. Using Legendre symbols, we can reformulate Proposition 27.3.1 succinctly as the *multiplicative law of Legendre symbols*: For any two integers a and b, both not multiples of p, the equality

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

holds. In fact, the Legendre symbol is the unique surjective function from the integers $\{1, \dots, p-1\}$ to $\{1, -1\}$ with this property.

Theorem 27.3.3. *Consider an odd prime p. Then the function $a \mapsto \left(\frac{a}{p}\right)$ is the unique surjective function $f : \{1, \dots, p-1\} \to \{1, -1\}$ preserving multiplication, in the sense that*

$$f(ab) = f(a)f(b)$$

for every two nonzero integers a and b modulo p.[1]

[1] In the language of group theory: The Legendre symbol is the unique surjective group homomorphism from the group $(\mathbb{Z}/p\mathbb{Z})^\times$ of invertible elements modulo p to the 2-element group S_2.

PROOF. We have already seen that the Legendre symbol is a surjective function preserving multiplication. Thus, our task is now to show that if $f : \{1, \dots, p-1\} \to \{1, -1\}$ is any surjective function preserving multiplication, then f is the Legendre symbol. Notice that for any primitive root g modulo p, we have

$$f(g^m) = f(g)^m.$$

since every element is of the form g^m, this implies that $f(g) = -1$. Then it follows that $f(g^m) = 1$ if and only if m is even, i.e., $f(a) = 1$ if and only if a is a quadratic residue modulo p. □

EXAMPLE 27.3.4. Recall that 2 is a primitive root of the prime 13, and is therefore a quadratic nonresidue. Using that the square of a Legendre symbol is always 1, we can compute the Legendre symbol $\left(\frac{8}{13}\right)$ as follows:

$$\left(\frac{8}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{2}{13}\right)\left(\frac{2}{13}\right) = \left(\frac{2}{13}\right) = -1.$$

Thus, 8 is a quadratic nonresidue modulo 13.

Similarly, using that $5 \equiv 18 \pmod{13}$ we can compute the Legendre symbol $\left(\frac{5}{13}\right)$ as follows:

$$\left(\frac{5}{13}\right) = \left(\frac{18}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right)\left(\frac{3}{13}\right) = \left(\frac{2}{13}\right) = -1.$$

We see that 5 is also a quadratic nonresidue modulo 13.

On the other hand, again using that the square of a Legendre symbol is always 1, we can compute the Legendre symbol $\left(\frac{3}{13}\right)$ as follows:

$$\left(\frac{3}{13}\right) = \left(\frac{3}{13}\right)\left(\frac{3}{13}\right)\left(\frac{3}{13}\right) = \left(\frac{27}{13}\right) = \left(\frac{1}{13}\right) = 1.$$

Thus we see that 3 is a quadratic residue modulo 13. In fact, we can readily verify that $3 \equiv 4^2 \pmod{13}$. The set of all nontrivial quadratic residues modulo 13 is

$$\{1, 3, 4, 9, 10, 12\}.$$

27.4 Euler's Criterion

Euler had a deep understanding of numbers that are congruent to a square modulo a prime. In 1748 he had published a result now known as *Euler's criterion*, which characterized precisely the squares modulo a prime.

THEOREM 27.4.1 (Euler's Criterion). *Consider an integer a and an odd prime p. Then we have*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Proof. First note that Theorem 16.1.1 (Fermat's Little Theorem) gives that if $b := a^{\frac{p-1}{2}}$, then

$$b^2 \equiv 1 \pmod{p}.$$

This implies that $b \equiv \pm 1 \pmod{p}$.

To prove the congruence in Euler's Criterion, consider a primitive root g modulo p, and suppose that $g^m \equiv a \pmod{p}$. Then a is a quadratic residue if and only if m is even. Also, we note that

$$\frac{m(p-1)}{2}$$

is a multiple of $p-1$ if and only if m is even. Thus we see that

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

if and only if a is a quadratic residue, and it is congruent to -1 otherwise. □

Using Euler's Criterion, we can give a new proof of Theorem 16.5.1. In the language of quadratic residues, Theorem 16.5.1 states that -1 is a quadratic residue modulo an odd prime p if and only if $p \equiv 1 \pmod{4}$. In other words,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

This description of the quadratic character of -1 is also called the *first supplement* of the law of quadratic reciprocity.

Proof of Theorem 16.5.1 using Euler's criterion. By Theorem 27.4.1 (Euler's Criterion), it follows that -1 is a quadratic residue modulo p if and only if

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Since $(-1)^m \equiv 1 \pmod{p}$ if and only if m is even, it follows that -1 is a quadratic residue modulo p if and only if $\frac{p-1}{2}$ is even, which holds if and only if

$$p \equiv 1 \pmod{4}.$$ □

27.5 Euler's Prime-Generating Polynomial

In the early 1770s, Leonhard Euler devised his famous prime-generating polynomial

$$n^2 + n + 41.$$

This polynomial produces prime numbers for any $0 \leq n \leq 39$. Note that

$$40^2 + 40 + 41 = 40(40+1) + 41 = 41^2$$



isn't prime anymore. We could easily imagine Euler pondering one day over the question of creating a quadratic polynomial that returns a surprising amount of primes, and it would be natural to wonder how he might have approached the problem.

Of course, there is no polynomial $f(x)$ other than a constant polynomial such that $f(x)$ is a prime number for every integer x.

PROPOSITION 27.5.1. *If every value of a polynomial $f(x)$ is prime, then $f(x)$ is constant.*

PROOF. Suppose $f(x)$ is a polynomial, all of whose values are prime. Then in particular $p := f(0)$ is prime. Then $p \mid f(kp)$ for every integer k. Since each value of f is prime, it follows that $f(kp) = p$ for every integer k. This implies that $f(x) - p$ has infinitely many roots, i.e., $f(x)$ is the constant polynomial with value p. □

As a reasonable starting point for our search, we take three consecutive primes of the form

$$q,\ q+2,\ \text{and}\ q+6.$$

By Theorem 20.4.2 (Lagrange's Interpolation Theorem), there is only one polynomial f such that $f(n)$ assumes those values for $n = 0, 1, 2$:

$$f(n) = n^2 + n + q.$$

Thus we are faced with the task of finding a prime q such that $n^2 + n + q$ is prime for $0 \leq n \leq q - 2$. One thing to note is that if the number

$$n^2 + n + q$$

is composite for some $0 \leq n \leq q - 2$, then it must have a prime factor below q. Indeed, we have $n^2 + n + q < q^2$ for such n, so if $n^2 + n + q$ is composite for any $0 \leq n \leq q - 2$ then it has an odd prime factor $p < q$. In other words, we want to find an odd prime q such that

$$n^2 + n + q \not\equiv 0 \pmod{p}$$

for any odd prime $p < q$. Recall from Theorem 27.1.2 that such an incongruence holds if and only if the discriminant $\Delta = 1 - 4q$ is a quadratic nonresidue modulo p for any odd prime $p < q$. By Theorem 27.4.1 (Euler's Criterion), this observation finally narrows our search: We are looking for a prime q such that

$$(1 - 4q)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

for any odd prime $p < q$.

We can now discover prime-generating polynomials of the form $n^2 + n + q$ by computing the integer $1 - 4q \pmod{p}$ for all odd primes $3 < p < q$. If we can find a prime p such that $1 - 4q$ is a quadratic residue mod p, we may discard that prime from the remainder of the search. This process resulted in Table 27.1, which reveals that the

$q \setminus p$	3	5	7	11	13	17	19	23	29	31	37
5	2										
7	0	-									
11	2	2	6								
13	0	-	-	-							
17	2	3	3	10	11						
19	0	-	-	-	-	-					
23	2	4	-	-	-	-	-				
29	2	0	-	-	-	-	-	-			
31	0	-	-	-	-	-	-	-	-		
37	0	-	-	-	-	-	-	-	-	-	
41	2	2	5	2	6	7	8	21	11	23	22

Table 27.1: Residues of the discriminant $\Delta = 1 - 4q$ modulo an odd prime $p < q$, for the polynomial $n^2 + n + q$.
Computations of residues for $q \leq p$ are omitted. A dash indicates that it was not necessary to compute this residue, because a quadratic residue has been encountered earlier.

following polynomials are prime-generating polynomials, in the sense that they yield prime numbers for all inputs $0 \leq n \leq q - 2$:

$$n^2 + n + 2 \qquad n^2 + n + 11$$
$$n^2 + n + 3 \qquad n^2 + n + 17$$
$$n^2 + n + 5 \qquad n^2 + n + 41.$$

A deep theorem, the Baker–Heegner–Stark Theorem, shows that these are the only prime-generating polynomials of the form $n^2 + n + q$. In other words, Euler had in fact found the quadratic polynomial of this kind with the longest streak of primes! For this reason, the number 41 is sometimes called Euler's lucky prime.



Exercises

Starter Exercises

27.1 Find all the quadratic residues modulo:

(a) 23,
(b) 29,
(c) 31,
(d) 37.

Confirm in each case that the number of quadratic residues is $(p-1)/2$.

27.2 Compute the Legendre symbols

(a) $\left(\frac{5}{11}\right)$,
(b) $\left(\frac{7}{17}\right)$,
(c) $\left(\frac{3}{19}\right)$.

27.3 Compute the Legendre symbols

(a) $\left(\frac{6}{11}\right)$,
(b) $\left(\frac{12}{17}\right)$,
(c) $\left(\frac{15}{19}\right)$.

27.4 List all the odd primes below 100 of which:

(a) 2 is a quadratic residue,
(b) 3 is a quadratic residue,
(c) 5 is a quadratic residue,
(d) 7 is a quadratic residue.

27.5 Show that the system of congruences

$$\begin{aligned} x + y &\equiv 0 \pmod{p}, \\ xy &\equiv 1 \pmod{p} \end{aligned}$$

is solvable if and only if $p \equiv 1 \pmod{4}$.

Routine-Building Exercises

27.6 Show that for any prime p, the polynomial $x^2 + x + 1$ has a root modulo p if and only if the polynomial $x^2 + x + 7$ has a root modulo p.

27.7 Consider an integer a and a prime p. Show that $-a$ is a quadratic residue modulo p if and only if p divides a number of the form $x^2 + ay^2$.

27.8 (a) Consider a prime $p \equiv 1 \pmod{4}$. Show that g is a primitive root modulo p if and only if $-g$ is a primitive root modulo p.
(b) Consider a prime $p \equiv 3 \pmod{4}$. Show that g is a primitive root modulo p if and only if $-g$ has order $(p-1)/2$ modulo p.

(f)

$p\backslash q$	3	5	7	11	13	17	19	23	29	31
3	-	1	2	1	2	1	2	1	1	2
5	1	-	1	4	1	1	2	1	2	4
7	1	1	-	2	3	1	1	2	6	1
11	2	2	1	-	1	1	1	10	1	2
13	4	3	1	1	-	2	1	2	4	3
17	1	1	1	1	4	-	2	1	1	1
19	1	2	6	6	1	2	-	2	1	3
23	2	1	1	1	2	1	1	-	2	2
29	1	2	4	1	2	7	1	4	-	1
31	1	10	2	1	1	1	2	3	3	-

Table 27.2: The value $(p-1)/\operatorname{ord}_p(q)$, with p and q ranging over the first ten odd primes. Note that the value 1 indicates that q is a primitive root modulo p.

27.9 Consider an odd prime p and an integer a.

(a) Show that if $\operatorname{ord}_p(a)$ is odd, then $\left(\frac{a}{p}\right) = 1$.

(b) Show that if $\left(\frac{a}{p}\right) = -1$, then $\operatorname{ord}_p(a)$ is even.

(c) Give an example where $p \equiv 1 \pmod 4$ and where a is an integer of even order modulo p, such that $\left(\frac{a}{p}\right) = 1$.

(d) Show that if $p \equiv 3 \pmod 4$ and $\operatorname{ord}_p(a) = 2k$ is an even number, then we have

$$\left(\frac{a}{p}\right) = -1,$$

and $a^k \equiv -1 \pmod p$. Thus, in the case where $p \equiv 3 \pmod 4$, the quadratic residues are precisely the integers of odd order, and the quadratic nonresidues are precisely the integers of even order.

(e) Show that if $p \equiv 1 \pmod 4$ and $\operatorname{ord}_p(a)$ is even, then $\left(\frac{a}{p}\right) = 1$ if and only if $\operatorname{ord}_p(a) \mid \frac{p-1}{2}$.

Combine the previous parts to show that for any odd prime p and for any integer $a \not\equiv 0 \pmod p$, we have the identity

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\operatorname{ord}_p(a)}}.$$

Table 27.2 lists the values of $\frac{p-1}{\operatorname{ord}_p(a)}$, where p and q range over the first ten primes.

(g) Using Exercise 21.7, give a direct proof of the identity

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\operatorname{ord}_p(a)}}.$$

27.10 Consider an odd prime p, an integer a, and an integer m. Show that

$$a^m \equiv \left(\frac{a}{p}\right) \pmod{p} \quad \Leftrightarrow \quad m \equiv \frac{p-1}{2} \left(\mathrm{mod}\ \ \operatorname{ord}_p(a)\right).$$

Challenge Exercises

27.11 Recall that a Fermat prime is a prime of the form $F_n := 2^{2^n} + 1$. Show that the following are equivalent for a prime number p:

(i) The prime p is a Fermat prime.

(ii) Every quadratic nonresidue modulo p is a primitive root.

27.12 (a) Show that $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{3}$.

(b) For any finite set $p_1, \ldots, p_k$ of primes congruent to 1 modulo 3, use the prime divisors of

$$n = (p_1 \cdots p_k)^2 + 3$$

to show that there is a prime $q \equiv 1 \pmod{3}$ that is not already among the primes $p_1, \ldots, p_k$. Conclude that there are infinitely many primes congruent to 1 modulo 3.

27.13 (a) Show that $\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right)$ holds for every prime $q \neq 5$. In other words, which two congruence classes 1, 2, 3, or 4 modulo 5 contain the primes q such that 5 to be a quadratic residue modulo q?

(b) For any finite set of primes $p_1, \ldots, p_k$ congruent to 1 modulo 5, use the prime divisors of

$$(2p_1 \cdots p_k)^4 + 5$$

to show that there is a prime $q \equiv 1 \pmod{5}$ that is not already among the primes $p_1, \ldots, p_k$. Conclude that there are infinitely many primes congruent to 1 modulo 5.

27.14 Consider an odd prime p.

(a) For any positive integer m and any integer a, show that a is a quadratic residue modulo p^m if and only if a is a quadratic residue modulo p.

(b) Conclude that there are exactly

$$\frac{(p-1)p^m}{2}$$

quadratic residues modulo p^{m+1} that are not divisible by p.

27.15 Recall that a prime p is said to be a Sophie Germain prime if the number $q = 2p + 1$ is prime.

(a) Show that p is a Sophie Germain prime if and only if every quadratic nonresidue modulo q apart from -1 is a primitive root modulo q.

(b) Show that if $p \equiv 1 \pmod 4$ is a Sophie Germain prime, then 2 is a primitive root modulo q.

(c) Show that if $p \equiv 3 \pmod 4$ is a Sophie Germain prime, then -2 is a primitive root modulo q.

27.16 Consider the Fibonacci sequence (F_n). For parts (a) and (b) assume that $p \neq 2, 5$ is a prime, and define

$$h := \frac{p - \left(\frac{5}{p}\right)}{2}.$$

(a) Show that

$$F_{n+2h} \equiv \left(\frac{5}{p}\right) F_n \pmod p.$$

(b) Show that

$$F_{h+n} \equiv (-1)^{n+1} \left(\frac{-1}{p}\right) F_{h-n} \pmod p.$$

(c) Show that there does not exist an odd prime p such that for all $0 \leq k \leq p-1$, we have $k \equiv s^2$ for some s if and only if $k \equiv F_n \pmod p$ for some Fibonacci number n.

Chapter 28

Quadratic Reciprocity

28.1 The Quadratic Character of 2

In this section we consider the question for which odd primes p we have that 2 is a quadratic residue. By Exercise 27.9, this is equivalent to the question for which primes p we have

$$\frac{p-1}{\operatorname{ord}_p(2)} \equiv 0 \pmod{2}.$$

In the following table we list the quantity $\frac{p-1}{\operatorname{ord}_p(2)}$ for the odd primes below 50:

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$\frac{p-1}{\operatorname{ord}_p(2)}$	1	1	2	1	1	2	1	2	1	6	1	2	3	2.

This table shows that 2 is a quadratic residue modulo p for the primes

$$7,\ 17,\ 23,\ 31,\ 41,\ 47,\ \ldots.$$

Unlike the case where we were seeking to characterize the primes for which -1 is a primitive root, these primes are not organized according to their residue class modulo 4. The pattern is slightly more complicated. However, we may observe that the primes for which 2 is a quadratic residue all happen to be close to a multiple of 8, while the primes for which 2 is a quadratic nonresidue are further from the multiples of 8. This turns out to be the right idea: The number 2 is a quadratic residue modulo p if and only if p is of the form $8k \pm 1$.

Note also that 2 is a primitive root if and only if $\operatorname{ord}_p(2) = p-1$, so we see from the previous table that 2 is a primitive root modulo p for the primes

$$3,\ 5,\ 11,\ 13,\ 19,\ 29,\ 37,\ \ldots.$$

However, it is not quite true that 2 is a primitive root modulo p whenever it is a quadratic nonresidue modulo p: The first prime for which 2 is neither a quadratic residue nor a primitive root is 43.

THEOREM 28.1.1. *The Legendre symbol of 2 modulo an odd prime p satisfies the identity*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

In other words, 2 is a quadratic residue if and only if $p \equiv \pm 1 \pmod 8$, and it is a quadratic nonresidue if and only if $p \equiv \pm 3 \pmod 8$.

Before we start the proof, recall that one of the proofs of Theorem 16.1.1 (Fermat's Little Theorem) was obtained by multiplying all the numbers $1, \ldots, p-1$ with an integer a to obtain the congruence

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod p.$$

Since $(p-1)!$ isn't divisible by p, it is invertible modulo p and thus we found that $a^{p-1} \equiv 1 \pmod p$.

PROOF. In this proof, we will write $P := \frac{p-1}{2}$ so that $2P = p-1$. By Theorem 27.4.1 (Euler's Criterion) we have $\left(\frac{2}{p}\right) \equiv 2^P \pmod p$, which gives us the congruences

$$\left(\frac{2}{p}\right)P! \equiv 2^P P! \equiv 2 \cdot 4 \cdot \cdots \cdot (2P) \pmod p$$

We proceed by carefully analyzing this product of all the even positive integers below p. If we define the numbers

$$s := \left\lfloor \frac{p-1}{4} \right\rfloor \qquad \text{and} \qquad t := \left\lfloor \frac{p+1}{4} \right\rfloor,$$

so that $s + t = P$, then we can partition the set of all even positive integers below p into two subsets

$$S := \{2k \mid 1 \le k \le s\} \qquad \text{and} \qquad T := \{2k \mid s+1 \le k \le P\},$$

so that S consists precisely of all the even positive integers up to and possibly including P, and T consists of all the larger even integers up to and including $2P$. Note that the set S has s elements and the set T has exactly t elements.

The key observation is that for every integer y in T there is a unique *odd* integer $1 \le x \le P$ so that $y = p - x$, which determines a bijection. Thus, taking the product

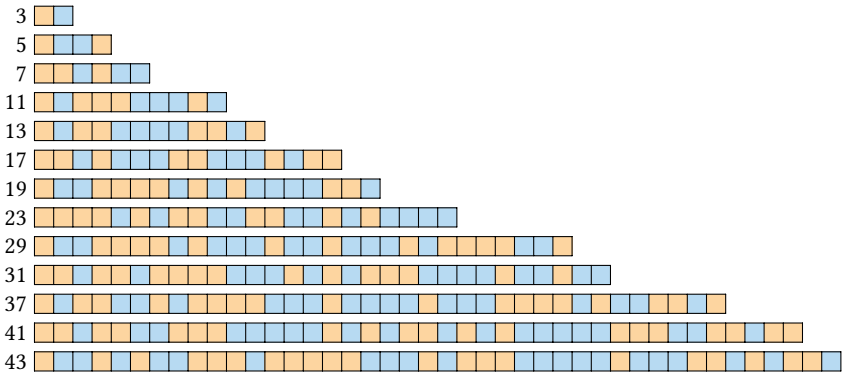


Figure 28.1: Quadratic residues (orange) and nonresidues (blue) among the integers $1, \dots, p-1$, for odd primes $3 \leq p \leq 43$.

modulo p of all the even integers up to p amounts to taking the product of all the integers $1 \leq x \leq P$ with a sign change for every odd integer, of which there are t. In other words, we have the congruence

$$\left(\frac{2}{p}\right) P! \equiv 2 \cdot 4 \cdot \cdots \cdot 2P \equiv (-1)^t P! \pmod{p}.$$

Since $P!$ is not divisible by p we apply the cancellation law to obtain

$$\left(\frac{2}{p}\right) = (-1)^t.$$

We conclude the proof by observing that the parity of t is determined according to the following cases:

$$t \equiv \begin{cases} 0 \pmod 2 & \text{if } p \equiv \pm 1 \pmod 8 \\ 1 \pmod 2 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

□

We will present a second combinatorial proof, due to Thomas Joannes Stieltjes [Sti1884].

Proof. We will write $P := \frac{p-1}{2}$. Call a number $1 \leq k \leq p-2$ a **variation** if one of k and $k+1$ is a residue and the other is a nonresidue. That is, if we color the residues orange and the nonresidues blue, as we did in Figure 28.1, then k is a variation if k and $k+1$ have distinct colors. We first claim that there are exactly P variations.

To see this, note that k is a variation if and only if $k(k+1)$ is a nonresidue. Defining $r_k := \frac{k+1}{k}$, so that $k^2 r_k \equiv k(k+1)$, we see that k is a variation if and only if r_k is a nonresidue. Furthermore, the map $k \mapsto r_k$ is a bijection

$$\{1, \dots, p-2\} \cong \{2, \dots, p-1\}$$

with inverse $k \mapsto \frac{1}{k-1}$. Since there are exactly P nonresidues in the latter set, the claim follows. Consequently, we observe that since the sequence $1, \dots, p-1$ begins with a residue and contains exactly P variations, it follows that $-1 \equiv p-1 \pmod{p}$ is a residue if and only if P is even. That is, -1 is a residue if and only if $p \equiv 1 \pmod{4}$.

Observe that k is a variation if and only if $p-k-1$ is a variation. Ideed, multiplying by -1 either preserves the residuosity of both members of a consecutive pair of numbers or reverses the residuosity of both. This implies that variations occur in pairs

$$\{k, p-k-1\}$$

Each of these sets has exactly two elements, except the set $\{P, p-P-1\} = \{P\}$. Since the number of variations is P, we see that P is a variation if and only if P is odd. It also follows that the number of variations in the set $\{1, \dots, P-1\}$ is

$$\begin{cases} \frac{p-1}{4} & \text{if } p \equiv 1 \pmod{4}, \\ \frac{p-3}{4} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

There are now two cases, each of which splits in two further cases. If $p \equiv 1 \pmod{4}$, then the congruence $2P \equiv -1 \pmod{p}$ shows that 2 is a residue if and only if P is. Furthermore, P is a residue if and only if P is preceeded by an even number of variations. The number of variations preceeding P is $(p-1)/4$, so we conclude that 2 is a residue if $p \equiv 1 \pmod{8}$, and a nonresidue if $p \equiv 5 \pmod{8}$.

If $p \equiv 3 \pmod{4}$, then the congruence $2P \equiv -1 \pmod{p}$ shows that 2 is a residue if and only if P is a nonresidue. As before, P is a residue if and only if P is preceeded by an even number of variations, which is $(p-3)/4$, so we conclude that 2 is a residue if $p \equiv 7 \pmod{8}$ and a nonresidue if $p \equiv 3 \pmod{8}$. □

The previous theorem is also known as the *Second Supplement* of the law of Quadratic Reciprocity. An immediate corollary of the second supplement is that

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 3 \pmod{8} \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{8}. \end{cases}$$

Since primitive roots are always quadratic nonresidues, we obtain the following corollary. Artin conjectured that there are infinitely many primes p for which 2 is a primitive root. More generally, he conjectured that for any integer a that is neither -1 nor a perfect square, there are infinitely many primes for which a is a primitive root.

COROLLARY 28.1.2. *If 2 is a primitive root modulo p, then* $p \equiv \pm 3 \pmod{8}$.

The second supplement can be used to show that there are infinitely many primes of the form $8k+r$ for any odd number $0 < r < 8$. We have already seen in Theorem 16.6.1 that there are infinitely many primes congruent to 1 modulo 2^n. In particular, there are infinitely many primes of the form $8k+1$. It remains prove the analogous claims for the residue classes 3, 5, and 7 modulo 8. We will be following Sierpiński [SIE1988]. The first ten primes congruent to r moduo 8 for each odd residue class r are given in Table 28.1.

	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th
$r = 1$	17	41	73	89	97	113	137	193	233	241
$r = 3$	3	11	19	43	59	67	83	107	131	139
$r = 5$	5	13	29	37	53	61	101	109	149	157
$r = 7$	7	23	31	47	71	79	103	127	151	167

Table 28.1: The first ten primes congruent to r modulo 8, for $r = 1, 3, 5, 7$.

Theorem 28.1.3. *There are infinitely many primes congruent to* 3 *modulo* 8.

Proof. If a is an odd integer, then $a^2 \equiv 1 \pmod 8$ so that

$$N_a := a^2 + 2$$

is congruent to 3 modulo 8. Not all prime divisors of N_a can be congruent to ± 1 modulo 8, since if they were, then N_a would likewise be congruent to ± 1 modulo 8. Therefore N_a has a prime divisor q so that

$$q \equiv \pm 3 \pmod 8.$$

Since $q \mid a^2 + 2$, it follows that -2 is a quadratic residue modulo q, so $q \not\equiv -3 \pmod 8$. Thus it follows that $q \equiv 3 \pmod 8$.

For a suitable choice of a, let p_n be the nth prime number, so that $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ and so forth. Then we define

$$a = p_2 p_3 \cdots p_n,$$

so that any prime divisor of N_a is larger than p_n. Since N_a has a prime divisor congruent to 3 modulo 8, it follows that there are arbitrarily large such primes. □

Theorem 28.1.4. *There are infinitely many primes congruent to* 5 *modulo* 8.

Proof. If a is an odd integer, then $a^2 \equiv 1 \pmod 8$ so that

$$N_a := a^2 + 4$$

is congruent to 5 modulo 8. As before, there must be a prime divisor q of N_a so that

$$q \equiv \pm 3 \pmod 8.$$

Since $q \mid a^2 + 4$, it follows that -4 is a quadratic residue modulo q. This implies that -1 is a quadratic residue modulo q, so that $q \equiv 1 \pmod 4$. Since we assumed that $q \not\equiv 1 \pmod 8$, it follows that $q \equiv -3 \pmod 8$.

For a suitable choice of a, define

$$a = p_2 p_3 \cdots p_n$$

so that any prime divisor of N_a is larger than p_n. Since N_a has a prime divisor congruent to 5 modulo 8, it follows that there are arbitrarily large such primes. □

THEOREM 28.1.5. *There are infinitely many primes congruent to* 7 *modulo* 8.

PROOF. The idea of the proof is to find a natural number N of the form

$$N = 2a^2 - b^2,$$

so that $N \equiv -1 \pmod 8$ and N is relatively prime to any $m \leq n$. Assuming that $n > 1$, a suitable choice of a and b is $a := n!$ and $b := 1$. Indeed, in this case a is even, so that $2a^2 - 1 \equiv -1 \pmod 8$.

Under these assumptions, N will have a prime factor $q \not\equiv 1 \pmod 8$, and furthermore we will have

$$2a^2 \equiv b^2 \pmod q.$$

Since a^2 and b^2 are clearly quadratic residues modulo q, it follows that 2 is a quadratic residue, implying that $q \equiv \pm 1 \pmod 8$. However, since we have chosen q so that $q \not\equiv 1 \pmod 8$, it follows that $q \equiv -1 \pmod 8$. Furthermore, since q is relatively prime to any $m \leq n$, it follows that $n < q$, which shows that there are arbitrarily large primes $q \equiv -1 \pmod 8$. □

28.2 The Statement of Quadratic Reciprocity

We have already established several facts about Legendre symbols. The Legendre symbol is multiplicative, meaning that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

The Legendre symbol $\left(\frac{-1}{p}\right)$ can be computed according to whether p is congruent to 1 or 3 modulo 4:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

The Legendre symbol $\left(\frac{2}{p}\right)$ can likewise be computed according to whether p is congruent to ± 1 or ± 3 modulo 8:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

We need one final piece to effectively compute Legendre symbols: a way to determine the Legendre symbol $\left(\frac{q}{p}\right)$ when q is an odd prime. The recipe for determining $\left(\frac{q}{p}\right)$ is given by the law of quadratic reciprocity.

To build some intuition for what the law of quadratic reciprocity should assert, we recall from Exercise 27.9 that the Legendre symbol of a modulo p can be computed by

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\operatorname{ord}_p(a)}}.$$

$p\backslash q$	3	5	7	11	13	17	19	23	29	31
3		−	+	−	+	−	+	−	−	+
5	−		−	+	−	−	+	−	+	+
7	−	−		+	−	−	−	+	+	−
11	+	+	−		−	−	−	+	−	+
13	+	−	−	−		+	−	+	+	−
17	−	−	−	−	+		+	−	−	−
19	−	+	+	+	−	+		+	−	−
23	+	−	−	−	+	−	−		+	+
29	−	+	+	−	+	−	−	+		−
31	−	+	+	−	−	−	+	−	−	

Table 28.2: The sign of the Legendre symbol $\left(\frac{q}{p}\right)$, ranging over pairs of distinct odd primes p and q.

Thus, the Legendre symbol of a modulo p depends only of the parity of the quantity

$$\frac{p-1}{\operatorname{ord}_p(a)},$$

which gives us a fairly quick way of determining the Legendre symbol $\left(\frac{q}{p}\right)$ for small odd primes p and q. We listed signs of the Legendre symbols of q modulo p in Table 28.2.

The patterns in this table might not be immediately apparent. However, those who did Exercise 27.13 might spot that column 5 is identical to row 5. Looking for more identical columns and rows, we create a new table by comparing the entry in row i and column j in Table 28.2 with the entry in row j and column i. When these two entries are equal, we mark it with a solid black circle (●), and if they are different we mark it with an open circle (○). This results in the following table:

Using this table, we quickly spot that columns 5, 13, 17, and 29 are identical to rows 5, 13, 17, and 29, respectively, which means that these columns were also identical to their respective rows in Table 28.2. Something special is going on with the primes

$$5,\ 13,\ 17,\ 29,$$

and something seems to be off about the primes

$$3,\ 7,\ 11,\ 19,\ 23,\ 31.$$

We are very familiar with this grouping of the primes by now: The first set of primes are all congruent to 1 modulo 4, while the second set of primes are all congruent to 3 modulo 4. These observations suggest the following:

$p\backslash q$	3	5	7	11	13	17	19	23	29	31
3		●	○	○	●	●	○	○	●	○
5	●		●	●	●	●	●	●	●	●
7	○	●		○	●	●	○	○	●	○
11	○	●	○		●	●	○	○	●	○
13	●	●	●	●		●	●	●	●	●
17	●	●	●	●	●		●	●	●	●
19	○	●	○	○	●	●		○	●	○
23	○	●	○	○	●	●	○		●	○
29	●	●	●	●	●	●	●	●		●
31	○	●	○	○	●	●	○	○	●	

(i) If at least one of p and q is congruent to 1 modulo 4, then we have

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

(ii) If both p and q are congruent to 3 modulo 4, then we have

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Legendre and Gauss spotted these patterns towards the end of the 18th century. They formulated it succinctly as follows:

THEOREM 28.2.1 (The Law of Quadratic Reciprocity). *For any two distinct odd primes p and q we have*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

EXAMPLE 28.2.2. The law of quadratic reciprocity is incredibly effective in computations of Legendre symbols. For example, since 17 and 101 are congruent to 1 modulo 4, we have

$$\left(\frac{17}{101}\right) = \left(\frac{101}{17}\right) = \left(\frac{16}{17}\right) = \left(\frac{4}{17}\right)\left(\frac{4}{17}\right) = 1.$$

Indeed, it turns out that $44^2 \equiv 17$ and $57^2 \equiv 17$ modulo 101.

On the other hand, both 23 and 43 are congruent to 3 modulo 4, so the law of quadratic reciprocity tells us that

$$\left(\frac{23}{43}\right) = -\left(\frac{43}{23}\right) = -\left(\frac{20}{23}\right) = -\left(\frac{4}{23}\right)\left(\frac{5}{23}\right) = -\left(\frac{5}{23}\right) = -\left(\frac{23}{5}\right) = -\left(\frac{3}{5}\right) = 1.$$

In this case, it turns out that $18^2 \equiv 23$ and $25^2 \equiv 23$ modulo 43.

As a final example, for good measure, note that 31 and 83 are both congruent to 3 modulo 4. Using the law of quadratic reciprocity we obtain that

$$\left(\frac{31}{83}\right) = -\left(\frac{83}{31}\right) = -\left(\frac{21}{31}\right) = -\left(\frac{3}{31}\right)\left(\frac{7}{31}\right) = -\left(\frac{31}{3}\right)\left(\frac{31}{7}\right) = -\left(\frac{1}{3}\right)\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = 1.$$

The quadratic residuosity of an odd prime q modulo a distinct odd prime p determines some important restrictions on the form of the prime p. We spell these out in the following theorem, which is essentially a reformulation of the law of quadratic reciprocity.

Theorem 28.2.3. *Consider two distinct odd primes p and q. The following two statements hold:*

(i) *If $p \equiv 1 \pmod 4$, then q is a quadratic residue modulo p if and only if there exists an odd integer $0 < a < q$ such that*

$$p \equiv a^2 \pmod{4q}.$$

(ii) *If $p \equiv 3 \pmod 4$, then q is a quadratic residue modulo p if and only if there exists an odd integer $0 < a < q$ such that*

$$p \equiv -a^2 \pmod{4q}.$$

Proof. Before proving each statement, we note that for any $u \not\equiv 0 \pmod q$, if the quadratic congruence

$$x^2 \equiv u \pmod q$$

is solvable, then it has two solutions. Of these two solutions, one is even and the other is odd. Thus, if it is solvable, we can always pick an odd solution.

For the first claim of the theorem, assume that $p \equiv 1 \pmod 4$. By the law of quadratic reciprocity, it follows that

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

Furthermore, $\left(\frac{p}{q}\right) = 1$ if and only if there exists an odd integer $0 < a < q$ such that $p \equiv a^2 \pmod q$. Furthermore, since a is odd and $p \equiv 1 \pmod 4$, it also follows that $p \equiv a^2 \pmod 4$. Thus we see that $\left(\frac{q}{p}\right) = 1$ if and only if there exists an odd integer $0 < a < q$ such that

$$p \equiv a^2 \pmod{4q}.$$

For the second claim, assume that $p \equiv 3 \pmod 4$. By the law of quadratic reciprocity, it follows that

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = (-1)^{\frac{q-1}{2}} = \left(\frac{-1}{q}\right).$$

By rearranging the terms, we find that $\left(\frac{q}{p}\right) = \left(\frac{-p}{q}\right)$, and thus there is an odd integer a such that

$$p \equiv -a^2 \pmod{q}.$$

Since a is assumed to be odd and $p \equiv 3 \pmod{4}$, we find furthermore that $-a^2 \equiv p \pmod{4}$. We conclude that $\left(\frac{q}{p}\right) = 1$ if and only if there is an odd integer $0 < a < q$ such that

$$p \equiv -a^2 \pmod{4q}.$$ □

The previous theorem can be used at once to characterize the primes p for which 3 is a quadratic residue modulo p. Taking $q = 3$ in the previous theorem, we find that 3 is a quadratic residue modulo p if and only if p is of the form $12k \pm 1$, since the only odd quadratic residue modulo 3 is 1. For any odd prime $p \neq 3$, we have thus shown that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

Likewise, we can characterize the primes p for which 5 is a quadratic residue modulo p. Taking $q = 5$ in the previous theorem, we find that 5 is a quadratic residue modulo p if and only if p is of the form $20k \pm 1$ or $20k \pm 9$, since the two odd squares modulo 5 are 1^2 and 3^2. For any odd prime $p \neq 5$, we have thus shown that

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{10}. \end{cases}$$

28.3 Gauss's Lemma

While it is customary to consider the standard residue classes modulo an odd prime p to be the integers $0 \leq r < p$, we have now the occasion to consider the complete residue system of integers between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$.

DEFINITION 28.3.1. The *least absolute residue* of an integer a modulo a natural number n is the unique integer

$$-\frac{n}{2} < x \leq \frac{n}{2}$$

such that $x \equiv a \pmod{n}$. We will write $\lfloor a \rceil_n$ for the least absolute residue of a modulo n, and we will write $\lVert a \rVert_n$ for its absolute value.

Thus, the least absolute residue of an integer a modulo an odd prime p, which is what we will be using this concept for, is the unique integer

$$-\frac{p-1}{2} \leq x \leq \frac{p-1}{2}$$

such that $x \equiv a \pmod{p}$. For example, the least absolute residue of 4 modulo 7 is -3, the least absolute residue of 6 modulo 13 is 6, and the least absolute residue of 12 modulo 13 is -1. In the following table, we list the least absolute residues modulo 11:

a	0	1	2	3	4	5	6	7	8	9	10
$\lfloor a \rceil_{11}$	0	1	2	3	4	5	-5	-4	-3	-2	-1.

If we consider an integer a relatively prime to an odd prime p, then multiplication by a defines a bijection on $\mathbb{Z}/p\mathbb{Z}$. It follows that the function

$$x \mapsto \lfloor ax \rceil_p : \{0, \dots, p-1\} \to \{-\tfrac{p-1}{2}, \dots, \tfrac{p-1}{2}\}$$

is also a bijection. Restricting this bijection to the set $\{1, \dots, \frac{p-1}{2}\}$, we obtain an injective function

$$x \mapsto \lfloor ax \rceil_p : \{1, \dots, \tfrac{p-1}{2}\} \to \{-\tfrac{p-1}{2}, \dots, \tfrac{p-1}{2}\}.$$

The following lemma implies that every $1 \leq x \leq \frac{p-1}{2}$ occurs exactly once as the absolute value of any number of the form $\lfloor ax \rceil_p$. This holds whenever a is relatively prime to the modulus $m \geq 3$, as illustrated in Figure 28.3.

Lemma 28.3.2. *Consider a modulus $m \geq 3$ with $m' := \lfloor \frac{m-1}{2} \rfloor$, and let a be an integer. Then the map r_a given by $x \mapsto \llbracket ax \rrbracket_m$ defines a function*

$$r_a : \{1, \dots, m'\} \to \{1, \dots, m'\}.$$

Furthermore, this function r_a is a bijection if and only if a is relatively prime to m.

Proof. Suppose first that $\gcd(a, m) = 1$. For any $1 \leq x \leq m'$, we have $0 < 2x < m$, so that $m \nmid 2ax$. Consequently,

$$0 < \llbracket ax \rrbracket_m < \frac{m}{2},$$

showing that r_a takes values in the indicated set.

To prove injectivity, suppose that $r_a(x) = r_a(y)$. Then

$$ax \equiv \pm ay \pmod{m},$$

and hence $x \equiv \pm y \pmod{m}$. The negative sign is impossible because $0 < x + y < m$. Thus $x \equiv y \pmod{m}$, which implies $x = y$. Since the domain and codomain have the same finite size, r_a is a bijection.

Conversely, suppose that the formula defines a bijection. Since $m \geq 3$, its codomain contains 1, so there is an x such that $\llbracket ax \rrbracket_m = 1$. Therefore $ax \equiv \pm 1 \pmod{m}$, which implies $\gcd(a, m) = 1$. □

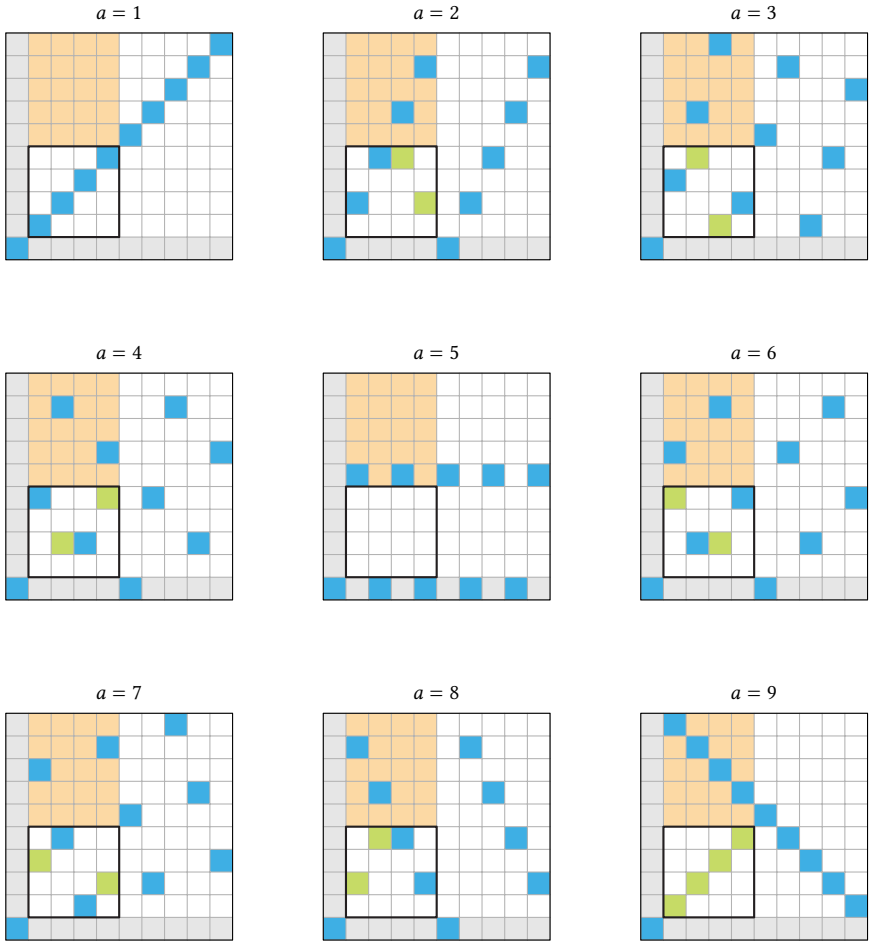


Figure 28.2: The least absolute residue function is a bijection on $\{1, \ldots, \lfloor (m-1)/2 \rfloor\}$ if and only if the multiplier a is relatively prime to m.

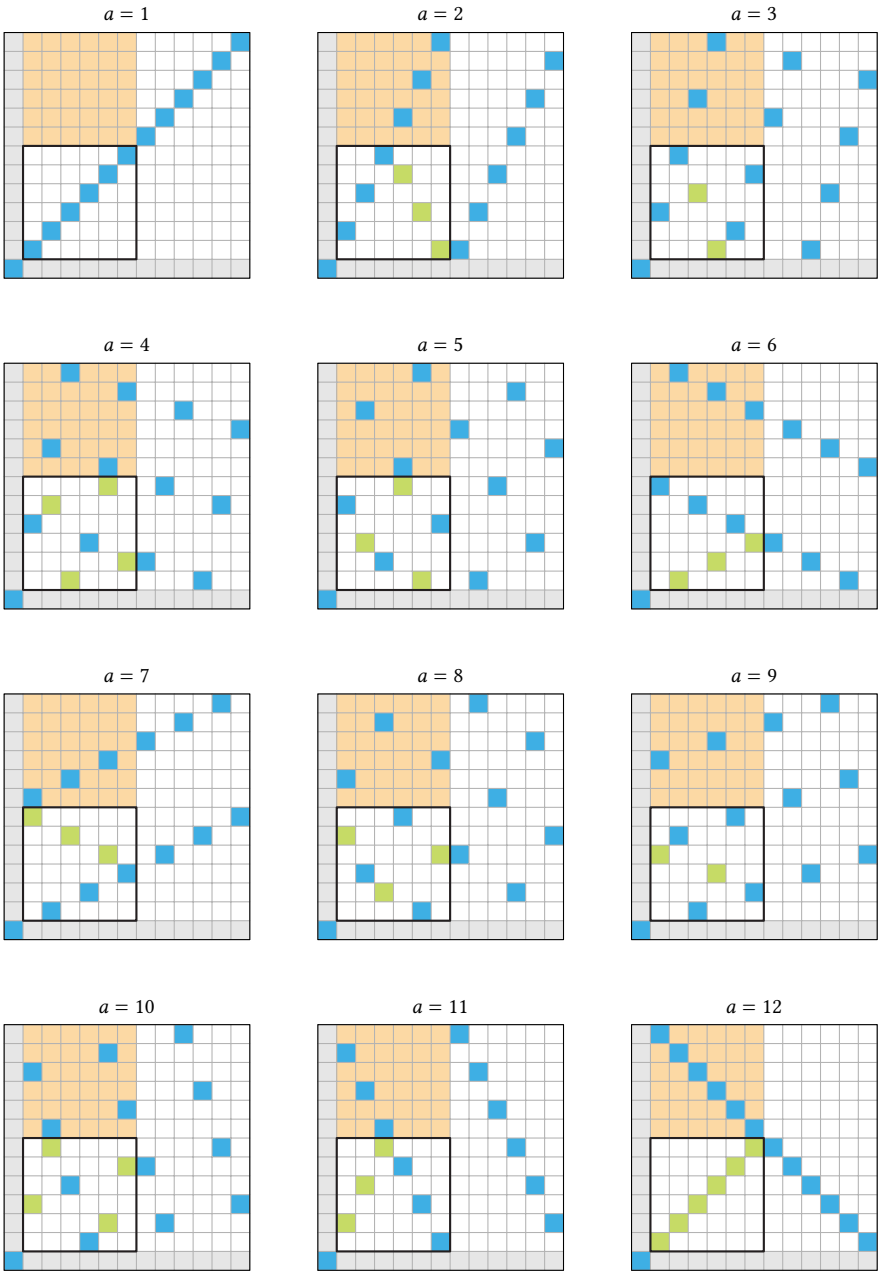


Figure 28.3: If p is an oodd prime, then the number of reflected residues of ax modulo p for $1 \leq x \leq \frac{p-1}{2}$ is even if and only if a is a quadratic residue.

LEMMA 28.3.3 (Gauss's Lemma). *Consider an odd prime p and an integer such that $p \nmid a$. Define μ to be the number of elements x among the residue classes*

$$a,\ 2a,\ 3a,\ \ldots,\ \tfrac{p-1}{2}a \pmod{p},$$

such that $\lfloor ax \rceil_p$ is negative. Then we have

$$\left(\frac{a}{p}\right) = (-1)^{\mu}.$$

PROOF. Write $P := (p-1)/2$. Then we have that $p \nmid P!$, so suffices to show that

$$\left(\frac{a}{p}\right) P! \equiv (-1)^{\mu} P! \pmod{p}.$$

By Theorem 27.4.1 (Euler's Criterion) we have $\left(\frac{a}{p}\right) \equiv a^P \pmod{p}$, so we obtain that

$$\left(\frac{a}{p}\right) P! \equiv a^P P! \pmod{p}.$$

Redistributing the P factors of a of the exponent a^P over $P!$, and using Lemma 28.3.3, we obtain:

$$a^P P! = (1a)(2a)\cdots(Pa) \equiv (-1)^{\mu} P! \pmod{p}. \qquad \square$$

28.4 Eisenstein's Proof of the Law of Quadratic Reciprocity

Gauss was the first to prove the law of quadratic reciprocity in 1796, when he was only 19 years old. This proof was included in his seminal work, *Disquisitiones Arithmeticae*, published in 1801. Gauss was very fond of this result, and throughout his life-time he would publish seven different proofs.

The proof we will present here is due to Gotthold Eisenstein, which he published in 1844. It is celebrated for its simplicity and for the insightful perspective it provides on geometric aspects of the quadratic reciprocity law.

In Eisenstein's proof of the law of quadratic reciprocity, we will make use of the *floor function* $x \mapsto \lfloor x \rfloor$, which is a function from the rational numbers or the real numbers, to the integers. The integer

$$\lfloor x \rfloor$$

is the largest integer below x. In other words, its defining property is that the floor function satisfies the logical equivalence

$$k \leq \lfloor x \rfloor \quad \Leftrightarrow \quad k \leq x$$

for every integer k and every rational or real number x. Concretely, we have the following examples:

$$\left\lfloor \frac{3}{2} \right\rfloor = 1, \qquad \left\lfloor \frac{29}{31} \right\rfloor = 0, \qquad \text{and} \qquad \left\lfloor -\frac{1}{4} \right\rfloor = -1.$$

Eisenstein's proof of Theorem 28.2.1 (The Law of Quadratic Reciprocity). By Lemma 28.3.3 (Gauss's Lemma) it suffices to show that

$$(-1)^{\mu(q,p)}(-1)^{\mu(p,q)} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

In other words, we have to show that

$$\mu(q,p) + \mu(p,q) \equiv \frac{p-1}{2}\frac{q-1}{2} \pmod 2.$$

This suggests that there should be a way of splitting a set of $\frac{p-1}{2}\frac{q-1}{2}$ points into two subsets S and T, so that their respective number of elements have the same parities as the quantities $\mu(q,p)$ and $\mu(p,q)$. There is indeed such a way. Figure 28.4 shows Eisenstein's setup in case of the primes $p = 17$ and $q = 13$.

Consider the set of $\frac{p-1}{2}$ by $\frac{q-1}{2}$ lattice points in the positive quadrant of the plane; that is, the points with positive integer coordinates within the rectangle spanned by the four points

$$\big(0,0\big),\ \big(\tfrac{p}{2},0\big),\ \big(\tfrac{p}{2},\tfrac{q}{2}\big),\ \text{and}\ \big(0,\tfrac{q}{2}\big).$$

We partition these lattice points by the diagonal of the rectangle: The set of lattice points below the diagonal is S, and the set of lattice points above the diagonal is T. Since the diagonal of this rectangle is given by the line $y = \frac{q}{p}x$, there is no point with positive integer coordinates on the diagonal, so there is no ambiguity as to which part a lattice point belongs to.

Now observe that the number $|S|$ of lattice points in the set S is given by

$$|S| = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor.$$

This formula is obtained by first recognizing that for each $1 \le k \le \frac{p-1}{2}$, a lattice point of the form (k,i) is in the set S if and only if

$$1 \le i \le \frac{q}{p}k.$$

The number of such lattice points is $\lfloor \frac{kq}{p} \rfloor$, so the total number of elements in S is obtained by summing up all of these totals. Similarly, the number $|T|$ of lattice points in the set T is given by

$$|T| = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$



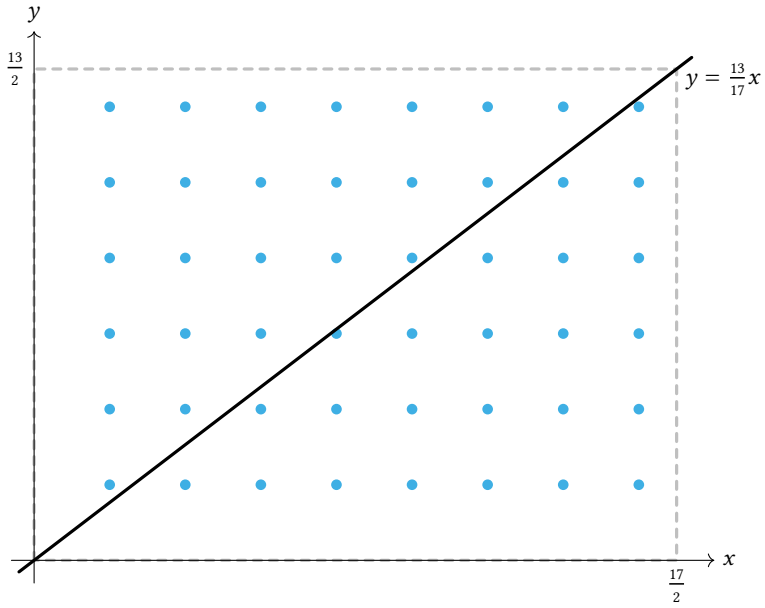


Figure 28.4: In Eisenstein's proof of quadratic reciprocity, we count the $\frac{p-1}{2}$ by $\frac{q-1}{2}$ lattice points in the marked rectangle as the sum of the number lattice points below the diagonal and the number of lattice points above the diagonal.

Thus, it remains to prove that

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor \equiv \mu(q,p) \pmod 2 \quad \text{and} \quad \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor \equiv \mu(p,q) \pmod 2.$$

We will verify these congruences separately in the following lemma. □

LEMMA 28.4.1. *Consider an odd prime p and an odd integer a not divisible by p, and let $\mu(a,p)$ be the quantity defined in Lemma 28.3.3 (Gauss's Lemma). Then*

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \equiv \mu(a,p) \pmod 2.$$

PROOF. For each k there are unique integers q_k and r_k such that $ka = q_k p + r_k$, where

$$-\frac{p-1}{2} \le r_k \le \frac{p-1}{2}.$$

It follows that

$$\left\lfloor \frac{ka}{p} \right\rfloor = \begin{cases} q_k & \text{if } r_k > 0 \\ q_k - 1 & \text{if } r_k < 0. \end{cases}$$

Adding up the integers $\lfloor \frac{ka}{p} \rfloor$ therefore amounts to adding up the integers q_k and subtracting the number of integers k such that r_k is negative:

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{\frac{p-1}{2}} q_k - \mu(a,p).$$

To complete the proof, it therefore suffices to show that

$$\sum_{k=1}^{\frac{p-1}{2}} q_k \equiv 0 \pmod 2.$$

To prove this, recall from Lemma 28.3.2 that the map $k \mapsto |r_k|$ is a permutation of the set $\{1, \dots, \frac{p-1}{2}\}$. In other words, every integer from 1 to $\frac{p-1}{2}$ occurs exactly once as an integer of the form $|r_k|$. Since the parity of an integer is unchanged by taking its absolute value, we have

$$\sum_{k=1}^{\frac{p-1}{2}} r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} |r_k| \equiv \sum_{k=1}^{\frac{p-1}{2}} k \pmod 2.$$

On the other hand, observe that since a and p are assumed to be odd, we have the congruences

$$k \equiv ka = q_k p + r_k \equiv q_k + r_k \pmod 2.$$

Thus we obtain the congruences

$$\sum_{k=1}^{\frac{p-1}{2}} k \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{k=1}^{\frac{p-1}{2}} r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{k=1}^{\frac{p-1}{2}} k \pmod 2.$$

Subtracting $\sum_k k$ from both sides, we find that $\sum_k q_k \equiv 0 \pmod 2$. □

Exercises

Starter Exercises

28.1 Compute the values of the following Legendre symbols:

$$\left(\frac{101}{163}\right), \quad \left(\frac{137}{359}\right), \quad \left(\frac{113}{479}\right), \quad \text{and} \quad \left(\frac{139}{953}\right).$$

28.2 Compute the values of the following Legendre symbols:

$$\left(\frac{113}{131}\right), \quad \left(\frac{131}{311}\right), \quad \text{and} \quad \left(\frac{311}{113}\right).$$

28.3 Compute the values of the following Legendre symbols:

$$\left(\frac{199}{919}\right), \quad \left(\frac{919}{991}\right), \quad \text{and} \quad \left(\frac{991}{199}\right).$$

28.4 Compute the values of the following Legendre symbols:

$$\left(\frac{337}{373}\right), \quad \left(\frac{373}{733}\right), \quad \text{and} \quad \left(\frac{733}{337}\right).$$

28.5 Show that the system of congruences

$$\begin{aligned} x - y &\equiv 1 \pmod{p}, \\ xy &\equiv 1 \pmod{p} \end{aligned}$$

has a solution if and only if $p \equiv \pm 1 \pmod{10}$.

Routine-Building Exercises

28.6 Consider a prime $p > 3$. Show that

$$\left(\frac{6}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 5 \pmod{24}, \\ -1 & \text{if } p \equiv \pm 7, \pm 11 \pmod{24}. \end{cases}$$

28.7 Consider an odd prime $p \neq 5$. Show that

$$\left(\frac{10}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}, \\ -1 & \text{if } p \equiv \pm 7, \pm 11, \pm 17, \pm 19 \pmod{40}. \end{cases}$$

28.8 Determine whether the following quadratic congruences have solutions:

(a) $x^2 + x + 1 \equiv 0 \pmod{13}$.
(b) $x^2 + x + 3 \equiv 0 \pmod{7}$.
(c) $2x^2 + 3x + 5 \equiv 0 \pmod{17}$.
(d) $x^2 + 4x + 8 \equiv 0 \pmod{23}$.

(e) $2x^2 + 3x + 4 \equiv 0 \pmod{11}$.
(f) $4x^2 + 7x + 14 \equiv 0 \pmod{31}$.

28.9 Show that 2 is a quadratic residue modulo any prime divisor of the nth Fermat number $F_n = 2^{2^n} + 1$, for $n \geq 2$.

28.10 Consider a prime p such that $q := 2p + 1$ and $r := 2(2p + 1) + 1 = 4p + 3$ are both prime. Prove that

$$\operatorname{ord}_r(2) = q.$$

Challenge Exercises

28.11 Show that if the nth Fermat number $F_n = 2^{2^n} + 1$ is prime, then 3 is a primitive root modulo F_n.

28.12 Consider an odd prime p. Show that the following are equivalent:

(i) The Mersenne number $M_p = 2^p - 1$ has a common prime divisor with $2p + 1$.

(ii) The prime p is a *Sophie Germain prime*, meaning that the number $2p + 1$ is prime, and furthermore $p \equiv 3 \pmod{4}$.

Conclude that

$$M_{11}, M_{23}, M_{83}, M_{131}, M_{179}, \text{ and } M_{191}$$

are all composite.

28.13 (a) Show that for any prime $p \equiv 3 \pmod{4}$ greater than 3, there exists a prime $q < p$ such that p is a quadratic nonresidue modulo q.
(b) Show that for any prime $p \equiv 1 \pmod{4}$, there exists a prime $q < p$ such that p is a quadratic nonresidue modulo q. Hint: First show that there exists a quadratic nonresidue $0 < a < p$ such that $a \equiv 1 \pmod{4}$.

28.14 (a) For any integer $a > 2$, let p be a prime factor of $a^4 - a^2 + 1$. Show that

$$\operatorname{ord}_p(a) = 12.$$

(b) Use a suitable choice of a in

$$N_a := a^6 + 1$$

to show that there are infinitely many primes congruent to 1 modulo 12.
(c) For each r in the set $\{5, 7, 11\}$, show that there are infinitely many primes congruent to r modulo 12.



Chapter 29

Primality Testing

29.1 Pépin's Primality Test for the Fermat Numbers

Édouard Lucas observed that the quadratic character of -1 can be used to reach a sharper conclusion on the congruence class of a prime dividing a Fermat number.

Theorem 29.1.1 (Lucas's refinement of Theorem 16.1.4). *Consider a prime divisor $p = k2^{n+1} + 1$ of the nth Fermat number F_n, where $n \geq 2$. Then k is even and*

$$\operatorname{ord}_p(k) = \operatorname{ord}_p(2^{n+1}) = 2^{n+1-\nu_2(n+1)}.$$

Consequently, we have $p \equiv 1 \pmod{2^{n+2}}$.

Théophile Pépin used the theory of quadratic residues to develop a deterministic primality test for Fermat primes.

Theorem 29.1.2 (Pépin's Primality Test). *For $n \geq 1$, the nth Fermat number F_n is prime if and only if*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

29.2 The Carmichael Numbers

Theorem 16.1.1 (Fermat's Little Theorem) asserts that if p is a prime number, then the congruence

$$x^p \equiv x \pmod{p}$$

holds for every integer x. Thus it is natural to wonder whether Fermat's Little Theorem can be used to test whether a number is prime. If we can find an integer x such that

$$x^n \not\equiv x \pmod{n}$$

then it is certain that n must be composite. This is a very useful test, since it provides a way to establish that the number n is composite without factoring it, and for many composite numbers it is indeed possible to find an integer x such that $x^n \not\equiv x \pmod{n}$.

However, if no such integer x exists, this simple test does not provide a guarantee for the primality of n. Robert Carmichael discovered that there are composite numbers that satisfy Fermat's congruence for every integer [CAR1912].

DEFINITION 29.2.1. A *Carmichael number* is a composite integer $n > 1$ such that the congruence

$$x^n \equiv x \pmod{n}$$

holds for every integer x.

Alternatively, we can define a Carmichael number to be a composite number n such that

$$n \mid x^n - x.$$

Thus, a Carmichael number is a composite number n dividing the fixed divisor of the polynomial x^n. In order to find examples of Carmichael numbers, it is therefore useful to first compute the fixed divisor of this polynomial.

Recall from Definition 20.5.1 that the fixed divisor of a polynomial $f(x)$ is the greatest common divisor of all the values of $f(x)$. In §20.5 we showed that the fixed divisor of $f(x) = x^n - x$ can be determined by computing the greatest common divisor of the values

$$f(2), \ldots, f(\lfloor \tfrac{n+1}{2} \rfloor).$$

While this theorem is useful to compute the fixed divisor of any specific polynomial, such as $x^7 - x$, we shall compute the fixed divisor of $x^n - x$ using Theorem 16.1.1 (Fermat's Little Theorem) and Theorem 20.3.2 (Lagrange's Theorem).

THEOREM 29.2.2. *Consider the polynomial $x^n - x$, for some natural number $n > 1$. Its fixed divisor is the square-free number*

$$\prod_{\substack{p \text{ prime} \\ p-1 \mid n-1}} p.$$

PROOF. First, we claim that a prime number p appears as a factor of the fixed divisor of $x^n - x$ if and only if

$$p - 1 \mid n - 1.$$

For the forward direction of this claim, suppose that p divides every integer of the form $x^n - x$ and write $n - 1 = k(p-1) + r$ where $0 \leq r < p - 1$. Since $x^n - x = x(x^{n-1} - 1)$ and p is prime, it follows from Theorem 16.1.1 (Fermat's Little Theorem) that

$$x^r - 1 \equiv x^{k(p-1)+r} - 1 \equiv x^{n-1} - 1 \equiv 0 \pmod{p},$$

when x is not divisible by p. However, Theorem 20.3.2 (Lagrange's Theorem) tells us that the polynomial $x^r - 1$ has at most $r < p-1$ roots modulo p when $r \neq 0$. Therefore we conclude that $r = 0$; that is, $p - 1 \mid n - 1$.

Conversely, if $p - 1 \mid n - 1$, then it follows by Fermat's Little Theorem that

$$x^{n-1} \equiv 1 \pmod{p}$$

for every x not divisible by p. This implies that $x(x^{n-1} - 1)$ is divisible by p for every x, completing the proof of the first claim.

To finish the proof, it remains to show that the fixed divisor of $x^n - x$ is square-free, i.e., that for each prime number p there is an integer x such that $p^2 \nmid x^n - x$. We choose $x = p$, because the integer $p^n - p = p(p^{n-1} - 1)$ is indeed not divisible by p^2. □

Theorem 29.2.2 can be used to obtain a characterization of the Carmichael numbers due to Alwin Korselt [Kor1899]. Since n is a Carmichael number if and only if n divides the fixed divisor of $x^n - x$, we see that such n must be square-free and for each of its prime divisors p we must have $p - 1 \mid n - 1$. Thus, we obtain:

Theorem 29.2.3 (Korselt's criterion). *A composite number $n > 1$ is a Carmichael number if and only if the following two conditions hold:*

(i) *The number n is squarefree.*

(ii) *For any prime divisor p of n, we have $p - 1 \mid n - 1$.*

In order to narrow our search for examples of Carmichael numbers further, we show that there are no Carmichael numbers of the form pq, and that they are always odd.

Theorem 29.2.4. *Any Carmichael number is an odd number with at least three prime factors.*

Proof. First, suppose n is an even Carmichael number. Since n is composite and square-free, there must exists an odd prime p dividing n. For such a prime p we have

$$p - 1 \mid n - 1.$$

However, $p - 1$ is even while $n - 1$ is odd, which is a contradiction. Any Carmichael number must therefore be odd.

Now consider a number $n = pq$ where p and q are distinct primes. In order for n to be a Carmichael number, we must have

$$p - 1 \mid pq - 1 \qquad \text{and} \qquad q - 1 \mid pq - 1.$$

By writing $pq - 1 = (p - 1)q + (q - 1)$ we see that

$$p - 1 \mid pq - 1 \quad \Leftrightarrow \quad p - 1 \mid q - 1$$

and we get a similar logical equivalence when we reverse the roles of p and q. This shows that $p = q$, contradicting the assumption that p and q are distinct. □



A trick similar to the factorization trick we used to rule out two-prime Carmichael numbers can be used to obtain some useful congruences involving the prime factors of a three-prime Carmichael number.

PROPOSITION 29.2.5. *Any three-prime Carmichael number $n = pqr$ satisfies the congruences*

$$\begin{aligned} qr &\equiv 1 \pmod{p-1} \\ pr &\equiv 1 \pmod{q-1} \\ pq &\equiv 1 \pmod{r-1}. \end{aligned}$$

PROOF. Since the three congruences are symmetric in p, q, and r, it suffices to show prove the first congruence. By writing $pqr - 1 = (p-1)qr + qr - 1$ we see that

$$p - 1 \mid pqr - 1 \quad \Leftrightarrow \quad p - 1 \mid qr - 1,$$

from which it follows that if $n = pqr$ is a Carmichael number then $qr \equiv 1 \pmod{p-1}$. □

We have now gathered enough information about three-prime Carmichael numbers to start hunting for small examples. In the following theorem we will show that there is exactly one three-prime Carmichael number divisible by 3. Similar techniques can be used to find the finitely many three-prime Carmichael numbers whose smallest prime divisor is a fixed small prime p such as $p = 5$ or $p = 7$.

THEOREM 29.2.6. *There is exactly one Carmichael number of the form $3qr$ with $3 < q < r$ prime, namely*

$$561 = 3 \cdot 11 \cdot 17.$$

PROOF. Suppose that the number $3qr$ is a Carmichael number. Then the congruences

$$\begin{aligned} qr &\equiv 1 \pmod{2} \\ 3r &\equiv 1 \pmod{q-1} \\ 3q &\equiv 1 \pmod{r-1} \end{aligned}$$

hold. The first one simply says that q and r are both odd, which we already knew. The second congruence says that 3 is invertible modulo $q - 1$. This implies that $q \equiv 0$ or $2 \pmod{3}$. However, since q is assumed to be a prime larger than 3 it follows that $q \equiv 2 \pmod{3}$.

Using that $q = 3u + 2$ with $0 < u$ we see that the congruences $3r \equiv 1 \pmod{q-1}$ and $3q \equiv 1 \pmod{r-1}$ can be stated equivalently as the congruences

$$\begin{aligned} r &\equiv 2u + 1 \pmod{3u+1} \\ 9u + 5 &\equiv 0 \pmod{r-1}. \end{aligned}$$

From the first of these congruences we see that $r = k(3u+1) + (2u+1)$, where we may note that $k \neq 0$ since $q < r$. However, the second congruence now gives us that $r \leq 9u + 6$. This inequality can be used to further restrict the possible values of the integer k:

$$k(3u+1) + (2u+1) \leq 9u + 6 \quad \Rightarrow \quad k \leq \frac{7u+5}{3u+1} \leq 3.$$

There are thus three options for k:

(i) If $k = 3$ then we must have $q = 5$ and $r = 15$. However, 15 is composite, so we conclude that $k \neq 3$.

(ii) If $k = 2$ then $r - 1 = 8u + 2$. However, no number of the form $8u + 2$ divides a number of the form $9u + 5$, so we conclude that $k \neq 2$.

(iii) The only remaining case is where $k = 1$ and $r - 1 = 5u + 1$. The divisibility relation

$$5u + 1 \mid 9u + 5$$

implies that $0 < u \leq 3$. Since

$$5 \cdot 1 + 1 \nmid 9 \cdot 1 + 5, \qquad 5 \cdot 2 + 1 \nmid 9 \cdot 2 + 5, \qquad \text{and} \qquad 5 \cdot 3 + 1 \mid 9 \cdot 3 + 5$$

we find that $u = 3$, and therefore $q = 11$ and $r = 17$. □

In 1994, William Robert Alford, Andrew Granville, and Carl Pomerance made extensive use of Korselt's criterion to show that there are infinitely many Carmichael numbers [AGP1994]. Thomas Wright showed in 2013 that there are infinitely many Carmichael numbers in any arithmetic progression $ax+b$ with a and b relatively prime [Wri2013].

29.3 The Lucas–Lehmer Primality Test

This test is named after Édouard Lucas and Derrick Henry Lehmer, who refined Lucas's ideas in the 1930s.

29.4 Pocklington's Criteria

Theorem 29.4.1 (Pocklington's Theorem). *Consider a number $n > 1$, and suppose there exist a positive integer a and a prime number p such that*

(i) $a^{n-1} \equiv 1 \pmod{n}$,

(ii) $p \mid n - 1$ *and* $p > \sqrt{n} - 1$,

(iii) $\gcd\left(a^{(n-1)/p} - 1, n\right) = 1$.

Then the number n is prime.



PROOF. Assume to the contrary that n is composite, and let q be a prime factor of n such that $q \leq \sqrt{n}$. Then we have

$$q - 1 \leq \sqrt{n} - 1 < p,$$

showing that $q - 1$ and p are relatively prime. Thus, it follows that there is an integer u such that $pu \equiv 1 \pmod{q-1}$. Now we get the following congruences modulo q:

$$\begin{aligned} a^{(n-1)/p} &\equiv a^{pu(n-1)/p} \\ &\equiv a^{u(n-1)} \\ &\equiv (a^{n-1})^u \\ &\equiv 1. \end{aligned}$$

The last congruence holds since $q \mid n$ and the assumption that $a^{n-1} \equiv 1 \pmod{n}$. Thus, it follows that q is a divisor of both $a^{(n-1)/p} - 1$ and n, which contradicts the assumption that they are relatively prime. □

EXAMPLE 29.4.2. In order to illustrate the Pocklington-Lehmer test, we will show that the number

$$11! + 1 = 39,916,801$$

is prime. Primes of the form $n! \pm 1$ are called *factorial primes*. The largest known example is $632,760! - 1$.

Given that $n := 11! + 1$, we have that

$$n - 1 = 11! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11.$$

29.5 Mersenne Primes

DEFINITION 29.5.1. The *Mersenne numbers* are the numbers of the form $M_n := 2^n - 1$. *Mersenne primes* are Mersenne numbers that are prime.

PROPOSITION 29.5.2. *If M_n is a Mersenne prime, then n is prime.*

LEMMA 29.5.3. *The congruence*

$$2^{M_p} \equiv 2 \pmod{M_p}.$$

holds for any prime number p.

PROOF. First observe that by the definition $M_n = 2^n - 1$, it follows that $\operatorname{ord}_{M_n}(2) = n$. This implies that

$$2^k \equiv 2^l \pmod{M_n}$$

if and only if $k \equiv l \pmod{n}$.

By Fermat's Little Theorem we have that $2^p \equiv 2 \pmod{p}$, so that $M_p \equiv 1 \pmod{p}$. Thus we obtain that

$$2^{M_p} \equiv 2^1 \pmod{M_p}.$$ □

Proposition 29.5.4. *The Mersenne number $M_{31} = 2,147,483,647$ is prime.*

Proof. We set $a := 2$ and $n := M_{31}$ so that $n - 1 = 2(2^{30} - 1)$. First, note that since 31 is prime, it follows from Lemma 29.5.3 that

$$2^{n-1} \equiv 1 \pmod{n}.$$

Thus, the first condition in the Pocklington–Lehmer primality test is satisfied.

First, we factor the number $M_{31} - 1 = 2^{31} - 2$, which is $2(2^{30} - 1)$. We do so by the following calculation:

$$\begin{aligned} 2^{30} - 1 &= (2^{15} - 1)(2^{15} + 1) \\ &= (2^5 - 1)(2^{10} + 2^5 + 1)(2^5 + 1)(2^{10} - 2^5 + 1) \\ &= 31 \cdot 1057 \cdot 33 \cdot 993 \\ &= 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331. \end{aligned}$$

The number $151 \cdot 331$ is strictly larger than $\sqrt{M_{31}}$, so it will be suitable for the Pocklington Lehmer test. □



Exercises

Routine-Building Exercises

29.1 Use Pocklington's criterion to show that the following numbers are prime:

(a) $13,421 = 11^4 - 11^3 + 11^2 - 11 + 1$,
(b) $28,393 = 13^4 - 13^2 + 1$,
(c) $2,311,921 = 39^4 - 39^2 + 1$.

Hints: $13,421$ divides $11^{10} - 1$, $28,393$ divides $13^{12} - 1$, and $2,311,921$ divides $39^{12} - 1$.

29.2 Prove that the following are equivalent:

(i) $2^{M_n} \equiv 2 \pmod{M_n}$.
(ii) $2^{n-1} \equiv 1 \pmod{n}$.

29.3 Show that for every integer n there is an integer x such that $\lambda(n)/2$ is the least positive integer k for which the congruence

$$x^k \equiv -1 \pmod{n}$$

is solvable.

29.4 Show that the only Carmichael numbers of the form $5qr$ are

$$1105 = 5 \cdot 13 \cdot 17, \qquad 2464 = 5 \cdot 17 \cdot 29, \qquad \text{and} \qquad 10585 = 5 \cdot 29 \cdot 73.$$

29.5 Show that any Carmichael number n is relatively prime to the value $\phi(n)$ of Euler's totient function. Numbers with this property are called *cyclic*.

Appendix A

Conjectures in Elementary Number Theory

Number theory is known for its wealth of open problems that have inspired mathematicians and enthusiasts to learn more about the subject. Some of the most famous problems, such as Goldbach's conjecture and the Twin Prime conjecture have remained elusive for centuries. We state here some open problems and conjectures in elementary number theory.

There are many more open problems, specifically concerning analytic number theory and advanced branches of algebraic number theory, which require tools beyond the scope of this text in order to be formulated. For a more comprehensive overview of the open problems and conjectures in number theory, see [Guy2004].

A.1 Conjectures About the Infinitude of Certain Classes of Primes

One of the oldest and most famous open problems about the infinitude of certain classes of primes is the Twin Prime Conjecture. A pair of *twin primes* is a pair of primes p and q such that $q - p = 2$. In Exercise 13.11 we stated some elementary congruences satisfied by pairs of twin primes.

Conjecture 1 (Twin Prime Conjecture). *There are infinitely many twin primes.*

Although the study of twin primes dates back to antiquity, the first publication in

which the twin prime conjecture was explicity stated was by Alphonse de Polignac [POL1846]. He also speculated about a generalization of the Twin Prime Conjecture.

CONJECTURE 2 (de Polignac's Conjecture). *For every even number n, there are infinitely many pairs of primes p and q such that $q - p = n$.*

A *Sophie Germain prime* is a prime p such that $2p + 1$ is also prime. Sophie Germain studied these primes in the context of Fermat's Last Theorem. In Exercise 13.12 we established an elementary congruence regarding Sophie Germain primes. In Exercise 27.15 we characterized Sophie Germain primes in terms of their primitive roots.

CONJECTURE 3 (Infinitude of Sophie Germain primes). *There are infinitely many Sophie Germain primes.*

Dickson's conjecture generalizes both conjectures of de Polignac and the conjectured infinitude of the Sophie Germain primes. Recall that we introduced the concept of fixed divisors in §20.5, where we proved Theorem 20.5.2 (Hensel's Fixed Divisor Theorem [HEN1896]).

CONJECTURE 4 (Dickson's Conjecture). *Consider a finite set of linear functions $f_i(x) = a_i x + b_i$ indexed by $1 \leq i \leq n$, which is* admissible *in the sense that their product*

$$\prod_{i=1}^{n} f_i(x)$$

has no fixed divisors. Then there are infinitely many positive integers x such that each $f_i(x)$ is prime for all $1 \leq i \leq n$.

One can also ask about the infinitude of primes that can be presented as the value of some polynomial. The simplest such conjecture is a conjecture of Landau.

CONJECTURE 5 (Landau's Conjecture). *There are infinitely many primes of the form $n^2 + 1$.*

Landau's conjecture is generalized by the following conjecture Bunyakovsky.

CONJECTURE 6 (Bunyakovsky's Conjecture). *Consider an irreducible polynomial $f(x)$ with integer coefficients, such that the leading coefficient is positive. If the fixed divisor of $f(x)$ is 1, then $f(x)$ is prime for infinitely many input values x.*

Schinzel's Hypothesis H is a sweeping generalization of both Dickson's conjecture and Bunyakovsky's conjecture.

CONJECTURE 7 (Schinzel's Hypothesis H). *Consider a finite set of nonconstant irreducible polynomials $f_i(x)$ with integer coefficients, such that their product*

$$\prod_{i=1}^{n} f_i(x)$$

has no fixed divisors. Then there are infinitely many integers x such that each $f_i(x)$ is prime.

There are many more conjectures on the infinitude of primes of a certain form, or primes satisfying a certain condition. The most famous such conjecture asserts the infinitude of the Mersenne primes.

Conjecture 8 (Infinitude of Mersenne primes). *There are infinitely many primes of the form* $M_p = 2^p - 1$.

Conjecture 9 (Infinitude of Wilson primes). *There are infinitely many Wilson primes; that is, there are infinitely many primes* p *such that*

$$(p-1)! \equiv -1 \pmod{p^2}.$$

Conjecture 10 (Infinitude of Wolstenholme primes). *There are infinitely many Wolstenholme primes; that is, there are infinitely many primes* p *such that*

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}.$$

Conjecture 11 (Infinitude of Fibonacci primes). *There are infinitely many Fibonacci primes.*

A prime number p is said to be *balanced* if the gap to its preceding prime is equal to the distance to its succeeding prime.

Conjecture 12 (Infinitude of balanced primes). *There are infinitely many balanced primes.*

Conjecture 13 (Infinitude of Pierpont primes). *There are infinitely many primes of the form* $2^a 3^b + 1$.

Conjecture 14 (Artin's Conjecture). *If* a *is a nonsquare integer distinct from* -1*, then there are infinitely many primes* p *for which* a *is a primitive root modulo* p.

A.2 Conjectures About Exceptional Primes

Conjecture 15 (Finiteness of Fermat primes). *There are only finitely many primes of the form* $F_n = 2^{2^n} + 1$.

Conjecture 16 (Finiteness of Wieferich primes). *There are only finitely many Wieferich primes.*

Although it is conjectured that there are only finitely many Wieferich primes, it has not yet been proven that there are infinitely many non-Wieferich primes.

Conjecture 17 (Infinitude of non-Wieferich primes). *There are infinitely many non-Wieferich primes.*

Conjecture 18 (Finiteness of Wal–Sun–Sun primes). *There are only finitely many Wal–Sun–Sun primes; that is, there are only finitely many primes* p *such that* p^2 *divides the* $(p - \left(\frac{p}{5}\right))^{th}$ *Fibonacci number. Here, the number* $\left(\frac{p}{5}\right)$ *is the Legendre symbol of* p *modulo* 5.



A.3 Conjectures About Gaps Between the Primes

CONJECTURE 19 (Legendre's Conjecture). *For every positive integer n, there is at least one prime between* n^2 *and* $(n+1)^2$.

CONJECTURE 20 (Andrica's Conjecture). *If p and q are two consecutive primes, then* $\sqrt{q} - \sqrt{p} < 1$.

CONJECTURE 21 (Cramér's Conjecture). *The asymptotic growth of the gap from a prime p to the next prime is* $O(\log(p)^2)$.

A.4 Conjectures About Conditions for Primality

CONJECTURE 22 (Lehmer's Conjecture). *If* $\phi(n) \mid n-1$, *then n is prime.*

CONJECTURE 23 (The Agoh–Giuga Conjecture). *An integer* $n > 1$ *is prime if and only if the congruence*

$$\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n}$$

holds.

CONJECTURE 24 (The Bateman–Selfridge–Wagstaff Conjecture (The New Mersenne Prime Conjecture)). *Let p be an odd natural number. If two of the following three conditions hold, then so does the third:*

(i) *There is an integer k such that* $p = 2^k \pm 1$ *or* $p = 4^k \pm 3$.

(ii) *The Mersenne number* $M_p = 2^p - 1$ *is prime.*

(iii) *The number* $(2^p + 1)/3$ *is prime.*

For the following conjecture, let p_n be the nth prime number, starting with $p_0 := 2$, $p_1 := 3$, and so on. Define the nth *primorial* by

$$p_n\# := \prod_{i=0}^{n} p_i.$$

CONJECTURE 25 (Fortune's Conjecture). *For each n, if* m_0 *is the least integer m such that* $p_n\# + m$ *is prime, then* m_0 *is prime.*

A.5 Conjectures About Prime Decompositions

CONJECTURE 26 (Square-freeness of Fermat numbers). *Every Fermat number* $F_n = 2^{2^n} + 1$ *is square-free [BW1967].*

Conjecture 27 (Square-freeness of Mersenne numbers with prime exponents). *Every Mersenne number M_p with prime exponent p is square-free [Rot1965; BW1967].*

In Exercise 16.21 we showed that for any two distinct primes p and q, any common prime divisor r of the numbers

$$\frac{p^q-1}{p-1} \qquad \text{and} \qquad \frac{q^p-1}{q-1}$$

satisfies $r \equiv 1 \pmod{2pq}$.

Conjecture 28 (The Feit–Thompson Conjecture). *There are no two distinct primes p and q such that*

$$\frac{p^q-1}{p-1} \qquad \textit{divides} \qquad \frac{q^p-1}{q-1}$$

Conjecture 29 (Grimm's Conjecture). *If the numbers $n+1, \ldots, n+k$ are all composite, then there is a set of k distinct primes p_i such that $p_i \mid n+i$ for each $1 \le i \le k$.*

A *Sierpiński number* is an odd number k such that every number of the form $k \cdot 2^n + 1$ is composite.

Conjecture 30 (Sierpiński's problem). *The smallest Sierpiński number is* $78,557$.

A *Riesel number* is an odd number k such that every number of the form $k \cdot 2^n - 1$ is composite.

Conjecture 31 (Riesel's problem). *The smallest Riesel number is* $509,203$.

A.6 Conjectures About Arithmetic Functions

Conjecture 32 (The nonexistence of odd perfect numbers). *There are no odd perfect numbers.*

Conjecture 33 (Infinitude of Amicable Numbers). *There are infinitely many pairs of amicable numbers; that is, there are infinitely many pairs of distinct numbers such that the sum of the proper divisors of either one of them equals the other.*

A number n is called *solitary* if for all $m \neq n$ we have

$$\frac{\sigma(m)}{m} \neq \frac{\sigma(n)}{n}.$$

In other words, n is solitary if n is the only number m such that $\frac{\sigma(m)}{m} = \frac{\sigma(n)}{n}$. For example, we have

$$\frac{\sigma(10)}{10} = \frac{1+2+5+10}{10} = \frac{9}{5}.$$

Conjecture 34 (The Solitary Number Conjecture). *The number* 10 *is solitary.*

Conjecture 35 (Carmichael's Conjecture). *If $k = \phi(n)$ for at least one n, then $k = \phi(n)$ for at least two distinct input values of n.*



A.7 Conjectures About Diophantine Problems

CONJECTURE 36 (The Erdős–Moser Conjecture). *The only solution to the equation*

$$1^k + 2^k + \cdots + m^k = (m+1)^k$$

is $1 + 2 = 3$.

CONJECTURE 37 (Brocard's Problem). *The only integer solutions to the equation*

$$n! + 1 = m^2$$

are $4! + 1 = 5^2$, $5! + 1 = 11^2$, *and* $7! + 1 = 71^2$.

PROBLEM 38 (Existence of Perfect Euler Bricks). *An* ***Euler brick*** *is a rectangular cuboid whose edges and face diagonals all have integer lengths. Does there exist a* ***perfect*** *Euler brick; that is, an Euler brick whose space diagonal is also an integer?*

CONJECTURE 39 (The Fermat–Catalan Conjecture). *There are only finitely many solutions in the positive integers to the equation*

$$x^a + y^b = z^c$$

satisfying $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1$.

CONJECTURE 40 (Beal's Conjecture). *If* $a, b, c, x, y, z > 2$ *are integers satisfying the equation*

$$x^a + y^b = z^c,$$

then $\gcd(x, y, z) > 1$.

CONJECTURE 41 (Goormaghtigh Conjecture). *The only solution in integers* $x > y > 1$ *with* $m, n > 2$ *satisfying*

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}$$

are

$$\frac{5^3 - 1}{5 - 1} = \frac{2^5 - 1}{2 - 1} \qquad \textit{and} \qquad \frac{90^3 - 1}{90 - 1} = \frac{2^{13} - 1}{2 - 1}.$$

That is, the only two integers that are repunits of length > 3 *in two different bases are*

$$31 = (111)_5 = (11111)_2 \qquad \textit{and} \qquad 8191 = (111)_{90} = (1111111111111)_2.$$

CONJECTURE 42 (The *abc*-Conjecture). *Let* $a, b,$ *and* c *be relatively prime positive integers such that* $a + b = c$. *Let* $\operatorname{rad}(n)$ *denote the* radical *of* n, *the product of the distinct prime factors of* n. *For every* $\epsilon > 0$, *there exist only finitely many triples* (a, b, c) *such that*

$$c > \operatorname{rad}(abc)^{1+\epsilon}.$$

Conjecture 43 (Hall's Conjecture). *For any $\varepsilon > 0$, there exists a constant C_ε such that for any two positive integers x and y such that $x^3 \neq y^2$, we have*

$$|y^2 - x^3| > C_\varepsilon x^{\frac{1}{2}-\varepsilon}.$$

Conjecture 44 (The Casas–Alvero Conjecture). *Let $f(x)$ be a polynomial of degree n with integer coefficients. If for each $0 \leq k < n$ there is an integer r_k such that both $f(r_k) = 0$ and $f^{(k)}(r_k) = 0$, then $f(x)$ must be of the form $c(x-r)^n$.*

A.8 Conjectures About Representations of Numbers

Problem 45 (The congruent number problem). *Find a complete characterization of all rational numbers that appear as the area of a right triangle with rational sides.*

Conjecture 46 (Goldbach's Conjecture). *Every even number greater than 2 can be written as the sum of two primes.*

In light of Vieta's formulas for the roots of a quadratic polynomial, we can reformulate Goldbach's conjecture as follows: *For every even number $n > 2$ there exists a positive integer c such that both roots of the polynomial $x^2 + nx + c$ are primes.*

Conjecture 47 (Lemoine's Conjecture). *Every odd integer greater than 5 can be written in the form $p + 2q$, where p and q are primes.*

Conjecture 48 (The Erdős–Straus Conjecture). *Every rational number of the form $4/n$ can be written as the sum of three unit fractions: There are integers a, b, and c such that*

$$\frac{4}{n} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c}.$$

Conjecture 49 (Pollock's Conjecture). *Every natural number is the sum of five tetrahedral numbers.*

Conjecture 50 (The Sums of Three Cubes Conjecture). *Every natural number $n \not\equiv \pm 4 \pmod 9$ can be written as a sum of three cubes.*

For the following conjecture, observe that every integer $a > 1$ occurs only a finite number of times in Pascal's triangle. That is, the integer a can be represented in only finitely many ways as a binomial coefficient $a = \binom{n}{k}$. This follows immediately from the observation that any occurrences of the integer a in Pascal's triangle are within the first $a+1$ rows. However, David Singmaster observed that the *number of times* any integer occurs in Pascal's triangle seems to be bounded [Sin1971]. Indeed, currently there are no known numbers that occur more than eight times in Pascal's triangle, and the number 3003 is the only known number that occurs eight times.

Conjecture 51 (Singmaster's Conjecture). *There exists a finite number N such that every integer $a > 1$ occurs at most N times in Pascal's triangle.*



CONJECTURE 52 (Rudin's Conjecture). *The maximum number of squares that can occur in an arithmetic progression of length n is asymptotically given by $O(\sqrt{n})$. Furthermore, it is conjectured that the maximum is always attained in the arithmetic progression $24k+1$ for $0 \leq k \leq n-1$ [RUD1960].*

A.9 Conjectures About Iterative and Dynamical Processes

CONJECTURE 53 (Collatz's Conjecture). *Let f be the map that sends n to $n/2$ if n is even and sends n to $3n+1$ if n is odd. Starting from any number, one can reach the number 1 by iteratively applying f.*

The Euclid–Mullin sequence p_n is defined by setting $p_0 := 2$ and letting p_{n+1} be the least prime factor of

$$1 + \prod_{k=0}^{n} p_k.$$

CONJECTURE 54 (The Mullin–Shanks Conjecture). *Every prime occurs in the Euclid–Mullin sequence.*

CONJECTURE 55 (Gilbreath's Conjecture). *Let $(g_0(n))_{n\in\mathbb{N}}$ be the sequence of primes starting with $g_0(0) := 2$, $g_0(1) := 3$, and so on. Define*

$$g_{n+1}(k) := |g_n(k+1) - g_n(k)|$$

so that the sequence g_{n+1} consists of the absolute differences between consecutive entries in the sequence g_n. Then $g_n(0) = 1$ for every $n > 0$.

CONJECTURE 56 (The Lonely Runner Conjecture). *Suppose there are n runners who run with distinct constant speeds on a circular track of length 1. Each runner will, at some time, be at distance $1/n$ from all the others.*

CONJECTURE 57 (The Catalan–Dickson Conjecture). *Define the aliquot sequence of a number n by $s_0(n) := n$ and $s_{k+1}(n) = \sigma(s_k(n)) - s_k(n)$. That is, $s_{k+1}(n)$ is the sum of the proper divisors of $s_k(n)$. For every n, the sequence $(s_k(n))_{k\in\mathbb{N}}$ is eventually periodic.*

CONJECTURE 58 (The 196 Problem (Lychrel Numbers)). *For any integer n written in base 10, let n' be the number written in base 10 obtained by reversing the digits of n. Define the sequence (a_n) by $a_0 := 196$, and $a_{n+1} = a_n + a_n'$. Then none of the numbers in the sequence (a_n) is palindromic.*

References

[AGP1994] William Robert Alford, Andrew Granville, and Carl Pomerance. *There are infinitely many Carmichael numbers*. In: Annals of Mathematics. 2nd Ser. 139.3 (1994), pp. 703–722. DOI: 10.2307/2118576.

[And1994] George E. Andrews. *Number Theory*. Dover Books on Mathematics. Dover Publications, 1994. ISBN: 9780486682525.

[Aub1912] Léon Aubry. *Solution de quelques questions d'analyse indéterminée*. In: Sphinx-Œdipe 7 (1912), pp. 81–84. Consulted via a handwritten prepublication manuscript.

[Bal1929] Hoon Balakram. *On the values of n which make* $(2n)!/(n+1)!(n+1)!$ *an integer*. In: Journal of the Indian Mathematical Society 18 (1929), pp. 97–100.

[Bas1964] Hyman Bass. *K-theory and stable algebra*. In: Publications Mathématiques de l'IHÉS 22 (1964), pp. 5–60. DOI: 10.1007/BF02684689. URL: https://www.numdam.org/item/PMIHES_1964__22__5_0/.

[Ben1965] Paul Benacerraf. *What numbers could not be*. In: The Philosophical Review 74.1 (1965), pp. 47–73.

[BQ2003] Arthur T. Benjamin and Jennifer J. Quinn. *Proofs That Really Count: The Art of Combinatorial Proof*. Vol. 27. Dolciani Mathematical Expositions. Mathematical Association of America, 2003. ISBN: 9780883853337.

[Ber1934] B. Berggren. *Pytagoreiska trianglar*. Swedish. In: Tidskrift för elementär matematik, fysik och kemi 17 (1934), pp. 129–139.

[Ber1845] Joseph Bertrand. *Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme*. French. In: Journal de l'École Royale Polytechnique 18.30 (1845), pp. 123–140.

[BB1817] Bhāskarācārya and Brahmagupta. *Algebra, with Arithmetic and Mensuration, from the Sanscrit of Brahmegupta and Bháscara*. Trans. by Henry Thomas Colebrooke. London: John Murray, 1817. url: https://archive.org/details/algebrawitharith00brahuoft.

[BM2011] Carl B. Boyer and Uta C. Merzbach. *A History of Mathematics*. 3rd ed. Hoboken, NJ: John Wiley & Sons, 2011.

[BW1967] Henry G. Bray and Leroy J. Warren. *On the square-freeness of Fermat and Mersenne numbers*. In: Pacific Journal of Mathematics 22.3 (1967), pp. 563–564.

[Bri+1996] Robert C. Brigham et al. *A tiling scheme for the Fibonacci numbers*. In: Journal of Recreational Mathematics 28.1 (1996), pp. 10–16.

[Caj1918] Florian Cajori. *Origin of the Name "Mathematical Induction"*. In: The American Mathematical Monthly 25.5 (1918), pp. 197–201. issn: 00029890, 19300972.

[Car1570] Girolamo Cardano. *Opus novum de proportionibus numerorum, motuum, ponderum, sonorum, aliarumque rerum mensurandarum*. Basel: Henricpetri, 1570. url: https://archive.org/details/ARes45217.

[Car1912] Robert D. Carmichael. *On Composite Numbers P Which Satisfy the Fermat Congruence* $a^{P-1} \equiv 1 \pmod{P}$. In: The American Mathematical Monthly 19.2 (1912), pp. 22–27. doi: 10.2307/2972687.

[CW2003] Daniel Cass and Gerald Wildenberg. *Math Bite: A Novel Proof of the Infinitude of Primes, Revisited*. In: Mathematics Magazine 76.3 (2003), p. 203. doi: 10.1080/0025570X.2003.11953179.

[Cas2001] Lionel Casson. *Libraries in the Ancient World*. Yale University Press, 2001.

[Cay1876] Arthur Cayley. *Theorem on Partitions*. In: The Messenger of Mathematics 5 (1876), p. 188.

[Che1852] Pafnuty Chebyshev. *Mémoire sur les nombres premiers*. French. In: Journal de Mathématiques Pures et Appliquées 17 (1852), pp. 366–390.

[Cla1953] Marshall Clagett. *The Medieval Latin Translations From the Arabic of the Elements of Euclid, with Special Emphasis on the Versions of Adelard of Bath*. In: Isis 44.1/2 (1953), pp. 16–42. doi: 10.1086/348186.

[Cox1989] David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics. New York, NY: Wiley-Interscience, 1989. ISBN: 9780471506546.

[De 1838] Augustus De Morgan. *Induction (Mathematics)*. In: *The Penny Cyclopaedia of the Society for the Diffusion of Useful Knowledge*. Vol. 12. Charles Knight and Co., 1838, pp. 465–466. URL: https://archive.org/details/pennycyclopaedi18unkngoog.

[Ded1871] Richard Dedekind. *Über die Composition der binären quadratischen Formen*. In: Peter Gustav Lejeune Dirichlet. *Vorlesungen über Zahlentheorie*. Ed. by Richard Dedekind. 2nd ed. Supplement X. Braunschweig: Friedrich Vieweg und Sohn, 1871, pp. 380–497.

[Ded1888] Richard Dedekind. *Was sind und was sollen die Zahlen?* Braunschweig: Friedrich Vieweg und Sohn, 1888.

[Dic1919] Leonard Eugene Dickson. *History of the Theory of Numbers. Divisibility and Primality*. Vol. 1. Carnegie Institution of Washington Publication 256. See Chapter III, pp. 59–61, for Fermat, Leibniz, and Euler. Washington, DC: Carnegie Institution of Washington, 1919. URL: https://archive.org/details/historyoftheoryo01dick.

[Dio1910] Diophantus. *Diophantus of Alexandria: A Study in the History of Greek Algebra*. Ed. by Thomas Little Heath. Cambridge: Cambridge University Press, 1910.

[Erd1932] Paul Erdős. *Beweis eines Satzes von Tschebyschef*. In: Acta Scientiarum Mathematicarum (Szeged) 5 (1932), pp. 194–198.

[Erd1938] Paul Erdős. *Über die Reihe $\sum \frac{1}{p}$*. German. In: Mathematica (Zutphen) B 7 (1938), pp. 1–2.

[ES1975] Paul Erdős and John Lewis Selfridge. *The product of consecutive integers is never a power*. In: Illinois Journal of Mathematics 19.2 (1975), pp. 292–301. DOI: 10.1215/ijm/1256050816.

[Euc2015] Euclid. *The Thirteen Books of Euclid's Elements*. Trans. by Thomas Little Heath. Cambridge University Press, 2015. ISBN: 9781107480421.

[Eul1744] Leonhard Euler. *De Fractionibus Continuis Dissertatio*. In: Commentarii Academiae Scientiarum Petropolitanae 9 (1744). Eneström #E71, pp. 98–137.

[Eul1988] Leonhard Euler. *Introduction to Analysis of the Infinite: Book I*. Trans. by John D. Blanton. Springer-Verlag, 1988.

[Eva1969] Ronald J. Evans. *On Blocks of N Consecutive Integers*. In: The American Mathematical Monthly 76.1 (1969), pp. 48–49.



[Far1816] John Farey. *On a curious property of vulgar fractions*. In: The Philosophical Magazine and Journal 47.217 (1816), pp. 385–386.

[Far2009] Bakir Farhi. *An Identity Involving the Least Common Multiple of Binomial Coefficients and Its Application*. In: The American Mathematical Monthly 116.9 (2009), pp. 836–839.

[Fei1985] Lenore Feigenbaum. *Brook Taylor and the method of increments*. In: Archive for History of Exact Sciences 34.1 (1985), pp. 1–140.

[FS1987] Leonardo Fibonacci and Laurence E. Sigler. *The Book of Squares: An Annotated Translation into Modern English*. Boston: Academic Press, 1987, pp. xx, 124. isbn: 9780126431308.

[Fra1972] Peter Marshall Fraser. *Ptolemaic Alexandria*. Oxford: Clarendon Press, 1972. isbn: 9780198142782.

[Fur1955] Harry Furstenberg. *On the Infinitude of Primes*. In: The American Mathematical Monthly 62.5 (1955), p. 353. doi: 10.2307/2307043.

[Gau1986] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Ed. by William C. Waterhouse. Trans. by Arthur A. Clarke. Revised edition. New York & Berlin: Springer-Verlag, 1986. isbn: 9780387962542.

[Ger1909] Levi ben Gerson. *Sefer Maasei Choscheb: Die Praxis des Rechners*. Trans. by Gerson Lange. Original Hebrew text written in 1321. Translated to German by G. Lange. Frankfurt am Main: Louis Golde, 1909.

[Gol1956] Solomon W. Golomb. *Combinatorial Proof of Fermat's "Little" Theorem*. In: The American Mathematical Monthly 63.10 (1956), p. 718.

[Gre1671] James Gregory. *Letter to John Collins*. Published in the "Gregory Memorial Volume", ed. H.W. Turnbull (1939). Feb. 1671.

[The2023] The Guardian. *US teens say they have new proof for 2,000-year-old mathematical theorem*. In: (Mar. 2023). url: https://www.theguardian.com/us-news/2023/mar/24/new-orleans-pythagoras-theorem-trigonometry-prove.

[Guy2004] Richard K. Guy. *Unsolved Problems in Number Theory*. 3rd ed. Problem Books in Mathematics. New York: Springer-Verlag, 2004, pp. xviii+437. isbn: 9780387208602.

[Har+2008] Godfrey H. Hardy et al. *An Introduction to the Theory of Numbers*. 6th ed. Oxford: Oxford University Press, 2008. isbn: 9780199219865.

[Hea1981] Thomas Little Heath. *A History of Greek Mathematics: From Thales to Euclid*. Vol. 1. Reprint of the 1921 original. Dover Publications, 1981.

[Hem1961] Hemachandra Suri. *Chandonuśāsana*. Sanskrit. In: Bombay: Adhisthata Singhi Jain Sastra Sikṣāpiṭha, 1961, approx. 427–448. URL: https://archive.org/details/in.ernet.dli.2015.311060.

[Hen1896] Kurt Hensel. *Ueber den grössten gemeinsamen Theiler aller Zahlen, welche durch eine ganze Function von n Veränderlichen darstellbar sind*. In: Journal für die reine und angewandte Mathematik 116 (1896), pp. 350–356. ISSN: 0075-4102.

[Höl2001] Günther Hölbl. *A History of the Ptolemaic Empire*. Routledge, 2001.

[Hum1978] David Hume. *A Treatise of Human Nature*. Ed. by L. A. Selby-Bigge and P. H. Nidditch. 2nd ed. Oxford: Oxford University Press, 1978.

[Ism+2025] Dan Ismailescu et al. *Shifting Lucas Sequences Away from Primes*. In: INTEGERS: The Electronic Journal of Combinatorial Number Theory 25.A42 (2025), pp. 1–20. DOI: 10.5281/zenodo.15283739.

[JJ2024] Ne'Kiya Jackson and Calcea Johnson. *Five or Ten New Proofs of the Pythagorean Theorem*. In: The American Mathematical Monthly 131.9 (2024), pp. 739–752. DOI: 10.1080/00029890.2024.2370240.

[Joy1997] André Joyal. *Disks, Duality and Θ-Categories*. Unpublished manuscript. 1997. URL: https://ncatlab.org/nlab/files/JoyalThetaCategories.pdf.

[KP2012] Noel Harold Kaylor Jr. and Philip Edward Phillips, eds. *A Companion to Boethius in the Middle Ages*. Brill's Companions to the Christian Tradition 30. Leiden and Boston: Brill, May 2012. ISBN: 9789004183544. DOI: 10.1163/9789004225381.

[Kle1998] Israel Kleiner. *From Numbers to Rings: The Early History of Ring Theory*. In: Elemente der Mathematik 53.1 (1998), pp. 18–35. DOI: 10.1007/S000170050029.

[Kor1899] Alwin Korselt. *Problème Chinois*. French. In: L'Intermédiaire des Mathématiciens 6 (1899), pp. 142–143.

[Kum1852] Ernst Eduard Kummer. *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*. In: Journal für die reine und angewandte Mathematik 44 (1852), pp. 93–146. DOI: 10.1515/crll.1852.44.93.

[Lag1770] Joseph-Louis Lagrange. *Réflexions sur la résolution algébrique des équations*. In: Histoire de l'Académie Royale des Sciences et Belles-Lettres de Berlin (1770), pp. 123–192.

[Lag1771] Joseph-Louis Lagrange. *Démonstration d'un théorème nouveau concernant les nombres premiers*. In: Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin (1771).

[Lan1912] Edmund Landau. *Gelöste und ungelöste Probleme aus der Theorie der Primzahlverteilung und der Riemannschen Zetafunktion.* In: Jahresbericht der Deutschen Mathematiker-Vereinigung 21 (1912), pp. 208–228. URL: http://eudml.org/doc/145337.

[Leg1798] Adrien-Marie Legendre. *Essai sur la théorie des nombres.* Paris: Duprat, 1798. URL: https://openlibrary.org/books/OL24146260M/Essai_sur_la_th%C3%A9orie_des_nombres.

[Leh1933] Derrick H. Lehmer. *On Euler's totient function.* In: Bulletin of the American Mathematical Society 38 (1933), pp. 745–751. DOI: 10.1090/s0002-9904-1932-05521-5.

[Lei1863] Gottfried Wilhelm Leibniz. *Nova algebrae promotio.* In: *Leibnizens mathematische Schriften. Zweite Abtheilung: Die mathematischen Abhandlungen Leibnizens enthaltend.* Ed. by Carl Immanuel Gerhardt. Vol. 7. See pp. 180–181 for the discussion of Fermat's little theorem. Halle: H. W. Schmidt, 1863, pp. 154–189. URL: https://gallica.bnf.fr/ark:/12148/bpt6k111375x.

[Ler1905] Matyáš Lerch. *Zur Theorie des Fermatschen Quotienten* $\frac{a^{p-1}-1}{p} = q(a)$. German. In: Mathematische Annalen 60.4 (Dec. 1905), pp. 471–490. ISSN: 0025-5831. DOI: 10.1007/BF01561092.

[LeV1956a] William J. LeVeque. *Topics in Number Theory, Volume 1.* Reading, MA: Addison-Wesley, 1956. ISBN: 9780201042252.

[LeV1956b] William J. LeVeque. *Topics in Number Theory, Volume 2.* Reading, MA: Addison-Wesley, 1956. ISBN: 9780201042269.

[Lio1857] Joseph Liouville. *Généralisation d'un théorème de l'arithmétique indienne.* In: Journal de Mathématiques Pures et Appliquées. 2nd ser. 2 (1857), pp. 393–396. URL: https://www.numdam.org/item/JMPA_1857_2_2__393_0/.

[LP2003] Florian Luca and Štefan Porubský. *Fibonacci Integers.* In: Journal of Number Theory 101.2 (2003), pp. 220–240.

[Luc1878a] Édouard Lucas. *Sur la théorie des fonctions numériques simplement périodiques.* In: Nouvelle Correspondance Mathématique 4 (1878). Continuation of the article begun in volume 3 (1877), pp. 1–8, 33–40, 65–71, 97–102, 129–134, 225–228. URL: https://gdz.sub.uni-goettingen.de/id/PPN598948236_0004.

[Luc1878b] Édouard Lucas. *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier.* In: Bulletin de la Société Mathématique de France 6 (1878), pp. 49–54. DOI: 10.24033/bsmf.127.

[Mah1912] Mahāvīrācārya. *The Gaṇita-sāra-sangraha of Mahāvīrācārya: With English Translation and Notes*. Trans. by M. Rangacharya. Madras: Government Press, 1912. URL: https://archive.org/details/ganitasarasangra00maha.

[Mah1994] Michael Sean Mahoney. *The Mathematical Career of Pierre de Fermat, 1601–1665*. 2nd ed. Princeton, NJ: Princeton University Press, 1994. ISBN: 9780691036663.

[Man2006] Mihai Manea. *Some $a^n \pm b^n$ Problems in Number Theory*. In: Mathematics Magazine 79.2 (2006), pp. 140–145. DOI: 10.1080/0025570X.2006.11953392.

[Mar1961] Angelo Margaris. *Successor Axioms for the Integers*. In: The American Mathematical Monthly 68.5 (May 1961), pp. 441–444. DOI: 10.1080/00029890.1961.11989693.

[Moh1978] S. P. Mohanty. *The Number of Primes Is Infinite*. In: The Fibonacci Quarterly 16.4 (Aug. 1978), pp. 381–384. DOI: 10.1080/00150517.1978.12430316. URL: https://www.fq.math.ca/Scanned/16-4/mohanty.pdf.

[Neb2003] Gabriele Nebe. *Even lattices with covering radius $< \sqrt{2}$*. In: Beiträge zur Algebra und Geometrie 44.1 (2003), pp. 229–234.

[Nic1926] Nicomachus of Gerasa. *Introduction to Arithmetic*. Ed. and trans. by Martin Luther D'Ooge. The Macmillan Company, 1926. URL: https://archive.org/details/nicomachus-introduction-to-arithmetic.

[Now2015] Andrzej Nowicki. *Strong Divisibility and LCM-Sequences*. In: The American Mathematical Monthly 122.10 (2015), pp. 958–966. arXiv: 1310.2416.

[OR2012] Pascal Ochem and Michaël Rao. *Odd perfect numbers are greater than 10^{1500}*. In: Mathematics of Computation 81.279 (2012), pp. 1869–1877. DOI: 10.1090/S0025-5718-2012-02563-4.

[OEI2025] OEIS Foundation. *A006992: Bertrand primes*. The On-Line Encyclopedia of Integer Sequences. 2025. URL: https://oeis.org/A006992.

[Pan2007] Hao Pan. *A q-analogue of Lehmer's congruence*. In: Acta Arithmetica 128.4 (2007), pp. 303–318. DOI: 10.4064/aa128-4-1.

[Pas1665] Blaise Pascal. *Traité du triangle arithmétique, avec quelques autres petits traitez sur la mesme matière*. Paris: Guillaume Desprez, 1665.

[Pea1889] Giuseppe Peano. *Arithmetices principia, nova methodo exposita*. 1st ed. Turin: Fratres Bocca, 1889.

[Pol1846] Alphonse de Polignac. *Recherches nouvelles sur les nombres premiers.* In: Comptes Rendus de l'Académie des Sciences de Paris 23 (1846), p. 397.

[Pól1919] Georg Pólya. *Verschiedene Bemerkungen zur Zahlentheorie.* In: Jahresbericht der Deutschen Mathematiker-Vereinigung 28 (1919), pp. 31–40.

[Poo2007] Alf van der Poorten. *Fermat's Four Squares Theorem.* 2007. arXiv: 0712.3850 [math.NT].

[Pro1992] Proclus. *A Commentary on the First Book of Euclid's Elements.* Trans. by Glenn R. Morrow. Princeton University Press, 1992.

[Rie2016] Emily Riehl. *Category Theory in Context.* Aurora: Dover Modern Math Originals. Dover Publications, 2016. isbn: 9780486809038.

[Rot1964] Gian-Carlo Rota. *On the Foundations of Combinatorial Theory I. Theory of Möbius Functions.* In: Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete 2.4 (1964), pp. 340–368. doi: 10.1007/BF00531932.

[Rot1965] Andrzej Rotkiewicz. *Sur les nombres de Mersenne dépourvus de diviseurs carrés et sur les nombres naturels n, tels que* $n^2 \mid 2^n - 2$. French. In: Matematički Vesnik 2(17).31 (1965), pp. 78–80. issn: 0025-5165. url: http://eudml.org/doc/259515.

[Rud1960] Walter Rudin. *Trigonometric series with gaps.* In: Journal of Mathematics and Mechanics 9.2 (1960), pp. 203–227.

[Sag2020] Bruce E. Sagan. *Combinatorics: The Art of Counting.* Graduate Studies in Mathematics 210. Providence, RI: American Mathematical Society, 2020. doi: 10.1090/gsm/210.

[Sai2006] Filip Saidak. *A New Proof of Euclid's Theorem.* In: The American Mathematical Monthly 113.10 (2006), pp. 937–938. doi: 10.2307/27642094.

[Sie1988] Wacław Sierpiński. *Elementary Theory of Numbers.* Ed. by A. Schinzel. 2nd English Edition. Amsterdam: North-Holland, 1988. isbn: 9780444866622.

[Sil2012] Joseph H. Silverman. *A Friendly Introduction to Number Theory.* 4th ed. Pearson, 2012. isbn: 9780321816191.

[Sin1971] David Singmaster. *Research Problems: How Often Does an Integer Occur as a Binomial Coefficient?* In: The American Mathematical Monthly 78.4 (1971), pp. 385–386. doi: 10.1080/00029890.1971.11992769.

[Sti1884] Thomas Joannes Stieltjes. *Sur le caractère du nombre 2 comme résidu ou non-résidu quadratique.* In: Bulletin des Sciences Mathématiques et Astronomiques. 2nd ser. 8.1 (1884), pp. 175–176. url: https://www.numdam.org/item/BSMA_1884_2_8_1_175_1/.

[Tay1715] Brook Taylor. *Methodus incrementorum directa et inversa.* London: Typis Pearsonianis: prostant apud Gul. Innys, 1715.

[Van1991] Emmanuel A. Vantieghem. *On a congruence only holding for primes.* In: Indagationes Mathematicae 2.2 (1991), pp. 253–255. ISSN: 0019-3577.

[War1936] Morgan Ward. *Note on Divisibility Sequences.* In: Bulletin of the American Mathematical Society 42.12 (1936), pp. 843–845.

[War1948] Morgan Ward. *Memoir on Elliptic Divisibility Sequences.* In: American Journal of Mathematics 70.1 (1948), pp. 31–74. DOI: 10.2307/2371930.

[War1782] Edward Waring. *Meditationes Algebraicæ: Editio tertia, recensita et aucta.* 3rd ed. Cambridge: Typis Academicis excudebat J. Archdeacon/apud J. Nicholson, J. C. & F. Rivington, S. Crowder, H. Gardner & S. Hayes; Oxonii apud J. Fletcher, 1782, 389 + [15] addenda/corrigenda.

[Web1893] Heinrich Weber. *Leopold Kronecker.* In: Jahresbericht der Deutschen Mathematiker-Vereinigung 2 (1893), pp. 5–31.

[Wei1984] André Weil. *Number Theory: An Approach through History from Hammurapi to Legendre.* Boston: Birkhäuser, 1984. ISBN: 9780817631413. DOI: 10.1007/978-0-8176-4571-7.

[Wha2010] Junho Peter Whang. *Another Proof of the Infinitude of the Prime Numbers.* In: The American Mathematical Monthly 117.2 (2010), p. 181.

[Wie1909] Arthur Wieferich. *Zum letzten Fermatschen Theorem.* In: Journal für die reine und angewandte Mathematik 136 (1909), pp. 293–302. URL: http://eudml.org/doc/149315.

[Wri2013] Thomas Wright. *Infinitely many Carmichael numbers in arithmetic progressions.* In: Bulletin of the London Mathematical Society 45.5 (2013), pp. 943–952. DOI: 10.1112/blms/bdt013.