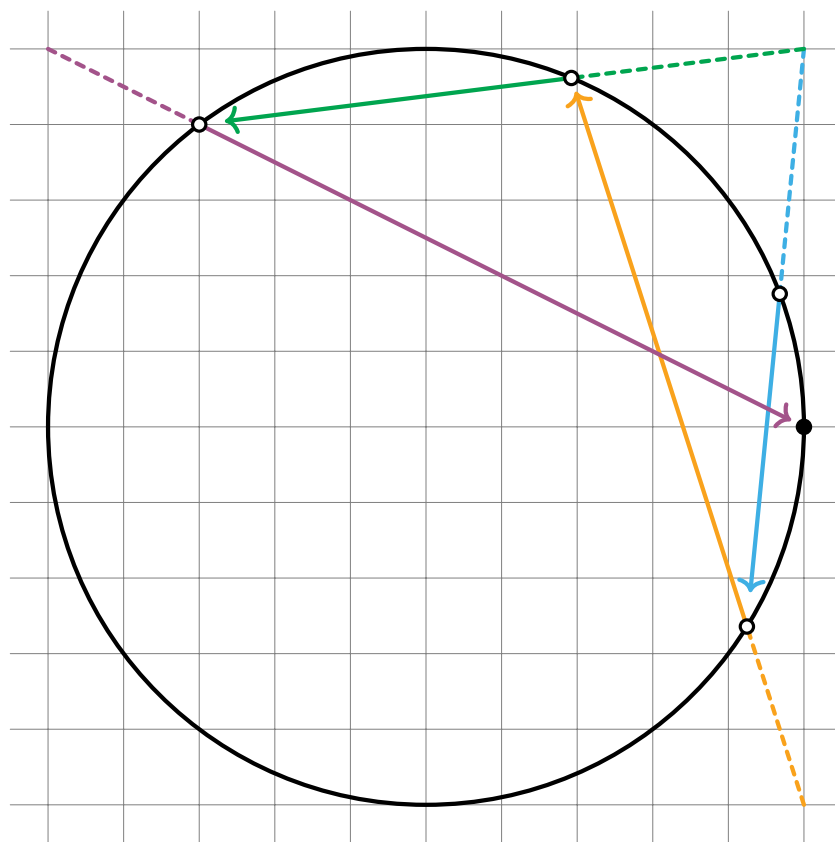


Johns Hopkins University

MATH 304

Egbert Rijke



Elementary Number Theory

Fall 2025

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 [Section 7.4](#) for a full explanation.

Contents

Contents	i
List of Figures	vii
Course Information	ix
Introduction	xi
 I The Logic of Numbers	 1
1 The Nature of Numbers	3
1.1 The Concept of Number Through History	3
1.2 Recursion and Induction	8
1.3 Addition of Natural Numbers	10
1.4 Arithmetic of Natural Numbers	12
1.5 Finite Sums and Products	13
1.6 Hemachandra's Counting Problem	15
Exercises	18
 2 Counting	 21
2.1 Hume's Principle	21
2.2 Equivalent Ways of Defining Bijections	25
2.3 Counting Bijections	26
2.4 Counting Subsets	28
2.5 The Binomial Theorem	33
2.6 The Inclusion-Exclusion Principle	34
Exercises	36
 3 The Integers	 41
3.1 Cyclic Sets	41
3.2 Maps Preserving Cyclic Structure	43

3.3	A Structural Definition of the Integers	45
3.4	Constructing the Integers from the Natural Numbers	48
3.5	Integer Arithmetic	50
	Exercises	53
II	From the Ancients to Fermat	55
4	Euclidean Division and Representability	57
4.1	Notation for Numbers	57
4.2	The Well-Ordering Principle of the Natural Numbers	59
4.3	Euclidean Division	60
4.4	The Representability Theorem	61
4.5	Combinatorial Applications	64
	Exercises	66
5	Linear Diophantine Equations	69
5.1	Divisibility	69
5.2	Ideals of Integers	72
5.3	The Ordering by Divisibility	73
5.4	Greatest Common Divisors	75
5.5	Euclid's Algorithm	77
5.6	Linear Diophantine Equations in Multiple Variables	80
	Exercises	82
6	The Rational Numbers	85
6.1	Integer Fractions	85
6.2	The Irrationality of Square Roots	88
6.3	Continued Fractions	89
6.4	Farey's Series of Fractions	94
6.5	A Structural Definition of the Rational Numbers	95
	Exercises	98
7	Pythagorean Triples	101
7.1	The Pythagorean Theorem	101
7.2	Euclid's Parametrization of the Pythagorean Triples	105
7.3	Rational Points on the Unit Circle	109
7.4	The Tree of Primitive Pythagorean Triples	112
7.5	Squares in Arithmetic Progressions	120
	Exercises	125

8	Infinite Descent	129
8.1	The Method of Infinite Descent	129
8.2	The Area of a Pythagorean Triangle is not a Square	130
8.3	The Unsolvability of $x^4 + y^4 = z^4$	131
8.4	The Nonexistence of Four Squares in an Arithmetic Progression	132
8.5	The Congruent Number Problem	133
8.6	Vieta Jumping	135
	Exercises	137
III	Congruences	139
9	Modular Arithmetic	141
9.1	The Congruence Relations	141
9.2	Equivalence Relations	146
9.3	Equivalence Classes and Residue Systems	149
9.4	The Integers Modulo n	151
9.5	The Multiplicative Order of an Integer Modulo n	153
	Exercises	157
10	Systems of Linear Congruences	159
10.1	Solving Linear Congruences	159
10.2	Solving Multiple Linear Congruences Simultaneously	161
10.3	The Chinese Remainder Theorem	162
10.4	A Method Suggested by Gauss	163
	Exercises	165
IV	Prime Numbers	167
11	Prime Numbers	169
11.1	The Fundamental Theorem of Arithmetic	169
11.2	The Infinitude of Primes	174
11.2.1	Saidak's Proof	175
11.2.2	Furstenberg's Proof, Following Cass–Wildenberg	175
11.2.3	Erdős's Proof	176
11.2.4	A Proof via the Stars-and-Bars Method	177
11.3	Fermat Primes	180
11.4	Legendre's Formula and Kummer's Theorem	181
11.5	Bertrand's Postulate	187
	Exercises	189

12	Multiplicative Functions	193
12.1	Perfect Numbers	193
12.2	Euler's Totient Function	196
12.3	Multiplicative Functions	199
12.4	The Möbius Function	201
12.5	Dirichlet Convolution	203
12.6	Dirichlet Inverses	204
	Exercises	207
V	Fermat's Discoveries Regarding the Primes	211
13	Fermat's Little Theorem and its Consequences	213
13.1	Fermat's Little Theorem	213
13.2	Euler's Theorem	217
13.3	Wilson's Theorem	218
13.4	Lucas's Theorem	219
13.5	The Quadratic Character of -1	220
13.6	The Infinitude of Primes Congruent to 1 Modulo Powers of 2	223
	Exercises	224
14	Fermat's Two-Squares Theorem	227
14.1	Numbers Representable as a Sum of Two Squares	227
14.2	Euler's Proof by Infinite Descent	232
	Exercises	233
VI	The Law of Quadratic Reciprocity	235
15	Polynomials	237
15.1	Polynomials with Integer Coefficients	237
15.2	Derivatives of Polynomials	239
15.3	Lagrange's Interpolation Theorem	241
15.4	Fixed Divisors of Integer Polynomials	245
	Exercises	247
16	Polynomial Congruences	249
16.1	Polynomial Congruences of Prime Moduli	249
16.2	Polynomial Congruences of Composite Moduli	251
16.3	Hensel's Lemma	252
	Exercises	254

17 Primitive Roots	255
17.1 Counting Elements of a Given Order Modulo a Prime	255
17.2 Primitive Roots	258
17.3 The Discrete Logarithm	260
17.4 The Moduli with Primitive Roots	261
17.4.1 Primitive Roots Modulo Odd Prime Powers	261
17.4.2 The Complete Characterization of Moduli with Primitive Roots	263
17.5 A Criterion for Congruences of Degree n	264
Exercises	267
18 Quadratic Residues	269
18.1 Quadratic Congruences	269
18.2 Quadratic Residues	271
18.3 Legendre Symbols	272
18.4 Euler's Criterion	274
18.5 Euler's Prime-Generating Polynomial	275
Exercises	278
19 Quadratic Reciprocity	281
19.1 The Quadratic Character of 2	281
19.2 The Statement of Quadratic Reciprocity	284
19.3 Gauss's Lemma	289
19.4 Eisenstein's Proof	290
Exercises	294
20 Conjectures in Elementary Number Theory	297
20.1 Conjectures About the Infinitude of Certain Classes of Primes	297
20.2 Conjectures About Exceptional Primes	299
20.3 Conjectures About Gaps Between the Primes	299
20.4 Conjectures About Conditions for Primality	300
20.5 Conjectures About Prime Decompositions	300
20.6 Conjectures About Arithmetic Functions	301
20.7 Conjectures About Diophantine Problems	301
20.8 Conjectures About Representations of Numbers	303
20.9 Conjectures About Iterative and Dynamical Processes	303
References	305

List of Figures

1	Euclid of Alexandria	xii
2	Pierre de Fermat	xiii
3	Leonhard Euler	xiv
4	Carl Friedrich Gauss	xv
1.1	Some Hemachandra tilings of a 1-by-19 grid	15
1.2	Hemachandra tilings of a 1-by-5 grid	16
2.1	A bijection	22
2.2	Not a bijection	23
2.3	Not a bijection	23
2.4	Composition of bijections	23
2.5	Pascal’s triangle	30
2.6	Parity in Pascal’s triangle	39
3.1	A bijection on a 12-element set.	41
3.2	A cyclic set with 12 elements	42
3.3	A cyclic-structure map from a 14-element set to a 7-element set.	43
3.4	Cyclic-structure maps	44
3.5	The infinite cyclic set of integers	45
3.6	The set of integers along the axis of the positive quadrant	48
6.1	Lattice points in a parallelogram	86
6.2	The Farey fractions with their adjacency relation	96
7.1	A diagram in the Jackson–Johnson proof	104
7.2	The Babylonian tablet Plimpton 322	105
7.3	Rational points on the unit circle	110
7.4	Vieta jumps between rational points on the unit circle	113
7.5	A forest.	116
7.6	The forest of rational points on the unit circle	117
7.7	The tree of primitive Pythagorean triples	119
7.8	Leonardo Pisano	120

7.9	Differences of squares congruent to 1 modulo 24	121
9.1	The 12-hour clock	142
11.1	The sieve of Eratosthenes	171
11.2	Example configurations of stars and bars	178
11.3	The 2-adic valuations of the numbers up to 15.	182
13.1	Golomb's proof of Fermat's Little Theorem	214
13.2	Carl Friedrich Gauss	220
14.1	Sums of two squares	228
14.2	Thue's Lemma	231
15.1	Example polynomial obtained by Lagrange interpolation	242
17.1	Doubling integers modulo 13	256
19.1	Eisenstein's proof of quadratic reciprocity	291

Course Information

Important Dates

- First lecture: August 26th.
 - First midterm: Friday September 26th
 - Fall break: 16-17 October
 - Second midterm: November 7th
 - Thanksgiving break: 24-28 November
 - Final lecture: December 2nd
 - Final exam: December 4th, 9-10:15AM.
- (i) Midterm 1 covers mathematical induction, counting with finite sets, the integers, Euclidean division, the representability theorem, divisibility, greatest common divisors, Euclid's algorithm, rational numbers, finite continued fractions, Pythagorean triples, infinite descent.
- (ii) Midterm 2 covers congruences, the Chinese remainder theorem, prime numbers, Legendre's formula, Kummer's theorem, arithmetic functions, Fermat's little theorem, Euler's theorem, Wilson's theorem, Lucas's theorem, the quadratic character of -1 , Fermat's two-square theorem.
- (iii) The final exam covers the entire course, including polynomials, polynomial congruences, primitive roots, quadratic residues, and quadratic reciprocity.

Grading

The course grade will be determined as follows:

- Homework: 60%

- Each exam (two midterms and final): 15% each

This adds up to a total of 105%, allowing students the opportunity to earn extra credit. The grading scale is as follows:

- $> 100\%$: A+
- 90–100%: A
- 80–90%: B
- 70–80%: C
- 60–70%: D
- $< 60\%$: F

If the median score for the class falls below a B, grades may be curved so that the median corresponds to a B. Any adjustments will be made consistently for all students.

Introduction

Number theory is the study of numbers, particularly the natural numbers (the numbers $0, 1, 2, \dots$ increasing indefinitely in increments of 1), the integers (the numbers $\dots, -2, -1, 0, 1, 2, \dots$), 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 inquiry 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 this course 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. An important aspect of the course is to learn how to make these intuitive ideas mathematically precise. Once we have developed a solid foundation, we will start building the edifice of number theory.

Concretely, we set out the following learning objectives for this course:

- Explain the structure of different number systems such as the natural numbers, the integers, the rational numbers, modular arithmetic, and the Gaussian integers, along with the methods of proof for properties involving each of them.
- Write mathematically rigorous proofs which demonstrate a clear progression of ideas and clearly state the principles of proof involved such as unique existence, mathematical induction, the well-ordering theorem, and the method of infinite descent.

- Solve some challenging number-theoretic problems, including selected contest-style problems.
- Apply some of the central theorems of elementary number theory, including Fermat's little theorem, Fermat's two-squares theorem, quadratic reciprocity, and Pell's equation.

A Short History of Number Theory

Number theory has a long history that dates back to antiquity. One of the earliest and most influential systematic treatments of mathematics is Euclid's *Elements* [Euc2015], written around 300 BCE in Alexandria. In this work, Euclid established several key results in number theory, including the infinitude of primes and the algorithm for finding the greatest common divisor, which bears his name.

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 groundbreaking contributions.

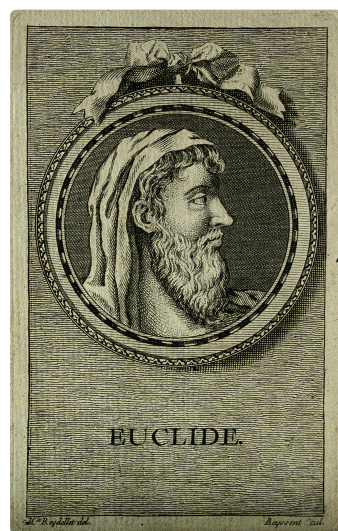


Figure 1: Euclid of Alexandria. Line engraving by S. Beyssent after Mlle. C. Reydell.

Pierre de Fermat (1607–1665) is often considered the founder of modern number theory [Mah1994; Wei1984]. He was a contemporary of Blaise Pascal and 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 geometry by applying the emerging methods of algebra and analytic geometry to classical geometric problems.

Fermat made several groundbreaking contributions to number theory. Among his most influential contributions 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, 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 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

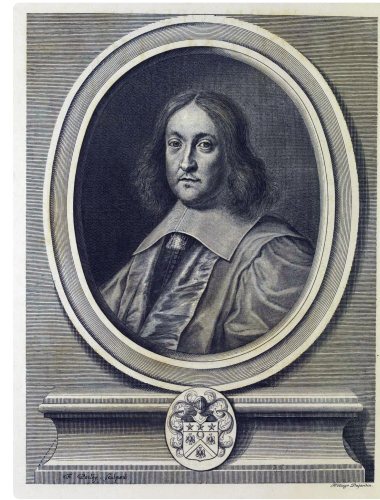


Figure 2: Pierre de Fermat. Engraving in *Oeuvres Mathématiques Diverses*.

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.

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

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

in which a and b are coprime, 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*

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

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*,

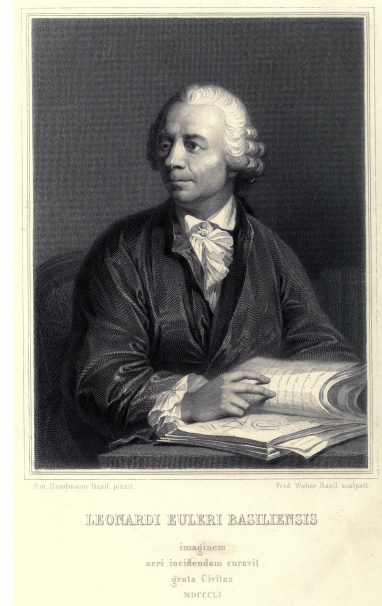


Figure 3: Leonhard Euler. Engraving by Friedrich Weber.

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.

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 a prime number is solvable. More precisely, it states that 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.



Figure 4: Carl Friedrich Gauss. Painting by Christian Albrecht Jensen.

A brief remark on the interesting etymology of the word theorem is in order. The English word *theorem* ultimately derives from the Ancient Greek $\theta\epsilon\omicron\rho\eta\mu\alpha$ (*theōrēma*), literally “that which is seen”, and by usage in classical philosophy as an “object of contemplation”. The verb $\theta\epsilon\omega\rho\epsilon\upsilon$ (*theōreîn*, “to observe, examine”) and the agent noun $\theta\epsilon\omega\rho\varsigma$ (*theōrós*, “spectator”) are close relatives, and ultimately give us both *theorem* and *theory* ($\theta\epsilon\omega\rho\alpha$).

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” ($\pi\theta\epsilon\sigma\iota\varsigma$, *hypóthesis*) and “proof” ($\pi\delta\epsilon\iota\chi\iota\varsigma$, *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.

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—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. A current effort led by Kevin Buzzard aims to formally verify Fermat’s Last Theorem.

Today, 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.

Overview of the Course

An integer a is said to *divide* an integer b if there exists an integer x such that $ax = b$. In other words, the number a divides b if the equation

$$ax = b$$

has a solution in the integers. In this case we say that a is a *divisor* of b , and we write $a \mid b$. This equation is the simplest example of a Diophantine equation. Diophantine equations are equations expressed using variables, integers, and arithmetic operations. The primary goal of solving a Diophantine equation is to find integers for each of the variables for which the equation is true. The study of Diophantine equations is a cornerstone of number theory.

For example, the equation

$$x^2 - 1 = 0$$

is a *quadratic Diophantine equation* with two solutions: $x = \pm 1$. One of the most well-known quadratic Diophantine equations is the equation

$$x^2 + y^2 = z^2,$$

which is a Diophantine equation in *three variables*. Its solutions are known as *Pythagorean triples*. These triples, such as (3, 4, 5) and (5, 12, 13), corresponds to the side lengths of right-angled triangles and have been studied since antiquity. Perhaps the most famous Diophantine equation is Fermat's equation

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

which has no solutions for nonzero integers x , y , and z when $n \geq 3$.

In this course, however, we will not go as far as proving Fermat's last theorem. The first target of this course is the Fundamental Theorem of Arithmetic, which establishes the prime numbers as the building blocks of all natural numbers. A number n is said to be prime if it has exactly one divisor $d \mid n$ such that $d \neq n$. If this is the case, then its unique divisor that is not equal to itself is the number 1. The Fundamental Theorem of Arithmetic asserts that any nonzero natural number n can be written as a product of primes

$$n = p_1 p_2 \cdots p_k,$$

and that this decomposition of n as a product of primes is unique up to the ordering of the primes.

In order to study divisibility properties more deeply, Gauss introduced in his *Disquisitiones Arithmeticae* the congruence relations of modular arithmetic. Following Gauss, we say that a number a is congruent to b modulo n , that is,

$$a \equiv b \pmod{n}$$

if $n \mid b - a$. Gauss used this new formalism to study quadratic residues, the Chinese Remainder theorem, and a variety of other problems in number theory, a thread we will also pick up on in this course.

Some of the most important theorems in this context are Fermat's Little Theorem, Euler's Theorem, and Wilson's Theorem. Fermat's theorem asserts that given any prime number p and any number a that is not divisible by p we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat's theorem is an important ingredient in primality tests: If the congruence $a^{n-1} \equiv 1 \pmod{n}$ is false then the number n cannot be prime. Testing this congruence for several values of a is a simple way of discovering that n is composite. This test is by itself, however, not conclusive because there are some numbers, the Carmichael numbers, that satisfy Fermat's congruence for all a relatively prime to n .

Euler's theorem is a sharper version of Fermat's Little Theorem, but it involves a new function: *Euler's totient function*. Euler's totient function ϕ counts the numbers less than n that are relatively prime to n , which means that they share no common divisors with n other than 1. For example, if p is a prime number then $\phi(p) = p - 1$ since every number $0 < n < p$ is relatively prime to p . Using the totient function, Euler's theorem asserts that the congruence relation

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

holds for any natural number n and any number a relatively prime to n . Euler's theorem has applications in cryptography.

Wilson's Theorem states that a number p is a prime number if and only if the congruence

$$(p - 1)! \equiv -1 \pmod{p}$$

holds. Here, the exclamation mark is used for the *factorial function*: The number $n!$ is the product $1 \cdot \dots \cdot n$ of all the numbers from 1 through n . Wilson's Theorem therefore gives another criterion for primality testing.

Euler's totient function is an example of an arithmetic function. Other such functions include the function $\tau(n)$, which returns the number of divisors of a number n , the function $\sigma(n)$, which returns the sum of the divisors of a number n , and the *Möbius function* μ . These and other functions have important relations between them, that we will investigate next. The Möbius inversion formula, for instance, states that if f and g are two arithmetic functions, then we have

$$f(n) = \sum_{d|n} g(d) \quad \text{if and only if} \quad g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right).$$

This result allows us to "invert" summation relations involving divisors.

The Möbius inversion is only one aspect of an algebraic structure that is present on the set of all arithmetic functions. Arithmetic functions can be multiplied by an operation known as *Dirichlet convolution*, which gives the set of arithmetic functions the structure of a *commutative ring*. Commutative rings are sets with operations of addition and multiplication satisfying the usual laws of arithmetic, and having such a structure on a set gives us a great opportunity to study them further. In our case, we get to study the primes more closely.

Experimentation is essential in number theory. By making lists of primes, lists of numbers that can be written as the sum of two squares or sums of three squares, lists of square-free numbers, and so on, you will start to gather data on numbers and perhaps start seeing patterns that might otherwise feel elusive. At the end of this section, we have produced two number grids with the numbers from 1 to 1584. The great masters all have endlessly created such lists to organize and discover patterns in various kinds of numbers. Feel free to print it as many times as you like, and color them according to your own rules, or whenever something in the course piques your interest. Some exercises throughout the course will ask you to color this number grid in a certain way.

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 in 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.

Online resources

There are plenty of ways to learn number theory and engage with communities of mathematicians and students online. First and foremost, *Wikipedia* has many excellent pages on topics from and related to number theory. The website *math.stackexchange.com* is dedicated to answering any kind of mathematical question, although more research-oriented questions are usually posed on *mathoverflow.net*. The website *artofproblemsolving.com* is dedicated to contest mathematics and the problem-solving techniques necessary to do well in competitions such as the International Mathematical Olympiad.

Furthermore, there are some popular channels on video-sharing sites such as YouTube, Twitch, and TikTok. We mention some of the most notable:

(i) Lectures:

- (a) *Richard Borcherds* is a Fields Medalist who has recorded many of his Berkeley lectures and made them available on YouTube. The topics of his lectures are always well-motivated and presented with great clarity.

(ii) Problem solving:

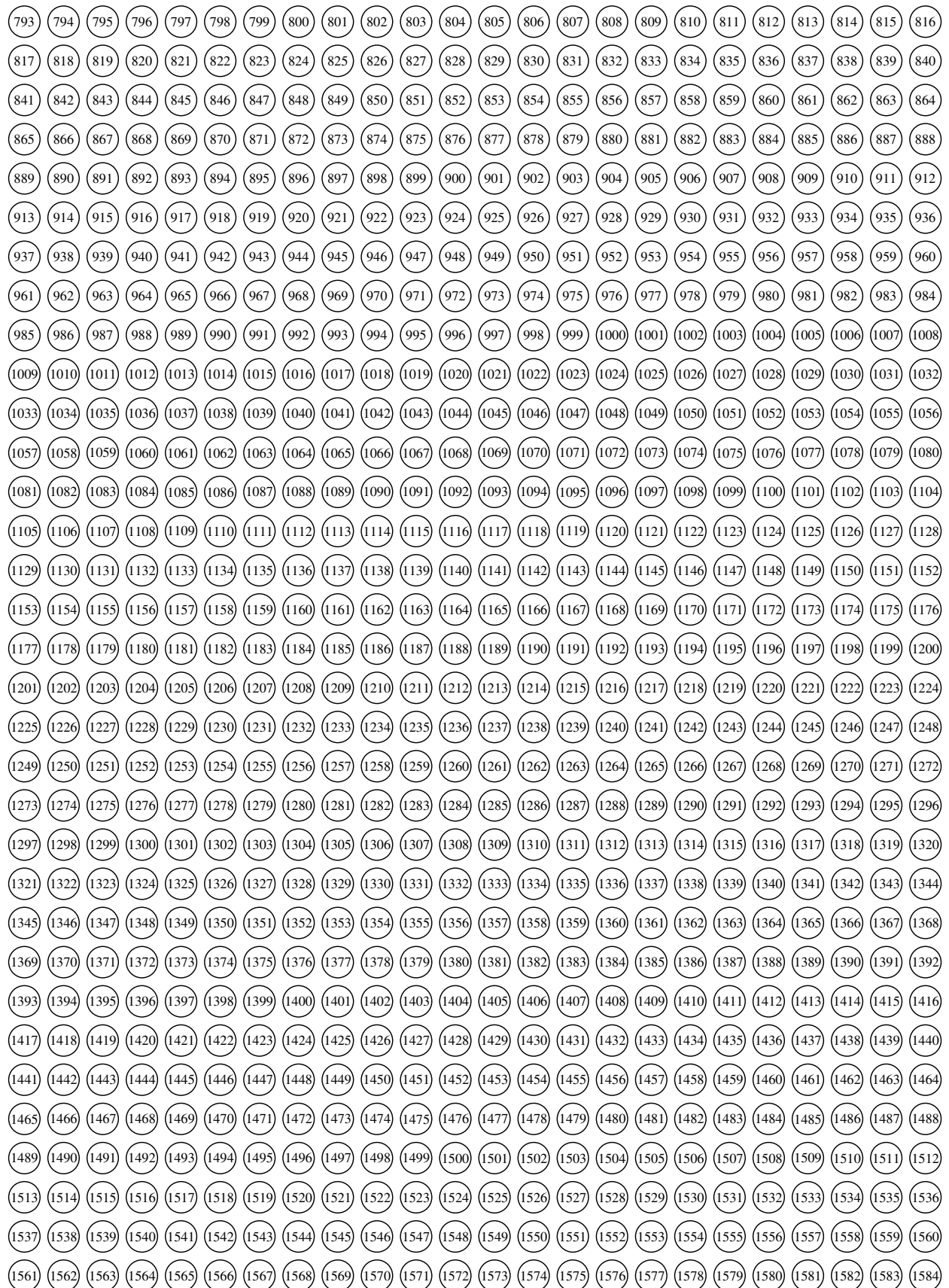
- (a) *Michael Penn* has an excellent YouTube channel in which he solves mathematical problems on a blackboard, at roughly the level of this course.
- (b) *vEnhance* (Evan Chen) is an IMO gold medalist and the author of the wonderful book *Euclidean Geometry in Mathematical Olympiads* [Che2016]. He streams live solves of Olympiad math problems on Twitch, and his videos are also available on YouTube.

- (c) *OmegaLearn* is Jonathan Huang’s YouTube channel focused on solving IMO problems. Some of his playlists dive deeper into specific techniques, such as Fermat’s method of infinite descent.
 - (d) *Blackpenredpen* is Steve Chow’s problem-solving channel, covering topics in calculus, algebra, and number theory.
- (iii) Mathematics for a broad audience:
- (a) *3Blue1Brown* explores a variety of topics related to computer science and mathematics using compelling visualizations.
 - (b) *Mathologer* is Burkard Polster’s YouTube channel for recreational mathematics. Many of his videos contain elegant visual proofs; his videos on Fermat’s Two-Square Theorem, the Quadratic Reciprocity Theorem, and Euler’s pentagonal theorem are especially worth watching.
 - (c) *Numberphile* is a long-running YouTube channel by Brady Haran, featuring mathematicians who explain a variety of mathematical phenomena, including topics in number theory. A closely related YouTube channel is *Tom Rocks Maths*, by Tom Crawford.
 - (d) *PeakMath* has an excellent series on the Riemann Hypothesis, called the *Riemann Hypothesis Saga*, in which they topics such as the Langlands program and the Birch–Swinnerton Dyer conjecture are made accessible.

You might also enjoy joining some Discord servers, such as the Art of Problem Solving (AoPS) Community Server, the Math Stack Exchange Discord, or the OmegaLearn Server. If you are interested in formalization of mathematics, using proof assistants such as Agda, Lean, or Rocq, you’ll also find thriving online communities that are focused on building large libraries of formalized mathematics. Lean’s *Natural Numbers Game* is especially worth trying, especially if you are new to induction and recursion. This set of lecture notes is currently being formalized in the *agda-unimath* library.

Finally, you might find generative AI tools such as ChatGPT useful in exploring mathematical topics. These tools are helpful because you can ask them to explain any topic that interests you, and the quality of their answers is quickly improving with each new version. Be careful, however, to ensure you understand the answers for yourself. AI-generated reasoning is not always reliable.

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



Part I

The Logic of Numbers

Chapter 1

The Nature of Numbers

Learning Objectives

In this chapter we discuss the trajectory through history that led to the modern definition of natural numbers, or the nonnegative integers. We embark on this journey in order to give a solid foundational footing to our subject. We will also make a first encounter with the idea of *structural* definitions; definitions of sets made entirely in terms of constants and functions. At the end of this chapter we will dive into a mathematical question posed by ancient Indian poets.

After having worked through this chapter, you will be able to:

- (i) Articulate the need for precise definitions of such basic objects as the natural numbers.
- (ii) Make recursive definitions.
- (iii) Write rigorous proofs by induction.

Learning induction and recursion is like learning to ride a bicycle: It is fun, it opens the door to proving lots of beautiful identities, and once it is learnt you will not unlearn it.

1.1 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. Our experience with numbers reveals patterns and properties that seem to always be true. For example, we quickly learn that it does not matter in which order we add two numbers: 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.

With Euclid, we see a shift away from 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 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 $S : \mathbb{N} \rightarrow \mathbb{N}$ such that every element of $\mathbb{N}$ can be reached by iteratively applying S to an 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 terminology, 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. 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 Cyclopaedia* 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 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 $h_n : A_n \rightarrow A_{n+1}$ for every natural number n .

The function f obtained in this manner satisfies the equations

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

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.

1.2 Recursion and Induction

When we say that the natural numbers are the numbers 0, 1, 2, . . . , we really mean that the natural numbers are generated from 0 and the *successor function* $n \mapsto n + 1$, which we also denote by S . As we saw in our exposition on the history of the concept of number, the definition of the natural numbers evolves around 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 1.2.1. The set $\mathbb{N}$ of natural numbers is a set equipped with an element 0 and a successor function $S : \mathbb{N} \rightarrow \mathbb{N}$, satisfying the following principle of *structural induction*: For any family of sets A_n indexed by the natural numbers equipped with

- (i) an element $a_0 \in A_0$,
- (ii) for each n a function $h_n : A_n \rightarrow A_{n+1}$,

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 equations

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

Thus, 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 $n + 1$. The last 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 define many further examples of recursive functions, is to iterate any function f on any set X . Here we pick A_n to be the set X (so it is not dependent on n), and we pick $h_n : X \rightarrow X$ to be the function f (again not dependent on n). In the following definition we give the precise definition of the n th iteration of f .

Definition 1.2.2. We define the n th 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 h is the *identity function*, which leaves all elements untouched, and the $(n+1)$ st iteration of h is obtained by applying f once more to the values of the n th iteration of h .

Notice that we made a choice in the definition of the $(n+1)$ 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 is a special case of structural induction.

Definition 1.2.3. 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,
- (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 .

Proofs by induction can thus be broken down into the following steps:

- (i) First identify the property $P(n)$ that you want to prove by induction. 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 1.2.4. *Consider a function $f : X \rightarrow X$ 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

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

This proves the base case. In the inductive step, we assume as our inductive hypothesis that

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

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 $f^{n+2}(y) = f(f^{n+1}(y))$ for all $y \in X$. This, together with the induction hypothesis, allows us to complete the proof:

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

1.3 Addition of Natural Numbers

Iterating functions is a basic operation that we can use to define many further operations. For example, addition is defined by iteratively adding 1 to a number m . In other words, addition is defined by iterating the successor function. The n th iteration of the successor function is denoted by S^n .

Definition 1.3.1. The *addition operation* $+$: $\mathbb{N} \rightarrow \mathbb{N} \rightarrow \mathbb{N}$ is a binary operation defined by iterating the successor function S :

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

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

For example $2 + 3$ is defined as $S(S(S(2)))$, which is equal to $S(S(3))$, which is equal to $S(4)$, which is equal to 5.

The operation $m, n \mapsto m + n$ satisfies the equalities

$$\begin{aligned} m + 0 &= m, \\ m + (n + 1) &= (m + n) + 1 \end{aligned}$$

by definition. However, these are the only equalities given to us via the computation rules of the strong induction principles. Other equalities, such as the equalities

$$\begin{aligned} 0 + n &= n, \\ (m + 1) + n &= (m + n) + 1 \end{aligned}$$

are still true, but require a short proof.

Proposition 1.3.2. *For any two natural numbers m and n we have*

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

Proof. The proof of both equalities is 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 1.3.3. *For any function $f : X \rightarrow X$, we have*

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

Proof. The proof is by induction on n . In the base case, we have $m + 0 = m$ and $f^0(x) = x$. Together, these identities give:

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

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

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

Here, we use that the equalities $m + (n + 1) = (m + n) + 1$ and $f^{n+1}(x) = f(f^n(x))$ hold by definition, and that the equality $f^m(f(x)) = f(f^m(x))$ holds by [Proposition 1.2.4](#). Together, these identities give:

$$\begin{aligned} f^{m+(n+1)}(x) &= f^{(m+n)+1}(x) = f(f^{m+n}(x)) = f(f^m(f^n(x))) \\ &= f^m(f(f^n(x))) = f^m(f^{n+1}(x)). \end{aligned} \quad \square$$

Corollary 1.3.4. *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 1.3.3](#), we obtain

$$(l + m) + n = S^n(S^m(l)) = S^{m+n}(l) = l + (m + n). \quad \square$$

Proposition 1.3.5. *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 1.3.2](#)

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

For the inductive step, assume that $m + n = n + m$. Then we use [Proposition 1.3.2](#) again to obtain:

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

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

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

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:

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

1.4 Arithmetic of Natural Numbers

Definition 1.4.1. The multiplication function $m, n \mapsto mn$ on the natural numbers is defined recursively by

$$\begin{aligned} m0 &:= 0, \\ m(n + 1) &:= mn + m. \end{aligned}$$

Proposition 1.4.2. *Multiplication of natural numbers satisfies the following laws:*

$$\begin{array}{ll}
 0n = 0, & m0 = 0, \\
 (m+1)n = mn + n, & m(n+1) = mn + m, \\
 1m = m, & m1 = m, \\
 l(m+n) = lm + ln, & (l+m)n = ln + mn, \\
 (lm)n = l(mn), & mn = nm.
 \end{array}$$

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

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

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

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

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

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

□

1.5 Finite Sums and Products

Definition 1.5.1. 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

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

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

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

Theorem 1.5.2. *For any natural number n we have*

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

Proof. Let $S_n := 0 + \cdots + n$, 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:

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

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

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

Theorem 1.5.3. *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

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

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. $\square$

1.6 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

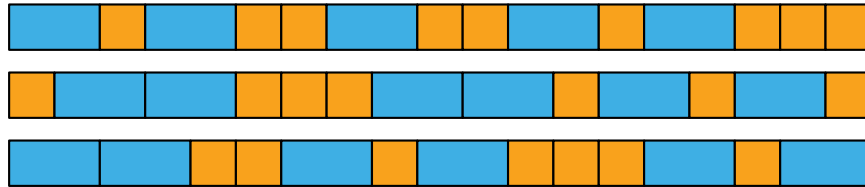


Figure 1.1: Three example tilings of a 1-by-19 grid using monominoes (1-by-1 tiles) and dominoes (1-by-2 tiles).

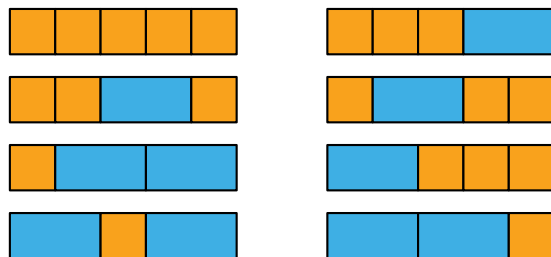


Figure 1.2: A list of all the possible tilings of a 1-by-5 grid using monominoes and dominoes.

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 1.1. 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 1.2 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 1.2, where we listed all the tilings of the 1-by-5 grid. There are five 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 1.6.1. The sequence F_n of *Fibonacci numbers* is defined by

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

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

- 1.1 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 (The Book of Squares)* [FS1987].

- 1.2 (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

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

- 1.3 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 $1 \leq n \leq 10$.
- 1.4 Gopa the grasshopper can jump either 5 or 8 steps. Find a recursive expression for the number of ways in which he can reach a spot n steps away, without jumping backwards, and determine in how many ways can he reach his favorite spot, 29 steps away.

Routine-Building Exercises

- 1.5 Prove the *formula for the difference of n th 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

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

1.6 Write T_n for the n th 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

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

1.7 Write T_n for the n th triangular number.

(a) The numbers

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

are called the *tetrahedral numbers*. 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

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

1.8 (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

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

1.9 (a) Prove *Nicomachus's Theorem*

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

(b) Prove that

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

1.10 Prove that

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

1.11 Prove that

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

Challenge Exercises

1.12 (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:

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

1.13 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.

1.14 Show that

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

1.15 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

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

1.16 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.

Chapter 2

Counting

2.1 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 $k!$.

We will begin by investigating more conceptually what mathematicians mean by counting, and work towards Hume’s principle. David Hume stated this principle in Part III of Book I of his *Treatise of Human Nature*, a philosophical work in which he set out to found a general “science of man” by applying empirical methods to understanding, the passions, and morals [Hum1978]. 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 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.

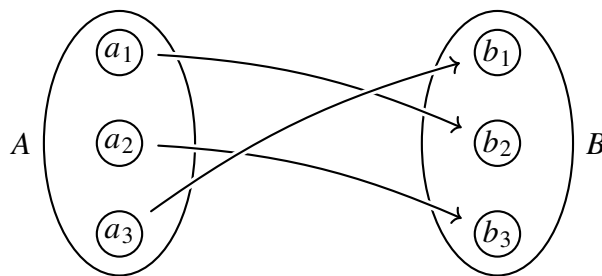


Figure 2.1: A bijection between two 3-element sets.

Definition 2.1.1. 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 element of A is labeled by *exactly one* number $0 \leq i < n$. By making sure that every element of A is labeled *at least once* we make sure that every element of A is accounted for, and by making sure that every element of A is labeled *at most once* we make sure to not overshoot the count.

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 2.1.2. A function $f : X \rightarrow Y$ 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 $[n] \cong X$.

In [Figure 2.4](#) 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 2.2](#), then any function $f : A \rightarrow B$ would necessarily repeat a value, while if B had more than 3 elements, as shown in [Figure 2.3](#), then no function $f : A \rightarrow B$ 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

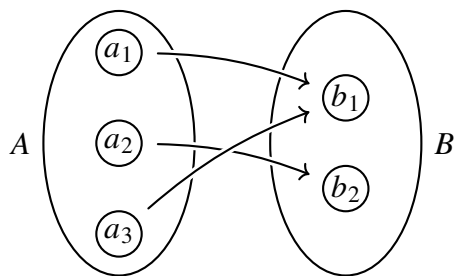


Figure 2.2: This function is not a bijection since b_1 is the value of the distinct elements a_1 and a_3 .

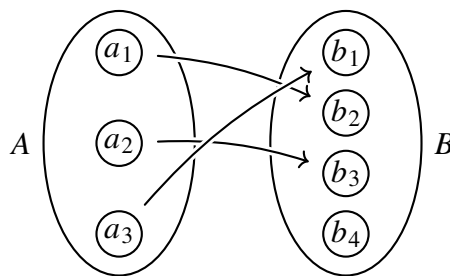


Figure 2.3: This function is not a bijection since b_4 is not the value of any element in A .

$g \circ f : A \cong C$. 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 $f : X \rightarrow Y$ is a bijection. The condition that a function $f : X \rightarrow Y$ 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 $f : X \rightarrow Y$ is a bijection. If we assume that $f : X \rightarrow Y$ 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.

Lemma 2.1.3. *Consider two bijections $f : A \cong B$ and $g : B \cong C$. Then the function $g \circ f$ defined by $a \mapsto g(f(a))$ 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 $g(f(x)) = z$.

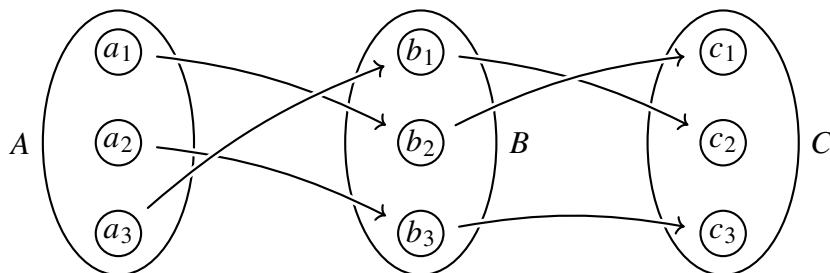


Figure 2.4: Composition of bijections between 3-element sets.

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 $f(x) = f(x')$. However, this shows that x and x' have the same value, which implies that $x = x'$ by the assumption that f is a bijection. This completes the proof that the element $x \in A$ is the only element of A mapping to z . $\square$

Lemma 2.1.4. *Consider an $(n + 1)$ -element set A equipped with an element a . Then the set*

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

is an n -element set.

Proof. Suppose $f : [n + 1] \rightarrow A$ is a bijection. Then there is a unique element $x < n + 1$ such that $f(x) = a$. We will first construct a bijection $h : [n + 1] \rightarrow [n + 1]$ such that $h(n) = x$. Once we have such a bijection, it follows that $f \circ h : [n + 1] \rightarrow A$ 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 $g := f \circ h : [n + 1] \rightarrow [n + 1]$ such that $g(n) = a$, it follows that the restriction of g to the set $[n]$ is a bijection from $[n]$ to $A \setminus \{a\}$. $\square$

Theorem 2.1.5 (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 direct, 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 $m + 1 = n' + 1 = n$. $\square$

2.2 Equivalent Ways of Defining Bijections

We have defined bijections to be functions $f : X \rightarrow Y$ 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 2.2.1. A function $f : X \rightarrow Y$ is said to be *surjective* if for every $y \in Y$ there exists an element $x \in X$ such that $f(x) = y$.

A function $f : X \rightarrow Y$ is said to be *injective* if for every $y \in Y$ there is at most one element $x \in X$ such that $f(x) = y$.

Thus, a function $f : X \rightarrow Y$ is surjective if every element of Y is a value of f . The function shown in [Figure 2.2](#) is an example of a surjective function.

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

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

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 2.3](#) 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. The concept of bijection is also closely related to the concept of *invertible function*.

Definition 2.2.2. A function $f : X \rightarrow Y$ is said to be *invertible* if there is a function $g : Y \rightarrow X$ such that

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

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 $f : X \rightarrow Y$ is an invertible function with inverse $g : Y \rightarrow X$, 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 2.2.3. *A function $f : X \rightarrow Y$ 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. $\square$

2.3 Counting Bijections

Recall that the set $[n]$ consists of all natural numbers strictly smaller than n . That is, the set $[n]$ is the set $\{0, \dots, n-1\}$. 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 $[n-1] \cong [n] \setminus \{x\}$

Definition 2.3.1. The *factorial function* $n \mapsto n!$ is defined recursively by

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

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 2.3.2. *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 $[n] \rightarrow [n]$, the empty function. This function is a bijection, because assuming an element of an empty set is an inherent contradiction.

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, because we can verify that the preimage $s_{y,n}^{-1}(z)$ is a singleton set for every $z \in [n+1]$. The preimage $s_{y,n}^{-1}(n)$ is the singleton set $\{y\}$; the preimage $s_{y,n}^{-1}(y)$ is the singleton set $\{n\}$, and the preimage $s_{y,n}^{-1}(x)$ is the singleton set $\{x\}$ otherwise.

Now we observe that the function

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

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 $[n+1]$. $\square$

To wrap up this section, we give a 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.

Theorem 2.3.3. *For any positive natural number n , we have the strict inequality*

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

Proof. For positive x , 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 theorem is obtained by rearranging. □

Remark 2.3.4. The strict lower bound for $n!$ given in [Theorem 2.3.3](#) 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 best 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.

2.4 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 . Predicates are propositions or conditions about indeterminate elements. For example, the assertion 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

$$0, 2, 4, 6, \dots$$

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 sets are conveniently defined by *set-builder notation*:

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

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

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

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 ourselves preferring expressions in natural language that convey the intended meaning more easily.

To avoid any complications of constructive logic, we shall assume that all predicates are decidable, meaning that for every predicate $P(x)$ on the indeterminate element x and for any element a , we can decide whether or not the property $P(a)$ holds. The typical predicates of concern in elementary number theory, until the real and complex numbers are considered, are indeed provably decidable.

Subsets of a finite set X are determined by a function $X \rightarrow \{0, 1\}$. 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 $f : X \rightarrow \{0, 1\}$ 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 immediately that if X is an n -element set, then the number of subsets of X is 2^n . To put it another way: In order to determine a subset of X , there are two possibilities for every element of X . It is either in the subset, or it isn't. Thus, there are 2^n combined possibilities determining distinct subsets.

Knowing that the total number of subsets of an n -element set is 2^n , we now turn to the question: How many k -element subsets are there of an n -element set? For example, the six 2-element subsets of the set $\{1, 2, 3, 4\}$ are

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

The binomial coefficients are introduced precisely to answer this question for general n and k .

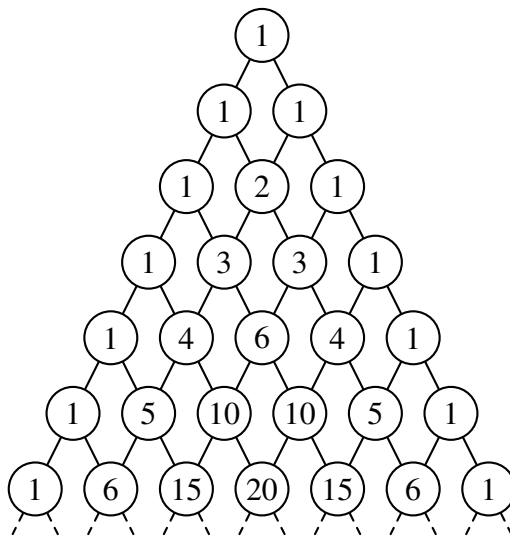


Figure 2.5: Pascal's triangle. Counting from 0 from the top, the k th entry in the n th row is the binomial coefficient $\binom{n}{k}$.

Definition 2.4.1. The *binomial coefficients* $\binom{n}{k}$ are defined recursively by

$$\begin{aligned} \binom{0}{0} &:= 1 & \binom{0}{k+1} &:= 0 \\ \binom{n+1}{0} &:= 1 & \binom{n+1}{k+1} &:= \binom{n}{k} + \binom{n}{k+1}. \end{aligned}$$

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 n th row from the top, we find the binomial coefficients $\binom{n}{k}$ for $0 \leq k \leq n$.

Theorem 2.4.2. Consider an n -element set S , and a natural number k . Then the number of k -element subsets of S is the binomial coefficient $\binom{n}{k}$.

Proof. Since the binomial coefficients are defined recursively, this theorem is best proven by induction on both variables.

If S has no elements and $k = 0$, then there is exactly one subset of S having k elements, the empty subset. This shows that the number of 0-element subsets of S is $\binom{0}{0}$.

If S has no elements, then there are no $(k+1)$ -element subsets of S , since any $(k+1)$ -element subset has at least one element, but S has no elements. This shows that the number of $(k+1)$ -element subsets of S is $\binom{0}{k+1}$.

If S has $n+1$ elements, then there is exactly one subset of S with no elements, the empty subset. This shows that the number of 0-element subsets of S is $\binom{n+1}{0}$.

If S has $n + 1$ elements, then S has at least one element x_0 . Now there are two classes of subsets having $(k + 1)$ elements: the subsets containing x_0 and the subsets not containing x_0 . A $(k + 1)$ -element subset of S containing x_0 is equivalently described as a k -element subset of the n -element set $S \setminus \{x_0\}$, because its $(k + 1)$ st element is the element x_0 . By the induction hypothesis, there are exactly $\binom{n}{k}$ such subsets. Furthermore, a $(k + 1)$ -element subset of S not containing x_0 is equivalently described as a $(k + 1)$ -element subset of the n -element set $S \setminus \{x_0\}$. By the induction hypothesis, there are exactly $\binom{n}{k+1}$ such subsets. Combining these two observations, we find that the number of $(k + 1)$ -element subsets of S is

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

Next, we turn to the question of proving that any product of k consecutive natural numbers in descending order

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

is divisible by $k!$. Such products are called *falling factorials*.

Definition 2.4.3. Let k and n be natural numbers such that $k \leq n$. The k th falling factorial of n is the number

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

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.

We will prove that the falling factorial n_k is divisible by the factorial $k!$ using a combinatorial argument, by first establishing that the falling factorials n_k count something called *k-permutations*. A k -permutation of n is essentially a list of length k of nonrepeating elements of the set $[n]$.

Definition 2.4.4. We define the set $P_k(S)$ of k -permutations of a set S recursively by:

- (i) The set $P_0(S)$ of 0-permutations of S is the set $\{*\}$ with one element.
- (ii) The set $P_{k+1}(S)$ of $(k + 1)$ -permutations of S is the set

$$\{(s, t) \mid s \in S, t \in P_k(S \setminus \{s\})\}$$

of pairs (s, t) consisting of an element in S and a k -permutation of the set $S \setminus \{s\}$.

Lemma 2.4.5. The number of k -permutations of an n -element set S is n_k .

Proof. The proof is by induction on k . There is exactly one 0-permutation of any n -element set. To see that the number of $(k + 1)$ -permutations of an n -element set is $n \cdots (n - k)$, note that such a $(k + 1)$ -permutation consists of a choice of an element of S , and a k -permutation on the remaining $n - 1$ -element set of elements. Thus, the number of $(k + 1)$ -permutations on an n -element set is n times the number of k -permutations on an $(n - 1)$ -element set, i.e., it is

$$n(n - 1) \cdots ((n - 1) - k + 1) = n(n - 1) \cdots (n - k). \quad \square$$

Proposition 2.4.6. *There is a bijection between the set of k -permutations of an n -element set S , and the set*

$$\{(A, f) \mid A \subseteq S, f : \{0, \dots, k - 1\} \cong A\}$$

of pairs (A, f) consisting of a subset $A \subseteq S$ and a bijection $\{0, \dots, k - 1\} \cong A$.

Proof. There is exactly one 0-permutation of any n -element set S , and likewise the set of empty subsets A of S equipped with a bijection $[0] \cong A$ also contains exactly one element: the empty subset equipped with the empty bijection.

For the inductive step, consider a $(k + 1)$ -permutation (s, t) of S , consisting of an element s and a k -permutation t of the set $S \setminus \{s\}$. By the induction hypothesis, the k -permutation t corresponds uniquely to a subset $A \subseteq S \setminus \{s\}$ equipped with a bijection $f : [n] \cong A$. Thus, the $(k + 1)$ -permutation (s, t) corresponds to the subset $B := A \cup \{s\} \subseteq S$, equipped with the bijection $g : [n + 1] \cong B$ given by $g(x) := f(x)$ for $x < n$ and $g(n) := s$. $\square$

Proposition 2.4.7. *The falling factorial n_k is divisible by $k!$.*

Proof. By [Proposition 2.4.6](#) there is a bijection between the set of k -permutations of the set $S := [n]$, and the set

$$\{(A, f) \mid A \subseteq S, f : \{0, \dots, k - 1\} \cong A\}.$$

These two sets therefore have the same number of elements. Thus, it follows that

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

showing that the left-hand side is divisible by $k!$. $\square$

Corollary 2.4.8. *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. By the previous proposition we have

$$\binom{n}{k} \cdot k! = n_k = \frac{n!}{(n - k)!}. \quad \square$$

2.5 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 result for 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 2.5.1. The binomial theorem. *In any number system, such as the natural numbers, the integers, the rational numbers, the reals, the complex numbers¹, 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

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

¹More 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

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

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*.

2.6 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:

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

Example 2.6.1. 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 2.6.2. Consider a 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

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

Exercises

Starter Exercises

- 2.1 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.
- 2.2 Prove that $2^n < n!$ for all $n \geq 4$.
- 2.3 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.

- 2.4 Find the first 20 positive integers that are not divisible by any Fibonacci number other than 1.
- 2.5 Define the *inclusion-exclusion sequence* a_n by $a_0 := 0$, $a_1 := 1$, and let a_{n+1} be the largest positive integer so that the number of positive integers $1 \leq x < a_{n+1}$ not divisible by any a_i for $2 \leq i \leq n$ is a_n . Determine the values for a_n for $1 \leq n \leq 10$.

Routine-Building Exercises

- 2.6 Show that the strict inequalities

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

hold for all $n \geq 1$.

- 2.7 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 .

- 2.8 *The hockey-stick identity.* Show that

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

- 2.9 *The Chu–Vandermonde identity.* Use the binomial theorem at the polynomial $(x+1)^m(x+1)^n$ to show that

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

2.10 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*.

2.11 Show that

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

2.12 Consider a set $A \subseteq \mathbb{N}$, and let the sets $\mathcal{P}_0(A)$ and $\mathcal{P}_1(A)$ be defined as follows:

$$\mathcal{P}_0(A) := \{S \subseteq A \mid \sum_{s \in S} s \text{ is even}\} \quad \text{and} \quad \mathcal{P}_1(A) := \{S \subseteq A \mid \sum_{s \in S} s \text{ is odd}\}.$$

Show that there is a bijection $f : \mathcal{P}_0(A) \rightarrow \mathcal{P}_1(A)$ 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

2.13 (a) Show that in the n th 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.

2.14 A *derangement* is a bijection $f : A \rightarrow A$ 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

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

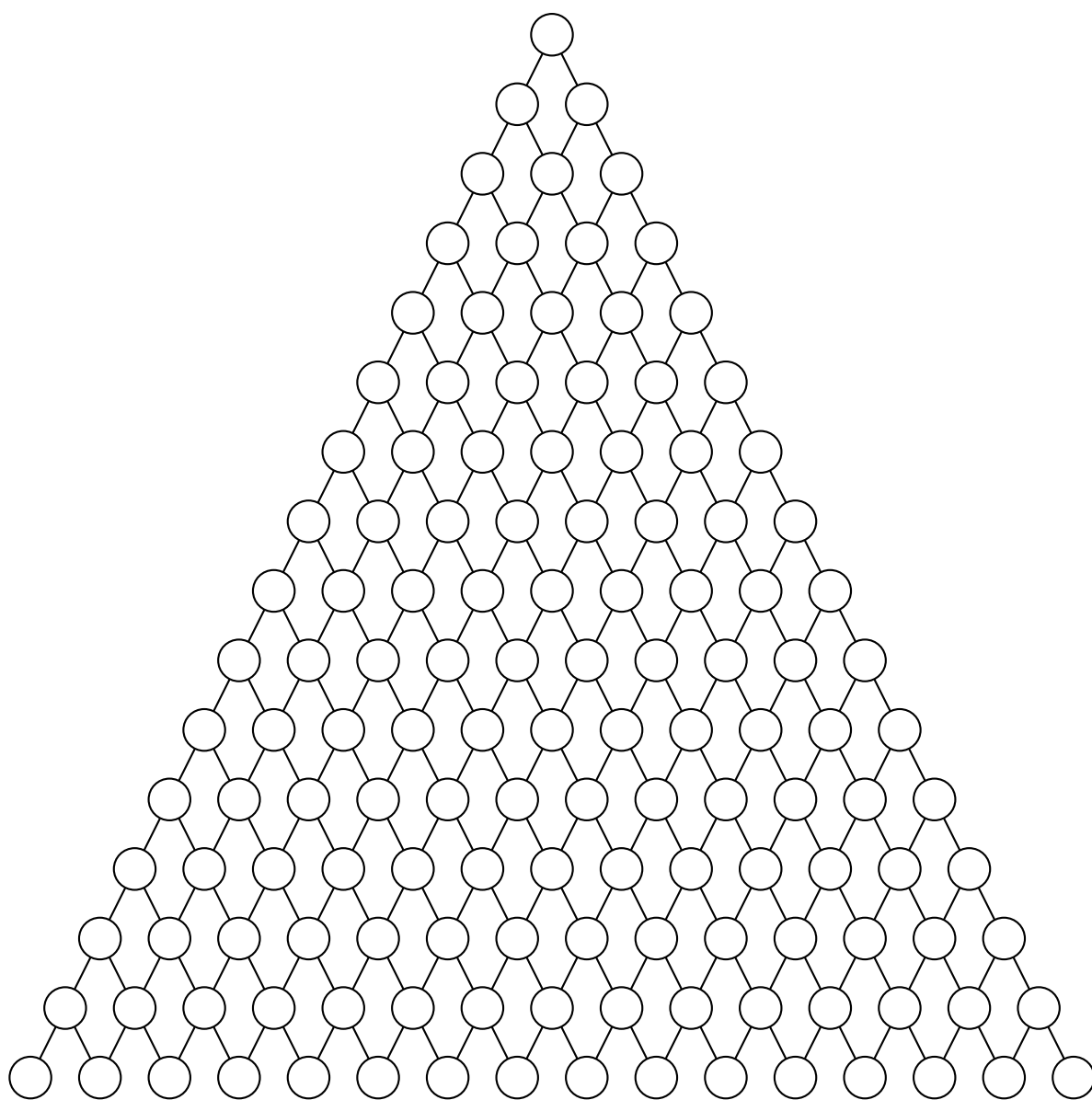


Figure 2.6: Shade all the circles in which the binomial coefficient is odd.

Chapter 3

The Integers

3.1 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 [Fermat's Little Theorem](#) and [Wilson's Theorem](#) use them.

When we map out a bijection $f : A \rightarrow A$ from a finite set A to itself by displaying an arrow between each element and its value under f , as we did in [Figure 3.1](#), 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

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

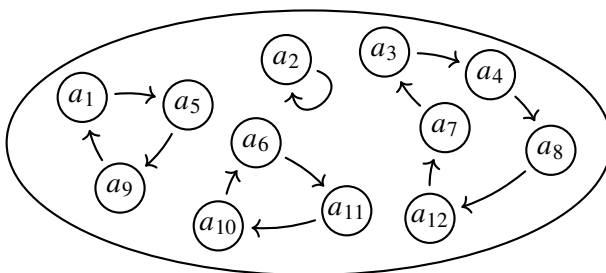


Figure 3.1: A bijection on a 12-element set.

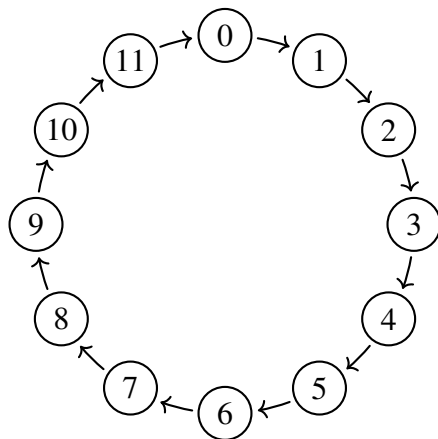


Figure 3.2: A cyclic set with 12 elements.

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 3.1.1. Consider a set X with a bijection $f : X \cong X$. Then we say that two elements $x, y \in X$ are *in the same orbit* of f if there exists a natural number k such that $f^k(x) = y$ or $f^k(y) = x$; that is, if one can be reached from the other by iteratively applying f .

An *orbit* of f is defined to be an inhabited subset $U \subseteq X$ so that all elements of U are in the same orbit.

The bijection on the 12-element set in Figure 3.1, for example, has three 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 3.2 we displayed an example of a cyclic set.

Definition 3.1.2. 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 3.1.3. 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 3.1.4. 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

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

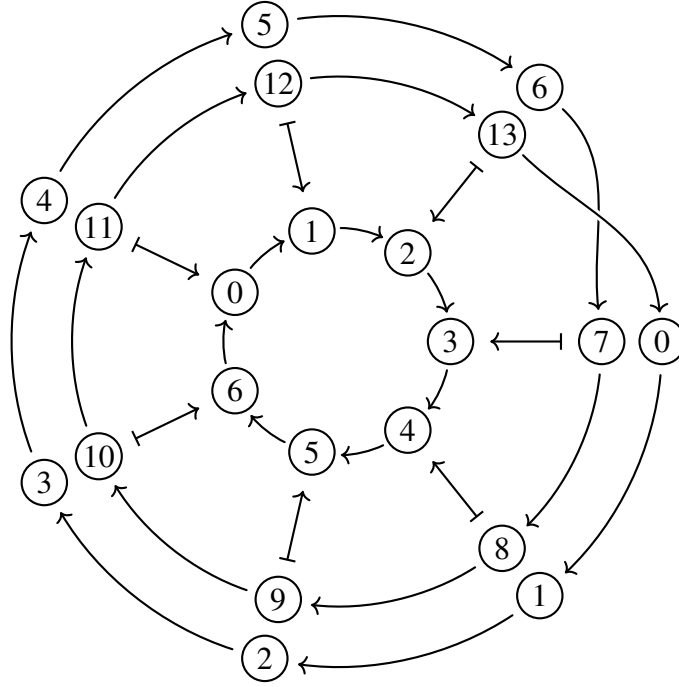


Figure 3.3: A cyclic-structure map from a 14-element set to a 7-element set.

This cyclic structure can be defined precisely without much trouble. However, to avoid cluttering these pages, we will postpone the definition until the [Euclidean Division Theorem](#).

3.2 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 3.2.1. Consider two cyclic sets (X, s) and (Y, t) . A map $f : X \rightarrow Y$ is said to be a *cyclic-structure map* if

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

for every $x \in X$. We will write $\text{hom}((X, s), (Y, t))$ 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

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

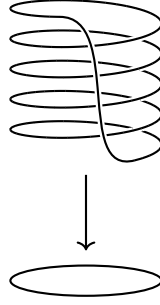


Figure 3.4: Cyclic-structure maps are defined by “winding” the source cyclic set around the target cyclic set.

holds trivially. In Figure 3.3 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 3.2.2. *Consider two cyclic sets (X, s) and (Y, t) with a cyclic-structure map $f : X \rightarrow Y$ 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 $s : X \rightarrow X$ restricts to a bijection

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

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 $f^{-1}(y)$. $\square$

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 $f, g : X \rightarrow Y$ 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:



Figure 3.5: The infinite cyclic set of integers.

Theorem 3.2.3. *Consider two cyclic sets (X, s) and (Y, t) . If the set*

$$\text{hom}((X, s), (Y, t))$$

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 $\text{hom}((X, s), (Y, t))$ to itself. To see that it has exactly one orbit, consider two cyclic-structure maps $f, g : X \rightarrow Y$, and let $x_0 \in X$. Then there exists an integer k such that

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

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 $h \mapsto t \circ h$. $\square$

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 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.

3.3 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 3.5. 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 3.3.1. The set of integers is specified to be a set $\mathbb{Z}$ equipped with an element $0 \in \mathbb{Z}$ and a 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 $f : \mathbb{Z} \rightarrow X$ 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*.

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 $f : A \rightarrow A$ 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 3.3.2. *For any bijection $f : A \cong B$ and any set X , there are bijections*

$$\begin{aligned} - \circ f &: (B \cong X) \cong (A \cong X) \\ f \circ - &: (X \cong A) \cong (X \cong B). \end{aligned}$$

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

$$g \circ f \circ f^{-1} = g \quad \text{and} \quad g \circ f^{-1} \circ f = g.$$

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

Definition 3.3.3. Consider a set X equipped with a bijection $f : X \cong X$. Then we define for each integer k the k th iteration of f by

$$\begin{aligned} f^0 &:= \text{id} \\ f^{S(k)} &:= f \circ f^k. \end{aligned}$$

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 .

Theorem 3.3.4 (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:

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

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 [Section 3.5](#) 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 $s : A \rightarrow A$, 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 $a \in A$, consider the unique integer b such that $S(b) = a$. Such an element is indeed uniquely determined since $S : \mathbb{Z} \rightarrow \mathbb{Z}$ is a bijection. Since $P(a)$ holds, it follows that $P(b)$ holds, so we find that $b \in A$. Thus, we define $t(a) := b$. 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 $f : \mathbb{Z} \rightarrow A$ such that

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

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 $\mathbb{Z} \rightarrow \mathbb{Z}$ satisfying the equations

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

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 $a \in \mathbb{Z}$. $\square$

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

Theorem 3.3.5. *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) there is a unique cyclic-structure preserving map from $(\mathbb{Z}, S)$ to (Y, t) .*

Proof. Our goal is to show by integer induction that every integer a is in the orbit of 0. Clearly 0 is in the same orbit as itself, 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 in the orbit of 0.

For the forward implication, there are two cases to consider. Either there is a natural number k such that $S^k(0) = x$ or there is a natural number k such that $S^k(x) = 0$. In the first case, it

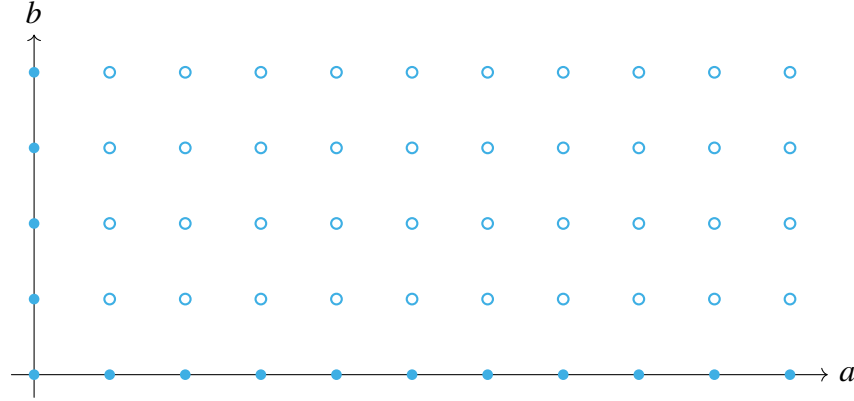


Figure 3.6: The set $\mathbb{Z}$ consists of the lattice points on the axes with natural number coordinates. Along the a -axis we find the nonnegative integers in their usual spots, while along the b -axis we find the nonpositive integers.

immediately follows that $S^{k+1}(0) = S(x)$. In the second case it follows that $S^k(S(x)) = S(0)$, which implies that $S^{k-1}(S(x)) = 0$. Thus we see that in both cases, $S(x)$ is in the orbit of 0.

For the reverse implication, there are again two cases to consider. Either there is a natural number k such that $S^k(0) = S(x)$ or there is a natural number k such that $S^k(S(x)) = 0$. In the first case, it follows that $S^{k-1}(0) = x$. In the second case, it follows that $S^{k+1}(x) = 0$. In both cases it follows that x is in the orbit of 0, completing the proof.

The final claim follows immediately by the integer recursion principle. $\square$

3.4 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 3.4.1. 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 $s : \mathbb{Z}_C \rightarrow \mathbb{Z}_C$ recursively on b by

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

Theorem 3.4.2. The successor function $s : \mathbb{Z}_C \rightarrow \mathbb{Z}_C$ is a bijection.

Proof. We prove that it is a bijection by constructing its inverse $t : \mathbb{Z}_C \rightarrow \mathbb{Z}_C$. 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 $s \circ t = \text{id}$ 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 $t \circ s = \text{id}$ 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. $\square$

Theorem 3.4.3. *The set $\mathbb{Z}_C$ equipped with the zero element $(0, 0)$ and the successor function s satisfies the specification of the integers in [Definition 3.3.1](#).*

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 $f : \mathbb{Z}_C \rightarrow X$ 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 $f : \mathbb{Z}_C \rightarrow X$ satisfying

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

It remains to show that this function f is unique. $\square$

Knowing that there is a set that meets the specification in [Definition 3.3.1](#), 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 3.3.1](#).

3.5 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 3.5.1. 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 b th 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 3.5.2. For any bijection $f : X \cong X$ with inverse f^{-1} , and for any $x \in X$, we have

$$\begin{aligned} f^{a+b}(x) &= f^b(f^a(x)) \\ f^{-a}(x) &= (f^{-1})^a(x). \end{aligned}$$

Proof. For the first identity, we will use [integer induction](#) 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 3.5.3. *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 3.5.4. We define the 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 3.5.5. *Multiplication of integers distributes from both sides over addition: For any three integers a , b , and c we have*

$$a(b+c) = ab+ac \quad \text{and} \quad (a+b)c = ac+bc.$$

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

3.1 Show that multiplication of integers is associative: For any three integers a , b , and c we have

$$(ab)c = a(bc).$$

3.2 Show that multiplication of integers is commutative: For any two integers a and b we have

$$ab = ba.$$

3.3 Show that multiplication with a nonzero integer a satisfies the cancellation law

$$ax = ay \quad \Rightarrow \quad x = y.$$

3.4 Prove that for any two integers a and b , either $b \leq a$ or $a \leq b$.

3.5 Suppose that X is a set equipped with an element $x_0 \in X$ and a bijection $h : X \cong X$. Show that the image of the unique map $f : \mathbb{Z} \rightarrow X$ determined by x_0 and h is a cyclic set.

3.6 Prove the identity

$$a^3 + b^3 + c^3 - 3abc = \frac{1}{2}(a + b + c)((a - b)^2 + (a - c)^2 + (b - c)^2)$$

and conclude that if $a + b + c = 0$, then we have

$$a^3 + b^3 + c^3 = 3abc.$$

Part II

From the Ancients to Fermat

Chapter 4

Euclidean Division and the Representability Theorem

4.1 Notation for 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 exist 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 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

	┌	┐	┑	┒	┓	└	┕	┖	┗
<	<┌	<┐	<┑	<┒	<┓	<└	<┕	<┖	<┗
<<	<<┌	<<┐	<<┑	<<┒	<<┓	<<└	<<┕	<<┖	<<┗
<<<	<<<┌	<<<┐	<<<┑	<<<┒	<<<┓	<<<└	<<<┕	<<<┖	<<<┗
⌞	⌞┌	⌞┐	⌞┑	⌞┒	⌞┓	⌞└	⌞┕	⌞┖	⌞┗
⌟	⌟┌	⌟┐	⌟┑	⌟┒	⌟┓	⌟└	⌟┕	⌟┖	⌟┗
┌	┌┌	┌┐	┌┑	┌┒	┌┓	┌└	┌┕	┌┖	┌┗
┌<	┌<┌	┌<┐	┌<┑	┌<┒	┌<┓	┌<└	┌<┕	┌<┖	┌<┗

Table 4.1: 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.

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 Coëdès. 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. The following mathematical theorem may not come as a surprise anymore: Any number $k > 1$ can serve as the basis of a numerical system. We will prove this theorem using the [Euclidean Division Theorem](#), which itself rests on the [Well-Ordering Principle of the Natural Numbers](#).

4.2 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 4.2.1 (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 . $\square$

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 4.2.2. *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 4.2.1](#). 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. $\square$

4.3 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 4.3.1 (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 4.2.2](#) 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

$$a = qd + r, \quad \text{and} \quad a = q'd + r'.$$

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. $\square$

4.4 The Representability Theorem

Theorem 4.4.1. *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 4.3.1](#), 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 theorem¹: 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 4.4.2. *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:

- (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

$$Q(n) := \forall_{(m \leq n)} P(m)$$

¹It should be noted that this digit appears last in the actual representation. It is the "ones digit" of the representation.

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. $\square$

Our earlier idea to prove the representability theorem can finally be made into a proof.

Proof of Theorem 4.4.1. 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 $\ell = (d_0, \dots, d_{l-1})$ 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 $(e_0, \dots, e_{l-1})$. Now we define the representation of $n + 1$ to be $(d_0, \dots, d_l)$, 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 $(d_1, \dots, d_{l-1})$ must be a representation of q , which is unique, thus completing the proof. $\square$

4.5 Some Combinatorial Applications of the Euclidean Division Theorem

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 4.5.1 (The Pigeonhole Principle). *Consider two natural numbers $m < n$, and a function $f : X \rightarrow Y$ 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 the .

Theorem 4.5.2. *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 . $\square$

Theorem 4.5.3. *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

$$0, a_1, a_1 + a_2, \dots, a_1 + \dots + a_n.$$

By [Theorem 4.5.2](#) it follows that 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. $\square$

Theorem 4.5.4. *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^n subsets of S , of which $2^n - 1$ are nonempty. By [Theorem 4.5.2](#) it follows that there are two distinct nonempty subsets of S such that the difference of their sums is divisible by m . $\square$

Exercises

Routine-Building Exercises

- 4.1 Prove that among any choice of $n + 1$ numbers from the set $\{1, \dots, 2n\}$, there will be two distinct numbers that sum to $2n + 1$.
- 4.2 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.

- 4.3 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 .

- 4.4 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 representation* of n .

Challenge Exercises

- 4.5 *Zeckendorf's representation theorem*. Show that 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 j th 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?

- 4.6 (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 5

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 $a_0, \dots, a_k$. The objective of a linear Diophantine equation such as the one above is to find integers $x_0, \dots, x_k$ for which the equation holds, to study conditions under which the equation has integer solutions, and ultimately to characterize all solutions.

5.1 Divisibility

The simplest linear Diophantine equation is the equation $ax = b$ in one variable x . The condition of its solvability leads to the concept of *divisibility*.

Definition 5.1.1. 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*.

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 $0x = 0$.

On the other hand, it follows that $0 \nmid 1$, and indeed that $0 \nmid b$ for any nonzero integer b .

- (iv) Similarly, but slightly more complicated, 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 .

If a is a nonzero integer, then there is always at most one solution to the equation $ax = b$. In other words, if a nonzero integer a divides an integer b , then its quotient is uniquely defined. On the other hand, we just saw that every integer is a solution to the equation $0x = 0$. The quotient is therefore not uniquely defined in this case. In the following lemma we remove this ambiguity by imposing an extra bound on the solution, that $|x| \leq |b|$. In the case where a is nonzero, then this condition is automatically satisfied, while in the case where $a = 0$ it imposes the zero solution.

Lemma 5.1.2. *Suppose that $a \mid b$. Then there is a unique integer x such that $|x| \leq |b|$ satisfying the equation $ax = b$. We will write a/b for this unique integer, which is called the quotient of b divided by a .*

Proof. There are two cases to consider: either $a = 0$ or $a \neq 0$. In the case where $a = 0$, having a solution $ax = b$ implies that $b = 0$. In this case, any x is a solution to the equation $ax = b$. However, only one solution x satisfies $|x| \leq b$, namely $x = 0$. Thus, the quotient $0/0$ is set to be 0.

If $a \neq 0$, then the function $x \mapsto ax$ is *injective*. This means that $ax = ay$ implies $x = y$. Consequently, there can be at most one integer x such that $ax = b$. Since we assumed that there is at least one such a solution, it follows that it is unique. Moreover, if $ax = b$, then $|x| \leq |a||x| = |ax| = |b|$, so x indeed satisfies the required bound. $\square$

Remark 5.1.3. While we have given an informal description, the 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 5.1.4. *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 5.1.5. *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

$$r : \{a, a+1, \dots, a+k-1\} \rightarrow \{0, 1, \dots, k-1\},$$

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 . $\square$

Another approach that often works well, which was suggested in class by Lucy, is a proof by contradiction. In proofs by contradiction, you assume the contrary and derive a contradiction. If the contrary is impossible, then the original claim must be true.

Proof by contradiction. Let's assume that there isn't a unique integer in the set

$$\{a, \dots, a+k-1\}$$

divisible by k . There are two cases to consider: Either there are no elements divisible by k , or there are at least two distinct elements divisible by k .

In the first case, by Euclid's division theorem there is a unique pair (q, r) such that $a = qk + r$, and since a is not divisible by k it must be the case that $r \neq 0$. Now it follows that $qk + k$ is an element in $\{a, \dots, a+k-1\}$, which is divisible by k , contrary to our assumption. Thus we conclude that it is not true that none of the elements of $\{a, \dots, a+k-1\}$ is divisible by k .

In the second case, let x and y be distinct elements of $\{a, \dots, a+k-1\}$ that are both divisible by k . Assume without loss of generality, that $x \leq y$. Then we have $0 \leq y - x < k$, and $y - x$ is divisible by k . By the Euclidean division theorem, we must have $y - x = 0$, which contradicts our assumption that x and y are distinct. $\square$

5.2 Ideals of Integers

Ideals are a concept from *ring theory*, which studies *rings*, which are sets equipped with addition, subtraction, and multiplication, satisfying the most familiar laws of arithmetic:

$$\begin{array}{ll} (x+y)+z = x+(y+z), & (xy)z = x(yz), \\ 0+x = x, & 1x = x, \\ x+0 = x, & x1 = x, \\ x-x = 0, & x(y+z) = xy+xz, \\ -x+x = 0, & (x+y)z = xz+yz, \\ x+y = y+x. & \end{array}$$

Rings such as the integers satisfy additionally the law $xy = yx$ of commutativity; such rings are called *commutative rings*. Notice that the set $\mathbb{N}$ of natural numbers isn't a ring, because it lacks subtraction. Sets with the structure of a ring appeared in David Hilbert's *Zahlbericht*, but their formal definition was first given by Emmy Noether in *Idealtheorie in Ringbereichen*, who was also the first to study them systematically.

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 $k, l \in \mathbb{Z}$. The subset $\{0\} \subseteq \mathbb{Z}$ satisfies the conditions of being an ideal in a trivial way; this ideal is called the *zero ideal*. 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 of this form.

Theorem 5.2.1. *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. $\square$

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.

5.3 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 5.3.1. 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 5.3.2. *The set of integers equipped with the divisibility relation $|$ is a preorder, and the set of natural numbers equipped with the divisibility relation $|$ 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

$$ax = a.$$

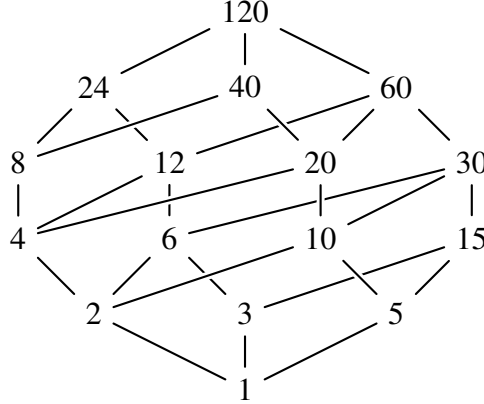
Therefore, it follows that $a | a$ for every integer a . To see that the divisibility relation is transitive, assume that $a | b$ and $b | c$. That is, assume that we have integers x and y such that $ax = b$ and $by = c$. Then it follows that

$$a(xy) = (ax)y = by = c.$$

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 $m | n$ and $n | m$; that is, that there are natural numbers x and y so that $mx = n$ and $ny = m$. By transitivity of divisibility it follows that $m(xy) = m$. $\square$

The diagram below is the *Hasse diagram* of the positive divisors of the number 120, a fragment of the poset of the natural numbers ordered by divisibility.



5.4 Greatest Common Divisors

Some preorders $(P, \leq)$ satisfy the property that for any two elements $a, b \in P$ there is a maximal element below both of them. This property can be formulated succinctly as follows: An element d is a maximal 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 maximal 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 5.4.1. 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 5.4.2. 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 5.4.3. 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 5.2.1](#). 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 $ax + by$. $\square$

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 common divisor of a and b must be 1. Such numbers are called *relatively prime* or *coprime*.

Definition 5.4.4. 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 5.4.5. 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 . $\square$

5.5 Euclid's Algorithm

Theorem 5.4.3 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 5.5.1. *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. $\square$

As an immediate corollary, we obtain:

Corollary 5.5.2. *If b is of the form $ka + 1$, then a and b are always relatively prime.*

Euclid's algorithm works by repeatedly using **Proposition 5.5.1**. For any pair (a, b) of integers, if $b \neq 0$ then there is a unique pair (q, r) such that $0 \leq r < |b|$ 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 5.5.1](#) 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 5.5.3. 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 the [Proposition 5.5.1](#), 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:

$$\begin{array}{ll} 154 = 1 \cdot 116 + 38 & \gcd(732, 578) = \gcd(116, 38), \\ 116 = 3 \cdot 38 + 2 & \gcd(732, 578) = \gcd(38, 2), \\ 38 = 19 \cdot 2 + 0 & \gcd(732, 578) = \gcd(2, 0). \end{array}$$

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 5.5.4. 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,

$$2 = 116 - 3 \cdot (154 - 116) \quad \Rightarrow \quad 2 = 4 \cdot 116 - 3 \cdot 154.$$

Furthermore, 116 is a linear combination of 154 and 578, giving us that

$$2 = 4 \cdot (578 - 3 \cdot 154) - 3 \cdot 154 \quad \Rightarrow \quad 2 = 4 \cdot 578 - 15 \cdot 154.$$

In the final step, we use that 154 is a linear combination of 732 and 578 to find

$$2 = 4 \cdot 578 - 15 \cdot (732 - 578) \quad \Rightarrow \quad 2 = -15 \cdot 732 + 19 \cdot 578.$$

Theorem 5.5.5. Every nonempty list $(q_0, \dots, q_N)$ 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

$$\{(q_0, \dots, q_N) \mid q_i \geq 1 \text{ for all } 0 \leq i \leq N\} \cong \{(a, b) \mid \gcd(a, b) = 1 \text{ and } a > b > 0\}.$$

5.6 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 5.6.1. *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 5.4.3](#) we defined $\gcd(a, b)$ to be the unique natural number d such that $(a) + (b) = (d)$. Such a natural number exists by [Theorem 5.2.1](#). 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 . $\square$

As an immediate corollary of the previous theorem, we note that:

Corollary 5.6.2. *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 5.6.3. *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

$$x = x_0 + bk, \quad \text{and} \quad y = y_0 - ak.$$

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 5.6.4. *Suppose that $ax_0, by_0 = c$ is a solution to the Diophantine equation*

$$ax + by = c.$$

Then every solution is of the form

$$x = x_0 + \frac{b}{d}k, \quad \text{and} \quad y = y_0 - \frac{a}{d}k.$$

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 . □

Exercises

Starter Exercises

- 5.1 Show that $a^n - 1$ is divisible by $a - 1$ for every integer a .
- 5.2 Show that $a^n + b^n$ is divisible by $a + b$ for any odd natural number n .
- 5.3 Show that if $a \mid b$, then $d \mid b/a$ if and only if $ad \mid b$.
- 5.4 Suppose that $a \mid b$ and $b \mid c$. Show that if $d \mid b/a$ then $d \mid c/a$.
- 5.5 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 natural number n .
- 5.6 Show that if a and ab are n th powers, then so is b .
- 5.7 Show that if ab and ac are squares, then so is bc .
- 5.8 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.
- 5.9 Show that $a \mid bc$ if and only if $a/\gcd(a, b) \mid c$.
- 5.10 Show that if $\gcd(a, b) = 1$ and both $a \mid c$ and $b \mid c$, then $ab \mid c$.
- 5.11 Show that $\gcd(a^n, b^n) = \gcd(a, b)^n$.
- 5.12 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 .
- 5.13 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

- 5.14 (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 .
- 5.15 (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 $(a^3 - a)/6$.
- 5.16 Show that $a^5 - a$ is divisible by 30 for every integer a .
- 5.17 (a) Show that any three consecutive Fibonacci numbers are pairwise relatively prime.
 (b) Find all n for which the five consecutive Fibonacci numbers $F_n, \dots, F_{n+4}$ are pairwise relatively prime.
- 5.18 Show that $n! + 1$ and $(n + 1)! + 1$ are relatively prime for all nonzero n .

Challenge Exercises

- 5.19 (a) Prove the *Fibonacci addition formula* $F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n$.
 (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) $d \mid F_{n+m}$.
 (c) Show that the Fibonacci sequence preserves and reflects divisibility: We have $m \mid n$ if and only if $F_m \mid F_n$.
- 5.20 (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 n th integer relatively prime to 24, then the number

$$\frac{a^2 - 1}{24}.$$

is the n th generalized pentagonal number.

- (c) Let $0 \leq a \leq b \leq c$ 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.
- 5.21 (a) Consider two positive integers a and n such that $\gcd(a, n) = 1$. Prove that there is a natural number m such that

$$n \mid \sum_{k=0}^m a^k.$$

Hint: Apply the pigeonhole principle.

- (b) Find the least positive integer m such that

$$7 \mid \sum_{k=0}^{m-1} 10^k = \underbrace{11 \cdots 1}_m.$$

- 5.22 Show that if x and y are positive integers such that xy divides $x^2 + y^2$, then $x = y$.
 5.23 Show that $2^m - 1$ and $2^n + 1$ are relatively prime, provided that m is odd.

5.24 Show that

$$\binom{a+k}{k} \mid \text{lcm}(a, a+1, \dots, a+k).$$

5.25 Show that in any subset of $n+1$ integers from the set $\{1, \dots, 2n\}$, 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 $\{1, \dots, 2n\}$?

5.26 (Erdős) Show that any set of $n+1$ integers chosen from an interval $a, \dots, a+2n-1$ must contain a pair of relatively prime integers.

5.27 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 n th power for $n > 1$ [ES1975].

5.28 Find all solutions to the equation

$$3^m - 2^n = 1.$$

5.29 An interval $a, \dots, a+n-1$ 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 $a, \dots, a+n-1$ 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, $\dots$, 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 6

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 the [Euclidean Division Theorem](#) which establishes division with remainder, and in the previous chapter we introduced the basics of the theory of integer divisibility. 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*.

6.1 Integer Fractions

Definition 6.1.1. 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*.

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 6.1.2. Two integer fractions $\frac{a}{b}$ and $\frac{c}{d}$ are considered the *same* if

$$ad - bc = 0.$$

We will write $\frac{a}{b} = \frac{c}{d}$ to mean that $\frac{a}{b}$ and $\frac{c}{d}$ are the same in this sense.

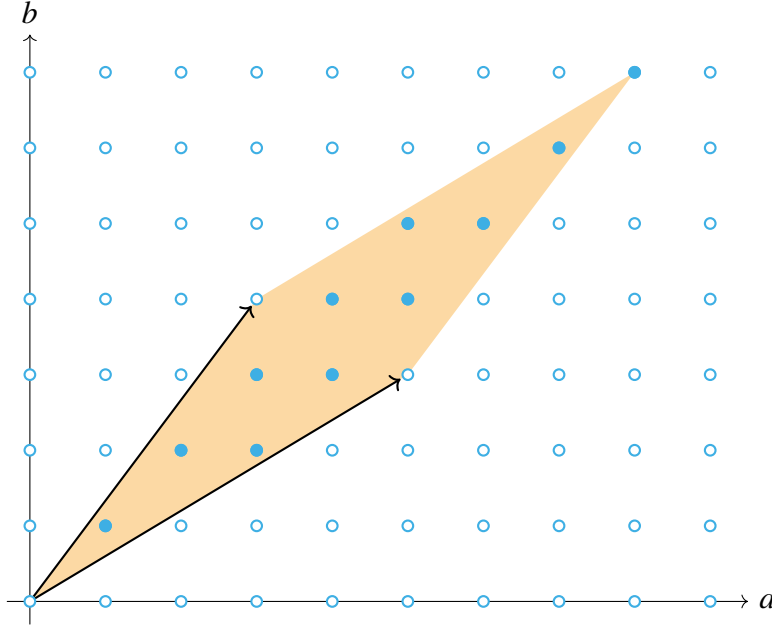


Figure 6.1: There are 11 lattice points in the parallelogram spanned by $(3, 4)$ and $(5, 3)$, not including the points $(0, 0)$, $(3, 4)$, and $(5, 3)$. This number is equal to the quantity $4 \cdot 5 - 3 \cdot 3$, and it is also equal to the number of reduced integer fractions between $\frac{3}{4}$ and $\frac{5}{3}$ with denominators not exceeding 7.

More generally, the quantity $|bc - ad|$ is a measure for how far apart the fractions $\frac{a}{b}$ and $\frac{c}{d}$ are. Assuming that the inequality $\frac{a}{b} \leq \frac{c}{d}$ holds so that $bc - ad \geq 0$, we will show in [Theorem 6.4.4](#) that the number

$$bc - ad$$

counts the number of fractions $\frac{a}{b} < \frac{s}{t} < \frac{c}{d}$ such that the denominator t does not exceed $b + d$. Indeed, if $\frac{a}{b} = \frac{c}{d}$ then there should be no fractions strictly between $\frac{a}{b}$ and $\frac{c}{d}$, as is signified by the number $bc - ad = 0$.

The quantity $|bc - ad|$ is also the area of the parallelogram spanned by (a, b) and (c, d) . Moreover, there are exactly k lattice points in this parallelogram, excluding multiples of (a, b) and (c, d) .

Theorem 6.1.3. *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

$$a' := \frac{a}{\gcd(a, b)} \quad \text{and} \quad b' := \frac{b}{\gcd(a, b)}.$$

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 5.4.5](#). 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 $a = c$. $\square$

By the remarks preceding the previous theorem, we should expect there to be exactly one reduced integer fraction in the interval strictly between $\frac{a}{b}$ and $\frac{c}{d}$, provided that

$$bc - ad = 1.$$

This is the content of the following theorem.

Theorem 6.1.4. *Suppose that $\frac{a}{b}$ and $\frac{c}{d}$ are reduced integer fractions satisfying*

$$bc - ad = 1.$$

Then there is exactly one reduced integer fraction $\frac{a}{b} < \frac{s}{t} < \frac{c}{d}$, namely the mediant

$$\frac{a + c}{b + d}.$$

Proof. First, we claim that the function

$$t \mapsto \frac{a + tc}{b + td}$$

defines a bijection from the positive reduced integer fractions to the reduced integer fractions in the interval of integer fractions strictly between $\frac{a}{b}$ and $\frac{c}{d}$. Indeed, if $\frac{p}{q}$ is a positive reduced integer fraction, then its value under this map is

$$\frac{qa + pc}{qb + pd}.$$

$\square$

Definition 6.1.5. Integer fractions can be added, subtracted, and multiplied according to the following rules:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}, \quad \text{and} \quad \frac{a}{b} \frac{c}{d} = \frac{ac}{bd}.$$

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 6.1.6. *Addition, subtraction, multiplication and inversion of integer fractions satisfies the axioms of a field:*

$$\begin{array}{ll} (x + y) + z = x + y + z & (xy)z = x(yz) \\ x + y = y + x & xy = yx \\ 0 + x = x & 1x = x \\ x - x = 0 & xx^{-1} = 1 \\ & x(y + z) = xy + xz. \end{array}$$

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.

6.2 The Irrationality of Square Roots

Theorem 6.2.1. *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 assumption that n is not a perfect square. $\square$

6.3 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:

$$\frac{193}{71} = 2 + \frac{1}{1 + \frac{20}{51}}.$$

Continuing this way, we find that

$$\frac{193}{71} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{4 + \frac{1}{2}}}}}}.$$

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 6.3.1. A *finite (simple) continued fraction* is an expression of the form

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots + \frac{1}{q_n}}}},$$

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 $[q_0, q_1, q_2, \dots, q_n]$.

Infinite continued fractions are infinite expressions of the form

$$q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots}}}.$$

A more compact notation for infinite continued fractions is $[q_0, q_1, \dots]$. The numbers q_i in a continued fraction $[q_0, q_1, \dots]$ are called the *partial quotients*.

Carl Friedrich Gauss had the following elegant notation for continued fractions, which is not widely used anymore:

$$q_0 + \mathbf{K}_{i=1}^{\infty} \frac{1}{q_i} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots}}}.$$

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 Pell's 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 6.3.2. *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 the [Euclidean Division Theorem](#) there is a unique 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 $[q_1, q_2, \dots, q_n]$. It follows that $[q, q_1, \dots, q_n]$ 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 $\frac{a}{b}$. $\square$

Definition 6.3.3. Consider a continued fraction $[q_0, \dots, q_n]$ or $[q_0, q_1, \dots]$. The continued fractions

$$\frac{a_i}{b_i} := [q_0, \dots, q_i]$$

are called the *convergents* of the continued fraction.

The first few convergents of a continued fraction $[q_0, q_1, \dots]$ are

$$\frac{a_0}{b_0} = \frac{q_0}{1}, \quad \frac{a_1}{b_1} = \frac{q_0 q_1 + 1}{q_1}, \quad \frac{a_2}{b_2} = \frac{q_0 q_1 q_2 + q_0 + q_2}{q_1 q_2 + 1}, \quad \dots$$

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:

$$\frac{a_0}{b_0} = \frac{2}{1}, \quad \frac{a_1}{b_1} = \frac{3}{1}, \quad \frac{a_2}{b_2} = \frac{8}{3}, \quad \frac{a_3}{b_3} = \frac{11}{4}, \quad \frac{a_4}{b_4} = \frac{19}{7}, \dots$$

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 $[q_0, \dots, q_n, x]$, 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 $[q_0, \dots, q_n, x]$ 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 n th convergent of the continued fraction $[q_0, q_1, \dots]$. 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

$$[q_0, \dots, q_n, r] = [q_0, \dots, q_n + \frac{1}{r}].$$

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 explicitly use the list of numbers $q_0, \dots, q_n$ in our notation for the numerator and denominator of $[q_0, \dots, q_n]$: They will be denoted by

$$a_{q_0, \dots, q_n} \quad \text{and} \quad b_{q_0, \dots, q_n}.$$

Or, to establish a more compact notation, if we write $\mathbf{q} = q_0, \dots, q_n$, then we can write $a_{\mathbf{q}}$ and $b_{\mathbf{q}}$ for the numerator and denominator of the continued fraction $[\mathbf{q}] = [q_0, \dots, q_n]$.

Theorem 6.3.4 (Recurrence Theorem for Convergents). *Define the numbers $a_{\mathbf{q}}$ and $b_{\mathbf{q}}$ for every finite continued fraction $[\mathbf{q}] := [q_0, \dots, q_n]$ by list recursion as follows:*

$$\begin{aligned} a_q &:= q & a_{q,r} &:= rq + 1, & a_{\mathbf{q},r,s} &:= sa_{\mathbf{q},r} + a_{\mathbf{q}}, \\ b_q &:= 1 & b_{q,r} &:= r, & b_{\mathbf{q},r,s} &:= sb_{\mathbf{q},r} + b_{\mathbf{q}}. \end{aligned}$$

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 $[\mathbf{q}] = [q_0, \dots, q_n]$ 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

$$\frac{a_{\mathbf{q},r,s,t}}{b_{\mathbf{q},r,s,t}} = \frac{ta_{\mathbf{q},r,s} + a_{\mathbf{q},r}}{tb_{\mathbf{q},r,s} + b_{\mathbf{q},r}} = \frac{a_{\mathbf{q},r,s} + \frac{a_{\mathbf{q},r}}{t}}{b_{\mathbf{q},r,s} + \frac{b_{\mathbf{q},r}}{t}} = \frac{(s + \frac{1}{t})a_{\mathbf{q},r} + a_{\mathbf{q}}}{(s + \frac{1}{t})b_{\mathbf{q},r} + b_{\mathbf{q}}} = \frac{a_{\mathbf{q},r,s+\frac{1}{t}}}{b_{\mathbf{q},r,s+\frac{1}{t}}} = [\mathbf{q}, r, s + \frac{1}{t}].$$

This completes the proof, since $[\mathbf{q}, r, s + \frac{1}{t}] = [\mathbf{q}, r, s, t]$. □

Theorem 6.3.5 (Determinant Identity for Convergents). *For any continued fraction $[\mathbf{q}, r] = [q_0, \dots, q_n, r]$ 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 6.3.6. *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 6.3.7. *Consider an infinite continued fraction $[q_0, q_1, \dots]$ and define the sequences a_n and b_n recursively by*

$$\begin{aligned} a_0 &:= q_0, & a_1 &:= q_1q_0 + 1, & a_{n+2} &:= q_{n+2}a_{n+1} + a_n, \\ b_0 &:= 1, & b_1 &:= q_1, & b_{n+2} &:= q_{n+2}b_{n+1} + b_n. \end{aligned}$$

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

$$\frac{a_{n+1}}{b_{n+1}} - \frac{a_n}{b_n} = \frac{(-1)^n}{b_nb_{n+1}}.$$

Example 6.3.8. 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 $(n + 2)$ nd Fibonacci number and $b_n = F_{n+1}$ is the $(n + 1)$ 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 formula now gives us that

$$\varphi = \frac{1 + \sqrt{5}}{2}.$$

This number is known as the *golden ratio*. The continued fraction $[1, 1, \dots]$ shows that the convergents

$$\frac{F_{n+1}}{F_n}$$

determine increasingly accurate approximations of the golden ratio.

6.4 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 $\mathcal{F}_n$, we must have

$$\frac{s}{t} = \frac{a + c}{b + d}.$$

Definition 6.4.1. The *mediant* of two reduced integer fractions $\frac{a}{b}$ and $\frac{c}{d}$ is the integer fraction

$$\frac{a}{b} \nabla \frac{c}{d} := \frac{a + c}{b + d}.$$

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:

$$\frac{a}{b} \nabla \frac{c}{d} = \frac{b}{b+d} \frac{a}{b} + \frac{d}{b+d} \frac{c}{d}.$$

Proposition 6.4.2. *The mediant satisfies the following laws:*

$$\begin{aligned} x \nabla y &= y \nabla x, \\ x \nabla x &= x, \\ \lambda x \nabla \lambda y &= \lambda(x \nabla y). \end{aligned}$$

Furthermore, we have

$$x \leq x \nabla y \leq y \quad \text{and} \quad x < x \nabla y < y$$

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 $x \nabla e = x$ and there are integer fractions x , y , and z such that $(x \nabla y) \nabla z = x \nabla (y \nabla z)$.

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

$$\left(\frac{a}{b} \nabla \frac{c}{d} \right) \nabla \left(\frac{e}{f} \nabla \frac{g}{h} \right) = \frac{a+c}{b+d} \nabla \frac{e+g}{f+h}$$

□

Theorem 6.4.3. *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

$$\frac{a+b}{c+d}.$$

Theorem 6.4.4. *Consider two reduced fractions $\frac{a}{b} < \frac{c}{d}$ and set*

$$k := bc - ad.$$

Then there are exactly k Farey fractions of order $\leq b + d$ strictly between $\frac{a}{b}$ and $\frac{c}{d}$.

6.5 A Structural Definition of the Rational Numbers

Definition 6.5.1. 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:

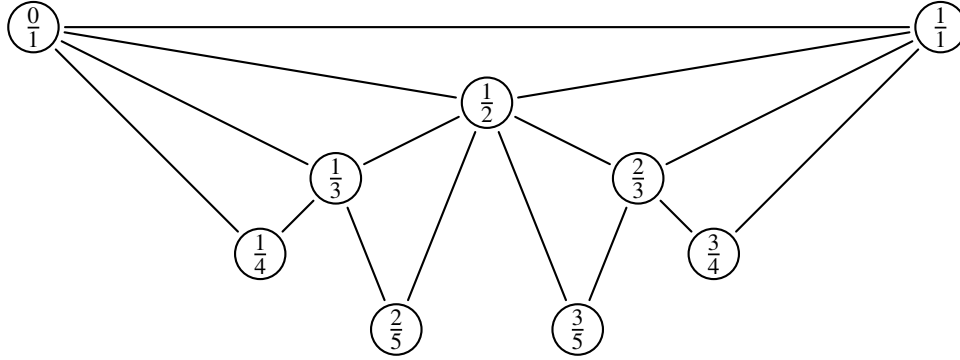


Figure 6.2: The Farey fractions with their adjacency relation

(i) a map $i : \mathbb{Z} \rightarrow \mathcal{Q}$,

(ii) a partial binary operation

$$m : \{(x, y) \in \mathcal{Q} \mid x \sim y\} \rightarrow \mathcal{Q}$$

called the *mediant*,

such that

(i) for any integer a , the relation $i(a) \sim i(a + 1)$ holds,

(ii) for any two elements $x, y \in \mathcal{Q}$ such that $x \sim y$ holds, the relations

$$x \sim m(x, y) \quad \text{and} \quad m(x, y) \sim y$$

hold.

Definition 6.5.2. The set $\mathcal{Q}$ equipped with the adjacency relation $\sim$ and a Farey structure (i, m) is a set of rational numbers if for every set $\mathcal{Q}'$ with an adjacency relation $\sim$ and Farey structure (i', m') , there is a unique map $f : \mathcal{Q} \rightarrow \mathcal{Q}'$ such that $x \sim y$ implies $f(x) \sim f(y)$, such that

$$\begin{aligned} f(i(a)) &= i'(a) \\ f(m(x, y)) &= m'(f(x), f(y)). \end{aligned}$$

The set $\mathbb{Q}$ is specified to be a set of rational numbers in this sense.

Example 6.5.3. We can use the specification of $\mathbb{Q}$ as a universal Farey structure to define a map

$$f : \mathbb{Q} \rightarrow X$$

into any set X equipped with a map $i : \mathbb{Z} \rightarrow X$ and a binary operation $m : X \times X \rightarrow X$. 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:

$$\begin{aligned} \text{num}(i(a)) &:= a, & \text{denom}(i(a)) &:= 1, \\ \text{num}(m(x, y)) &:= \text{num}(x) + \text{num}(y), & \text{denom}(m(x, y)) &:= \text{denom}(x) + \text{denom}(y). \end{aligned}$$

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,

Exercises

Routine-Building Exercises

- 6.1 For every integer a , show that there are infinitely many pairs of rational numbers x and y satisfying the equation

$$x^2 - y^2 = a.$$

- 6.2 Find all the integers of the form $x + \frac{1}{x}$, where x is a rational number.
 6.3 Prove that

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

- 6.4 Prove that

$$\prod_{k=2}^n \left(1 - \frac{1}{k}\right) = \frac{1}{n}.$$

- 6.5 Prove that

$$\prod_{k=1}^n \left(1 - \frac{1}{k^2}\right) = \frac{n+1}{2n}.$$

- 6.6 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 $n > 0$.

- 6.7 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 .

- 6.8 Consider the binary operation D on the reduced integer fractions, defined by

$$D\left(\frac{a}{b}, \frac{c}{d}\right) := |bc - ad|.$$

Show that D satisfies the axioms of a *metric*:

- (i) D is *positive definite*: $D\left(\frac{a}{b}, \frac{c}{d}\right) = 0$ if and only if $\frac{a}{b} = \frac{c}{d}$.

(ii) D is symmetric: $D\left(\frac{a}{b}, \frac{c}{d}\right) = D\left(\frac{c}{d}, \frac{a}{b}\right)$.

(iii) D satisfies the *triangle inequality*:

$$D\left(\frac{a}{b}, \frac{e}{f}\right) \leq D\left(\frac{a}{b}, \frac{c}{d}\right) + D\left(\frac{c}{d}, \frac{e}{f}\right).$$

Chapter 7

Pythagorean Triples

Pythagorean triples have been studied since antiquity. While this topic is very accessible, many aspects of the theory of 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 [Section 8.5](#): the congruent number problem.

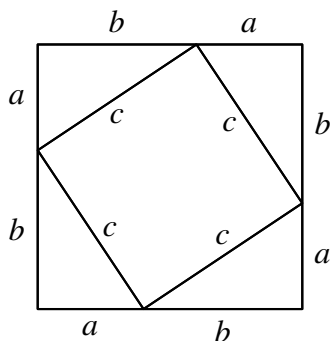
7.1 The Pythagorean Theorem

Recall that a right triangle is a triangle in which one of the angles is a right angle; that is, it is exactly 90° . The [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 [[Gua2023](#)].

Theorem 7.1.1 (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.

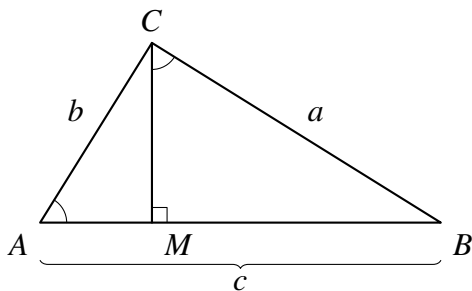


The area of the square is $(a + b)^2$. On the other hand, the area of each triangle is $ab/2$. Combined with the area of the inner square, whose sides are the hypotenuses of the four triangles, we obtain that

$$(a + b)^2 = c^2 + 4 \frac{ab}{2} = c^2 + 2ab.$$

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

$$a^2 = cy \quad \text{and} \quad b^2 = cx.$$

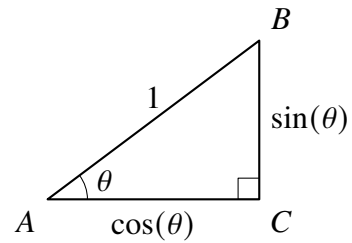
Since $x + y = c$, we find that $a^2 + b^2 = c^2$. □

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

$$\sin(\theta) = \frac{a}{c} \quad \text{and} \quad \cos(\theta) = \frac{b}{c}.$$



In the proof of the [Pythagorean Theorem](#), we will make use of the addition formulas for sine and cosine:

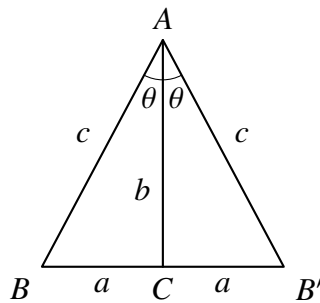
$$\begin{aligned} \sin(\theta + \phi) &= \sin(\theta) \cos(\phi) + \cos(\theta) \sin(\phi) \\ \cos(\theta + \phi) &= \sin(\theta) \sin(\phi) - \cos(\theta) \cos(\phi). \end{aligned}$$

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.

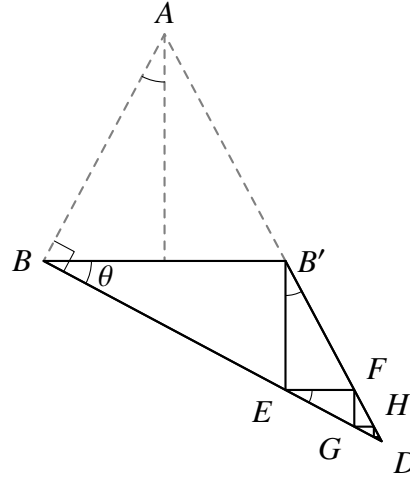
In the special case where ACB is isosceles, meaning that $a = b$, the hypotenuse is the diagonal of an a -by- a square, which gives us that $c^2 = 2a^2$. Hence, we may assume that ACB is nonisosceles.

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 7.1](#).

Figure 7.1: The recursive subdivision of the triangle BDB' .

We will now subdivide the triangle BDB' by first dropping a line down from B' at a right angle from the line BD , 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 1.5.3](#):

$$|B'D| = \sum_{k=0}^{\infty} 2c \left(\frac{a}{b} \right)^{2k+2} = 2c \left(\frac{a}{b} \right)^2 \sum_{k=0}^{\infty} \left(\frac{a}{b} \right)^{2k} = \frac{2c \left(\frac{a}{b} \right)^2}{1 - \left(\frac{a}{b} \right)^2} = \frac{2ca^2}{b^2 - a^2}.$$

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

$$1 + \frac{2a^2}{b^2 - a^2} = \frac{c^2}{b^2 - a^2}.$$

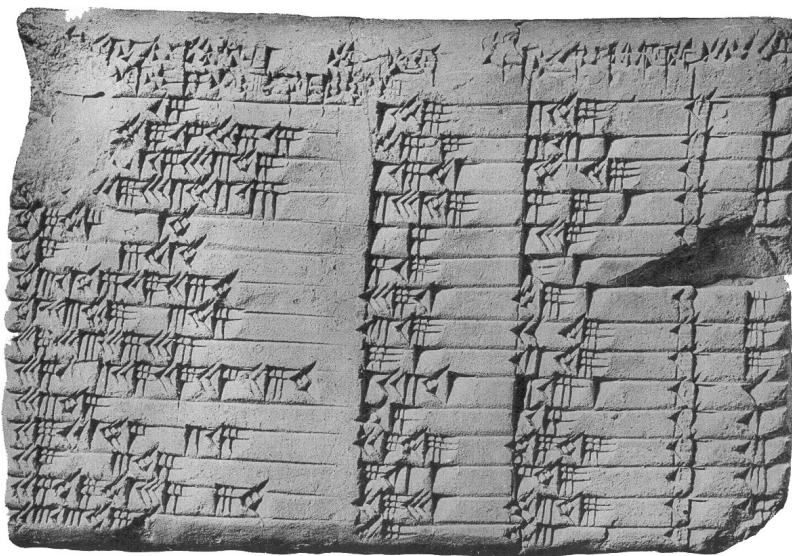


Figure 7.2: The Babylonian tablet Plimpton 322, listing Pythagorean triples.

Rearranging this equation gives us that $(b^2 - a^2) + 2a^2 = c^2$, which yields

$$a^2 + b^2 = c^2.$$

□

7.2 Euclid's Parametrization of the Pythagorean Triples

Our goal in this section is to describe all the solutions of the quadratic Diophantine equation

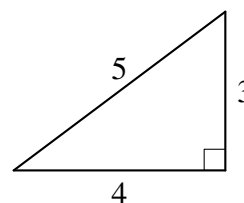
$$a^2 + b^2 = c^2,$$

where c is a nonzero integer. By the [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 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



$$(5, 12, 13), \quad (21, 20, 29), \quad \text{and} \quad (15, 8, 17).$$

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 n th odd number, so that $a^2 = 2n + 1$, then by [Exercise 1.1](#) there are positive integers b and c such that

$$b^2 = \sum_{i=0}^{n-1} (2i + 1), \quad \text{and} \quad c^2 = \sum_{i=0}^n (2i + 1)$$

For this choice of a , b , and c , we have

$$a^2 + b^2 = c^2.$$

Proposition 7.2.1. *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 7.2.2. A *primitive Pythagorean triple* is a triple (a, b, c) satisfying

$$a^2 + b^2 = c^2$$

such that $\gcd(a, b) = 1$.

Example 7.2.3. All the Pythagorean triples generated by Fibonacci's method are primitive, since $\gcd(2b + 1, b) = 1$.

Lemma 7.2.4. *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

$$a' := a/k, \quad b' := b/k, \quad \text{and} \quad c' := c/k.$$

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 $ka' = la''$, and we get $b' = b''$ from the equation $kb' = lb''$. We conclude that $(a', b', c') = (a'', b'', c'')$. $\square$

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 7.3](#) 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 7.2.5. *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 only 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. $\square$

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 7.2.6. *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*

$$c - a = 2s^2 \quad \text{and} \quad c + a = 2t^2.$$

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

$$\frac{c - a}{2} = s^2 \quad \text{and} \quad \frac{c + a}{2} = t^2.$$

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. $\square$

Theorem 7.2.7 (Euclid's Parametrization of the 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*

$$a = t^2 - s^2, \quad b = 2st, \quad \text{and} \quad c = t^2 + s^2.$$

Proof. To prove that two relatively prime integers $0 < s < t$ exist as specified, we will use s and t as determined in Lemma 7.2.6, where

$$\frac{c - a}{2} = s^2, \quad \text{and} \quad \frac{c + a}{2} = t^2.$$

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

$$a = v^2 - u^2, \quad b = 2uv, \quad \text{and} \quad c = v^2 + u^2.$$

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 $t = v$. $\square$

7.3 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, b, c) determines the point

$$\left(\frac{a}{c}, \frac{b}{c}\right),$$

which satisfies $(\frac{a}{c})^2 + (\frac{b}{c})^2 = (a^2 + b^2)/c^2 = 1$. Thus we see that if (a, b, c) is a primitive Pythagorean triple, then $(\frac{a}{c}, \frac{b}{c})$ is a rational point on the unit circle. We will show that *every* rational point on the unit circle arises in this way.

In order to prove that all rational points on the unit circle are determined by primitive Pythagorean triples, we need a systematic way of studying the rational points on the unit circle. A standard way to classify all (rational) points on the unit circle is to parametrize them using a single parameter. We will use a parametrization called the *stereographic projection*. This starts with a single rational point on the unit circle, in our case we start with the point $(-1, 0)$. Then we consider all the lines through this point with a rational slope. 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*, which is the topic of [Section 8.6](#).

Theorem 7.3.1 (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*

$$r + s = B \quad \text{and} \quad rs = C.$$

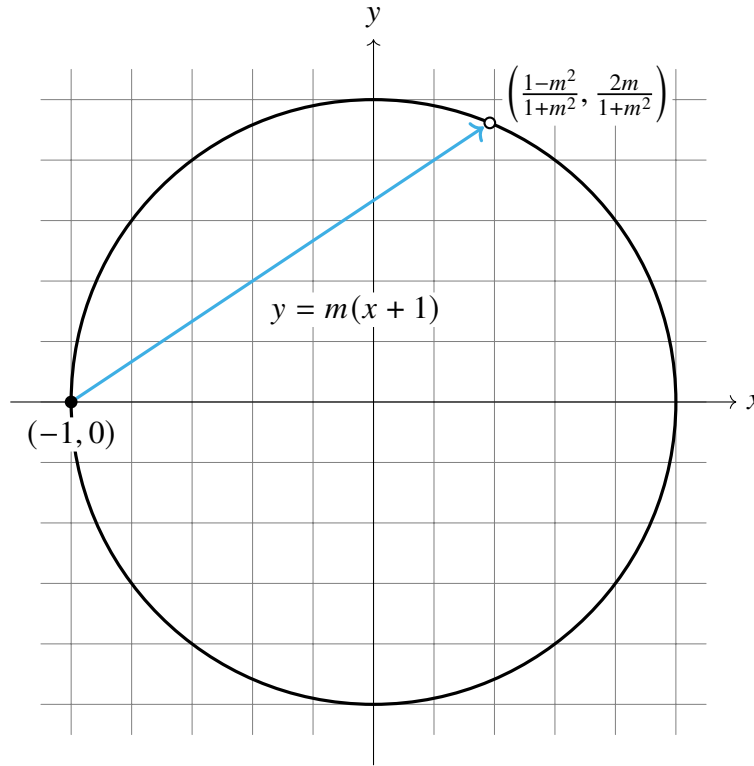


Figure 7.3: A point (x, y) on the unit circle is rational if and only if the line through $(-1, 0)$ and (x, y) has a rational slope.

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 7.3.2. 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 7.3.1](#): The other intersection point is at (x, y) , where

$$x = \frac{1 - m^2}{1 + m^2} \quad \text{and} \quad y = \frac{2m}{1 + m^2}. \quad \square$$

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.

Theorem 7.3.3. *The map*

$$(a, b, c) \mapsto \left(\frac{a}{c}, \frac{b}{c} \right)$$

from primitive Pythagorean triples (a, b, c) , where $a, b \in \mathbb{Z}$ are allowed to be negative and $c > 0$, to the rational points on the unit circle is a bijection.

Proof. Since we require $c > 0$, the assumption that $\gcd(a, b, c) = 1$ implies that if $(\frac{a}{c}, \frac{b}{c}) = (\frac{a'}{c'}, \frac{b'}{c'})$, then we must have $c = c'$ and consequently $a = a'$ and $b = b'$, so it follows immediately that the map $(a, b, c) \mapsto (\frac{a}{c}, \frac{b}{c})$ is injective. Therefore, it suffices to show that it is surjective.

Consider a rational point (x, y) on the unit circle. If $(x, y) = (-1, 0)$, then the unique primitive Pythagorean triple corresponding to (x, y) is $(-1, 0, 1)$. It remains to show that if $(x, y) \neq (-1, 0)$, then there exists a primitive Pythagorean triple (a, b, c) such that $x = \frac{a}{c}$ and $y = \frac{b}{c}$.

By the previous theorem, it follows that (x, y) is of the form

$$\left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2} \right),$$

where m is a rational number. Writing m as the integer fraction $\frac{s}{t}$, which we assume to be in lowest terms, we have

$$x = \frac{t^2 - s^2}{t^2 + s^2} \quad \text{and} \quad y = \frac{2st}{t^2 + s^2}.$$

The triple (a, b, c) given by $a := t^2 - s^2$, $b := 2st$, and $c := t^2 + s^2$ describes a Pythagorean triple, since the equation

$$(t^2 - s^2)^2 + (2st)^2 = (t^2 + s^2)^2$$

holds. Note that this Pythagorean triple is not necessarily primitive. For instance, when both s and t are odd, then a , b , and c are all divisible by 2. Nevertheless, by reducing this triple to a primitive triple if necessary, we obtain a primitive Pythagorean triple whose corresponding point on the unit circle is (x, y) . $\square$

7.4 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

$$A = \begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}, \quad \text{and} \quad C = \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{pmatrix}.$$

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 7.3.2, where we established the stereographic projection of the (rational) points on the unit circle.

Theorem 7.4.1 (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

$$t^2 + \frac{2vm - 2um^2}{1 + m^2}t + \frac{(mu - v)^2 - 1}{1 + m^2} = 0.$$

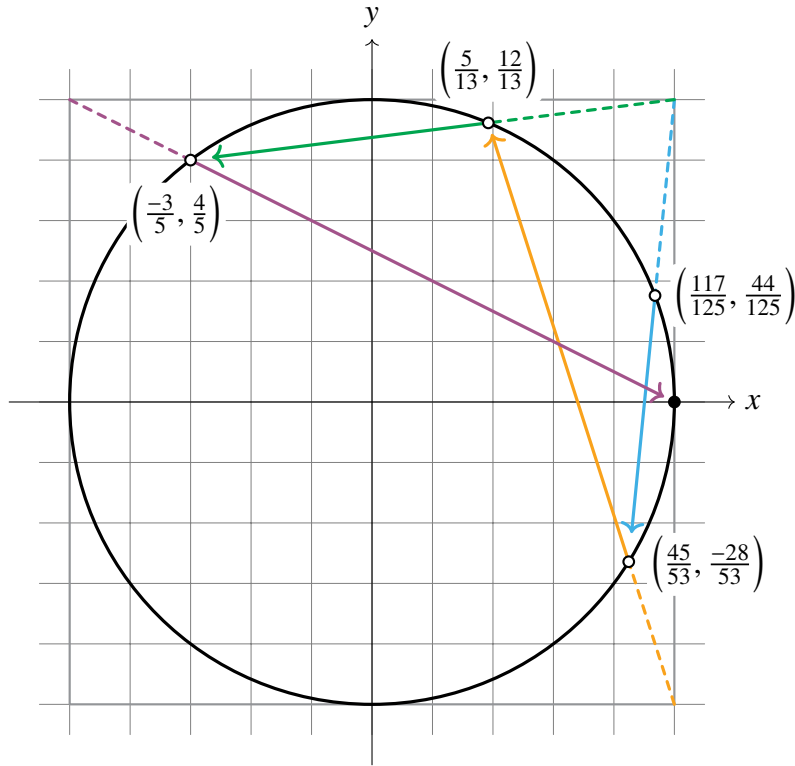


Figure 7.4: For any rational point (x, y) on the unit circle apart from $(0, \pm 1)$ and $(\pm 1, 0)$, draw a straight line through it from the outer corner of its quadrant to find a new rational point (x', y') on the unit circle. The common denominator of the fractions x' and y' , when brought to lowest terms, is strictly smaller than that of x and y , so that this process eventually terminates at $(0, \pm 1)$ or $(\pm 1, 0)$.

We have thus reached a quadratic equation of the form $t^2 + Bt + C$, which has by assumption one rational solution at $t = x$. Thus we obtain from [Theorem 7.3.1](#) a second rational solution x' satisfying the relation

$$xx' = \frac{(mu - v)^2 - 1}{1 + m^2}. \quad \square$$

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 a primitive Pythagorean triple (a', b', c') satisfying $0 < c' < c$. Intuitively, 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 alluded to previously is given by

$$u := \operatorname{sgn}(a) \quad \text{and} \quad v := \operatorname{sgn}(b).$$

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 7.4](#).

Example 7.4.2. Consider the Pythagorean triple $(a, b, c) := (117, 44, 125)$, which corresponds to the rational point $(x, y) := (\frac{117}{125}, \frac{44}{125})$ on the unit circle. Since both a and b are positive, we have $u = v = 1$, and the new point (x', y') on the line through (u, v) and (x, y) and the unit circle satisfies

$$xx' = \frac{(m-1)^2 - 1}{1 + m^2},$$

where $m = \frac{y-1}{x-1}$. Since $x = \frac{a}{c}$ and $y = \frac{b}{c}$, 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 $x' = \frac{45}{53}$ and $y' = \frac{-28}{53}$, 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 $x = \frac{a}{c}$ and $y = \frac{b}{c}$ in lowest terms with identical denominators, which we always take to be positive. This observation is a direct consequence of [Theorem 7.3.3](#). 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

$$2ab \leq a^2 + b^2. \quad (*)$$

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 7.4.3 (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*

$$x = \frac{a}{c} \quad \text{and} \quad y = \frac{b}{c}.$$

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 7.4.1](#), 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 $u = \text{sgn}(x)$ and $v = \text{sgn}(y)$, then we have $0 < c' < c$.

Proof. The rational point (x', y') obtained from [Theorem 7.4.1](#) 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 $x = \frac{a}{c}$ and $y = \frac{b}{c}$, 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:

$$xx' = \frac{(bu - av)^2 - (a - uc)^2}{(a - uc)^2 + (b - vc)^2} = \frac{b^2 - c^2 - 2uvab + 2uac}{-2uac - 2vbc + a^2 + b^2 + 2c^2} = \frac{a - a - 2uvb + 2uc}{c - 2ua - 2vb + 3c}.$$

Thus, we obtain the following expressions for a' and c' , so that $x' = \frac{a'}{c'}$:

$$\begin{aligned} a' &= -a - 2uvb + 2uc, \\ c' &= -2ua - 2vb + 3c. \end{aligned}$$

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

$$\frac{b' - b}{a' - a} = m.$$

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

$$2c < 2|a| + 2|b| < 3c.$$

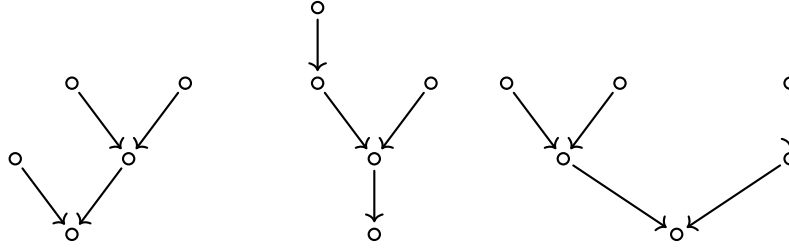


Figure 7.5: A forest.

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

$$4c^2 < 4(|a| + |b|)^2 = 4c^2 + 8|a||b| \leq 4c^2 + 4c^2 < 9c^2. \quad \square$$

The [Pythagorean Descent Theorem](#) 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* $h : F \rightarrow \mathbb{N}$, and for each height n a *parent function*

$$p : \{x \in F \mid h(x) = n + 1\} \rightarrow \{x \in F \mid h(x) = n\}.$$

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 7.5](#) we have drawn an example of a forest.

Example 7.4.4 (The forest of rational points on the unit circle). In [Pythagorean Descent Theorem](#), 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

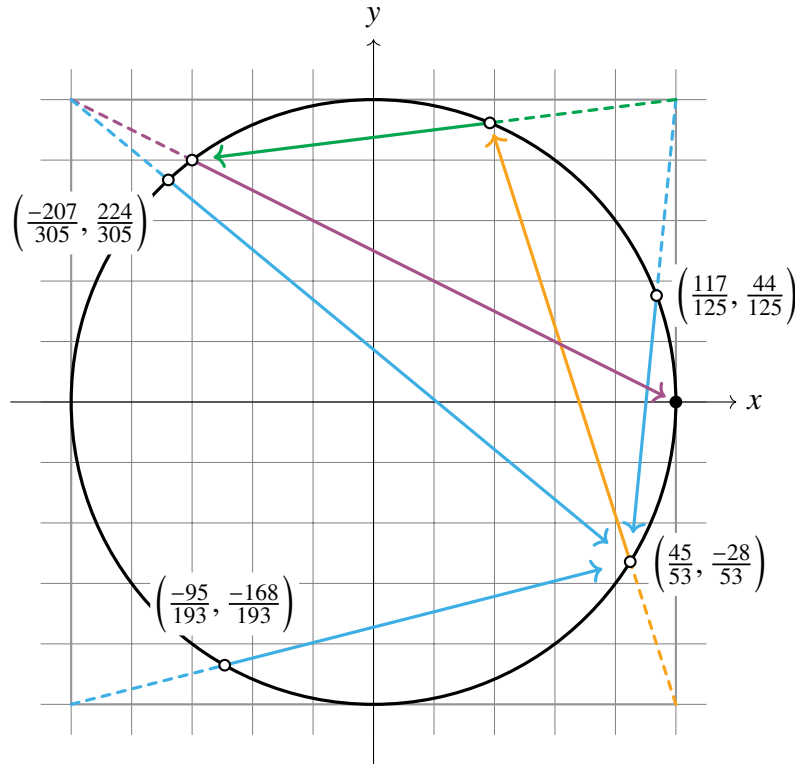


Figure 7.6: Each rational point on the unit circle other than $(\pm 1, 0)$ or $(0, \pm 1)$ is the target of a Vieta jump from three rational points on the unit circle with larger common denominator, one for each quadrant other than its own. Here, the purple, green, and orange jumps are drawn exactly as in Figure 7.4. The point $(\frac{45}{53}, -\frac{28}{53})$ 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 $(0, \pm 1)$.

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 7.6 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 $(\frac{\pm 3}{5}, \frac{\pm 4}{5})$ and $(\frac{\pm 4}{5}, \frac{\pm 3}{5})$. 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 x -axis, the line $y = x$, the y -axis, 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 7.4.5 (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 the [Pythagorean Descent Theorem](#) 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

$$M_{u,v} := \begin{pmatrix} -1 & -2uv & 2u \\ -2uv & -1 & 2v \\ -2u & -2v & 3 \end{pmatrix}.$$

When $u := \text{sgn}(a)$ and $v := \text{sgn}(b)$, 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 -coordinates, 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:

$$A = \begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}, \quad \text{and} \quad C = \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{pmatrix}$$

By the [Pythagorean Descent Theorem](#) 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 7.7](#).

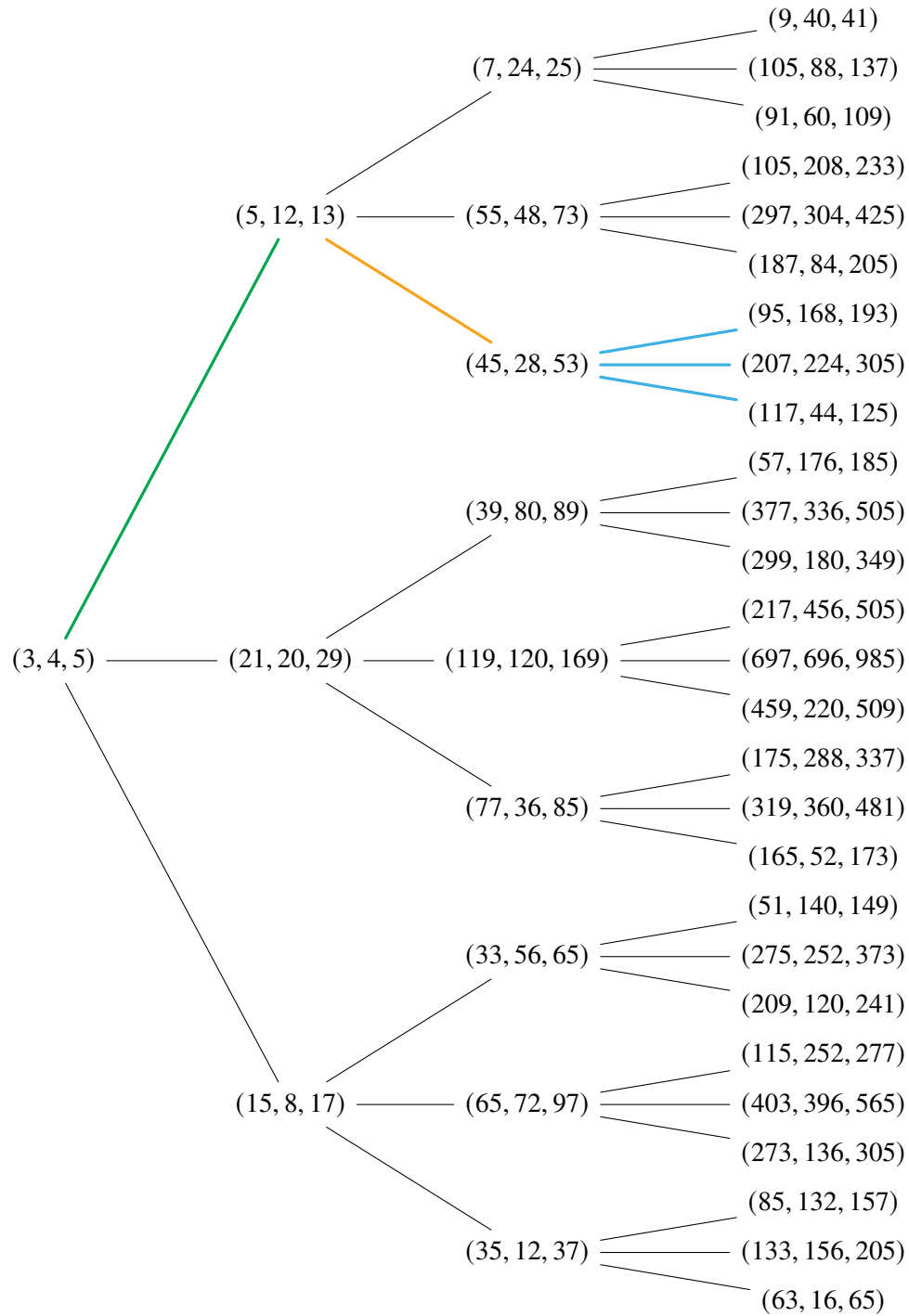


Figure 7.7: The tree of primitive Pythagorean triples. The edges that were drawn in green, orange, or blue in Figure 7.6 have been drawn here in the same color.

7.5 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

$$q^2 - 5 \quad \text{and} \quad q^2 + 5$$

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 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

$$b^2 - a^2 = 5t^2 \quad \text{and} \quad c^2 - b^2 = 5t^2.$$

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 7.5.1. 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 5.20](#) 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 $2 \cdot 3 \cdot 5 \cdot 24 = 720$.



Figure 7.8: Leonardo Pisano.

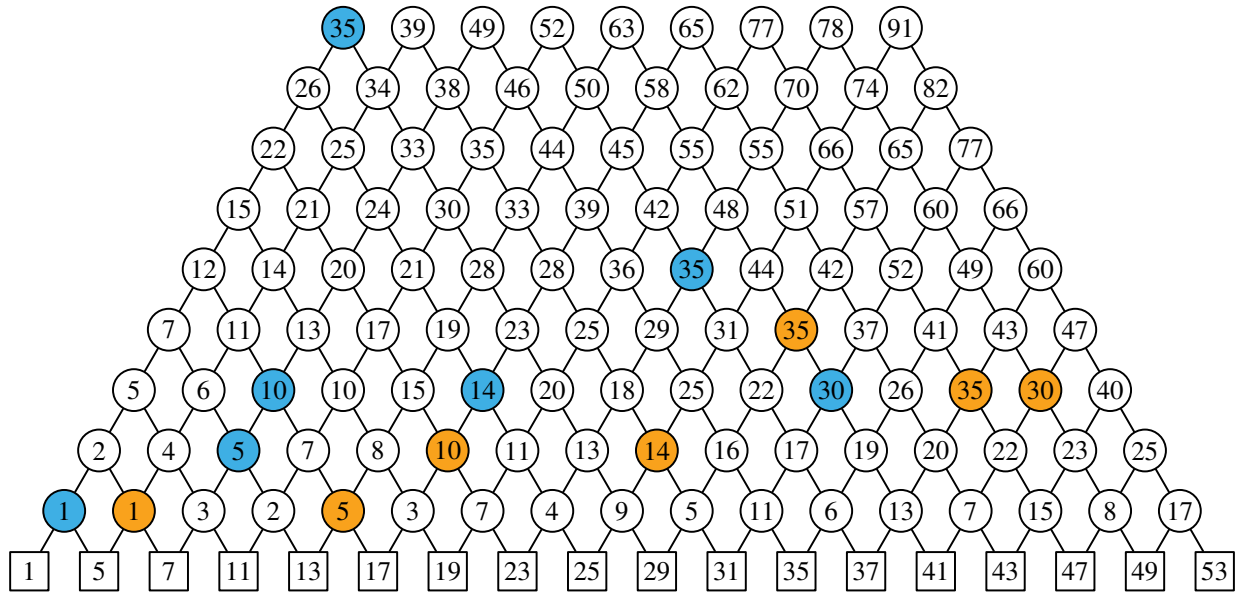


Figure 7.9: The numbers in squares at the base of the grid are the numbers of the form $6m \pm 1$, which correspond exactly to all the numbers n such that $n^2 - 1$ is divisible by 24. If x and y are two numbers in squares at the base of the grid, then the number k at the apex of the triangle spanned 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.

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 reduces the search space for arithmetic triples of squares. If a_n is the n th 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 7.9, 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

$$x := \frac{c-a}{2}, \quad y := \frac{c+a}{2}, \quad \text{and} \quad z := b$$

determine a Pythagorean triple (x, y, z) . Conversely, if (x, y, z) is a Pythagorean triple, then we define

$$a := |y-x|, \quad b := z, \quad \text{and} \quad c := y+x,$$

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:

$$\begin{aligned}(1^2, 5^2, 7^2) &\Leftrightarrow (3, 4, 5), \\ (7^2, 13^2, 17^2) &\Leftrightarrow (5, 12, 13), \\ (1^2, 29^2, 41^2) &\Leftrightarrow (21, 20, 29), \\ (7^2, 17^2, 23^2) &\Leftrightarrow (15, 8, 17).\end{aligned}$$

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 7.5.2. *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 7.5.3. *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*

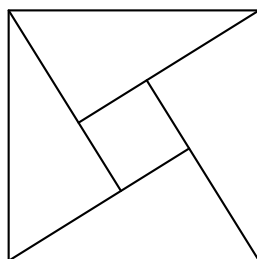
$$a = 2st - t^2 + s^2, \quad b = t^2 + s^2, \quad \text{and} \quad c = 2st + t^2 - s^2$$

with common difference $d = 2st(t - s)^2$.

Exercises

Starter Exercises

- 7.1 *Bhaskara's proof of the Pythagorean Theorem.* Use the following diagram to give a proof of the [Pythagorean Theorem](#):



Routine-Building Exercises

- 7.2 *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.

- 7.3 Consider a primitive Pythagorean triple (x, y, z) .
- Prove that exactly one of x , y , and z is divisible by 3.
 - Prove that exactly one of x , y , and z is divisible by 5.
 - Find all Pythagorean triples (x, y, z) in which $x = 30$ or $y = 30$. Can any of them be primitive?
 - 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.

- 7.4 Find three distinct triangular numbers in an arithmetic progression.
- 7.5 Find three distinct tetrahedral numbers, that is, numbers of the form $\binom{n+2}{3}$, in an arithmetic progression.
- 7.6 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 $\gcd(a, b) = 1$.

- Show that if (a, b, c) is a primitive Egyptian triple, then $\gcd(a, c) = \gcd(b, c) = 1$.
- 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

$$a = s(s + t), \quad b = t(s + t), \quad c = st.$$

Challenge Exercises

- 7.7 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.
- 7.8 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.

- 7.9 Show that for every positive integer y divisible by 4, there is a primitive Pythagorean triple (a, b, c) with $b = y$.
- 7.10 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 $a = x$.
- 7.11 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 k th Fibonacci number. Show that (x_n, y_n, z_n) is a Pythagorean triple for each n .

- 7.12 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 1.15](#), so that (a_n^2, b_n^2, c_n^2) is an arithmetic triple of squares. Show that

$$\gcd(a_n, b_n, c_n) = \begin{cases} 2 & \text{if } n \equiv 1 \pmod{3}, \\ 1 & \text{otherwise.} \end{cases}$$

- 7.13 Consider three squares a^2 , b^2 , and c^2 in an arithmetic progression in increasing order.

- (a) Show that at least one of

$$c - b, \quad c - a, \quad \text{and} \quad b - a$$

is divisible by 3.

- (b) Show that at least one of

$$c - b, \quad c - a, \quad \text{and} \quad b - a$$

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.

7.14 Find all solutions to the equation $x^2 - 2y^2 = 1$.

7.15 *Master Theodore's problem for Leonardo Pisano* [FS1987, Proposition 24]. Find three positive integers x , y , and z such that the numbers

$$x + y + z + x^2, \quad x + y + z + x^2 + y^2, \quad \text{and} \quad x + y + z + x^2 + y^2 + z^2$$

are all squares.

7.16 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

$$a = 2(su - tv),$$

$$b = 2(sv + tu),$$

$$c = s^2 + t^2 - u^2 - v^2,$$

$$d = s^2 + t^2 + u^2 + v^2.$$

Chapter 8

Infinite Descent

8.1 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 8.1.1. *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

$$A := \{a_0, a_1, a_2, \dots\}$$

is a nonempty subset of the natural numbers, and by 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. $\square$

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 8.1.2 (Method of Infinite Descent). *Consider a set A equipped with a function $f : A \rightarrow A$ and a function $h : A \rightarrow \mathbb{N}$. 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 $h(a_0) > h(a_1) > h(a_2) > \cdots$, which is an infinite descending sequence of natural numbers. Thus, the assumption that A is inhabited was false. $\square$

8.2 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 8.2.1. *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 [Euclid's parametrization of the Pythagorean triples](#), we can find two relatively prime integers $s < t$ of opposite parity, such that

$$a = t^2 - s^2, \quad b = 2st, \quad \text{and} \quad c = t^2 + s^2.$$

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 5.5.1](#) 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. $\square$

8.3 The Unsolvability of $x^4 + y^4 = z^4$

Theorem 8.3.1. *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 $f : A \rightarrow A$ 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

$$\begin{aligned} x^2 &= t^2 - s^2, \\ y^2 &= 2st, \\ z &= t^2 + s^2. \end{aligned}$$

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

$$\begin{aligned} x &= v^2 - u^2 \\ s &= 2uv \\ t &= v^2 + u^2. \end{aligned}$$

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

$$\gcd(u, v^2 + u^2) = \gcd(u, v^2) = 1 \quad \text{and} \quad \gcd(v, v^2 + u^2) = \gcd(v, u^2) = 1,$$

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 $f : A \rightarrow A$. 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 the [method of infinite descent](#) that the set A must be empty. $\square$

Corollary 8.3.2. *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. $\square$

8.4 The Nonexistence of Four Squares in an Arithmetic Progression

We have shown in [Theorem 7.5.2](#) 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 the step size is a number of the form $2n$, where it follows from [Exercise 5.20](#) 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

$$y^2 = a^2 b^2 c^2 d^2 = (x - 3n)(x - n)(x + n)(x + 3n) = (x^2 - n^2)(x^2 - 9n^2).$$

By completing the square, we see that

$$y^2 = x^4 - 10n^2 x^2 + 9n^4 = (x^2 - 5n^2)^2 - 16n^4.$$

Thus we obtain a 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. This Pythagorean triple is our entry into a descent argument.

Lemma 8.4.1. *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 $2uv$.*

Theorem 8.4.2 (Fermat–Euler). *Every arithmetic progression of length four of the integer squares is constant.*

8.5 The Congruent Number Problem

Recall from [Section 7.5](#) the challenge that Master John posed in the early 13th century to Leonardo Fibonacci: To find a rational number q such that both

$$q^2 - 5, \quad \text{and} \quad q^2 + 5$$

are both rational. 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 8.5.1. A positive integer a is said to be a *congruent number* if it occurs as the area of a right triangle with rational sides and rational hypotenuse.

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

$$a = \frac{3}{2}, \quad b = \frac{20}{3}, \quad \text{and} \quad c = \frac{41}{6}.$$

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.

Lemma 8.5.2. *A number n is congruent if and only if there is a primitive Pythagorean triangle whose area is n times a square.*

Proof. Consider three rational numbers a , b , and c such that

$$a^2 + b^2 = c^2, \quad \text{and} \quad \frac{ab}{2} = n,$$

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

$$A^2 + B^2 = C^2, \quad \text{and} \quad \frac{AB}{2} = nm^2$$

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 the claim. $\square$

Theorem 8.5.3. *No square positive integer is a congruent number.*

Proof. This claim follows from [Lemma 8.5.2](#) and Fermat's [Theorem 8.2.1](#), which states that the area of a Pythagorean triangle cannot be a square. $\square$

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 8.5.4. *If a positive integer is twice a square, then it isn't congruent.*

Proof. This theorem can be stated equivalently as: The area of a primitive Pythagorean triangle cannot be twice a square. To derive a contradiction, we assume that a Pythagorean triple (A, B, C) exists with

$$\frac{AB}{2} = 2m^2.$$

By Euclid's parametrization of the primitive Pythagorean triples, a Pythagorean triple as described above is uniquely determined by a pair of relatively prime positive integers $s < t$ of opposite parity, with

$$A = t^2 - s^2, \quad B = 2st, \quad \text{and} \quad C := t^2 + s^2.$$

Using this parametrization, we find the following equation for the area:

$$st(t^2 - s^2) = 2m^2.$$

However, the integers s , t , and $t^2 - s^2$ are all relatively prime, which implies that exactly one of them—either s or t —is twice a square and the other two are squares. $\square$

Corollary 8.5.5. *No power of 2 is congruent.*

Proof. Any power of 2 is either a square or twice a square, so it can't be congruent by [Theorems 8.5.3](#) and [8.5.4](#). $\square$

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.

8.6 Vieta Jumping

Vieta jumping is a problem-solving technique that builds on the observation that

$$(x - r)(x - s) = x^2 - (r + s)x + rs.$$

We saw in [Theorem 7.3.1](#) that if r is a root of a monic polynomial $x^2 - Bx + C$, then the other root s satisfies

$$s = B - r = \frac{C}{r}.$$

Thus, if we know one root of a quadratic polynomial then we can easily 'jump' to the other root using one of the above formulas. Vieta jumping became a popular problem-solving technique for international contests such as the International Mathematics Olympiad.

Example 8.6.1. In [Exercise 5.22](#) 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 and y satisfy this polynomial equation, then so must

$$x' := \frac{x}{\gcd(x, y)} \quad \text{and} \quad y' := \frac{y}{\gcd(x, y)}.$$

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 $xy \mid x^2 + y^2$.

Exercises

Starter Exercises

- 8.1 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 $t > 0$.

- 8.2 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

- 8.3 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.

- 8.4 Show that there are no positive integer squares of the form

$$2x^2 + 2xy + 2y^2.$$

- 8.5 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 $t > 0$.

- 8.6 Prove that the area of a Pythagorean triangle cannot be twice a square.

Challenge Exercises

- 8.7 Prove that the Diophantine equation

$$x^4 - y^4 = z^2$$

has no solutions in the positive integers.

- 8.8 Show that if x and y are positive integers such that xy divides $x^2 + y^2 + 1$, then

$$\frac{x^2 + y^2 + 1}{xy} = 3.$$

- 8.9 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.

- 8.10 Show that the only triangular number which is also a fourth power is 1.

Part III

Congruences

Chapter 9

Modular Arithmetic

9.1 The Congruence Relations

Carl Friedrich Gauss introduced the congruence relations in his monumental work, *Disquisitiones Arithmeticae* [Gau1986]. The congruence relations allowed him to systematically simplify the study of the integers. Prior to Gauss's invention, number theory was pursued with a variety of ad hoc techniques that often made proofs less transparent than they could be. His key insight was that many properties of the integers depend not on their exact size, but rather on their remainder when divided by a fixed number.

Definition 9.1.1. 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 9.1.2. 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 9.1.3. 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

$$9 + 8 \equiv 5 \pmod{12},$$

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.

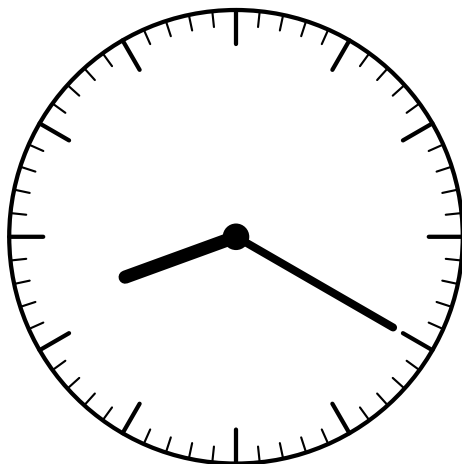


Figure 9.1: The 12-hour clock contains two systems of modular arithmetic: A system with modulus 12 to mark the hours and a system with modulus 60 to mark the minutes.

Example 9.1.4. 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 correspondence 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

$$m' := \begin{cases} m + 12 & \text{if } m = 1 \text{ or } m = 2, \\ m & \text{otherwise,} \end{cases} \quad \text{and} \quad y' := \begin{cases} y - 1 & \text{if } m = 1 \text{ or } m = 2, \\ y & \text{otherwise.} \end{cases}$$

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 14, 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 9.1.5. 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 9.1.6. *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

$$n \mid (qn + r) - (pn + s) \quad \text{if and only if} \quad n \mid (q - p)n + (r - s).$$

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. $\square$

Example 9.1.7. Recall from [Theorem 4.4.1](#) 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 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 9.1.8. *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 9.1.9. *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 9.1.10. 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

$$\gcd(6, 15) \not\equiv \gcd(16, 25) \pmod{10}.$$

9.2 Equivalence Relations

The congruence relations are examples of equivalence relations, which we will now define.

Definition 9.2.1. 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 9.2.2. 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 9.2.3. 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 $af - be = 0$. $\square$

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 $f : A \rightarrow B$, there is an equivalence relation $\sim_f$ on the set A , given by

$$x \sim_f y \quad \text{if and only if} \quad f(x) = f(y).$$

This relation is also called the *kernel* of f .

Proposition 9.2.4. For any function $f : A \rightarrow B$, 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. $\square$

Example 9.2.5. Consider the function $r : \mathbb{Z} \rightarrow \{0, \dots, n-1\}$, defined via 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 $T : X \rightarrow X$. We illustrate this by an example first.

Example 9.2.6. Recall from [Exercise 4.5](#) 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

$$17 \sim_F 28 \sim_F 45 \sim_F \dots$$

The general method of obtaining equivalence relations of this kind assumes an arbitrary operation $T : A \rightarrow A$. Given such an operation, we define the equivalence relation $\sim_T$ by declaring that

$$x \sim_T y \quad \text{if and only if} \quad \exists_{(s,t \in \mathbb{N})} T^s(x) = T^t(y).$$

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 9.2.7. *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:

$$3, 10, 5, 16, 8, 4, 2, 1, 4, \dots$$

Once the sequence reaches 1, it enters the cycle

$$1 \mapsto 4 \mapsto 2 \mapsto 1 \mapsto \dots$$

The famous and elusive *Collatz conjecture* states that for every positive integer n , the sequence

$$n, T(n), T^2(n), \dots$$

eventually reaches the value 1. In our notation, the Collatz conjecture asserts that $n \sim_T 1$ for every positive natural number n .

9.3 Equivalence Classes and Residue Systems

Definition 9.3.1. 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 9.3.2. 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

$$a \mapsto [a] : A \rightarrow A/\sim$$

sending an element to its equivalence class is called the *quotient map*. We often write q for the quotient map.

Proposition 9.3.3. *For any equivalence relation $\sim$ on a set A , the quotient map*

$$a \mapsto [a] : A \rightarrow A/\sim$$

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*

$$[a] = [b] \quad \text{if and only if} \quad a \sim b.$$

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. $\square$

Definition 9.3.4. 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 9.3.5. 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 9.3.6. 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

$$\mathbb{N}/(\equiv \pmod{n}) \cong \{r_0, \dots, r_{n-1}\}.$$

9.4 The Integers Modulo n

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 9.4.1. 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:

$$\begin{aligned}[a] + [b] &:= [a + b] \\ [a][b] &:= [ab]\end{aligned}$$

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 9.3.3](#) 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 9.1.8](#) 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

$$\begin{aligned}[a] + [b] &= [a'] + [b'] \\ [a][b] &= [a'][b'].\end{aligned}$$

This ensures that the definitions of addition and multiplication on the integers modulo n is *well-defined* on the congruence classes modulo n .

Remark 9.4.2. The definitions of addition and multiplication on the integers modulo n follow a general pattern of defining functions $f : A/\sim \rightarrow B$ out of quotient sets. Given a function $g : A \rightarrow B$, a function $f : A/\sim \rightarrow B$ 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 9.4.3. 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 9.4.4. *The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n satisfies the following laws of arithmetic:*

$(x + y) + z = x + (y + z)$	$(xy)z = x(yz)$
$0 + x = x$	$1x = x$
$x + 0 = x$	$x1 = x$
$x - x = 0$	$x(y + z) = xy + xz$
$-x + x = 0$	$(x + y)z = xz + yz$
$x + y = y + x$	$xy = yx$

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 $a(b + c) = ab + ac$. $\square$

9.5 The Multiplicative Order of an Integer Modulo n

Expanding a fraction such as $\frac{1}{7}$ 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 $\frac{1}{7}$, 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 $\frac{1}{7}$ can be computed as the integer part of the number $\frac{10}{7}$, which has all the decimal digits of $\frac{1}{7}$ shifted by one position to the left. It also follows that the remainder of the digits coincide with the digits of $\frac{3}{7}$, where the numerator is the remainder of 10 after division by 7. The first digit of the fractional part of $\frac{3}{7}$ is the integer part of $\frac{30}{7}$, 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 $\frac{20}{7}$. If we keep going in this manner, we find that

$$d_1 = \left\lfloor \frac{10}{7} \right\rfloor, \quad d_2 = \left\lfloor \frac{30}{7} \right\rfloor, \quad d_3 = \left\lfloor \frac{20}{7} \right\rfloor, \quad d_4 = \left\lfloor \frac{60}{7} \right\rfloor, \quad d_5 = \left\lfloor \frac{40}{7} \right\rfloor, \quad d_6 = \left\lfloor \frac{50}{7} \right\rfloor, \quad d_7 = \left\lfloor \frac{10}{7} \right\rfloor.$$

Here we see that our task at hand begins to repeat itself. We have already computed the integer part of $\frac{10}{7}$ in the first step, which led us to compute the integer part of $\frac{30}{7}$, and so on. Thus, we find that the decimal expansion of $\frac{1}{7}$ is given by

$$\frac{1}{7} = 0.142857142857142857 \dots$$

This satisfies the property that, after shifting the decimal expansion for $\frac{1}{7}$ by 6 places, the decimal digits will line up exactly. A mathematically precise way of expressing that decimal expansion of the fraction $\frac{1}{7}$ 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 9.5.1. 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 $\text{ord}_n(a)$ 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 $\text{ord}_n(a) = 0$.

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 $\text{ord}_n(a)$ and numbers dividing $a^k - 1$.

Theorem 9.5.2 (Order Theorem). *The multiplicative order of an integer a modulo n satisfies the logical equivalence*

$$\text{ord}_n(a) \mid k \Leftrightarrow n \mid a^k - 1.$$

Proof. We have two cases to consider: either $\gcd(a, n) = 1$ or $\gcd(a, n) \neq 1$. In the first case, $\text{ord}_n(a)$ 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 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 $\text{ord}_n(a) \mid k$. This proves the claim in the first case.

In the second case we have $\text{ord}_n(a) = 0$. Then the condition that $\text{ord}_n(a) \mid k$ 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 $k = 0$. $\square$

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 9.5.3. *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 $\text{ord}_b(10)$.

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 the [Order Theorem](#) it follows that this congruence holds if and only if $\text{ord}_b(10) \mid k$. $\square$

The logical equivalence in the [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 9.5.4. *For any integer a of order $k = \text{ord}_n(a)$, we have*

$$\text{ord}_n(a^m) = \frac{k}{\gcd(m, k)}.$$

In particular, we have $\text{ord}_n(a^m) = k$ if and only if m and k are relatively prime.

Proof. We have the following chain of logical equivalences:

$$\text{ord}_n(a^m) \mid l \Leftrightarrow n \mid (a^m)^l - 1 \Leftrightarrow \text{ord}_n(a) \mid ml \Leftrightarrow \frac{\text{ord}_n(a)}{\gcd(m, \text{ord}_n(a))} \mid l.$$

Thus, we see that $\text{ord}_n(a^m)$ and $k/\gcd(m, k)$ divide the same numbers, so they must be equal. $\square$

Exercises

Starter Exercises

- 9.1 Describe a complete residue system modulo 7 consisting entirely of multiples of 3.
 9.2 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 .
 9.3 Find the multiplicative inverses of 1, 2, 3, 4, 5, and 6 modulo 7.
 9.4 Find the multiplicative inverses of 1, 3, 7, 9, 11, 13, 17, and 19 modulo 20.

Routine-Building Exercises

- 9.5 (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.
 9.6 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 $ab \equiv 1 \pmod{n}$.
 9.7 (a) Find integers k , a , and b such that

$$ka \equiv kb \pmod{4}, \quad \text{but} \quad a \not\equiv b \pmod{4}.$$

- (b) Prove that if $\gcd(k, n) = d$, then we have

$$ka \equiv kb \pmod{n} \quad \text{if and only if} \quad a \equiv b \pmod{\frac{n}{d}}.$$

- 9.8 Show that if $a \equiv b \pmod{m}$, then we have

$$\gcd(a, m) = \gcd(b, m).$$

- 9.9 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.
 9.10 Show that if $ab \equiv 1 \pmod{n}$, then

$$\text{ord}_n(a) = \text{ord}_n(b).$$

- 9.11 Consider an integer a . Show that if

$$a^m - 1 \mid a^n - 1,$$

then $m \mid n$.

- 9.12 Show that $\text{ord}_{a^k-1}(a) = k$.

Challenge Exercises

9.13 Let $F_n = 2^{2^n} + 1$ be the n th Fermat number. Show that $F_n \equiv 17 \pmod{24}$ for $n \geq 2$.

9.14 Prove that for any $n > 1$ and any k , we have

$$(n-1)^2 \mid n^k - 1 \quad \text{if and only if} \quad n-1 \mid k.$$

Chapter 10

Systems of Linear Congruences

10.1 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 $x \equiv x' \pmod{n}$, 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 10.1.1. 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 5.6.4](#) 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

$$x = x_0 + k \frac{n}{d}, \quad \text{and} \quad y = y_0 - k \frac{a}{d},$$

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 5.6.4](#) in modular arithmetic as follows.

Theorem 10.1.2. *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 10.1.3. 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 10.1.4. *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 10.1.5. The invertible congruence classes modulo 5 are the congruence classes of 1, 2, 3, and 4. Indeed, one can verify that

$$\begin{array}{ll} 1 \cdot 1 \equiv 1 \pmod{5} & 2 \cdot 3 \equiv 1 \pmod{5} \\ 3 \cdot 2 \equiv 1 \pmod{5} & 4 \cdot 4 \equiv 1 \pmod{5}. \end{array}$$

Corollary 10.1.6. Consider an integer a relatively prime to n . Then the operation $x \mapsto [a]x$ is a bijection on $\mathbb{Z}/n\mathbb{Z}$.

10.2 Solving Multiple Linear Congruences Simultaneously

Consider the linear congruences

$$\begin{aligned} 10x &\equiv 4 \pmod{12} \\ 15x &\equiv 6 \pmod{21}, \end{aligned}$$

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 10.1.2](#), 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

$$\begin{aligned} x &\equiv 4 \pmod{6} \\ x &\equiv 6 \pmod{7}. \end{aligned}$$

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 5.6.1](#), 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 5.6.1](#) 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 the [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 $x \equiv 118 \pmod{210}$.

10.3 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

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

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 10.3.1 (Chinese Remainder Theorem). *Consider two linear congruences*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}, \end{aligned}$$

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. $\square$

10.4 A Method Suggested by Gauss

Gauss mentions in his *Disquisitiones Arithmeticae* [Gau1986, Article 36] that he sometimes prefers the following method of solving systems

$$x \equiv a_1 \pmod{m_1}, \dots, x \equiv a_n \pmod{m_n}$$

of linear congruences, where $m_1, \dots, m_n$ are pairwise relatively prime. First, we are to find numbers e_i such that

$$e_i \equiv \begin{cases} 1 \pmod{m_j} & \text{if } j = i, \\ 0 \pmod{m_j} & \text{if } j \neq i. \end{cases} \quad (10.1)$$

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 10.4.1. To illustrate Gauss's preferred method, consider the system of linear congruences

$$7x \equiv 2 \pmod{15}, \quad 11x \equiv 1 \pmod{14}, \quad 5x \equiv 3 \pmod{11}.$$

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

$$x \equiv 7 \pmod{15}, \quad x \equiv 9 \pmod{14}, \quad \text{and} \quad x \equiv 5 \pmod{11}.$$

In order to find e_i as specified in [Equation \(10.1\)](#), we need to separately solve the linear congruences

$$154u_1 \equiv 1 \pmod{15}, \quad 165u_2 \equiv 1 \pmod{14}, \quad \text{and} \quad 210u_3 \equiv 1 \pmod{11}.$$

These simplify as follows:

$$4u_1 \equiv 1 \pmod{15}, \quad 11u_2 \equiv 1 \pmod{14}, \quad \text{and} \quad u_3 \equiv 1 \pmod{11}.$$

Using the methods described in [Section 10.1](#), we find the following solutions:

$$u_1 \equiv 4 \pmod{15}, \quad u_2 \equiv 9 \pmod{14}, \quad \text{and} \quad u_3 \equiv 1 \pmod{11}.$$

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

$$x \equiv 7 \cdot 4 \cdot 154 + 9 \cdot 9 \cdot 165 + 5 \cdot 1 \cdot 210 \equiv 247 \pmod{2310}$$

Exercises

Starter Exercises

- 10.1 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

$$x \equiv 2 \pmod{3},$$

$$x \equiv 3 \pmod{5},$$

$$x \equiv 2 \pmod{7}.$$

- 10.2 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

- 10.3 Find all integers x satisfying the linear congruences

$$x \equiv 4 \pmod{9},$$

$$x \equiv 3 \pmod{10},$$

$$x \equiv 2 \pmod{11}.$$

- 10.4 Find all integers x satisfying the linear congruences

$$x \equiv 3 \pmod{5},$$

$$x \equiv 6 \pmod{11},$$

$$x \equiv 9 \pmod{17}.$$

- 10.5 Consider the congruence

$$xy + 7x + 4y \equiv 10 \pmod{13}.$$

Compute the congruence class of y modulo 13 for $x \equiv 2, 5, 8 \pmod{13}$.

Part IV

Prime Numbers

Chapter 11

Prime Numbers

Learning Objectives

In this chapter we define primes, discuss the sieve of Eratosthenes, the fundamental theorem of arithmetic, and we prove in several ways the infinitude of primes. We also introduce the concept of p -adic valuation, which is used to prove Legendre's formula for $n!$ and Kummer's theorem about the prime factorization of binomial coefficients. Finally, we prove Bertrand's Postulate, which states that there is a prime number between n and $2n$, for any n .

After working through this chapter, you will be able to:

- (i) Compute prime factorizations and p -adic valuations of structured numbers such as $a^n - 1$, $n!$, or $\binom{n}{k}$, using algebraic factorizations, Legendre's formula, and Kummer's theorem.
- (ii) Establish elementary congruence constraints involving primes.
- (iii) Prove divisibility properties using prime factorizations.

11.1 The Fundamental Theorem of Arithmetic

Definition 11.1.1. 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.

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 11.1 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 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 n th 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	$\emptyset$	$\{2, 3, 4, 5, 6, 7, 8, \dots\}$
1	$\{2\}$	$\{3, 5, 7, 9, 11, 13, 15, \dots\}$
2	$\{2, 3\}$	$\{5, 7, 11, 13, 17, 19, 23, \dots\}$
3	$\{2, 3, 5\}$	$\{7, 11, 13, 17, 19, 23, 29, \dots\}$
4	$\{2, 3, 5, 7\}$	$\{11, 13, 17, 19, 23, 29, 31, \dots\}$
5	$\{2, 3, 5, 7, 11\}$	$\{13, 17, 19, 23, 29, 31, 37, \dots\}$

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

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

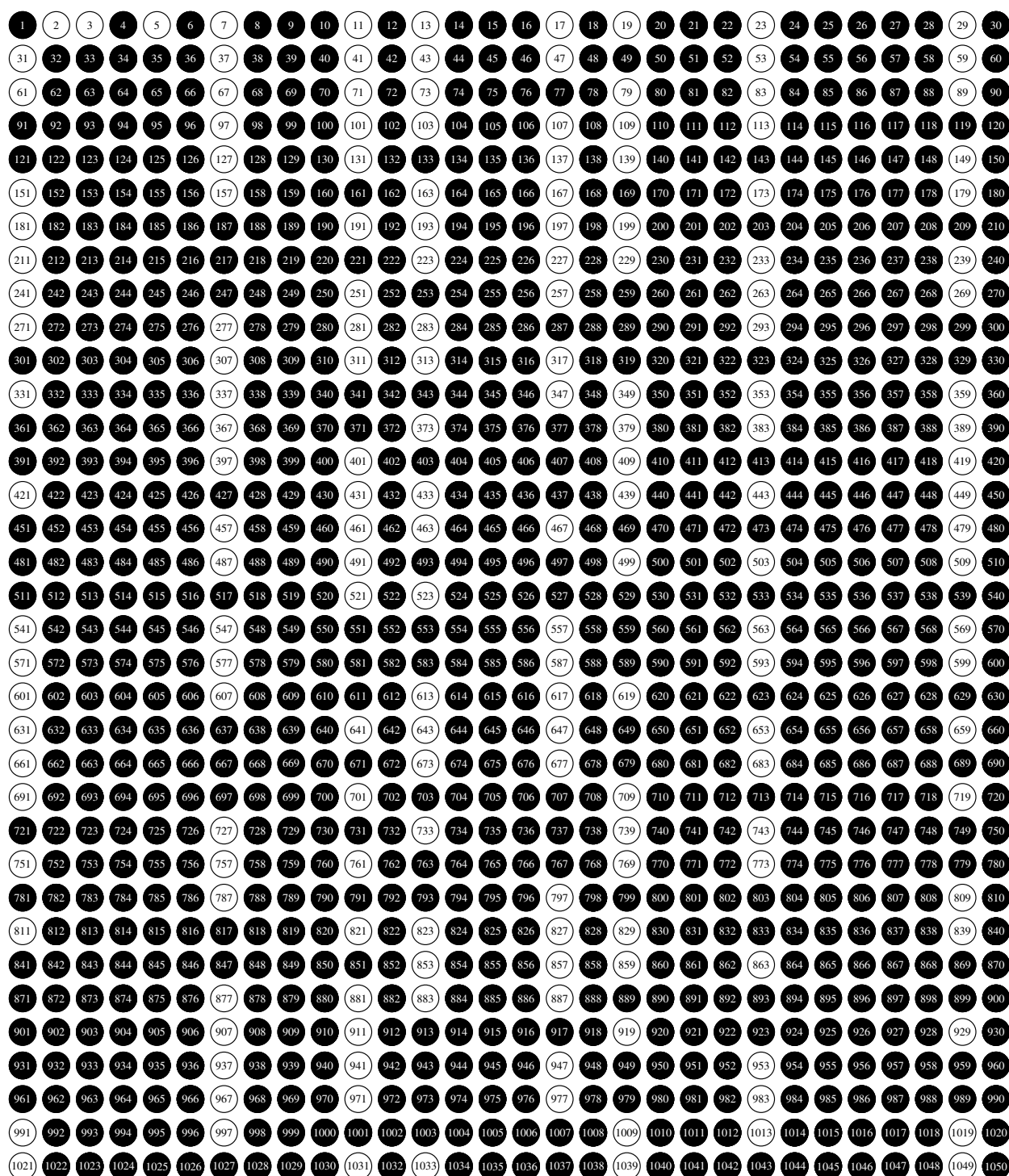


Figure 11.1: The sieve of Eratosthenes up to 1050: The number 1 and every composite number are marked in black, leaving just the primes in white circles.

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 11.1.2. *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 the [Well-Ordering Principle](#) 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. $\square$

The following proposition is due to Euclid, who included it as proposition 30 of book VII of the *Elements*.

Lemma 11.1.3. *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 $p \mid a$. $\square$

Proposition 11.1.4. *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 11.1.3](#) that a and b are relatively prime. This allows us to apply [Proposition 5.4.5](#), 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. $\square$

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 mentioned that prior authors often assumed it or gave inadequate reasons for its truth.

Theorem 11.1.5. *For any natural number $n > 0$, there is a unique list $\ell = (p_0, \dots, p_{l-1})$ of length l , consisting of primes $p_0 \leq p_1 \leq \dots \leq p_{l-1}$ 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

$$p_0 \leq p_1 \leq \dots \leq p_l.$$

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 $(r_0, \dots, r_k)$ 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. $\square$

Corollary 11.1.6. *For any positive integer n with prime factorization $n = p_1^{m_1} \cdots p_k^{m_k}$, the map*

$$x \mapsto (x \bmod p_1^{m_1}, \dots, x \bmod p_k^{m_k})$$

is a bijection

$$\mathbb{Z}/n\mathbb{Z} \cong \prod_k \mathbb{Z}/p_k^{m_k}\mathbb{Z}.$$

Remark 11.1.7. 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.

11.2 The Infinitude of Primes

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 11.2.1. *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. $\square$

Theorem 11.2.2. *There are infinitely many prime numbers.*

Euclid's proof of Theorem 11.2.2. 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 $\{p_0, \dots, p_k\}$. $\square$

11.2.1 Saidak's Proof

There are many proofs of the infinitude of primes. The following is due to Filip Saidak [Sai2006], who 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 11.2.2. 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. $\square$

11.2.2 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

$$x \in A \quad \Leftrightarrow \quad x + n \in \mathbb{Z}.$$

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 $A_1, \dots, A_m$ is a finite family of periodic subsets of $\mathbb{Z}$, each with their own periods, then the union

$$A_1 \cup \dots \cup A_m$$

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.

The Furstenberg proof of [Theorem 11.2.2](#), 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 it 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. $\square$

11.2.3 Erdős's Proof

Definition 11.2.3. 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 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 11.2.4. 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 the [Well-Ordering Principle](#), 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 $m = d$. $\square$

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 11.2.2. 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 11.2.4](#) 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 $p_1, \dots, p_n$. $\square$

11.2.4 A Proof via the Stars-and-Bars Method

The stars-and-bars problem asks in how many ways it is possible to place $n - 1$ bars between k stars. In [Figure 11.2](#) we displayed some example configurations for the stars-and-bars problem.

The stars-and-bars problem admits several equivalent formulations. For example, the stars-and-bars problem is equivalently posed by asking in how many ways one can place k indistinguishable balls in n distinguishable boxes. It is also equivalent to the problem of writing k as an ordered sum of n natural numbers. The four example configurations of [Figure 11.2](#) correspond to writing

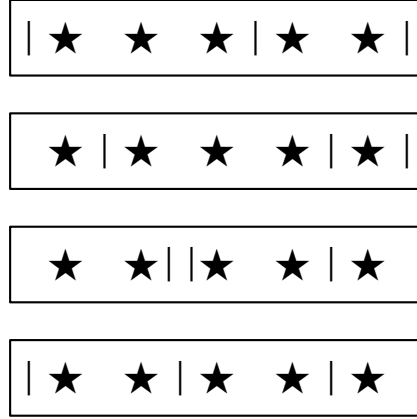


Figure 11.2: Four example configurations with five stars and three bars.

$5 = 0 + 3 + 2 + 0$, $5 = 1 + 3 + 1 + 0$, $5 = 2 + 0 + 2 + 1$, and $5 = 0 + 2 + 2 + 1$. Making use of the [Fundamental Theorem of Arithmetic](#), we find yet another equivalent way of formulating the stars-and-bars problem: Given a set $p_1, \dots, p_n$ primes, how many natural numbers are there of the form

$$p_1^{m_1} \cdots p_n^{m_n},$$

so that $m_1 + \cdots + m_n = k$? We establish the answer in the following theorem.

Theorem 11.2.5. *Given a set $p_1, \dots, p_n$ of n distinct primes, there are exactly $\binom{k+n-1}{n-1}$ natural numbers that can be written in the form*

$$p_1^{m_1} \cdots p_n^{m_n},$$

so that $m_1 + \cdots + m_n = k$.

Proof. Since the primes $p_1, \dots, p_n$ are distinct, the Fundamental Theorem of Arithmetic implies that distinct choices for $(m_1, \dots, m_n)$ yield distinct natural numbers. Thus, we merely need to determine in how many ways we can decompose k as an ordered sum of n natural numbers.

In order to do so, we claim that there is a bijection between the set of n -tuples $(m_1, \dots, m_n)$ satisfying $m_1 + \cdots + m_n = k$, and the set of $(n-1)$ -element subsets of the set $\{1, \dots, k+n-1\}$. This bijection takes an n -tuple $(m_1, \dots, m_n)$ to the subset

$$\{(m_1 + 1) + \cdots + (m_i + 1) \mid 1 \leq i < n\}.$$

For example, the four 4-tuples corresponding to the configurations in [Figure 11.2](#) are mapped to 3-element subsets of $\{1, \dots, 8\}$ as follows:

$$\begin{aligned} (0, 3, 2, 0) &\mapsto \{1, 5, 8\}, \\ (1, 3, 1, 0) &\mapsto \{2, 6, 8\}, \\ (2, 0, 2, 1) &\mapsto \{3, 4, 7\}, \\ (0, 2, 2, 1) &\mapsto \{1, 4, 7\}. \end{aligned}$$

Conversely, given an $(n-1)$ -element subset $S = \{s_1 \leq \dots \leq s_{n-1}\}$ of $\{1, \dots, k+n-1\}$, we define $s_0 := 0$ and $s_n := k+n$ in order to define $m_i := (s_i - 1) - s_{i-1}$ for all $1 \leq i \leq n$. Then we can compute the sum of the numbers m_i as a telescopic sum:

$$\sum_{i=1}^n m_i = \sum_{i=1}^n (s_i - 1 - s_{i-1}) = (k+n) - n = k.$$

It is fairly immediate from these definitions that we have defined mutually inverse maps, so that we have a bijection between n -tuples that sum to k and $(n-1)$ -element subsets of a $(k+n-1)$ -element set. Since the number of such subsets is

$$\binom{k+n-1}{n-1},$$

this completes the proof. $\square$

Theorem 11.2.6. *Given a set $p_1, \dots, p_n$ of distinct primes, the set of numbers of the form*

$$p_1^{m_1} \cdots p_n^{m_n}$$

such that $m_1 + \dots + m_n \leq k$ has exactly $\binom{k+n}{n}$ elements.

Proof. By the hockey-stick identity (Exercise 2.8), we have

$$\sum_{i=0}^k \binom{i+n-1}{n-1} = \binom{k+n}{n}. \quad \square$$

Proof of Theorem 11.2.2. Consider a set $p_1, \dots, p_n$ of distinct primes, and let N be such that all the numbers $1 \leq m \leq N$ can be written as a product of the primes $p_1, \dots, p_n$.

For any $m = p_1^{m_1} \cdots p_n^{m_n} \leq N$, we have

$$m_1 + \dots + m_n \leq \frac{m_1 \log p_1 + \dots + m_n \log p_n}{\log 2} = \frac{\log m}{\log 2} \leq \frac{\log N}{\log 2}.$$

By Theorem 11.2.6 it follows that

$$N \leq \binom{\left\lfloor \frac{\log N}{\log 2} \right\rfloor + n}{n} \leq \frac{\left(\frac{\log N}{\log 2} + n \right)^n}{n!}.$$

Assuming that our initial list of primes includes all the primes below 12 so that $n \geq 5$, this inequality fails for $N \geq 2^{2^n}$. This shows that any finite set $p_1, \dots, p_n$ of primes cannot be the set of all primes, so there must be infinitely many primes. $\square$

11.3 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 11.3.1. *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 n th Fermat number is given by

$$F_n := 2^{2^n} + 1.$$

The first few Fermat numbers are:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

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 13.1.5](#) and [13.1.6](#) 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 11.3.2 (Product formula for the Fermat numbers). *The n th Fermat number satisfies the identity*

$$F_n - 2 = \prod_{0 \leq k < n} F_k.$$

Proof. We will prove the claim by strong induction. In the base case, we have

$$F_0 - 2 = 2^{2^0} - 1 = 1 = \prod_{0 \leq k < 0} F_k,$$

since the product on the right-hand side is empty.

For the inductive step, we use the formula for the difference of squares:

$$(F_{n+1} - 2) = 2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1) = F_n \cdot \prod_{0 \leq k < n} F_k = \prod_{0 \leq k < n+1} F_k. \quad \square$$

Theorem 11.3.3 (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 the [Product formula of 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 11.2.2. Since any two distinct Fermat numbers are relatively prime, and since any number $n > 1$ has a prime divisor, it follows that if we pick a prime divisor of each Fermat number F_n , then we picked infinitely many distinct prime numbers. $\square$

11.4 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 11.4.1. 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

$$p^k \mid n \quad \Leftrightarrow \quad k \leq v_p(n)$$

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 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 11.3](#).

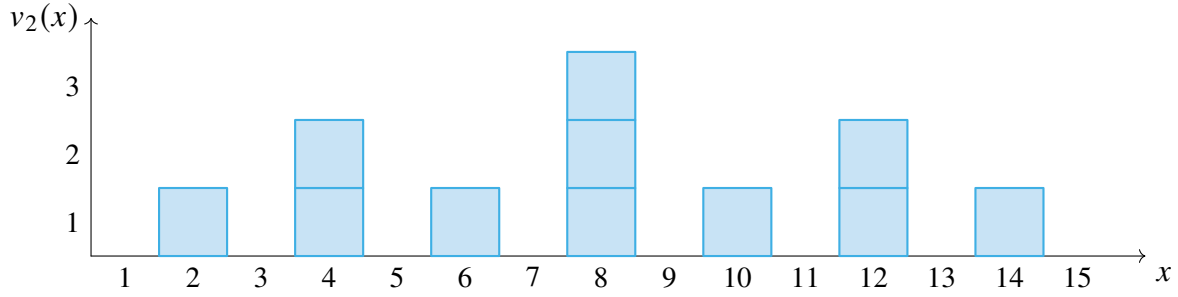


Figure 11.3: The 2-adic valuations of the numbers up to 15.

Example 11.4.2. 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

$$v_p(\text{lcm}(n_1, \dots, n_k)) = \max(v_p(n_1), \dots, v_p(n_k)).$$

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

$$\gcd(60, 525) = 3 \cdot 5 = 15 \quad \text{and} \quad \text{lcm}(60, 525) = 2^2 \cdot 3 \cdot 5^2 \cdot 7 = 2100.$$

An immediate consequence of the definition of p -adic valuations is the following proposition:

Proposition 11.4.3. *For any two positive integers a and b , the following are equivalent:*

- (i) $a \mid b$.
- (ii) $v_p(a) \leq v_p(b)$ for every prime p .

Example 11.4.4. 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 11.4.5 (Legendre's formula). *For any natural number n , we have*

$$n! = \prod_{p \leq n} p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots}.$$

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 k th 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

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor. \quad \square$$

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 11.2.2. 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 $p_1, \dots, p_m$, 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 $p_1, \dots, p_m$. $\square$

In the following theorem we give a useful alternative expression for the p -adic valuation of $n!$.

Theorem 11.4.6 (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

$$\frac{n - \sum_{j=0}^l a_j}{p - 1} = \sum_{j=0}^l a_j \frac{p^j - 1}{p - 1} = \sum_{k=1}^l \left\lfloor \frac{n}{p^k} \right\rfloor. \quad \square$$

Example 11.4.7. 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 i th prime power in the prime factorization of $\binom{64}{32}$. This gives:

$$d_1 = 2, d_2 = 8, d_3 = 2, d_4 = 2, \dots, d_{13} = 4.$$

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

$$m = \sum_{i=0}^{l_m} a_i p^i \quad \text{and} \quad n = \sum_{i=0}^{l_n} b_i p^i.$$

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 11.4.8 (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*

$$m = \sum_{i=0}^{l_m} a_i p^i \quad \text{and} \quad n = \sum_{i=0}^{l_n} b_i p^i,$$

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. $\square$

Example 11.4.9. Consider two natural numbers m and n such that

$$m = \sum_{i=0}^k a_i 2^i \quad \text{and} \quad n - m = \sum_{i=0}^k b_i 2^i,$$

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 $1, 2, \dots, n$. 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 11.4.10. For any $0 \leq k \leq n$ we have

$$\binom{n}{k} \mid \text{lcm}(1, \dots, n).$$

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

$$p^{v_p \binom{n}{k}} \mid \text{lcm}(1, \dots, n).$$

Since this is true for every prime $p \leq n$, and $\binom{n}{k}$ contains only prime divisors up to n , the claim follows. $\square$

11.5 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 [Che1850]. We will give a proof by Paul Erdős [Erd1932], which can be obtained through the methods of the previous section.

Lemma 11.5.1 (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. $\square$

Theorem 11.5.2. *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 11.4.10](#) 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

$$\prod_{p^2 \mid \binom{2n}{n}} p^{\nu_p \binom{2n}{n}} \leq (2n)^{\sqrt{2n}}.$$

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 2.6](#), and the last inequality follows from [Lemma 11.5.1](#). 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 . $\square$

Exercises

Starter Exercises

11.1 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.

11.2 Find the first ten primes of the form $n^2 + 1$. The first of Landau's four open problems about primes asks whether there are infinitely many such primes [Lan1912].

11.3 Find the first ten primes p such that $2p - 1$ is also prime. It is unknown whether there are infinitely many such primes.

11.4 Given a prime $p > 3$, show that $p^2 \equiv 1 \pmod{24}$.

11.5 By computing its prime factorization, show that

$$\binom{50}{3}$$

is a square number.

11.6 Show that

$$a^2 \equiv 1 \pmod{p} \Leftrightarrow a \equiv \pm 1 \pmod{p}.$$

11.7 Show that

$$\sum_{k=1}^n k^3 \mid \prod_{k=1}^n k^3$$

holds for every n , except when $n + 1$ is an odd prime.

Routine-Building Exercises

11.8 Find the longest arithmetic progression of primes under 1000. Hint: Use congruences to constrain the step size.

11.9 Compute the prime factorizations of the following numbers:

- (a) $5^{15} - 1$.
- (b) $3^{18} - 1$.
- (c) $2^{48} - 1$.

11.10 Show that there are no primes p such that $p + 8$ and $p + 22$ are also prime.

11.11 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 $pq \equiv -1 \pmod{9}$.

11.12 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

$$p(2p + 1) \equiv 1 \pmod{18}.$$

11.13 (a) Show that any odd prime of the form $x^2 + y^2$ must be congruent to 1 (mod 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 (mod 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.

11.14 Show that

$$p \mid \binom{p}{k}$$

for any $0 < k < p$, and any prime number p .

11.15 Determine the number of trailing zeros in the decimal representations of $100!$ and $2^{10}!$.

11.16 (a) In Figure 11.3 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 $0 \leq m \leq n$.

11.17 Show that

$$\binom{42}{6} \mid \binom{42}{12} \quad \text{and} \quad \binom{42}{6} \mid \binom{42}{18}.$$

11.18 (a) Show that

$$\binom{30}{2} \mid \binom{30}{2k}$$

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 $1 \leq k \leq p - 1$.

11.19 Show that

$$\text{lcm}(1, 2, \dots, n) = e^{\sum_{p \leq n} \lfloor \log_p n \rfloor \log p}.$$

11.20 (a) Show that

$$\frac{\text{lcm}(1, \dots, n)}{\text{lcm}(1, \dots, m)} = \prod_{k \geq 1} \prod_{\substack{p \text{ prime} \\ m < p^k \leq n}} p.$$

Use this formula to conclude that

$$\frac{\text{lcm}(1, \dots, n)}{\text{lcm}(1, \dots, n-1)} = \begin{cases} p & \text{if } n = p^k \text{ for some prime } p \text{ and } k \geq 1, \\ 1 & \text{otherwise.} \end{cases}$$

(b) Show that

$$\frac{\text{lcm}(1, \dots, n)}{\text{lcm}(1, \dots, m)}$$

is square-free for every $m \leq n$ such that $n \leq 2m$.

(c) Show that

$$\frac{\text{lcm}(1, \dots, n)}{\text{lcm}(1, \dots, m)} \mid \binom{n}{m}.$$

for every $m \leq n$ such that $n \leq 2m$.

Challenge Exercises

11.21 Show that for any prime p , if $p^2 + 2$ is prime then $p + 2$ is prime.

11.22 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.

11.23 Consider a prime $p \equiv 3 \pmod{4}$, and suppose that $\nu_p(n)$ 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 .

11.24 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 .

11.25 Show that there is exactly one positive integer k such that both $2^k - 1$ and $2^k + 1$ are prime.

11.26 In this exercise F_n denotes the n th 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 $p \equiv \pm 2 \pmod{5}$.

11.27 Prove the following identity of Bakir Farhi [Far2009]:

$$\text{lcm} \left(\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n} \right) = \frac{\text{lcm}(1, \dots, n+1)}{n+1}.$$

11.28 Show that there are infinitely many numbers not divisible by any Fibonacci numbers other than 1.

11.29 Use Bertrand's Postulate to show that

$$\frac{1}{n+1} + \frac{1}{n+2} + \dots + \frac{1}{2n}$$

is never an integer.

Chapter 12

Multiplicative Functions

12.1 Perfect Numbers

The number 6 satisfies the curious property that the sum of its divisors $1 + 2 + 3$ is equal to the number 6 itself. This property of a number being equal to the sum of its own divisors, was deemed so special in ancient times, that these numbers were called *perfect*.

Definition 12.1.1. A number n is said to be *perfect* if the sum of its divisors, including n itself, is $2n$.

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 $0 \leq i \leq k$, it follows that the divisors of $2^k(2^m - 1)$ are exactly

$$1, 2, \dots, 2^k, \quad \text{and} \quad (2^m - 1), 2(2^m - 1), \dots, 2^k(2^m - 1).$$

The sum of the divisors of $2^k(2^m - 1)$ is thus

$$(2^{k+1} - 1) + (2^{k+1} - 1)(2^m - 1) = (2^{k+1} - 1)2^m.$$

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 12.1.2 (Euclid). *If the number $2^m - 1$ is prime, then $2^{m-1}(2^m - 1)$ is perfect.*

Using Euclid's method, we can find the first few perfect numbers. [Table 12.1](#) displays the prime factorization of the number $2^m - 1$ for $2 \leq m \leq 11$.

m	2	3	4	5	6	7	8	9	10	11
$2^m - 1$	3	7	$3 \cdot 5$	31	$3^2 \cdot 7$	127	$3 \cdot 5 \cdot 17$	$7 \cdot 73$	$3 \cdot 11 \cdot 31$	$23 \cdot 89$

Table 12.1: The Mersenne numbers M_m for $2 \leq m \leq 11$.

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 12.1.3. *If the m th 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:

$$2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1) \sum_{k=0}^{b-1} (2^a)^k. \quad \square$$

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 12.1.4. 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 $0 \leq k \leq m$, so the sum of the divisors of p^m is the finite geometric series $1 + p + p^2 + \cdots + p^m$.

Proposition 12.1.5. *Suppose m and n are relatively prime. Then*

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Proof. Consider a divisor $d \mid mn$. Since m and n are relatively prime, it follows that $d = \gcd(d, m) \gcd(d, n)$. Thus we can assign to every divisor $d \mid mn$ a pair of numbers (u, v) such that $u \mid m$, $v \mid n$, and $d = uv$.

Conversely, if we start a pair (u, v) of numbers such that $u \mid m$ and $v \mid n$, then $u = \gcd(uv, m)$ and $v = \gcd(uv, n)$. This shows that the operation $d \mapsto (\gcd(d, m), \gcd(d, n))$ is inverse to the operation $u, v \mapsto uv$. Thus we obtain a bijection

$$\{u \mid u \mid m\} \times \{v \mid v \mid n\} \cong \{d \mid d \mid mn\}$$

given by $(u, v) \mapsto uv$. Using this bijection, we see that

$$\left(\sum_{u \mid m} u \right) \left(\sum_{v \mid n} v \right) = \sum_{u \mid m} \sum_{v \mid n} uv = \sum_{d \mid mn} d. \quad \square$$

The multiplicative property of the sum-of-divisors function along with the expressions for $\Sigma(p^m)$ completely determine the values of the function σ for any positive integer of which the prime factorization is known.

Corollary 12.1.6. *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 12.1.7. We saw in [Example 11.4.4](#) 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 12.1.8 (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. $\square$

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} .

12.2 Euler's Totient Function

Before we introduce reduced residue systems, let us prove a lemma.

Lemma 12.2.1. *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. $\square$

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 12.2.2. 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 12.2.3. 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. $\square$

Theorem 12.2.4. 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 the [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

$$\gcd(x, mn) = 1 \Leftrightarrow \gcd(x, m) = 1 \text{ and } \gcd(x, n) = 1.$$

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 $d = 1$. $\square$

Since multiplicative functions are fully determined by their values on prime powers, we obtain the following important expression for Euler's totient function.

2^k	Fermat primes	$\{n \mid \phi(n) = 2^k\}$
1		$\{1, 2\}$
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 12.2: Lists of numbers n for which $\phi(n) = 2^k$

Theorem 12.2.5. 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 12.2.6. 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 $\phi(n)$. $\square$

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 12.2.7. 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 12.2.8. We will use [Theorem 12.2.5](#) 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

$$3, 5, 17, 257, \text{ and } 65537.$$

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 12.2](#) lists the numbers n for which $\phi(n) = 2^k$ up to $2^k = 128$.

12.3 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 :

$$\tau(n) := \sum_{d|n} 1 \quad \text{and} \quad \sigma(n) := \sum_{d|n} d.$$

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 $\{1, 2, 3, \dots\}$. 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 12.3.1. 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 12.3.2. 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 $f(1) = 1$. $\square$

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 12.3.3. If f is a multiplicative function and $n = p_1^{m_1} \cdots p_k^{m_k}$, where the primes $p_1, \dots, p_k$ are distinct, then

$$f(n) = f(p_1^{m_1}) \cdots f(p_k^{m_k}).$$

Proof. Since the primes $p_1, \dots, p_k$ are assumed to be distinct, it follows that the prime powers $p_1^{m_1}, \dots, p_k^{m_k}$ are pairwise relatively prime, hence the claim follows by induction on k . $\square$

The following theorem provides a useful way of proving that a function is multiplicative.

Theorem 12.3.4. Suppose f is a multiplicative function, and define the function F by

$$F(n) := \sum_{d|n} f(d).$$

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

$$\begin{aligned} F(mn) &= \sum_{e|mn} f(e) = \sum_{c|m} \sum_{d|n} f(cd) \\ &= \sum_{c|m} \sum_{d|n} f(c)f(d) = \sum_{c|m} f(c) \sum_{d|n} f(d) = F(m)F(n). \end{aligned} \quad \square$$

Theorem 12.3.5. The functions τ and σ are multiplicative.

Proof. The functions τ and σ are defined by

$$\tau(n) := \sum_{d|n} 1, \quad \text{and} \quad \sigma(n) := \sum_{d|n} d.$$

Clearly the constant function $n \mapsto 1$ and the identity function $n \mapsto n$ are multiplicative, so it follows from [Theorem 12.3.4](#) that τ and σ are multiplicative. $\square$

The previous theorem implies that if $n = p_1^{m_1} \cdots p_k^{m_k}$ is a product of distinct primes, then

$$\tau(n) = \prod_{i=1}^k (m_i + 1), \quad \text{and} \quad \sigma(n) = \prod_{i=1}^k \frac{p_i^{m_i+1} - 1}{p_i - 1}.$$

Indeed, for any prime power p^m , the divisors of p^m are the prime powers p^i where $0 \leq i \leq m$. 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 12.3.6. Many identities of arithmetic functions involve reindexing double sums such as in the proof of [Theorem 12.3.4](#). Another reindexing identity that is occasionally helpful is:

$$\sum_{c|n} \sum_{d|c} f(c, d) = \sum_{d|n} \sum_{e|\frac{n}{d}} f(de, d).$$

12.4 The Möbius Function

Definition 12.4.1. 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 12.4.2. *The Möbius function is multiplicative, and it satisfies*

$$\sum_{d|n} \mu(d) = \varepsilon(n).$$

*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 $\mu(d) = -1$. $\square$

Arithmetic proof. Likewise, the arithmetic function

$$F(n) := \sum_{d \mid n} \mu(d)$$

is multiplicative by [Theorem 12.3.4](#). 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

$$\sum_{d \mid p^k} \mu(p^k) = \mu(p^0) + \mu(p^1) + 0 = 1 - 1 = 0. \quad \square$$

Remark 12.4.3. 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](#)].

12.5 Dirichlet Convolution

The set of arithmetic functions with values taken in a fixed, chosen number system such as the integers, the real numbers, or the complex numbers, possesses an interesting algebraic structure that can be used effectively to obtain many algebraic results and identities about numbers. The most important operation on arithmetic functions is *Dirichlet convolution*, a way of combining two arithmetic functions f and g into a new arithmetic function $f * g$.

Definition 12.5.1. Consider two arithmetic functions f and g . We define their *Dirichlet convolution* $f * g$ by

$$(f * g)(n) := \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Theorem 12.5.2. *Dirichlet convolution is associative and commutative, meaning that*

$$(f * g) * h = f * (g * h), \quad \text{and} \quad f * g = g * f,$$

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 calculation:

$$\begin{aligned} ((f * g) * h)(n) &= \sum_{\substack{c,d \\ cd=n}} (f * g)(c)h(d) \\ &= \sum_{\substack{c,d \\ cd=n}} \sum_{\substack{a,b \\ ab=c}} f(a)g(b)h(d) \\ &= \sum_{\substack{a,b,d \\ abd=n}} f(a)g(b)h(d) \\ &= \sum_{\substack{a,e \\ ae=n}} \sum_{\substack{b,d \\ bd=e}} f(a)g(b)h(d) \\ &= \sum_{\substack{a,e \\ ae=n}} f(a)(g * h)(e) \\ &= (f * (g * h))(n). \end{aligned}$$

□

Theorem 12.5.3. Let ε be the function given by

$$\varepsilon(n) := \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

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. $\square$

12.6 Dirichlet Inverses

Definition 12.6.1. Consider an arithmetic function f such that $f(1)$ is nonzero. Then we define the *Dirichlet inverse* f^{-1} of f by

$$f^{-1}(1) := \frac{1}{f(1)} \quad \text{and} \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d \neq n}} f^{-1}(d) f\left(\frac{n}{d}\right) \quad (\text{for } n > 1).$$

Theorem 12.6.2. 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

$$f^{-1} * f = \varepsilon \quad \text{and} \quad f * f^{-1} = \varepsilon.$$

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

$$f^{-1} = f^{-1} * \varepsilon = f^{-1} * (f * g) = (f^{-1} * f) * g = \varepsilon * g = g. \quad \square$$

Example 12.6.3. The Dirichlet inverse of the constant function 1 is the Möbius function μ . Indeed, we saw in [Theorem 12.4.2](#) that $\mu * 1 = \varepsilon$.

Remark 12.6.4. If $f^{-1} = g$ for some arithmetic functions f and g , then it follows that $g^{-1} = f$. Indeed, the equations

$$f * g = \varepsilon \quad \text{and} \quad g * f = \varepsilon$$

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 12.6.5 (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

$$\begin{aligned} 1 * f &= 1 * (\mu * g) \\ &= (1 * \mu) * g \\ &= \varepsilon * g \\ &= g. \end{aligned}$$

□

Corollary 12.6.6. *Euler's totient function satisfies the identity*

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

*In other words, $\phi = \mu * \text{id}$.*

Proof. By [Theorem 17.1.1](#) we have $\text{id} = 1 * \phi$, so we have $\phi = \mu * \text{id}$ by the Möbius inversion formula. □

We also give a direct proof of [Corollary 12.6.6](#), offering a second perspective on the totient function.

Direct proof of Corollary 12.6.6. 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 12.4.2 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 . $\square$

Exercises

Starter Exercises

- 12.1 Compute $\phi(n)$ for $n = 1, \dots, 12$.
 12.2 Show that the number $\tau(n)$ of divisors of n is odd if and only if n is a square number.
 12.3 Compute $\mu * \sigma$.

Routine-Building Exercises

- 12.4 Let $M_n := 2^n - 1$ be the n th Mersenne number.
 (a) Show that if n is even, then $3 \mid M_n$.
 (b) Show that if $3 \mid n$, then $7 \mid M_n$.
 12.5 Show that any Mersenne prime $M_p = 2^p - 1$ with p an odd prime satisfies the congruence

$$M_p \equiv 7 \pmod{24}.$$

- 12.6 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

$$q \equiv 1 \pmod{2p}.$$

Hint: Apply the [Order Theorem](#).

- 12.7 (a) Show that

$$\sigma(p^m) \mid \sigma(p^n) \Leftrightarrow m + 1 \mid n + 1.$$

- (b) Let $d := \gcd(m + 1, n + 1)$. Show that

$$\gcd(\sigma(p^m), \sigma(p^n)) = \sigma(p^{d-1}).$$

- 12.8 (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

$$\sum_{\substack{a < n \\ \gcd(a, n) = 1}} a = \frac{n\phi(n)}{2}.$$

- 12.9 Prove that there is no positive integer $n < 2^{65}$ such that $\phi(n) = 2^{64}$.
 12.10 For any $d \mid \phi(n)$ such that $d > 2$, prove that

$$\prod_{\substack{0 < x < n \\ \text{ord}_n(x) = d}} x \equiv 1 \pmod{n}.$$

12.11 (a) Show that

$$\frac{\phi(n)}{2} \equiv 1 \pmod{2}$$

if and only if

$$n = 4, \quad \text{or} \quad n = p^k, \quad \text{or} \quad n = 2p^k,$$

where $p \equiv 3 \pmod{4}$ is a prime.

(b) Show that

$$\frac{\phi(n)}{2} \equiv 1 \pmod{4}$$

if and only if

$$n = 4, \quad \text{or} \quad n = p^k, \quad \text{or} \quad n = 2p^k,$$

where either $p \equiv 3 \pmod{8}$ and k is odd or $p \equiv 7 \pmod{8}$ and k is even.

12.12 Compute $\mu * \mu$.

12.13 Prove that

$$\sum_{k=1}^n \gcd(k, n) \mu(\gcd(k, n)) = \mu(n).$$

12.14 (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.

12.15 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

$$f^{-1}(p) = -f(p) \quad \text{and} \quad f^{-1}(p^2) = f(p^2) - f(p)^2$$

for every prime number p .

(c) Show that

$$f^{-1}(p^m) = \sum_{k=1}^m (-1)^k \left(\sum_{\substack{i_1 + \dots + i_k = m \\ i_1, \dots, i_k \geq 1}} f(p^{i_1}) \cdots f(p^{i_k}) \right).$$

12.16 Consider a prime p . Show that

$$\sum_{\substack{0 < n < p-1 \\ \gcd(n, p-1)=1}} a^n \equiv \mu(\text{ord}_p(a)) \frac{\phi(p-1)}{\phi(\text{ord}_p(a))} \pmod{p}.$$

12.17 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

$$A_n(k) := \sum_{d|k} \mu\left(\frac{k}{d}\right) R_n(d).$$

Challenge Exercises

12.18 Determine the number of reduced fractions $\frac{a}{b}$, where $0 \leq a \leq b \leq n$.

12.19 Consider the n th Fermat number $F_n = 2^{2^n} + 1$ and the m th Mersenne number $M_m = 2^m - 1$. Show that

$$\gcd(F_n, M_m) = \begin{cases} F_n & \text{if } 2^{n+1} \mid m, \\ 1 & \text{otherwise.} \end{cases}$$

12.20 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 $\gcd(a, b) = d$.

12.21 For how many congruence classes $b \pmod{n}$ is the linear congruence

$$ax \equiv b \pmod{n}$$

solvable?

12.22 (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 $p \nmid m$.

12.23 Show that

$$\sigma(2^n - 1) = \prod_{\substack{p \text{ odd prime} \\ d := \text{ord}_p(2) \mid n}} \frac{p^{v_p(2^d - 1) + v_p(n/d) + 1} - 1}{p - 1}.$$

12.24 Define *Jordan's totient function* $J_k(n)$ by

$$J_k(n) = \#\{(x_1, \dots, x_k) \mid 1 \leq x_1, \dots, x_k \leq n \text{ and } \gcd(x_1, \dots, x_k, n) = 1\}.$$

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 $1 \leq n \leq 12$.

(b) Show that for any divisor d of n , the number of elements in the set

$$\left\{ (x_1, \dots, x_k) \mid 1 \leq x_1, \dots, x_k \leq n \text{ and } \gcd(x_1, \dots, x_k, n) = \frac{n}{d} \right\}$$

is exactly $J_k(d)$.

(c) Show that

$$\sum_{d|n} J_k(d) = n^k \quad \text{and} \quad \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^k = J_k(n).$$

(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 $m \geq 1$.

(f) Show that

$$J_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k}\right).$$

12.25 Let Ω be the arithmetic function given by

$$\Omega(m) = m_1 + \dots + m_n$$

for any $m = p_1^{m_1} \cdots p_n^{m_n}$, where the prime factors $p_1, \dots, p_n$ 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.

Part V

Fermat's Discoveries Regarding the Primes

Chapter 13

Fermat's Little Theorem and its Consequences

13.1 Fermat's Little Theorem

Theorem 13.1.1 (Fermat's Little Theorem). *Consider a prime number p and an integer a . Then the congruence*

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

holds.

Remark 13.1.2. 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.

Fermat's 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 $a^p \equiv a \pmod{p}$. 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. $\square$

Golomb's combinatorial proof [[Gol1956](#)]. Consider a set A with a elements, and a cyclic set C with p elements. There are a^p functions from C to A . Each such function $f : C \rightarrow A$ can be viewed as a labelling of each of the elements of C by an element of A .

Since the set C is cyclically ordered, it is natural to consider two such labellings equivalent if one can be obtained from the other by rotating the cyclic set C . We indicated this equivalence in [Figure 13.1](#). We claim that the number of functions that are equivalent to a labelling f is always a

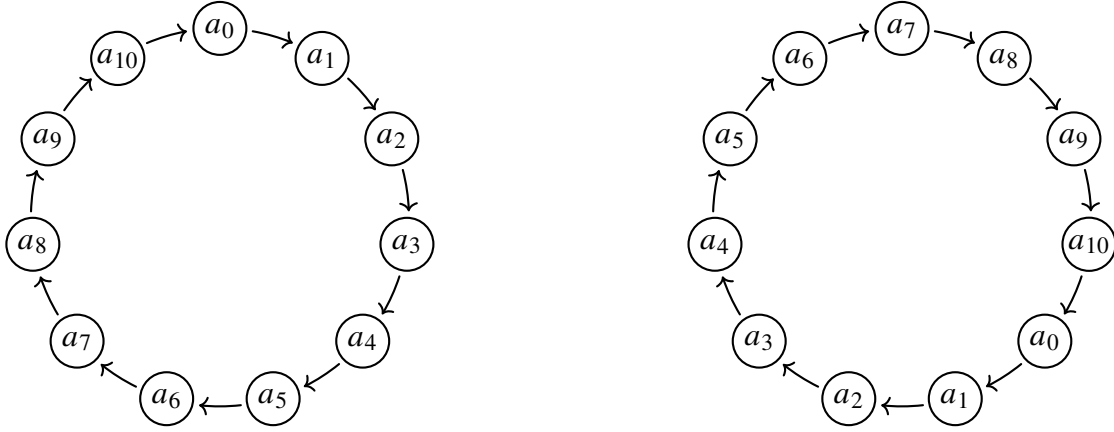


Figure 13.1: In Golomb's proof of Fermat's Little Theorem, two labellings of a cyclic set C with elements from a set A are considered the same—or equivalent—if one can be obtained from the other by rotation.

divisor of the number of elements of C , which is p . Indeed, if $s : C \rightarrow C$ is the one-step rotation, then the number of functions equivalent to f is equal to the least positive integer k such that

$$f \circ s^k = f.$$

Moreover, since s^p is the identity on C , we always have $f \circ s^p = f$, and therefore $k \mid p$. By the assumption that p is prime, there are two possibilities:

- (i) In the first case, f is the only function equivalent to itself. This is the case if and only if f is constant.
- (ii) In the second case, there are exactly p functions equivalent to f , including f itself. This is the case if and only if f is nonconstant.

Now note that the number of constant functions from C to A is exactly a . The number of nonconstant functions is therefore $a^p - a$. Since the nonconstant functions are partitioned into equivalence classes of size p , it follows that $a^p - a$ is divisible by p . $\square$

Corollary 13.1.3. *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

$$ax \equiv ay \pmod{p} \quad \Rightarrow \quad x \equiv y \pmod{p}. \quad \square$$

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 13.1.4. *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 the that $\text{ord}_p(2) \mid 2^{n+1}$. In particular, $\text{ord}_p(2) = 2^k$ for some number $k \leq n + 1$. However, note that

$$2^{2^k} \equiv 1 \pmod{p} \quad \text{implies} \quad 2^{2^{k+1}} = (2^{2^k})^2 \equiv 1 \pmod{p}.$$

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 $\text{ord}_p(2) = 2^{n+1}$. By [Fermat's Little Theorem](#), we conclude that

$$2^{n+1} \mid p - 1. \quad \square$$

Corollary 13.1.5. *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 11.1](#) reveals that the only two primes $p \equiv 1 \pmod{33}$ below 256 are 97 and 193. A quick computation gives that

$$F_4 \equiv 62 \pmod{97} \quad \text{and} \quad F_4 \equiv 110 \pmod{193},$$

so that neither 97 nor 193 is a prime divisor of F_4 , and therefore we conclude that F_4 is prime. $\square$

Corollary 13.1.6. *The fifth Fermat number $2^{2^5} + 1 = 4,294,967,297$ is composite, and its smallest prime factor is 641.*

Proof. By [Theorem 13.1.4](#) 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 11.1](#). 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 $\text{ord}_{193}(3) = 16$. It follows that

$$1 \equiv 3^{16} \equiv (-2)^{6 \cdot 16} \equiv 2^{96} \pmod{193},$$

which allows us to conclude that $\text{ord}_{193}(2) \mid 96$. Now observe that if $193 \mid F_5$ so that $2^{32} \equiv -1 \pmod{193}$, then we'd have $\text{ord}_{193}(2) = 64 \nmid 96$, a contradiction.

- (ii) Note that 257 is itself a Fermat number. In [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 13.1.7. Édouard Lucas showed that any prime divisor $p \mid F_n$ of the n th 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!

13.2 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 13.2.1 (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 $r_1, \dots, r_{\phi(n)}$ modulo n . We claim that

$$ar_1, \dots, ar_{\phi(n)}$$

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 $ar_1, \dots, ar_{\phi(n)}$ 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 $ar_1, \dots, ar_{\phi(n)}$ 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 $a^{\phi(n)} \equiv 1 \pmod{n}$. $\square$

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

$$b \sim c \quad \text{if and only if} \quad \exists_{0 \leq i < k} ba^i \equiv c \pmod{n}.$$

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

$$\{b, ba, ba^2, \dots, ba^{k-1}\}$$

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 $a^{\phi(n)} \equiv 1 \pmod{n}$. $\square$

Remark 13.2.2. 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

$$(xy)z = x(yz)$$

$$x1 = x$$

$$1x = x$$

$$xx^{-1} = 1$$

$$x^{-1}x = 1.$$

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 $\{1, a, a^2, \dots, a^{k-1}\}$ 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 [Fermat's Little Theorem](#) is also a direct corollary of [Euler's Theorem](#).

Remark 13.2.3. We saw the multiplicative order featuring in the second proof of [Euler's Theorem](#). Thus, using the second proof of Euler's theorem we immediately observe that

$$\text{ord}_n(a) \mid \phi(n),$$

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](#)].

13.3 Wilson's Theorem

The following theorem 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 13.3.1 (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 11.6](#) 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. $\square$

13.4 Lucas's Theorem

[Kummer's Theorem](#) gave a complete description of the prime factorization of binomial coefficients. In principle, this is sufficient to know the congruence class of $\binom{n}{m}$ modulo a prime p . In the following theorem, which is due to Édouard Lucas, we establish a way of determining the congruence class of the binomial coefficient modulo p . If this congruence class is shown to be 0, the p -valuation can be computed precisely with Kummer's Theorem.

Theorem 13.4.1. *Consider a prime number p , and natural numbers m and n written in base p as*

$$m = \sum_{i=0}^k a_i p^i \quad \text{and} \quad n = \sum_{i=0}^k b_i p^i.$$

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. Recall from the [Binomial Theorem](#) that $\binom{n}{m}$ is the coefficient of the x^m -term in $(x + 1)^n$. We will prove the asserted congruence by computing this coefficient in another way.

By [Fermat's Little Theorem](#) it follows that $a^{p^k} \equiv a \pmod{p}$. This implies that

$$(a + b)^{p^k} \equiv a + b \equiv a^{p^k} + b^{p^k} \pmod{p}.$$

Using the base- p representation $n = \sum_{i=0}^k b_i p^i$ of n , we find that

$$(x + 1)^n = \prod_{i=0}^k (x + 1)^{b_i p^i} \equiv \prod_{i=0}^k (x^{p^i} + 1)^{b_i} \pmod{p}.$$

Expanding the polynomial $(x^{p^i} + 1)^{b_i}$ we obtain:

$$(x + 1)^n \equiv \prod_{i=0}^k \sum_{t_i=0}^{p-1} \binom{b_i}{t_i} x^{t_i p^i} \equiv \sum_{0 \leq t_0, \dots, t_k < p} \left(\prod_{i=0}^k \binom{b_i}{t_i} \right) x^{\sum_{i=0}^k t_i p^i} \pmod{p}.$$

Since every number has a unique representation base p , we see that the coefficient of x^m is $\prod_{i=0}^k \binom{b_i}{b_i}$, and thus we obtain:

$$\binom{n}{m} \equiv \prod_{i=0}^k \binom{b_i}{b_i} \pmod{p}.$$

□

13.5 The Quadratic Character of -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](#)], 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 [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



Figure 13.2: Carl Friedrich Gauss. Pastel painting by Johann Christian August Schwartz, 1803.

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 18 and 19](#).

Theorem 13.5.1 (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 [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 [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 . $\square$

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, and 137.

Theorem 13.5.2. *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 $1 \leq i \leq k$. 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. $\square$

Theorem 13.5.1 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 13.5.3. *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 13.5.1**. 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 $b := a^{2^m}$ 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 **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 $\{1, \dots, p-1\}$ into classes of 2^{k+1} numbers of the form $\{x, ax, \dots, a^{2^{k+1}-1}x\}$. 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 **Wilson's Theorem** that

$$-1 \equiv (p-1)! \equiv \prod_{i=1}^c \prod_{j=0}^{2^{k+1}-1} a^j x_i \equiv \prod_{i=1}^c (-1) x_i^{2^{k+1}} \equiv (-1)^c \prod_{i=1}^c x_i^{2^{k+1}} \equiv \left(\prod_{i=1}^c x_i \right)^{2^{k+1}} \pmod{p}. \quad \square$$

13.6 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

$$\text{ord}_p(a) = n.$$

By the [Order Theorem](#) and [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 13.6.1. *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 $p_1, \dots, p_k$ 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 $\text{ord}_q(a) \mid 2^{n+1}$, while clearly $\text{ord}_q(a) \nmid 2^n$. Thus, we must have $\text{ord}_q(a) = 2^{n+1}$, and this allows us to conclude that $q \equiv 1 \pmod{2^{n+1}}$. $\square$

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

13.1 For every prime $p \equiv 1 \pmod{4}$ below 100, find the least positive integer a such that $a^2 \equiv -1 \pmod{p}$.

13.2 (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.

13.3 (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

13.4 Show that

$$2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \pmod{p}$$

for any prime number $p \neq 3$.

13.5 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

$$\sum_{k=1}^{p-1} q_p(k) \equiv W_p \pmod{p}.$$

13.6 Show that

$$3^{3^{3^3}} \equiv 3^{3^3} \pmod{97}.$$

13.7 (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.

13.8 Prove that if

$$a^n \equiv a \pmod{n}$$

for every integer a , then $n = 2$ or n is odd.

13.9 Consider two distinct primes p and q , and an integer $a \geq 0$. Prove that

$$a^{pq} + a \equiv a^p + a^q \pmod{pq}$$

13.10 Consider an odd prime $p = 2n + 1$. Show that

$$\binom{2n}{n} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

13.11 Consider a prime p and two numbers m and n . Prove that

$$\binom{p^k n}{p^k m} \equiv \binom{n}{m} \pmod{p}.$$

13.12 Show that the congruence

$$\sum_{k=1}^n k^n \equiv 0 \pmod{n}$$

holds if and only if n is odd.

13.13 (a) Consider a prime p and an integer $p \nmid a$. Show that

$$a^p \equiv a \pmod{p^2} \iff a^{p^2} \equiv a \pmod{p^2}.$$

(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

13.14 Find the least integer $k > 1$ such that every integer of the form $x^k - x$ is divisible by 47 and 89.

13.15 Find a prime $p > 3$ such that

$$3^{3^3} \equiv 3^3 \pmod{p}.$$

13.16 For any integer a and any prime number p , show that

$$a^{p^k} \equiv a^{p^{k-1}} \pmod{p^k}.$$

13.17 Find all the solutions to the equation

$$p^q - q^p = p + q,$$

where p and q are prime numbers.

13.18 Consider two primes p and q . Show that

$$pq \mid (13^p - 5^p)(13^q - 5^q) \quad \Leftrightarrow \quad pq \mid 12.$$

13.19 (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

$$3^{24} - 1.$$

13.20 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.

13.21 (a) Consider an odd prime q . Show that the numbers

$$2^q - 1 \quad \text{and} \quad q + 1.$$

are relatively prime.

(b) Consider two distinct primes p and q , and let r be a common prime divisor of the numbers

$$\frac{p^q - 1}{p - 1} \quad \text{and} \quad \frac{q^p - 1}{q - 1}.$$

Show that $r \equiv 1 \pmod{2pq}$.

Chapter 14

Fermat's Two-Squares Theorem

14.1 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 14.1](#).

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 14.1.1. *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 $p \mid b$.*

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 $p \mid b$. $\square$

The previous lemma can be used to find an obstruction to numbers being representable as a sum of two squares.

Corollary 14.1.2. *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.*

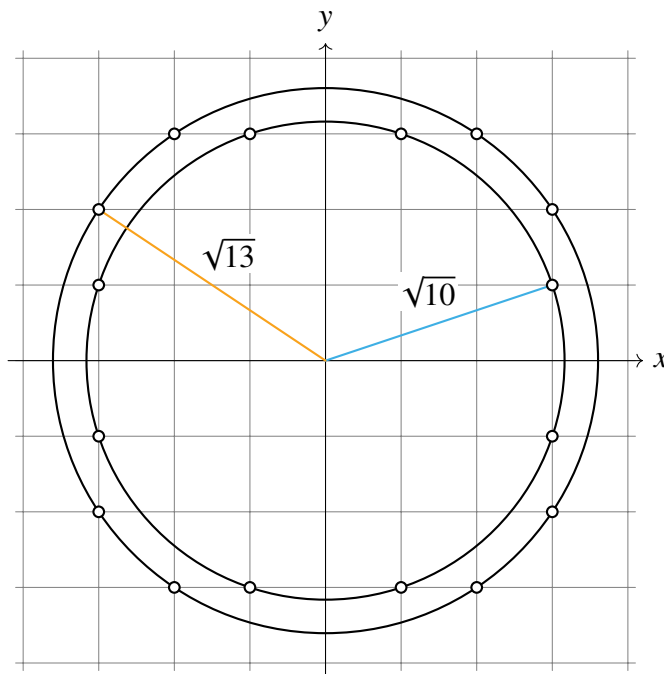


Figure 14.1: Representing a number as a sum of two squares is equivalent to finding an integer lattice point on the circle of radius $\sqrt{n}$. Here we displayed the integer lattice points on the circles of radii $\sqrt{10}$ and $\sqrt{13}$.

Proof. By [Lemma 14.1.1](#) it follows that if n is divisible by a prime $p \equiv 3 \pmod{4}$, then we also have $p^2 \mid n$. Writing $n = p^2 n'$, $a = pa'$ 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. $\square$

One of Fermat's most remarkable discoveries was that the statement in [Corollary 14.1.2](#) 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 14.1.3. 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 14.1.2](#) 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 14.1.4. *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 (mod 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 ??.

Lemma 14.1.5 (The Brahmagupta–Fibonacci Identity). *For any 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:

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= a^2c^2 \pm 2abcd + b^2d^2 + a^2d^2 \mp 2abcd + b^2c^2 \\ &= (ac \pm bd)^2 + (ad \mp bc)^2. \end{aligned} \quad \square$$

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:

$$65 = 1^2 + 8^2 \quad \text{and} \quad 65 = 4^2 + 7^2.$$

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, something stronger is true: Every prime $p \equiv 1 \pmod{4}$ can be *uniquely* represented as a sum of two squares.

Proposition 14.1.6. *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

$$(xy^{-1})^2 \equiv -1 \pmod{p} \quad \text{and} \quad (uv^{-1})^2 \equiv -1 \pmod{p}.$$

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 $y = v$. $\square$

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

$$0, a, 2a, 3a, \dots, ma$$

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 .

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 14.1.7 (Thue's Lemma). *Consider two positive integers a and n such that $\gcd(a, n) = 1$. For any natural number m , there is some $1 \leq k \leq m$ such that*

$$|ka|_n \leq \frac{n}{m+1}.$$

Proof. We will assume that $m < n$, for if m is greater then we find $|na|_n = 0$. For each $0 \leq i, j \leq m$, write $d_{i,j} := |(i-j)a|_n$ be the distance to the nearest multiple of n from the difference between

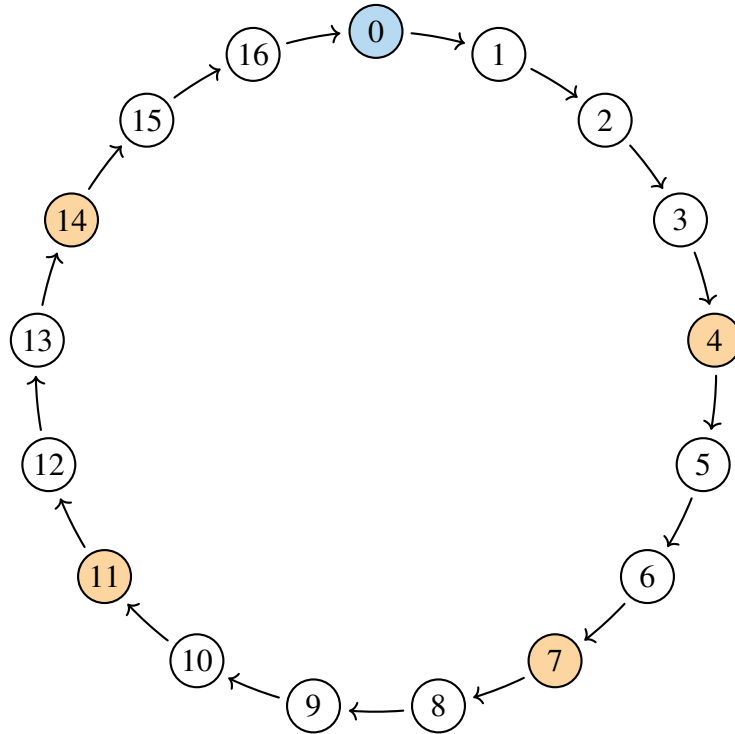


Figure 14.2: By Thue's lemma, in any set of m multiples $\{a, 2a, \dots, ma\}$ modulo any prime p , there is one multiple whose cyclic distance to 0 does not exceed $\frac{p}{m+1}$. Here we see that there is a number of the form $k \cdot 7$, for $1 \leq k \leq 4$, whose cyclic distance to 0 is 3, which is indeed below $\frac{17}{5}$.

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 $0 \leq i, j \leq m$ such that

$$d_{i,j} = |(i - j)a|_n \leq \frac{n}{m + 1}.$$

Now define $k := j - i$. Then we clearly have $0 < k \leq m$, and we have

$$|ka|_n = |(i - j)a|_n \leq \frac{n}{m + 1}.$$

□

Theorem 14.1.8. 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 [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. $\square$

Theorem 14.1.9 (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 (mod 4).*

We will give three more proofs of Fermat's Two-Squares Theorem in remainder of this chapter.

14.2 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 14.1.8. 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 13.5.1 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

$$u \equiv a \pmod{r}, \quad v \equiv b \pmod{r}, \quad \text{and} \quad |u|, |v| \leq \frac{r}{2}.$$

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 (mod 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 $(a^2 + b^2)(u^2 + v^2) = r^2 sp$. 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. $\square$

Exercises

Starter Exercises

- 14.1 For every prime $p \equiv 1 \pmod{4}$ below 100, write p as a sum of two squares.
14.2 Show that no odd prime p can be written as a sum of two cubes.

Routine-Building Exercises

- 14.3 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 1.6](#).

Part VI

The Law of Quadratic Reciprocity

Chapter 15

Polynomials

15.1 Polynomials with Integer Coefficients

Definition 15.1.1. An *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 integers a_k are called the *coefficients* of $f(x)$. The *zero polynomial* is the constant polynomial $f(x) = 0$ and the *unit polynomial* is the constant polynomial $f(x) = 1$.

The coefficients of a polynomial may be taken from any number system. When we wish to specify that the coefficients are integers or rational numbers. In such cases we speak of *polynomials with integer coefficients* or *polynomials with rational coefficients*.

There is a subtle, yet important distinction between polynomials and the functions they describe, which has to do with equality of polynomials. Two polynomials

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \quad \text{and} \quad b_n x^n + b_{n-1} x^{n-1} + \cdots + b_0$$

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 [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 15.3.3](#) that two polynomials with integer coefficients have equal coefficients if and only if they define equal functions.

Definition 15.1.2. A function $f : \mathbb{Z} \rightarrow \mathbb{Z}$ is said to be *polynomial in the integers* if there is a polynomial with integer coefficients such as the above, such that

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

for all $x \in \mathbb{Z}$.

Remark 15.1.3. 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, polynomials satisfy the laws of arithmetic. More precisely, the polynomials with integer coefficients form a commutative ring. We say that a polynomial $g(x)$ *divides* a polynomial $f(x)$ if there is a polynomial $h(x)$ such that

$$f(x) = g(x)h(x).$$

Definition 15.1.4. A *root* of a polynomial $f(x)$ is a number 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 number system. However, to keep the statement concrete we will state the factor theorem only for polynomials with integer coefficients.

Theorem 15.1.5 (Factor Theorem). *Consider a nonzero polynomial $f(x)$ of degree n with integer coefficients. An integer r is a root of $f(x)$ if and only if there is a polynomial $g(x)$ of degree $n - 1$ with integer coefficients 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 no polynomial $g(x)$ of degree -1 such that $f(x) = (x - r)g(x)$.

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 k th powers, which was stated in [Exercise 1.5](#), we can factor $x^k - r^k$ as

$$x^k - r^k = (x - r)q_k(x), \quad \text{where} \quad q_k(x) = \sum_{i=0}^{k-1} x^i r^{k-1-i}$$

is a polynomial of degree $k - 1$. Now define $g(x) := \sum_{k=1}^n a_k q_k(x)$. Then we compute

$$(x - r)g(x) = \sum_{k=1}^n a_k (x - r)q_k(x) = \sum_{k=1}^n a_k (x^k - r^k) = f(x) - f(r) = f(x). \quad \square$$

The [Factor Theorem](#) has some important corollaries. One of them states that a polynomial of degree n has at most n roots, and the second is a factor theorem for modular arithmetic, which we will establish in [Theorem 16.1.1](#).

Corollary 15.1.6. *A polynomial of degree n with integer coefficients 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 the [Factor Theorem](#), where $g(x)$ is a polynomial of degree n . Then the product $(x - r)g(x) = 0$ if and only if $x - r = 0$ or $g(x) = 0$. Thus we see that x is a root of $f(x)$ if and only if $x = r$ or x is a root of $g(x)$, so there are at most $n + 1$ roots of the polynomial $f(x)$. $\square$

15.2 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

$$f'(x) := \lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h}$$

Intuitively, such a limit exists if we can determine a unique value $y = f'(x)$ so that the quantity $(f(x+h) - f(x))/h$ 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 requires knowledge of the derivatives of polynomials: In our proof of [Hensel's Lemma](#) we will make use of the [Taylor Expansion Theorem](#) 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 15.2.1. 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 k th powers, which was stated in [Exercise 1.5](#), 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 k th powers is divisible by h , we see that the polynomial $f(x+h) - f(x)$ is divisible by h . It follows that

$$f(x+h) - f(x) = \sum_{k=0}^n a_k ((x+h)^k - x^k) = h \sum_{k=1}^n a_k \sum_{i=0}^{k-1} x^i (x+h)^{k-1-i}. \quad \square$$

Theorem 15.2.2. 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 $h \rightarrow 0$ 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 $h(x) = a f(x) + b g(x)$ is a linear combination of the polynomials $f(x)$ and $g(x)$, then the derivative of h can be written as the linear combination

$$h'(x) = a f'(x) + b g'(x).$$

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 k th derivative 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 15.2.3 (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

$$f(x+y) = f(x) + y f'(x) + y^2 g(x, y).$$

Proof. We will first prove the theorem for $f(x) := x^n$. By 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

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k = \sum_{k=0}^n \frac{1}{k!} \frac{d^k}{dx^k} x^n y^k.$$

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, the polynomial $g(x, y)$ is given by the tail of the series:

$$g(x, y) = \sum_{k=2}^n \frac{f^{(k)}(x)}{k!} y^{k-2}.$$

□

15.3 Lagrange's Interpolation Theorem

Lagrange's Interpolation Theorem establishes that for any set of data points, as illustrated in [Figure 15.1](#), 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

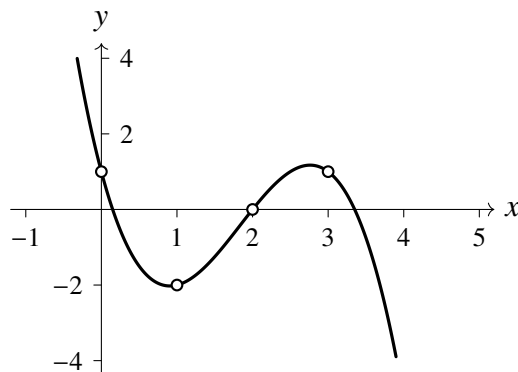


Figure 15.1: A polynomial of degree 3 obtained by Lagrange interpolation.

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 15.3.1. In [Figure 15.1](#), we started with the set of points

$$(0, 1), (1, -2), (2, 0), (3, 1).$$

Then we define the polynomials

$$g_0 := \frac{1}{6}(x - 1)(x - 2)(x - 3)$$

$$g_1 := -x(x - 2)(x - 3)$$

$$g_2 := 0$$

$$g_3 := \frac{1}{6}x(x - 1)(x - 2),$$

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 15.3.2 (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 $0 \leq i \leq n$.

Proof. For any $0 \leq i \leq n$, 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 15.1.6](#) this is only possible if $f(x) - g(x)$ is the zero polynomial, that is, if $f(x) = g(x)$. $\square$

Corollary 15.3.3. *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

$$f(0), \dots, f(n).$$

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

$$f(0), \dots, f(n)$$

are integers, then $f(x)$ is an integer for every integer x .

Definition 15.3.4. 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

$$f(x) = \sum_{k=0}^n f(k)g_k(x).$$

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 15.3.5. Consider a polynomial $f(x)$. Then each value $f(x)$ can be written as a linear combination of the values $f(0), \dots, f(n)$; 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 $f(0), \dots, f(n)$ are integers.

Theorem 15.3.6. 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 [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. □

15.4 Fixed Divisors of Integer Polynomials

In [Chapter 5](#), 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 15.4.1. The *fixed divisor* of a function $f : X \rightarrow \mathbb{Z}$ into the integers is the greatest common divisor of all values of f , i.e.,

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

[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 15.4.2 (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 x -axis, 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 15.3.6](#) 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. $\square$

Example 15.4.3. 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

$$f(0), \dots, f(m),$$

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 5.15](#) 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 5.16](#) has the values

$$f(2) = 30 \quad \text{and} \quad f(3) = 240.$$

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

$$f(2) = 126 \quad \text{and} \quad f(3) = 2184.$$

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 ??.

Exercises

Routine-Building Exercises

15.1 Show that $x^{13} - x$ has fixed divisor

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13.$$

15.2 *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.

Chapter 16

Polynomial Congruences

16.1 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 16.1.1 (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 15.1.5](#). 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 15.1.5](#). $\square$

Theorem 16.1.2 (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 the [Factor Theorem for 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 11.1.4](#) 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 $f(x) \equiv 0 \pmod{p}$. $\square$

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 [Lagrange's Theorem](#) establishes an upper bound for the number of incongruent solutions of a polynomial congruence modulo a prime, we can use [Fermat's Little Theorem](#) to find examples of polynomial congruences that have the maximum allowable number of solutions.

Theorem 16.1.3. *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

$$x^n - 1 \equiv 0 \pmod{p} \quad \text{and} \quad q(x) \equiv 0 \pmod{p}$$

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. $\square$

Lagrange's Theorem can also be used to give another proof of **Theorem 13.5.1**, 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 13.5.1. 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 **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 . $\square$

16.2 Polynomial Congruences of Composite Moduli

In the following theorem we generalize the **Chinese Remainder Theorem** to polynomial congruences.

Theorem 16.2.1. *Consider an integer polynomial f and consider two relatively prime integers m and n . Then any solution of the system*

$$\begin{aligned} f(x) &\equiv 0 \pmod{m} \\ f(x) &\equiv 0 \pmod{n} \end{aligned}$$

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 $f(y) \equiv 0 \pmod{m}$ 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

$$\pi : N_{mn}(f) \rightarrow N_m(f) \times N_n(f)$$

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

$$\begin{aligned} f(y) &\equiv 0 \pmod{m} \\ f(z) &\equiv 0 \pmod{n}. \end{aligned}$$

By the assumption that $\gcd(m, n) = 1$, we obtain from the [Chinese Remainder Theorem](#) there a unique $0 \leq x < mn$ such that

$$\begin{aligned} x &\equiv y \pmod{m} \\ x &\equiv z \pmod{n}. \end{aligned}$$

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 $f(x) \equiv 0 \pmod{mn}$. $\square$

Corollary 16.2.2. 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 . $\square$

16.3 Hensel's Lemma

Theorem 16.3.1 (Hensel's Lemma). Consider a prime number p and a polynomial $f(x)$ with integer coefficients. Furthermore, consider an integer a such that

$$f(a) \equiv 0 \pmod{p} \quad \text{and} \quad f'(a) \not\equiv 0 \pmod{p},$$

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

$$a_{k+1} \equiv a_k \pmod{p^k}, \quad \text{and} \quad f(a_k) \equiv 0 \pmod{p^k}$$

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

$$f(a_k) \equiv 0 \pmod{p^k} \quad \text{and} \quad f'(a_k) \not\equiv 0 \pmod{p^k},$$

there is a unique integer $a_{k+1} \pmod{p^{k+1}}$ satisfying

$$f(a_{k+1}) \equiv 0 \pmod{p^{k+1}} \quad \text{and} \quad f'(a_{k+1}) \not\equiv 0 \pmod{p^{k+1}}.$$

Our goal is to obtain an integer $a_{k+1} = a_k + tp^k$ for some $0 \leq t < p$. Observe that by the [Taylor Expansion Theorem](#), 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. $\square$

Exercises

Routine-Building Exercises

- 16.1 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 $x = 0$.
- 16.2 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 .
- 16.3 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 [Lagrange's Interpolation Theorem](#) to show that every function $\mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ is polynomial.

- 16.4 Define the k th power sum

$$p_k(a_1, \dots, a_n) := a_1^k + \dots + a_n^k.$$

We will simply write p_k for $p_k(a_1, \dots, a_n)$ and e_k for $e_k(a_1, \dots, a_n)$.

- (a) *The Newton-Girard identities.* Show that for all k we have

$$p_k = e_1 p_{k-1} - e_2 p_{k-2} + \dots + (-1)^{k-1} e_{k-1} p_1 + (-1)^{k-1} k e_k.$$

Hint: This looks more complicated than it is.

- (b) Prove that the congruence

$$1^k + \dots + (p-1)^k \equiv 0 \pmod{p}$$

holds for every $0 < k < p-1$, and every prime number p .

Chapter 17

Primitive Roots

17.1 Counting Elements of a Given Order Modulo a Prime

Euler's Theorem tells us that

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

for every integer a such that $\gcd(a, n) = 1$. By the Order Theorem, this implies that

$$\text{ord}_n(a) \mid \phi(n).$$

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 $\text{ord}_{13}(2) = 12$:

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 17.1. Using Theorem 9.5.4, we can use this table to compute the orders of all the nonzero integers modulo 13. Recall that Theorem 9.5.4 states that

$$\text{ord}_n(a^m) = \frac{\text{ord}_n(a)}{\gcd(m, \text{ord}_n(a))}.$$

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
$\text{ord}_{13}(a)$	1	12	3	6	4	12	12	4	3	6	12	2.

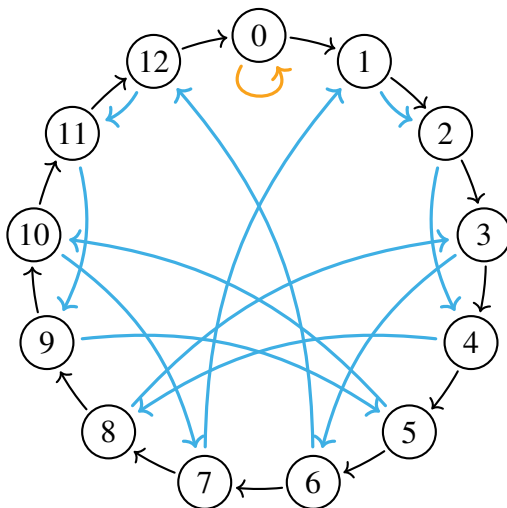


Figure 17.1: Doubling integers modulo 13.

While the orders of the integers modulo 13 might at first glance appear to be somewhat unwieldy, [Theorem 9.5.4](#) is the key to some important patterns. For example, given an integer $a \pmod{p}$ with $\text{ord}_p(a) = p - 1$ such as $2 \pmod{13}$, [Theorem 9.5.4](#) tells us that

$$\text{ord}_p(a^m) = k \Leftrightarrow \frac{p-1}{\gcd(m, p-1)} = k$$

In particular, $\text{ord}_p(a^m) = p - 1$ 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 proposition 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 $\phi(k)$. To make this observation precise, we first need a fundamental property of the totient function.

Theorem 17.1.1. *For every positive integer n , we have*

$$\sum_{d \mid n} \phi(d) = n,$$

where the sum ranges over the positive integers d dividing n .

In terms of Dirichlet convolution, the identity in [Theorem 17.1.1](#) can be stated as follows:

$$\phi * 1 = \text{id}.$$

We will give a combinatorial and an arithmetic proof.

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

$$f_d : \{1 \leq x \leq d \mid \gcd(x, d) = 1\} \rightarrow \{1, \dots, n\}$$

by $x \mapsto \frac{n}{d}x$, and define the set A_d to be the image of f_d . Since $\frac{n}{d}$ is a positive integer, it follows that the map f_d is injective, and therefore each set A_d has exactly $\phi(d)$ elements. Now notice that

$$y \in A_d \quad \Leftrightarrow \quad \gcd(y, n) = \frac{n}{d},$$

since if $x = y/\gcd(y, n)$, then $\gcd(x, d) = \gcd(y/\gcd(y, n), n/\gcd(y, n)) = 1$. Therefore, it follows that for every $1 \leq y \leq n$ there is exactly one $d \mid n$ such that $y \in A_d$, so it follows that the sets A_d partition the set $\{1, \dots, n\}$. The sum of the numbers of elements of each A_d is therefore n . $\square$

Arithmetic proof. Recall from [Theorem 12.2.4](#) that ϕ is a multiplicative function, which implies by [Theorem 12.3.4](#) that the function

$$n \mapsto \sum_{d \mid n} \phi(d)$$

is multiplicative. Since multiplicative functions are completely determined by their values on prime powers, it suffices to show that

$$\sum_{d \mid p^m} \phi(d) = p^m.$$

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

$$\sum_{d \mid p^m} \phi(d) = \sum_{k=0}^m \phi(p^k) = 1 + \sum_{k=1}^m (p^k - p^{k-1}) = 1 + (p^m - 1) = p^m. \quad \square$$

Theorem 17.1.2. *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 16.1.3](#). To emphasize this observation, we will prove [Theorem 17.1.2](#) as a consequence of the following more general theorem.

Theorem 17.1.3. *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 the [Order Theorem](#) and [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:

$$1, a, \dots, a^{k-1}.$$

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 9.5.4](#) 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 $k \mid \phi(n)$. $\square$

17.2 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 17.2.1. A *primitive root* modulo a natural number n is an integer g such that

$$\text{ord}_n(g) = \phi(n).$$

Theorem 17.2.2. 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 17.1.3. 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 $\text{ord}_n(g) = \phi(n)$, it follows from the 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 $x^d \equiv 1 \pmod{n}$. $\square$

Corollary 17.2.3. The number of primitive roots of a prime number p is $\phi(p-1)$. In particular, every prime p admits a primitive root.

Example 17.2.4. The number 9 has the primitive root 2. Indeed $\phi(9) = 6$, and $2^3 \equiv -1 \pmod{9}$ so that $\text{ord}_9(2) = 6$. 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 $x \equiv 1, 4, \text{ and } 7 \pmod{9}$.

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 17.4.5.

17.3 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 $0 \leq i < \phi(n)$. Having a primitive root therefore gives a convenient way of representing all the elements of a reduced residue system.

Definition 17.3.1. 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*

$$\text{ind}_g(a)$$

of a base g to be the unique integer k modulo $\phi(n)$ such that $g^k = a$.

Theorem 17.3.2. Consider a natural number n with a primitive root g .

(i) For any two integers a and b relatively prime to n , we have

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad \text{ind}_g(a) \equiv \text{ind}_g(b) \pmod{\phi(n)}.$$

(ii) Furthermore, we have

$$\begin{aligned} \text{ind}_g(ab) &\equiv \text{ind}_g(a) + \text{ind}_g(b) \pmod{\phi(n)} \\ \text{ind}_g(a^m) &\equiv m \text{ind}_g(a) \pmod{\phi(n)}. \end{aligned}$$

Example 17.3.3. 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

$$\text{ind}_2(7) + \text{ind}_2(x) \equiv \text{ind}_2(3) \pmod{12}.$$

Since $\text{ind}_2(7) = 11$ and $\text{ind}_2(3) = 4$, we find that $\text{ind}_2(x) \equiv 5 \pmod{12}$. Thus, we conclude that

$$x \equiv 6 \pmod{13}$$

is a solution of the original linear congruence.

17.4 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.

17.4.1 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.

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 17.4.1. *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 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

$$v_p(a^p - b^p) = s + 1. \quad \square$$

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 [\[Man2006\]](#).

Lemma 17.4.2 (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 17.4.1](#). $\square$

Recall that for any integer a not divisible by p , the integer $a^{p-1} - 1$ is divisible by p by [Theorem 13.1.1](#). 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 17.4.3. *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 $\text{ord}_p(g) \mid \text{ord}_{p^k}(g)$, 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 the [Lifting the Exponent Lemma](#) 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 $r = p^{\max(0, k-m)}(p-1)$. $\square$

Theorem 17.4.4. *Any prime power p^k with $k \geq 1$ admits a primitive root.*

Proof. By [Lemma 17.4.3](#) 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

$$v_p(h_t^{p-1} - 1) = 1. \quad \square$$

17.4.2 The Complete Characterization of Moduli with Primitive Roots

Theorem 17.4.5. *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 17.2.2](#) 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 :

$$x = -1 \quad \text{and} \quad x = 2^{k-1} \pm 1.$$

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 the [Chinese Remainder Theorem](#), it follows that any pair of solutions

$$\begin{aligned} x^2 &\equiv 1 \pmod{k}, \\ y^2 &\equiv 1 \pmod{m}, \end{aligned}$$

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 17.4.4](#). 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

$$\text{ord}_{2p^k}(g) = \text{ord}_{p^k}(g) = p^{k-1}(p-1) = \phi(2p^k),$$

so we see that g is also a primitive root of $2p^k$. □

17.5 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 n th degree congruence

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

The following theorem is a significant generalization of [Euler's Criterion](#).

Theorem 17.5.1. *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*

$$\frac{p-1}{\text{ord}_p(a)} \equiv 0 \pmod{\gcd(n, p-1)}$$

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 $m := (p-1)/\text{ord}_p(a)$, 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 10.1.2](#) 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 $\gcd(n, p-1) \mid m$. $\square$

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 [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 k th 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

$$y^n = x^{vld} \equiv a^{lv} \equiv a^{1-ku} \equiv a(a^k)^{-u} \equiv a1^{-u} \equiv a \pmod{p}.$$

$\square$

Corollary 17.5.2. *Consider an integer a such that $\text{ord}_p(a) \mid n$. Then the congruence*

$$x^n \equiv a \pmod{p}$$

is solvable if and only if

$$p \equiv 1 \pmod{\text{ord}_p(a) \cdot \gcd(n, p-1)}.$$

Corollary 17.5.3. *Consider a prime p and a natural number n relatively prime to $p-1$. Then every n th 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

$$x^n \equiv -1 \pmod{p}$$

is solvable if and only if $p \equiv 1 \pmod{2^{k+1}}$.

Corollary 17.5.4. *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

- 17.1 (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 $1, \dots, 22$, find its index base g modulo 23.
 (e) Solve the linear congruence

$$8x \equiv 9 \pmod{23}$$

using indices.

- 17.2 (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

- 17.3 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 [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

$$\text{ord}_p(a_i) = q_i^{\alpha_i}.$$

- (b) Show that

$$\text{ord}_p(a_1 \cdots a_n) = p-1$$

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.

17.4 Consider a prime $p \neq 3$. Prove that the product of all primitive roots modulo p is congruent to 1 modulo p .

17.5 (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 $\text{ord}_p(a)$.

(b) Find a solution to the congruence

$$x^3 \equiv 5 \pmod{13}$$

of the form $x = 5^k$.

Challenge Exercises

17.6 For any prime p and any integer a not divisible by p , show that the number of primitive roots g modulo p such that

$$g^{\frac{p-1}{\text{ord}_p(a)}} \equiv a \pmod{p}.$$

is $\phi(p-1)/\phi(\text{ord}_p(a))$. Conclude that such a primitive root always exists.

17.7 Consider a prime $p > 2$ and an odd number m . Show that the congruence $x^{2^m} \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{2^{m+1}}$.

17.8 Consider a prime p of the form $n^2 + 1$. Show that

$$x^n \equiv a \pmod{p} \text{ is solvable} \quad \Leftrightarrow \quad a^n \equiv 1 \pmod{p}.$$

17.9 [Gau1986, art. 81] Consider a prime p . Prove that the sum of all primitive roots satisfies the following property:

$$\sum_{g \text{ primitive root (mod } p)} g \equiv \mu(p-1) \pmod{p}.$$

17.10 [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 the [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 18

Quadratic Residues

18.1 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 18.1.1. *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 [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 18.1.2. *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. $\square$

18.2 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 18.2.1. 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 18.2.2. Consider a prime p with a primitive root g . An integer $a \not\equiv 0 \pmod{p}$ is a nontrivial quadratic residue modulo 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 $a \equiv g^{2k} \pmod{p}$. $\square$

Corollary 18.2.3. There are exactly $(p-1)/2$ nontrivial quadratic residues modulo p in the set $\{1, \dots, p-1\}$, 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 18.2.4. *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*

$$\varepsilon(n) := \begin{cases} 0 & \text{if } n \text{ is odd,} \\ -1 & \text{if } n \text{ is even but not divisible by 4,} \\ 0 & \text{if } n \text{ is divisible by 4 but not by 8,} \\ 1 & \text{if } n \text{ is divisible by 8.} \end{cases}$$

18.3 Legendre Symbols

The fact that the integers $1, 2, \dots, p-1$ 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 18.3.1. *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 18.3.2. 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 18.2.2 is that

$$\left(\frac{a}{p}\right) = (-1)^{\text{ind}_g(a)}$$

for any primitive root g modulo p . Using Legendre symbols, we can reformulate Proposition 18.3.1 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 18.3.3. Consider an odd prime p . Then the function $a \mapsto \left(\frac{a}{p}\right)$ is the unique surjective function $f : \{1, \dots, p-1\} \rightarrow \{1, -1\}$ preserving multiplication, in the sense that

$$f(ab) = f(a)f(b)$$

for every two nonzero integers a and b modulo p ¹.

Proof. We have already seen that the Legendre symbol is a surjective function preserving multiplication. Thus, our task is now to show that if $f : \{1, \dots, p-1\} \rightarrow \{1, -1\}$ 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 . $\square$

Example 18.3.4. 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:

$$\left(\frac{8}{13}\right) = \left(\frac{2}{13}\right) \left(\frac{2}{13}\right) \left(\frac{2}{13}\right) = \left(\frac{2}{13}\right) = -1.$$

¹In 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 .

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

$$\{1, 3, 4, 9, 10, 12\}.$$

18.4 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 18.4.1 (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 [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 13.5.1](#). In the language of quadratic residues, [Theorem 13.5.1](#) 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 13.5.1 using Euler's Criterion. By [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

$$p \equiv 1 \pmod{4}. \quad \square$$

18.5 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 18.5.1. *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 . $\square$

As a reasonable starting point for our search, we take three consecutive primes of the form

$$q, q + 2, \text{ and } q + 6.$$

By [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 18.1.2](#) 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 [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 18.1](#), which reveals that the following polynomials are prime-generating polynomials, in the sense that they yield prime numbers for all inputs $0 \leq n \leq q - 2$:

$n^2 + n + 2$	$n^2 + n + 11$
$n^2 + n + 3$	$n^2 + n + 17$
$n^2 + n + 5$	$n^2 + n + 41$.

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.

$q \setminus p$	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 18.1: 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.

Exercises

Starter Exercises

18.1 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 $(p - 1)/2$.

18.2 Compute the Legendre symbols

- (a) $\left(\frac{5}{11}\right)$,
- (b) $\left(\frac{7}{17}\right)$,
- (c) $\left(\frac{3}{19}\right)$.

18.3 Compute the Legendre symbols

- (a) $\left(\frac{6}{11}\right)$,
- (b) $\left(\frac{12}{17}\right)$,
- (c) $\left(\frac{15}{19}\right)$.

18.4 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.

Routine-Building Exercises

18.5 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 $x^2 + ay^2$.

18.6 (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 .

18.7 Consider an odd prime p and an integer a .

- (a) Show that if $\text{ord}_p(a)$ is odd, then $\left(\frac{a}{p}\right) = 1$.
- (b) Show that if $\left(\frac{a}{p}\right) = -1$, then $\text{ord}_p(a)$ 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 $\left(\frac{a}{p}\right) = 1$.

$p \backslash q$	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 18.2: The value $(p-1)/\text{ord}_p(q)$, 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 .

- (d) Show that if $p \equiv 3 \pmod{4}$ and $\text{ord}_p(a) = 2k$ 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 $\text{ord}_p(a)$ is even, then $\left(\frac{a}{p}\right) = 1$ if and only if $\text{ord}_p(a) \mid \frac{p-1}{2}$.
- (f) 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

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\text{ord}_p(a)}}.$$

Table 18.2 lists the values of $\frac{p-1}{\text{ord}_p(a)}$, where p and q range over the first ten primes.

- (g) Using Exercise 17.6, give a direct proof of the identity

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\text{ord}_p(a)}}.$$

18.8 Consider an odd prime p , an integer a , and an integer m . Show that

$$a^m \equiv \left(\frac{a}{p}\right) \pmod{p} \quad \Leftrightarrow \quad m \equiv \frac{p-1}{2} \pmod{\text{ord}_p(a)}.$$

Challenge Exercises

18.9 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.

- 18.10 (a) Show that $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{3}$.
 (b) For any finite set $p_1, \dots, p_k$ 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 $p_1, \dots, p_k$. Conclude that there are infinitely many primes congruent to 1 modulo 3.

- 18.11 (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 $p_1, \dots, p_k$ 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 $p_1, \dots, p_k$. Conclude that there are infinitely many primes congruent to 1 modulo 5.

- 18.12 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 .

- 18.13 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 .

Chapter 19

Quadratic Reciprocity

19.1 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 18.7](#), this is equivalent to the question for which primes p we have

$$\frac{p-1}{\text{ord}_p(2)} \equiv 0 \pmod{2}.$$

In the following table we list the quantity $\frac{p-1}{\text{ord}_p(2)}$ for the odd primes below 50:

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$\frac{p-1}{\text{ord}_p(2)}$	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

$$7, 17, 23, 31, 41, 47, \dots$$

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 $\text{ord}_p(2) = p - 1$, so we see from the previous table that 2 is a primitive root modulo p for the primes

$$3, 5, 11, 13, 19, 29, 37, \dots$$

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 19.1.1. *The Legendre symbol of 2 modulo 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 [Fermat's Little Theorem](#) was obtained by multiplying all the numbers $1, \dots, p-1$ 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 [Euler's Criterion](#) we have $\left(\frac{2}{p}\right) \equiv 2^P \pmod{p}$, which gives us the congruences

$$\left(\frac{2}{p}\right)P! \equiv 2^P P! \equiv 2 \cdot 4 \cdot \dots \cdot (2P) \pmod{p}$$

We proceed by carefully analyzing this product of all the even positive integers below p . If we define the numbers

$$s := \left\lfloor \frac{p-1}{4} \right\rfloor \quad \text{and} \quad t := \left\lfloor \frac{p+1}{4} \right\rfloor,$$

so that $s+t = P$, then we can partition the set of all even positive integers below p into two subsets

$$S := \{2k \mid 1 \leq k \leq s\} \quad \text{and} \quad T := \{2k \mid s+1 \leq k \leq P\},$$

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 $1 \leq x \leq P$ so that $y = p - x$, which determines a bijection. Thus, taking the product 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

$$\left(\frac{2}{p}\right)P! \equiv 2 \cdot 4 \cdot \dots \cdot 2P \equiv (-1)^t P! \pmod{p}.$$

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:

$$t \equiv \begin{cases} 0 \pmod{2} & \text{if } p \equiv \pm 1 \pmod{8} \\ 1 \pmod{2} & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

□

	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 19.1: The first ten primes congruent to r modulo 8, for $r = 1, 3, 5, 7$.

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 19.1.2. *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 13.6.1](#) 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 modulo 8 for each odd residue class r are given in [Table 19.1](#).

Theorem 19.1.3. *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 n th 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. $\square$

Theorem 19.1.4. *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. $\square$

Theorem 19.1.5. *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 $q \equiv -1 \pmod{8}$. $\square$

19.2 The Statement of Quadratic Reciprocity

We have already established several facts about Legendre symbols. The Legendre symbol is multiplicative, meaning that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

$p \backslash q$	3	5	7	11	13	17	19	23	29	31
3		-	+	-	+	-	+	-	-	+
5	-		-	+	-	-	+	-	+	+
7	-	-		+	-	-	-	+	+	-
11	+	+	-		-	-	-	+	-	+
13	+	-	-	-		+	-	+	+	-
17	-	-	-	-	+		+	-	-	-
19	-	+	+	+	-	+		+	-	-
23	+	-	-	-	+	-	-		+	+
29	-	+	+	-	+	-	-	+		-
31	-	+	+	-	-	-	+	-	-	

Table 19.2: The sign of the Legendre symbol $\left(\frac{q}{p}\right)$, ranging over pairs of distinct odd primes p and q .

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 18.7](#) that the Legendre symbol of a modulo p can be computed by

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\text{ord}_p(a)}}.$$

Thus, the Legendre symbol of a modulo p depends only of the parity of the quantity

$$\frac{p-1}{\text{ord}_p(a)},$$

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 19.2](#).

The patterns in this table might not be immediately apparent. However, those who did [Exercise 18.11](#) 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 19.2 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:

$p \backslash q$	3	5	7	11	13	17	19	23	29	31
3		●	○	○	●	●	○	○	●	○
5	●		●	●	●	●	●	●	●	●
7	○	●		○	●	●	○	○	●	○
11	○	●	○		●	●	○	○	●	○
13	●	●	●	●		●	●	●	●	●
17	●	●	●	●	●		●	●	●	●
19	○	●	○	○	●	●		○	●	○
23	○	●	○	○	●	●	○		●	○
29	●	●	●	●	●	●	●	●		●
31	○	●	○	○	●	●	○	○	●	

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 19.2. 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:

- (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 19.2.1 (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 19.2.2. 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 19.2.3. *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

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{10}. \end{cases}$$

19.3 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 19.3.1. 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 $[a]_n$ for the least absolute residue of a modulo n , and we will write $\|a\|_n$ 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
$[a]_{11}$	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

$$x \mapsto [ax]_p : \{0, \dots, p-1\} \rightarrow \left\{-\frac{p-1}{2}, \dots, \frac{p-1}{2}\right\}$$

is also a bijection. Restricting this bijection to the set $\{1, \dots, \frac{p-1}{2}\}$, we obtain an injective function

$$x \mapsto [ax]_p : \{1, \dots, \frac{p-1}{2}\} \rightarrow \left\{-\frac{p-1}{2}, \dots, \frac{p-1}{2}\right\}.$$

The following lemma shows that every $1 \leq x \leq \frac{p-1}{2}$ occurs exactly once as the absolute value of any number of the form $[ax]_p$.

Lemma 19.3.2. *The function*

$$r_a : \{1, \dots, \frac{p-1}{2}\} \rightarrow \{1, \dots, \frac{p-1}{2}\}$$

given by $r_a(x) := \|[ax]_p\|_p$ is a bijection.

Proof. Since r_a is a function between two sets of finite size $\frac{p-1}{2}$, it suffices to show that r_a is injective. To this end, consider x and y such that $r_a(x) = r_a(y)$. Since the function $x \mapsto \lfloor ax \rfloor_p$ is injective, this implies that

$$\lfloor ax \rfloor_p = -\lfloor ay \rfloor_p$$

or, equivalently, that $ax - ay$ is divisible by p . Since a is relatively prime to p , this implies that $x - y$ is divisible by p , i.e., that $x = y$. $\square$

Lemma 19.3.3 (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*

$$a, 2a, 3a, \dots, \frac{p-1}{2}a \pmod{p},$$

such that $\lfloor ax \rfloor_p$ 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 [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 19.3.3](#), we obtain:

$$a^P P! = (1a)(2a) \cdots (Pa) \equiv (-1)^\mu P! \pmod{p}. \quad \square$$

19.4 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

$$\lfloor x \rfloor$$

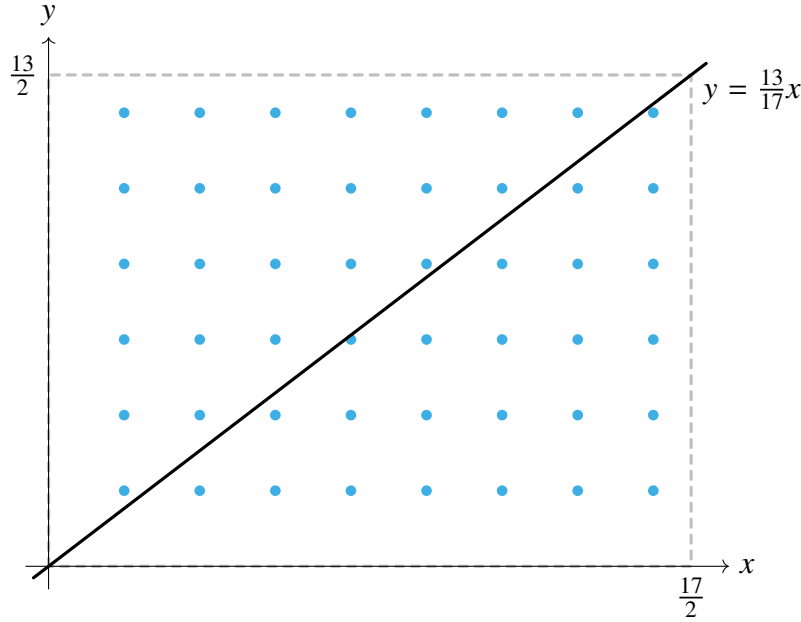


Figure 19.1: In Eisenstein's proof of quadratic reciprocity, we count the $\frac{p-1}{2}$ by $\frac{q-1}{2}$ lattice points in the marked rectangle as the sum of the number lattice points below the diagonal and the number of lattice points above the diagonal.

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:

$$\left\lfloor \frac{3}{2} \right\rfloor = 1, \quad \left\lfloor \frac{29}{31} \right\rfloor = 0, \quad \text{and} \quad \left\lfloor -\frac{1}{4} \right\rfloor = -1.$$

Eisenstein's Proof of The Law of Quadratic Reciprocity. By [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 19.1](#) 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

$$(0, 0), \left(\frac{p}{2}, 0\right), \left(\frac{p}{2}, \frac{q}{2}\right), \text{ and } (0, \frac{q}{2}).$$

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 $1 \leq k \leq \frac{p-1}{2}$, a lattice point of the form (k, i) is in the set S if and only if

$$1 \leq i \leq \frac{q}{p}k.$$

The number of such lattice points is $\left\lfloor \frac{kq}{p} \right\rfloor$, 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

$$|T| = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

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 19.4.1. *Consider an odd prime p and an odd integer a not divisible by p , and let $\mu(a, p)$ be the quantity defined in [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

$$-\frac{p-1}{2} \leq r_k \leq \frac{p-1}{2}.$$

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 19.3.2](#) 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

19.1 Compute the values of the following Legendre symbols:

$$\left(\frac{101}{163}\right), \quad \left(\frac{137}{359}\right), \quad \left(\frac{113}{479}\right), \quad \text{and} \quad \left(\frac{139}{953}\right).$$

19.2 Compute the values of the following Legendre symbols:

$$\left(\frac{113}{131}\right), \quad \left(\frac{131}{311}\right), \quad \text{and} \quad \left(\frac{311}{113}\right).$$

19.3 Compute the values of the following Legendre symbols:

$$\left(\frac{199}{919}\right), \quad \left(\frac{919}{991}\right), \quad \text{and} \quad \left(\frac{991}{199}\right).$$

19.4 Compute the values of the following Legendre symbols:

$$\left(\frac{337}{373}\right), \quad \left(\frac{373}{733}\right), \quad \text{and} \quad \left(\frac{733}{337}\right).$$

19.5 Consider a prime $p > 3$. Show that

$$\left(\frac{6}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 5 \pmod{24}, \\ -1 & \text{if } p \equiv \pm 7, \pm 11 \pmod{24}. \end{cases}$$

19.6 Consider an odd prime $p \neq 5$. Show that

$$\left(\frac{10}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}, \\ -1 & \text{if } p \equiv \pm 7, \pm 11, \pm 17, \pm 19 \pmod{40}. \end{cases}$$

Routine-Building Exercises

19.7 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) $4x^2 + 7x + 14 \equiv 0 \pmod{31}$.

19.8 Show that 2 is a quadratic residue modulo any prime divisor of the n th Fermat number $F_n = 2^{2^n} + 1$, for $n \geq 2$.

19.9 Consider a prime p such that $q := 2p + 1$ and $r := 2(2p + 1) + 1 = 4p + 3$ are both prime. Prove that

$$\text{ord}_r(2) = q.$$

Challenge Exercises

19.10 Show that if the n th Fermat number $F_n = 2^{2^n} + 1$ is prime, then 3 is a primitive root modulo F_n .

19.11 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.

- 19.12 (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 $a \equiv 1 \pmod{4}$.
- 19.13 (a) For any integer $a > 2$, let p be a prime factor of $a^4 - a^2 + 1$. Show that

$$\text{ord}_p(a) = 12.$$

- (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 20

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].

20.1 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 11.11](#) 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 explicitly 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 11.12](#) we established an elementary congruence regarding Sophie Germain primes. In [Exercise 18.13](#) 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 [Section 15.4](#), where we proved [Hensel's Fixed Divisor Theorem](#).

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 (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 .*

20.2 Conjectures About Exceptional Primes

Conjecture 14 (Finiteness of Fermat primes). *There are only finitely many primes of the form $F_n = 2^{2^n} + 1$.*

Conjecture 15 (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 16 (Infinitude of non-Wieferich primes). *There are infinitely many non-Wieferich primes.*

Conjecture 17 (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 $(p - (\frac{p}{5}))$ th Fibonacci number. Here, the number $(\frac{p}{5})$ is the Legendre symbol of p modulo 5.*

20.3 Conjectures About Gaps Between the Primes

Conjecture 18 (Legendre's Conjecture). *For every positive integer n , there is at least one prime between n^2 and $(n+1)^2$.*

Conjecture 19 (Andrica's Conjecture). *If p and q are two consecutive primes, then $\sqrt{q} - \sqrt{p} < 1$.*

Conjecture 20 (Cramér's Conjecture). *The asymptotic growth of the gap from a prime p to the next prime is $O(\log(p)^2)$.*

20.4 Conjectures About Conditions for Primality

Conjecture 21 (Lehmer's Conjecture). *If $\phi(n) \mid n - 1$, then n is prime.*

Conjecture 22 (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 23 (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 n th prime number, starting with $p_0 := 2$, $p_1 := 3$, and so on. Define the n th *primorial* by

$$p_n\# := \prod_{i=0}^n p_i.$$

Conjecture 24 (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.*

20.5 Conjectures About Prime Decompositions

Conjecture 25 (Square-freeness of Fermat numbers). *Every Fermat number $F_n = 2^{2^n} + 1$ is square-free [BW1967].*

Conjecture 26 (Square-freeness of Mersenne numbers with prime exponents). *Every Mersenne number M_p with prime exponent p is square-free [Rot1965; BW1967].*

In [Exercise 13.21](#) we showed that for any two distinct primes p and q , any common prime divisor r of the numbers

$$\frac{p^q - 1}{p - 1} \quad \text{and} \quad \frac{q^p - 1}{q - 1}$$

satisfies $r \equiv 1 \pmod{2pq}$.

Conjecture 27 (The Feit–Thompson Conjecture). *There are no two distinct primes p and q such that*

$$\frac{p^q - 1}{p - 1} \quad \text{divides} \quad \frac{q^p - 1}{q - 1}$$

Conjecture 28 (Grimm’s Conjecture). *If the numbers $n + 1, \dots, n + k$ are all composite, then there is a set of k distinct primes p_i such that $p_i \mid n + i$ for each $1 \leq i \leq k$.*

A *Sierpiński number* is an odd number k such that every number of the form $k \cdot 2^n + 1$ is composite.

Conjecture 29 (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 30 (Riesel’s problem). *The smallest Riesel number is 509,203.*

20.6 Conjectures About Arithmetic Functions

Conjecture 31 (The nonexistence of odd perfect numbers). *There are no odd perfect numbers.*

Conjecture 32 (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 33 (The Solitary Number Conjecture). *The number 10 is solitary.*

Conjecture 34 (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 .*

20.7 Conjectures About Diophantine Problems

Conjecture 35 (The Erdős–Moser Conjecture). *The only solution to the equation*

$$1^k + 2^k + \dots + m^k = (m + 1)^k$$

is $1 + 2 = 3$.

Conjecture 36 (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 37 (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 38 (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 39 (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 40 (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

$$\frac{5^3 - 1}{5 - 1} = \frac{2^5 - 1}{2 - 1} \quad \text{and} \quad \frac{90^3 - 1}{90 - 1} = \frac{2^{13} - 1}{2 - 1}.$$

That is, the only two integers that are repunits of length > 3 in two different bases are

$$31 = (111)_5 = (11111)_2 \quad \text{and} \quad 8191 = (111)_{90} = (1111111111111)_2.$$

Conjecture 41 (The *abc*-Conjecture). *Let a, b , and c be relatively prime positive integers such that $a + b = c$. Let $\text{rad}(n)$ 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*

$$c > \text{rad}(abc)^{1+\epsilon}.$$

Conjecture 42 (Hall's Conjecture). *For any $\epsilon > 0$, 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*

$$|y^2 - x^3| > C_\epsilon x^{\frac{1}{2}-\epsilon}.$$

Conjecture 43 (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 $c(x - r)^n$.*

20.8 Conjectures About Representations of Numbers

Problem 44 (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 45 (Goldbach's Conjecture). *Every even number greater than 2 can be written as the sum of two primes.*

Conjecture 46 (Lemoine's Conjecture). *Every odd integer greater than 5 can be written in the form $p + 2q$, where p and q are primes.*

Conjecture 47 (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 48 (Pollock's Conjecture). *Every natural number is the sum of five tetrahedral numbers.*

Conjecture 49 (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 50 (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 51 (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].*

20.9 Conjectures About Iterative and Dynamical Processes

Conjecture 52 (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 53 (The Mullin–Shanks Conjecture). *Every prime occurs in the Euclid–Mullin sequence.*

Conjecture 54 (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 55 (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 56 (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 57 (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

- [And1994] George E. Andrews. *Number Theory*. Dover Books on Mathematics. Dover Publications, 1994. ISBN: 9780486682525.
- [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: 978-0-88385-700-6.
- [Ber1934] B. Berggren. “Pytagoreiska triangular”. 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). Available at <https://books.google.com/books?id=WTa-qRIWckoC&pg=PA123>, pp. 123–140.
- [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). Issue labeled 1996–97; published January 1997, 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.
- [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](https://doi.org/10.1080/0025570X.2003.11953179). URL: <https://www.tandfonline.com/doi/abs/10.1080/0025570X.2003.11953179>.
- [Che1850] Pafnuty Chebyshev. “Mémoire sur les nombres premiers”. French. In: *Journal de Mathématiques Pures et Appliquées* 17 (1850), pp. 366–390.
- [Che2016] Evan Chen. *Euclidean Geometry in Mathematical Olympiads*. MAA Problem Books. Washington, D.C.: Mathematical Association of America, 2016. ISBN: 978-0-88385-839-4. URL: <https://web.evanchen.cc/geombook.html>.

- [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](https://doi.org/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: 0-471-62471-4.
- [De 1838] Augustus De Morgan. “Induction (Mathematics)”. In: *The Penny Cyclopaedia of the Society for the Diffusion of Useful Knowledge* 12 (1838), pp. 465–466. URL: <https://archive.org/details/pennycyclopaedi18unkngoog>.
- [Ded1888] Richard Dedekind. *Was sind und was sollen die Zahlen?* First edition. Braunschweig: Friedrich Vieweg und Sohn, 1888.
- [Dio1910] Diophantus. *Diophantus of Alexandria: A Study in the History of Greek Algebra*. Ed. by Thomas Little Heath. Includes an English translation of *Arithmetica*. 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](https://doi.org/10.1215/ijm/1256050816).
- [Euc2015] Euclid. *The Thirteen Books of Euclid’s Elements*. Trans. by Thomas L. Heath. Cambridge University Press, 2015. ISBN: 9781107480421.
- [Eul1744] Leonhard Euler. “De Fractionibus Continuis Dissertatio”. In: *Commentarii Academiae Scientiarum Petropolitanae* 9 (1744). Presented 7 March 1737; Eneström #E71, pp. 98–137.
- [Eul1988] Leonhard Euler. *Introductio in Analysin Infinitorum*. 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), p. 48.
- [Far1816] John Farey Sr. “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: *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*. Translation of *Liber Quadratorum*. Boston: Academic Press, 1987, pp. xx, 124. ISBN: 9780126431308.
- [Fur1955] Hillel Furstenberg. “On the Infinitude of Primes”. In: *American Mathematical Monthly* 62.5 (1955), p. 353. DOI: [10.2307/2307043](https://doi.org/10.2307/2307043). URL: <https://doi.org/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, pp. xx + 472. ISBN: 978-0-387-96254-2.
- [Gol1956] Solomon W. Golomb. “Combinatorial Proof of Fermat’s “Little” Theorem”. In: *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.
- [Gua2023] 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: 0-387-20860-7.
- [Har+2008] Godfrey H. Hardy et al. *An Introduction to the Theory of Numbers*. 6th. With a foreword by Andrew Wiles. Oxford: Oxford University Press, 2008. ISBN: 9780199219865.
- [Hem1961] Hemachandra Suri. *Chandonuśāsana*. Sanskrit. Composed circa 1150 CE. Bombay: Adhithata 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; 1435-5345/e.
- [Hum1978] David Hume. *A Treatise of Human Nature*. Ed. by L. A. Selby-Bigge and P. H. Nidditch. Second Edition. Oxford: Oxford University Press, 1978.
- [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](https://doi.org/10.1080/00029890.2024.2370240).
- [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: 978-90-04-18354-4. DOI: [10.1163/9789004225381](https://doi.org/10.1163/9789004225381). URL: <https://brill.com/abstract/title/14271>.

- [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](https://doi.org/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](https://doi.org/10.1090/s0002-9904-1932-05521-5).
- [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](https://doi.org/10.1007/BF01561092). URL: <https://link.springer.com/article/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.
- [Mah1994] Michael Sean Mahoney. *The Mathematical Career of Pierre de Fermat, 1601-1665*. 2nd ed. Princeton, NJ: Princeton University Press, 1994. ISBN: 978-0-691-08582-9.
- [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](https://doi.org/10.1080/0025570X.2006.11953392).
- [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>.
- [OEI2025] OEIS Foundation. A006992: *Bertrand primes*. <https://oeis.org/A006992>. The On-Line Encyclopedia of Integer Sequences. 2025.
- [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*. First edition. 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.
- [Poo2007] Alf van der Poorten. *Fermat’s Four Squares Theorem*. 2007. arXiv: [0712.3850](https://arxiv.org/abs/0712.3850) [math.NT]. URL: <https://arxiv.org/abs/0712.3850>.
- [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](https://doi.org/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.
- [Rud1960] Walter Rudin. “Trigonometric series with gaps”. In: *Journal of Mathematics and Mechanics* 9.2 (1960), pp. 203–227.
- [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](https://doi.org/10.2307/27642094).
- [Sie1988] Waław Sierpiński. *Elementary Theory of Numbers*. Ed. by A. Schinzel. Second English Edition. Amsterdam: North-Holland, 1988. ISBN: 978-0-444-86662-2.
- [Sil2012] Joseph H. Silverman. *A Friendly Introduction to Number Theory*. 4th. Pearson, 2012. ISBN: 978-0321816191.
- [Sin1971] David Singmaster. “Research Problems: How Often Does an Integer Occur as a Binomial Coefficient?” In: *American Mathematical Monthly* 78.4 (1971), pp. 385–386. DOI: [10.1080/00029890.1971.11992769](https://doi.org/10.1080/00029890.1971.11992769).
- [Tay1715] Brook Taylor. *Methodus incrementorum directa et inversa*. London: Typis Pearsonianis: prostant apud Gul. Innys, 1715.
- [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). The famous quote “Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk” is attributed to Kronecker in this obituary., pp. 5–31.

- [Wei1984] André Weil. *Number Theory: An Approach through History from Hammurapi to Legendre*. Boston: Birkhäuser, 1984. ISBN: 978-0-8176-3147-6. DOI: [10.1007/978-1-4684-0150-4](https://doi.org/10.1007/978-1-4684-0150-4).
- [Wha2010] Junho Peter Whang. “Another Proof of the Infinitude of the Prime Numbers”. In: *The American Mathematical Monthly* 117.2 (2010), p. 181. DOI: [10.4169/000298910X480375](https://doi.org/10.4169/000298910X480375).
- [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>.