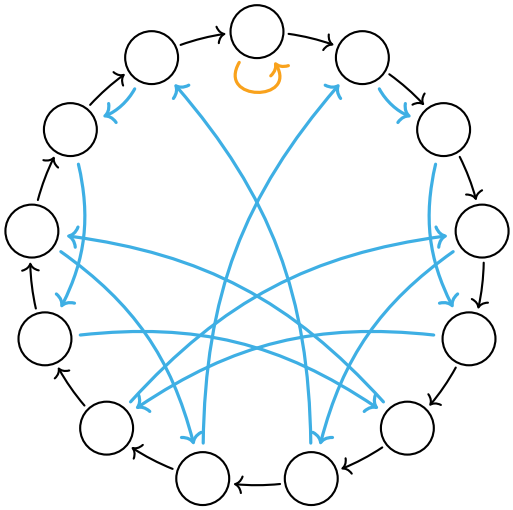
Johns Hopkins University

Egbert Rijke



The Multiplicative Nature of Numbers

Book II

of

The Great Story of Numbers

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

© 2025 Egbert Rijke.
All rights reserved.

Citing this work:

```
@book{rijke-0.261124-vol-2,
  author = {Egbert Rijke},
  title = {Book II of The Great Story of Numbers: The Multiplicative
    Nature of Numbers},
  year = {2026},
  month = nov,
  note = {Version 0.261124-vol-2},
  url = {https://egbertrijke.github.io/notes/number-theory/}
}
```

Contents

13 Prime Numbers · 211
13.1 The Fundamental Theorem of Arithmetic · 211
13.2 The Infinitude of Primes · 216
13.2.1 Euclid's Proof · 216
13.2.2 Saidak's Proof · 217
13.2.3 Furstenberg's Proof, Following Cass–Wildenberg · 217
13.2.4 Erdős's Proof · 218
13.2.5 A Proof via the Stars-and-Bars Method · 219
13.3 Fermat Primes · 220
13.4 Legendre's Formula and Kummer's Theorem · 222
13.5 Bertrand's Postulate · 228
Exercises · 231

14 Multiplicative Functions · 235
14.1 Perfect Numbers · 235
14.2 Euler's Totient Function · 239
14.3 Multiplicative Functions · 241
14.4 The Möbius Function · 243
14.5 Dirichlet Convolution · 245
14.6 Dirichlet Inverses · 247
Exercises · 249

15 Cyclic Counting · 253
15.1 Hemachandra Wheels · 253
15.2 The Prime–Fixed Point Congruence · 255
15.3 Lucas's Theorem · 256
15.4 The Orbit–Counting Formula · 257

15.5 The Divisor Sum of the Totient Function · 259
15.6 Arithmetic Functions of Orbits and Fixed Points · 261
Exercises · 264

16 Fermat's Little Theorem and its Consequences · 267
16.1 Fermat's Little Theorem · 267
16.2 Euler's Theorem · 270
16.3 Wilson's Theorem · 272
16.4 Concerning Strong Divisibility Sequences · 273
16.5 The Quadratic Character of −1 · 275
16.6 The Infinitude of Primes Congruent to 1 Modulo Powers of 2 · 278
Exercises · 280

17 Fermat's Two-Squares Theorem · 283
17.1 Numbers Representable as a Sum of Two Squares · 283
17.2 Euler's Proof by Infinite Descent · 289
Exercises · 291

18 The Gaussian Integers · 293
18.1 Definition and Basic Properties of the Gaussian Integers · 293
18.2 Euclidean Division of Gaussian Integers · 294
18.3 The Greatest Common Divisor of Gaussian Integers · 295
18.4 Primes in the Gaussian Integers · 295
18.5 Fermat's Two-Square Theorem · 295
18.6 The Biquadratic Character of −1 · 295
Exercises · 296

19 Strong Divisibility Sequences · 297
19.1 Lucas Sequences · 297
19.2 The Rank of Apparition · 302
19.3 Primitive Sequences · 306
19.4 LCM-sequences · 307
19.5 The Lifting the Exponent Lemma · 308
Exercises · 310

20 Polynomials · 313
20.1 Polynomials with Abstract Coefficients · 313
20.2 The Factor Theorem · 316
20.3 Polynomial Congruences of Prime Moduli · 317
20.4 Lagrange's Interpolation Theorem · 320
20.5 Fixed Divisors of Integer Polynomials · 324
Exercises · 326

21 Primitive Roots · 329
21.1 Counting Elements of a Given Order Modulo a Prime · 329

21.2 Primitive Roots · 332
21.3 The Discrete Logarithm · 333
21.4 A Criterion for Congruences of Degree n · 334
Exercises · 337

22 The Moduli with Primitive Roots · 339
22.1 Primitive Roots Modulo Odd Prime Powers · 339
22.2 The Complete Characterization of Moduli with Primitive Roots · 340
22.3 Carmichael's Function · 341

23 Polynomial Congruences · 343
23.1 Polynomial Congruences of Composite Moduli · 343
23.2 Derivatives of Polynomials · 344
23.3 Hensel's Lemma · 346
23.4 The Elementary Symmetric Polynomials · 347
23.5 Reduced Polynomials Modulo a Prime · 348

24 Divisibility and Irreducebility of Polynomials · 349
24.1 Primitive Polynomials and Gauss's Lemma · 349
24.2 Euclid's Algorithm for Polynomials · 351
24.3 Irreducible Polynomials · 352
24.4 Eisenstein's Criterion · 354
Exercises · 357

25 Cyclotomic Polynomials · 359
25.1 The Primitive Factors of $x^n - 1$ · 359
25.2 The Möbius Inversion Formula for the Cyclotomic Polynomials · 362
25.3 Irreducibility of the Cyclotomic Polynomials · 362
25.4 Zsigmondy's Theorem · 363
25.5 The Infinitude of Primes Congruent to 1 Modulo n · 366
25.6 Vantieghem's Theorem · 367
Exercises · 370

26 Integer Factorizations of Polynomial Values · 371
26.1 The Reducibility of $x^n - a$ · 371
26.2 Aurifeuillean Factorizations · 371
26.3 Obstructions to the Infinitude of Primes in Lucas Sequences · 371

References · 375



Illustrations

13.1 The sieve of Eratosthenes · 212
13.2 The 2-adic valuations of the numbers up to 15 · 223

15.1 Hemachandra wheels · 254
15.2 A bijection on a 12-element set · 257
15.3 Hemachandra wheels of order 7 · 264

16.1 Carl Friedrich Gauss · 276

17.1 Sums of two squares · 284
17.2 Thue's Lemma · 287
17.3 Thue's lemma in Lucas' weaving patterns · 288

18.1 The Gaussian integers · 294

20.1 Example polynomial obtained by Lagrange interpolation · 321

21.1 Doubling integers modulo 13 · 330



Chapter 13

Prime Numbers

13.1 The Fundamental Theorem of Arithmetic

Definition 13.1.1. An integer a is said to be **prime** if it has exactly one positive proper divisor. Any integer $a \neq \pm 1$ that is not prime is said to be a **composite number**.

The numbers 0 and 1 are not prime. To see that 0 isn't prime, simply note that any positive integer is a proper divisor of 0. To see that 1 isn't prime, note that 1 doesn't have any proper divisors. Indeed, it has exactly one positive divisor, namely 1 itself, but this divisor isn't proper. We also note that if $a > 1$ is prime, then the number 1 is always a positive proper divisor. Thus we see that $a > 1$ is prime if and only if the number 1 is its unique positive proper divisor. We note that older literature often uses the name *aliquot divisors* for what we have called proper divisors.

To see that the number 2 is prime, note that its positive divisors are a subset of the set $\{1, 2\}$ consisting of all the positive integers below 2. Its proper divisors are therefore a subset of $\{1\}$. The integer 1 is indeed a positive divisor, so we see that 2 has exactly one positive proper divisor.

To see that the number 3 is prime, note that its positive divisors are a subset of the set $\{1, 2, 3\}$ consisting of all positive integers below 3. The number 1 is a proper divisor, the number 2 doesn't divide 3, and 3 itself is a divisor but it isn't proper. Therefore we see that the number 3 has exactly one positive proper divisor.

The number 4 isn't prime, because the numbers 1 and 2 are two distinct proper divisors of 4. This process of finding all primes up to a desired bound is formalized in the **sieve of Eratosthenes**, which we will now describe. Figure 13.1 displays the sieve of Eratosthenes up to 1120.

The sieve of Eratosthenes is an iterative process that generates at stage n a set P_n



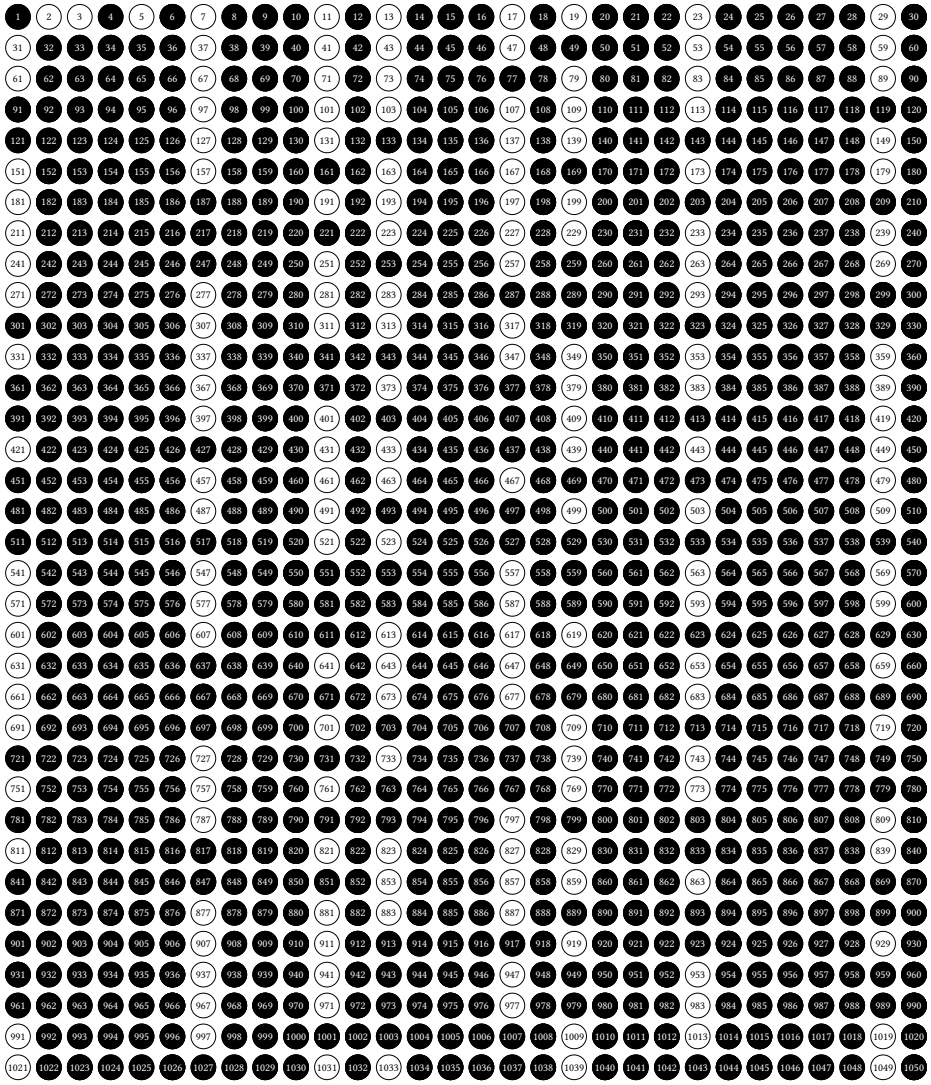


Figure 13.1: The sieve of Eratosthenes up to 1050: The number 1 and every composite number are marked in black, leaving just the primes in white circles.

of numbers known to be prime at stage n, and a set Q_n of prime candidates. In other words, the sets P_n form an increasing sequence

$$P_0 \subseteq P_1 \subseteq P_2 \subseteq \cdots$$

of sets of numbers known to be prime, where at each higher stage the set of known primes becomes larger, and the sets Q_n form a decreasing sequence

$$Q_0 \supseteq Q_1 \supseteq Q_2 \supseteq \cdots$$

of candidates, from which we pick our next prime. We will define the sets P_n and Q_n by a recursive process. Initially, the set P_0 is empty and $Q_0 = \{n \in \mathbb{N} \mid n \geq 2\}$ is the set of all numbers ≥ 2. Now we define P_{n+1} to be $P_n \cup \{p(n)\}$, where $p(n) := \min(Q_n)$, and we define

$$Q_{n+1} := Q_n \setminus \{kp(n) \mid k \geq 1\}.$$

In other words, the nth prime $p(n)$ is the minimal element of $Q(n)$, and the set Q_{n+1} of candidates is the set Q_n minus all the multiples of $p(n)$. In the first five stages, these sets look as follows:

n	P_n	Q_n
0	$\emptyset$	$\{2, 3, 4, 5, 6, 7, 8, \ldots\}$
1	$\{2\}$	$\{3, 5, 7, 9, 11, 13, 15, \ldots\}$
2	$\{2, 3\}$	$\{5, 7, 11, 13, 17, 19, 23, \ldots\}$
3	$\{2, 3, 5\}$	$\{7, 11, 13, 17, 19, 23, 29, \ldots\}$
4	$\{2, 3, 5, 7\}$	$\{11, 13, 17, 19, 23, 29, 31, \ldots\}$
5	$\{2, 3, 5, 7, 11\}$	$\{13, 17, 19, 23, 29, 31, 37, \ldots\}$

Notice that not only the minimal element of Q_n is prime, but every element $q \in Q_n$ such that $q < (\max(P_n))^2$ is prime. This is because if $q < (\max(P_n))^2$ is composite, then its lowest factor must be a prime number $p < \max(P_n)$, i.e., it must be a prime number in P_n. However, all the multiples of the primes in P_n have been removed from Q_n, so there are no such composite numbers.

We can use this observation to obtain the list of all primes below 100, at stage 5 in the sieve of Eratosthenes. The list of primes below 100 is

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

The sieve of Eratosthenes either terminates, i.e., it reaches a stage for which Q_n is empty, or there are infinitely many primes. We will now show that there are infinitely many primes. In the following lemma we use the concept of **nontrivial divisors**, which are divisors d of a natural number n such that $d \neq 1$. The concept of nontrivial divisors should not be confused with the concept of proper divisors, which are divisors d of a natural number n such that $d \neq n$.



THEOREM 13.1.2. *Any natural number $n > 1$ has a least nontrivial divisor, and this divisor is prime.*

PROOF. Suppose that $n > 1$. Then the set of nontrivial divisors $d \neq 1$ of n contains the number n, so it has a least element p by Theorem 5.2.1 (The Well-Ordering Principle of the Natural Numbers) of the natural numbers. Then the set of divisors of p itself is the set $\{1, p\}$, because any divisor of p also divides n, and p is assumed to be the least nontrivial divisor. This shows that p has exactly one proper divisor, and therefore p is prime. □

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

LEMMA 13.1.3. *Suppose that p is prime, and that a is an integer. Then either $p \mid a$ or* $\gcd(p, a) = 1$.

PROOF. The greatest common divisor of p and a is in particular a divisor of p, so it is either 1 or p. If $\gcd(p, a) = p$, then we have $p \mid a$. □

PROPOSITION 13.1.4. *Consider a positive integer a. The following are equivalent:*

(i) *The integer a is prime.*

(ii) *We have $a > 1$, and for any two integers b and c such that $a \mid bc$, we have that $a \mid b$ or $a \mid c$.*

PROOF. Suppose first that a is prime. Since 0 and 1 aren't prime, it follows that $a > 1$. Now consider two integers b and c such that $a \mid bc$. There are two cases to consider: either $a \mid b$, in which case we are done immediately, or $a \nmid b$. In the case where $a \nmid b$, it follows from Lemma 13.1.3 that a and b are relatively prime. This allows us to apply Proposition 7.1.5, by which we conclude that $a \mid c$.

For the converse, suppose that for any two integers b and c such that $a \mid bc$, we have $a \mid b$ or $a \mid c$, and let d be a proper divisor of a. Now consider any positive proper divisor d of a, and write $a = dk$. Then it follows in particular that $a \mid dk$, so by assumption we have either $a \mid d$ or $a \mid k$. The first condition can be ruled out, because d is assumed to be a proper divisor and therefore $a \nmid d$. Thus we find ourselves in the second case, where $a \mid k$ and $k \mid a$. The integer k is also positive, since a and d are positive, so it follows that $a = k$. This implies that $d = 1$, and hence we conclude that a is prime. □

The fundamental theorem of arithmetic asserts that every positive integer can be written uniquely, up to reordering, as a product of primes. Gauss is often credited for being the first to state this fact as a theorem. He did so in Article 16 of his *Disquisitiones Arithmeticae* [GAU1986], where he has mentioned that prior authors often assumed it or gave inadequate reasons for its truth.

Theorem 13.1.5. *For any natural number $n > 0$, there is a unique list $\ell = (p_0, \dots, p_{l-1})$ of length l, consisting of primes $p_0 \leq p_1 \leq \cdots \leq p_{l-1}$ such that*

$$n = \prod_{i=0}^{l-1} p_i.$$

This unique list of primes is called the ***prime decomposition of*** *n.*

Proof. We apply strong induction on n, with base case 1. In the base case, we let ℓ be the empty list. The empty list satisfies the increasing primes condition vacuously, and empty products are 1 by definition, so the empty list is indeed a prime decomposition of 1.

For the inductive step, recall that any natural number $n + 1 > 1$ has a least prime divisor. If p is the least prime divisor of $n + 1$, then it follows that $(n + 1)/p \leq n$. By the strong induction hypothesis we have a unique prime decomposition $(q_0, \dots, q_{l-1})$ of $(n + 1)/p$. Now define the list $\ell := (p_0, p_1, \dots, p_l)$ by $p_0 := p$ and $p_{i+1} := q_i$. Then each p_i is a prime divisor of $n + 1$, and since p_0 is the least prime divisor of $n + 1$ we have the inequalities

$$p_0 \leq p_1 \leq \cdots \leq p_l.$$

Furthermore, we have

$$n + 1 = p \cdot ((n + 1)/p) = p_0 \cdot \prod_{i=1}^{l} p_i = \prod_{i=0}^{l} p_i.$$

This proves that the prime decomposition of $n + 1$ exists.

To show that the prime decomposition of $n + 1$ is unique, let $(r_0, \cdots, r_k)$ be a prime decomposition of $n + 1$. The smallest prime divisor p of $n + 1$ then divides the product

$$p \mid \prod_{i=0}^{k} r_i.$$

This implies that $p \mid r_i$ for some $0 \leq i \leq k$, i.e., that $p = r_i$. However, p is assumed to be the smallest prime factor of $n + 1$, so it follows that $p = r_0$. Now it follows that $(r_1, \dots, r_k)$ is a prime decomposition of $(n + 1)/p$, which is unique, and therefore we conclude that $n + 1$ has a unique prime factorization. □

Corollary 13.1.6. *For any positive integer n with prime factorization $n = p_1^{m_1} \cdots p_k^{m_k}$, the map*

$$x \mapsto \left(x \mod p_1^{m_1}, \dots, x \mod p_k^{m_k}\right)$$

is a bijection

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

REMARK 13.1.7. Although the prime factorization of arbitrary large numbers can be an arduous task, numbers of special forms can sometimes be factorized more easily. For instance, using the formula for the difference of squares we see that

$$\begin{aligned} 2^{16} - 1 &= (2^8 - 1)(2^8 + 1) \\ &= (2^4 - 1)(2^4 + 1)(2^8 + 1) \\ &= (2^2 - 1)(2^2 + 1)(2^4 + 1)(2^8 + 1) \\ &= 3 \cdot 5 \cdot 17 \cdot 257. \end{aligned}$$

Even though $2^{16} - 1 = 65535$ is a fairly large number, finding its prime factorization was fairly effortless.

13.2 The Infinitude of Primes

13.2.1 Euclid's Proof

The theorem asserting the infinitude of primes asserts that no finite set of primes is the set of all primes. Many proofs of the infinitude of primes require the following lemma:

LEMMA 13.2.1. *If a and b are relatively prime integers, then any prime divisors of a are distinct from any prime divisors of b.*

PROOF. Suppose that a and b are relatively prime, and that p and q are prime divisors of a and b, respectively. By the assumption that a and b are relatively prime, it follows that $p \nmid b$ and that $q \nmid a$. Therefore it follows that p and q cannot be the same. □

THEOREM 13.2.2. *There are infinitely many prime numbers.*

EUCLID'S PROOF OF THEOREM 13.2.2. We will prove that there are infinitely many prime numbers by showing that for any finite set of prime numbers, there is a prime number not belonging to the finite set.

Consider a finite set $\{p_0, \dots, p_k\}$ of primes, and define

$$n := 1 + \prod_{i=0}^{k} p_i.$$

Then there exists, for each $0 \leq i \leq k$, a natural number q_i such that $n = q_i p_i + 1$. Indeed, we can simply define

$$q_i := \prod_{j=0, j \neq i}^{k} p_j.$$

Since n can be written in this way, it follows that n is relatively prime to each p_i. Consequently, the least prime divisor of n is relatively prime to each p_i. In other words, the least prime divisor of n is not in the set of primes $\{p_0, \dots, p_k\}$. □

13.2.2 Saidak's Proof

There are many proofs of the infinitude of primes. The following is due to Filip Saidak [Sai2006], who has published his proof in 2006, based on the idea that if $n = ab$ is the product of two numbers that are relatively prime and both at least 2, then n must have two prime factors.

Saidak's proof of Theorem 13.2.2. Let $N_0 := 1$, and define

$$N_{n+1} := N_n(N_n + 1).$$

We claim that N_n has at least n prime factors. In the base case, we note that it is indeed true that 1 has at least zero prime factors. For the inductive step, suppose that N_n has at least n prime factors. The number $N_n + 1$ is relatively prime to N_n, so its prime factors are all distinct from the prime factors of N_n. Furthermore, we have $1 < N_n + 1$, so $N_n + 1$ indeed has at least one prime factor. Thus it follows that N_{n+1} has at least $n + 1$ prime factors, and therefore there must be infinitely many primes. □

13.2.3 Furstenberg's Proof, Following Cass–Wildenberg

The following proof of the infinitude of primes is, in its essence, due to Hillel Furstenberg [Fur1955]. In its original formulation, this proof makes clever use of a topology on $\mathbb{Z}$. Although topologies are not hard to define, motivating them is beyond the scope of this course. We will therefore present a revised version of Furstenberg's proof, following Daniel Cass and Gerald Wildenberg [CW2003].

The Cass–Wildenberg approach to prove the infinitude of primes makes use of the concept of a periodic subset of $\mathbb{Z}$. A subset $A \subseteq \mathbb{Z}$ is said to be **periodic with period** n, or simply **periodic** if we merely assume such a natural number n to exist, if we have

$$x \in A \quad \Leftrightarrow \quad x + n \in A.$$

Thus, if A is a periodic subset of $\mathbb{Z}$ with period n, and $x \in A$, then

$$x + kn \in A$$

for all $k \in \mathbb{Z}$. In particular, all inhabited periodic subsets of $\mathbb{Z}$ are infinite. We note two basic facts about periodic subsets of $\mathbb{Z}$, which we leave to the reader to verify:

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

$$A_1 \cup \cdots \cup A_m$$

is again a periodic subset of $\mathbb{Z}$. The period of the union is the least common multiple of the periods of the subsets A_i.

(ii) If A is a periodic subset of $\mathbb{Z}$, then its complement $A^c := \{x \in \mathbb{Z} \mid x \notin A\}$ is periodic with the same period.



FURSTENBERG'S PROOF OF THEOREM 13.2.2, FOLLOWING CASS–WILDENBERG. Consider the subsets

$$S_p := \{kp \mid k \in \mathbb{Z}\},$$

where p is a prime number, and define

$$S := \bigcup_{p \text{ prime}} S_p.$$

Since every integer besides ± 1 is divisible by a prime, it follows that S consists of all the integers besides ± 1. The complement of S is therefore the set $\{-1, 1\}$. Note that the subset $\{-1, 1\}$ of $\mathbb{Z}$ cannot be periodic, since is inhabited and finite. This allows us to conclude that the subset S of $\mathbb{Z}$ is not periodic. However, if there were only finitely many primes, then S would be periodic because it would be a finite union of periodic subsets of $\mathbb{Z}$. Thus we conclude that there must be infinitely many primes. □

13.2.4 Erdős's Proof

DEFINITION 13.2.3. A natural number n is said to be **square-free** if the only square dividing n is 1. In other words, n is square-free if

$$k^2 \mid n \quad \Rightarrow \quad k = 1$$

for every natural number k.

By Theorem 13.1.5 (The Fundamental Theorem of Arithmetic) it follows that square-free numbers are those numbers of which the prime decomposition

$$n = p_1 \cdots p_n$$

is a product of distinct primes. In particular, if n is square free then the exponents in the prime factorization of n do not exceed 1. For instance, the numbers $3 \cdot 5 \cdot 17$ and $2 \cdot 11 \cdot 37$ are square-free, while the numbers $3^3 \cdot 5 \cdot 31$ and $2^5 \cdot 5^{11} \cdot 61$ aren't.

THEOREM 13.2.4. *Every natural number n can be written uniquely in the form*

$$n = k^2 m,$$

*where m is a square-free number. This is called the **square-free decomposition** of n, and the number m is called the **square-free part** of n.*

PROOF. Consider the set of natural numbers

$$S := \{d \in \mathbb{N} \mid \text{There exists a } k \in \mathbb{N} \text{ such that } k^2 d = n\}.$$

Clearly, this set contains the element n itself, since $n/n = 1$ is a perfect square. By Theorem 5.2.1 (The Well-Ordering Principle of the Natural Numbers), it follows that

S has a least element, which we call m. By definition, n/m is a perfect square, so there is a natural number k such that

$$n = k^2 m.$$

Next, we need to show that m is square-free. Suppose $d^2 \mid m$ is a positive divisor of m. Then the quotient $q = m/d^2$ is a divisor of n such that n/q is the perfect square $(kd)^2$. Since $q \leq m$ it follows by minimality that $q = m$ and hence that $d^2 = 1$. This implies that $d = 1$.

To finish the proof, we need to show that the square-free decomposition of n is unique. To this end, suppose that $n = l^2 d$, where d is square-free. We claim that any prime divisor of k is a prime divisor of l and conversely that any prime divisor of l is a prime divisor of k. To see this, note that for any prime $p \mid k$ we have $p^2 \mid k^2$ and consequently $p^2 \mid l^2 d$. Since d is square-free, this implies that $p \mid l^2$ and hence that $p \mid l$. The same argument applies the other way around, so it follows that $k = l$ and consequently $m = d$. □

Now that we have established that every natural number has a unique square-free decomposition, we are able to give Erdős's proof of the infinitude of primes. This proof was originally published in [Erd1938].

Erdős's proof of Theorem 13.2.2. Consider a finite list of primes $p_1, \dots, p_n$. We claim that for any x, there are at most

$$\sqrt{x} 2^n$$

numbers below x with all prime factors from the list $p_1, \dots, p_n$. To see this, recall from Theorem 13.2.4 that any number can be written in the form $k^2 m$ where m is square free. Then we have $k \leq \sqrt{x}$, leaving at most $\sqrt{x}$ choices for the number k. Furthermore, there are only 2^n square-free numbers m whose prime factors are from the list $p_1, \dots, p_n$, leaving at most 2^n choices for the value of m.

If all the numbers below x are products of powers of primes from the list $p_1, \dots, p_n$, we find that $x \leq \sqrt{x} 2^n$, or equivalently that

$$\sqrt{x} \leq 2^n.$$

However, this inequality clearly fails when x exceeds 2^{2n}, so there must be primes other than $p_1, \dots, p_n$. □

13.2.5 A Proof via the Stars-and-Bars Method

In Theorem 3.7.2 we have shown that the number of n-tuples $(m_1, \dots, m_n)$ such that $m_1 + \cdots + m_n = k$ is

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

Making use of Theorem 13.1.5 (The Fundamental Theorem of Arithmetic), we consequently find that for any list $p_1, \dots, p_n$ of distinct primes there are $\binom{k+n-1}{n}$ distinct natural numbers that can be written in the form

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

where $m_1 + \cdots + m_n = k$. Furthermore, there are $\binom{k+n}{n}$ distinct numbers that can be written in the form

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

where $m_1 + \cdots + m_n \leq k$. We will use this observation to obtain a bound on numbers N such that the prime factors of all positive integers $\leq N$ are among the primes $p_1, \dots, p_n$, which yields another proof of the infinitude of primes.

PROOF OF THEOREM 13.2.2. Consider a set $p_1, \dots, p_n$ of distinct primes, where $n \geq 5$, and let N be such that all the numbers $1 \leq x \leq N$ can be written as products of the primes $p_1, \dots, p_n$.

For any $x = p_1^{m_1} \cdots p_n^{m_n} \leq N$, we have $2^{m_1 + \cdots + m_n} \leq x \leq N$, so that

$$m_1 + \cdots + m_n \leq \log_2 N.$$

The set of ordered tuples $(m_1, \dots, m_n)$ with sum $\leq \log_2$ is in bijection with the set of ordered tuples $(m_0, \dots, m_n)$ satisfying

$$m_0 + m_1 + \cdots + m_n = \log_2 N.$$

The number of such ordered $(n+1)$-tuples is determined in Theorem 3.7.2, by which it follows that

$$N \leq \binom{\lfloor \log_2 N \rfloor + n}{n} \leq \frac{(\log_2 N + n)^n}{n!} \leq (\log_2 N + n)^n$$

Note that if $p_1, \dots, p_n$ were indeed a list of all the primes, then N would always satisfy this inequality. It remains to find a number N for which this inequality fails. We are permitted to pick a large number of a suitable form so as to reach a quick contradiction. Let us choose $N = 2^{2^n}$. Then we have

$$2^{2^n} \leq (2^n + n)^n < (2^n + 2^n)^n = 2^{n(n+1)}.$$

Now observe that for $n \geq 5$, as we have assumed at the start of the proof, we have $n(n+1) < 2^n$, which shows that $2^{n(n+1)} < 2^{2^n}$. Thus we have reached a contradiction, and we conclude that there must be infinitely many primes. □

13.3 Fermat Primes

During the 17th century, when computational resources were limited to human cognitive capacity aided with pen and paper, it was a significant challenge to come up with

large prime numbers. The hunt for large primes was focused primes of the form $2^n - 1$ and $2^n + 1$, since such numbers have a simple form yet grow very fast. Fermat observed that if $2^n + 1$ is a prime, then n cannot have any odd divisors.

Theorem 13.3.1. *If a number of the form $2^n + 1$ is prime, then $n = 2^k$ for some natural number k.*

Proof. Write $n = 2^k m$, where m is odd. Recall that when m is odd, then we have the following algebraic identity:

$$a^m + b^m = (a + b) \sum_{i=0}^{m-1} (-1)^i a^i b^{m-i-1}$$

By this formula for the sum of odd powers, we obtain the factorization

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

Thus, if $2^{2^k m} + 1$ is prime, then we must have $m = 1$. □

In other words, all primes of the form $2^n + 1$ are in fact of the form $2^{2^k} + 1$. Such numbers are called **Fermat numbers**: The nth Fermat number is given by

$$F_n := 2^{2^n} + 1.$$

The first few Fermat numbers are:

$$F_0 = 3, \qquad F_1 = 5, \qquad F_2 = 17, \qquad F_3 = 257, \qquad F_4 = 65537.$$

Of these numbers, F_0 through F_3 are easily seen to be prime. The number F_4 is also prime, but to prove this in a clean manner requires us to develop some more theory. Fermat famously conjectured that all Fermat numbers are prime. Goldbach brought this claim to Euler's attention in his letter, who was sceptical. A little later, Euler was able to prove that F_5 is indeed composite. Fermat had an extremely strong record of correct mathematical claims and conjectures, but this was one of the very few he got wrong. We will prove in Corollaries 16.1.5 and 16.1.6 that F_4 is prime and that F_5 is composite, once we have developed a bit more theory to help us reduce the search for prime factors.

Our next proof of the infinitude of primes is due to Goldbach, from 1730. In the 18th century, it was customary among mathematicians to share their findings private correspondences. In July of 1730, Goldbach wrote a letter to Euler, in which he established that all distinct Fermat numbers are relatively prime, and that hence there must be infinitely many primes. Recall that the Fermat numbers F_n are defined by

$$F_n := 2^{2^n} + 1.$$

THEOREM 13.3.2 (Product formula for the Fermat numbers). *The nth Fermat number satisfies the identity*

$$F_n - 2 = \prod_{0 \le k < n} F_k.$$

PROOF. We will prove the claim by strong induction. In the base case, we have

$$F_0 - 2 = 2^{2^0} - 1 = 1 = \prod_{0 \le k < 0} F_k,$$

since the product on the right-hand side is empty.

For the inductive step, we use the formula for the difference of squares:

$$(F_{n+1} - 2) = 2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1) = F_n \cdot \prod_{0 \le k < n} F_k = \prod_{0 \le k < n+1} F_k. \qquad \square$$

THEOREM 13.3.3 (Goldbach's Theorem). *Any two distinct Fermat numbers are relatively prime.*

PROOF. Consider two distinct natural numbers m and n, and assume that $m < n$. Using Theorem 13.3.2 (Product formula for the Fermat numbers), we see that $F_m \mid F_n - 2$. It follows that any common divisor d of F_m and F_n is also a divisor of 2, i.e., $d = 1$ or $d = 2$. However, all Fermat numbers are clearly odd, and this implies that any common divisor of F_m and F_n is 1. In other words, F_m and F_n are relatively prime. $\square$

GOLDBACH'S PROOF OF THEOREM 13.2.2. Since any two distinct Fermat numbers are relatively prime, and since any number ≥ 2 has a prime divisor, it follows that choosing a prime divisor for each Fermat number F_n yields infinitely many distinct primes. $\square$

13.4 Legendre's Formula and Kummer's Theorem

In some cases we can give precise expressions of the prime factorization of a number. We will describe here two such cases: The prime factorization of the factorial $n!$, which is due to Adrien-Marie Legendre, and the prime factorization of the binomial coefficients $\binom{n}{m}$, which is due to Ernst Kummer. We will use a corollary to Kummer's theorem in the proof of Bertrand's Postulate.

DEFINITION 13.4.1. The **p-adic valuation** of a positive integer n is the largest exponent m such that $p^m \mid n$. That is, the p-adic valuation $v_p(n)$ of n satisfies the logical equivalence

$$p^k \mid n \quad \Leftrightarrow \quad k \le v_p(n)$$

for every natural number k.

In other words, the p-adic valuation of n is the exponent of p in the prime factorization of n. For example, the 2-adic valuation of 24 is $v_2(24) = 3$ because the exponent of 2 in $24 = 2^3 \cdot 3$ is 3, and its 3-adic valuation is $v_3(24) = 1$ because the exponent

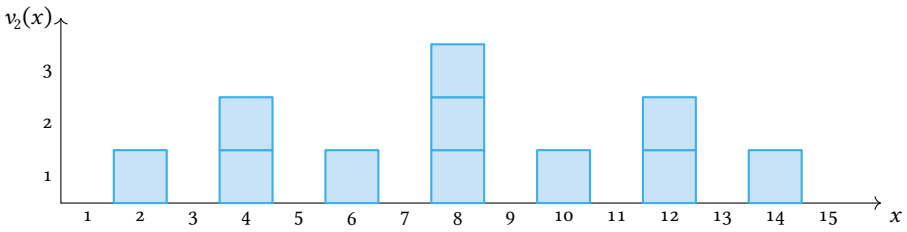


Figure 13.2: The 2-adic valuations of the numbers up to 15.

of 3 in $2^3 \cdot 3$ is 1. On the other hand, the 5-adic valuation of 24 is $v_5(24) = 0$ since 24 is not divisible by 5. The 2-adic valuations of the numbers up to 15 are displayed in Figure 13.2.

Example 13.4.2. A useful application of p-adic valuations is that the p-adic valuation of the greatest common divisor of two numbers is the minimum of their respective p-adic valuations. More generally, if the greatest common divisor is taken of multiple natural numbers we obtain

$$v_p(\gcd(n_1, \dots, n_k)) = \min(v_p(n_1), \dots, v_p(n_k)).$$

Likewise, the p-adic valuation of the least common multiple of $n_1, \dots, n_k$ is

$$v_p(\operatorname{lcm}(n_1, \dots, n_k)) = \max(v_p(n_1), \dots, v_p(n_k)).$$

For example the greatest common divisor and the least common multiple of $60 = 2^2 \cdot 3 \cdot 5$ and $525 = 3 \cdot 5^2 \cdot 7$ are

$$\gcd(60, 525) = 3 \cdot 5 = 15 \qquad \text{and} \qquad \operatorname{lcm}(60, 525) = 2^2 \cdot 3 \cdot 5^2 \cdot 7 = 2100.$$

An immediate consequence of the definition of p-adic valuations is the following proposition:

Proposition 13.4.3. *For any two positive integes a and b, the following are equivalent:*

(i) $a \mid b$.

(ii) $v_p(a) \leq v_p(b)$ *for every prime* p.

Example 13.4.4. The prime factorization of 15! can be obtained by computing the prime factorization of the numbers 1 through 15 individually, which are:

$$1, 2, 3, 2^2, 5, 2 \cdot 3, 7, 2^3, 3^2, 2 \cdot 5, 11, 2^2 \cdot 3, 13, 2 \cdot 7, 3 \cdot 5.$$

Thus, we obtain

$$15! = 2^{11} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13.$$

THEOREM 13.4.5 (Legendre's formula). *For any natural number n, we have*

$$n! = \prod_{p \leq n} p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots}.$$

PROOF. Another way of stating Legendre's formula for $n!$ is that the p-adic valuation of $n!$ is given by

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

To see this, note that each integer $1 \leq x \leq n$ divisible by p contributes a factor p to $n!$. Each integer $1 \leq x \leq n$ divisible by p^2 contributes a second factor of p to $n!$, and more generally, each integer $1 \leq x \leq n$ divisible by p^k contributes a kth factor of p.

Since there are $\left\lfloor \frac{n}{p^k} \right\rfloor$ integers from 1 to n divisible by p^k, it follows that the number of factors of p in $n!$ is

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor. \qquad \square$$

Incidentally, Legendre's formula can be used to give yet another proof of the infinitude of primes, due to Junho Peter Whang [WHA2010].

WHANG'S PROOF OF THEOREM 13.2.2. The p-adic valuation of $n!$ is bounded from above by

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \leq \sum_{k=1}^{\infty} \frac{n}{p^k} = \frac{n}{p-1}.$$

Now suppose that n is a natural number so that all the primes below n are from the list $p_1, \ldots, p_m$, and define

$$M := \prod_{i=1}^{m} p_i^{\frac{1}{p_i - 1}}.$$

Then it follows from Legendre's formula that

$$n! \leq M^n.$$

To give a quick lower bound for $n!$, note that for $1 \leq k \leq n$ we have $n \leq k(n+1-k)$. This gives the inequalities

$$n^{\frac{n}{2}} \leq n! \leq M^n.$$

However, this inequality fails when n exceeds M^2, so it follows that for $n > M^2$ there must be a prime not in the list $p_1, \ldots, p_m$. $\square$

In the following theorem we give a useful alternative expression for the p-adic valuation of $n!$.

Theorem 13.4.6 (de Polignac's formula). *Consider a natural number $n \geq 1$ written in its base p representation*

$$\sum_{i=0}^{l} a_i p^i,$$

where we have $0 \leq a_i < p$ for each i. Then p-adic valuation of $n!$ is

$$v_p(n!) = \frac{n - \sum_{i=0}^{l} a_i}{p-1}.$$

Proof. Given the base-p representation of n, the base-p representation of $\lfloor \frac{n}{p^k} \rfloor$ is given by dropping the digits first k digits in the base-p representation of n:

$$\left\lfloor \frac{n}{p^k} \right\rfloor = a_k + a_{k+1} p + \cdots + a_l p^{l-k}.$$

Using this observation, we obtain:

$$\sum_{k=1}^{l} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{l} \sum_{j=k}^{l} a_j p^{j-k} = \sum_{j=1}^{l} a_j \sum_{k=1}^{j} p^{j-k} = \sum_{j=1}^{l} a_j \frac{p^j - 1}{p-1}.$$

On the other hand, we have

$$n - \sum_{j=0}^{l} a_j = \sum_{j=0}^{l} a_j p^j - a_j = \sum_{j=0}^{l} a_j (p^j - 1).$$

This gives

$$\frac{n - \sum_{j=0}^{l} a_j}{p-1} = \sum_{j=0}^{l} a_j \frac{p^j - 1}{p-1} = \sum_{k=1}^{l} \left\lfloor \frac{n}{p^k} \right\rfloor. \qquad \square$$

Example 13.4.7. We can use Legendre's formula and de Polignac's formula to compute the prime factorizations of binomial coefficients. For example, it follows immediately from Legendre's formula that all the prime factors of the central binomial coefficient

$$\binom{64}{32}$$

are bounded from above by 64. Moreover, every prime $32 < p \leq 64$ occurs with p-adic valuation 1. Furthermore, the central binomial coefficient $\binom{64}{32}$ is not divisible by any prime $\frac{2}{3}32 < p \leq 32$, showing that the 23-, 29-, and 31-adic valuations of $\binom{64}{32}$ are 0. To compute the p-adic valuations for the lower primes, we use de Polignac's formula, for which it is necessary to write 32 and 64 in base p. Using letters A, B, C, and so forth for digits representing values of 10 and higher, we gather all the calculations for de Polignac's formula in the following table:

p	32 base p	64 base p	$\frac{2s_p(32)-s_p(64)}{p-1}$
2	$(100000)_2$	$(1000000)_2$	1
3	$(1012)_3$	$(2101)_3$	2
5	$(112)_5$	$(224)_5$	0
7	$(44)_7$	$(121)_7$	2
11	$(2A)_{11}$	$(59)_{11}$	1
13	$(26)_{13}$	$(4C)_{13}$	0
17	$(1F)_{17}$	$(3D)_{17}$	1
19	$(1D)_{19}$	$(37)_{19}$	1

Thus, we see that

$$\binom{64}{32} = 2 \cdot 3^2 \cdot 7^2 \cdot 11 \cdot 17 \cdot 19 \cdot 37 \cdot 41 \cdot 43 \cdot 47 \cdot 53 \cdot 59 \cdot 61.$$

Even though the binomial coefficient $\binom{64}{32}$ is a fairly large number with 19 decimal digits, we didn't need to evaluate it in order to obtain its prime factorization. In fact, without fully evaluating it, we can now determine the last decimal digit of $\binom{64}{32}$ by the following procedure: Start with $d_0 := 1$ and let d_{i+1} be the remainder of the product $d_i p_i^{m_i}$ after division by 10, where $p_i^{m_i}$ is the ith prime power in the prime factorization of $\binom{64}{32}$. This gives:

$$d_1 = 2,\ d_2 = 8,\ d_3 = 2,\ d_4 = 2,\ \ldots,\ d_{13} = 4.$$

The last decimal digit of $\binom{64}{32}$ is therefore a 4.

In the following theorem, which is due to Ernst Kummer [KUM1852], we will compute the p-adic valuation of the binomial coefficients in full generality. Before we do this, we need to recall addition of two natural numbers written in base p. Suppose that

$$m = \sum_{i=0}^{l_m} a_i p^i \qquad \text{and} \qquad n = \sum_{i=0}^{l_n} b_i p^i.$$

Then their sum $m + n$ has base-p representation

$$m + n = \sum_{i=0}^{l_n} c_i p^i,$$

where c_i is obtained by the following recursive procedure, simultaneously with a number $u(m,n)_i \in \{0,1\}$ recording whether a 1 needs to be carried over to the next digit: Set $u(m,n)_0 = 0$ and define

$$(c_i, u(m,n)_{i+1}) := \begin{cases} (a_i + b_i + u(m,n)_i, 0) & \text{if } a_i + b_i + u(m,n)_i < p, \\ (a_i + b_i + u(m,n)_i - p, 1) & \text{if } a_i + b_i + u(m,n)_i \geq p. \end{cases}$$

Theorem 13.4.8 (Kummer's Theorem). *Consider two natural numbers m and n. The p-adic valuation of the binomial coefficient $\binom{m+n}{m}$ is the number of carries in the addition of m and n in base p: If m and n have base p-representations*

$$m = \sum_{i=0}^{l_m} a_i p^i \qquad \text{and} \qquad n = \sum_{i=0}^{l_n} b_i p^i,$$

then

$$v_p\binom{m+n}{m} = \#\{0 \leq i \leq l_n \mid u(m,n)_i = 1\}.$$

Proof. Write $s_p(x)$ for the sum of the digits of the p-adic representation of a natural number x. By de Polignac's formula for the p-adic valuation of $(m+n)!$ we find that

$$v_p\binom{m+n}{m} = v_p((m+n)!) - v_p(m!) - v_p(n!) = \frac{s_p(m) + s_p(n) - s_p(m+n)}{p-1}.$$

The p-adic representation of $m+n$ is given by

$$m+n = \sum_{i=0}^{l_{m+n}} c_i p^i,$$

where

$$c_i = \begin{cases} a_i + b_i + u(m,n)_i & \text{if } a_i + b_i + u(m,n)_i < p, \\ a_i + b_i + u(m,n)_i - p & \text{otherwise.} \end{cases}$$

We therefore find that the numerator in de Polignac's expression for $v_p\binom{m+n}{m}$ contains a term $p - u(m,n)_{i+1}$ for every time $u(m,n)_{i+1} = 1$. That is, the numerator is of the form $C(p-1)$ where C is the number of carries. This proves the theorem. □

Example 13.4.9. Consider two natural numbers m and n such that

$$m = \sum_{i=0}^{k} a_i 2^i \qquad \text{and} \qquad n - m = \sum_{i=0}^{k} b_i 2^i,$$

where $0 \leq a_i, b_i < 2$ for every i. Then the binomial coefficient $\binom{n}{m}$ is odd if and only if $a_i b_i = 0$ for every $0 \leq i \leq k$, since only in this situation there are no carries when m and n are added in base 2.

Kummer's theorem can be used to show that the binomial coefficient $\binom{n}{k}$ always divides the least common multiple of $1, 2, \ldots, n$. In order to prove this result, note that the largest exponent m such that $p^m \leq n$ is the number

$$m = \lfloor \log_p(n) \rfloor.$$

In other words, if m is the largest integer not exceeding $\log_p(n)$, then the leading digit in the base-p representation of n belongs to p^m.



COROLLARY 13.4.10. *For any $0 \leq k \leq n$ we have*

$$\binom{n}{k} \Big| \operatorname{lcm}(1, \ldots, n).$$

PROOF. Suppose that the base-p representation of n is

$$n = \sum_{i=0}^{l} a_i p^i.$$

Then there are clearly at most l carries when we add k to $n-k$. Since $p^l \leq n$, it follows that

$$p^{\nu_p\binom{n}{k}} \mid \operatorname{lcm}(1, \ldots, n).$$

Since this is true for every prime $p \leq n$, and $\binom{n}{k}$ contains only prime divisors up to n, the claim follows. □

13.5 Bertrand's Postulate

In 1845, Joseph Bertrand observed that for any $1 \leq n \leq 3,000,000$ there is always a prime between n and $2n$, and conjectured that this must be true for all n [BER1845]. Nowadays on a computer, it is really easy to generate lists of primes p_i so that the prime p_{i+1} is strictly below $2p_i$ for each i. Taking each time the largest possible prime satisfying this requirement, we obtain the list

2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259,

2503, 5003, 9973, 19937, 39869, 79699, 159389,

318751, 637499, 1274989, 2549951, 5099893, ...

The primes in this list are sometimes called the **Bertrand primes**, and they are listed as A006992 in the On-Line Encyclopedia of Integer Sequences [OEI2025]. Bertrand's conjecture was proven five years later by Pafnuty Chebyshev, who contributed many more results about the distribution of the primes using analytical methods [CHE1852]. We will give a proof by Paul Erdős [ERD1932], which can be obtained through the methods of the previous section.

LEMMA 13.5.1 (Chebyshev's primorial bound). *For any positive integer n, we have*

$$\prod_{p \leq n} p < 4^n.$$

PROOF. The proof is by induction on n. For $n = 1$, there are no primes $p \leq 1$, so the product over all the primes $p \leq 1$ is just 1, which is indeed strictly below 4. Likewise, the theorem holds for $n = 2$, because $2 < 4^2$.

For the inductive step, assume that $n \geq 2$ and that $\prod_{p \leq n} p < 4^n$. In order to show that

$$\prod_{p \leq n+1} p < 4^{n+1},$$

there are two cases to consider: Either $n+1$ is even or $n+1$ is odd. The even case is immediate: We have

$$\prod_{p \leq n+1} p = \prod_{p \leq n} p < 4^n < 4^{n+1}.$$

In the odd case, there is an m such that $2m+1 = n+1$. Since every prime $m+2 \leq p \leq 2m+1$ divides the binomial coefficient $\binom{2m+1}{m}$, it follows that

$$\prod_{p \leq 2m+1} p \leq \binom{2m+1}{m} \cdot \prod_{p \leq m+1} p < \binom{2m+1}{m} 4^{m+1}.$$

To finish the proof, it suffices to show that $\binom{2m+1}{m} \leq 4^m$. This follows, since the binomial coefficients $\binom{2m+1}{m}$ and $\binom{2m+1}{m+1}$ occur separately in the expansion of $(1+1)^{2m+1}$. However, they are equal, so neither of them can exceed $\frac{1}{2} 2^{2m+1} = 4^m$, which proves the lemma. □

Theorem 13.5.2. *For any positive integer n, there is a prime $n < p \leq 2n$.*

Proof. Consider an integer $n \geq 2$ for which there is no prime $n < p < 2n$, and let p be a prime divisor of the central binomial coefficient $\binom{2n}{n}$. Such a prime divisor must then be less than or equal to $\frac{2}{3}n$, since $q^3 \nmid (2n)!$ for any prime $\frac{2}{3}n < q \leq n$, while $q^2 \mid (n!)^2$.

Now, recall from Corollary 13.4.10 that any prime power $p^m \mid \binom{2n}{n}$ must satisfy $p^m \leq 2n$. In particular, the number of primes p such that $p^2 \mid \binom{2n}{n}$ is bound from above by the inequality

$$p \leq \sqrt{2n}.$$

This shows that there are at most $\sqrt{2n}$ primes in the prime factorization of $\binom{2n}{n}$, of which the exponent is larger than 1. Furthermore, it follows that

$$\prod_{p^2 \mid \binom{2n}{n}} p^{v_p\binom{2n}{n}} \leq (2n)^{\sqrt{2n}}.$$

Combined with the fact that the prime factors of $\binom{2n}{n}$ don't exceed $\frac{2n}{3}$, we obtain the following estimates:

$$\frac{4^n}{2n+1} < \binom{2n}{n} \leq (2n)^{\sqrt{2n}} \cdot \prod_{p \leq 2n/3} p < (2n)^{\sqrt{2n}} \cdot 4^{\frac{2n}{3}}.$$

Here, the first inequality was established in Exercise 3.6, and the last inequality follows from Lemma 13.5.1. Rearranging this strict inequality, we obtain

$$4^{\frac{n}{3}} < (2n+1)(2n)^{\sqrt{2n}} < 2(2n)^{\sqrt{2n}+1}.$$



Taking logarithms base 2 on both sides, we find that

$$\frac{2n}{3} < (\sqrt{2n} + 1)\log_2(2n) + 1.$$

We see that this strict inequality fails for $n \geq 2^9 = 512$, since

$$341 \leq \frac{2^{10}}{3} \not< 331 = (2^5 + 1) \cdot 10 + 1.$$

We have thus proven that if there does not exist a prime $n < p \leq 2n$, then we must have $p < 512$. However, using the Bertrand primes up to 631, we see that for every $n < 512$ there exists a prime $n < p \leq 2n$. Thus Bertrand's postulate is proven for all n. □

Exercises

Starter Exercises

13.1 In the number grid provided at the end of the introduction, shade the numbered cells in two colors:

(i) Leave all the prime numbers unshaded.

(ii) Shade the number 1 and all square-free composite numbers in one color.

(iii) Shade all non-square-free numbers in the other color.

Explain your method.

13.2 Find the first ten primes of the form $n^2 + 1$. The first of Laundau's four open problems about primes asks whether there are infinitely many such primes [Lan1912].

13.3 Find the first ten primes p such that $2p - 1$ is also prime. It is unknown whether there are infinitely many such primes.

13.4 Given a prime $p > 3$, show that $p^2 \equiv 1 \pmod{24}$.

13.5 By computing its prime factorization, show that

$$\binom{50}{3}$$

is a square number.

13.6 Show that

$$a^2 \equiv 1 \pmod{p} \Leftrightarrow a \equiv \pm 1 \pmod{p}.$$

13.7 Show that

$$\sum_{k=1}^{n} k^3 \Bigg| \prod_{k=1}^{n} k^3$$

holds for every n, except when $n + 1$ is an odd prime.

Routine-Building Exercises

13.8 Find the longest arithmetic progression of primes under 1000. Hint: Use congruences to constrain the step size.

13.9 Compute the prime factorizations of the following numbers:

(a) $5^{15} - 1$.
(b) $3^{18} - 1$.
(c) $2^{48} - 1$.

13.10 Show that there are no primes p such that $p + 8$ and $p + 22$ are also prime.

13.11 A pair of **twin primes** is a pair of primes p and q such that $q - p = 2$. Consider a pair of twin primes p and q strictly greater than 3.

(a) Show that $p + q \equiv 0 \pmod{12}$.



(b) Show that $pq \equiv -1 \pmod 9$.

13.12 A **Sophie Germain prime** is a prime p such that $2p+1$ is also prime. Show that if $p > 3$ is a Sophie Germain prime, then

$$p(2p+1) \equiv 1 \pmod{18}.$$

13.13 (a) Show that any odd prime of the form $x^2 + y^2$ must be congruent to $1 \pmod 4$, and find the first ten primes of this form.

(b) Show that any prime $p > 3$ of the form $x^2 + 3y^2$ must be congruent to $1 \pmod 6$, and find the first ten primes of this form.

(c) Show that any prime $p \neq 5$ of the form $x^2 + 5y^2$ must satisfy

$$p \equiv 1 \text{ or } 9 \pmod{20}$$

and find the first ten primes of this form.

(d) Show that any prime p of the form $x^2 + 6y^2$ must satisfy

$$p \equiv 1 \text{ or } 7 \pmod{24}$$

and find the first ten primes of this form.

The book [Cox1989] contains a beautiful exposition of the theory of primes of the form $x^2 + ny^2$, and serves as a wonderful introduction to class field theory.

13.14 Determine the number of trailing zeros in the decimal representations of $100!$ and $2^{10}!$.

13.15 Show that the inequality

$$2^{v_2\binom{2n}{n}} - 1 \leq n$$

holds for all $n \geq 0$.

13.16 (a) In Figure 13.2 we saw that $v_2((2^4-1)!) = 11$. More generally, prove that

$$v_p((p^k-1)!) = \frac{p^k-1}{p-1} - k$$

(b) Show that

$$v_p\left(\binom{p^n-1}{p^m-1}\right) = 0$$

for any $0 \leq m \leq n$.

13.17 Show that

$$\binom{42}{6} \,\Big|\, \binom{42}{12} \qquad \text{and} \qquad \binom{42}{6} \,\Big|\, \binom{42}{18}.$$

13.18 (a) Show that

$$\binom{30}{2} \,\Big|\, \binom{30}{2k}$$

for every $1 \leq k \leq 14$.

(b) Show that if p is a prime such that $q = 2p - 1$ is also a prime, then

$$\binom{2p}{2} \mid \binom{2p}{2k}$$

for every $1 \leq k \leq p - 1$.

13.19 (a) Show that

$$\frac{\operatorname{lcm}(1, \ldots, n)}{\operatorname{lcm}(1, \ldots, m)} = \prod_{k \geq 1} \prod_{\substack{p \text{ prime} \\ m < p^k \leq n}} p.$$

Use this formula to conclude that

$$\frac{\operatorname{lcm}(1, \ldots, n)}{\operatorname{lcm}(1, \ldots, n-1)} = \begin{cases} p & \text{if } n = p^k \text{ for some prime } p \text{ and } k \geq 1, \\ 1 & \text{otherwise.} \end{cases}$$

(b) Show that

$$\frac{\operatorname{lcm}(1, \ldots, n)}{\operatorname{lcm}(1, \ldots, m)}$$

is square-free for every $m \leq n$ such that $n \leq 2m$.

(c) Show that

$$\frac{\operatorname{lcm}(1, \ldots, n)}{\operatorname{lcm}(1, \ldots, m)} \mid \binom{n}{m}.$$

for every $m \leq n$ such that $n \leq 2m$.

Challenge Exercises

13.20 Show that for any prime p, if $p^2 + 2$ is prime then $p + 2$ is prime.

13.21 Consider $n \geq 1$. Prove that among any 2^n integers all of whose prime factors are less than or equal to n, there are two distinct integers such that their product is a square.

13.22 Consider a prime $p \equiv 3 \pmod 4$, and suppose that $v_p(n)$ is odd. Show that there is a bijection between the set of divisors $d \equiv 1 \pmod 4$ of n and the set of divisors $d \equiv 3 \pmod 4$ of n.

13.23 For any n, let $\omega(n)$ be the number of its prime divisors. Show that the number of integers $0 < x < n$ such that $x^2 \equiv x \pmod n$ is $2^{\omega(n)}$. Hint: Use the Chinese Remainder Theorem to show that there is a bijection between the integers x such that $x^2 \equiv x \pmod n$ and the subsets of the set of prime divisors of n.

13.24 Show that there is exactly one positive integer k such that both $2^k - 1$ and $2^k + 1$ are prime.

13.25 In this exercise F_n denotes the nth Fibonacci number. Show that a prime p divides F_{p-1} if and only if $p \equiv \pm 1 \pmod 5$ and p divides F_{p+1} if and only if $p \equiv \pm 2 \pmod 5$.



13.26 Prove the following identity of Bakir Farhi [FAR2009]:

$$\operatorname{lcm}\left(\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}\right) = \frac{\operatorname{lcm}(1, \ldots, n+1)}{n+1}.$$

13.27 Show that there are infinitely many numbers not divisible by any Fibonacci numbers other than 1.

13.28 Use Bertrand's Postulate to show that

$$\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n}$$

is never an integer.

Chapter 14

Multiplicative Functions

14.1 Perfect Numbers

The number 6 satisfies the curious property that the sum of its proper divisors $1+2+3$ is equal to the number 6 itself. This property of a number being equal to the sum of its own proper divisors, which is also called the *aliquot sum*, was deemed so special in ancient times, that these numbers were called *perfect*.

Definition 14.1.1. Consider a positive natural number n. The **aliquot sum** $s(n)$ of n is defined by

$$s(n) := \sum_{d \mid n,\ d<n} d$$

(i) The number n is called **perfect** if $s(n) = n$.

(ii) The number n is called **deficient** if $s(n) < n$.

(iii) The number n is called **abundant** if $s(n) > n$.

Example 14.1.2. The number 6 is perfect, since $6 = 1+2+3$; the number 8 is deficient, since $1+2+4 = 7 < 8$, and the number 12 is abundant, since $1+2+3+4+6 = 16 > 12$.

Euclid observed that if $2^m - 1$ is prime, then we can always find a number k such that

$$2^k(2^m - 1)$$

is perfect. Indeed, since the divisors of 2^k are precisely the numbers 2^i with $0 \le i \le k$, it follows that the divisors of $2^k(2^m-1)$ are exactly

$$1,\ 2, \dots,\ 2^k, \qquad \text{and} \qquad (2^m-1),\ 2(2^m-1), \dots,\ 2^k(2^m-1).$$

The sum of the divisors of $2^k(2^m - 1)$ is therefore

$$(2^{k+1} - 1) + (2^{k+1} - 1)(2^m - 1) = (2^{k+1} - 1)2^m.$$

The equation

$$(2^{k+1} - 1)2^m = 2 \cdot 2^k(2^m - 1)$$

now implies that $m = k + 1$. Thus, we have proven the following proposition, which Euclid recorded as Proposition 36 in Book IX of the Elements.

PROPOSITION 14.1.3 (Euclid). *If the number $2^m - 1$ is prime, then the number $2^{m-1}(2^m - 1)$, which is indeed the $(2^m - 1)^{th}$ triangular number, is perfect.*

Using Euclid's method, we can find the first few perfect numbers. Table 14.1 displays the prime factorization of the *Mersenne number* $2^m - 1$ for $2 \leq m \leq 11$.

m	2	3	4	5	6	7	8	9	10	11
$2^m - 1$	**3**	7	3·5	**31**	3^2·7	**127**	3·5·17	7·73	3·11·31	23·89

Table 14.1: The Mersenne numbers M_m for $2 \leq m \leq 11$.

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 14.1.4. *If the mth Mersenne number $M_m = 2^m - 1$ is prime, then m is prime.*

PROOF. We prove the contrapositive: If m is composite, so that $m = ab$ for some $a, b > 1$, then M_m is composite. This follows directly from the formula for the difference of powers:

$$2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1) \sum_{k=0}^{b-1} (2^a)^k. \qquad \square$$

Mersenne numbers which are prime are called **Mersenne primes**. They are used in the search for extremely large prime numbers. Note, however, that not every Mersenne number M_p with p prime is a prime number. For example, $M_{11} = 23 \cdot 89$.

No perfect numbers other than the ones described by Euclid have been found, so it is natural to wonder whether Euclid described all of them. This leads us to Euler, who was able to prove in the 18th century that every *even* perfect number is of Euclid's form. Euler did so by analyzing the function σ, which returns for each n the sum of its divisors. Euler's proof marks the beginning of the theory of *arithmetic functions*.

Definition 14.1.5. We define the **sum-of-divisors** function σ by

$$\sigma(n) := \sum_{d|n} d.$$

Thus, a number n is perfect if $\sigma(n) = 2n$. Notice that a number n is prime if and only if $\sigma(n) = n+1$. The next easiest sum of divisors to calculate is the sum of divisors of a prime power. For any prime p we have

$$\sigma(p^m) = \sum_{k=0}^{m} p^k = \frac{p^{m+1}-1}{p-1}.$$

Indeed, $d \mid p^m$ if and only if $d = p^k$ for some $0 \le k \le m$, so the sum of the divisors of p^m is the finite geometric series $1 + p + p^2 + \cdots + p^m$.

Proposition 14.1.6. *Suppose m and n are relatively prime. Then*

$$\sigma(mn) = \sigma(m)\sigma(n).$$

Proof. We first claim that the operation $u, v \mapsto uv$, which takes a pair of numbers $u \mid m$ and $v \mid n$ and returns their product, which is a divisor of mn, defines a bijection

$$\{u \mid u \mid m\} \times \{v \mid v \mid n\} \cong \{d \mid d \mid mn\}$$

To see this, we need to define an inverse function. That is, given a divisor $d \mid mn$ we need to construct divisors of m and n. Observe that, since m and n are relatively prime, it follows that $d = \gcd(d,m)\gcd(d,n)$. Thus, we define $u_d := \gcd(d,m)$ and $v_d := \gcd(d,n)$. Furthermore, when $u \mid m$ and $v \mid n$ are arbitrary, then we have $\gcd(uv,m) = u$ and $\gcd(uv,n) = v$. These equations show that the map $d \mapsto (u_d, v_d)$ is indeed inverse to the function $u, v \mapsto uv$.

Using the bijection we just constructed, we see that

$$\left(\sum_{u|m} u\right)\left(\sum_{v|n} v\right) = \sum_{u|m}\sum_{v|n} uv = \sum_{d|mn} d. \qquad \square$$

The multiplicative property of the sum-of-divisors function along with the expressions for $\sum(p^m)$ completely determine the values of the function σ for any positive integer of which the prime factorization is known.

Corollary 14.1.7. *Suppose that $n = p_1^{m_1} \cdots p_k^{m_k}$, where all the primes p_i are distinct. Then*

$$\sigma(n) = \frac{p_1^{m_1+1}-1}{p_1-1} \cdots \frac{p_k^{m_k+1}-1}{p_k-1}.$$



EXAMPLE 14.1.8. We saw in Example 13.4.4 that $15! = 2^{11}\cdot 3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13$. It follows that

$$\sigma(15!) = (2^{12}-1)\cdot\frac{3^7-1}{2}\cdot\frac{5^4-1}{4}\cdot\frac{7^3-1}{6}\cdot 12\cdot 14 = 2^5\cdot 3^5\cdot 5\cdot 7^2\cdot 13^2\cdot 19\cdot 1093.$$

THEOREM 14.1.9 (Euclid–Euler). *An even number n is perfect if and only if it is of the form*

$$2^{p-1}(2^p-1)$$

for some prime p, where the number 2^p-1 is prime.

PROOF. We have already seen that n is perfect if $n = 2^{p-1}(2^p-1)$, provided that 2^p-1 is prime. Furthermore, since the condition that 2^p-1 is prime implies that p is prime, and hence that 2^{p-1} is divisible by 2, it follows that numbers of the form $2^{p-1}(2^p-1)$ are even.

For the converse, assume that n is an even perfect number, so that $\sigma(n) = 2n$. Using the 2-adic decomposition, we can write $n = 2^k m$ where m is odd. Since odd numbers are relatively prime to powers of 2, it follows that

$$\sigma(2^k m) = \sigma(2^k)\sigma(m) = (2^{k+1}-1)\sigma(m).$$

By the assumption that $2^k m$ is perfect, we obtain that

$$(2^{k+1}-1)\sigma(m) = 2^{k+1}m.$$

Since the number $s := 2^{k+1}-1$ is relatively prime to 2^{k+1}, it follows that $s \mid m$. If we write $m = st$, then the displayed equation simplifies to

$$\sigma(m) = 2^{k+1}t = (s+1)t = t + st.$$

Now observe that both t and st are divisors of m. They are distinct, since n is assumed to be even and thus we have $s > 1$. Since $\sigma(m) = t + st$ is the sum of all the divisors of m, it follows that t and st are the only divisors of m. We conclude that $t = 1$ and $s = m$. Furthermore, we obtain that $\sigma(m) = m + 1$, which implies that m is prime. We have thus shown that

$$n = 2^k(2^{k+1}-1),$$

and that $2^{k+1}-1$ is prime. This last property implies that $k+1$ is prime, which completes the proof. □

The Euclid–Euler theorem completely characterizes even perfect numbers. However, it doesn't tell us anything about odd perfect numbers. No odd perfect numbers have ever been found, and it is conjectured that none exist. It has been shown that any odd perfect number must be greater than 10^{1500} [OR2012].

14.2 Euler's Totient Function

Before we introduce reduced residue systems, let us prove a lemma.

Lemma 14.2.1. *Suppose that* $a \equiv b \pmod{n}$. *Then* $\gcd(a,n) = \gcd(b,n)$. *Consequently, we have* $\gcd(a,n) = 1$ *if and only if* $\gcd(b,n) = 1$.

Proof. By the assumption that a and b are congruent modulo n, it follows that they have the same remainder after division by n. Let r be this remainder. Since $\gcd(a,n) = \gcd(r,n)$ and $\gcd(b,n) = \gcd(r,n)$ we see that

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

This equality implies that the left hand side equals 1 if and only if the right hand side equals 1. □

By the previous lemma, we can test whether an integer is relatively prime to n by testing any element in its congruence class. This allows us to make the following definition.

Definition 14.2.2. A **reduced residue system** modulo n is a set

$$\{r_1, \dots, r_k\}$$

of integers satisfying the condition that for every integer a relatively prime to n, there is exactly one index $1 \leq i \leq k$ such that

$$a \equiv r_i \pmod{n}.$$

Corollary 14.2.3. *Any two reduced residue systems modulo* n *have the same size, for which we write* $\phi(n)$. *The function* ϕ *is called* ***Euler's totient function****.*

Proof. Reduced residue systems are choices of representatives of the congruence classes in which all elements are relatively prime to n. Thus, the size of a reduced residue system is always equal to the number of such congruence classes. □

Theorem 14.2.4. *Euler's totient function* ϕ *is multiplicative: For any two relatively prime numbers* m *and* n *we have*

$$\phi(mn) = \phi(m)\phi(n).$$

Proof. We prove the claim by a counting argument: We claim that the bijection of Theorem 9.3.1 (Chinese Remainder Theorem)

$$\{0 \leq x < mn\} \cong \{0 \leq a < m\} \times \{0 \leq b < n\},$$

given by $x \mapsto (x \pmod{m}, x \pmod{n})$, restricts to a bijection

$$\{0 \leq x < mn \mid \gcd(x, mn) = 1\} \cong \{0 \leq a < m \mid \gcd(a,m) = 1\} \times \{0 \leq b < n \mid \gcd(b,n) = 1\}.$$

To see this, note that x is relatively prime to a number k if and only if $x \pmod{k}$ is relatively prime to k. Thus, we have to show that

$$\gcd(x, mn) = 1 \quad \Leftrightarrow \quad \gcd(x, m) = 1 \text{ and } \gcd(x, n) = 1.$$

For the forward direction, suppose that $\gcd(x, mn) = 1$. In this case, any d dividing both x and m is also a common divisor of x and mn so it must be 1. Thus, it is clear that if $\gcd(x, mn) = 1$, then $\gcd(x, m) = \gcd(x, n) = 1$.

For the converse, suppose that $\gcd(x, m) = \gcd(x, n) = 1$, and suppose that $d \mid x$ and $d \mid mn$. Since m and n are relatively prime, we can uniquely determine two numbers a and b satisfying $d = ab$, such that $a \mid m$ and $b \mid n$. For these numbers, we obtain that $a \mid \gcd(x, m) = 1$ and $b \mid \gcd(x, n) = 1$ so that both $a = 1$ and $b = 1$. This shows that $d = 1$. □

Since multiplicative functions are fully determined by their values on prime powers, we obtain the following important expression for Euler's totient function.

THEOREM 14.2.5. *Consider a positive integer n with prime factorization $n = p_1^{m_1} \cdots p_k^{m_k}$. Then*

$$\phi(n) = \prod_{i=1}^{k} (p_i^{m_i} - p_i^{m_i - 1}) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

COROLLARY 14.2.6. *The value $\phi(n)$ of Euler's totient function is even for $n > 2$.*

PROOF. For $k \geq 2$ we have $\phi(2^k) = 2^{k-1}$, which is even. Furthermore, every odd prime factor p contributes an even factor $p - 1$ to $\phi(n)$. □

Since $\phi(p^k) = p^{k-1}(p - 1)$, it follows that if $k \leq l$, then $\phi(p^k) \mid \phi(p^l)$. Since Euler's totient function is multiplicative by theorem:multiplicative-totient, we obtain the following corollary:

COROLLARY 14.2.7. *The function $n \mapsto \phi(n)$ is a divisibility sequence: For any two natural numbers m and n, we have*

$$m \mid n \quad \Rightarrow \quad \phi(m) \mid \phi(n).$$

EXAMPLE 14.2.8. We will use Theorem 14.2.5 to determine all n for which $\phi(n) = 2^k$ for some k.

If p is an odd prime so that $p^a - p^{a-1} = p^{a-1}(p-1)$ is a power of 2, then it follows that $a - 1 = 0$. In other words, in order for $p^a - p^{a-1}$ to be a power of 2, we must have $a = 1$. This shows that if $\phi(n)$ is a power of 2, then n must be of the form

$$n = 2^a \prod_{p \in S} p,$$

where S is a subset of the **Fermat primes**; that is, every prime in S is the form $2^b + 1$. The only known such primes are

$$3,\ 5,\ 17,\ 257,\ \text{and } 65537.$$

2^k	Fermat primes $p \leq 2^k + 1$	n such that $\phi(n) = 2^k$
1	none	1, 2
2	3	3, 4, 6
4	3, 5	5, 8, 10, 12
8	3, 5	15, 16, 20, 24, 30
16	3, 5, 17	17, 32, 34, 40, 48, 60
32	3, 5, 17	51, 64, 68, 80, 96, 102, 120
64	3, 5, 17	85, 128, 136, 160, 170, 192, 204, 240
128	3, 5, 17	255, 256, 272, 320, 340, 384, 408, 480, 510

Table 14.2: Lists of numbers n for which $\phi(n) = 2^k$

We conclude that the only numbers n for which $\phi(n) = 4$ are 5, 8, 10, and 12, and the only numbers n for which $\phi(n) = 8$ are 15, 16, 20, 24, and 30. Table 14.2 lists the numbers n for which $\phi(n) = 2^k$ up to $2^k = 128$.

14.3 Multiplicative Functions

A function f defined on the positive integers with output in any number system, such as the integers, real numbers, or complex numbers, is called an **arithmetic function**. For example, Euler's totient function ϕ, which returns for each n the number of elements $0 < k < n$ relatively prime to n, is an arithmetic function. Some other important arithmetic functions include the **number of divisors function** τ and the **sum of divisors function** σ:

$$\tau(n) := \sum_{d|n} 1 \qquad \text{and} \qquad \sigma(n) := \sum_{d|n} d.$$

Note that the number of divisors and the sum of divisors are not defined for $n = 0$. Arithmetic functions are typically only defined on the positive integers $\{1, 2, 3, \ldots\}$. Even for functions which are defined on 0, such as Euler's totient function, when we consider them as arithmetic functions we will consider their domain of definition to be the positive integers.

Other functions, which are worth naming are the **constant function** $n \mapsto 1$, which we will simply denote by 1, and the **identity function** $n \mapsto n$, which we will denote by id. In the pages that follow, we shall encounter two more arithmetic functions: the *unit function* ε and the *Möbius function* μ.

Definition 14.3.1. An arithmetic function f is said to be **multiplicative** if for any two relatively prime natural numbers m and n we have

$$f(mn) = f(m)f(n).$$

Proposition 14.3.2. *If f is a nonzero multiplicative function, then $f(1) = 1$.*



PROOF. Since f is assumed to be nonzero, there is a natural number n such that $f(n) \neq 0$. Thus,

$$f(n) = f(1n) = f(1)f(n)$$

by the assumption that f is multiplicative. Since multiplication by a nonzero number is injective, it follows that $f(1) = 1$. □

It follows that the constant function 1 is the only constant multiplicative function. By the following proposition, we see that any multiplicative function is determined by its values on prime powers.

PROPOSITION 14.3.3. *If f is a multiplicative function and $n = p_1^{m_1} \cdots p_k^{m_k}$, where the primes $p_1, \ldots, p_k$ are distinct, then*

$$f(n) = f(p_1^{m_1}) \cdots f(p_k^{m_k}).$$

PROOF. Since the primes $p_1, \ldots, p_k$ are assumed to be distinct, it follows that the prime powers $p_1^{m_1}, \ldots, p_k^{m_k}$ are pairwise relatively prime, hence the claim follows by induction on k. □

The following theorem provides a useful way of proving that a function is multiplicative.

THEOREM 14.3.4. *Suppose f is a multiplicative function, and define the function F by*

$$F(n) := \sum_{d \mid n} f(d).$$

PROOF. Consider two relatively prime natural numbers m and n. Then there is a bijection $(c, d) \mapsto cd$ from the set

$$\{c \mid c \text{ divides } m\} \times \{d \mid d \text{ divides n}\}$$

to the set of divisors of mn. For the inverse function, define the function

$$e \mapsto (\gcd(e, m), \gcd(e, n)),$$

which sends a divisor e of mn to a pair of divisors of m and n. To see that this is indeed an inverse, note that if $c \mid m$ and $d \mid n$, then $\gcd(d, m) = 1$ so that

$$c = \gcd(cd, m).$$

Similarly, we have that $\gcd(c, n) = 1$ so that $d = \gcd(cd, n)$. This shows that

$$(c, d) = (\gcd(cd, m), \gcd(cd, n)).$$

We also have to show that $\gcd(e, m)\gcd(e, n) = e$ for any divisor e of mn. Write $c = \gcd(e, m)$ and $d = \gcd(e, n)$. Since c and d are relatively prime and since both are divisors of e, it follows that $cd \mid e$. Now, suppose that $kcd = e$. Since $\gcd(kcd, m) = c$ it

follows that $\gcd(k,m) = 1$. Similarly, $\gcd(k,n) = 1$. However, if p is any prime divisor of k, which divides mn, it follows that $p \mid m$ or $p \mid n$. Since this is impossible, it follows that $k = 1$. This completes the proof that the map $(c,d) \mapsto cd$ is a bijection.

Using this bijection, we find that

$$\begin{aligned} F(mn) = \sum_{e \mid mn} f(e) &= \sum_{c \mid m} \sum_{d \mid n} f(cd) \\ &= \sum_{c \mid m} \sum_{d \mid n} f(c)f(d) = \sum_{c \mid m} f(c) \sum_{d \mid n} f(d) = F(m)F(n). \end{aligned}$$ □

Theorem 14.3.5. *The functions τ and σ are multiplicative.*

Proof. The functions τ and σ are defined by

$$\tau(n) := \sum_{d \mid n} 1, \qquad \text{and} \qquad \sigma(n) := \sum_{d \mid n} d.$$

Clearly the constant function $n \mapsto 1$ and the identity function $n \mapsto n$ are multiplicative, so it follows from Theorem 14.3.4 that τ and σ are multiplicative. □

The previous theorem implies that if $n = p_1^{m_1} \cdots p_k^{m_k}$ is a product of distinct primes, then

$$\tau(n) = \prod_{i=1}^{k} (m_i + 1), \qquad \text{and} \qquad \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{m_1+1} - 1}{p_i - 1}.$$

Indeed, for any prime power p^m, the divisors of p^m are the prime powers p^i where $0 \le i \le m$. There are $m+1$ powers of p in this range, and their sum is computed by the formula for the geometric series

$$1 + p + \cdots + p^m = \frac{p^{m+1} - 1}{p - 1}.$$

Remark 14.3.6. Many identities of arithmetic functions involve reindexing double sums such as in the proof of Theorem 14.3.4. Another reindexing identity that is occasionally helpful is:

$$\sum_{c \mid n} \sum_{d \mid c} f(c,d) = \sum_{d \mid n} \sum_{e \mid \frac{n}{d}} f(de, d).$$

14.4 The Möbius Function

Definition 14.4.1. The **Möbius function** μ is defined by

$$\mu(n) := \begin{cases} (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes,} \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p. \end{cases}$$



For example, $\mu(3 \cdot 7 \cdot 17^3) = 0$ because the input is divisible by 17^2. On the other hand, $\mu(3 \cdot 7 \cdot 17) = (-1)^3 = -1$ because the input is the product of three distinct primes. The following table lists the values of $\mu(n)$ for the first 15 natural numbers

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(n)$	0	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1	1

It is immediate from the definition that the Möbius function is multiplicative. We will give two proofs of the following theorem: a combinatorial and an arithmetic proof.

THEOREM 14.4.2. *The Möbius function is multiplicative, and it satisfies*

$$\sum_{d \mid n} \mu(d) = \varepsilon(n).$$

In other words, $\mu * 1 = \varepsilon$.

COMBINATORIAL PROOF. It is clear that the formula holds for $n = 1$. For $n > 1$, we prove the formula by showing that there is a bijection

$$\{d \mid n \mid \mu(d) = 1\} \cong \{d \mid n \mid \mu(d) = -1\}$$

To describe such a bijection, let $p \mid n$ be a prime divisor of n, and define the map on a square-free divisor of n by

$$\theta_p(d) := \begin{cases} pd & \text{if } p \nmid d \\ \frac{d}{p} & \text{if } p \mid d. \end{cases}$$

In other words, θ_p is defined by "toggling" the prime p in a square-free divisor d of n. Note that $\theta_p(d)$ is again square-free, and that

$$\mu(\theta_p(d)) = -\mu(d).$$

Furthermore, the equality $\theta_p(\theta_p(d)) = d$ holds for every d, so we conclude that θ_p defines a bijection between the set of divisors d of n such that $\mu(d) = 1$ and the set of divisors d of n such that $\mu(d) = -1$. □

ARITHMETIC PROOF. Likewise, the arithmetic function

$$F(n) := \sum_{d \mid n} \mu(d)$$

is multiplicative by Theorem 14.3.4. Since multiplicative functions are completely determined by their values on prime powers, and ε is the multiplicative function given by

$$\varepsilon(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise,} \end{cases}$$

it suffices to show that $F(p^k) = 0$ for any $k \geq 1$. To see this, we simply evaluate

$$\sum_{d \mid p^k} \mu(p^k) = \mu(p^0) + \mu(p^1) + 0 = 1 - 1 = 0.$$ □

Remark 14.4.3. The previous theorem could be viewed as a recurrence relation that is satisfied by the Möbius function:

$$\mu(n) = -\sum_{\substack{d \mid n \\ d \neq n}} \mu(d)$$

Gian-Carlo Rota used this perspective to make the theory of arithmetic functions and the Möbius function applicable to a wide class of partially ordered sets [Rot1964].

14.5 Dirichlet Convolution

The set of arithmetic functions with values in a fixed number system such as the integers, the real numbers, or the complex numbers, possesses algebraic structure that can be used to obtain number-theoretic properties such as identities or divisibility results. The fundamental operation on arithmetic functions is *Dirichlet convolution*, a way of combining two arithmetic functions into a new one.

Definition 14.5.1. Consider two arithmetic functions f and g. We define their **Dirichlet convolution** $f * g$ by

$$(f * g)(n) := \sum_{d \mid n} f(d) g\left(\frac{n}{d}\right).$$

Example 14.5.2. Let 1 be the constant arithmetic function given by $1(n) = 1$. Then we have

$$(1 * f)(n) = \sum_{d \mid n} 1(d) f\left(\frac{n}{d}\right) = \sum_{d \mid n} f\left(\frac{n}{d}\right) = \sum_{d \mid n} f(d).$$

Recall that the arithmetic function F given by $F(n) = \sum_{d \mid n} f(d)$ is the subject of Theorem 14.3.4, where we have established that if f is multiplicative, then so is F. We also note that

$$(1 * 1)(n) = \sum_{d \mid n} 1 = \tau(n).$$

Thus, we have the identity of arithmetic functions $1 * 1 = \tau$.

Example 14.5.3. Define the arithmetic function d_k by

$$d_k(n) := \#\{(a_1, \ldots, a_k) \mid a_1 \cdots a_k = n\}.$$

That is, $d_k(n)$ is the number of ways of writing n as an ordered product of k positive integers. For example, we have $d_2(n) = \tau(n)$ since every divisor $d \mid n$ uniquely determines an ordered pair (d, e) such that $de = n$. Thus, it follows from Example 14.5.2 that $1 * 1 = d_2$.

Next, observe that we can define 1^{*k} by iteratively convolving with the arithmetic function 1. That is, 1^{*1} is defined to be the arithmetic function 1, and $1^{*(k+1)}$ is defined to be the arithmetic function $1 * 1^{*k}$. We claim that

$$1^{*k} = d_k.$$



The proof is by induction on $k \geq 1$. Note that $d_1(n)$ is the number of ways of writing n as a single number. There is of course exactly one such way, so we have $d_1(n) = 1$ for all n. That is, we have $d_1 = 1$.

We have already seen that $1 * 1 = d_2$. For the inductive step, assume that $1^{*k} = d_k$. Then we have

$$1^{*(k+1)}(n) = (1 * 1^{*k})(n) = \sum_{d|n} 1(d) \cdot d_k\left(\frac{n}{d}\right) = \sum_{d|n} \#\{(a_1, \dots, a_k) \mid a_1 \cdots a_k = \tfrac{n}{d}\}.$$

Note that the data of d along with $(a_1, \dots, a_k)$ such that $a_1 \cdots a_k = \frac{n}{d}$ is equivalent to the data of $(d, a_1, \dots, a_k)$ such that $da_1 \cdots a_k = n$. The number of such $(k+1)$-tuples is $d_{k+1}(n)$, which completes the inductive step.

Using Theorem 14.3.4 repeatedly along with the fact that 1 is a multiplicative function, we obtain as a consequence of the identity $1^{*k} = d_k$ that d_k is a multiplicative function for each k. It follows that the values of d_k are determined by the values $d_k(p^a)$ at the prime powers p^a. Since each divisor of p^a is itself a power of p, it follows that $d_k(p^a)$ is equal to the number of ways of writing a as an ordered sum with k terms:

$$m_1 + \cdots + m_k = a.$$

Thus, it follows by Theorem 3.7.2 that $d_k(p^a) = \binom{a+k-1}{a}$. For $n = p_1^{a_1} \cdots p_m^{a_m}$ we therefore conclude:

$$d_k(n) = \prod_{1 \leq i \leq m} \binom{a_i + k - 1}{a_i}.$$

In the previous example, one might wonder whether it matters whether we define $1^{*k} = 1 * (1 * (\cdots * 1))$ or $1^{*k} = ((1 * \cdots) * 1) * 1$. Indeed, this shouldn't make a difference, as we prove in the following theorem.

THEOREM 14.5.4. *Dirichlet convolution is associative and commutative, meaning that*

$$(f * g) * h = f * (g * h), \qquad \textit{and} \qquad f * g = g * f,$$

respectively.

PROOF. Another way of writing the Dirichlet convolution of f and g is

$$(f * g)(n) = \sum_{\substack{c,d \\ cd=n}} f(c)g(d).$$

Since this expression is symmetric in f and g, we see immediately that the Dirichlet convolution is commutative. Furthermore, to see that the Dirichlet convolution is

associative we make the following two calculations:

$$\begin{aligned}((f*g)*h)(n) &= \sum_{\substack{c,d\\cd=n}} (f*g)(c)h(d) & (f*(g*h))(n) &= \sum_{\substack{a,e\\ae=n}} f(a)(g*h)(e)\\ &= \sum_{\substack{c,d\\cd=n}} \sum_{\substack{a,b\\ab=c}} f(a)g(b)h(d) & &= \sum_{\substack{a,e\\ae=n}} \sum_{\substack{b,d\\bd=e}} f(a)g(b)h(d)\\ &= \sum_{\substack{a,b,d\\abd=n}} f(a)g(b)h(d), & &= \sum_{\substack{a,b,d\\abd=n}} f(a)g(b)h(d). \qquad \square\end{aligned}$$

Example 14.5.5. By associativity of Dirichlet convolution, it follows that $1^{*k} * 1^{*l} = 1^{*(k+l)}$. Since $1^{*k} = d_k$ for each k by Example 14.5.3, it follows that $d_k * d_l = d_{k+l}$.

Theorem 14.5.6. *Let ε be the function given by*

$$\varepsilon(n) := \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Then $\varepsilon * f = f$ and $f * \varepsilon = f$ for any arithmetic function f.

Proof. Consider an arithmetic function f. Then

$$(\varepsilon * f)(n) = \sum_{d|n} \varepsilon(d) f\left(\frac{n}{d}\right) = f(n),$$

since the only term contributing to the sum is $d = 1$. The fact that $f * \varepsilon = f$ follows by commutativity of the Dirichlet convolution. $\square$

14.6 Dirichlet Inverses

Definition 14.6.1. Consider an arithmetic function f such that $f(1)$ is nonzero. Then we define the **Dirichlet inverse** f^{-1} of f by

$$f^{-1}(1) := \frac{1}{f(1)} \qquad \text{and} \qquad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n\\d\neq n}} f^{-1}(d) f\left(\frac{n}{d}\right) \qquad (\text{for } n > 1).$$

Theorem 14.6.2. *For every arithmetic function f such that $f(1)$ is nonzero, the arithmetic function f^{-1} is the inverse of f with respect to Dirichlet involution, in the sense that*

$$f^{-1} * f = \varepsilon \qquad \text{and} \qquad f * f^{-1} = \varepsilon.$$

Furthermore, f^{-1} is the unique such arithmetic function.



PROOF. To show that $(f * f^{-1})(n) = \varepsilon(n)$ for every $n \geq 1$, there are two cases to consider. In the case where $n = 1$, we have

$$(f * f^{-1})(1) = f(1)f^{-1}(1) = f(1)\frac{1}{f(1)} = 1 = \varepsilon(1).$$

In the case where $n > 1$, we have

$$(f * f^{-1})(n) = \sum_{d|n} f(d)f^{-1}\left(\frac{n}{d}\right) = f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d \neq n}} f(d)f^{-1}\left(\frac{n}{d}\right),$$

which is 0 by the definition of f^{-1}. This completes the proof that $f * f^{-1} = \varepsilon$. The equality $f^{-1} * f = \varepsilon$ follows by commutativity of Dirichlet convolution.

Uniqueness of the inverse follows from a purely algebraic argument. Suppose that g is another arithmetic function such that $f * g = \varepsilon$. Then we obtain

$$f^{-1} = f^{-1} * \varepsilon = f^{-1} * (f * g) = (f^{-1} * f) * g = \varepsilon * g = g. \qquad \square$$

EXAMPLE 14.6.3. The Dirichlet inverse of the constant function 1 is the Möbius function μ. Indeed, we saw in Theorem 14.4.2 that $\mu * 1 = \varepsilon$.

REMARK 14.6.4. If $f^{-1} = g$ for some arithmetic functions f and g, then it follows that $g^{-1} = f$. Indeed, the equations

$$f * g = \varepsilon \qquad \text{and} \qquad g * f = \varepsilon$$

simultaneously imply that g is the inverse of f and f is the inverse of g. Thus, we have that $1^{-1} = \mu$ and $\mu^{-1} = 1$.

THEOREM 14.6.5 (The Möbius Inversion Formula). *Consider two arithmetic functions f and g. Then we have*

$$g(n) = \sum_{d|n} f(d) \quad \Leftrightarrow \quad f(n) = \sum_{d|n} \mu(d)g\left(\frac{n}{d}\right).$$

In other words, if $g = 1 * f$ then $f = \mu * g$.

PROOF. If $g = 1 * f$, then

$$\begin{aligned} \mu * g &= \mu * (1 * f) \\ &= (\mu * 1) * f \\ &= \varepsilon * f \\ &= f. \end{aligned}$$

Conversely, if $f = \mu * g$, then

$$\begin{aligned} 1 * f &= 1 * (\mu * g) \\ &= (1 * \mu) * g \\ &= \varepsilon * g \\ &= g. \end{aligned}$$

$\square$

Exercises

Starter Exercises

14.1 Show that every even perfect number is congruent to 6 or 8 modulo 10.

14.2 Show that every even perfect number other than 28 is congruent to ±1 modulo 7.

14.3 Show that the Mersenne numbers M_n satisfy the recurrence relation

$$M_{n+2} = 3M_{n+1} - 2M_n.$$

14.4 Compute $\phi(n)$ for $n = 1, \ldots, 12$.

14.5 Show that the number $\tau(n)$ of divisors of n is odd if and only if n is a square number.

14.6 Compute $\mu * \sigma$.

Routine-Building Exercises

14.7 Let $M_n := 2^n - 1$ be the nth Mersenne number.

(a) Show that if n is even, then $3 \mid M_n$.
(b) Show that if $3 \mid n$, then $7 \mid M_n$.

14.8 Show that any Mersenne prime $M_p = 2^p - 1$ with p an odd prime satisfies the congruence

$$M_p \equiv 7 \pmod{24}.$$

14.9 Suppose that p is an odd prime, and that q is a prime divisor of the Mersenne number $M_p = 2^p - 1$. Show that

$$q \equiv 1 \pmod{2p}.$$

Conclude that $\gcd(k, M_p) = 1$ for all $1 \leq k \leq 2p$. Also use this congruence to give yet another proof of the infinitude of primes. Hint: Apply Theorem 8.5.2 (Order Theorem).

14.10 Prove the following identity, first found by Joseph Liouville [Lio1857]:

$$\sum_{d \mid n} \tau(d)^3 = \left(\sum_{d \mid n} \tau(d) \right)^2.$$

14.11 (a) Show that

$$\sigma(p^m) \mid \sigma(p^n) \quad \Leftrightarrow \quad m+1 \mid n+1.$$

(b) Let $d := \gcd(m+1, n+1)$. Show that

$$\gcd(\sigma(p^m), \sigma(p^n)) = \sigma(p^{d-1}).$$



14.12 (a) Prove that if $\gcd(a,b) = d$, then

$$\phi(ab) = \frac{d\phi(a)\phi(b)}{\phi(d)}.$$

(b) For any $n > 1$, prove that

$$\sum_{\substack{a<n \\ \gcd(a,n)=1}} a = \frac{n\phi(n)}{2}.$$

14.13 Prove that there is no positive integer $n < 2^{65}$ such that $\phi(n) = 2^{64}$.

14.14 For any $d \mid \phi(n)$ such that $d > 2$, prove that

$$\prod_{\substack{0<x<n \\ \mathrm{ord}_n(x)=d}} x \equiv 1 \pmod{n}.$$

14.15 (a) Show that

$$\frac{\phi(n)}{2} \equiv 1 \pmod{2}$$

if and only if

$$n = 4, \qquad \text{or} \qquad n = p^k, \qquad \text{or} \qquad n = 2p^k,$$

where $p \equiv 3 \pmod{4}$ is a prime.

(b) Show that

$$\frac{\phi(n)}{2} \equiv 1 \pmod{4}$$

if and only if

$$n = 4, \qquad \text{or} \qquad n = p^k, \qquad \text{or} \qquad n = 2p^k,$$

where either $p \equiv 3 \pmod{8}$ and k is odd or $p \equiv 7 \pmod{8}$ and k is even.

14.16 Compute $\mu * \mu$.

14.17 (a) Show that if two out of three arithmetic functions f, g, and $f * g$ are multiplicative, then so is the third.

(b) Show that if f is an arithmetic function such that $f(1)$ is nonzero, then f is multiplicative if and only if f^{-1} is multiplicative.

14.18 Let f be a multiplicative function.

(a) Show that

$$f^{-1}(n) = \mu(n)f(n)$$

for every square-free natural number n.

(b) Show that

$$f^{-1}(p) = -f(p) \qquad \text{and} \qquad f^{-1}(p^2) = f(p^2) - f(p)^2$$

for every prime number p.

(c) Show that

$$f^{-1}(p^m) = \sum_{k=1}^{m} (-1)^k \left(\sum_{\substack{i_1+\cdots+i_k=m \\ i_1,\ldots,i_k \geq 1}} f(p^{i_1}) \cdots f(p^{i_k}) \right).$$

14.19 Consider a prime p. Show that

$$\sum_{\substack{0<n<p-1 \\ \gcd(n,p-1)=1}} a^n \equiv \mu(\operatorname{ord}_p(a)) \frac{\phi(p-1)}{\phi(\operatorname{ord}_p(a))} \pmod{p}.$$

14.20 Write $R_n(k)$ for the number of integers $0 \leq x < n$ such that

$$x^k \equiv 1 \pmod{n}.$$

(a) Show that the function $n \mapsto R_n(k)$ is multiplicative, for each $k > 0$.
(b) Show that the number of integers $0 \leq x < n$ of order k is given by the quantity

$$A_n(k) := \sum_{d \mid k} \mu\left(\frac{k}{d}\right) R_n(k).$$

14.21 Consider a natural number of the form $n = 2^k p$, where p is an odd prime. Show that the following are equivalent:

(i) n is perfect,
(ii) $2n \mid \binom{2n}{n}$.

Hint: Use Theorem 13.4.8 (Kummer's Theorem). The forward direction was discovered by Hoon Balakram [Bal1929].

Challenge Exercises

14.22 Determine the number of reduced fractions $\frac{a}{b}$, where $0 \leq a \leq b \leq n$.

14.23 Consider the nth Fermat number $F_n = 2^{2^n} + 1$ and the mth Mersenne number $M_m = 2^m - 1$. Show that

$$\gcd(F_n, M_m) = \begin{cases} F_n & \text{if } 2^{n+1} \mid m, \\ 1 & \text{otherwise.} \end{cases}$$

14.24 For any two natural numbers $0 \leq d \leq n$, determine the number of ordered pairs (a, b) of nonnegative integers a and b such that $a + b = n$ and $\gcd(a, b) = d$.

14.25 For how many congruence classes $b \pmod{n}$ is the linear congruence

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

solvable?

14.26 (a) Find all primes p and exponents m such that

$$v_2\left(\frac{p^{m+1}-1}{p-1}\right) = 0.$$

(b) Find all primes p and exponents m such that

$$v_2\left(\frac{p^{m+1}-1}{p-1}\right) = 1.$$

(c) (Euler) Show that if n is an odd perfect number, then n is of the form

$$p^\alpha m^2$$

where p is a prime such that $p \equiv \alpha \equiv 1 \pmod 4$ and $p \nmid m$.

14.27 Show that

$$\sigma(2^n - 1) = \prod_{\substack{p \text{ odd prime} \\ d := \operatorname{ord}_p(2) \mid n}} \frac{p^{v_p(2^d-1)+v_p(n/d)+1} - 1}{p-1}.$$

14.28 Let Ω be the arithmetic function given by

$$\Omega(m) = m_1 + \cdots + m_n$$

for any $m = p_1^{m_1} \cdots p_n^{m_n}$, where the prime factors $p_1, \ldots, p_n$ are assumed to be distinct. Thus, Ω returns the number of prime factors, counted with multiplicity. Show that

$$\Omega(m) \leq \frac{\log m}{\log\left(\frac{1}{n}\sum_{i=1}^n p_i\right)}.$$

Hint: Use Jensen's inequality.

Chapter 15

Cyclic Counting

15.1 Hemachandra Wheels

In §2.6 we considered the problem of counting the number H_n of ways we can subdivide a strip of n blocks into squares and dominoes. An equivalent formulation of this problem was stated Exercise 2.4, where the task was to find a recursive expression for the number of ways in which we could color some squares along a strip of length n blue, so that no two blue squares are adjacent; this number is H_{n+1}. How do these counts change, if instead we ask for the number of Hemachandra colorings of a cyclic strip? And how do we determine the number of those Hemachandra colorings that are rotationally distinct?

Definition 15.1.1. A **Hemachandra wheel** of order n is an n-element cyclic set in which the elements are colored white and blue, so that no two adjacent elements are both colored blue. Two Hemachandra wheels are considered to be the same when one can be obtained from the other by rotation. Elements of Hemachandra wheels will be called **segments**.

A Hemachandra wheel is said to be **labeled** if its n segments are labeled 0 through $n-1$ in cyclic ordering. Two labeled Hemachandra wheels of order n are considered to be the same if segments with matching labels have the same color.

We write W_n for the number of labeled Hemachandra wheels of order n, and we write $\tilde{W}_n$ for the number of (unlabeled) Hemachandra wheels of order n.

Remark 15.1.2. The number W_n of labeled Hemachandra wheels can be determined by considering two cases: Either the element labeled 0 is white or it is blue. In the first case, the remaining elements of the Hemachandra wheel form a strip of elements labeled 1



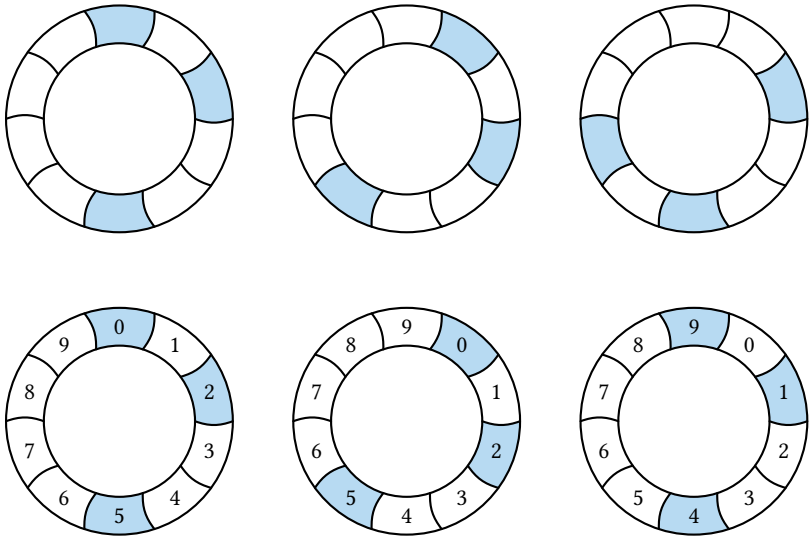


Figure 15.1: The top row displays three unlabeled Hemachandra wheels. The first and second are the same up to rotation, while the third is distinct from the other two. The bottom row displays three labeled Hemachandra wheels. The first two are the same, since their colorings match the labeling. The third is distinct from the first two since it is the only wheel among the three with a blue segment labeled 9.

through $n-1$, and the number of colorings of this strip is the Fibonacci number F_{n+1}. In the second case, the blue element labeled 0 cannot have an adjacent blue element, so the coloring of the remaining strip is determined by the coloring of the elements 2 through $n-2$. Their number is F_{n-1}. Therefore, we conclude that

$$W_n = F_{n+1} + F_{n-1}.$$

Since $F_{n+1} + F_{n-1}$ is the nth Lucas number L_n, we find that $W_n = L_n$.

THEOREM 15.1.3. *The number $\tilde{W}_p$ of unlabeled Hemachandra wheels of prime order p is*

$$\tilde{W}_p = \frac{1}{p}(F_{p+1} + F_{p-1} + p - 1),$$

where F_i denotes the ith Fibonacci number.

PROOF. All labelings of the entirely white Hemachandra wheel are the same, so it corresponds to exactly one labeled wheel. Every wheel with at least one blue segment has p distinct labelings. Indeed, if this were not so then its coloring would be preserved by a rotation through k positions for some $0 < k < p$. Since p is prime, the positions $0, k, 2k, \ldots, (p-1)k$ exhaust the wheel. Every position would therefore have the same color, a contradiction. Consequently, we have

$$W_p = 1 + p(\tilde{W}_p - 1),$$

and the result follows. □

Corollary 15.1.4. *For any prime number p we have the congruence*

$$F_{p-1} + F_{p+1} \equiv 1 \pmod{p}.$$

Proof. The number $\tilde{W}_p$ is an integer, so $p \mid F_{p+1} + F_{p-1} - 1$. □

In many cases, our main method to prove congruences is by algebraic manipulation. In the previous theorem we found a new source of congruences: *rotational symmetry!* In the present chapter we will refine this method and find many congruences that can be proven naturally with rotational symmetry.

15.2 The Prime–Fixed Point Congruence

Definition 15.2.1. We define the set of **fixed points** of a map $f : X \to X$ by

$$\mathrm{Fix}(f) := \{x \in X \mid f(x) = x\}.$$

Theorem 15.2.2 (The Prime–Fixed Point Congruence). *Consider a finite set X and a map $f : X \to X$ such that $f^p(x) = x$ for all $x \in X$, where p is a prime number. Then we have*

$$\#X \equiv \#\mathrm{Fix}(f) \pmod{p}.$$

In particular, if $\#X \not\equiv 0 \pmod{p}$, then f has a fixed point.

Proof. If $f(x) \neq x$, then the least positive n for which $f^n(x) = x$ is p. Indeed, by the assumption that p is prime, if $1 < n < p$ then there is an integer k such that $kn \equiv 1 \pmod{p}$. For such k we find that $f(x) = f^{kn}(x) = x$, contradicting our assumption on x. Thus we see that X is partitioned into orbits of size 1 and of size p, and the claim follows. □

Example 15.2.3. The congruence of Corollary 15.1.4 is an instance of Theorem 15.2.2 (The Prime–Fixed Point Congruence), since the total number of Hemachandra wheels of order p is

$$F_{p-1} + F_{p+1},$$

and the only fixed point under rotation is the entirely white Hemachandra wheel.

Example 15.2.4. Consider a set A with a elements, and a cyclic set C with p elements, where p is a prime number. Then there are a^p functions from C to A, which we view as A-colorings of the elements of C. The fixed points under rotation are precisely the colorings defined by a constant function $C \to A$. The number of such constant functions is a. Therefore we obtain from Theorem 15.2.2 (The Prime–Fixed Point Congruence) the congruence

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

That is, we have proven *Fermat's Little Theorem*. This theorem is of such great consequence in the theory of numbers, that we will devote the entire next chapter to it and its consequences. The proof given here was found by Solomon Golomb [Gol1956].



15.3 Lucas's Theorem

Our next application of Theorem 15.2.2 is a theorem due to Édouard Lucas [LUC1878b], which allows us to compute the residue class of binomial coefficients modulo a prime. This theorem is complementary to Theorem 13.4.8 (Kummer's Theorem), which gives a complete description of the prime factorization of binomial coefficients. The proof we present below is due to Bruce Sagan [SAG2020, Theorem 6.5.6].

THEOREM 15.3.1 (Lucas's Theorem). *Consider a prime number p, and natural numbers m and n written in base p as*

$$m = \sum_{i=0}^{k} a_i p^i \qquad \text{and} \qquad n = \sum_{i=0}^{k} b_i p^i.$$

Then the congruence

$$\binom{n}{m} \equiv \prod_{i=0}^{k} \binom{b_i}{a_i} \pmod{p}$$

holds. In particular, if $b_i < a_i$ for some i, then $\binom{n}{m}$ is divisible by p.

PROOF. By Euclidean division, write $m = m'p + a_0$ and $n = n'p + b_0$, so that

$$m' = \sum_{i=0}^{k-1} a_{i+1} p^i \qquad \text{and} \qquad n' = \sum_{i=0}^{k-1} b_{i+1} p^i$$

It suffices to show that

$$\binom{n}{m} \equiv \binom{n'}{m'}\binom{b_0}{a_0} \pmod{p},$$

since the claim follows by iterating this congruence. Consider an n-element set X and a map $f : X \to X$ so that the number of p-cycles is n' and the number of fixed points is b_0. Then we can define a map φ on the set of m-element subsets of X by

$$\varphi(U) := \{f(x) \mid x \in U\}.$$

The image of an m-element subset U under f is indeed again an m-element subset. Furthermore, since f satisfies $f^p(x) = x$ for all $x \in X$, it also follows that $\varphi^p(U) = U$ for every m-element subset of X. Therefore it follows by Theorem 15.2.2 that

$$\binom{n}{m} \equiv \#\mathrm{Fix}(\varphi) \pmod{p}.$$

Now observe that $\varphi(U) = U$ if and only if for every $x \in U$ we have $f(x) \in U$. This means that for every $x \in U$, the entire orbit under f is contained in U. As we have seen in Theorem 15.2.2, these orbits have either p elements or 1 element. Since the number of fixed points of f is $0 \leq b_0 < p$, it follows that every m-element subset contains

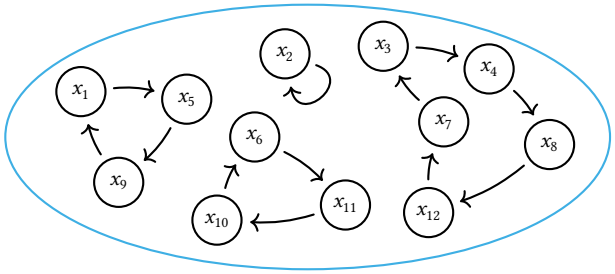


Figure 15.2: A bijection on a 12-element set.

of a number t of orbits with p elements, and a number $0 \leq c < p$ of fixed points, which allows us to write $m = tp + c$. By the uniqueness property of Theorem 5.3.1 (The Euclidean Division Theorem), it follows that $t = m'$ and $c = a_0$. We conclude that a fixed point U of φ consists of a choice of m' orbits with p elements and a choice of a_0 fixed points of f, so that

$$\#\mathrm{Fix}(\varphi) = \binom{n'}{m'}\binom{b_0}{a_0}. \qquad \square$$

15.4 The Orbit–Counting Formula

Recall from Exercise 8.14 that if the orbit of x under a bijection $f : X \to X$ contains exactly t elements, then

$$f^k(x) = x \quad \Leftrightarrow \quad t \mid k. \tag{$*$}$$

That is, x is a *fixed point* of the map $f^k : X \to X$ if and only if k is a multiple of the number of elements in the orbit of x.

Example 15.4.1. Consider the bijection f displayed in Figure 15.2. Since x_1 is in a 3-element orbit, it follows that x_1 is a fixed point for f^k if and only if k is a multiple of 3. Likewise, x_3 is in a 5-element orbit so it is a fixed point for f^k if and only if k is a multiple of 5. The element x_2 is a fixed point of f, so it is a fixed point of f^k for every $k \geq 0$.

The bijection displayed in Figure 15.2 satisfies $f^{15}(x) = x$ for all $x \in X$, since the length of every orbit is a divisor of 15. Running through all $0 \leq k < 15$, we see that the orbit of length 1 contributes a fixed point for every k; each orbit of length 3 contributes 3 fixed points every third k; and the orbit of length 5 contributes 5 fixed points every fifth k. Indeed, listing out the number of fixed points for f^k we get the following table

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\#\mathrm{Fix}(f^k)$	12	1	1	7	1	6	7	1	1	7	6	1	7	1	1

Adding up all these totals gives us $60 = 4 \cdot 15$. We therefore see that the average number of fixed points of f^k over $0 \leq k < 15$ is exactly the number of orbits. We note also

that $\#\mathrm{Fix}(f^k) = 1$ precisely when $\gcd(k, 15) = 1$; that $\#\mathrm{Fix}(f^k) = 7$ precisely when $\gcd(k, 15) = 3$; and that $\#\mathrm{Fix}(f^k) = 6$ precisely when $\gcd(k, 15) = 5$. Since for any $k \mid l$ we have $\gcd(l, n) = k$ if and only if $\gcd(l/k, n/k) = 1$, the number of which are determined by Euler's totient function ϕ, these observations suggest that

$$\frac{1}{15} \sum_{k \mid 15} \phi(15/k)\, \#\mathrm{Fix}(f^k) = 4.$$

That is, the average number of fixed points of f^k, being equal to the number of orbits, can be organized as a divisor-sum. We establish this relation between orbits and fixed points in the following theorem.

THEOREM 15.4.2 (The Orbit–Counting Formula). *Consider a bijection $f : X \to X$ on a finite set X, and suppose that $f^n(x) = x$ for all $x \in X$, where n is a positive integer. Let N be the number of orbits of f. Then we have*

$$N = \frac{1}{n} \sum_{k \mid n} \phi(n/k)\, \#\mathrm{Fix}(f^k).$$

PROOF. For each divisor $k \mid n$ and each $1 \leq l \leq n$ such that $\gcd(l, n) = k$, we have $\#\mathrm{Fix}(f^l) = \#\mathrm{Fix}(f^k)$. To see this, consider an element x in an orbit of length t. Since t is a divisor of n, it follows that $t \mid l$ if and only if $t \mid k$, which implies the claim. The number of integers $1 \leq l \leq n$ such that $\gcd(l, n) = k$ is $\phi(n/k)$, so we obtain that

$$\frac{1}{n} \sum_{k \mid n} \phi(n/k)\, \#\mathrm{Fix}(f^k) = \frac{1}{n} \sum_{k=1}^{n} \#\mathrm{Fix}(f^k) = \frac{1}{n} \sum_{k=0}^{n-1} \#\mathrm{Fix}(f^k).$$

Now label the orbits of f with indices 1 through N, and let f_i be the restriction of f to the ith orbit. Then it follows that

$$\#\mathrm{Fix}(f^k) = \sum_{i=1}^{N} \#\mathrm{Fix}(f_i^k).$$

Consequently, we have

$$\sum_{k=0}^{n-1} \#\mathrm{Fix}(f^k) = \sum_{k=0}^{n-1} \sum_{i=1}^{N} \#\mathrm{Fix}(f_i^k) = \sum_{i=1}^{N} \sum_{k=0}^{n-1} \#\mathrm{Fix}(f_i^k).$$

Therefore it suffices to prove that

$$\frac{1}{n} \sum_{k=0}^{n-1} \#\mathrm{Fix}(f_i^k) = 1$$

for all $1 \leq i \leq N$.

For each $1 \leq i \leq N$, write t_i for the number of elements in the ith orbit. By the logical equivalence Equation (*), which was shown in Exercise 8.14, it follows that

$$\#\mathrm{Fix}(f_i^k) = \begin{cases} t_i & \text{if } t_i \mid k, \\ 0 & \text{otherwise.} \end{cases}$$

Since the number of multiples of t_i among the integers 0 through $n-1$ is n/t_i, we conclude that

$$\sum_{k=0}^{n-1} \#\mathrm{Fix}(f_i^k) = \frac{n}{t_i} t_i = n,$$

and the claim follows. □

Remark 15.4.3. Theorem 15.4.2 (The Orbit–Counting Formula) is a special case of a more general theorem of group theory, called *Burnside's Lemma*.

Example 15.4.4. Let B be a cyclic set consisting of n beads, with one-step rotation $r : B \to B$, and let C be a set of c colors. Then a C-coloring of B is a function $B \to C$, and we obtain a bijection f on the C-colorings of B by the rotation on B. Two C-colorings are considered the same if one can be obtained from the other by rotation; that is, if they are in the same orbit under f.

For each $k \mid n$, the colorings fixed under the k-step rotation f^k are precisely the colorings that are constant on the orbits of r^k on B, of which there are k. Therefore we have

$$\#\mathrm{Fix}(f^k) = c^k.$$

Now it follows by Theorem 15.4.2 (The Orbit–Counting Formula) that the number of rotationally distinct ways to color the cyclic set B is

$$\frac{1}{n} \sum_{k \mid n} \phi(n/k) \cdot c^k.$$

For example, the number of 3-colored necklaces with 10 beads is

$$\frac{1}{10}(\phi(10) \cdot 3^1 + \phi(5) \cdot 3^2 + \phi(2) \cdot 3^5 + \phi(1) \cdot 3^{10}) = 5934.$$

15.5 The Divisor Sum of the Totient Function

The orbit–counting theorem implies an important identity, which is sometimes known as **Gauss's theorem**.

Theorem 15.5.1. *Euler's totient function ϕ satisfies the following divisor-sum identity:*

$$\sum_{k \mid n} \phi(k) = n.$$



PROOF VIA THE ORBIT–COUNTING THEOREM. Consider the singleton set $X = \{\star\}$ and let $f : X \to X$ be the identity function. Then f has one orbit. Furthermore, $\#\mathrm{Fix}(f^k) = 1$ for every k, so we obtain by Theorem 15.4.2

$$1 = \frac{1}{n} \sum_{k|n} \phi(k). \qquad \square$$

Of an identity so fair as the one obtained in Theorem 15.5.1 it is only appropriate to admire and treasure it. What better way is there to savor a theorem than to prove it again, to established it on its own, and then yet again?

COMBINATORIAL PROOF. The sum suggests that there is a way of partitioning the set $\{1, \dots, n\}$ into sets A_d of size $\phi(d)$, and this is indeed how this theorem is proven. For each positive divisor d of n, define the map

$$f_k : \{1 \leq x \leq k \mid \gcd(x, k) = 1\} \to \{1, \dots, n\}$$

by $x \mapsto \frac{n}{k} x$, and define the set A_k to be the image of f_k. Since $\frac{n}{k}$ is a positive integer, it follows that the map f_k is injective, and therefore each set A_k has exactly $\phi(k)$ elements. Now notice that

$$y \in A_k \quad \Leftrightarrow \quad \gcd(y, n) = \frac{n}{k},$$

since if $x = y/\gcd(y, n)$, then $\gcd(x, k) = \gcd(y/\gcd(y, n), n/\gcd(y, n)) = 1$. Therefore, it follows that for every $1 \leq y \leq n$ there is exactly one $k \mid n$ such that $y \in A_k$, so it follows that the sets A_k partition the set $\{1, \dots, n\}$. The sum of the numbers of elements of each A_k is therefore n. $\square$

ARITHMETIC PROOF. Recall from Theorem 14.2.4 that ϕ is a multiplicative function, which implies by Theorem 14.3.4 that the function

$$n \mapsto \sum_{k|n} \phi(k)$$

is multiplicative. Since multiplicative functions are completely determined by their values on prime powers, it suffices to show that

$$\sum_{k|p^m} \phi(k) = p^m.$$

The only divisors of p^m are p^k for $0 \leq k \leq m$, and for any $k \geq 1$ we have $\phi(p^k) = p^k - p^{k-1}$. Thus, it follows that

$$\sum_{k|p^m} \phi(k) = \sum_{k=0}^{m} \phi(p^k) = 1 + \sum_{k=1}^{m} p^k - p^{k-1} = 1 + (p^m - 1) = p^m. \qquad \square$$

In terms of Dirichlet convolution, the identity in Theorem 15.5.1 can be stated as follows:

$$\phi * 1 = \mathrm{id}.$$

Corollary 15.5.2. *Euler's totient function satisfies the identity*

$$\phi(n) = \sum_{k|n} \mu(k)\frac{n}{k}$$

In other words, $\phi = \mu * \mathrm{id}$.

Proof. By Theorem 15.5.1 we have $\mathrm{id} = 1 * \phi$, so we have $\phi = \mu * \mathrm{id}$ by the Möbius inversion formula. □

We also give a direct proof of Corollary 15.5.2.

Direct proof of Corollary 15.5.2. Note that Euler's totient function ϕ can be written in the form

$$\phi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{\gcd(k,n)} \right\rfloor.$$

Then it follows from Theorem 14.4.2 that

$$\phi(n) = \sum_{k=1}^{n} \sum_{d\,|\,\gcd(k,n)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d) = \sum_{d|n} \sum_{\substack{k=1 \\ d|k}}^{n} \mu(d) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

The last step follows, since there are exactly $\frac{n}{d}$ multiples of d among the numbers from 1 to n. □

15.6 Arithmetic Functions of Orbits and Fixed Points

The formula

$$\frac{1}{n}\sum_{k|n} \phi(n/k)\,\#\mathrm{Fix}(f^k)$$

for the number of orbits of a bijection $f : X \to X$ satisfying $f^n(x) = x$ for all x suggests that we can treat of orbits and fixed points in terms of arithmetic functions and their Dirichlet convolution.

Definition 15.6.1. Consider a map $f : X \to X$ on a finite set X. We write

$$\nu_f(n) := \#\mathrm{Fix}(f^n) \qquad \text{and} \qquad \gamma_f(n) := \#\{f\text{-orbits of length } n\}.$$

Since x is a fixed point for f^n if and only if the length of the orbit of x divides n, we obtain the formula

$$\nu_f(n) = \sum_{k|n} k\,\gamma_f(k). \tag{15.1}$$



We will write $f \cdot g$ for the *pointwise multiplication* of f and g and we will write f/g for the *pointwise division* of f by g; that is,

$$(f \cdot g)(n) = f(n)g(n) \qquad \text{and} \qquad (f/g)(n) = f(n)/g(n).$$

Using these conventions, we see that the arithmetic functions ν_f and γ_f are related to each other by the following identities.

PROPOSITION 15.6.2. *Consider a bijection $f : X \to X$ on a finite set X. Then*

$$\nu_f = 1 * (\mathrm{id} \cdot \gamma_f) \qquad \textit{and} \qquad \gamma_f = \frac{\mu * \nu_f}{\mathrm{id}}.$$

The following corollary generalizes the Theorem 15.2.2 (The Prime–Fixed Point Congruence).

COROLLARY 15.6.3 (The Gauss congruence). *For any bijection $f : X \to X$ on a finite set X, we have*

$$\sum_{d|n} \mu(d)\nu_f(n/d) \equiv 0 \pmod{n}.$$

In particular, we have

$$\nu_f(p^m) \equiv \nu_f(p^{m-1}) \pmod{p^m}.$$

PROOF. Since the quantity

$$\gamma_f(n) = \frac{1}{n} \sum_{d|n} \mu(d)\nu_f(n/d)$$

is the integer, determining the number of f-orbits of length n, it follows that the sum is an integer divisible by n. □

Defining

$$\omega_f := (\nu_f * \phi)/\mathrm{id},$$

Theorem 15.4.2 asserts that $\omega_f(n)$ is the number of orbits of f if $f^n(x) = x$ for all $x \in X$.

THEOREM 15.6.4. *Consider a bijection f on a finite set X. Then*

$$\omega_f = 1 * \gamma_f.$$

Consequently, the quantity

$$\frac{1}{n} \sum_{k|n} \phi(n/k)\, \#\mathrm{Fix}(f^k) = \sum_{k|n} \gamma_f(k)$$

is an integer for every n, and counts the number of orbits whose length divides n.

Proof. Since $\nu_f = (\mathrm{id} \cdot \gamma_f) * 1$, it follows that

$$\nu_f * \phi = \nu_f * \mu * \mathrm{id} = (\mathrm{id} \cdot \gamma_f) * \mathrm{id} = \mathrm{id} \cdot (\gamma_f * 1). \qquad \square$$

Example 15.6.5. Consider an n-element cyclic set C with one-step rotation r. For each $k \mid n$, the k-step rotation r^k by partitions C into k orbits of size n/k. An m-element subset of C is then fixed under r^k precisely when it is a union of r^k-orbits. More conveniently, an m-element subset of C is fixed under $r^{n/k}$ precisely when it is a union of $r^{n/k}$-orbits, of which there are k. Therefore, it follows that

$$\nu_f(n/k) = \begin{cases} \binom{n/k}{m/k} & \text{if } k \mid m, \\ 0 & \text{otherwise.} \end{cases}$$

This implies that

$$\gamma_r(n) = \frac{1}{n} \sum_{k \mid \gcd(m,n)} \mu(k) \binom{n/k}{m/k}.$$

Gauss's congruence in this case asserts that

$$\sum_{k \mid \gcd(m,n)} \mu(k) \binom{n/k}{m/k} \equiv 0 \pmod{n}.$$

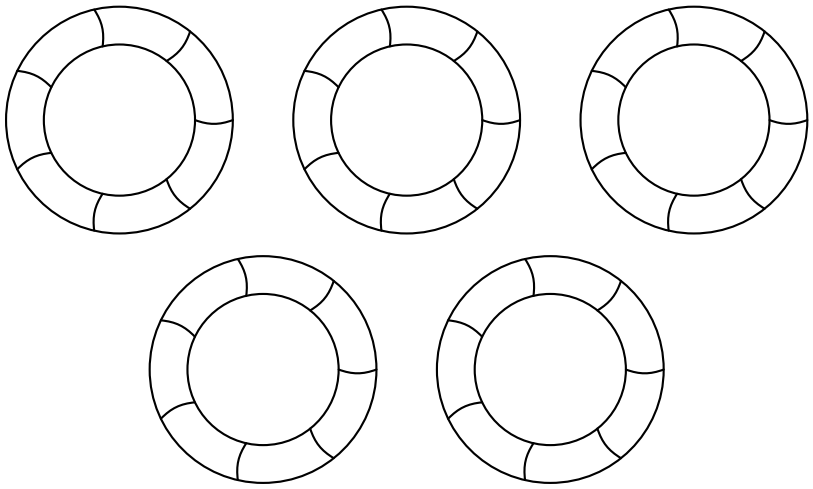


Figure 15.3: Shade the segments of these wheels so as to find all Hemachandra wheels of order 7.

Exercises

Starter Exercises

15.1 Find all the distinct unlabeled Hemachandra wheels of order 7.

Routine-Building Exercises

15.2 Let $n = mp^k$, where p is a prime such that $p \nmid m$, and let F be the sequence of Fibonacci numbers. Prove the **Gauss congruence** for Lucas numbers

$$F_{n-1} + F_{n+1} \equiv F_{n/p-1} + F_{n/p+1} \pmod{p^k}.$$

15.3 Consider a prime p. Show that

$$\binom{n}{m} \equiv \binom{n-p}{m-p} + \binom{n-p}{m} \pmod{p}.$$

15.4 Determine the number of labeled and unlabeled bicolored wheels with n segments in which no three adjacent segments all have the same color.

15.5 Prove that

$$\sum_{k=1}^{n} \gcd(k,n)\mu(\gcd(k,n)) = \mu(n).$$

Challenge Exercises

15.6 Define **Jordan's totient function** $J_k(n)$ by

$$J_k(n) = \#\{(x_1, \dots, x_k) \mid 1 \le x_1, \dots, x_k \le n \text{ and } \gcd(x_1, \dots, x_k, n) = 1\}.$$

In other words, Jordan's totient function counts the number of k-tuples $(x_1, \dots, x_k)$ of positive integers not exceeding n such that if d simultaneously divides all the integers $x_1, \dots, x_k$ and n, then $d = 1$. Note that $J_1(n)$ is just Euler's totient function ϕ.

(a) Find $J_2(n)$ for $1 \le n \le 12$.

(b) Show that for any divisor d of n, the number of elements in the set

$$\left\{(x_1, \dots, x_k) \,\middle|\, 1 \le x_1, \dots, x_k \le n \text{ and } \gcd(x_1, \dots, x_k, n) = \frac{n}{d}\right\}$$

is exactly $J_k(d)$.

(c) Show that

$$\sum_{d \mid n} J_k(d) = n^k \qquad \text{and} \qquad \sum_{d \mid n} \mu(d) \left(\frac{n}{d}\right)^k = J_k(n).$$

(d) Show that J_k is a multiplicative function.

(e) Show that

$$J_k(p^m) = p^{km} - p^{k(m-1)}$$

for any prime p and any exponent $m \ge 1$.

(f) Show that

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

Chapter 16

Fermat's Little Theorem and its Consequences

16.1 Fermat's Little Theorem

Theorem 16.1.1 (Fermat's Little Theorem). *Consider a prime number p and an integer a. Then the congruence*

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

holds.

Remark 16.1.2. Note that the congruence $(-a)^p \equiv -a^p \pmod{p}$ holds for all primes p, so it suffices to prove the claim for the nonnegative integers.

We already saw a proof of Fermat's Little Theorem in Example 15.2.4. The following proof, which proceeds by mathematical induction and makes use of the Theorem 3.5.1 (The Binomial Theorem), was first published by Leonhard Euler. Euler, however, was not the first to discover it [Dic1919, p. 59]. Several decades prior, this proof was discovered by Gottfried Wilhelm Leibniz, which was only published posthumously in [Lei1863].

The additive proof. This proof is by induction on a. The base case $0^p \equiv 0 \pmod{p}$ clearly holds. For the inductive step, assume that $a^p \equiv a \pmod{p}$. Theorem 3.5.1 (The Binomial Theorem) then gives us that

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k$$

However, note that $p \mid \binom{p}{k}$ for any $0 < k < p$. We therefore find that

$$(a+1)^p \equiv a^p + 1 \pmod{p}.$$

Since $a^p \equiv a \pmod{p}$ holds by the induction hypothesis, the claim follows. □

COROLLARY 16.1.3. *Consider a prime number p and an integer a not divisible by p. Then the congruence*

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

holds.

PROOF. Since a is not divisible by p, it follows that a is relatively prime to p, and therefore the claim follows from the cancellation law

$$ax \equiv ay \pmod{p} \quad \Rightarrow \quad x \equiv y \pmod{p}.$$ □

Fermat's Little Theorem can be used to analyze the prime divisors of special numbers such as Fermat numbers or Mersenne numbers. Regarding Fermat numbers, we have the following theorem, which is of great help when trying to prove or disprove that a Fermat number is prime.

THEOREM 16.1.4. *If p is a prime divisor of a Fermat number $F_n := 2^{2^n} + 1$, then*

$$p \equiv 1 \pmod{2^{n+1}}.$$

PROOF. If p is a prime divisor of $2^{2^n} + 1$, then it follows that

$$2^{2^n} \equiv -1 \pmod{p}.$$

This implies via Theorem 8.5.2 (Order Theorem) that $\operatorname{ord}_p(2) \mid 2^{n+1}$. In particular, $\operatorname{ord}_p(2) = 2^k$ for some number $k \leq n+1$. However, note that

$$2^{2^k} \equiv 1 \pmod{p} \qquad \text{implies} \qquad 2^{2^{k+1}} = (2^{2^k})^2 \equiv 1 \pmod{p}.$$

Since $2^{2^n} \equiv -1 \pmod{p}$, it follows that the order of 2 modulo p cannot divide 2^n. Thus, it follows that $\operatorname{ord}_p(2) = 2^{n+1}$. By Theorem 16.1.1 (Fermat's Little Theorem), we conclude that

$$2^{n+1} \mid p - 1.$$ □

COROLLARY 16.1.5. *The fourth Fermat number $2^{2^4} + 1 = 65537$ is prime.*

PROOF. Any prime divisor of $F_4 = 2^{2^4} + 1$ must satisfy the congruence $p \equiv 1 \pmod{33}$. If F_4 is composite, then it must have a prime divisor below $\sqrt{F_4}$, and thus below $2^8 = 256$. The sieve of Eratosthenes displayed in Figure 13.1 reveals that the only two primes $p \equiv 1 \pmod{33}$ below 256 are 97 and 193. A quick computation gives that

$$F_4 \equiv 62 \pmod{97} \qquad \text{and} \qquad F_4 \equiv 110 \pmod{193},$$

so that neither 97 nor 193 is a prime divisor of F_4, and therefore we conclude that F_4 is prime. □

Corollary 16.1.6. *The fifth Fermat number* $2^{2^5}+1 = 4,294,967,297$ *is composite, and its smallest prime factor is* 641.

Proof. By Theorem 16.1.4 it follows that any prime divisor of $2^{2^5}+1$ must satisfy

$$p \equiv 1 \pmod{2^6}.$$

The prime numbers of the form $64k+1$ below one thousand are 193, 257, 449, 577, and 641, as can be read off of Figure 13.1. We will prove that 193, 257, 449, and 577 do not divide F_5, and that 641 does.

(i) First, we note that $3 \cdot 2^6 \equiv -1 \pmod{193}$, which implies that

$$3 \equiv -2^{-6} \pmod{193}.$$

A quick computation shows that $3^2 = 9$, $3^4 = 81 = 2^6 + 2^4 + 1$, and $3^8 = 6561 = 34 \cdot 193 - 1$, so that

$$3^8 \equiv -1 \pmod{193}$$

and thus $\operatorname{ord}_{193}(3) = 16$. It follows that

$$1 \equiv 3^{16} \equiv (-2)^{6\cdot 16} \equiv 2^{96} \pmod{193},$$

which allows us to conclude that $\operatorname{ord}_{193}(2) \mid 96$. Now observe that if $193 \mid F_5$ so that $2^{32} \equiv -1 \pmod{193}$, then we'd have $\operatorname{ord}_{193}(2) = 64 \nmid 96$, a contradiction.

(ii) Note that 257 is itself a Fermat number. In Theorem 13.3.3 (Goldbach's Theorem) we showed that any two distinct Fermat numbers are relatively prime, so that $257 \nmid F_5$.

(iii) To show that $449 \nmid 2^{32}+1$, we will simply compute $2^{32} \pmod{449}$. Note that $2^9 \equiv 2^6 - 1 \pmod{449}$. This allows us to compute

$$\begin{aligned} 2^{16} &\equiv 2^7(2^6-1) \\ &\equiv 2^{13} - 2^7 \\ &\equiv 2^4(2^6-1) - 2^7 \\ &\equiv 2^{10} - 2^7 - 2^4 \\ &\equiv 2(2^6-1) - 2^7 - 2^4 \\ &\equiv -2^4 - 2 \pmod{449}. \end{aligned}$$

It follows that $2^{32} \equiv (-2^4-2)^2 \equiv 2^8 + 2^6 + 2^2 \equiv 324 \pmod{449}$, so we see that $2^{32} \not\equiv -1 \pmod{449}$.

(iv) Here we note that $2^9 \equiv -(2^6+1) \pmod{577}$. By a similar calculation as above, we compute that

$$2^{32} \equiv -2^8 - 2^5 - 2 \equiv 287 \pmod{577}.$$

Since $2^{32} \not\equiv -1 \pmod{577}$, it follows that $577 \nmid F_5$.

(v) Finally, we prove that $641 \mid F_5$. Euler's insight was that $641 = 5^4 + 2^4$, so that

$$5^4 \equiv -2^4 \pmod{641}.$$

Furthermore, we have $641 = 5 \cdot 2^7 + 1$, so that $5 \equiv -2^{-7} \pmod{641}$. It follows that

$$2^{32} \equiv 2^4 \cdot 2^{7\cdot 4} \equiv -5^4 \cdot 2^{7\cdot 4} \equiv -(5 \cdot 2^7)^4 \equiv -(-1)^4 \equiv -1 \pmod{641}.$$

We conclude that $641 \mid 2^{32} + 1$. □

REMARK 16.1.7. Édouard Lucas showed that any prime divisor $p \mid F_n$ of the nth Fermat number F_n, where $n \geq 2$, must in fact be of the form $k2^{n+2} + 1$. Had Euler known this stronger restriction on the prime divisors of the Fermat numbers, he wouldn't even have to cover the cases 193, 449, and 577!

16.2 Euler's Theorem

Euler figured out a way to generalize Fermat's Little Theorem to the composite moduli. He made use of his totient function ϕ, which counts for each n the number of $0 \leq m < n$ relatively prime to n.

THEOREM 16.2.1 (Euler's Theorem). *Consider a natural number n and an integer a such that $\gcd(a, n) = 1$. The congruence*

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

holds

We present two proofs of Euler's Theorem. The first is the standard proof, and the other is inspired by methods of group theory.

FIRST PROOF OF EULER'S THEOREM. Consider an integer a relatively prime to n, and consider a reduced residue system $r_1, \ldots, r_{\phi(n)}$ modulo n. We claim that

$$ar_1, \ldots, ar_{\phi(n)}$$

is again a reduced residue system modulo n. Indeed, since multiplying by a induces a bijection on $\mathbb{Z}/n\mathbb{Z}$, we see that all integers $ar_1, \ldots, ar_{\phi(n)}$ are incongruent. Furthermore, the product of any two integers relatively prime to n is again relatively prime to n, so all the integers ar_i are relatively prime to n. Since any set of $\phi(n)$ incongruent integers relatively prime to n form a reduced residue system, the claim follows.

Using that the integers $ar_1, \ldots, ar_{\phi(n)}$ form a reduced residue system, it follows that

$$\prod_{i=1}^{\phi(n)} r_i \equiv \prod_{i=1}^{\phi(n)} ar_i = a^{\phi(n)} \prod_{i=1}^{\phi(n)} r_i \pmod{n}$$

Since $\prod_{i=1}^{\phi(n)} r_i$ is relatively prime to n, it follows that $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Second proof of Euler's theorem. Consider the least positive integer k such that $a^k \equiv 1 \pmod{n}$, and consider the relation $\sim$ on the set of integers $0 \leq b < n$ relatively prime to n, where

$$b \sim c \qquad \text{if and only if} \qquad \exists_{0 \leq i < k} ba^i \equiv c \pmod{n}.$$

This relation is reflexive, because $ba^0 \equiv b \pmod{n}$. It is symmetric, because if $ba^i \equiv c \pmod{n}$ for some nonzero i, then $ca^{k-i} \equiv ba^i a^{k-i} \equiv b \pmod{n}$. Furthermore, it is transitive, because if $ba^i \equiv c$ and $ca^j \equiv d$, then $ba^{i+j} \equiv d$. If $k \leq i + j$, then we find that also $ba^{i+j-k} \equiv d$. Thus, the relation $\sim$ is an equivalence relation.

We claim that each equivalence class has size k. Indeed, for each b, the set

$$\{b, ba, ba^2, \ldots, ba^{k-1}\}$$

consists of k distinct elements, because multiplying with b is a bijection. Thus we have partitioned the set of all numbers $0 \leq b < n$ relatively prime to n into equivalence classes of size k. On the other hand, the total number of elements $0 \leq b < n$ relatively prime to n is the number $\phi(n)$. This shows that $k \mid \phi(n)$, so it follows that $a^{\phi(n)} \equiv 1 \pmod{n}$. □

Remark 16.2.2. The second proof of Euler's theorem can be simplified using the language of group theory. A **group** is a set G equipped with a binary operation $x, y \mapsto xy$, a unary operation $x \mapsto x^{-1}$, and a unit element 1, satisfying the axioms

$$\begin{aligned} (xy)z &= x(yz) \\ x1 &= x \\ 1x &= x \\ xx^{-1} &= 1 \\ x^{-1}x &= 1. \end{aligned}$$

One can show that the set of integers modulo n relatively prime to n forms a group, where the binary operation is multiplication, the unit element is the integer 1, and the inverse x^{-1} of an integer x modulo n is the unique solution to the equation $xy \equiv 1 \pmod{n}$. The number of elements in this group is $\phi(n)$. For any integer a modulo n relatively prime to n such that $a^k \equiv 1 \pmod{n}$, the set $\{1, a, a^2, \ldots, a^{k-1}\}$ is a subgroup, which means that it is closed under the group operations. The argument where we introduced an equivalence relation $\sim$ to partition the set of all integers modulo n relatively prime to n into equivalence classes of size k is an instance of a much more general result, Lagrange's Theorem, which asserts that the size of any subgroup of a finite group divides the size of the entire group.

Since $\phi(p) = p - 1$, it follows that Theorem 16.1.1 (Fermat's Little Theorem) is also a direct corollary of Theorem 16.2.1 (Euler's Theorem).



REMARK 16.2.3. We saw the multiplicative order featuring in the second proof of Theorem 16.2.1 (Euler's Theorem). Thus, using the second proof of Euler's theorem we immediately observe that

$$\mathrm{ord}_n(a) \mid \phi(n),$$

for any a and n such that $\gcd(a, n) = 1$.

Some questions about Euler's totient function remain unresolved. While we have seen that $\phi(p) = p - 1$ for any prime number p, Lehmer asked whether there is any composite number n such that

$$\phi(n) \mid n - 1.$$

This open problem is now known as **Lehmer's problem** [LEH1933].

16.3 Wilson's Theorem

The following theorem is a factorial criterion by which to decide whether a number is prime. It states that n is prime if and only if the congruence

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

holds.

In the European mathematical tradition, it was first published by Edward Waring, who attributed it as follows to John Wilson [WAR1782, p. 380] along with high praise: *This most elegant property of prime numbers was discovered by the most illustrious and most skilled mathematician, John Wilson, Esquire.* However, neither Wilson nor Waring were able to rigorously prove this property of the prime numbers. The first to give a proof was Joseph–Louis Lagrange [LAG1771]. Euler, and later Gauss, gave separate proofs of this fact.

THEOREM 16.3.1 (Wilson's Theorem). *A natural number $n \geq 2$ is prime if and only if*

$$(n-1)! \equiv -1 \pmod{n}.$$

PROOF. First, we observe that the claim holds for $n = 2$, since $1 \equiv -1 \pmod{2}$.

Suppose that n is prime strictly greater than 2. Then every integer $0 < a < n$ has a multiplicative inverse modulo n, meaning that for every integer a there is an integer a^{-1} such that

$$aa^{-1} \equiv 1.$$

Now we group the integers $1 \leq a < n$ into pairs with their inverses. By Exercise 13.6 and the assumption that $n \neq 2$, there are exactly two integers that would pair up with themselves because they are their own inverses: The integers 1 and -1 are the only two integers a modulo n for which the congruence $a^2 \equiv 1 \pmod{n}$ holds. The other integers come in proper pairs (a, a^{-1}). Therefore, we have

$$(n-1)! \equiv 1(n-1) \equiv -1 \pmod{n}.$$

Conversely, suppose that the congruence $(n-1)! \equiv -1 \pmod{n}$ holds. Since any $0 < a < n$ is a divisor of $(n-1)!$, it follows that for any such a there is a solution to the linear congruence

$$ax \equiv -1 \pmod{n}.$$

This implies that any $0 < a < n$ is invertible modulo n, so it follows that $\gcd(a, n) = 1$ for all $0 < a < n$. We conclude that the only proper divisor of n is 1, and therefore n is prime. □

Second proof of the forward direction of Theorem 16.3.1 (Wilson's Theorem). Consider a prime p, and consider the monic polynomial

$$f(x) = \prod_{k=0}^{p-1}(x-k).$$

Since every element is a root of $f(x)$ modulo p, it follows by Theorem 16.1.1 (Fermat's Little Theorem) that $f(x) \equiv x^p - x \pmod{p}$. Since $f(x) = xg(x)$, where $g(x) := \prod_{k=1}^{p-1}(x-k)$, it follows by the product rule for differentiation that

$$f'(x) = xg'(x) + g(x).$$

This shows that $f'(0) = g(0)$. On the other hand the derivative of $x^p - x$ is $px^{p-1} - 1$. Thus, we conclude that

$$k! = \prod_{k=1}^{p-1}(0-k) \equiv -1 \pmod{p}.$$ □

16.4 Some Theorems Concerning Strong Divisibility Sequences

Example 16.4.1. Consider the pth Mersenne number $M_p = 2^p - 1$, where p is an odd prime. We claim that the following congruence holds:

$$\prod_{k=1}^{p-1}(2^k + 1) \equiv 1 \pmod{M_p}.$$

To see this, set $A := \prod_{k=1}^{p-1}(2^k - 1)$ and $B := \prod_{k=1}^{p-1}(2^k + 1)$. Then we have

$$AB = \prod_{k=1}^{p-1}(2^{2k} - 1).$$

The order of 2 modulo M_p is p. It follows that $2^k - 1 \equiv 2^l - 1 \pmod{M_p}$ if and only if $k \equiv l \pmod{p}$. Since p was assumed to be odd, multiplication by 2 is a bijection modulo p, so we conclude that

$$\prod_{k=1}^{p-1}(2^{2k} - 1) \equiv \prod_{k=1}^{p-1}(2^k - 1) \pmod{M_p},$$



since both products have the same factors modulo M_p. This shows that $AB \equiv A \pmod{M_p}$. Moreover, A is invertible modulo M_p, since A is a product of invertible numbers:

$$\gcd(2^k - 1, 2^p - 1) = 2^{\gcd(k,p)} - 1 = 1.$$

Therefore, we cancel A on both sides to obtain $B \equiv 1 \pmod{M_p}$.

This example relies on having a bijection which rearranges the order of the factors in a product. This idea is generalizable; particularly to the setting of strong divisibility sequences.

THEOREM 16.4.2. *Let (u_m) be a strong divisibility sequence. Furthermore, suppose there is a natural number n and an integer c such that*

$$u_{m+n} \equiv cu_m \pmod{u_n}$$

for all m. Then the congruence

$$\prod_{\substack{k=1 \\ \gcd(n,k)=1}}^{n-1} \frac{u_{rk}}{u_k} \equiv c^{(r-1)\varphi(n)/2} \pmod{u_n}$$

holds for every r relatively prime to n.

PROOF. For each k relatively prime to n, write $rk = q_k n + s_k$, where $1 \leq s_k < n$. Since $\gcd(r, n) = 1$, multiplying by r is a bijection on reduced residue classes modulo n, so that the map $k \mapsto s_k$ is also bijection on reduced residue classes modulo n.

By the congruence $u_{m+n} \equiv cu_m \pmod{u_n}$, it follows that

$$u_{rk} \equiv c^{q_k} u_{s_k} \pmod{u_n}.$$

Consequently, we obtain the congruence

$$\prod_{\substack{1 \leq k < n \\ \gcd(n,k)=1}} u_{rk} \equiv c^{\sum_k q_k} \prod_{\substack{1 \leq k < n \\ \gcd(n,k)=1}} u_k \pmod{u_n}.$$

By the assumption that (u_m) is a strong divisibility sequence, it follows that $\gcd(u_n, u_k) = u_{\gcd(n,k)} = 1$, so that $\prod_k u_k$ is invertible modulo u_n.

It remains to evaluate the sum $\sum_k q_k$. Observe that

$$n \sum_k q_k = \sum_k (rk - s_k) = \sum_k (r-1)k = n(r-1)\varphi(n)/2. \qquad \square$$

COROLLARY 16.4.3. *For every Lucas sequence (u_n) with $u_{n+2} = au_{n+1} - bu_n$, where $\gcd(a, b) = 1$, and every r relatively prime to n, we have the following congruence:*

$$\prod_{\substack{1 \leq k \leq n-1 \\ \gcd(n,k)=1}} \frac{u_{rk}}{u_k} \equiv u_{n+1}^{(r-1)\varphi(n)/2} \pmod{u_n}.$$

Proof. The Lucas sequence (u_n) is strongly divisible by Theorem 19.1.12. Moreover, (u_n) satisfies the following addition formula by Proposition 19.1.8:

$$u_{m+n} = u_{n+1}u_m - bu_nu_{m-1}.$$

This implies the congruence

$$u_{m+n} \equiv u_{n+1}u_m \pmod{u_n}.$$

Thus, the claim follows from Theorem 16.4.2 with $c := u_{n+1}$. □

Example 16.4.4. Consider the Lucas sequence given by $u_n = n$, which satisfies the recurrence relation $u_{n+2} = 2u_{n+1} - u_n$. Then we have $u_{n+1} \equiv 1 \pmod{u_n}$. Assuming r relatively prime to n, the congruence of Corollary 16.4.3 is therefore exactly Theorem 16.2.1 (Euler's Theorem):

$$r^{\varphi(n)} \equiv 1 \pmod{n}.$$

Example 16.4.5. Consider the Lucas sequence given by $u_n = 1 + a + \cdots + a^{n-1}$, which satisfies the recurrence relation $u_{n+2} = (a+1)u_{n+1} - au_n$. Since $u_{n+1} = 1 + au_n$, it follows that $u_{n+1} \equiv 1 \pmod{u_n}$. Moreover, note that

$$\frac{u_{rk}}{u_k} = \frac{a^{rk}-1}{a^k-1} = 1 + a^k + \cdots + a^{k(r-1)}.$$

Assuming r relatively prime to n, the congruence of Corollary 16.4.3 is therefore:

$$\prod_{\substack{1\le k\le n-1\\ \gcd(n,k)=1}} 1 + a^k + \cdots + a^{k(r-1)} \equiv 1 \pmod{u_n}.$$

This is Hao Pan's q-analogue of Euler's Theorem [Pan2007].

Example 16.4.6. Consider the Fibonacci numbers F_n, and set $r = 2$. Since $F_{2k} = F_kL_k$, it follows from the congruence of Corollary 16.4.3 that

$$\prod_{k=1}^{p-1} L_k \equiv F_{p+1}^{\frac{p-1}{2}} \pmod{F_p}$$

for any odd prime p.

16.5 The Quadratic Character of −1

Theorem 16.3.1 (Wilson's Theorem) can be used to prove a historically important result in the development of modular arithmetic: that −1 is congruent to a square modulo an odd prime p if and only if $p \equiv 1 \pmod 4$. In his *Disquisitiones Arithmeticae* [Gau1986],



Figure 16.1: Carl Friedrich Gauss. Pastel painting by Johann Christian August Schwartz, 1803.

Gauss writes of this result that when he encountered it in 1795—he was 19 at the time—he considered it to be a result of rare beauty and suspected deep connections with even more profound results, that he concentrated all his efforts into understanding its underlying principles. He became so attracted by the questions of this nature, that he could not let them be. Ultimately, Gauss's investigations into higher arithmetic, as he preferred to call it, led him to prove the celebrated Theorem 28.2.1 (The Law of Quadratic Reciprocity).

While the law of quadratic reciprocity is certainly the central theorem of our subject, the quadratic character of -1 modulo a prime is a key result on its own. In this section we will show that it can be used to show that there are infinitely many primes congruent to 1 modulo 4. Furthermore, we will use the fact that -1 is congruent to a square modulo p when $p \equiv 1 \pmod 4$ in the next chapter to prove Fermat's *Two-Square Theorem*, which asserts that every such prime is the sum of two squares. Questions similar to the quadratic character of -1 modulo a prime will be investigated more fully in Chapters 27 and 28.

THEOREM 16.5.1 (The Quadratic Character of -1). *Consider an odd prime p. Then there exists an integer a such that*

$$a^2 \equiv -1 \pmod p$$

if and only if $p \equiv 1 \pmod 4$.

PROOF. First, we show that if there is an integer a such that $a^2 \equiv -1 \pmod p$, then we must have $p \equiv 1 \pmod 4$. By Theorem 16.1.1 (Fermat's Little Theorem) it follows that

$$(-1)^{\frac{p-1}{2}} \equiv (a^2)^{\frac{p-1}{2}} \equiv a^{p-1} \equiv 1 \pmod p$$

This shows that $\frac{p-1}{2}$ must be even, which is equivalent to the congruence $p \equiv 1 \pmod 4$.

For the converse, assume that $p \equiv 1 \pmod 4$. By Theorem 16.3.1 (Wilson's Theorem) we know that $(p-1)! \equiv -1 \pmod p$. Now, observe that the integers $1, \dots, p-1$ can be arranged in pairs, where each i is paired with $p-i$, which is always distinct from i because $p-1$ is even. Since $i(p-i) \equiv -i^2 \pmod p$, we obtain the congruences

$$-1 \equiv (p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod p.$$

The last congruence holds, because $(p-1)/2$ is even by the assumption that $p \equiv 1 \pmod 4$. Thus, we have presented -1 as a square modulo p. □

The previous theorem describing the quadratic character of -1 modulo an odd prime p can be used to show that there are infinitely many primes congruent to 1 modulo 4. The first fifteen primes congruent to 1 modulo 4 are:

$$5,\ 13,\ 17,\ 29,\ 37,\ 41,\ 53,\ 61,\ 73,\ 89,\ 97,\ 101,\ 109,\ 113,\ \text{and } 137.$$

Theorem 16.5.2. *There are infinitely many primes congruent to* 1 *modulo* 4.

Proof. Consider a finite set of primes $p_1, \dots, p_k$ that are all congruent to 1 modulo 4, and define

$$n = (2p_1 \cdots p_k)^2 + 1.$$

Notice that $n \equiv 1 \pmod 4$ is greater than 1, and $p_i \nmid n$ for any $1 \le i \le k$. It follows that for any prime divisor q of n, we have

$$(2p_1 \cdots p_k)^2 \equiv -1 \pmod q,$$

showing that -1 is a quadratic residue modulo q. Since -1 is a quadratic residue modulo q if and only if $q \equiv 1 \pmod 4$, it follows that any prime divisor q of n is congruent to 1 modulo 4. Since none of the prime divisors of n are among the primes p_i we started out with, the primes p_i could not have listed all the primes congruent to 1 modulo 4. □

Theorem 16.5.1 and its proof can be generalized to arbitrary exponents. For example, the following theorem implies that the congruence $x^4 \equiv -1 \pmod p$ is solvable if and only if $p \equiv 1 \pmod 8$, that the congruence $x^8 \equiv -1 \pmod p$ is solvable if and only if $p \equiv 1 \pmod{16}$, and so on.

Theorem 16.5.3. *Consider an odd prime p and consider a natural number n with 2-adic decomposition $n = 2^k m$. Then the congruence*

$$x^n \equiv -1 \pmod p$$

is solvable if and only if $p \equiv 1 \pmod{2^{k+1}}$.

PROOF. The proof is by induction on k. For $k = 0$, the statement is trivial, and for $k = 1$, the proof was given in Theorem 16.5.1. For the inductive step, assume that for any number n with 2-adic decomposition $n = 2^k m$, the congruence $x^n \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{2^{k+1}}$, and consider a number n with 2-adic decomposition $n = 2^{k+1}m$.

For the forward direction, assume that a is an integer such that $a^n \equiv -1 \pmod{p}$. Then $b := a^{2m}$ is an integer such that

$$b^{2^k} \equiv -1 \pmod{p},$$

so we see that $p \equiv 1 \pmod{2^{k+1}}$. Consequently, the fraction

$$\frac{p-1}{2^{k+1}}$$

is an integer. By Theorem 16.1.1 (Fermat's Little Theorem) it follows that

$$(-1)^{\frac{p-1}{2^{k+1}}} \equiv (a^{2^{k+1}m})^{\frac{p-1}{2^{k+1}}} \equiv (a^m)^{p-1} \equiv 1 \pmod{p}.$$

This implies that $\frac{p-1}{2^{k+1}}$ is even, so that $p \equiv 1 \pmod{2^{k+2}}$.

For the converse, suppose that $p \equiv 1 \pmod{2^{k+2}}$ and consider an integer a such that $a^{2^k} \equiv -1 \pmod{p}$. Such an integer exists by the inductive hypothesis. Now partition the set of numbers $\{1, \ldots, p-1\}$ into classes of 2^{k+1} numbers of the form $\{x, ax, \ldots, a^{2^{k+1}-1}x\}$. We will write c for the number of such classes. Then we have $p = 2^{k+1}c + 1$, so we see that c is even.

Since the number of classes is c, we can label them by C_i for each $1 \leq i \leq c$, and we can pick a representative $x_i \in C_i$ for each i. Now it follows by Theorem 16.3.1 (Wilson's Theorem) that

$$-1 \equiv (p-1)! \equiv \prod_{i=1}^{c} \prod_{j=0}^{2^{k+1}-1} a^j x_i \equiv \prod_{i=1}^{c} (-1) x_i^{2^{k+1}} \equiv (-1)^c \prod_{i=1}^{c} x_i^{2^{k+1}} \equiv \left(\prod_{i=1}^{c} x_i \right)^{2^{k+1}} \pmod{p}.$$

□

16.6 The Infinitude of Primes Congruent to 1 Modulo Powers of 2

One way to show that a prime p is congruent to 1 modulo n is by finding an integer a such that

$$\operatorname{ord}_p(a) = n.$$

By Theorem 8.5.2 (Order Theorem) and Theorem 16.1.1 (Fermat's Little Theorem), this implies that $n \mid p-1$. We will use this idea to show that there are infinitely many primes congruent to 1 modulo any power of 2. In particular, there are infinitely many primes congruent to 1 modulo 4, modulo 8, modulo 16, and so on.

Theorem 16.6.1. *For any positive natural number n, there are infinitely many primes congruent to 1 modulo 2^n.*

Proof. Since $p \equiv 1 \pmod{2^{n+1}}$ implies that $p \equiv 1 \pmod{2^n}$, it suffices to show that for any finite list $p_1, \ldots, p_k$ of primes congruent to 1 modulo 2^{n+1}, there is a prime $q \equiv 1 \pmod{2^{n+1}}$ which is not among the primes p_i.

Given such a list of primes p_i, let

$$a := 2p_1 \cdots p_k,$$

and let q be a prime divisor of the integer $b := a^{2^n} + 1$. Note that q is necessarily an odd prime, since a is even and hence b is odd. Since $p_i \nmid b$ for any i, it follows that q is not among the primes p_i. Furthermore, we observe that

$$a^{2^n} \equiv -1 \pmod{q}.$$

This implies that $\mathrm{ord}_q(a) \mid 2^{n+1}$, while clearly $\mathrm{ord}_q(a) \nmid 2^n$. Thus, we must have $\mathrm{ord}_q(a) = 2^{n+1}$, and this allows us to conclude that $q \equiv 1 \pmod{2^{n+1}}$. □

The previous theorem is a special case of a deep theorem in analytic number theory: *Dirichlet's Theorem*. Dirichlet's Theorem shows that for any integer a relatively prime to n, there are infinitely many primes

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

The techniques of proving Dirichlet's Theorem are beyond the scope of this course. However, having taken this course, you are well equipped to read LeVeque's excellent *Topics in Number Theory* [LeV1956a; LeV1956b], a two-volume work that contains well-explained proofs of Dirichlet's Theorem as well as the Prime Number Theorem.

Exercises

Starter Exercises

16.1 For every prime $p \equiv 1 \pmod 4$ below 100, find the least positive integer a such that $a^2 \equiv -1 \pmod p$.

16.2 (a) Consider two integers a and b, and a prime number p. Prove, without using Fermat's Little Theorem, that

$$(a+b)^p \equiv a^p + b^p \pmod p.$$

(b) Suppose that $a \geq 0$. Use the previous congruence and the fact that $a = \sum_{i=1}^{a} 1$ to give your own proof of Fermat's Little Theorem.

16.3 (a) Prove that

$$5^{5^5} \equiv 5^5 \pmod{31}.$$

(b) Prove that

$$7^{7^7} \equiv 7^7 \pmod{43}.$$

Routine-Building Exercises

16.4 Show that

$$2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \pmod p$$

for any prime number $p \neq 3$.

16.5 For any positive integer n we define the **Euler quotient**

$$q_n(x) := \frac{x^{\phi(n)} - 1}{n},$$

where x is assumed to be relatively prime to n. In the special case where n is a prime, $q_n(x)$ is called the **Fermat quotient**.

(a) Show that

$$q_n(ab) \equiv q_n(a) + q_n(b) \pmod n$$

for any two integers a and b relatively prime to n, and conclude that $q_n(a^k) \equiv kq_n(a) \pmod n$ for a relatively prime to n.

(b) For any prime p, define the **Wilson quotient** W_p by

$$W_p := \frac{(p-1)! + 1}{p}.$$

Prove **Lerch's formula** [LER1905], which asserts that

$$\sum_{k=1}^{p-1} q_p(k) \equiv W_p \pmod p.$$

16.6 Show that

$$3^{3^{3^3}} \equiv 3^{3^3} \pmod{97}.$$

16.7 (a) Show that any number of the form

$$m^5 n - n^5 m$$

is divisible by 30.

(b) Show that for any two odd primes p and q, the number

$$p^5 q - q^5 p$$

is divisible by 240.

16.8 Prove that if

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

for every integer a, then $n = 2$ or n is odd.

16.9 Consider two distinct primes p and q, and an integer $a \geq 0$. Prove that

$$a^{pq} + a \equiv a^p + a^q \pmod{pq}$$

16.10 Consider an odd prime $p = 2n + 1$. Show that

$$\binom{2n}{n} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

16.11 Consider a prime p and two numbers m and n. Prove that

$$\binom{p^k n}{p^k m} \equiv \binom{n}{m} \pmod{p}.$$

16.12 Show that the congruence

$$\sum_{k=1}^{n} k^n \equiv 0 \pmod{n}$$

holds if and only if n is odd.

16.13 (a) Consider a prime p and an integer $p \nmid a$. Show that

$$a^p \equiv a \pmod{p^2} \quad \Leftrightarrow \quad a^{p^2} \equiv a \pmod{p^2}.$$

(b) A prime satisfying $a^p \equiv a \pmod{p^2}$ is called a **Wieferich prime base** a. Wieferich encountered this condition by showing that if $x^p + y^p = z^p$ with $p \nmid xyz$, then p must be a Wieferich prime base 2 [Wie1909]. The only known Wieferich primes base 2 are $p = 1093$ and $p = 3511$, and there are no smaller Wieferich primes base 2.
In bases larger than 2 there are smaller Wieferich primes, although they are still rare. The only known Wieferich primes base 3 are $p = 11$ and $p = 1006003$. Show that 5 is a Wieferich prime base 32.

Challenge Exercises

16.14 Find the least integer $k > 1$ such that every integer of the form $x^k - x$ is divisible by 47 and 89.

16.15 Find a prime $p > 3$ such that

$$3^{3^3} \equiv 3^3 \pmod{p}.$$

16.16 For any integer a and any prime number p, show that

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

16.17 Find all the solutions to the equation

$$p^q - q^p = p + q,$$

where p and q are prime numbers.

16.18 Consider two primes p and q. Show that

$$pq \mid (13^p - 5^p)(13^q - 5^q) \quad \Leftrightarrow \quad pq \mid 12.$$

16.19 (a) Show that the number $6481 = 3^8 - 3^4 + 1$ is prime. Hint: In order to avoid trying out all the primes below 80, show first that every prime factor p of 6481 satisfies $p \equiv 1 \pmod{24}$.

(b) Compute the prime factorization of the number

$$3^{24} - 1.$$

16.20 Consider the function $f(n) = 2n + 1$. Show for every prime p, the sequence

$$k \mapsto f^k(p)$$

obtained by iterating the function f, contains composite numbers.

16.21 (a) Consider an odd prime q. Show that the numbers

$$2^q - 1 \qquad \text{and} \qquad q + 1.$$

are relatively prime.

(b) Consider two distinct primes p and q, and let r be a common prime divisor of the numbers

$$\frac{p^q - 1}{p - 1} \qquad \text{and} \qquad \frac{q^p - 1}{q - 1}.$$

Show that $r \equiv 1 \pmod{2pq}$.

16.22 Let F_n be the nth Fibonacci number. Show that if p is prime, then

$$F_{p-1} + F_{p+1} \equiv 1 \pmod{p}.$$

Chapter 17

Fermat's Two-Squares Theorem

17.1 Numbers Representable as a Sum of Two Squares

In this chapter we are concerned with the question which numbers are representable as a sum of two squares. In other words, our goal is to find a precise characterization of the numbers n that can be written in the form

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

Here, we permit ourselves to pick $a = 0$ or $b = 0$, so that any perfect square is trivially representable as a sum of two squares. The problem of finding those numbers n that can be written as the sum of two squares is equivalent to the problem of finding integer lattice points on the circle of radius $\sqrt{n}$, as illustrated in Figure 17.1.

Using modular arithmetic, we can find some basic obstructions to the possibility of representing a number as a sum of two squares. Recall that the square of an even number is always divisible by 4, and the square of an odd number is always of the form $4k + 1$. As a direct consequence we see that if n is of the form $4k + 3$ then it is not representable as a sum of two squares. This observation leads to the following lemma.

Lemma 17.1.1. *Suppose that $n = a^2 + b^2$ and consider a prime $p \equiv 3 \pmod 4$ such that $p \mid n$. Then $p \mid a$ and $p \mid b$.*



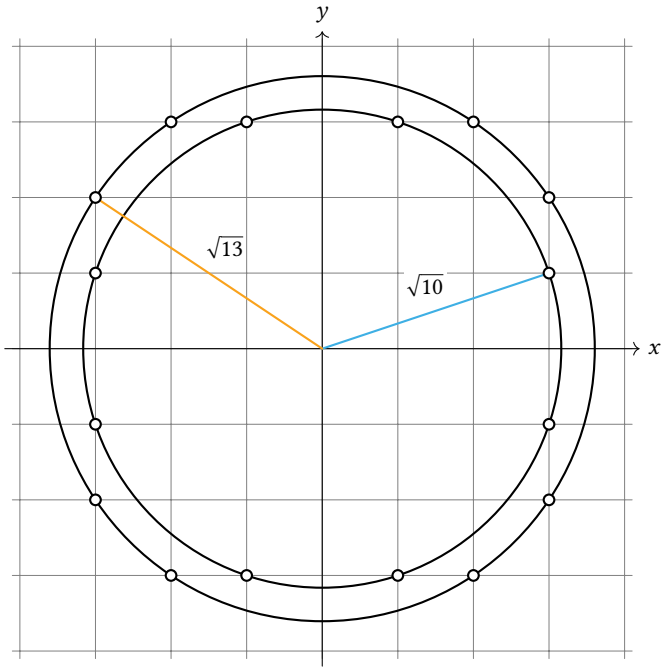


Figure 17.1: Representing a number as a sum of two squares is equivalent to finding an integer lattice point on the circle of radius $\sqrt{n}$. Here we displayed the integer lattice points on the circles of radii $\sqrt{10}$ and $\sqrt{13}$.

PROOF. If $p \nmid a$, then the integer a is invertible modulo p. Then the congruence $a^2+b^2 \equiv 0 \pmod{p}$ implies that

$$(a^{-1}b)^2 \equiv -1 \pmod{p}.$$

This is a contradiction, since the congruence $x^2 \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{4}$. Thus, it follows that $p \mid a$ and consequently we also obtain $p \mid b$. □

The previous lemma can be used to find an obstruction to numbers being representble as a sum of two squares.

COROLLARY 17.1.2. *If the square-free part of a natural number n is divisible by a prime $p \equiv 3 \pmod{4}$, then n is not representable as a sum of two squares.*

PROOF. By Lemma 17.1.1 it follows that if n is divisible by a prime $p \equiv 3 \pmod{4}$, then we also have $p^2 \mid n$. Writing $n = p^2n'$, $a = pa'$ and $b = pb'$, we find that

$$n' = a'^2 + b'^2.$$

By iterating this process, we see that the p-adic valuation of n is even. Thus, if the p-adic valuation of n is odd, which is equivalent to the condition that the square-free part of n is divisible by p, then n is not representable as a sum of two squares. □

One of Fermat's most remarkable discoveries was that the statement in Corollary 17.1.2 is sharp: A number is representable as a sum of two squares if and only if its square-free part is not divisible by any primes congruent to $3 \pmod 4$. The first published proof of this claim was due to Euler. Fermat's discovery is now known as *Fermat's Two-Squares Theorem*. We will give Euler's proof in the next section. Another classic proof is Don Zagier's, who famously wrote it up in a single—rather complicated—sentence.

A commonality between all these proofs is a reduction to the primes, which we will also perform here. Just as we did for the Pythagorean triples, we will consider numbers that are representable as a sum of two squares, which are relatively prime to each other. Such representations will be called **primitive**.

Definition 17.1.3. We say that a number n is **primitively representable** as a sum of two squares if there are relatively prime positive integers a and b such that

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

By Corollary 17.1.2 it follows immediately that numbers divisible by a prime $p \equiv 3 \pmod 4$ are never primitively representable as a sum of two squares: Either they are not representable at all, or they are representable as the sum of two squares of numbers, each of which is divisible by p. Likewise, any number divisible by 4 is not primitively representable, since two squares only sum to a number divisible by 4 if they are both even. Thus, we obtain the following corollary.

Corollary 17.1.4. *Any number divisible by 4 or by any prime $p \equiv 3 \pmod 4$ is not primitively representable as a sum of two squares.*

We can thus formulate the Two-Squares Theorem for primitive representations as sums of two squares as follows: A number n has a primitive representation as a sum of two squares if and only if n is a product of primes congruent to $1 \pmod 4$ or n is twice such a product.

In order to reduce the Two-Squares Theorem to the primes $p \equiv 1 \pmod 4$, we first recall the **Brahmagupta–Fibonacci identity**, from which it follows that products of numbers representable as sums of two squares are again so representable. While this identity might appear to come out of thin air, it has a natural interpretation in the Gaussian integers, which we will discuss in Chapter 18.

Lemma 17.1.5 (The Brahmagupta–Fibonacci Identity). *For an integers a, b, c, and d, we have*

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2.$$

Proof. This identity can be verified by a simple calculation:

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= a^2c^2 \pm 2abcd + b^2d^2 + a^2d^2 \mp 2abcd + b^2c^2 \\ &= (ac \pm bd)^2 + (ad \mp bc)^2.\end{aligned}$$

□

By the Brahmagupta–Fibonacci identity it is easy to note that the number 65 can be represented as a sum of two squares in two distinct ways:

$$65 = 1^2 + 8^2 \qquad \text{and} \qquad 65 = 4^2 + 7^2.$$

Indeed, the Brahmagupta–Fibonacci identity gives that

$$65 = 13 \cdot 5 = (2^2 + 3^2)(1^2 + 2^2) = (6 \pm 2)^2 + (4 \mp 3)^2.$$

We have thus reduced the Two-Squares Theorem to the following statement: Every prime $p \equiv 1 \pmod 4$ can be represented as a sum of two squares. In fact, somthing stronger is true: Every prime $p \equiv 1 \pmod 4$ can be *uniquely* represented as a sum of two squares.

PROPOSITION 17.1.6. *Any prime number p can be represented in at most one way as a sum of two squares.*

PROOF. We have already seen that primes of the form $p \equiv 3 \pmod 4$ are not representable as the sum of two squares, which means that the claim is indeed true for such primes. The only way to represent 2 as a sum of two squares is

$$2 = 1^2 + 1^2.$$

The only remaining case is $p \equiv 1 \pmod 4$.

Consider a prime $p \equiv 1 \pmod 4$, and suppose that $p = x^2 + y^2$ and $p = u^2 + v^2$ are two distinct representations of p as a sum of two squares with $x < y$ and $u < v$. Any such representations are automatically primitive, since p is prime. It follows that y and v are invertible modulo p, so we have

$$(xy^{-1})^2 \equiv -1 \pmod p \qquad \text{and} \qquad (uv^{-1})^2 \equiv -1 \pmod p.$$

This implies that $xy^{-1} \equiv \pm uv^{-1} \pmod p$. By changing the sign of u, which doesn't affect the equation $u^2 + v^2 = p$, we may assume that $xy^{-1} \equiv uv^{-1} \pmod p$, which is equivalent to

$$xv \equiv yu \pmod p.$$

However, note that all of x, y, u, and v are strictly below $\sqrt{p}$. Hence it follows that $xv = yu$. This implies that the fractions $\frac{x}{y}$ and $\frac{u}{v}$ are equal. Since they are in lowest terms, we must have $x = u$ and $y = v$. □

In order to prove this claim, suppose that $a^2 \equiv -1 \pmod p$. Such a solution indeed exists, since $p \equiv 1 \pmod 4$. We will now analyze the multiples of a

$$0,\ a,\ 2a,\ 3a, \ldots, ma$$

modulo p, up to some bound $m < p$ which is yet to be determined. At first sight, we don't know much about the distribution of these residues, except that they are all distinct since the integer a is invertible modulo p.

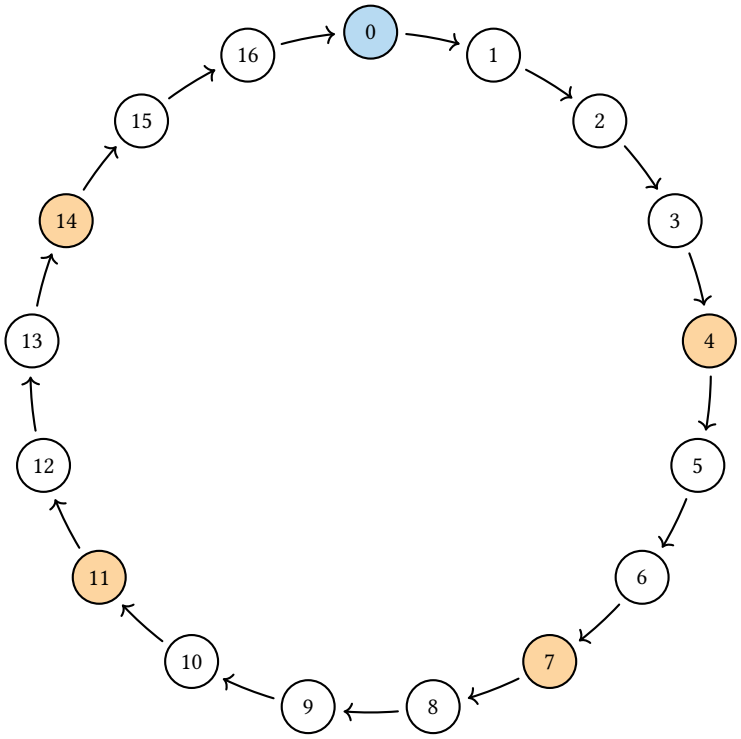


Figure 17.2: By Thue's lemma, in any set of m multiples $\{a, 2a, \dots, ma\}$ modulo any prime p, there is one multiple whose cyclic distance to 0 does not exceed $\frac{p}{m+1}$. Here we see that there is a number of the form $k \cdot 7$, for $1 \le k \le 4$, whose cyclic distance to 0 is 3, which is indeed below $\frac{17}{5}$.

In order to analyze them further, write $|x|_p$ for the least distance to a multiple of p. The least distance from any number to a multiple of p is always at most $p/2$. For example, $|13|_5 = 2$ and $|39|_7 = 3$. The following lemma, which is due to Axel Thue, will be of use.

Lemma 17.1.7 (Thue's Lemma). *Consider two positive integers a and n such that $\gcd(a, n) = 1$. For any natural number m, there is some $1 \le k \le m$ such that*

$$|ka|_n \le \frac{n}{m+1}.$$

Proof. We will assume that $m < n$, for if m is greater then we find $|na|_n = 0$. For each $0 \le i, j \le m$, write $d_{i,j} := |(i-j)a|_n$ be the distance to the nearest multiple of n from the difference between ia and ja. Since i ranges over $m+1$ numbers, the shortest such distance can be no longer than $n/(m+1)$. In other words, we can find distinct numbers $0 \le i, j \le m$ such that

$$d_{i,j} = |(i-j)a|_n \le \frac{n}{m+1}.$$

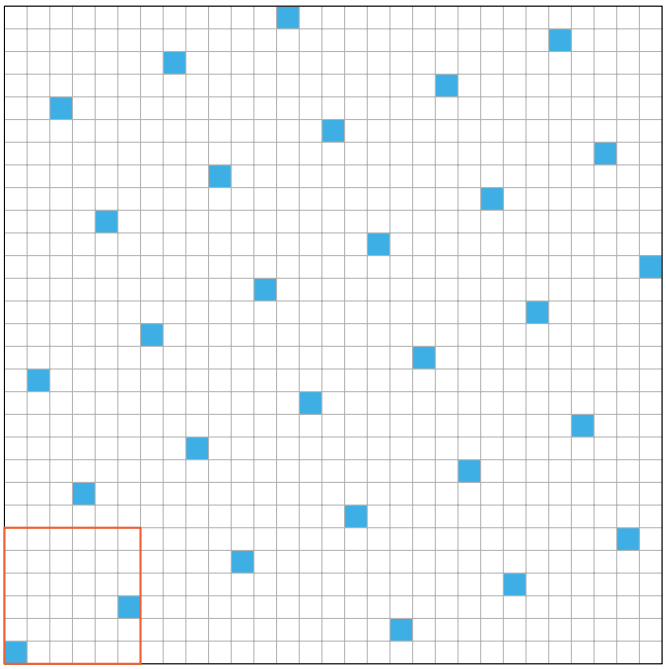


Figure 17.3: Thue's lemma in Lucas' weaving patterns. Here we displayed the points (x, y) satisfying $y \equiv 12x \pmod{29}$.

Now define $k := j - i$. Then we clearly have $0 < k \leq m$, and we have

$$|ka|_n = |(i-j)a|_n \leq \frac{n}{m+1}. \qquad \square$$

Another way of looking at Thue's lemma is by the weaving patterns of Lucas, as illustrated in Figure 17.3. If $\gcd(a, n) = 1$ and $m = \lfloor \sqrt{n} \rfloor$, then there must be a nonzero square with coordinates (x, y) with $0 \leq x, y \leq m$ satisfying $y \equiv ax \pmod{n}$.

THEOREM 17.1.8. *Any prime $p \equiv 1 \pmod{4}$ has a unique primitive representation as a sum of two squares.*

PROOF. Consider a prime $p \equiv 1 \pmod{4}$. We have already seen that there is at most one way to represent p as a sum of two squares, so it remains to prove existence.

Consider an integer $0 \leq a < p$ such that $a^2 \equiv -1 \pmod{p}$. Such an integer exists, since $p \equiv 1 \pmod{4}$. By Lemma 17.1.7 (Thue's Lemma) with $m := \lfloor \sqrt{p} \rfloor$, we find that there is some $1 \leq k < \sqrt{p}$ such that

$$|ka|_p \leq \frac{p}{\sqrt{p}+1} < \sqrt{p}.$$

If we define $r := |ka|_p$, then it follows that $0 < r^2 + k^2 < 2p$. On the other hand, since $a^2 \equiv -1 \pmod{p}$ we have $r^2 + k^2 \equiv (ka)^2 + k^2 \equiv -k^2 + k^2 \equiv 0 \pmod{p}$. Thus, $r^2 + k^2$ is a multiple of p strictly between 0 and $2p$, so we conclude that $r^2 + k^2 = p$. This shows that p can be represented as the sum of two squares. □

Theorem 17.1.9 (Fermat's Two-Squares Theorem). *A natural number n is presentable as the sum of two squares if and only if the prime divisors of its square-free part are either 2 or congruent to $1 \pmod{4}$.*

We will give three more proofs of Fermat's Two-Squares Theorem in remainder of this chapter.

17.2 Euler's Proof by Infinite Descent

Euler proved that every prime $p \equiv 1 \pmod{4}$ can be written as a sum of two squares by using the Brahmagupta–Fibonacci identity in a clever descent argument.

Proof of Theorem 17.1.8. Consider a prime $p \equiv 1 \pmod{4}$. First we observe that there are integers a and b such that

$$p \mid a^2 + b^2.$$

Indeed, it follows from Theorem 16.5.1 that -1 is congruent to a square modulo p, which shows that $p \mid a^2 + 1^2$ for some integer a.

Now assume that a and b are integers such that $p \mid a^2 + b^2$. We claim that if $a^2 + b^2 = rp$ for some $r > 1$, then we can find integers x and y such that $x^2 + y^2 = sp$ for some $s < r$. The theorem then follows at once, since we can keep writing smaller multiples of p as sums of two squares until we have written p itself as a sum of two squares.

To prove the claim, consider let u and v be two integers satisfying the conditions

$$u \equiv a \pmod{r}, \qquad v \equiv b \pmod{r}, \qquad \text{and} \qquad |u|, |v| \leq \frac{r}{2}.$$

Then $u^2 + v^2 \equiv a^2 + b^2 \equiv 0 \pmod{r}$, so that $u^2 + v^2 = rs$. We also observe that it is not possible for both u and v to be congruent to $0 \pmod{r}$. Indeed, if this were the case, then a and b would be divisible by r, which would make the prime p divisible by r. The inequality $u^2 + v^2 \leq \frac{r^2}{2}$ implies that $s \leq \frac{r}{2}$.

Multiplying a^2+b^2 with u^2+v^2 gives $(a^2+b^2)(u^2+v^2) = r^2sp$. By the Brahmagupta–Fibonacci identity, we can write this as

$$(a^2 + b^2)(c^2 + d^2) = (au + bv)^2 + (av - bu)^2.$$

Now we observe that $au + bv \equiv a^2 + b^2 \equiv 0 \pmod{r}$, and that $av - bu \equiv ab - ab \equiv 0 \pmod{r}$. This shows that both $au + bv$ and $av - bu$ are divisible by r, so we obtain the identity

$$\left(\frac{au + bv}{r}\right)^2 + \left(\frac{av - bu}{r}\right)^2 = sp.$$

Thus we have written a smaller multiple of p as a sum of two squares, so the theorem is proven. □

Exercises

Starter Exercises

17.1 For every prime $p \equiv 1 \pmod 4$ below 100, write p as a sum of two squares.

17.2 Show that no odd prime p can be written as a sum of two cubes.

Routine-Building Exercises

17.3 Show that a natural number n can be written as the sum of two triangular numbers if and only if $8n + 2$ can be written as the sum of two squares. Hint: Use one of the identities stated in Exercise 2.6.

Chapter 18

The Gaussian Integers

18.1 Definition and Basic Properties of the Gaussian Integers

Definition 18.1.1. A **Gaussian integer** is an expression of the form

$$a + bi$$

in which a and b are integers. We say that the **real part** of $a + bi$ is the integer a, and the **complex part** of $a + bi$ is the integer b.

We will write $\mathbb{Z}[i]$ for the set of Gaussian integers. Gaussian integers are added, subtracted, and multiplied according to the following rules:

$$(a + ib) + (c + id) = (a + c) + i(b + d)$$
$$(a + ib) - (c + id) = (a - c) + i(b - d)$$
$$(a + ib)(c + id) = (ac - bd) + i(ad + bc).$$

Definition 18.1.2. The **norm** of a Gaussian integer $\alpha = a + bi$ is given by

$$N(\alpha) = a^2 + b^2.$$

Proposition 18.1.3 (The Brahmagupta–Fibonacci identity). *The norm function N is completely multiplicative in the sense that*

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

for any two Gaussian integers α and β.



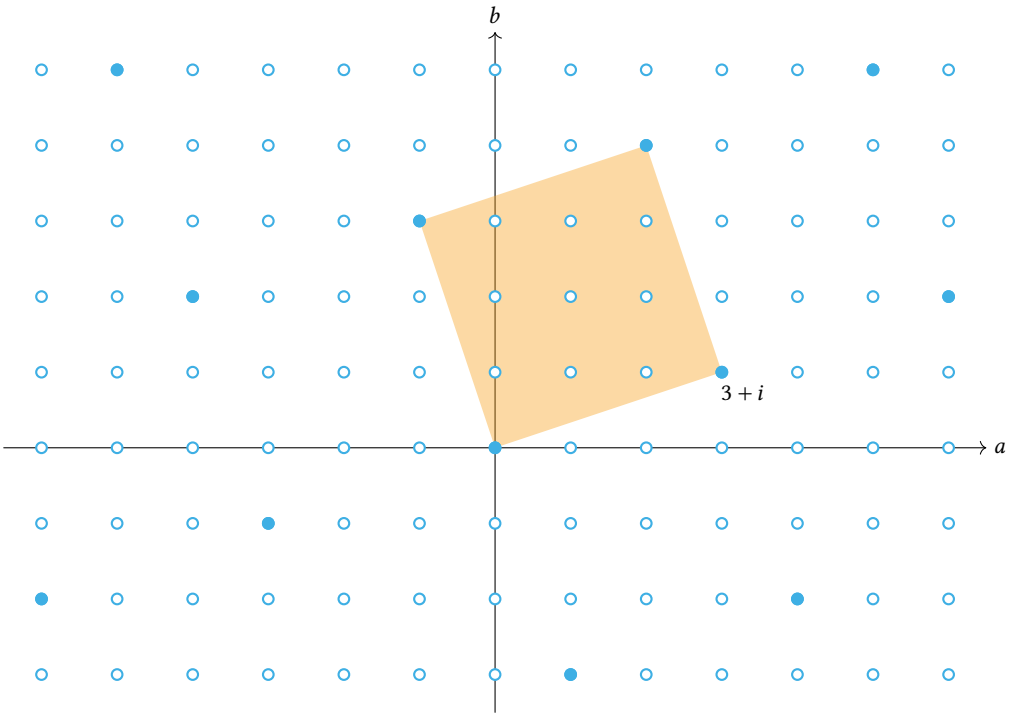


Figure 18.1: The set of Gaussian integers. All the multiples of $3 + i$ are marked with solid dots, and all the nonmultiples are marked with open dots. The norm of $3 + i$ is the area of the square shaded in orange.

DEFINITION 18.1.4. A Gaussian integer α is said to **divide** a Gaussian integer β if there exists a Gaussian integer κ such that

$$\kappa\alpha = \beta.$$

Any Gaussian integer dividing 1 is called a **unit**.

THEOREM 18.1.5. *The only units among the Gaussian integers are* ± 1 *and* $\pm i$.

18.2 Euclidean Division of Gaussian Integers

EXAMPLE 18.2.1. The following choices of α and β show that there can be multiple pairs of Gaussian integers κ and ρ with $N(\rho) < N(\beta)$ such that

$$\alpha = \kappa\beta + \rho.$$

(i) Consider $\alpha := 8 + 11i$ and $\beta = 3 + i$, so that $N(\beta) = 10$. Then

$$\frac{\alpha}{\beta} = \frac{(8+11i)(3-i)}{3^2+1^2} = \frac{35+25i}{10} = (3+2i) + \frac{1+i}{2}.$$

This shows that $\alpha = (3+2i)\beta + (1+2i)$. Note that $N(1+2i) = 5 < 10$. However, we can also write

$$\begin{aligned} \alpha &= (4+2i)\beta + (-2+i), & N(-2+i) &= 5, \\ \alpha &= (3+3i)\beta + (2-i), & N(2-i) &= 5, \\ \alpha &= (4+3i)\beta + (-2-i), & N(-2-i) &= 5. \end{aligned}$$

(ii) Consider $\alpha := 2 + 3i$ and $\beta = 4$, so that $N(\beta) = 16$. Then we can write

$$\begin{aligned} \alpha &= i\beta + (2-i), & N(2-i) &= 5, \\ \alpha &= (1+i)\beta + (-2-i), & N(-2-i) &= 5. \end{aligned}$$

Define the half-open fundamental square to be the following subset of $\mathbb{C}$:

$$\mathcal{S} := \{x + yi \in \mathbb{C} \mid -\tfrac{1}{2} < x, y \leq \tfrac{1}{2}\}.$$

Theorem 18.2.2. *Consider two Gaussian integers α and β with $N(\alpha) > N(\beta)$. Then there exist unique Gaussian integers κ and ρ with $N(\rho) < N(\beta)$, such that*

$$\alpha = \kappa\beta + \rho$$

and $\frac{\rho}{\beta} \in \mathcal{S}$.

18.3 The Greatest Common Divisor of Gaussian Integers

The definition of a greatest common divisor carries over directly from the integers to the Gaussian integers.

Definition 18.3.1. Consider two Gaussian integers α and β. A Gaussian integer δ is said to be the **greatest common divisor** of α and β if it satisfies the following logical equivalence for every Gaussian integer ξ:

$$(\xi \mid \alpha) \wedge (\xi \mid \beta) \Leftrightarrow (\xi \mid \delta).$$

18.4 Primes in the Gaussian Integers

18.5 Fermat's Two-Square Theorem

18.6 The Biquadratic Character of -1



Exercises

Challenge Exercises

18.1 (a) Consider a Gaussian integer $\alpha = a+bi$ such that $\gcd(a, b) = 1$. Show that the number of Gaussian integers in the interior (that is, not on the boundary) of the square spanned by the Gaussian integers 0, α, $i\alpha$, and $(1+i)\alpha$ is $N(\alpha)-1$. See Figure 18.1 for such a square with $\alpha = 3 + i$.

(b) For any Gaussian integer $\alpha = a + bi$, determine the number of Gaussian integers in the interior of the square spanned by the Gaussian integers 0, α, $i\alpha$, and $(1 + i)\alpha$.

Chapter 19

Strong Divisibility Sequences

19.1 Lucas Sequences

The French mathematician Édouard Lucas observed that the familiar Fibonacci sequence was just a single instance of a larger family of recursively defined sequences that all share similar properties.

Definition 19.1.1. Consider two integers a and b. The **Lucas sequence** u_n at a and b is defined by

$$u_0 := 0, \qquad u_1 := 1, \qquad \text{and} \qquad u_{n+2} := au_{n+1} - bu_n.$$

If the parameters a and b are not clear from the context, we will write $u(a,b)_n$ for u_n. When a and b are relatively prime, we say that the Lucas sequence (u_n) is **reduced**.

Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = au_{n+1} - bu_n$. The **characteristic polynomial** of this Lucas sequence is the polynomial

$$x^2 - ax + b,$$

and its **characteristic form** is the binary quadratic form

$$x^2 - axy + y^2.$$

The roots $\alpha := \frac{a+\sqrt{a^2-4b}}{2}$ and $\beta := \frac{a-\sqrt{a^2-4b}}{2}$ of the characteristic polynomial are called the **characteristic roots**. By the Vieta relations, the characteristic roots satisfy the identites

$$\alpha + \beta = a \qquad \text{and} \qquad \alpha\beta = b.$$



EXAMPLE 19.1.2. Some special cases of Lucas sequences are famous:

(i) When $a = 1$ and $b = -1$, then the sequence (u_n) is the Fibonacci sequence

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

The characteristic polynomial of the Fibonacci sequence is $x^2 - x - 1$ and its characteristic roots are

$$\alpha = \frac{1+\sqrt{5}}{2} \qquad \text{and} \qquad \beta = \frac{1-\sqrt{5}}{2}.$$

(ii) When $a = 2$ and $b = -1$, then the sequence (u_n) is the **Pell sequence**

$$0, 1, 2, 5, 12, 29, 70, 169, 408, 985, \ldots$$

The characteristic polynomial of the Pell sequence is $x^2 - 2x - 1$ and its characteristic roots are

$$\alpha = 1 + \sqrt{2} \qquad \text{and} \qquad \beta = 1 - \sqrt{2}.$$

(iii) In Exercise 14.3 we saw that the sequence (M_n) of Mersenne numbers satisfies the recurrence

$$M_{n+2} = 3M_{n+1} - 2M_n.$$

Thus, the Mersenne numbers also form an example of a Lucas sequence. The characteristic polynomial of the Mersenne numbers is $x^2 - 3x + 4$ and its characteristic roots are

$$\alpha = 4 \qquad \text{and} \qquad \beta = -1.$$

(iv) More generally, for any two distinct integers a and b, the sequence defined by

$$u_n := \frac{a^n - b^n}{a - b}$$

is a Lucas sequence satisfying

$$u_0 = 0, \qquad u_1 = 1, \qquad \text{and} \qquad u_{n+2} = (a+b)u_{n+1} + abu_n.$$

(v) The Lucas sequence (u_n) given by

$$u_0 = 0, \qquad u_1 = 1, \qquad \text{and} \qquad u_{n+2} = 2u_{n+1} - u_n$$

is the sequence of nonnegative integers: For each $n \geq 0$ we have $u_n = n$.

In the following theorem we establish two fundamental identities for a Lucas sequence.

Theorem 19.1.3. *Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = au_{n+1} - bu_n$ and characteristic roots α and β. Then we have the identities*

$$u_{n+1} - \alpha u_n = \beta^n \qquad \text{and} \qquad u_{n+1} - \beta u_n = \alpha^n.$$

Proof. We prove the first identity by induction on n. The second identity can be proven similarly. For the base case, we note that $u_1 - \alpha u_0 = 1 = \beta^0$. For the inductive step, we use that $a = \alpha + \beta$ and $b = \alpha\beta$ to compute

$$u_{n+2} - \alpha u_{n+1} = au_{n+1} - bu_n = (\alpha+\beta)u_{n+1} - \alpha\beta u_n - \alpha u_{n+1} = \beta(u_{n+1} - \alpha u_n) = \beta^{n+1}. \qquad \square$$

Theorem 19.1.4 (Binet's Formula). *Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = au_{n+1} - bu_n$ and characteristic roots α and β. Then α and β are distinct, and*

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Proof. By the identities $u_{n+1} - \alpha u_n = \beta^n$ and $u_{n+1} - \beta u_n = \alpha^n$ established in Theorem 19.1.3, it follows that

$$(\alpha - \beta)u_n = (u_{n+1} - \beta u_n) - (u_{n+1} - \alpha u_n) = \alpha^n - \beta^n. \qquad \square$$

Binet's formula can be used to show that if $m \mid n$, then $u_m \mid u_n$. Sequences with this property are called *divisibility sequences*. We will additionally assume that divisibility sequences (a_n) satisfy $a_0 = 0$ and $a_1 = 1$. Such divisibility sequences are sometimes called *normalized*.

Definition 19.1.5. An integer sequence (a_n) is said to be a **divisibility sequence** if $a_0 = 0$, $a_1 = 1$, and it preserves the divisibility relation, meaning that it satisfies the condition

$$m \mid n \Rightarrow a_m \mid a_n$$

for all m and n.

Theorem 19.1.6. *Consider two integers a and b such that $a^2 - 4b \neq 0$. Then the Lucas sequence (u_n) at a and b is a divisibility sequence.*

Proof. Suppose that $n = km$. Then we have

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{(\alpha^m - \beta^m)\sum_{i=0}^{k}(\alpha^m)^i(\beta^m)^{k-i}}{\alpha - \beta} = u_m \sum_{i=0}^{k}(\alpha^m)^i(\beta^m)^{k-i}$$

by the formula for the difference of mth powers. This shows that if $m \mid n$, then $u_m \mid u_n$. $\square$

When the parameters a and b in the recursive law of a Lucas sequence (u_n) are relatively prime, the Lucas sequence has the further property of preserving greatest common divisors. Divisibility sequences that preserve greatest common divisors are called *strong divisibility sequences*.



DEFINITION 19.1.7. A divisibility sequence (a_n) is said to be a **strong divisibility sequence** if (a_n) preserves greatest common divisors, meaning that it satisfies the equation

$$a_{\gcd(m,n)} = \gcd(a_m, a_n)$$

for all m and n.

Our first target is to prove an addition formula for Lucas sequences. This law generalizes the addition formula for the Fibonacci numbers, which we stated in Exercise 6.12.

PROPOSITION 19.1.8 (Addition formula for Lucas sequences). *For any two natural numbers m and n, we have*

$$u_{m+n+1} = u_{m+1}u_{n+1} - bu_mu_n$$

INDUCTIVE PROOF. The proof is by induction on n. In the base case, we calculate

$$u_{m+1} = u_{m+1} \cdot 1 - 0 = u_{m+1}u_1 - bu_mu_0.$$

For the inductive step, assume that the identity $u_{m+n+1} = u_{m+1}u_{n+1} - bu_mu_n$ holds for all m. Then we calculate

$$\begin{aligned} u_{m+1}u_{n+2} - bu_mu_{n+1} &= u_{m+1}(au_{n+1} - bu_n) - bu_mu_{n+1} \\ &= (au_{m+1} - bu_m)u_{n+1} - bu_{m+1}u_n \\ &= u_{m+2}u_{n+1} - bu_{m+1}u_n \\ &= u_{(m+1)+n+1} \\ &= u_{m+n+2}. \end{aligned}$$

□

We give a second proof of the addition law, making use of the fundamental identities stated in Theorem 19.1.3. Even though our previous inductive proof is perfectly legitimate, our second proof illustrates something important: Numbers of the form $x + \alpha y$ form their own domain of arithmetic. We will address this point more fully when we study quadratic fields.

PROOF BY THE FUNDAMENTAL IDENTITIES. In this proof, we will assume that α and β are distinct, or equivalently, that $a^2 - 4b \neq 0$.

Given the identity $u_{n+1} - \beta u_n = \alpha^n$ established in Theorem 19.1.3, it follows that

$$\alpha^{m+n} = \alpha^m\alpha^n = (u_{m+1} - \beta u_m)(u_{n+1} - \beta u_n) = u_{m+1}u_{n+1} - \beta(u_mu_{n+1} + u_{m+1}u_n) + \beta^2 u_mu_n.$$

Since β is a root of the equation $x^2 - ax + b$, it follows that $\beta^2 = a\beta - b$. This implies that

$$\alpha^{m+n} = u_{m+1}u_{n+1} - bu_mu_n - \beta(u_mu_{n+1} + u_{m+1}u_n - au_mu_n).$$

Similarly, using the identity $u_{n+1} - \alpha u_n = \beta^n$, we find that

$$\beta^{m+n} = u_{m+1}u_{n+1} - bu_mu_n - \alpha(u_mu_{n+1} + u_{m+1}u_n - au_mu_n).$$

Combining these equations, it follows that

$$u_{m+n} = \frac{\alpha^{m+n} - \beta^{m+n}}{\alpha - \beta} = u_m u_{n+1} + u_{m+1} u_n - a u_m u_n.$$

Using this expression for u_{m+n} in our earlier identity for α^{m+n}, we find that

$$\alpha^{m+n} = u_{m+1} u_{n+1} - b u_m u_n - \beta u_{m+n}.$$

On the other hand, we have $\alpha^{m+n} = u_{m+n+1} - \beta u_{m+n}$. Combining these identities gives us

$$u_{m+n+1} = u_{m+1} u_{n+1} - b u_m u_n.$$ □

Corollary 19.1.9. *For any Lucas sequence (u_n) with recurrence relation $u_{n+2} = a u_{n+1} - b u_n$ we have the identities*

$$u_{2n+1} = u_{n+1}^2 - b u_n^2 \qquad \text{and} \qquad u_{2n+2} = u_{n+1}(u_{n+2} - b u_n).$$

Proposition 19.1.10 (Cassini's identity). *Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = a u_{n+1} - b u_n$. Then we have*

$$u_{n+2} u_n - u_{n+1}^2 = -b^n.$$

Proof. The proof is by induction on n. In the base case, we have

$$u_2 u_0 - u_1^2 = -1.$$

For the inductive step, we have

$$\begin{aligned} u_{n+3} u_{n+1} - u_{n+2}^2 &= (a u_{n+2} - b u_{n+1}) u_{n+1} - (a u_{n+1} - b u_n) u_{n+2} \\ &= b u_{n+2} u_n - b u_{n+1}^2 \\ &= b(u_{n+2} u_n - u_{n+1}^2) \\ &= -b^{n+1}. \end{aligned}$$ □

Corollary 19.1.11. *Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = a u_{n+1} - b u_n$. Then any two consecutive terms u_n and u_{n+1} are relatively prime.*

Proof. By Proposition 19.1.10 (Cassini's identity) it follows that $\gcd(u_n, u_{n+1})$ divides b^n. However, modulo b we see that (u_n) satisfies the recurrence

$$u_{n+2} \equiv a u_{n+1} \pmod{b}.$$

Since $u_1 = 1$ and a is invertible modulo b, it follows that u_n is relatively prime to b for every n. Thus we conclude that $\gcd(u_n, u_{n+1}) = 1$. □

Theorem 19.1.12. *Consider the Lucas sequence (u_n) with recurrence $u_{n+2} = a u_{n+1} - b u_n$. If a and b are relatively prime, then (u_n) is a strong divisibility sequence.*

PROOF. First, we show that if $n = qm + r$ with $0 \leq r < m$, then

$$\gcd(u_n, u_m) = \gcd(u_m, u_r).$$

The identity $n = qm + r$ implies that

$$u_n = u_{qm+1}u_r - bu_{qm}u_{r-1}$$

Since $u_m \mid u_{qm}$, it follows that $u_n \equiv u_{qm+1}u_r \pmod{u_m}$. However, u_{qm+1} is relatively prime to u_{qm} and hence to u_m. Thus, any common divisor d of u_n and u_m must also be a divisor of u_r. This shows that

$$\gcd(u_n, u_m) \mid \gcd(u_m, u_r).$$

On the other hand, we see that u_n can be written as a linear combination of u_m and u_r, so that $\gcd(u_n, u_m) \mid u_n$. This implies that

$$\gcd(u_m, u_r) \mid \gcd(u_n, u_m).$$

□

EXAMPLE 19.1.13. There are many examples of strong divisibility sequences beyond the class of Lucas sequences. A particularly self-evident example is the sequence

$$u_n := n^2.$$

To see that this is not a Lucas sequence, we show that the equations

$$4 = a \cdot 1 - b \cdot 0$$
$$9 = a \cdot 4 - b \cdot 1$$
$$16 = a \cdot 9 - b \cdot 4$$

has no solutions. The first equation implies that $a = 4$. Given this constraint, the second equation gives that $b = 7$. However, $4 \cdot 9 - 7 \cdot 4 = 8 \neq 16$. Thus we conclude that the sequence (n^2) is not a Lucas sequence for any choice of integers a and b.

An important further class of strong divisibility sequences is the class of *elliptic divisibility sequences* of Morgan Ward [WAR1948].

19.2 The Rank of Apparition

EXAMPLE 19.2.1.

(i) When we look at the Fibonacci sequence modulo a prime p, we see clear patterns emerging:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F_n \pmod 2$	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0
$F_n \pmod 3$	0	1	1	2	0	2	2	1	0	1	1	2	0	2	2	1
$F_n \pmod 5$	0	1	1	2	3	0	3	3	1	4	0	4	4	3	2	0
$F_n \pmod 7$	0	1	1	2	3	5	1	6	0	6	6	5	4	2	6	1

(ii) When we look at the Pell sequence modulo a prime p, we again see clear patterns emerging:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_n \pmod 2$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$P_n \pmod 3$	0	1	2	2	0	2	1	1	0	1	2	2	0	2	1	1
$P_n \pmod 5$	0	1	2	0	2	4	0	4	3	0	3	1	0	1	2	0
$P_n \pmod 7$	0	1	2	5	5	1	0	1	2	5	5	1	0	1	2	5

(iii) When we look at the Mersenne numbers modulo a prime p, we obtain the following:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$M_n \pmod 2$	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$M_n \pmod 3$	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$M_n \pmod 5$	0	1	3	2	0	1	3	2	0	1	3	2	0	1	3	2
$M_n \pmod 7$	0	1	3	0	1	3	0	1	3	0	1	3	0	1	3	0

Definition 19.2.2. Consider an integer sequence (a_n) and a positive integer m. The **rank of apparition** $\rho_a(m)$ of m is the least positive integer n such that $m \mid a_n$.

Theorem 19.2.3 (Rank of Apparition Theorem). *Suppose that $f : \mathbb{N} \to \mathbb{N}$ is a divisibility sequence. Then the following are equivalent:*

(i) *There is a function $g : \mathbb{N} \to \mathbb{N}$ satisfying the logical equivalence*

$$g(m) \mid n \quad \Leftrightarrow \quad m \mid f(n).$$

(ii) *The divisibility sequence f is a strong divisibility sequence.*

If the first condition holds, then the function g is equal to the rank of apparition function; that is, $g(m) = \rho_f(m)$ for every natural number m.

Proof. Suppose first that there exists a function g satisfying the logical equivalence

$$g(m) \mid n \quad \Leftrightarrow \quad m \mid f(n).$$



Then it follows that

$$\begin{aligned} d \mid f(\gcd(m,n)) &\Leftrightarrow g(d) \mid \gcd(m,n) \\ &\Leftrightarrow g(d) \mid m \wedge g(d) \mid n \\ &\Leftrightarrow d \mid f(m) \wedge d \mid f(n) \\ &\Leftrightarrow d \mid \gcd(f(m), f(n)). \end{aligned}$$

Since $f(\gcd(m,n))$ and $\gcd(f(m), f(n))$ have the exact same set of divisors, they must be equal.

For the converse, suppose that $f(0) = 0$ and that f preserves greatest common divisors. More generally, we will have for any finite list of natural numbers

$$f(\gcd_i(n_i)) = \gcd_i(f(n_i)).$$

Here, the expression $gcd_i(n_i)$ means that the greatest common divisor is taken over all the numbers n_i in the list. Now consider for any natural number m the ideal

$$I_m := \left\{ k_1 n_1 + \cdots + k_r n_r \,\middle|\, m \mid f(n_i) \text{ for all } i \right\}$$

and define the function g by letting $g(m)$ be the unique natural number such that $I_m = (g(m))$.

To see that g is a divisibility sequence, suppose that $m \mid m'$. Then any linear combination of natural numbers n such that $m' \mid f(n)$ is also a linear combination of natural numbers n such that $m \mid f(n)$. In particular $g(m')$ is in the ideal $(g(m))$, which means that $g(m) \mid g(m')$.

We claim that the function g satisfies the logical equivalence

$$g(m) \mid n \quad \Leftrightarrow \quad m \mid f(n).$$

If $m \mid f(n)$, then it follows that $n \in I_m$ so that $g(m) \mid n$. This proves the reverse direction.

For the forward direction, suppose that $g(m) \mid n$. Then it also follows that $n \in I_m$, so that we can write

$$n = \sum_i k_i n_i$$

for some finite list of natural numbers n_i satisfying $m \mid f(n_i)$. By the assumption that $m \mid f(n_i)$, it follows that $m \mid \gcd_i(f(n_i))$. Furthermore, since $\gcd_i(n_i) \mid n$ it follows that

$$f(\gcd_i(n_i)) \mid f(n).$$

Combined with the fact that $m \mid \gcd_i(f(n_i))$ and the assumption that f preserves greatest common divisors, we conclude that

$$m \mid f(n).$$

□

By Theorem 8.5.2 (Order Theorem), it follows that the function g defined by $g(m) := \mathrm{ord}_m(a)$ satisfies the logical equivalence in the first condition of Theorem 19.2.3 (Rank of Apparition Theorem). Thus we obtain the following corollary:

Corollary 19.2.4. *The function $n \mapsto a^n - 1$ is a strong divisibility sequence. Thus, for any integer $a > 1$ and any two natural numbers m and n we have*

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1.$$

Proof. Note that the function $k \mapsto a^k - 1$ is a divisibility sequence, since for $qm = n$ we have the identity

$$a^n - 1 = (a^m)^q - 1^q = (a^m - 1) \sum_{k=0}^{q-1} a^{km}$$

by the formula for the difference of qth powers (Exercise 2.5). The fact that it is a strong divisibility sequence now follows directly from Theorem 19.2.3 and Theorem 8.5.2 (Order Theorem). □

Example 19.2.5. Consider two relatively prime integers a and b with $b < a$, and consider the Lucas sequence (u_n) with recurrence $u_{n+2} = (a + b)u_{n+1} - abu_n$. By Binet's formula, we have

$$u_n = \frac{a^n - b^n}{a - b}.$$

By the assumption that a and b are relatively prime it follows that the sequence u_n is a strong divisiblity sequence. Thus, the rank-of-apparition function ρ satisfies

$$\rho(m) \mid n \quad \Leftrightarrow \quad m \mid u_n.$$

We make a more detailed analysis of the rank of apparition of a prime, depending on whether it divides $a - b$, a, b, or none of these numbers.

First, we will assume that $p \nmid ab(a - b)$. In this case, we have

$$p \mid u_n \Leftrightarrow p \mid a^n - b^n \Leftrightarrow a^n \equiv b^n \pmod{p}.$$

Since a and b are invertible modulo p, it follows that $(a/b)^n \equiv 1 \pmod{p}$, which is equivalent to the condition that $\mathrm{ord}_p(a/b) \mid n$. Thus, we conclude that

$$\mathrm{ord}_p(a/b) \mid n \quad \Leftrightarrow \quad p \mid u_n.$$

It follows that $\rho(p) = \mathrm{ord}_p(a/b)$. We can extend these observation to moduli m with $\gcd(m, ab(a - b)) = 1$. Here again, a and b are invertible modulo m, from which it follows that

$$p \mid u_n \Leftrightarrow a^n \equiv b^n \pmod{p} \Leftrightarrow \mathrm{ord}_m(a/b) \mid n.$$

Thus we find that $\rho(m) = \mathrm{ord}_m(a/b)$. Moreover, one can show that

$$\rho(m_1 m_2) = \mathrm{lcm}(\rho(m_1), \rho(m_2))$$



when m_1 and m_2 are relatively prime integers, both relatively prime to $ab(a-b)$.

Next, we will assume that $p \mid a-b$. Since $a-b$ is relatively prime to both a and b, it follows again that both a and b are invertible modulo p. Then we can rewrite u_n using the formula for the difference of nth powers, and subsequently use the congruence $a \equiv b \pmod{p}$ to obtain:

$$u_n = \frac{a^n - b^n}{a-b} = \sum_{k=0}^{n-1} a^{n-1-k}b^k \equiv \sum_{k=0}^{n-1} a^{n-1-k}a^k = na^{n-1} \pmod{p}.$$

Given that $p \nmid a$, it follows that

$$p \mid n \quad \Leftrightarrow \quad p \mid u_n.$$

In other words, the rank of apparition of p is $\rho(p) = p$.

Finally, we show that $\rho(p) = 0$ when $p \mid a$ and $p \nmid b(a-b)$, from which we also obtain that $\rho(p) = 0$ in the symmetric case where $p \mid b$ and $p \nmid a(a-b)$. Recall that $\rho(p) = 0$ means that $p \nmid u_n$ for all $n > 1$. Note that if $p \mid a$, then we have

$$u_n \equiv b^{n-1} \pmod{p}$$

whenever $n \geq 1$. Since we assumed that $p \nmid b$, this shows that $p \nmid u_n$.

REMARK 19.2.6. More generally, if $(P, \leq_P)$ and $(Q, \leq_Q)$ are two posets, a **Galois connection** between P and Q consists of order preserving maps $f : P \to Q$ and $g : Q \to P$ satisfying the logical equivalence

$$g(x) \leq_P y \quad \Leftrightarrow \quad x \leq_Q f(y)$$

for any $x \in Q$ and $y \in P$. In this case, the map f is said to be the **upper adjoint**, and the map g is said to be the **lower adjoint** of the Galois connection. Thus we have proven in this section that the function $n \mapsto a^n - 1$ is the upper adjoint of a Galois connection, and we have used this fact to show that f preserves greatest common divisors. Theorem 19.2.3 generalizes to the setting of arbitrary posets, and indeed, some readers may recognize it as a special case of the *Adjoint Functor Theorem*.

Another famous Galois connection on the natural numbers ordered by divisibility is the Fibonacci sequence. We will give the full statement of this fact in the exercises.

19.3 Primitive Sequences

DEFINITION 19.3.1. Consider a divisibility sequence $n \mapsto a_n$ indexed by the natural numbers, with $a_1 = 1$. The **primitive sequence** of a_n is the sequence (u_n) of rational numbers defined by

$$u_n := \prod_{d \mid n} a_d^{\mu(n/d)}.$$

THEOREM 19.3.2. *The primitive sequence (u_n) of a divisibility sequence (a_n) satisfies the identity*

$$a_n = \prod_{d|n} u_d.$$

PROOF. By interchanging the product, we find that

$$\prod_{e|n}\prod_{d|e} a_d^{\mu(e/d)} = \prod_{d|n}\prod_{c|\frac{n}{d}} a_d^{\mu(c)} = \prod_{d|n} a_d^{\sum_{c|\frac{n}{d}}\mu(c)} = \prod_{d|n} a_d^{\varepsilon(n/d)} = a_n. \qquad \square$$

19.4 LCM-sequences

DEFINITION 19.4.1. The **lcm-sequence** (m_n) of an integer sequence (a_n) is given by $m_1 := 1$ and

$$m_n := \frac{\operatorname{lcm}(a_1, \dots, a_n)}{\operatorname{lcm}(a_1, \dots, a_{n-1})} \qquad \text{for } n \geq 2.$$

THEOREM 19.4.2. *Consider a divisibility sequence (a_n) indexed by the natural numbers, with $a_1 = 1$. Then the following are equivalent:*

(i) *The sequence (a_n) is a strong divisibility sequence; that is,*

$$a_{\gcd(m,n)} = \gcd(a_m, a_n)$$

for every m and n.

(ii) [WAR1936] *For each prime p, we have $p^k \mid a_n$ if and only if $\rho_k(p) \mid n$, where $\rho_k(p)$ is the rank of apparition of p^k.*

(iii) *Each u_n in the primitive sequence (u_n) of (a_n) is an integer, and furthermore u_m and u_n are relatively prime when $m \nmid n$ and $n \nmid m$.*

(iv) [NOW2015] *The sequence (a_n) satisfies the following divisor-product formula, where (m_n) is the lcm-sequence of (a_n):*

$$a_n = \prod_{d|n} m_d.$$

The following corollary, due to Morgan Ward [WAR1936], is a generalization of a theorem of Édouard Lucas [LUC1878a].

COROLLARY 19.4.3. *If (a_n) is a strong divisibility sequence, then*

$$\prod_{i=1}^{k} a_i \,\Big|\, \prod_{i=n+1}^{n+k} a_i.$$

19.5 The Lifting the Exponent Lemma

For the following lemma, recall that $v_p(a-b) = m$ if and only if $a \equiv b \pmod{p^m}$ but $a \not\equiv b \pmod{p^{m+1}}$. We also recall that for any prime p and any $0 < i < p$, the binomial coefficient $\binom{p}{i}$ is divisible by p.

LEMMA 19.5.1. *Consider an odd prime p, and two integers $a \equiv b \pmod{p}$ such that neither a nor b is divisible by p. Then*

$$v_p(a^p - b^p) = v_p(a-b) + 1.$$

PROOF. Write $s := v_p(a-b)$, so that $s \geq 1$ by the assumption that $a \equiv b \pmod{p}$. Then we have $a \equiv b \pmod{p^s}$, so we can write $b = a + tp^s$, where $p \nmid t$. The value of b^p can therefore be computed using Theorem 3.5.1 (The Binomial Theorem) by

$$b^p = (a+tp^s)^p = \sum_{i=0}^{p} \binom{p}{i} a^i (tp^s)^{p-i} \equiv a^p + a^{p-1}tp^{s+1} \pmod{p^{s+2}}.$$

Since neither a nor t is divisible by p, it follows that $a^p \not\equiv b^p \pmod{p^{s+2}}$. On the other hand, we see from the binomial expansion of b^p that $a^p \equiv b^p \pmod{p^{s+1}}$. Therefore we conclude that

$$v_p(a^p - b^p) = s + 1. \qquad \square$$

The previous lemma can be iterated to obtain a general lemma called the *Lifting the Exponent Lemma*. This lemma was popularized by the Romanian mathematician Mihai Manea [MAN2006].

THEOREM 19.5.2 (Lifting the Exponent). *Consider an odd prime p, and let $x \equiv y \pmod{p}$, where neither x nor y is divisible by p. Then for any natural number $n \geq 1$, we have*

$$v_p(x^n - y^n) = v_p(x-y) + v_p(n).$$

PROOF. Write $n = p^k m$ with $p \nmid m$, so that $v_p(n) = k$, and write $s = v_p(x-y)$. Since we have assumed that $x \equiv y \pmod{p}$, we have $s \geq 1$. We will prove the claim by induction on k.

In the base case, where $k = 0$, the claim is simply that

$$v_p(x^m - y^m) = s.$$

To see this, write $y = x + tp^s$, where $p \nmid t$. Then we have

$$y^m = (x+tp^s)^m \equiv x^m + mx^{m-1}tp^s \pmod{p^{s+1}}.$$

Now observe that m, x, and t are not divisible by p by assumption, so it follows that $mx^{m-1}t$ is not divisible by p. This implies that $y^m \not\equiv x^m \pmod{p^{s+1}}$. On the other hand, the congruence $x \equiv y \pmod{p^s}$ clearly implies that $x^m \equiv y^m \pmod{p^s}$, so we conclude that

$$v_p(x^m - y^m) = s.$$

The inductive step is a direct consequence of Lemma 19.5.1. $\square$

Example 19.5.3. In Example 19.2.5 we saw that for $p \mid a - b$ with a and b relatively prime, the rank of apparition of p in the Lucas sequence given by

$$u_n = \frac{a^n - b^n}{a - b}$$

is $\rho(p) = p$. Now we claim that $\rho(p^k) = p^k$. Using Theorem 19.5.2 (Lifting the Exponent), we see that

$$v_p(u_n) = v_p(a^n - b^n) - v_p(a - b) = v_p(n).$$

This shows that $p^k \mid u_n$ if and only if $p^k \mid n$, and the claim follows.

Definition 19.5.4. A strong divisibility sequence is said to satisfy the **law of repetition** if for any prime p, we have

$$v_p(a_{n\rho_a(p)}) = v_p(a_{\rho_a(p)}) + v_p(n).$$

Theorem 19.5.5. *Consider a strong divisibility sequence (a_n), such that for each prime p we have*

$$\rho_a(p^k) = \rho_a(p)p^{k-1}.$$

Then (a_n) satisfies the law of repetition.

Example 19.5.6. For any two relatively prime integers a and b, the sequence

$$(a^n - b^n)$$

satisfies the law of repetition.

Example 19.5.7. Any Lucas sequence satisfies the law of repetition.



Exercises

Starter Exercises

19.1 Show that consecutive terms of a Lucas sequence (u_n) with characteristic form $x^2 - axy + by^2$ satisfy

$$u_{n+1}^2 - au_{n+1}u_n + bu_n^2 = b^n.$$

Routine-Building Exercises

19.2 Show that

$$\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(m,n)} - b^{\gcd(m,n)}.$$

19.3 Consider a positive integer a, and write $S_m := \sum_{k=0}^{m} a^k$. Prove that

$$\gcd(S_m, S_n) = S_{\gcd(m+1,n+1)-1}.$$

19.4 Consider a Lucas sequence (u_n) with recursion $u_{n+2} = au_{n+1} - bu_n$. Show that

$$u_{n+1}^2 \equiv b^n \pmod{u_n}.$$

19.5 Consider a Lucas sequence (u_n) and let m be such that $u_m \neq 0$. Define the **cofactor sequence** $(\tilde{u}_k)$ by

$$\tilde{u}_k := u_{km}/u_m.$$

Show that $(\tilde{u}_k)$ is again a Lucas sequence.

Challenge Exercises

19.6 Show that for any odd prime p the following congruence holds:

$$\prod_{k=1}^{p-1} L_k \equiv F_{p+1}^{\frac{p-1}{2}} \pmod{F_p}$$

19.7 (a) Show that the function $(x, y) \mapsto (y, x + y)$ is a bijection on the set of pairs of elements $x, y \in \mathbb{Z}/n\mathbb{Z}$.

(b) Show that for any m, the Fibonacci sequence is periodic modulo m. Its period is called the **Pisano period**.

(c) Show that for any natural number m, there is a least positive number n such that

$$m \mid F_n.$$

We will call this number G_m. By virtue of its duality to the Fibonacci sequence, we will call the sequence G the **cofibonacci sequence**.

(d) Show that $G(m)$ satisfies the following logical equivalence

$$G_m \mid n \quad \Leftrightarrow \quad m \mid F_n.$$

Conclude that the Fibonacci sequence is a strong divisibility sequence.

19.8 Use methods similar to the previous exercise to show that the sequence of Pell numbers P_n, which are defined by

$$P_0 := 0, \qquad P_1 := 1, \qquad \text{and} \qquad P_{n+2} = 2P_{n+1} + P_n,$$

forms a strong divisibility sequence.

19.9 Define a **Mersenne integer** to be any integer that can be written in the form

$$\frac{M_{i_1} \cdots M_{i_m}}{M_{j_1} \cdots M_{j_n}}.$$

Show that the number 23 is not a Mersenne integer.

19.10 Define a **Fibonacci integer** to be any integer that can be written in the form

$$\frac{F_{i_1} \cdots F_{i_m}}{F_{j_1} \cdots F_{j_n}}.$$

Show that the number 37 is not a Fibonacci integer [LP2003].

19.11 (The Dickson–Lucas polynomial) Consider a Lucas sequence (u_n) with associated sequence (v_n) given by

$$v_0 := 2, \qquad v_1 := a, \qquad \text{and} \qquad v_{n+2} = av_{n+1} - bv_n.$$

Show that

$$v_m = \sum_{j=0}^{\lfloor m/2 \rfloor} (-1)^j \frac{m}{m-j} \binom{m-j}{j} a^{m-2j} b^j.$$



Chapter 20

Polynomials

20.1 Polynomials with Abstract Coefficients

Definition 20.1.1. A **polynomial** in one variable x is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

in which we require that the **leading coefficient** a_n is nonzero, unless $n = 0$. A polynomial $f(x)$ as above with leading coefficient a_n is said to be of **degree** n. The numbers a_k are called the **coefficients** of $f(x)$. The **zero polynomial** is the constant polynomial $f(x) = 0$.

The coefficients of a polynomial may be taken from any number system. When we wish to specify that the coefficients are integers, rational, or real numbers, we speak of **polynomials with integer coefficients**, **polynomials with rational coefficients**, or **polynomials with real coefficients**. Other number systems from which we will occasionally take coefficients include the rings $\mathbb{Z}/n$ of modular arithmetic. Since there is such a large variety of number systems which will eventually play a role one way or another in number theory, it will be useful to us to develop methods general enough so as to cover all these cases at once.



DEFINITION 20.1.2. A **commutative ring** is a set R equipped with constants 0 and 1 and operations + for addition, − for subtraction, and · for multiplication, satisfying the following laws of arithmetic:

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

The adjective **commutative** refers to the law asserting that $xy = yx$. A commutative ring with $0 \neq 1$ is said to be a **integral domain** if it satisfies the following condition:

$$xy = 0 \Rightarrow x = 0 \vee y = 0.$$

A commutative ring with $0 \neq 1$ is said to be a **field** if it comes equipped with a further operation $(-)^{-1}$ defined on all nonzero elements, such that

$$xx^{-1} = 1.$$

Examples of commutative rings include most number systems we have encountered so far: $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{Z}/n$ for any n. The Gaussian integers $\mathbb{Z}[i]$ are another important example of a ring. There is one important omission: The set of natural numbers with the usual operations of addition and multiplication is not a ring because it lacks subtraction.

The sharp reader may have observed that some laws of arithmetic, such as $0x = 0$, are not stated in the definition of a (commutative) ring. Indeed, this law can be proven:

$$0x = 0x + 0 = 0x + (0x - 0x) = (0x + 0x) - 0x = (0+0)x - 0x = 0x - 0x = 0.$$

Most rings satisfy the condition that $0 \neq 1$. Indeed, if $0 = 1$ in a ring R, then any element equals 0 because

$$x = 1x = 0x = 0.$$

Thus, only the ring $\mathbb{Z}/1$ satisfies $0 = 1$. This ring is called the **trivial ring** for understandable reasons.

The condition of being an integral domain is quite innocent-looking: It guarantees that the product of any two nonzero numbers is nonzero. This condition is true in familiar number systems such as $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}$, and $\mathbb{R}$, which are therefore integral domains. However, the ring $\mathbb{Z}/n$ is only an integral domain when n is prime. For composite n, we can find examples of nonzero numbers that multiply to 0. For instance, we have $2 \cdot 2 \equiv 0 \pmod 4$ in $\mathbb{Z}/4$, and we have $2 \cdot 3 \equiv 0 \pmod 6$ in $\mathbb{Z}/6$. Having such examples shows that the condition of being an integral domain is not provable from the laws of arithmetic stated in the definition of a ring.

Of the examples we have seen so far, only $\mathbb{Q}$ and $\mathbb{Z}/p$ are fields. Other familiar fields include the field $\mathbb{R}$ of real numbers and the field $\mathbb{C}$ of complex numbers. We note

that any field is an integral domain: If $xy = 0$ and $x \neq 0$, then x has a multiplicative inverse. This allows us to calculate as follows and find that

$$y = 1y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0 = 0.$$

The previous definitions of rings, integral domains, and fields are extremely general. There are many examples of rings that have little to do with numbers, except that they satisfy the laws of arithmetic. We stress here that our goal is not to develop the general theory of rings, where we would have to be concerned with the vast scope of the subject. Instead, our goal is simply to avoid having to reprove essentially the same theorems about polynomials separately for polynomials with integer coefficients, rational coefficients, real coefficients, and so on. By stating them in terms of polynomials with coefficients in a ring or integral domain, we cover all those cases at once.

Remark 20.1.3. There is another subtle, yet important aspect of polynomials which needs to be emphasized: The distinction between polynomials and the functions they describe. This distinction comes to light when considering equality of polynomials. Two polynomials

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \qquad \text{and} \qquad b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$$

are said to be equal if their coefficients are equal, meaning that $a_i = b_i$ for all $0 \leq i \leq n$, while functions are considered equal if their values are equal. This is an important distinction, because for some number systems such as the integers modulo n, polynomials aren't necessarily equal as polynomials when they are equal as functions. For instance, by Theorem 16.1.1 (Fermat's Little Theorem) we have that

$$x^p \equiv x \pmod{p},$$

while the polynomials x^p and x clearly can be distinguished by their coefficients. Nevertheless, we will show in Corollary 20.4.3 that two polynomials with integer coefficients have equal coefficients if and only if they define equal functions.

Definition 20.1.4. Consider a ring R. A function $f : R \to R$ is said to be **polynomial in** R if there exists a polynomial with coefficients in R such as the above, such that

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

for all $x \in R$.

Remark 20.1.5. Polynomials can be added, subtracted, and multiplied in the same way as integers. To add two polynomials, we add their corresponding coefficients, taking missing coefficients as zero when necessary. Polynomials are multiplied by the formula

$$\begin{aligned}\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{m} b_j x^j\right) &= \sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j x^{i+j} \\ &= \sum_{k=0}^{n+m}\sum_{i=0}^{n} a_i b_{k-i} x^k.\end{aligned}$$

These operations of addition, subtraction, and multiplication of polynomials satisfy the laws of arithmetic. More precisely, the polynomials with coefficients in a commutative ring form itself a commutative ring.

20.2 The Factor Theorem

DEFINITION 20.2.1. Consider a polynomial $f(x)$ with coefficients in a ring R. A **root** of $f(x)$ is an element $r \in R$ such that

$$f(r) = 0.$$

Sometimes we will write $N(f)$ for the set of roots of f.

In the following theorem we will prove that if r is a root of the polynomial $f(x)$, then we can factor $f(x)$ as $(x-r)g(x)$. This theorem applies for polynomials in any commutative ring.

THEOREM 20.2.2 (Factor Theorem). *Consider a ring R, and a nonzero polynomial $f(x)$ of degree n with coefficients in R. An element $r \in R$ is a root of $f(x)$ if and only if there is a polynomial $g(x)$ of degree $n-1$ with coefficients in R such that $f(x) = (x-r)g(x)$.*

PROOF. We will prove the claim by induction on n. In the base case $f(x)$ is a nonzero constant polynomial, so it has no roots and there is nothing to prove.

For the inductive step, it is clear that if there is a polynomial $g(x)$ such that $f(x) = (x-r)g(x)$, then r is a root of the polynomial $f(x)$. For the converse, suppose that r is a root of $f(x)$. Then

$$f(x) = f(x) - f(r) = a_n(x^n - r^n) + \cdots + a_1(x-r).$$

By the formula for the difference of kth powers, which was stated in Exercise 2.5 and which holds in any ring, we can factor $x^k - r^k$ as

$$x^k - r^k = (x-r)q_k(x), \qquad \text{where} \qquad q_k(x) = \sum_{i=0}^{k-1} x^i r^{k-1-i}$$

is a polynomial of degree $k-1$. Now define $g(x) := \sum_{k=1}^{n} a_k q_k(x)$. Then we compute

$$(x-r)g(x) = \sum_{k=1}^{n} a_k(x-r)q_k(x) = \sum_{k=1}^{n} a_k(x^k - r^k) = f(x) - f(r) = f(x). \qquad \square$$

Theorem 20.2.2 (Factor Theorem) has some important corollaries. One of them states that in an integral domain, where the product of any two nonzero numbers is guaranteed to be nonzero, any polynomial of degree n has at most n roots.

COROLLARY 20.2.3. *Consider an integral domain R. A polynomial of degree n with coefficients in R has at most n roots.*

Proof. The proof is by induction on the degree n. If $f(x)$ is a constant polynomial of degree 0 and its leading coefficient is nonzero, then $f(x)$ is always nonzero and so $f(x)$ has no roots.

For the inductive step, assume that all polynomials of degree n have at most n roots, and consider a polynomial $f(x)$ of degree $n+1$. Then either $f(x)$ has no roots, in which case we are done immediately, or $f(x)$ has a root r, in which case $f(x)$ factors as

$$f(x) = (x - r)g(x)$$

by Theorem 20.2.2 (Factor Theorem), where $g(x)$ is a polynomial of degree n. Since we assumed that R is an integral domain, it follows that for any element $x \in R$, the identity $(x - r)g(x) = 0$ holds in R if and only if one of the identities $x - r = 0$ or $g(x) = 0$ holds in R. Thus we see that x is a root of the polynomial $f(x)$ if and only if $x = r$ or x is a root of the polynomial $g(x)$. We conclude that the polynomial $f(x)$ has at most $n + 1$ roots. □

The Factor Theorem also raises an immediate question of uniqueness. If $f(x)$ and $g(x)$ are two polynomials, is there always at most one way in which we can write

$$f(x) = g(x)h(x)?$$

Proposition 20.2.4 (Cancellation Law for Polynomials). *Let $f(x)$ be a nonzero polynomial with coefficients in an integral domain. Consider two polynomials $h(x)$ and $k(x)$ satisfying the identity of polynomials*

$$f(x)h(x) = f(x)k(x).$$

Then $h(x) = k(x)$.

Proof. By the assumption that $f(x)h(x) = f(x)k(x)$, it follows that

$$f(x)(h(x) - k(x)) = 0.$$

Write $g(x) := h(x) - k(x)$. Note that all the coefficients of the polynomial $f(x)g(x)$ are 0. However $f(x)$ is a nonzero polynomial, so it has a leading coefficient a_n. Now, suppose for a contradiction that $g(x)$ is nonzero, with leading coefficient b_m. Their product $f(x)g(x)$ has leading coefficient $a_n b_m$, which is nonzero since it is a product of nonzero elements of an integral domain. Hence $f(x)g(x)$ is nonzero, which is a contradiction. □

20.3 Polynomial Congruences of Prime Moduli

Even though a polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$



has at most n roots in the integers, the same is not true in modular arithmetic. A fairly easy example, the quadratic congruence

$$x^2 \equiv 1 \pmod{8}$$

has four solutions, the numbers 1, 3, 5, and 7. On the other hand, we will prove in this section that the number of solutions of a polynomial congruence modulo a prime is, just as in the integer case, at most the degree of the polynomial.

THEOREM 20.3.1 (Factor Theorem in Modular Arithmetic). *An integer r is a solution to the polynomial congruence*

$$f(x) \equiv 0 \pmod{n},$$

if and only if

$$f(x) \equiv (x-r)g(x) \pmod{n}$$

for some polynomial $g(x)$.

PROOF. The proof is very similar to the proof of Theorem 20.2.2. First, we note that the converse direction is trivial, so we focus on the forward direction. Suppose that

$$f(r) \equiv 0 \pmod{n}$$

and consider the polynomial $f(x) - f(r)$. Then we have

$$f(x) \equiv f(x) - f(r) \pmod{n},$$

and the factorization of $f(x) - f(r)$ as $(x-r)g(x)$ follows in the same way as for Theorem 20.2.2. □

THEOREM 20.3.2 (Lagrange's Theorem). *Consider a polynomial*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

and a prime p such that $p \nmid a_n$. Then the polynomial congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n solutions.

PROOF. We prove the claim by induction on the degree n of the polynomial f. If f has degree zero, then $f(x) = a_0$, and since the leading term of f is assumed to be not divisible by p, it follows that $a_0 \not\equiv 0 \pmod{p}$. Thus, the polynomial f has no solutions modulo p.

Now suppose that any polynomial congruence modulo p of degree n has at most n solutions, and consider a polynomial congruence $f(x) \equiv 0 \pmod{p}$ of degree $n+1$. If this congruence has no roots, then the number of solutions is certainly below $n+1$.

On the other hand, if $f(r) \equiv 0 \pmod{p}$ is a solution, then by Theorem 20.3.1 (Factor Theorem in Modular Arithmetic) we can find a polynomial $g(x)$ of degree n such that

$$f(x) \equiv (x-r)g(x) \pmod{p}.$$

It follows that the polynomial congruences $f(x) \equiv 0 \pmod{p}$ and

$$(x-r)g(x) \equiv 0 \pmod{p}$$

have the same sets of solutions. Since p is prime, we have by Proposition 13.1.4 that $ab \equiv 0 \pmod{p}$ if and only if $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. Any solution x of the congruence $(x-r)g(x) \equiv 0 \pmod{p}$ must therefore satisfy $x - r \equiv 0 \pmod{p}$ or $g(x) \equiv 0 \pmod{p}$. There are at most d solutions of the polynomial congruence $g(x) \equiv 0 \pmod{p}$, so we conclude that there are at most $d+1$ solutions to the polynomial congruence $f(x) \equiv 0 \pmod{p}$. □

The previous theorem is due to Joseph-Louis Lagrange, published in 1770 in *Réflexions sur la résolution algébrique des équations* [Lag1770]. Lagrange demonstrated that the roots of polynomials can be studied by their permutations. His ideas would eventually lead to the emergence of group theory (the study of symmetry), and Galois theory.

While Theorem 20.3.2 (Lagrange's Theorem) establishes an upper bound for the number of incongruent solutions of a polynomial congruence modulo a prime, we can use Theorem 16.1.1 (Fermat's Little Theorem) to find examples of polynomial congruences that have the maximum allowable number of solutions.

Theorem 20.3.3. *Consider a prime p and a positive integer n such that $n \mid p-1$. Then the polynomial congruence*

$$x^n \equiv 1 \pmod{p}$$

has exactly n incongruent solutions.

Proof. Note that the polynomial congruence $x^{p-1} - 1 \equiv 0 \pmod{p}$ has exactly $p-1$ solutions. By the formula for the difference of powers, we have

$$(x^{p-1} - 1) \equiv (x^n - 1)q(x) \pmod{p}$$

for some polynomial q of degree $p - 1 - n$. Now we observe that the polynomial congruences

$$x^n - 1 \equiv 0 \pmod{p} \qquad \text{and} \qquad q(x) \equiv 0 \pmod{p}$$

have at most n and $p - 1 - n$ solutions, respectively. Since their product has $p - 1$ solutions, it follows that the polynomial congruence $x^n - 1 \equiv 0 \pmod{p}$ must have exactly n solutions. □

Theorem 20.3.2 (Lagrange's Theorem) can also be used to give another proof of Theorem 16.5.1, which states that for an odd prime p, the quadratic congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.

PROOF OF THEOREM 16.5.1. We prove that if $p \equiv 1 \pmod 4$, then there is a square root of -1 modulo p. Consider a prime p of the form $4k + 1$. Then Theorem 16.1.1 (Fermat's Little Theorem) implies that

$$(x^{2k} + 1)(x^{2k} - 1) = x^{4k} - 1 \equiv 0 \pmod p.$$

Since p is prime, this implies that $x^{2k} + 1 \equiv 0 \pmod p$ or $x^{2k} - 1 \equiv 0 \pmod p$ for every integer x. However, the polynomial congruence

$$x^{2k} - 1 \equiv 0 \pmod p$$

has at most $2k$ solutions modulo p, which is strictly fewer than p. Thus, there must exist an integer x such that

$$x^{2k} + 1 \equiv 0 \pmod p.$$

Given such an integer x, we see that $y := x^k$ is a square root of -1 modulo p. □

20.4 Lagrange's Interpolation Theorem

Lagrange's Interpolation Theorem establishes that for any set of data points, as illustrated in Figure 20.1, there is always a way of defining a polynomial that exactly matches the data. Moreover, it gives the unique way of defining such a polynomial in the lowest degree. Interpolation theorems such as Lagrange's or Newton's addressed a practical need for geometers of the 17th and 18th centuries: It allowed them to estimate intermediate values of a function from a finite amount of data such as tables of planetary positions or values of trigonometric functions.

Lagrange's Interpolation Theorem has the important consequence that any polynomial of degree n is uniquely determined by any $n + 1$ of its values. We will also use Lagrange's Interpolation Theorem in the next section to derive a divisibility property of polynomials due to Kurt Hensel.

The idea underlying Lagrange's Interpolation Theorem is to break the problem into several subproblems: For each data point (x_i, y_i), we create a polynomial that has roots at x_j for all the other data points (x_j, y_j). This is very easy to do: we just take the product

$$g_i(x) = (x - x_0) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_j).$$

Then we have that $g_i(x_j) = 0$ for all $j \neq i$ and $g_i(x_i) \neq 0$. Thus there is some constant c_i such that $c_i g_i(x_i) = y_i$. Adding them all up gives the Lagrange Interpolation Theorem.

EXAMPLE 20.4.1. In Figure 20.1, we started with the set of points

$$(0, 1),\ (1, -2),\ (2, 0),\ (3, 1).$$

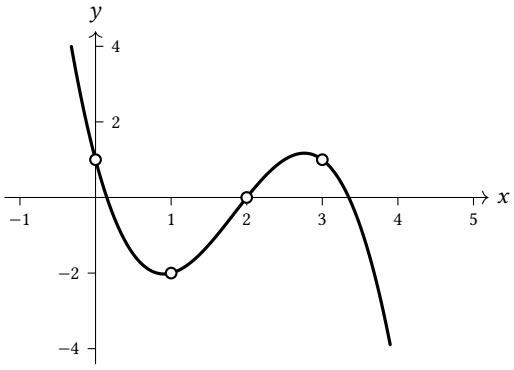


Figure 20.1: A polynomial of degree 3 obtained by Lagrange interpolation.

Then we define the polynomials

$$\begin{aligned} g_0 &:= \tfrac{1}{6}(x-1)(x-2)(x-3) \\ g_1 &:= -x(x-2)(x-3) \\ g_2 &:= 0 \\ g_3 &:= \tfrac{1}{6}x(x-1)(x-2), \end{aligned}$$

which we have already rescaled so that $g_0(0) = 1$, $g_1(1) = -2$, $g_2(2) = 0$, and $g_3(3) = 1$. Adding them up gives the polynomial

$$f(x) := \frac{1}{6}(x-1)(x-2)(x-3) - x(x-2)(x-3) + \frac{1}{6}x(x-1)(x-2),$$

which exactly matches the values specified in the initial data set.

Theorem 20.4.2 (Lagrange's Interpolation Theorem). *For any choice of $n+1$ points (x_i, y_i) such that the x_i are pairwise distinct, there is a unique polynomial $f(x)$ of degree at most n such that*

$$f(x_i) = y_i$$

for all $0 \le i \le n$.

Proof. For any $0 \le i \le n$, define the **basis polynomial** for Lagrange interpolation $g_i(x)$ by

$$g_i(x) := \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j}.$$

Then $g_i(x)$ is a polynomial of degree n, whose n roots are the points x_j for $j \neq i$. Furthermore, we have defined g_i in such a way that $g_i(x_i) = 1$. Now we define the polynomial $f(x)$ of degree n by

$$f(x) = \sum_{i=0}^{n} y_i g_i(x).$$

Then $f(x_i) = y_i$ since $g_j(x_i) = 0$ for $j \neq i$ and $g_i(x_i) = 1$. Thus f satisfies the criteria of the theorem.

To see that the polynomial $f(x)$ is the unique polynomial of degree at most n that satisfies $f(x_i) = y_i$, consider a second polynomial $g(x)$ of degree at most n that satisfies the same requirement. Then the polynomial

$$f(x) - g(x)$$

is a polynomial of degree at most n with $n + 1$ roots. By virtue of Corollary 20.2.3 this is only possible if $f(x) - g(x)$ is the zero polynomial, that is, if $f(x) = g(x)$. □

COROLLARY 20.4.3. *Consider two polynomials $f(x)$ and $g(x)$. Then the following are equivalent:*

(i) *The polynomials $f(x)$ and $g(x)$ have equal coefficients; that is, they are equal as polynomials.*

(ii) *The polynomials $f(x)$ and $g(x)$ have equal values; that is, they are equal as functions.*

(iii) *The polynomials $f(x)$ and $g(x)$ have equal values of any set of $n + 1$ inputs.*

In particular, any polynomial $f(x)$ is uniquely determined by the values

$$f(0), \ldots, f(n).$$

Even though the basis polynomials of Lagrange's Interpolation Theorem don't always have integer coefficients, we can use Lagrange's Interpolation Theorem to show that for any polynomial f with real coefficients, if

$$f(0), \ldots, f(n)$$

are integers, then $f(x)$ is an integer for every integer x.

DEFINITION 20.4.4. A polynomial $f(x)$ with real coefficients is said to be **integer valued** if $f(x)$ is an integer for every integer x.

A simple example of an integer valued polynomial that doesn't have integer coefficients is the polynomial

$$\frac{x(x+1)}{2},$$

which returns the triangular numbers.

Lagrange's Interpolation Theorem establishes a polynomial $f(x)$ as a linear combination of the basis polynomials, thus obtaining

$$f(x) = \sum_{k=0}^{n} f(k) g_i(x).$$

However, we can turn this perspective around. Each value $f(x)$ can be written as a linear combination of the values $f(k)$ for $0 \leq k \leq n$. This observation is important enough that we establish it in its own lemma, which is a direct corollary of Lagrange's Interpolation Theorem.

Lemma 20.4.5. *Consider a polynomial $f(x)$. Then each value $f(x)$ can be written as a linear combination of the values $f(0)$, ..., $f(n)$; that is, there are coefficients $a_i(x)$ for each $0 \leq i \leq n$ depending on x such that*

$$f(x) = \sum_{i=0}^{n} a_i(x) f(i).$$

Proof. The coefficients $a_k(x)$ are given by the basis polynomials $g_k(x)$. □

Equipped with this change of perspective, we can prove that a polynomial of degree n is integer values as soon as its values $f(0)$, ..., $f(n)$ are integers.

Theorem 20.4.6. *Consider a polynomial $f(x)$ of degree n with real coefficients. If the values*

$$f(0), \dots, f(n)$$

are integers, then $f(x)$ is an integer for every integer x.

Proof. The basis polynomials of f are

$$g_i(x) = \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x-j}{i-j}.$$

We can express $g_i(x)$ using binomial coefficients as

$$g_i(x) = \prod_{j=0}^{i-1} \frac{x-j}{i-j} \prod_{j=i+1}^{n} \frac{x-j}{i-j} = (-1)^{n-i} \binom{x}{i} \binom{x-i-1}{n-i},$$

which is an integer for every integer x. Therefore it follows by Theorem 20.4.2 (Lagrange's Interpolation Theorem) that every value $f(x)$ can be written as an integer linear combination of the integers $f(0), \dots, f(n)$, which proves the theorem. □



20.5 Fixed Divisors of Integer Polynomials

In Chapter 7, we have done a few exercises which asked us to show that integers in certain polynomial forms satisfy a divisibility property. For example, we showed that $a^3 - a$ is always divisible by 6, and that $a^5 - a$ is always divisible by 30. We also showed that the product of any n consecutive integers is always divisible by $n!$. In this section we will establish a vast generalization of these facts.

DEFINITION 20.5.1. The **fixed divisor** of a function $f : X \to \mathbb{Z}$ into the integers is the greatest common divisor of all values of f, i.e.,

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

Theorem 20.4.2 (Lagrange's Interpolation Theorem) can be used to determine the greatest common divisor of all the values of a polynomial, by examining only one more value than its degree. This observation is due to Kurt Hensel, who was a student of Leopold Kronecker.

THEOREM 20.5.2 (Hensel's Fixed Divisor Theorem [HEN1896]). *Consider a polynomial $f(x)$ of degree n, with integer coefficients. Then the fixed divisor of f is the greatest common divisor*

$$\gcd(f(a), \dots, f(a+n))$$

of any $n+1$ values of consecutive inputs of f.

PROOF. First, we note that by translating the polynomial along the axis of abscissas, which we can do by considering the polynomial $f(a)$, it suffices to show that for any polynomial $f(x)$ of degree n with integer coefficients, the fixed divisor of f is the greatest common divisor of the integers

$$f(0), \dots, f(n).$$

Now recall from Theorem 20.4.6 that the values $f(x)$ are integer linear combinations of the values $f(0), \dots, f(n)$:

$$f(x) = \sum_{i=0}^{n} f(i) g_i(x).$$

It follows that

$$\gcd(f(0), \dots, f(n)) \mid f(x).$$

Since the fixed divisor of f divides this greatest common divisor, this establishes the theorem. □

EXAMPLE 20.5.3. Consider the polynomial

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

When n is even, then f is an **even function**, which means that $f(-x) = f(x)$, and when n is odd, then f is an **odd function** which means that $f(-x) = -f(x)$. In either

case, this implies that the fixed divisor of $x^n - x$ is equal to the greatest common divisor of the elements

$$f(0), \ldots, f(m),$$

where m is the largest integer such that $2m \leq n + 1$. In other words, to compute the fixed divisor of $x^n - x$, we only have to inspect about half the amount of values of Hensel's Fixed Divisor Theorem. Furthermore, the polynomial $f(x) = x^n - x$ always satisfies $f(0) = 0$ and $f(1) = 0$, reducing the amount of cases even further. Thus, the fixed divisor of $x^n - x$ is

$$\gcd(\{f(k) \mid 2 \leq k \leq (n+1)/2\}).$$

(i) For $n = 3$, the only number $2 \leq k \leq (n+1)/2$ is the number 2. The polynomial $f(x) = x^3 - x$ from Exercise 6.9 has the value

$$f(2) = 6,$$

so the fixed divisor of $x^3 - x$ is 6, which is $2 \cdot 3$.

(ii) For $n = 5$, the only two numbers $2 \leq k \leq (n+1)/2$ are the numbers 2 and 3. The polynomial $f(x) = x^5 - x$ from Exercise 6.10 has the values

$$f(2) = 30 \qquad \text{and} \qquad f(3) = 240.$$

Since 240 is divisible by 30 it follows that the fixed divisor of $x^5 - x$ is 30, which is $2 \cdot 3 \cdot 5$.

(iii) For $n = 7$, the only three numbers $2 \leq k \leq (n+1)/2$ are the numbers 2, 3, and 4. The polynomial $f(x) = x^7 - x$ has the values

$$f(2) = 126 \qquad \text{and} \qquad f(3) = 2184.$$

Furthermore, using that $4^7 = (2^7)^2$ we see that $f(4)$ factors as $(2^7 - 2)(2^7 + 2)$ by the formula for the difference of squares. Therefore it follows that the fixed divisor of $f(x)$ is the greatest common divisor of $f(2)$, $f(3)$, and $f(4)$, which is just the greatest common divisor of $f(2)$ and $f(3)$, which is

$$\gcd(126, 2184) = 42 = 2 \cdot 3 \cdot 7.$$

We will generalize these examples in Theorem 29.2.2.



Exercises

Starter Exercises

20.1 Find two integers a and b such that

$$a + b = 150 \qquad \text{and} \qquad ab = 2025.$$

Hint: To avoid guessing, use that a and b are roots of the polynomial $x^2 - (a + b)x + ab$ by Vieta's relations.

20.2 Find a polynomial $f(x)$ such that

$$(x + 1)(x + 2)(x + 3)(x + 4) + 1 = f(x)^2.$$

Routine-Building Exercises

20.3 Show that $x^{13} - x$ has fixed divisor

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13.$$

20.4 *The rational root theorem.* Show that if the polynomial equation

$$a_n x^n + \cdots a_1 x + a_0 = 0$$

with integer coefficients has a rational solution $x_0 = \frac{s}{t}$ with $\gcd(s, t) = 1$, then $s \mid a_0$ and $t \mid a_n$. Conclude that if the polynomial is monic, meaning that $a_n = 1$, then any rational root is an integer. Also conclude that $\sqrt[3]{7}$ is irrational.

20.5 (a) (Sophie Germain's identity) Write

$$x^4 + 4y^4$$

as a difference of two squares.

(b) Compute the fixed divisor of the polynomial $f(x) = x^4 + 4$.

(c) Compute the polynomial $g(x) = \gcd(x^4 + 4, (x + 2)^4 + 4)$, and show that $g(x) > 1$ for every integer x.

(d) Find all positive integers x and y for which $x^4 + 4y^4$ is prime.

20.6 (Gauss's Gem) Write

$$f(x, y, z) := x^3 + y^3 + z^3 - 3xyz$$

in the form $\frac{1}{2}d(a^2 + b^2 + c^2)$ for some quadruple of integers a, b, c, d depending on x, y, and z. Hint: For $x + y + z = 0$, evaluate $f(x, y, z)$.

20.7 Show that a number n is square-free if and only if the only integer x satisfying the congruence $x^2 \equiv 0 \pmod{n}$ is $x = 0$.

20.8 Show that there are only two polynomials f such that any two values $f(x)$ and $f(y)$ are relatively prime for distinct inputs x and y.

20.9 Consider a prime number p. Construct for every integer $0 \leq a < p$ a polynomial $f(x)$ of degree $< p$ with coefficients in $\mathbb{Z}/p\mathbb{Z}$ such that

$$f(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{otherwise.} \end{cases}$$

Use these polynomials similarly to the basis polynomials in Theorem 20.4.2 (Lagrange's Interpolation Theorem) to show that every function $\mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is polynomial.

20.10 Define the kth **power sum**

$$p_k(a_1, \ldots, a_n) := a_1^k + \cdots + a_n^k.$$

We will simply write p_k for $p_k(a_1, \ldots, a_n)$ and e_k for $e_k(a_1, \ldots, a_n)$.

(a) *The Newton-Girard identities.* Show that for all k we have

$$p_k = e_1 p_{k-1} - e_2 p_{k-2} + \cdots + (-1)^{k-1} e_{k-1} p_1 + (-1)^{k-1} k e_k.$$

Hint: This looks more complicated than it is.

(b) Prove that the congruence

$$1^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$$

holds for every $0 < k < p - 1$, and every prime number p.

Challenge Exercises

20.11 (Pólya [Pól1919]) Consider a polynomial $f(x)$ of degree n with rational coefficients. Show that if there exists $n + 1$ distinct integers $x_0, \ldots, x_n$ such that

$$\sum_{i=0}^{n} |f(x_i)| < \frac{n!}{2^n},$$

then $f(x)$ cannot be a polynomial with integer coefficients.



Chapter 21

Primitive Roots

21.1 Counting Elements of a Given Order Modulo a Prime

Theorem 16.2.1 (Euler's Theorem) tells us that

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

for every integer a such that $\gcd(a, n) = 1$. By Theorem 8.5.2 (Order Theorem), this implies that

$$\mathrm{ord}_n(a) \mid \phi(n).$$

Euler's theorem therefore gives an upper bound for the order of any element modulo n. For example, since 13 is a prime number, we have $\phi(13) = 12$, so all integers relatively prime to 13 have an order dividing the number 12. Computing the powers of 2, for instance, we see that $\mathrm{ord}_{13}(2) = 12$:

m	0	1	2	3	4	5	6	7	8	9	10	11
$2^m \pmod{13}$	1	2	4	8	3	6	12	11	9	5	10	7.

The process of doubling integers modulo 13 is illustrated in Figure 21.1. Using Theorem 8.5.4, we can use this table to compute the orders of all the nonzero integers modulo 13. Recall that Theorem 8.5.4 states that

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

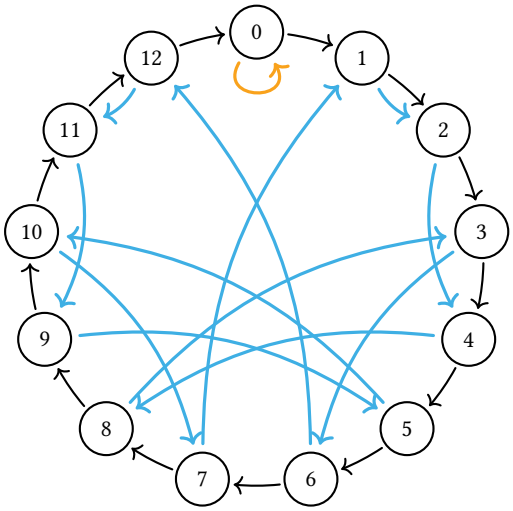


Figure 21.1: Doubling integers modulo 13.

For example, since $3 \equiv 2^4 \pmod{13}$, it follows that the order of 3 modulo 13 is 3. Similarly, since $5 \equiv 2^9 \pmod{13}$, it follows that

$$5^4 \equiv (2^9)^4 \equiv (2^{12})^3 \equiv 1 \pmod{13}.$$

Computing the orders of all the elements from 1 to 12 modulo 13 this way, we obtain:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ord}_{13}(a)$	1	12	3	6	4	12	12	4	3	6	12	2.

While the orders of the integers modulo 13 might at first glance appear to be somewhat unwieldy, Theorem 8.5.4 is the key to some important patterns. For example, given an integer $a \pmod{p}$ with $\operatorname{ord}_p(a) = p - 1$ such as $2 \pmod{13}$, Theorem 8.5.4 tells us that

$$\operatorname{ord}_p(a^m) = k \quad \Leftrightarrow \quad \frac{p-1}{\gcd(m, p-1)} = k$$

In particular, $\operatorname{ord}_p(a^m) = p - 1$ if and only if $\gcd(m, p - 1) = 1$. Indeed, we see that there are four integers modulo 13 of order 12, corresponding to the powers of 2 with exponents 1, 5, 7, and 11.

However, we can go further: There are two integers that have order 6 modulo 13, and indeed $\phi(6) = 2$ as well. Similarly, we find that there are $\phi(1)$, $\phi(2)$, $\phi(3)$, and $\phi(4)$ integers of order 1, 2, 3, and 4, respectively. The following theorem tells us that modulo a prime p, the number of integers of order k modulo p is either 0 or $\phi(k)$. This suggests that for any prime number p and any $k \mid p - 1$, it should be true that the number of elements of order k is exactly $\phi(k)$.

Theorem 21.1.1. *Consider a prime number p. Then there are for every $k \mid p-1$ exactly $\phi(k)$ integers of order k modulo p.*

The proof of this theorem makes essential use of the fact that any polynomial congruence of the form

$$x^d \equiv 1 \pmod{p}$$

has at most d solutions. This was established in Theorem 20.3.3. To emphasize this observation, we will prove Theorem 21.1.1 as a consequence of the following more general theorem.

Theorem 21.1.2. *Consider a number n with the property that every polynomial congruence of the form*

$$x^d \equiv 1 \pmod{n}$$

has at most d solutions. Then there are for every $k \mid \phi(n)$ exactly $\phi(k)$ integers of order k modulo n.

Proof. In this proof, let us write $\psi(k)$ for the number of integers of order k modulo n. We claim that

$$\psi(k) = \begin{cases} \phi(k) & \text{if } k \mid \phi(n), \\ 0 & \text{otherwise.} \end{cases}$$

The fact that if $k \nmid \phi(n)$ then $\psi(k) = 0$ follows immediately from Theorem 8.5.2 (Order Theorem) and Theorem 16.1.1 (Fermat's Little Theorem). Thus, it remains to show that $\psi(k) = \phi(k)$ for any $k \mid \phi(n)$.

Consider an integer a of order k modulo n. By definition, every integer of order k modulo n is a solution to the polynomial congruence

$$x^k \equiv 1 \pmod{n}.$$

This polynomial congruence has at most k solutions. Given that the integer a has order k modulo n, we see that the set of solutions can be described exactly as the following set of numbers:

$$1,\ a,\ \ldots,\ a^{k-1}.$$

Thus, we see that every solution is congruent to a power of a. In particular, it follows that every integer of order k modulo n is itself a power of a. Recall from Theorem 8.5.4 that an integer of the form a^m has order k if and only if $\gcd(m,k) = 1$. Thus we conclude that, given an element of order k, there are exactly $\phi(k)$ integers of order k. In other words, $\psi(k)$ is either 0 or $\phi(k)$, and certainly we have that $\psi(k) \leq \phi(k)$.

To finish the proof, observe that, since every element $1 \leq x < n$ relatively prime to n has an order modulo n, we have

$$\phi(n) = \sum_{k \mid \phi(n)} \psi(k) \leq \sum_{k \mid \phi(n)} \phi(k) = \phi(n).$$

It follows that the inequality is in fact an equality, and since $\psi(k) \leq \phi(k)$ for every $k \mid \phi(n)$ it follows that $\psi(k) = \phi(k)$ for every $k \mid \phi(n)$. □

21.2 Primitive Roots

We saw in the previous section that there are exactly $\phi(k)$ integers of order k modulo p, for every $k \mid p-1$. It follows that there are

$$\phi(p-1)$$

integers of order $p-1$. Since $\phi(p-1) > 0$, it follows that for every prime number p, there is an integer g such that the integers

$$1, g, g^2, \dots, g^{p-2}$$

form a reduced residue system modulo p. That is, there is an integer g such that every integer a relatively prime to p is congruent to exactly one power g^k, where $0 \leq k < p-1$. Such integers are called *primitive roots*. In the previous section we saw that 2 is a primitive root of the prime 13.

DEFINITION 21.2.1. A **primitive root** modulo a natural number n is an integer g such that

$$\operatorname{ord}_n(g) = \phi(n).$$

THEOREM 21.2.2. *Consider a natural number n. The following are equivalent:*

(i) *The number n admits a primitive root modulo n.*

(ii) *Any polynomial congruence of the form*

$$x^d \equiv 1 \pmod{n}$$

has at most d solutions.

Furthermore, if the first condition holds then there are $\phi(\phi(n))$ primitive roots, and if the last condition holds and the polynomial congruence $x^d \equiv 1 \pmod{n}$ has a solution, then it has exactly $\gcd(d, \phi(n))$ solutions.

PROOF. We have already proven that ii implies i in Theorem 21.1.2. To prove that i implies ii, consider a primitive root g modulo n, and consider the polynomial congruence

$$x^d \equiv 1 \pmod{n}.$$

An integer $a \equiv g^m \pmod{n}$ is a solution if and only if $g^{dm} \equiv 1 \pmod{n}$. Since we assumed that $\operatorname{ord}_n(g) = \phi(n)$, it follows from Theorem 8.5.2 (Order Theorem) that the congruence $g^{dm} \equiv 1 \pmod{n}$ holds if and only if $\phi(n) \mid dm$. The number of $0 \leq m < \phi(n)$ such that $\phi(n) \mid dm$ is exactly $\gcd(d, \phi(n))$, which is at most d. Therefore, it follows that there are at most d solutions to the congruence $x^d \equiv 1 \pmod{n}$. □

COROLLARY 21.2.3. *The number of primitive roots of a prime number p is $\phi(p-1)$. In particular, every prime p admits a primitive root.*

Example 21.2.4. The number 9 has the primitive root 2. Indeed $\phi(9) = 6$, and $2^3 \equiv -1 \pmod 9$ so that $\operatorname{ord}_9(2) = 6$. Thus, by the previous theorem it follows that the congruence $x^d \equiv 1 \pmod 9$ has at most d solutions.

Nevertheless, there are polynomials $f(x)$ of degree 2 that are not of this form that have more than two solutions among the integers relatively prime to 9. For example, the polynomial congruence

$$x^2 + x + 7 \equiv 0 \pmod 9,$$

has the three solutions $x \equiv 1$, 4, and 7 $\pmod 9$.

Some further composite numbers with primitive roots include 4 and 6: The number 3 is a primitive root of 4, and 5 is a primitive root of 6.

The number 8, on the other hand, does not have primitive roots because $\phi(8) = 4$ while the odd integers 3, 5, and 7 all have order 2. In fact, it is possible to precisely classify all the natural numbers that have primitive roots. We will do so in Theorem 22.2.1.

21.3 The Discrete Logarithm

It is useful to have access to primitive roots, if they exist, because if g is a primitive root modulo n, then the integers

$$1, g, g^2, \dots, g^{\phi(n)-1}$$

form a reduced residue system modulo n. This means that every number relatively prime to n is congruent to exactly one of the integers g^i, for $0 \le i < \phi(n)$. Having a primitive root therefore gives a convenient way of representing all the elements of a reduced residue system.

Definition 21.3.1. Suppose g is a primitive root modulo n, and let a be an integer relatively prime to n. Then we define the **discrete logarithm** or **index**

$$\operatorname{ind}_g(a)$$

of a base g to be the unique integer k modulo $\phi(n)$ such that $g^k = a$.

Theorem 21.3.2. *Consider a natural number n with a primitive root g.*

(i) *For any two integers a and b relatively prime to n, we have*

$$a \equiv b \pmod n \quad \Leftrightarrow \quad \operatorname{ind}_g(a) \equiv \operatorname{ind}_g(b) \pmod{\phi(n)}.$$

(ii) *Furthermore, we have*

$$\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g(a) + \operatorname{ind}_g(b) \pmod{\phi(n)}$$
$$\operatorname{ind}_g(a^m) \equiv m \operatorname{ind}_g(a) \pmod{\phi(n)}.$$



EXAMPLE 21.3.3. Solving linear congruences becomes quite a straightforward task when a primitive root is known. For example, the congruence

$$14x \equiv 6 \pmod{26}$$

is solvable if and only if $7x \equiv 3 \pmod{13}$ is. By the previous theorem, this linear congruence is equivalent to the linear congruence

$$\operatorname{ind}_2(7) + \operatorname{ind}_2(x) \equiv \operatorname{ind}_2(3) \pmod{12}.$$

Since $\operatorname{ind}_2(7) = 11$ and $\operatorname{ind}_2(3) = 4$, we find that $\operatorname{ind}_2(x) \equiv 5 \pmod{12}$. Thus, we conclude that

$$x \equiv 6 \pmod{13}$$

is a solution of the original linear congruence.

21.4 A Criterion for Congruences of Degree n

While we are primarily interested in the quadratic congruence

$$x^2 \equiv a \pmod{p}$$

in this introductory course on elementary number theory, the techniques that we have developed so far perfectly allow us to cover the nth degree congruence

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

The following theorem is a significant generalization of Theorem 27.4.1 (Euler's Criterion).

THEOREM 21.4.1. *Consider an integer a and a prime p so that $p \nmid a$. The following are equivalent:*

(i) *The congruence*

$$x^n \equiv a \pmod{p}$$

has a solution.

(ii) *The congruence*

$$\frac{p-1}{\operatorname{ord}_p(a)} \equiv 0 \pmod{\gcd(n, p-1)}$$

holds.

(iii) *The congruence*

$$a^{\frac{p-1}{\gcd(n,p-1)}} \equiv 1 \pmod{p}$$

holds.

If the first condition holds, then the congruence $x^n \equiv a$ has exactly $d := \gcd(n, p-1)$ solutions.

Proof by primitive roots. Let $m := (p-1)/\operatorname{ord}_p(a)$, and consider a primitive root g modulo p such that

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

Then the congruence

$$x^n \equiv a \pmod{p}$$

is solvable if there exists an integer t such that

$$g^{tn} \equiv g^m \pmod{p}.$$

In other words, the first congruence is solvable if and only if the congruence

$$tn \equiv m \pmod{p-1}$$

is solvable. It follows from Theorem 9.1.2 that this congruence is solvable if and only if $d := \gcd(n, p-1) \mid m$, and in this case there are exactly d solutions. Thus we have shown that *1.* is equivalent to *2.*

To show that *3.* is equivalent to *2.*, consider the condition that

$$a^{\frac{p-1}{\gcd(n,p-1)}} \equiv 1 \pmod{p}.$$

This holds if and only if $\frac{m(p-1)}{\gcd(n,p-1)}$ is an integer multiple of $p-1$, which is equivalent to the condition that $\gcd(n, p-1) \mid m$. □

Proof by Lagrange's theorem. For both directions of the proof, we will write $d := \gcd(n, p-1)$, so that there are integers k and l such that $kd = p-1$ and $ld = n$. It follows that k and l are relatively prime, so that there are integers u and v such that

$$ku + lv = 1.$$

To prove the forward implication, assume that x is an integer such that $x^n \equiv a \pmod{p}$. Then we have by Theorem 16.1.1 (Fermat's Little Theorem)

$$a^k \equiv x^{kn} = x^{kld} = (x^{p-1})^l \equiv 1^l = 1 \pmod{p}.$$

Since $k = (p-1)/\gcd(n, p-1)$, we have proven the forward implication.

For the converse, assume that $a^k \equiv 1 \pmod{p}$. Now we can use the formula for the difference of kth powers to write

$$x^{p-1} - 1 = x^{kd} - 1 \equiv x^{kd} - a^k = (x^d - a) \sum_{i=0}^{k-1} x^{di} a^{k-1-i}.$$

Since the polynomial $x^{p-1} - 1$ has exactly $p - 1$ roots modulo p, it follows that the number of roots of each factor on the right-hand side is equal to its degree. In other words, the polynomial

$$x^d - a$$

has d roots. Given a root $x^d \equiv a \pmod{p}$, we define $y := x^v$ where $ku + lv = 1$. Then we have

$$y^n = x^{vld} \equiv a^{lv} \equiv a^{1-ku} \equiv a(a^k)^{-u} \equiv a1^{-u} \equiv a \pmod{p}. \qquad \square$$

COROLLARY 21.4.2. *Consider an integer a such that $\operatorname{ord}_p(a) \mid n$. Then the congruence*

$$x^n \equiv a \pmod{p}$$

is solvable if and only if

$$p \equiv 1 \pmod{\operatorname{ord}_p(a) \cdot \gcd(n, p-1)}.$$

COROLLARY 21.4.3. *Consider a prime p and a natural number n relatively prime to $p-1$. Then every nth degree congruence*

$$x^n \equiv a \pmod{p}$$

has a unique solution. In other words, the map $x \mapsto x^n$ is a bijection on $\mathbb{Z}/p\mathbb{Z}$.

In the following corollary, we show that the congruence $x^n \equiv -1 \pmod{p}$ is solvable if and only if the 2-adic valuation of n is strictly smaller than the 2-adic valuation of $p - 1$. In other words, for any number $n = 2^k m$ with m odd, the congruence

$$x^n \equiv -1 \mod p$$

is solvable if and only if $p \equiv 1 \pmod{2^{k+1}}$.

COROLLARY 21.4.4. *The congruence*

$$x^n \equiv -1 \pmod{p}$$

is solvable if and only if $v_2(n) < v_2(p-1)$.

PROOF. Since the congruence $x^n \equiv -1 \pmod{p}$ is solvable if and only if

$$(-1)^{\frac{p-1}{\gcd(n,p-1)}} \equiv 1 \pmod{p},$$

it suffices to show that the exponent $\frac{p-1}{\gcd(n,p-1)}$ is an even integer if and only if $v_2(n) < v_2(p-1)$. Indeed, this exponent is even if and only if $\min(v_2(n), v_2(p-1)) = v_2(\gcd(n, p-1)) < v_2(p-1)$. This strict inequality holds if and only if $v_2(n) < v_2(p-1)$. $\square$

Exercises

Starter Exercises

21.1 (a) Find the least primitive root g modulo 23, and give a table of the congruence classes of its powers.
(b) Find all primitive roots modulo 23.
(c) For each $k \mid \phi(23)$, find all elements of order k modulo 23.
(d) For each integer $1, \ldots, 22$, find its index base g modulo 23.
(e) Solve the linear congruence

$$8x \equiv 9 \pmod{23}$$

using indices.

21.2 (a) Show that the number of solutions to the congruence

$$x^n \equiv a \pmod{p}$$

is either $\gcd(n, p-1)$ or 0.
(b) Find, as Gauss did in article 60 of *Disquisitiones Arithmeticae* [Gau1986], all the solutions to the congruence

$$x^{15} \equiv 11 \pmod{19}.$$

Routine-Building Exercises

21.3 In article 55 of *Disquisitiones Arithmeticae* [Gau1986], Gauss gives a second, more explicit construction of primitive roots. In this exercise we will follow this method.
Consider a prime p and suppose that the prime factorization of $p-1$ is

$$p - 1 = q_1^{\alpha_1} \cdots q_n^{\alpha_n}.$$

(a) By Theorem 20.3.2 (Lagrange's Theorem) it follows that for each prime q_i, the congruence

$$x^{\frac{p-1}{q_i}} \equiv 1 \pmod{p}$$

has strictly fewer than $p-1$ solutions, so there must exist a residue x which is not a solution. Using such x, construct an element a_i such that

$$\operatorname{ord}_p(a_i) = q_i^{\alpha_i}.$$

(b) Show that

$$\operatorname{ord}_p(a_1 \cdots a_n) = p - 1$$

and conclude that the product $a_1 \cdots a_n$ is a primitive root.



(c) Use this method to find a primitive root modulo 67.

21.4 Consider a prime $p \neq 3$. Prove that the product of all primitive roots modulo p is congruent to 1 modulo p.

21.5 (a) Consider a prime number p. Show that the following are equivalent:

(i) There is a solution to the congruence

$$x^n \equiv a \pmod{p}$$

of the form $x = a^k$.

(ii) The exponent n is relatively prime to $\operatorname{ord}_p(a)$.

(b) Find a solution to the congruence

$$x^3 \equiv 5 \pmod{13}$$

of the form $x = 5^k$.

21.6 Consider a prime p with a primitive root g, and let $d \mid p-1$. Prove the congruence

$$\sum_{\substack{0 \leq m < p-1 \\ m \equiv 0 \pmod{d}}} g^m \equiv \left\lfloor \frac{d}{p-1} \right\rfloor \pmod{p}.$$

Challenge Exercises

21.7 For any prime p and any integer a not divisible by p, show that the number of primitive roots g modulo p such that

$$g^{\frac{p-1}{\operatorname{ord}_p(a)}} \equiv a \pmod{p}.$$

is $\phi(p-1)/\phi(\operatorname{ord}_p(a))$. Conclude that such a primitive root always exists.

21.8 Consider a prime $p > 2$ and an odd number m. Show that the congruence $x^{2^n m} \equiv -1 \pmod{p}$ is solvable if and only if $p \equiv 1 \pmod{2^{n+1}}$.

21.9 Consider a prime p of the form $n^2 + 1$. Show that

$$x^n \equiv a \pmod{p} \text{ is solvable} \quad \Leftrightarrow \quad a^n \equiv 1 \pmod{p}.$$

21.10 [GAU1986, art. 81] Consider a prime p. Prove that the sum of all primitive roots satisfies the following property:

$$\sum_{g \text{ primitive root } \pmod{p}} g \equiv \mu(p-1) \pmod{p}.$$

21.11 [GAU1986, art. 78] For any positive integer n, show that

$$\prod_{\substack{0 < x < n \\ \gcd(x,n) = 1}} x \equiv \begin{cases} -1 \pmod{n} & \text{if there is a primitive root modulo } n, \\ 1 \pmod{n} & \text{otherwise.} \end{cases}$$

Hint: Use Theorem 9.3.1 (Chinese Remainder Theorem) to show that the number of integers $0 \leq x < n$ such that $x^2 \equiv 1 \pmod{n}$ is a power of 2.

Chapter 22

The Moduli with Primitive Roots

We have established the existence of primitive roots modulo any prime. In this section, we will give a complete characterization of those moduli for which a primitive root exists.

22.1 Primitive Roots Modulo Odd Prime Powers

Our first target is to show that any odd prime power p^k has a primitive root. Our approach to this problem is of an arithmetic nature, based on an analysis of the p-valuations of differences of powers.

Recall that for any integer a not divisible by p, the integer $a^{p-1}-1$ is divisible by p by Theorem 16.1.1. Therefore, its p-adic valuation $\alpha := v_p(a^{p-1}-1)$ is at least 1. In the following lemma we will establish that the order of a modulo p^k can be determined in terms of α.

Lemma 22.1.1. *Consider an odd prime p and a primitive root g modulo p. Furthermore, let*

$$m := v_p(g^{p-1}-1).$$

Then the order of g modulo p^k is $p^{\max(0,k-m)}(p-1)$.



PROOF. First, we observe that $\operatorname{ord}_p(g) \mid \operatorname{ord}_{p^k}(g)$, so the order of g modulo p^k must be a multiple of $p-1$. Write $g^{p-1} = kp^m + 1$, so that $p \nmid k$. By Theorem 19.5.2 (Lifting the Exponent) it follows that

$$v_p(g^{p^t(p-1)} - 1) = m + t.$$

Consequently, for any integer s not divisible by p we have

$$g^{p^t s(p-1)} = (kp^{m+t} + 1)^s \equiv 1 + skp^{m+t} \pmod{p^{m+t+1}}.$$

This shows that $v_p(g^{p^t s(p-1)} - 1) = m + t$ for such s. The first exponent r such that $g^r \equiv 1 \pmod{p^k}$ is therefore $r = p^{\max(0,k-m)}(p-1)$. □

THEOREM 22.1.2. *Any prime power p^k with $k \geq 1$ admits a primitive root.*

PROOF. By Lemma 22.1.1 it suffices to construct a primitive root h modulo p such that $v_p(h^{p-1} - 1) = 1$.

Consider a primitive root g modulo p. Write $g^{p-1} = kp+1$, and define $h_t := g+tp$. Then we have

$$h_t^{p-1} = (g + tp)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}tp \equiv 1 + p(k - g^{p-2}t) \pmod{p^2}.$$

Thus we see that $h_t^{p-1} \equiv 1 \pmod{p^2}$ if and only if

$$k \equiv g^{p-2}t \pmod{p}.$$

This linear congruence has the unique solution $t \equiv kg \pmod{p}$. Thus we see that for any $t \not\equiv kg \pmod{p}$, we have $h_t^{p-1} \not\equiv 1 \pmod{p^2}$ and hence

$$v_p(h_t^{p-1} - 1) = 1.$$ □

22.2 The Complete Characterization of Moduli with Primitive Roots

THEOREM 22.2.1. *Consider a positive integer n. The following are equivalent:*

(i) *The number n admits a primitive root.*

(ii) *Either $n = 2$, or there is a unique element of order 2 modulo n.*

(iii) *We have*

$$n = 2,\ 4,\ p^k,\ \text{or}\ 2p^k,$$

where p is an odd prime.

Proof. We saw in Theorem 21.2.2 that if n admits a primitive root, then the congruence

$$x^d \equiv 1 \pmod{n}$$

had at most d solutions, for any $d \geq 0$. In particular, there are at most two solutions to the congruence $x^2 \equiv 1 \pmod{n}$. One of them is the number 1, which is of order 1. The other is -1, which is of order 2. Since any element of order 2 is a solution to the congruence $x^2 \equiv 1 \pmod{n}$, we see that i implies ii.

Next, assume that there is a unique element of order 2 modulo n. The case $n = 4$ is swiftly dealt with, since -1 is the unique integer of order 2 modulo 4. If $n = 2^k$ for some $k \geq 3$, then there are three integers of order 2 modulo 2^k:

$$x = -1 \qquad \text{and} \qquad x = 2^{k-1} \pm 1.$$

Thus we see that if $n = 2^k$ for some $k \geq 3$, then n does not satisfy the hypothesis in ii.

Now suppose that $n = km$, where $\gcd(k, m) = 1$ and m is odd and strictly greater than 1. By Theorem 9.3.1 (Chinese Remainder Theorem), it follows that any pair of solutions

$$x^2 \equiv 1 \pmod{k},$$
$$y^2 \equiv 1 \pmod{m},$$

determines a unique solution to the congruence $z^2 \equiv 1 \pmod{km}$. It follows that one of them can have only one nontrivial solution. Since we assumed that $m > 1$ is odd, and thus has two distinct solutions, it follows that there is only one solution to the congruence $x^2 \equiv 1 \pmod{k}$. Observe that there is only one such solution if and only if $k = 1$ or $k = 2$. Furthermore, the previous observation implies that m cannot have distinct prime factors, so we conclude that m must be of the form $m = p^k$ for some odd prime p. Thus we have proven that ii implies iii.

Finally, we have to show that any number of the form $n = 2, 4, p^k$, or $2p^k$, where p is an odd prime, admits a primitive root. The number 1 is a primitive root modulo 2, and the number -1 is a primitive root modulo 4. The fact that any odd prime power p^k admits primitive roots was established in Theorem 22.1.2. To finish the proof that iii implies i, it therefore remains to show that each number of the form $n = 2p^k$, where p is an odd prime, has a primitive root. To see this, observe that the integers relatively prime to $2p^k$ are exactly the odd integers $1 \leq x < 2p^k$ relatively prime to p^k. Among those odd integers is a primitive root g modulo p^k. Its order modulo $2p^k$ is

$$\operatorname{ord}_{2p^k}(g) = \operatorname{ord}_{p^k}(g) = p^{k-1}(p-1) = \phi(2p^k),$$

so we see that g is also a primitive root of $2p^k$. □

22.3 Carmichael's Function



Chapter 23

Polynomial Congruences

23.1 Polynomial Congruences of Composite Moduli

In the following theorem we generalize Theorem 9.3.1 (Chinese Remainder Theorem) to polynomial congruences.

Theorem 23.1.1. *Consider an integer polynomial f and consider two relatively prime integers m and n. Then any solution of the system*

$$f(x) \equiv 0 \pmod{m}$$
$$f(x) \equiv 0 \pmod{n}$$

of polynomial congruences corresponds uniquely to a solution of the polynomial congruence

$$f(x) \equiv 0 \pmod{mn}.$$

Proof. First note that if $f(x) \equiv 0 \pmod{mn}$, then it follows that $f(x) \equiv 0 \pmod{m}$ and $f(x) \equiv 0 \pmod{n}$, simply because divisibility is transitive. Consequently, if y is the unique nonnegative integer strictly below m such that $x \equiv y \pmod{m}$, then $f(y) \equiv \pmod{m}$ is also a solution, and similar for the modulus n. Thus if we write $N_{mn}(f)$ for the set of roots of f modulo mn, and $N_m(f)$ and $N_n(f)$ for the sets of roots of f modulo m and n, respectively, then we define a map

$$\pi : N_{mn}(f) \to N_m(f) \times N_n(f)$$

by $x \mapsto (x \pmod{m}, x \pmod{n})$. We claim that the map π is a bijection.

To see that the map π is a bijection, consider $0 \leq y < m$ and $0 \leq z < n$ such that

$$f(y) \equiv 0 \pmod{m}$$
$$f(z) \equiv 0 \pmod{n}.$$

By the assumption that $\gcd(m, n) = 1$, we obtain from Theorem 9.3.1 (Chinese Remainder Theorem) there a unique $0 \leq x < mn$ such that

$$x \equiv y \pmod{m}$$
$$x \equiv z \pmod{n}.$$

Consequently, we have that $f(x) \equiv 0 \pmod{m}$ and $f(x) \equiv 0 \pmod{n}$. Applying the Chinese Remainder Theorem once more to the number $f(x)$, using that 0 is the only integer u modulo mn such that $u \equiv 0 \pmod{m}$ and $u \equiv 0 \pmod{n}$, we find that $f(x) \equiv 0 \pmod{mn}$. □

COROLLARY 23.1.2. *Consider $n = p_1^{k_1} \cdots p_m^{k_m}$, where all the primes p_i are distinct. A polynomial congruence*

$$f(x) \equiv 0 \pmod{n}$$

is solvable if and only if the polynomial congruence

$$f(x) \equiv 0 \left(\mathrm{mod}\ p_i^{k_i}\right)$$

is solvable for each i.

PROOF. By induction on the number of prime factors of n. □

23.2 Derivatives of Polynomials

The derivative of a function f at a point x, if it exists, measures the rate of change of f in close vicinity of x. It is formally defined as the limit

$$f'(x) := \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

Intuitively, such a limit exists if we can determine a unique value $y = f'(x)$ so that the quanitity $(f(x+h) - f(x))/h$ gets arbitrarily close to y as h gets arbitrarily close to 0. When such a limit exists for every x, we say that f is **differentiable**. Many of the most common functions are differentiable, except at obvious points of discontinuity as seen, for instance, in step functions, or functions with sudden change of direction such as the absolute value function. In this short section we will prove that all polynomials are differentiable. There is an important theorem in number theory that require knowledge of the derivatives of polynomials: In our proof of Theorem 23.3.1 (Hensel's Lemma) we will make use of Theorem 23.2.3 (Taylor Expansion Theorem for Polynomials) proven below.

The following theorem is not only useful when h approaches 0. For example, in the case where h is a prime p it tells us that $f(x+p) - f(x)$ is always a multiple of p.

Theorem 23.2.1. *Consider the polynomial*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Then the polynomial $f(x+h) - f(x)$ is divisible by h, with quotient

$$\frac{f(x+h)-f(x)}{h} = \sum_{k=1}^{n} \sum_{i=0}^{k-1} a_k x^i (x+h)^{k-1-i}.$$

Proof. By the formula for the difference of kth powers, which was stated in Exercise 2.5, we can write

$$(x+h)^k - x^k = h \sum_{i=0}^{k-1} x^i (x+h)^{k-1-i}$$

In particular, since each of these differences of kth powers is divisible by h, we see that the polynomial $f(x+h) - f(x)$ is divisible by h. It follows that

$$f(x+h) - f(x) = \sum_{k=0}^{n} a_k ((x+h)^k - x^k) = h \sum_{k=1}^{n} a_k \sum_{i=0}^{k-1} x^i (x+h)^{k-1-i}. \qquad \square$$

Theorem 23.2.2. *Consider the polynomial $f(x) = a_n x^n + \cdots + a_0$. Then f is differentiable at every x, and the derivative can be computed by the formula*

$$f'(x) = \sum_{k=1}^{n} k a_k x^{k-1}.$$

Proof. Since polynomials are continuous functions, we can compute the limit as $h \to 0$ simply by evaluating the quotient of $f(x+h) - f(x)$ divided by h at 0:

$$f'(x) = \sum_{k=1}^{n} \sum_{i=0}^{k-1} a_k x^i (x+0)^{k-1-i} = \sum_{k=1}^{n} \sum_{i=0}^{k-1} a_k x^{k-1} = \sum_{k=1}^{n} k a_k x^{k-1}$$

In the last equality we used that the summands in the inner summation do not depend on the summation index i. $\square$

The derivative of any polynomial $f(x)$ is again a polynomial. An immediate consequence of the previous theorem is that if $h(x) = af(x) + bg(x)$ is a linear combination of the polynomials $f(x)$ and $g(x)$, then the derivative of h can be written as the linear combination

$$h'(x) = af'(x) + bg'(x).$$

It also follows that, since the derivative is again a polynomial, it is again differentiable. Thus we have iterated derivatives of polynomials. We will write $\frac{d^k}{dx^k} f(x)$ or $f^{(k)}(x)$ for the kth deriviative of $f(x)$. A straightforward induction argument shows that

$$\frac{d^k}{dx^k} x^n = n(n-1)\cdots(n-k+1)x^{n-k}.$$



We can phrase this identity equivalently as:

$$\frac{1}{k!}\frac{d^k}{dx^k}x^n = \binom{n}{k}x^{n-k}.$$

This leads to the following theorem by Brook Taylor, who stated the result more generally in terms of *fluent quantities* in his work *Methodus incrementorum directa et inversa* [TAY1715]. Although Taylor was the first to prove the series expansion that now bears his name, the method was discovered first without proof by James Gregory, who shared his insight in a letter to John Collins in 1671 [GRE1671]. More on the history of Taylor series can be found in [FEI1985].

THEOREM 23.2.3 (Taylor Expansion Theorem for Polynomials). *Consider the polynomial*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Then we have for each y, the identity

$$f(x+y) = \sum_{k=0}^{n} \frac{f^{(k)}(x)}{k!}y^k.$$

In particular, there is a polynomial $g(x,y)$ in the variables x and y, such that

$$f(x+y) = f(x) + yf'(x) + y^2 g(x,y).$$

PROOF. We will first prove the theorem for $f(x) := x^n$. By Theorem 3.5.1 (The Binomial Theorem) and our earlier observation that $\frac{1}{k!}\frac{d^k}{dx^k}x^n = \binom{n}{k}x^{n-k}$, it follows that

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k = \sum_{k=0}^{n}\frac{1}{k!}\frac{d^k x^n}{dx^k}y^k.$$

This shows that the Taylor expansion formula holds for $f(x) = x^n$. The general claim follows, since every polynomial is a linear combination of polynomials of the form x^i and differentiation preserves linear combinations. Finally, observe that

$$f(x+y) = f(x) + yf'(x) + y^2\sum_{k=2}^{n}\frac{f^{(k)}(x)}{k!}y^{k-2}.$$

This completes the proof of the final claim. □

23.3 Hensel's Lemma

THEOREM 23.3.1 (Hensel's Lemma). *Consider a prime number p and a polynomial $f(x)$ with integer coefficients. Furthermore, consider an integer a such that*

$$f(a) \equiv 0 \pmod{p} \qquad \textit{and} \qquad f'(a) \not\equiv 0 \pmod{p},$$

where $f'(x)$ is the derivative of f. Then there exists for every $k \geq 1$ a unique integer a_k modulo p^k with $a_1 \equiv a \pmod{p}$ such that the congruences

$$a_{k+1} \equiv a_k \pmod{p^k}, \qquad \text{and} \qquad f(a_k) \equiv 0 \pmod{p^k}$$

hold for all k.

Proof. We prove the claim by induction. That is, we prove by induction that for each $k \geq 1$ and every integer $a_k \equiv a \pmod{p}$ satisfying

$$f(a_k) \equiv 0 \pmod{p^k} \qquad \text{and} \qquad f'(a_k) \not\equiv 0 \pmod{p^k},$$

there is a unique integer $a_{k+1} \pmod{p^{k+1}}$ satisfying

$$f(a_{k+1}) \equiv 0 \pmod{p^{k+1}} \qquad \text{and} \qquad f'(a_{k+1}) \not\equiv 0 \pmod{p^{k+1}}.$$

Our goal is to obtain an integer $a_{k+1} = a_k + tp^k$ for some $0 \leq t < p$. Observe that by Theorem 23.2.3 (Taylor Expansion Theorem for Polynomials), we have the congruence

$$f(a_k + tp^k) \equiv f(a_k) + tp^k f'(a_k) \pmod{p^{k+1}}.$$

Since $f(a_k) \equiv 0 \pmod{p^k}$ and $f'(a_k) \not\equiv 0 \pmod{p^k}$, it follows that there is a unique integer t_0 such that

$$f(a_k) + t_0 p^k f'(a_k) \equiv 0 \pmod{p^{k+1}}.$$

We define $a_{k+1} := a_k + t_0 p^k$. Then we have $f(a_{k+1}) \equiv 0 \pmod{p^{k+1}}$ by definition. Furthermore, we have $a_{k+1} \equiv a_k \equiv a \pmod{p}$. This implies that $f'(a_{k+1}) \equiv f'(a) \not\equiv 0 \pmod{p}$. Therefore it follows that $f'(a_{k+1}) \not\equiv 0 \pmod{p^{k+1}}$, completing the proof. □

23.4 The Elementary Symmetric Polynomials

Using the fact that equivalent reduced polynomials must be congruent, we obtain the following factorization of the polynomial $x^{p-1} - 1$ in $\mathbb{Z}/p\mathbb{Z}$, which has roots at the numbers $1, \ldots, p-1$.

Theorem 23.4.1. *Consider a prime p. Then we have*

$$x^{p-1} - 1 \equiv (x-1)\cdots(x-p+1) \pmod{p}$$

for every x. Hence their coefficients are congruent.

Proof. Both polynomials are equivalent and reduced, so they must be congruent. □

The previous theorem provides another way of proving Theorem 16.3.1 (Wilson's Theorem). This proof is due to Lagrange, who was the first to publish a proof of Wilson's theorem.



PROOF OF THEOREM 16.3.1 (WILSON'S THEOREM). The integer $(p-1)!$ is the constant coefficient of the polynomial $(x-1)\cdots(x-p+1)$, which is congruent to the polynomial $x^{p-1}-1$ with constant coefficient -1. □

Using the elementary symmetric polynomials, we find another way of stating Theorem 23.4.1:

THEOREM 23.4.2. *For each prime p and each $1 \leq k < p-1$ we have*

$$e_k(1,\ldots,p-1) \equiv 0 \pmod{p}.$$

23.5 Reduced Polynomials Modulo a Prime

DEFINITION 23.5.1. Two polynomials $f(x)$ and $g(x)$ are said to be **congruent** modulo a prime p if their coefficients are congruent modulo p.

DEFINITION 23.5.2. Two polynomials $f(x)$ and $g(x)$ are said to be **equivalent** modulo a prime p if for each integer x the polynomial congruence

$$f(x) \equiv g(x) \pmod{p}$$

holds.

DEFINITION 23.5.3. A polynomial $f(x)$ is said to be **reduced** modulo p if it is of degree less than p.

THEOREM 23.5.4. *Any two equivalent reduced polynomials modulo p are congruent.*

PROOF. Consider two equivalent reduced polynomials $f(x)$ and $g(x)$. Then $f(x)-g(x)$ is a reduced polynomial equivalent to 0. However, if $f(x)-g(x)$ were nonzero then its number of roots would be strictly less than p. Since the number of roots is p, it follows that $f(x)-g(x)$ is congruent to the zero polynomial. □

THEOREM 23.5.5. *For every polynomial $f(x)$ there is a unique reduced polynomial $g(x)$ equivalent to $f(x)$.*

Chapter 24

Divisibility and Irreducibility of Polynomials

24.1 Primitive Polynomials and Gauss's Lemma

In Theorem 10.2.1 we showed that unless n is a perfect square, the square root of n is irrational. In other words, the roots of the polynomial

$$x^2 - n$$

are either integers or irrational numbers. Theorem 24.1.3 (Gauss's Lemma for Polynomials) is a generalization of this observation, with the consequence that the roots of a polynomial such as

$$f(x) = x^3 - 3x^2 + 3x - 2$$

are either integers or irrational. The crucial property, besides f having integer coefficients, is that the leading coefficient is 1. Such polynomials are called **monic**. Note that the polynomial $x^2 - n$ of our previous example is also monic.

Before we can proceed to stating and proving Gauss's Lemma, we introduce Gauss's concept of primitive polynomials and prove a key property about them.

Definition 24.1.1. A polynomial $f(x)$ with integer coefficients is said to be **primitive** if the greatest common divisor of its coefficients is 1.

Theorem 24.1.2. *The product of two primitive polynomials is primitive.*



PROOF. Consider two primitive polynomials

$$g(x) := \sum_{i=0}^{m} b_i x^i \qquad \text{and} \qquad h(x) := \sum_{j=0}^{n} c_j x^j,$$

and let $f(x) := g(x)h(x)$ be their product. The coefficients for $f(x)$ are given by

$$a_n := \sum_{k=0}^{n} b_{n-k} c_k.$$

If f is not primitive, then there is a prime p such that $p \mid a_n$ for each coefficient a_n. However, since $g(x)$ and $h(x)$ are primitive, there are least indices i_0 and j_0 such that $p \nmid b_{i_0}$ and $p \nmid c_{j_0}$. Now observe that

$$a_{i_0+j_0} = \sum_{k=0}^{i_0+j_0} b_{i_0+j_0-k} c_k \equiv b_{i_0} c_{j_0} \not\equiv 0 \pmod{p},$$

where the first congruence holds because $p \mid c_k$ for $k < j_0$ and $p \mid b_{i_0+j_0-k}$ for $k > j_0$. This is a contradiction, since we have assumed that $p \mid a_{i_0+j_0}$. We conclude that f is primitive. □

THEOREM 24.1.3 (Gauss's Lemma for Polynomials). *Consider a monic polynomial $f(x)$ with integer coefficients, and let $g(x)$ and $h(x)$ be two polynomials with rational coefficients satisfying the polynomial identity*

$$f(x) = g(x)h(x).$$

Then the coefficients of both $g(x)$ and $h(x)$ are integers.

PROOF. Since $g(x)$ and $h(x)$ are polynomials with rational coefficients, there are least positive integers c and d such that $cg(x)$ and $dh(x)$ are polynomials with integer coefficients. Note that $cg(x)$ and $dh(x)$ are primitive polynomials, hence their product

$$cd\,f(x) = (cg(x))(dh(x))$$

is again primitive. Since the integer cd divides each coefficient of $cd\,f(x)$, it follows that $cd = 1$. We conclude that $c = d = 1$. In other words, $g(x)$ and $h(x)$ had integer coefficients to start with. □

COROLLARY 24.1.4. *Suppose $f(x)$ is a monic polynomial with integer coefficients. Then any rational root r is an integer.*

PROOF. If r is a rational root, then it follows from Theorem 20.2.2 (Factor Theorem) that $f(x)$ factors as

$$f(x) = (x - r)g(x),$$

where $g(x)$ is a polynomial with rational coefficients. By Theorem 24.1.3 (Gauss's Lemma for Polynomials) it follows that $x - r$ is a polynomial with integer coefficients; that is, r is an integer. □

24.2 Euclid's Algorithm for Polynomials

Example 24.2.1. Consider the polynomials $f(x) = x^4 + x^2 + 1$ and $g(x) = x^2 + x + 1$. We can apply the ideas behind Theorem 5.3.1 (The Euclidean Division Theorem) to divide out $g(x)$ from $f(x)$ as best we can. To do this, we first write

$$x^4 + x^2 + 1 = x^2(x^2 + x + 1) - x^3 + 1.$$

In the same manner, we can divide out $x^2 + x + 1$ from $-x^3 + 1$:

$$-x^3 + 1 = -x(x^2 + x + 1) + x^2 + x + 1.$$

Finally, we note that the remainder $x^2 + x + 1$ is equal to $g(x)$. For completeness sake, we write the final step:

$$x^2 + x + 1 = 1(x^2 + x + 1) + 0.$$

Having reached 0, the process terminates here. As a parenthetical remark, we note that the process could also have terminated by reaching in the remainder a polynomial of strictly smaller degree than the degree of $g(x)$. Combining the previous calculations, we obtain the polynomial identity

$$x^4 + x^2 + 1 = (x^2 - x + 1)(x^2 + x + 1).$$

The process we have exhibited here is called **Euclidean division** or **long division** for polynomials.

Definition 24.2.2. We say that a polynomial $g(x)$ **divides** a polynomial $f(x)$ if there is a polynomial $h(x)$ such that

$$f(x) = g(x)h(x).$$

Theorem 24.2.3 (Euclidean Division for Polynomials). *Consider two polynomials $f(x)$ and $g(x)$ with coefficients in an integral domain, and assume that $g(x)$ is a monic polynomial of degree m. Then we can determine unique polynomials $q(x)$ and $r(x)$ satisfying the polynomial identity*

$$f(x) = q(x)g(x) + r(x),$$

such that $\deg(r(x)) < m$.

Proof. The proof is by induction on the degree of $f(x)$. If $\deg(f(x)) < m$, then we simply choose $q(x) = 0$ and $r(x) = f(x)$. These choices are forced, since the degree of any nonzero multiple of $g(x)$ is at least the degree of $g(x)$.

Now suppose that the claim holds for any polynomial of degree $< m + n$, and let $f(x)$ be of degree $m + n$ with leading coefficient a. Then

$$h(x) = f(x) - ax^n g(x)$$



has degree $< m+n$. Consequently, there are unique polynomials $q(x)$ and $r(x)$ of degree $< m$ satisfying the polynomial identity

$$h(x) = q(x)g(x) + r(x).$$

It follows that

$$f(x) = (ax^n + q(x))g(x) + r(x).$$

It remains to show that this choice of polynomials is uniquely determined. Let $p(x)$ and $s(x)$ be polynomials with $\deg(s(x)) < m$ satisfying the polynomial identity $f(x) = p(x)g(x) + s(x)$. Let b be the leading coefficient of $p(x)$. Since $g(x)$ was assumed to be monic, it follows that b is then the leading coefficient of $p(x)g(x)$. Moreover, since $\deg(s(x)) < m$ we see that the leading coefficient of $p(x)g(x)+s(x)$ is b, so we conclude that $a = b$. It also follows by these same considerations that $\deg(p(x)) = n$. Now we see that

$$(p(x) - ax^n)g(x) + s(x) = f(x) - ax^n g(x) = h(x) = q(x)g(x) + r(x).$$

This shows that $s(x) = r(x)$ and $ax^n + q(x) = p(x)$, completing the proof of uniqueness. □

24.3 Irreducible Polynomials

DEFINITION 24.3.1. A polynomial $f(x)$ with coefficients in R is said to be **irreducible** if it cannot be written in the form

$$f(x) = g(x)h(x)$$

where neither $g(x)$ nor $h(x)$ are constant at an invertible element of R.

Theorem 24.1.3 (Gauss's Lemma for Polynomials) can be stated in the form of an irreducibility criterion:

COROLLARY 24.3.2. *Consider a monic polynomial $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is irreducible as a polynomial with integer coefficients, then it is also irreducible as a polynomial with rational coefficients.*

COROLLARY 24.3.3. *Consider a primitive polynomial $f(x)$ with integer coefficients, and consider a prime p such that the leading coefficient of $f(x)$ is not divisible by p. Let $\bar{f}(x) \in (\mathbb{Z}/p)[x]$ be the reduction of $f(x)$ to $\mathbb{Z}/p$. If $\bar{f}(x)$ is irreducible in $(\mathbb{Z}/p)[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.*

EXAMPLE 24.3.4. Consider the polynomial $f(x) = x^2 - x + 1$. This is a quadratic polynomial, so it is only reducible in $\mathbb{Q}[x]$ if it has rational roots. Note that any root would have to be a root modulo 5 as well. However, a quick calculation shows that $f(a) \not\equiv 0 \pmod 5$ for each integer $0 \leq a < 5$. Therefore, it follows that $f(x)$ is irreducible modulo 5, and this is sufficient to conclude that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example 24.3.5. Our next example is due to Georg Pólya, who showed that the polynomial

$$P_n(x) := (x+1)\cdots(x+n)+1$$

is irreducible in $\mathbb{Z}[x]$ for all $n \neq 4$ [Pól1919]. In the case $n = 4$ we have the factorization

$$(x+1)(x+2)(x+3)(x+4)+1 = (x^2+5x+5)^2.$$

Knowing that the polynomial $P_n(x)$ is irreducible for $n \neq 4$ is consistent with the conjecture that infinitely many numbers of the form $n!+1$ are prime. Primes of the form $n! \pm 1$ are called **factorial primes**. Even though it is still a long way to proving the conjecture, Pólya's observation rules out the simplest algebraic obstruction: The number $P_n(0) = n!+1$ is not automatically composite for purely polynomial reasons.

Note that a polynomial $f(x)$ is irreducible in $\mathbb{Z}[x]$ if and only if every translation $f(x+a)$ is also irreducible. In other words, translations have no effect on the irreducibility of a polynomial. We use this to bring Pólya's polynomial to slightly more convenient form. We define

$$H_n(x) := (x-1)\cdots(x-n)+1,$$

so that $P_n(x) = H_n(x+n+1)$.

Suppose that $H_n(x) = f(x)g(x)$ for two integer polynomials $f(x)$ and $g(x)$ of degree ≥ 1. Since $H_n(k) = 1$ for every $1 \leq k \leq n$, it follows that

$$f(k)g(k) = 1$$

for every $1 \leq k \leq n$. This implies that either $f(k) = 1$ and $g(k) = 1$, or $f(k) = -1$ and $g(k) = -1$. In particular, we find that $f(k) = g(k)$ for each $1 \leq k \leq n$. Since $\deg(f), \deg(g) < n$, we conclude by Theorem 20.4.2 (Lagrange's Interpolation Theorem) that the polynomial identity $f(x) = g(x)$ holds. Therefore, it follows that

$$H_n(x) = f(x)^2,$$

and $n = 2m$, where m is the degree of f.

Now define the sets

$$I := \{1 \leq k \leq 2m \mid f(k) = 1\} \qquad \text{and} \qquad J := \{1 \leq k \leq 2m \mid f(k) = -1\}.$$

Note that I consists of the integer roots of $f(x)-1$, and J consists of the integer roots of $f(x)+1$. In particular, since the degree of $f(x)$ is m, it follows that $|I| \leq m$ and $|J| \leq m$. On the other hand, the union $I \cup J$ consists of all the numbers $1, \ldots, 2m$, so that $|I| + |J| = 2m$. This allows us to conclude that both I and J consist of exactly m elements, that I consists of all the roots of $f(x)-1$, and that J consists of all the roots of $f(x)+1$. Consequently, we have the polynomial identities

$$f(x)-1 = \prod_{i \in I}(x-i) \qquad \text{and} \qquad f(x)+1 = \prod_{j \in J}(x-j).$$



It follows that for each $i_0 \in I$, we have

$$\prod_{j \in J}(i_0 - j) = \prod_{j \in J}(i_0 - j) - \prod_{i \in I}(i_0 - i) = 2.$$

This integer factorization of 2 shows that the distance $|i_0 - j| \leq 2$ for every integer $j \in J$. Now observe that when J contains at least three integers, then there is at most one integer distinct from all the integers in J such that $|x - j| \leq 2$ for all $j \in J$. However, since I and J contain the same number of elements, this shows that J cannot contain 3 or more integers. We conclude that $m \leq 2$.

We have shown so far that if $P_n(x)$ factors as a product of two polynomials, then $n = 2m$ for $1 \leq m \leq 2$. To finish the proof of Pólya's claim, it remains to show that $P_2(x)$ is irreducible. Reducing Pólya's polynomial $P_2(x)$ modulo 2 gives

$$(x+1)(x+2)+1 \equiv x^2 + x + 1 \pmod{2}.$$

Since quadratic polynomials are only reducible if they have roots, and this polynomial has no roots modulo 2, this immediately implies that $P_2(x)$ cannot have roots and is therefore irreducible.

24.4 Eisenstein's Criterion

THEOREM 24.4.1 (Eisenstein's Criterion). *Consider a polynomial $f(x) = a_n x^n + \cdots + a_0$ with integer coefficients. Suppose that there is a prime number p such that:*

(i) *The prime p is a prime divisor of a_i for every $0 \leq i < n$,*

(ii) *The coefficient a_n is not divisible by p,*

(iii) *The coefficient a_0 is not divisible by p^2.*

Then the polynomial f is irreducible in $\mathbb{Q}[x]$.

PROOF. First, we note that $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $\lambda f(x)$ is irreducible in $\mathbb{Q}[x]$, for any nonzero rational number λ. Taking $d := \gcd(a_0, \ldots, a_n)$ and $\lambda := 1/d$, then the polynomial $\lambda f(x)$ is primitive. Furthermore, $\lambda f(x)$ still satisfies the conditions of Eisenstein's criterion, since $p \nmid d$. Thus, we may assume that $f(x)$ is primitive. By Theorem 24.1.3 (Gauss's Lemma for Polynomials) it suffices to show that $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Suppose that $f(x)$ is reducible in $\mathbb{Z}[x]$, so that $f(x) = g(x)h(x)$ for two polynomials

$$g(x) = b_r x^r + \cdots + b_0 \qquad \text{and} \qquad h(x) = c_s x^s + \cdots + c_0$$

with integer coefficients, where r and s are positive integers such that $r + s = n$. Then we have

$$a_i = \sum_{\substack{j,k \\ i=j+k}} b_j c_k.$$

Since $a_0 = b_0c_0$ is divisible by p but not by p^2, it follows that exactly one of b_0 and c_0 is divisible by p. We will assume without loss of generality that p divides b_0. We claim that every coefficient of $g(x)$ is divisible by p. Using the identity

$$a_i = \sum_{\substack{j,k \\ i=j+k}} b_j c_k = (b_0c_j + \cdots + b_{i-1}c_1) + b_ic_0,$$

this claim follows by induction. Indeed, if $p \mid b_j$ for each $j < i$ and $p \mid a_i$, then we must have $p \mid b_ic_0$. Since we assumed that $p \nmid c_0$, we must have $p \mid b_i$.

However, it follows that $a_n = b_rc_s$ is divisible by p, which is in contradiction with the assumption that $p \nmid a_n$. □

Example 24.4.2. Consider two distinct integers a and b. We claim that the polynomial

$$f(x) = (x+a)^n - (x+b)^n$$

is irreducible if and only if n is prime.

If n is composite, say $n = km$, then we can factor $f(x)$ using the formula for the difference of mth powers:

$$f(x) = ((x+a)^k - (x+b)^k) \sum_{i=0}^{m-1} (x+a)^i (x+b)^{m-1-i}.$$

This shows that for composite n, the polynomial $f(x)$ is reducible.

It remains to show that $f(x)$ is irreducible if $n = p$, where p is prime. To see this, consider $c = a - b$ and the polynomial

$$g(x) = (x+c)^p - x^p.$$

Then we have $f(x) = g(x+b)$, so it follows that $f(x)$ is irreducible if and only if $g(x)$ is. Furthermore, we observe that rescaling also doesn't affect irreducibility in $\mathbb{Q}[x]$: A polynomial $F(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if the polynomial $F(qx)$ is irreducible, where q is a nonzero rational number. Note that

$$g(x) = c^p((x/c)+1)^p - (x/c)^p.$$

It follows that $g(x)$ is irreducible if and only if the polynomial

$$h(x) = (x+1)^p - x^p$$

is irreducible. Thus, it remains to show that the polynomial $h(x)$ is irreducible.

Example 24.4.3. For every prime p, the polynomial

$$f(x) := 1 + x + x^2 + \cdots x^{p-1}$$



is irreducible. Indeed, if we substitute $x = y + 1$ in

$$f(x) = \frac{x^p - 1}{x - 1},$$

we obtain

$$f(y+1) = \frac{(y+1)^p - 1}{y} = \sum_{i=0}^{p-1} \binom{p}{i+1} y^i.$$

This polynomial has coefficients $a_i = \binom{p}{i+1}$. Thus we see that

(i) The binomial coefficient $\binom{p}{i+1}$ is divisible by p for every $0 \leq i < p - 1$.

(ii) The binomial coefficient $\binom{p}{p} = 1$ is not divisible by p.

(iii) The binomial coefficient $\binom{p}{1} = p$ is not divisible by p^2.

Thus it follows from Eisenstein's criterion that $f(y + 1)$ is irreducible, which implies that $f(x)$ is irreducible.

EXAMPLE 24.4.4.

(i) Consider a prime p and an even integer $2 \leq n < p - 1$ such that $p \nmid B_n$. Then the polynomial

$$(x+1)^n + \cdots + (x+p-1)^n$$

is irreducible over $\mathbb{Q}$.

(ii) Show that the polynomial

$$x^6 + 3x^5 + 6x^4 + 9x^3 + 6x^2 + 3x^1 + 1$$

is irreducible over $\mathbb{Q}$.

(iii) Show that the polynomial

$$\frac{(x+2)^n - x^n - 2^n}{x}$$

is irreducible over $\mathbb{Q}$.

Exercises

Starter Exercises

24.1 Show that the following polynomials are irreducible in $\mathbb{Q}[x]$:

(a) $x^2 - x + 3$,
(b) $x^2 + 2x + 3$,
(c) $x^3 - x + 1$,
(d) $x^3 + 2x + 2$,
(e) $x^4 + 3x + 3$.

Routine-Building Exercises

24.2 Suppose that $f(x)$ is an irreducible polynomial of degree n, and consider a, b, c, d with $ad - bc \neq 0$. Show that the polynomial

$$g(x) = (cx + d)^n f\left(\frac{ax + b}{cx + d}\right)$$

is again irreducible.



Chapter 25

Cyclotomic Polynomials

25.1 The Primitive Factors of $x^n - 1$

Consider a prime factor p of $a^n - 1$. Since $p \mid a^n - 1$, it follows that $a^n \equiv 1 \pmod{p}$. By the Theorem 8.5.2 (Order Theorem) it follows that $\mathrm{ord}_p(a) \mid n$. By Theorem 16.1.1 (Fermat's Little Theorem) it follows that the order of a modulo p is itself a divisor of $p - 1$.

Definition 25.1.1. The nth **cyclotomic polynomial** Φ_n is defined by

$$\Phi_n(x) := \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - e^{2\pi i k/n}).$$

Example 25.1.2. Another way of expressing the defining identity of the cyclotomic polynomial $\Phi_{pq}(x)$ is

$$x^{pq} - 1 = \frac{(x^p - 1)(x^q - 1)}{x - 1} \Phi_{pq}(x).$$

In other words, $\Phi_{pq}(x)$ can be expressed as the following fraction of polynomials:

$$\frac{(x^{pq} - 1)(x - 1)}{(x^p - 1)(x^q - 1)} = \Phi_{pq}(x).$$

The idea is now to write $(x^{pq} - 1)(x - 1)$ as a combination of polynomials of the form $(x^{up} - 1)(x^{vq} - 1)$. Note first that p is invertible modulo q and q is invertible modulo



p. Thus, there are integers $0 \leq s < q$ and $0 \leq t < p$ such that $sp \equiv 1 \pmod{q}$ and $tq \equiv 1 \pmod{p}$. Combining these congruences, we obtain

$$sp + tq \equiv 1 \pmod{pq}.$$

Moreover, we have $0 \leq sp + tq < pq + pq$, so that in fact the identity

$$sp + tq = pq + 1$$

holds. With this choice of s and t, we calculate

$$\begin{aligned}(x^{pq}-1)(x-1) - (x^{sp}-1)(x^{tq}-1) &= x^{pq+1} - x^{pq} - x + 1 - x^{sp+tq} + x^{sp} + x^{tq} - 1 \\ &= -x(x^{pq-1} - x^{sp-1} - x^{tq-1} + 1) \\ &= -x(x^{sp-1}-1)(x^{tq-1}-1) \\ &= -x(x^{(q-s)p}-1)(x^{(p-t)q}-1).\end{aligned}$$

This shows that

$$(x^{pq}-1)(x-1) = (x^{sp}-1)(x^{tq}-1) - x(x^{(q-s)p}-1)(x^{(p-t)q}-1).$$

This shows that

$$\Phi_{pq}(x) = \frac{(x^{sp}-1)(x^{tq}-1)}{(x^p-1)(x^q-1)} - x\frac{(x^{(q-s)p}-1)(x^{(p-t)q}-1)}{(x^p-1)(x^q-1)}.$$

In other words, we find that

$$\Phi_{pq}(x) = \left(\sum_{i=0}^{s-1} x^{ip}\right)\left(\sum_{j=0}^{t-1} x^{jq}\right) - x\left(\sum_{i=0}^{q-s-1} x^{ip}\right)\left(\sum_{j=0}^{p-t-1} x^{jq}\right).$$

THEOREM 25.1.3. *For any natural number n we have the identity*

$$\Phi_n(x) = \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x).$$

THEOREM 25.1.4. *The cyclotomic polynomials $\Phi_n(x)$ have integer coefficients*

In the following theorem we will establish that the coefficients of the cyclotomic polynomials are palindromic, meaning that they read the same forward and back.

THEOREM 25.1.5. *The cyclotomic polynomials $\Phi_n(x)$ are **reciprocal** in the sense that*

$$\Phi_n\left(\tfrac{1}{x}\right) x^{\phi(n)} = \Phi_n(x).$$

Theorem 25.1.6. *Consider a cyclotomic polynomial $\Phi_n(x)$ and a prime p. Then we have*

$$\Phi_n(x) \equiv 0 \pmod{p} \text{ is solvable} \quad \Leftrightarrow \quad n \mid p-1.$$

Furthermore, if $\Phi_n(x) \equiv 0 \pmod{p}$ is solvable, then $\Phi_n(x)$ has exactly $\phi(n)$ roots modulo p.

Definition 25.1.7. We define

$$\Phi_n(x,y) := y^{\phi(n)}\Phi_n\left(\frac{x}{y}\right).$$

Proposition 25.1.8. *For any x, y, and n, we have:*

$$x^n - y^n = \prod_{d \mid n} \Phi_d(x,y).$$

Lemma 25.1.9. *Consider integers a, b, and c, and a prime p such that $p \nmid ab$ and $c \equiv a/b \pmod{p}$. If $\operatorname{ord}_p(c) = k$, then*

$$\Phi_k(c) \equiv 0 \pmod{p} \quad \Leftrightarrow \quad p \mid \Phi_k(a,b)$$

Lemma 25.1.10. *If $p \nmid m$, then $\Phi_m(x^p) = \Phi_{mp}(x)\Phi_m(x)$.*

Lemma 25.1.11. *Consider a prime p, and let $n = p^\alpha m$, where $\alpha \geq 1$ and $p \nmid m$. Then we have*

$$\Phi_n(x) \equiv \Phi_m(x)^{\phi(p^\alpha)} \pmod{p}.$$

Consequently, if $p \mid \Phi_n(a,b)$ then $p \mid \Phi_m(a,b)$.

Proposition 25.1.12. *Consider a prime $p \nmid n$. Then*

$$\operatorname{ord}_p(a) = n \quad \Leftrightarrow \quad p \mid \Phi_n(a)$$

Recall from Theorem 19.5.2 (Lifting the Exponent) that for any odd prime p and any $n = p^\alpha m$ with $p \nmid m$, we have

$$v_p(a^n - b^n) - v_p(a^m - b^m) = \alpha.$$

Since we have expressed $a^n - b^n$ as a product in terms of the homogenized cyclotomic polynomials $\Phi_n(a,b)$, we can thus compute the p-adic valuation of $\Phi_n(a,b)$.

Proposition 25.1.13. *Consider an odd prime p such that $p \nmid ab$. Let $k = \rho(p)$ be the rank of apparition of p in $(a^n - b^n)$. Then we have*

$$v_p(\Phi_n(a,b)) = \begin{cases} v_p(a^k - b^k) & \text{if } n = k, \\ 1 & \text{if } n = p^\alpha k \text{ for some } \alpha \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. □

25.2 The Möbius Inversion Formula for the Cyclotomic Polynomials

THEOREM 25.2.1. *For any n, we have the identity*

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

EXAMPLE 25.2.2. Theorem 25.2.1 can be used effectively to compute the coefficients of a cyclotomic polynomial. For example, in order to compute $\Phi_{12}(x)$, we note that the values $\mu(12/d)$ of the Möbius function are as follows:

$$\mu(12/1) = 0,\ \mu(12/2) = 1,\ \mu(12/3) = 0,\ \mu(12/4) = -1,\ \mu(12/6) = -1,\ \mu(12/12) = 1.$$

This shows that

$$\Phi_{12}(x) = (x^2 - 1)(x^4 - 1)^{-1}(x^6 - 1)^{-1}(x^{12} - 1) = x^4 - x^2 + 1.$$

25.3 Irreducibility of the Cyclotomic Polynomials

DEFINITION 25.3.1. We say that a polynomial $f(x)$ is **square-free** if $r(x)^2 \mid x^n - 1$ implies that $r(x)$ is constant, for every polynomial $r(x)$. Furthermore, we say that $f(x)$ is **square-free modulo** p if $r(x)^2 \mid x^n - 1 \pmod{p}$ implies that $r(x)$ is constant modulo p, for every polynomial $r(x)$.

The polynomial $x^n - 1$ is square-free in the ordinary sense, since it does not have repeated roots. In the following lemma we will prove the stronger property that $x^n - 1$ is square-free modulo primes p not dividing n.

LEMMA 25.3.2. *The polynomial $x^n - 1$ is square-free modulo p for every prime $p \nmid n$.*

PROOF. It suffices that there cannot be an irreducible polynomial $r(x)$ such that

$$x^n - 1 = r(x)^2 s(x) \pmod{p}.$$

By taking derivatives, we see that

$$nx^{n-1} = 2r(x)r'(x)s(x) + r(x)^2 s(x) \pmod{p}.$$

In particular, we see that $r(x) \mid nx^{n-1}$ in $\mathbb{F}_p[x]$. By the assumption that $p \nmid n$ it follows that n is invertible, and hence we obtain

$$r(x) \mid x^{n-1}.$$

Since $r(x)$ is assumed to be irreducible, it follows that $r(x) \mid x$. That is, $x \mid r(x)$. This leads to a contradiction, however, since

$$x \nmid x^n - 1.$$

□

Theorem 25.3.3. *The nth cyclotomic polynomial $\Phi_n(x)$ is irreducible for every $n \geq 1$.*

Proof. Let $\zeta = e^{2\pi i/n}$. We claim that if $f(x)$ is an irreducible polynomial such that $f(\zeta) = 0$, then $f(\zeta^a) = 0$ for every integer a coprime to n. To prove this claim, it suffices to show that $f(\zeta^p) = 0$ for every prime $p \nmid n$.

We observe first that ζ^p is a primitive root of unity, since $(\zeta^p)^m = 1$ implies $n \mid pm$, which implies $n \mid m$ since $p \nmid n$. Now, since we have assumed that $f(\zeta) = 0$ it follows that

$$\Phi_n(x) = f(x)g(x).$$

Therefore, if $f(\zeta^p) \neq 0$, it follows that $g(\zeta^p) = 0$. This shows that ζ is a root of the polynomial $g(x^p)$. Since $f(x)$ is an irreducible polynomial with root ζ, it follows that $f(x) \mid g(x^p)$.

As a consequence of the fact that ζ^a is a root of every irreducible polynomial $f(x)$ such that $f(\zeta) = 0$, for every integer a relatively prime to n, every such polynomial is of degree $\varphi(n)$. It follows that the polynomial $\Phi_n(x)$ is of minimal degree such that $\Phi_n(\zeta) = 0$, and therefore must be irreducible. □

25.4 Zsigmondy's Theorem

Definition 25.4.1. Consider a sequence (a_n) of integers. A prime p is said to be a **primitive prime divisor** of a_n if the rank of apparition of p satisfies $\rho(p) = n$.

Proposition 25.4.2. *Consider two relatively prime integers a and b, and a prime p such that $p \mid \Phi_n(a, b)$, where $n \geq 1$. Then there are two mutually exclusive possibilities:*

(i) *Either $p \equiv 1 \pmod{n}$, in which case p is a primitive prime divisor of $a^n - b^n$, or*

(ii) *$p \mid n$, in which case p is the largest prime factor of n, and provided that $n > 2$ we have furthermore $p^2 \nmid \Phi_n(a, b)$.*

Proof. Since $a^n - b^n = \prod_{d \mid n} \Phi_d(a, b)$, it follows that $a^n \equiv b^n \pmod{p}$. Furthermore a and b are assumed to be relatively prime, the congruence $a^n \equiv b^n \pmod{p}$ implies that neither a nor b is divisible by p. We find that

$$(a/b)^n \equiv 1 \pmod{p},$$

and hence $k := \operatorname{ord}_p(a/b)$ is a divisor of n by Theorem 8.5.2 (Order Theorem). There are two cases to consider: Either $k = n$ or k is a proper divisor of n.

If $k = n$, then it follows by Theorem 16.1.1 (Fermat's Little Theorem) that $n \mid p - 1$, which is another way of saying that $p \equiv 1 \pmod{n}$. Since $k \mid m$ for any m such that $p \mid a^m - b^m$, it follows that p is a primitive divisor of $a^n - b^n$.

For the second case, suppose that k is a proper divisor of n. Since $p \mid \Phi_k(a, b)$ and $p \mid \Phi_n(a, b)$ both hold, it follows that the polynomial congruence

$$x^n - 1 \pmod{p}$$

has roots of multiplicity > 1. It follows that

$$\gcd(x^n - 1, nx^{n-1}) \neq 1,$$

from which we conclude that $p \mid n$.

To show that p is the largest prime factor of n, write $n = p^\alpha m$, where $p \nmid m$. By the implication

$$p \mid \Phi_n(a,b) \Rightarrow p \mid \Phi_m(a,b)$$

it follows that $p \mid \Phi_m(a,b)$. However, since $p \nmid m$ this brings us back to the first case with the exponent m, so we conclude that $m \mid p-1$. In particular, any prime divisor of m is a prime divisor of $p-1$, which implies that p must have been the largest prime divisor of n.

Finally, we have to show that $v_p(\Phi_n(a,b)) = 1$. We consider two cases: Either $p = 2$ or p is odd. If $p = 2$, write $n = 2^\alpha m$. As before, it follows that $m \mid p-1$, so we have $m = 1$ and $n = 2^\alpha$. By the assumption that $n > 2$ it follows that $\alpha \geq 2$. Since a and b are both odd, it follows that

$$\Phi_n(a,b) = a^{2^{\alpha-1}} + b^{2^{\alpha-1}} \equiv 2 \pmod 4,$$

from which we conclude that $v_2(\Phi_n(a,b)) = 1$.

For the case where p is odd, write $n = p^\alpha m$ as before. Then we obtain from Theorem 19.5.2 (Lifting the Exponent) that

$$v_p(a^n - b^n) - v_p(a^m - b^m) = \alpha.$$

The right-hand side can be evaluated using the formula $a^n - b^n = \prod_{d \mid n} \Phi_d(a,b)$. Note that for any divisor d of n, we have $p \mid \Phi_d(a,b)$ if and only if $d = p^i m$ for some $0 \leq i \leq \alpha$. Thus we obtain:

$$\sum_{i=1}^{\alpha} v_p(\Phi_{p^i m}(a,b)) = \alpha.$$

Since $p \mid \Phi_{p^i m}(a,b)$, this implies that

$$v_p(\Phi_{p^i m}(a,b)) = 1$$

for every $1 \leq i \leq \alpha$. The case $i = \alpha$ proves the claim. □

THEOREM 25.4.3 (Zsigmondy's Theorem). *Consider two integers $1 \leq b < a$ with $\gcd(a,b) = 1$ and let $n \geq 1$. Then the number $a^n - b^n$ has a primitive prime divisor, except in the following three cases:*

(i) *$n = 1$ and $a - b = 1$,*

(ii) *$n = 2$ and $a + b$ is a power of 2,*

(iii) *$n = 6$, $a = 2$, and $b = 1$.*

Proof. In order to dispose of the first case, note that if $n = 1$, then any prime divisor of $a - b$ is primitive. Thus, the only case where $a - b$ does not have primitive prime divisors is when $a - b = 1$.

Next, we deal with the case $n = 2$. Suppose that $a^2 - b^2$ does not have primitive prime divisors. An equivalent way of saying this is that any prime divisor $p \mid \Phi_2(a, b) = a + b$ is also a prime divisor of $a - b$. However, we observe that $\gcd(a + b, a - b)$ divides both $2a$ and $2b$, which implies that the only prime possible prime divisor of $a + b$ is 2. In other words, $a + b$ is a power of 2.

For the remainder of the proof we suppose that $n > 2$. We will show that if $a^n - b^n$ has no primitive prime divisors, then $n = 6$, $a = 2$, and $b = 1$. By Proposition 25.4.2 it follows that if $a^n - b^n$ has no primitive prime divisors, then

$$\Phi_n(a, b) = p,$$

where p is the largest prime divisor of n and moreover p is odd. Write $n = p^\alpha m$, where $p \nmid m$.

We claim that $m = 1$ is impossible. To see this, note that

$$\Phi_{p^\alpha}(a, b) = \frac{a^{p^\alpha} - b^{p^\alpha}}{a^{p^{\alpha-1}} - b^{p^{\alpha-1}}} = a^{p^{\alpha-1}(p-1)} + \cdots + b^{p^{\alpha-1}(p-1)}.$$

It follows immediately from this description that $\Phi_{p^\alpha}(a, b) > p$, which contradicts the fact that $\Phi_n(a, b) = p$.

Next, we claim that $m \geq 3$ is impossible, so that only the case $m = 2$ remains. Suppose to the contrary that $m \geq 3$, and define $A := a^{p^{\alpha-1}}$ and $B := b^{p^{\alpha-1}}$, so that $\Phi_n(a, b) = \Phi_{pm}(A, B)$. Since $p \nmid m$, we have the identity

$$\Phi_{pm}(A, B) = \frac{\Phi_m(A^p, B^p)}{\Phi_m(A, B)}.$$

We estimate the magnitude of the numerator and denominator separately. Recall that $\Phi_m(x, y) = \prod(x - \zeta y)$ where the product runs over the numbers of the form $\zeta = e^{2\pi i k/n}$ where $\gcd(k, m) = 1$. Since $m \geq 3$, we note that $\zeta \neq 1$ for every such k. Thus, for every such ζ, we have the strict inequalities $|A^p - \zeta B^p| > A^p - B^p$ and $|A - \zeta B| < A + B$. It follows that

$$\Phi_{pm}(A, B) > \frac{(A^p - B^p)^{\phi(m)}}{(A + B)^{\phi(m)}} = \left(\frac{A^p - B^p}{A + B}\right)^{\phi(m)}.$$

Since $a > b \geq 1$, we have $A \geq 2$ and $B \geq 1$. Furthermore, p is the largest prime factor of n, so p is odd, implying $p \geq 3$. The function $f(x) = (x^p - 1)/(x + 1)$ is increasing for $x \geq 2$, so the term in the parentheses is at least $(2^p - 1)/3$. Combining this with the fact that $\phi(m) \geq 2$ for $m \geq 3$, we obtain

$$\Phi_{pm}(A, B) > \left(\frac{2^p - 1}{3}\right)^2.$$



For $p = 3$, the right-hand side is $(7/3)^2 > 5 > p$. For $p \geq 5$, the inequality holds even more strongly. In all cases we have $\Phi_n(a, b) > p$, which is a contradiction.

By the previous eliminations, we conclude that $m = 2$; that is, $n = 2p^\alpha$. It follows that

$$p = \Phi_{2p^\alpha}(a, b) = \frac{A^p + B^p}{A + B}.$$

Note that $p(A + B) = A^p + B^p \geq 2(\frac{A+B}{2})^p = \frac{(A+B)^p}{2^{p-1}}$, from which we obtain

$$\left(\frac{3}{2}\right)^{p-1} \leq \left(\frac{A+B}{2}\right)^{p-1} \leq p.$$

Since this inequality fails for $p \geq 4$, it follows that $p = 3$. We find that

$$\left(\frac{A+B}{2}\right)^2 \leq 3,$$

which implies that $(A + B)^2 \leq 12$, and consequently $A + B \leq 3$. It follows that $a^{p^{\alpha-1}} = A = 2$ and $B = 1$, which gives us that $\alpha = 1$, so that $n = 6$, $a = 2$, and $b = 1$. □

25.5 The Infinitude of Primes Congruent to 1 Modulo n

THEOREM 25.5.1. *For each $n \geq 1$, there are infinitely many primes $p \equiv 1 \pmod{n}$.*

PROOF. The statement is self-evident for $n \leq 2$, so we will assume that $n > 2$. Consider a finite set $p_1, \ldots, p_k$ of distinct primes such that

$$p_i \equiv 1 \pmod{n}$$

for each $1 \leq i \leq k$, let $a := n \cdot p_1 \cdots p_k$, and define

$$N := \Phi_n(a).$$

Observe that the number N has at least one prime factor. Indeed, this follows directly from Theorem 25.4.3 (Zsigmondy's Theorem), since $n, a \geq 3$.

We claim that any prime factor $q \mid N$ satisfies $q \equiv 1 \pmod{n}$ and is distinct from the primes p_i. Since the constant term of $\Phi_n(x)$ is 1, it follows that $N \equiv 1 \pmod{p_i}$. This immediately implies that $q \neq p_i$ for each $1 \leq i \leq k$. We also observe that the congruence $N \equiv 1 \pmod{n}$ holds, for the same reason. This shows that any prime factor $q \mid N$ is of the first kind in Proposition 25.4.2, which shows that $q \equiv 1 \pmod{n}$. □

25.6 Vantieghem's Theorem

Emmanuel Vantieghem provided a characterization of the prime numbers in terms of the Mersenne numbers [Van1991]. More precisely, he showed that a natural number $n \geq 3$ is prime if and only if

$$\prod_{k=1}^{n-1} M_k \equiv n \pmod{M_n}.$$

Recall that the nth Mersenne number is given by $M_n := 2^n - 1$. The sequence (M_n) of Mersenne numbers is a strong divisibility sequence. There are some analogies between Vantieghem's theorem and Theorem 16.3.1 (Wilson's Theorem). In Wilson's theorem, we make use of the congruence

$$x^p \equiv x \pmod{p},$$

which holds by Theorem 16.1.1 (Fermat's Little Theorem). For instance, in the second proof of Wilson's theorem, this congruence was used to observe that

$$\prod_{k=0}^{p-1}(x-k) \equiv x^p - x \pmod{p}.$$

Similarly, in the proof of Vantieghem's theorem, we will use the congruence $2^p \equiv 1 \pmod{M_p}$ to observe that

$$\prod_{k=1}^{p-1}(x-2^k) \equiv x^p - 1 \pmod{M_p}.$$

We will prove this congruence in the following proposition.

Proposition 25.6.1. *Consider the monic polynomial*

$$f(x) = \prod_{k=0}^{p-1}(x-2^k)$$

Then we have $f(x) \equiv x^p - 1 \pmod{M_p}$.

Proof. To start the proof, we first note that

$$f(0) \equiv \prod_{k=0}^{p-1}(0-2^k) \equiv -2^{\frac{p(p-1)}{2}} \equiv -1 \pmod{M_p}.$$

This shows that the constant term of $f(x)$ is indeed congruent to -1 modulo M_p. Since $f(x)$ is a monic polynomial, it therefore suffices to show that its coefficients of degree $0 < k < p$ are all 0.



To see this, we first claim that $f(2x) \equiv f(x) \pmod{M_p}$. Indeed, using that $2^p \equiv 1 \pmod{M_p}$, which implies that $2^{-1} \equiv 2^{p-1} \pmod{M_p}$, we see that

$$f(2x) = \prod_{k=0}^{p-1}(2x - 2^k) = (2x-1)2^{p-1}\prod_{k=1}^{p-1}(x - 2^{k-1}) \equiv \prod_{k=0}^{p-1}(x - 2^k) \pmod{M_p}.$$

Writing $f = a_p x^p + \cdots + a_0$, it follows that

$$0 \equiv f(2x) - f(x) \equiv \sum_{k=0}^{p} a_k(2^k - 1)x^k \pmod{M_p}.$$

Since $2^k \equiv 1 \pmod{M_p}$ implies $p \mid k$, it follows that $a_k \equiv 0 \pmod{M_p}$ for $0 < k < p$, which completes the proof. □

Recall from the second proof of Theorem 16.3.1 (Wilson's Theorem), that after having established that $\prod_k (x-k) \equiv x^p - x \pmod{p}$, we proceeded by taking derivatives on both sides. This strategy again works in the proof of the forward direction of Vantieghem's theorem. For the converse direction, we will make use of Theorem 25.4.3 (Zsigmondy's Theorem).

THEOREM 25.6.2 (Vantieghem's Theorem). *A natural number $n \geq 3$ is prime if and only if*

$$\prod_{k=1}^{n-1} M_k \equiv n \pmod{M_n}$$

PROOF. First, suppose that $n = p$, where p is a prime. Consider the polynomial

$$f(x) = \prod_{k=0}^{p-1}(x - 2^k)$$

which satisfies the congruence $f(x) \equiv x^p - 1 \pmod{M_p}$ by Proposition 25.6.1. It follows that $f'(1) \equiv p \pmod{M_p}$. On the other hand, writing $f(x) = (x-1)g(x)$, where $g(x) = \prod_{k=1}^{p-1}(x - 2^k)$, we find that $f'(x) = (x-1)g'(x) + g(x)$. Evaluating at 1 gives taht

$$\prod_{k=1}^{p-1}(1 - 2^k) = g(1) = f'(1) \equiv p \pmod{M_p}.$$

Since $p-1$ is even, we can multiply each factor with -1 to conclude that $\prod_{k=1}^{p-1} M_k \equiv p \pmod{M_p}$. This completes the proof of the forward direction.

For the converse, assume that the congruence $\prod_{k=1}^{n-1} M_k \equiv n \pmod{M_n}$ holds. Let p be the largest prime divisor of n, so that $M_p \mid M_n$. Then we have the congruence

$$\prod_{k=1}^{n-1} M_k \equiv n \pmod{M_p}$$

We will use this congruence to show that if p is a proper divisor of n, then there is a prime divisor $q > p$ of n. Clearly, such q is again a proper divisor, so there would be by the same argument another prime divisor $r > q$ of n, and so on. Since any natural number has only finitely many prime divisors, this shows that $p = n$.

Suppose, as we announced, that p is a proper divisor of n. Then M_p is among the factors on the left-hand side, which shows that $0 \equiv n \pmod{M_p}$. Thus, we find that $M_p \mid n$. By Theorem 25.4.3 (Zsigmondy's Theorem) it follows that the Mersenne number M_p has a primitive prime divisor $q \mid M_p$. Indeed, p is an odd prime, so we are not in any of the exceptional cases of Zsigmondy's theorem. Since $q \nmid p$, it follows from Proposition 25.4.2 that $q \equiv 1 \pmod{p}$. In particular, we must have $q > p$. □

Exercises

Routine-Building Exercises

25.1 Let $M_n = 2^n - 1$ be the nth Mersenne number. Show that if $d \mid n$, then

$$\Phi_d(2) \mid M_n.$$

25.2 Compute the prime factorization of the Mersenne number $M_{60} = 2^{60} - 1$.

25.3 (a) Show that

$$\Phi_n(1) = \begin{cases} 0 & \text{if } n = 1, \\ p & \text{if } n = p^k \text{ for some prime } p \text{ and } k \geq 1, \\ 1 & \text{if two distinct primes divide } n. \end{cases}$$

(b) Show that for $n \geq 2$ we have

$$\Phi_n(1) = \frac{\operatorname{lcm}(1, \ldots, n)}{\operatorname{lcm}(1, \ldots, n-1)}.$$

25.4 Let $\sigma(n)$ be the sum of the divisors of a natural number n. Show that

$$\sigma(p^m) = \prod_{\substack{d \mid m+1 \\ d>1}} \Phi_d(p).$$

25.5 Suppose that a and b are relatively prime. Show that

$$\frac{2^{ab} - 1}{(2^a - 1)(2^b - 1)} = \prod_{\substack{c \mid a \\ c>1}} \prod_{\substack{d \mid b \\ d>1}} \Phi_{cd}(2).$$

Chapter 26

Integer Factorizations of Polynomial Values

26.1 The Reducibility of $x^n - a$

Theorem 26.1.1 (Vahlen–Capelli). *Consider a rational number a. The polynomial $x^n - a$ is reducible over $\mathbb{Q}$ if and only if either $a = b^k$ for some divisor $k \mid n$, or $n \equiv 0 \pmod 4$ and $a = -4b^4$ for some rational number b.*

26.2 Aurifeuillean Factorizations

26.3 Obstructions to the Infinitude of Primes in Lucas Sequences

In this section, we consider two relatively prime integers a and b, and the associated Lucas sequence (u_n) defined by

$$u_0 = 0, \qquad u_1 = 1, \qquad \text{and} \qquad u_{n+2} = au_{n+1} - bu_n.$$

The central question we are concerned with here, is to determine some conditions on a and b for which all but finitely many numbers u_n are composite. That is, we wish to determine a list of conditions that rule out the possibility of having infinitely many primes of the form u_n, with the goal to better understand restrictions a Lucas sequence must satisfy in order for it to contain infinitely many primes. Some famous conjectures

state that there are infinitely many Mersenne primes and infinitely many Fibonacci primes.

THEOREM 26.3.1 (First obstruction). *Consider two relatively prime integers a and b. Furthermore, assume that $b = k^2$ for some positive integer k, and that $a \geq 3$ as well as $a \geq 2k$. Let (u_n) be the Lucas sequence given by*

$$u_0 = 0, \qquad u_1 = 1, \qquad \text{and} \qquad u_{n+2} = au_{n+1} - bu_n.$$

Then u_n is composite for every $n \geq 3$.

PROOF. Recall from Corollary 19.1.9 that the Lucas sequence (u_n) satisfies the following identities:

$$u_{2n+1} = u_{n+1}^2 - bu_n^2 \qquad \text{and} \qquad u_{2n+2} = u_{n+1}(u_{n+2} - bu_n).$$

By the assumption that $b = k^2$, the first identity shows that any odd idexed entry satisfies the identity

$$u_{2n+1} = (u_{n+1} - ku_n)(u_{n+1} + ku_n).$$

We claim that both factors are ≥ 2, for $n \geq 1$. To see this, it suffices to prove that $u_{n+1} > ku_n + 1$ for $n \geq 1$. This claim is proven by induction. In the base case, there are two cases to consider: Either $k = 1$ or $k > 1$. If $k = 1$, then $u_2 = a \geq 3 > ku_1 + 1$. If $k > 1$, then $u_2 = a \geq 2k > k + 1$. For the inductive step, note that

$$u_{n+2} = au_{n+1} - k^2u_n > 2ku_{n+1} - ku_{n+1} - ku_{n+1}.$$

□

THEOREM 26.3.2 (Second obstruction). *Let α and β be the two roots of the polynomial $x^2 - ax + b$. If $\frac{\alpha}{\beta}$ is a root of unity, then all but finitely many numbers of the form u_n are composite.*

EXAMPLE 26.3.3. The first and second obstructions do not cover all Lucas sequences that are known to have only finitely many primes. To construct a Lucas sequence that is composite for all but finitely many entries outside of the domain of the two obstructions we have so far, we will use Sophie Germain's identity

$$x^4 + 4y^4 = (x^2 - 2xy + 2y^2)(x^2 + 2xy + 2y^2).$$

The only pair of positive integers x and y for which $x^4 + 4y^4$ is prime consists of $x = 1$ and $y = 1$, where we have $1^4 + 4 \cdot 1^4 = 5$. It follows from Sophie Germain's identity that

$$4^{2n+1} + 1 = 2^{4n+2} + 1 = (1 - 2^{n+1} + 2^{2n+1})(1 + 2^{n+1} + 2^{2n+1})$$

is composite except when $n = 0$. Now consider the sequence

$$u_n = \frac{4^n - (-1)^n}{5},$$

which is the Lucas sequence satisfying the recurrence $u_{n+2} = 3u_{n+1} + 4u_n$. The first few values of u_n are $0, 1, 3, 13, 51, 205, 819, \ldots$.

At even exponents, we find the factorization

$$u_{2n} = \frac{4^{2n} - 1}{5} = \frac{(4^n - 1)(4^n + 1)}{5},$$

which shows that u_{2n} is not prime for $n \geq 2$. At odd exponents, we find

$$u_{2n+1} = \frac{4^{2n+1} + 1}{5} = \frac{(1 - 2^{n+1} + 2^{2n+1})(1 + 2^{n+1} + 2^{2n+1})}{5}.$$

Both factors in the numerator are strictly greater than 5 when $n \geq 2$, implying that the denominator 5 is at best a proper divisor of either factor. This shows that u_{2n+1} is composite for $n \geq 2$. Combined with the previous observation about the compositeness of u_{2n}, we find that u_n is composite for all $n \geq 4$. The Lucas sequence (u_n) constructed in this example was discovered in [Ism+2025].

Theorem 26.3.4 (Aurifeuillian obstruction). *Consider a squarefree integer $t > 1$, and set*

$$\mu(t) := \begin{cases} t & \text{if } t \equiv 1 \pmod 4, \\ 2t & \text{if } t \equiv 2, 3 \pmod 4. \end{cases}$$

Consider an integer B of the form $B = s^2 t$, and let (u_n) be the Lucas sequence with characteristic roots

$$\alpha = B^r \qquad \text{and} \qquad \beta = \varepsilon,$$

where $r \geq 1$ is an integer such that $\mu(t) \mid 2r$, and where $\varepsilon = \pm 1$ is chosen such that $\alpha^n - \beta^n$ contains the cyclotomic factor $\Phi_{\mu(t)}(B^n)$ for all odd n. Then the sequence (u_n) contains only finitely many primes.

Definition 26.3.5. A Lucas sequence (u_n) with recurrence relation $u_{n+2} = au_{n+1} - bu_n$ is said to be **regular** if $\gcd(a, b) = 1$.

Definition 26.3.6. A Lucas sequence (u_n) with recurrence relation $u_{n+2} = au_{n+1} - bu_n$ and characteristic roots α and β is said to be **degenerate** if α/β is a root of unity, meaning that there exists an exponent k such that

$$(\alpha/\beta)^k = 1.$$

Theorem 26.3.7. *A Lucas sequence (u_n) with distinct characteristic roots is degenerate if and only if there exists an $n > 0$ such that $u_n = 0$.*

In the following theorem, we give a characterization of the condition that a Lucas sequence *reflects* divisibility. The usual condition for divisibility sequences is that if $m \mid n$, then $u_m \mid u_n$. The property that (u_n) reflects divisibility is the reverse: If $u_m \mid u_n$, then it must be the case that $m \mid n$. A special instance of this condition is that if $u_m = 0$, then $m = 0$.



THEOREM 26.3.8. *Consider a Lucas sequence (u_n) with recurrence $u_{n+2} = au_{n+1} - bu_n$ and characteristic roots α and β. Assume that (u_n) is regular and nondegenerate. Then the following are equivalent:*

(i) *The Lucas sequence (u_n) reflects divisibility, in the sense that*

$$u_m \mid u_n \quad \Rightarrow \quad m \mid n.$$

(ii) *We have $|u_n| > 1$ for all $n \geq 2$.*

A Lucas sequence which reflects divisibility will be called a ***reflecting Lucas sequence****.*

PROOF. Suppose that m and n are natural numbers such that $u_m \mid u_n$. □

References

[Bal1929] Hoon Balakram. *On the values of n which make* $(2n)!/(n+1)!(n+1)!$ *an integer*. In: Journal of the Indian Mathematical Society 18 (1929), pp. 97–100.

[Ber1845] Joseph Bertrand. *Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme*. French. In: Journal de l'École Royale Polytechnique 18.30 (1845), pp. 123–140.

[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.

[Che1852] Pafnuty Chebyshev. *Mémoire sur les nombres premiers*. French. In: Journal de Mathématiques Pures et Appliquées 17 (1852), pp. 366–390.

[Cox1989] David A. Cox. *Primes of the Form* $x^2 + ny^2$*: Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics. New York, NY: Wiley-Interscience, 1989. isbn: 9780471506546.

[Dic1919] Leonard Eugene Dickson. *History of the Theory of Numbers. Divisibility and Primality*. Vol. 1. Carnegie Institution of Washington Publication 256. See Chapter III, pp. 59–61, for Fermat, Leibniz, and Euler. Washington, DC: Carnegie Institution of Washington, 1919. url: https://archive.org/details/historyoftheoryo01dick.

[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.

[Far2009] Bakir Farhi. *An Identity Involving the Least Common Multiple of Binomial Coefficients and Its Application*. In: The American Mathematical Monthly 116.9 (2009), pp. 836–839.

[Fei1985] Lenore Feigenbaum. *Brook Taylor and the method of increments*. In: Archive for History of Exact Sciences 34.1 (1985), pp. 1–140.

[Fur1955] Harry Furstenberg. *On the Infinitude of Primes*. In: The American Mathematical Monthly 62.5 (1955), p. 353. doi: 10.2307/2307043.

[Gau1986] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Ed. by William C. Waterhouse. Trans. by Arthur A. Clarke. Revised edition. New York & Berlin: Springer-Verlag, 1986. isbn: 9780387962542.

[Gol1956] Solomon W. Golomb. *Combinatorial Proof of Fermat's "Little" Theorem*. In: The American Mathematical Monthly 63.10 (1956), p. 718.

[Gre1671] James Gregory. *Letter to John Collins*. Published in the "Gregory Memorial Volume", ed. H.W. Turnbull (1939). Feb. 1671.

[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.

[Ism+2025] Dan Ismailescu et al. *Shifting Lucas Sequences Away from Primes*. In: INTEGERS: The Electronic Journal of Combinatorial Number Theory 25.A42 (2025), pp. 1–20. doi: 10.5281/zenodo.15283739.

[Kum1852] Ernst Eduard Kummer. *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*. In: Journal für die reine und angewandte Mathematik 44 (1852), pp. 93–146. doi: 10.1515/crll.1852.44.93.

[Lag1770] Joseph-Louis Lagrange. *Réflexions sur la résolution algébrique des équations*. In: Histoire de l'Académie Royale des Sciences et Belles-Lettres de Berlin (1770), pp. 123–192.

[Lag1771] Joseph-Louis Lagrange. *Démonstration d'un théorème nouveau concernant les nombres premiers*. In: Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin (1771).

[Lan1912] Edmund Landau. *Gelöste und ungelöste Probleme aus der Theorie der Primzahlverteilung und der Riemannschen Zetafunktion*. In: Jahresbericht der Deutschen Mathematiker-Vereinigung 21 (1912), pp. 208–228. url: http://eudml.org/doc/145337.

[Leh1933] Derrick H. Lehmer. *On Euler's totient function*. In: Bulletin of the American Mathematical Society 38 (1933), pp. 745–751. doi: 10.1090/s0002-9904-1932-05521-5.

[Lei1863] Gottfried Wilhelm Leibniz. *Nova algebrae promotio*. In: *Leibnizens mathematische Schriften. Zweite Abtheilung: Die mathematischen Abhandlungen Leibnizens enthaltend*. Ed. by Carl Immanuel Gerhardt. Vol. 7. See pp. 180–181 for the discussion of Fermat's little theorem. Halle: H. W. Schmidt, 1863, pp. 154–189. URL: https://gallica.bnf.fr/ark:/12148/bpt6k111375x.

[Ler1905] Matyáš Lerch. *Zur Theorie des Fermatschen Quotienten* $\frac{a^{p-1}-1}{p} = q(a)$. German. In: Mathematische Annalen 60.4 (Dec. 1905), pp. 471–490. ISSN: 0025-5831. DOI: 10.1007/BF01561092.

[LeV1956a] William J. LeVeque. *Topics in Number Theory, Volume 1*. Reading, MA: Addison-Wesley, 1956. ISBN: 9780201042252.

[LeV1956b] William J. LeVeque. *Topics in Number Theory, Volume 2*. Reading, MA: Addison-Wesley, 1956. ISBN: 9780201042269.

[Lio1857] Joseph Liouville. *Généralisation d'un théorème de l'arithmétique indienne*. In: Journal de Mathématiques Pures et Appliquées. 2nd ser. 2 (1857), pp. 393–396. URL: https://www.numdam.org/item/JMPA_1857_2_2__393_0/.

[LP2003] Florian Luca and Štefan Porubský. *Fibonacci Integers*. In: Journal of Number Theory 101.2 (2003), pp. 220–240.

[Luc1878a] Édouard Lucas. *Sur la théorie des fonctions numériques simplement périodiques*. In: Nouvelle Correspondance Mathématique 4 (1878). Continuation of the article begun in volume 3 (1877), pp. 1–8, 33–40, 65–71, 97–102, 129–134, 225–228. URL: https://gdz.sub.uni-goettingen.de/id/PPN598948236_0004.

[Luc1878b] Édouard Lucas. *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier*. In: Bulletin de la Société Mathématique de France 6 (1878), pp. 49–54. DOI: 10.24033/bsmf.127.

[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.

[Now2015] Andrzej Nowicki. *Strong Divisibility and LCM-Sequences*. In: The American Mathematical Monthly 122.10 (2015), pp. 958–966. arXiv: 1310.2416.

[OR2012] Pascal Ochem and Michaël Rao. *Odd perfect numbers are greater than* 10^{1500}. In: Mathematics of Computation 81.279 (2012), pp. 1869–1877. DOI: 10.1090/S0025-5718-2012-02563-4.



[OEI2025] OEIS Foundation. *A006992: Bertrand primes*. The On-Line Encyclopedia of Integer Sequences. 2025. URL: https://oeis.org/A006992.

[Pan2007] Hao Pan. *A q-analogue of Lehmer's congruence*. In: Acta Arithmetica 128.4 (2007), pp. 303–318. DOI: 10.4064/aa128-4-1.

[Pól1919] Georg Pólya. *Verschiedene Bemerkungen zur Zahlentheorie*. In: Jahresbericht der Deutschen Mathematiker-Vereinigung 28 (1919), pp. 31–40.

[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.

[Sag2020] Bruce E. Sagan. *Combinatorics: The Art of Counting*. Graduate Studies in Mathematics 210. Providence, RI: American Mathematical Society, 2020. DOI: 10.1090/gsm/210.

[Sai2006] Filip Saidak. *A New Proof of Euclid's Theorem*. In: The American Mathematical Monthly 113.10 (2006), pp. 937–938. DOI: 10.2307/27642094.

[Tay1715] Brook Taylor. *Methodus incrementorum directa et inversa*. London: Typis Pearsonianis: prostant apud Gul. Innys, 1715.

[Van1991] Emmanuel A. Vantieghem. *On a congruence only holding for primes*. In: Indagationes Mathematicae 2.2 (1991), pp. 253–255. ISSN: 0019-3577.

[War1936] Morgan Ward. *Note on Divisibility Sequences*. In: Bulletin of the American Mathematical Society 42.12 (1936), pp. 843–845.

[War1948] Morgan Ward. *Memoir on Elliptic Divisibility Sequences*. In: American Journal of Mathematics 70.1 (1948), pp. 31–74. DOI: 10.2307/2371930.

[War1782] Edward Waring. *Meditationes Algebraicæ: Editio tertia, recensita et aucta*. 3rd ed. Cambridge: Typis Academicis excudebat J. Archdeacon/apud J. Nicholson, J. C. & F. Rivington, S. Crowder, H. Gardner & S. Hayes; Oxonii apud J. Fletcher, 1782, 389 + [15] addenda/corrigenda.

[Wha2010] Junho Peter Whang. *Another Proof of the Infinitude of the Prime Numbers*. In: The American Mathematical Monthly 117.2 (2010), p. 181.

[Wie1909] Arthur Wieferich. *Zum letzten Fermatschen Theorem*. In: Journal für die reine und angewandte Mathematik 136 (1909), pp. 293–302. URL: http://eudml.org/doc/149315.