Number Theory

Lecture Notes

Master M1 — 2025–2026

Yaë Ulrich Gaba

"Mathematics is the queen of the sciences and number theory is the queen of mathematics."

— Carl Friedrich Gauss

March 25, 2026

Preface

Number theory, often called the *queen of mathematics*, is one of the oldest and most beautiful branches of the discipline. Its central objects—the integers—are deceptively simple, yet the questions they raise have challenged mathematicians for millennia and continue to drive deep research today.

This text aims to provide a rigorous, self-contained introduction to classical number theory, beginning with the most elementary notions of divisibility and building steadily toward the distribution of prime numbers, modular arithmetic, quadratic reciprocity, and selected modern applications including cryptography.

Prerequisites. The reader is expected to be familiar with basic logic, proof techniques (induction, contradiction, contrapositive), and elementary properties of the integers as covered in a first course in discrete mathematics or algebra. No prior exposure to number theory is assumed.

How to use this book. Definitions, theorems, and propositions are stated precisely and proved in full unless explicitly noted otherwise. Numerous examples illustrate the theory, and each chapter concludes with a graded set of exercises:

$\star$ — routine applications of definitions and theorems;
$\star\star$ — problems requiring some ingenuity or the combination of several results;
$\star\star\star$ — challenging problems, often connected to competition mathematics or research.

The reader is strongly encouraged to attempt exercises before continuing to the next chapter: number theory is learned by *doing*.

Acknowledgements. The exposition owes a debt to the classic texts of Hardy and Wright, Niven–Zuckerman–Montgomery, Ireland and Rosen, and Apostol, as well as to generations of students whose questions have shaped the presentation.

Notation and Conventions

Throughout this text we adopt the following conventions.

Symbol	Meaning
$\mathbb{N}$	The set of natural numbers $\{0, 1, 2, \ldots\}$
$\mathbb{N}^*$	The set of positive integers $\{1, 2, 3, \ldots\}$
$\mathbb{Z}$	The ring of integers
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	The fields of rational, real, and complex numbers
$\mathbb{F}_p$	The finite field with p elements (p prime)
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\gcd(a, b)$	Greatest common divisor of a and b
$\operatorname{lcm}(a, b)$	Least common multiple of a and b
(a, b)	Shorthand for $\gcd(a, b)$ when context is clear
$a \equiv b \pmod{n}$	n divides $a - b$
$\lfloor x \rfloor$	Floor function: greatest integer $\leq x$
$\lceil x \rceil$	Ceiling function: least integer $\geq x$
$\pi(x)$	Number of primes $\leq x$
$\left(\frac{a}{p}\right)$	Legendre symbol
$\varphi(n)$	Euler's totient function
$\operatorname{ord}_n(a)$	Multiplicative order of a modulo n
$\log$	Natural logarithm (unless otherwise stated)

All rings are commutative with unity unless stated otherwise. When we write p without further qualification, it denotes a prime number. The notation $\sum_{p \leq x}$ means the sum over all primes p not exceeding x.

Contents

Chapter 1

Divisibility and the Euclidean Algorithm

"The laws of nature are but the mathematical thoughts of God."
— attributed to Euclid

1.1 Historical context: Euclid's *Elements*

The systematic study of divisibility properties of integers traces back at least to Books VII–IX of Euclid's *Elements* (c. 300 BCE). In these books, Euclid established the foundation upon which all of number theory rests: the notion of divisibility, the Euclidean algorithm for computing greatest common divisors, and the celebrated proof that there are infinitely many prime numbers.

Euclid's approach was geometric in flavour—integers were represented as line segments, and "a divides b" meant that a measures b exactly. Despite the geometric language, the logical structure is purely arithmetic and translates directly into modern algebraic notation. The *Euclidean algorithm*, Proposition 2 of Book VII, is arguably the oldest non-trivial algorithm still in everyday use: it underlies the computation of modular inverses in cryptographic protocols executed billions of times per day.

In this chapter we develop divisibility theory from first principles, prove the division algorithm and the correctness of the Euclidean algorithm, establish Bézout's identity, and introduce the least common multiple and the notion of coprimality.

1.2 Divisibility: definition and elementary properties

Definition 1.1 (Divisibility)**.** Let $a, b \in \mathbb{Z}$. We say that a *divides* b, written $a \mid b$, if there exists $k \in \mathbb{Z}$ such that $b = ak$. When $a \mid b$ we also say that a is a *divisor* (or *factor*) of b, and that b is a *multiple* of a. If a does not divide b we write $a \nmid b$.

Example 1.2. We have $3 \mid 12$ since $12 = 3 \cdot 4$, and $7 \mid (-21)$ since $-21 = 7 \cdot (-3)$. On the other hand, $5 \nmid 13$ because there is no integer k with $13 = 5k$.

Proposition 1.3 (Basic properties of divisibility)**.** *Let $a, b, c \in \mathbb{Z}$.*

(i) ***Reflexivity:*** *$a \mid a$ for all $a \in \mathbb{Z}$.*

(ii) ***Transitivity:*** *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

(iii) ***Linearity:*** *If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$.*

(iv) ***Comparison:*** *If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.*

(v) ***Antisymmetry on $\mathbb{N}^*$:*** *If $a, b \in \mathbb{N}^*$ with $a \mid b$ and $b \mid a$, then $a = b$.*

(vi) $a \mid 0$ for every $a \in \mathbb{Z}$, and $1 \mid a$ for every $a \in \mathbb{Z}$.

(vii) If $a \mid 1$, then $a \in \{-1, 1\}$.

Proof. (i) $a = a \cdot 1$.

(ii) Write $b = ak_1$ and $c = bk_2$. Then $c = a(k_1 k_2)$.

(iii) Write $b = ak_1$ and $c = ak_2$. Then $bx + cy = a(k_1 x + k_2 y)$.

(iv) Write $b = ak$ with $k \in \mathbb{Z} \setminus \{0\}$ (since $b \neq 0$). Then $|b| = |a|\,|k| \geq |a|$.

(v) By (iv), $a \leq b$ and $b \leq a$, so $a = b$.

(vi) $0 = a \cdot 0$ and $a = 1 \cdot a$.

(vii) Write $1 = ak$. Then $|a|\,|k| = 1$ with $|a|, |k| \in \mathbb{N}^*$, so $|a| = |k| = 1$. □

Remark 1.4. Properties (i), (ii), and (v) show that divisibility is a partial order on $\mathbb{N}^*$. We shall visualise this order with a *Hasse diagram* at the end of the chapter (see Figure 1.1).

1.3 The division algorithm

The following result is the cornerstone of integer arithmetic. Despite the traditional name, it is a *theorem of existence and uniqueness*, not a constructive procedure (though its proof is readily made constructive).

Theorem 1.5 (Division algorithm)**.** *Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ with $b > 0$. There exist unique integers q (the* quotient*) and r (the* remainder*) such that*

$$a = bq + r, \qquad 0 \leq r < b.$$

Proof. **Existence.** Consider the set

$$S = \{a - bk : k \in \mathbb{Z}\} \cap \mathbb{N} = \{a - bk \geq 0 : k \in \mathbb{Z}\}.$$

We claim $S \neq \varnothing$. Indeed, if $a \geq 0$ take $k = 0$; if $a < 0$ take $k = a$ (then $a - ba = a(1 - b) \geq 0$ since $a < 0$ and $1 - b \leq 0$). By the well-ordering principle, S has a least element $r = a - bq$ for some $q \in \mathbb{Z}$. By construction $r \geq 0$.

Suppose for contradiction that $r \geq b$. Then

$$a - b(q+1) = r - b \geq 0,$$

so $r - b \in S$ and $r - b < r$, contradicting the minimality of r. Therefore $0 \leq r < b$.

Uniqueness. Suppose $a = bq_1 + r_1 = bq_2 + r_2$ with $0 \leq r_1, r_2 < b$. Then

$$b(q_1 - q_2) = r_2 - r_1.$$

Since $|r_2 - r_1| < b$ and $b \mid (r_2 - r_1)$, we must have $r_2 - r_1 = 0$, i.e. $r_1 = r_2$. It follows immediately that $q_1 = q_2$. □

Example 1.6. Divide $a = -17$ by $b = 5$: we seek q, r with $-17 = 5q + r$ and $0 \leq r < 5$. We find $q = -4$ and $r = 3$ since $-17 = 5(-4) + 3$.

Remark 1.7. We write $r = a \bmod b$ or equivalently $r = a - b\lfloor a/b \rfloor$. This extends naturally to $b < 0$; some authors require $0 \leq r < |b|$ for the general case.

1.4 Greatest common divisor and the Euclidean algorithm

Definition 1.8 (Greatest common divisor)**.** Let $a, b \in \mathbb{Z}$, not both zero. The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is the largest positive integer d such that $d \mid a$ and $d \mid b$.

Remark 1.9. By convention, $\gcd(0, 0) = 0$. For all a, $\gcd(a, 0) = |a|$.

Proposition 1.10 (Characterisation of the gcd)**.** *Let $d = \gcd(a, b)$. Then:*

(i) $d \mid a$ and $d \mid b$.

(ii) If $c \mid a$ and $c \mid b$, then $c \mid d$.

Conversely, any positive integer satisfying (i) and (ii) equals $\gcd(a, b)$.

Proof. Property (i) is immediate from the definition. For (ii), suppose $c \mid a$ and $c \mid b$. We shall prove $c \mid d$ after establishing Bézout's identity (Theorem 1.15), which gives $d = ax + by$ for some $x, y \in \mathbb{Z}$. Since $c \mid a$ and $c \mid b$, linearity of divisibility (Proposition 1.3(iii)) yields $c \mid d$. □

Lemma 1.11 (Key reduction for the Euclidean algorithm)**.** *For any $a \in \mathbb{Z}$ and $b \in \mathbb{N}^*$,*

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

Proof. Write $a = bq + r$ with $0 \le r < b$ (Theorem 1.5). If $d \mid a$ and $d \mid b$, then $d \mid (a - bq) = r$. Conversely, if $d \mid b$ and $d \mid r$, then $d \mid (bq + r) = a$. Hence the set of common divisors of (a, b) equals the set of common divisors of (b, r), so their greatest elements coincide. □

Theorem 1.12 (Euclidean algorithm)**.** *Let $a, b \in \mathbb{N}$ with $b > 0$. Define the sequence*

$$\begin{aligned} r_0 &= a, \quad r_1 = b, \\ r_{i+1} &= r_{i-1} \bmod r_i, \qquad i = 1, 2, \dots \end{aligned}$$

There exists $n \ge 1$ such that $r_{n+1} = 0$, and then $\gcd(a, b) = r_n$.

Proof. **Termination.** The sequence (r_i) satisfies $b = r_1 > r_2 > \cdots \ge 0$. Since a strictly decreasing sequence of non-negative integers must be finite, there exists a smallest n with $r_{n+1} = 0$.

Correctness. By repeated application of Lemma 1.11:

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0) = r_n. \qquad \square$$

Example 1.13. Compute $\gcd(252, 198)$:

$$\begin{aligned} 252 &= 198 \cdot 1 + 54, \\ 198 &= 54 \cdot 3 + 36, \\ 54 &= 36 \cdot 1 + 18, \\ 36 &= 18 \cdot 2 + 0. \end{aligned}$$

Hence $\gcd(252, 198) = 18$.

Remark 1.14 (Complexity of the Euclidean algorithm). Lamé proved in 1844 that the number of division steps is at most 5 times the number of digits of the smaller input. More precisely, the worst case is achieved by consecutive Fibonacci numbers: computing $\gcd(F_{n+1}, F_n)$ requires exactly $n - 1$ steps. This gives a time complexity of $O((\log \min(a, b))^2)$ when using standard integer arithmetic.

1.5 Bézout's identity and the extended Euclidean algorithm

Theorem 1.15 (Bézout's identity)**.** *Let $a, b \in \mathbb{Z}$, not both zero, and let $d = \gcd(a, b)$. There exist $x, y \in \mathbb{Z}$ such that*

$$ax + by = d.$$

Moreover, d is the smallest positive element of the set $\{ax + by : x, y \in \mathbb{Z}\}$.

Proof. Consider the set

$$S = \{ax + by : x, y \in \mathbb{Z}\} \cap \mathbb{N}^*.$$

The set S is non-empty (it contains $|a|$ or $|b|$, at least one of which is positive). By the well-ordering principle, S has a least element $d_0 = ax_0 + by_0$.

We claim $d_0 \mid a$. Apply the division algorithm: $a = d_0 q + r$ with $0 \le r < d_0$. Then

$$r = a - d_0 q = a - (ax_0 + by_0)q = a(1 - x_0 q) + b(-y_0 q).$$

So $r \in \{ax + by : x, y \in \mathbb{Z}\}$ and $0 \le r < d_0$. Since d_0 is the smallest *positive* element of this set, we must have $r = 0$. Therefore $d_0 \mid a$. By the same argument, $d_0 \mid b$.

Since d_0 is a common divisor of a and b, we have $d_0 \le d$. Conversely, $d \mid a$ and $d \mid b$ imply $d \mid (ax_0 + by_0) = d_0$, so $d \le d_0$. Thus $d = d_0$. □

Corollary 1.16. *An integer c is a $\mathbb{Z}$-linear combination of a and b if and only if $\gcd(a, b) \mid c$.*

Proof. If $c = ax + by$ and $d = \gcd(a, b)$, then $d \mid c$ by linearity. Conversely, if $d \mid c$, write $c = dk$ and $d = ax_0 + by_0$; then $c = a(kx_0) + b(ky_0)$. □

Definition 1.17 (Extended Euclidean algorithm)**.** The *extended Euclidean algorithm* computes, alongside $\gcd(a, b)$, integers x and y satisfying $ax + by = \gcd(a, b)$. It does so by tracking Bézout coefficients through the recurrence:

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} x_{i-2} \\ y_{i-2} \end{pmatrix} - q_i \begin{pmatrix} x_{i-1} \\ y_{i-1} \end{pmatrix},$$

starting from $(x_0, y_0) = (1, 0)$ and $(x_1, y_1) = (0, 1)$, where $q_i = \lfloor r_{i-1}/r_i \rfloor$ at step i.

Example 1.18. Find x, y with $252x + 198y = \gcd(252, 198) = 18$.

i	r_i	q_i	x_i	y_i
0	252	—	1	0
1	198	1	0	1
2	54	3	1	-1
3	36	1	-3	4
4	18	2	4	-5
5	0	—	—	—

We read off $x = 4$, $y = -5$, and verify: $252 \cdot 4 + 198 \cdot (-5) = 1008 - 990 = 18$. ✓

1.6 Coprime integers, Gauss's lemma, and the LCM

Definition 1.19 (Coprime integers)**.** Integers a and b are *coprime* (or *relatively prime*) if $\gcd(a, b) = 1$.

Proposition 1.20. *a and b are coprime if and only if there exist $x, y \in \mathbb{Z}$ with $ax + by = 1$.*

Proof. If $\gcd(a, b) = 1$, Bézout gives the desired x, y. Conversely, if $ax + by = 1$, any common divisor d of a and b divides 1, so $d = \pm 1$, hence $\gcd(a, b) = 1$. □

Theorem 1.21 (Gauss's lemma)**.** *If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. By Bézout, write $ax + by = 1$. Multiply by c:

$$acx + bcy = c.$$

Since $a \mid acx$ and $a \mid bc$ (hence $a \mid bcy$), we obtain $a \mid c$. □

Corollary 1.22 (Euclid's lemma)**.** *If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. If $p \nmid a$ then $\gcd(p, a) = 1$ (the only positive divisors of p are 1 and p). By Gauss's lemma, $p \mid b$. □

Corollary 1.23. *If p is prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i.*

Proof. Induction on n, using Corollary 1.22 as the base case. □

Definition 1.24 (Least common multiple)**.** The *least common multiple* of $a, b \in \mathbb{Z} \setminus \{0\}$, denoted $\operatorname{lcm}(a, b)$, is the smallest positive integer m such that $a \mid m$ and $b \mid m$.

Proposition 1.25. *For $a, b \in \mathbb{N}^*$:*

(i) $\operatorname{lcm}(a, b) = \dfrac{ab}{\gcd(a, b)}$.

(ii) If $a \mid n$ and $b \mid n$, then $\operatorname{lcm}(a, b) \mid n$.

Proof. (i) Let $d = \gcd(a, b)$ and $m = ab/d$. Write $a = da'$, $b = db'$ with $\gcd(a', b') = 1$. Then $m = da'b'$, so $a \mid m$ (since $m = b \cdot a'$) and $b \mid m$ (since $m = a \cdot b'$). Hence m is a common multiple.

Now let n be any positive common multiple. Write $n = ak_1 = bk_2$. Then $da'k_1 = db'k_2$, so $a'k_1 = b'k_2$. Since $\gcd(a', b') = 1$, Gauss's lemma gives $b' \mid k_1$, say $k_1 = b'\ell$. Then $n = ak_1 = da'b'\ell = m\ell$, so $m \mid n$ and thus $m \leq n$.

(ii) This was shown in the proof of (i). □

1.7 Divisibility lattice

The divisibility relation $\mid$ defines a partial order on $\mathbb{N}^*$. For a fixed positive integer n, the set of divisors of n ordered by divisibility forms a lattice in which the meet is gcd and the

join is lcm.

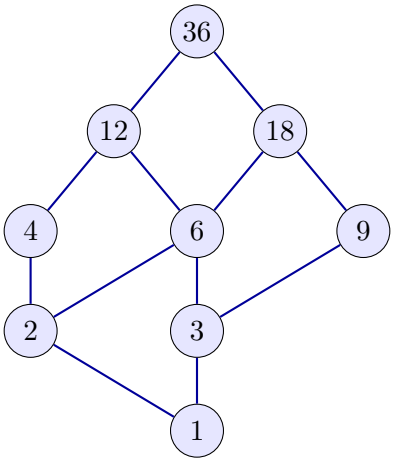


Figure 1.1: Hasse diagram of the divisibility lattice of 36. For example, $\gcd(12, 18) = 6$ (meet) and $\operatorname{lcm}(12, 18) = 36$ (join).

1.8 Connections to cryptography

The Euclidean algorithm and Bézout's identity are not merely theoretical curiosities; they are essential tools in modern cryptography.

In the **RSA cryptosystem**, one selects two large primes p and q, computes $n = pq$, and chooses an encryption exponent e with $\gcd(e, \varphi(n)) = 1$, where $\varphi(n) = (p-1)(q-1)$ is Euler's totient. The decryption exponent d is then the modular inverse of e modulo $\varphi(n)$:

$$ed \equiv 1 \pmod{\varphi(n)}.$$

This inverse is computed via the *extended Euclidean algorithm*. The security of the system rests on the difficulty of factoring n, but its *implementation* depends fundamentally on the efficient computation of gcd and modular inverses.

Remark 1.26. In practice, the integers involved have thousands of decimal digits. The $O((\log n)^2)$ complexity of the Euclidean algorithm (with fast multiplication improvements) makes this entirely feasible, while the factoring problem for the same size integers remains computationally intractable.

1.9 Exercises

Exercise 1.1 ($\star$)**.** Prove that if $a \mid b$ and $b \mid c$, then $a \mid (b + c)$.

Exercise 1.2 ($\star$)**.** Show that if $n^2 \mid n$ for some $n \in \mathbb{Z}$, then $n \in \{-1, 0, 1\}$.

Exercise 1.3 ($\star$)**.** Use the Euclidean algorithm to compute $\gcd(1001, 385)$. Then find integers x, y with $1001x + 385y = \gcd(1001, 385)$.

Exercise 1.4 ($\star$)**.** Prove that any two consecutive integers are coprime.

Exercise 1.5 ($\star$)**.** Let $a, b \in \mathbb{N}^*$. Prove that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Exercise 1.6 ($\star\star$)**.** Determine all integer solutions (x, y) of $12x + 8y = 28$.

Exercise 1.7 ($\star\star$)**.** Let $a, b, c \in \mathbb{Z}$ with $\gcd(a, b) = 1$. Prove that $\gcd(a, bc) = \gcd(a, c)$.

Exercise 1.8 ($\star\star$)**.** Let (F_n) be the Fibonacci sequence with $F_1 = F_2 = 1$. Prove that $\gcd(F_m, F_n) = F_{\gcd(m,n)}$ for all $m, n \geq 1$.

Exercise 1.9 ($\star\star$)**.** Show that the Bézout coefficients x, y in $ax + by = \gcd(a, b)$ are not unique. Describe all solutions (x, y).

Exercise 1.10 ($\star\star\star$)**.** Prove **Lamé's theorem**: the Euclidean algorithm applied to $\gcd(a, b)$ with $a > b > 0$ requires at most $\lfloor (\log_\phi b) \rfloor - 1$ divisions, where $\phi = (1 + \sqrt{5})/2$ is the golden ratio. *Hint:* show that if the algorithm takes n steps, then $b \geq F_{n+1}$, where F_k is the kth Fibonacci number.

Exercise 1.11 ($\star\star\star$)**.** Let $a, b \in \mathbb{N}^*$ with $\gcd(a, b) = 1$. Prove that the largest integer that *cannot* be expressed as $ax + by$ with $x, y \in \mathbb{N}$ is $ab - a - b$. This is the **Frobenius number** $g(a, b)$.

Chapter summary

- **Divisibility** $(a \mid b)$ is a partial order on $\mathbb{N}^*$; it is reflexive, transitive, antisymmetric, and linear in the sense that divisibility is preserved under $\mathbb{Z}$-linear combinations.
- The **division algorithm** guarantees unique quotient and remainder for any division by a positive integer.
- The **Euclidean algorithm** computes $\gcd(a, b)$ in $O((\log b)^2)$ time; the **extended** version also yields Bézout coefficients.
- **Bézout's identity**: $\gcd(a, b)$ is the smallest positive $\mathbb{Z}$-linear combination of a and b.
- **Gauss's lemma**: if $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$. As a consequence, **Euclid's lemma**: if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.
- The **lcm** satisfies $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.
- These tools underpin **RSA cryptography**: modular inverses are computed via the extended Euclidean algorithm.

Chapter 2

Prime Numbers: Infinity, Arithmetic, and Distribution

> *"Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery into which the human mind will never penetrate."*
> — *Leonhard Euler*

2.1 Primes and the fundamental dichotomy

Definition 2.1 (Prime and composite numbers)**.** An integer $p > 1$ is *prime* if its only positive divisors are 1 and p. An integer $n > 1$ that is not prime is called *composite*.

Remark 2.2. The integer 1 is neither prime nor composite; it is the *unit* of $(\mathbb{Z}, \cdot)$. This convention is essential for the uniqueness statement of the Fundamental Theorem of Arithmetic.

Example 2.3. The first few primes are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots$ The integer 2 is the only even prime.

Lemma 2.4. *Every integer $n > 1$ has a prime divisor. Moreover, the smallest divisor of n greater than 1 is prime.*

Proof. Let d be the smallest element of $\{k \in \mathbb{N} : k > 1,\ k \mid n\}$; this set is non-empty since n itself belongs to it. Suppose d is composite, i.e. $d = ab$ with $1 < a, b < d$. Then $a \mid d$ and $d \mid n$, so $a \mid n$, contradicting the minimality of d. Hence d is prime. □

Corollary 2.5. *If $n > 1$ is composite, then n has a prime factor $p \leq \sqrt{n}$.*

Proof. If $n = ab$ with $1 < a \leq b < n$, then $a^2 \leq ab = n$, so $a \leq \sqrt{n}$. By Lemma 2.4, a has a prime divisor $p \leq a \leq \sqrt{n}$. □

2.2 Infinitude of primes

The fact that there are infinitely many primes is one of the most celebrated results in all of mathematics. We present three proofs, each illuminating a different aspect of the structure.

2.2.1 Euclid's proof

Theorem 2.6 (Euclid, c. 300 BCE)**.** *There are infinitely many prime numbers.*

Proof. Suppose for contradiction that there are only finitely many primes, $p_1, p_2, \ldots, p_n$. Consider the integer

$$N = p_1 p_2 \cdots p_n + 1.$$

Since $N > 1$, by Lemma 2.4, N has a prime divisor p. Now $p = p_i$ for some i, so $p_i \mid N$ and $p_i \mid p_1 \cdots p_n$. Hence $p_i \mid (N - p_1 \cdots p_n) = 1$, a contradiction. Therefore the set of primes is infinite. □

Remark 2.7. Euclid's proof is often misquoted as "$p_1 \cdots p_n + 1$ is always prime." This is false in general: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \times 509$. What the proof shows is that N has a prime factor *not in the list*, whether or not N itself is prime.

2.2.2 Euler's analytic proof

Theorem 2.8 (Euler, 1737)**.** *The sum* $\displaystyle\sum_{p} \frac{1}{p}$ *over all primes* p *diverges. In particular, there are infinitely many primes.*

Proof sketch. For $s > 1$ one has the *Euler product*:

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

The left side diverges as $s \to 1^+$ (harmonic series). If there were only finitely many primes, the right side would be a finite product of finite values, a contradiction. A more careful analysis shows that

$$\sum_{p \le x} \frac{1}{p} = \log\log x + M + O\left(\frac{1}{\log x}\right),$$

where $M \approx 0.2615$ is the *Meissel–Mertens constant*, confirming divergence. □

2.2.3 A proof via Fermat numbers

Theorem 2.9. *The Fermat numbers* $F_n = 2^{2^n} + 1$ *(*$n = 0, 1, 2, \ldots$*) are pairwise coprime. Hence there are infinitely many primes.*

Proof. We first show that for $m < n$, $F_m \mid F_n - 2$. By induction, one verifies

$$F_n - 2 = F_0 F_1 \cdots F_{n-1}, \qquad n \geq 1.$$

Base case: $F_1 - 2 = 3 - 2 = 1$ and $F_0 = 3$; but we actually compute $F_1 - 2 = 2^2 + 1 - 2 = 3 = F_0$, which works since the product $F_0 = 3$.

Inductive step: Suppose $F_n - 2 = F_0 \cdots F_{n-1}$. Then $F_{n+1} = (F_n - 1)^2 + 1 = F_n^2 - 2F_n + 2$, so

$$F_{n+1} - 2 = F_n(F_n - 2) = F_n \cdot F_0 \cdots F_{n-1} = F_0 F_1 \cdots F_n.$$

Now if $d \mid F_m$ and $d \mid F_n$ with $m < n$, then $d \mid F_n - 2$ and $d \mid F_n$, so $d \mid 2$. Since each F_k is odd, d is odd, so $d = 1$. Hence $\gcd(F_m, F_n) = 1$.

Each $F_n > 1$ has at least one prime divisor, and these prime divisors are distinct for different n. Thus there are infinitely many primes. □

2.3 The Fundamental Theorem of Arithmetic

Theorem 2.10 (Fundamental Theorem of Arithmetic)**.** *Every integer $n > 1$ can be written as a product of primes:*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \qquad p_1 < p_2 < \cdots < p_k, \quad a_i \geq 1.$$

Moreover, this representation is unique *(up to the order of factors).*

Proof. **Existence** (by strong induction on n).

Base case: $n = 2$ is prime, so it is a product of one prime.

Inductive step: Assume every integer m with $2 \leq m < n$ is a product of primes. If n is prime, we are done. Otherwise, n is composite: $n = ab$ with $1 < a, b < n$. By the inductive hypothesis, both a and b are products of primes, hence so is $n = ab$.

Uniqueness (by strong induction on n).

Suppose

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

where the p_i and q_j are primes (written with repetitions, not necessarily in order). We prove $r = s$ and the p_i are a permutation of the q_j.

Since $p_1 \mid q_1 q_2 \cdots q_s$, Corollary 1.23 gives $p_1 \mid q_j$ for some j. Since q_j is prime and $p_1 > 1$, we have $p_1 = q_j$. Cancel this factor:

$$p_2 \cdots p_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s.$$

If $r = 1$, both sides equal 1, forcing $s = 1$ and we are done. If $r > 1$, the common value $n/p_1 < n$, and by the inductive hypothesis the two factorisations of n/p_1 agree up to reordering. Prepending $p_1 = q_j$ gives the result. □

Notation 2.11 (Canonical factorisation). We write the factorisation of n in *canonical form*:

$$n = \prod_{p \text{ prime}} p^{v_p(n)},$$

where $v_p(n) \geq 0$ is the *p-adic valuation* of n and all but finitely many exponents are zero. Then:

$$\gcd(a, b) = \prod_p p^{\min(v_p(a),\, v_p(b))}, \qquad \operatorname{lcm}(a, b) = \prod_p p^{\max(v_p(a),\, v_p(b))}.$$

Example 2.12. $360 = 2^3 \cdot 3^2 \cdot 5$ and $150 = 2 \cdot 3 \cdot 5^2$. Therefore $\gcd(360, 150) = 2 \cdot 3 \cdot 5 = 30$ and $\operatorname{lcm}(360, 150) = 2^3 \cdot 3^2 \cdot 5^2 = 1800$.

2.4 The Sieve of Eratosthenes

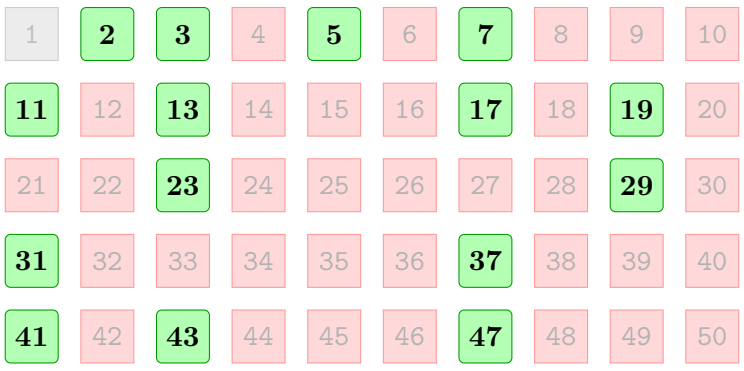
The *Sieve of Eratosthenes* (c. 240 BCE) is the oldest known systematic method for listing all primes up to a given bound N. The idea is simple: write down all integers from 2 to N, then iteratively mark off the multiples of each prime found.

Algorithm.

1. List the integers $2, 3, 4, \ldots, N$.
2. Let $p = 2$ (the smallest prime).
3. Mark all multiples of p from p^2 to N as composite. (Multiples $2p, 3p, \ldots, (p-1)p$ have already been handled.)
4. Find the next unmarked integer $> p$; call it p'. Set $p \leftarrow p'$.
5. If $p^2 \leq N$, go to step 3. Otherwise, stop: all unmarked numbers are prime.

Proposition 2.13. *The Sieve of Eratosthenes correctly identifies all primes up to N. Its time complexity is $O(N \log \log N)$.*

Proof of correctness. By Corollary 2.5, every composite $n \leq N$ has a prime factor $p \leq \sqrt{N}$. The sieve marks n as composite in the iteration for p. Conversely, a prime $q \leq N$ is never marked: it is not a proper multiple of any smaller prime. □



Green = prime, Red = composite, Gray = 1 (unit)

Figure 2.1: Result of the Sieve of Eratosthenes for integers 1 to 50.

2.5 The prime counting function and the Prime Number Theorem

Definition 2.14. For $x \geq 0$, the *prime counting function* is

$$\pi(x) = \#\{p \leq x : p \text{ is prime}\}.$$

Example 2.15. $\pi(10) = 4$ (the primes $2, 3, 5, 7$), $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10^6) = 78{,}498$.

The central question of analytic number theory is: *how does $\pi(x)$ grow as $x \to \infty$?*

2.5.1 Chebyshev's bounds

In the 1850s, Chebyshev obtained the correct order of growth without the precise asymptotic constant.

Theorem 2.16 (Chebyshev, 1852)**.** *There exist positive constants c_1, c_2 such that for all sufficiently large x:*

$$c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x}.$$

Chebyshev showed one can take $c_1 = \frac{\log 2}{2} \approx 0.347$ and $c_2 = \frac{6 \log 2}{5} \approx 0.832$.

Proof idea. The lower bound follows from an analysis of the central binomial coefficient $\binom{2n}{n}$. Since $\binom{2n}{n} \leq 4^n$ and every prime $n < p \leq 2n$ divides $\binom{2n}{n}$, one obtains $\pi(2n) - \pi(n) \leq$ a controlled quantity. The upper bound similarly uses the prime factorisation of $\binom{2n}{n}$ to bound $\sum_{p \leq 2n} \log p$ from above. We refer to Chapter 5 of Hardy and Wright for complete details. $\square$

2.5.2 The Prime Number Theorem

Theorem 2.17 (Prime Number Theorem — Hadamard, de la Vallée-Poussin, 1896)**.**

$$\pi(x) \sim \frac{x}{\log x} \qquad \text{as } x \to \infty.$$

Equivalently, $\lim_{x \to \infty} \dfrac{\pi(x) \log x}{x} = 1$. *A better approximation is given by the* logarithmic integral*:*

$$\pi(x) \sim \operatorname{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

Remark 2.18. The original proofs used complex analysis (properties of the Riemann zeta function $\zeta(s)$ on the line $\operatorname{Re}(s) = 1$). Elementary proofs were given independently by Erdős and Selberg in 1949, though "elementary" here means "avoiding complex

analysis," not "simple."

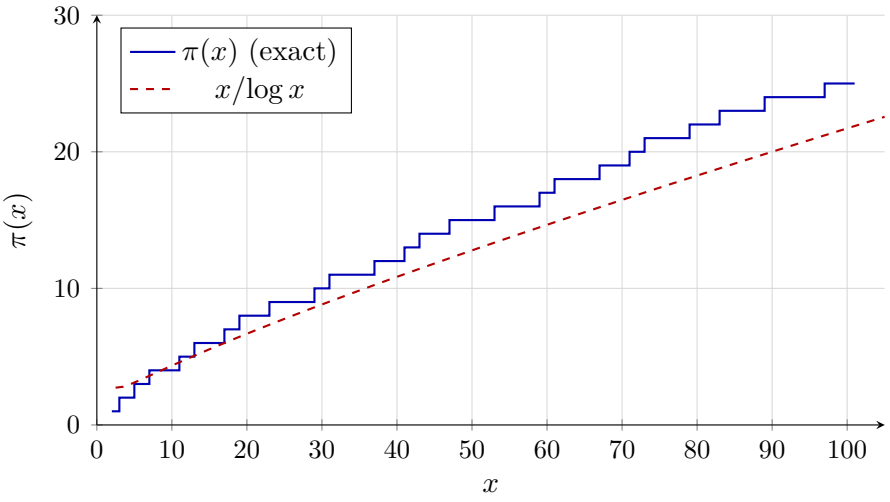


Figure 2.2: The prime counting function $\pi(x)$ (blue, step function) and the approximation $x/\log x$ (red, dashed) for $x \leq 100$.

2.6 Special primes and open problems

2.6.1 Mersenne primes

Definition 2.19 (Mersenne number)**.** A *Mersenne number* is an integer of the form $M_n = 2^n - 1$ for $n \in \mathbb{N}^*$. If M_n is prime, it is called a *Mersenne prime*.

Proposition 2.20. *If $M_n = 2^n - 1$ is prime, then n is prime.*

Proof. Suppose $n = ab$ with $1 < a, b < n$. Then

$$2^n - 1 = (2^a)^b - 1 = (2^a - 1)\Big((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 1\Big),$$

so $2^a - 1 \mid 2^n - 1$ with $1 < 2^a - 1 < 2^n - 1$. Hence M_n is composite. □

Remark 2.21. The converse is false: $M_{11} = 2047 = 23 \times 89$. As of 2024, 52 Mersenne primes are known; the largest, $M_{136,279,841}$, has over 41 million digits. Whether infinitely many Mersenne primes exist is an open problem.

2.6.2 Fermat primes

Definition 2.22 (Fermat number)**.** The nth *Fermat number* is $F_n = 2^{2^n} + 1$ for $n \geq 0$.

Remark 2.23. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ are all prime. Fermat conjectured that every F_n is prime, but Euler showed in 1732 that $F_5 = 4{,}294{,}967{,}297 = 641 \times 6{,}700{,}417$ is composite. No Fermat prime beyond F_4 has been found.

2.6.3 Twin primes and the Goldbach conjecture

Definition 2.24. *Twin primes* are pairs $(p, p+2)$ where both p and $p+2$ are prime.

Example 2.25. The first few twin prime pairs are $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$.

Twin Prime Conjecture. There are infinitely many twin primes. This remains unproved, though Zhang (2013) showed there are infinitely many pairs $(p, p+k)$ of primes with $k \leq 70{,}000{,}000$, subsequently improved to $k \leq 246$ by the Polymath project.

Goldbach's Conjecture (1742). Every even integer $n \geq 4$ is the sum of two primes. Verified computationally for $n \leq 4 \times 10^{18}$ and known to hold for all sufficiently large odd integers (Helfgott, 2013: every odd $n \geq 7$ is a sum of three primes).

2.7 Prime spirals: Ulam and Sacks

In 1963, Stanislaw Ulam noticed that when integers are arranged in a spiral pattern, the primes exhibit a striking tendency to fall along certain diagonal lines. This visual pattern, while not fully explained theoretically, reflects the fact that certain quadratic polynomials (e.g., $4n^2 + bn + c$) produce many primes.

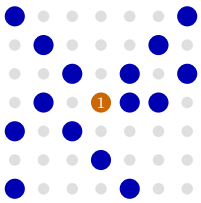


Figure 2.3: A small Ulam spiral: integers are placed on a spiral path starting from 1 (orange centre). Blue dots are primes; grey dots are composites. Even in this small example, diagonal alignments are visible.

2.8 Why large primes matter: RSA revisited

The security of RSA encryption depends on the following asymmetry:

- **Easy:** Given two large primes p, q, compute $n = pq$.
- **Hard:** Given n, recover p and q (the *integer factorisation problem*).

The Fundamental Theorem of Arithmetic guarantees that the factorisation *exists and is unique*, but says nothing about the *computational complexity* of finding it. Current RSA implementations use primes with 1024 or more bits (over 300 decimal digits each),

producing a modulus n of roughly 2048 bits. No known classical algorithm factors such integers in feasible time.

Remark 2.26 (Primality testing vs. factoring). It is far easier to *test* whether a number is prime than to *factor* a composite number. The AKS algorithm (2002) proves primality in deterministic polynomial time, while no polynomial-time factoring algorithm is known for classical computers. (Shor's quantum algorithm factors in polynomial time on a quantum computer, motivating the transition to post-quantum cryptography.)

2.9 Exercises

Exercise 2.1 ($\star$)**.** List all primes up to 100 using the Sieve of Eratosthenes. How many are there?

Exercise 2.2 ($\star$)**.** Find the canonical factorisation of 2520, 10!, and $\binom{20}{10}$.

Exercise 2.3 ($\star$)**.** Show that for every $n \geq 2$, the $n-1$ consecutive integers $n!+2, n!+3, \ldots, n!+n$ are all composite.

Exercise 2.4 ($\star$)**.** Let p be prime and $1 \leq k \leq p-1$. Prove that $p \mid \binom{p}{k}$.

Exercise 2.5 ($\star\star$)**.** Use the Fundamental Theorem of Arithmetic to prove that $\sqrt{2}$ is irrational.

Exercise 2.6 ($\star\star$)**.** Prove that there are infinitely many primes of the form $4k+3$. *Hint:* adapt Euclid's argument, noting that a product of integers $\equiv 1 \pmod 4$ is again $\equiv 1 \pmod 4$.

Exercise 2.7 ($\star\star$)**.** Prove **Legendre's formula**: for prime p and $n \geq 1$,

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

Use this to compute $v_2(100!)$ and $v_5(100!)$, and deduce the number of trailing zeros of 100!.

Exercise 2.8 ($\star\star$)**.** (**Bertrand's postulate — verification for small cases.**) Verify directly that for each n with $1 \leq n \leq 50$, there is a prime p with $n < p \leq 2n$.

Exercise 2.9 ($\star\star\star$)**.** Prove the Euler product formula: for $s > 1$,

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

Hint: expand each factor $(1-p^{-s})^{-1} = \sum_{k=0}^{\infty} p^{-ks}$ and use the Fundamental Theorem of Arithmetic.

Exercise 2.10 ($\star\star\star$)**.** Prove Chebyshev's lower bound: there exists $c > 0$ such that $\pi(x) \geq c\,x/\log x$ for all $x \geq 2$. *Hint:* analyse $v_p(\binom{2n}{n})$ using Legendre's formula and bound $\log \binom{2n}{n}$ from below.

Exercise 2.11 ($\star\star\star$)**.** Prove that for every $\varepsilon > 0$, there exist consecutive primes p_n, p_{n+1} with $p_{n+1} - p_n > \varepsilon \log p_n$. *Hint:* if all gaps were $\leq \varepsilon \log p_n$, sum to get a contradiction with the Prime Number Theorem.

Chapter summary

- Every integer > 1 has a prime divisor; a composite n has a prime factor $\leq \sqrt{n}$.
- **Infinitude of primes:** proved by Euclid (contradiction), Euler ($\sum 1/p$ diverges), and via Fermat numbers (pairwise coprime).
- The **Fundamental Theorem of Arithmetic** asserts that every integer > 1 has a *unique* prime factorisation. The proof of uniqueness relies on Euclid's lemma.
- The **Sieve of Eratosthenes** finds all primes up to N in $O(N \log \log N)$ time.
- The **Prime Number Theorem**: $\pi(x) \sim x/\log x$. Chebyshev obtained the correct order of growth; Hadamard and de la Vallée-Poussin proved the asymptotic.
- **Mersenne primes** $(2^p - 1)$ and **Fermat primes** $(2^{2^n} + 1)$ are special families; their infinitude is unknown.
- The **Twin Prime Conjecture** and **Goldbach's Conjecture** remain major open problems.
- **RSA cryptography** depends on the ease of primality testing versus the difficulty of factoring large composites.

Chapter 3

Congruences and Modular Arithmetic

3.1 Historical Context: Gauss's *Disquisitiones Arithmeticae*

In 1801, Carl Friedrich Gauss, then only twenty-four years old, published his masterwork *Disquisitiones Arithmeticae*. This treatise transformed number theory from a collection of scattered results into a systematic and rigorous discipline. The very first section of the *Disquisitiones* introduces the concept of *congruence*, a relation that Gauss recognised as the natural language for discussing divisibility and residues.

Gauss wrote:

> *If a number a divides the difference of the numbers b and c, b and c are said to be* congruent *with respect to a; if not,* incongruent. *The number a is called the* modulus.

He introduced the now-universal notation $b \equiv c \pmod{a}$ and proceeded to develop the arithmetic of congruences with the same rigour that Euclid had applied to geometry. The ideas in this chapter follow the path laid out in the *Disquisitiones*, enriched by the algebraic perspective that emerged over the following two centuries.

3.2 The Congruence Relation

Definition 3.1 (Congruence modulo n)**.** Let n be a positive integer. Two integers a and b are said to be *congruent modulo n*, written

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

if $n \mid (a - b)$, that is, if there exists an integer k such that $a - b = kn$. The integer n is called the *modulus* of the congruence.

Example 3.2 (Basic congruences)**.**

(i) $17 \equiv 2 \pmod{5}$, since $17 - 2 = 15 = 3 \cdot 5$.

(ii) $-3 \equiv 4 \pmod{7}$, since $-3 - 4 = -7 = (-1) \cdot 7$.

(iii) For any integer a, $a \equiv a \bmod n \pmod n$, where $a \bmod n$ denotes the remainder upon division by n.

Theorem 3.3 (Congruence is an equivalence relation)**.** *For every positive integer n, the relation $\equiv \pmod n$ is an equivalence relation on $\mathbb{Z}$. That is, for all $a, b, c \in \mathbb{Z}$:*

(i) ***Reflexivity:*** $a \equiv a \pmod n$.

(ii) ***Symmetry:*** *If* $a \equiv b \pmod n$, *then* $b \equiv a \pmod n$.

(iii) ***Transitivity:*** *If* $a \equiv b \pmod n$ *and* $b \equiv c \pmod n$, *then* $a \equiv c \pmod n$.

Proof.

(i) Since $a - a = 0 = 0 \cdot n$, we have $n \mid 0$, so $a \equiv a \pmod n$.

(ii) If $n \mid (a - b)$, write $a - b = kn$. Then $b - a = (-k)n$, so $n \mid (b - a)$.

(iii) If $a - b = k_1 n$ and $b - c = k_2 n$, then $a - c = (a - b) + (b - c) = (k_1 + k_2)n$, so $n \mid (a - c)$. □

The equivalence classes are the *residue classes* modulo n. The class containing the integer a is

$$\bar{a} = [a]_n = \{a + kn : k \in \mathbb{Z}\}.$$

There are exactly n distinct residue classes, represented by $\{0, 1, 2, \ldots, n - 1\}$.

Theorem 3.4 (Compatibility with arithmetic)**.** *Let $a \equiv a' \pmod n$ and $b \equiv b' \pmod n$. Then:*

(i) $a + b \equiv a' + b' \pmod n$.

(ii) $a - b \equiv a' - b' \pmod n$.

(iii) $ab \equiv a'b' \pmod n$.

(iv) For every non-negative integer k, $a^k \equiv (a')^k \pmod n$.

Proof. Write $a = a' + sn$ and $b = b' + tn$ for some $s, t \in \mathbb{Z}$.

(i) $a + b = a' + b' + (s + t)n$, so $n \mid (a + b - a' - b')$.

(ii) Identical reasoning with $s - t$.

(iii) $ab = (a' + sn)(b' + tn) = a'b' + (a't + b's + stn)n$, so $n \mid (ab - a'b')$.

(iv) Induction on k using (iii): the base case $k = 0$ gives $1 \equiv 1$, and if $a^k \equiv (a')^k$ then $a^{k+1} = a \cdot a^k \equiv a' \cdot (a')^k = (a')^{k+1} \pmod n$. □

Remark 3.5 (Cancellation requires care). Unlike ordinary equations, one cannot freely cancel a common factor. For instance, $2 \cdot 3 \equiv 2 \cdot 0 \pmod 6$, but $3 \not\equiv 0 \pmod 6$.

Cancellation of a from $ab \equiv ac \pmod{n}$ is valid precisely when $\gcd(a, n) = 1$.

Proposition 3.6 (Cancellation law)**.** *If $ab \equiv ac \pmod{n}$ and $d = \gcd(a, n)$, then $b \equiv c \pmod{n/d}$. In particular, if $\gcd(a, n) = 1$ then $b \equiv c \pmod{n}$.*

Proof. From $ab \equiv ac \pmod{n}$ we get $n \mid a(b - c)$. Writing $a = da'$, $n = dn'$ with $\gcd(a', n') = 1$, we have $dn' \mid da'(b - c)$, so $n' \mid a'(b - c)$. Since $\gcd(a', n') = 1$, Euclid's lemma gives $n' \mid (b - c)$, i.e. $b \equiv c \pmod{n/d}$. □

3.3 The Ring $\mathbb{Z}/n\mathbb{Z}$

Definition 3.7 (The ring $\mathbb{Z}/n\mathbb{Z}$)**.** The set of residue classes modulo n,

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\},$$

equipped with the operations

$$\bar{a} + \bar{b} = \overline{a + b}, \qquad \bar{a} \cdot \bar{b} = \overline{ab},$$

forms a commutative ring with identity $\bar{1}$.

The well-definedness of these operations is precisely the content of Theorem 3.4.

Definition 3.8 (Units and zero divisors)**.** An element $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is a *unit* (or *invertible element*) if there exists $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ with $\bar{a}\bar{b} = \bar{1}$. An element $\bar{a} \neq \bar{0}$ is a *zero divisor* if there exists $\bar{b} \neq \bar{0}$ with $\bar{a}\bar{b} = \bar{0}$.

Theorem 3.9 (Units and zero divisors in $\mathbb{Z}/n\mathbb{Z}$)**.** *Let $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ with $a \not\equiv 0 \pmod{n}$.*

(i) $\bar{a}$ is a unit if and only if $\gcd(a, n) = 1$.

(ii) $\bar{a}$ is a zero divisor if and only if $\gcd(a, n) > 1$.

In particular, every nonzero element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor.

Proof.

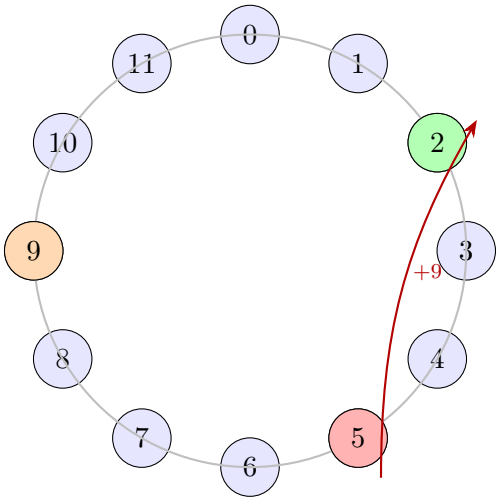
(i) $\bar{a}$ is a unit iff $\exists\, b$ with $ab \equiv 1 \pmod{n}$, iff the equation $ax + ny = 1$ has a solution in integers, iff $\gcd(a, n) = 1$ (by Bézout's identity).

(ii) If $d = \gcd(a, n) > 1$, set $b = n/d$. Then $1 \leq b < n$ and $ab = a(n/d) = (a/d) \cdot n \equiv 0 \pmod{n}$, so $\bar{a}$ is a zero divisor. Conversely, if $\gcd(a, n) = 1$ then $\bar{a}$ is a unit, hence $\bar{a}\bar{b} = \bar{0}$ implies $\bar{b} = \bar{0}$, so $\bar{a}$ is not a zero divisor. □

Corollary 3.10 ($\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime)**.** *The ring $\mathbb{Z}/n\mathbb{Z}$ is a field (i.e. every nonzero element is a unit) if and only if n is prime.*

Proof. If $n = p$ is prime, then for $1 \le a \le p-1$ we have $\gcd(a, p) = 1$, so $\bar{a}$ is a unit. Conversely, if n is composite, say $n = ab$ with $1 < a, b < n$, then $\bar{a}\bar{b} = \bar{0}$ with $\bar{a}, \bar{b} \neq \bar{0}$, so $\mathbb{Z}/n\mathbb{Z}$ has zero divisors and is not a field. □

Notation 3.11 (Group of units). The group of units of $\mathbb{Z}/n\mathbb{Z}$ is denoted $(\mathbb{Z}/n\mathbb{Z})^\times$. Its order is given by Euler's totient function $\varphi(n)$, which we study in Chapter 4.



Clock arithmetic: $5 + 9 \equiv 2 \pmod{12}$

Figure 3.1: Addition in $\mathbb{Z}/12\mathbb{Z}$ visualised as clock arithmetic.

$\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Multiplication table of $(\mathbb{Z}/7\mathbb{Z})^\times$; entries equal to 1 are highlighted.

Figure 3.2: Multiplication table of $(\mathbb{Z}/7\mathbb{Z})^\times$.

3.4 Linear Congruences

The equation $ax \equiv b \pmod{n}$ is the modular analogue of the linear equation $ax = b$. Its solvability depends on the relationship between a, b, and n.

Theorem 3.12 (Existence and number of solutions)**.** *Let $a, b \in \mathbb{Z}$ and $n \ge 1$. Set $d = \gcd(a, n)$.*

(i) The congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$.

(ii) When $d \mid b$, there are exactly d incongruent solutions modulo n. If x_0 is one

solution, the complete set of solutions is

$$x \equiv x_0 + k \cdot \frac{n}{d} \pmod{n}, \qquad k = 0, 1, \ldots, d-1.$$

Proof.

(i) The congruence $ax \equiv b \pmod{n}$ is equivalent to the existence of integers x, y with $ax - ny = b$, i.e. $ax + n(-y) = b$. By the characterisation of the image of the map $(x, y) \mapsto ax + ny$ (which equals $d\mathbb{Z}$), this has a solution if and only if $d \mid b$.

(ii) Suppose $d \mid b$. Dividing $ax \equiv b \pmod{n}$ through by d yields

$$\frac{a}{d}\, x \equiv \frac{b}{d} \pmod{\frac{n}{d}},$$

where $\gcd(a/d,\, n/d) = 1$. By Proposition 3.6 (or by Bézout), a/d has an inverse modulo n/d, so there is a unique solution x_0 modulo n/d.

The solutions modulo n that reduce to x_0 modulo n/d are precisely

$$x_0,\ x_0 + \frac{n}{d},\ x_0 + 2 \cdot \frac{n}{d},\ \ldots,\ x_0 + (d-1) \cdot \frac{n}{d},$$

and these are d values that are pairwise incongruent modulo n (since their differences are non-zero multiples of n/d that are less than n). □

Example 3.13 (Solving a linear congruence)**.** Solve $12x \equiv 9 \pmod{15}$.
We have $d = \gcd(12, 15) = 3$ and $3 \mid 9$, so solutions exist. Dividing by 3: $4x \equiv 3 \pmod{5}$. Since $4 \cdot 4 = 16 \equiv 1 \pmod{5}$, the inverse of 4 modulo 5 is 4. Thus $x \equiv 4 \cdot 3 = 12 \equiv 2 \pmod{5}$.
The three solutions modulo 15 are

$$x \equiv 2, \quad x \equiv 7, \quad x \equiv 12 \pmod{15}.$$

Example 3.14 (No solution)**.** The congruence $6x \equiv 5 \pmod{9}$ has no solution because $\gcd(6, 9) = 3$ and $3 \nmid 5$.

3.5 Divisibility Criteria via Congruences

Congruences provide elegant proofs of the familiar divisibility tests learned in school. Let N be a positive integer with decimal representation $N = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$.

Proposition 3.15 (Divisibility by 3 and 9)**.** $N \equiv a_k + a_{k-1} + \cdots + a_0 \pmod{9}$. *In particular,* $3 \mid N$ *iff* 3 *divides the digit sum, and* $9 \mid N$ *iff* 9 *divides the digit sum.*

Proof. Since $10 \equiv 1 \pmod{9}$, we have $10^j \equiv 1 \pmod{9}$ for all $j \geq 0$. Hence $N \equiv \sum_{j=0}^{k} a_j \cdot 1 = \sum a_j \pmod{9}$. The criterion for 3 follows because $3 \mid 9$. □

Proposition 3.16 (Divisibility by 11)**.** $N \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \pmod{11}$. *Hence* $11 \mid N$ *if and only if* 11 *divides the alternating digit sum.*

Proof. Since $10 \equiv -1 \pmod{11}$, we have $10^j \equiv (-1)^j \pmod{11}$, so $N \equiv \sum_{j=0}^{k} (-1)^j a_j \pmod{11}$. □

Proposition 3.17 (Divisibility by 7, 11, and 13)**.** *Since* $7 \cdot 11 \cdot 13 = 1001$ *and* $10^3 \equiv -1 \pmod{1001}$*, one can test divisibility by* 7*,* 11*, or* 13 *by forming alternating sums of three-digit blocks from right to left.*

Example 3.18. Consider $N = 2\,358\,271$. The three-digit blocks from the right are 271, 358, 2. The alternating sum is $271 - 358 + 2 = -85$. Since $-85 = -5 \cdot 17$, we see that N is not divisible by 7, 11, or 13.

3.6 Fast Modular Exponentiation

Computing $a^k \bmod n$ by repeated multiplication requires $k - 1$ multiplications, which is infeasible when k is hundreds of digits long (as in cryptographic applications). The method of *repeated squaring* (also known as *binary exponentiation*) reduces the cost to at most $2\lfloor \log_2 k \rfloor$ multiplications modulo n.

Definition 3.19 (Binary exponentiation)**.** Write k in binary: $k = (b_\ell b_{\ell-1} \cdots b_1 b_0)_2$ with $b_\ell = 1$. Then

$$a^k = a^{2^\ell b_\ell + \cdots + 2b_1 + b_0} = \prod_{i=0}^{\ell} \left(a^{2^i}\right)^{b_i}.$$

Each successive a^{2^i} is obtained by squaring the previous one.

Example 3.20 (Computing $3^{45} \bmod 67$)**.** We have $45 = (101101)_2 = 32 + 8 + 4 + 1$. Build the table:

$$\begin{aligned} 3^1 &\equiv 3 \pmod{67}, \\ 3^2 &\equiv 9, \\ 3^4 &\equiv 81 \equiv 14, \\ 3^8 &\equiv 14^2 = 196 \equiv 62 \equiv -5, \\ 3^{16} &\equiv 25, \\ 3^{32} &\equiv 625 \equiv 625 - 9 \cdot 67 = 625 - 603 = 22. \end{aligned}$$

Therefore $3^{45} \equiv 3^{32} \cdot 3^8 \cdot 3^4 \cdot 3^1 \equiv 22 \cdot (-5) \cdot 14 \cdot 3 \pmod{67}$.
Computing step by step: $22 \cdot (-5) = -110 \equiv -110 + 2 \cdot 67 = 24$, then $24 \cdot 14 = 336 \equiv 336 - 5 \cdot 67 = 336 - 335 = 1$, then $1 \cdot 3 = 3$. So $3^{45} \equiv 3 \pmod{67}$.

Remark 3.21 (Complexity). The binary exponentiation algorithm computes $a^k \bmod n$ using $O(\log k)$ modular multiplications, each of which costs $O((\log n)^2)$ bit opera-

tions (using schoolbook multiplication). The total cost is thus $O((\log k)(\log n)^2)$ bit operations.

3.7 Connections to Cryptography

Modular arithmetic is the computational backbone of modern public-key cryptography. We highlight two points; a full treatment of RSA and Diffie–Hellman appears in Chapter 4.

1. **One-way functions.** The map $x \mapsto g^x \bmod p$ (for a prime p and generator g of $(\mathbb{Z}/p\mathbb{Z})^\times$) is easy to compute via repeated squaring, but inverting it—the *discrete logarithm problem*—is believed to be computationally hard.

2. **Modular inverses in RSA.** The RSA cryptosystem relies on computing modular inverses via the extended Euclidean algorithm, and on the difficulty of factoring a product $n = pq$ of two large primes.

3.8 Exercises

Exercise 3.1. Determine the last two digits of 7^{999} (i.e. compute $7^{999} \bmod 100$).

Exercise 3.2. Find all solutions of $35x \equiv 14 \pmod{91}$.

Exercise 3.3. Prove that if p is an odd prime and $a \not\equiv 0 \pmod p$, then $ax \equiv b \pmod p$ has a unique solution modulo p.

Exercise 3.4. List all units and all zero divisors in $\mathbb{Z}/12\mathbb{Z}$. For each unit, find its multiplicative inverse.

Exercise 3.5. Using $10^3 \equiv 1 \pmod{37}$, derive a test for divisibility by 37 based on splitting the decimal representation into three-digit blocks.

Exercise 3.6. Use binary exponentiation to compute $5^{117} \bmod 19$.

Exercise 3.7. Solve the system of congruences $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$. (This foreshadows the Chinese Remainder Theorem.)

Exercise 3.8. Let $n = p^k$ for a prime p and $k \geq 1$. Prove that $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent (i.e. $\bar{a}^m = \bar{0}$ for some $m \geq 1$) if and only if $p \mid a$.

Exercise 3.9. Find all idempotent elements ($e^2 = e$) in $\mathbb{Z}/n\mathbb{Z}$ for $n = 6, 10, 15$. What pattern do you observe?

Exercise 3.10 (Challenge)**.** Prove that for every $n \geq 2$, the product of all units in $(\mathbb{Z}/n\mathbb{Z})^\times$ equals $-\bar{1}$ if $n = 1, 2, 4, p^k$, or $2p^k$ (for odd prime p), and equals $\bar{1}$ otherwise.

3.9 Chapter Summary

1. **Congruence** $a \equiv b \pmod{n}$ means $n \mid (a - b)$. It is an equivalence relation compatible with addition and multiplication.

2. The quotient ring $\mathbb{Z}/n\mathbb{Z}$ consists of n residue classes. Its units are the classes $\bar{a}$ with $\gcd(a, n) = 1$; the remaining nonzero classes are zero divisors. $\mathbb{Z}/n\mathbb{Z}$ is a field iff n is prime.

3. The linear congruence $ax \equiv b \pmod{n}$ has solutions iff $\gcd(a, n) \mid b$, and then exactly $\gcd(a, n)$ incongruent solutions.

4. Classical divisibility tests follow from $10 \equiv 1 \pmod{9}$, $10 \equiv -1 \pmod{11}$, etc.

5. Binary exponentiation computes $a^k \bmod n$ in $O(\log k)$ multiplications, enabling efficient cryptographic computations.

Chapter 4

Theorems of Fermat, Euler, and Wilson

4.1 Historical Context: Fermat's Letter to Frénicle

On 18 October 1640, Pierre de Fermat wrote a letter to Bernard Frénicle de Bessy in which he stated, without proof, a remarkable observation:

> *If p is prime and a is not divisible by p, then $a^{p-1} - 1$ is always divisible by p.*

Fermat added, characteristically, "I would send you the proof, if I did not fear it being too long." The first published proof was given by Euler in 1736, who later generalised the result to composite moduli using what we now call *Euler's totient function*.

Wilson's theorem, stating that $(p-1)! \equiv -1 \pmod{p}$ for every prime p, was first conjectured by the English mathematician John Wilson around 1770. Lagrange provided the first proof in 1771.

This chapter presents complete proofs of these classical theorems and explores their far-reaching applications, including the RSA cryptosystem and the Diffie–Hellman key exchange protocol.

4.2 Euler's Totient Function

Definition 4.1 (Euler's totient function)**.** For $n \geq 1$, *Euler's totient function* $\varphi(n)$ is the number of integers a with $1 \leq a \leq n$ and $\gcd(a, n) = 1$. Equivalently,

$$\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^{\times}\right|.$$

Example 4.2 (Small values)**.** $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(10) = 4$, $\varphi(12) = 4$.

Proposition 4.3 (Totient of a prime)**.** *If p is prime, then $\varphi(p) = p - 1$.*

Proof. Every integer a with $1 \leq a \leq p-1$ satisfies $\gcd(a, p) = 1$. □

Proposition 4.4 (Totient of a prime power)**.** *For a prime p and $k \geq 1$,*

$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k\left(1 - \frac{1}{p}\right).$$

Proof. Among $\{1, 2, \ldots, p^k\}$, the integers *not* coprime to p^k are exactly the multiples of p: these are $p, 2p, 3p, \ldots, p^{k-1} \cdot p$, and there are p^{k-1} of them. Hence $\varphi(p^k) = p^k - p^{k-1}$. □

Theorem 4.5 (Multiplicativity of φ)**.** *If $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. By the Chinese Remainder Theorem, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ as rings when $\gcd(m, n) = 1$. This isomorphism restricts to an isomorphism of unit groups:

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

Taking cardinalities gives $\varphi(mn) = \varphi(m)\varphi(n)$. □

Theorem 4.6 (Product formula for φ)**.** *For any $n \geq 2$ with prime factorisation $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$,*

$$\varphi(n) = n \prod_{p \mid n}\left(1 - \frac{1}{p}\right) = n \cdot \frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdots \frac{p_r - 1}{p_r}.$$

Proof. Combine multiplicativity (Theorem 4.5) with the prime-power formula (Proposition 4.4):

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{k_i}) = \prod_{i=1}^{r} p_i^{k_i}\left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right).$$ □

Example 4.7 (Computing $\varphi(360)$)**.** We have $360 = 2^3 \cdot 3^2 \cdot 5$, so

$$\varphi(360) = 360 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96.$$

Theorem 4.8 (Gauss's divisor sum for φ)**.** *For every $n \geq 1$,*

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

Proof. Partition $\{1, 2, \ldots, n\}$ according to $\gcd(a, n)$. For each divisor d of n, the number of integers a with $1 \leq a \leq n$ and $\gcd(a, n) = d$ equals the number of integers b with $1 \leq b \leq n/d$ and $\gcd(b, n/d) = 1$, which is $\varphi(n/d)$. Summing over all divisors d of n:

$$n = \sum_{d \mid n} \varphi\left(\frac{n}{d}\right) = \sum_{d \mid n} \varphi(d),$$

where the last equality holds because as d ranges over divisors of n, so does n/d. □

4.3 Euler's Theorem

Theorem 4.9 (Euler's theorem)**.** *If $n \geq 1$ and $\gcd(a, n) = 1$, then*

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

Proof. Let $(\mathbb{Z}/n\mathbb{Z})^\times = \{r_1, r_2, \ldots, r_{\varphi(n)}\}$ be the group of units. Since $\gcd(a, n) = 1$, multiplication by $\bar{a}$ is a bijection from $(\mathbb{Z}/n\mathbb{Z})^\times$ to itself. Therefore the set $\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$ is simply a rearrangement of $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ modulo n.

Taking the product of all elements in each set:

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

The left side equals $a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} r_i$. Let $P = \prod_{i=1}^{\varphi(n)} r_i$. Then

$$a^{\varphi(n)} \cdot P \equiv P \pmod{n}.$$

Since each r_i is a unit, P is also a unit and may be cancelled, yielding $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Remark 4.10. From the viewpoint of group theory, Euler's theorem is an immediate consequence of Lagrange's theorem: the order of any element of a finite group divides the order of the group. Applied to the element $\bar{a}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$, whose order is $\varphi(n)$, we obtain $\bar{a}^{\varphi(n)} = \bar{1}$.

4.4 Fermat's Little Theorem

Corollary 4.11 (Fermat's little theorem)**.** *If p is prime and $p \nmid a$, then*

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

Equivalently, for any integer a,

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

Proof. The first form follows from Euler's theorem with $n = p$, since $\varphi(p) = p - 1$. For the second form: if $p \mid a$, both sides are $\equiv 0$; if $p \nmid a$, multiply the first form by a. □

Example 4.12 (Application of Fermat)**.** Compute $2^{100} \bmod 13$. By Fermat, $2^{12} \equiv 1 \pmod{13}$. Since $100 = 12 \cdot 8 + 4$, we get $2^{100} = (2^{12})^8 \cdot 2^4 \equiv 1^8 \cdot 16 \equiv 3 \pmod{13}$.

Remark 4.13 (Fermat pseudoprimes). The converse of Fermat's little theorem is false. A composite number n satisfying $2^{n-1} \equiv 1 \pmod{n}$ is called a *Fermat pseudoprime* to base 2. The smallest example is $n = 341 = 11 \cdot 31$. Composite numbers that satisfy $a^{n-1} \equiv 1 \pmod{n}$ for *all* a with $\gcd(a, n) = 1$ are called *Carmichael numbers*; the smallest is $561 = 3 \cdot 11 \cdot 17$.

4.5 Wilson's Theorem

Theorem 4.14 (Wilson's theorem)**.** *An integer $p \geq 2$ is prime if and only if*

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

Proof. We prove both directions.

($\Rightarrow$) If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Consider the elements $1, 2, \ldots, p-1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, each element a has a unique multiplicative inverse a^{-1}, and $a = a^{-1}$ if and only if $a^2 \equiv 1 \pmod{p}$, i.e. $p \mid (a-1)(a+1)$. Since p is prime, this forces $a \equiv 1$ or $a \equiv -1 \pmod{p}$.

Thus, in the product $(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1)$, the elements $2, 3, \ldots, p-2$ can be paired off: each a with its inverse $a^{-1} \neq a$. Each such pair contributes $a \cdot a^{-1} = 1$ to the product. The only unpaired elements are 1 and $p-1 \equiv -1$. Therefore

$$(p-1)! \equiv 1 \cdot (-1) \cdot \prod_{\text{pairs}} 1 = -1 \pmod{p}.$$

($\Leftarrow$) If $(p-1)! \equiv -1 \pmod{p}$, then p is prime.

Suppose p is composite. Then p has a divisor d with $1 < d < p$, so d appears as one of the factors in $(p-1)!$, hence $d \mid (p-1)!$. Since $d \mid p$, we would need $d \mid ((p-1)! + 1)$ and $d \mid (p-1)!$, forcing $d \mid 1$, a contradiction. Hence p must be prime. □

Example 4.15. For $p = 7$: $6! = 720 = 102 \cdot 7 + 6 = 103 \cdot 7 - 1$, confirming $6! \equiv -1 \pmod{7}$.
The pairing: $2 \leftrightarrow 4$ (since $2 \cdot 4 = 8 \equiv 1$), $3 \leftrightarrow 5$ (since $3 \cdot 5 = 15 \equiv 1$). Unpaired: 1 and 6. So $6! \equiv 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 1 \cdot 1 \cdot 1 \cdot (-1) = -1 \pmod{7}$.

Corollary 4.16. *If p is an odd prime, then*

$$\Big(((p-1)/2)!\Big)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Proof. Note that $k \equiv -(p-k) \pmod{p}$ for $1 \leq k \leq p-1$. Thus

$$\begin{aligned}(p-1)! &= \prod_{k=1}^{(p-1)/2} k \cdot \prod_{k=(p+1)/2}^{p-1} k = \prod_{k=1}^{(p-1)/2} k \cdot \prod_{j=1}^{(p-1)/2} (p-j) \\ &\equiv \prod_{k=1}^{(p-1)/2} k \cdot \prod_{j=1}^{(p-1)/2} (-j) = (-1)^{(p-1)/2} \left(\left(\frac{p-1}{2}\right)!\right)^2 \pmod{p}.\end{aligned}$$

By Wilson, the left side is $\equiv -1 \pmod{p}$, so $\Big(((p-1)/2)!\Big)^2 \equiv (-1) \cdot (-1)^{-(p-1)/2} = (-1)^{1-(p-1)/2} = (-1)^{(3-p)/2} = (-1)^{(p+1)/2} \pmod{p}$, where the last equality uses $(-1)^{(3-p)/2} = (-1)^{(p+1)/2}$ since $(3-p)/2 + (p+1)/2 = 2$ is even. □

4.6 Primitive Roots

Definition 4.17 (Order of an element)**.** Let $\gcd(a, n) = 1$. The *order* of a modulo n, denoted $\mathrm{ord}_n(a)$, is the smallest positive integer d such that $a^d \equiv 1 \pmod{n}$.

Proposition 4.18 (Basic properties of the order)**.** *Let* $\gcd(a, n) = 1$ *and* $d = \mathrm{ord}_n(a)$. *Then:*

(i) $a^k \equiv 1 \pmod{n}$ *if and only if* $d \mid k$.

(ii) $d \mid \varphi(n)$.

(iii) $\mathrm{ord}_n(a^j) = d/\gcd(j, d)$.

Proof.

(i) ($\Leftarrow$) If $k = dq$, then $a^k = (a^d)^q \equiv 1$. ($\Rightarrow$) Write $k = dq + r$ with $0 \le r < d$. Then $a^r = a^k \cdot (a^d)^{-q} \equiv 1 \pmod{n}$. By minimality of d, $r = 0$.

(ii) By Euler's theorem, $a^{\varphi(n)} \equiv 1$, so $d \mid \varphi(n)$ by (i).

(iii) Let $e = \mathrm{ord}_n(a^j)$. Then $(a^j)^e = a^{je} \equiv 1$, so $d \mid je$, i.e. $(d/g) \mid e$ where $g = \gcd(j, d)$. Conversely, $(a^j)^{d/g} = (a^d)^{j/g} \equiv 1$, so $e \mid (d/g)$. Hence $e = d/g$. □

Definition 4.19 (Primitive root)**.** A *primitive root modulo* n is an integer g with $\gcd(g, n) = 1$ and $\mathrm{ord}_n(g) = \varphi(n)$. Equivalently, g is a primitive root iff $\bar{g}$ generates the cyclic group $(\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem 4.20 (Existence of primitive roots for primes)**.** *For every prime* p, *the group* $(\mathbb{Z}/p\mathbb{Z})^\times$ *is cyclic of order* $p - 1$. *In other words, there exists a primitive root modulo* p.

Proof. We use a counting argument. For each divisor d of $p - 1$, let $\psi(d)$ denote the number of elements of order d in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Step 1: The polynomial $x^d - 1$ has at most d roots in $\mathbb{Z}/p\mathbb{Z}$.
Since $\mathbb{Z}/p\mathbb{Z}$ is a field, a polynomial of degree d over $\mathbb{Z}/p\mathbb{Z}$ has at most d roots.

Step 2: For each $d \mid (p-1)$, $x^d \equiv 1 \pmod{p}$ has exactly d solutions.
Since $d \mid (p - 1)$, we can write $x^{p-1} - 1 = (x^d - 1) \cdot q(x)$ for some polynomial q of degree $p - 1 - d$. The polynomial $x^{p-1} - 1$ has exactly $p - 1$ roots (namely $1, 2, \ldots, p - 1$, by Fermat), and $q(x)$ has at most $p - 1 - d$ roots. Therefore $x^d - 1$ must have at least $(p - 1) - (p - 1 - d) = d$ roots, and by Step 1, at most d. So it has exactly d roots.

Step 3: If $\psi(d) > 0$ for some $d \mid (p-1)$, then $\psi(d) = \varphi(d)$.
Suppose a has order d. Then $a, a^2, \ldots, a^d$ are d distinct elements satisfying $x^d \equiv 1$. By Step 2 these are *all* solutions of $x^d \equiv 1$. Among them, a^j has order d iff $\gcd(j, d) = 1$ (by Proposition 4.18(iii)), and there are exactly $\varphi(d)$ such values of j. Hence $\psi(d) = \varphi(d)$.

Step 4: $\psi(d) = \varphi(d)$ for all $d \mid (p-1)$.

Every element of $(\mathbb{Z}/p\mathbb{Z})^\times$ has some order d dividing $p-1$, so

$$p - 1 = \sum_{d \mid (p-1)} \psi(d).$$

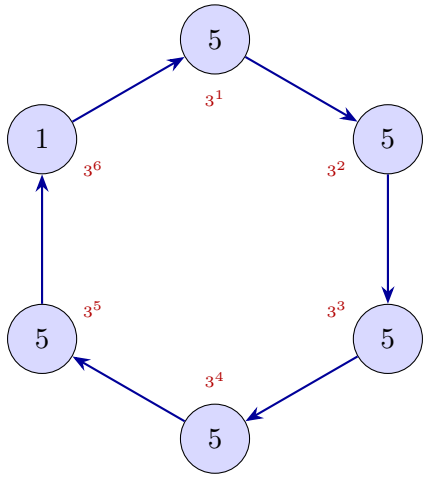
From Gauss's identity (Theorem 4.8), $p-1 = \sum_{d\mid(p-1)} \varphi(d)$. Since $\psi(d) \le \varphi(d)$ for all d (by Step 3 and the fact that $\psi(d) \in \{0, \varphi(d)\}$), equality of the sums forces $\psi(d) = \varphi(d)$ for every d.

In particular, $\psi(p-1) = \varphi(p-1) \ge 1$, so there exists an element of order $p-1$, which is a primitive root. □

Example 4.21 (Primitive roots modulo 7)**.** The elements of $(\mathbb{Z}/7\mathbb{Z})^\times = \{1,2,3,4,5,6\}$ have orders:

a	1	2	3	4	5	6
$\operatorname{ord}_7(a)$	1	3	6	3	6	2

The primitive roots are 3 and 5 (each has order $\varphi(7) = 6$). Note $\varphi(6) = 2$, matching the count.



The cyclic group $(\mathbb{Z}/7\mathbb{Z})^\times = \langle 3 \rangle$: successive powers of $g = 3$.

Figure 4.1: The cyclic structure of $(\mathbb{Z}/7\mathbb{Z})^\times$ generated by the primitive root $g = 3$.

Theorem 4.22 (Characterisation of moduli with primitive roots)**.** *Primitive roots exist modulo n if and only if $n \in \{1, 2, 4, p^k, 2p^k\}$, where p is an odd prime and $k \ge 1$.*

Remark 4.23. The proof of this complete characterisation requires tools beyond the scope of this chapter (specifically, the structure of the groups $(\mathbb{Z}/2^k\mathbb{Z})^\times$ for $k \ge 3$ and the Chinese Remainder Theorem applied to unit groups). We have proved the case $n = p$ in Theorem 4.20.

Proposition 4.24 (Number of primitive roots)**.** *If primitive roots exist modulo n, then there are exactly $\varphi(\varphi(n))$ of them.*

Proof. Let g be a primitive root. Then every unit modulo n is g^j for a unique $j \in \{0, 1, \ldots, \varphi(n) - 1\}$. By Proposition 4.18(iii), g^j is a primitive root iff $\gcd(j, \varphi(n)) = 1$, and there are $\varphi(\varphi(n))$ such values. □

$a \backslash k$	1	2	3	4	5	6	7	8	9	10
2	6	6	6	6	6	6	6	6	6	1
3	4	4	4	4	4	4	4	4	4	1
5	9	9	9	9	9	9	9	9	9	1
10	10	10	10	10	10	10	10	10	10	1

Powers $a^k \bmod 11$ for selected bases; entries equal to 1 are highlighted.

Figure 4.2: Power table modulo 11: $a = 2$ is a primitive root (order 10), while $a = 3, 5$ have order 5 and $a = 10$ has order 2.

4.7 The RSA Cryptosystem

The RSA cryptosystem, invented by Rivest, Shamir, and Adleman in 1977, is perhaps the most celebrated application of number theory. Its security rests on the difficulty of factoring large integers.

4.7.1 Key Generation

1. Choose two distinct large primes p and q. Set $n = pq$.
2. Compute $\varphi(n) = (p - 1)(q - 1)$.
3. Choose an integer e with $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$. (The common choice is $e = 65537 = 2^{16} + 1$.)
4. Compute $d \equiv e^{-1} \pmod{\varphi(n)}$, i.e. find d with $ed \equiv 1 \pmod{\varphi(n)}$.
5. The *public key* is (n, e); the *private key* is (n, d).

4.7.2 Encryption and Decryption

To encrypt a message m (an integer with $0 \le m < n$):

$$c \equiv m^e \pmod{n} \qquad \text{(ciphertext)}.$$

To decrypt:

$$m \equiv c^d \pmod{n} \qquad \text{(recover plaintext)}.$$

4.7.3 Proof of Correctness

Theorem 4.25 (RSA correctness)**.** *With notation as above, $c^d \equiv m \pmod{n}$ for every integer m with $0 \le m < n$.*

Proof. Since $ed \equiv 1 \pmod{\varphi(n)}$, write $ed = 1 + k\varphi(n)$ for some non-negative integer k. We must show $m^{ed} \equiv m \pmod{n}$, i.e. $m^{1+k(p-1)(q-1)} \equiv m \pmod{pq}$.

By the Chinese Remainder Theorem, it suffices to prove the congruence modulo p and modulo q separately.

Modulo p: If $p \mid m$, then $m \equiv 0 \pmod{p}$ and $m^{ed} \equiv 0 \equiv m$. If $p \nmid m$, then by Fermat's little theorem $m^{p-1} \equiv 1 \pmod{p}$, so

$$m^{ed} = m^{1+k(p-1)(q-1)} = m \cdot \left(m^{p-1}\right)^{k(q-1)} \equiv m \cdot 1^{k(q-1)} = m \pmod{p}.$$

Modulo q: By the identical argument, $m^{ed} \equiv m \pmod{q}$.

Since $\gcd(p, q) = 1$ and $m^{ed} \equiv m$ both mod p and mod q, we conclude $m^{ed} \equiv m \pmod{pq} = m \pmod{n}$. □

Example 4.26 (Toy RSA)**.** Let $p = 11$, $q = 13$, so $n = 143$ and $\varphi(n) = 10 \cdot 12 = 120$. Choose $e = 7$. Then $d \equiv 7^{-1} \pmod{120}$. Since $7 \cdot 103 = 721 = 6 \cdot 120 + 1$, we get $d = 103$.
Encrypt $m = 9$: $c \equiv 9^7 \pmod{143}$. We compute: $9^2 = 81$, $9^4 \equiv 81^2 = 6561 \equiv 6561 - 45 \cdot 143 = 6561 - 6435 = 126$, $9^7 = 9^4 \cdot 9^2 \cdot 9 \equiv 126 \cdot 81 \cdot 9 \pmod{143}$. Now $126 \cdot 81 = 10206 \equiv 10206 - 71 \cdot 143 = 10206 - 10153 = 53$, then $53 \cdot 9 = 477 \equiv 477 - 3 \cdot 143 = 477 - 429 = 48$. So $c = 48$.
Decrypt: $m \equiv 48^{103} \pmod{143}$. Using repeated squaring (which we omit for brevity), one verifies $48^{103} \equiv 9 \pmod{143}$, recovering the original message.

Remark 4.27 (Security of RSA). An adversary who knows n and e can recover d if they can compute $\varphi(n) = (p-1)(q-1)$. This is equivalent in difficulty to factoring $n = pq$, which—for n of several thousand bits—is believed to be computationally infeasible with current algorithms. In practice, one uses primes of at least 1024 bits each, giving n of at least 2048 bits.

4.8 Diffie–Hellman Key Exchange

Published in 1976 by Whitfield Diffie and Martin Hellman, the Diffie–Hellman protocol allows two parties—traditionally called Alice and Bob—to establish a shared secret over an insecure channel.

4.8.1 Protocol Description

1. **Public parameters:** A large prime p and a primitive root g modulo p are agreed upon publicly.
2. **Alice's step:** Alice chooses a secret integer a ($1 \le a \le p-2$) and sends $A \equiv g^a \pmod{p}$ to Bob.

3. **Bob's step:** Bob chooses a secret integer b ($1 \leq b \leq p-2$) and sends $B \equiv g^b \pmod{p}$ to Alice.

4. **Shared secret:** Alice computes $s \equiv B^a \equiv g^{ab} \pmod{p}$. Bob computes $s \equiv A^b \equiv g^{ab} \pmod{p}$. Both arrive at the same shared secret s.

Remark 4.28 (Security). An eavesdropper who observes p, g, $A = g^a \bmod p$, and $B = g^b \bmod p$ must compute $g^{ab} \bmod p$. This is the *Diffie–Hellman problem*, which is believed to be as hard as the discrete logarithm problem—computing a from $g^a \bmod p$—for which no efficient classical algorithm is known.

Example 4.29 (Toy Diffie–Hellman)**.** Let $p = 23$ and $g = 5$ (a primitive root modulo 23).

- Alice picks $a = 6$ and sends $A \equiv 5^6 \equiv 15625 \equiv 15625 - 679 \cdot 23 = 15625 - 15617 = 8 \pmod{23}$.
- Bob picks $b = 15$ and sends $B \equiv 5^{15} \pmod{23}$. Using repeated squaring: $5^2 = 25 \equiv 2$, $5^4 \equiv 4$, $5^8 \equiv 16$, $5^{15} = 5^8 \cdot 5^4 \cdot 5^2 \cdot 5 \equiv 16 \cdot 4 \cdot 2 \cdot 5 = 640 \equiv 640 - 27 \cdot 23 = 640 - 621 = 19 \pmod{23}$.
- Alice computes $s \equiv B^a = 19^6 \pmod{23}$. $19^2 = 361 \equiv 361 - 15 \cdot 23 = 16$, $19^4 \equiv 16^2 = 256 \equiv 256 - 11 \cdot 23 = 3$, $19^6 = 19^4 \cdot 19^2 \equiv 3 \cdot 16 = 48 \equiv 2 \pmod{23}$.
- Bob computes $s \equiv A^b = 8^{15} \pmod{23}$. $8^2 = 64 \equiv 18$, $8^4 \equiv 324 \equiv 324 - 14 \cdot 23 = 2$, $8^8 \equiv 4$, $8^{15} = 8^8 \cdot 8^4 \cdot 8^2 \cdot 8 \equiv 4 \cdot 2 \cdot 18 \cdot 8 = 1152 \equiv 1152 - 50 \cdot 23 = 1152 - 1150 = 2 \pmod{23}$.
- Both obtain the shared secret $s = 2$.

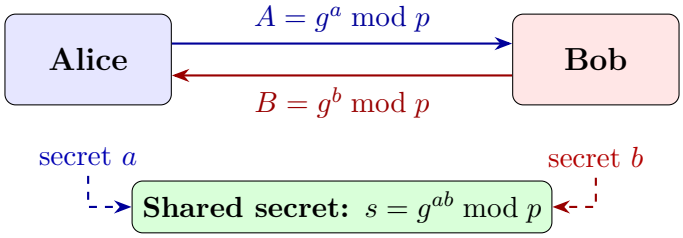


Figure 4.3: The Diffie–Hellman key exchange protocol.

4.9 Exercises

Exercise 4.1. Compute $\varphi(n)$ for $n = 100, 252, 1000, 2520$.

Exercise 4.2. Use Euler's theorem to compute $3^{1000} \bmod 35$.

Exercise 4.3. Find the remainder when 2^{2025} is divided by 17.

Exercise 4.4. Using Wilson's theorem, find the least non-negative residue of $18! \pmod{23}$.

Exercise 4.5. Find all primitive roots modulo 11. Verify that there are $\varphi(\varphi(11)) = \varphi(10) = 4$ of them.

Exercise 4.6. Prove that $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic. (Hence there is no primitive root modulo 8.)

Exercise 4.7. Let p be prime and $\gcd(a, p) = 1$. Prove that if $\operatorname{ord}_p(a) = d$, then $\{a^0, a^1, \ldots, a^{d-1}\}$ are the d distinct roots of $x^d - 1 \equiv 0 \pmod{p}$.

Exercise 4.8. In a toy RSA system with $p = 7$, $q = 11$, $e = 13$:

(a) Compute n, $\varphi(n)$, and d.

(b) Encrypt $m = 5$ and then decrypt to verify correctness.

Exercise 4.9. In a toy Diffie–Hellman exchange with $p = 29$, $g = 2$, Alice picks $a = 11$ and Bob picks $b = 19$. Compute the values exchanged and the shared secret.

Exercise 4.10. Verify that $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number by checking that $a^{560} \equiv 1 \pmod{561}$ for all a with $\gcd(a, 561) = 1$. *Hint:* Use Korselt's criterion: n is a Carmichael number iff n is square-free and $(p-1) \mid (n-1)$ for every prime $p \mid n$.

Exercise 4.11. Prove that $\sum_{d \mid n} \varphi(d) = n$ using Möbius inversion, providing an alternative to the direct counting argument of Theorem 4.8.

Exercise 4.12 (Challenge)**.** Let p be an odd prime. Prove that the product of all primitive roots modulo p is congruent to 1 modulo p. *Hint:* If g is a primitive root, the primitive roots are g^k with $\gcd(k, p-1) = 1$. Sum the exponents and use the fact that $\sum_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} k = \frac{n\varphi(n)}{2}$ for $n > 2$.

Exercise 4.13 (Challenge)**.** Let $\gcd(a, n) = \gcd(b, n) = 1$ and suppose $\gcd(\operatorname{ord}_n(a), \operatorname{ord}_n(b)) = 1$. Prove that $\operatorname{ord}_n(ab) = \operatorname{ord}_n(a) \cdot \operatorname{ord}_n(b)$. Give a counterexample when the orders are not coprime.

4.10 Chapter Summary

1. **Euler's totient function** $\varphi(n)$ counts integers $1 \le a \le n$ with $\gcd(a, n) = 1$. It is multiplicative and satisfies $\varphi(n) = n \prod_{p \mid n} (1 - 1/p)$.

2. **Euler's theorem:** $a^{\varphi(n)} \equiv 1 \pmod{n}$ whenever $\gcd(a, n) = 1$.

3. **Fermat's little theorem:** $a^{p-1} \equiv 1 \pmod{p}$ for prime p and $p \nmid a$. Equivalently, $a^p \equiv a \pmod{p}$ for all a.

4. **Wilson's theorem:** $(p-1)! \equiv -1 \pmod{p}$ if and only if p is prime.

5. **Primitive roots:** $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic for every prime p. More generally, primitive roots exist for $n = 1, 2, 4, p^k, 2p^k$.

6. **RSA:** Encryption $c = m^e \bmod n$, decryption $m = c^d \bmod n$, where $ed \equiv 1 \pmod{\varphi(n)}$ and $n = pq$. Correctness follows from Fermat/Euler.

7. **Diffie–Hellman:** Two parties exchange g^a and g^b modulo a prime, arriving at a shared secret g^{ab}. Security relies on the hardness of the discrete logarithm problem.

Chapter 5

Chinese Remainder Theorem and Applications

Historical Introduction

The problem of solving simultaneous congruences appears in the *Sunzi Suanjing* (*Master Sun's Mathematical Manual*), a Chinese text from the 3rd–5th century CE. The classic formulation asks:

> *There are certain things whose number is unknown. If we count them by threes, the remainder is* 2*; if we count them by fives, the remainder is* 3*; if we count them by sevens, the remainder is* 2*. How many things are there?*

Sun Tzu[1] gave the answer 23 and a method of solution. Centuries later, **Qin Jiushao** (1202–1261) developed a general algorithm in his *Mathematical Treatise in Nine Sections* (1247), which systematically solved systems of simultaneous congruences using what we would now call the extended Euclidean algorithm. His work preceded the European rediscovery by several hundred years.

In the West, the theorem was stated by Euler and given its modern algebraic formulation by Gauss in the *Disquisitiones Arithmeticae* (1801).

5.1 Systems of Linear Congruences

We begin with the motivating problem: given congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \dots, \quad x \equiv a_k \pmod{m_k},$$

when does a simultaneous solution exist, and when is it unique?

Example 5.1 (Sun Tzu's problem)**.** We seek x satisfying

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7}.$$

By inspection, $x = 23$ works. We shall soon see that this is the unique solution modulo $3 \cdot 5 \cdot 7 = 105$, so the full solution set is $\{23 + 105k : k \in \mathbb{Z}\}$.

[1] Not to be confused with the military strategist of the same name.

Lemma 5.2 (Two-congruence case)**.** *Let $m_1, m_2 \in \mathbb{Z}_{>0}$. The system*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}$$

has a solution if and only if $\gcd(m_1, m_2) \mid (a_1 - a_2)$*. When a solution exists, it is unique modulo* $\operatorname{lcm}(m_1, m_2)$*.*

Proof. The system is equivalent to the existence of integers k_1, k_2 with $a_1 + m_1 k_1 = a_2 + m_2 k_2$, i.e., $m_1 k_1 - m_2 k_2 = a_2 - a_1$. By the characterisation of the image of the linear map $(k_1, k_2) \mapsto m_1 k_1 - m_2 k_2$, this equation is solvable if and only if $\gcd(m_1, m_2) \mid (a_2 - a_1)$.

For uniqueness, suppose x_0 and x_0' are both solutions. Then $m_1 \mid (x_0' - x_0)$ and $m_2 \mid (x_0' - x_0)$, whence $\operatorname{lcm}(m_1, m_2) \mid (x_0' - x_0)$. □

5.2 The Chinese Remainder Theorem

Theorem 5.3 (Chinese Remainder Theorem — CRT)**.** *Let $m_1, m_2, \ldots, m_k$ be pairwise coprime positive integers, and set $M = m_1 m_2 \cdots m_k$. Then for any integers $a_1, a_2, \ldots, a_k$, the system*

$$x \equiv a_i \pmod{m_i}, \qquad i = 1, 2, \ldots, k, \tag{5.1}$$

has a solution, and any two solutions are congruent modulo M. Explicitly, the unique solution modulo M is

$$x \equiv \sum_{i=1}^{k} a_i \, M_i \, y_i \pmod{M}, \tag{5.2}$$

where $M_i = M/m_i$ and y_i is any integer satisfying $M_i \, y_i \equiv 1 \pmod{m_i}$.

Proof. We give a constructive proof in two parts.

Existence. For each $i \in \{1, \ldots, k\}$, define $M_i = M/m_i = \prod_{j \neq i} m_j$. Since the m_j are pairwise coprime, every prime factor of m_i divides m_i but none of the m_j $(j \neq i)$, so $\gcd(M_i, m_i) = 1$. By Bézout's identity, there exists $y_i \in \mathbb{Z}$ with

$$M_i \, y_i \equiv 1 \pmod{m_i}.$$

Now set

$$x_0 = \sum_{i=1}^{k} a_i \, M_i \, y_i.$$

We verify that x_0 solves each congruence. Fix any index j. For $i \neq j$, the factor M_i contains m_j as one of its factors (since $j \neq i$), so $m_j \mid M_i$ and thus $a_i M_i y_i \equiv 0 \pmod{m_j}$. For $i = j$, we have $a_j M_j y_j \equiv a_j \cdot 1 = a_j \pmod{m_j}$. Therefore

$$x_0 \equiv a_j \pmod{m_j}$$

for every j, as required.

Uniqueness. Suppose x_0 and x_0' both satisfy (5.1). Then $m_i \mid (x_0' - x_0)$ for all i. Since $m_1, \ldots, m_k$ are pairwise coprime, it follows that $M = m_1 \cdots m_k$ divides $x_0' - x_0$ (this is a straightforward induction using the fact that if $\gcd(a, b) = 1$ and $a \mid n$, $b \mid n$, then $ab \mid n$). Hence $x_0' \equiv x_0 \pmod{M}$. □

Example 5.4 (Solving Sun Tzu's problem via CRT)**.** With $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, we have $M = 105$, and

$$M_1 = 35, \quad M_2 = 21, \quad M_3 = 15.$$

We find the inverses modulo each m_i:

- $35y_1 \equiv 1 \pmod 3$: since $35 \equiv 2 \pmod 3$, we need $2y_1 \equiv 1 \pmod 3$, giving $y_1 = 2$.
- $21y_2 \equiv 1 \pmod 5$: since $21 \equiv 1 \pmod 5$, we get $y_2 = 1$.
- $15y_3 \equiv 1 \pmod 7$: since $15 \equiv 1 \pmod 7$, we get $y_3 = 1$.

Therefore

$$x_0 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 30 = 233 \equiv 23 \pmod{105}.$$

5.3 Algebraic Formulation

The CRT admits a clean algebraic reformulation as a ring isomorphism.

Theorem 5.5 (CRT — algebraic form)**.** *Let m, n be positive integers with $\gcd(m, n) = 1$. The map*

$$\varphi \colon \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \qquad x \bmod mn \longmapsto (x \bmod m,\ x \bmod n) \tag{5.3}$$

is a ring isomorphism.

Proof. Well-definedness and homomorphism. If $x \equiv x' \pmod{mn}$, then $x \equiv x' \pmod m$ and $x \equiv x' \pmod n$, so φ is well-defined. It clearly preserves addition and multiplication (since reduction modulo m or n is a ring homomorphism) and sends 1 to $(1, 1)$.

Injectivity. If $\varphi(x) = (0, 0)$, then $m \mid x$ and $n \mid x$. Since $\gcd(m, n) = 1$, we get $mn \mid x$, so $x \equiv 0 \pmod{mn}$.

Surjectivity. Both sides are finite sets of the same cardinality $mn = m \cdot n$, so injectivity implies surjectivity. Alternatively, surjectivity is exactly the existence statement of Theorem 5.3. □

Corollary 5.6 (Euler's totient is multiplicative)**.** *If $\gcd(m, n) = 1$, then $\varphi(mn) = \varphi(m)\,\varphi(n)$, where φ denotes Euler's totient function.*

Proof. The ring isomorphism $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ restricts to a group isomorphism on the unit groups: $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Taking cardinalities gives $\varphi(mn) = \varphi(m)\,\varphi(n)$. □

Corollary 5.7 (General CRT)**.** *If $m_1, \ldots, m_k$ are pairwise coprime, then*

$$\mathbb{Z}/M\mathbb{Z} \ \cong\ \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

as rings, where $M = m_1 m_2 \cdots m_k$.

Proof. Apply Theorem 5.5 iteratively. At each step, the remaining product is coprime to the factor being split off, since pairwise coprimality is preserved. □

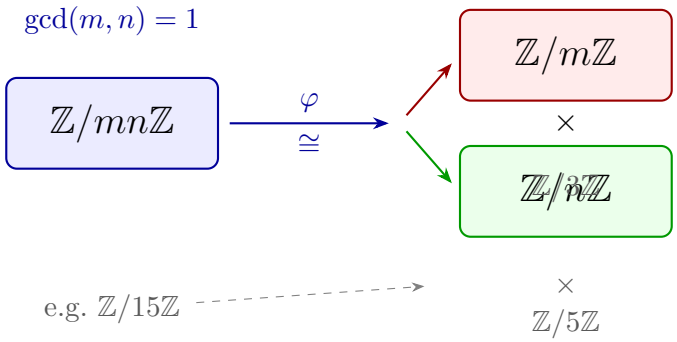


Figure 5.1: The CRT isomorphism $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for coprime m, n.

5.4 Applications

5.4.1 Solving simultaneous congruences

The constructive proof of the CRT yields an explicit algorithm.

Example 5.8 (A four-modulus system)**.** Solve the system

$$x \equiv 1 \pmod 2, \quad x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 4 \pmod 7.$$

Here $M = 210$, and

$$\begin{aligned}
&M_1 = 105,\ y_1 : 105y_1 \equiv 1 \pmod 2 \implies y_1 = 1,\\
&M_2 = 70,\ y_2 : 70y_2 \equiv 1 \pmod 3 \implies y_2 = 1 \ (\text{since } 70 \equiv 1),\\
&M_3 = 42,\ y_3 : 42y_3 \equiv 1 \pmod 5 \implies y_3 = 3 \ (\text{since } 42 \equiv 2,\ 2 \cdot 3 = 6 \equiv 1),\\
&M_4 = 30,\ y_4 : 30y_4 \equiv 1 \pmod 7 \implies y_4 = 4 \ (\text{since } 30 \equiv 2,\ 2 \cdot 4 = 8 \equiv 1).
\end{aligned}$$

Then

$$x_0 = 1{\cdot}105{\cdot}1 + 2{\cdot}70{\cdot}1 + 3{\cdot}42{\cdot}3 + 4{\cdot}30{\cdot}4 = 105 + 140 + 378 + 480 = 1103 \equiv 53 \pmod{210}.$$

One checks: $53 = 26 \cdot 2 + 1$, $53 = 17 \cdot 3 + 2$, $53 = 10 \cdot 5 + 3$, $53 = 7 \cdot 7 + 4$.

5.4.2 Calendar computations

Many calendar systems involve independent cycles of different periods. For instance, the *Chinese sexagenary cycle* combines a cycle of 10 Heavenly Stems with a cycle of 12 Earthly Branches. Since $\gcd(10, 12) = 2 \neq 1$, the CRT does not directly apply to the full pair—but the reduced coprime pair $(5, 12)$ governs the 60-year cycle, since $\operatorname{lcm}(10, 12) = 60 = 5 \cdot 12$.

Example 5.9 (Day of the week)**.** Suppose an event recurs every 7 days (weekly) and another every 4 days. Since $\gcd(7,4)=1$, by the CRT the combined pattern repeats every 28 days. If the weekly event falls on day 3 and the 4-day event on day 1, we solve

$$x \equiv 3 \pmod 7, \qquad x \equiv 1 \pmod 4.$$

Using $M_1 = 4$, $y_1 = 2$ (since $4 \cdot 2 = 8 \equiv 1 \pmod 7$) and $M_2 = 7$, $y_2 = 3$ (since $7 \cdot 3 = 21 \equiv 1 \pmod 4$):

$$x \equiv 3 \cdot 4 \cdot 2 + 1 \cdot 7 \cdot 3 = 24 + 21 = 45 \equiv 17 \pmod{28}.$$

5.4.3 Error detection and secret sharing

The CRT underlies several practical schemes:

(i) **Redundant residue number systems.** Represent an integer by its residues modulo several coprime moduli. Adding extra moduli provides error-detection capability, since any single residue error yields a tuple outside the image of the CRT isomorphism.

(ii) **Shamir-type secret sharing.** A variant due to Asmuth and Bloom uses the CRT: choose pairwise coprime moduli $m_1 < m_2 < \cdots < m_n$ and a threshold k. The secret S is encoded modulo m_0 and shared as $S_i \equiv S \pmod{m_i}$. Any k shares suffice to reconstruct S via the CRT, while fewer than k leave S undetermined.

5.4.4 RSA speed-up via CRT

In the RSA cryptosystem, decryption computes $c^d \bmod n$ where $n = pq$. By the CRT isomorphism $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$, we may instead compute

$$m_p \equiv c^{d \bmod (p-1)} \pmod p, \qquad m_q \equiv c^{d \bmod (q-1)} \pmod q,$$

and then recombine using Garner's formula:

$$m \equiv m_q + q\Big[q^{-1}(m_p - m_q) \bmod p\Big] \pmod n.$$

Since modular exponentiation is roughly cubic in the bit-length of the modulus, working with p and q separately yields an approximate $4\times$ speed-up.

Remark 5.10. Garner's formula is preferred over the symmetric CRT formula in practice because it avoids reduction modulo the full product n.

5.5 Exercises

Exercise 5.1. Solve the system $x \equiv 3 \pmod 7$, $x \equiv 5 \pmod{11}$, $x \equiv 8 \pmod{13}$.

Exercise 5.2. Show that $x \equiv 3 \pmod 6$, $x \equiv 5 \pmod{10}$ has a solution, and find it. What is the modulus of the general solution? (Hint: $\gcd(6,10) = 2$ and $2 \mid (5-3)$.)

Exercise 5.3. Use the CRT to show that $(\mathbb{Z}/n\mathbb{Z})^\times$ is not cyclic when n has at least two distinct odd prime factors. (Hint: if $n = p_1^{a_1}\cdots p_k^{a_k}$, the group splits as a direct product, each factor of even order.)

Exercise 5.4. Let p, q be distinct primes. Show that the number of solutions of $x^2 \equiv 1 \pmod{pq}$ is exactly 4.

Exercise 5.5. Find the smallest positive integer satisfying

$$x \equiv 1 \pmod 2, \quad x \equiv 1 \pmod 3, \quad x \equiv 1 \pmod 5, \quad x \equiv 0 \pmod 7.$$

Exercise 5.6. Using the CRT and the formula $\varphi(p^a) = p^{a-1}(p-1)$, derive the general formula

$$\varphi(n) = n \prod_{p \mid n} \Big(1 - \frac{1}{p}\Big).$$

Exercise 5.7. An element e of a ring R is called *idempotent* if $e^2 = e$. Show that $\mathbb{Z}/n\mathbb{Z}$ contains exactly 2^k idempotents, where k is the number of distinct prime divisors of n. (Hint: use the CRT and note that the only idempotents in $\mathbb{Z}/p^a\mathbb{Z}$ are 0 and 1.)

Exercise 5.8 (RSA speed-up)**.** Let $p = 61$, $q = 53$, $n = 3233$, $e = 17$, $d = 2753$. Compute $c^d \bmod n$ for $c = 2790$ using the CRT method described in Section 5.4.4. Verify that you recover $m = 65$.

Chapter Summary

- The **Chinese Remainder Theorem** states that a system of congruences with pairwise coprime moduli $m_1, \dots, m_k$ always has a unique solution modulo $M = m_1 \cdots m_k$.
- The explicit solution is $x \equiv \sum_{i=1}^{k} a_i M_i y_i \pmod M$, where $M_i = M/m_i$ and $M_i y_i \equiv 1 \pmod{m_i}$.
- Algebraically, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ when $\gcd(m,n) = 1$, which implies the multiplicativity of Euler's totient function.
- Applications range from ancient calendar problems to modern cryptography (RSA) and secret-sharing schemes.

Chapter 6

Quadratic Residues and Quadratic Reciprocity

Historical Introduction

The study of quadratic residues is one of the crown jewels of elementary number theory. **Euler** investigated which primes could be represented by binary quadratic forms such as x^2+ny^2, leading him to discover (around 1783) the law of quadratic reciprocity empirically, though he could not prove it.

Legendre (1785) stated the law precisely and introduced the symbol $\left(\frac{a}{p}\right)$ that bears his name, but his proof contained a gap (it relied on Dirichlet's theorem on primes in arithmetic progressions, which would not be proven for another fifty years).

It was **Gauss** who, at the age of eighteen, gave the first complete proof in 1796. He called it the *theorema aureum* — the golden theorem — and over the course of his life produced no fewer than **eight** distinct proofs, a testament to the theorem's depth and centrality. Today, over 240 proofs are known.

6.1 Quadratic Residues

Definition 6.1 (Quadratic residue)**.** Let p be an odd prime and a an integer with $p \nmid a$. We say that a is a *quadratic residue modulo* p (abbreviated QR) if the congruence $x^2 \equiv a \pmod{p}$ has a solution. Otherwise, a is a *quadratic non-residue* (abbreviated QNR).

Proposition 6.2 (Counting quadratic residues)**.** *Let p be an odd prime. Among the residues $1, 2, \ldots, p-1$, exactly $\frac{p-1}{2}$ are quadratic residues and $\frac{p-1}{2}$ are quadratic non-residues.*

Proof. Consider the squaring map $\sigma\colon (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ defined by $\sigma(x) = x^2$. We claim that for each QR a, the equation $x^2 \equiv a \pmod{p}$ has exactly two solutions $\pm x_0$.

Indeed, if $x_0^2 \equiv a$ then $(-x_0)^2 \equiv a$, and these are distinct since p is odd ($x_0 \not\equiv -x_0 \pmod{p}$ because $p \nmid 2x_0$). Conversely, if $x^2 \equiv x_0^2$ then $p \mid (x - x_0)(x + x_0)$, so $x \equiv \pm x_0$.

Thus σ is a 2-to-1 map from $(\mathbb{Z}/p\mathbb{Z})^\times$ (of order $p-1$) onto the set of quadratic residues, which therefore has cardinality $\frac{p-1}{2}$. □

Example 6.3 (Quadratic residues modulo 13)**.** We compute $x^2 \bmod 13$ for $x = 1, \dots, 6$ (the other squares are the same by $(-x)^2 = x^2$):

$$1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 3, \quad 5^2 = 12, \quad 6^2 = 10.$$

So the QRs mod 13 are $\{1, 3, 4, 9, 10, 12\}$ and the QNRs are $\{2, 5, 6, 7, 8, 11\}$.

6.2 Euler's Criterion

Theorem 6.4 (Euler's criterion)**.** *Let p be an odd prime and a an integer with $p \nmid a$. Then*

$$a^{(p-1)/2} \equiv \begin{cases} 1 \pmod{p} & \text{if } a \text{ is a QR mod } p, \\ -1 \pmod{p} & \text{if } a \text{ is a QNR mod } p. \end{cases} \tag{6.1}$$

Proof. By Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$, so

$$\left(a^{(p-1)/2}\right)^2 \equiv 1 \pmod{p}.$$

Since $\mathbb{Z}/p\mathbb{Z}$ is a field, the polynomial $t^2 - 1$ has at most two roots, namely $t \equiv \pm 1$. Thus $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

Case 1: a is a QR. Write $a \equiv x_0^2$. Then

$$a^{(p-1)/2} \equiv x_0^{p-1} \equiv 1 \pmod{p}$$

by Fermat's little theorem.

Case 2: a is a QNR. Since $a^{(p-1)/2} \equiv \pm 1$ and Case 1 accounts for all $(p-1)/2$ quadratic residues as roots of $t^{(p-1)/2} - 1 \equiv 0$, and this polynomial has at most $(p-1)/2$ roots, the remaining $(p-1)/2$ elements (the QNRs) must all satisfy $a^{(p-1)/2} \equiv -1$. □

6.3 The Legendre Symbol

Definition 6.5 (Legendre symbol)**.** For an odd prime p and an integer a, the *Legendre symbol* is

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a QR mod } p, \\ -1 & \text{if } a \text{ is a QNR mod } p. \end{cases}$$

By Euler's criterion, we have the useful identity

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}. \tag{6.2}$$

Proposition 6.6 (Properties of the Legendre symbol)**.** *Let p be an odd prime and $a, b \in \mathbb{Z}$. Then:*

(i) *If* $a \equiv b \pmod p$, *then* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. (*Complete multiplicativity.*)

(iii) $\left(\frac{a^2}{p}\right) = 1$ *whenever* $p \nmid a$.

(iv) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. *In particular,* -1 *is a QR mod* p *if and only if* $p \equiv 1 \pmod 4$.

Proof. (i) is immediate from the definition. For (ii), use Euler's criterion:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p.$$

Since both sides are ± 1 or 0 and $p \geq 3$, congruence modulo p implies equality. Part (iii) follows from (ii), and (iv) is Euler's criterion applied to $a = -1$. □

Example 6.7. Is -3 a quadratic residue modulo 23? We compute

$$\left(\frac{-3}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{3}{23}\right).$$

Since $23 \equiv 3 \pmod 4$, we have $\left(\frac{-1}{23}\right) = (-1)^{11} = -1$. For $\left(\frac{3}{23}\right)$, we use Euler's criterion: $3^{11} \bmod 23$. Compute: $3^2 = 9$, $3^4 = 81 \equiv 12$, $3^8 \equiv 144 \equiv 6$, so $3^{11} = 3^8 \cdot 3^2 \cdot 3 \equiv 6 \cdot 9 \cdot 3 = 162 \equiv 162 - 7 \cdot 23 = 1$. Thus $\left(\frac{3}{23}\right) = 1$ and $\left(\frac{-3}{23}\right) = (-1)(1) = -1$; hence -3 is a QNR mod 23.

6.4 Gauss's Lemma

Theorem 6.8 (Gauss's lemma)**.** *Let* p *be an odd prime and* a *an integer with* $p \nmid a$. *Consider the set*

$$S = \left\{a \cdot 1,\ a \cdot 2,\ \ldots,\ a \cdot \tfrac{p-1}{2}\right\}$$

reduced modulo p *into the range* $\{1, 2, \ldots, p-1\}$. *Let* ν *be the number of elements of this reduced set that are greater than* $\frac{p}{2}$ (*i.e., lie in* $\left\{\frac{p+1}{2}, \ldots, p-1\right\}$). *Then*

$$\left(\frac{a}{p}\right) = (-1)^{\nu}. \tag{6.3}$$

Proof. For $j = 1, 2, \ldots, \frac{p-1}{2}$, let r_j be the least positive residue of aj modulo p, so $r_j \in \{1, \ldots, p-1\}$. Define

$$\varepsilon_j = \begin{cases} +1 & \text{if } r_j \leq \frac{p-1}{2}, \\ -1 & \text{if } r_j > \frac{p-1}{2}, \end{cases} \qquad \text{and} \qquad s_j = \begin{cases} r_j & \text{if } r_j \leq \frac{p-1}{2}, \\ p - r_j & \text{if } r_j > \frac{p-1}{2}. \end{cases}$$

Then $r_j \equiv \varepsilon_j s_j \pmod p$ (since if $r_j > \frac{p-1}{2}$, then $p - r_j \equiv -r_j \pmod p$), and $s_j \in \left\{1, \ldots, \frac{p-1}{2}\right\}$.

Claim: The values $s_1, s_2, \ldots, s_{(p-1)/2}$ are a permutation of $\left\{1, 2, \ldots, \frac{p-1}{2}\right\}$.

Proof of claim. It suffices to show they are all distinct. Suppose $s_j = s_k$ for $j \neq k$. Then $r_j \equiv \pm r_k \pmod{p}$. If $r_j \equiv r_k$, then $aj \equiv ak$, so $j \equiv k \pmod{p}$, impossible since $1 \leq j, k \leq \frac{p-1}{2} < p$. If $r_j \equiv -r_k$, then $a(j+k) \equiv 0 \pmod{p}$, so $p \mid (j+k)$, but $2 \leq j+k \leq p-1$, contradiction. This proves the claim.

Now multiply all the congruences $aj \equiv \varepsilon_j\, s_j \pmod{p}$ for $j = 1, \ldots, \frac{p-1}{2}$:

$$a^{(p-1)/2} \cdot \prod_{j=1}^{(p-1)/2} j \;\equiv\; \left(\prod_{j=1}^{(p-1)/2} \varepsilon_j\right) \cdot \prod_{j=1}^{(p-1)/2} s_j \pmod{p}.$$

Since $\{s_j\}$ is a permutation of $\left\{1, \ldots, \frac{p-1}{2}\right\}$, both products $\prod j$ and $\prod s_j$ equal $\left(\frac{p-1}{2}\right)!$, which is coprime to p. Cancelling gives

$$a^{(p-1)/2} \equiv \prod_{j=1}^{(p-1)/2} \varepsilon_j = (-1)^{\nu} \pmod{p}.$$

By Euler's criterion, $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$, so $\left(\frac{a}{p}\right) = (-1)^{\nu}$. □

Example 6.9. Let $p = 7$, $a = 2$. The set $S = \{2, 4, 6\}$ reduced modulo 7 is $\{2, 4, 6\}$. The elements greater than $\frac{7}{2} = 3.5$ are 4 and 6, so $\nu = 2$. Hence $\left(\frac{2}{7}\right) = (-1)^2 = 1$. Indeed, $3^2 = 9 \equiv 2 \pmod{7}$.

6.5 The First and Second Supplements

Using Gauss's lemma, we can determine $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$.

Theorem 6.10 (First supplement)**.** *For any odd prime p,*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases} \tag{6.4}$$

Proof. This follows immediately from Euler's criterion: $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$. Since both sides are ± 1 and $p \geq 3$, congruence implies equality. □

Theorem 6.11 (Second supplement)**.** *For any odd prime p,*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases} \tag{6.5}$$

Proof. We apply Gauss's lemma with $a = 2$. The set is $S = \{2, 4, 6, \ldots, p-1\}$, and we need to count how many of the elements $2j$ (for $j = 1, \ldots, \frac{p-1}{2}$) satisfy $2j > \frac{p}{2}$, i.e., $j > \frac{p}{4}$.

The number of such j is

$$\nu = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

A case-by-case check on p mod 8 shows:

$p \bmod 8$	1	3	5	7
$\frac{p-1}{2}$	$\frac{p-1}{2}$	$\frac{p-1}{2}$	$\frac{p-1}{2}$	$\frac{p-1}{2}$
$\lfloor p/4 \rfloor$	$\frac{p-1}{4}$	$\frac{p-3}{4}$	$\frac{p-1}{4}$	$\frac{p-3}{4}$
ν	$\frac{p-1}{4}$	$\frac{p+1}{4}$	$\frac{p-1}{4}$	$\frac{p+1}{4}$
$\nu \bmod 2$	0	1	1	0

Thus $(-1)^\nu = 1$ when $p \equiv \pm 1 \pmod 8$ and $(-1)^\nu = -1$ when $p \equiv \pm 3 \pmod 8$.

It remains to verify that $(-1)^\nu = (-1)^{(p^2-1)/8}$. Observe that $p^2 - 1 = (p-1)(p+1)$. Writing $p = 8k + r$ for $r \in \{1, 3, 5, 7\}$:

$$\begin{aligned}
p \equiv 1 \pmod 8&: \tfrac{p^2-1}{8} = \tfrac{(8k)(8k+2)}{8} = k(4k+1), \text{ even;}\\
p \equiv 3 \pmod 8&: \tfrac{p^2-1}{8} = \tfrac{(8k+2)(8k+4)}{8} = (4k+1)(2k+1), \text{ odd;}\\
p \equiv 5 \pmod 8&: \tfrac{p^2-1}{8} = \tfrac{(8k+4)(8k+6)}{8} = (2k+1)(4k+3), \text{ odd;}\\
p \equiv 7 \pmod 8&: \tfrac{p^2-1}{8} = \tfrac{(8k+6)(8k+8)}{8} = (4k+3)(k+1), \text{ even.}
\end{aligned}$$

This matches the table above, completing the proof. □

6.6 Quadratic Reciprocity

Theorem 6.12 (Law of quadratic reciprocity)**.** *Let p and q be distinct odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{6.6}$$

Equivalently:

(a) *If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$ (i.e., not both $\equiv 3 \pmod 4$), then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.*

(b) *If $p \equiv q \equiv 3 \pmod 4$, then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.*

We present Eisenstein's elegant proof via lattice-point counting.

Proof. Consider the rectangle $R = (0, p) \times (0, q)$ in $\mathbb{R}^2$ and the line ℓ: $qx = py$ passing through the origin and the corner (p, q).

Step 1: Relate the Legendre symbols to lattice-point counts.

By Gauss's lemma (Theorem 6.8), $\left(\frac{q}{p}\right) = (-1)^\mu$ where μ is the number of $j \in \{1, \dots, \frac{p-1}{2}\}$ such that the least positive residue of jq modulo p exceeds $\frac{p}{2}$. One can reformulate this count as follows. For each integer j with $1 \le j \le \frac{p-1}{2}$, the residue of jq modulo p exceeds $\frac{p}{2}$ if and only if $\left\lfloor \frac{jq}{p} \right\rfloor$ and jq have different parities. A careful parity analysis (see Lemma 6.13 below) shows that

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{(p-1)/2} \lfloor jq/p \rfloor}. \tag{6.7}$$

Step 2: Count lattice points.

The quantity $\left\lfloor \frac{jq}{p} \right\rfloor$ equals the number of integers k with $1 \le k \le \frac{jq}{p}$, i.e., the number of lattice points (j,k) with $1 \le k < \frac{jq}{p}$ (strict inequality since $p \nmid jq$ for $1 \le j \le \frac{p-1}{2}$). Thus

$$\sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor = \#\Big\{(j,k) \in \mathbb{Z}^2 : 1 \le j \le \tfrac{p-1}{2},\ 1 \le k,\ k < \tfrac{jq}{p}\Big\}.$$

This is the number of lattice points in the interior of the triangle T_1 below the line ℓ with $1 \le j \le \frac{p-1}{2}$ and $k \ge 1$.

Similarly,

$$\sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor = \#\Big\{(j,k) \in \mathbb{Z}^2 : 1 \le k \le \tfrac{q-1}{2},\ 1 \le j,\ j < \tfrac{kp}{q}\Big\},$$

which counts lattice points in the triangle T_2 above the line ℓ with $1 \le k \le \frac{q-1}{2}$ and $j \ge 1$.

Step 3: No lattice points on the line.

Since p and q are distinct primes, the equation $qj = pk$ with $1 \le j \le \frac{p-1}{2}$ and $1 \le k \le \frac{q-1}{2}$ would require $p \mid j$ and $q \mid k$, which is impossible in these ranges. So no lattice point in the rectangle $[1, \frac{p-1}{2}] \times [1, \frac{q-1}{2}]$ lies on ℓ.

Step 4: Combine.

Every lattice point (j,k) with $1 \le j \le \frac{p-1}{2}$, $1 \le k \le \frac{q-1}{2}$ lies either in T_1 (below ℓ) or T_2 (above ℓ). Therefore

$$\sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

By (6.7) and its analogue for $\left(\frac{p}{q}\right)$:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum \lfloor jq/p \rfloor + \sum \lfloor kp/q \rfloor} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

□

We now state and prove the key lemma used in Step 1.

Lemma 6.13 (Eisenstein's reformulation of Gauss's lemma)**.** *Let p be an odd prime and a an integer with $p \nmid a$ and a odd. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{j=1}^{(p-1)/2} \lfloor ja/p \rfloor}.$$

Proof. With notation as in the proof of Gauss's lemma (Theorem 6.8), we have $aj = \left\lfloor \frac{aj}{p} \right\rfloor \cdot p + r_j$, where r_j is the least positive residue. Recall that $s_j = r_j$ when $r_j \le \frac{p-1}{2}$ and $s_j = p - r_j$ otherwise, and $\{s_j\}$ is a permutation of $\{1, \dots, \frac{p-1}{2}\}$.

Summing $aj = \left\lfloor \frac{aj}{p} \right\rfloor p + r_j$ over $j = 1, \dots, \frac{p-1}{2}$:

$$a \sum_{j=1}^{(p-1)/2} j = p \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{aj}{p} \right\rfloor + \sum_{j=1}^{(p-1)/2} r_j.$$

Also, $r_j = s_j$ when $\varepsilon_j = +1$ and $r_j = p - s_j$ when $\varepsilon_j = -1$, so $\sum r_j = \sum s_j + \nu p - 2\sum_{j:\varepsilon_j=-1} s_j$. But actually, more simply: $r_j + s_j = 0$ or $r_j + s_j = p$ depending on whether $\varepsilon_j = +1$ or -1. So $r_j = s_j + \frac{1-\varepsilon_j}{2}\cdot(p - 2s_j)$.

It is cleaner to note:

$$\sum r_j = \sum_{\varepsilon_j=1} s_j + \sum_{\varepsilon_j=-1} (p - s_j) = \sum s_j + \nu p - 2\sum_{\varepsilon_j=-1} s_j.$$

Since $\{s_j\}$ is a permutation of $\{1, \dots, \frac{p-1}{2}\}$, we have $\sum s_j = \sum_{j=1}^{(p-1)/2} j$. Substituting:

$$a\sum j = p\sum \left\lfloor \frac{aj}{p} \right\rfloor + \sum j + \nu p - 2\sum_{\varepsilon_j=-1} s_j.$$

Reducing modulo 2 (note p is odd, so $p \equiv 1 \pmod 2$):

$$(a-1)\sum j \equiv \sum \left\lfloor \frac{aj}{p} \right\rfloor + \nu \pmod 2.$$

Since a is odd, $a - 1$ is even, so the left side is $\equiv 0 \pmod 2$. Therefore $\nu \equiv \sum \left\lfloor \frac{aj}{p} \right\rfloor \pmod 2$, and

$$\left(\frac{a}{p}\right) = (-1)^{\nu} = (-1)^{\sum \lfloor aj/p \rfloor}. \qquad \square$$

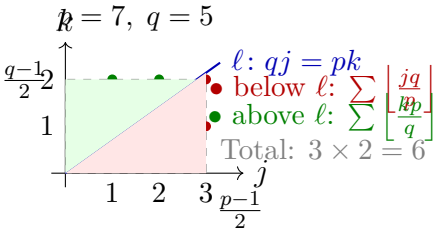


Figure 6.1: Eisenstein's lattice-point proof for $p = 7$, $q = 5$. The $3 + 3 = 6 = \frac{6}{2}\cdot\frac{4}{2}$ lattice points split between the two triangles below and above the line ℓ.

Example 6.14 (Applying quadratic reciprocity)**.** Is 5 a quadratic residue modulo 41? Since $41 \equiv 1 \pmod 4$, quadratic reciprocity gives

$$\left(\frac{5}{41}\right) = \left(\frac{41}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

So 5 is a QR mod 41. Indeed, $28^2 = 784 = 19\cdot 41 + 5$, confirming $28^2 \equiv 5 \pmod{41}$.

Example 6.15 (A more involved computation)**.** Evaluate $\left(\frac{70}{571}\right)$. We factor and use multiplicativity:

$$\left(\frac{70}{571}\right) = \left(\frac{2}{571}\right)\left(\frac{5}{571}\right)\left(\frac{7}{571}\right).$$

Since $571 \equiv 3 \pmod 8$, the second supplement gives $\left(\frac{2}{571}\right) = -1$.

For $\left(\frac{5}{571}\right)$: since $571 \equiv 3 \pmod 4$ and $5 \equiv 1 \pmod 4$ (not both $\equiv 3$), reciprocity gives $\left(\frac{5}{571}\right) = \left(\frac{571}{5}\right) = \left(\frac{1}{5}\right) = 1$.
For $\left(\frac{7}{571}\right)$: both $7 \equiv 3$ and $571 \equiv 3 \pmod 4$, so $\left(\frac{7}{571}\right) = -\left(\frac{571}{7}\right) = -\left(\frac{4}{7}\right) = -(1) = -1$, since $571 = 81 \cdot 7 + 4$ and $\left(\frac{4}{7}\right) = \left(\frac{2^2}{7}\right) = 1$.
Therefore $\left(\frac{70}{571}\right) = (-1)(1)(-1) = 1$.

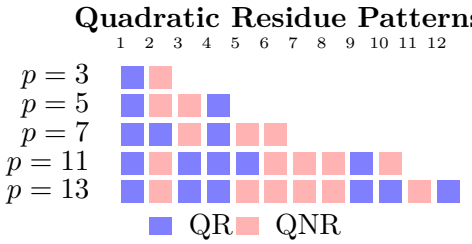


Figure 6.2: Quadratic residue patterns for small primes: blue cells are QRs, red cells are QNRs. Note the symmetric/antisymmetric patterns governed by $\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right)$ when $p \equiv 1 \pmod 4$.

6.7 The Jacobi Symbol

The Legendre symbol is defined only for prime moduli. The Jacobi symbol extends it to arbitrary odd moduli, which greatly facilitates computations.

Definition 6.16 (Jacobi symbol)**.** Let $n > 1$ be an odd integer with prime factorisation $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. For any integer a, the *Jacobi symbol* is

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_r}\right)^{e_r}.$$

Remark 6.17. The Jacobi symbol $\left(\frac{a}{n}\right) = 1$ does *not* imply that a is a quadratic residue modulo n. For instance, $\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)^2 = (-1)^2 = 1$, but $x^2 \equiv 2 \pmod 9$ has no solution (checking $x = 0, 1, \ldots, 8$). However, $\left(\frac{a}{n}\right) = -1$ *does* imply that a is a QNR modulo n.

Proposition 6.18 (Properties of the Jacobi symbol)**.** *Let m, n be odd positive integers and $a, b \in \mathbb{Z}$. Then:*

(i) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

(ii) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

(iii) *If* $a \equiv b \pmod n$, *then* $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

(iv) $\left(\frac{1}{n}\right) = 1$ *and* $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

(v) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

Proof. Properties (i)–(iii) follow directly from the definition and the corresponding properties of the Legendre symbol.

For (iv), $\left(\frac{-1}{n}\right) = \prod \left(\frac{-1}{p_i}\right)^{e_i} = \prod (-1)^{e_i(p_i-1)/2} = (-1)^{\sum e_i(p_i-1)/2}$. One verifies that $\sum e_i(p_i-1)/2 \equiv (n-1)/2 \pmod 2$ by induction on the number of prime factors, using the identity: if $n = ab$ with a, b odd, then $\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2$.

Property (v) follows similarly from the identity $\frac{(ab)^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod 2$ for odd a, b. □

Theorem 6.19 (Reciprocity for the Jacobi symbol)**.** *Let m, n be odd positive integers with $\gcd(m, n) = 1$. Then*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}. \tag{6.8}$$

Proof. Write $m = p_1 \cdots p_s$ and $n = q_1 \cdots q_t$ (with repetition according to multiplicity). Then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i,j}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i,j}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}} = (-1)^{\sum_{i,j}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.$$

Now $\sum_{i,j}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2} = \left(\sum_i \frac{p_i-1}{2}\right)\left(\sum_j \frac{q_j-1}{2}\right)$. By the same parity identity used in Proposition 6.18(iv), $\sum_i \frac{p_i-1}{2} \equiv \frac{m-1}{2} \pmod 2$ and likewise for n. □

Example 6.20 (Efficient computation with the Jacobi symbol)**.** Evaluate $\left(\frac{1001}{9907}\right)$, where 9907 is prime (so the Jacobi symbol equals the Legendre symbol and determines quadratic residuosity).

$$\left(\frac{1001}{9907}\right) = \left(\frac{7}{9907}\right)\left(\frac{11}{9907}\right)\left(\frac{13}{9907}\right).$$

Since $9907 \equiv 3 \pmod 4$, $7 \equiv 3$, $11 \equiv 3$, $13 \equiv 1$:

$$\left(\frac{7}{9907}\right) = -\left(\frac{9907}{7}\right) = -\left(\frac{3}{7}\right),$$
$$\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) \cdot (-1)^{\frac{2}{2}\cdot\frac{6}{2}} = \left(\frac{7}{3}\right) \cdot (-1)^3 = -\left(\frac{1}{3}\right) = -1,$$
$$\text{so } \left(\frac{7}{9907}\right) = -(-1) = 1.$$

$$\left(\frac{11}{9907}\right) = -\left(\frac{9907}{11}\right) = -\left(\frac{9907 \bmod 11}{11}\right) = -\left(\frac{7}{11}\right),$$
$$\left(\frac{7}{11}\right) = \left(\frac{11}{7}\right) \cdot (-1)^{\frac{6}{2}\cdot\frac{10}{2}} = \left(\frac{11}{7}\right) \cdot (-1)^{15} = -\left(\frac{4}{7}\right) = -(1) = -1,$$
$$\text{so } \left(\frac{11}{9907}\right) = -(-1) = 1.$$

$$\left(\frac{13}{9907}\right) = \left(\frac{9907}{13}\right) = \left(\frac{9907 \bmod 13}{13}\right) = \left(\frac{3}{13}\right),$$
$$\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) \cdot (-1)^{\frac{2}{2}\cdot\frac{12}{2}} = \left(\frac{1}{3}\right) \cdot (-1)^6 = 1.$$

Therefore $\left(\frac{1001}{9907}\right) = 1 \cdot 1 \cdot 1 = 1$, so 1001 is a quadratic residue modulo 9907.

Remark 6.21 (Computational complexity). The Jacobi symbol $\left(\frac{a}{n}\right)$ can be computed in $O(\log^2 n)$ bit operations using a procedure analogous to the Euclidean algorithm: repeatedly apply reciprocity and reduce modulo the smaller argument. This does *not* require factoring n, which is why the Jacobi symbol is useful in primality testing (e.g., the Solovay–Strassen test).

6.8 Exercises

Exercise 6.1. List all quadratic residues modulo 17 and modulo 19.

Exercise 6.2. Use Euler's criterion to determine whether 3 is a quadratic residue modulo 31.

Exercise 6.3. Let p be an odd prime. Show that the product of all quadratic residues modulo p is congruent to $(-1)^{(p+1)/2} \pmod p$. (Hint: pair each QR a with its "complement" a^{-1}.)

Exercise 6.4. Prove that for an odd prime p,

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Exercise 6.5. Using quadratic reciprocity and the supplements, determine exactly which primes p satisfy $\left(\frac{-3}{p}\right) = 1$. Show that -3 is a QR mod p if and only if $p = 3$ or $p \equiv 1 \pmod 3$.

Exercise 6.6. Apply Gauss's lemma directly (without Euler's criterion) to compute $\left(\frac{3}{11}\right)$ and $\left(\frac{5}{13}\right)$.

Exercise 6.7. Give an alternative derivation of the second supplement $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ using Euler's criterion and the identity

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} \pmod{p}$$

by working in a suitable extension (e.g., $\mathbb{Z}[i]$ or $\mathbb{Z}[\sqrt{2}]$).

Exercise 6.8. Compute $\left(\frac{295}{1009}\right)$ using only the properties of the Jacobi symbol (reciprocity, supplements, multiplicativity). Is 295 a QR mod 1009? (Note: 1009 is prime.)

Exercise 6.9. Show that for any prime $p > 5$, there exist consecutive integers $a, a+1$ that are both quadratic residues modulo p. (Hint: consider x^2 and $(x+1)^2$ and count.)

Exercise 6.10. Give an example showing that $\left(\frac{a}{n}\right) = 1$ does not imply a is a QR mod n when n is not prime. Prove that if $n = pq$ with $p \neq q$ odd primes, then a is a QR mod n if and only if $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$.

Exercise 6.11 (Primes of the form x^2+5y^2)**.** Show that if an odd prime p divides x^2+5y^2 with $\gcd(p, y) = 1$, then $\left(\frac{-5}{p}\right) = 1$. Use reciprocity to show this holds if and only if $p \equiv 1, 3, 7, 9 \pmod{20}$.

Chapter Summary

- An integer a with $p \nmid a$ is a **quadratic residue** mod p if $x^2 \equiv a \pmod{p}$ is solvable. Exactly half of $\{1, \ldots, p-1\}$ are QRs.
- **Euler's criterion:** $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.
- The **Legendre symbol** $\left(\frac{a}{p}\right)$ encodes quadratic residuosity and is completely multiplicative.
- **Gauss's lemma** expresses $\left(\frac{a}{p}\right)$ as $(-1)^\nu$, where ν counts how many of $a, 2a, \ldots, \frac{p-1}{2}a$ have residues exceeding $\frac{p}{2}$.
- The **law of quadratic reciprocity**: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ for distinct odd primes p, q.
- **Supplements:** $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ and $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
- The **Jacobi symbol** extends the Legendre symbol to composite odd moduli, preserving multiplicativity and reciprocity, enabling efficient computation without factoring.

Chapter 7

Representations by Quadratic Forms

> *"Numerorum primorum, qui sunt aggregata duorum quadratorum, insignes proprietates."* — Pierre de Fermat, 1640

One of the oldest and most beautiful questions in number theory asks: which integers can be expressed as sums of squares? Fermat claimed in 1640 that every prime $p \equiv 1 \pmod 4$ is a sum of two squares, but his proof was never published. The first complete proofs were given by Euler (1749) after years of effort. In this chapter we develop the theory systematically, beginning with binary quadratic forms, proving Fermat's two-square theorem completely, characterising all integers representable as sums of two squares, and stating Lagrange's four-square theorem.

7.1 Binary Quadratic Forms

Definition 7.1 (Binary quadratic form)**.** A **binary quadratic form** is a polynomial

$$f(x, y) = ax^2 + bxy + cy^2, \qquad a, b, c \in \mathbb{Z}.$$

The form is called **positive definite** if $f(x, y) > 0$ for all $(x, y) \neq (0, 0)$. The **discriminant** of f is

$$D = b^2 - 4ac.$$

Remark 7.2. A binary quadratic form $ax^2 + bxy + cy^2$ with $a > 0$ is positive definite if and only if $D < 0$. Indeed, we may complete the square:

$$f(x, y) = a\left(x + \frac{b}{2a}\, y\right)^2 + \frac{4ac - b^2}{4a}\, y^2,$$

which is positive for all $(x, y) \neq (0, 0)$ precisely when $a > 0$ and $4ac - b^2 > 0$.

Definition 7.3 (Representation by a form)**.** An integer n is **represented** by the form f if there exist $x_0, y_0 \in \mathbb{Z}$ with $f(x_0, y_0) = n$. The representation is **proper** if $\gcd(x_0, y_0) = 1$.

Definition 7.4 (Equivalence of forms)**.** Two forms f and g are **(properly) equivalent**, written $f \sim g$, if there exists a matrix $\left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$g(x, y) = f(\alpha x + \beta y,\, \gamma x + \delta y).$$

Equivalent forms have the same discriminant and represent exactly the same set of integers.

Example 7.5. The forms $x^2 + y^2$ and $x^2 + xy + y^2$ have discriminants $D = -4$ and $D = -3$ respectively. Both are positive definite. For $D = -4$, the only reduced form is $x^2 + y^2$, so the class number is $h(-4) = 1$.

7.2 Sums of Two Squares: Preliminary Results

We aim to determine which integers are representable as $x^2 + y^2$. The key algebraic tool is the following identity.

Lemma 7.6 (Brahmagupta–Fibonacci identity)**.** *For all integers a, b, c, d,*

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ad - bc)^2.$$

Proof. Direct expansion of both sides. Alternatively, this is the multiplicativity of the norm in the Gaussian integers: $|z|^2 \cdot |w|^2 = |zw|^2$ where $z = a + bi$ and $w = c + di$. □

Corollary 7.7. *If m and n are each sums of two squares, then so is mn.*

Lemma 7.8. *If p is an odd prime with $p \equiv 1 \pmod 4$, then -1 is a quadratic residue modulo p. That is, there exists $x \in \mathbb{Z}$ with $x^2 \equiv -1 \pmod p$.*

Proof. By Wilson's theorem, $(p-1)! \equiv -1 \pmod p$. Write

$$(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-1).$$

Since $p - k \equiv -k \pmod p$, we get $(p-1)! \equiv (-1)^{(p-1)/2} \left(\frac{p-1}{2}!\right)^2 \pmod p$. When $p \equiv 1 \pmod 4$, the exponent $(p-1)/2$ is even, so $(p-1)! \equiv \left(\frac{p-1}{2}!\right)^2 \pmod p$. Hence $\left(\frac{p-1}{2}!\right)^2 \equiv -1 \pmod p$, and $x = \left(\frac{p-1}{2}\right)!$ works. □

7.3 Fermat's Two-Square Theorem

Theorem 7.9 (Fermat's two-square theorem)**.** *An odd prime p is a sum of two squares if and only if $p \equiv 1 \pmod 4$.*

Proof. **Necessity.** Suppose $p = x^2 + y^2$. Since p is odd, x and y have different parities. Modulo 4, squares are $\equiv 0$ or 1, so $x^2 + y^2 \equiv 0 + 1 = 1 \pmod 4$. Thus $p \equiv 1 \pmod 4$.

Sufficiency. We give Zagier's celebrated "one-sentence proof" restructured for clarity, then a second self-contained descent proof.

Step 1: There exists m with $1 \leq m < p$ and $mp = x^2 + y^2$.

By Lemma 7.8, there exists r with $r^2 \equiv -1 \pmod p$ and $0 < r < p$. Then $r^2 + 1 \equiv 0 \pmod p$, so $p \mid (r^2 + 1^2)$ and $mp = r^2 + 1$ for some m with $1 \leq m < p$ (since $r^2 + 1 < p^2$).

Step 2 (Descent): Reduce m to 1.

Let m be the smallest positive integer such that $mp = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. We show $m = 1$.

Suppose for contradiction that $m > 1$. If m is even, then x and y have the same parity, and

$$\frac{m}{2}\, p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2,$$

contradicting the minimality of m. So m is odd and $m \geq 3$.

Choose u, v with $u \equiv x \pmod m$, $v \equiv y \pmod m$, and $|u|, |v| \leq (m-1)/2 < m/2$. Then

$$u^2 + v^2 \equiv x^2 + y^2 \equiv 0 \pmod m,$$

so $u^2 + v^2 = m\, m'$ for some positive integer m'. Note that $u^2 + v^2 \leq 2(m/2)^2 = m^2/2 < m^2$, so $m' < m$.

Moreover m' cannot be zero (that would force $u = v = 0$, hence $m \mid x$ and $m \mid y$, giving $m^2 \mid (x^2 + y^2) = mp$, so $m \mid p$; since $1 < m < p$, this is impossible).

By the Brahmagupta–Fibonacci identity (Lemma 7.6),

$$m^2\, m'\, p = (u^2 + v^2)(x^2 + y^2) = (ux + vy)^2 + (uy - vx)^2.$$

Since $ux + vy \equiv x^2 + y^2 \equiv 0 \pmod m$ and similarly $uy - vx \equiv xy - yx = 0 \pmod m$, we can divide:

$$m'\, p = \left(\frac{ux + vy}{m}\right)^2 + \left(\frac{uy - vx}{m}\right)^2,$$

where both quotients are integers. Since $0 < m' < m$, this contradicts the minimality of m.

Therefore $m = 1$ and $p = x^2 + y^2$. □

Remark 7.10 (Uniqueness). Fermat also claimed (and Euler proved) that the representation $p = x^2 + y^2$ with $x, y > 0$ and $x \geq y$ is *unique*. This follows from the fact that $\mathbb{Z}[i]$ is a unique factorisation domain, or equivalently that the class number $h(-4) = 1$.

7.4 The Gaussian Integers Approach

The theory of sums of two squares is intimately connected to the ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ of Gaussian integers.

Definition 7.11 (Gaussian integers and norm)**.** The ring $\mathbb{Z}[i]$ has a multiplicative norm $N(a + bi) = a^2 + b^2$. An element $\pi \in \mathbb{Z}[i]$ is a **Gaussian prime** if it is not a unit and its only divisors are units and associates.

Theorem 7.12 (Primes in $\mathbb{Z}[i]$)**.** *The Gaussian primes are, up to associates:*

(i) $1+i$ *(with* $N(1+i)=2$*),*

(ii) $a+bi$ *where* $a^2+b^2=p$ *is a rational prime* $\equiv 1 \pmod 4$*,*

(iii) rational primes $p \equiv 3 \pmod 4$ *(which remain prime in* $\mathbb{Z}[i]$*).*

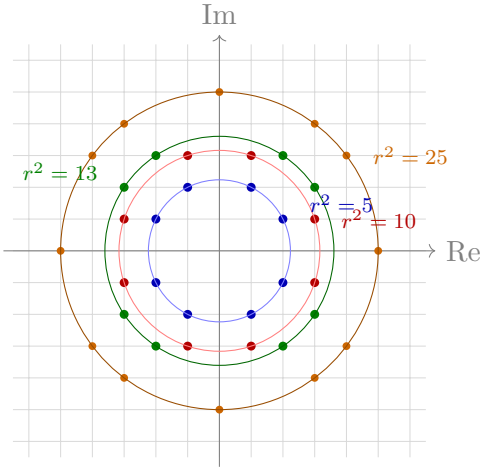


Figure 7.1: Lattice points $(x, y) \in \mathbb{Z}^2$ on circles $x^2 + y^2 = n$ for $n = 5, 10, 13, 25$.

7.5 Which Integers Are Sums of Two Squares?

Theorem 7.13 (Characterisation of sums of two squares)**.** *A positive integer* n *is a sum of two squares if and only if every prime factor* $p \equiv 3 \pmod 4$ *appears to an even power in the prime factorisation of* n*.*

Proof. **Sufficiency.** Suppose $n = 2^{a_0}\prod p_i^{a_i}\prod q_j^{2b_j}$ where each $p_i \equiv 1 \pmod 4$ and each $q_j \equiv 3 \pmod 4$. Now $2 = 1^2+1^2$, each $p_i = x_i^2+y_i^2$ by Theorem 7.9, and $q_j^{2b_j} = (q_j^{b_j})^2+0^2$. By repeated application of the Brahmagupta–Fibonacci identity (Corollary 7.7), n is a sum of two squares.

Necessity. Suppose $n = x^2+y^2$ and let $q \equiv 3 \pmod 4$ be a prime with $q^k \| n$ (meaning $q^k \mid n$ but $q^{k+1} \nmid n$). We must show k is even.

Let $d = \gcd(x, y)$ and write $x = dx'$, $y = dy'$ with $\gcd(x', y') = 1$. Then $n = d^2(x'^2+y'^2)$. Let $q^\ell \| d$, so $q^{2\ell} \| d^2$. Set $n' = x'^2+y'^2$; then $q^{k-2\ell} \| n'$.

If $q \mid n'$, then $q \mid (x'^2+y'^2)$, so $x'^2 \equiv -y'^2 \pmod q$. Since $\gcd(x', y') = 1$, we have $q \nmid y'$, so $(x'y'^{-1})^2 \equiv -1 \pmod q$, meaning -1 is a quadratic residue mod q. But $q \equiv 3 \pmod 4$ implies $\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2} = -1$, a contradiction.

Therefore $q \nmid n'$, so $k - 2\ell = 0$, i.e. $k = 2\ell$ is even. □

Example 7.14.

(a) $45 = 3^2 \cdot 5$. The prime $3 \equiv 3 \pmod 4$ appears to an even power, and $5 \equiv 1 \pmod 4$. Indeed $45 = 6^2 + 3^2$.

(b) $21 = 3 \cdot 7$. Both 3 and 7 are $\equiv 3 \pmod 4$ and appear to odd powers, so 21 is *not* a sum of two squares.

(c) $50 = 2 \cdot 5^2 = 1^2 + 7^2 = 5^2 + 5^2$.

Proposition 7.15 (Counting representations)**.** *Let $r_2(n)$ denote the number of representations of n as $x^2 + y^2$ (with order and signs). Then*

$$r_2(n) = 4\sum_{d \mid n} \chi(d), \qquad \text{where } \chi(d) = \begin{cases} +1 & \text{if } d \equiv 1 \pmod 4, \\ -1 & \text{if } d \equiv 3 \pmod 4, \\ 0 & \text{if } 2 \mid d. \end{cases}$$

Here χ is the non-principal character modulo 4.

7.6 Lagrange's Four-Square Theorem

Fermat's theorem handles primes $\equiv 1 \pmod 4$. What about all positive integers? Lagrange proved the following remarkable result in 1770.

Theorem 7.16 (Lagrange's four-square theorem)**.** *Every positive integer is a sum of four squares of non-negative integers. That is, for every $n \geq 1$ there exist $a, b, c, d \in \mathbb{Z}_{\geq 0}$ with*

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

Proof sketch. The proof follows the same pattern as for two squares.

Step 1 (Euler's four-square identity). The product of two sums of four squares is itself a sum of four squares. This follows from the multiplicativity of the norm in the quaternions $\mathbb{H}$: $N(q_1 q_2) = N(q_1)N(q_2)$ where $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$. It therefore suffices to prove the theorem for primes.

Step 2. For any prime p, there exist a, b with $0 \leq a, b \leq (p-1)/2$ and $a^2 + b^2 + 1 \equiv 0 \pmod p$. This is proved by a pigeonhole argument on the sets $\{a^2 : 0 \leq a \leq (p-1)/2\}$ and $\{-1 - b^2 : 0 \leq b \leq (p-1)/2\}$, each of size $(p+1)/2$.

Step 3 (Descent). Starting from $mp = a^2 + b^2 + c^2 + d^2$ with $1 \leq m < p$, a descent argument analogous to that in Theorem 7.9 reduces m to 1. $\square$

Example 7.17.

- $7 = 4 + 1 + 1 + 1 = 2^2 + 1^2 + 1^2 + 1^2$.
- $15 = 9 + 4 + 1 + 1 = 3^2 + 2^2 + 1^2 + 1^2$.
- $23 = 9 + 9 + 4 + 1 = 3^2 + 3^2 + 2^2 + 1^2$.

Remark 7.18 (Three squares). Legendre (1798) and Gauss showed that a positive integer n is a sum of three squares if and only if n is *not* of the form $4^a(8b + 7)$ for non-negative integers a, b. Thus $7, 15, 23, 28, 60, \ldots$ require four squares.

7.7 Waring's Problem and Further Directions

Definition 7.19 (Waring's problem)**.** For each positive integer k, let $g(k)$ denote the smallest s such that every positive integer is a sum of at most s perfect k-th powers. Waring's problem asks for the value of $g(k)$ for each k.

Remark 7.20. Known values include $g(1) = 1$, $g(2) = 4$ (Lagrange), $g(3) = 9$ (Wieferich–Kempner), and $g(4) = 19$ (Balasubramanian–Deshouillers–Dress). Hilbert proved in 1909 that $g(k)$ is finite for all k.

Remark 7.21 (Ternary quadratic forms). Ramanujan (1916) determined all *universal* positive definite diagonal quaternary forms $ax^2 + by^2 + cz^2 + dw^2$ that represent all positive integers. The "15-theorem" of Conway and Schneeberger (1993) states that a positive definite integer-matrix quadratic form represents all positive integers if and only if it represents every integer from 1 to 15.

7.8 Exercises

Exercise 7.1. Find all integers n with $1 \le n \le 50$ that are sums of two squares. For each such n, give an explicit representation.

Exercise 7.2. Use the Brahmagupta–Fibonacci identity to write $5 \cdot 13 = 65$ as a sum of two squares in two different ways.

Exercise 7.3. Show directly (without using the Legendre symbol) that if $p \equiv 3 \pmod 4$ is prime, then p cannot be written as $x^2 + y^2$.

Exercise 7.4. Determine all units of $\mathbb{Z}[i]$ and prove that $\mathbb{Z}[i]$ is a Euclidean domain with respect to the norm $N(a + bi) = a^2 + b^2$.

Exercise 7.5. Prove that if n is a sum of two squares, then so is n^2. Give two proofs: one using the Brahmagupta–Fibonacci identity and one using the characterisation theorem (Theorem 7.13).

Exercise 7.6. Show that the integers of the form $4^a(8b + 7)$ are not sums of three squares. *Hint:* Show that if $n \equiv 7 \pmod 8$ then n is not a sum of three squares by considering squares modulo 8.

Exercise 7.7. Prove that an odd prime p is represented by the form $x^2 + 2y^2$ if and only if $p \equiv 1$ or $3 \pmod 8$. *Hint:* Show that -2 is a quadratic residue modulo p if and only if $p \equiv 1$ or $3 \pmod 8$, then apply a descent argument.

Exercise 7.8. Find all representations of 30 as a sum of three squares (where order and signs matter). How many are there?

Exercise 7.9. Show that for every positive integer k, there exist infinitely many integers that require exactly k terms when written as sums of squares (for $k \le 4$).

Exercise 7.10. Compute $r_2(n)$ for $n = 1, 2, 5, 10, 25$ using the formula in Proposition 7.15, and verify by direct enumeration.

Chapter Summary

- A **binary quadratic form** $ax^2+bxy+cy^2$ has discriminant $D = b^2-4ac$. Equivalent forms represent the same integers.
- **Fermat's two-square theorem**: an odd prime $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$. The proof uses the existence of a square root of -1 modulo p and a descent argument.
- A positive integer n is a sum of two squares $\iff$ every prime $q \equiv 3 \pmod 4$ dividing n appears to an even power.
- **Lagrange**: every positive integer is a sum of four squares.
- The Gaussian integers $\mathbb{Z}[i]$ provide a structural explanation: $n = x^2+y^2$ iff $n = N(\alpha)$ for some $\alpha \in \mathbb{Z}[i]$.
- **Waring's problem**: $g(k)$ is finite for every k (Hilbert, 1909).

Chapter 8

Arithmetic Functions

> *"The theory of numbers is the queen of mathematics, and the theory of forms and functions is the queen of number theory."* — adapted from Gauss

Arithmetic functions assign a value to each positive integer and encode deep information about the multiplicative structure of $\mathbb{Z}$. In this chapter we study the principal arithmetic functions—Euler's totient, divisor functions, the Möbius function, and the von Mangoldt function—prove their key properties, and develop the powerful tool of Dirichlet convolution and Möbius inversion.

8.1 The Main Arithmetic Functions

Definition 8.1 (Arithmetic function)**.** An **arithmetic function** is any function $f\colon \mathbb{Z}_{>0} \to \mathbb{C}$. It is **multiplicative** if $f(1) = 1$ and

$$f(mn) = f(m)f(n) \quad \text{whenever } \gcd(m,n) = 1.$$

It is **completely multiplicative** if this holds for *all* m, n (without the coprimality condition).

8.1.1 Euler's Totient Function

Definition 8.2 (Euler's totient)**.** For $n \geq 1$, $\varphi(n)$ is the number of integers k with $1 \leq k \leq n$ and $\gcd(k,n) = 1$:

$$\varphi(n) = \#\{k \in \mathbb{Z} : 1 \leq k \leq n,\ \gcd(k,n) = 1\} = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Proposition 8.3 (Multiplicativity of φ)**.** *φ is multiplicative.*

Proof. Let $\gcd(m,n) = 1$. By the Chinese Remainder Theorem, $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, and an element (a,b) is a unit in the product ring if and only if a is a unit mod m and b is a unit mod n. Hence

$$\varphi(mn) = (\mathbb{Z}/mn\mathbb{Z})^\times = |(\mathbb{Z}/m\mathbb{Z})^\times| \cdot |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(m)\,\varphi(n). \qquad \square$$

Proposition 8.4 (Formula for prime powers)**.** *For a prime p and $a \geq 1$, $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$.*

Proof. Among $1, 2, \ldots, p^a$, those *not* coprime to p^a are exactly the multiples of p: there are p^{a-1} of them. So $\varphi(p^a) = p^a - p^{a-1}$. □

8.1.2 Divisor Functions

Definition 8.5 (Divisor functions τ and σ)**.** For $n \geq 1$, define:

$$\tau(n) = \sum_{d|n} 1 = \text{number of positive divisors of } n,$$
$$\sigma(n) = \sum_{d|n} d = \text{sum of positive divisors of } n.$$

More generally, $\sigma_s(n) = \sum_{d|n} d^s$ for $s \in \mathbb{C}$, so $\tau(n) = \sigma_0(n)$ and $\sigma(n) = \sigma_1(n)$.

Proposition 8.6. *The functions τ and σ (and more generally σ_s for each s) are multiplicative.*

Proof. Let $\gcd(m, n) = 1$. Every divisor d of mn can be uniquely written as $d = d_1 d_2$ with $d_1 \mid m$ and $d_2 \mid n$ (and $\gcd(d_1, d_2) = 1$). Therefore

$$\sigma_s(mn) = \sum_{d|mn} d^s = \sum_{d_1|m} \sum_{d_2|n} (d_1 d_2)^s = \left(\sum_{d_1|m} d_1^s\right)\left(\sum_{d_2|n} d_2^s\right) = \sigma_s(m)\,\sigma_s(n).$$ □

Proposition 8.7 (Formulas on prime powers)**.** *For a prime p and $a \geq 1$:*

$$\tau(p^a) = a + 1, \qquad \sigma(p^a) = \frac{p^{a+1} - 1}{p - 1}.$$

Proof. The divisors of p^a are $1, p, p^2, \ldots, p^a$, giving $a+1$ divisors and sum $1 + p + \cdots + p^a = (p^{a+1} - 1)/(p - 1)$. □

8.1.3 The Möbius Function

Definition 8.8 (Möbius function)**.** The Möbius function $\mu \colon \mathbb{Z}_{>0} \to \{-1, 0, 1\}$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ for distinct primes } p_i, \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p. \end{cases}$$

Proposition 8.9. *μ is multiplicative.*

Proof. Let $\gcd(m,n)=1$. If $p^2 \mid m$ or $p^2 \mid n$, then $p^2 \mid mn$ and both sides of $\mu(mn)=\mu(m)\mu(n)$ are zero. Otherwise $m=p_1\cdots p_j$ and $n=q_1\cdots q_k$ with all primes distinct (since $\gcd(m,n)=1$), so $\mu(mn)=(-1)^{j+k}=(-1)^j(-1)^k=\mu(m)\mu(n)$. □

Proposition 8.10. *For all $n \geq 1$,*

$$\sum_{d\mid n}\mu(d)=\begin{cases}1 & \text{if } n=1,\\ 0 & \text{if } n>1.\end{cases}$$

In other words, $\mu * \mathbf{1}=\varepsilon$, where $\mathbf{1}(n)=1$ for all n and $\varepsilon(n)=[n=1]$.

Proof. The case $n=1$ is immediate: $\mu(1)=1$.

For $n>1$, write $n=p_1^{a_1}\cdots p_r^{a_r}$. Since $\mu(d)=0$ whenever d has a squared prime factor, only the squarefree divisors contribute:

$$\sum_{d\mid n}\mu(d)=\sum_{S\subseteq\{p_1,\dots,p_r\}}\mu\Big(\prod_{p\in S}p\Big)=\sum_{k=0}^{r}\binom{r}{k}(-1)^k=(1-1)^r=0.$$ □

8.1.4 The von Mangoldt Function

Definition 8.11 (Von Mangoldt function)**.** The **von Mangoldt function** is

$$\Lambda(n)=\begin{cases}\log p & \text{if } n=p^k \text{ for some prime } p \text{ and } k\geq 1,\\ 0 & \text{otherwise.}\end{cases}$$

Proposition 8.12. *For all $n \geq 1$, $\sum_{d\mid n}\Lambda(d)=\log n$.*

Proof. Write $n=p_1^{a_1}\cdots p_r^{a_r}$. The divisors d of n with $\Lambda(d)\neq 0$ are p_i^j for $1\leq j\leq a_i$ and $1\leq i\leq r$. Therefore

$$\sum_{d\mid n}\Lambda(d)=\sum_{i=1}^{r}\sum_{j=1}^{a_i}\log p_i=\sum_{i=1}^{r}a_i\log p_i=\log\Big(\prod p_i^{a_i}\Big)=\log n.$$ □

Remark 8.13. The von Mangoldt function is *not* multiplicative: $\Lambda(1)=0\neq 1$. It plays a central role in analytic number theory, particularly in the prime number theorem through the Chebyshev functions $\psi(x)=\sum_{n\leq x}\Lambda(n)$.

8.2 The Identity $\sum_{d\mid n}\varphi(d)=n$

Theorem 8.14. *For every positive integer n,*

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

Proof. We give two proofs.

Proof 1 (Counting). Partition the set $\{1, 2, \ldots, n\}$ according to the value of $\gcd(k, n)$. For each divisor d of n, the integers k with $1 \le k \le n$ and $\gcd(k, n) = d$ are exactly the integers of the form $k = d\ell$ where $1 \le \ell \le n/d$ and $\gcd(\ell, n/d) = 1$. There are $\varphi(n/d)$ such integers. Since every $k \in \{1, \ldots, n\}$ has $\gcd(k, n) = d$ for exactly one divisor d,

$$n = \sum_{d \mid n} \varphi\left(\frac{n}{d}\right) = \sum_{d \mid n} \varphi(d),$$

where the last equality holds because as d runs over divisors of n, so does n/d.

Proof 2 (Multiplicative functions). Define $F(n) = \sum_{d \mid n} \varphi(d)$. Since φ is multiplicative, F is also multiplicative (a general fact about Dirichlet convolution, Proposition 8.18). For a prime power p^a:

$$F(p^a) = \sum_{j=0}^{a} \varphi(p^j) = 1 + \sum_{j=1}^{a} p^{j-1}(p-1) = 1 + (p-1) \cdot \frac{p^a - 1}{p - 1} = p^a.$$

The identity function $\mathrm{id}(n) = n$ is also multiplicative and satisfies $\mathrm{id}(p^a) = p^a$. Since two multiplicative functions that agree on prime powers agree everywhere, $F = \mathrm{id}$. □

8.3 Dirichlet Convolution

Definition 8.15 (Dirichlet convolution)**.** Given arithmetic functions f and g, their **Dirichlet convolution** $f * g$ is defined by

$$(f * g)(n) = \sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right) = \sum_{\substack{ab = n \\ a, b \ge 1}} f(a)\, g(b).$$

Proposition 8.16 (Ring structure)**.** *The set of arithmetic functions with pointwise addition and Dirichlet convolution forms a commutative ring with identity.*

(i) ***Commutativity:*** $f * g = g * f$.

(ii) ***Associativity:*** $(f * g) * h = f * (g * h)$.

(iii) ***Identity:*** $f * \varepsilon = f$, *where* $\varepsilon(n) = [n = 1]$ *is the Dirichlet identity.*

(iv) ***Distributivity:*** $f * (g + h) = f * g + f * h$.

Proof. (i) follows from the bijection $(a, b) \leftrightarrow (b, a)$ on pairs with $ab = n$.
(ii) Both sides equal $\sum_{abc = n} f(a)\, g(b)\, h(c)$.
(iii) $(f * \varepsilon)(n) = \sum_{d \mid n} f(d)\, \varepsilon(n/d) = f(n) \cdot 1 = f(n)$ since $\varepsilon(n/d) = 0$ unless $d = n$.
(iv) Direct computation. □

Notation 8.17. We use the following standard arithmetic functions:

$$\varepsilon(n) = [n = 1], \qquad \mathbf{1}(n) = 1, \qquad \mathrm{id}(n) = n, \qquad \mathrm{id}_s(n) = n^s.$$

With this notation, the identities we have proved become elegant convolution equations:

$$\tau = \mathbf{1} * \mathbf{1}, \tag{8.1}$$
$$\sigma = \mathrm{id} * \mathbf{1}, \tag{8.2}$$
$$\mathrm{id} = \varphi * \mathbf{1}, \tag{8.3}$$
$$\varepsilon = \mu * \mathbf{1}, \tag{8.4}$$
$$\Lambda = \mu * (-\log). \tag{8.5}$$

Proposition 8.18 (Multiplicativity preserved by convolution)**.** *If f and g are multiplicative, then so is $f * g$.*

Proof. Let $\gcd(m,n) = 1$. Every divisor d of mn factors uniquely as $d = d_1 d_2$ with $d_1 \mid m$, $d_2 \mid n$, and $\gcd(d_1, d_2) = 1$. Then

$$\begin{aligned}(f*g)(mn) &= \sum_{d \mid mn} f(d)\, g\!\left(\frac{mn}{d}\right) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1 d_2)\, g\!\left(\frac{m}{d_1} \cdot \frac{n}{d_2}\right) \\ &= \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1) f(d_2)\, g\!\left(\frac{m}{d_1}\right) g\!\left(\frac{n}{d_2}\right) \\ &= \left(\sum_{d_1 \mid m} f(d_1)\, g\!\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2 \mid n} f(d_2)\, g\!\left(\frac{n}{d_2}\right)\right) = (f*g)(m)\,(f*g)(n).\end{aligned}$$

Also $(f*g)(1) = f(1)g(1) = 1$. □

Theorem 8.19 (Dirichlet inverse)**.** *An arithmetic function f has a Dirichlet inverse (i.e., there exists g with $f * g = \varepsilon$) if and only if $f(1) \neq 0$. In this case, g is unique and is given recursively by $g(1) = 1/f(1)$ and, for $n > 1$,*

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d \mid n \\ d < n}} f\!\left(\frac{n}{d}\right) g(d).$$

Moreover, if f is multiplicative, then so is f^{-1}.

Proof. From $(f*g)(1) = f(1)g(1) = \varepsilon(1) = 1$, we need $g(1) = 1/f(1)$, which requires $f(1) \neq 0$. For $n > 1$, $(f*g)(n) = 0$ gives $f(1)g(n) + \sum_{d \mid n,\, d<n} f(n/d)\, g(d) = 0$, yielding the recursion. Uniqueness follows since g is determined recursively.

For multiplicativity of f^{-1} when f is multiplicative: since $f * f^{-1} = \varepsilon$ is multiplicative, one shows by induction on mn (for $\gcd(m,n) = 1$) that $f^{-1}(mn) = f^{-1}(m) f^{-1}(n)$. □

Figure 8.1: Dirichlet convolution identities: $\mu * \mathbf{1} = \varepsilon$ and $\varphi * \mathbf{1} = \mathrm{id}$.

8.4 Möbius Inversion

Theorem 8.20 (Möbius inversion formula)**.** *Let f and g be arithmetic functions. Then*

$$g(n) = \sum_{d|n} f(d) \quad \text{for all } n \geq 1$$

if and only if

$$f(n) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) \quad \text{for all } n \geq 1.$$

In convolution notation: $g = f * \mathbf{1}$ if and only if $f = g * \mu = \mu * g$.

Proof. **Forward direction.** Suppose $g = f * \mathbf{1}$. Then

$$(g * \mu)(n) = ((f * \mathbf{1}) * \mu)(n) = (f * (\mathbf{1} * \mu))(n) = (f * \varepsilon)(n) = f(n),$$

using associativity (Proposition 8.16(ii)) and the identity $\mathbf{1} * \mu = \varepsilon$ (Proposition 8.10).

Backward direction. Conversely, if $f = g * \mu$, then

$$(f * \mathbf{1})(n) = ((g * \mu) * \mathbf{1})(n) = (g * (\mu * \mathbf{1}))(n) = (g * \varepsilon)(n) = g(n).$$

Both directions are instances of the same algebraic fact: $\mu = \mathbf{1}^{-1}$ in the Dirichlet ring. □

Corollary 8.21 (Möbius inversion for φ)**.** *From* $\mathrm{id} = \varphi * \mathbf{1}$*, Möbius inversion gives*

$$\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Proof. By Möbius inversion, $\varphi = \mathrm{id} * \mu$. Thus

$$\varphi(n) = \sum_{d|n} \mu(d)\, \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}.$$

For $n = p_1^{a_1} \cdots p_r^{a_r}$, only squarefree divisors d (products of subsets of $\{p_1, \ldots, p_r\}$) give $\mu(d) \neq 0$:

$$\sum_{d|n} \frac{\mu(d)}{d} = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

□

Example 8.22 (Application: counting primitive n-th roots of unity)**.** The cyclotomic polynomial $\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - e^{2\pi i k/n})$ has degree $\varphi(n)$. Since $x^n - 1 = \prod_{d|n} \Phi_d(x)$, taking degrees gives $n = \sum_{d|n} \varphi(d)$, recovering Theorem 8.14.

Example 8.23 (Counting square-free integers)**.** Let $Q(x) = \#\{n \leq x : n \text{ is squarefree}\}$. Using the identity $[n \text{ squarefree}] = \sum_{d^2|n} \mu(d)$, one shows $Q(x) = \frac{6}{\pi^2}\, x + O(\sqrt{x})$.

8.5 Dirichlet Series and Euler Products

Definition 8.24 (Dirichlet series)**.** The **Dirichlet series** associated to an arithmetic function f is the formal series

$$F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

Proposition 8.25. *If $F(s) = \sum f(n)/n^s$ and $G(s) = \sum g(n)/n^s$, then (in the region of absolute convergence)*

$$F(s)\,G(s) = \sum_{n=1}^{\infty} \frac{(f * g)(n)}{n^s}.$$

That is, Dirichlet convolution corresponds to multiplication of Dirichlet series.

Proof.

$$F(s)G(s) = \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} \frac{f(m)\,g(n)}{(mn)^s} = \sum_{N=1}^{\infty} \frac{1}{N^s} \sum_{mn=N} f(m)\,g(n) = \sum_{N=1}^{\infty} \frac{(f*g)(N)}{N^s}. \qquad \square$$

Theorem 8.26 (Euler product)**.** *If f is multiplicative, then (in the region of absolute convergence)*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \text{ prime}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\right).$$

Proof. By the fundamental theorem of arithmetic, every n factors uniquely as $n = p_1^{a_1} \cdots p_r^{a_r}$. The multiplicativity of f gives $f(n) = f(p_1^{a_1}) \cdots f(p_r^{a_r})$, and $n^{-s} = p_1^{-a_1 s} \cdots p_r^{-a_r s}$. Expanding the product over all primes and collecting terms recovers the Dirichlet series. $\square$

Example 8.27 (Standard Euler products)**.**

(a) $\zeta(s) = \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-s}}$ (Riemann zeta function, $\mathrm{Re}(s) > 1$).

(b) $\displaystyle\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_{p}(1 - p^{-s})$.

(c) $\displaystyle\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s}$ (from $\varphi = \mathrm{id} * \mu$).

(d) $\displaystyle-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$.

8.6 Perfect Numbers and $\sigma(n)$

Definition 8.28 (Perfect number)**.** A positive integer n is **perfect** if $\sigma(n) = 2n$, i.e., n equals the sum of its proper divisors.

Theorem 8.29 (Euler–Euclid theorem)**.** *An even integer n is perfect if and only if $n = 2^{p-1}(2^p - 1)$ where $2^p - 1$ is a Mersenne prime.*

Proof. **Sufficiency** (Euclid). Let $M = 2^p - 1$ be prime and $n = 2^{p-1}M$. Since $\gcd(2^{p-1}, M) = 1$,

$$\sigma(n) = \sigma(2^{p-1})\,\sigma(M) = (2^p - 1)(M + 1) = M \cdot 2^p = 2n.$$

Necessity (Euler). Let $n = 2^a m$ with $a \geq 1$ and m odd. Then $\sigma(n) = \sigma(2^a)\sigma(m) = (2^{a+1} - 1)\sigma(m)$. Setting $\sigma(n) = 2n = 2^{a+1}m$ gives

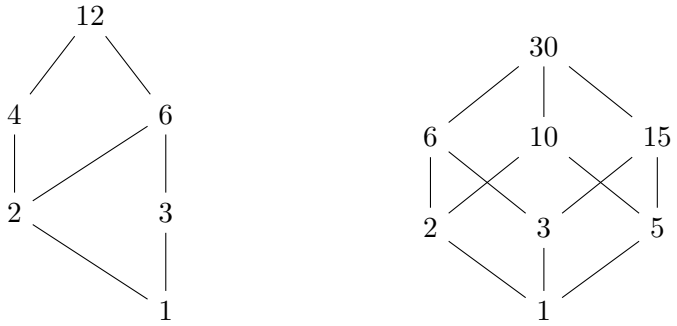
$$(2^{a+1} - 1)\,\sigma(m) = 2^{a+1}\,m.$$

Since $\gcd(2^{a+1} - 1, 2^{a+1}) = 1$, we need $(2^{a+1} - 1) \mid m$. Write $m = (2^{a+1} - 1)\,q$. Then $\sigma(m) = 2^{a+1}\,q$. But $\sigma(m) \geq m + 1 = (2^{a+1} - 1)q + 1$ (if $m > 1$) and also $\sigma(m) \geq m + q + 1$ (if $q > 1$ and $q \neq m$).

If $q = 1$, then $m = 2^{a+1} - 1$ and $\sigma(m) = 2^{a+1}$, so $\sigma(m) = m + 1$, forcing m to be prime. Thus $n = 2^a(2^{a+1} - 1)$ with $2^{a+1} - 1$ prime, as desired.

If $q > 1$, then q is a proper divisor of m distinct from 1 and m, so $\sigma(m) \geq 1 + q + m = 1 + q + (2^{a+1} - 1)q > 2^{a+1}q = \sigma(m)$, a contradiction. □

Remark 8.30. It is unknown whether any odd perfect numbers exist. It has been verified that none exist below 10^{2200} (Ochem–Rao, 2012). Any odd perfect number must have at least 10 distinct prime factors and exceed 10^{1500}.



Divisor lattice of 12 Divisor lattice of 30

Figure 8.2: Divisor lattices (Hasse diagrams) of $12 = 2^2 \cdot 3$ and $30 = 2 \cdot 3 \cdot 5$.

8.7 Summary Table of Arithmetic Functions

Function	Definition	Mult.?	At p^a	Dirichlet series
$\varphi(n)$	$\#\{k \le n : \gcd(k,n) = 1\}$	Yes	$p^{a-1}(p-1)$	$\zeta(s-1)/\zeta(s)$
$\tau(n)$	$\#\{d : d \mid n\}$	Yes	$a+1$	$\zeta(s)^2$
$\sigma(n)$	$\sum_{d\mid n} d$	Yes	$\frac{p^{a+1}-1}{p-1}$	$\zeta(s)\zeta(s-1)$
$\mu(n)$	$(-1)^k$ if $n = p_1\cdots p_k$	Yes	$\begin{cases} -1 & a=1 \\ 0 & a \ge 2 \end{cases}$	$1/\zeta(s)$
$\Lambda(n)$	$\log p$ if $n = p^k$	No	$\log p$	$-\zeta'(s)/\zeta(s)$

Table 8.1: Key arithmetic functions and their properties.

8.8 Exercises

Exercise 8.1. Compute $\varphi(n)$ for $n = 1, 2, \ldots, 20$. Verify that $\varphi(n)$ is even for all $n \ge 3$.

Exercise 8.2. Compute $\tau(n)$ and $\sigma(n)$ for $n = 360$. Is 360 a *highly composite number*?

Exercise 8.3. Verify the identity $\sum_{d\mid n} \varphi(d) = n$ for $n = 12$ by computing each term explicitly.

Exercise 8.4. Let $f(n) = n^2$ and $g(n) = \sum_{d\mid n} f(d) = \sum_{d\mid n} d^2$. Use Möbius inversion to express f in terms of g and μ, then verify for $n = 6$.

Exercise 8.5. Show that $\sum_{d\mid n} |\mu(d)| = 2^{\omega(n)}$, where $\omega(n)$ is the number of distinct prime factors of n.

Exercise 8.6. Prove directly (without using Dirichlet series) that Dirichlet convolution is associative.

Exercise 8.7. Use Möbius inversion on $\sum_{d\mid n} \Lambda(d) = \log n$ to derive the formula $\Lambda(n) = -\sum_{d\mid n} \mu(d)\log d$. *Hint:* Apply Möbius inversion to $f = \Lambda$ and $g = \log$.

Exercise 8.8. Prove that $\sigma(n) < 2n\log n$ for all $n \ge 2$. *Hint:* Show $\sigma(n)/n = \sum_{d\mid n} 1/d \le \sum_{k=1}^{n} 1/k$.

Exercise 8.9. Show that $2^{p-1}(2^p - 1)$ is even and that if $2^p - 1$ is composite then $2^{p-1}(2^p - 1)$ is not perfect.

Exercise 8.10. Compute the Dirichlet inverse of $\mathrm{id}(n) = n$. That is, find the arithmetic function h such that $\mathrm{id} * h = \varepsilon$. Express h in terms of μ and verify for small values of n.

Exercise 8.11. Starting from $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$, derive the Euler product for $\zeta(s)^2$ and identify the corresponding arithmetic function.

Exercise 8.12. Prove that a multiplicative function is completely determined by its values on prime powers. That is, if f and g are multiplicative and $f(p^a) = g(p^a)$ for all primes p and $a \ge 1$, then $f = g$.

Chapter Summary

- The main arithmetic functions are $\varphi(n)$, $\tau(n)$, $\sigma(n)$, $\mu(n)$, and $\Lambda(n)$; all except Λ are multiplicative.
- Key identity: $\sum_{d|n} \varphi(d) = n$, proved by counting or by multiplicative function arguments.
- **Dirichlet convolution** $(f * g)(n) = \sum_{d|n} f(d)\, g(n/d)$ makes the arithmetic functions into a commutative ring with identity ε. Multiplicativity is preserved under convolution.
- **Möbius inversion**: $g = f * \mathbf{1}$ iff $f = g * \mu$. This powerful tool converts summatory relations into explicit formulas.
- **Dirichlet series** $\sum f(n)/n^s$ convert convolution into multiplication. When f is multiplicative, the series has an **Euler product** over primes.
- An even number is **perfect** iff it has the form $2^{p-1}(2^p - 1)$ with $2^p - 1$ a Mersenne prime (Euler–Euclid).

Chapter 9

Introduction to p-adic Numbers

> *"The p-adic numbers are just as 'real' as the real numbers."* — attributed to various number theorists

Throughout this course, we have worked within the familiar world of the integers and rational numbers, occasionally invoking properties of the real or complex numbers. In this chapter we introduce a fundamentally different way to complete the rationals: the *p-adic numbers*. Whereas the real numbers arise from completing $\mathbb{Q}$ with respect to the usual absolute value, the p-adic numbers $\mathbb{Q}_p$ arise from a completion governed entirely by divisibility by a prime p. Far from being a curiosity, p-adic methods have become indispensable in modern number theory, from solving Diophantine equations to the proof of Fermat's Last Theorem.

9.1 Historical Background: Hensel and p-adic Analysis

Kurt Hensel introduced the p-adic numbers in 1897, motivated by an analogy between the ring of integers $\mathbb{Z}$ and the ring of polynomials $k[x]$ over a field k. Just as a polynomial can be expanded as a power series in $(x - a)$ around a point a, Hensel proposed that every integer could be expanded as a series in powers of a prime p. This bold analogy proved extraordinarily fruitful: it opened the door to applying techniques of analysis — convergence, completeness, and continuity — to purely arithmetic questions.

The idea gained further momentum through the work of Hasse, who in the 1920s formulated the celebrated *local-global principle*, stating that certain equations have rational solutions if and only if they have solutions in every p-adic field $\mathbb{Q}_p$ and in $\mathbb{R}$. Today, p-adic analysis underpins vast swathes of algebraic number theory, arithmetic geometry, and the Langlands programme.

9.2 The p-adic Valuation

Fix a prime number p.

Definition 9.1 (p-adic valuation)**.** For a nonzero integer $n \in \mathbb{Z}$, the *p-adic valuation* of n, denoted $v_p(n)$, is the largest exponent $k \geq 0$ such that $p^k \mid n$. We extend this to

$\mathbb{Q}^*$ by setting

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b),$$

and by convention $v_p(0) = +\infty$.

Example 9.2 (Computing v_p)**.** We have $v_2(12) = 2$ since $12 = 2^2 \cdot 3$, and $v_3(12) = 1$, while $v_5(12) = 0$. For a rational number, $v_3(45/98) = v_3(45) - v_3(98) = 2 - 0 = 2$.

Proposition 9.3 (Properties of the p-adic valuation)**.** *For all $x, y \in \mathbb{Q}^*$:*

1. $v_p(xy) = v_p(x) + v_p(y)$;
2. $v_p(x+y) \geq \min\big(v_p(x),\, v_p(y)\big)$, *with equality when $v_p(x) \neq v_p(y)$.*

Proof. Property (1) follows directly from unique factorisation. For (2), write $x = p^a \cdot (r/s)$ and $y = p^b \cdot (u/v)$ where $p \nmid ruv$ and $a = v_p(x)$, $b = v_p(y)$. Without loss of generality assume $a \leq b$. Then $x + y = p^a\big(r/s + p^{b-a} \cdot u/v\big)$. The term in parentheses has p-adic valuation ≥ 0, so $v_p(x+y) \geq a = \min(v_p(x), v_p(y))$. If $a < b$, the term r/s has $v_p = 0$ while $p^{b-a} \cdot u/v$ has $v_p \geq 1$, so the sum has $v_p = 0$ and equality holds. □

9.3 The p-adic Absolute Value and the Ultrametric Inequality

Definition 9.4 (p-adic absolute value)**.** The *p-adic absolute value* on $\mathbb{Q}$ is defined by

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

Example 9.5 (Sizes reversed)**.** In the 5-adic world, $|5^3|_5 = 5^{-3} = 1/125$ is very small, while $|1/5^3|_5 = 5^3 = 125$ is very large. High divisibility by p makes a number *small*, the opposite of the Archimedean intuition.

Theorem 9.6 (Ultrametric inequality)**.** *For all $x, y \in \mathbb{Q}$,*

$$|x+y|_p \leq \max\big(|x|_p\,,\, |y|_p\big).$$

Moreover, equality holds whenever $|x|_p \neq |y|_p$.

Proof. If $x = 0$ or $y = 0$ the result is immediate. Otherwise, by Proposition 9.3(2),

$$v_p(x+y) \geq \min\big(v_p(x),\, v_p(y)\big).$$

Applying $p^{-(\cdot)}$ (a decreasing function) to both sides reverses the inequality:

$$|x+y|_p = p^{-v_p(x+y)} \le p^{-\min(v_p(x),\,v_p(y))} = \max\!\Big(p^{-v_p(x)},\,p^{-v_p(y)}\Big) = \max\!\Big(|x|_p,\,|y|_p\Big).$$

The equality statement follows from the corresponding equality in Proposition 9.3(2). □

Remark 9.7 (Consequences of ultrametricity). The ultrametric inequality is far stronger than the usual triangle inequality $|x+y| \le |x| + |y|$. Among its striking consequences:

- Every triangle in $\mathbb{Q}_p$ is isosceles: if $|x|_p \neq |y|_p$ then $|x+y|_p = \max(|x|_p, |y|_p)$.
- Every point of an open ball is its centre.
- Two open balls are either disjoint or one contains the other.

9.4 The p-adic Integers and p-adic Numbers

Definition 9.8 (p-adic integers and p-adic numbers)**.** The *p-adic numbers* $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|\cdot|_p$. The *p-adic integers* are the closed unit ball:

$$\mathbb{Z}_p = \Big\{x \in \mathbb{Q}_p : |x|_p \le 1\Big\} = \Big\{x \in \mathbb{Q}_p : v_p(x) \ge 0\Big\}.$$

Every element $\alpha \in \mathbb{Z}_p$ admits a unique representation as a *p-adic expansion*:

$$\alpha = a_0 + a_1\,p + a_2\,p^2 + a_3\,p^3 + \cdots, \quad a_i \in \{0, 1, \ldots, p-1\}.$$

This converges in $|\cdot|_p$ because $|a_n p^n|_p \le p^{-n} \to 0$. A general element of $\mathbb{Q}_p$ has the form $\alpha = \sum_{n=k}^{\infty} a_n\,p^n$ for some $k \in \mathbb{Z}$ (possibly negative).

Example 9.9 (The element -1 in $\mathbb{Z}_p$)**.** In $\mathbb{Z}_p$, we have

$$-1 = (p-1) + (p-1)\,p + (p-1)\,p^2 + \cdots = \sum_{n=0}^{\infty} (p-1)\,p^n,$$

since the partial sums are $\sum_{n=0}^{N}(p-1)\,p^n = p^{N+1} - 1$, and $\Big|p^{N+1} - 1 - (-1)\Big|_p = \Big|p^{N+1}\Big|_p = p^{-(N+1)} \to 0$.

Proposition 9.10 (Structure of $\mathbb{Z}_p$)**.**

1. *$\mathbb{Z}_p$ is a local ring with unique maximal ideal $p\mathbb{Z}_p$.*
2. *The units of $\mathbb{Z}_p$ are $\mathbb{Z}_p^{\times} = \{x \in \mathbb{Z}_p : |x|_p = 1\} = \{x \in \mathbb{Z}_p : v_p(x) = 0\}$.*
3. *$\mathbb{Z}_p$ is compact in the p-adic topology.*
4. *$\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, i.e., every p-adic number has the form $p^{-k}\alpha$ for some $\alpha \in \mathbb{Z}_p$ and $k \ge 0$.*

9.5 Hensel's Lemma

Hensel's lemma is the p-adic analogue of Newton's method: a simple root modulo p can be "lifted" to a root in $\mathbb{Z}_p$.

Theorem 9.11 (Hensel's lemma, simple case)**.** *Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial. Suppose there exists $a_0 \in \mathbb{Z}_p$ such that*

$$|f(a_0)|_p < |f'(a_0)|_p^2 .$$

Then there exists a unique $a \in \mathbb{Z}_p$ with $f(a) = 0$ and $|a - a_0|_p \le |f(a_0)|_p / |f'(a_0)|_p < |f'(a_0)|_p$.

Proof. We construct a sequence (a_n) by the p-adic Newton iteration:

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

Set $\varepsilon = |f(a_0)|_p / |f'(a_0)|_p^2 < 1$ and $\delta = |f(a_0)|_p / |f'(a_0)|_p$.

Step 1: The derivative stays bounded. We claim $|f'(a_n)|_p = |f'(a_0)|_p$ for all n. Indeed, by Taylor expansion,

$$f'(a_1) = f'(a_0) + (a_1 - a_0)\, g(a_0, a_1)$$

for some polynomial g. Since $|a_1 - a_0|_p = \delta < |f'(a_0)|_p$ and $|g(\dots)|_p \le 1$, the ultrametric inequality gives $|f'(a_1)|_p = |f'(a_0)|_p$. Inductively this holds for all n.

Step 2: Rapid convergence. By Taylor's theorem for polynomials,

$$f(a_{n+1}) = f(a_n) + f'(a_n)(a_{n+1} - a_n) + (a_{n+1} - a_n)^2\, h$$

for some $h \in \mathbb{Z}_p$. Since $a_{n+1} - a_n = -f(a_n)/f'(a_n)$, the first two terms cancel, giving

$$|f(a_{n+1})|_p \le |a_{n+1} - a_n|_p^2 = \frac{|f(a_n)|_p^2}{|f'(a_0)|_p^2}.$$

This yields the bound $|f(a_{n+1})|_p \le \varepsilon \cdot |f(a_n)|_p$, so $|f(a_n)|_p \to 0$ at least as fast as $\varepsilon^{2^n - 1}$.

Step 3: Convergence and uniqueness. The sequence (a_n) is Cauchy in $\mathbb{Q}_p$: for $m > n$, $|a_m - a_n|_p \le \max_{k=n}^{m-1} |a_{k+1} - a_k|_p \to 0$. By completeness, $a_n \to a \in \mathbb{Z}_p$, and continuity of f gives $f(a) = 0$. Uniqueness in the stated ball follows from the ultrametric inequality: if $f(a) = f(b) = 0$ with both in the ball, then $0 = f(a) - f(b) = (a - b)\big(f'(a) + (a - b)h\big)$; since $|a - b|_p < |f'(a)|_p$, the factor in brackets is a unit, forcing $a = b$. □

Corollary 9.12 (Practical lifting criterion)**.** *If $f(x) \in \mathbb{Z}[x]$ and $a_0 \in \mathbb{Z}$ satisfies $f(a_0) \equiv 0 \pmod p$ with $f'(a_0) \not\equiv 0 \pmod p$, then there exists a unique $a \in \mathbb{Z}_p$ with $f(a) = 0$ and $a \equiv a_0 \pmod p$.*

9.6 Applications of Hensel's Lemma

Example 9.13 (Solving $x^2 = -1$ in $\mathbb{Q}_5$)**.** Consider $f(x) = x^2 + 1$. We look for a root modulo 5: trying $a_0 = 2$ gives $f(2) = 5 \equiv 0 \pmod 5$, and $f'(2) = 4 \not\equiv 0 \pmod 5$. By Corollary 9.12, there exists $i \in \mathbb{Z}_5$ with $i^2 = -1$ and $i \equiv 2 \pmod 5$.
We can compute the first few digits. Newton's iteration gives:

$$a_0 = 2,$$
$$a_1 = a_0 - \frac{f(a_0)}{f'(a_0)} = 2 - \frac{5}{4} = 2 - 5 \cdot 4^{-1} \equiv 2 - 5 \cdot 4 \equiv 2 + 5 \cdot 1 = 7 \pmod{25},$$
$$a_2 \equiv 7 - \frac{50}{14} \equiv 7 - 50 \cdot 14^{-1} \pmod{125}.$$

Continuing, one obtains the 5-adic expansion $i = 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + \cdots \in \mathbb{Z}_5$. Note that $-i$ is also a root, with expansion starting $3 + 3 \cdot 5 + 2 \cdot 5^2 + \cdots$

Remark 9.14 (When does $\sqrt{-1}$ exist in $\mathbb{Q}_p$?). A square root of -1 exists in $\mathbb{Q}_p$ if and only if $p \equiv 1 \pmod 4$ or $p = 2$ (but the case $p = 2$ requires care: $\sqrt{-1}$ does not exist in $\mathbb{Q}_2$). This is closely related to our earlier study of quadratic residues (Chapter 6).

9.7 The Local-Global Principle

One of the most powerful ideas in number theory is that solving an equation over $\mathbb{Q}$ can be reduced to solving it over each "local" completion $\mathbb{Q}_p$ (for every prime p) and over $\mathbb{R}$.

Theorem 9.15 (Hasse–Minkowski)**.** *A quadratic form $Q(\mathbf{x}) = \sum_{i,j} a_{ij} x_i x_j$ with $a_{ij} \in \mathbb{Q}$ represents zero nontrivially over $\mathbb{Q}$ (i.e., there exists $\mathbf{x} \neq \mathbf{0}$ in $\mathbb{Q}^n$ with $Q(\mathbf{x}) = 0$) if and only if it represents zero nontrivially over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime p.*

Remark 9.16 (Limitations of the local-global principle). The Hasse–Minkowski theorem holds for quadratic forms but *fails* in general. A famous counterexample due to Selmer is the cubic curve $3x^3 + 4y^3 + 5z^3 = 0$, which has nontrivial solutions in $\mathbb{R}$ and in every $\mathbb{Q}_p$, but no nontrivial solution in $\mathbb{Q}$. Understanding when and why the local-global principle fails is a central theme in modern arithmetic geometry, involving the Brauer–Manin obstruction.

9.8 Ostrowski's Theorem

The p-adic absolute values, together with the usual absolute value, exhaust all possibilities for measuring size on $\mathbb{Q}$.

Theorem 9.17 (Ostrowski's theorem)**.** *Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to either:*

1. *the usual (Archimedean) absolute value $|\cdot|_\infty$, or*

2. the p-adic absolute value $|\cdot|_p$ for some prime p.

Here, two absolute values are equivalent *if they induce the same topology on $\mathbb{Q}$.*

Remark 9.18 (Product formula). For every $x \in \mathbb{Q}^*$,

$$|x|_\infty \cdot \prod_{p \text{ prime}} |x|_p = 1.$$

This elegant identity encodes the idea that the "places" of $\mathbb{Q}$ — one for each prime and one Archimedean — together capture all arithmetic information.

9.9 Visualising p-adic Structure

The p-adic integers have a tree-like structure: truncating the p-adic expansion to n digits gives a map $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$, and the preimages of each residue class form a ball of radius p^{-n}.

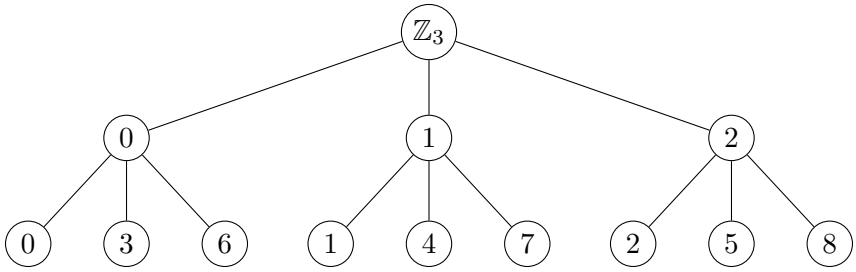


Figure 9.1: The tree structure of $\mathbb{Z}_3$: the first two levels correspond to residues modulo 3 and modulo 9. Each path from root to leaf determines the first digits of a 3-adic expansion.

9.10 Exercises

Exercise 9.1. Prove *Legendre's formula*: for any prime p and positive integer n,

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

Use this to compute $v_2(100!)$ and $v_5(100!)$.

Exercise 9.2. Let $(K, |\cdot|)$ be a field with an ultrametric absolute value. Prove that in any triangle with side lengths a, b, c (i.e., $a = |x - y|$, etc.), the two largest sides have equal length.

Exercise 9.3. Determine for which primes $p \leq 13$ the equation $x^2 = 2$ has a solution in $\mathbb{Z}_p$. For $p = 7$, find the first three digits of the 7-adic expansion of $\sqrt{2}$.

Exercise 9.4. Show that the series $\sum_{n=0}^{\infty} n!$ converges in $\mathbb{Q}_p$ for every prime p. What is its p-adic absolute value?

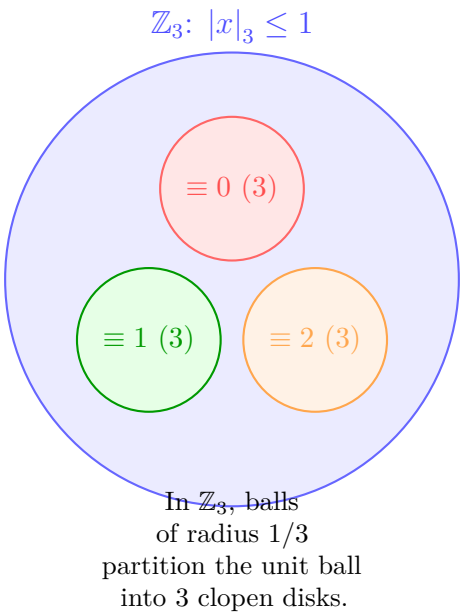


Figure 9.2: Disk structure of $\mathbb{Z}_3$. The unit ball decomposes into three disjoint balls of radius 1/3, each consisting of elements with a given residue modulo 3.

Exercise 9.5. Prove that $\mathbb{Z}_p$ is compact by showing it is a closed and totally bounded subset of the complete metric space $\mathbb{Q}_p$.

Exercise 9.6. Verify the product formula $|x|_\infty \prod_p |x|_p = 1$ for $x = 75/14$.

Exercise 9.7. Write out the 7-adic expansion of -1 (first five digits) and verify your answer by computing the partial sums.

Exercise 9.8 (Challenging)**.** Show that $\mathbb{Z}_p$ is not a field but that $\mathbb{Q}_p$ is. Identify the non-units of $\mathbb{Z}_p$ explicitly.

9.11 Chapter Summary

- The **p-adic valuation** v_p measures divisibility by p; the p-adic absolute value $|x|_p = p^{-v_p(x)}$ makes highly divisible numbers *small*.
- The **ultrametric inequality** $|x+y|_p \leq \max(|x|_p, |y|_p)$ leads to exotic but useful topology: every point is a centre, and all triangles are isosceles.
- The completion $\mathbb{Q}_p$ contains $\mathbb{Z}_p$ (the unit ball), whose elements have p-adic expansions analogous to power series.
- **Hensel's lemma** lifts simple roots modulo p to exact roots in $\mathbb{Z}_p$, providing a powerful tool for solving polynomial equations.
- **Ostrowski's theorem** classifies all absolute values on $\mathbb{Q}$: the usual one and the p-adic ones.
- The **Hasse–Minkowski theorem** exemplifies the local-global principle for quadratic forms, connecting $\mathbb{Q}_p$-solutions for all p and $\mathbb{R}$-solutions to $\mathbb{Q}$-solutions.

Chapter 10

Preview of Analytic Number Theory

> *"The primes are the atoms of arithmetic, and the zeta function is the spectrograph that reveals their hidden structure."*

Throughout this course, we have studied the primes using algebraic and combinatorial methods. In this final chapter, we catch a glimpse of *analytic number theory*, where the tools of calculus and complex analysis are brought to bear on the distribution of primes. The central object is the Riemann zeta function, and the central result is the Prime Number Theorem.

10.1 The Riemann Zeta Function

Definition 10.1 (Riemann zeta function)**.** For a complex variable s with $\operatorname{Re}(s) > 1$, the *Riemann zeta function* is

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Proposition 10.2 (Convergence)**.** *The series $\sum_{n=1}^{\infty} n^{-s}$ converges absolutely for $\operatorname{Re}(s) > 1$ and uniformly on every half-plane $\operatorname{Re}(s) \geq 1 + \delta$ with $\delta > 0$.*

Proof. For $s = \sigma + it$ with $\sigma > 1$, we have $|n^{-s}| = n^{-\sigma}$, and $\sum n^{-\sigma}$ converges by the integral test since $\int_1^{\infty} x^{-\sigma}\,dx = 1/(\sigma - 1) < \infty$. Uniform convergence on $\sigma \geq 1 + \delta$ follows from the Weierstrass M-test with $M_n = n^{-(1+\delta)}$. $\square$

10.2 Euler Product

The deep connection between $\zeta(s)$ and the primes is encoded in the following identity, discovered by Euler in 1737 for real $s > 1$ and extended by Riemann to the complex half-plane.

Theorem 10.3 (Euler product formula)**.** *For $\operatorname{Re}(s) > 1$,*

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

Proof. We give the classical sieve argument. For $\mathrm{Re}(s) > 1$, each factor $(1 - p^{-s})^{-1} = \sum_{k=0}^{\infty} p^{-ks}$ converges absolutely.

Let $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ be the primes in order. Consider the finite product:

$$P_N(s) = \prod_{j=1}^{N} \frac{1}{1 - p_j^{-s}} = \prod_{j=1}^{N} \sum_{k_j=0}^{\infty} p_j^{-k_j s}.$$

Expanding the product, we obtain a sum over all n of the form $n = p_1^{k_1} p_2^{k_2} \cdots p_N^{k_N}$, i.e., all positive integers whose prime factors are among $\{p_1, \ldots, p_N\}$:

$$P_N(s) = \sum_{\substack{n \geq 1 \\ p \mid n \Rightarrow p \leq p_N}} \frac{1}{n^s}.$$

By the fundamental theorem of arithmetic, each such n appears exactly once.

Now we estimate the difference:

$$|\zeta(s) - P_N(s)| = \left| \sum_{\substack{n \geq 1 \\ \exists\, p > p_N,\, p \mid n}} \frac{1}{n^s} \right| \leq \sum_{n > p_N} \frac{1}{n^{\sigma}}.$$

Since $\sigma > 1$, this tail of a convergent series tends to 0 as $N \to \infty$. Hence $P_N(s) \to \zeta(s)$, establishing the product formula. □

Corollary 10.4 ($\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$)**.** *Since each factor $(1-p^{-s})^{-1}$ is nonzero for $\mathrm{Re}(s) > 1$ and the product converges absolutely, we have $\zeta(s) \neq 0$ in this half-plane.*

Corollary 10.5 (Infinitude of primes, analytic proof)**.** *Since $\zeta(s) \to \infty$ as $s \to 1^+$ (the harmonic series diverges), the Euler product $\prod_p (1 - p^{-1})^{-1}$ must be an infinite product, hence there are infinitely many primes.*

10.3 Special Value: $\zeta(2) = \pi^2/6$

The evaluation of $\zeta(2)$ was a famous open problem (the *Basel problem*) solved by Euler in 1735.

Theorem 10.6 (Basel problem)**.** $\zeta(2) = \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

Sketch of proof. Consider the function $f(x) = x^2$ on $[-\pi, \pi]$. Its Fourier series is

$$x^2 = \frac{\pi^2}{3} + 4 \sum_{n=1}^{\infty} \frac{(-1)^n}{n^2} \cos(nx).$$

Setting $x = \pi$, and using $\cos(n\pi) = (-1)^n$, we obtain:

$$\pi^2 = \frac{\pi^2}{3} + 4 \sum_{n=1}^{\infty} \frac{1}{n^2},$$

which gives $\sum_{n=1}^{\infty} n^{-2} = \pi^2/6$.

An alternative elegant proof uses the Weierstrass product for $\sin(\pi x)/(\pi x)$:

$$\frac{\sin(\pi x)}{\pi x} = \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2}\right).$$

Expanding both sides and comparing the coefficient of x^2 yields the result. □

10.4 Dirichlet L-Functions

To study primes in arithmetic progressions, Dirichlet generalised the zeta function using *characters*.

Definition 10.7 (Dirichlet character)**.** A *Dirichlet character modulo* q is a function $\chi\colon \mathbb{Z} \to \mathbb{C}$ satisfying:

1. $\chi(n+q) = \chi(n)$ for all n (periodicity);
2. $\chi(mn) = \chi(m)\chi(n)$ for all m, n (complete multiplicativity);
3. $\chi(n) = 0$ if and only if $\gcd(n, q) > 1$.

The *principal character* χ_0 has $\chi_0(n) = 1$ whenever $\gcd(n, q) = 1$.

Definition 10.8 (Dirichlet L-function)**.** For a Dirichlet character χ and $\mathrm{Re}(s) > 1$,

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

Remark 10.9 (Relation to the zeta function). For the principal character χ_0 modulo q,

$$L(s, \chi_0) = \zeta(s) \prod_{p \mid q} (1 - p^{-s}),$$

so $L(s, \chi_0)$ is essentially $\zeta(s)$ with finitely many Euler factors removed.

10.5 Dirichlet's Theorem on Primes in Arithmetic Progressions

Theorem 10.10 (Dirichlet, 1837)**.** *If a and q are coprime positive integers, then the arithmetic progression*

$$a, \quad a+q, \quad a+2q, \quad a+3q, \quad \ldots$$

contains infinitely many primes. More precisely,

$$\sum_{\substack{p \le x \\ p \equiv a \pmod q}} \frac{1}{p} \sim \frac{1}{\varphi(q)} \ln \ln x \quad \text{as } x \to \infty,$$

where φ is Euler's totient function.

Remark 10.11 (Key idea of the proof). The proof uses the orthogonality of Dirichlet characters to isolate primes in a given residue class: for $\gcd(a, q) = 1$,

$$\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi(a)}\, \chi(n) = \begin{cases} 1 & \text{if } n \equiv a \pmod q, \\ 0 & \text{otherwise.} \end{cases}$$

The critical analytic input is that $L(1, \chi) \neq 0$ for all nonprincipal characters χ. The proof of non-vanishing is the deepest part of the argument, especially for real characters.

10.6 The Prime Number Theorem

Definition 10.12 (Prime-counting function)**.** For $x > 0$, let $\pi(x) = \#\{p \le x : p \text{ is prime}\}$.

The Prime Number Theorem, conjectured independently by Legendre and Gauss in the 1790s, gives the asymptotic law governing the distribution of primes.

Theorem 10.13 (Prime Number Theorem)**.** *As $x \to \infty$,*

$$\pi(x) \sim \frac{x}{\ln x},$$

meaning $\lim_{x \to \infty} \pi(x)/(x/\ln x) = 1$.

The PNT was proved independently by Hadamard and de la Vallée-Poussin in 1896. Both proofs relied on showing that $\zeta(1 + it) \neq 0$ for all real $t \neq 0$ — that is, the zeta function has no zeros on the line $\mathrm{Re}(s) = 1$.

Remark 10.14 (A better approximation: $\mathrm{Li}(x)$). A significantly better approximation to $\pi(x)$ is the *logarithmic integral*:

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t}.$$

Gauss conjectured that $\pi(x) \sim \mathrm{Li}(x)$, and indeed the PNT can be stated as $\pi(x) = \mathrm{Li}(x) + o(x/\ln x)$. The function $\mathrm{Li}(x)$ typically overestimates $\pi(x)$ for "small" x (up to about 10^{316}), but Littlewood showed that $\pi(x) - \mathrm{Li}(x)$ changes sign infinitely often.

Remark 10.15 (Historical significance). The PNT was one of the crowning achievements of 19th-century mathematics. It demonstrated that deep questions about the discrete world of primes could be answered using the continuous methods of complex analysis. In 1949–50, Erdős and Selberg gave "elementary" (i.e., not using complex analysis) proofs, though these are far from simple.

10.7 Chebyshev Functions

Chebyshev introduced two functions that are technically more convenient than $\pi(x)$ for studying the distribution of primes.

Definition 10.16 (Chebyshev functions)**.**

$$\theta(x) = \sum_{p \le x} \ln p,$$
$$\psi(x) = \sum_{p^k \le x} \ln p = \sum_{n \le x} \Lambda(n),$$

where $\Lambda(n)$ is the *von Mangoldt function*: $\Lambda(n) = \ln p$ if $n = p^k$ for some prime p and $k \ge 1$, and $\Lambda(n) = 0$ otherwise.

Proposition 10.17 (Equivalence with PNT)**.** *The following are equivalent:*

1. $\pi(x) \sim x/\ln x$;
2. $\theta(x) \sim x$;
3. $\psi(x) \sim x$.

Remark 10.18 (Why $\psi(x)$ is preferred). The function $\psi(x)$ has a beautiful explicit formula connecting it to the zeros of $\zeta(s)$:

$$\psi(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \ln(2\pi) - \frac{1}{2}\ln(1 - x^{-2}),$$

where the sum is over the nontrivial zeros ρ of $\zeta(s)$. This formula makes precise how the distribution of primes is governed by the zeros of the zeta function.

10.8 The Riemann Hypothesis

The zeta function can be analytically continued to all of $\mathbb{C} \setminus \{1\}$ (with a simple pole at $s = 1$). It satisfies the *functional equation*

$$\pi^{-s/2}\,\Gamma\!\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\,\Gamma\!\left(\frac{1-s}{2}\right)\zeta(1-s).$$

The zeros at $s = -2, -4, -6, \ldots$ are called *trivial zeros*. All other zeros lie in the *critical strip* $0 \leq \mathrm{Re}(s) \leq 1$.

Definition 10.19 (The Riemann Hypothesis)**.** The *Riemann Hypothesis* (RH) asserts that every nontrivial zero of $\zeta(s)$ has real part equal to $1/2$. That is, all nontrivial zeros lie on the *critical line* $\mathrm{Re}(s) = 1/2$.

Remark 10.20 (Consequences of the Riemann Hypothesis). If RH is true, the error in the Prime Number Theorem becomes remarkably sharp:

$$\pi(x) = \mathrm{Li}(x) + O\Big(\sqrt{x}\,\ln x\Big).$$

Among the many other consequences:

- Sharp bounds on gaps between consecutive primes.
- The Lindelöf hypothesis on the growth of $\zeta(1/2 + it)$.
- Improved estimates in the distribution of primes in arithmetic progressions.
- Implications for the distribution of eigenvalues of random matrices.

Remark 10.21 (The Millennium Prize). The Riemann Hypothesis is one of the seven Millennium Prize Problems selected by the Clay Mathematics Institute in 2000, each carrying a prize of \$1,000,000. As of this writing, the RH remains unresolved, despite enormous computational evidence (over 10^{13} nontrivial zeros have been verified to lie on the critical line) and more than 160 years of effort by the world's best mathematicians since Riemann's 1859 memoir.

10.9 Visualising Prime Distribution and the Critical Strip

10.10 Open Problems in Number Theory

We conclude this course by listing several famous unsolved problems, each of which has resisted the efforts of mathematicians for decades or centuries.

Definition 10.22 (Goldbach's conjecture)**.** *Goldbach's conjecture* (1742) asserts that every even integer greater than 2 can be expressed as the sum of two primes.

Despite extensive computational verification (up to at least 4×10^{18}), Goldbach's conjecture remains unproven. The best partial result is due to Helfgott (2013), who proved the *weak* (or ternary) Goldbach conjecture: every odd integer greater than 5 is the sum of three primes.

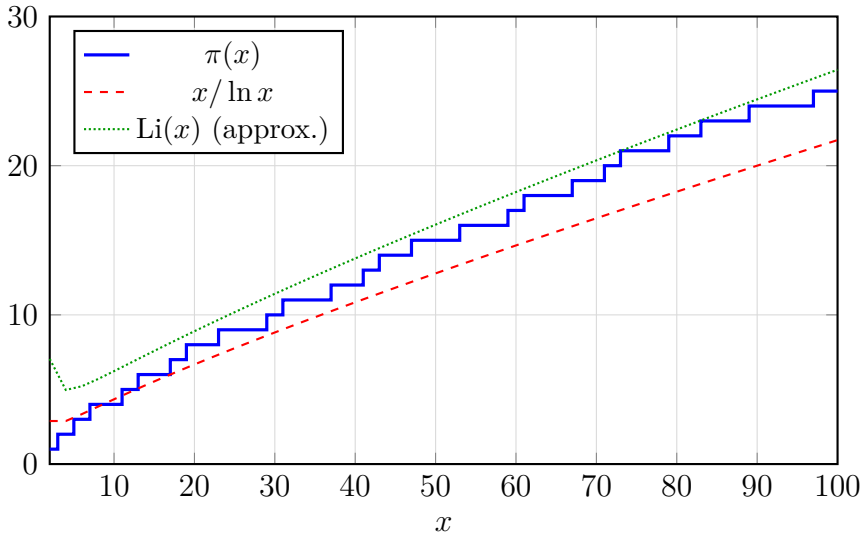


Figure 10.1: Comparison of the prime-counting function $\pi(x)$ (blue step function) with the estimates $x/\ln x$ (red, dashed) and $\mathrm{Li}(x)$ (green, dotted). The logarithmic integral provides a visibly superior approximation.

Definition 10.23 (Twin prime conjecture)**.** The *twin prime conjecture* asserts that there are infinitely many pairs of primes $(p, p+2)$.

A major breakthrough was achieved by Zhang (2013), who proved that there are infinitely many pairs of primes differing by at most 70,000,000. This bound has been reduced to 246 through the collaborative Polymath project, but the gap to 2 remains.

Remark 10.24 (Other notable open problems).

- **Riemann Hypothesis**: discussed in Section 10.8; the most important open problem in mathematics.
- **Birch and Swinnerton-Dyer conjecture**: relates the rank of an elliptic curve to the order of vanishing of its L-function at $s = 1$. Another Millennium Prize problem.
- **Legendre's conjecture**: there is always a prime between n^2 and $(n+1)^2$.
- **Are there infinitely many Mersenne primes?**: primes of the form $2^p - 1$. As of 2024, 51 Mersenne primes are known.
- **Collatz conjecture**: for the map $n \mapsto n/2$ (if even) or $3n+1$ (if odd), does every positive integer eventually reach 1?

10.11 Exercises

Exercise 10.1. Verify the Euler product by computing $\prod_{p \le 7}(1 - p^{-2})^{-1}$ and comparing it with $\sum_{n=1}^{N} n^{-2}$ for a suitable N. How close is your answer to $\pi^2/6$?

Exercise 10.2. Using the identity $\zeta(2) = \pi^2/6$, show that $\zeta(4) = \pi^4/90$. *Hint:* use the Fourier series of x^4 on $[-\pi, \pi]$, or the identity $\zeta(4) = (1/3)\big(\zeta(2)^2 + \zeta(2)\big)$ – correction.

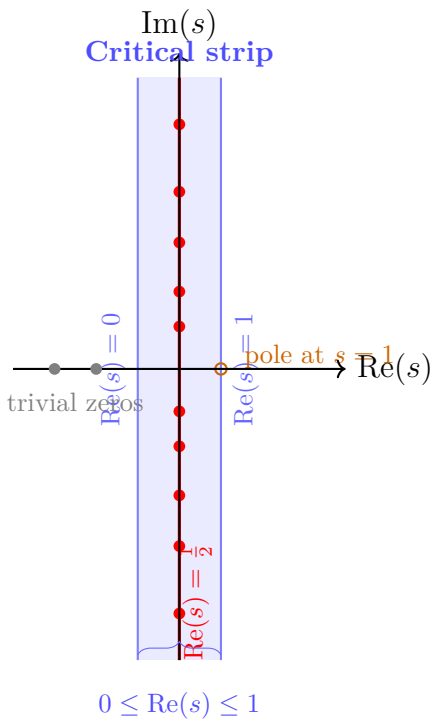


Figure 10.2: The critical strip and the critical line of the Riemann zeta function. The nontrivial zeros (red dots) are shown on the critical line $\operatorname{Re}(s) = 1/2$, as predicted by the Riemann Hypothesis. Trivial zeros (grey dots) lie at $s = -2, -4, \ldots$ on the real axis.

Alternatively, use the product formula for $\sin(\pi x)/(\pi x)$ and compare the x^4 coefficient.

Exercise 10.3. Use Dirichlet's theorem to show that there are infinitely many primes of the form $4k + 3$. Can you give an elementary proof (without L-functions)?

Exercise 10.4. Assuming the PNT, show that the n-th prime p_n satisfies $p_n \sim n \ln n$ as $n \to \infty$.

Exercise 10.5. *Mertens' theorem* states that $\sum_{p \le x} 1/p = \ln \ln x + M + o(1)$, where $M \approx 0.2615$ is the Meissel–Mertens constant. Use this to show that the product $\prod_{p \le x} (1 - 1/p) \sim e^{-\gamma} / \ln x$, where γ is the Euler–Mascheroni constant.

Exercise 10.6. Prove that for all $x \ge 2$,

$$\frac{1}{6} \frac{x}{\ln x} \le \pi(x) \le 6 \frac{x}{\ln x}.$$

Hint: consider $\binom{2n}{n}$ and use the fact that every prime $n < p \le 2n$ divides $\binom{2n}{n}$.

Exercise 10.7. Show that for all $n \ge 1$, $\sum_{d \mid n} \Lambda(d) = \ln n$. Use Möbius inversion to deduce $\Lambda(n) = -\sum_{d \mid n} \mu(d) \ln d$.

Exercise 10.8. Show that $\zeta(s)$ has a simple pole at $s = 1$ with residue 1: $\lim_{s \to 1} (s - 1)\zeta(s) = 1$. *Hint:* compare $\sum n^{-s}$ with $\int_1^\infty x^{-s}\, dx$.

Exercise 10.9. Verify Goldbach's conjecture for all even integers from 4 to 100.

Exercise 10.10 (Challenging)**.** Look up Dirichlet's class number formula and explain how $L(1, \chi)$ for a quadratic character χ relates to the class number of a quadratic number field. What role does the non-vanishing $L(1, \chi) \neq 0$ play?

10.12 Chapter Summary

- The **Riemann zeta function** $\zeta(s) = \sum n^{-s} = \prod_p (1-p^{-s})^{-1}$ encodes the distribution of primes via its Euler product.
- The **Euler product** is proved by expanding geometric series and using unique factorisation; it gives an analytic proof that there are infinitely many primes.
- **Dirichlet L-functions** $L(s,\chi)$ generalise the zeta function and underpin Dirichlet's theorem that every coprime arithmetic progression contains infinitely many primes.
- The **Prime Number Theorem** states $\pi(x) \sim x/\ln x$; the better approximation $\mathrm{Li}(x) = \int_2^x dt/\ln t$ captures finer behaviour.
- The **Chebyshev functions** $\theta(x)$ and $\psi(x)$ provide technically convenient equivalents of the PNT, with $\psi(x)$ directly connected to the zeros of $\zeta(s)$.
- The **Riemann Hypothesis** — that all nontrivial zeros of ζ lie on $\mathrm{Re}(s) = 1/2$ — remains the most important open problem in mathematics, with profound implications for prime distribution.
- Famous open problems including **Goldbach's conjecture**, the **twin prime conjecture**, and the **RH** illustrate that number theory remains a vibrant and active field of research.

Bibliography

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1976.

[2] H. Davenport, *Multiplicative Number Theory*, 3rd ed., revised by H. L. Montgomery, Graduate Texts in Mathematics 74, Springer-Verlag, New York, 2000.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, Oxford, 2008.

[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics 84, Springer-Verlag, New York, 1990.

[5] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Graduate Texts in Mathematics 58, Springer-Verlag, New York, 1984.

[6] M. B. Nathanson, *Elementary Methods in Number Theory*, Graduate Texts in Mathematics 195, Springer-Verlag, New York, 2000.

[7] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, New York, 1991.

[8] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag, New York, 1973.

Index