Algebra IIIc: Number Theory (Structures)

Gudfit

Contents

0 Algebraic Foundations 4
- 0.1 The Integers 4
- 0.2 Polynomials 8
- 0.3 Divisibility and Ideals in $\mathbb{Z}$ 10
- 0.4 Exercises 13

1 Greatest Common Divisor and Least Common Multiple 16
- 1.1 GCD 16
- 1.2 Euclid's Algorithm 19
- 1.3 Prime Numbers and Unique Factorisation 21
- 1.4 Exercises 25

2 Congruences 29
- 2.1 The Congruence Relation 29
- 2.2 Residue Classes 34
- 2.3 Reduced Residue Systems 36
- 2.4 Linear Congruences and Inverses 37
- 2.5 Exercises 41

3 The Multiplicative Group of Integers 43
- 3.1 The Ring Structure of $\mathbb{Z}/n\mathbb{Z}$ 43
- 3.2 Theorems of Fermat and Euler 46
- 3.3 Exercises 51

4 Polynomial Congruences and Systems 53
- 4.1 Polynomial Congruences Modulo p 53
- 4.2 Systems of Linear Congruences 56
- 4.3 Applications 62
- 4.4 Exercises 64

5 Primitive Roots and Group Structure 68
- 5.1 The Order of an Integer 68
- 5.2 Primitive Roots Modulo Primes 69
- 5.3 Classification and Non-Existence 72
- 5.4 Discrete Logarithms 74
- 5.5 The Structure of $(\mathbb{Z}/2^k\mathbb{Z})^\times$ 76
- 5.6 Exercises 79

6 *Quadratic Residues* 83
- 6.1 *Quadratic Congruences* 83
- 6.2 *The Legendre Symbol* 85
- 6.3 *Gauss's Lemma* 88
- 6.4 *The Law of Quadratic Reciprocity* 90
- 6.5 *Exercises* 93

7 *Indeterminate Equations* 97
- 7.1 *The Jacobi Symbol* 97
- 7.2 *Local Solvability and the Hasse Principle* 100
- 7.3 *Pythagorean Triples* 103
- 7.4 *Fermat's Equation* 104
- 7.5 *Sum of Two Squares* 106
- 7.6 *Sums of Three and Four Squares* 109
- 7.7 *Generalisations: Waring's Problem and Universal Forms* 112
- 7.8 *Exercises* 114

A *Appendix: Pell's Equation* 117
- A.1 *The Equation and Quadratic Rings* 117
- A.2 *Structure of Solutions* 120
- A.3 *Existence of Solutions* 121
- A.4 *Exercises* 125

B *Appendix: Continued Fractions and Approximation* 126
- B.1 *Rational Continued Fractions* 126
- B.2 *Infinite Continued Fractions* 127
- B.3 *Best Approximations* 129
- B.4 *Connection to Pell's Equation* 131
- B.5 *Transcendence and Liouville's Theorem* 132
- B.6 *Exercises* 133

C *Appendix: Primes in Arithmetic Progressions* 135
- C.1 *Elementary Cases* 135
- C.2 *Cyclotomic Polynomials* 137
- C.3 *Arithmetic Functions and M"obius Inversion* 138
- C.4 *Exercises* 138

D *Appendix: Distribution of Prime Numbers* 139
- D.1 *Asymptotic Notation and Chebychev's Bounds* 139
- D.2 *The Brun-Titchmarsh Theorem and Selberg Sieve* 140
- D.3 *Exercises* 140

0
Algebraic Foundations

We begin by establishing the fundamental algebraic structures that underpin the study of Number Theory and Linear Algebra. We denote the set of *positive integers* (or *natural numbers*) by $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$. While the rigorous construction of these numbers via the Peano axioms is foundational, we shall restrict our attention to their operational and order-theoretic properties.

0.1 The Integers

Addition and multiplication are well-defined operations on $\mathbb{Z}^+$. For any $a, b \in \mathbb{Z}^+$, their sum $a + b$ and product ab satisfy the following fundamental laws:

> **Axiom 1.** ***Associativity of Addition.***
> For all $a, b, c \in \mathbb{Z}^+$, $(a + b) + c = a + (b + c)$.
>
> 公理

> **Axiom 2.** ***Commutativity of Addition.***
> For all $a, b \in \mathbb{Z}^+$, $a + b = b + a$.
>
> 公理

> **Axiom 3.** ***Associativity of Multiplication.***
> For all $a, b, c \in \mathbb{Z}^+$, $(ab)c = a(bc)$.
>
> 公理

> **Axiom 4.** ***Commutativity of Multiplication.***
> For all $a, b \in \mathbb{Z}^+$, $ab = ba$.
>
> 公理

> **Axiom 5.** ***Distributivity.***
> For all $a, b, c \in \mathbb{Z}^+$, $a(b + c) = ab + ac$.
>
> 公理

Axiom 6. ***Multiplicative Identity.***
There exists an element $1 \in \mathbb{Z}^+$ such that for all $a \in \mathbb{Z}^+$, $a \cdot 1 = a$.

公理

The set $\mathbb{Z}^+$ is also endowed with a strict total ordering, denoted by $<$. For any $a, b \in \mathbb{Z}^+$, exactly one of the following holds:

$$a < b, \quad a = b, \quad \text{or} \quad b < a.$$

This order respects the arithmetic operations:

(i) If $a < b$, then $a + c < b + c$ for any c.
(ii) If $a < b$, then $ac < bc$ for any c.
(iii) If $a < b$ and $b < c$, then $a < c$ (Transitivity).

The structural essence of the positive integers is captured by the Induction Axiom.

Axiom 7. ***Induction Axiom.***
Let $S \subseteq \mathbb{Z}^+$. If S satisfies:
(i) $1 \in S$, and
(ii) For any $k \in \mathbb{Z}^+$, $k \in S \implies k + 1 \in S$,
then $S = \mathbb{Z}^+$.

公理

This axiom provides the basis for the First Principle of Mathematical Induction.

Theorem 0.1. ***First Principle of Mathematical Induction.***
Let $P(n)$ be a proposition regarding positive integers. If:
(i) $P(1)$ is true, and
(ii) $P(k) \implies P(k+1)$ for any $k \in \mathbb{Z}^+$,
then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

定理

An equivalent and equally powerful property of $\mathbb{Z}^+$ is the existence of minimal elements in non-empty subsets. To establish this, we first state a preliminary result.

Lemma 0.1. Lower Bound Property If a subset $S \subseteq \mathbb{Z}^+$ has no least element, then for every $n \in \mathbb{Z}^+$, $n \notin S$.

引理

Proof

We proceed by induction on n. If $1 \in S$, then 1 would be the least element (as $1 \leq x$ for all $x \in \mathbb{Z}^+$), contradicting our hypothesis. Thus $1 \notin S$. Assume $1, 2, \ldots, k \notin S$. If $k + 1 \in S$, then since all integers smaller than $k+1$ are not in S, $k+1$ would be the least element of S, again a contradiction. Thus $k + 1 \notin S$. By the induction axiom, $S = \emptyset$.

■

Theorem 0.2. ***Least Number Principle.***
Let S be a non-empty subset of $\mathbb{Z}^+$. Then there exists $m \in S$ such that for all $x \in S$, $m \leq x$. We call m the least element of S.

定理

Proof

Suppose S has no least element. By the preceding lemma, $n \notin S$ for all $n \in \mathbb{Z}^+$, which implies S is empty. This contradicts the assumption that S is non-empty. Thus, S must possess a least element.

■

Conversely, if a set is bounded from above, it possesses a maximal element.

Theorem 0.3. ***Greatest Number Principle.***
Let $S \subseteq \mathbb{Z}^+$ be non-empty. If S has an upper bound (i.e., there exists $M \in \mathbb{Z}^+$ such that $x \leq M$ for all $x \in S$), then there exists $g \in S$ such that for all $x \in S$, $x \leq g$.

定理

The *Least Number Principle* allows us to establish the Second Principle of Mathematical Induction (often called Strong Induction), which is frequently more useful when the recursive step depends on multiple preceding terms.

Theorem 0.4. ***Second Principle of Mathematical Induction.***
Let $P(n)$ be a proposition regarding positive integers. If:

(i) $P(1)$ is true, and
(ii) For any $k \in \mathbb{Z}^+$, if $P(j)$ holds for all $1 \leq j \leq k$, then $P(k+1)$ holds,

then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

定理

By adjoining the neutral element 0 and the additive inverses (negative integers) to $\mathbb{Z}^+$, we obtain the set of integers, denoted by $\mathbb{Z}$. The addition operation extends to $\mathbb{Z}$ such that $a + 0 = a$ for all a, and for every $a \in \mathbb{Z}$, there exists a unique element $-a$ such that $a + (-a) = 0$. This allows for the definition of subtraction: $a - b = a + (-b)$. We formalise the algebraic structure of $\mathbb{Z}$ using the language of abstract algebra.

Definition 0.1. ***Group.***
A set G equipped with a binary operation $\cdot$ is called a *group* if it satisfies:

(i) **Associativity:** For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(ii) **Identity:** There exists an element $e \in G$ (often denoted 1) such

that for all $a \in G$, $a \cdot e = e \cdot a = a$.

(iii) **Inverses:** For every $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

If the operation is also commutative (i.e., $a \cdot b = b \cdot a$ for all $a, b \in G$), the group is called *abelian*.

定義

Definition 0.2. ***Additive Group.***
A set G equipped with an operation $+$ is called an additive group if it satisfies:

(i) Associativity and Commutativity of $+$.
(ii) Existence of an identity element 0.
(iii) Existence of additive inverses for every element.

Thus, $\mathbb{Z}$ forms an additive group.

定義

Definition 0.3. ***Commutative Ring.***
A set R equipped with addition $(+)$ and multiplication $(\cdot)$ is called a commutative ring if:

(i) R is an additive group under $+$.
(ii) Multiplication is associative and commutative.
(iii) Multiplication distributes over addition: $a(b + c) = ab + ac$.
(iv) There exists a multiplicative identity 1.

定義

Definition 0.4. ***Zero Divisors and Integral Domains.***
Let R be a commutative ring. A non-zero element $a \in R$ is called a *zero divisor* if there exists a non-zero element $b \in R$ such that $ab = 0$. A commutative ring that contains no zero divisors is called an *integral domain*.

定義

The set of integers $\mathbb{Z}$ is an integral domain. Furthermore, $\mathbb{Z}$ possesses a crucial property regarding products: $ab = 0$ if and only if $a = 0$ or $b = 0$. Consequently, the cancellation law holds in $\mathbb{Z}$: if $ab = ac$ and $a \neq 0$, then $b = c$.
The order properties of $\mathbb{Z}^+$ extend naturally to $\mathbb{Z}$. We also define the absolute value function $|\cdot| : \mathbb{Z} \to \mathbb{Z}^+ \cup \{0\}$ by:

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0 \end{cases}$$

The absolute value satisfies the Triangle Inequality:

$$|a + b| \leq |a| + |b|. \tag{1}$$

Definition 0.5. ***Floor Function.***
For any real number x, the *floor function* (or integer part), denoted by $\lfloor x \rfloor$, is defined as the largest integer n such that $n \leq x$. That is, $\lfloor x \rfloor \in \mathbb{Z}$ and $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

定義

The set of rational numbers is defined as $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$, where $p/q = r/s$ if and only if $ps = qr$. The integers are embedded in $\mathbb{Q}$ by identifying n with $n/1$. In $\mathbb{Q}$, every non-zero element x possesses a multiplicative inverse x^{-1} such that $x \cdot x^{-1} = 1$.
This property distinguishes $\mathbb{Q}$ from $\mathbb{Z}$.

Definition 0.6. ***Field.***
A set F is called a field if:

(i) F is a commutative ring.

(ii) For every $a \in F \setminus \{0\}$, there exists a multiplicative inverse $a^{-1} \in F$.

In other words, a field is a structure where addition, subtraction, multiplication, and division (by non-zero divisors) are well-defined.

定義

Thus, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields, whereas $\mathbb{Z}$ is not. We call $\mathbb{Q}$ the field of quotients of $\mathbb{Z}$.
The real numbers $\mathbb{R}$ may be constructed as the completion of $\mathbb{Q}$ (via Cauchy sequences or Dedekind cuts), enabling the treatment of limits. The complex numbers $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ extend $\mathbb{R}$ to an *algebraically closed field*, meaning that every non-constant polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$. We recall Euler's formula, which connects the exponential function to trigonometry:

$$e^{i\theta} = \cos\theta + i\sin\theta,$$

where θ is the argument of the complex number.
Since $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, we say that $\mathbb{R}$ is an *extension field* of $\mathbb{Q}$, and $\mathbb{C}$ is an extension field of $\mathbb{R}$ (in general, a field E is an extension of F if F is a subfield of E).

0.2 Polynomials

Let K represent a field (such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$). A univariate polynomial over K is a formal expression of the form:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \tag{2}$$

where n is a non-negative integer and the coefficients a_i belong to K.
The symbol x is called an *indeterminate*. It is not an unknown number

to be solved for, but a formal symbol that commutes with elements of K and satisfies the laws of exponents.
The set of all such polynomials is denoted by $K[x]$.

Definition 0.7. ***Degree and Terms.***
Consider the polynomial in *Equation 2*.
- The term $a_k x^k$ is the term of degree k.
- $a_n x^n$ is the *leading term* and a_n is the *leading coefficient*, provided $a_n \neq 0$.
- The degree of $f(x)$, denoted $\deg(f)$, is the largest integer n such that $a_n \neq 0$.

Two polynomials are equal if and only if the coefficients of terms of the same degree are identical. The polynomial with all coefficients equal to zero is the *zero polynomial*, denoted by 0. Its degree is undefined.

定義

Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{j=0}^{m} b_j x^j$. We define addition and multiplication as follows:
Addition: $f(x) + g(x) = \sum (a_k + b_k) x^k$, where we assume $a_k = 0$ for $k > n$ and $b_k = 0$ for $k > m$.
Multiplication: $f(x)g(x) = \sum_k c_k x^k$, where $c_k = \sum_{i+j=k} a_i b_j$.
Under these operations, $K[x]$ forms a commutative ring. The additive identity is the zero polynomial, and the multiplicative identity is the constant polynomial 1. Unlike functions in calculus, where equality depends on the values taken, in algebra, polynomial equality is purely structural (coefficient-wise).

Example 0.1. Univariate Polynomial Addition. Consider the polynomials $f(x) = 3x^2 + 2x + 5$ and $g(x) = 4x - 1$ in the ring $\mathbb{Q}[x]$. Their sum is calculated by combining coefficients of terms with matching degrees: $f(x) + g(x) = 3x^2 + (2 + 4)x + (5 - 1) = 3x^2 + 6x + 4$.

範例

We extend these concepts to polynomials in n indeterminates $x_1, \ldots, x_n$. The set of all such *multivariate polynomials* is denoted by $K[x_1, \ldots, x_n]$. A monomial is an expression of the form $a x_1^{k_1} \ldots x_n^{k_n}$, where $a \in K$ and k_i are non-negative integers. An n-variate polynomial is a finite formal sum of monomials.
Addition and subtraction are performed by combining coefficients of like terms (monomials with identical exponents for all indeterminates). Multiplication is defined distributively: the product of two polynomials is the sum of the products of their constituent monomials, where

$$(x_1^{p_1} \ldots x_n^{p_n}) \cdot (x_1^{q_1} \ldots x_n^{q_n}) = x_1^{p_1+q_1} \ldots x_n^{p_n+q_n}.$$

The set $K[x_1, \ldots, x_n]$ also forms a commutative ring.

Example 0.2. Multivariate Polynomial Multiplication. Consider the polynomials $f(x,y) = x + 2y$ and $g(x,y) = 3x - y$ in $\mathbb{R}[x,y]$. The product is obtained by distributing the terms: $(x + 2y)(3x - y) = x(3x) + x(-y) + 2y(3x) + 2y(-y) = 3x^2 - xy + 6xy - 2y^2 = 3x^2 + 5xy - 2y^2$.

範例

0.3 *Divisibility and Ideals in $\mathbb{Z}$*

While addition, subtraction, and multiplication are always defined within $\mathbb{Z}$, division is not. That is, for integers a and b with $b \neq 0$, the quotient $\frac{a}{b}$ is not necessarily an integer. This observation gives rise to the fundamental concept of divisibility in number theory.

Definition 0.8. ***Divisibility.***
Let $a, b \in \mathbb{Z}$ with $b \neq 0$. We say that b *divides* a, denoted $b \mid a$, if there exists an integer c such that $a = bc$. In this case, b is called a divisor or factor of a, and a is a multiple of b. If no such integer c exists, then b does not divide a, denoted $b \nmid a$.

定義

Remark (Divisor Search and Order Comparison).

To determine the set of all positive divisors of $a \in \mathbb{Z}^+$, it is sufficient to examine integers in the interval $[1, \sqrt{a}]$. Furthermore, while the strict total ordering of $\mathbb{Z}$ satisfies trichotomy, the divisibility relation does not. For integers $a, b \in \mathbb{Z}^+$, it is possible that $a \nmid b$, $b \nmid a$, and $a \neq b$, as exemplified by the set $\{2, 7\}$.

From this definition, several basic properties of divisibility follow directly.

Theorem 0.5. ***Properties of Divisibility.***
Let $a, b, c \in \mathbb{Z}$.

(i) If $b \mid a$ and $a \mid c$, then $b \mid c$.
(ii) If $b \mid a$, then $b \mid ca$ for any $c \in \mathbb{Z}$.
(iii) If $c \mid a$ and $c \mid b$, then $c \mid (xa + yb)$ for any integers $x, y \in \mathbb{Z}$. This property indicates that any integer linear combination of multiples of c is also a multiple of c.
(iv) If $b \mid a$ and $a \neq 0$, then $|b| \leq |a|$. Consequently, if $a \mid b$ and $b \mid a$, then $a = \pm b$. If additionally $a, b \in \mathbb{Z}^+$, then $a = b$.

定理

Proof

(i) If $b \mid a$, then $a = bk$ for some $k \in \mathbb{Z}$. If $a \mid c$, then $c = al$ for some $l \in \mathbb{Z}$. Substituting a, we get $c = (bk)l = b(kl)$. Since $kl \in \mathbb{Z}$, we conclude $b \mid c$.

(ii) If $b \mid a$, then $a = bk$ for some $k \in \mathbb{Z}$. Then $ca = c(bk) = b(ck)$. Since $ck \in \mathbb{Z}$, we conclude $b \mid ca$.

(iii) If $c \mid a$, then $a = ck$ for some $k \in \mathbb{Z}$. If $c \mid b$, then $b = cl$ for some $l \in \mathbb{Z}$. Then for any integers x, y, $xa + yb = x(ck) + y(cl) = c(xk + yl)$. Since $xk + yl \in \mathbb{Z}$, we conclude $c \mid (xa + yb)$.

(iv) If $b \mid a$ and $a \neq 0$, then $a = bk$ for some $k \in \mathbb{Z}$. Since $a \neq 0$, we must have $k \neq 0$. Thus $|k| \geq 1$. Taking absolute values, $|a| = |b||k|$. As $|k| \geq 1$, it follows that $|a| \geq |b|$. If $a \mid b$ and $b \mid a$, then $|a| \leq |b|$ and $|b| \leq |a|$. This implies $|a| = |b|$, so $a = \pm b$. If $a, b \in \mathbb{Z}^+$, then $a = b$.

■

The cornerstone of integer arithmetic is the Division Algorithm, which formalises the process of division with a remainder.

Theorem 0.6. ***The Division Algorithm.***
Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$. Then there exist unique integers q and r such that $a = qb + r$, where $0 \leq r < b$.

定理

Proof

We first prove the existence of q and r. Consider the set $S = \{a - xb \mid x \in \mathbb{Z}, a - xb \geq 0\}$. If $a \geq 0$, then choosing $x = 0$ yields $a \in S$, so S is non-empty. If $a < 0$, we can choose x such that $a - xb \geq 0$. For instance, if $b = 1$, $a - x \geq 0 \implies x \leq a$. We can choose $x = a$ to get $0 \in S$. More generally, choose x such that $xb \leq a$. For $a < 0$, we can choose a sufficiently negative x. For example, $x = a - 1$ implies $a - (a - 1)b = a - ab + b$. If a is negative, say $a = -5$ and $b = 2$, then $a - (a - 1)b = -5 - (-6)2 = -5 + 12 = 7 \geq 0$. So S is always non-empty.

Since S is a non-empty subset of non-negative integers (which can be viewed as $\mathbb{Z}^+ \cup \{0\}$), by the *Least Number Principle* (extended to include o), S has a least element, say r. By definition of S, $r = a - qb$ for some integer q, and $r \geq 0$. We must show that $r < b$. Assume, for contradiction, that $r \geq b$. Then $r - b \geq 0$. We can write $r - b = (a - qb) - b = a - (q + 1)b$. Since $r - b \geq 0$, $r - b$ is an element of S. However, $r - b < r$ (because $b > 0$), which contradicts the choice of r as the least element of S. Thus, our assumption $r \geq b$ must be false, so $r < b$. This establishes existence.

For uniqueness, suppose there exist two such pairs (q_1, r_1) and (q_2, r_2) satisfying the conditions: $a = q_1 b + r_1$, with $0 \leq r_1 < b$, and

$a = q_2b + r_2$, with $0 \leq r_2 < b$. Subtracting the two equations gives $0 = (q_1 - q_2)b + (r_1 - r_2)$. Thus, $r_2 - r_1 = (q_1 - q_2)b$. This implies that $b \mid (r_2 - r_1)$. From $0 \leq r_1 < b$ and $0 \leq r_2 < b$, it follows that $-b < r_2 - r_1 < b$. The only multiple of b that lies strictly between $-b$ and b is 0. Therefore, $r_2 - r_1 = 0$, which means $r_1 = r_2$. Substituting $r_1 = r_2$ back into $r_2 - r_1 = (q_1 - q_2)b$, we get $0 = (q_1 - q_2)b$. Since $b \neq 0$, we must have $q_1 - q_2 = 0$, so $q_1 = q_2$. Hence, q and r are unique.

■

Remark (Quotient and Remainder).

In *Theorem 0.6*, q is called the quotient and r is the remainder when a is divided by b. The condition $r = 0$ signifies that a is divisible by b.

A direct consequence of *Theorem 0.6* is that any integer can be classified by its remainder upon division by a given positive integer. For instance, integers divided by 2 yield remainders of 0 or 1. Those with remainder 0 are even, and those with remainder 1 are odd. Similarly, for division by 3, any integer n can be expressed in one of three forms: $3k$, $3k + 1$, or $3k + 2$, for some integer k.
The concept of divisibility leads naturally to the study of subsets of $\mathbb{Z}$ with particular closure properties.

Definition 0.9. ***Ideal.***
A non-empty subset I of a ring R is called an *ideal* of R if:

(i) For any $a, b \in I$, $a - b \in I$ (closure under subtraction).

(ii) For any $a \in I$ and $r \in R$, $ra \in I$ (closure under multiplication by ring elements).

定義

For the ring of integers $\mathbb{Z}$, the second condition implies closure under multiplication by any integer. From the first condition, if I is non-empty, let $a \in I$. Then $a - a = 0 \in I$. For any $a \in I$, $0 - a = -a \in I$. And if $a, b \in I$, then $a - (-b) = a + b \in I$, so I is also closed under addition. Combined, I is an additive subgroup of $\mathbb{Z}$.

Theorem 0.7. ***Structure of Ideals in $\mathbb{Z}$.***
Let I be a non-empty ideal of $\mathbb{Z}$. Then there exists a unique non-negative integer d such that I consists of all multiples of d. That is, $I = \{kd \mid k \in \mathbb{Z}\}$. We denote this ideal as $\langle d \rangle$.

定理

Proof

If $I = \{0\}$, then we can take $d = 0$, and $I = \{k \cdot 0 \mid k \in \mathbb{Z}\} = \{0\}$. In this case, $d = 0$ is uniquely determined.
Now, suppose $I \neq \{0\}$. Since I is non-empty and contains non-zero

elements, and if $x \in I$ then $-x \in I$, it must contain positive integers. By the *Least Number Principle*, there exists a smallest positive integer in I. Let this smallest positive integer be d.
We claim that $I = \{kd \mid k \in \mathbb{Z}\}$. First, consider any multiple of d, say kd for $k \in \mathbb{Z}$. By the second property of an ideal (closure under multiplication by ring elements), since $d \in I$ and $k \in \mathbb{Z}$, $kd \in I$. So, $\{kd \mid k \in \mathbb{Z}\} \subseteq I$.
Conversely, let a be an arbitrary element of I. By *Theorem 0.6*, since $d \in \mathbb{Z}^+$, we can write $a = qd + r$ for unique integers q, r such that $0 \leq r < d$. Since $a \in I$ and $qd \in I$ (as shown above), and I is closed under subtraction, it follows that $r = a - qd \in I$. However, d was chosen as the *smallest positive integer* in I. Since $r \in I$ and $0 \leq r < d$, for r not to contradict the minimality of d, r must be 0. Thus, $a = qd$, which means a is a multiple of d. This shows that $I \subseteq \{kd \mid k \in \mathbb{Z}\}$.
Combining both inclusions, we have $I = \{kd \mid k \in \mathbb{Z}\}$. The uniqueness of d follows from its definition as the smallest positive integer in I. If there were another such non-negative integer d', it would also be the smallest positive element, thus $d' = d$.

■

Remark (Principal Ideal Ring).

An ideal generated by a single element, such as $\langle d \rangle = \{kd \mid k \in \mathbb{Z}\}$, is called a *principal ideal*. *Theorem 0.7* demonstrates that every ideal in $\mathbb{Z}$ is a principal ideal. For this reason, $\mathbb{Z}$ is known as a *principal ideal domain*, or PID, a concept we shall revisit in ring theory.

0.4 Exercises

1. **Power Inheritance.** Let $a, b \in \mathbb{Z}$, with $a \neq 0$, and let k be a positive integer. Prove that if $a \mid b$, then $a \mid b^k$.
2. **Common Remainders.** Let n be a positive integer. We say two integers a and b are related if n divides their difference $a - b$.
   (i) Prove that $n \mid (a - b)$ if and only if a and b leave the same remainder when divided by n (as per the Division Algorithm).
   (ii) Let a be an odd integer. Prove that 8 divides $a^2 - 1$.
3. **Cubic Divisibility and Sums.**
   (i) Prove that for any integer n, $n^3 - n$ is divisible by 6.
   (ii) If $n^3 - n$ is divisible by 6, does it strictly follow that n itself is divisible by 6? Provide a proof or a counter-example.
   (iii) Using the result in (i), prove that if the sum of integers $a_1, a_2, \ldots, a_k$ is divisible by 6, then the sum of their cubes

$a_1^3 + \cdots + a_k^3$ is also divisible by 6.

4. **Squares of Odd Integers.** Let $a, b \in \mathbb{Z}$ be odd. Prove that $a^2 - b^2$ is divisible by 8.

5. **Counting Multiples.** The notation $\lfloor x \rfloor$ denotes the largest integer not exceeding x (i.e., $x - 1 < \lfloor x \rfloor \leq x$). Let $n, k \in \mathbb{Z}^+$. Prove that the number of elements in the set $\{1, 2, \ldots, n\}$ that are divisible by k is exactly $\lfloor n/k \rfloor$.

6. **The Quotient Formula.**
   (i) Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$. Using the Division Algorithm ($a = qb + r$ with $0 \leq r < b$), prove that the quotient is given explicitly by $q = \lfloor a/b \rfloor$.
   (ii) Derive a similar expression for q when b is a negative integer.

7. **Parity and Quadratic Residues.** Let $n \in \mathbb{Z}$.
   (i) Prove that n can be uniquely represented as $n = 2q + r$ where $r \in \{0, 1\}$.
   (ii) Prove that if n leaves a remainder r when divided by 2, then n^2 leaves a remainder r^2 when divided by 4. Conclude that a perfect square leaves a remainder of either 0 or 1 when divided by 4.

8. **Quintic Divisibility.** Prove that $n^5 - n$ is divisible by 30 for any integer n.

9. **Septic Divisibility.** Prove that $n^7 - n$ is divisible by 42 for any integer n.

10. **Integral Harmonic Sums.** Let $n > 1$ be an odd integer. Prove that the integer

$$S = \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n-1}\right)(n-1)!,$$

where $(n-1)!$ denotes the factorial product $1 \cdot 2 \cdot \cdots \cdot (n-1)$, is divisible by n.

11. **Exponential Non-Divisibility.** Let m, n be positive integers with $m > 2$. Prove that $2^m - 1$ does not divide $2^n + 1$.

12. **Base-q Representation.** Let $q > 1$ be an integer.
    (i) Prove that any positive integer n can be uniquely represented in the form:

$$n = a_k q^k + a_{k-1} q^{k-1} + \cdots + a_1 q + a_0,$$

where each coefficient satisfies $0 \leq a_i \leq q - 1$ and $a_k \neq 0$.

(ii) Prove that the coefficients are given explicitly by the formula:

$$a_i = \left\lfloor \frac{n}{q^i} \right\rfloor - q \left\lfloor \frac{n}{q^{i+1}} \right\rfloor.$$

13. Inequalities of the Integer Part. Let x, y, α, β be real numbers and n be a positive integer. Prove the following properties of the floor function:

(i) For any real numbers $a_1, \ldots, a_n$:

$$\sum_{i=1}^{n} \lfloor a_i \rfloor \leq \left\lfloor \sum_{i=1}^{n} a_i \right\rfloor \leq \sum_{i=1}^{n} \lfloor a_i \rfloor + n - 1.$$

(ii) $\lfloor 2\alpha \rfloor + \lfloor 2\beta \rfloor \geq \lfloor \alpha \rfloor + \lfloor \beta \rfloor + \lfloor \alpha + \beta \rfloor$.

14. Hermite's Identity. Prove that for any real number x and any integer $n \geq 2$:

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n} \right\rfloor = \lfloor nx \rfloor.$$

15. ⋆ The Euclidean Ideal. Let a and b be integers, not both zero. Consider the set of all integer linear combinations of a and b:

$$I = \{ax + by \mid x, y \in \mathbb{Z}\}.$$

(a) Prove that I is an ideal of $\mathbb{Z}$.
(b) By *Theorem 0.7*, I is generated by a unique positive integer d (i.e., $I = \langle d \rangle$). Prove that d divides both a and b.
(c) Prove that if c is any integer such that $c \mid a$ and $c \mid b$, then $c \mid d$.

16. ⋆ Polynomial Integrity. Let K be a field and let $f(x), g(x) \in K[x]$ be non-zero polynomials with degrees n and m respectively.

(a) Prove that the degree of the product $f(x)g(x)$ is exactly $n + m$.
(b) Deduce that the ring of polynomials $K[x]$ contains no zero divisors. That is, if $f(x)g(x) = 0$, then either $f(x) = 0$ or $g(x) = 0$.

1

Greatest Common Divisor and Least Common Multiple

We now turn to the constructive aspects of divisibility for a finite collection of integers. Let $a_1, a_2, \ldots, a_n$ be integers, not all of which are zero.

1.1 GCD

Definition 1.1. ***Greatest Common Divisor.***
The greatest common divisor of $a_1, \ldots, a_n$, denoted by $(a_1, \ldots, a_n)$, is the unique integer d satisfying:
Common Divisor: $d \mid a_k$ for all $k = 1, \ldots, n$.
Maximality: If d' is any positive integer such that $d' \mid a_k$ for all k, then $d' \leq d$.
Since the set of positive common divisors is finite (bounded by $\min |a_k|$ where $a_k \neq 0$) and includes 1, the greatest common divisor exists. Furthermore, if d is a common divisor, so is $-d$; thus, the greatest common divisor is always a positive integer.

定義

Definition 1.2. ***Coprimality.***
Integers $a_1, \ldots, a_n$ are said to be *coprime* (or relatively prime) if $(a_1, \ldots, a_n) = 1$. They are said to be *pairwise coprime* if $(a_i, a_j) = 1$ for all $i \neq j$. Clearly, pairwise coprimality implies coprimality, but the converse does not hold.

定義

Example 1.1. Coprimality versus Pairwise Coprimality. Consider the set of integers $\{6, 10, 15\}$. The greatest common divisor of the set is $(6, 10, 15) = 1$, which satisfies the condition for the integers to be coprime. However, the pairs within the set are not coprime:

$$(6, 10) = 2$$
$$(6, 15) = 3$$
$$(10, 15) = 5.$$

Since there exists at least one pair (i, j) such that $(a_i, a_j) > 1$, the set

is not pairwise coprime.

範例

The greatest common divisor exhibits several elementary invariance properties.

Theorem 1.1. ***Basic Properties of GCD.***
Let $a, b, \ldots, c$ be integers.

(i) **Sign Invariance:** $(a, b, \ldots, c) = (|a|, |b|, \ldots, |c|)$.
(ii) **Symmetry:** The value is independent of the order of the arguments.
(iii) **Idempotence:** If $a \neq 0$, then $(a, a, \ldots, a) = |a|$.
(iv) **Linearity:** For any integers $x, \ldots, y$,

$$(a, b, \ldots, c) = (a, b + ax, \ldots, c + ay).$$

In particular, $(a, b) = (a, b + a)$.

定理

Proof

Properties (1)-(3) follow directly from the definition. For (4), let $d = (a, b, \ldots, c)$ and $d' = (a, b + ax, \ldots, c + ay)$. Since d divides $a, b, \ldots, c$, it divides any linear combination of them. Thus $d \mid (b + ax)$, and so d is a common divisor of the set in the right-hand side. Hence $d \leq d'$. Conversely, since a is in the set, d' divides a. Thus d' divides $b = (b + ax) - x(a)$. It follows that d' is a common divisor of the original set, so $d' \leq d$. Therefore $d = d'$.

■

The following theorem connects the geometric notion of the GCD with the algebraic structure of ideals in $\mathbb{Z}$.

Theorem 1.2. ***GCD as a Linear Combination.***
Let $a_1, \ldots, a_n$ be integers, not all zero. The set of all integer linear combinations

$$S = \{a_1 x_1 + \cdots + a_n x_n \mid x_i \in \mathbb{Z}\}$$

consists exactly of all multiples of $d = (a_1, \ldots, a_n)$. That is, $S = \langle d \rangle$.

定理

Proof

The set S is closed under subtraction and multiplication by integers. Since some $a_j \neq 0$, we have $a_j \in S$ and hence $|a_j| \in S$, so S has a positive element. By *Theorem 0.7*, S is a principal ideal generated by its smallest positive element, say D. Thus $S = \{kD \mid k \in \mathbb{Z}\}$. We must show $D = d$.
First, since $D \in S$, there exist integers x_i such that $D = \sum a_i x_i$. Let

$d = (a_1, \ldots, a_n)$. Since $d \mid a_i$ for all i, by Theorem 2.3.1 (iii), d divides any linear combination of the a_i. Thus $d \mid D$. Since both are positive, $d \leq D$.
Conversely, since each a_i can be written as a trivial linear combination (e.g., $a_1 = 1 \cdot a_1 + 0 \cdot \ldots$), $a_i \in S$ for all i. Therefore, every a_i is a multiple of D. This implies D is a common divisor of all a_i.
By the maximality property of the GCD, $D \leq d$. Combining these inequalities, $D = d$.

■

Corollary 1.1. *Bézout's Identity.* Let $a_1, \ldots, a_n$ be integers, not all zero. There exist integers $x_1, \ldots, x_n$ such that

$$a_1 x_1 + \cdots + a_n x_n = (a_1, \ldots, a_n).$$

In particular, $a_1, \ldots, a_n$ are coprime if and only if there exist integers x_i such that $\sum a_i x_i = 1$.

推論

With this algebraic characterisation, we derive powerful arithmetic properties.

Theorem 1.3. ***Algebraic Properties of GCD.***
Let a, b, c be integers.

(i) **Divisibility by GCD:** Every common divisor of $a, \ldots, c$ divides $(a, \ldots, c)$.
(ii) **Associativity:** $(a, b, c) = ((a, b), c)$.
(iii) **Homogeneity:** For any $m \in \mathbb{Z}^+$, $(ma, mb, \ldots, mc) = m(a, b, \ldots, c)$.
(iv) **Reduction:** If $(a, b, \ldots, c) = d$, then $(a/d, b/d, \ldots, c/d) = 1$.
(v) **Coprimality with Products:** If $(a, m) = 1$ and $(b, m) = 1$, then $(ab, m) = 1$.
(vi) **Euclid's Lemma Variant:** If $c \mid ab$ and $(c, b) = 1$, then $c \mid a$.

定理

Proof

(i) Let k be a common divisor. Then k divides any linear combination of $a, \ldots, c$. By *Bézout's Identity*, $(a, \ldots, c)$ is such a linear combination, so $k \mid (a, \ldots, c)$.
(ii) Let $d = (a, b, c)$ and $d' = ((a, b), c)$. Since $d' \mid (a, b)$ and $d' \mid c$, and $(a, b) \mid a$ and $(a, b) \mid b$, it follows that d' is a common divisor of a, b, c. Thus $d' \leq d$. Conversely, $d \mid a$ and $d \mid b$ implies $d \mid (a, b)$ by part (1). Since $d \mid c$, d is a common divisor of (a, b) and c, so $d \leq d'$. Thus $d = d'$.
(iii) Let $d = (a, \ldots, c)$. By Bézout's Identity, $d = \sum a_i x_i$. Multiplying by m gives $md = \sum (ma_i) x_i$. Thus $(ma, \ldots, mc)$ divides md,

so $(ma, \ldots, mc) \leq md$. Conversely, $md \mid ma_i$, so md is a common divisor of the scaled integers. Thus $md \leq (ma, \ldots, mc)$. Equality follows.

(iv) Using Homogeneity: $d = (d \cdot a/d, \ldots, d \cdot c/d) = d(a/d, \ldots, c/d)$. Cancelling d yields the result.

(v) Since $(a, m) = 1$, there exist x, y such that $ax + my = 1$. Similarly, $bx' + my' = 1$. Multiplying these equations:

$$(ax + my)(bx' + my') = ab(xx') + m(axy' + bx'y + myy') = 1.$$

Thus, 1 is a linear combination of ab and m, implying $(ab, m) = 1$.

(vi) Since $(c, b) = 1$, we can write $cx + by = 1$. Multiplying by a: $acx + aby = a$. Clearly $c \mid acx$. By hypothesis $c \mid ab$, so $c \mid aby$. Thus $c \mid (acx + aby)$, which means $c \mid a$.

■

1.2 *Euclid's Algorithm*

Theorem 3.1.3 (ii) implies that computing the GCD of multiple integers reduces to the case of two integers. We employ Euclid's Algorithm, which exploits the property $(a, b) = (a, b - qa)$.
Let a, b be integers with $b \neq 0$. We apply the Division Algorithm repeatedly:

$$\begin{aligned}
a &= bq_0 + r_0, && 0 \leq r_0 < |b| \\
b &= r_0q_1 + r_1, && 0 \leq r_1 < r_0 \\
r_0 &= r_1q_2 + r_2, && 0 \leq r_2 < r_1 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1} + 0.
\end{aligned}$$

If $r_0 = 0$, the algorithm stops at the first step; otherwise continue until the first zero remainder occurs. Since the remainders form a decreasing sequence of non-negative integers and a zero remainder terminates the process, the algorithm must stop. By the recursive property of the GCD:

$$(a, b) = (b, r_0) = (r_0, r_1) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Thus, the last non-zero remainder is the greatest common divisor. By working backwards from the penultimate equation, we can express r_n as a linear combination of a and b, providing a constructive method for finding the coefficients in Bézout's Identity:

$$(a, b) = r_n = r_{n-2} - r_{n-1}q_n.$$

Substituting $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$ yields (a, b) in terms of r_{n-2} and r_{n-3}, and so on, until a and b are reached.

Example 1.2. Extended Euclidean Algorithm. To find $d = (240, 46)$ and express it as a linear combination of 240 and 46, we apply the division algorithm repeatedly:

$$\begin{aligned} 240 &= 5 \cdot 46 + 10 \\ 46 &= 4 \cdot 10 + 6 \\ 10 &= 1 \cdot 6 + 4 \\ 6 &= 1 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

The last non-zero remainder is 2, so $(240, 46) = 2$. By back-substitution:

$$\begin{aligned} 2 &= 6 - 1 \cdot 4 \\ 2 &= 6 - 1 \cdot (10 - 1 \cdot 6) = 2 \cdot 6 - 10 \\ 2 &= 2 \cdot (46 - 4 \cdot 10) - 10 = 2 \cdot 46 - 9 \cdot 10 \\ 2 &= 2 \cdot 46 - 9 \cdot (240 - 5 \cdot 46) = 47 \cdot 46 - 9 \cdot 240. \end{aligned}$$

Thus, $x = -9$ and $y = 47$ are the Bézout coefficients.

範例

Least Common Multiple

The dual concept to the greatest common divisor is the least common multiple.

Definition 1.3. ***Least Common Multiple.***
Let $a_1, \ldots, a_n$ be non-zero integers. The least common multiple, denoted by $[a_1, \ldots, a_n]$, is the unique integer D satisfying:

(i) **Common Multiple:** $D \geq 1$ and $a_k \mid D$ for all k.
(ii) **Minimality:** If D' is any positive integer such that $a_k \mid D'$ for all k, then $D \leq D'$.

定義

Theorem 1.4. ***Properties of LCM.***
Let $a, b, \ldots, c$ be non-zero integers.

(i) **Universal Multiple:** Every common multiple of $a, \ldots, c$ is divisible by $[a, \ldots, c]$.
(ii) **Associativity:** $[a, b, \ldots, c] = [[a, b], \ldots, c]$.
(iii) **Homogeneity:** For $m \in \mathbb{Z}^+$, $[ma, mb, \ldots, mc] = m[a, b, \ldots, c]$.
(iv) **Product Formula:** $(a, b)[a, b] = |ab|$.
(v) If $a, b, \ldots, c$ are pairwise coprime, then $[a, b, \ldots, c] = |ab \ldots c|$.

定理

Proof

1. Let $S \subseteq \mathbb{Z}$ be the set of all integer common multiples of $a_1, \ldots, a_n$. Since $0 \in S$ and $|a_1 \ldots a_n| \in S$, the set is nonempty. The set S is an ideal, so $S = \langle D \rangle$ where D is its least positive element. By definition, $D = [a_1, \ldots, a_n]$.
2. Follows from (1) and the definition, analogous to Theorem 3.1.3 (ii).
3. Let $D = [ma, \ldots, mc]$. Since $m[a, \ldots, c]$ is a common multiple of the scaled set, $D \leq m[a, \ldots, c]$. Conversely, D is a multiple of ma, so D/m is an integer multiple of a. Repeating for all terms, D/m is a common multiple of $a, \ldots, c$, so $[a, \ldots, c] \leq D/m$. Thus $m[a, \ldots, c] \leq D$.
4. Since $(a, b) = (|a|, |b|)$ and $[a, b] = [|a|, |b|]$, it suffices to assume $a, b > 0$. If $(a, b) = 1$, then $ax = [a, b] = by$ implies $b \mid ax$. By Theorem 3.1.3 (vi), $b \mid x$. Thus $x = kb$, so $[a, b] = akb$. The product ab is a common multiple, so $[a, b] \leq ab$, hence $k = 1$, and $[a, b] = ab$. Generally, let $d = (a, b)$. Then $(a/d, b/d) = 1$.

$$[a, b] = d[a/d, b/d] = d(a/d \cdot b/d) = ab/d.$$

   Therefore, $d[a, b] = |ab|$.
5. Follows from (2) and (4) by induction.

■

1.3 *Prime Numbers and Unique Factorisation*

The study of the integers is fundamentally concerned with the multiplicative building blocks known as prime numbers.

Definition 1.4. ***Prime and Composite Numbers.***
An integer $p > 1$ is called a *prime number* (or simply a prime) if its only positive divisors are 1 and p. An integer $n > 1$ that is not prime is called *composite*. The set of positive integers $\mathbb{Z}^+$ is thus partitioned into three disjoint classes: the unit $\{1\}$, the primes, and the composite numbers.

定義

It is an elementary observation that every integer $n > 1$ possesses at least one prime divisor. Indeed, the set of divisors of n strictly greater than 1 is non-empty (containing n itself). By the *Least Number Principle*, this set has a least element, say q. If q were composite, it would have a divisor $1 < d < q$, which would also divide n, contradicting the minimality of q. Thus, the smallest non-trivial divisor of any integer is prime.

Remark (Distribution of Primes).

The density of primes decreases as $n \to \infty$. Empirical counts indicate there are 25 primes up to 100, 168 primes up to 1,000, and 1,229 primes up to 10,000.

Theorem 1.5. ***Euclid's Theorem.***
There are infinitely many prime numbers.

定理

Proof

Assume, for the sake of contradiction, that there exists only a finite number of primes, enumerated as $\{p_1, p_2, \ldots, p_n\}$. Consider the integer

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

Since $N > 1$, it must have a prime divisor q. By hypothesis, q must be one of the p_i. Consequently, q divides the product $p_1 \ldots p_n$. Since q divides both N and the product, it must divide their difference:

$$q \mid (N - p_1 \ldots p_n) \implies q \mid 1.$$

This is impossible. Therefore, the set of primes is infinite.

■

Factorial Variation Proof

For any $n \in \mathbb{Z}^+$, consider the integer $N = n! + 1$. Since $N > 1$, it possesses at least one prime divisor p. If $p \leq n$, then p divides $n!$, which implies $p \mid (N - n!)$, or $p \mid 1$, which is impossible. Therefore, $p > n$, demonstrating that for any integer n, there exists a prime strictly greater than n.

■

To establish the uniqueness of factorisation, we require a critical property of primes regarding divisibility.

Theorem 1.6. ***Euclid's Lemma.***
Let p be a prime and $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

定理

Proof

Suppose $p \mid ab$ and $p \nmid a$. Since the only positive divisors of p are 1 and p, and p does not divide a, the greatest common divisor $(a, p) = 1$. By Theorem 3.1.3 (vi), if p divides a product and is coprime to one factor, it must divide the other. Thus $p \mid b$.

■

Generalising by induction, if a prime p divides a product $a_1 \ldots a_n$, then p must divide at least one a_i.

Theorem 1.7. ***The Fundamental Theorem of Arithmetic.***
Every integer $n > 1$ can be represented as a product of prime numbers. This representation is unique, up to the ordering of the factors. Specifically, every $n > 1$ can be written uniquely in the *standard form*:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

where $p_1 < p_2 < \dots < p_k$ are primes and $\alpha_i \in \mathbb{Z}^+$.

定理

Proof

We prove the existence first then uniqueness:

Existence: We proceed by strong induction on n. For $n = 2$, the statement holds. Assume every integer k with $1 < k < n$ has a prime factorisation. If n is prime, we are done. If n is composite, $n = ab$ with $1 < a, b < n$. By the induction hypothesis, a and b are products of primes; thus their product n is also a product of primes.

Uniqueness: Suppose n has two factorisations: $n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$. Consider p_1. Since $p_1 \mid n$, it divides the product $q_1 \dots q_t$. By *Theorem 1.6*, p_1 must divide some q_j. Since q_j is prime, $p_1 = q_j$. We can reorder the q's so that $p_1 = q_1$. Dividing both sides by p_1, we obtain: $p_2 \dots p_s = q_2 \dots q_t$. Repeating this argument (formally, by induction on the number of factors), we find that each p_i matches a unique q_i, and $s = t$.

■

Remark (Hilbert's Example).

While the existence of factorisation follows from the well-ordering of $\mathbb{Z}^+$, uniqueness is non-trivial and relies heavily on the Euclidean property (specifically *Theorem 1.6*). Consider the set of integers $S = \{4k + 1 \mid k \in \mathbb{Z}_{\geq 0}\} = \{1, 5, 9, 13, 17, 21, \dots\}$. This set is closed under multiplication. An element $x \in S \setminus \{1\}$ is "irreducible" in S if it cannot be written as ab with $a, b \in S \setminus \{1\}$. In this system, $9, 21, 49$ are irreducibles. However, $441 \in S$ has two distinct factorisations into irreducibles:

$$441 = 21 \times 21 = 9 \times 49.$$

Thus, unique factorisation fails in S because it lacks the division algorithm and the resulting property that irreducibles are prime (in the sense of *Theorem 1.6*). Integers possess the unique factorisation property because $\mathbb{Z}$ is a Principal Ideal Domain.

The standard factorisation allows for a precise arithmetic characterisation of divisors, GCDs, and LCMs.

Corollary 1.2. *Divisors, GCD, and LCM via Factorisation.* Let the standard factorisations of two positive integers a and b be given by:

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{k} p_i^{\beta_i},$$

where we allow exponents to be zero to use a common set of primes.

(i) $d \mid a$ if and only if $d = \prod p_i^{\delta_i}$ with $0 \le \delta_i \le \alpha_i$ for all i.

(ii) $(a, b) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$.

(iii) $[a, b] = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$.

推論

Proof

(i) Let d be a positive divisor of a. By *Theorem 1.7*, any prime divisor of d must be among $\{p_1, \ldots, p_k\}$. Thus d can be written as $d = \prod_{i=1}^{k} p_i^{\delta_i}$. The condition $d \mid a$ is equivalent to the existence of an integer c such that $dc = a$. Let $c = \prod p_i^{\gamma_i}$. Then

$$\prod p_i^{\delta_i} \prod p_i^{\gamma_i} = \prod p_i^{\delta_i + \gamma_i} = \prod p_i^{\alpha_i}.$$

By the uniqueness of prime factorisation in *Theorem 1.7*, $\delta_i + \gamma_i = \alpha_i$. Since $\gamma_i \ge 0$, it follows that $0 \le \delta_i \le \alpha_i$ for all i. Conversely, if $0 \le \delta_i \le \alpha_i$, then $a/d = \prod p_i^{\alpha_i - \delta_i}$ is an integer, so $d \mid a$.

(ii) Let $g = \prod p_i^{\min(\alpha_i, \beta_i)}$. Since $\min(\alpha_i, \beta_i) \le \alpha_i$ and $\min(\alpha_i, \beta_i) \le \beta_i$ for all i, g is a common divisor of a and b by part (i). Let $d = \prod p_i^{\delta_i}$ be any common divisor. Then $\delta_i \le \alpha_i$ and $\delta_i \le \beta_i$, which implies $\delta_i \le \min(\alpha_i, \beta_i)$. Thus $d \mid g$, and by the maximality property in the definition of the GCD, $g = (a, b)$.

(iii) Let $L = \prod p_i^{\max(\alpha_i, \beta_i)}$. Since $\max(\alpha_i, \beta_i) \ge \alpha_i$ and $\max(\alpha_i, \beta_i) \ge \beta_i$ for all i, both a and b divide L by part (i), so L is a common multiple. Let M be any positive common multiple. The exponent of p_i in the factorisation of M must be at least α_i and at least β_i, so it is at least $\max(\alpha_i, \beta_i)$. Thus $L \mid M$, and by the minimality property in the definition of the LCM, $L = [a, b]$.

■

Arithmetic Functions

We conclude this chapter by introducing functions defined on $\mathbb{Z}^+$, known as number-theoretic functions.

Definition 1.5. ***Divisor Functions.***
For $n \in \mathbb{Z}^+$, let $\tau(n)$ denote the number of positive divisors of n, and $\sigma(n)$ denote the sum of positive divisors of n. If $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, then by *corollary 1.2*:

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1) = \prod_{i=1}^{k} (\alpha_i + 1), \tag{1.1}$$

$$\sigma(n) = \prod_{i=1}^{k} \left(\sum_{j=0}^{\alpha_i} p_i^j \right) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}. \tag{1.2}$$

定義

Example 1.3. Computing Divisor Functions. Let $n = 360$. The standard prime factorisation is $360 = 2^3 \cdot 3^2 \cdot 5^1$. Using the formulas for τ and σ:

$$\begin{aligned} \tau(360) &= (3+1)(2+1)(1+1) = 4 \cdot 3 \cdot 2 = 24. \\ \sigma(360) &= \frac{2^4 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} \\ &= 15 \cdot \frac{26}{2} \cdot \frac{24}{4} \\ &= 15 \cdot 13 \cdot 6 = 1170. \end{aligned}$$

There are 24 positive divisors of 360, and their sum is 1170.

範例

Definition 1.6. ***Multiplicative Functions.***
A function $f : \mathbb{Z}^+ \to \mathbb{C}$ is called *multiplicative* if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$. If f is multiplicative and not identically zero, it is completely determined by its values on prime powers:

$$f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \dots f(p_k^{\alpha_k}).$$

From *Equation 1.1* and *Equation 1.2*, it is evident that both τ and σ are multiplicative functions.

定義

1.4 *Exercises*

1. **General Solution.** Let a, b, c be integers such that $(a, b) \mid c$. Prove that if (x_0, y_0) is a particular integer solution to $ax + by = c$, then

the set of all integer solutions is given by:

$$x = x_0 + \frac{b}{(a,b)}t, \quad y = y_0 - \frac{a}{(a,b)}t, \quad \text{for all } t \in \mathbb{Z}.$$

2. **Euclidean Algorithm Practice.** Use Euclid's algorithm to find $d = (963, 657)$. Then find one integer solution (x_0, y_0) and the general solution to:
$$963x + 657y = d.$$

3. **The Frobenius Coin Problem (Two Variables).** Let a, b be coprime positive integers.
   (a) Prove that if $n > ab - a - b$, the equation $ax + by = n$ has a non-negative integer solution.
   (b) Show that for $n = ab - a - b$, the equation $ax + by = n$ has **no** non-negative integer solution.

4. **Solving Linear Systems.** Find all integer solutions to the following equations:
   (a) $x + 2y + 3z = 10$
   (b) $6x + 20y - 15z = 23$
   (c) $9x + 24y - 5z = 4$
   (d) $25x + 13y + 7z = 2$

5. **The $\sqrt{n}$ Test.** Let $n \geq 2$ be an integer. Prove that if n is not divisible by any prime p such that $p \leq \sqrt{n}$, then n is prime.

6. **Alternative Characterisation.** Let $n > 1$. Prove that n is prime if and only if for every integer m, either m is a multiple of n or $(m, n) = 1$.

7. **Bertrand's Postulate (Weak Form).** Let $n > 2$. Prove that there exists at least one prime p such that $n < p < n!$. Use this to deduce that there are infinitely many primes.

8. **Prime Gaps.** Let $n \geq 2$. Prove that there exist n consecutive positive integers, none of which is prime.

   Consider the sequence starting with $(n+1)! + 2$.

9. **Primes in Arithmetic Progressions.**
   (a) Prove that there are infinitely many primes of the form $4m + 3$.
   (b) Prove that there are infinitely many primes of the form $6m + 5$.

10. **Prime Triplets.** Prove that the only triplet of prime numbers of the form $(p, p+2, p+4)$ is $(3, 5, 7)$.

11. **Repunits.** Let R_n be the integer consisting of n ones:
$$R_n = 10^{n-1} + 10^{n-2} + \cdots + 1 = \frac{10^n - 1}{9}.$$

(a) Prove that if R_n is prime, then n must be prime.
(b) Show that the converse is false by finding a counter-example (i.e., a prime n for which R_n is composite).

12. Fermat Primes.

(a) Let m be a positive integer. Prove that if $2^m + 1$ is prime, then m must be a power of 2.
(b) Let $F_n = 2^{2^n} + 1$ be the n-th Fermat number. Prove that if $m > n$, then $F_n \mid (F_m - 2)$.
(c) Deduce that for $m \neq n$, $(F_m, F_n) = 1$. Conclude that there are infinitely many primes.

13. Mersenne Primes.

(a) Let $m, n > 1$. Prove that if $m^n - 1$ is prime, then $m = 2$ and n is prime.
(b) Let $M_p = 2^p - 1$ where p is prime. Prove that if p and q are distinct primes, then $(M_p, M_q) = 1$.

14. ⋆ The GCD of Powers. Let $a > 1$ be an integer and let m, n be positive integers. Prove that:

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

This generalizes the result on Mersenne numbers. Hint: Use the Euclidean algorithm logic on the exponents.

15. Composite Sum of Powers. Let a, b, c, d be positive integers satisfying $ab = cd$. Prove that $N = a^4 + b^4 + c^4 + d^4$ is a composite number.

Consider the parametrisation $a = kux, b = lvy, c = kvy, d = lux$ or similar structures derived from (a, c) and (a, d).

16. Legendre's Formula. Let n be a positive integer and p be a prime. We write $p^k \parallel n$ (read as "p^k exactly divides n") if $p^k \mid n$ but $p^{k+1} \nmid n$ (i.e., k is the exponent of p in the factorisation of n). Let e be the exponent of p in $n!$. Prove:

(a) $e = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.
(b) If $S_p(n)$ is the sum of the digits of n in base p, then

$$e = \frac{n - S_p(n)}{p - 1}.$$

17. Integrality of Multinomial Coefficients.

(a) Let $a_1, \ldots, a_k$ be positive integers. Prove that the multinomial coefficient

$$\frac{(a_1 + \cdots + a_k)!}{a_1! \ldots a_k!}$$

is an integer.
(b) Let m, n be positive integers. Prove that the following expression is an integer:

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}.$$

18. Difference-Quotient Divisibility. Let a, b be distinct integers and n be a positive integer. Prove that if $n \mid (a^n - b^n)$, then

$$n \mid \frac{a^n - b^n}{a - b}.$$

19. Divisor Function Properties. Let $\tau(n)$ denote the number of positive divisors of n. Prove:

(a) n is a perfect square if and only if $\tau(n)$ is odd.
(b) The product of the positive divisors of n is equal to $n^{\tau(n)/2}$.
(c) $\tau(n) \leq 2\sqrt{n}$. (Can you improve this to $\tau(n) \leq 2\sqrt{n} + 1$?)

20. ⋆ Harmonic Sums. Let

$$H_n = \sum_{k=1}^{n} \frac{1}{k}.$$

Prove that for any integer $n > 1$, H_n is **not** an integer.

Consider the term with the highest power of 2 in the denominator. Let 2^k be the largest power of 2 such that $2^k \leq n$. Show that 2^k divides the least common multiple of $1, \ldots, n$ but 2^{k+1} does not, and use this to analyse the numerator of the sum.

2
Congruences

We shift our focus from the multiplicative building blocks of integers (primes) to the arithmetic properties of remainders. While questions regarding the distribution of primes within polynomial values remain deep, exemplified by Euler's polynomial $n^2 + n + 41$, which yields primes for $0 \leq n \leq 40$ but fails at $n = 41$, the theory of congruences, introduced by Gauss, provides a nice framework for "clock arithmetic" and is the backbone for the study of Diophantine equations and algebraic structures.

2.1 *The Congruence Relation*

Let n be a fixed positive integer, referred to as the *modulus*.

Definition 2.1. ***Congruence.***
Let $a, b \in \mathbb{Z}$. We say that a is congruent to b modulo n, denoted by $a \equiv b \pmod{n}$, if n divides the difference $a - b$. If n does not divide $a - b$, we say a is *incongruent* to b modulo n, denoted $a \not\equiv b \pmod{n}$.

定義

By the *The Division Algorithm*, $a \equiv b \pmod{n}$ if and only if a and b leave the same remainder upon division by n. Visually, if one arranges the integers on a circle of size n, congruent numbers occupy the same position.

Example 2.1. Congruence Examples. Consider the modulus $n = 12$.
- $1 \equiv 13 \pmod{12}$ since $12 \mid (1 - 13)$.
- $-3 \equiv 9 \pmod{12}$ since $12 \mid (-3 - 9)$.
- $5^2 = 25 \equiv 1 \pmod{12}$ since $12 \mid (25 - 1)$.

範例

Theorem 2.1. ***Equivalence Relation.***
Congruence modulo 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 $a \equiv c \pmod{n}$.

定理

Proof

(i) Since $a - a = 0$ and $n \mid 0$, reflexivity holds.
(ii) If $n \mid (a - b)$, then $n \mid -(a - b) = b - a$.
(iii) If $n \mid (a - b)$ and $n \mid (b - c)$, then by linearity of divisibility, n divides $(a - b) + (b - c) = a - c$.

■

The utility of congruences stems from their compatibility with the standard arithmetic operations of $\mathbb{Z}$.

Theorem 2.2. ***Modular Algebraic Properties.***
Let $n \in \mathbb{Z}^+$ and let $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:
(i) $a \pm c \equiv b \pm d \pmod{n}$.
(ii) $ac \equiv bd \pmod{n}$.
(iii) $a^k \equiv b^k \pmod{n}$ for any $k \in \mathbb{Z}^+$.

定理

Proof

By hypothesis, $a - b = kn$ and $c - d = ln$ for some $k, l \in \mathbb{Z}$.
(i) $(a \pm c) - (b \pm d) = (a - b) \pm (c - d) = n(k \pm l)$. Thus n divides the difference.
(ii) Consider the difference $ac - bd$. We add and subtract bc:

$$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = c(kn) + b(ln) = n(ck + bl).$$

Since $ck + bl \in \mathbb{Z}$, $n \mid (ac - bd)$.
(iii) Follows from (ii) by induction on k.

■

Repeated application of *Theorem 2.2* leads to the following result for polynomials.

Corollary 2.1. *Polynomial Congruence.* Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. If $a \equiv b \pmod{n}$, then $f(a) \equiv f(b) \pmod{n}$.

推論

Theorem 2.3. ***Multivariate Polynomial Congruence.***
Let $F(x_1, \ldots, x_k) \in \mathbb{Z}[x_1, \ldots, x_k]$ be a k-variate polynomial with inte-

ger coefficients. If $a_i \equiv b_i \pmod{n}$ for $1 \le i \le k$, then

$$F(a_1, \dots, a_k) \equiv F(b_1, \dots, b_k) \pmod{n}.$$

定理

We proceed by induction on the structure of F.

Base cases.

If F is a constant $C \in \mathbb{Z}$, then $F(\mathbf{a}) = C = F(\mathbf{b})$, so the congruence holds. If $F(x_1, \dots, x_k) = x_i$, then $F(\mathbf{a}) = a_i \equiv b_i = F(\mathbf{b}) \pmod{n}$.

証明終

Inductive steps.

Assume the theorem holds for polynomials G and H.
Addition: For $F = G + H$,

$$\begin{aligned} F(\mathbf{a}) &= G(\mathbf{a}) + H(\mathbf{a}) \\ &\equiv G(\mathbf{b}) + H(\mathbf{b}) \pmod{n} \quad \text{(by Theorem 2.2(i))} \\ &= F(\mathbf{b}). \end{aligned}$$

Multiplication: For $F = G \cdot H$,

$$\begin{aligned} F(\mathbf{a}) &= G(\mathbf{a}) \cdot H(\mathbf{a}) \\ &\equiv G(\mathbf{b}) \cdot H(\mathbf{b}) \pmod{n} \quad \text{(by Theorem 2.2(ii))} \\ &= F(\mathbf{b}). \end{aligned}$$

証明終

Since every polynomial is constructed from variables and constants by finitely many additions and multiplications, the result follows.

Remark (Root Finding).

This theorem provides a necessary condition for the existence of integer roots. If the congruence $f(x) \equiv 0 \pmod{n}$ has no solution, then the polynomial equation $f(x) = 0$ has no integer solution.

As an arithmetic application, we prove that no non-constant polynomial with integer coefficients can generate only prime numbers.

Theorem 2.4. ***Composite Values of Polynomials.***
Let $f(x) \in \mathbb{Z}[x]$ be a non-constant polynomial. There exists an integer x_0 such that $|f(x_0)|$ is composite.

定理

Proof

Assume, for contradiction, that $|f(x)|$ is prime for all $x \in \mathbb{Z}$. Let y be an integer such that $f(y) \neq 0$ and let $p = |f(y)|$. Since p is prime, $p \ge 2$. For any integer k, consider the evaluation at $y + kp$.

By *Theorem 2.3*:

$$y + kp \equiv y \pmod{p} \implies f(y + kp) \equiv f(y) \pmod{p}.$$

Since $f(y) = \pm p \equiv 0 \pmod{p}$, it follows that p divides $f(y + kp)$ for all $k \in \mathbb{Z}$. By hypothesis, $|f(y + kp)|$ is prime. The only prime divisible by p is p itself. Thus, for all k,

$$|f(y + kp)| = p.$$

This implies that the polynomial $f(x)$ assumes the values p or $-p$ infinitely many times. By the pigeonhole principle, at least one of these values is attained infinitely often. However, a non-constant polynomial of degree d can assume any given value at most d times. This is a contradiction.

■

Unlike in $\mathbb{Q}$ or $\mathbb{R}$, the cancellation law ($ac = bc \implies a = b$ for $c \neq 0$) does not hold unrestrictedly in modular arithmetic.

Example 2.2. Failure of Cancellation. Consider the congruence $4 \cdot 2 \equiv 10 \cdot 2 \pmod{12}$. This simplifies to $8 \equiv 20 \pmod{12}$, which holds as $12 \mid -12$. However, cancelling the factor 2 yields $4 \equiv 10 \pmod{12}$, which is false since $12 \nmid -6$.

範例

The correct formulation of cancellation requires adjusting the modulus by the greatest common divisor of the cancelled factor and the modulus.

Theorem 2.5. ***Cancellation Law.***
Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. If $ac \equiv bc \pmod{n}$, then

$$a \equiv b \pmod{\frac{n}{(c, n)}},$$

where (c, n) is the greatest common divisor of c and n. In particular, if $(c, n) = 1$, then $a \equiv b \pmod{n}$.

定理

Proof

The congruence $ac \equiv bc \pmod{n}$ implies $n \mid c(a - b)$. Let $d = (c, n)$. We can write $c = dc'$ and $n = dn'$ where $(c', n') = 1$ (by Theorem 3.1.3 (iv)). The divisibility condition becomes $dn' \mid dc'(a - b)$, which simplifies to $n' \mid c'(a - b)$. By Euclid's Lemma, since $(n', c') = 1$, we must have $n' \mid (a - b)$. Thus $a \equiv b \pmod{n'}$. Since $n' = n/d = n/(c, n)$, the result follows.

■

We conclude this section with standard properties regarding the

change of modulus.

Theorem 2.6. ***Properties of the Modulus.***
Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.

(i) If $a \equiv b \pmod{m}$ and $d \mid m$, then $a \equiv b \pmod{d}$.

(ii) For any $k \in \mathbb{Z} \setminus \{0\}$, $a \equiv b \pmod{m}$ if and only if $ka \equiv kb \pmod{km}$.

(iii) If $a \equiv b \pmod{m_i}$ for $i = 1, \ldots, r$, then $a \equiv b \pmod{[m_1, \ldots, m_r]}$, where $[\cdot]$ denotes the least common multiple.

定理

Proof

(i) If $m \mid (a-b)$ and $d \mid m$, then by transitivity of divisibility, $d \mid (a-b)$.

(ii) $a \equiv b \pmod{m} \iff m \mid (a-b) \iff km \mid k(a-b) \iff ka \equiv kb \pmod{km}$.

(iii) Let $L = [m_1, \ldots, m_r]$. Since $a \equiv b \pmod{m_i}$, we have $m_i \mid (a-b)$ for all i. By the universal property of the LCM (*Theorem 1.4*(i)), $L \mid (a-b)$.

■

To analyse congruences modulo a composite number n, it is often effective to decompose the modulus into its prime power factors. The following proposition relies on the properties of the least common multiple and the unique factorisation of integers.

Proposition 2.1. ***Reduction to Prime Powers.***
Let $n > 1$ have the standard prime factorisation $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. For any integers a and b:

$$a \equiv b \pmod{n} \iff a \equiv b \pmod{p_i^{\alpha_i}} \quad \text{for all } i = 1, \ldots, k.$$

命題

Proof

Let $L = [p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}]$. Since the prime powers $p_i^{\alpha_i}$ are pairwise coprime, their least common multiple is their product (Theorem 3.2.3 (v)). Thus $L = n$.

($\Longrightarrow$) If $a \equiv b \pmod{n}$, then $n \mid (a-b)$. Since $p_i^{\alpha_i} \mid n$, it follows by transitivity that $p_i^{\alpha_i} \mid (a-b)$ for all i.

($\Longleftarrow$) If $p_i^{\alpha_i} \mid (a-b)$ for all i, then $a - b$ is a common multiple of all $p_i^{\alpha_i}$. By the universal property of the LCM (Theorem 3.2.3 (i)), $a - b$ must be divisible by L. Since $L = n$, we have $a \equiv b \pmod{n}$.

■

This result allows us to solve polynomial congruences $f(x) \equiv 0 \pmod{n}$ by solving them modulo each prime power component $p_i^{\alpha_i}$ and combining the results. This necessary condition is recorded in the Root Finding remark following *corollary 2.1*.

Remark.

Testing modulo primes p alone may yield false positives, as a polynomial may have roots modulo every prime yet fail to have roots modulo a prime power.

Example 2.3. Non-existence of Integer Roots. Consider the polynomial $f(x) = x^5 - x^2 + x - 3$. We investigate its roots modulo small integers.

Modulo 2:

$$f(0) = -3 \equiv 1 \pmod{2}$$
$$f(1) = 1 - 1 + 1 - 3 = -2 \equiv 0 \pmod{2}.$$

Thus, $x \equiv 1$ is a root modulo 2.

Modulo 3:

$$f(0) = -3 \equiv 0 \pmod{3}.$$

Thus, $x \equiv 0$ is a root modulo 3.

Modulo 4: We test all residue classes in $\mathbb{Z}/4\mathbb{Z}$:

$$f(0) = -3 \equiv 1 \pmod{4}$$
$$f(1) = 1 - 1 + 1 - 3 = -2 \equiv 2 \pmod{4}$$
$$f(2) = 32 - 4 + 2 - 3 = 27 \equiv 3 \pmod{4}$$
$$f(3) \equiv (-1)^5 - (-1)^2 + (-1) - 3 \pmod{4}$$
$$= -1 - 1 - 1 - 3 = -6 \equiv 2 \pmod{4}.$$

Since $f(x) \equiv 0 \pmod{4}$ has no solution, the equation $f(x) = 0$ has no integer solutions, despite having solutions modulo 2 and modulo 3.

範例

2.2 *Residue Classes*

Since congruence modulo n is an equivalence relation (*Theorem 2.1*), it partitions the set of integers into disjoint equivalence classes. We now formalise this structure, which forms the basis of modular arithmetic.

Definition 2.2. ***Congruence Class.***
The congruence class of a modulo n, denoted $[a]$, is the set of all inte-

gers congruent to a modulo n:

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\} = \{kn + a \mid k \in \mathbb{Z}\}.$$

Any element $x \in [a]$ is called a *representative* of the class.

定義

By *Theorem 2.1*, for any integers a and b, either $[a] = [b]$ (if $a \equiv b \pmod{n}$) or $[a] \cap [b] = \emptyset$. This partition is exhaustive and finite.

Theorem 2.7. ***Partition of Integers.***
The set of integers $\mathbb{Z}$ is partitioned into exactly n distinct residue classes modulo n. These classes are given by:

$$[0], [1], [2], \ldots, [n-1].$$

定理

Proof

By the *The Division Algorithm*, for any integer a, there exist unique integers q, r such that $a = nq + r$ with $0 \leq r < n$. Thus, $a \equiv r \pmod{n}$, which implies $[a] = [r]$. This demonstrates that every integer belongs to one of the classes $\{[0], \ldots, [n-1]\}$.
To establish that these classes are distinct, suppose $[r_1] = [r_2]$ with $0 \leq r_1 \leq r_2 < n$. Then $r_2 \equiv r_1 \pmod{n}$, which implies $n \mid (r_2 - r_1)$. Since $0 \leq r_2 - r_1 < n$, the only multiple of n in this interval is 0. Thus $r_2 - r_1 = 0$, or $r_1 = r_2$.

■

Definition 2.3. ***Complete Set of Residues.***
A set $\{x_1, \ldots, x_n\} \subset \mathbb{Z}$ is called a *complete set of residues* modulo n if the elements are pairwise incongruent modulo n. The set $\{0, 1, \ldots, n-1\}$ is the least non-negative complete system modulo n.

定義

The set of all congruence classes modulo n is denoted by $\mathbb{Z}/n\mathbb{Z}$. While constructed from integers, these classes are abstract objects in their own right. For example, modulo 2, there are two classes: $[0]$ (the even integers) and $[1]$ (the odd integers).

Definition 2.4. ***Operations on $\mathbb{Z}/n\mathbb{Z}$.***
We define addition and multiplication of residue classes by representatives:

$$[a] + [b] = [a + b], \quad [a] \cdot [b] = [ab].$$

These operations are well-defined by *Theorem 2.2*. That is, the result is independent of the choice of representatives a and b.

定義

Consequently, $\mathbb{Z}/n\mathbb{Z}$ forms a commutative ring with identity $[1]$.

When n is a prime p, every non-zero class $[a]$ possesses a multiplicative inverse, making $\mathbb{Z}/p\mathbb{Z}$ a field.

Remark (Ill-defined Operations).

One must be cautious not to treat the exponent in modular arithmetic as a residue class. The expression $[a]^{[b]}$ is ill-defined because $b \equiv d \pmod{n}$ does not imply $a^b \equiv a^d \pmod{n}$. For instance, with $n = 3$, we have $1 \equiv 4 \pmod{3}$. However, taking $[2]$ as the base:

$$2^1 = 2 \equiv 2 \pmod{3}, \quad \text{but} \quad 2^4 = 16 \equiv 1 \pmod{3}.$$

Thus, exponentiation is an operation of $\mathbb{Z}$ on $\mathbb{Z}/n\mathbb{Z}$, defined as $[a]^k = [a^k]$ for integer k, not an operation between two residue classes.

2.3 *Reduced Residue Systems*

The multiplicative structure of $\mathbb{Z}/n\mathbb{Z}$ is of particular interest. By Theorem 3.1.1 (iv), $(a, n) = (a + kn, n)$ for any integer k. Therefore, if a representative a of a class $[a]$ is coprime to n, then every element of that class is coprime to n.

Definition 2.5. ***Reduced Congruence Class.***
A residue class $[a] \in \mathbb{Z}/n\mathbb{Z}$ is called a *reduced congruence class* if $(a, n) = 1$. The set of all such classes is the set of *units* of the ring $\mathbb{Z}/n\mathbb{Z}$, denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$.

定義

Definition 2.6. ***Euler's Totient Function.***
The Euler φ-function, denoted $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$, counts the number of integers in $\{1, \ldots, n\}$ that are coprime to n. In the context of rings, it is the cardinality of the set of units:

$$\varphi(n) = \left|(\mathbb{Z}/n\mathbb{Z})^\times\right| = \sum_{\substack{1 \le k \le n \\ (k,n)=1}} 1.$$

定義

The set $(\mathbb{Z}/n\mathbb{Z})^\times$ is closed under multiplication: if $(a, n) = 1$ and $(b, n) = 1$, then $(ab, n) = 1$ by Theorem 3.1.3 (v). Furthermore, it contains the multiplicative identity $[1]$.

Definition 2.7. ***Reduced Residue System.***
A subset $R \subseteq \mathbb{Z}$ is a *reduced residue system* modulo n if:

(i) $|R| = \varphi(n)$.
(ii) For every $r \in R$, $(r, n) = 1$.
(iii) The elements of R are pairwise incongruent modulo n.

Equivalently, R is a set of representatives for the classes in $(\mathbb{Z}/n\mathbb{Z})^\times$.
The *least positive reduced residue system* consists of those integers in $\{1, \dots, n-1\}$ coprime to n.

定義

Example 2.4. Reduced System Modulo 12. Let $n = 12$. The integers in $[1, 12]$ coprime to 12 are $\{1, 5, 7, 11\}$. Thus $\varphi(12) = 4$, and this set forms a reduced residue system. Another such system is $\{1, -1, 5, -5\}$, since $7 \equiv -5 \pmod{12}$ and $11 \equiv -1 \pmod{12}$.

範例

A fundamental property of residue systems is their invariance (as a set) under multiplication by a unit.

Theorem 2.8. ***Permutation of Residues.***
Let $a, b \in \mathbb{Z}$ with $(a, n) = 1$.

(i) If $\{c_1, \dots, c_n\}$ is a complete set of residues modulo n, then the set of affine transforms $\{ac_1 + b, \dots, ac_n + b\}$ is also a complete set of residues modulo n.

(ii) If $R = \{r_1, \dots, r_{\varphi(n)}\}$ is a reduced residue system modulo n, then the set of multiples $aR = \{ar_1, \dots, ar_{\varphi(n)}\}$ is also a reduced residue system modulo n.

定理

Proof

(i) The set $\{ac_i + b\}$ contains n integers. Suppose $ac_i + b \equiv ac_j + b \pmod{n}$ for some indices i, j. Subtracting b yields $ac_i \equiv ac_j \pmod{n}$. Since $(a, n) = 1$, the Cancellation Law implies $c_i \equiv c_j \pmod{n}$. As the original set $\{c_k\}$ was a complete system, we must have $i = j$. Thus, the elements of the new set are pairwise incongruent modulo n. Being a set of n incongruent integers, it forms a complete residue system.

(ii) Let $R = \{r_1, \dots, r_{\varphi(n)}\}$. Since $(a, n) = 1$ and $(r_i, n) = 1$ for all i, it follows that $(ar_i, n) = 1$. Thus, every element of aR is coprime to n. Suppose $ar_i \equiv ar_j \pmod{n}$. Since $(a, n) = 1$, cancellation yields $r_i \equiv r_j \pmod{n}$, which implies $i = j$. The set aR therefore consists of $\varphi(n)$ distinct integers coprime to n, satisfying the definition of a reduced residue system.

■

2.4 *Linear Congruences and Inverses*

The permutation property of complete residue systems allows us to determine the solvability of linear congruences.

Theorem 2.9. ***Existence and Multiplicity of Solutions.***
The linear congruence $ax \equiv b \pmod{n}$ admits a solution if and only if $d = (a, n)$ divides b. If solutions exist, there are exactly d distinct solutions modulo n, given by:

$$x = x_0 + t \cdot \frac{n}{d}, \quad \text{for } t = 0, 1, \ldots, d-1,$$

where x_0 is any particular solution.

定理

Proof

By definition, a solution exists if and only if the linear Diophantine equation $ax + ny = b$ is solvable for integers x, y. By *Theorem 1.2*, the linear combinations of a and n generate the ideal $\langle d \rangle$. Thus, $ax + ny = b$ has a solution if and only if $b \in \langle d \rangle$, i.e., $d \mid b$.
Now assume $d \mid b$. Since $d \mid a$ and $d \mid n$, we may divide the entire congruence by d to obtain the equivalent form:

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

Let $a' = a/d$, $b' = b/d$, and $n' = n/d$. Since $(a', n') = 1$, the element $[a']$ is invertible in $(\mathbb{Z}/n'\mathbb{Z})^\times$ (by *corollary 1.1*). Multiplying by its inverse yields a unique solution x_0 modulo n'. In terms of the original modulus n, the integers satisfying $x \equiv x_0 \pmod{n'}$ are of the form $x = x_0 + kn'$. We seek the number of distinct classes modulo n. Two solutions $x_0 + k_1 n'$ and $x_0 + k_2 n'$ are congruent modulo n if and only if:

$$(k_1 - k_2)n' \equiv 0 \pmod{n} \iff (k_1 - k_2)\frac{n}{d} = mn \iff k_1 - k_2 = md.$$

Thus, the solutions are distinct for $k \in \{0, 1, \ldots, d-1\}$.

■

This theorem provides a constructive algorithm for solving linear congruences: reduce the coefficients by their greatest common divisor, invert the leading coefficient modulo the reduced modulus, and then lift the solution to the original modulus.

Example 2.5. Solving a Linear Congruence. Consider the congruence $10x \equiv 6 \pmod{14}$. Here $a = 10, b = 6, n = 14$. The greatest common divisor is $d = (10, 14) = 2$. Since $2 \mid 6$, solutions exist, and there are exactly $d = 2$ distinct solutions modulo 14. Dividing the congruence by 2:

$$5x \equiv 3 \pmod{7}.$$

Since $(5, 7) = 1$, we compute the inverse of 5 modulo 7. Observing that $3 \times 5 = 15 \equiv 1 \pmod{7}$, the inverse is 3. Multiplying both

sides by 3:

$$x \equiv 3 \cdot 3 \equiv 9 \equiv 2 \pmod 7.$$

The general integer solution is $x = 2 + 7k$. The solutions modulo 14 correspond to $k = 0$ and $k = 1$: $x_1 = 2, x_2 = 9$. Thus, the solution set is $\{[2], [9]\} \subset \mathbb{Z}/14\mathbb{Z}$.

範例

We can prove a more general theorem:

Corollary 2.2. ***Existence of Solutions.***
Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. If $(a, n) = 1$, then the linear congruence

$$ax \equiv b \pmod n$$

has a solution x. Moreover, all such solutions belong to a single congruence class modulo n.

推論

Proof

Let $\{c_1, \ldots, c_n\}$ be a complete residue system modulo n (for instance, $\{0, 1, \ldots, n-1\}$). By Theorem 5.4.1 (i), since $(a, n) = 1$, the set $\{ac_1, \ldots, ac_n\}$ (taking the affine shift $b = 0$) is also a complete residue system modulo n. Consequently, the integer b must be congruent to exactly one element in this set. That is, there exists a unique index i such that $ac_i \equiv b \pmod n$. Then $x = c_i$ is a solution. If x and x' are two solutions, then $ax \equiv b \equiv ax' \pmod n$. By the cancellation law, $x \equiv x' \pmod n$, so they reside in the same congruence class.

■

Definition 2.8. ***Modular Inverse.***
Let $(a, n) = 1$. The unique solution class $[x]$ to the congruence $ax \equiv 1 \pmod n$ is called the *multiplicative inverse* of a modulo n. We denote the representative by a^{-1} or sometimes $1/a$. Thus, $a \cdot a^{-1} \equiv 1 \pmod n$.

定義

The existence of inverses is what endows $(\mathbb{Z}/n\mathbb{Z})^\times$ with its specific algebraic structure (that of an abelian group). Computationally, the inverse can be found using the Extended Euclidean Algorithm.

Example 2.6. Calculation of Inverse and Solution. Find all x satisfying $24x \equiv 7 \pmod{59}$. Since 59 is prime and $59 \nmid 24$, we have $(24, 59) = 1$. We first find $24^{-1} \pmod{59}$. Using the Euclidean

algorithm on 59 and 24:

$$\begin{aligned} 59 &= 2 \cdot 24 + 11 \\ 24 &= 2 \cdot 11 + 2 \\ 11 &= 5 \cdot 2 + 1. \end{aligned}$$

Back-substituting to express 1:

$$\begin{aligned} 1 &= 11 - 5(2) \\ &= 11 - 5(24 - 2 \cdot 11) = 11 \cdot 11 - 5 \cdot 24 \\ &= 11(59 - 2 \cdot 24) - 5 \cdot 24 = 11 \cdot 59 - 27 \cdot 24. \end{aligned}$$

Thus, $-27 \cdot 24 \equiv 1 \pmod{59}$. The inverse is $-27 \equiv 32 \pmod{59}$. The solution to the original congruence is:

$$x \equiv 24^{-1} \cdot 7 \equiv (-27) \cdot 7 \equiv -189 \pmod{59}.$$

Reducing -189 modulo 59:

$$-189 = -4(59) + 47.$$

So $x \equiv 47 \pmod{59}$.

範例

Theorem 2.10. ***Properties of Modular Inverses.***
Let $m \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$ with $(a, m) = (b, m) = 1$.

(i) $(ab)^{-1} \equiv a^{-1}b^{-1} \pmod{m}$.
(ii) $a^{-1} \equiv b^{-1} \pmod{m}$ if and only if $a \equiv b \pmod{m}$.
(iii) If $R = \{r_1, \ldots, r_{\varphi(m)}\}$ is a reduced residue system modulo m, then the set of inverses $R^{-1} = \{r_1^{-1}, \ldots, r_{\varphi(m)}^{-1}\}$ is also a reduced residue system modulo m.

定理

Proof

(i) We verify the product: $(ab)(a^{-1}b^{-1}) = (aa^{-1})(bb^{-1}) \equiv 1 \cdot 1 \equiv 1 \pmod{m}$. By uniqueness, $a^{-1}b^{-1}$ is the inverse of ab.
(ii) If $a^{-1} \equiv b^{-1} \pmod{m}$, multiplying by ab gives $b \equiv a \pmod{m}$. The converse holds similarly.
(iii) Since each r_i is coprime to m, its inverse r_i^{-1} exists and is coprime to m. Suppose $r_i^{-1} \equiv r_j^{-1} \pmod{m}$. By part (ii), this implies $r_i \equiv r_j \pmod{m}$, so $i = j$. The set R^{-1} contains $\varphi(m)$ distinct residues coprime to m, so it is a reduced system.

■

Example 2.7. Sum of Inverse Squares. Let $p \geq 5$ be a prime. We show that

$$\sum_{k=1}^{p-1} (k^{-1})^2 \equiv 0 \pmod{p}.$$

Let $S = \sum_{k=1}^{p-1} (k^{-1})^2$. Since $\{1, \ldots, p-1\}$ is a reduced residue system modulo p, for any integer a not divisible by p, the set $\{a \cdot 1, \ldots, a(p-1)\}$ is also a reduced residue system. Consequently, the sum of the squares of their inverses must be congruent to S modulo p:

$$\sum_{k=1}^{p-1} ((ak)^{-1})^2 \equiv S \pmod{p}.$$

Distributing the inverse:

$$\sum_{k=1}^{p-1} a^{-2}k^{-2} \equiv a^{-2} \sum_{k=1}^{p-1} k^{-2} \equiv a^{-2}S \pmod{p}.$$

Thus, $S \equiv a^{-2}S \pmod{p}$, which implies $(1 - a^{-2})S \equiv 0 \pmod{p}$. Multiplying by a^2, we get $(a^2 - 1)S \equiv 0 \pmod{p}$. To deduce $S \equiv 0 \pmod{p}$, we must find an a such that $a^2 - 1 \not\equiv 0 \pmod{p}$. The congruence $a^2 \equiv 1 \pmod{p}$ is equivalent to $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$. Since $p \geq 5$, the set $\{1, \ldots, p-1\}$ contains at least 4 elements. We can choose an $a \in \{2, \ldots, p-2\}$, ensuring $a \not\equiv \pm 1 \pmod{p}$. For such an a, $p \nmid (a^2 - 1)$. By Euclid's Lemma, it follows that $p \mid S$, i.e., $S \equiv 0 \pmod{p}$.
Alternatively, this can be proved more directly: Since $1, \frac{1}{2}, \cdots, \frac{1}{p-1}$ is a reduced system modulo p, the sum of squares of inverses is congruent to the sum of squares of the integers themselves. We have (for $p \geq 5$):

$$\sum_{i=1}^{p-1} \left(\frac{1}{i}\right)^2 \equiv \sum_{i=1}^{p-1} i^2 = \frac{1}{6}p(p-1)(2p-1) \equiv 0 \pmod{p},$$

since p is coprime to 6.

範例

2.5 *Exercises*

1. **Clock Arithmetic.**
   (a) Find the remainder when 2^{50} is divided by 7.
   (b) Determine whether 1234567 is congruent to 3 modulo 10.
   (c) Find an integer x such that $x \equiv -25 \pmod{11}$ and $0 \leq x < 11$.
2. **Modular Exponentiation.** Let a, b, n be integers with $n > 0$. Give

a counter-example to show that $a \equiv b \pmod{n}$ does **not** imply $k^a \equiv k^b \pmod{n}$.

3. **Cancellation Caution.** Use *Theorem 2.5* to simplify the congruence $24x \equiv 36 \pmod{50}$.
4. **Linear Congruences.** Solve the following linear congruences. If no solution exists, state why. If solutions exist, list all distinct solutions modulo n.
   (a) $3x \equiv 2 \pmod{7}$
   (b) $6x \equiv 15 \pmod{21}$
   (c) $15x \equiv 9 \pmod{12}$
5. **Polynomial Roots.** Consider the polynomial $f(x) = x^2 - 1$.
   (a) Find all roots of $f(x) \equiv 0 \pmod{5}$.
   (b) Find all roots of $f(x) \equiv 0 \pmod{8}$.
   (c) Explain why the number of roots differs from the degree of the polynomial in the second case.
6. **Prime Power Reduction.**
   (a) Verify that $x \equiv 7 \pmod{12}$ implies $x \equiv 1 \pmod{3}$ and $x \equiv 3 \pmod{4}$.
   (b) Use this decomposition to check if $x^2 \equiv 1 \pmod{12}$ has any solutions.
7. **Composite Polynomial Values.** Let $f(x) = x^2 + x + 41$.
   (a) Verify that $f(n)$ is prime for $n = 0, 1, 2$.
   (b) Prove that $f(41)$ is composite.
   (c) Prove generally that for any polynomial $P(x) \in \mathbb{Z}[x]$ with constant term $a_0 \neq 0$, $P(a_0)$ is divisible by a_0. Use this to construct a composite value for $f(x)$.
8. ⋆ **The Square Root of Unity.**
   (a) Let p be a prime. Prove that the congruence $x^2 \equiv 1 \pmod{p}$ has exactly two distinct solutions: $x \equiv 1$ and $x \equiv -1$.
   (b) Let $n = pq$ where p and q are distinct odd primes. Prove that $x^2 \equiv 1 \pmod{n}$ has exactly **four** distinct solutions.

For (a): Factorise $x^2 - 1$ and use Euclid's Lemma, which holds in $\mathbb{Z}$ and implies properties in $\mathbb{Z}/p\mathbb{Z}$.

For (b): Use *proposition 2.1* to decompose the problem into systems: $x \equiv \pm 1 \pmod{p}$ and $x \equiv \pm 1 \pmod{q}$. Count the valid combinations.

3
The Multiplicative Group of Integers

The transition from the integers $\mathbb{Z}$ to the quotient structure $\mathbb{Z}/n\mathbb{Z}$ introduces new algebraic phenomena, most notably the existence of zero divisors and the formation of finite fields.

3.1 The Ring Structure of $\mathbb{Z}/n\mathbb{Z}$

The set of congruence classes $\mathbb{Z}/n\mathbb{Z}$, equipped with the addition and multiplication operations defined in *chapter 2*, satisfies the axioms of a commutative ring with identity $[1]$. However, the arithmetic in this ring differs fundamentally from that of $\mathbb{Z}$ when n is composite.

Definition 3.1. ***Zero Divisors.***
An element $[a] \in \mathbb{Z}/n\mathbb{Z}$ is called a *zero divisor* if $[a] \neq [0]$ and there exists a non-zero element $[b] \in \mathbb{Z}/n\mathbb{Z}$ such that

$$[a] \cdot [b] = [0].$$

If a commutative ring with identity $1 \neq 0$ contains no zero divisors, it is called an *integral domain*.

定義

The existence of zero divisors obstructs the cancellation law and the existence of multiplicative inverses. If $[a]$ is a zero divisor, suppose for contradiction that it possesses an inverse $[a]^{-1}$. Then $[a][b] = [0]$ implies:

$$[b] = ([a]^{-1}[a])[b] = [a]^{-1}([a][b]) = [a]^{-1}[0] = [0],$$

contradicting the hypothesis that $[b] \neq [0]$. Consequently, zero divisors are never units.

Proposition 3.1. ***Structure of Residue Rings.***
The ring $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime.

命題

Proof

We consider the cases based on the primality of n.

(n is composite): If n is composite, there exist integers a, b such that $n = ab$ with $1 < a, b < n$. In $\mathbb{Z}/n\mathbb{Z}$, the classes $[a]$ and $[b]$ are non-zero, yet $[a][b] = [n] = [0]$. Thus, $\mathbb{Z}/n\mathbb{Z}$ possesses zero divisors and is not an integral domain.

(n is prime): Let $n = p$ be a prime. Suppose $[a][b] = [0]$ in $\mathbb{Z}/p\mathbb{Z}$. This implies $p \mid ab$. By Euclid's Lemma, $p \mid a$ or $p \mid b$, which means $[a] = [0]$ or $[b] = [0]$. Thus, $\mathbb{Z}/p\mathbb{Z}$ contains no zero divisors.

■

When $n = p$ is prime, every non-zero element $[a]$ is coprime to p, and thus by Bézout's Identity, possesses a multiplicative inverse. A commutative ring in which every non-zero element is invertible is called a field.

Definition 3.2. ***The Finite Field*** $\mathbb{F}_p$**.**
For a prime p, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field, denoted by $\mathbb{F}_p$. It consists of p elements and admits the four fundamental arithmetic operations: addition, subtraction, multiplication, and division by non-zero elements. The set of non-zero elements forms the *multiplicative group of the field*, denoted $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{[0]\}$. This is an abelian group of order $p - 1$.

定義

We distinguish the field of residue classes $\mathbb{F}_p$ (or $\mathbb{Z}/p\mathbb{Z}$) from the ring of p-adic integers $\mathbb{Z}_p$[1].

[1] The ring of p-adic integers arises by completing $\mathbb{Z}$ with respect to the p-adic absolute value; we will not develop this theory here.

Wilson's Theorem

The group structure of $\mathbb{F}_p^\times$ imposes strong constraints on products of its elements. Since every element $a \in \mathbb{F}_p^\times$ has a unique inverse a^{-1}, we can analyze the product of all elements in the group by pairing them with their inverses. The only elements that do not pair with a distinct inverse are those that are their own inverse.

Lemma 3.1. ***Self-Inverses Modulo*** p**.**
For a prime p, the congruence $x^2 \equiv 1 \pmod{p}$ has exactly two solutions: $x \equiv 1 \pmod{p}$ and $x \equiv -1 \pmod{p}$, provided $p > 2$. If $p = 2$, the unique solution is $x \equiv 1 \pmod{2}$.

引理

Proof

The congruence $x^2 \equiv 1 \pmod{p}$ is equivalent to $x^2 - 1 \equiv 0 \pmod{p}$, or $(x-1)(x+1) \equiv 0 \pmod{p}$. Since $\mathbb{F}_p$ is a field, it has no zero divisors. Therefore, either $x - 1 \equiv 0 \pmod{p}$ or $x + 1 \equiv 0$

$(\text{mod } p)$. For $p > 2$, $[1]$ and $[-1]$ are distinct classes. For $p = 2$, $1 \equiv -1$, yielding a single solution.

■

This lemma provides the mechanism for proving one of the classical theorems of number theory.

Theorem 3.1. ***Wilson's Theorem.***
An integer $n > 1$ is a prime number if and only if

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

定理

Proof

We prove the necessary and sufficient conditions separately.

$(\Longrightarrow)$ Let $n = p$ be a prime. If $p = 2$, then $(2-1)! = 1 \equiv -1 \pmod 2$, so the statement holds. Assume $p \geq 3$. Consider the product $P = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ modulo p. This product ranges over all elements of $\mathbb{F}_p^\times$. We pair each element $a \in \{2, \ldots, p-2\}$ with its multiplicative inverse a^{-1}. By *lemma 3.1*, the only elements equal to their own inverses are $[1]$ and $[p-1] = [-1]$. Thus, for every $a \in \{2, \ldots, p-2\}$, the inverse a^{-1} is distinct from a and lies in the same set. The product of these pairs is 1. The product of the entire set is therefore determined by the self-inverses:

$$(p-1)! \equiv 1 \cdot \left(\prod_{\substack{a \in \mathbb{F}_p^\times \\ a \neq a^{-1}}} a \right) \cdot (-1) \equiv 1 \cdot 1 \cdot (-1) \equiv -1 \pmod{p}.$$

$(\Longleftarrow)$ Suppose $(n-1)! \equiv -1 \pmod n$. We proceed by contradiction. Assume n is composite. Then n has a prime divisor q such that $q < n$. Since $q \leq n-1$, the integer q appears as a factor in the product $(n-1)!$. Therefore, $q \mid (n-1)!$. By hypothesis, $(n-1)! \equiv -1 \pmod n$, which implies $(n-1)! = kn - 1$ for some integer k. Since $q \mid n$, we have $q \mid kn$. It follows that q divides the linear combination $kn - (n-1)! = 1$. This implies $q = 1$, contradicting that q is prime. Thus, n must be prime.

■

Example 3.1. Verification of Wilson's Theorem. Consider $p = 7$. We evaluate the factorial modulo 7:

$$6! = 1 \times 2 \times 3 \times 4 \times 5 \times 6.$$

In $\mathbb{F}_7^\times$, we identify the inverses:
· $2 \times 4 = 8 \equiv 1 \pmod 7$, so $2^{-1} = 4$.
· $3 \times 5 = 15 \equiv 1 \pmod 7$, so $3^{-1} = 5$.
The elements 1 and $6 \equiv -1$ are self-inverses. Rearranging the product:

$$6! = 1 \times (2 \times 4) \times (3 \times 5) \times 6 \equiv 1 \times 1 \times 1 \times (-1) \equiv -1 \pmod 7.$$

Conversely, consider the composite number $n = 6$: $(6-1)! = 5! = 120$. Since $120 = 20 \times 6$, we have $120 \equiv 0 \pmod 6$. This confirms $0 \not\equiv -1 \pmod 6$. In general, for any composite $n > 4$, $(n-1)! \equiv 0 \pmod n$ because both factors a and b (where $n = ab$) appear in the factorial product.

範例

3.2 *Theorems of Fermat and Euler*

Recall from *definition* 2.6 that $\varphi(n)$ counts the number of positive integers not exceeding n that are coprime to n. We first establish the multiplicative nature of this function, which permits its efficient evaluation via prime factorisation.

Theorem 3.2. ***Multiplicativity of*** φ**.**
The function φ is multiplicative. That is, if $m, n \in \mathbb{Z}^+$ with $(m, n) = 1$, then

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

定理

Proof

Consider the set of integers $S = \{1, 2, \ldots, mn\}$. We arrange these integers in a grid with n rows and m columns:

$$\begin{array}{cccc} 1 & 2 & \cdots & m \\ m+1 & m+2 & \cdots & 2m \\ \vdots & \vdots & \ddots & \vdots \\ (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+m \end{array}$$

An integer x in this grid is coprime to mn if and only if $(x, m) = 1$ and $(x, n) = 1$.
We first determine the number of entries coprime to m. Since $x \equiv x' \pmod m$ implies $(x, m) = (x', m)$, and every column consists of integers congruent modulo m, coprimality with m is a property of the column index. There are exactly $\varphi(m)$ columns whose entries are coprime to m.

Now, consider such a column corresponding to a value r with $1 \leq r \leq m$ and $(r, m) = 1$. The elements of this column are of the form

$$\{qm + r \mid 0 \leq q \leq n - 1\}.$$

Since $(m, n) = 1$, as q ranges from 0 to $n - 1$, the values $qm + r$ form a complete set of residues modulo n (by Theorem 5.4.1 (i)). Thus, exactly $\varphi(n)$ elements in this column are coprime to n. Since there are $\varphi(m)$ such columns, and each contains $\varphi(n)$ valid integers, the total number of integers in S coprime to mn is $\varphi(m)\varphi(n)$.

■

Example 3.2. Calculation of φ. Using multiplicativity, we compute $\varphi(72)$. Since $72 = 2^3 \cdot 3^2$ and $(2^3, 3^2) = 1$,

$$\varphi(72) = \varphi(2^3)\varphi(3^2) = (2^3 - 2^2)(3^2 - 3) = 4 \cdot 6 = 24.$$

Equivalently, using the product formula derived below:

$$\varphi(72) = 72\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 24.$$

範例

Theorem 3.3. ***Euler's Product Formula.***
Let $n \geq 2$ have the prime factorisation $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. Then

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

定理

Proof

We proceed by induction on the number of distinct prime factors. First, consider a prime power p^α. The integers in $\{1, \dots, p^\alpha\}$ that are *not* coprime to p^α are precisely the multiples of p: $\{p, 2p, \dots, p^{\alpha-1}p\}$. There are $p^{\alpha-1}$ such multiples. Thus:

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

Since φ is multiplicative (*Theorem 3.2*) and distinct prime powers are

pairwise coprime,

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1}) \dots \varphi(p_k^{\alpha_k}) \\ &= \prod_{i=1}^{k} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) \\ &= \left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \\ &= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).\end{aligned}$$

■

The totient function satisfies a beautiful summation identity known as Gauss's Sum.

Theorem 3.4. ***Gauss's Summation Formula.***
For any $n \in \mathbb{Z}^+$,

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

定理

Proof

Let $f(n) = \sum_{d|n} \varphi(d)$. This is the Dirichlet convolution of φ with the constant function $\mathbf{1}(n) = 1$, where the convolution of arithmetic functions g and h is defined by $(g * h)(n) = \sum_{d|n} g(d)h(n/d)$. Because both φ and $\mathbf{1}$ are multiplicative and convolution preserves multiplicativity, f is multiplicative. It suffices to evaluate f on prime powers. For $n = p^\alpha$:

$$\begin{aligned}f(p^\alpha) &= \sum_{k=0}^{\alpha} \varphi(p^k) \\ &= 1 + \sum_{k=1}^{\alpha} (p^k - p^{k-1}) \\ &= 1 + (p-1) + (p^2 - p) + \dots + (p^\alpha - p^{\alpha-1}).\end{aligned}$$

This is a telescoping sum, reducing to p^α. Since $f(n) = \prod f(p_i^{\alpha_i}) = \prod p_i^{\alpha_i} = n$, the identity holds.

■

Alternative Set-Theoretic Proof

Consider the set of integers $S = \{1, 2, \dots, n\}$. We partition S based on the greatest common divisor with n. For each divisor d of n, let $A_d = \{k \in S : (k, n) = d\}$. Since every integer $k \in S$ has a unique gcd with n, and that gcd must be a divisor of n, we have the

disjoint union

$$S = \bigsqcup_{d|n} A_d.$$

Consequently, summing the cardinalities yields $n = \sum_{d|n} |A_d|$. The condition $(k, n) = d$ is equivalent to $(\frac{k}{d}, \frac{n}{d}) = 1$, where $1 \leq \frac{k}{d} \leq \frac{n}{d}$. Thus, the elements of A_d are in one-to-one correspondence with the integers up to n/d that are coprime to n/d. Therefore, $|A_d| = \varphi(n/d)$. Substituting this into the sum:

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right).$$

As d runs through all divisors of n, the term n/d also runs through all divisors of n. Thus, the summation is equivalent to $\sum_{d|n} \varphi(d) = n$.

■

We now apply the structure of the group $(\mathbb{Z}/n\mathbb{Z})^\times$ to derive Euler's Theorem.

Theorem 3.5. ***Euler's Theorem.***
Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ with $(a, n) = 1$. Then

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

定理

Proof

Let $R = \{r_1, r_2, \ldots, r_{\varphi(n)}\}$ be a reduced residue system modulo n. Since $(a, n) = 1$, the set $aR = \{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$ is also a reduced residue system modulo n (by Theorem 5.4.1 (ii)). Consequently, the product of the elements in R is congruent to the product of the elements in aR:

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

Factoring out a from the right-hand side yields:

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

Let $P = \prod r_i$. Since each r_i is coprime to n, their product P is coprime to n. By the Cancellation Law, we may cancel P from both sides, leaving $1 \equiv a^{\varphi(n)} \pmod{n}$.

■

Restricting Euler's Theorem to prime moduli yields Fermat's Little Theorem. Since $\varphi(p) = p - 1$, the result follows immediately.

Corollary 3.1. *Fermat's Little Theorem.* Let p be a prime.

(i) If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

(ii) For any integer a, $a^p \equiv a \pmod{p}$.

推論

Proof

Part (i) is a direct instance of *Theorem 3.5*. For part (ii), if $p \nmid a$, multiplying (i) by a yields $a^p \equiv a \pmod{p}$. If $p \mid a$, then $a \equiv 0 \pmod{p}$, so $a^p \equiv 0 \equiv a \pmod{p}$. Thus the congruence holds for all a.

■

We provide an alternative, self-contained proof of Fermat's Little Theorem that relies on the binomial expansion rather than group theory. This approach highlights the arithmetic properties of binomial coefficients modulo p.

Lemma 3.2. Prime Divisibility of Binomial Coefficients Let p be a prime and k an integer such that $1 \leq k \leq p-1$. Then

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

引理

Proof

Since $1 \leq k \leq p-1$, none of the prime factors appearing in $k!(p-k)!$ equals p, so the denominator is coprime to p even though it divides $(p-1)!$. Writing

$$\binom{p}{k} = \frac{p(p-1)!}{k!(p-k)!},$$

the numerator supplies a factor of p that cannot be cancelled by the denominator. Hence $p \mid \binom{p}{k}$.

■

Remark (The Carmichael Function).

The exponent $\varphi(n)$ in Euler's Theorem is not always the smallest integer k such that $a^k \equiv 1 \pmod{n}$ for all units a. The smallest such universal exponent is given by the *Carmichael function*, $\lambda(n)$. For $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $\lambda(n) = [\lambda(p_1^{\alpha_1}), \dots, \lambda(p_k^{\alpha_k})]$, where $\lambda(p^\alpha) = \varphi(p^\alpha)$ for odd primes or $p^\alpha = 2, 4$, and $\lambda(2^\alpha) = \frac{1}{2}\varphi(2^\alpha)$ for $\alpha \geq 3$. For example, modulo 8, we have $\varphi(8) = 4$, yet $a^2 \equiv 1 \pmod{8}$ for all odd a. Here $\lambda(8) = 2$.

3.3 *Exercises*

1. **Group Tables.**
   (a) Construct the addition and multiplication tables for the ring $\mathbb{Z}/6\mathbb{Z}$. Identify the units and zero divisors.
   (b) Construct the multiplication table for the field $\mathbb{F}_7$.
2. **Counting Zero Divisors.** Let $n > 1$ be an integer. Determine the number of zero divisors in the ring $\mathbb{Z}/n\mathbb{Z}$.

A zero divisor is a non-zero class $[a]$ with $1 < (a, n) < n$, which is equivalent to $(a, n) > 1$ and $[a] \neq [0]$.

3. **Group Cancellation.** Let $n > 1$. Prove that the cancellation law holds in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. That is, if $a, b, c \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.
4. **The Cayley Property.** Let $n > 1$. Prove that for any fixed unit $u \in (\mathbb{Z}/n\mathbb{Z})^\times$, the map $x \mapsto ux$ is a bijection from $(\mathbb{Z}/n\mathbb{Z})^\times$ to itself. Conclude that the product of u with all elements of the group yields exactly the elements of the group.
5. **Field Properties.** Let p be a prime.
   (a) Prove that for any $a \in \mathbb{F}_p$, the sum of a with itself p times is zero (i.e., $pa \equiv 0 \pmod{p}$).
   (b) Let $n \in \mathbb{Z}$ and $a \in \mathbb{F}_p$ with $a \neq 0$. Prove that if $na \equiv 0 \pmod{p}$, then $p \mid n$.
   (c) Prove the "Freshman's Dream" in characteristic p: for any $\alpha, \beta \in \mathbb{F}_p$, $(\alpha + \beta)^p = \alpha^p + \beta^p$.
6. **Reduced Residue Systems.** Let p be a prime.
   (a) Let $R = \{r_1, \ldots, r_{p-1}\}$ and $R' = \{r'_1, \ldots, r'_{p-1}\}$ be two reduced residue systems modulo p. Prove that the set of products $\{r_1 r'_1, \ldots, r_{p-1} r'_{p-1}\}$ is **not** a reduced residue system modulo p for $p > 2$.
   (b) Prove that $1^2 \cdot 3^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$ for any odd prime p.
7. **Computation.**
   (a) Calculate $\varphi(360)$ and $\varphi(429)$.
   (b) Find the last two digits of 3^{999} in its decimal representation.
8. **Properties of φ.**
   (a) Prove that $\varphi(n)$ is even for all $n \geq 3$.
   (b) Prove that the sum of positive integers less than n and coprime to n is $\frac{1}{2} n\varphi(n)$ for $n > 1$.
9. **Applications of Euler's Theorem.**
   (a) Let m, n be coprime positive integers. Prove that $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}$.
   (b) Let $(a, 10) = 1$. Prove that $a^{100} \equiv 1 \pmod{1000}$. (Note: The text exercise said 100, but 1000 is a stronger result implied by $\lambda(1000) = 100$).
   (c) Use Euler's theorem to provide an explicit formula for the modular inverse $a^{-1} \pmod{n}$ in terms of a and $\varphi(n)$.

10. Power Towers. Let a be an odd integer. Prove that for any $n \geq 1$:

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

11. The Möbius Function. Define $\mu(n)$ as 0 if n is not square-free, and $(-1)^k$ if n is the product of k distinct primes (with $\mu(1) = 1$).

(a) Prove that μ is a multiplicative function.

(b) Prove the fundamental identity: $\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$.

12. Möbius Inversion Formula. Let f and F be arithmetic functions.

(a) Prove that if $F(n) = \sum_{d|n} f(d)$, then $f(n) = \sum_{d|n} \mu(d)F(n/d)$.

(b) Use this to invert Gauss's Sum $\sum_{d|n} \varphi(d) = n$, deriving the formula $\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$.

(c) From the derived formula, provide an alternative proof of Euler's Product Formula (*Theorem 3.3*).

13. Summation Identities.

(a) Prove that $\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}$.

(b) Prove that $\sum_{d|n} \frac{\mu(d)}{\varphi(d)} = \frac{n}{\varphi(n)}$.

14. Binomials Modulo p. Let p be a prime.

(a) Prove that $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ for $0 \leq k \leq p-1$.

(b) Prove Lucas's Theorem (Base Case): $\binom{n}{p} \equiv \lfloor n/p \rfloor \pmod{p}$.

15. GCD of Sums. Let a, b be coprime integers with $a + b \neq 0$, and let p be an odd prime. Prove that:

$$\left(a + b, \frac{a^p + b^p}{a + b}\right) \in \{1, p\}.$$

16. Factorials and Divisibility. Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Prove that:

$$n! \mid b^{n-1}a(a + b)(a + 2b) \cdots (a + (n-1)b).$$

Consider the polynomial $P(x) = x(x+1)\cdots(x+n-1)$. What are its roots modulo n? Alternatively, consider the combinatorial interpretation of the generalized binomial coefficient.

17. ⋆ Composite Sums. Let $S_1 = \{0, 1, \ldots, n-1\}$ be a complete set of residues modulo n.

(a) If n is odd, show that the sum of elements in S_1 is divisible by n.

(b) Let n be even. Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$ be two complete systems of residues modulo n. Prove that the set of sums $\{a_1 + b_1, \ldots, a_n + b_n\}$ is **not** a complete system of residues modulo n.

4
Polynomial Congruences and Systems

We address the general problem of finding integer roots of polynomial congruences. Having established the theory for linear congruences in Theorem 5.3.1, we extend our scope to systems of congruences and higher-degree polynomials.

4.1 *Polynomial Congruences Modulo p*

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. A fundamental problem is to determine the number of solutions to $f(x) \equiv 0 \pmod{n}$. We count solutions as the number of distinct residue classes modulo n that satisfy the congruence.
For a general modulus n, this problem can be intricate. However, when the modulus is a prime p, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field ($\mathbb{F}_p$). This allows us to import results regarding polynomials over fields, most notably the restriction on the number of roots.

Theorem 4.1. ***Lagrange's Theorem.***
Let p be a prime and let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients such that $p \nmid a_n$ (i.e., the degree of f modulo p is n). Then the congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n solutions.

定理

Proof

We proceed by induction on the degree n.

Base Case ($n = 1$): The congruence is $a_1 x + a_0 \equiv 0 \pmod{p}$ with $p \nmid a_1$. By Theorem 5.3.1, since $(a_1, p) = 1$, there is exactly one solution.

Inductive Step: Assume the theorem holds for all polynomials of degree $n - 1$. Let $f(x)$ be of degree n. If $f(x) \equiv 0$

$(\mathrm{mod}\ p)$ has no solutions, the theorem holds. Suppose there exists a solution x_1. Then $f(x_1) \equiv 0 \pmod{p}$. We can write $f(x) - f(x_1) = \sum_{k=1}^{n} a_k(x^k - x_1^k)$. Using the algebraic identity

$$x^k - x_1^k = (x - x_1)(x^{k-1} + x^{k-2}x_1 + \cdots + x_1^{k-1}),$$

we can factor out $(x - x_1)$:

$$f(x) \equiv f(x) - f(x_1) \equiv (x - x_1)g(x) \pmod{p},$$

where $g(x)$ is a polynomial of degree $n - 1$ with leading coefficient a_n. Now, if x is any solution of $f(x) \equiv 0 \pmod{p}$, then

$$(x - x_1)g(x) \equiv 0 \pmod{p}.$$

Since p is prime, $\mathbb{Z}/p\mathbb{Z}$ has no zero divisors (Proposition 6.1.1). Thus, either $x - x_1 \equiv 0 \pmod{p}$ or $g(x) \equiv 0 \pmod{p}$. The first case yields the solution $x \equiv x_1$. By the induction hypothesis, the congruence $g(x) \equiv 0 \pmod{p}$ has at most $n - 1$ solutions. Therefore, $f(x) \equiv 0 \pmod{p}$ has at most $1 + (n - 1) = n$ solutions.

■

Remark (Composite Moduli Failure).

The primality of the modulus is essential. If n is composite, a polynomial of degree k may have more than k roots. Consider $f(x) = x^2 - 1$ modulo 8. The congruence $x^2 \equiv 1 \pmod{8}$ admits four solutions:

$$x \equiv 1, 3, 5, 7 \pmod{8}.$$

Here, the degree is 2, but there are 4 roots. This occurs because $\mathbb{Z}/8\mathbb{Z}$ contains zero divisors (e.g., $(3 - 1)(3 + 1) = 2 \cdot 4 = 8 \equiv 0$), preventing the crucial inference that $(x - x_1)g(x) \equiv 0 \implies x \equiv x_1$ or $g(x) \equiv 0$.

Corollary 4.1. *Roots of $x^{p-1} - 1$.* Let p be a prime. The polynomial $x^{p-1} - 1$ has exactly $p - 1$ distinct roots modulo p, namely $1, 2, \ldots, p - 1$.

推論

Proof

By Fermat's Little Theorem, every integer a with $(a, p) = 1$ satisfies $a^{p-1} \equiv 1 \pmod{p}$. Thus the residue classes $1, \ldots, p - 1$ are roots. Since the degree is $p - 1$, *Theorem 4.1* shows there are no other roots.

■

To solve polynomial congruences modulo composite moduli, we

often solve modulo prime factors and lift the results to higher powers. Hensel's Lemma provides a procedural method for this lifting, analogous to Newton's Method in calculus.

Theorem 4.2. ***Hensel's Lemma.***
Let $f(x)$ be a polynomial with integer coefficients, p be a prime, and $k \geq 1$. Suppose x_0 is a solution to the congruence

$$f(x) \equiv 0 \pmod{p^k}.$$

(i) If $f'(x_0) \not\equiv 0 \pmod{p}$, then there is a unique integer x_1 modulo p^{k+1} such that

$$f(x_1) \equiv 0 \pmod{p^{k+1}} \quad \text{and} \quad x_1 \equiv x_0 \pmod{p^k}.$$

This lift is given by the formula

$$x_1 = x_0 - f(x_0) \cdot (f'(x_0))^{-1} \pmod{p^{k+1}},$$

where $(f'(x_0))^{-1}$ is the modular inverse modulo p.

(ii) If $f'(x_0) \equiv 0 \pmod{p}$ and $f(x_0) \equiv 0 \pmod{p^{k+1}}$, then x_0 lifts to p distinct solutions modulo p^{k+1}, given by $x_1 = x_0 + tp^k$ for $t = 0, \ldots, p-1$.

(iii) If $f'(x_0) \equiv 0 \pmod{p}$ and $f(x_0) \not\equiv 0 \pmod{p^{k+1}}$, then x_0 has no lifts to modulo p^{k+1}.

定理

Proof

We seek a solution of the form $x_1 = x_0 + tp^k$ for some integer t. Using the Taylor expansion of polynomials (which terminates for polynomials):

$$f(x_0 + tp^k) = f(x_0) + tp^k f'(x_0) + \frac{(tp^k)^2}{2} f''(x_0) + \ldots$$

Modulo p^{k+1}, terms involving $(p^k)^2$ and higher vanish (since $2k \geq k+1$). Thus:

$$f(x_1) \equiv f(x_0) + tp^k f'(x_0) \pmod{p^{k+1}}.$$

We want $f(x_1) \equiv 0 \pmod{p^{k+1}}$. This is equivalent to

$$tp^k f'(x_0) \equiv -f(x_0) \pmod{p^{k+1}}.$$

Since x_0 is a root modulo p^k, we know $f(x_0) = mp^k$ for some integer m. Dividing the entire congruence by p^k, we seek t solving:

$$tf'(x_0) \equiv -m \equiv -\frac{f(x_0)}{p^k} \pmod{p}.$$

This is a linear congruence in t.

- If $p \nmid f'(x_0)$, there is a unique solution for t modulo p, yielding the unique lift x_1.
- If $p \mid f'(x_0)$, the coefficient of t is $0 \pmod{p}$.
  - If $f(x_0) \equiv 0 \pmod{p^{k+1}}$, the RHS is $0 \pmod{p}$. The congruence becomes $0 \cdot t \equiv 0 \pmod{p}$, which is satisfied by any $t \in \{0, \ldots, p-1\}$.
  - If $f(x_0) \not\equiv 0 \pmod{p^{k+1}}$, the RHS is non-zero, and $0 \cdot t \equiv c \pmod{p}$ has no solution.

■

Example 4.1. Lifting Solutions. Solve $x^2 \equiv 2 \pmod{49}$. Let $f(x) = x^2 - 2$. We first solve modulo $p = 7$.

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

The squares mod 7 are $\{0, 1, 4, 2\}$, so $x_0 \equiv 3$ and $x_0 \equiv 4$ are solutions.Consider $x_0 = 3$. We compute the derivative $f'(x) = 2x$.

$$f'(3) = 6 \equiv -1 \not\equiv 0 \pmod{7}.$$

Since the derivative is non-zero, a unique lift exists.

$$x_1 = x_0 - f(x_0)(f'(x_0))^{-1} \pmod{49}.$$

We calculate terms: $f(3) = 3^2 - 2 = 7$. The inverse of $f'(3) \equiv -1 \pmod{7}$ is -1.

$$x_1 = 3 - 7(-1) = 10 \pmod{49}.$$

Check: $10^2 = 100 = 2 \times 49 + 2 \equiv 2 \pmod{49}$. The second root corresponds to lifting $x_0 = 4$ (which is -3), yielding $x \equiv -10 \equiv 39 \pmod{49}$.

範例

4.2 *Systems of Linear Congruences*

We continue the congruence notation from *chapter 2* and seek a simultaneous solution for a single variable x. The simplest case involves pairwise coprime moduli.

Theorem 4.3. ***Chinese Remainder Theorem.***
Let $m_1, m_2, \ldots, m_k$ be pairwise coprime positive integers. For any se-

quence of integers $b_1, \ldots, b_k$, the system of congruences

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_k \pmod{m_k} \end{aligned}$$

has a solution. Moreover, this solution is unique modulo $M = m_1 m_2 \ldots m_k$.

定理

Proof

Existence: Let $M = \prod_{j=1}^{k} m_j$. For each i, define $M_i = M/m_i$. Since the moduli are pairwise coprime, $(M_i, m_i) = 1$. By Bézout's Identity, M_i possesses a multiplicative inverse modulo m_i. Let y_i be an integer such that

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

Construct the solution

$$x = \sum_{i=1}^{k} b_i M_i y_i.$$

We verify that x satisfies the j-th congruence. For any $i \neq j$, $m_j \mid M_i$, so $M_i \equiv 0 \pmod{m_j}$. Thus, the sum collapses to the j-th term:

$$x \equiv b_j M_j y_j \equiv b_j(1) \equiv b_j \pmod{m_j}.$$

Uniqueness: Suppose x and x' are two solutions. Then for each i, $x \equiv x' \pmod{m_i}$, which implies $m_i \mid (x - x')$. Since the m_i are pairwise coprime, their product M must divide $x - x'$ (by Theorem 3.2.3 (v)). Thus $x \equiv x' \pmod{M}$.

■

Example 4.2. Sun-Tzu's Problem. This theorem is famously associated with the Chinese mathematician Sun Zi (c. 3rd century AD), who posed the problem:

> "There are things of an unknown number. If we count them by threes, we have two left over; by fives, we have three left over; by sevens, two are left over. How many things are there?"

This corresponds to the system:

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

Here $n_1 = 3, n_2 = 5, n_3 = 7$. The moduli are pairwise coprime. The

total modulus is $N = 3 \times 5 \times 7 = 105$. We compute the partial products C_i and their modular inverses y_i:

1. $C_1 = 5 \times 7 = 35$. We solve $35y_1 \equiv 1 \pmod 3$. Reducing coefficients, $2y_1 \equiv 1 \pmod 3$. Multiplying by 2 gives $4y_1 \equiv y_1 \equiv 2 \pmod 3$. So $y_1 = 2$.
2. $C_2 = 3 \times 7 = 21$. We solve $21y_2 \equiv 1 \pmod 5$. Reducing coefficients, $y_2 \equiv 1 \pmod 5$. So $y_2 = 1$.
3. $C_3 = 3 \times 5 = 15$. We solve $15y_3 \equiv 1 \pmod 7$. Reducing coefficients, $y_3 \equiv 1 \pmod 7$. So $y_3 = 1$.

Using the construction in the proof of *Theorem 4.3*:

$$\begin{aligned} x &= 2(35)(2) + 3(21)(1) + 2(15)(1) \\ &= 140 + 63 + 30 \\ &= 233. \end{aligned}$$

Reducing modulo $N = 105$:

$$233 = 2 \times 105 + 23 \implies x \equiv 23 \pmod{105}.$$

Checking: $23 \equiv 2 \pmod 3$, $23 \equiv 3 \pmod 5$, $23 \equiv 2 \pmod 7$.

範例

Remark (Practical Reduction).

When solving congruences such as $15y_3 \equiv 1 \pmod 7$ in *Example 4.2*, one can reduce coefficients immediately. If the coefficient is coprime but greater than 1, for example $3x \equiv 7 \pmod{25}$, add multiples of the modulus to the right-hand side until divisibility is achieved:

$$3x \equiv 7 \equiv 32 \equiv 57 \pmod{25}.$$

Since $3 \mid 57$, we divide by 3 to find $x \equiv 19 \pmod{25}$.

Example 4.3. System with Composite Moduli. Consider the system:

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

Here $N = 4 \times 3 \times 5 = 60$.

1. $C_1 = 15$. Congruence: $15y_1 \equiv 1 \pmod 4 \implies 3y_1 \equiv -y_1 \equiv 1 \implies y_1 = -1 \equiv 3$.
2. $C_2 = 20$. Congruence: $20y_2 \equiv 1 \pmod 3 \implies 2y_2 \equiv -y_2 \equiv 1 \implies y_2 = -1 \equiv 2$.
3. $C_3 = 12$. Congruence: $12y_3 \equiv 1 \pmod 5 \implies 2y_3 \equiv 1 \pmod 5$. Note $2 \times 3 = 6 \equiv 1$, so $y_3 = 3$.

Constructing the solution:

$$\begin{aligned} x &= 1(15)(3) + 2(20)(2) + 3(12)(3) \\ &= 45 + 80 + 108 \\ &= 233. \end{aligned}$$

Reducing modulo 60:

$$233 = 3 \times 60 + 53 \implies x \equiv 53 \pmod{60}.$$

範例

If the moduli are not pairwise coprime, a solution may not exist. For instance, $x \equiv 1 \pmod 4$ and $x \equiv 2 \pmod 6$ is inconsistent, as the first implies x is odd while the second implies x is even. In general, a system $x \equiv a_i \pmod{n_i}$ is solvable if and only if $a_i \equiv a_j \pmod{(n_i, n_j)}$ for all pairs i, j. If solvable, the solution is unique modulo the least common multiple $[n_1, \ldots, n_k]$.

Corollary 4.2. *Solvability of Linear Systems.* Let $m_1, \ldots, m_k$ be pairwise coprime positive integers. The system of linear congruences

$$a_i x \equiv b_i \pmod{m_i} \quad (1 \le i \le k)$$

has a solution if and only if each individual congruence $a_i x \equiv b_i \pmod{m_i}$ is solvable.

推論

Proof

The condition is clearly necessary. Conversely, if each congruence is solvable, let x_i be a particular solution such that $a_i x_i \equiv b_i \pmod{m_i}$. The system then reduces to $x \equiv x_i \pmod{m_i/d_i}$ where $d_i = (a_i, m_i)$. Since the original moduli m_i are pairwise coprime, the reduced moduli m_i/d_i are also pairwise coprime. By *Theorem 4.3*, a simultaneous solution exists.

■

Applications and extensions

While the Chinese Remainder Theorem is often employed for systems $x \equiv b_i \pmod{m_i}$ where the coefficients of x are strictly 1, many problems involve coefficients, such as $a_i x \equiv b_i \pmod{m_i}$, or moduli that are not pairwise coprime. Consider a system of the form $c_i x \equiv d_i \pmod{n_i}$. Before applying the standard algorithm, each congruence must be simplified to the form $x \equiv a_i \pmod{m_i}$.

1. Check solvability for each congruence using Theorem 5.5.1: verify $(c_i, n_i) \mid d_i$.

2. Divide by (c_i, n_i) to reduce the modulus and coefficients.
3. Multiply by the modular inverse of the reduced coefficient of x to isolate x.

Example 4.4. System with Coefficients. Solve the system:

$$\begin{aligned} 7x &\equiv 3 \pmod{12} \\ 10x &\equiv 6 \pmod{14} \end{aligned}$$

For the first congruence, $(7, 12) = 1$. The inverse of $7 \pmod{12}$ is 7 (since $49 \equiv 1$). Thus:

$$x \equiv 7 \cdot 3 \equiv 21 \equiv 9 \pmod{12}.$$

For the second congruence, $(10, 14) = 2$, which divides 6. Dividing by 2:

$$5x \equiv 3 \pmod{7}.$$

The inverse of $5 \pmod{7}$ is 3 (since $15 \equiv 1$). Thus:

$$x \equiv 3 \cdot 3 \equiv 9 \equiv 2 \pmod{7}.$$

We now solve the reduced system:

$$\begin{aligned} x &\equiv 9 \pmod{12} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

Here $m_1 = 12, m_2 = 7$ are coprime. $M = 84$. $M_1 = 7, M_2 = 12$. Inverses: $7y_1 \equiv 1 \pmod{12} \implies y_1 = 7$. $12y_2 \equiv 1 \pmod{7} \implies 5y_2 \equiv 1 \implies y_2 = 3$. Solution:

$$x = 9(7)(7) + 2(12)(3) = 441 + 72 = 513.$$

Modulo 84: $513 = 6 \cdot 84 + 9$. Thus $x \equiv 9 \pmod{84}$.

範例

Non-Coprime Moduli If the moduli n_i are not pairwise coprime, the system can be solved by breaking each congruence into prime power components. A congruence $x \equiv a \pmod{p_1^{e_1} \dots p_k^{e_k}}$ is equivalent to the system $x \equiv a \pmod{p_j^{e_j}}$ for all j. After decomposing all moduli, one checks for consistency. For a fixed prime p, if we have conditions $x \equiv a \pmod{p^e}$ and $x \equiv b \pmod{p^f}$ with $e \leq f$, consistency requires $b \equiv a \pmod{p^e}$. If consistent, keep only the stronger condition $x \equiv b \pmod{p^f}$ and discard the weaker one. After this pruning for each prime, the remaining prime power moduli are pairwise coprime, so the Chinese Remainder Theorem applies.

Example 4.5. System with Non-Coprime Moduli. Solve the system

$$x \equiv 2 \pmod 6, \qquad x \equiv 5 \pmod 9.$$

Here $(6,9) = 3$ and $2 \equiv 5 \pmod 3$ is false ($2 \not\equiv 5$), so the system is inconsistent. However, consider the modified system:

$x \equiv 2 \pmod 6, \qquad x \equiv 5 \pmod 9 \to$ Replace with $x \equiv 8 \pmod 9$.

Decompose into prime powers:

$$x \equiv 2 \pmod 6 \implies x \equiv 0 \pmod 2, \quad x \equiv 2 \pmod 3,$$
$$x \equiv 8 \pmod 9 \implies x \equiv 8 \equiv 2 \pmod 3.$$

For the prime 3 we keep the stronger condition $x \equiv 8 \pmod 9$ and discard $x \equiv 2 \pmod 3$. The reduced system is

$$x \equiv 0 \pmod 2, \qquad x \equiv 8 \pmod 9.$$

These moduli are coprime. Solving gives $x \equiv 8 \pmod{18}$.

範例

Example 4.6. System with Non-Coprime Moduli and Coefficients. Consider the system:

$$5x \equiv 7 \pmod{12}, \quad 7x \equiv 1 \pmod{10}.$$

The moduli 12 and 10 are not coprime, so *Theorem 4.3* does not apply directly. We decompose the congruences into prime powers.

1. $5x \equiv 7 \pmod{12}$ implies:
   - $5x \equiv 7 \pmod 3 \implies 2x \equiv 1 \implies x \equiv 2 \pmod 3$.
   - $5x \equiv 7 \pmod 4 \implies x \equiv 3 \pmod 4$.
2. $7x \equiv 1 \pmod{10}$ implies:
   - $7x \equiv 1 \pmod 2 \implies x \equiv 1 \pmod 2$.
   - $7x \equiv 1 \pmod 5 \implies 2x \equiv 1 \implies x \equiv 3 \pmod 5$.

The conditions $x \equiv 3 \pmod 4$ and $x \equiv 1 \pmod 2$ are consistent (since $3 \equiv 1 \pmod 2$), and the condition modulo 4 implies the condition modulo 2. The system reduces to:

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

These moduli are pairwise coprime. Applying *Theorem 4.3*, we find $x \equiv 23 \pmod{60}$.

範例

4.3 *Applications*

Square Roots of Unity

Using the reduction to prime powers above together with the Chinese Remainder Theorem, we enumerate solutions to polynomial congruences. A fundamental case is the number of square roots of unity, that is, solutions to $x^2 \equiv 1 \pmod{n}$.

Proposition 4.1. ***Square Roots Modulo Prime Powers.***
Let p be a prime and $e \geq 1$. The number of solutions to $x^2 \equiv 1 \pmod{p^e}$ is:
- 2 if p is odd.
- 1 if $p = 2, e = 1$.
- 2 if $p = 2, e = 2$.
- 4 if $p = 2, e \geq 3$.

命題

Proof

The congruence is equivalent to $p^e \mid (x-1)(x+1)$.

- **Odd prime p:** $\gcd(x-1, x+1)$ divides $(x+1) - (x-1) = 2$. Since p is odd, p cannot divide both factors. Thus p^e must divide entirely $x-1$ or $x+1$, yielding $x \equiv \pm 1 \pmod{p^e}$.
- **$p = 2$:** Here $\gcd(x-1, x+1) = 2$ (assuming x is odd; if x is even, $x^2 \not\equiv 1$). Both factors are even. For $e = 1, 1 \equiv -1$, so one solution. For $e = 2, 1 \equiv -1 \pmod{2}$ but distinct modulo 4. $1^2 \equiv 1$, $3^2 \equiv 9 \equiv 1$. So two solutions. For $e \geq 3$, one factor is divisible by 2 and the other by 2^{e-1}. The solutions are $x \equiv \pm 1$ and $x \equiv 2^{e-1} \pm 1 \pmod{2^e}$.

■

Combining this with the Chinese Remainder Theorem, if $n = 2^e p_1^{e_1} \dots p_k^{e_k}$, the number of solutions is the product of the solution counts for each prime power.

Theorem 4.4. ***Number of Square Roots.***
The number of solutions to $x^2 \equiv 1 \pmod{n}$ is

$$\begin{cases} 2^{\omega(n)} & \text{if } n \text{ is odd or } 4 \mid n,\ 8 \nmid n, \\ 2^{\omega(n)-1} & \text{if } 2 \mid n,\ 4 \nmid n, \\ 2^{\omega(n)+1} & \text{if } 8 \mid n, \end{cases}$$

where $\omega(n)$ is the number of distinct prime factors of n.

定理

Divisibility of Power Sums

The Chinese Remainder Theorem allows us to prove properties of integers by verifying them modulo prime powers. We apply this to sums of powers.

Theorem 4.5. ***Divisibility of Power Sums.***
Let $n > 1$ be an odd integer and k a positive integer. If $(p-1) \nmid k$ for every prime divisor p of n, then

$$\sum_{i=1}^{n} i^k \equiv 0 \pmod{n}.$$

定理

Let $S_k(n) = \sum_{i=1}^{n} i^k$. We proceed by first establishing a lemma for the prime factors of n.

Claim 4.1. For every prime divisor p of n, there exists an integer a_p such that $p \nmid a_p$ and $p \nmid (a_p^k - 1)$.

主張

Proof of Claim

By hypothesis, $(p-1) \nmid k$. We apply the division algorithm to write $k = q(p-1) + r$ with $0 < r < p-1$. Consider the polynomial $x^r - 1$ over the field $\mathbb{F}_p$. By Lagrange's Theorem, it has at most r roots. Since $r < p-1$, there exists at least one non-zero residue $a_p \in \{1, \ldots, p-1\}$ such that $a_p^r \not\equiv 1 \pmod{p}$. By Fermat's Little Theorem, $a_p^{p-1} \equiv 1 \pmod{p}$, so

$$a_p^k = (a_p^{p-1})^q \cdot a_p^r \equiv 1^q \cdot a_p^r \equiv a_p^r \not\equiv 1 \pmod{p}.$$

Thus, $p \nmid (a_p^k - 1)$ and clearly $p \nmid a_p$.

証明終

General Case ($n \in \mathbb{Z}$).

Let $p_1, \ldots, p_m$ be the distinct prime factors of n. By the Claim, for each j, there exists an integer a_j such that $(a_j, p_j) = 1$ and $(a_j^k - 1, p_j) = 1$. We use the Chinese Remainder Theorem to construct a single integer a satisfying:

$$a \equiv a_j \pmod{p_j} \quad \text{for all } j = 1, \ldots, m.$$

For each prime factor p_j, we have $a \equiv a_j \not\equiv 0 \pmod{p_j}$ and $a^k - 1 \equiv a_j^k - 1 \not\equiv 0 \pmod{p_j}$. Consequently, no prime factor of n divides a or $a^k - 1$, implying

$$(a, n) = 1 \quad \text{and} \quad (a^k - 1, n) = 1.$$

Since $(a, n) = 1$, the map $x \mapsto ax$ permutes any complete set of

residues modulo n (Theorem 6.1.1 (i)). In particular, $\{0, 1, \ldots, n-1\}$ is a complete residue system. Thus:

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

Let $S'_k(n) = \sum_{x=0}^{n-1} x^k$. The equivalence above implies $(a^k - 1)S'_k(n) \equiv 0 \pmod{n}$. We relate $S'_k(n)$ back to $S_k(n)$. Since $k \geq 1$, $n^k \equiv 0 \pmod{n}$. Thus:

$$S_k(n) = \sum_{i=1}^{n-1} i^k + n^k \equiv \sum_{i=1}^{n-1} i^k + 0 = \sum_{x=0}^{n-1} x^k = S'_k(n) \pmod{n}.$$

Substituting this into our previous equation yields:

$$(a^k - 1)S_k(n) \equiv 0 \pmod{n}.$$

Since $(a^k - 1, n) = 1$, the integer $a^k - 1$ is invertible modulo n. Multiplying by its inverse gives

$$S_k(n) \equiv 0 \pmod{n}.$$

証明終

4.4 *Exercises*

1. **Linear Congruence Solvability.** Determine which of the following linear congruences have solutions. If a solution exists, find the general solution and the number of distinct solutions modulo the given modulus.
   (a) $12x \equiv 16 \pmod{20}$
   (b) $35x \equiv 14 \pmod{91}$
   (c) $21x \equiv 14 \pmod{35}$
2. **Systematic Solving (CRT).** Use the Chinese Remainder Theorem to solve the following systems. Express your answer as $x \equiv a \pmod{N}$.
   (a) $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$
   (b) $2x \equiv 1 \pmod{5}$, $3x \equiv 2 \pmod{7}$, $4x \equiv 1 \pmod{11}$
3. **Systems with Non-Coprime Moduli.** Solve the following systems. If inconsistent, state why.
   (a) $x \equiv 3 \pmod{10}$, $x \equiv 8 \pmod{15}$, $x \equiv 5 \pmod{84}$
   (b) $x \equiv 7 \pmod{9}$, $x \equiv 4 \pmod{12}$, $x \equiv 16 \pmod{21}$
   (c) $x \equiv 3 \pmod{8}$, $x \equiv 11 \pmod{20}$, $x \equiv 1 \pmod{15}$
4. **High-Power Remainders.**

(a) Compute the remainder when 3^{323} is divided by 28.
(b) Determine the last two digits of $7^{100} - 3^{100}$ in its decimal representation.
(c) Calculate the remainder when 2^{100} is divided by 319. (Note: $319 = 11 \times 29$).

5. Polynomial Roots and Solutions.

(a) Find all solutions to $x^3 + 2x + 3 \equiv 0 \pmod 5$.
(b) Find all solutions to $x^2 + x + 1 \equiv 0 \pmod 7$.
(c) Find all solutions to $x^2 \equiv 1 \pmod{360}$. Determine the total count using prime factorisation properties.
(d) Determine the number of solutions to $x^2 \equiv 1 \pmod{210}$.

6. Generalised Chinese Remainder Theorem. Let $m_1, \ldots, m_k$ be positive integers, not necessarily coprime. Let $a_1, \ldots, a_k$ be integers.

(a) Prove that the system $x \equiv a_i \pmod{m_i}$ for $i = 1, \ldots, k$ has a solution if and only if $(m_i, m_j) \mid (a_i - a_j)$ for all $i \neq j$.
(b) Prove that if a solution exists, it is unique modulo the least common multiple $[m_1, \ldots, m_k]$.

7. Structure of Residue Systems. Let $m_1, \ldots, m_k$ be pairwise coprime positive integers, and let $M = m_1 \ldots m_k$. Define $M_i = M/m_i$.

(a) Prove that the set

$$S = \left\{ \sum_{i=1}^{k} M_i x_i \;\middle|\; 0 \leq x_i < m_i \right\}$$

forms a complete residue system modulo M.
(b) Prove that if each x_i is restricted to a reduced residue system modulo m_i, then S forms a reduced residue system modulo M.
(c) Use part (b) to provide an alternative proof that the Euler totient function is multiplicative: $\varphi(M) = \varphi(m_1) \ldots \varphi(m_k)$.

8. Lagrange Interpolation Modulo p. Let p be a prime and let $(x_0, y_0), \ldots, (x_n, y_n)$ be $n + 1$ pairs of integers where $x_i \not\equiv x_j \pmod p$ for $i \neq j$. Prove that there exists a unique polynomial $f(x) \in \mathbb{F}_p[x]$ of degree at most n such that $f(x_i) \equiv y_i \pmod p$ for all i.

9. Polynomial Mappings. Let p be a prime and k a positive integer such that $(k, p - 1) = 1$.

(a) Prove that the map $f : \mathbb{F}_p \to \mathbb{F}_p$ defined by $f(x) = x^k$ is a bijection.
(b) Conclude that for every $a \in \mathbb{F}_p$, the congruence $x^k \equiv a \pmod p$ has a unique solution given by $x \equiv a^u \pmod p$,

where u is the modular inverse of k modulo $p-1$.

10. **Euler's Criterion for Quadratic Residues.** Let p be an odd prime and a an integer not divisible by p.
    (a) Prove that if $x^2 \equiv a \pmod{p}$ has a solution, then $a^{(p-1)/2} \equiv 1 \pmod{p}$.
    (b) Prove that if $x^2 \equiv a \pmod{p}$ has no solution, then $a^{(p-1)/2} \equiv -1 \pmod{p}$.

11. **The Legendre Symbol Sum.** Let p be an odd prime. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined as 1 if a is a quadratic residue modulo p, -1 if it is a quadratic non-residue, and 0 if $p \mid a$. Prove that:

$$\sum_{x=1}^{p-1} \left(\frac{x^2+x}{p}\right) = -1.$$

12. **Linear Congruence Practice.** Solve the following congruence equations.
    (a) $32x \equiv 12 \pmod{8}$
    (b) $28x \equiv 124 \pmod{116}$
    (c) $5x \equiv 44 \pmod{81}$

13. **System Practice.** Solve the following systems of linear congruences.
    (a) $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$, $x \equiv 2 \pmod{7}$
    (b) $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{9}$

14. **CRT with Coefficients.** Use the Chinese Remainder Theorem to solve the congruence equation $37x \equiv 31 \pmod{77}$.

15. **Idempotent Elements.** An element $e \in \mathbb{Z}/n\mathbb{Z}$ is called an *idempotent* if $e^2 \equiv e \pmod{n}$.
    (a) Find all idempotents modulo 6 and modulo 12.
    (b) Let $n = p_1 p_2 \dots p_k$ be a product of distinct primes. Determine the number of idempotents modulo n.
    (c) Prove that if e is a non-trivial idempotent ($e \not\equiv 0, 1$), then n must be composite and $\gcd(e, n) > 1$.

16. **CRT Constructions.**
    (a) **Visibility:** Use the CRT to prove that for any $k \geq 1$, there exists a $k \times k$ square grid of points in $\mathbb{Z}^2$, none of which are visible from the origin (i.e., $\gcd(x, y) > 1$ for all points in the grid).
    (b) **Square-Free Blocks:** Use the CRT to prove that for any $k \geq 1$, there exist k consecutive integers $n, n+1, \dots, n+k-1$ such that each integer in the block is divisible by a perfect square

greater than 1.

17. Coprimes in Arithmetic Progressions. Let a, b be coprime integers and m a positive integer.

(a) Let P be the product of all prime factors of m that do not divide b. Construct a linear congruence involving b, P, a.
(b) Show that there exists an integer k such that $(a + kb, m) = 1$.
(c) Conclude that the arithmetic progression $a, a + b, a + 2b, \ldots$ contains infinitely many terms coprime to m.

18. Fixed Points of the Inversion Map. Let $N(n)$ denote the number of solutions to $x^2 \equiv 1 \pmod{n}$. Prove that the product of the solutions to $x^2 \equiv 1 \pmod{n}$ is congruent to $-1 \pmod{n}$ if $N(n) = 2$, and $1 \pmod{n}$ if $N(n) > 2$.

5
Primitive Roots and Group Structure

We now investigate the internal structure of the set of reduced residue classes modulo m, denoted by $(\mathbb{Z}/m\mathbb{Z})^\times$. Our primary objective is to determine when this group is cyclic, a property intimately linked to the existence of generators known as primitive roots. This inquiry synthesises the results from *chapter 2* regarding Euler's Theorem and *chapter 4* concerning polynomial roots.

5.1 *The Order of an Integer*

Recall from Euler's Theorem that for any integer a coprime to $m > 1$, we have $a^{\varphi(m)} \equiv 1 \pmod{m}$. This implies that the powers of a cycle periodically. We formalise the length of this cycle.

Definition 5.1. ***Multiplicative Order.***
Let $m > 1$ and let a be an integer such that $(a, m) = 1$. The *multiplicative order* of a modulo m, denoted $\mathrm{ord}_m(a)$, is the smallest positive integer n such that

$$a^n \equiv 1 \pmod{m}.$$

In the context of the group $(\mathbb{Z}/m\mathbb{Z})^\times$, this is precisely the order of the element $[a]$.

定義

The existence of such an integer $n \leq \varphi(m)$ is guaranteed by Euler's Theorem. The fundamental divisibility property of the order is given by the following lemma.

Lemma 5.1. ***Properties of Order.***
Let $(a, m) = 1$.

(i) There exists a positive integer $n < m$ such that $a^n \equiv 1 \pmod{m}$.

(ii) Let $n = \mathrm{ord}_m(a)$. Then for integers k and l,

$$a^k \equiv a^l \pmod{m} \iff k \equiv l \pmod{n}.$$

In particular, $a^k \equiv 1 \pmod{m}$ if and only if $n \mid k$.

引理

Proof

(i) Consider the sequence of powers $a, a^2, \dots, a^m$. Since $(a, m) = 1$, each power is coprime to m. By the pigeonhole principle, there must exist distinct indices $1 \le l < k \le m$ such that $a^k \equiv a^l \pmod{m}$. This implies

$$a^l(a^{k-l} - 1) \equiv 0 \pmod{m}.$$

Since $(a^l, m) = 1$, we may cancel a^l (by the Cancellation Law) to obtain $a^{k-l} \equiv 1 \pmod{m}$. Setting $n = k - l$, we have $1 \le n < m$.

(ii) Let n be the smallest positive integer such that $a^n \equiv 1 \pmod{m}$. Suppose $a^k \equiv a^l \pmod{m}$ with $k \ge l$. Let $N = k - l$. Then $a^N \equiv 1 \pmod{m}$. By the *The Division Algorithm*, we can write $N = nq + r$ with $0 \le r < n$. Then

$$a^N = a^{nq+r} = (a^n)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{m}.$$

Thus $a^r \equiv 1 \pmod{m}$. Since $0 \le r < n$ and n is the minimal positive exponent yielding 1, we must have $r = 0$. Therefore, $n \mid N$, or $k \equiv l \pmod{n}$. The converse is immediate.

■

It follows directly that $\mathrm{ord}_m(a)$ must divide $\varphi(m)$.

Definition 5.2. ***Primitive Root.***
If there exists an integer g such that $\mathrm{ord}_m(g) = \varphi(m)$, then g is called a *primitive root* modulo m. If g is a primitive root, the set of powers $\{g, g^2, \dots, g^{\varphi(m)}\}$ contains $\varphi(m)$ distinct integers coprime to m. Since $|(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$, these powers constitute a reduced residue system modulo m. Algebraically, this means the group $(\mathbb{Z}/m\mathbb{Z})^\times$ is a *cyclic group* generated by g.

定義

5.2 *Primitive Roots Modulo Primes*

Not every modulus admits a primitive root. However, the structure is particularly elegant when the modulus is a prime p. To establish existence, we first analyse how the order changes when raising an element to a power.

Lemma 5.2. ***Order of Powers.***
Let $(a, m) = 1$ and let $n = \mathrm{ord}_m(a)$. Then for any integer k,

$$\mathrm{ord}_m(a^k) = \frac{n}{(k, n)}.$$

In particular, $\text{ord}_m(a^k) = n$ if and only if $(k, n) = 1$.

引理

Proof

Let L be the order of a^k. By Lemma 8.1.1 (ii), the congruence $(a^k)^L \equiv 1 \pmod{m}$ is equivalent to $n \mid kL$. Dividing by $d = (k, n)$, this condition becomes

$$\frac{n}{d} \mid L\frac{k}{d}.$$

Since n/d and k/d are coprime, it follows that $\frac{n}{d} \mid L$. Thus the smallest positive L is exactly $\frac{n}{d}$.

■

Theorem 5.1. ***Existence of Primitive Roots Modulo*** p**.**
For every odd prime p, there exists a primitive root modulo p.

定理

Proof

The orders of the elements $1, 2, \ldots, p-1$ modulo p are all divisors of $\varphi(p) = p - 1$. For each divisor d of $p - 1$, define the set

$$S(d) = \{x \in \{1, \ldots, p-1\} \mid \text{ord}_p(x) = d\}.$$

Let $R_d = |S(d)|$. Since every element has a unique order, the sets $S(d)$ partition the non-zero residues:

$$\sum_{d|p-1} R_d = p - 1.$$

We recall Gauss's Summation Formula: $\sum_{d|p-1} \varphi(d) = p - 1$. Thus, it suffices to prove that $R_d \leq \varphi(d)$ for all d. If this inequality holds, the equality of the sums forces $R_d = \varphi(d)$ for all d.
The elements of $S(d)$ satisfy $x^d \equiv 1 \pmod{p}$. By Lagrange's Theorem, the polynomial $x^d - 1$ has at most d roots in $\mathbb{Z}/p\mathbb{Z}$. If $S(d)$ is empty, then $R_d = 0 \leq \varphi(d)$. If $S(d)$ is not empty, there exists an element a of order d. By Lemma 8.1.1, the d powers $1, a, \ldots, a^{d-1}$ are distinct modulo p and satisfy $(a^k)^d = (a^d)^k \equiv 1 \pmod{p}$. Thus, these powers are precisely the d roots of $x^d - 1 \equiv 0 \pmod{p}$. Consequently, any element of order d must be of the form a^k. By *lemma* 5.2, a^k has order d if and only if $(k, d) = 1$. The number of such exponents k with $1 \leq k \leq d$ is $\varphi(d)$. Thus, if $R_d > 0$, then $R_d = \varphi(d)$. Since $R_d \leq \varphi(d)$ for all d, we conclude that $R_d = \varphi(d)$ for all divisors d. In particular, $R_{p-1} = \varphi(p-1) \geq 1$. Hence, there exists at least one element of order $p - 1$.

■

Example 5.1. Finding Primitive Roots. Consider $p = 13$. We have $\varphi(13) = 12$. The possible orders are divisors of 12: $1, 2, 3, 4, 6, 12$. We test $a = 2$:

$$\begin{aligned} 2^1 &\equiv 2 \\ 2^2 &\equiv 4 \\ 2^3 &\equiv 8 \\ 2^4 &= 16 \equiv 3 \\ 2^6 &= 2^4 \cdot 2^2 \equiv 3 \cdot 4 = 12 \equiv -1. \end{aligned}$$

Since $2^6 \equiv -1 \not\equiv 1$, the order is not $1, 2, 3$, or 6. Since $2^4 \equiv 3 \not\equiv 1$, the order is not 4. Thus $\operatorname{ord}_{13}(2) = 12$, and 2 is a primitive root. There are exactly $\varphi(\varphi(13)) = \varphi(12) = 4$ primitive roots modulo 13. They are $2^1, 2^5, 2^7, 2^{11}$.

範例

Having established the existence of primitive roots for primes, we extend this result to powers of primes.

Theorem 5.2. ***Primitive Roots Modulo*** p^l**.**
Let p be an odd prime. For any integer $l \geq 1$, there exists a primitive root modulo p^l.

定理

Proof

We construct a primitive root modulo p^l by lifting a primitive root modulo p.

Step 1. Selection of generator modulo p^2**.** Let g be a primitive root modulo p. We claim that either g or $g + p$ is a primitive root modulo p^2. The order of g modulo p^2, let us call it d, must divide $\varphi(p^2) = p(p-1)$. Also, $g^d \equiv 1 \pmod{p^2}$ implies $g^d \equiv 1 \pmod{p}$, so $p - 1 \mid d$. Thus d is either $p - 1$ or $p(p-1)$. If $d = p(p-1)$, g is a primitive root. Suppose $d = p - 1$, i.e., $g^{p-1} \equiv 1 \pmod{p^2}$. Consider $g_0 = g + p$. Since $g_0 \equiv g \pmod{p}$, g_0 is a primitive root modulo p. Using the Binomial Theorem:

$$(g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \cdots \equiv 1 + (p-1)pg^{p-2} \pmod{p^2}.$$

Since $(g, p) = 1$, we have $(p-1)pg^{p-2} \not\equiv 0 \pmod{p^2}$. Thus $(g+p)^{p-1} \not\equiv 1 \pmod{p^2}$. It follows that the order of g_0 modulo p^2 must be $p(p-1)$. We designate this element (either g or $g + p$) as g.

Step 2. Inductive Lifting. We prove by induction that for any $r \geq$

1,

$$g^{\varphi(p^r)} = 1 + k_r p^r \quad \text{where } p \nmid k_r.$$

For $r = 1$, this holds by our choice of g in Step 1 (as $g^{p-1} \not\equiv 1 \pmod{p^2}$). Assume the statement holds for r. Then

$$g^{\varphi(p^{r+1})} = (g^{\varphi(p^r)})^p = (1 + k_r p^r)^p = 1 + p(k_r p^r) + \binom{p}{2}(k_r p^r)^2 + \dots$$

Modulo p^{r+2}, terms with p^{2r} vanish (since $2r \geq r+2$ for $r \geq 2$, and the binomial coefficient provides an extra p for $r = 1$). Thus:

$$g^{\varphi(p^{r+1})} \equiv 1 + k_r p^{r+1} \pmod{p^{r+2}}.$$

Setting $k_{r+1} = k_r$, we have $p \nmid k_{r+1}$.

Step 3. Conclusion. Let d be the order of g modulo p^l. Then $d \mid \varphi(p^l) = p^{l-1}(p-1)$. Since g is primitive modulo p, $p - 1 \mid d$. Thus $d = p^s(p-1)$ for some $s < l$. By our inductive result, $g^{\varphi(p^s)} = 1 + k_s p^s \not\equiv 1 \pmod{p^{s+1}}$. For g to satisfy $g^d \equiv 1 \pmod{p^l}$, we must have the exponent large enough to cover the modulus. The derivation implies we need $s = l - 1$. Thus $d = \varphi(p^l)$.

■

The case for double prime powers follows easily from the odd prime case.

Theorem 5.3. ***Primitive Roots Modulo*** $2p^l$**.**
Let p be an odd prime and $l \geq 1$. There exists a primitive root modulo $2p^l$.

定理

Proof

Let g be a primitive root modulo p^l. Let g_0 be the odd integer in $\{g, g + p^l\}$. Since $(g_0, 2) = 1$ and $(g_0, p^l) = 1$, we have $(g_0, 2p^l) = 1$. The order of g_0 modulo $2p^l$, say d, divides $\varphi(2p^l) = \varphi(2)\varphi(p^l) = \varphi(p^l)$. Conversely, $g_0^d \equiv 1 \pmod{2p^l}$ implies $g_0^d \equiv 1 \pmod{p^l}$. Since $g_0 \equiv g \pmod{p^l}$, d must be a multiple of $\varphi(p^l)$. Therefore $d = \varphi(2p^l)$, and g_0 is a primitive root.

■

5.3 *Classification and Non-Existence*

We have shown that primitive roots exist for moduli $2, 4, p^l, 2p^l$. We now demonstrate that these are the *only* moduli that admit primitive

roots.

Lemma 5.3. ***Non-Existence Criteria.***
There is no primitive root modulo m if:
(i) $m = 2^l$ with $l \geq 3$.
(ii) m is divisible by two distinct odd primes.
(iii) $m = 2^l p^k$ where $l \geq 2$ and p is an odd prime.

引理

Proof

(i) Let $m = 2^l$ with $l \geq 3$. The units modulo 2^l are the odd integers. For any odd integer a, induction shows $a^{2^{l-2}} \equiv 1 \pmod{2^l}$. Since $\varphi(2^l) = 2^{l-1}$, the maximum order is at most $\varphi(m)/2$. Thus no element has order $\varphi(m)$.
(ii) Suppose $m = rs$ where $(r, s) = 1$ and $r, s > 2$. For any a coprime to m, we have $a^{\varphi(r)} \equiv 1 \pmod{r}$ and $a^{\varphi(s)} \equiv 1 \pmod{s}$. Let $L = [\varphi(r), \varphi(s)]$. Then $a^L \equiv 1 \pmod{m}$. Since $r, s > 2$, both $\varphi(r)$ and $\varphi(s)$ are even. Therefore:

$$L = \frac{\varphi(r)\varphi(s)}{(\varphi(r), \varphi(s))} \leq \frac{\varphi(r)\varphi(s)}{2} = \frac{\varphi(m)}{2}.$$

Thus no integer has order $\varphi(m)$. This covers cases where m has two distinct odd primes (take r, s as prime powers) or $m = 2^l p^k$ with $l \geq 2$ (take $r = 2^l, s = p^k$, noting $\varphi(4) = 2$ is even).

■

Theorem 5.4. ***The Primitive Root Theorem.***
An integer $m > 1$ possesses a primitive root if and only if

$$m = 2, \quad 4, \quad p^l, \quad \text{or} \quad 2p^l,$$

where p is an odd prime and $l \geq 1$.

定理

Proof

The sufficiency follows from Theorems 5.1, 5.2, and 5.3, along with the trivial cases $m = 2$ (1 is primitive) and $m = 4$ (3 is primitive). The necessity is provided by *lemma* 5.3, which eliminates all other composite numbers.

■

Example 5.2. Failure of Primitive Roots. Consider $m = 15 = 3 \times 5$. $\varphi(15) = \varphi(3)\varphi(5) = 2 \times 4 = 8$. The units are $\{1, 2, 4, 7, 8, 11, 13, 14\}$. We compute the orders:
· $2^4 = 16 \equiv 1 \pmod{15}$.

· $4^2 = 16 \equiv 1 \pmod{15}$.
· $7^2 = 49 \equiv 4$, $7^4 \equiv 16 \equiv 1 \pmod{15}$.
Every element a satisfies $a^4 \equiv 1 \pmod{15}$. The maximum order is $4 < 8$. The group $(\mathbb{Z}/15\mathbb{Z})^\times$ is not cyclic; it is isomorphic to $C_2 \times C_4$.

範例

We this section conclude with a counting result for elements of specific orders.

Proposition 5.1. ***Count of Elements of Order*** d**.**
If m possesses a primitive root, then for every divisor d of $\varphi(m)$, there are exactly $\varphi(d)$ elements of order d modulo m.

命題

Proof

Let g be a primitive root. The reduced residues are $\{g^1, g^2, \ldots, g^{\varphi(m)}\}$. By *lemma 5.2*, the order of g^k is

$$\frac{\varphi(m)}{(k, \varphi(m))}.$$

This order equals d if and only if

$$(k, \varphi(m)) = \frac{\varphi(m)}{d}.$$

Let $k = a \cdot \frac{\varphi(m)}{d}$. Then the condition becomes $(a, d) = 1$ with $1 \leq a \leq d$. There are exactly $\varphi(d)$ such integers a.

■

5.4 *Discrete Logarithms*

The existence of primitive roots allows us to linearise multiplicative arithmetic modulo n by transforming exponentiation into multiplication and multiplication into addition. This structural isomorphism is analogous to the theory of logarithms in real analysis.

Definition 5.3. ***Discrete Logarithm.***
Let n be an integer admitting a primitive root g. For any integer a coprime to n, the unique integer k such that

$$a \equiv g^k \pmod{n}, \quad 0 \leq k < \varphi(n),$$

is called the *index* or *discrete logarithm* of a relative to the base g. We denote this by $\operatorname{ind}_g(a)$ or simply $\operatorname{ind}(a)$ if the base is fixed.

定義

This mapping establishes a group isomorphism between the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ and the additive group $\mathbb{Z}/\varphi(n)\mathbb{Z}$. Consequently, the properties of indices mirror those of logarithms.

Theorem 5.5. ***Properties of Indices.***
Let n possess a primitive root g, and let a, b be integers coprime to n.

(i) $\operatorname{ind}_g(1) \equiv 0 \pmod{\varphi(n)}$ and $\operatorname{ind}_g(g) \equiv 1 \pmod{\varphi(n)}$.

(ii) $\operatorname{ind}_g(ab) \equiv \operatorname{ind}_g(a) + \operatorname{ind}_g(b) \pmod{\varphi(n)}$.

(iii) $\operatorname{ind}_g(a^k) \equiv k \cdot \operatorname{ind}_g(a) \pmod{\varphi(n)}$ for any $k \in \mathbb{Z}$.

(iv) **Change of Base:** If g_1 is another primitive root modulo n, then

$$\operatorname{ind}_g(a) \equiv \operatorname{ind}_{g_1}(a) \cdot \operatorname{ind}_g(g_1) \pmod{\varphi(n)}.$$

定理

Proof

Let $u = \operatorname{ind}_g(a)$ and $v = \operatorname{ind}_g(b)$. Then $a \equiv g^u$ and $b \equiv g^v \pmod{n}$.

(i) $g^0 \equiv 1$ and $g^1 \equiv g$ are immediate from the definition.

(ii) The product $ab \equiv g^u g^v = g^{u+v} \pmod{n}$. By Lemma 8.1.1 (ii), $g^x \equiv g^y \pmod{n}$ if and only if $x \equiv y \pmod{\varphi(n)}$. Thus $\operatorname{ind}(ab) \equiv u + v \pmod{\varphi(n)}$.

(iii) Follows from (ii) by induction.

(iv) Let $x = \operatorname{ind}_{g_1}(a)$ and $y = \operatorname{ind}_g(g_1)$. Then $a \equiv g_1^x$ and $g_1 \equiv g^y \pmod{n}$. Substitution yields $a \equiv (g^y)^x = g^{xy} \pmod{n}$. Thus $\operatorname{ind}_g(a) \equiv xy \pmod{\varphi(n)}$.

■

Discrete logarithms provide a systematic method for analysing binomial congruences of the form $x^k \equiv a \pmod{n}$. If such a congruence has a solution, a is called a *k-th power residue* modulo n.

Theorem 5.6. ***Solvability of*** $x^k \equiv a$.
Let n be an integer having a primitive root, and let $(a, n) = 1$. Let $d = (k, \varphi(n))$.

(i) The congruence $x^k \equiv a \pmod{n}$ has solutions if and only if $d \mid \operatorname{ind}_g(a)$. Equivalently, solutions exist if and only if Euler's criterion is satisfied:

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

(ii) If solutions exist, there are exactly d distinct solutions modulo n.

(iii) The number of k-th power residues modulo n is $\frac{\varphi(n)}{d}$.

定理

Proof

Let g be a primitive root. Taking indices with respect to g, the con-

gruence $x^k \equiv a \pmod{n}$ transforms into the linear congruence in $y = \text{ind}_g(x)$:

$$k \cdot y \equiv \text{ind}_g(a) \pmod{\varphi(n)}.$$

(i) By the theory of linear congruences (Theorem 5.3.1), this equation is solvable if and only if $d = (k, \varphi(n))$ divides the constant term $\text{ind}_g(a)$. To see the equivalence with the power condition: $d \mid \text{ind}_g(a)$ implies $\frac{\varphi(n)}{d}\text{ind}_g(a) \equiv 0 \pmod{\varphi(n)}$. Exponentiating base g:

$$a^{\varphi(n)/d} \equiv g^0 \equiv 1 \pmod{n}.$$

(ii) If solvable, the linear congruence in indices has exactly d solutions modulo $\varphi(n)$. Since the index map is a bijection, these correspond to d distinct residues x modulo n.

(iii) The indices of k-th power residues are precisely the multiples of d in $\{0, \ldots, \varphi(n) - 1\}$. There are $\varphi(n)/d$ such multiples.

■

Example 5.3. Cubic Residues Modulo 11. Solve the congruence $x^3 \equiv 3 \pmod{11}$. Here $n = 11$, so $\varphi(11) = 10$. We use the primitive root $g = 2$. We compute the index of 3. Powers of 2 mod 11: $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3$. Thus $\text{ind}_2(3) = 8$. The discrete logarithm equation is:

$$3 \cdot \text{ind}_2(x) \equiv 8 \pmod{10}.$$

We check solvability: $d = (3, 10) = 1$. Since $1 \mid 8$, a solution exists. Multiplying by the inverse of 3 modulo 10 (which is 7):

$$\text{ind}_2(x) \equiv 8 \cdot 7 = 56 \equiv 6 \pmod{10}.$$

The unique index is 6. Retrieving x:

$$x \equiv 2^6 \equiv 9 \pmod{11}.$$

Checking: $9^3 = 729$. $729 = 66 \times 11 + 3$, so $9^3 \equiv 3 \pmod{11}$.

範例

5.5 *The Structure of* $(\mathbb{Z}/2^k\mathbb{Z})^\times$

The Primitive Root Theorem establishes that $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is not cyclic for $k \geq 3$. To complete the description of the multiplicative group of integers, we determine the structure of this group. While it lacks a single generator, we show it is generated by two elements: -1 and 5.

Lemma 5.4. ***Order of 5 Modulo*** 2^k**.**
For any integer $k \geq 3$, the order of 5 modulo 2^k is 2^{k-2}.

引理

Proof

We prove by induction that for all integers $m \geq 0$:

$$5^{2^m} \equiv 1 + 2^{m+2} \pmod{2^{m+3}}.$$

Base Case ($m = 0$): $5^1 = 1 + 4 = 1 + 2^2$. The congruence $5 \equiv 5 \pmod 8$ holds.

Inductive Step: Assume $5^{2^m} = 1 + j2^{m+2}$ where j is odd. Squaring both sides:

$$\begin{aligned} 5^{2^{m+1}} &= (1 + j2^{m+2})^2 \\ &= 1 + 2(j2^{m+2}) + (j2^{m+2})^2 \\ &= 1 + j2^{m+3} + j^2 2^{2m+4}. \end{aligned}$$

Since $m \geq 0$, we have $2m + 4 \geq m + 4$. Thus, modulo 2^{m+4}, the term $j^2 2^{2m+4}$ vanishes:

$$5^{2^{m+1}} \equiv 1 + j2^{m+3} \pmod{2^{m+4}}.$$

Since j is odd, the induction hypothesis is preserved.

Let $n = \operatorname{ord}_{2^k}(5)$. Applying the lemma with $m = k - 4$ (for $k \geq 4$), we find $5^{2^{k-3}} = 1 + j2^{k-1} \not\equiv 1 \pmod{2^k}$. Applying the lemma with $m = k - 3$, we find $5^{2^{k-2}} = 1 + j2^k \equiv 1 \pmod{2^k}$. Thus, the order divides 2^{k-2} but does not divide 2^{k-3}. The order is exactly 2^{k-2}.
(For the case $k = 3$, the order of 5 modulo 8 is $2 = 2^{3-2}$, consistent with the result).

■

Theorem 5.7. ***Structure of*** $(\mathbb{Z}/2^k\mathbb{Z})^\times$**.**
For $k \geq 3$, the group $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is isomorphic to $C_2 \times C_{2^{k-2}}$. Specifically, every odd integer a satisfies a unique representation modulo 2^k:

$$a \equiv (-1)^s 5^t \pmod{2^k},$$

where $s \in \{0, 1\}$ and $t \in \{0, 1, \ldots, 2^{k-2} - 1\}$.

定理

Proof

The group $(\mathbb{Z}/2^k\mathbb{Z})^\times$ has order $\varphi(2^k) = 2^{k-1}$. Let $H = \langle 5 \rangle$. By *lemma 5.4*, $|H| = 2^{k-2}$. Let $K = \langle -1 \rangle = \{1, -1\}$. Since $-1 \equiv 2^k - 1 \pmod{2^k}$, its order is 2. We claim $H \cap K = \{1\}$. Elements of

H satisfy $5^t \equiv 1 \pmod 4$ (since $5 \equiv 1 \pmod 4$). However, elements of $K \setminus \{1\}$ satisfy $-1 \equiv 3 \pmod 4$. Thus $-1 \notin H$. The product of the orders is $|K| \cdot |H| = 2 \cdot 2^{k-2} = 2^{k-1}$, which equals the order of the full group. Since $H \cap K = \{1\}$ and the group is abelian, $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong K \times H \cong C_2 \times C_{2^{k-2}}$.

■

Example 5.4. Generators of U_{16}. Let $n = 16 = 2^4$. The group order is 8. The powers of 5 modulo 16 are:

$$5^1 \equiv 5, \quad 5^2 = 25 \equiv 9, \quad 5^3 = 45 \equiv 13, \quad 5^4 \equiv 1.$$

Multiplying these by $-1 \equiv 15$:

$$15 \cdot 1 \equiv 15, \quad 15 \cdot 5 = 75 \equiv 11, \quad 15 \cdot 9 = 135 \equiv 7, \quad 15 \cdot 13 = 195 \equiv 3.$$

The set $\{1, 3, 5, 7, 9, 11, 13, 15\}$ accounts for all units. Any odd number a can be written as $(-1)^s 5^t$. For example, $3 \equiv -1 \cdot 5^3 \equiv 15 \cdot 13 \pmod{16}$.

範例

Combining this with the decomposition for odd prime powers, we obtain the general structure of the unit group.

Theorem 5.8. ***General Structure of Unit Groups.***
Let the prime factorisation of n be $n = 2^k p_1^{e_1} \dots p_r^{e_r}$. The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ decomposes as:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong G_2 \times C_{\varphi(p_1^{e_1})} \times \cdots \times C_{\varphi(p_r^{e_r})},$$

where

$$G_2 \cong \begin{cases} \{1\} & \text{if } k = 0, 1 \\ C_2 & \text{if } k = 2 \\ C_2 \times C_{2^{k-2}} & \text{if } k \geq 3. \end{cases}$$

定理

Proof

This follows directly from the Chinese Remainder Theorem, which provides the ring isomorphism $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/2^k\mathbb{Z} \times \prod \mathbb{Z}/p_i^{e_i}\mathbb{Z}$. Restricting to the group of units yields the direct product of the unit groups of each component. The structure of $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ is cyclic (*Theorem 5.2*), and the structure of $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is given by *Theorem 5.7*.

■

5.6 *Exercises*

In the following exercises, unless otherwise specified, p denotes an odd prime and n denotes a positive integer.

1. **Orders of Products and Inverses.** Let n be a positive integer.
   (a) Prove that for any a coprime to n, the order of a modulo n is equal to the order of its modular inverse a^{-1} modulo n.
   (b) Let $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$ with multiplicative orders k and m respectively. Prove that if $(k, m) = 1$, then the order of the product ab is km.
   (c) Show by example that if $(k, m) \neq 1$, the order of ab need not be $\operatorname{lcm}(k, m)$.
   (d) Prove generally that there exists an element $c \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\operatorname{ord}_n(c) = \operatorname{lcm}(k, m)$.

   > *Remark.*
   > Write k and m in terms of prime powers and construct c using powers of a and b that have coprime orders.

2. **Order Modulo a Product.** Let m and n be coprime positive integers. Let the order of an integer a modulo m be d_1 and modulo n be d_2.
   (a) Prove that the order of a modulo mn is $\operatorname{lcm}(d_1, d_2)$.
   (b) Using this result, prove that for any integer $n > 1$, $\varphi(n) > \sqrt{n}$.
   (c) Prove that $n \mid \varphi(a^n - 1)$ for any $a > 1$.

3. **The Lucas Primality Test.** The converse of Fermat's Little Theorem is false. However, primitive roots provide a deterministic test for primality.
   (a) Prove that an integer $n > 1$ is prime if and only if there exists an integer a satisfying:
      (i) $a^{n-1} \equiv 1 \pmod{n}$, and
      (ii) $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all prime factors q of $n - 1$.

   > *Remark.*
   > What does condition (ii) imply about the order of a modulo n?

   (b) Use this criterion (or similar reasoning) to find a primitive root modulo 7^2 and modulo 5^3.

4. ⋆ **Special Primes.** Primitive roots allow us to analyse divisors of special forms.
   (a) Let $a > 2$. Prove that any prime divisor of $a^p - 1$ that does not divide $a - 1$ must be of the form $2kp + 1$.

(b) Deduce that there are infinitely many primes of the form $2p + 1$ (assuming one can vary a). More rigorously, prove there are infinitely many primes of the form $2px + 1$ by considering Euclidean polynomials.

(c) Let $F_n = 2^{2^n} + 1$ be the n-th Fermat number. Prove that every prime divisor of F_n is of the form $2^{n+1}k + 1$.

5. Operations on Primitive Roots. Let g be a primitive root modulo an odd prime p.

(a) Determine the multiplicative order of $-g$ modulo p.

> *Remark.*
>
> Consider the cases $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$ separately.

(b) Prove that if $p > 3$, the product of any two primitive roots modulo p is *never* a primitive root.

> *Remark.*
>
> Consider the parity of the indices.

6. ⋆ Aggregate Properties of Primitive Roots. Let $p > 3$ be a prime. Let P be the set of all primitive roots modulo p.

(a) Prove that the product of all primitive roots is congruent to 1 modulo p:

$$\prod_{g \in P} g \equiv 1 \pmod p.$$

(b) Prove that the sum of all incongruent primitive roots modulo p is congruent to $\mu(p-1) \pmod p$, where μ is the Möbius function (defined in Chapter 3 Exercises).

> *Remark.*
>
> Recall that the primitive roots are the roots of $x^{p-1} - 1$ that are not roots of $x^d - 1$ for any $d \mid p - 1$.

7. Criteria for Lifting. In the proof of the existence of primitive roots modulo p^2, we often show that if g is a primitive root modulo p, then either g or $g + p$ is a primitive root modulo p^2. Prove the stronger condition: A primitive root g modulo p is a primitive root modulo p^2 *if and only if*

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

> *Remark.*
>
> We proved the forward implication. For the reverse, assume $g^{p-1} = 1 + mp$. What does the condition $(m, p) = 1$ imply about the order?

8. **Power Sums.** Let p be a prime and k be a positive integer. Let $S_k = \sum_{x=1}^{p-1} x^k$. Using the existence of a primitive root g modulo p, prove that:
$$S_k \equiv \begin{cases} -1 \pmod{p} & \text{if } (p-1) \mid k, \\ 0 \pmod{p} & \text{if } (p-1) \nmid k. \end{cases}$$

> *Remark.*
> Express the sum as a geometric series in terms of g.

9. **Wilson's Theorem and Generalisations.**
   (a) Use the existence of a primitive root modulo p to provide a constructive proof of Wilson's Theorem: $(p-1)! \equiv -1 \pmod{p}$.
   (b) Let $p \equiv 2 \pmod 3$. Prove that for any integers a, b, the congruence $a^3 \equiv b^3 \pmod{p}$ implies $a \equiv b \pmod{p}$.
   (c) Generalise part (b): Prove that the map $x \mapsto x^k$ is a permutation of $(\mathbb{Z}/p\mathbb{Z})^\times$ if and only if $(k, p-1) = 1$.

10. **Counting Square Roots of Unity.** Let $n = 2^k p_1^{e_1} \dots p_r^{e_r}$ where p_i are distinct odd primes. Using the structural decomposition of $(\mathbb{Z}/n\mathbb{Z})^\times$, prove that the number of solutions to $x^2 \equiv 1 \pmod{n}$ is $2^{\omega(n)+\delta}$, where $\omega(n) = r$ is the number of distinct odd prime factors, and
$$\delta = \begin{cases} 0 & \text{if } k = 0, 1, \\ 1 & \text{if } k = 2, \\ 2 & \text{if } k \geq 3. \end{cases}$$

11. **The Carmichael Function.** The Carmichael function $\lambda(n)$ is defined as the smallest positive integer m such that $a^m \equiv 1 \pmod{n}$ for all integers a coprime to n. Using the general structure of unit groups, prove that $\lambda(n) = \operatorname{lcm}(\lambda(2^k), \varphi(p_1^{e_1}), \dots, \varphi(p_r^{e_r}))$, where
$$\lambda(2^k) = \begin{cases} \varphi(2^k) & \text{if } k < 3, \\ \frac{1}{2}\varphi(2^k) & \text{if } k \geq 3. \end{cases}$$
Compute $\varphi(120)$ and $\lambda(120)$ to demonstrate that the exponent can be significantly smaller than the group order.

12. **Subgroups of $(\mathbb{Z}/2^k\mathbb{Z})^\times$.** For $k \geq 3$, the group $(\mathbb{Z}/2^k\mathbb{Z})^\times$ is generated by -1 and 5.
   (a) Prove that the elements of order 2 in $(\mathbb{Z}/2^k\mathbb{Z})^\times$ are precisely -1, $2^{k-1}-1$, and $2^{k-1}+1$.
   (b) Prove that the subgroup of squares $S = \{x^2 \mid x \in (\mathbb{Z}/2^k\mathbb{Z})^\times\}$ consists of all units a such that $a \equiv 1 \pmod 8$.

13. Change of Base. Let g and h be two primitive roots modulo n. Prove the change of base formula for discrete logarithms: for any a coprime to n,

$$\operatorname{ind}_h(a) \equiv \operatorname{ind}_h(g) \cdot \operatorname{ind}_g(a) \pmod{\varphi(n)}.$$

Conclude that $\operatorname{ind}_h(g) \cdot \operatorname{ind}_g(h) \equiv 1 \pmod{\varphi(n)}$.

14. Quadratic Residues and Indices. Let p be an odd prime and g a primitive root modulo p.

(a) Prove that $x^2 \equiv a \pmod{p}$ has a solution if and only if $\operatorname{ind}_g(a)$ is even.
(b) Use properties of indices to show that $\operatorname{ind}_g(-1) = (p-1)/2$.
(c) Combine these results to give a one-line proof of the first supplement to the Law of Quadratic Reciprocity: -1 is a square modulo p if and only if $p \equiv 1 \pmod{4}$.

15. Solving Congruences.

(a) Solve $x^2 \equiv 3 \pmod{13}$ and $x^2 \equiv 3 \pmod{143}$.

> *Remark.*
>
> For the latter, solve modulo 11 and 13 separately, then combine.

(b) Solve $6 \cdot 3^x \equiv 7 \pmod{11}$ using indices.
(c) Determine all 8th-power residues modulo 37.

6
Quadratic Residues

Having established the theory of linear congruences and the structure of multiplicative groups modulo n, we turn to polynomial congruences of degree two. Specifically, we investigate the solvability of quadratic equations in $\mathbb{Z}/p\mathbb{Z}$, which leads to the definition of the Legendre symbol and Euler's Criterion.

6.1 *Quadratic Congruences*

We consider the general quadratic congruence modulo an odd prime p. Let $a, b, c \in \mathbb{Z}$ with $p \nmid a$. We seek solutions to:

$$ax^2 + bx + c \equiv 0 \pmod{p}. \tag{6.1}$$

Since p is an odd prime, $(4a, p) = 1$. We may multiply *Equation 6.1* by $4a$ to complete the square:

$$4a(ax^2 + bx + c) = 4a^2x^2 + 4abx + 4ac = (2ax + b)^2 - (b^2 - 4ac).$$

Thus, the congruence is equivalent to:

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}.$$

Let $y = 2ax + b$ and $D = b^2 - 4ac$. Since $(2a, p) = 1$, the linear transformation $x \mapsto 2ax + b$ is a bijection on the residue classes modulo p. Consequently, finding x is equivalent to finding y such that:

$$y^2 \equiv D \pmod{p}.$$

If $p \mid D$, there is a unique solution $y \equiv 0 \pmod{p}$. If $p \nmid D$, the problem reduces to determining whether the integer D is a perfect square modulo p. We generally study the simplified congruence:

$$x^2 \equiv a \pmod{p}, \quad \text{where } p \nmid a.$$

Definition 6.1. ***Quadratic Residue.***
Let p be an odd prime and a an integer not divisible by p. If the congruence $x^2 \equiv a \pmod{p}$ has a solution, a is called a *quadratic residue* modulo p. If it has no solution, a is called a *quadratic non-residue* modulo p.

定義

If a is a quadratic residue, there exists x_0 such that $x_0^2 \equiv a \pmod{p}$. Then $(-x_0)^2 \equiv x_0^2 \equiv a \pmod{p}$. Since p is odd and $p \nmid a$, $x_0 \not\equiv -x_0 \pmod{p}$. Thus, every quadratic residue has exactly two distinct square roots modulo p.

Theorem 6.1. ***Distribution of Quadratic Residues.***
Let p be an odd prime. In any complete residue system modulo p, there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues. The quadratic residues are congruent to the numbers:

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

定理

Proof

Every quadratic residue is congruent to the square of some integer in $\{1, \ldots, p-1\}$. Since $(p-k)^2 \equiv (-k)^2 \equiv k^2 \pmod{p}$, the squares of the elements in the second half of the range $\{\frac{p+1}{2}, \ldots, p-1\}$ repeat the squares of the first half. Thus, the quadratic residues are generated by the squares of $1, 2, \ldots, \frac{p-1}{2}$.
We show these squares are distinct modulo p. Suppose $x^2 \equiv y^2 \pmod{p}$ with $1 \leq x, y \leq \frac{p-1}{2}$. Then

$$x^2 - y^2 = (x-y)(x+y) \equiv 0 \pmod{p}.$$

This implies $p \mid (x-y)$ or $p \mid (x+y)$. However, $2 \leq x+y \leq p-1 < p$, so $p \nmid (x+y)$. Similarly, $-(p-1)/2 \leq x-y \leq (p-1)/2$. The only multiple of p in this range is 0, so $x = y$. Therefore, the $\frac{p-1}{2}$ values listed are distinct incongruent residues. The remaining $(p-1) - \frac{p-1}{2} = \frac{p-1}{2}$ classes are quadratic non-residues.

■

Example 6.1. Residues Modulo 13. Let $p = 13$. The quadratic residues are the squares of $\{1, 2, 3, 4, 5, 6\}$:
· $1^2 \equiv 1$
· $2^2 \equiv 4$
· $3^2 \equiv 9$
· $4^2 \equiv 16 \equiv 3$

- $5^2 \equiv 25 \equiv 12$
- $6^2 \equiv 36 \equiv 10$

The set of residues is $\{1, 3, 4, 9, 10, 12\}$. The non-residues are $\{2, 5, 6, 7, 8, 11\}$.

範例

The arithmetic properties of residues follow a specific algebraic structure, akin to signs in real multiplication.

Theorem 6.2. ***Product of Residues.***
Let p be an odd prime.

(i) The product of two quadratic residues is a quadratic residue.
(ii) The product of a quadratic residue and a quadratic non-residue is a quadratic non-residue.
(iii) The product of two quadratic non-residues is a quadratic residue.

定理

Proof

(i) Let $a \equiv x^2$ and $b \equiv y^2 \pmod{p}$. Then $ab \equiv (xy)^2 \pmod{p}$, so ab is a residue.
(ii) Let a be a residue and b a non-residue. Suppose for contradiction that ab is a residue, say $ab \equiv y^2 \pmod{p}$. Let $a \equiv x^2 \pmod{p}$. Since $p \nmid a$, x is invertible. Then:

$$b \equiv a^{-1}(ab) \equiv (x^{-1})^2 y^2 \equiv (x^{-1}y)^2 \pmod{p}.$$

This implies b is a residue, a contradiction.
(iii) Let b be a non-residue. Consider the mapping $f : x \mapsto bx \pmod{p}$ on the set of units. This map is a bijection. Let R be the set of quadratic residues and N be the set of non-residues. By (ii), for every $r \in R$, the product br lies in N. Since $|R| = |N| = \frac{p-1}{2}$, the image of R under multiplication by b is exactly N. Since f is a bijection on the entire set of units, the image of N must be the remaining elements, which is R. Thus, for any $n \in N$, $bn \in R$.

■

6.2 *The Legendre Symbol*

To facilitate calculations involving quadratic residues, we introduce the Legendre symbol, which encodes the solvability of $x^2 \equiv a \pmod{p}$.

Definition 6.2. ***Legendre Symbol.***
Let p be an odd prime and a an integer. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } p \mid a. \end{cases}$$

定義

Using this notation, *Theorem 6.2* can be restated as the total multiplicativity of the symbol: for any $a, b \in \mathbb{Z}$,

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

Since $\left(\frac{a}{p}\right)$ depends only on $a \pmod p$, it is a periodic function of a with period p. The number of solutions to $x^2 \equiv a \pmod p$ is given by $1 + \left(\frac{a}{p}\right)$.
To evaluate the Legendre symbol without listing all squares, we utilise Euler's Criterion.

Theorem 6.3. ***Euler's Criterion.***
Let p be an odd prime and a an integer not divisible by p. Then

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

定理

Proof
By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod p$. We factorise:

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

Thus $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$.
If $\left(\frac{a}{p}\right) = 1$, then $a \equiv x^2 \pmod p$ for some x. Hence:

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \pmod p.$$

If $\left(\frac{a}{p}\right) = -1$, we assume for contradiction that $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Consider the polynomial $f(y) = y^{\frac{p-1}{2}} - 1$. By Lagrange's Theorem, $f(y) \equiv 0 \pmod p$ has at most $\frac{p-1}{2}$ roots. We have already established that the $\frac{p-1}{2}$ quadratic residues are roots of $f(y)$. If the non-residue a were also a root, $f(y)$ would have at least $\frac{p-1}{2} + 1$ roots, a contradiction. Therefore, $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.
In both cases, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

■

Example 6.2. Calculation using Euler's Criterion. Determine $\left(\frac{3}{17}\right)$. Here $p = 17$, so $\frac{p-1}{2} = 8$.

$$3^8 = (3^4)^2 = 81^2 \equiv (-4)^2 = 16 \equiv -1 \pmod{17}.$$

Thus $\left(\frac{3}{17}\right) = -1$, so 3 is a quadratic non-residue modulo 17.

範例

Euler's Criterion allows us to explicitly determine when -1 and 2 are quadratic residues.

Corollary 6.1. *The Value of* $(-1/p)$. For any odd prime p,

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

推論

Proof

By *Theorem 6.3*, $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$. Since both sides are ± 1 and $p > 2$, the congruence implies equality. The exponent is even if $p = 4k+1$ and odd if $p = 4k+3$.

■

Corollary 6.2. *The Value of* $(2/p)$. For any odd prime p,

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

推論

Proof

Consider the congruences for the first $\frac{p-1}{2}$ multiples of 2 modulo p:

$$\begin{aligned} 1 \cdot (-1)^1 &\equiv -1 \equiv p-1 \pmod p \\ 2 \cdot (-1)^2 &\equiv 2 \pmod p \\ 3 \cdot (-1)^3 &\equiv -3 \equiv p-3 \pmod p \\ &\vdots \\ k \cdot (-1)^k &\equiv \begin{cases} k & \text{if } k \text{ is even} \\ p-k & \text{if } k \text{ is odd} \end{cases} \end{aligned}$$

Let $r = \frac{p-1}{2}$. The set of values on the right-hand side is precisely the set of even integers $E = \{2, 4, \ldots, 2r\}$. This is because for any $j \in \{1, \ldots, r\}$, if j is even, it appears directly; if j is odd, $p - j$ is even

and $2 \leq p-j \leq p-1$. We take the product of these r congruences:

$$\prod_{k=1}^{r} k \cdot (-1)^k \equiv \prod_{j=1}^{r} (2j) \pmod{p}.$$

The left side is $r!(-1)^{\sum_{k=1}^{r} k}$. The right side is $2^r r!$. Cancelling $r!$ (since $(r!, p) = 1$):

$$(-1)^{\frac{r(r+1)}{2}} \equiv 2^r \pmod{p}.$$

Substituting $r = \frac{p-1}{2}$, the exponent becomes $\frac{(p-1)(p+1)}{8} = \frac{p^2-1}{8}$. Thus $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$. By Euler's Criterion, this is $\left(\frac{2}{p}\right)$. ■

Example 6.3. Composite Legendre Calculation. Determine if 18 is a quadratic residue modulo 23. We factor $18 = 2 \cdot 3^2$.

$$\left(\frac{18}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{3^2}{23}\right).$$

Since $3 \not\equiv 0 \pmod{23}$, $\left(\frac{3^2}{23}\right) = \left(\frac{3}{23}\right)^2 = 1$. For the factor 2, we check $23 \pmod 8$. Since $23 = 16 + 7 \equiv 7 \equiv -1 \pmod 8$, *corollary 6.2* gives $\left(\frac{2}{23}\right) = 1$. Thus $\left(\frac{18}{23}\right) = 1 \cdot 1 = 1$. Indeed, $5^2 = 25 \equiv 2 \pmod{23}$, so $(3 \cdot 5)^2 = 15^2 = 225 = 9 \cdot 23 + 18 \equiv 18 \pmod{23}$.

範例

6.3 *Gauss's Lemma*

While Euler's Criterion characterises residues theoretically, Gauss's Lemma provides a combinatorial approach essential for proving the Law of Quadratic Reciprocity. It relates the Legendre symbol to the distribution of multiples of a in the intervals $[1, \frac{p-1}{2}]$ and $[\frac{p+1}{2}, p-1]$.

Theorem 6.4. ***Gauss's Lemma.***
Let p be an odd prime and a an integer such that $(a, p) = 1$. Consider the set of multiples

$$S = \left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}.$$

Let l be the number of elements in S whose least positive residues modulo p exceed $\frac{p}{2}$. Then

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

定理

Proof

Let $r = \frac{p-1}{2}$. For each $k \in \{1, \ldots, r\}$, let u_k be the remainder of ka upon division by p, so $0 < u_k < p$. We partition the remainders $\{u_1, \ldots, u_r\}$ into two sets:

$$A = \{u_k \mid 1 \leq u_k \leq r\},$$
$$B = \{u_k \mid r < u_k < p\}.$$

Let $|B| = l$. We denote the elements of A by $\{r_1, \ldots, r_{r-l}\}$ and the elements of B by $\{b_1, \ldots, b_l\}$. Consider the set $C = \{p - b_1, \ldots, p - b_l\}$. Clearly $C \subseteq \{1, \ldots, r\}$.

We claim that $A \cap C = \emptyset$. Suppose $r_i = p - b_j$ for some i, j. Then $r_i + b_j \equiv 0 \pmod{p}$. However, $r_i \equiv xa$ and $b_j \equiv ya$ for distinct $x, y \in \{1, \ldots, r\}$. Thus $(x + y)a \equiv 0 \pmod{p}$, implying $x + y$ is a multiple of p. But $2 \leq x + y \leq 2r = p - 1 < p$, a contradiction.

The set $A \cup C$ contains $(r - l) + l = r$ distinct integers in the range $\{1, \ldots, r\}$. Therefore, $A \cup C = \{1, \ldots, r\}$. We now compute the product of these elements:

$$\prod_{x \in A} x \cdot \prod_{y \in C} y = r!.$$

Substituting the definitions of A and C:

$$\prod_{i=1}^{r-l} r_i \cdot \prod_{j=1}^{l} (p - b_j) = r!.$$

Working modulo p:

$$\prod_{i=1}^{r-l} r_i \cdot \prod_{j=1}^{l} (-b_j) \equiv (-1)^l \prod_{k=1}^{r} u_k \equiv r! \pmod{p}.$$

Recall that $\{u_1, \ldots, u_r\}$ are simply the residues of $a, 2a, \ldots, ra$. Thus:

$$\prod_{k=1}^{r} u_k \equiv \prod_{k=1}^{r} (ka) = a^r r! \pmod{p}.$$

Substituting this back:

$$(-1)^l a^r r! \equiv r! \pmod{p}.$$

Cancelling $r!$, we obtain $a^{\frac{p-1}{2}} \equiv (-1)^l \pmod{p}$. By *Theorem 6.3*, $\left(\frac{a}{p}\right) = (-1)^l$.

■

Example 6.4. Application of Gauss's Lemma. Compute $\left(\frac{7}{11}\right)$ using Gauss's Lemma. Here $p = 11, r = 5, a = 7$. The set

$S = \{7, 14, 21, 28, 35\}$. Modulo 11, the residues are:

$$\begin{aligned} 7 &\equiv 7 > 5.5 \quad (\in B) \\ 14 &\equiv 3 \leq 5.5 \quad (\in A) \\ 21 &\equiv 10 > 5.5 \quad (\in B) \\ 28 &\equiv 6 > 5.5 \quad (\in B) \\ 35 &\equiv 2 \leq 5.5 \quad (\in A) \end{aligned}$$

The set $B = \{7, 10, 6\}$, so $l = 3$. Thus $\left(\frac{7}{11}\right) = (-1)^3 = -1$.

範例

6.4 *The Law of Quadratic Reciprocity*

Gauss's Lemma serves as the foundation for the most celebrated theorem in elementary number theory: the Law of Quadratic Reciprocity. This law connects the Legendre symbol $\left(\frac{p}{q}\right)$ with $\left(\frac{q}{p}\right)$ for distinct odd primes p and q.

Theorem 6.5. ***Law of Quadratic Reciprocity.***
Let p and q be distinct odd primes. Then

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

Equivalently,

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4, \\ \left(\frac{q}{p}\right) & \text{otherwise.} \end{cases}$$

定理

Proof

Let $r = \frac{p-1}{2}$ and $s = \frac{q-1}{2}$. We begin by establishing an analytic formulation for the exponent l in Gauss's Lemma.

Step 1: Eisenstein's Lemma. Let a be an odd integer coprime to p.
For each $k \in \{1, \ldots, r\}$, the division algorithm yields

$$ka = p\left\lfloor \frac{ka}{p} \right\rfloor + u_k, \quad 1 \leq u_k < p.$$

Here u_k is the least positive residue. If $u_k \leq r$, then the numerically least residue is $\alpha_k = u_k$ (positive). If $u_k > r$, then $\alpha_k = u_k - p$ (negative). Let μ be the number of u_k such that $u_k > r$. This is exactly the l in Gauss's Lemma, so $\left(\frac{a}{p}\right) = (-1)^{\mu}$. Summing the

division equations:

$$a\sum_{k=1}^{r} k = p\sum_{k=1}^{r}\left\lfloor \frac{ka}{p}\right\rfloor + \sum_{k=1}^{r} u_k.$$

Let $U = \sum u_k$. We partition the residues u_k into those $\leq r$ (say $b_1,\dots,b_{r-\mu}$) and those $> r$ (say $c_1,\dots,c_\mu$). Then $U = \sum b_i + \sum c_j$. Recall from the proof of Gauss's Lemma that $\{b_1,\dots,b_{r-\mu}\}\cup\{p-c_1,\dots,p-c_\mu\} = \{1,\dots,r\}$. Summing these integers:

$$\sum_{k=1}^{r} k = \sum b_i + \sum(p-c_j) = \sum b_i + \mu p - \sum c_j = U - 2\sum c_j + \mu p.$$

Solving for U: $U \equiv \sum k + \mu p \pmod 2$. Substituting back into the sum of multiples:

$$a\sum k \equiv p\sum\left\lfloor \frac{ka}{p}\right\rfloor + \left(\sum k + \mu p\right) \pmod 2.$$

Since p and a are odd, $p \equiv 1 \pmod 2$ and $a \equiv 1 \pmod 2$. The equation simplifies to:

$$\sum k \equiv \sum\left\lfloor \frac{ka}{p}\right\rfloor + \sum k + \mu \pmod 2 \implies \mu \equiv \sum_{k=1}^{r}\left\lfloor \frac{ka}{p}\right\rfloor \pmod 2.$$

Thus, for distinct odd primes p, q:

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{r}\lfloor \frac{kq}{p}\rfloor} \quad\text{and}\quad \left(\frac{p}{q}\right) = (-1)^{\sum_{j=1}^{s}\lfloor \frac{jp}{q}\rfloor}.$$

Step 2: Lattice Point Counting. We must determine the parity of the total exponent:

$$E = \sum_{k=1}^{r}\left\lfloor \frac{kq}{p}\right\rfloor + \sum_{j=1}^{s}\left\lfloor \frac{jp}{q}\right\rfloor.$$

Consider the rectangle $\mathcal{R}$ in the xy-plane with vertices $(0,0),(p/2,0),(p/2,q/2),(0,q/2)$. We count the number of interior lattice points (x,y) such that $1 \leq x \leq r$ and $1 \leq y \leq s$. The total number of such points is rs. The diagonal $\mathcal{D}$ connecting $(0,0)$ to $(p/2,q/2)$ has equation $y = \frac{q}{p}x$. Since $(p,q) = 1$, no integer point lies on $\mathcal{D}$ for $0 < x < p/2$. The number of lattice points below the diagonal is given by summing over possible x:

$$N_{\text{below}} = \sum_{x=1}^{r}\left\lfloor \frac{qx}{p}\right\rfloor.$$

Similarly, the number of lattice points above the diagonal (counting by y) is:

$$N_{\text{above}} = \sum_{y=1}^{s}\left\lfloor \frac{py}{q}\right\rfloor.$$

Since every lattice point is either above or below $\mathcal{D}$:

$$rs = N_{\text{below}} + N_{\text{above}} = \sum_{k=1}^{r} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{j=1}^{s} \left\lfloor \frac{jp}{q} \right\rfloor .$$

Therefore:

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{N_{\text{below}}}(-1)^{N_{\text{above}}} = (-1)^{rs} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

■

Remark (Geometric Interpretation).
The term $\frac{p-1}{2}\frac{q-1}{2}$ is odd if and only if both factors are odd, which requires $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$. In this case, the product of the symbols is -1, implying the reciprocity is "negative". In all other cases, the product is 1, meaning p is a residue mod q if and only if q is a residue mod p.

Applications of Reciprocity

The reciprocity law reduces the evaluation of $\left(\frac{a}{p}\right)$ to the evaluation of symbols with smaller moduli, similar to the Euclidean algorithm.

Example 6.5. Composite Numerator. Determine if the congruence $x^2 \equiv 219 \pmod{383}$ is solvable. Note that 383 is prime. We factorise $219 = 3 \times 73$.

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right).$$

1. Evaluate $\left(\frac{3}{383}\right)$. Since $383 = 4 \times 95 + 3 \equiv 3 \pmod 4$ and $3 \equiv 3 \pmod 4$, reciprocity implies a sign change:
$$\left(\frac{3}{383}\right) = -\left(\frac{383}{3}\right) = -\left(\frac{2}{3}\right).$$
Since $3 \equiv 3 \pmod 8$, $\left(\frac{2}{3}\right) = -1$. Thus $\left(\frac{3}{383}\right) = -(-1) = 1$.
2. Evaluate $\left(\frac{73}{383}\right)$. Since $73 \equiv 1 \pmod 4$, reciprocity implies no sign change:
$$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right).$$
Reducing modulo 73: $383 = 5 \times 73 + 18$.
$$\left(\frac{18}{73}\right) = \left(\frac{2 \cdot 3^2}{73}\right) = \left(\frac{2}{73}\right) \cdot 1.$$
Since $73 \equiv 1 \pmod 8$, $\left(\frac{2}{73}\right) = 1$.

Combining these, $\left(\frac{219}{383}\right) = 1 \cdot 1 = 1$. The congruence is solvable.

範例

We can also determine for which primes a specific integer is a quadratic residue.

Theorem 6.6. *Quadratic Character of 3.*
Let $p > 3$ be a prime. Then 3 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \pmod{12}$.

定理

Proof

By the Reciprocity Law:

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2}\frac{p-1}{2}} = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}.$$

We analyse the cases modulo 12 (since we need conditions modulo 3 and 4).

- If $p \equiv 1 \pmod{12}$: $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$. $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. Exponent $\frac{p-1}{2}$ is even. Result: $1 \cdot 1 = 1$.
- If $p \equiv 5 \pmod{12}$: $p \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 4$. $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$. Exponent is even. Result: $-1 \cdot 1 = -1$.
- If $p \equiv 7 \pmod{12}$: $p \equiv 1 \pmod 3$ and $p \equiv 3 \pmod 4$. $\left(\frac{p}{3}\right) = 1$. Exponent is odd. Result: $1 \cdot (-1) = -1$.
- If $p \equiv 11 \equiv -1 \pmod{12}$: $p \equiv 2 \pmod 3$ and $p \equiv 3 \pmod 4$. $\left(\frac{p}{3}\right) = -1$. Exponent is odd. Result: $(-1) \cdot (-1) = 1$.

Thus $\left(\frac{3}{p}\right) = 1 \iff p \equiv 1, 11 \pmod{12}$.

■

6.5 *Exercises*

1. **Gauss's Lemma Calculation.** Let p be an odd prime. Use Gauss's Lemma to explicitly compute $\left(\frac{2}{p}\right)$ by analysing the number of elements in the set $S = \{2, 4, \ldots, p-1\}$ that exceed $p/2$.
2. **Legendre Symbol Computations.** Compute the following Legendre symbols using the properties derived in the text.
   (a) $\left(\frac{17}{23}\right)$
   (b) $\left(\frac{19}{37}\right)$
   (c) $\left(\frac{60}{79}\right)$
   (d) $\left(\frac{92}{101}\right)$
3. **Residues of Small Integers.** Using the Law of Quadratic Reciprocity, determine all primes p for which:

(a) -3 is a quadratic residue.
(b) 5 is a quadratic residue.
(c) 15 is a quadratic residue.

4. **Constructing Square Roots.** While Euler's Criterion determines *existence*, it does not provide the solution.

   (a) Let $p \equiv 3 \pmod 4$. Prove that if a is a quadratic residue modulo p, then $x \equiv \pm a^{(p+1)/4} \pmod p$ are the solutions to $x^2 \equiv a \pmod p$.
   (b) Let $p \equiv 5 \pmod 8$. Prove that 2 is a quadratic non-residue modulo p. Deduce that $x = 2^{(p-1)/4}$ is a solution to the congruence $x^2 \equiv -1 \pmod p$.

> *Remark.*
>
> For (b), apply Euler's Criterion to the element 2, observing that $2^{(p-1)/2} \equiv -1$.

5. **Primes of Specific Forms.** Prove that there are infinitely many primes of the following forms:

   (a) $4n + 1$.

   > *Remark.*
   >
   > Consider divisors of $N = (n!)^2 + 1$.

   (b) $6n + 1$.
   (c) $8n + 3$, $8n + 5$, and $8n + 7$.

6. **The Least Quadratic Non-Residue.** Let p be an odd prime. Let n be the smallest positive integer that is a quadratic non-residue modulo p. Prove that n must be prime.

7. **Product of Residues.** Let p be an odd prime. Prove that the product of the quadratic residues modulo p satisfies:

$$\prod_{\substack{r=1 \\ \left(\frac{r}{p}\right)=1}}^{p-1} r \equiv -\left(\frac{-1}{p}\right) \pmod p.$$

8. **Sums of Residues.** Let p be a prime with $p \equiv 1 \pmod 4$. Prove the following identities:

   (a)
$$\sum_{\substack{r=1 \\ \left(\frac{r}{p}\right)=1}}^{p-1} r = \frac{p(p-1)}{4}.$$

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

(c)
$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{k^2}{p} \right\rfloor = \frac{(p-1)(p-5)}{24}.$$

9. Character Sum of a Linear Polynomial. Let p be an odd prime and let a, b be integers with $p \nmid a$. Prove that
$$\sum_{x=0}^{p-1} \left(\frac{ax+b}{p} \right) = 0.$$

> *Remark.*
> As x ranges over a complete residue system, so does $ax + b$.

10. Quadratic Sum with Linear Term. Let p be an odd prime, and a be an integer with $p \nmid a$. Prove
$$\sum_{x=0}^{p-1} \left(\frac{x^2+ax}{p} \right) = -1.$$

11. The Hyperbola Equation. Let p be an odd prime, and a be an integer.

(i) Prove: The congruence equation $x^2 - y^2 \equiv a \pmod{p}$ always has a solution.

(ii) If (x, y) and (x', y') are both solutions to the above congruence, we consider them the same solution modulo p when $x \equiv x'$ and $y \equiv y' \pmod{p}$. Prove: The number of solutions in part (i) is $p - 1$ (if $p \nmid a$) or $2p - 1$ (if $p \mid a$).

12. Character Sum of a Quadratic. Let p be an odd prime and let a be an integer such that $p \nmid a$.

(a) Prove that the number of solutions to $y^2 \equiv k \pmod{p}$ is given by $1 + \left(\frac{k}{p}\right)$.

(b) Evaluate the sum $\sum_{x=0}^{p-1} \left(\frac{x^2+a}{p}\right)$ by summing the result of part (a) over all $k = x^2 + a$ and adjusting for the count. Specifically, show that:
$$\sum_{x=0}^{p-1} \left(\frac{x^2+a}{p} \right) = -1.$$

13. The General Quadratic Character Sum. Let p be an odd prime, $f(x) = ax^2 + bx + c$ with $p \nmid a$. Let $D = b^2 - 4ac$. Prove
$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right) = \begin{cases} -\left(\frac{a}{p}\right), & \text{if } p \nmid D, \\ (p-1)\left(\frac{a}{p}\right), & \text{if } p \mid D. \end{cases}$$

14. Points on a Circle. Let p be an odd prime. Let N be the number of solutions $(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2$ to the congruence

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

Using the sum from the previous exercise, prove that

$$N = p - (-1)^{\frac{p-1}{2}}.$$

Verify this formula explicitly for $p = 3$ and $p = 5$.

> *Remark.*
>
> Express N as $\sum_{x=0}^{p-1} N_y(1 - x^2)$, where $N_y(k)$ is the number of solutions to $y^2 \equiv k$.

15. Lifting Solutions. Let p be an odd prime and a an integer not divisible by p. Prove that the congruence $x^2 \equiv a \pmod{p^k}$ has a solution for $k \geq 1$ if and only if $\left(\frac{a}{p}\right) = 1$. When this condition is met, prove there are exactly two solutions modulo p^k.

> *Remark.*
>
> Use mathematical induction and the Taylor expansion $(x_0 + tp^k)^2 \equiv x_0^2 + 2x_0tp^k \pmod{p^{k+1}}$.

16. ⋆ Quadratic Residues Modulo Powers of Two. Let a be an odd integer. Then

(i) $x^2 \equiv a \pmod{2}$ has a solution for all a.

(ii) $x^2 \equiv a \pmod{4}$ has a solution if and only if $a \equiv 1 \pmod{4}$, and when this condition is satisfied, there are exactly two distinct solutions.

(iii) The congruence equation $x^2 \equiv a \pmod{2^k}$ ($k \geq 3$) has a solution if and only if $a \equiv 1 \pmod{8}$. When the condition holds, there are exactly four solutions. If x_0 is one solution, then $\pm x_0, \pm x_0 + 2^{k-1}$ are all the solutions.

7
Indeterminate Equations

We now turn our attention to the theory of indeterminate equations, broadly defined as polynomial equations where the number of unknowns exceeds the number of constraints, and the solutions are required to lie within a specific arithmetic set, typically $\mathbb{Z}$ or $\mathbb{Q}$. While linear indeterminate equations are fully resolved by the theory of the greatest common divisor and linear congruences, higher-degree equations present significant challenges.
To analyse the solvability of such equations, particularly quadratic forms, we first extend the arithmetic of quadratic residues to composite moduli. This generalisation, the Jacobi symbol, provides an essential computational tool for determining local solvability conditions.

7.1 The Jacobi Symbol

While the Legendre symbol $\left(\frac{a}{p}\right)$ provides a complete arithmetic characterisation of quadratic residues modulo a prime, its definition restricts the modulus to be prime. This limitation becomes computationally cumbersome when evaluating $\left(\frac{a}{p}\right)$ for large p via reciprocity, as it necessitates the prime factorisation of the numerator at every inversion step. To mitigate this, we introduce the Jacobi symbol.

Definition 7.1. ***Jacobi Symbol.***
Let n be an odd positive integer with prime factorisation $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. For any integer a, the *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined as the product of the Legendre symbols of a with respect to the prime factors of n:

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i}.$$

If $(a, n) > 1$, then $p_i \mid a$ for some i, implying $\left(\frac{a}{p_i}\right) = 0$, and thus $\left(\frac{a}{n}\right) = 0$. Like the Legendre symbol, the Jacobi symbol takes values in $\{0, 1, -1\}$.

定義

The utility of the Jacobi symbol lies in its preservation of the algebraic properties of the Legendre symbol while allowing for composite moduli.

Theorem 7.1. ***Properties of the Jacobi Symbol.***
Let n, m be odd positive integers and $a, b \in \mathbb{Z}$.

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

(ii) **Multiplicativity (Numerator):** $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

(iii) **Multiplicativity (Denominator):** $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

(iv) **Square Factors:** $\left(\frac{a}{n^2}\right) = 1$ provided $(a, n) = 1$. Similarly, $\left(\frac{a^2}{n}\right) = 1$ if $(a, n) = 1$.

定理

Proof

These properties follow directly from the definition and the corresponding properties of the Legendre symbol. For (iii), let $m = \prod p_i^{\alpha_i}$ and $n = \prod q_j^{\beta_j}$. Then $mn = \prod p_i^{\alpha_i} \prod q_j^{\beta_j}$. The symbol $\left(\frac{a}{mn}\right)$ expands to the product of Legendre symbols for all prime factors counting multiplicity, which partitions into the product for m and the product for n.

■

Crucially, the Jacobi symbol adheres to a generalised Law of Quadratic Reciprocity. This allows for the inversion of the symbol $\left(\frac{a}{n}\right)$ without determining the prime factorisation of a, provided a is odd.

Theorem 7.2. ***Generalised Reciprocity Laws.***
Let n and m be odd coprime positive integers.

(i) **First Supplement:** $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

(ii) **Second Supplement:** $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

(iii) **Quadratic Reciprocity:** $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$.

定理

Proof

Let the prime factorisations of n and m be $n = \prod_{i=1}^{k} p_i$ and $m = \prod_{j=1}^{l} q_j$, where the primes are listed with multiplicity. Since n and m are odd, all p_i and q_j are odd primes. We rely on two elementary congruences for odd integers a and b:

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod{2}, \tag{7.1}$$

$$\frac{a^2b^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod{2}. \tag{7.2}$$

Equation 7.1 follows from the identity $\frac{ab-1}{2} - \frac{a-1}{2} - \frac{b-1}{2} = \frac{(a-1)(b-1)}{2}$. Since a, b are odd, $a-1$ and $b-1$ are even, so their product is divis-

ible by 4. Similarly, *Equation 7.2* follows because $a^2 \equiv 1 \pmod 8$ for odd a, implying $8 \mid (a^2 - 1)$. By induction, these congruences extend to finite products.

First Supplement: By definition, $\left(\frac{-1}{n}\right) = \prod_{i=1}^{k} \left(\frac{-1}{p_i}\right)$. Using the property for Legendre symbols (*corollary 6.1*):

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

Applying *Equation 7.1* inductively to $n = \prod p_i$, we have $\sum_{i=1}^{k} \frac{p_i-1}{2} \equiv \frac{n-1}{2} \pmod 2$. Thus, $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

Second Supplement: By definition, $\left(\frac{2}{n}\right) = \prod_{i=1}^{k} \left(\frac{2}{p_i}\right)$. Using *corollary 6.2*:

$$\left(\frac{2}{n}\right) = \prod_{i=1}^{k} (-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum_{i=1}^{k} \frac{p_i^2-1}{8}}.$$

Applying *Equation 7.2* inductively, $\sum_{i=1}^{k} \frac{p_i^2-1}{8} \equiv \frac{n^2-1}{8} \pmod 2$. Thus, $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Quadratic Reciprocity: By definition, $\left(\frac{m}{n}\right) = \prod_{i=1}^{k} \left(\frac{m}{p_i}\right) = \prod_{i=1}^{k} \prod_{j=1}^{l} \left(\frac{q_j}{p_i}\right)$. Similarly, $\left(\frac{n}{m}\right) = \prod_{j=1}^{l} \prod_{i=1}^{k} \left(\frac{p_i}{q_j}\right)$. Multiplying these expressions and applying the Law of Quadratic Reciprocity for Legendre symbols to each pair (p_i, q_j):

$$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \prod_{i=1}^{k}\prod_{j=1}^{l}\left[\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)\right] \\ &= \prod_{i=1}^{k}\prod_{j=1}^{l}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} \\ &= (-1)^{\sum_{i=1}^{k}\sum_{j=1}^{l}\frac{p_i-1}{2}\frac{q_j-1}{2}}.\end{aligned}$$

The exponent factors as a product of sums:

$$\sum_{i=1}^{k}\sum_{j=1}^{l}\frac{p_i-1}{2}\frac{q_j-1}{2} = \left(\sum_{i=1}^{k}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{l}\frac{q_j-1}{2}\right).$$

Using the congruence from part (i), this is congruent modulo 2 to:

$$\frac{n-1}{2}\cdot\frac{m-1}{2}.$$

Therefore, $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$.

■

Remark (Connection to Quadratic Residues).

The arithmetic interpretation of $\left(\frac{a}{n}\right)$ for composite n is subtle. If a

is a quadratic residue modulo n, then $x^2 \equiv a \pmod{n}$ is solvable. This implies $x^2 \equiv a \pmod{p}$ for every prime $p \mid n$. Consequently, $\left(\frac{a}{p}\right) = 1$ for all $p \mid n$, leading to $\left(\frac{a}{n}\right) = 1$. The converse is false. If $\left(\frac{a}{n}\right) = 1$, a is not necessarily a quadratic residue modulo n.

Example 7.1. Non-Residue with Jacobi Symbol 1. Consider $n = 15 = 3 \cdot 5$ and $a = 2$. The Legendre symbols are:

$$\left(\frac{2}{3}\right) = -1 \quad \text{and} \quad \left(\frac{2}{5}\right) = -1.$$

Thus, 2 is not a square modulo 3 (and hence not modulo 15). However, the Jacobi symbol is:

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1.$$

This demonstrates that $\left(\frac{a}{n}\right) = 1$ is a necessary but not sufficient condition for a to be a quadratic residue modulo n. Conversely, $\left(\frac{a}{n}\right) = -1$ strictly implies that a is a quadratic non-residue.

範例

7.2 *Local Solvability and the Hasse Principle*

We focus on polynomial indeterminate equations of the form

$$F(x_1, \ldots, x_n) = 0, \tag{7.1}$$

where $F \in \mathbb{Z}[x_1, \ldots, x_n]$. The simplest instance is the linear equation $a_1x_1 + \cdots + a_nx_n = b$. By Bézout's Identity, integer solutions exist if and only if $(a_1, \ldots, a_n)$ divides b. For non-linear polynomials, no such simple criterion exists.
A necessary condition for the existence of integer solutions is solvability in "local" structures: the field of real numbers $\mathbb{R}$ and the rings $\mathbb{Z}/m\mathbb{Z}$ for all m.

Definition 7.2. ***Local Solvability.***
The equation $F(x_1, \ldots, x_n) = 0$ is said to be *locally solvable* if:

(i) It possesses real solutions in $\mathbb{R}$.
(ii) For every integer $m > 1$, the congruence $F(x_1, \ldots, x_n) \equiv 0 \pmod{m}$ has solutions.

定義

If an integer solution $\mathbf{x}^*$ exists to *Equation 7.1*, it is trivial that $\mathbf{x}^*$ is a real solution and reduces to a solution modulo m for all m. Thus, local solvability is a necessary condition for integer solvability.

Testing solvability modulo every integer m appears computationally infeasible. However, the problem reduces to prime powers via the Chinese Remainder Theorem.

Proposition 7.1. ***Reduction to Prime Powers.***
The congruence $F(\mathbf{x}) \equiv 0 \pmod{m}$ is solvable for all $m > 1$ if and only if it is solvable modulo p^k for every prime p and every integer $k \geq 1$.

命題

Proof

The forward implication is immediate. Conversely, let $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. Suppose that for each $j \in \{1, \dots, r\}$, there exists a solution $\mathbf{x}^{(j)}$ satisfying $F(\mathbf{x}^{(j)}) \equiv 0 \pmod{p_j^{\alpha_j}}$. We construct a solution modulo m by solving the system of congruences for each coordinate $i \in \{1, \dots, n\}$:

$$x_i \equiv x_i^{(j)} \pmod{p_j^{\alpha_j}} \quad \text{for } j = 1, \dots, r.$$

By the Chinese Remainder Theorem, such integers x_i exist. Since polynomial evaluation commutes with modular reduction,

$$F(\mathbf{x}) \equiv F(\mathbf{x}^{(j)}) \equiv 0 \pmod{p_j^{\alpha_j}}.$$

Since this holds for all prime power factors, $F(\mathbf{x}) \equiv 0 \pmod{m}$.

■

Consequently, to prove that an equation has *no* integer solutions, it suffices to exhibit a single modulus m (often a small prime or prime power) or show the absence of real solutions.

Example 7.2. Obstruction Modulo 4. Consider the equation $x^2 + y^2 - 4z^2 = 3$. Modulo 4, the term $4z^2$ vanishes, reducing the equation to $x^2 + y^2 \equiv 3 \pmod{4}$. The quadratic residues modulo 4 are 0 and 1. The possible sums of two residues are $0 + 0 = 0$, $0 + 1 = 1$, and $1 + 1 = 2$. Since 3 is not a sum of two squares modulo 4, the congruence has no solution. Hence, the original equation has no integer solutions.

範例

Example 7.3. Obstruction via Reciprocity. Consider the equation $y^2 = x^3 + 7$. We first determine the parity of x. If x is even, then $x^3 \equiv 0 \pmod{8}$ (or $\pmod{4}$), implying $y^2 \equiv 7 \equiv 3 \pmod{4}$, which is impossible. Thus x must be odd. We rewrite the equation as:

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4) = (x + 2)((x - 1)^2 + 3).$$

Since x is odd, $x - 1$ is even, so $(x - 1)^2 \equiv 0 \pmod{4}$. It follows

that the factor $((x-1)^2+3) \equiv 3 \pmod 4$. An integer congruent to $3 \pmod 4$ must have at least one prime factor q such that $q \equiv 3 \pmod 4$. Considering the equation modulo such a prime q, we have

$$y^2+1 \equiv 0 \implies y^2 \equiv -1 \pmod q.$$

This implies that -1 is a quadratic residue modulo q. By *corollary 6.1*, this requires $q \equiv 1 \pmod 4$. This contradicts the existence of a prime factor $q \equiv 3 \pmod 4$. Thus, no integer solutions exist.

範例

The Failure of the Local-Global Principle

For certain classes of polynomials, such as quadratic forms (homogeneous polynomials of degree 2), local solvability implies integer (or rational) solvability. This phenomenon is known as the Hasse Principle. However, this principle is not universal; for higher degree equations or specific non-homogeneous cases, local solvability does not guarantee global solvability.

Example 7.4. Counter-example to Hasse Principle. Consider the equation:

$$(x^2-13)(x^2-17)(x^2-221)=0.$$

Integer solvability requires 13, 17, or 221 to be a perfect square in $\mathbb{Z}$, which is false. Thus, there are no integer solutions. However, we claim the equation is locally solvable.

Real solutions: Trivially exist (e.g., $x=\sqrt{13}$).

Modulo p: We show that for any prime p, the congruence

$$(x^2-13)(x^2-17)(x^2-221) \equiv 0 \pmod p$$

is solvable. This requires showing that at least one of 13, 17, or 221 is a quadratic residue modulo p. Using the Legendre symbol properties:

$$\left(\frac{221}{p}\right)=\left(\frac{13\cdot 17}{p}\right)=\left(\frac{13}{p}\right)\left(\frac{17}{p}\right).$$

If $\left(\frac{13}{p}\right) \neq -1$ or $\left(\frac{17}{p}\right) \neq -1$, a solution exists. The only remaining case is $\left(\frac{13}{p}\right)=-1$ and $\left(\frac{17}{p}\right)=-1$. But their product is then $(-1)(-1)=1$, implying $\left(\frac{221}{p}\right)=1$. Thus, for any p, one of the factors corresponds to a quadratic residue (or 0), making the congruence solvable modulo p.

Modulo p^k: For odd primes, Hensel's Lemma lifts the simple roots from modulo p to p^k. For $p=2$, we note $17 \equiv 1 \pmod 8$. By the

structure of squares modulo 2^k, $x^2 \equiv 17 \pmod{2^k}$ is solvable for all $k \geq 1$.

This equation is locally solvable everywhere but has no global integer solution.

範例

7.3 *Pythagorean Triples*

We apply the theory of divisibility to the Diophantine equation

$$x^2 + y^2 = z^2. \tag{7.2}$$

Positive integer solutions to this equation correspond to the side lengths of right-angled triangles and are known as *Pythagorean triples*.

Definition 7.3. ***Primitive Solutions.***
A solution (x, y, z) in positive integers is called *primitive* if $(x, y, z) = 1$. Observe that if d divides both x and y, then $d^2 \mid (x^2 + y^2) = z^2$, which implies $d \mid z$. Consequently, any integer solution can be reduced to a primitive solution by dividing by the greatest common divisor. In a primitive solution, the integers are pairwise coprime.

定義

Theorem 7.3. ***Classification of Pythagorean Triples.***
All primitive solutions to $x^2 + y^2 = z^2$ with y even are given by the parametrisation

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2,$$

where $a > b > 0$ are coprime integers of opposite parity.

定理

Proof

Let (x, y, z) be a primitive solution. We first determine the parity of the components. If x and y were both even, then $(x, y) \geq 2$, contradicting primitivity. If x and y were both odd, then $x^2 \equiv 1 \pmod 4$ and $y^2 \equiv 1 \pmod 4$. This implies $z^2 = x^2 + y^2 \equiv 2 \pmod 4$, which is impossible for a perfect square. Thus, exactly one of x or y is even. Without loss of generality, we assume y is even. It follows that x and z are odd.

We rewrite *Equation 7.2* as:

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

Since y is even, y^2 is divisible by 4. Dividing the equation by 4

yields:

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right).$$

Let $u = (z-x)/2$ and $v = (z+x)/2$. Since x and z are both odd, u and v are integers. We compute their greatest common divisor:

$$(u,v) = \left(\frac{z-x}{2}, \frac{z+x}{2}\right) = (u+v, v) = \left(z, \frac{z+x}{2}\right).$$

Since $(z,x) = 1$, it follows that $(z, z+x) = 1$. Since z is odd, $(z, (z+x)/2) = 1$. Thus, u and v are coprime.

The product uv is a perfect square. By the fundamental theorem of arithmetic, since $(u,v) = 1$, both u and v must be perfect squares. Let $v = a^2$ and $u = b^2$ for some positive integers a, b. Solving for x, y, z:

$$\begin{aligned} z &= v + u = a^2 + b^2, \\ x &= v - u = a^2 - b^2, \\ y^2 &= 4uv = 4a^2b^2 \implies y = 2ab. \end{aligned}$$

The condition $(u,v) = 1$ implies $(a^2, b^2) = 1$, so $(a,b) = 1$. Finally, since $z = a^2 + b^2$ is odd, a^2 and b^2 must have opposite parity, implying a and b have opposite parity.

Conversely, direct substitution confirms that these formulae satisfy $x^2 + y^2 = z^2$. To verify primitivity, let $d = (x,z) = (a^2 - b^2, a^2 + b^2)$. Then d divides the sum $2a^2$ and the difference $2b^2$. Since $(a,b) = 1$, d must divide 2. As x is odd (since a, b have opposite parity), d must be 1.

■

7.4 *Fermat's Equation*

Fermat's equation refers to the indeterminate equation

$$x^n + y^n = z^n, \quad n \geq 3.$$

Pierre de Fermat famously asserted that this equation possesses no non-trivial integer solutions (i.e., solutions where $xyz \neq 0$). This claim, known as *Fermat's Last Theorem*, remained unproven for over three centuries until Andrew Wiles provided a complete proof in 1995.

We present Fermat's own proof for the case $n = 4$. This proof utilises the *Method of Infinite Descent*, a powerful variation of the well-ordering principle tailored for Diophantine equations.

Remark (The Method of Infinite Descent).

To prove that a property P holds for no positive integer (or that an equation has no solution):

1. Assume for the sake of contradiction that a solution exists.
2. Select a solution that is "minimal" with respect to some positive integer parameter (typically one of the variables, such as z).
3. Construct a new valid solution from the existing one that is strictly smaller with respect to that parameter.
4. This contradicts the minimality assumption (since a strictly decreasing sequence of positive integers cannot be infinite), proving that no such solution exists.

Theorem 7.4. ***Fermat's Last Theorem for*** $n = 4$**.**
The equation

$$x^4 + y^4 = z^2 \tag{7.3}$$

has no solutions in positive integers. Since any solution to $x^4 + y^4 = w^4$ corresponds to a solution of *Equation 7.3* with $z = w^2$, it follows that $x^4 + y^4 = w^4$ has no non-trivial integer solutions.

定理

Proof

Assume there exists a solution (x_0, y_0, z_0) in positive integers. By the well-ordering principle, we may choose the solution with the minimal value of z_0.

We first show that we can assume $(x_0, y_0) = 1$. If $d = (x_0, y_0) > 1$, then $d^4 \mid (x_0^4 + y_0^4) = z_0^2$. Thus $d^2 \mid z_0$. The triple $(x_0/d, y_0/d, z_0/d^2)$ would be a solution with a strictly smaller z component ($z_0/d^2 < z_0$), contradicting minimality. Hence, we assume the solution is primitive.

The equation can be written as $(x_0^2)^2 + (y_0^2)^2 = z_0^2$. Since $(x_0, y_0) = 1$, $(x_0^2, y_0^2) = 1$. Thus (x_0^2, y_0^2, z_0) is a primitive Pythagorean triple. By *Theorem 7.3*, assuming y_0^2 is even (one of the squares must be even), there exist coprime integers a, b of opposite parity such that:

$$x_0^2 = a^2 - b^2, \quad y_0^2 = 2ab, \quad z_0 = a^2 + b^2.$$

The first equation rearranges to $x_0^2 + b^2 = a^2$. Since $(a, b) = 1$, it follows that $(x_0, b) = 1$. Thus, (x_0, b, a) is another primitive Pythagorean triple.

We must determine the parity of b. Since $a^2 + b^2 = z_0$ is odd (primitive triple hypotenuse), a and b have opposite parity. Furthermore, $x_0^2 = a^2 - b^2$ implies x_0 is odd (if x_0 were even, $x_0^2 \equiv 0 \pmod 4$, requiring $a^2 \equiv b^2$, impossible for opposite parity coprime squares). Since x_0 is odd, b must be even (as part of the triple $x_0^2 + b^2 = a^2$).

Applying *Theorem 7.3* to $x_0^2 + b^2 = a^2$, with b even, there exist coprime integers c, d of opposite parity such that:

$$x_0 = c^2 - d^2, \quad b = 2cd, \quad a = c^2 + d^2.$$

We substitute these expressions back into the equation for y_0^2:

$$y_0^2 = 2ab = 2(c^2 + d^2)(2cd) = 4cd(c^2 + d^2).$$

This implies

$$\left(\frac{y_0}{2}\right)^2 = cd(c^2 + d^2).$$

Since c and d are coprime, they are pairwise coprime to $c^2 + d^2$. Since their product is a perfect square, c, d, and $c^2 + d^2$ must each be perfect squares. Let $c = r^2$, $d = s^2$, and $c^2 + d^2 = t^2$ for positive integers r, s, t. Substituting c and d into the last equation yields:

$$(r^2)^2 + (s^2)^2 = t^2 \implies r^4 + s^4 = t^2.$$

Thus, (r, s, t) is a solution to the original equation *Equation 7.3*. We now compare t to our minimal z_0:

$$t = \sqrt{c^2 + d^2} = \sqrt{a} \leq \sqrt{a^2 + b^2} = \sqrt{z_0}.$$

Since z_0 is part of a primitive triple, $z_0 > 1$, so $\sqrt{z_0} < z_0$. Thus $t < z_0$. We have constructed a solution (r, s, t) with a strictly smaller hypotenuse value. This contradicts the minimality of z_0. Therefore, no such solution exists.

■

7.5 *Sum of Two Squares*

We apply the arithmetic tools developed in previous sections to the classical problem of representing integers as sums of squares. This investigation classifies integers n for which the Diophantine equation

$$x_1^2 + x_2^2 + \cdots + x_k^2 = n$$

admits integer solutions. We focus on the cases $k = 2, 3, 4$, culminating in Lagrange's Four-Square Theorem.
We consider the representation of a positive integer n as the sum of two squares, $n = x^2 + y^2$. A fundamental tool is the algebraic identity relating sums of squares to the modulus of complex numbers.

Lemma 7.1. ***Brahmagupta–Fibonacci Identity.***

For any integers a, b, c, d:

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

Consequently, the set of integers representable as a sum of two squares is closed under multiplication.

引理

Proof

Consider the complex numbers $z_1 = a + bi$ and $z_2 = c + di$. The identity follows immediately from the multiplicative property of the modulus, $|z_1 z_2|^2 = |z_1|^2 |z_2|^2$, upon observing that $|a + bi|^2 = a^2 + b^2$.

■

Since n can be decomposed into prime factors, the problem reduces to determining which primes p are sums of two squares. The prime 2 is trivially representable as $1^2 + 1^2$. For odd primes, the solvability is dictated by their residue modulo 4.

Theorem 7.5. ***Fermat's Theorem on Sums of Two Squares.***
An odd prime p is expressible as a sum of two integer squares if and only if $p \equiv 1 \pmod 4$. Moreover, this representation is unique up to the order and signs of x, y.

定理

Necessity.

Suppose $p = x^2 + y^2$. Since p is odd, x and y have opposite parity. Thus, modulo 4,

$$p \equiv x^2 + y^2 \equiv 0 + 1 \equiv 1 \pmod 4,$$

since squares are congruent to 0 or $1 \pmod 4$.

証明終

Sufficiency.

Let $p \equiv 1 \pmod 4$. By the First Supplement to the *Law of Quadratic Reciprocity*, $\left(\frac{-1}{p}\right) = 1$. Thus, there exists an integer z such that $z^2 \equiv -1 \pmod p$. We can choose $|z| \leq p/2$. Consequently, $z^2 + 1 = mp$ for some integer m. Since $z^2 < p^2/4$, we have

$$0 < mp = z^2 + 1 \leq \frac{p^2}{4} + 1 < p^2,$$

which implies $0 < m < p$. Thus, a multiple of p is a sum of two squares. Let m_0 be the least positive integer such that $m_0 p = x^2 + y^2$. We claim $m_0 = 1$. Suppose for contradiction that $m_0 > 1$. We proceed by infinite descent. Let u and v be the least magnitude residues of x and y modulo m_0, respectively. That

is,

$$u \equiv x \pmod{m_0}, \quad v \equiv y \pmod{m_0}, \quad -\frac{m_0}{2} < u, v \leq \frac{m_0}{2}.$$

Then

$$u^2 + v^2 \equiv x^2 + y^2 \equiv m_0 p \equiv 0 \pmod{m_0}.$$

Let $u^2 + v^2 = km_0$. Since $|u|, |v| \leq m_0/2$, we have $u^2 + v^2 \leq m_0^2/2$. Thus $km_0 \leq m_0^2/2$, implying $0 \leq k \leq m_0/2 < m_0$. If $k = 0$, then $u = v = 0$, so $m_0 \mid x$ and $m_0 \mid y$. Then $m_0^2 \mid (x^2 + y^2) = m_0 p$, so $m_0 \mid p$. Since $m_0 < p$, this forces $m_0 = 1$, a contradiction. Thus $0 < k < m_0$. Now, we multiply the representations using *Lemma 7.1*:

$$m_0 p \cdot km_0 = (x^2 + y^2)(u^2 + v^2) = (xu + yv)^2 + (xv - yu)^2.$$

We verify the divisibility of the terms on the RHS by m_0:

$$xu + yv \equiv x(x) + y(y) = x^2 + y^2 = m_0 p \equiv 0 \pmod{m_0},$$
$$xv - yu \equiv x(y) - y(x) = 0 \pmod{m_0}.$$

Thus, $X = (xu + yv)/m_0$ and $Y = (xv - yu)/m_0$ are integers. Substituting back:

$$m_0^2 kp = (m_0 X)^2 + (m_0 Y)^2 \implies kp = X^2 + Y^2.$$

We have found a representation of a multiple kp as a sum of two squares with $0 < k < m_0$. This contradicts the minimality of m_0. Therefore, $m_0 = 1$, and $p = x^2 + y^2$.

証明終

Uniqueness.

Suppose $p = a^2 + b^2 = c^2 + d^2$. Then $p^2 = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$. Also $(ac + bd)(ac - bd) = a^2c^2 - b^2d^2 = a^2c^2 - (p - a^2)(p - c^2) \equiv a^2c^2 - a^2c^2 \equiv 0 \pmod{p}$. Thus p divides one of the factors. If $p \mid (ac - bd)$, then $(ac - bd)^2$ is divisible by p^2. In the equation for p^2, since $(ac + bd)^2 > 0$, we must have $ad - bc = 0$ (otherwise $(ad - bc)^2 \geq p^2$, impossible). $ad = bc \implies a/b = c/d$. Since a, b are coprime (as their sum of squares is prime) and c, d are coprime, it follows that $\{a, b\} = \{c, d\}$.

証明終

This characterisation allows us to classify all integers expressible as a sum of two squares.

Theorem 7.6. ***Sum of Two Squares Theorem.***
A positive integer n can be written as a sum of two squares if and only if in the prime factorisation of n, every prime of the form $q \equiv 3 \pmod{4}$ occurs with an even exponent.

定理

Proof

Let $n = 2^k \prod p_i^{e_i} \prod q_j^{f_j}$, where $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$.

Sufficiency: If all f_j are even, then $q_j^{f_j}$ is a perfect square, say $s_j^2 = s_j^2 + 0^2$, which is a sum of two squares. The primes p_i are sums of two squares by *Theorem 7.5*, and $2 = 1^2 + 1^2$. By *Lemma 7.1*, the set of representable integers is closed under multiplication. Thus n is a sum of two squares.

Necessity: Suppose $n = x^2 + y^2$. Let q be a prime divisor of n such that $q \equiv 3 \pmod 4$. Then $x^2 + y^2 \equiv 0 \pmod q$. If $q \nmid x$, there exists a modular inverse x^{-1} modulo q. Then $(yx^{-1})^2 \equiv -1 \pmod q$. This implies $\left(\frac{-1}{q}\right) = 1$, contradicting $q \equiv 3 \pmod 4$ (*corollary 6.1*). Therefore, $q \mid x$. Since $q \mid (x^2 + y^2)$, it follows that $q \mid y^2$, so $q \mid y$. We can write $x = qx_1$ and $y = qy_1$. Then $n = q^2(x_1^2 + y_1^2)$. The exponent of q in n is 2 plus the exponent of q in $x_1^2 + y_1^2$. By infinite descent (induction on the power of q), the total exponent of q must be even.

■

7.6 *Sums of Three and Four Squares*

While not every integer is a sum of two squares, the set of representable integers expands as we allow more squares.

Sum of Three Squares

Theorem 7.7. ***Legendre's Three-Square Theorem (Necessity).***
If a positive integer n is of the form $4^k(8m+7)$, then n cannot be expressed as the sum of three squares.

定理

Proof

We first consider the case $k = 0$, so $n \equiv 7 \pmod 8$. The quadratic residues modulo 8 are $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 1$. Thus $x^2 \equiv 0, 1, 4 \pmod 8$. We examine all possible sums of three elements from $\{0, 1, 4\}$ modulo 8:

- Maximum sum: $4 + 4 + 4 \equiv 4$.
- Combinations with 1: $1 + 1 + 1 = 3$, $4 + 1 + 1 = 6$, $4 + 4 + 1 = 1$, etc.

It is verified by exhaustion that no sum of three residues yields 7 $\pmod 8$. Thus, $n \equiv 7 \pmod 8$ is not a sum of three squares.

Suppose now $n = 4^k(8m + 7)$. We proceed by induction on k. The base case is proved. Suppose $n = 4N$ and $n = x^2 + y^2 + z^2$. Then

$x^2 + y^2 + z^2 \equiv 0 \pmod 4$. Since squares modulo 4 are 0 or 1, the only solution to $a + b + c \equiv 0 \pmod 4$ is $a \equiv b \equiv c \equiv 0 \pmod 4$ (as $1 + 1 + 1 = 3 \not\equiv 0$). Thus x, y, z must all be even. Let $x = 2x_1, y = 2y_1, z = 2z_1$. Then $4N = 4(x_1^2 + y_1^2 + z_1^2)$, so $N = x_1^2 + y_1^2 + z_1^2$. This reduces the problem to N. If $n = 4^k(8m + 7)$, repeated division by 4 eventually yields an integer of the form $8m + 7$, which is not representable.

■

Remark.

Legendre proved that this condition is also sufficient, though the proof is significantly more involved than the two-square case, relying on the theory of ternary quadratic forms.

Lagrange's Four-Square Theorem

We finally address the representation by four squares. We begin with Euler's four-square identity, which establishes the multiplicativity of the form $x^2 + y^2 + z^2 + w^2$.

Lemma 7.2. ***Euler's Four-Square Identity.***
For any sets of integers (x_k) and (y_k):

$$\left(\sum_{i=1}^{4} x_i^2\right)\left(\sum_{i=1}^{4} y_i^2\right) = \sum_{i=1}^{4} z_i^2,$$

where

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \\ z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3, \\ z_3 &= x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4, \\ z_4 &= x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2. \end{aligned}$$

引理

Remark.

This identity relates to the norm of quaternions. The norm of the product of two quaternions is the product of their norms. Alternatively, it represents the determinant of the matrix product

$$\begin{bmatrix} x_1 + ix_2 & x_3 + ix_4 \\ -x_3 + ix_4 & x_1 - ix_2 \end{bmatrix} \begin{bmatrix} y_1 + iy_2 & y_3 + iy_4 \\ -y_3 + iy_4 & y_1 - iy_2 \end{bmatrix}.$$

Since the form is multiplicative, to prove that every positive integer is a sum of four squares, it suffices to prove the result for primes. Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, we focus on odd primes.

Lemma 7.3. ***Existence of a Multiple.***
Let p be an odd prime. There exists an integer m with $1 \leq m < p$ such that mp is a sum of four squares.

引理

Proof

Consider the sets of residues $S_1 = \{x^2 : 0 \leq x \leq (p-1)/2\}$ and $S_2 = \{-1 - y^2 : 0 \leq y \leq (p-1)/2\}$. Both sets contain $(p+1)/2$ distinct elements (since $x^2 \equiv z^2 \pmod{p} \implies x \equiv \pm z$). The total number of elements is $p + 1$, which exceeds p. By the pigeonhole principle, S_1 and S_2 must share a residue modulo p. Thus, there exist x, y such that $x^2 \equiv -1 - y^2 \pmod{p}$, or

$$x^2 + y^2 + 1^2 + 0^2 = mp$$

for some integer m. Since $x, y < p/2$,

$$mp = x^2 + y^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2.$$

Thus $0 < m < p$.

■

Theorem 7.8. ***Lagrange's Four-Square Theorem.***
Every positive integer n can be expressed as the sum of four integer squares.

定理

Proof

By *Lemma 7.2*, it suffices to prove this for primes. Let p be an odd prime. Let m_0 be the least positive integer such that $m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2$. By *Lemma 7.3*, we know $1 \leq m_0 < p$. We assume $m_0 > 1$ and derive a contradiction.

Case 1: m_0 ***is even.*** If m_0 is even, then $\sum x_i^2$ is even. Thus, either all x_i are even, all are odd, or two are even and two are odd. In all cases, we can reorder such that $x_1 \equiv x_2 \pmod{2}$ and $x_3 \equiv x_4 \pmod{2}$. Then

$$\frac{m_0}{2} p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2.$$

This gives a representation for a smaller multiple $m_0/2$, contradicting the minimality of m_0. Thus m_0 must be odd.

Case 2: m_0 ***is odd.*** For each i, let y_i be the numerically least residue of x_i modulo m_0, i.e., $y_i \equiv x_i \pmod{m_0}$ and $|y_i| < m_0/2$ (strict inequality holds since m_0 is odd). Then

$$\sum y_i^2 \equiv \sum x_i^2 = m_0 p \equiv 0 \pmod{m_0}.$$

Let $\sum y_i^2 = km_0$. Since $|y_i| < m_0/2$,

$$km_0 = \sum y_i^2 < 4\left(\frac{m_0}{2}\right)^2 = m_0^2 \implies k < m_0.$$

Also $k > 0$, for if $k = 0$, then $y_i = 0$ for all i, implying $m_0 \mid x_i$. This would imply $m_0^2 \mid m_0 p$, so $m_0 \mid p$, impossible as $1 < m_0 < p$. We apply *Lemma 7.2* to the product $(m_0 p)(km_0)$:

$$m_0^2 kp = \left(\sum x_i^2\right)\left(\sum y_i^2\right) = \sum z_i^2.$$

Recall the first term in Euler's identity is $z_1 = \sum x_i y_i$. Since $y_i \equiv x_i \pmod{m_0}$,

$$z_1 = \sum x_i y_i \equiv \sum x_i^2 \equiv 0 \pmod{m_0}.$$

Similarly, one can verify that z_2, z_3, z_4 are divisible by m_0. For instance,

$$z_2 = x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3 \equiv x_1 x_2 - x_2 x_1 + \cdots \equiv 0 \pmod{m_0}.$$

Let $Z_i = z_i/m_0$. Then

$$kp = \sum Z_i^2.$$

Since $0 < k < m_0$, this contradicts the minimality of m_0. Therefore, m_0 must be 1, so p is a sum of four squares.

■

7.7 *Generalisations: Waring's Problem and Universal Forms*

Having established *Theorem 7.8*, which asserts that every positive integer is the sum of at most four squares, it is natural to inquire whether similar results hold for higher powers or more general quadratic forms. These questions form the basis of Waring's Problem and the theory of universal quadratic forms.

Waring's Problem

In 1770, Edward Waring conjectured a profound generalisation of Lagrange's result. He proposed that for every integer $k \geq 2$, there exists a fixed integer $g(k)$ such that every positive integer can be expressed as the sum of at most $g(k)$ k-th powers of non-negative integers. Specifically, Waring posited that every integer is a sum of 9 cubes, 19 fourth powers, and so on. The existence of such a bound was finally proven by Hilbert in 1909.

Theorem 7.9. ***Hilbert-Waring Theorem.***
For every integer $k \geq 2$, there exists a minimal positive integer $g(k)$

such that every $n \in \mathbb{Z}^+$ can be written as

$$n = x_1^k + x_2^k + \cdots + x_s^k,$$

with $s = g(k)$ and $x_i \in \mathbb{Z}_{\geq 0}$.

定理

While Hilbert established existence, determining the precise value of $g(k)$ is a distinct computational challenge. We know from *Theorem 7.8* that $g(2) = 4$. For $k = 3$, it was proved that $g(3) = 9$. For $k = 4$, it was established in 1986 that $g(4) = 19$.

Example 7.5. Inefficiency of Greedy Decompositions. The representation of integers as sums of powers is not necessarily achieved by the greedy algorithm (subtracting the largest possible power at each step). Consider $n = 32$ for sums of squares ($k = 2$). The greedy algorithm yields:

$$32 = 25 + 7 = 25 + 4 + 3 = 25 + 4 + 1 + 1 + 1,$$

requiring 5 squares. However, the optimal representation is $32 = 16 + 16$, which uses only 2 squares. This illustrates that minimal decompositions often require arithmetic insight beyond size reduction.

範例

Polygonal Numbers

A parallel generalisation considers the geometry of the summands. Just as squares correspond to the area of a square grid, one may define *polygonal numbers* representing triangles, pentagons, and higher m-gons.

Definition 7.4. ***Polygonal Numbers.***
For $m \geq 3$, the n-th m-gonal number $P_m(n)$ is given by the formula:

$$P_m(n) = \frac{(m-2)n^2 - (m-4)n}{2}.$$

For $m = 3$, these are the *triangular numbers* $T_n = \frac{n(n+1)}{2}$. For $m = 4$, these are the squares n^2.

定義

Fermat conjectured that every positive integer is the sum of at most m m-gonal numbers. The general conjecture was subsequently proved by Cauchy in 1813.

Theorem 7.10. ***Fermat's Polygonal Number Theorem.***
For every $m \geq 3$, every positive integer is the sum of at most m m-gonal numbers.

定理

Universal Quadratic Forms

Returning to quadratic forms, we define a form to be *universal* if it represents every positive integer. *Theorem 7.8* states that the form $x^2 + y^2 + z^2 + w^2$ is universal. Conversely, *Theorem 7.7* implies that no ternary form can be universal. Thus, a universal positive definite form must have rank at least 4.
Ramanujan (1916) systematically analysed diagonal quaternary forms $ax^2 + by^2 + cz^2 + dw^2$ and identified 54 such forms that appeared to be universal. Determining the universality of a general form is non-trivial. However, the Conway-Schneeberger 15-Theorem provides a remarkably simple sufficiency criterion for forms with integer matrix coefficients.

Theorem 7.11. ***The 15-Theorem.***
Let f be a positive definite quadratic form with integer matrix coefficients. If f represents every positive integer in the set $\{1, 2, \ldots, 15\}$, then f is universal.

定理

For general integer-valued forms (where the matrix may have half-integer off-diagonal entries), a stronger condition is required. This was established by Manjul Bhargava.

Theorem 7.12. ***The 290-Theorem.***
Let f be a positive definite quadratic form that takes integer values on $\mathbb{Z}^n$. If f represents every integer in the set $\{1, 2, \ldots, 290\}$, then f is universal.

定理

These theorems reduce the infinite problem of universality to a finite computation. For instance, to verify *Theorem 7.8*, one need only check that $x^2 + y^2 + z^2 + w^2$ represents the integers up to 15.

7.8 *Exercises*

1. **Sum of Two Squares: Computation.** Determine which of the following integers can be expressed as the sum of two squares of integers. For those that can, find at least one explicit representation $n = x^2 + y^2$.
   (a) 54
   (b) 171
   (c) 282
   (d) 379
   (e) 487

(f) 6291
(g) 40003

2. **Difference of Two Squares.**
   (a) Determine necessary and sufficient conditions for an integer n to be expressible as the difference of two integer squares, i.e., $n = x^2 - y^2$.
   (b) Prove that for any integer n, the equation $x^2 + y^2 - z^2 = n$ has infinitely many solutions in positive integers x, y, z.

For (b): Try setting $z = y + k$ and reducing the equation to a linear one in y.

3. **Sum of Three Squares Obstruction.** Show that the integers 7, 15, 23, and 28 cannot be expressed as the sum of three squares of integers.

4. **Prime Powers and Sums of Squares.** Let p be a prime number with $p \equiv 3 \pmod 4$. Prove that for all $k \geq 1$, p^k cannot be expressed as the sum of two squares of *positive* integers.

Distinguish between integer solutions (where one square could be zero) and positive integer solutions. Note that $p^k = p^k + 0^2$ is a valid sum of squares in $\mathbb{Z}$, but the question asks for positive integers.

5. **Gaps in Sums of Two Squares.** Prove that for any given $n \geq 1$, there exist n consecutive positive integers such that none of them can be expressed as the sum of two squares of integers.

6. **Jacobi Symbol Computation.** Let $n = 77$.
   (a) Evaluate the Jacobi symbols $\left(\frac{-1}{77}\right)$ and $\left(\frac{2}{77}\right)$ using the Generalised Reciprocity Laws.
   (b) Verify your results by computing the Legendre symbols $\left(\frac{a}{7}\right)$ and $\left(\frac{a}{11}\right)$ directly.

7. **Local Solvability Counter-Example.** Verify that the equation $2x^2 + 7y^2 = 1$ has solutions modulo m for every integer $m > 1$, but has no rational solutions.

8. **Pythagorean Triples.** Find all primitive Pythagorean triples (x, y, z) such that $x + y + z = 40$.

9. **Fermat for $n = 4$ Variant.** Show that the equation $x^4 - y^4 = z^2$ has no solutions in non-zero integers.

10. **Sums of Squares in $\mathbb{Z}_p$.** Let p be an odd prime. Prove that the set of squares $S = \{x^2 \pmod p\}$ satisfies $S + S = \mathbb{Z}_p$. That is, every element in $\mathbb{Z}_p$ is the sum of two squares.

11. **Waring's Problem Bound.** Prove that $g(2) \geq 4$. That is, finding an integer that requires 4 squares. Prove that $g(3) \geq 9$.

Consider integers of the form $2^n - 1$ or similar specific structures.

12. ⋆ **The 15-Theorem Application.** Determine whether the quadratic form $Q(x, y, z, w) = x^2 + 2y^2 + 5z^2 + 5w^2$ is universal.

Check representability of integers $1, \ldots, 15$.

13. **Liouville's Formula.** Let $r_2(n)$ denote the number of representations of n as a sum of two squares (counting order and signs). Prove that $r_2(n) = 4(d_1(n) - d_3(n))$, where $d_1(n)$ is the number

of divisors of n of the form $4k+1$, and $d_3(n)$ is the number of divisors of the form $4k+3$.

A
Appendix: Pell's Equation

We now turn our attention to one of the most famous Diophantine equations, the study of which bridges elementary number theory and the arithmetic of quadratic fields. This investigation naturally introduces the concept of algebraic integers and the group structure of units in quadratic rings.

A.1 The Equation and Quadratic Rings

Let $d \in \mathbb{Z}_{>1}$ be a squarefree integer. **Pell's equation** is the quadratic Diophantine equation

$$x^2 - dy^2 = 1. \tag{A.1}$$

We seek integral solutions $(x, y) \in \mathbb{Z}^2$. The factorisation of the left-hand side over $\mathbb{R}$ suggests the introduction of an algebraic structure extending the integers:

$$x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d}).$$

This motivates the study of the ring $\mathbb{Z}[\sqrt{d}]$.

Definition A.1. ***Ring Adjunction.***
Let $\alpha \in \mathbb{C}$. We define $\mathbb{Z}[\alpha]$ as the smallest subring of $\mathbb{C}$ containing α. Equivalently, it is the intersection of all subrings of $\mathbb{C}$ containing α. Explicitly,

$$\mathbb{Z}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Z}[X]\} = \{a_0 + a_1\alpha + \cdots + a_n\alpha^n \mid n \in \mathbb{Z}_{\geq 0}, a_i \in \mathbb{Z}\}.$$

定義

Example A.1. Examples of Adjoined Rings.

- If $\alpha = 1$, then $\mathbb{Z}[1] = \mathbb{Z}$.
- If $\alpha = i$, then $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, known as the Gaussian integers.
- Consider $\alpha = \sqrt[3]{2}$. The set $\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z}\}$ is *not* a ring because it is not closed under multiplication (it does not contain $(\sqrt[3]{2})^2 = \sqrt[3]{4}$). Thus $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}$.

· If $\alpha = 1/p$ for a prime p, then $\mathbb{Z}[1/p] = \{a/p^n \mid a \in \mathbb{Z}, n \geq 0\}$.

範例

To study Pell's equation systematically, we restrict our attention to quadratic extensions.

Definition A.2. ***Algebraic Integers of Degree Two.***
A number $\alpha \in \mathbb{C}$ is an *algebraic integer of degree two* if $\alpha \notin \mathbb{Z}$ and α is a root of a monic quadratic polynomial with integer coefficients:

$$X^2 + aX + b = 0, \quad a, b \in \mathbb{Z}.$$

定義

For Pell's equation, we are interested in $\alpha = \sqrt{d}$. Since d is squarefree and $d > 1$, α is a root of $X^2 - d = 0$, satisfying the definition.

Proposition A.1. ***Structure of Quadratic Rings.***
If α is an algebraic integer of degree two, then

$$\mathbb{Z}[\alpha] = \{x + y\alpha \mid x, y \in \mathbb{Z}\}.$$

命題

Proof

First, we show that $\alpha \notin \mathbb{Q}$. Suppose $\alpha = r/s$ with $(r, s) = 1$ and $s > 0$. Substituting into $X^2 + aX + b = 0$, we obtain

$$\frac{r^2}{s^2} + a\frac{r}{s} + b = 0 \implies r^2 + ars + bs^2 = 0.$$

Thus $s \mid r^2$. Since $(r, s) = 1$, this implies $s \mid 1$, so $s = 1$ and $\alpha \in \mathbb{Z}$, a contradiction.
Consequently, if $x, y \in \mathbb{Z}$ and $x + y\alpha = 0$, then $x = y = 0$. This ensures the representation $x + y\alpha$ is unique. Let $S = \{x + y\alpha \mid x, y \in \mathbb{Z}\}$. Clearly $S \subseteq \mathbb{Z}[\alpha]$ and S is an additive group containing 1. To show $S = \mathbb{Z}[\alpha]$, it suffices to show S is closed under multiplication. Let $z = x + y\alpha$ and $w = X + Y\alpha$. Then:

$$zw = (x + y\alpha)(X + Y\alpha) = xX + (xY + yX)\alpha + yY\alpha^2.$$

Since $\alpha^2 = -a\alpha - b$, we substitute:

$$zw = (xX - byY) + (xY + yX - ayY)\alpha.$$

Since $a, b \in \mathbb{Z}$, the coefficients remain integers, so $zw \in S$.

■

We distinguish between **real quadratic subrings** (where $\alpha \in \mathbb{R}$) and **imaginary quadratic subrings** (where $\alpha \notin \mathbb{R}$). For Pell's equation,

$\mathbb{Z}[\sqrt{d}]$ is real quadratic.

Norms and Units

Associated with the quadratic equation $X^2 + aX + b = 0$ is the conjugation map. Let α^* be the other root of the polynomial. For $z = x + y\alpha \in \mathbb{Z}[\alpha]$, we define the conjugate $z^* = x + y\alpha^*$. Note that $\alpha + \alpha^* = -a$ and $\alpha\alpha^* = b$.

Definition A.3. ***Norm.***
The *norm* map $N : \mathbb{Z}[\alpha] \to \mathbb{Z}$ is defined by

$$N(z) = zz^*.$$

For $z = x + y\alpha$, explicit calculation yields:

$$N(x+y\alpha) = (x+y\alpha)(x+y\alpha^*) = x^2 + xy(\alpha+\alpha^*) + y^2\alpha\alpha^* = x^2 - axy + by^2.$$

Since $a, b \in \mathbb{Z}$, the norm is integer-valued.

定義

The norm is totally multiplicative. Since $(zw)^* = z^*w^*$, we have

$$N(zw) = zw(zw)^* = zz^*ww^* = N(z)N(w).$$

Furthermore, $N(x + y\alpha) = 0$ if and only if $x = y = 0$.

Remark (Pell Connection).
In the specific case $\alpha = \sqrt{d}$, the roots of $X^2 - d$ are $\pm\sqrt{d}$. Thus $\alpha^* = -\sqrt{d}$. The norm becomes:

$$N(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

Notice that $N(\sqrt{d}) = -d < 0$. In real quadratic fields, the norm may be negative. The solutions to Pell's equation $x^2 - dy^2 = 1$ correspond precisely to elements $z \in \mathbb{Z}[\sqrt{d}]$ such that $N(z) = 1$.

Definition A.4. ***Units.***
The group of *units* of $\mathbb{Z}[\alpha]$, denoted $\mathbb{Z}[\alpha]^\times$, consists of elements with multiplicative inverses in the ring:

$$\mathbb{Z}[\alpha]^\times = \{z \in \mathbb{Z}[\alpha] \mid \exists w \in \mathbb{Z}[\alpha], zw = 1\}.$$

Using the multiplicative property of the norm, z is a unit if and only if $N(z) = \pm 1$. We define the subgroup of **1-units** as:

$$\mathbb{Z}[\alpha]^{\times,1} = \{z \in \mathbb{Z}[\alpha] \mid N(z) = 1\}.$$

定義

For $\mathbb{Z}[\sqrt{d}]$, the set of solutions to Pell's equation corresponds exactly to $\mathbb{Z}[\sqrt{d}]^{\times,1}$.

A.2 *Structure of Solutions*

We now analyse the structure of $\mathbb{Z}[\sqrt{d}]^{\times,1}$. It trivially contains ± 1. We seek to determine if there are non-trivial solutions.

Lemma A.1. ***Sign Properties.***
Let $u = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]^{\times,1}$. Then:

$$\begin{aligned} x > 0,\ y > 0 &\iff u > 1, \\ x > 0,\ y < 0 &\iff 0 < u < 1, \\ x < 0,\ y > 0 &\iff -1 < u < 0, \\ x < 0,\ y < 0 &\iff u < -1. \end{aligned}$$

引理

Proof

Suppose $x, y > 0$. Then $x + y\sqrt{d} > y\sqrt{d} \geq \sqrt{d} > 1$. Since $N(u) = 1$, we have $(x + y\sqrt{d})(x - y\sqrt{d}) = 1$. Thus $x - y\sqrt{d} = u^{-1}$. Since $u > 1$, it follows that $0 < u^{-1} < 1$. Replacing y with $-y$ corresponds to taking the inverse $u^{-1} = x - y\sqrt{d}$. Thus $x > 0, y < 0 \iff u \in (0, 1)$. The negative cases follow by considering $-u = -x - y\sqrt{d}$. These four cases exhaust all possibilities for non-zero x, y.

■

Lemma A.2. ***Monotonicity.***
Let $z = x + y\sqrt{d}$ and $z' = x' + y'\sqrt{d}$ be elements of $\mathbb{Z}[\sqrt{d}]^{\times,1}$ with $z, z' > 1$ (implying $x, y, x', y' > 0$). Then $z > z'$ if and only if $y > y'$.

引理

Proof

Consider the function $f(t) = t - 1/t$. Its derivative is $1 + 1/t^2 > 0$, so it is strictly increasing for $t > 0$. For any unit $u = x + y\sqrt{d}$ with norm 1, we have $u^{-1} = x - y\sqrt{d}$. Thus $u - u^{-1} = (x + y\sqrt{d}) - (x - y\sqrt{d}) = 2y\sqrt{d}$. Therefore, $z > z' \iff z - 1/z > z' - 1/z' \iff 2y\sqrt{d} > 2y'\sqrt{d} \iff y > y'$.

■

This monotonicity allows us to identify a generator for the group of units. If there exists any unit $z > 1$, there must exist a smallest such unit, as the integer component y must be a positive integer and cannot decrease indefinitely.

Definition A.5. ***Fundamental Unit.***
The *fundamental 1-unit* ϵ of $\mathbb{Z}[\sqrt{d}]$ is the smallest element of $\mathbb{Z}[\sqrt{d}]^{\times,1}$ such that $\epsilon > 1$. By *Lemma A.2*, this corresponds to the solution $x + y\sqrt{d}$ with the minimal positive y.

定義

Proposition A.2. ***Structure of the Unit Group.***
If $\mathbb{Z}[\sqrt{d}]^{\times,1} \neq \{\pm 1\}$, then

$$\mathbb{Z}[\sqrt{d}]^{\times,1} = \{\pm\epsilon^n \mid n \in \mathbb{Z}\},$$

where ϵ is the fundamental 1-unit.

命題

Proof

Let $z \in \mathbb{Z}[\sqrt{d}]^{\times,1}$. If $z = \pm 1$, the claim holds with $n = 0$. Otherwise, by replacing z with $-z$, z^{-1}, or $-z^{-1}$, we may assume $z > 1$. Suppose z is not an integer power of ϵ. Since $\epsilon > 1$, the sequence ϵ^n tends to infinity. There exists a unique integer $n \geq 1$ such that

$$\epsilon^n < z < \epsilon^{n+1}.$$

Multiply by ϵ^{-n}:

$$1 < z\epsilon^{-n} < \epsilon.$$

Let $w = z\epsilon^{-n}$. Since units form a group, $w \in \mathbb{Z}[\sqrt{d}]^{\times,1}$. However, we have found a unit w strictly between 1 and the fundamental unit ϵ. This contradicts the minimality of ϵ. Thus, $z = \epsilon^n$.

■

Example A.2. Pell's Equation for $d = 2$. Consider $x^2 - 2y^2 = 1$. The smallest positive solution is $x = 3, y = 2$. Thus $\epsilon = 3 + 2\sqrt{2}$. All other solutions are generated by powers of ϵ:
- $n = 1$: $3 + 2\sqrt{2}$ $(x = 3, y = 2)$.
- $n = 2$: $(3 + 2\sqrt{2})^2 = 9 + 8 + 12\sqrt{2} = 17 + 12\sqrt{2}$. Check: $17^2 - 2(12)^2 = 289 - 288 = 1$.

範例

A.3 *Existence of Solutions*

We have established the structure of the solution set contingent on the existence of at least one non-trivial solution. To prove existence, we employ Dirichlet's Diophantine approximation. The geometry of the hyperbola $x^2 - dy^2 = 1$ implies that for large x, y, we have $x/y \approx \sqrt{d}$.

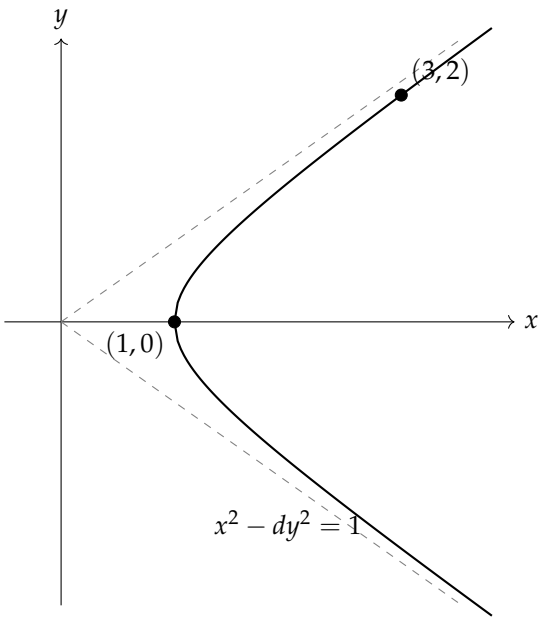

Figure A.1: The positive branch of the hyperbola $x^2 - dy^2 = 1$. Solutions correspond to integer lattice points on the curve.

Theorem A.1. ***Dirichlet's Approximation Theorem.***
Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and let $Q \in \mathbb{Z}_{>1}$. There exist integers p, q such that

$$1 \leq q < Q, \quad |p - q\alpha| < \frac{1}{Q}.$$

定理

Proof

For each $k \in \{1, \ldots, Q-1\}$, let $a_k = \{k\alpha\} = k\alpha - \lfloor k\alpha \rfloor$ denote the fractional part. Clearly $a_k \in (0,1)$. Consider the partition of $[0,1]$ into Q sub-intervals:

$$\left[0, \frac{1}{Q}\right), \left[\frac{1}{Q}, \frac{2}{Q}\right), \ldots, \left[\frac{Q-1}{Q}, 1\right].$$

Consider the set of $Q+1$ points:

$$S = \{0, a_1, a_2, \ldots, a_{Q-1}, 1\}.$$

By the Pigeonhole Principle, at least two points from S must fall into the same sub-interval. The distance between these two points is less than $1/Q$.

- If one point is 1 and another is a_q, then $|1 - (q\alpha - \lfloor q\alpha \rfloor)| < 1/Q$. Let $p = \lfloor q\alpha \rfloor + 1$. Then $|p - q\alpha| < 1/Q$.
- If one point is 0 and another is a_q, then $|q\alpha - p| < 1/Q$ with $p = \lfloor q\alpha \rfloor$.

- If the points are a_j and a_k with $j < k$, then $|\{k\alpha\} - \{j\alpha\}| < 1/Q$.

$$|(k\alpha - \lfloor k\alpha \rfloor) - (j\alpha - \lfloor j\alpha \rfloor)| = |(k-j)\alpha - (\lfloor k\alpha \rfloor - \lfloor j\alpha \rfloor)| < \frac{1}{Q}.$$

Let $q = k - j$ and $p = \lfloor k\alpha \rfloor - \lfloor j\alpha \rfloor$. Then $1 \leq q < Q$ and $|q\alpha - p| < 1/Q$.

■

Corollary A.1. *Infinite Approximations.* For any irrational α, there exist infinitely many pairs of coprime integers (p, q) with $q > 0$ such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

推論

Proof

By *Theorem A.1*, there exists at least one such pair (p, q) satisfying $|p - q\alpha| < 1/Q \leq 1/q$, which implies $|\alpha - p/q| < 1/q^2$. Suppose there were only finitely many such pairs $(p_1, q_1), \ldots, (p_n, q_n)$. Let $\delta = \min_i |\alpha - p_i/q_i|$. Since α is irrational, $\delta > 0$. Choose an integer Q such that $1/Q < \delta$. By *Theorem A.1*, there exists a pair (p', q') with $1 \leq q' < Q$ such that

$$\left|\alpha - \frac{p'}{q'}\right| < \frac{1}{q'Q} \leq \frac{1}{Q} < \delta.$$

Also $1/(q'Q) < 1/(q')^2$. This new pair (p', q') satisfies the inequality and is distinct from all (p_i, q_i) because the difference $|\alpha - p'/q'|$ is strictly smaller than δ. This contradiction establishes the existence of infinitely many solutions.

■

We are now equipped to prove the solvability of Pell's equation.

Theorem A.2. ***Existence of Solutions.***
If $d > 1$ is squarefree, then there exists a non-trivial solution to $x^2 - dy^2 = 1$.

定理

Proof

Let $\alpha = \sqrt{d}$. By *Corollary A.1*, there exist infinitely many distinct pairs (p_k, q_k) with $q_k > 0$ such that $|p_k - q_k\sqrt{d}| < 1/q_k$. For such pairs, we bound the norm:

$$|p_k + q_k\sqrt{d}| = |p_k - q_k\sqrt{d} + 2q_k\sqrt{d}| < \frac{1}{q_k} + 2q_k\sqrt{d} \leq q_k(1 + 2\sqrt{d}) < 3q_k\sqrt{d}.$$

(Using $q_k \geq 1$ and $1/q_k \leq q_k$). Calculating the norm:

$$|N(p_k + q_k\sqrt{d})| = |p_k - q_k\sqrt{d}| \cdot |p_k + q_k\sqrt{d}| < \frac{1}{q_k} \cdot 3q_k\sqrt{d} = 3\sqrt{d}.$$

Thus, for infinitely many pairs (p_k, q_k), the integer value $N(p_k + q_k\sqrt{d})$ lies in the bounded interval $(-3\sqrt{d}, 3\sqrt{d})$. By the Pigeonhole Principle, there exists an integer $M \in (-3\sqrt{d}, 3\sqrt{d}) \setminus \{0\}$ such that

$$N(p_k + q_k\sqrt{d}) = p_k^2 - dq_k^2 = M$$

for infinitely many k. Let this subset of pairs be S_M.
Since there are infinitely many pairs in S_M but only M^2 possible residue classes modulo $|M|$, there must exist two distinct pairs (p_i, q_i) and (p_j, q_j) in S_M such that

$$p_i \equiv p_j \pmod{|M|} \quad \text{and} \quad q_i \equiv q_j \pmod{|M|}.$$

Let $z_i = p_i + q_i\sqrt{d}$ and $z_j = p_j + q_j\sqrt{d}$. We construct a unit by considering their quotient $u = z_i z_j^{-1}$. Working in $\mathbb{Q}[\sqrt{d}]$:

$$u = \frac{p_i + q_i\sqrt{d}}{p_j + q_j\sqrt{d}} = \frac{(p_i + q_i\sqrt{d})(p_j - q_j\sqrt{d})}{p_j^2 - dq_j^2} = \frac{(p_ip_j - dq_iq_j) + (q_ip_j - p_iq_j)\sqrt{d}}{M}.$$

We verify the integrality of the coefficients:
Coefficient of $\sqrt{d}$: $q_ip_j - p_iq_j$. Since $p_i \equiv p_j$ and $q_i \equiv q_j \pmod{|M|}$,

$$q_ip_j - p_iq_j \equiv q_jp_j - p_jq_j \equiv 0 \pmod{|M|}.$$

Rational part: $p_ip_j - dq_iq_j$.

$$p_ip_j - dq_iq_j \equiv p_i^2 - dq_i^2 \equiv M \equiv 0 \pmod{|M|}.$$

Thus $u = x + y\sqrt{d}$ with $x, y \in \mathbb{Z}$. Finally, the norm of the quotient is the quotient of the norms:

$$N(u) = N(z_i/z_j) = N(z_i)/N(z_j) = M/M = 1.$$

Since $(p_i, q_i) \neq (p_j, q_j)$, it can be shown that $u \neq \pm 1$. Thus we have found a non-trivial solution to Pell's equation.

■

The Negative Pell Equation Consider the related equation

$$x^2 - dy^2 = -1.$$

This equation does not always have solutions. For example, if $d = 3$, modulo 3 gives $x^2 \equiv -1 \pmod{3}$, which is impossible. A solution exists if and only if there exists a unit $u \in \mathbb{Z}[\sqrt{d}]^\times$ with norm -1. If

such a fundamental unit u exists, all solutions to $x^2 - dy^2 = \pm 1$ are of the form $\pm u^n$. The even powers give solutions to the $+1$ equation, and odd powers give solutions to the -1 equation.

A.4 Exercises

1. **Solving Pell's Equation.** Find the fundamental solution (x_1, y_1) and the next two positive solutions for the following values of d:
   (a) $d = 3$
   (b) $d = 5$
   (c) $d = 7$
2. **Unit Group Structure.** Consider the ring $\mathbb{Z}[\sqrt{6}]$.
   (a) Find the fundamental unit ϵ with norm 1.
   (b) Prove that there is no unit with norm -1.
   (c) Describe the set of all integer solutions to $x^2 - 6y^2 = 1$.
3. **Negative Pell Equation Obstructions.** Prove that $x^2 - dy^2 = -1$ has no integer solutions if $d \equiv 3 \pmod 4$.
4. **Approximation by Rationals.** Use the continued fraction expansion of $\sqrt{2}$ (or trial and error) to find three rational numbers p/q such that $|\sqrt{2} - p/q| < 1/q^2$.
5. **Units in Gaussian Integers.** Determine the group of units for the ring of Gaussian integers $\mathbb{Z}[i]$. Explain why this group is finite, unlike the real quadratic case.
6. **Norm Properties.** Let $\alpha = \sqrt{d}$. Prove that for any $z, w \in \mathbb{Z}[\alpha]$, $N(zw) = N(z)N(w)$.
7. **Triangular Square Numbers.** A number is called a *triangular square* if it is both a triangular number ($T_n = n(n+1)/2$) and a perfect square (m^2).
   (a) Show that finding triangular square numbers is equivalent to solving the Pell equation $x^2 - 2y^2 = 1$.
   (b) Find the first three triangular square numbers.

B
Appendix: Continued Fractions and Approximation

Having investigated Pell's equation $x^2 - dy^2 = 1$ using Dirichlet's Approximation Theorem, we now develop the general theory of continued fractions. This framework provides an algorithmic approach to finding best rational approximations and fundamental units.

B.1 Rational Continued Fractions

We begin with the continued fraction expansion for rational numbers, which is intimately connected to the Euclidean algorithm.

Definition B.1. ***Finite Continued Fraction.***
Let $x \in \mathbb{Q}$. We can write x uniquely as

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}},$$

where $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{Z}_{\geq 1}$ for $i \geq 1$. We denote this expansion by $[a_0; a_1, \ldots, a_n]$. The algorithm proceeds as follows: Let $x_0 = x$. For $i \geq 0$, define $a_i = \lfloor x_i \rfloor$. If $x_i \in \mathbb{Z}$, stop. Otherwise, define $x_{i+1} = \frac{1}{x_i - a_i}$.

定義

Example B.1. Expansion of 40/19. Consider $x = \frac{40}{19}$.

$$x_0 = \frac{40}{19} = 2 + \frac{2}{19} \implies a_0 = 2,\ r_0 = \frac{2}{19}.$$
$$x_1 = \frac{1}{r_0} = \frac{19}{2} = 9 + \frac{1}{2} \implies a_1 = 9,\ r_1 = \frac{1}{2}.$$
$$x_2 = \frac{1}{r_1} = 2 = 2 + 0 \implies a_2 = 2.$$

The process terminates, yielding $\frac{40}{19} = [2; 9, 2]$. Checking: $2 + \frac{1}{9 + \frac{1}{2}} = 2 + \frac{1}{19/2} = 2 + \frac{2}{19} = \frac{40}{19}$.

範例

B.2 *Infinite Continued Fractions*

For irrational numbers, the algorithm does not terminate, leading to an infinite sequence of coefficients.

Definition B.2. ***Infinite Expansion.***
Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. We define the sequences $\{a_i\}$ and $\{r_i\}$ by:

$$\alpha = a_0 + r_0, \quad a_0 = \lfloor \alpha \rfloor, \quad 0 < r_0 < 1.$$

For $i \geq 0$, if $r_i \neq 0$:

$$\frac{1}{r_i} = a_{i+1} + r_{i+1}, \quad a_{i+1} = \left\lfloor \frac{1}{r_i} \right\rfloor \geq 1, \quad 0 < r_{i+1} < 1.$$

We write $\alpha = [a_0; a_1, a_2, \dots]$.

定義

Example B.2. Expansion of $\sqrt{3}$. Let $\alpha = \sqrt{3} \approx 1.732$.
1. $a_0 = \lfloor \sqrt{3} \rfloor = 1$. Remainder $r_0 = \sqrt{3} - 1$.
2. $x_1 = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}$. Since $1 < \sqrt{3} < 2$, $2 < \sqrt{3}+1 < 3$, so $1 < x_1 < 1.5$. Thus $a_1 = \lfloor x_1 \rfloor = 1$. Remainder $r_1 = \frac{\sqrt{3}+1}{2} - 1 = \frac{\sqrt{3}-1}{2}$.
3. $x_2 = \frac{1}{r_1} = \frac{2}{\sqrt{3}-1} = \sqrt{3}+1$. Clearly $2 < x_2 < 3$. Thus $a_2 = \lfloor x_2 \rfloor = 2$. Remainder $r_2 = (\sqrt{3}+1) - 2 = \sqrt{3} - 1$.

Observe that $r_2 = r_0$. The process repeats with period 2. Thus $\sqrt{3} = [1; 1, 2, 1, 2, \dots] = [1; \overline{1, 2}]$.

範例

Convergents

The truncation of an infinite continued fraction yields a sequence of rational approximations called convergents.

Definition B.3. ***Convergents.***
Given a sequence $a_0, a_1, \dots$, we define the sequences $\{p_n\}$ and $\{q_n\}$ recursively:

$$\begin{aligned} p_0 &= a_0, & q_0 &= 1, \\ p_1 &= a_0 a_1 + 1, & q_1 &= a_1, \\ p_n &= a_n p_{n-1} + p_{n-2}, & q_n &= a_n q_{n-1} + q_{n-2} \quad \text{for } n \geq 2. \end{aligned}$$

The n-th convergent is defined as $c_n = \frac{p_n}{q_n}$.

定義

Lemma B.1. ***Value of Finite Continued Fractions.***

For any real numbers $a_0, \ldots, a_n$ with $a_i > 0$ for $i \geq 1$:

$$[a_0; a_1, \ldots, a_n] = \frac{p_n}{q_n}.$$

引理

Proof

We proceed by induction on n. For $n = 0$, $[a_0] = a_0/1 = p_0/q_0$. For $n = 1$, $[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}$. For $n > 1$, observe that

$$[a_0; a_1, \ldots, a_n] = \left[a_0; a_1, \ldots, a_{n-2}, a_{n-1} + \frac{1}{a_n}\right].$$

Let p'_k, q'_k be the sequences for the modified fraction of length $n - 1$. Note that for $k \leq n - 2$, the coefficients are identical, so $p'_k = p_k$ and $q'_k = q_k$. By the inductive hypothesis:

$$[a_0; \ldots, a_{n-1} + 1/a_n] = \frac{p'_{n-1}}{q'_{n-1}}.$$

Using the recurrence relation for index $n - 1$ with the modified last term $\tilde{a}_{n-1} = a_{n-1} + \frac{1}{a_n}$:

$$\begin{aligned} p'_{n-1} &= \left(a_{n-1} + \frac{1}{a_n}\right) p_{n-2} + p_{n-3} = \frac{(a_n a_{n-1} + 1)p_{n-2} + a_n p_{n-3}}{a_n} \\ &= \frac{a_n(a_{n-1} p_{n-2} + p_{n-3}) + p_{n-2}}{a_n} = \frac{a_n p_{n-1} + p_{n-2}}{a_n} = \frac{p_n}{a_n}. \end{aligned}$$

Similarly, $q'_{n-1} = \frac{q_n}{a_n}$. Thus the ratio is $\frac{p_n/a_n}{q_n/a_n} = \frac{p_n}{q_n}$.

■

Since $a_i \geq 1$ for all $i \geq 1$, the denominators q_n grow at least as fast as the Fibonacci sequence, implying exponential growth.

Lemma B.2. ***Determinant Identity.***
For all $n \geq 1$:

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}.$$

Consequently, $\gcd(p_n, q_n) = 1$.

引理

Proof

For $n = 1$: $p_1 q_0 - q_1 p_0 = (a_0 a_1 + 1)(1) - a_1(a_0) = 1 = (-1)^0$. For $n > 1$:

$$\begin{aligned} p_n q_{n-1} - q_n p_{n-1} &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - (a_n q_{n-1} + q_{n-2}) p_{n-1} \\ &= p_{n-2} q_{n-1} - q_{n-2} p_{n-1} \\ &= -(p_{n-1} q_{n-2} - q_{n-1} p_{n-2}). \end{aligned}$$

The result follows by induction.

■

This identity implies that successive convergents are close:

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}.$$

Lemma B.3. ***Alternating Bounds.***
Let α be an irrational number. The even convergents are strictly increasing and bounded above by α, while the odd convergents are strictly decreasing and bounded below by α. Specifically:

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \alpha < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

引理

Proof

From *Lemma B.1*, we can express α using the complete quotient $1/r_n$. Let α_n be the tail of the continued fraction starting at index n, so $\alpha = [a_0; a_1, \ldots, a_n, \alpha_{n+1}]$, where $\alpha_{n+1} > 1$. Then

$$\alpha = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}.$$

. Consider the function $f(x) = \frac{x p_n + p_{n-1}}{x q_n + q_{n-1}}$.

$$f'(x) = \frac{p_n(x q_n + q_{n-1}) - q_n(x p_n + p_{n-1})}{(x q_n + q_{n-1})^2} = \frac{p_n q_{n-1} - q_n p_{n-1}}{(\ldots)^2} = \frac{(-1)^{n-1}}{(\ldots)^2}.$$

.

- If n is even, $f'(x) < 0$. $f(x)$ is decreasing. Since $\alpha_{n+1} < \infty$, $\alpha = f(\alpha_{n+1}) > \lim_{x\to\infty} f(x) = \frac{p_n}{q_n}$.
- If n is odd, $f'(x) > 0$. $f(x)$ is increasing. Thus $\alpha < \frac{p_n}{q_n}$.

The monotonicity of the subsequences follows from comparing p_n/q_n and p_{n+2}/q_{n+2}.

■

Corollary B.1. *Convergence.* Since

$$|\alpha - p_n/q_n| < |p_n/q_n - p_{n+1}/q_{n+1}| = \frac{1}{q_n q_{n+1}},$$

, and q_n grows exponentially, $\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$.

推論

B.3 *Best Approximations*

The convergents provide the "best" rational approximations to α in a strong sense.

Theorem B.1. *Best Rational Approximation I.*
Let α be irrational. Let $n \geq 1$. For any integers h, k with $0 < k < q_{n+1}$,

$$|k\alpha - h| \geq |q_n\alpha - p_n|.$$

Equality implies $h/k = p_n/q_n$.

定理

Proof

Consider the system of linear equations for integers u, v:

$$\begin{bmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{bmatrix} \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} h \\ k \end{bmatrix}.$$

The determinant is $p_nq_{n+1} - p_{n+1}q_n = (-1)^{n+1} \in \{\pm 1\}$. Thus, unique integer solutions u, v exist. $k = uq_n + vq_{n+1}$. If $v = 0$, then $k = uq_n$. Since $0 < k < q_{n+1}$, we must have $u \neq 0$. Then $|k\alpha - h| = |u||q_n\alpha - p_n| \geq |q_n\alpha - p_n|$. If $v \neq 0$, we claim $u \neq 0$ and u, v have opposite signs. Suppose $u = 0$. Then $k = vq_{n+1}$, impossible since $k < q_{n+1}$. Suppose u, v have the same sign. Then $|k| = |u|q_n + |v|q_{n+1} \geq q_{n+1}$, contradiction.
Now consider the approximation error:

$$k\alpha - h = u(q_n\alpha - p_n) + v(q_{n+1}\alpha - p_{n+1}).$$

Recall that $q_n\alpha - p_n$ and $q_{n+1}\alpha - p_{n+1}$ have opposite signs (*Lemma B.3*). Since u, v have opposite signs, the terms $u(q_n\alpha - p_n)$ and $v(q_{n+1}\alpha - p_{n+1})$ have the *same* sign. Thus:

$$|k\alpha - h| = |u||q_n\alpha - p_n| + |v||q_{n+1}\alpha - p_{n+1}| > |q_n\alpha - p_n|.$$

■

Corollary B.2. *Legendre's Criterion.* If $\left|\alpha - \frac{h}{k}\right| < \frac{1}{2k^2}$, then $\frac{h}{k}$ is a convergent of the continued fraction of α.

推論

Proof

Suppose h/k is not a convergent. Then $q_n \leq k < q_{n+1}$ for some n. By *Theorem B.1*, $|k\alpha - h| \geq |q_n\alpha - p_n|$.

$$\left|\alpha - \frac{h}{k}\right| \geq \frac{1}{k}|q_n\alpha - p_n| = \frac{q_n}{k}\left|\alpha - \frac{p_n}{q_n}\right|.$$

Also $\left|\alpha - \frac{p_n}{q_n}\right| > \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| - \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right|$ is not the right way. Instead, use triangle inequality on $\frac{1}{kq_n} \leq \left|\frac{h}{k} - \frac{p_n}{q_n}\right| \leq \left|\alpha - \frac{h}{k}\right| + \left|\alpha - \frac{p_n}{q_n}\right|$. Assume $|alpha - h/k| < \frac{1}{2k^2}$. From *Theorem B.1*, $|k\alpha - h| \geq$

$|q_n\alpha - p_n|$, so $|alpha - p_n/q_n| \leq \frac{k}{q_n}|alpha - h/k| < \frac{k}{q_n}\frac{1}{2k^2} = \frac{1}{2kq_n}$. Then $\frac{1}{kq_n} \leq \frac{1}{2k^2} + \frac{1}{2kq_n}$. Multiply by $2kq_n$: $2 \leq \frac{q_n}{k} + 1$, so $1 \leq \frac{q_n}{k}$, i.e., $k \leq q_n$. Since we assumed $q_n \leq k$, we must have $k = q_n$, so $h/k = p_n/q_n$.

■

B.4 Connection to Pell's Equation

We can now resolve the question of finding solutions to $x^2 - dy^2 = \pm 1$.

Proposition B.1. ***Solutions are Convergents.***
Let $d > 1$ be squarefree. If $x, y \in \mathbb{Z}^+$ satisfy $x^2 - dy^2 = 1$, then x/y is a convergent of the continued fraction of $\sqrt{d}$.

命題

Proof

$x^2 - dy^2 = (x - y\sqrt{d})(x + y\sqrt{d}) = 1$. Since $x, y > 0$, $x + y\sqrt{d} > 2$. Thus $0 < x - y\sqrt{d} < 1/2$. This implies $x > y\sqrt{d}$.

$$\left|\frac{x}{y} - \sqrt{d}\right| = \frac{1}{y}|x - y\sqrt{d}| = \frac{1}{y(x + y\sqrt{d})} < \frac{1}{y(2y\sqrt{d})} = \frac{1}{2\sqrt{d}y^2} < \frac{1}{2y^2}.$$

By *Corollary B.2*, x/y must be a convergent.

■

Similarly, for $x^2 - dy^2 = -1$, we have $|y^2 - x^2/d| = 1/d$, which implies $|fracyx - \frac{1}{\sqrt{d}}| < \frac{1}{2x^2}$. Thus y/x is a convergent of $1/\sqrt{d}$. Since $1/\sqrt{d} = [0; a_0, a_1, \dots]$, its convergents correspond to reciprocals of convergents of $\sqrt{d}$.

Periodicity and Fundamental Units

The continued fraction of a quadratic irrational like $\sqrt{d}$ exhibits specific structure.

Theorem B.2. ***Periodic Structure.***
The continued fraction of $\sqrt{d}$ is of the form

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \dots, a_{m-1}, 2a_0}],$$

where $a_1, \dots, a_{m-1}$ is a palindromic sequence (symmetric). The period length is m.

定理

The fundamental unit of $\mathbb{Z}[\sqrt{d}]$ (and the smallest solution to Pell's equation) can be read directly from the convergents at the end of the period.

- Let m be the period length.
- If m is even, the fundamental solution to $x^2 - dy^2 = 1$ is (p_{m-1}, q_{m-1}). The equation $x^2 - dy^2 = -1$ has no solution.
- If m is odd, the fundamental solution to $x^2 - dy^2 = -1$ is (p_{m-1}, q_{m-1}). The fundamental solution to $x^2 - dy^2 = 1$ is (p_{2m-1}, q_{2m-1}).

Example B.3. Examples of Periods.

- $\sqrt{2} = [1;\overline{2}]$. Period $m = 1$ (odd). Convergent $c_0 = 1/1$. $1^2 - 2(1)^2 = -1$. Solution to negative Pell. Solution to positive Pell at $c_{2m-1} = c_1$: $[1;2] = 1 + 1/2 = 3/2$. $3^2 - 2(2)^2 = 1$.
- $\sqrt{3} = [1;\overline{1,2}]$. Period $m = 2$ (even). Solution at c_1: $[1;1] = 2/1$. $2^2 - 3(1)^2 = 1$.
- $\sqrt{13} = [3;\overline{1,1,1,6}]$. Period $m = 5$ (odd). Negative solution at c_4. Convergents: $3,\ 3+1=4,\ 4+3/2\ldots$
  Table:

i	0	1	2	3	4
a_i	3	1	1	1	1
p_i	3	4	7	11	18
q_i	1	1	2	3	5

  Check: $18^2 - 13(5)^2 = 324 - 13(25) = 324 - 325 = -1$. Fundamental unit for positive equation is the square of $18 + 5\sqrt{13}$.

範例

B.5 *Transcendence and Liouville's Theorem*

We close this chapter by observing that while quadratic irrationals have periodic approximations, "too good" approximations imply a number is not algebraic at all.

Theorem B.3. ***Liouville's Theorem.***
Let α be an algebraic number of degree $d \geq 2$. There exists a constant $c(\alpha) > 0$ such that for all rationals p/q:

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^d}.$$

定理

Proof

Let $f(x)$ be the minimal polynomial of α over $\mathbb{Z}$, of degree d. Thus $f(\alpha) = 0$. By the Mean Value Theorem, $f(p/q) - f(\alpha) = f'(\xi)(p/q - \alpha)$ for some ξ between p/q and α. Assume $|alpha - p/q| < 1$ (otherwise the bound holds for small c). Then $|xi| < |\alpha| + 1$. Since f' is a polynomial, $|f'(\xi)|$ is bounded by

some M. Thus $|f(p/q)| < M|p/q - \alpha|$. Note $f(p/q) = \frac{P}{q^d}$ for some integer P. Since f is irreducible and $d \geq 2$, $f(p/q) \neq 0$. Thus $|f(p/q)| \geq 1/q^d$. Therefore, $\frac{1}{q^d} \leq M\left|\alpha - \frac{p}{q}\right|$, implying $\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{Mq^d}$.

■

Example B.4. Liouville Numbers. The number $\alpha = \sum_{n=1}^{\infty} 10^{-n!} = 0.110001\ldots$ is transcendental. Let p_k/q_k be the partial sum up to $n = k$. Then $q_k = 10^{k!}$. The error is roughly $10^{-(k+1)!} = (q_k)^{-(k+1)}$. For any fixed d, for sufficiently large k, the error is smaller than $1/q_k^d$. Thus α cannot be algebraic of degree d.

範例

This result was vastly improved by Roth (1955), who showed that for any algebraic α, the exponent can be reduced to $2 + \epsilon$. This implies that algebraic numbers behave like rationals or quadratic irrationals regarding approximation stability.

Theorem B.4. ***Roth's Theorem.***
If α is algebraic irrational, then for any $\epsilon > 0$, there are only finitely many solutions to

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}.$$

定理

This confirms that the highly approximable numbers constructed by Liouville are indeed exceptional in the landscape of real numbers.

B.6 Exercises

1. **Rational Expansion.** Compute the finite continued fraction expansion for the following rational numbers:
   (a) $187/57$
   (b) $71/31$
   (c) 1.414 (as a fraction $1414/1000$)
2. **Quadratic Irrationals.** Find the periodic continued fraction expansion for:
   (a) $\sqrt{7}$
   (b) $\sqrt{19}$
   (c) $\frac{1+\sqrt{5}}{2}$ (the Golden Ratio)
3. **Convergents and Recurrence.** Calculate the first five convergents $c_0, \ldots, c_4$ for $\sqrt{7}$. Verify that the determinant identity $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$ holds for each step.

4. **Pell's Equation via CF.** Use the continued fraction expansion of $\sqrt{11}$ to find:
   (a) The fundamental unit of $\mathbb{Z}[\sqrt{11}]$.
   (b) The smallest positive integer solution to $x^2 - 11y^2 = 1$.
5. **Legendre's Criterion Application.** Determine whether $355/113$ is a convergent of the continued fraction of $\pi \approx 3.14159265$. (Hint: Check the error $|pi - 355/113|$ against $1/(2 \cdot 113^2)$).
6. **Liouville's Condition.** Prove that the number $\beta = \sum_{n=1}^{\infty} 2^{-3^n}$ is transcendental.
7. **Fibonacci and CF.** Show that the convergents of the Golden Ratio $\phi = [1; 1, 1, \dots]$ are given by the ratio of successive Fibonacci numbers F_{n+1}/F_n.

C
Appendix: Primes in Arithmetic Progressions

A fundamental question in analytic number theory is how prime numbers are distributed modulo n. Specifically, does the arithmetic progression

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

contain infinitely many primes? If $(a,n) = d > 1$, then every term is divisible by d, so the progression contains at most one prime. Thus, a necessary condition is $(a,n) = 1$. Dirichlet's Theorem asserts that this condition is also sufficient.

> **Theorem C.1.** ***Dirichlet's Theorem on Primes in Arithmetic Progressions.***
> If a and n are coprime positive integers, then there are infinitely many primes p such that $p \equiv a \pmod{n}$.
>
> 定理

While the general proof requires complex analysis (specifically, Dirichlet L-functions), elementary methods suffice for specific cases such as $a = 1$ or $a = -1$. We first review some classical results.

C.1 Elementary Cases

We recall the proof of the infinitude of primes, which serves as a template for variations in specific progressions.

> **Theorem C.2.** ***Infinitude of Primes.***
> There are infinitely many primes.
>
> 定理

> *Proof*
>
> See *Theorem 1.5* in Chapter 1 for the classical Euclidean proof. ■

We can adapt this argument to arithmetic progressions by constructing an integer Q such that its prime factors must lie in the desired residue class.

Theorem C.3. ***Primes Congruent to*** $3 \pmod 4$**.**
There are infinitely many primes of the form $4k+3$.

定理

Proof

Suppose there are finitely many such primes $S = \{p_1, \ldots, p_k\}$. Let

$$Q = 4p_1 \ldots p_k - 1.$$

Then $Q \equiv -1 \equiv 3 \pmod 4$. Let $Q = q_1 \ldots q_r$ be the prime factorisation of Q. Since Q is odd, all q_i are odd. If every prime factor $q_i \equiv 1 \pmod 4$, then their product $Q \equiv 1 \pmod 4$, a contradiction. Thus, at least one prime factor q must satisfy $q \equiv 3 \pmod 4$. However, if $q \in S$, then $q \mid (Q+1)$. Since $q \mid Q$, this implies $q \mid 1$, impossible. Thus $q \notin S$, a contradiction.

■

For the case $p \equiv 1 \pmod 4$, we cannot simply use linear forms. We rely on the quadratic character of -1.

Lemma C.1. ***Divisors of*** x^2+1**.**
Let $x \in \mathbb{Z}$. If p is an odd prime divisor of x^2+1, then $p \equiv 1 \pmod 4$.

引理

Proof

Since $p \mid (x^2+1)$, we have $x^2 \equiv -1 \pmod p$. This means -1 is a quadratic residue modulo p. By the First Supplement to the Law of Quadratic Reciprocity (*corollary 6.1*), $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$.

■

Theorem C.4. ***Primes Congruent to*** $1 \pmod 4$**.**
There are infinitely many primes of the form $4k+1$.

定理

Proof

Suppose there are finitely many such primes $S = \{p_1, \ldots, p_k\}$. Let

$$Q = (2p_1 \ldots p_k)^2 + 1.$$

Let q be a prime divisor of Q. Since Q is odd, $q \neq 2$. By *Lemma C.1*, any prime divisor of $x^2 + 1$ must be $1 \pmod 4$. Thus $q \equiv 1 \pmod 4$. Clearly $q \notin S$ because $Q \equiv 1 \pmod{p_i}$ for all i. Thus q is a new prime of the form $4k+1$.

■

C.2 Cyclotomic Polynomials

To generalise the $p \equiv 1 \pmod{n}$ case, we require polynomials whose prime divisors satisfy specific modular properties. The natural candidates are the cyclotomic polynomials $\Phi_n(X)$.

Definition C.1. ***Cyclotomic Polynomial.***
For $n \geq 1$, the n-th cyclotomic polynomial is defined as

$$\Phi_n(X) = \prod_{1 \leq k \leq n \ (k,n)=1} \left(X - e^{2\pi i k/n}\right).$$

Its degree is $\phi(n)$, the Euler totient function.

定義

Lemma C.2. ***Cyclotomic Decomposition.***
For any $n \geq 1$:

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X).$$

Consequently, $\Phi_n(X) \in \mathbb{Z}[X]$.

引理

Proof

The roots of $X^n - 1$ are the n-th roots of unity. Grouping these roots by their multiplicative order d (where $d \mid n$) gives the desired factorisation. Integer coefficients follow by induction and monic long division.

■

Theorem C.5. ***Prime Divisors of*** $\Phi_n(a)$**.**
Let $n \in \mathbb{Z}_{\geq 1}$ and $a \in \mathbb{Z}$. Let p be a prime divisor of $\Phi_n(a)$. If $p \nmid n$, then $p \equiv 1 \pmod{n}$.

定理

Proof

Let $p \mid \Phi_n(a)$. Then $a^n \equiv 1 \pmod{p}$. Let d be the order of a modulo p. Then $d \mid n$. If $d < n$, then p divides $a^d - 1$. Since $a^d - 1 = \prod_{k \mid d} \Phi_k(a)$, p would divide both $\Phi_n(a)$ and some $\Phi_k(a)$ for $k < n$. This would imply a is a multiple root of $X^n - 1 \pmod{p}$. However, $(X^n - 1)' = nX^{n-1} \not\equiv 0 \pmod{p}$ since $p \nmid n$ and $p \nmid a$, so $X^n - 1$ has no multiple roots. Thus $d = n$, and since $d \mid (p-1)$ by Fermat's Little Theorem, $n \mid (p-1)$, or $p \equiv 1 \pmod{n}$.

■

Theorem C.6. ***Primes Congruent to*** $1 \pmod{n}$**.**
For any integer $n > 1$, there are infinitely many primes $p \equiv 1 \pmod{n}$.

定理

Proof

Suppose there are finitely many such primes $\{p_1, \ldots, p_k\}$. Let $M = np_1 \ldots p_k$. Let q be a prime divisor of $\Phi_n(M)$. Since $q \mid \Phi_n(M) \mid (M^n - 1)$, we have $q \nmid M$, so $q \nmid n$ and $q \notin \{p_1, \ldots, p_k\}$. By *Theorem C.5*, $q \equiv 1 \pmod{n}$. Thus q is a new prime in the progression. ■

C.3 *Arithmetic Functions and M"obius Inversion*

The M"obius function and inversion formula, introduced in Chapter 3 exercises, provide the formal tools for evaluating cyclotomic polynomials.

Definition C.2. ***M"obius Function.***
The M"obius function $\mu(n)$ is defined as 1 if $n = 1$, $(-1)^k$ if n is the product of k distinct primes, and 0 if n is not squarefree.

定義

Theorem C.7. ***M"obius Inversion Formula.***
Let f, g be arithmetic functions. Then

$$g(n) = \sum_{d \mid n} f(d) \iff f(n) = \sum_{d \mid n} \mu(d) g(n/d).$$

定理

Example C.1. Cyclotomic Inversion. By applying multiplicative M"obius inversion to $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$, we obtain:

$$\Phi_n(X) = \prod_{d \mid n} (X^{n/d} - 1)^{\mu(d)}.$$

範例

C.4 *Exercises*

1. **Primes modulo 6.** Prove that there are infinitely many primes of the form $6k + 5$.
2. **Primes modulo 3.** Show that there are infinitely many primes of the form $3k + 1$. (Hint: Consider $\Phi_3(X) = X^2 + X + 1$).
3. **Values of Cyclotomic Polynomials.** Calculate $\Phi_n(1)$ for all $n > 1$.
4. **Dirichlet Convolution.** Prove that if f and g are multiplicative functions, then their Dirichlet convolution $f * g$ is also multiplicative.
5. **Average order of ϕ.** Show that $\sum_{n \leq X} \phi(n) = \frac{3}{\pi^2} X^2 + O(X \log X)$.

D
Appendix: Distribution of Prime Numbers

We conclude these notes by exploring the asymptotic distribution of primes, culminating in the Prime Number Theorem (PNT) and the method of the Selberg sieve. Let $\pi(X)$ denote the prime-counting function, defined as the number of primes p such that $p \leq X$.

D.1 Asymptotic Notation and Chebychev's Bounds

To rigorously describe the growth of $\pi(X)$, we recall standard asymptotic notation.

Definition D.1. ***Asymptotic Notation.***
Let $f, g : \mathbb{R} \to \mathbb{R}$ be functions.
- $f(x) \ll g(x)$ (or $f(x) = O(g(x))$) if there exists a constant $C > 0$ such that $|f(x)| \leq C|g(x)|$ for sufficiently large x.
- $f(x) = o(g(x))$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.
- $f(x) \sim g(x)$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

定義

The central result of analytic number theory is the Prime Number Theorem.

Theorem D.1. ***Prime Number Theorem.***

$$\pi(X) \sim \frac{X}{\log X} \quad \text{as } X \to \infty.$$

定理

While the full proof of the PNT requires complex analysis, we can prove weaker bounds using purely elementary methods due to Chebychev.

Theorem D.2. ***Chebychev's Bounds.***
There exist positive constants c_1, c_2 such that for sufficiently large X:

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

定理

Lower Bound.

We analyze the central binomial coefficient $\binom{2n}{n}$. By Legendre's Formula (Chapter 1), the exponent of p in $\binom{2n}{n}$ is $\sum(\lfloor 2n/p^k \rfloor - 2\lfloor n/p^k \rfloor)$. Since $p^v \leq 2n$, and $v \leq 1$ for $p > \sqrt{2n}$, we have

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

Taking logarithms and using the fact that $(2n)^{\sqrt{2n}}$ is small relative to 4^n, we obtain $\pi(2n) \gg n/\log n$.

証明終

Upper Bound.

Using the bound $\prod_{n<p\leq 2n} p \leq \binom{2n}{n} < 4^n$, we have $\sum_{n<p\leq 2n} \log p < n \log 4$. Summing over dyadic intervals yields $\pi(X) \ll X/\log X$.

証明終

D.2 The Brun-Titchmarsh Theorem and Selberg Sieve

The density of primes in short intervals is bounded by the Brun-Titchmarsh theorem.

Theorem D.3. ***Brun-Titchmarsh Theorem.***
For $Y > X^\epsilon$,

$$\pi(X+Y) - \pi(X) \leq \frac{(2+o(1))Y}{\log Y}.$$

定理

The proof using the Selberg sieve involves constructing weights λ_d to minimize a quadratic form $Q = \sum Y/[d_1, d_2]$. The solution yields the bound $2Y/\log Y$, illustrating the "parity problem" where sieve methods often miss the true density by a factor of 2.

D.3 Exercises

1. **Bertrand's Postulate.** Using Chebychev's methods, prove that for any $n > 1$, there exists a prime p such that $n < p < 2n$. (Note: This requires specific values for c_1, c_2).
2. **Sum of Reciprocal Primes.** Prove that $\sum_{p\leq X} \frac{1}{p} = \log\log X + O(1)$.
3. **Logarithmic Integral.** Show that the Prime Number Theorem is equivalent to $\pi(X) \sim \mathrm{Li}(X) = \int_2^X \frac{dt}{\log t}$.
4. **Sieve of Eratosthenes.** Prove that the number of integers $n \leq X$ not divisible by any prime $p \leq \sqrt{X}$ is $O(X/\log X)$.
5. **Mertens' Theorem.** State and prove a weak form of Mertens' product theorem: $\prod_{p\leq X}(1-1/p) \asymp 1/\log X$.