Discrete II: Elementary Number Theory

Gudfit

Contents

0
Divisibility

The set of integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ forms the bedrock of number theory. While the arithmetic operations of addition and multiplication are closed within $\mathbb{Z}$, division is not. The study of number theory is, in many respects, the study of this breakdown: when does one integer divide another, and if it does not, what is the residue?

To answer these questions, we require not just arithmetic intuition but robust proof techniques. We begin by formalising the principle of Mathematical Induction, the primary engine for proving statements over countable sets, before establishing the fundamental algorithm of Euclidean arithmetic.

0.1 *Variants of Mathematical Induction*

The Well-Ordering Principle states that every non-empty set of positive integers contains a least element. This axiom underpins the Principle of Mathematical Induction. While the standard form is likely familiar, number theoretic problems often demand subtler variations.

Standard and Strong Induction

Definition 0.1. ***First Principle of Mathematical Induction.***
Let $P(n)$ be a proposition concerning an integer n. If:

Base Case: $P(a)$ is true for some integer a;

Inductive Step: For any $k \geq a$, the assumption that $P(k)$ is true implies $P(k+1)$ is true;

then $P(n)$ is true for all integers $n \geq a$.

定義

Example 0.1. The Frobenius Coin Problem (Specific Case). We prove that any integer $n \geq 8$ can be expressed as a non-negative

linear combination of 3 and 5. That is, $n = 3a + 5b$ for $a, b \in \mathbb{N}_0$.

範例

Base Case ($n = 8$).

$8 = 3(1) + 5(1)$. The proposition holds.

証明終

Inductive Step.

Assume $k = 3a + 5b$ holds for some $k \geq 8$. We examine $k + 1$.

1. If $b \geq 1$, we can replace one 5 with two 3s (since $6 - 5 = 1$).

$$k+1 = 3a+5(b-1)+5+1 = 3a+5(b-1)+6 = 3(a+2)+5(b-1).$$

2. If $b = 0$, then $k = 3a$. Since $k \geq 8$, $3a \geq 8 \implies a \geq 3$. We replace three 3s with two 5s (since $10 - 9 = 1$).

$$k + 1 = 3(a-3) + 9 + 1 = 3(a-3) + 10 = 3(a-3) + 5(2).$$

証明終

In both cases, $k + 1$ has the required form. By *definition* 0.1, the statement holds for all $n \geq 8$.
Often, knowing $P(k)$ is insufficient to prove $P(k + 1)$; we may need the history of the sequence.

Definition 0.2. ***Second Principle (Strong) of Mathematical Induction.***

Let $P(n)$ be a proposition. If $P(a)$ is true, and the assumption that $P(m)$ *is true for all* $a \leq m \leq k$ implies $P(k+1)$ is true, then $P(n)$ is true for all $n \geq a$.

定義

Example 0.2. A Symmetric Game. Consider two piles of counters, each containing n items. Two players move alternately. A move consists of removing any positive number of counters from a *single* pile. The player who removes the last counter wins. We prove the second player has a winning strategy for all $n \geq 1$.

範例

Let $P(n)$ be the proposition that the second player wins starting with configurations (n, n).

Base Case.

If $n = 1$, Player 1 must take the only counter from one pile. Player 2 takes the counter from the remaining pile and wins.

証明終

Inductive Step.

Assume the second player wins for all initial sizes $1 \leq m \leq k$. Consider a game starting with $(k+1, k+1)$. Player 1 must remove l counters ($1 \leq l \leq k+1$) from one pile, leaving the state $(k+1, k+1-l)$. Player 2 can now mimic this move on the other pile, removing l counters to reach the state $(k+1-l, k+1-l)$. Let $m = k+1-l$. Since $l \geq 1$, we have $0 \leq m \leq k$.

- If $m = 0$, Player 2 has removed the last counter and won immediately.
- If $m > 0$, the game is now in state (m, m) with Player 1 to move. By the inductive hypothesis, the second player wins from this state.

Thus, the second player wins for $n = k+1$.

証明終

Non-Standard Inductive Patterns

Structure in number theory does not always propagate linearly from n to $n+1$.

Theorem 0.1. ***Backward Induction.***
Let $P(n)$ be a proposition. If:

1. There exists an infinite sequence of integers $n_1 < n_2 < \dots$ such that $P(n_i)$ is true for all i;
2. The truth of $P(k+1)$ implies the truth of $P(k)$;

then $P(n)$ is true for all $n \geq n_1$.

定理

Example 0.3. Fermat's Little Theorem (Prime Modulus). Let p be a prime. We prove that $n^p - n$ is divisible by p for all positive integers n.

範例

Infinite Step.

Let $m = lp$. Then $(lp)^p - lp = p(l^p p^{p-1} - l)$, which is clearly a multiple of p. Thus $P(lp)$ is true for all $l = 1, 2, \dots$.

証明終

Backward Step.

Assume $P(k+1)$ is true. That is, $(k+1)^p - (k+1)$ is a multiple of p. Expanding using the Binomial Theorem:

$$(k+1)^p - (k+1) = \left(k^p + \sum_{i=1}^{p-1} \binom{p}{i} k^i + 1\right) - k - 1 = (k^p - k) + \sum_{i=1}^{p-1} \binom{p}{i} k^i.$$

For $1 \leq i \leq p-1$, the binomial coefficient $\binom{p}{i}$ contains the factor p in the numerator which is not cancelled by the denominator. Thus $\binom{p}{i}$ is a multiple of p. The expression becomes $(k^p - k) + p \times (\text{Integer})$. Since the entire sum is a multiple of p (by assumption $P(k+1)$), it follows that $k^p - k$ must be a multiple of p. Thus $P(k)$ is true.

証明終

Theorem 0.2. ***Seesaw Induction.***
Let A_n and B_n be two indexed propositions. If:
1. A_1 is true;
2. $A_n \implies B_n$;
3. $B_n \implies A_{n+1}$;

then both A_n and B_n are true for all $n \geq 1$.

定理

This technique is particularly effective for coupled recurrence relations.

Example 0.4. Counting Solutions. Let $r(m)$ be the number of non-negative integer solutions to $x + 2y = m$. We prove:

$$A_l : r(2l-1) = l \quad \text{and} \quad B_l : r(2l) = l + 1.$$

範例

Base Case (A_1).

Consider $x + 2y = 1$. Since $x, y \geq 0$, the only solution is $(1, 0)$. Thus $r(1) = 1$, so A_1 holds.

証明終

Step $A_k \implies B_k$.

We assume $r(2k-1) = k$. Consider $x + 2y = 2k$.

Case 1: $x = 0$. Then $2y = 2k \implies y = k$. Solution $(0, k)$. (1 solution).

Case 2: $x \geq 1$. Let $x' = x - 1 \geq 0$. The equation becomes $(x' + 1) + 2y = 2k \implies x' + 2y = 2k - 1$. The number of solutions is exactly $r(2k-1)$.

Thus, $r(2k) = 1 + r(2k-1) = 1 + k$. B_k holds.

証明終

Step $B_k \implies A_{k+1}$.

We assume $r(2k) = k + 1$. Consider $x + 2y = 2k + 1$.

Case 1: $x = 0$. Then $2y = 2k + 1$, which has no integer solution.

Case 2: $x \geq 1$. Let $x' = x - 1$. The equation becomes $x' + 2y = 2k$.

The number of solutions is $r(2k)$.

Thus, $r(2k+1) = 0 + r(2k) = k+1$. This is precisely proposition A_{k+1} (since $2(k+1)-1 = 2k+1$).

証明終

By *theorem* 0.2, the formulae hold for all l.

0.2 *Divisibility*

We now apply these structural tools to the integers themselves. Unless otherwise specified, all lowercase letters $a, b, c, \ldots$ denote integers.

Definition 0.3. ***Divisibility.***
Let b be a non-zero integer. We say that b **divides** a, denoted $b \mid a$, if there exists an integer q such that $a = bq$. If $b \mid a$, we call b a **divisor** or **factor** of a, and a a **multiple** of b. If no such integer exists, we write $b \nmid a$.

定義

Remark.

If $b \mid a$ and $1 < |b| < |a|$, b is a proper divisor of a.

Proposition 0.1. ***Linearity and Transitivity.***
Let a, b, c be integers with $c \neq 0$.

1. **Transitivity:** If $c \mid b$ and $b \mid a$, then $c \mid a$.
2. **Linearity:** If $c \mid a$ and $c \mid b$, then $c \mid (ma + nb)$ for any integers m, n.
3. **Cancellation:** $c \mid a \iff mc \mid ma$ for any $m \neq 0$.

命題

Proof

We prove (2). Let $a = ca_1$ and $b = cb_1$ for integers a_1, b_1. Then $ma + nb = m(ca_1) + n(cb_1) = c(ma_1 + nb_1)$. Since $\mathbb{Z}$ is **closed** under multiplication and addition, the term $(ma_1 + nb_1)$ is an integer. Thus $c \mid (ma + nb)$.

■

Remark.

To be "closed under addition and multiplication" means that if you take any two numbers from a set (like the integers) and add or multiply them, the result is always another number that is still inside that same set.

Consecutive Integers

A subtle but powerful property of integers is that in any sequence of consecutive integers, divisibility is guaranteed by the length of the sequence. For a positive integer k, the **factorial** $k!$ denotes the product $k(k-1)\dots 2\cdot 1$.

Theorem 0.3. ***Product of Consecutive Integers.***
The product of any k consecutive integers is divisible by $k!$.

$$k! \mid n(n-1)\dots(n-k+1).$$

定理

Let $P(n,k) = n(n-1)\dots(n-k+1)$.

Positive Integers ($n \geq k$).

We recall the binomial coefficient $\binom{n}{k}$, which counts the number of subsets of size k from a set of size n. By definition, this count must be an integer. Algebraically,

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!} = \frac{P(n,k)}{k!}.$$

Since $\binom{n}{k} \in \mathbb{Z}$, it follows that $k! \mid P(n,k)$.

証明終

Integers containing 0.

If the sequence includes 0, the product is 0. Since $k! \mid 0$ for all k, the statement holds.

証明終

Negative Integers.

If the terms are negative, factor out $(-1)^k$. The divisibility depends only on the magnitude of the product, reducing this to Case 1.

証明終

The Division Algorithm

Though labelled an "algorithm", this is an existence theorem fundamental to Euclidean domains. It connects the abstract concept of divisibility to the concrete geometry of the number line.

Theorem 0.4. ***The Division Algorithm.***
Given integers a and b with $b > 0$, there exist unique integers q (quotient) and r (remainder) such that:

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

定理

Existence.

Consider the set $S = \{a - bx \mid x \in \mathbb{Z} \text{ and } a - bx \geq 0\}$. We must show S is non-empty. If $a \geq 0$, take $x = 0$; then $a \in S$. If $a < 0$, take $x = a$; then $a - ba = a(1 - b)$. Since $b \geq 1, 1 - b \leq 0$, so $a(1 - b) \geq 0$. By the Well-Ordering Principle, S contains a least element; call it r. By definition, $r = a - bq$ for some q, so $a = bq + r$ with $r \geq 0$. We assert $r < b$. Suppose for contradiction that $r \geq b$. Then

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

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

証明終

Uniqueness.

Suppose $a = bq + r = bq' + r'$ with $0 \leq r, r' < b$. Assume without loss of generality $r \geq r'$.

$$b(q - q') = r' - r.$$

Thus $b \mid (r' - r)$. However, since $0 \leq r, r' < b$, the difference satisfies $-b < r' - r < b$. The only multiple of b in the interval $(-b, b)$ is 0. Thus $r' - r = 0 \implies r = r'$, which implies $b(q - q') = 0 \implies q = q'$.

証明終

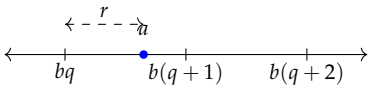


Figure 1: Geometric interpretation of the Division Algorithm. The integer a falls in a unique interval $[bq, b(q + 1))$, determining r.

Example 0.5. Divisibility by 24. Let a be an odd integer. Prove that $24 \mid a(a^2 - 1)$.
Let $a = 2k + 1$ for some integer k. Substituting this into the expression:

$$a(a^2-1) = (2k+1)((2k+1)^2-1) = (2k+1)(4k^2+4k) = 4(2k+1)k(k+1).$$

We rewrite the term $(2k + 1)$ as $[(k - 1) + (k + 2)]$:

$$\begin{aligned} a(a^2 - 1) &= 4[(k - 1) + (k + 2)]k(k + 1) \\ &= 4(k - 1)k(k + 1) + 4k(k + 1)(k + 2). \end{aligned}$$

By *theorem* 0.3, the product of 3 consecutive integers is divisible by $3! = 6$. Thus, $(k - 1)k(k + 1)$ is divisible by 6, and $k(k + 1)(k + 2)$ is divisible by 6. Consequently, the entire expression is divisible by $4 \times 6 = 24$.

範例

Example 0.6. Linear Combination Divisibility. Suppose $m \mid (10a - b)$ and $m \mid (10c - d)$. Prove $m \mid (ad - bc)$.

We construct a specific linear combination to eliminate the coefficient 10:

$$(10a - b)c - (10c - d)a = 10ac - bc - 10ac + ad = ad - bc.$$

Since m divides $(10a - b)$ and m divides $(10c - d)$, by the *linearity* property, m must divide their linear combination. Therefore, $m \mid (ad - bc)$.

範例

Example 0.7. Smallest Linear Combination. Let S be the set of values $ax + by$. Let $d = ax_0 + by_0$ be the smallest positive integer in this set. Prove that $d \mid (ax + by)$.
By *theorem* 0.4, we can write any element $n = ax + by$ as $n = dq + r$ with $0 \leq r < d$. Rearranging for r:

$$r = n - dq = (ax + by) - q(ax_0 + by_0) = a(x - qx_0) + b(y - qy_0).$$

Thus r is also a number of the form $ax + by$. Since d is the smallest positive integer of this form, and $0 \leq r < d$, the only possibility is $r = 0$. Therefore $n = dq$, which implies $d \mid (ax + by)$.

範例

Example 0.8. Harmonic Series. Prove $S = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ is not an integer for $n > 1$.
Let k be the largest integer such that $2^k \leq n$. Let P be the product of all odd positive integers not exceeding n. Consider the number $2^{k-1}PS$. Expanding the sum:

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

The term corresponding to $\frac{1}{2^k}$ becomes:

$$2^{k-1}P \cdot \frac{1}{2^k} = \frac{P}{2}.$$

Since P is a product of odd integers, P is odd, so $\frac{P}{2}$ is not an integer. For any other term $\frac{1}{m}$ in the sum (where $m \neq 2^k$), the denominator m contains at most 2^{k-1} as a factor. Since P contains all odd factors up to n, the term $2^{k-1}P$ cancels the denominator m completely, resulting in an integer. Thus, $2^{k-1}PS = \text{Integer} + \frac{P}{2}$. This sum is not an integer, which implies S cannot be an integer.

範例

Example 0.9. Mersenne Primes and Divisibility. We use algebraic divisibility to restrict primality candidates. Prove that if $2^n - 1$ is prime, then n must be prime.
We use the polynomial factorisation identity:

$$x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \cdots + 1).$$

Let $a = 2^n - 1$. Suppose n is composite, say $n = ab$ with $1 < a, b < n$. Then $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1$. Let $x = 2^a$. Then by the identity above, $(x-1) \mid (x^b - 1)$. Substituting back, $(2^a - 1) \mid (2^{ab} - 1)$. Since $1 < a < n$, we have $1 < 2^a - 1 < 2^n - 1$. Thus $2^n - 1$ has a non-trivial factor $(2^a - 1)$, so it is composite. By contrapositive, if $2^n - 1$ is prime, n cannot have factors a, b, so n is prime.

範例

0.3 *Prime and Composite Numbers*

Following our exploration of divisibility and the integers, we observe that the number 1 possesses a unique structural property: it has exactly one positive divisor. For any integer $n > 1$, the set of divisors includes at least $\{1, n\}$. The classification of integers based on the cardinality of this set is central to number theory.

Definition 0.4. ***Prime and Composite Numbers.***
Let $n > 1$ be a positive integer. If the only positive divisors of n are 1 and n, then n is called a **prime number**. If n has a positive divisor other than 1 and n, then n is called a **composite number**.

定義

Note

The integer 1 is neither prime nor composite.

We denote the set of prime numbers by a sequence $p_1, p_2, \ldots$, where $p_1 = 2, p_2 = 3, p_3 = 5$, and so on. A divisor p of an integer n is called a **prime factor** if p is itself a prime.

Remark.

It should be easy to see why 2 is the only even prime.

The Infinitude of Primes

The fundamental question regarding the distribution of primes was resolved by Euclid.

Theorem 0.5. ***Infinitude of Primes.***
The set of prime numbers is infinite.

定理

Proof

Suppose, for the sake of contradiction, that there are only finitely many prime numbers. Let this complete list be $\{p_1, p_2, \ldots, p_k\}$. Consider the integer N constructed by the product of all primes plus one:

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

Since $N > 1$, N must have at least one prime divisor, say q. If q were in our finite list, then $q = p_i$ for some $1 \leq i \leq k$. Consequently, p_i divides the product $p_1 p_2 \ldots p_k$. By the *linearity of divisibility*, if $p_i \mid N$ and $p_i \mid (p_1 \ldots p_k)$, then p_i must divide their difference:

$$p_i \mid (N - p_1 \ldots p_k) \implies p_i \mid 1.$$

This is impossible, as $p_i \geq 2$. Therefore, the prime divisor q is not in the list $\{p_1, \ldots, p_k\}$. This contradicts the assumption that the list contained all prime numbers.

■

The construction used in *theorem* 0.5 provides a weak but certain bound on the gaps between primes.

Theorem 0.6. ***Existence of Primes in Intervals.***
For any integer $n > 2$, there exists a prime number p such that $n < p < n!$.

定理

Proof

Let $p_1, p_2, \ldots, p_k$ be the list of all primes not exceeding n. Consider the integer $N = p_1 p_2 \ldots p_k + 1$. As shown in the proof of *theorem* 0.5, N has a prime divisor q that is distinct from $p_1, \ldots, p_k$. Since q is not in the list of primes less than or equal to n, it follows that $q > n$. Furthermore, since $p_1, \ldots, p_k$ are distinct integers less than or equal to n, their product is a divisor of $n!$. Specifically:

$$N = p_1 \ldots p_k + 1 \leq n! + 1.$$

The prime divisor q must be less than or equal to N. Thus, we have found a prime q such that $n < q \leq n! + 1$. For $n > 2$, $n!$ is not prime, so we can strengthen the inequality to $q < n!$.

■

While primes never stop appearing, they can become arbitrarily sparse.

Theorem 0.7. ***Arbitrary Gaps Between Primes.***
For any integer $K \geq 1$, there exist K consecutive integers that are all

composite.

定理

Proof

Consider the sequence of K integers starting from $(K+1)!+2$:

$$(K+1)!+2, \quad (K+1)!+3, \quad \ldots, \quad (K+1)!+(K+1).$$

Let $x_i = (K+1)!+i$ for $2 \leq i \leq K+1$. By construction, $i \leq K+1$, so i is one of the factors in $(K+1)!$. Thus $i \mid (K+1)!$. We also know $i \mid i$. By linearity, i divides the sum $(K+1)!+i$. Since $2 \leq i \leq K+1$, the number x_i has a divisor i such that $1 < i \leq x_i$. To confirm i is a proper divisor, we note $x_i = (K+1)!+i > i$. Thus, each term in the sequence is composite.

■

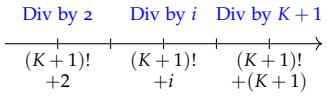


Figure 2: Construction of K consecutive composite integers using factorials.

Primes in Arithmetic Progressions

Euclid's method can be adapted to prove the infinitude of primes in certain arithmetic progressions.

Proposition 0.2. ***Primes of the Form*** $4n+3$**.**
There are infinitely many prime numbers of the form $4n+3$.

命題

Proof

Assume there are finitely many such primes, denoted $\{p_1, p_2, \ldots, p_k\}$. Construct the integer $N = 4p_1p_2\ldots p_k - 1$. This can be written as $N = 4(p_1p_2\ldots p_k - 1) + 3$, so N is of the form $4k + 3$. Consider the prime factorisation of N. The number N is odd, so 2 is not a factor. Any odd prime is either of the form $4m+1$ or $4m + 3$. The product of two numbers of the form $4m + 1$ is also of that form:

$$(4a+1)(4b+1) = 16ab + 4a + 4b + 1 = 4(4ab + a + b) + 1.$$

If all prime factors of N were of the form $4m + 1$, their product N would also be of the form $4m + 1$. But N is of the form $4k + 3$. Therefore, N must have at least one prime factor q of the form $4m + 3$. If q were in our list $\{p_1, \ldots, p_k\}$, then $q \mid (4p_1 \ldots p_k)$. Since $q \mid N$, it would divide their difference $4p_1 \ldots p_k - N = 1$, which is impossible. Hence, q is a new prime of the form $4n + 3$, a contradiction.

■

We now examine specific constraints on prime constellations.

Example 0.10. Primes in a Short Sequence. Find all primes p such that p, $p+10$, and $p+14$ are all prime.
We analyse the forms of primes with respect to division by 3. By the *theorem* 0.4, any integer p can be written as $3k$, $3k+1$, or $3k+2$.

1. If $p = 3$, then $p+10 = 13$ and $p+14 = 17$. All three are prime, so $p = 3$ is a solution.
2. If p is of the form $3k+1$ for $k \geq 1$ (since $p > 3$), then $p+14 = (3k+1)+14 = 3k+15 = 3(k+5)$. Since $k \geq 1$, $k+5 \geq 6$, so $p+14$ is a multiple of 3 greater than 3, and thus composite.
3. If p is of the form $3k+2$ for $k \geq 1$, then $p+10 = (3k+2)+10 = 3k+12 = 3(k+4)$. Since $k \geq 1$, $k+4 \geq 5$, so $p+10$ is a composite multiple of 3.

The only prime not of the form $3k+1$ or $3k+2$ (for $k \geq 1$) is $p = 3$ itself. Thus, $p = 3$ is the unique solution.

範例

Proposition 0.3. ***Square of a Prime and Division by 12.***
Let p be a prime greater than 3. The remainder when p^2 is divided by 12 is 1.

命題

Proof

Any prime $p > 3$ is not divisible by 2 or 3. By *theorem* 0.4, any integer can be written in the form $6k, 6k+1, 6k+2, 6k+3, 6k+4, 6k+5$. Since p is prime and $p > 3$:

- p cannot be $6k$, $6k+2$, $6k+4$ (divisible by 2).
- p cannot be $6k+3$ (divisible by 3).

Thus p must be of the form $6k+1$ or $6k+5$. Note that $6k+5$ can be written as $6(k+1)-1$. So any prime $p > 3$ is of the form $6k \pm 1$ for some integer $k \geq 1$. We square this expression:

$$p^2 = (6k \pm 1)^2 = 36k^2 \pm 12k + 1 = 12(3k^2 \pm k) + 1.$$

Let $q = 3k^2 \pm k$. This is an integer, so $p^2 = 12q + 1$. By the uniqueness part of the Division Algorithm, the remainder when p^2 is divided by 12 is 1.

■

Example 0.11. Divisibility of the Difference of Prime Squares. Let $p \geq q \geq 5$ be prime numbers. Prove that $24 \mid (p^2 - q^2)$.
Let $X = p^2 - q^2$. First, we show that $3 \mid X$. Since $p, q \geq 5$, neither is divisible by 3. As shown in the preceding proposition, the square of such a prime leaves a remainder of 1 when divided by 3.

So $p^2 = 3k_1 + 1$ and $q^2 = 3k_2 + 1$ for some integers k_1, k_2. Then $X = (3k_1 + 1) - (3k_2 + 1) = 3(k_1 - k_2)$, so $3 \mid X$.
Next, we show that $8 \mid X$. Any prime $p \geq 5$ is odd. Let $p = 2m + 1$. Then $p^2 - 1 = (2m + 1)^2 - 1 = (4m^2 + 4m + 1) - 1 = 4m(m + 1)$. The product of two consecutive integers $m(m + 1)$ is always even, so $m(m + 1) = 2n$ for some integer n. Thus, $p^2 - 1 = 4(2n) = 8n$, which means $8 \mid (p^2 - 1)$. Similarly, since q is an odd prime, $8 \mid (q^2 - 1)$. By linearity, $8 \mid ((p^2 - 1) - (q^2 - 1))$, which simplifies to $8 \mid (p^2 - q^2)$.
So we have established $3 \mid X$ and $8 \mid X$. Since $8 \mid X$, we can write $X = 8k$ for some integer k. Now, since $3 \mid X$, we have $3 \mid 8k$. As 3 is a prime number and does not divide 8, it must divide k. So $k = 3j$ for some integer j. Substituting this back, we get $X = 8(3j) = 24j$. Therefore, $24 \mid (p^2 - q^2)$.

範例

0.4 *Special Types of Primes*

Historically, mathematicians sought a "magic formula" — a function $f(n)$ that produces a prime number for every integer input n. Euler identified several quadratic polynomials with remarkable properties. For instance, the polynomial

$$f(n) = n^2 + n + 41$$

yields prime numbers for every integer $0 \leq n \leq 39$. Similarly, $n^2 + n + 17$ produces primes for $0 \leq n \leq 15$. Despite these successes over finite intervals, the search for a polynomial that generates *only* primes over the integers is futile.

Theorem 0.8. ***Non-existence of Prime-Generating Polynomials.*** Let $f(n) = c_k n^k + \cdots + c_1 n + c_0$ be a polynomial with integer coefficients and degree $k \geq 1$. There is no such function where $f(n)$ is prime for all positive integers n.

定理

Proof

Assume the contrary: that $f(n)$ takes only prime values for all $n \geq 1$. Fix a specific input n_0 and let $p = f(n_0)$. By assumption, p is a prime number. Consider the evaluation of the function at $n_0 + tp$, where t is any integer. The polynomial term $c_j(n_0 + tp)^j$ can be expanded using the binomial theorem:

$$c_j(n_0 + tp)^j = c_j \left(n_0^j + \text{terms containing a factor of } p \right).$$

Summing over all terms $j = 0$ to k:

$$f(n_0 + tp) = \sum_{j=0}^{k} c_j n_0^j + p \cdot (\text{Integer}) = f(n_0) + p \cdot (\text{Integer}).$$

Since $f(n_0) = p$, we can factor out p:

$$f(n_0 + tp) = p(1 + \text{Integer}).$$

Thus, for any integer t, $f(n_0 + tp)$ is divisible by p. Since f is a non-constant polynomial, $|f(n)|$ tends to infinity as n increases. We can choose t large enough such that $|f(n_0 + tp)| > p$. Consequently, $f(n_0 + tp)$ is a number divisible by p but strictly greater than p, which implies it is composite. This contradicts the assumption that $f(n)$ generates only primes.

■

Having established that no simple polynomial captures the primes, we turn to specific forms of integers that have historically been candidates for primality.

Fermat Primes

Fermat studied numbers of the form $2^m + 1$. He observed that for such a number to be prime, the exponent m must possess a specific structure.

Proposition 0.4. ***Condition for*** $2^m + 1$ ***to be Prime.***
Let $m \geq 1$. If $2^m + 1$ is a prime number, then m must be a power of 2. That is, $m = 2^n$ for some integer $n \geq 0$.

命題

Proof

Suppose m has an odd divisor $k > 1$. Let $m = k \cdot l$. We use the algebraic identity for the sum of odd powers:

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

Substituting $x = 2^l$:

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

Since $k > 1$, the factor $2^l + 1$ satisfies $1 < 2^l + 1 < 2^m + 1$. Thus $2^m + 1$ is composite. By contrapositive, if $2^m + 1$ is prime, m cannot have any odd divisor greater than 1. Therefore, m must be a power of 2.

■

Definition 0.5. ***Fermat Numbers.***
Integers of the form $F_n = 2^{2^n} + 1$ for $n \geq 0$ are called **Fermat numbers**. If F_n is prime, it is called a **Fermat prime**.

定義

The first five Fermat numbers are prime:

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

Fermat conjectured that all F_n are prime. This stood until 1732, when Euler disproved it by factoring F_5.

Example 0.12. Euler's Factorisation of F_5. We prove that $F_5 = 2^{32} + 1$ is composite by showing it is divisible by 641.
Let $a = 2^7 = 128$ and $b = 5$. We observe two algebraic relationships:

(i) $a - b^3 = 128 - 125 = 3$.

(ii) $1 + ab - b^4 = 1 + 640 - 625 = 1 + 15 = 16 = 2^4$.

We wish to check divisibility by $641 = 1 + ab$. Express F_5 in terms of a and b:

$$F_5 = 2^{32} + 1 = 2^{28} \cdot 2^4 + 1 = (2^7)^4 \cdot 2^4 + 1 = a^4 2^4 + 1.$$

Substitute $2^4 = 1 + ab - b^4$:

$$\begin{aligned} F_5 &= a^4(1 + ab - b^4) + 1 \\ &= a^4 + a^5 b - a^4 b^4 + 1 \\ &= a^4 + a^5 b - (ab)^4 + 1 \\ &= 1 + a^4 + ab(a^4 - a^3 b^3) \\ &= 1 + a^4 + ab(a^4 - (ab)^3). \end{aligned}$$

This direct expansion is cumbersome. Instead, use the relation $1 + ab \mid (1 - (ab)^2)$ and simpler grouping. From $2^4 = 1 + ab - b^4$, we write:

$$F_5 = a^4(1 + ab - b^4) + 1 = (1 + ab)a^4 - (ab)^4 + 1.$$

Note that $1 - (ab)^4$ is a difference of squares: $(1 - (ab)^2)(1 + (ab)^2)$. Since $(1 + ab)$ divides $(1 - (ab)^2)$, it divides $1 - (ab)^4$. Thus $(1 + ab)$ divides both terms on the right hand side. Therefore, $641 \mid F_5$.

範例

Despite the failure of primality, Fermat numbers possess a property that provides an alternative proof for the infinitude of primes.

Theorem 0.9. ***Coprimality of Fermat Numbers.***
For distinct non-negative integers n and m, the Fermat numbers F_n and F_m are coprime. That is, if d divides both F_n and F_m, then $d = 1$.

定理

Proof

We establish the recurrence relation:

$$F_n - 2 = F_0 F_1 F_2 \dots F_{n-1}.$$

We proceed by induction. For $n = 1$, $F_1 - 2 = 5 - 2 = 3 = F_0$. Assume the product holds for k. Consider $F_{k+1} - 2$:

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

Since $2^{2^k} + 1 = F_k$, and by hypothesis $2^{2^k} - 1 = F_k - 2 = \prod_{i=0}^{k-1} F_i$, we have:

$$F_{k+1} - 2 = \left(\prod_{i=0}^{k-1} F_i \right) F_k = \prod_{i=0}^{k} F_i.$$

Now, let $m > n$ and let d be a common divisor of F_m and F_n. From the recurrence, $F_m - 2 = F_n \cdot (\text{product of other Fermat numbers})$. Since $d \mid F_n$, it follows that $d \mid (F_m - 2)$. We are given $d \mid F_m$. By linearity, d must divide the difference:

$$d \mid F_m - (F_m - 2) \implies d \mid 2.$$

The divisors of 2 are 1 and 2. However, all Fermat numbers are odd. Thus $d \neq 2$. Therefore, $d = 1$.

■

Remark.

Since each F_n is coprime to all others, each F_n must introduce at least one new prime factor into the set of all primes. This implies there are infinitely many primes.

Mersenne Primes

Another form of interest involves powers of 2 minus one.

Definition 0.6. ***Mersenne Numbers.***
Integers of the form $M_n = 2^n - 1$ for $n \geq 1$ are called **Mersenne numbers**. If M_n is prime, it is called a **Mersenne prime**.

定義

Just as with Fermat numbers, the exponent of a Mersenne prime is restricted.

Proposition 0.5. ***Necessary Condition for Mersenne Primes.***
Let $n > 1$. If $a^n - 1$ is prime, then $a = 2$ and n is prime.

命題

Suppose $a > 2$.

We have the factorisation $a^n - 1 = (a-1)(a^{n-1} + \cdots + 1)$. Since $a > 2$, $a - 1 > 1$. Also $n > 1$ implies the second factor is greater than 1. Thus $a^n - 1$ is composite. So we must have $a = 2$.

証明終

Suppose n is composite.

Let $n = kl$ with $1 < k < n$. Then $2^n - 1 = (2^k)^l - 1$. Using the identity $x^l - 1 = (x-1)(x^{l-1} + \cdots + 1)$ with $x = 2^k$: $2^k - 1$ divides $2^n - 1$. Since $1 < k < n$, we have $1 < 2^k - 1 < 2^n - 1$. Thus $2^n - 1$ has a non-trivial factor. Therefore, if M_n is prime, n must be prime.

証明終

Remark.

The condition is necessary but not sufficient. For example, $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$.

Example 0.13. A Composite Sequence. Let the sequence $\{g(n)\}$ satisfy $g(1) = 1$ and $g(n+1) = g(n)^2 + 4g(n) + 2$. Prove that if n is even, $g(n)$ is composite (except for $g(2) = 7$).
Let $h(n) = g(n) + 2$. Substituting into the recurrence:

$$h(n+1) = g(n+1) + 2 = g(n)^2 + 4g(n) + 4 = (g(n) + 2)^2 = h(n)^2.$$

With $h(1) = g(1) + 2 = 3$, we have the closed form $h(n) = 3^{2^{n-1}}$. Thus $g(n) = 3^{2^{n-1}} - 2$.
When $n = 2$, $g(2) = 3^2 - 2 = 7$, which is prime. When $n > 2$ and n is even, we show that $g(n)$ is divisible by 7. We can rewrite $g(n)$ by introducing a -9 and $+7$ to factor the expression:

$$g(n) = 3^{2^{n-1}} - 9 + 7 = 3^2(3^{2^{n-1}-2} - 1) + 7.$$

Consider the exponent $E = 2^{n-1} - 2$. Factoring out 2, we get $E = 2(2^{n-2} - 1)$. Since n is even, let $n - 2 = 2k$. Then $2^{n-2} - 1 = 2^{2k} - 1 = 4^k - 1$. Using the identity $x - 1 \mid x^k - 1$, we know that $4 - 1 \mid 4^k - 1$, so $3 \mid (2^{n-2} - 1)$. This implies that $6 \mid 2(2^{n-2} - 1)$, so the exponent E is a multiple of 6. We can therefore write $3^E - 1$ as $3^{6m} - 1$ for some integer m. Using the factorisation $x^m - 1 = (x-1)(x^{m-1} + \cdots + 1)$ with $x = 3^6$:

$$(3^6 - 1) \mid (3^{6m} - 1).$$

We calculate $3^6 - 1 = 729 - 1 = 728$. Since $728 = 7 \times 104$, $7 \mid (3^6 - 1)$. By transitivity, $7 \mid (3^E - 1)$. Substituting this back into the expression for $g(n)$:

$$g(n) = 9(3^E - 1) + 7.$$

> Since 7 divides both terms on the right hand side, $7 \mid g(n)$. For $n > 2$, $g(n) > 7$, so $g(n)$ is composite.
>
> 範例

0.5 *Exercises*

1. **Induction on Exponents.** For any positive integer $n \geq 3$, prove that there always exist odd integers x and y such that
$$2^n = 7x^2 + y^2.$$

2. **The Binet Formula.** The Fibonacci sequence $\{f_n\}$ is defined by $f_1 = 1$, $f_2 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$. Prove via induction that:
$$f_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].$$

3. **Summation of Structured Sequences.** Let $\{a_n\}$ be a sequence where $a_{2k} = 3k^2$ and $a_{2k-1} = 3k(k-1) + 1$ for positive integers k. Let S_n denote the sum of the first n terms. Prove that:
$$S_{2l-1} = \frac{1}{2} l(4l^2 - 3l + 1) \quad \text{and} \quad S_{2l} = \frac{1}{2} l(4l^2 + 3l + 1).$$

4. **Cantor's Pairing Function.** Prove that the function $f(m,n) = m + \frac{1}{2}(m+n-2)(m+n-1)$ is a bijection from $\mathbb{Z}^+ \times \mathbb{Z}^+$ to $\mathbb{Z}^+$. That is, as m and n range over all positive integers, the value $f(m,n)$ takes every positive integer value exactly once.

5. **Linear Combination Divisibility.** Given integers m, n, p, q such that $(m-p) \mid (mn+pq)$, prove that $(m-p) \mid (mq+np)$.

6. **Polynomial Integer Values.** Prove that for any integer n, the polynomial $f(n) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$ always evaluates to an integer.

7. **Divisibility by Square Factors.** Let $n \neq 1$ be an integer. Prove that $(n-1)^2 \mid (n^k - 1)$ if and only if $(n-1) \mid k$.

8. **Divisibility by 16.** Let n be an odd integer. Prove that $16 \mid (n^4 + 4n^2 + 11)$.

9. **Inductive Divisibility.** Let n be a positive integer. Use mathematical induction to prove that
$$11 \mid (3^{n+1} + 3^{n-1} + 6^{8(n-1)}).$$

10. **System of Divisors.** Find three positive integers greater than 1 such that the product of any two, plus 1, is divisible by the third.

11. **Modular Arithmetic with Powers.** Let n be an odd number. Prove that the last two digits of $2^{2^n}(2^{2n+1}-1)$ are 28.

12. **Propagating Divisibility.** Let l be a fixed positive integer. Suppose d is an integer such that $d \mid (a+b+c)$, $d \mid (a^l - b^l)$, and $d \mid (b^l - 1)$. Prove that for any positive integer n,
$$d \mid (a^{n+1} + b^{n+1} + c).$$

13. **Sum and Difference Divisibility.** Let a, b be integers not divisible by 3. Prove that exactly one of $a+b$ or $a-b$ is divisible by 3.

14. **Harmonic Sums.** Prove that the sum $S = \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n+1}$ for $n \geq 1$ is never an integer.

15. **Triangular Decomposition.** Let n be a positive integer. Prove that there exists a unique pair of integers k, l such that $n = \frac{k(k-1)}{2} + l$, where $0 \leq l < k$.

16. **Base-k Representation.** Let $k \geq 2$ be an integer. Prove that any positive integer a can be uniquely expressed in the form
$$a = b_n k^n + b_{n-1}k^{n-1} + \cdots + b_1 k + b_0,$$
where $0 < b_n < k$ and $0 \leq b_i < k$ for $i = 0, \ldots, n-1$.

17. **Sophie Germain Primes.** Let $p > 5$ be a prime. If $2p+1$ is also prime, prove that $4p+1$ must be composite.

18. **Simultaneous Primes.** Determine all primes p such that $p^2 - 2$, $2p^2 - 1$, and $3p^2 + 4$ are all prime numbers.

19. **Primes in Arithmetic Progression.** Prove that there are infinitely many primes of the form $6n+5$.

20. **Decomposition into Consecutive Sums.** Let $n \geq 3$ be an odd number. Prove that n is prime if and only if n cannot be expressed as the sum of three or more consecutive positive integers.

21. **Wilson's Theorem Converse Variant.** Let $m > 1$ be a positive integer. Prove that $m \mid (m-1)!$ if and only if m is a composite number greater than 4. (Note: Text exercise specified > 5, but $4 \nmid 3! = 6$. Check boundary cases carefully).

22. **Composite Polynomials.** Prove that for any integer $n \geq 1$, the number $n^4 + 4^n$ is composite. (Hint: Consider the cases n even and n odd separately; use the Sophie Germain Identity for odd n).

23. **Composite Neighbours.**
    (a) De Bouelles asserted that for all $n \geq 1$, at least one of $6n-1$ and $6n+1$ is prime. Find a counterexample.
    (b) Prove that there are infinitely many n such that $6n-1$ and $6n+1$ are both composite.

24. Distinct Prime Divisors. Let $n > 2$. Prove that for the sequence of $n-1$ consecutive integers

$$n!+2, n!+3, \ldots, n!+n,$$

each term has a prime divisor that does not divide any of the other $n-2$ terms.

25. Square Divisibility of Factorials. Find all odd numbers n such that $n^2 \mid (n-1)!$.

26. Growth of Primes. Let $p_1 = 2, p_2 = 3, \ldots$ be the sequence of primes in increasing order. Prove that $p_n \leq 2^{2^{n-1}}$.

27. Arithmetic Progressions of Primes. Find 6 primes less than 160 that form an arithmetic progression. Then, prove that there cannot be 7 primes all less than 200 forming an arithmetic progression.

28. Infinite Product Inequality. Let N be a positive integer, and $p_1, \ldots, p_n$ be all primes not exceeding N. Prove:

$$\prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right)^{-1} > \sum_{i=1}^{N} \frac{1}{i}.$$

Use the divergence of the harmonic series to deduce that there are infinitely many primes.

29. Fermat Primes Structure. Let m be a positive integer such that $2^m + 1$ is prime. Prove that m must be a power of 2.

30. Euclid-Mullin Sequence Properties. Let $A_1 = 2$ and $A_{n+1} = A_n^2 - A_n + 1$ for $n \geq 1$.

(a) Prove that $A_{n+1} = A_1 A_2 \cdots A_n + 1$.

(b) Prove that if $m \neq n$ and $d > 1$ divides A_n, then $d \nmid A_m$.

(c) Use this mutual coprimality to provide an alternative proof that there are infinitely many primes.

1
Greatest Common Divisor

While divisibility defines a relationship between two integers, the study of number theory often requires comparing the multiplicative structures of multiple integers simultaneously. The central concept in this comparison is the greatest common divisor.
We generalise the concept of a common divisor to sets of integers.

Definition 1.1. ***Greatest Common Divisor.***
Let $a_1, a_2, \ldots, a_n$ be integers, not all zero. An integer d is a **common divisor** of the set if $d \mid a_i$ for all $i = 1, \ldots, n$. The **greatest common divisor** (GCD), denoted $(a_1, a_2, \ldots, a_n)$, is the largest such integer.

定義

Definition 1.2. ***Coprimality.***
The integers $a_1, a_2, \ldots, a_n$ are **coprime** (or relatively prime) if their greatest common divisor is 1. They are **pairwise coprime** if $(a_i, a_j) = 1$ for all $1 \leq i < j \leq n$.

定義

Note

The set $\{6, 10, 15\}$ is coprime because no integer greater than 1 divides all three, but it is not pairwise coprime since $(6, 10) = 2$.

Since divisibility is defined by integer multiples, the sign of an integer does not influence its divisors.

Proposition 1.1. ***Absolute Value Invariance.***
Let $a_1, \ldots, a_n$ be integers, not all zero. Then:

$$(a_1, a_2, \ldots, a_n) = (|a_1|, |a_2|, \ldots, |a_n|).$$

命題

Proof

Let d be a common divisor of $a_1, \ldots, a_n$. Since $d \mid a_i$, it follows that $d \mid |a_i|$. Thus d is a common divisor of the absolute values. Con-

versely, if $d \mid |a_i|$, then $d \mid a_i$. Since the sets of common divisors are identical, their maximum elements must be identical.

■

Proposition 1.2. ***Zero Element.***
For any non-zero integer b, $(0, b) = |b|$.

命題

Proof

Since $b \mid 0$ (as $0 = b \cdot 0$) and $b \mid b$, $|b|$ is a common divisor. No divisor of b can exceed $|b|$, so $|b|$ is the greatest common divisor.

■

These properties allow us to restrict our attention to positive integers without loss of generality.

1.1 The Euclidean Algorithm

The calculation of the GCD does not require factorisation. Instead, it relies on the repeated application of the Division Algorithm (*theorem* 0.4). We first establish a reduction lemma, known historically from Euclid's *Elements* (Book VII, Proposition 2).

Theorem 1.1. ***Euclidean Reduction.***
If $a = bk + c$ for integers a, b, c, k, then $(a, b) = (b, c)$.

定理

Proof

Let $d = (a, b)$. Since $d \mid a$ and $d \mid b$, by linearity, $d \mid (a - bk)$, which implies $d \mid c$. Thus d is a common divisor of b and c, so $d \leq (b, c)$. Conversely, let $e = (b, c)$. Since $e \mid b$ and $e \mid c$, linearity implies $e \mid (bk + c)$, so $e \mid a$. Thus e is a common divisor of a and b, so $e \leq (a, b)$. Therefore, $(a, b) = (b, c)$.

■

This theorem transforms the problem of finding (a, b) into finding the GCD of smaller numbers (b, r), where r is the remainder when a is divided by b. Iterating this process yields the Euclidean Algorithm.

Theorem 1.2. ***The Euclidean Algorithm.***
Let a and b be positive integers. By repeated application of the Division Algorithm:

$$
\begin{aligned}
a &= bq_1 + r_1, & 0 < r_1 < b \\
b &= r_1 q_2 + r_2, & 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, & 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1} + 0.
\end{aligned}
$$

The last non-zero remainder r_n is the greatest common divisor of a and b.

定理

Proof

Applying *theorem 1.1* sequentially:

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n, 0).$$

By the Zero Element property, $(r_n, 0) = r_n$.

■

Corollary 1.1. *Divisibility of Common Divisors.* Every common divisor of a and b divides (a, b).

推論

Proof

Let d be a common divisor. In the algorithm above, $d \mid a$ and $d \mid b \implies d \mid r_1$. Since $d \mid b$ and $d \mid r_1$, $d \mid r_2$. Inductively, d divides every remainder, including $r_n = (a, b)$.

■

Example 1.1. Calculation of GCD. We find $(6731, 2809)$.

$$
\begin{aligned}
6731 &= 2809 \times 2 + 1113 \\
2809 &= 1113 \times 2 + 583 \\
1113 &= 583 \times 1 + 530 \\
583 &= 530 \times 1 + 53 \\
530 &= 53 \times 10 + 0
\end{aligned}
$$

The last non-zero remainder is 53. Thus $(6731, 2809) = 53$.

範例

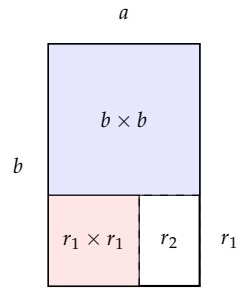


Figure 1.1: Geometric visualisation of the Euclidean Algorithm. We decompose a rectangle of size $a \times b$ into squares of size b, then squares of size r_1, and so on.

Structural Properties

The GCD behaves linearly with respect to multiplication and is invariant under linear shifts.

Proposition 1.3. ***Homogeneity and Division.***
Let a, b be integers and k be a positive integer. Let $(a, b) = d$.
1. $(ka, kb) = k(a, b) = kd$.
2. $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

命题

Proof

For (2), let $d' = (a/d, b/d)$. Then $d' \mid (a/d)$ and $d' \mid (b/d)$, so $dd' \mid a$ and $dd' \mid b$. Thus dd' is a common divisor of a and b. By definition, $dd' \leq (a, b) = d$, which implies $d' = 1$. For (1), let $g = (ka, kb)$. Since $k \mid ka$ and $k \mid kb$, *corollary* 1.1 gives $k \mid g$, so write $g = kg_1$. Because $g \mid ka$ and $g \mid kb$, we have $g_1 \mid a$ and $g_1 \mid b$, so $g_1 \leq (a, b) = d$. Hence $g \leq kd$. Conversely, kd divides both ka and kb, so $kd \leq g$. Therefore $g = kd$.

■

Theorem 1.3. ***Invariance under Linear Combination.***
For any integer k, $(a, b) = (a, b + ka)$.

定理

Proof

If $d \mid a$ and $d \mid b$, then $d \mid (b + ka)$. Thus every common divisor of a, b is a common divisor of $a, b + ka$. Conversely, if $d \mid a$ and $d \mid (b + ka)$, then $d \mid (b + ka - ka) = b$. Hence the sets of common divisors coincide, so the GCDs are equal.

■

We can apply these structural theorems to prove properties of number-theoretic sequences.

Example 1.2. Factorials and Shifted Indices. Find $(n! + 1, (n + 1)! + 1)$.
Using *theorem* 1.3 with $a = n! + 1$ and $b = (n + 1)! + 1$:
Note that

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

Thus,

$$((n + 1)! + 1, n! + 1) = (-n, n! + 1) = (n, n! + 1).$$

Since n divides $n!$, any common divisor of n and $n! + 1$ must divide 1. Therefore, the GCD is 1.

範例

Example 1.3. GCD of Linear Forms. Calculate $(30n + 2, 12n + 1)$ for any integer n.

We use the Euclidean reduction repeatedly:

$$\begin{aligned}(30n+2, 12n+1) &= (30n+2-2(12n+1), 12n+1)\\ &= (6n, 12n+1)\\ &= (6n, 12n+1-2(6n))\\ &= (6n, 1).\end{aligned}$$

Thus, the GCD is 1 for all n.

範例

GCD of Multiple Integers

The definition of the GCD extends recursively to multiple integers.

Theorem 1.4. ***Associativity of GCD.***
For integers $a_1, \ldots, a_n$:

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2), a_3, \ldots, a_n).$$

定理

Proof

Let $d = (a_1, \ldots, a_n)$ and $g = ((a_1, a_2), a_3, \ldots, a_n)$. If k divides all a_i, then $k \mid (a_1, a_2)$. Thus k divides (a_1, a_2) and $a_3, \ldots, a_n$, so $k \mid g$. Hence $d \mid g$. Conversely, if $k \mid g$, then $k \mid (a_1, a_2)$ and $k \mid a_i$ for $i \geq 3$. Since $k \mid (a_1, a_2)$, $k \mid a_1$ and $k \mid a_2$. Thus k divides all a_i, so $g \mid d$. Therefore $d = g$.

■

Corollary 1.2. *Distributive Property of GCD.*

$$(a_1, \ldots, a_n)(b_1, \ldots, b_m) = (a_1 b_1, \ldots, a_i b_j, \ldots, a_n b_m).$$

In particular, $(a, b)(c, d) = (ac, ad, bc, bd)$.

推論

Proof

Consider the case $n = 2, m = 2$. Let $d = (a_1, a_2)$ and $e = (b_1, b_2)$. By *proposition* 1.3, $(a_1 e, a_2 e) = e(a_1, a_2) = de$. Since $e = (b_1, b_2)$, homogeneity also gives

$$(a_1 e, a_2 e) = ((a_1 b_1, a_1 b_2), (a_2 b_1, a_2 b_2)).$$

By *theorem* 1.4, this equals $(a_1 b_1, a_1 b_2, a_2 b_1, a_2 b_2)$. The general case follows by induction.

■

Example 1.4. Algebraic Verification. We verify that $(a,b)^2 = (a^2, ab, b^2)$.
Using *corollary* 1.2:

$$(a,b)(a,b) = (a\cdot a, a\cdot b, b\cdot a, b\cdot b) = (a^2, ab, ab, b^2).$$

Since the set of numbers is $\{a^2, ab, b^2\}$, the GCD is (a^2, ab, b^2).

範例

Application to Special Numbers

The Euclidean Algorithm allows us to compute the GCD of numbers defined by exponents without expanding the terms.

Example 1.5. Fermat-style GCD. Let $m > n \geq 0$. We calculate $(a^{2^m}+1, a^{2^n}+1)$.
Let $m = n + r$ with $r \geq 1$. Let $x = a^{2^n}$. Then $a^{2^m} - 1 = x^{2^r} - 1$. Since $x^{2^r} - 1 = (x-1)(x+1)(x^2+1)\cdots(x^{2^{r-1}}+1)$, we have $x+1 \mid x^{2^r} - 1$. Thus $a^{2^m} - 1 = (a^{2^n}+1)M$ for some integer M.
We can explicitly write:

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

Since $(a^{2^n}+1)$ divides $(a^{2^m}-1)$, we can apply *theorem* 1.1:

$$(a^{2^m}+1, a^{2^n}+1) = (a^{2^m} - 1 + 2, a^{2^n}+1) = (2, a^{2^n}+1).$$

Thus, the GCD is 1 if a is even, and 2 if a is odd.

範例

Theorem 1.5. ***GCD of Mersenne Numbers.***
For positive integers m, n:

$$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1.$$

定理

Proof

Assume without loss of generality $m > n$. By *theorem* 0.4, we write $m = nq + r$ where $0 \leq r < n$. We decompose the term $2^m - 1$ as follows:

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

We recall that $x - 1$ divides $x^q - 1$. Letting $x = 2^n$, we see that $2^n - 1$ divides $(2^n)^q - 1 = 2^{nq} - 1$. Thus, there exists an integer k such that $2^{nq} - 1 = k(2^n - 1)$. Substituting this back into our expression:

$$2^m - 1 = 2^r \cdot k(2^n - 1) + (2^r - 1).$$

This is a linear combination of the form $A = BQ + R$, where $A = 2^m - 1$, $B = 2^n - 1$, and $R = 2^r - 1$. By *theorem* 1.1, the GCD satisfies:

$$(2^m - 1, 2^n - 1) = (2^n - 1, 2^r - 1).$$

This step exactly mirrors the first step of the Euclidean Algorithm applied to the exponents m and n, where $m = nq + r$. Repeating this process follows the Euclidean Algorithm on the exponents:

$$(2^m - 1, 2^n - 1) \to (2^n - 1, 2^r - 1) \to \cdots \to (2^d - 1, 2^0 - 1),$$

where $d = (m, n)$. Since $2^0 - 1 = 0$, the final result is $2^d - 1$.

■

Example 1.6. Complex Fraction GCD. Prove that

$$\left(\frac{a}{(a,c)}, \frac{b}{(b,a)}, \frac{c}{(c,b)}\right) = 1.$$

Let $X = (a,b)(b,c)(c,a)$. By the distributive property:

$$X = (ab, ac, b^2, bc)(c,a) = (abc, a^2b, ac^2, a^2c, b^2c, ab^2, bc^2, abc).$$

Rearranging the terms and removing duplicates in the GCD set:

$$X = (a^2b, a^2c, ab^2, b^2c, ac^2, bc^2, abc).$$

Now consider the expression we wish to simplify. Let

$$Y = (a(a,b)(b,c), b(b,c)(c,a), c(c,a)(a,b)).$$

Expanding the terms inside Y using distributivity:

1. $a(a,b)(b,c) = a(ab, ac, b^2, bc) = (a^2b, a^2c, ab^2, abc)$.
2. $b(b,c)(c,a) = b(bc, ab, c^2, ac) = (b^2c, ab^2, bc^2, abc)$.
3. $c(c,a)(a,b) = c(ac, bc, a^2, ab) = (ac^2, bc^2, a^2c, abc)$.

Combining these sets, Y is the GCD of all terms listed above. Observe that the union of these sets is exactly the set of terms defining X. Thus $Y = X$. Let $G = (a,b)(b,c)(c,a) = X$. Then

$$Y = (a(a,b)(b,c), b(b,c)(c,a), c(c,a)(a,b)) = \left(G \cdot \frac{a}{(a,c)}, G \cdot \frac{b}{(b,a)}, G \cdot \frac{c}{(c,b)}\right).$$

By *proposition* 1.3, $Y = G\left(\frac{a}{(a,c)}, \frac{b}{(b,a)}, \frac{c}{(c,b)}\right)$. Since $Y = G$, it follows that $\left(\frac{a}{(a,c)}, \frac{b}{(b,a)}, \frac{c}{(c,b)}\right) = 1$.

範例

1.2 *The Linear Structure of Divisibility*

The Euclidean Algorithm provides more than just the numerical value of the greatest common divisor; its recursive structure reveals that (a, b) can be expressed as a linear combination of a and b. This property, known as Bézout's Identity, bridges the gap between the multiplicative structure of integers (divisibility) and their additive structure.
We begin by formalizing the coefficients generated during the Euclidean Algorithm. These coefficients allow us to "unwind" the algorithm to express the remainder in terms of the initial inputs.

Lemma 1.1. Extended Euclidean Recurrence Let a, b be positive integers. Consider the sequences of quotients q_k and remainders r_k generated by the Euclidean Algorithm, where $r_0 = b, r_{-1} = a$. Define the sequences P_k and Q_k recursively by:

$$P_0 = 1, \quad P_1 = q_1, \quad P_k = q_k P_{k-1} + P_{k-2} \quad (k \geq 2);$$
$$Q_0 = 0, \quad Q_1 = 1, \quad Q_k = q_k Q_{k-1} + Q_{k-2} \quad (k \geq 2).$$

Then for $k \geq 1$, the remainders satisfy the identity:

$$Q_k a - P_k b = (-1)^{k-1} r_k.$$

引理

We proceed by induction on k.

Base Case ($k = 1$).

From the definition, $Q_1 = 1$ and $P_1 = q_1$. The first step of the Euclidean algorithm is $a = bq_1 + r_1$, which rearranges to $1 \cdot a - q_1 \cdot b = r_1$. Thus, $Q_1 a - P_1 b = (-1)^0 r_1$, and the statement holds.

証明終

Base Case ($k = 2$).

The next Euclidean step is $b = r_1 q_2 + r_2$, so $r_2 = b - r_1 q_2$. Substituting $r_1 = a - bq_1$ gives

$$r_2 = b - q_2(a - bq_1) = (1 + q_1 q_2)b - q_2 a.$$

Thus $-r_2 = q_2 a - (q_1 q_2 + 1)b$. Since $Q_2 = q_2$ and $P_2 = q_2 q_1 + 1$, we have $Q_2 a - P_2 b = -r_2 = (-1)^1 r_2$.

証明終

Inductive Step.

Assume the identity holds for $k - 1$ and k. We prove it for $k + 1$. Recall the recurrence $r_{k-1} = r_k q_{k+1} + r_{k+1}$, which implies $r_{k+1} =$

$r_{k-1} - r_k q_{k+1}$. Multiplying by $(-1)^k$:

$$\begin{aligned}(-1)^k r_{k+1} &= (-1)^k r_{k-1} - (-1)^k r_k q_{k+1} \\ &= (-1)^{k-2} r_{k-1} + q_{k+1}[(-1)^{k-1} r_k] \\ &= (Q_{k-1}a - P_{k-1}b) + q_{k+1}(Q_k a - P_k b) \quad \text{(by hypothesis)} \\ &= (Q_{k-1} + q_{k+1}Q_k)a - (P_{k-1} + q_{k+1}P_k)b.\end{aligned}$$

By the recursive definitions of P and Q, this simplifies to $Q_{k+1}a - P_{k+1}b$. Thus the identity holds for all steps of the algorithm.

証明終

This constructive lemma leads directly to one of the most fundamental theorems in elementary number theory.

Theorem 1.6. ***Bézout's Identity.***
Let a and b be integers, not both zero. There exist integers s and t such that:

$$as + bt = (a, b).$$

定理

Proof

If a or b is zero, the result is trivial (e.g., if $a = 0$, $(0, b) = |b|$, so choose $s = 0, t = \pm 1$). Assume $a, b > 0$. Let the Euclidean algorithm terminate at step n with remainder $r_n = (a, b)$. By *lemma* 1.1, we have:

$$Q_n a - P_n b = (-1)^{n-1} r_n.$$

Multiplying by $(-1)^{n-1}$ (which is ± 1):

$$(-1)^{n-1} Q_n a + (-1)^n P_n b = r_n = (a, b).$$

Let $s = (-1)^{n-1} Q_n$ and $t = (-1)^n P_n$. These are the required integers.

■

Remark.

The integers s and t are often called **Bézout coefficients**. They are not unique; if (s, t) is a solution, then $(s + kb/(a, b), t - ka/(a, b))$ is also a solution for any integer k.

Corollary 1.3. *General Linear Combinations.* Let $a_1, \ldots, a_n$ be integers. There exist integers $k_1, \ldots, k_n$ such that:

$$\sum_{i=1}^{n} k_i a_i = (a_1, \ldots, a_n).$$

推論

Proof

This follows by induction using the associative property of the GCD established in the previous section.

■

Coprimality and Euclid's Lemma

Bézout's Identity provides a powerful algebraic characterisation of coprimality. While the definition of $(a, b) = 1$ is about the *absence* of common divisors, Bézout's Identity transforms this into the *existence* of a solution to a linear equation.

Corollary 1.4. *Characterisation of Coprimality.* Integers a and b are coprime if and only if there exist integers s and t such that:

$$as + bt = 1.$$

推論

Necessity.

If $(a, b) = 1$, *theorem* 1.6 guarantees s, t exist.

証明終

Sufficiency.

Suppose $as + bt = 1$. Let $d = (a, b)$. Then $d \mid a$ and $d \mid b$, so by linearity, $d \mid (as + bt)$, which implies $d \mid 1$. Thus $d = 1$.

証明終

This characterisation allows us to manipulate divisibility relations algebraically without prime factorisation.

Theorem 1.7. ***Preservation of GCD.***
Let a, b, c be integers. If $(a, c) = 1$, then $(ab, c) = (b, c)$.

定理

Proof

Since $(a, c) = 1$, there exist s, t such that $as + ct = 1$. Multiply this equation by b:

$$(as + ct)b = b \implies (ab)s + c(bt) = b.$$

Let $d = (ab, c)$. Then $d \mid ab$ and $d \mid c$. By linearity on the equation above, $d \mid ((ab)s + c(bt))$, so $d \mid b$. Thus d is a common divisor of b and c, implying $d \leq (b, c)$. Conversely, any divisor of b and c also divides ab and c, so $(b, c) \leq (ab, c)$. Therefore, $(ab, c) = (b, c)$.

■

This theorem immediately yields the standard form of Euclid's Lemma.

Corollary 1.5. *Euclid's Lemma.* If $c \mid ab$ and $(c, a) = 1$, then $c \mid b$.

推論

Proof

By *theorem 1.7*, $(ab, c) = (b, c)$. Since $c \mid ab$, we have $(ab, c) = |c|$. Therefore, $|c| = (b, c)$, which implies $c \mid b$.

■

Corollary 1.6. *Product Coprimality.* If $(a_i, b_j) = 1$ for all $1 \leq i \leq n$ and $1 \leq j \leq m$, then:

$$\left(\prod_{i=1}^{n} a_i, \prod_{j=1}^{m} b_j\right) = 1.$$

In particular, if $(a, b) = 1$, then $(a^n, b^m) = 1$ for any $n, m \geq 1$.

推論

Proof

By repeated application of *theorem 1.7*. First, fix b_j. Then $(a_1, b_j) = 1 \implies (a_1 a_2, b_j) = (a_2, b_j) = 1$. Inductively, $(\prod a_i, b_j) = 1$. Now let $A = \prod a_i$. We have $(A, b_j) = 1$ for all j. Applying the logic again, $(A, b_1 b_2) = (A, b_2) = 1$. Inductively, $(A, \prod b_j) = 1$.

■

We conclude this section with the property that defines the role of prime numbers in the multiplicative structure of integers.

Theorem 1.8. ***Prime Divisibility Property.***
Let p be a prime and a be an integer. Then either $p \mid a$ or $(p, a) = 1$. Consequently, if $p \mid a_1 a_2 \dots a_n$, then p divides at least one factor a_k.

定理

Proof

Let $d = (p, a)$. Since $d \mid p$, d must be either 1 or p. If $d = p$, then $p \mid a$. If $d = 1$, they are coprime. For the consequence: Suppose $p \mid a_1 \dots a_n$. If p divides no a_k, then $(p, a_k) = 1$ for all k. By the Product Coprimality corollary, $(p, \prod a_k) = 1$, contradicting $p \mid \prod a_k$.

■

1.3 *Applications and Diophantine Examples*

Example 1.7. The Measuring Problem. Two containers have capacities of 27 litres and 15 litres. How can one measure exactly 9 litres of oil from a barrel using only these containers?
We seek integer solutions to the linear combination $27x + 15y = 9$. First, check solvability: $(27, 15) = 3$. Since $3 \mid 9$, a solution exists.

Apply the Euclidean algorithm to 27 and 15:

$$27 = 1 \times 15 + 12$$

$$15 = 1 \times 12 + 3$$

Back-substitute to find the combination for 3:

$$3 = 15 - 12 = 15 - (27 - 15) = 2 \times 15 - 1 \times 27.$$

Multiply by 3 to get 9:

$$9 = 6 \times 15 - 3 \times 27.$$

Operational interpretation: The term 6×15 implies filling the 15-litre container 6 times. The term -3×27 implies emptying the 27-litre container 3 times.

· Fill B (15L), pour into A (27L). A has 15L.

· Fill B, pour into A. A is full (needs 12L). B has 3L left. Empty A.

· Pour B (3L) into A. A has 3L.

· ... Repeat this process until the net result is achieved.

範例

Example 1.8. Extraction of k-th Powers. Let a, b, c, k be positive integers such that $ab = c^k$ and $(a, b) = 1$. Prove that a and b are perfect k-th powers.

Let $d = (a, c)$. Since $d \mid a$ and $d \mid c$, we can write $a = da'$ and $c = dc'$ where $(a', c') = 1$. Consider the term $(a, c)^k = d^k$. Since $(a, b) = 1$, a shares no factors with b. Since $ab = c^k$, all prime factors of a must appear in c^k with multiplicity divisible by k. More formally, we use the property $(x, y) = 1 \implies (x^n, y^n) = 1$. We claim $a = (a, c)^k$. Consider the GCD:

$$(a^k, c^k) = (a, c)^k.$$

Also consider (a^k, ab). Since $(a, b) = 1 \implies (a^{k-1}, b) = 1$:

$$(a^k, ab) = a(a^{k-1}, b) = a \cdot 1 = a.$$

Substituting $ab = c^k$:

$$a = (a^k, c^k) = (a, c)^k.$$

Thus a is a perfect k-th power. Similarly $b = (b, c)^k$.

範例

Example 1.9. Divisibility by 11. Prove that $11 \mid (a^2 + 5b^2)$ if and only if $11 \mid a$ and $11 \mid b$.

範例

Sufficiency.

If $11 \mid a$ and $11 \mid b$, then $a = 11k, b = 11m$. $a^2 + 5b^2 = 121k^2 + 605m^2$, which is clearly divisible by 11.

証明終

Necessity.

Suppose $11 \mid (a^2 + 5b^2)$. We prove $11 \mid b$ by contradiction. Assume $11 \nmid b$. By *theorem 1.8*, $(11, b) = 1$. By *Bézout's Identity*, there exists an inverse-like integer t such that $bt + 11s = 1$. Consider the expression $a^2 + 5b^2$. Multiply by t^2:

$$t^2(a^2 + 5b^2) = (at)^2 + 5(bt)^2.$$

Since $bt = 1 - 11s$, we have $(bt)^2 = (1 - 11s)^2 = 1 - 22s + 121s^2$. Thus $(bt)^2 = 1 + 11K$ for some integer K. Substituting back:

$$t^2(a^2 + 5b^2) = (at)^2 + 5(1 + 11K) = (at)^2 + 5 + 55K.$$

Since $11 \mid (a^2 + 5b^2)$, 11 divides the LHS. Thus $11 \mid ((at)^2 + 5)$. Let $x = at$. We apply the Division Algorithm: $x = 11q + r$ where $0 \leq r \leq 10$. Then $x^2 + 5 = (11q + r)^2 + 5 = 11(11q^2 + 2qr) + r^2 + 5$. For 11 to divide the whole expression, we must have $11 \mid (r^2 + 5)$. We test all possible remainders $r \in \{0, 1, \ldots, 10\}$:

- $r = 0 \implies r^2 + 5 = 5$ (No)
- $r = 1 \implies 6$ (No)
- $r = 2 \implies 9$ (No)
- $r = 3 \implies 14$ (No)
- $r = 4 \implies 21$ (No)
- $r = 5 \implies 30$ (No)
- $r = 6 \implies 41$ (No)
- $r = 7 \implies 54$ (No)
- $r = 8 \implies 69$ (No)
- $r = 9 \implies 86$ (No)
- $r = 10 \implies 105$ (No)

This is a contradiction. Thus the assumption $11 \nmid b$ is false. So $11 \mid b$. Since $11 \mid b$, $11 \mid 5b^2$. Since $11 \mid (a^2 + 5b^2)$, by linearity $11 \mid a^2$. Since 11 is prime, $11 \mid a$.

証明終

Example 1.10. Factorial Divisibility. Let m, n be coprime positive integers. Prove that $m!n!$ divides $(m + n - 1)!$.

Consider the integers:

$$A = \binom{m+n-1}{n} = \frac{(m+n-1)!}{n!(m-1)!} \quad \text{and} \quad B = \binom{m+n-1}{m} = \frac{(m+n-1)!}{m!(n-1)!}.$$

Since these are binomial coefficients, A and B are integers. We can write:

$$(m+n-1)! = A \cdot n!(m-1)! = B \cdot m!(n-1)!.$$

Let $X = (m+n-1)!$. The equations imply:

$$X = A \cdot n! \frac{m!}{m} \implies mX = A \cdot n!m!.$$

$$X = B \cdot m! \frac{n!}{n} \implies nX = B \cdot m!n!.$$

We see that $m!n!$ divides mX and nX. Let $Y = m!n!$. Then $Y \mid mX$ and $Y \mid nX$. Since $(m,n) = 1$, by *Bézout's Identity*, there exist s,t such that $ms + nt = 1$. By *linearity of divisibility*, since Y divides mX and nX, it divides any linear combination of them:

$$Y \mid (mX)s + (nX)t \implies Y \mid X(ms+nt) \implies Y \mid X \cdot 1.$$

Therefore, $m!n! \mid (m+n-1)!$.

範例

1.4 *Least Common Multiple*

Parallel to the greatest common divisor is the concept of the least common multiple. While the GCD captures the intersection of divisor sets, the least common multiple captures the union of multiple sets.

Definition 1.3. ***Least Common Multiple.***
Let $a_1, \ldots, a_n$ be non-zero integers. An integer m is a **common multiple** if $a_i \mid m$ for all i. The **least common multiple** (LCM), denoted $[a_1, \ldots, a_n]$, is the smallest positive common multiple.

定義

Proposition 1.4. ***Basic Properties of LCM.***
Let $a_1, \ldots, a_n$ be non-zero integers.

1. **Absolute Value:** $[a_1, \ldots, a_n] = [|a_1|, \ldots, |a_n|]$.
2. **Divisibility:** If M is any common multiple, then $[a_1, \ldots, a_n] \mid M$.
3. **Homogeneity:** For any $k > 0$, $[ka_1, \ldots, ka_n] = k[a_1, \ldots, a_n]$.

命題

Proof

Property (1) follows immediately from the definition of divisibility.
For (2), let $m = [a_1, \ldots, a_n]$ and let M be a common multiple. By the *Division Algorithm*, $M = mq + r$ with $0 \leq r < m$. Since $a_i \mid M$ and $a_i \mid m$, linearity implies $a_i \mid r$ for all i. Thus r is a non-negative common multiple strictly smaller than the least positive common multiple m. This forces $r = 0$.
For (3), let $L = [ka_1, \ldots, ka_n]$. Since $ka_i \mid k[a_1, \ldots, a_n]$, we have $L \mid km$. Thus L/k is an integer. Since $ka_i \mid L \implies a_i \mid (L/k)$, L/k is a common multiple of the a_i's, so $m \leq L/k \implies km \leq L$. Thus $L = km$.

■

Theorem 1.9. ***The GCD-LCM Relation.***
For positive integers a and b:

$$[a, b](a, b) = ab.$$

定理

Proof

Let $d = (a, b)$. We first show that $m = \frac{ab}{d}$ is a common multiple. Since $b = db'$ for some integer b', $m = ab'$. Thus $a \mid m$. Similarly $b \mid m$. Let M be any common multiple of a and b. Then $M = ax = by$ for integers x, y. Dividing by d:

$$\frac{a}{d}x = \frac{b}{d}y.$$

Since $(a/d, b/d) = 1$, Euclid's Lemma implies $\frac{b}{d} \mid x$. So $x = k\frac{b}{d}$ for some integer k. Substituting back: $M = a\left(k\frac{b}{d}\right) = k\frac{ab}{d} = km$. Thus any common multiple is a multiple of ab/d. Therefore $[a, b] = \frac{ab}{d}$.

■

Corollary 1.7. *Power Property of LCM.* For any positive integer n, $[a^n, b^n] = [a, b]^n$.

推論

Proof

$$[a^n, b^n] = \frac{a^n b^n}{(a^n, b^n)} = \frac{(ab)^n}{(a, b)^n} = \left(\frac{ab}{(a, b)}\right)^n = [a, b]^n.$$

■

Theorem 1.10. ***Associativity of LCM.***

For integers $a_1, \ldots, a_n$:

$$[a_1, \ldots, a_n] = [[a_1, a_2], a_3, \ldots, a_n].$$

定理

The proof mirrors that of the GCD associativity and relies on the fact that the set of common multiples of $\{a_1, \ldots, a_n\}$ is identical to the set of common multiples of $\{[a_1, a_2], a_3, \ldots, a_n\}$.

Applications of LCM

Example 1.11. Planetary Alignment. Venus orbits the Sun in 225 days, and Earth in 365 days. If they are aligned today, when will they align again at the same position?
We seek the least common multiple of 225 and 365. Using the Euclidean Algorithm to find $(225, 365)$:

$$\begin{aligned} 365 &= 225 \times 1 + 140 \\ 225 &= 140 \times 1 + 85 \\ 140 &= 85 \times 1 + 55 \\ 85 &= 55 \times 1 + 30 \\ 55 &= 30 \times 1 + 25 \\ 30 &= 25 \times 1 + 5 \\ 25 &= 5 \times 5 + 0. \end{aligned}$$

Thus $(225, 365) = 5$. By *theorem* 1.9:

$$[225, 365] = \frac{225 \times 365}{5} = \frac{82125}{5} = 16425 \text{ days}.$$

This corresponds to $16425/365 = 45$ Earth years and $16425/225 = 73$ Venusian years.

範例

Example 1.12. Counting Solutions to GCD-LCM Constraints. Find the number of triples (a, b, c) of positive integers satisfying:

$$(a, b, c) = 10 \quad \text{and} \quad [a, b, c] = 100.$$

Let $a = 10x, b = 10y, c = 10z$. The conditions simplify to:

$$(x, y, z) = 1 \quad \text{and} \quad [x, y, z] = 10.$$

The variables x, y, z must be divisors of 10. Thus $x, y, z \in \{1, 2, 5, 10\}$. We analyse the possible multisets $\{x, y, z\}$ based on cardinality of distinct elements.

Case 1: All three are equal. If $x = y = z = k$, then $(k, k, k) = k$ and

$[k,k,k] = k$. We require $k = 1$ and $k = 10$ simultaneously, which is impossible. (0 solutions).

Case 2: Two are equal. Let the set be $\{k,k,m\}$ with $k \neq m$. The conditions require $(k,m) = 1$ and $[k,m] = 10$. We check possible pairs from $\{1,2,5,10\}$:

- If $k = 10$, we need $[10,m] = 10$ (always true for divisors) and $(10,m) = 1$. The only coprime divisor is $m = 1$. Set: $\{10,10,1\}$.
- If $k = 5$, we need $[5,m] = 10 \implies m \in \{2,10\}$. We need $(5,m) = 1$. If $m = 2$, $(5,2) = 1$ (Valid). Set: $\{5,5,2\}$. If $m = 10$, $(5,10) = 5 \neq 1$ (Invalid).
- If $k = 2$, we need $[2,m] = 10 \implies m \in \{5,10\}$. We need $(2,m) = 1$. If $m = 5$, $(2,5) = 1$ (Valid). Set: $\{2,2,5\}$. If $m = 10$, $(2,10) = 2 \neq 1$ (Invalid).
- If $k = 1$, we need $[1,m] = 10 \implies m = 10$. We need $(1,10) = 1$ (Valid). Set: $\{1,1,10\}$.

There are 4 valid multisets. For each multiset with two identical elements (e.g., $\{10,10,1\}$), there are $\frac{3!}{2!} = 3$ permutations. Total solutions in this case: $4 \times 3 = 12$.

Case 3: All three are distinct. We choose 3 distinct elements from $\{1,2,5,10\}$. There are $\binom{4}{3} = 4$ possible sets. We verify if they satisfy $(x,y,z) = 1$ and $[x,y,z] = 10$:

- $\{10,5,2\}$: GCD is 1, LCM is 10. (Valid).
- $\{10,5,1\}$: GCD is 1, LCM is 10. (Valid).
- $\{10,2,1\}$: GCD is 1, LCM is 10. (Valid).
- $\{5,2,1\}$: GCD is 1, LCM is 10. (Valid).

All 4 sets are valid. For each set of 3 distinct elements, there are $3! = 6$ permutations. Total solutions in this case: $4 \times 6 = 24$.

Summing the cases, the total number of solutions is $12 + 24 = 36$.

範例

Example 1.13. Coprimes in Arithmetic Progressions. Let a, b, m be positive integers with $(a,b) = 1$. Prove there are infinitely many terms in the sequence $a, a+b, a+2b, \ldots$ that are coprime to m.

範例

Proof

Let c be the largest divisor of m such that $(c,a) = 1$. We consider the term $X = a + bc$. We calculate (X,m). Let $d = (a+bc, m)$. Since $d \mid m$ and $c \mid m$, any common factor of d and c must divide m. Also $d \mid (a+bc)$. If $k \mid d$ and $k \mid c$, then $k \mid bc$, so $k \mid a$. But $(c,a) = 1$, so

$k = 1$. Thus $(d, c) = 1$.
Now consider prime factors of m. Let $p \mid m$. If $p \mid c$, then $p \nmid a$ (since $(c, a) = 1$) and $p \mid bc$. Thus $p \nmid (a + bc)$, so $p \nmid d$. If $p \nmid c$, then by the maximality of c, we must have $p \mid a$ (otherwise cp would be a larger divisor coprime to a). If $p \mid a$ and $p \nmid c$, then $p \nmid bc$ (since $(a, b) = 1$). Thus $p \nmid (a + bc)$, so $p \nmid d$. In all cases, no prime factor of m divides d. Thus $d = 1$. So $(a + bc, m) = 1$. The term $a + (c + km)b = (a + bc) + k(mb)$ satisfies:

$$((a + bc) + kmb, m) = (a + bc, m) = 1.$$

This generates infinitely many such terms as k varies.

■

1.5 *Exercises*

1. **Euclidean Computations.** Use the Euclidean algorithm to calculate the greatest common divisor for the following pairs:
   (a) $(4935, 13912)$
   (b) $(51425, 13310)$
2. **Coprimality of Power Forms.** Let m and n be positive integers. Prove that if m is odd, then:
   $$(2^m - 1, 2^n + 1) = 1.$$
3. **Minimal Linear Combinations.** Let a, b be integers, not both zero. Let $d = ax_0 + by_0$ be the smallest positive integer expressible in the form $ax + by$ with $x, y \in \mathbb{Z}$. Prove that $d = (a, b)$.
4. **Mersenne Coprimality.** Prove that $(2^p - 1, 2^q - 1) = 1$ if and only if $(p, q) = 1$.
5. **Coprime Arithmetic Progressions.** Let $n \geq 2$. Prove that there exist n composite numbers in arithmetic progression such that any two of them are coprime.
6. **Symbolic GCDs.** Evaluate the following greatest common divisors in terms of n:
   (a) $(2^{n+1} + 1, 2^{n-1} + 1)$ for $n > 0$.
   (b) $(n - 1, n^2 + n + 1)$.
7. **Setwise vs Pairwise Coprimality.** Construct a set of four positive integers such that their collective greatest common divisor is 1, yet no subset of three integers is coprime (i.e., every triplet shares a common factor greater than 1).
8. **Multiple GCD Computation.** Calculate the greatest common

divisor of the set $(353430, 530145, 165186)$.

9. **GCD Identity.** Prove the following identity for any positive integers a, b, c:
$$(a, b, c)(ab, bc, ca) = (a, b)(b, c)(c, a).$$

10. **Gear Synchronization.** Two meshing gears A and B have 437 and 323 teeth respectively. If a specific tooth on A touches a specific tooth on B, find the minimum number of revolutions each gear must make before these two specific teeth touch again.

11. **Constrained Solutions.** Find all pairs of positive integers (a, b) such that $(a, b) = 10$ and $[a, b] = 100$.

12. **Consecutive LCM.** Determine the least common multiple of three consecutive positive integers $n, n + 1, n + 2$. Express your answer in terms of n (cases may be required based on the parity of n).

13. **Divisibility by 13.** Let a, b be integers. Prove that $13 \mid (a^2 - 7b^2)$ if and only if $13 \mid a$ and $13 \mid b$.

14. **Bounded Bézout Coefficients.** Let $a, b > 1$ be coprime integers. Prove that there exist integers ξ, η such that:
$$a\xi - b\eta = 1$$
satisfying the bounds $0 < \xi < b$ and $0 < \eta < a$.

15. **Cyclic Divisibility.** Find all sets of three distinct positive integers $\{x, y, z\}$ such that:
    (i) They are pairwise coprime;
    (ii) The sum of any two is divisible by the third.

16. **Reciprocal Equation and Squares.** Let a, b, c be positive integers satisfying $(a, b, c) = 1$ and the equation:
$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c}.$$
Prove that $a + b$, $a - c$, and $b - c$ are all perfect squares.

17. **Sum of Reciprocals of Coprimes.** Let $m > n > 1$. Let $a_1 < a_2 < \cdots < a_k$ be all positive integers not exceeding m that are coprime to n. Define the sum $S = \sum_{i=1}^{k} \frac{1}{a_i}$. Prove that S is not an integer.

2
Applications

We have seen that the set of integers $\mathbb{Z}$ is equipped with a division algorithm and a structure of primality. However, the true power of prime numbers lies not in their definition, but in their role as the unique building blocks of all integers.

2.1 *Fundamental Theorem of Arithmetic*

Theorem 2.1. ***Fundamental Theorem of Arithmetic.***
Every integer $n > 1$ can be represented as a product of prime numbers. This representation is unique, up to the order of the factors.

定理

Existence.

We proceed by the *Second Principle of Mathematical Induction*. For $n = 2$, the number is prime, so the statement holds. Assume the statement holds for all integers k such that $2 \leq k < n$. If n is prime, the representation exists (it is simply n). If n is composite, there exist integers a, b such that $n = ab$ with $1 < a, b < n$. By the inductive hypothesis, a and b can be written as products of primes:

$$a = p_1 \dots p_r, \quad b = q_1 \dots q_s.$$

Thus $n = p_1 \dots p_r q_1 \dots q_s$ is a product of primes. By the Strong Induction Principle, existence holds for all $n > 1$.

証明終

Uniqueness.

Suppose n has two factorisations. By arranging the prime factors in non-decreasing order, let:

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_m,$$

where $p_1 \leq p_2 \leq \cdots \leq p_k$ and $q_1 \leq q_2 \leq \cdots \leq q_m$ are primes. We consider p_1. Since $p_1 \mid n$, it follows that $p_1 \mid q_1 q_2 \dots q_m$. By *theorem* 1.8 (Prime Divisibility Property), p_1 must divide at least one

factor q_j. Since q_j is prime, the only positive divisors are 1 and q_j. As $p_1 > 1$, we must have $p_1 = q_j$. Since the q's are sorted, $q_1 \leq q_j$, so $q_1 \leq p_1$. By symmetry, applying the same argument to q_1 yields $q_1 \mid \prod p_i$, implying $q_1 = p_i$ for some i. Thus $p_1 \leq p_i$, so $p_1 \leq q_1$. Therefore, $p_1 = q_1$. We can cancel this common factor from the equation:

$$p_2 \dots p_k = q_2 \dots q_m.$$

Repeating this argument yields $p_2 = q_2$, and so on. If $k < m$, we would eventually reach $1 = q_{k+1} \dots q_m$, which is impossible since $q_i \geq 2$. Similarly $k > m$ is impossible. Thus $k = m$ and $p_i = q_i$ for all i.

証明終

Definition 2.1. ***Standard Factorisation.***
By collecting identical primes, any integer $n > 1$ can be written uniquely in the form:

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k},$$

where $p_1 < p_2 < \cdots < p_k$ are primes and $a_i \geq 1$ are integers. This is called the **standard factorisation** of n.

定義

Remark.

For theoretical convenience, we may write $n = \prod_p p^{v_p(n)}$, where the product extends over all primes and the exponent $v_p(n)$ is zero for all but finitely many primes. The exponent $v_p(n)$ is often called the *p-adic valuation* of n.

Example 2.1. Factorisation of a Large Integer. Find the standard factorisation of $n = 82,798,848$.
We extract factors sequentially:

$$\begin{aligned} 82,798,848 &= 2 \times 41,399,424 \\ &= 2^8 \times 323,433 \quad \text{(after removing all factors of 2)} \\ &= 2^8 \times 3 \times 107,811 \\ &= 2^8 \times 3^5 \times 1,331 \quad \text{(after removing factors of 3).} \end{aligned}$$

Recognising $1,331 = 11^3$, we achieve the form:

$$n = 2^8 \cdot 3^5 \cdot 11^3.$$

範例

Example 2.2. Irrationality of Logarithms. Prove that $\log_{10} 2$ is irrational.
Assume for contradiction that $\log_{10} 2 \in \mathbb{Q}$. Let $\log_{10} 2 = \frac{a}{b}$ for posi-

tive integers a, b. Then $10^{a/b} = 2$, which implies $10^a = 2^b$. Substituting the standard factorisation of $10 = 2 \cdot 5$:

$$(2 \cdot 5)^a = 2^b \implies 2^a \cdot 5^a = 2^b.$$

By the uniqueness of the standard factorisation (*theorem 2.1*), the exponent of the prime 5 on the left hand side must equal the exponent of 5 on the right hand side. On the LHS, the exponent is a. On the RHS, it is 0. Thus $a = 0$. However, a must be a positive integer since $\log_{10} 2 > 0$ (as $2 > 1$). This is a contradiction. Therefore, $\log_{10} 2$ is irrational.

範例

Divisors and Factorisation

The standard factorisation allows us to characterise all divisors of an integer.

Corollary 2.1. *Structure of Divisors.* Let $n = p_1^{a_1} \dots p_k^{a_k}$. An integer d divides n if and only if

$$d = p_1^{b_1} \dots p_k^{b_k},$$

where $0 \leq b_i \leq a_i$ for all $i = 1, \dots, k$.

推論

Proof

If d has this form, then $n = d \cdot \prod p_i^{a_i - b_i}$, where the cofactor is an integer since $a_i - b_i \geq 0$. Thus $d \mid n$. Conversely, if $d \mid n$, all prime factors of d must be prime factors of n. Let $d = \prod p_i^{b_i}$. If any $b_i > a_i$, then $p_i^{b_i}$ would divide n, implying $p_i^{b_i} \mid p_i^{a_i} \times$ (other primes). By unique factorisation, this is impossible. Thus $b_i \leq a_i$.

■

This characterisation provides an arithmetic formula for the GCD and LCM.

Theorem 2.2. ***GCD and LCM via Prime Powers.***
Let $m = p_1^{a_1} \dots p_k^{a_k}$ and $n = p_1^{b_1} \dots p_k^{b_k}$, where we allow exponents to be zero to include all prime factors of both numbers. Then:

$$(m, n) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_k^{\min(a_k, b_k)},$$
$$[m, n] = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_k^{\max(a_k, b_k)}.$$

定理

Proof

Let $g = \prod p_i^{\min(a_i,b_i)}$. Since $\min(a_i,b_i) \le a_i$ and $\min(a_i,b_i) \le b_i$, g divides both m and n. Suppose d is any common divisor. By *corollary 2.1*, $d = \prod p_i^{e_i}$ with $e_i \le a_i$ and $e_i \le b_i$. Thus $e_i \le \min(a_i,b_i)$. This implies $d \mid g$. Hence g is the greatest common divisor. The proof for the least common multiple is analogous, using the property that any common multiple must have exponents at least $\max(a_i,b_i)$.

■

Remark.

The identity $(m,n)[m,n] = mn$ follows immediately from this theorem, since for any numbers x, y, we have $\min(x,y) + \max(x,y) = x + y$.

Example 2.3. Calculating GCD and LCM. Find $(1008, 1260, 882, 1134)$ and $[1008, 1260, 882, 1134]$.
We determine the prime factorisations:

$$\begin{aligned} 1008 &= 2^4 \cdot 3^2 \cdot 7^1, \\ 1260 &= 2^2 \cdot 3^2 \cdot 5^1 \cdot 7^1, \\ 882 &= 2^1 \cdot 3^2 \cdot 7^2, \\ 1134 &= 2^1 \cdot 3^4 \cdot 7^1. \end{aligned}$$

The relevant primes are $\{2,3,5,7\}$. We align the exponents:

n	$v_2(n)$	$v_3(n)$	$v_5(n)$	$v_7(n)$
1008	4	2	0	1
1260	2	2	1	1
882	1	2	0	2
1134	1	4	0	1

For the GCD, we take the column minima: $2^1 \cdot 3^2 \cdot 5^0 \cdot 7^1 = 2 \cdot 9 \cdot 1 \cdot 7 = 126$. For the LCM, we take the column maxima: $2^4 \cdot 3^4 \cdot 5^1 \cdot 7^2 = 16 \cdot 81 \cdot 5 \cdot 49 = 317,520$.

範例

Example 2.4. Bound on Prime Factors. Prove that for any integer $n > 1$, $\log_{10} n \ge k \log_{10} 2$, where k is the number of distinct prime factors of n.
Let $n = p_1^{a_1} \dots p_k^{a_k}$ be the standard factorisation. Since the primes are distinct and the smallest prime is 2, we have $p_i \ge 2$ for all i. Also $a_i \ge 1$. Thus:

$$n = p_1^{a_1} \dots p_k^{a_k} \ge 2^1 \cdot 2^1 \dots 2^1 = 2^k.$$

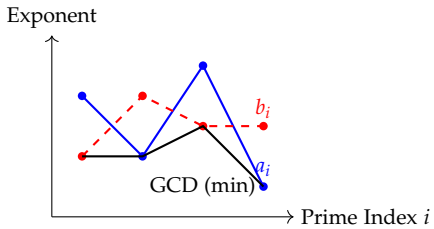


Figure 2.1: Visualisation of GCD exponents. For each prime p_i, the exponent of the GCD is the minimum of the exponents in m (blue) and n (red).

Taking logarithms (base 10) is an increasing function:

$$\log_{10} n \geq \log_{10}(2^k) = k \log_{10} 2.$$

This inequality provides a quick upper bound on the number of distinct prime factors: $k \leq \frac{\log_{10} n}{\log_{10} 2}$.

範例

Square-Free Integers

Integers can be classified by the multiplicity of their factors. An integer is **square-free** if it is not divisible by any perfect square greater than 1.

Proposition 2.1. ***Square-Free Decomposition.***
Every positive integer n can be written uniquely as $n = k^2 l$, where l is a square-free integer.

命題

Proof

Let $n = \prod p_i^{a_i}$. For each exponent a_i, by the *Division Algorithm*, we can write $a_i = 2q_i + r_i$, where $r_i \in \{0, 1\}$. We construct:

$$k = \prod p_i^{q_i}, \quad l = \prod p_i^{r_i}.$$

Then:

$$k^2 l = \left(\prod p_i^{2q_i}\right)\left(\prod p_i^{r_i}\right) = \prod p_i^{2q_i + r_i} = \prod p_i^{a_i} = n.$$

Since $r_i \in \{0, 1\}$, every prime factor in l has exponent 1 (or 0), so l is square-free. Uniqueness follows from the uniqueness of the quotient and remainder in integer division. If $n = k_1^2 l_1 = k_2^2 l_2$ with l_1, l_2 square-free, then comparing prime exponents shows $l_1 = l_2$ and $k_1 = k_2$.

■

Example 2.5. Perfect Powers and GCDs. Prove that if n is a perfect square and a perfect cube, it is a perfect sixth power.
Let $n = \prod p_i^{e_i}$. If n is a perfect square, $n = k^2$, so e_i must be even for all i. Thus $2 \mid e_i$. If n is a perfect cube, $n = m^3$, so e_i must be a multiple of 3 for all i. Thus $3 \mid e_i$. Since 2 and 3 are coprime, $2 \mid e_i$ and $3 \mid e_i$ implies $6 \mid e_i$. Let $e_i = 6j_i$. Then:

$$n = \prod p_i^{6j_i} = \left(\prod p_i^{j_i}\right)^6.$$

Thus n is a perfect sixth power.

範例

2.2 *Primality Testing and Sieves*

The *Fundamental Theorem of Arithmetic* guarantees the existence of a unique prime factorisation, but it provides no algorithm for finding it. To determine whether a given integer n is prime, or to generate the sequence of primes, we rely on the properties of divisors.

Theorem 2.3. ***Smallest Divisor.***
Let $n > 1$ be a composite integer. The smallest divisor d of n such that $d > 1$ is a prime number.

定理

Proof

Suppose d is the smallest divisor of n greater than 1. If d were composite, there would exist integers a, b such that $d = ab$ with $1 < a < d$. By transitivity, $a \mid d$ and $d \mid n$ implies $a \mid n$. Thus a is a divisor of n strictly between 1 and d. This contradicts the minimality of d. Therefore, d must be prime.

■

This observation leads to the standard trial division test.

Theorem 2.4. ***The Square Root Test.***
If $n > 1$ is not divisible by any prime $p \leq \sqrt{n}$, then n is prime.

定理

Proof

Assume n is composite. By the preceding theorem, let p be the smallest divisor of n greater than 1. Then p is prime. Since n is composite, we can write $n = p \cdot m$ where $1 < p \leq m$. Multiplying by p gives $p^2 \leq pm = n$. Taking the square root, we obtain $p \leq \sqrt{n}$. By contrapositive, if no prime $p \leq \sqrt{n}$ divides n, then n cannot be composite.

■

Example 2.6. Primality of 2003. Determine if 2003 is prime.
We estimate $\sqrt{2003} \approx 44.7$. It suffices to test divisibility by primes $p \leq 43$. The list of primes is $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43\}$.
· 2003 is odd (not divisible by 2).
· Sum of digits is 5 (not divisible by 3).
· Does not end in 0 or 5 (not divisible by 5).
· $2003 = 7 \times 286 + 1$ ($7 \nmid 2003$).
· Alternating sum $2 - 0 + 0 - 3 = -1$ (not divisible by 11).
Continuing trial division for the remaining primes yields non-zero remainders in all cases. Therefore, 2003 is prime.

範例

The Sieve of Eratosthenes

The Square Root Test allows us to generate a table of primes up to a bound N by systematically eliminating composite numbers. This method, known as the Sieve of Eratosthenes, relies on the fact that every composite number $n \leq N$ has a prime factor $p \leq \sqrt{N}$.

Algorithm:

1. List all integers from 2 to N.
2. Let $p = 2$. Mark all multiples of p greater than p (i.e., $2p, 3p, \dots$) as composite.
3. Find the smallest unmarked number greater than p; let this be the new p.
4. Repeat step 2 until $p > \sqrt{N}$.
5. All remaining unmarked numbers are prime.

Example 2.7. Sieve up to 50. We list integers $2, \dots, 50$. The sieving primes are those $\leq \sqrt{50} \approx 7.07$, i.e., $\{2, 3, 5, 7\}$.

1. Eliminate multiples of 2: $4, 6, 8, \dots, 50$.
2. Eliminate multiples of 3: $9, 15, 21, \dots$ (some like 6, 12 were already removed).
3. Eliminate multiples of 5: $25, 35, \dots$ (others like 10, 15, 20 removed).
4. Eliminate multiples of 7: 49 (others like 14, 21, 28, 35, 42 removed).

The remaining numbers are the primes:

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}.$$

範例

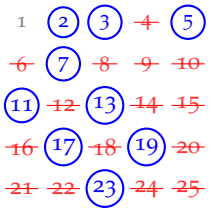


Figure 2.2: A visual representation of sieving for $N = 25$. Multiples of 2, 3, 5 are eliminated; primes are circled.

The Sieve of Sundaram

While Eratosthenes sieves by additive multiples, the Sieve of Sundaram uses a specific arithmetic progression structure to isolate odd primes.

Consider the infinite table of integers defined by $a_{ij} = i + j + 2ij$, where $1 \leq i \leq j$.

$$\begin{array}{cccc} 4 & 7 & 10 & \dots \\ 7 & 12 & 17 & \dots \\ 10 & 17 & 24 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{array}$$

The first row has common difference 3 ($4, 7, 10, \dots$). The second row has common difference 5 ($7, 12, 17, \dots$). The i-th row is an arithmetic progression with first term $4 + 3(i-1)$ and common difference $2i + 1$.

Theorem 2.5. ***Sundaram's Primality Condition.***
A positive integer N appears in the Sundaram table if and only if $2N+1$ is composite. Consequently, $2N+1$ is prime if and only if N does not appear in the table.

定理

Proof

Let N be an entry in the table. Then $N = i + j + 2ij$ for some $1 \leq i \leq j$. We examine $2N+1$:

$$2N + 1 = 2(i + j + 2ij) + 1 = 4ij + 2i + 2j + 1.$$

Factoring by grouping:

$$4ij + 2i + 2j + 1 = 2i(2j + 1) + 1(2j + 1) = (2i + 1)(2j + 1).$$

Since $i, j \geq 1$, the factors $2i+1$ and $2j+1$ are both at least 3. Thus $2N+1$ is composite.
Conversely, suppose $M = 2N+1$ is a composite odd integer. Then $M = AB$ where A, B are odd integers greater than 1. Let $A = 2i+1$ and $B = 2j+1$ for some integers $i, j \geq 1$. Then $2N+1 = (2i+1)(2j+1) = 4ij+2i+2j+1$. Subtracting 1 and dividing by 2 yields $N = 2ij + i + j$. Assuming without loss of generality $i \leq j$, N appears in the table at row i, column j.

■

Example 2.8. Application of Sundaram's Sieve. We determine if $M = 17$ and $M = 9$ are prime using the parameter $N = (M-1)/2$.
For $M = 17$, $N = 8$. We check if 8 can be written as $i + j + 2ij$. Since $i \geq 1$, we must have $2ij < 8$, so $ij < 4$. Possible pairs (i, j) with $1 \leq i \leq j$:
· $(1,1) \implies 1+1+2(1) = 4 \neq 8$.
· $(1,2) \implies 1+2+2(2) = 7 \neq 8$.
· $(1,3) \implies 1+3+2(3) = 10 > 8$.
Since 8 is not in the table, $2(8)+1 = 17$ is prime.
For $M = 9$, $N = 4$. Checking $(1,1) \implies 1+1+2 = 4$. Since 4 is in the table, $2(4)+1 = 9$ is composite.

範例

Properties of Prime Divisors

The distribution of primes often imposes constraints on the structure of remainders and factorisations.

Example 2.9. Remainder Modulo 30. Let p be a prime such that when divided by 30, the remainder is r. Prove that if $r \neq 1$, then r is prime.

Let $p = 30k + r$ with $1 < r < 30$ (since $r \neq 1$). We analyse the divisibility of r by the prime factors of 30, which are 2, 3, and 5. If $p \in \{2, 3, 5\}$, then $r \in \{2, 3, 5\}$, which are primes. Assume $p > 5$. Then $(p, 30) = 1$. Since $r = p - 30k$, any common divisor of r and 30 must divide p. Thus $(r, 30) = (p, 30) = 1$. This implies r is not divisible by 2, 3, or 5. Suppose for contradiction that r is composite. Then r must have a prime factor $q \leq \sqrt{r}$. Since $r < 30$, $q \leq \sqrt{29} \approx 5.38$. So q must be 2, 3, or 5. But we established $(r, 30) = 1$, so r has no such factors. Contradiction. Thus r is prime.

範例

Example 2.10. Factors of Cube Root Magnitude. Prove that if a composite integer n has no prime factor less than or equal to $\sqrt[3]{n}$, then n is the product of exactly two primes.

Since n is composite, let $n = p_1 p_2 \dots p_k$ be its prime factorisation with $k \geq 2$. By hypothesis, $p_i > n^{1/3}$ for all i. Suppose $k \geq 3$. Then:

$$n = p_1 p_2 p_3 \dots p_k > n^{1/3} \cdot n^{1/3} \cdot n^{1/3} = n.$$

This implies $n > n$, a contradiction. Since $k \geq 2$ and $k < 3$, we must have $k = 2$. Thus $n = p_1 p_2$.

範例

Example 2.11. Odd Primes and Arithmetic Progressions. Prove that the odd primes less than n^2 are exactly the odd numbers greater than 1 that do not belong to the sequences $\{r(r + 2k)\}_{k \geq 0}$ for any odd $r \geq 3$.

Let S be the set of odd numbers greater than 1. Consider the subset $C = \{r^2, r^2 + 2r, r^2 + 4r, \dots\}$ where r ranges over all odd integers ≥ 3. The general term of a sequence in C is $a = r^2 + 2rk = r(r + 2k)$. Since $r \geq 3$ is odd, and $r + 2k \geq 3$ is odd, a represents a composite odd integer. Conversely, let $m < n^2$ be a composite odd integer. Let r be the smallest prime factor of m. Since m is odd, $r \geq 3$. Since m is composite, $m = r \cdot b$ where $b \geq r$ is odd. We can write $b = r + 2k$ for some integer $k \geq 0$. Thus $m = r(r + 2k)$, so $m \in C$. Therefore, the odd numbers in $S \setminus C$ are exactly those which are not composite, i.e., the odd primes.

範例

2.3 *Exercises*

1. **Factorisation of Large Integers.** Determine the standard prime factorisation of the integer $N = 81,057,226,635,000$.
2. **GCD and LCM Calculation.** Calculate the greatest common divisor and least common multiple of the set $\{198, 240, 360\}$.
3. **Inverse GCD-LCM Problem.** Find all pairs of positive integers (a, b) such that $(a, b) = 24$ and $[a, b] = 144$.
4. **Counting LCM Solutions.** Let $\omega(n)$ denote the number of distinct prime factors of n. Let d be a square-free integer. Prove that the number of ordered pairs of positive integers (d_1, d_2) such that $[d_1, d_2] = d$ is exactly $3^{\omega(d)}$.

   Consider the prime factorisation of $d = p_1 \dots p_k$ and the possible exponents of p_i in d_1 and d_2.
5. **Remainder of Prime Squares.** If a prime $p > 7$, prove that the remainder when p^2 is divided by 30 must be 1 or 19.
6. **Primality Test Condition.** Let $n > 5$ be an odd integer. Suppose there exist positive even integers a and b such that:

$$a - b = n \quad \text{and} \quad a + b = \prod_{i=1}^{s} p_i,$$

   where $p_1, \dots, p_s$ are all the odd primes not exceeding $\sqrt{n}$. Prove that n is prime.
7. **Coprimality in Arithmetic Sequences.** Let $p_1, p_2, \dots$ be the sequence of primes in increasing order. Let $P_n = p_1 p_2 \dots p_n$. Consider the sequence of integers defined by $a_k = 1 + kP_n$ for $k = 0, 1, \dots, n-1$. Prove that for any distinct indices $i, j \in \{0, \dots, n-1\}$, $(a_i, a_j) = 1$.
8. **Factorial Constraints.** Let n be a positive integer. Prove that if $n!$ is divisible by n^2, then n cannot be prime. Determine for which composite n this divisibility holds.

3
The Gauss Function

While divisibility and primality explore the multiplicative structure of integers, many number-theoretic problems require analysing the position of real numbers relative to consecutive integers. We introduce the Gauss function, widely known as the floor function, to bridge the continuous domain of real numbers $\mathbb{R}$ and the discrete domain of integers $\mathbb{Z}$.

Definition 3.1. ***The Floor Function.***
Let x be a real number. The **floor function** or **Gauss function**, denoted $\lfloor x \rfloor$, is the unique integer satisfying:

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

We refer to $\lfloor x \rfloor$ as the **integer part** of x. The **fractional part** of x is defined as $\{x\} = x - \lfloor x \rfloor$.

定義

Note

By definition, $0 \leq \{x\} < 1$ for all real numbers x.

The floor function behaves predictably under integer translation and order.

Proposition 3.1. ***Monotonicity.***
For real numbers x and y, if $x \leq y$, then $\lfloor x \rfloor \leq \lfloor y \rfloor$.

命題

This follows immediately from the definition, indicating that $\lfloor x \rfloor$ is a non-decreasing function.

Proposition 3.2. ***Integer Translation.***
Let $x \in \mathbb{R}$ and $n \in \mathbb{Z}$. Then:

$$\lfloor n + x \rfloor = n + \lfloor x \rfloor.$$

Conversely, if $\lfloor n + x \rfloor = n + \lfloor x \rfloor$ for all x, then n is an integer.

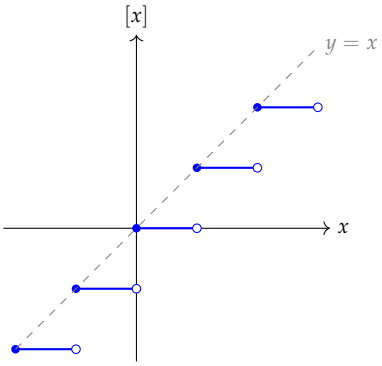


Figure 3.1: The graph of the floor function $[x]$. It is a step function that lies on or below the line $y = x$.

命題

Proof

Let $k = \lfloor x \rfloor$. By definition, $k \leq x < k+1$. Adding the integer n to the inequality yields:

$$n + k \leq n + x < n + k + 1.$$

Since $n + k$ is an integer, it must be the floor of $n + x$. Thus $\lfloor n + x \rfloor = n + k = n + \lfloor x \rfloor$.

■

Theorem 3.1. ***Subadditivity.***
For any real numbers x and y:

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor.$$

定理

Proof

From the definition, $\lfloor x \rfloor \leq x$ and $\lfloor y \rfloor \leq y$. Adding these gives $\lfloor x \rfloor + \lfloor y \rfloor \leq x + y$. Since the left-hand side is an integer, applying *proposition 3.1* yields:

$$\lfloor \lfloor x \rfloor + \lfloor y \rfloor \rfloor \leq \lfloor x + y \rfloor \implies \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor.$$

■

Example 3.1. Simple Bounds involving Floor. Find all real solutions to $x + \{x\} = 1.6$.
We substitute $x = \lfloor x \rfloor + \{x\}$ into the equation:

$$\lfloor x \rfloor + 2\{x\} = 1.6.$$

Since $\lfloor x \rfloor$ is an integer and $0 \leq \{x\} < 1$, we have bounds on $2\{x\}$:

$$0 \leq 2\{x\} < 2.$$

Rearranging for the integer part: $\lfloor x \rfloor = 1.6 - 2\{x\}$. Using the bounds for $2\{x\}$, we have:

$$1.6 - 2 < \lfloor x \rfloor \leq 1.6 - 0 \implies -0.4 < \lfloor x \rfloor \leq 1.6.$$

Thus, the possible integer values for $\lfloor x \rfloor$ are 0 and 1.
1. If $\lfloor x \rfloor = 0$, then $2\{x\} = 1.6 \implies \{x\} = 0.8$. Thus $x = 0.8$.
2. If $\lfloor x \rfloor = 1$, then $2\{x\} = 0.6 \implies \{x\} = 0.3$. Thus $x = 1.3$.

The solutions are $x \in \{0.8, 1.3\}$.

範例

Arithmetic Relationships

The interaction between the floor function and arithmetic operations produces several identities useful for simplifying sums and solving equations.

Theorem 3.2. ***Reflection Formula.***
For any real number x:

$$\lfloor -x \rfloor = \begin{cases} -\lfloor x \rfloor - 1 & \text{if } x \notin \mathbb{Z}, \\ -\lfloor x \rfloor & \text{if } x \in \mathbb{Z}. \end{cases}$$

定理

Proof

We write $x = \lfloor x \rfloor + \{x\}$. Negating this yields $-x = -\lfloor x \rfloor - \{x\}$. We can express this as $-x = -\lfloor x \rfloor - 1 + (1 - \{x\})$.

- If $x \in \mathbb{Z}$, then $\{x\} = 0$, so $\lfloor -x \rfloor = -x = -\lfloor x \rfloor$.
- If $x \notin \mathbb{Z}$, then $0 < \{x\} < 1$, which implies $0 < 1 - \{x\} < 1$. Thus, the integer part of $-x$ is $-\lfloor x \rfloor - 1$.

Alternatively, using fractional parts: $\{-x\} = 1 - \{x\}$ for non-integers, leading to the same result.

■

Theorem 3.3. ***Sum of Fractional Parts.***
If $\{x\} + \{y\} = 1$, then $\lfloor x \rfloor + \lfloor y \rfloor = \lfloor x + y \rfloor - 1$.

定理

Proof

We expand $x + y$:

$$x + y = (\lfloor x \rfloor + \{x\}) + (\lfloor y \rfloor + \{y\}) = (\lfloor x \rfloor + \lfloor y \rfloor) + (\{x\} + \{y\}).$$

Given $\{x\} + \{y\} = 1$, this becomes $x + y = \lfloor x \rfloor + \lfloor y \rfloor + 1$. Taking the floor of both sides (noting the RHS is an integer):

$$\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + 1.$$

Rearranging gives the result.

■

Theorem 3.4. ***The Halving Identity.***
For any real number x:

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor.$$

定理

Proof

Let $x = n + \theta$ where $n = \lfloor x \rfloor$ and $0 \leq \theta < 1$. We consider two cases for the fractional part θ:

Case $0 \leq \theta < 1/2$. Then $\lfloor x + 1/2 \rfloor = \lfloor n + \theta + 1/2 \rfloor = n$, since $\theta + 1/2 < 1$. Also $2x = 2n + 2\theta$, where $0 \leq 2\theta < 1$. Thus $\lfloor 2x \rfloor = 2n$. The identity holds: $n + n = 2n$.

Case $1/2 \leq \theta < 1$. Then $\lfloor x + 1/2 \rfloor = \lfloor n + \theta + 1/2 \rfloor = n + 1$, since $1 \leq \theta + 1/2 < 1.5$. Also $2x = 2n + 2\theta$, where $1 \leq 2\theta < 2$. Thus $\lfloor 2x \rfloor = 2n + 1$. The identity holds: $n + (n + 1) = 2n + 1$.

■

This theorem implies that the sequence of "binary digits" of x affects the floor of multiples of x. We can generalise the separation of floors based on the difference of their arguments.

Theorem 3.5. ***Difference of Floors.***
For any real numbers α and β:

$$\lfloor \alpha \rfloor - \lfloor \beta \rfloor = \lfloor \alpha - \beta \rfloor \quad \text{or} \quad \lfloor \alpha - \beta \rfloor + 1.$$

定理

Proof

We expand $\lfloor \alpha - \beta \rfloor$:

$$\begin{aligned} \lfloor \alpha - \beta \rfloor &= \lfloor (\lfloor \alpha \rfloor + \{\alpha\}) - (\lfloor \beta \rfloor + \{\beta\}) \rfloor \\ &= \lfloor (\lfloor \alpha \rfloor - \lfloor \beta \rfloor) + (\{\alpha\} - \{\beta\}) \rfloor \\ &= \lfloor \alpha \rfloor - \lfloor \beta \rfloor + \lfloor \{\alpha\} - \{\beta\} \rfloor. \end{aligned}$$

Since $0 \leq \{\cdot\} < 1$, the difference satisfies $-1 < \{\alpha\} - \{\beta\} < 1$. Consequently, the term $\lfloor \{\alpha\} - \{\beta\} \rfloor$ can only take the value 0 (if $\{\alpha\} \geq \{\beta\}$) or -1 (if $\{\alpha\} < \{\beta\}$). Rearranging yields the two possible cases.

■

Example 3.2. Nested Floors. Let n be a positive integer and a be a real number. Prove that

$$\left\lfloor \frac{\lfloor na \rfloor}{n} \right\rfloor = \lfloor a \rfloor.$$

Let $\lfloor na \rfloor = nq + r$ where $0 \leq r < n$. By the definition of the floor, q is an integer. Then $na = nq + r + \{na\}$. Dividing by n:

$$a = q + \frac{r + \{na\}}{n}.$$

We evaluate the RHS of the identity:

$$\left\lfloor \frac{\lfloor na \rfloor}{n} \right\rfloor = \left\lfloor \frac{nq + r}{n} \right\rfloor = \left\lfloor q + \frac{r}{n} \right\rfloor = q + \left\lfloor \frac{r}{n} \right\rfloor.$$

Since $0 \leq r < n$, we have $0 \leq r/n < 1$, so $\lfloor r/n \rfloor = 0$. Thus the LHS is q. Now evaluate $\lfloor a \rfloor$:

$$\lfloor a \rfloor = \left\lfloor q + \frac{r + \{na\}}{n} \right\rfloor = q + \left\lfloor \frac{r + \{na\}}{n} \right\rfloor.$$

Since $0 \leq r \leq n - 1$ and $0 \leq \{na\} < 1$, the numerator satisfies $0 \leq r + \{na\} < n$. Thus the fraction is strictly between 0 and 1, so its floor is 0. Therefore, $\lfloor a \rfloor = q$. The identity holds.

範例

Hermite's Identity

The *The Halving Identity* is a specific instance ($n = 2$) of a more powerful summation property discovered by Charles Hermite. This identity connects the sum of floors of arithmetic progressions to the floor of a scaled multiple.

Theorem 3.6. ***Hermite's Identity.***
For any real number a and positive integer n:

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

定理

Proof

Let $\lfloor na \rfloor = nq + r$ with $0 \leq r < n$. Using the decomposition from the previous example, we write $a = q + \frac{r + \{na\}}{n}$. Consider the general term in the sum, denoted $T_k = \lfloor a + \frac{k}{n} \rfloor$ for $0 \leq k \leq n - 1$. Substituting a:

$$T_k = \left\lfloor q + \frac{r + \{na\} + k}{n} \right\rfloor = q + \left\lfloor \frac{r + k + \{na\}}{n} \right\rfloor.$$

The value of the floor $\lfloor \frac{r+k+\{na\}}{n} \rfloor$ depends on the numerator $N_k = r + k + \{na\}$. Since $0 \leq \{na\} < 1$, the integer part of the fraction is determined by $r + k$.

- If $r + k < n$, then $0 \leq N_k < n + 1$. Since N_k is not an integer (unless $\{na\} = 0$), $\lfloor N_k/n \rfloor = 0$.
- If $r + k \geq n$, since $r < n$ and $k < n$, we have $n \leq r + k < 2n$. Thus $1 \leq N_k/n < 2$, so $\lfloor N_k/n \rfloor = 1$.

We split the summation based on the condition $r + k \geq n \iff k \geq n - r$:

$$\sum_{k=0}^{n-1} T_k = \sum_{k=0}^{n-r-1} (q+0) + \sum_{k=n-r}^{n-1} (q+1).$$

The first sum has $(n-r)$ terms. The second sum has $(n-1)-(n-r)+1 = r$ terms. Total sum $= (n-r)q + r(q+1) = nq - rq + rq + r = nq + r$. By definition, $nq + r = \lfloor na \rfloor$.

■

Example 3.3. Calculating a Large Sum. Evaluate $S = \sum_{n=0}^{502} \lfloor \frac{305n}{503} \rfloor$. Note that 503 is prime, so for $1 \leq n \leq 502$, the term $305n$ is not divisible by 503. Thus $\frac{305n}{503}$ is never an integer. We pair the term for n with the term for $503 - n$:

$$x_n = \frac{305n}{503}, \quad y_n = \frac{305(503-n)}{503} = 305 - x_n.$$

Observe that $x_n + y_n = 305$, which is an integer. Thus $\{x_n\} + \{y_n\} = 0$ (if integer) or 1 (if not). Since x_n is not an integer, $\{x_n\} + \{y_n\} = 1$. By the *The Halving Identity*, we have:

$$\lfloor x_n \rfloor + \lfloor y_n \rfloor = \lfloor x_n + y_n \rfloor - 1 = \lfloor 305 \rfloor - 1 = 304.$$

The sum runs from $n = 0$ to 502. The term for $n = 0$ is 0. The remaining 502 terms can be grouped into 251 pairs.

$$S = 0 + \sum_{n=1}^{502} \lfloor x_n \rfloor = \frac{1}{2} \sum_{n=1}^{502} (\lfloor x_n \rfloor + \lfloor y_n \rfloor) = \frac{1}{2}(502 \times 304) = 251 \times 304 = 76,304.$$

範例

Applications and Diophantine Equations

Example 3.4. Parity of Powers. Prove that the sequence $u_n = \lfloor (1+\sqrt{2})^n \rfloor$ alternates between even and odd integers.
Let $\alpha = 1 + \sqrt{2}$ and $\beta = 1 - \sqrt{2}$. These are roots of $x^2 - 2x - 1 = 0$. Define $U_n = \alpha^n + \beta^n$. The characteristic equation implies $U_{n+2} = 2U_{n+1} + U_n$. Since $U_1 = 2$ and $U_2 = 6$, all U_n are even by induction. Since $-1 < \beta < 0$:

(i) If n is odd, $-1 < \beta^n < 0$. Thus $\lfloor \alpha^n \rfloor = \lfloor U_n - \beta^n \rfloor = U_n$. (Even)

(ii) If n is even, $0 < \beta^n < 1$. Thus $\lfloor \alpha^n \rfloor = \lfloor U_n - \beta^n \rfloor = U_n - 1$. (Odd)

範例

Example 3.5. Inequality of Floors. Prove that for all real numbers α, β:

$$\lfloor 2\alpha \rfloor + \lfloor 2\beta \rfloor \geq \lfloor \alpha \rfloor + \lfloor \alpha + \beta \rfloor + \lfloor \beta \rfloor.$$

Assume without loss of generality that $\{\alpha\} \geq \{\beta\}$. This implies $2\{\alpha\} \geq \{\alpha\} + \{\beta\}$. We expand the LHS:

$$\lfloor 2\alpha \rfloor + \lfloor 2\beta \rfloor = (2\lfloor \alpha \rfloor + \lfloor 2\{\alpha\} \rfloor) + (2\lfloor \beta \rfloor + \lfloor 2\{\beta\} \rfloor).$$

We expand the RHS:

$$\begin{aligned} \text{RHS} &= \lfloor \alpha \rfloor + \lfloor \beta \rfloor + \lfloor (\lfloor \alpha \rfloor + \{\alpha\}) + (\lfloor \beta \rfloor + \{\beta\}) \rfloor \\ &= 2\lfloor \alpha \rfloor + 2\lfloor \beta \rfloor + \lfloor \{\alpha\} + \{\beta\} \rfloor. \end{aligned}$$

Subtracting common integer parts, it suffices to prove:

$$\lfloor 2\{\alpha\} \rfloor + \lfloor 2\{\beta\} \rfloor \geq \lfloor \{\alpha\} + \{\beta\} \rfloor.$$

Since $0 \leq \{\beta\} \leq \{\alpha\} < 1$, the sum $\{\alpha\} + \{\beta\}$ is strictly less than 2. Thus $\lfloor \{\alpha\} + \{\beta\} \rfloor$ is either 0 or 1.

- If $\lfloor \{\alpha\} + \{\beta\} \rfloor = 0$, the inequality holds trivially as the LHS is non-negative.
- If $\lfloor \{\alpha\} + \{\beta\} \rfloor = 1$, then $\{\alpha\} + \{\beta\} \geq 1$. From our assumption $2\{\alpha\} \geq \{\alpha\} + \{\beta\}$, we have $2\{\alpha\} \geq 1$, so $\lfloor 2\{\alpha\} \rfloor \geq 1$. Thus the LHS is at least $1 + 0 = 1$. The inequality holds.

範例

Example 3.6. Square Root Identity. Prove that for any positive integer n, $\lfloor \sqrt{n} + \sqrt{n+1} \rfloor = \lfloor \sqrt{4n+2} \rfloor$.
We bound the expression $X = (\sqrt{n} + \sqrt{n+1})^2 = 2n + 1 + 2\sqrt{n(n+1)}$. Using the arithmetic geometric mean inequality on the term under the square root:

$$n < \sqrt{n(n+1)} < n + 1.$$

Substituting this into the expression for X:

$$2n + 1 + 2n < X < 2n + 1 + 2(n+1) \implies 4n + 1 < X < 4n + 3.$$

Taking the square root of the inequality:

$$\sqrt{4n+1} < \sqrt{n} + \sqrt{n+1} < \sqrt{4n+3}.$$

Let $k = \lfloor \sqrt{4n+1} \rfloor$. Then $k^2 \leq 4n + 1$. Consider the possible values of perfect squares. Any integer m is either even ($2j$) or odd ($2j+1$).

- If $m = 2j$, then $m^2 = 4j^2$, which is a multiple of 4.
- If $m = 2j + 1$, then $m^2 = 4j^2 + 4j + 1 = 4(j^2 + j) + 1$, which is a multiple of 4 plus 1.

Thus, no perfect square is of the form $4N + 2$ or $4N + 3$. This implies that strictly between the integers $4n + 1$ and $4n + 4$, there are no perfect squares. Therefore, the floor of the square root remains constant:

$$\lfloor\sqrt{4n+1}\rfloor = \lfloor\sqrt{4n+2}\rfloor = \lfloor\sqrt{4n+3}\rfloor = k.$$

Since our target value lies strictly in this interval, its floor is also k.

範例

Example 3.7. Equation with No Solution. Prove that the equation $\lfloor x\rfloor + \lfloor 2x\rfloor + \lfloor 4x\rfloor + \lfloor 8x\rfloor + \lfloor 16x\rfloor + \lfloor 32x\rfloor = 12,345$ has no real solution.
Let $f(x)$ be the LHS. Using the bound $\lfloor kx\rfloor \leq kx$, we have:

$$f(x) \leq x(1+2+4+8+16+32) = 63x.$$

If a solution exists, $63x \geq 12,345$, which implies $x \geq 195\frac{20}{21}$. We evaluate $f(x)$ at $x = 196$:

$$f(196) = 196 \times 63 = 12,348.$$

Since $f(x)$ is non-decreasing, the solution must satisfy $195 < x < 196$. Let $x = 195 + y$ where $0 < y < 1$. By integer translation, $\lfloor k(195+y)\rfloor = 195k + \lfloor ky\rfloor$.

$$f(195+y) = 195(63) + f(y) = 12,285 + f(y).$$

We maximize $f(y)$ for $y < 1$:

$$f(y) = \sum_{k=0}^{5} \lfloor 2^k y\rfloor < 0+1+3+7+15+31 = 57.$$

Thus $f(x) < 12,285 + 57 = 12,342$. Since $12,342 < 12,345$, there is no solution.

範例

Example 3.8. Diophantine with Squares. Solve for $x \in \mathbb{R}$: $\lfloor x^2\rfloor = \lfloor x\rfloor^2 + 3$.
Let $\lfloor x\rfloor = n$. Then $n \leq x < n+1$, which implies $n^2 \leq x^2 < (n+1)^2 = n^2 + 2n + 1$. The equation becomes $\lfloor x^2\rfloor = n^2 + 3$. By definition of the floor:

$$n^2 + 3 \leq x^2 < n^2 + 4.$$

For a solution to exist, the interval $[n^2 + 3, n^2 + 4)$ must overlap with $[n^2, n^2 + 2n + 1)$. Specifically, the lower bound of the required interval must be strictly less than the upper bound of the possible

values for x^2:

$$n^2+3 < n^2+2n+1 \implies 2 < 2n \implies n > 1.$$

We test integer values for n:

If $n = 2$. Overlap is $[7,8) \cap [4,9) = [7,8)$. We need $x^2 \in [7,8)$. This corresponds to $x \in [\sqrt{7}, \sqrt{8})$. One choice is $x = \sqrt{7.5} \approx 2.73$. Then $\lfloor x \rfloor = 2$, $\lfloor x \rfloor^2 + 3 = 7$, and $\lfloor 7.5 \rfloor = 7$.

If $n = 3$. Overlap is $[12,13) \cap [9,16) = [12,13)$. Solutions $x \in [\sqrt{12}, \sqrt{13})$.

General solution: For any integer $n \geq 2$, $x \in [\sqrt{n^2+3}, \sqrt{n^2+4})$.

範例

3.1 *Factorisation of Factorials*

The floor function provides the analytic machinery required to determine the prime factorisation of factorials without computing the products explicitly. This result, attributed to Legendre, relates the p-adic valuation of $n!$ to the base-p expansion of n.
We begin by establishing a counting lemma for multiples in a bounded interval.

Lemma 3.1. Counting Multiples Let x be a positive real number and b be a positive integer. The number of positive integers not exceeding x that are divisible by b is $\lfloor x/b \rfloor$.

引理

Proof

The positive multiples of b are $b, 2b, 3b, \ldots, kb, \ldots$. We seek the largest integer k such that $kb \leq x$. This inequality is equivalent to $k \leq \frac{x}{b}$. Since k must be an integer, the maximal such k is $\lfloor x/b \rfloor$.

■

Computations involving higher powers of primes often require nested applications of the floor function.

Lemma 3.2. Iterated Division Let n, a, b be positive integers. Then:

$$\left\lfloor \frac{n}{ab} \right\rfloor = \left\lfloor \frac{\lfloor n/a \rfloor}{b} \right\rfloor.$$

引理

Proof

Let $k = \lfloor \frac{n}{ab} \rfloor$. By definition, $k \leq \frac{n}{ab} < k+1$. Multiplying by b yields

$bk \leq \frac{n}{a} < b(k+1)$. Since bk is an integer, it satisfies $bk \leq \lfloor \frac{n}{a} \rfloor$. However, the strict inequality $\frac{n}{a} < bk + b$ implies $\lfloor \frac{n}{a} \rfloor < bk + b$. Dividing by b:

$$k \leq \frac{\lfloor n/a \rfloor}{b} < k + 1.$$

Thus, the floor of the middle term is k.

■

Remark.

This lemma is particularly useful for calculation. To find $\lfloor n/p^{k+1} \rfloor$, one simply divides $\lfloor n/p^k \rfloor$ by p and takes the integer part.

Legendre's Formula

We now derive the formula for the exponent of a prime p in the standard factorisation of $n!$. We denote this exponent by $v_p(n!)$.

Theorem 3.7. ***Legendre's Formula.***
Let n be a positive integer and p be a prime. The exponent of p in the prime factorisation of $n!$ is:

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

定理

Note

The sum is finite since $\lfloor n/p^k \rfloor = 0$ once $p^k > n$.

Proof

Let the standard factorisation of $n!$ be $\prod_{p \leq n} p^{h_p}$. The exponent h_p is the sum of the valuations of the factors $1, 2, \ldots, n$:

$$h_p = \sum_{j=1}^{n} v_p(j).$$

Instead of summing term-by-term, we count the contribution of each power of p across the entire set $\{1, \ldots, n\}$. Let c_k be the number of integers in $\{1, \ldots, n\}$ divisible by p^k. By the Counting Multiples lemma, $c_k = \lfloor n/p^k \rfloor$. Let d_k be the number of integers in $\{1, \ldots, n\}$ exactly divisible by p^k (i.e., $v_p(j) = k$). By inclusion-exclusion, an integer is divisible by p^k exactly if it is divisible by p^k but not p^{k+1}. Thus, $d_k = c_k - c_{k+1}$. The total exponent is:

$$h_p = \sum_{k=1}^{\infty} k \cdot d_k = 1(c_1 - c_2) + 2(c_2 - c_3) + 3(c_3 - c_4) + \ldots$$

This is a telescoping sum. Regrouping terms by c_k:

$$h_p = c_1 + (2-1)c_2 + (3-2)c_3 + \cdots = \sum_{k=1}^{\infty} c_k = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

■

Example 3.9. Exponent of a Prime. Find the exponent of 7 in the factorisation of 2000!.
We apply Legendre's formula with $n = 2000, p = 7$.

$$v_7(2000!) = \left\lfloor \frac{2000}{7} \right\rfloor + \left\lfloor \frac{2000}{49} \right\rfloor + \left\lfloor \frac{2000}{343} \right\rfloor + \left\lfloor \frac{2000}{2401} \right\rfloor.$$

The last term is 0 since $2401 > 2000$. Using *lemma 3.2* for sequential calculation:

$$\begin{aligned} \lfloor 2000/7 \rfloor &= 285 \\ \lfloor 285/7 \rfloor &= 40 \\ \lfloor 40/7 \rfloor &= 5 \end{aligned}$$

Summing these values: $285 + 40 + 5 = 330$.

範例

Example 3.10. Trailing Zeros. Determine the number of zeros at the end of the decimal representation of 1000!.
A trailing zero is produced by a factor of $10 = 2 \times 5$. The number of zeros is determined by the number of pairs of prime factors $(2, 5)$. Since $2 < 5$, factors of 2 are much more abundant than factors of 5. Thus, $v_5(1000!) < v_2(1000!)$, and the number of zeros is simply $v_5(1000!)$.

$$v_5(1000!) = \sum_{k=1}^{4} \left\lfloor \frac{1000}{5^k} \right\rfloor.$$

Calculation:

$$\begin{aligned} \lfloor 1000/5 \rfloor &= 200 \\ \lfloor 200/5 \rfloor &= 40 \\ \lfloor 40/5 \rfloor &= 8 \\ \lfloor 8/5 \rfloor &= 1 \end{aligned}$$

Total: $200 + 40 + 8 + 1 = 249$. There are 249 trailing zeros.

範例

Example 3.11. Legendre's Formula and Base Expansion. Let $s_p(n)$ denote the sum of the digits of n when written in base p. Prove

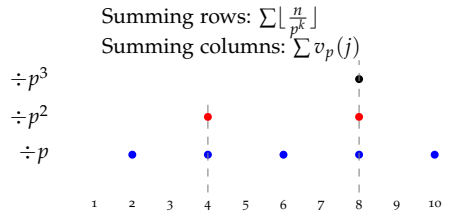


Figure 3.2: Visualising Legendre's Formula for $n = 10, p = 2$. Each dot represents a factor of p. The number 8 contributes 3 dots (vertical), while the row for p^2 counts multiples of 4 (horizontal).

that:

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

Let the base-p expansion of n be $n = \sum_{i=0}^{m} a_i p^i$, where $0 \leq a_i < p$. Consider the term $\lfloor n/p^k \rfloor$. Dividing the expansion by p^k shifts the digits:

$$\left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{i=k}^{m} a_i p^{i-k}.$$

Summing over $k \geq 1$:

$$v_p(n!) = \sum_{k=1}^{m} \sum_{i=k}^{m} a_i p^{i-k}.$$

We swap the order of summation. For a fixed coefficient a_i, it appears in the sum for $k = 1, 2, \ldots, i$.

$$v_p(n!) = \sum_{i=1}^{m} a_i \left(\sum_{k=1}^{i} p^{i-k} \right) = \sum_{i=1}^{m} a_i (p^{i-1} + \cdots + 1).$$

Using the geometric series formula:

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

Note that the $i = 0$ term vanishes in the sum on the left but is included here for completeness (as $p^0 - 1 = 0$). Recognising the sums: $\sum a_i p^i = n$ and $\sum a_i = s_p(n)$. Thus, $v_p(n!) = \frac{n - s_p(n)}{p-1}$.

範例

Example 3.12. Inverse Legendre Problem. Does there exist a positive integer n such that $n!$ ends in exactly 153 trailing zeros?
We seek n such that $v_5(n!) = 153$. Approximating using the formula from the previous example: $v_5(n!) \approx \frac{n}{4}$. Estimate $n \approx 4 \times 153 = 612$. We test $n = 615$ (a multiple of 5):

$$v_5(615!) = 123 + 24 + 4 + 0 = 151.$$

We need 2 more factors of 5. Moving to the next multiple of 5, $n = 620$: $v_5(620!) = v_5(615!) + v_5(616 \times 617 \times 618 \times 619 \times 620)$. The only multiple of 5 is 620. Since $620 = 5 \times 124$, it contributes one factor of 5. Thus $v_5(620!) = 151 + 1 = 152$. Next multiple $n = 625$: Since $625 = 5^4$, this number contributes 4 factors of 5. $v_5(625!) = 152 + 4 = 156$. The function $v_5(n!)$ jumps from 152 to 156. It never takes the value 153. Thus, no such integer n exists.

範例

Divisibility Applications

Legendre's formula provides a robust method for proving divisibility relations involving factorials, often reducing the problem to checking an inequality of floor functions.

Example 3.13. Divisibility of Product Sequences. Prove that 2^n divides the product $(n+1)(n+2)\dots(2n)$.
We can rewrite the product as:

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

We determine the exponent of 2 in the prime factorisation of P:

$$v_2(P) = v_2((2n)!) - v_2(n!).$$

Using Legendre's formula:

$$v_2((2n)!) = \sum_{k=1}^{\infty} \left\lfloor \frac{2n}{2^k} \right\rfloor = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^{k-1}} \right\rfloor = n + \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor.$$

The infinite sum on the right is exactly $v_2(n!)$. Therefore:

$$v_2(P) = (n + v_2(n!)) - v_2(n!) = n.$$

Since the exponent of 2 in P is exactly n, 2^n divides P.

範例

Example 3.14. Factorial Divisibility Condition. Let m, n be positive integers. Prove that $(2m)!(2n)!$ is divisible by $m!n!(m+n)!$.
We must show that for every prime p, the valuation of the numerator is at least that of the denominator:

$$v_p((2m)!(2n)!) \geq v_p(m!n!(m+n)!).$$

Applying Legendre's formula, this inequality is equivalent to:

$$\sum_{k=1}^{\infty} \left(\left\lfloor \frac{2m}{p^k} \right\rfloor + \left\lfloor \frac{2n}{p^k} \right\rfloor \right) \geq \sum_{k=1}^{\infty} \left(\left\lfloor \frac{m}{p^k} \right\rfloor + \left\lfloor \frac{n}{p^k} \right\rfloor + \left\lfloor \frac{m+n}{p^k} \right\rfloor \right).$$

It suffices to prove the inequality term-wise for each k. Let $\alpha = m/p^k$ and $\beta = n/p^k$. We require:

$$\lfloor 2\alpha \rfloor + \lfloor 2\beta \rfloor \geq \lfloor \alpha \rfloor + \lfloor \beta \rfloor + \lfloor \alpha + \beta \rfloor.$$

This is precisely the inequality established in the previous section (Example: Inequality of Floors). Since the inequality holds for every term in the summation, the divisibility holds.

範例

3.2 *Arithmetic Functions*

Many properties of integers depend on their divisors. We now introduce two fundamental arithmetic functions: the divisor counting function $d(n)$ and the divisor sum function $\sigma(n)$. These functions are multiplicative, meaning their value for a product of coprime integers is the product of their values.

Definition 3.2. ***Divisor Functions.***
Let n be a positive integer. The **divisor counting function**, denoted $d(n)$, is the number of positive divisors of n:

$$d(n) = \sum_{d|n} 1.$$

The **divisor sum function**, denoted $\sigma(n)$, is the sum of the positive divisors of n:

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

定義

Note

The trivial divisors 1 and n are included in these sums.

The Divisor Counting Function $d(n)$

To compute $d(n)$, we rely on the standard prime factorisation. Every divisor is built from the prime factors of n.

Theorem 3.8. ***Formula for*** $d(n)$**.**
Let the standard factorisation of n be $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Then:

$$d(n) = (a_1 + 1)(a_2 + 1) \dots (a_k + 1) = \prod_{i=1}^{k} (a_i + 1).$$

定理

Proof

Any divisor d of n must be of the form $d = p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}$, where $0 \leq x_i \leq a_i$ for each i. For each prime p_i, there are $a_i + 1$ choices for the exponent x_i (specifically, $\{0, 1, \dots, a_i\}$). By the multiplication principle, the total number of distinct divisors is the product of the number of choices for each exponent.

■

Corollary 3.1. *Multiplicativity of* $d(n)$. If m and n are coprime, then $d(mn) =$

$d(m)d(n)$.

推論

Proof

Since $(m,n) = 1$, they share no prime factors. The prime factorisation of mn is simply the concatenation of the factorisations of m and n. The formula in the theorem splits over the distinct sets of primes. ■

Example 3.15. Smallest Integer with Fixed Divisor Count. Find the smallest positive integer n such that $d(n) = 12$.
Let $n = p_1^{a_1} p_2^{a_2} \dots$. Then $\prod(a_i + 1) = 12$. We factor 12 in all possible ways and assign the largest exponents to the smallest primes to minimise n. Possible factorisations of 12:
1. $12 \implies a_1 = 11$. $n = 2^{11} = 2048$.
2. $6 \times 2 \implies a_1 = 5, a_2 = 1$. $n = 2^5 \cdot 3^1 = 32 \cdot 3 = 96$.
3. $4 \times 3 \implies a_1 = 3, a_2 = 2$. $n = 2^3 \cdot 3^2 = 8 \cdot 9 = 72$.
4. $3 \times 2 \times 2 \implies a_1 = 2, a_2 = 1, a_3 = 1$. $n = 2^2 \cdot 3^1 \cdot 5^1 = 4 \cdot 3 \cdot 5 = 60$.

The smallest such integer is 60.

範例

Example 3.16. Product of Proper Divisors. Prove that if a positive integer n is equal to the product of all its proper divisors, then $n = p^3$ or $n = p_1 p_2$ (where p, p_1, p_2 are primes).
Let P be the product of all positive divisors of n. We can pair divisors d and n/d:

$$P^2 = \left(\prod_{d|n} d\right)\left(\prod_{d|n} \frac{n}{d}\right) = \prod_{d|n}\left(d \cdot \frac{n}{d}\right) = \prod_{d|n} n = n^{d(n)}.$$

Thus $P = n^{d(n)/2}$. The product of proper divisors excludes n. So the product is $P/n = n^{d(n)/2-1}$. We are given that this product equals n. Thus:

$$n^{d(n)/2-1} = n^1 \implies \frac{d(n)}{2} - 1 = 1 \implies d(n) = 4.$$

We solve $d(n) = 4$. The possible factorisations of 4 are:
1. $4 \implies a_1 = 3$. Then $n = p^3$.
2. $2 \times 2 \implies a_1 = 1, a_2 = 1$. Then $n = p_1 p_2$.

範例

Example 3.17. Existence of Solutions. Prove that for any $k \geq 1$, there exists an integer n such that $d(n) = k$.
Simply choose $n = 2^{k-1}$. Then $d(n) = (k-1) + 1 = k$.

範例

The Divisor Sum Function $\sigma(n)$

The sum of divisors also admits a closed form derived from the geometric series.

Theorem 3.9. ***Formula for*** $\sigma(n)$**.**
Let $n = p_1^{a_1} \dots p_k^{a_k}$. Then:

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1} = \prod_{i=1}^{k} (1 + p_i + p_i^2 + \cdots + p_i^{a_i}).$$

定理

Proof

Consider the expansion of the product:

$$\left(\sum_{j=0}^{a_1} p_1^j \right) \left(\sum_{j=0}^{a_2} p_2^j \right) \cdots \left(\sum_{j=0}^{a_k} p_k^j \right).$$

A typical term in the expanded sum is of the form $p_1^{x_1} p_2^{x_2} \dots p_k^{x_k}$ with $0 \leq x_i \leq a_i$. By the fundamental theorem of arithmetic, these terms correspond exactly to the divisors of n, with each divisor appearing exactly once. Summing the geometric series for each prime factor yields the formula.

■

Corollary 3.2. *Multiplicativity of* $\sigma(n)$. If $(m, n) = 1$, then $\sigma(mn) = \sigma(m)\sigma(n)$.

推論

Example 3.18. Solving for $\sigma(n)$. Find a number of the form $n = 2^m \cdot 3^k$ such that $\sigma(n) = 403$.
Using the formula:

$$\sigma(n) = \frac{2^{m+1} - 1}{2 - 1} \cdot \frac{3^{k+1} - 1}{3 - 1} = (2^{m+1} - 1) \frac{3^{k+1} - 1}{2} = 403.$$

Thus $(2^{m+1} - 1)(3^{k+1} - 1) = 806$. Factorising $806 = 2 \times 13 \times 31$. The term $2^{m+1} - 1$ must be a divisor of 806 of the form $2^x - 1$. The divisors of 806 are $1, 2, 13, 26, 31, 62, 403, 806$. Numbers of the form $2^x - 1$:
· $x = 1 \implies 1$ (Trivial, $m = 0$, but $3^{k+1} - 1 = 806$ has no solution).
· $x = 4 \implies 15$ (Not a divisor).
· $x = 5 \implies 31$. This is a divisor.
If $2^{m+1} - 1 = 31$, then $m + 1 = 5 \implies m = 4$. The remaining factor is $(3^{k+1} - 1) = 806/31 = 26$. $3^{k+1} = 27 \implies k + 1 = 3 \implies k = 2$.

Thus $n = 2^4 \cdot 3^2 = 16 \cdot 9 = 144$.

範例

Example 3.19. Perfect Squares in Divisor Sums. Find all primes p such that $\sigma(p^4)$ is a perfect square.
We have $\sigma(p^4) = 1 + p + p^2 + p^3 + p^4 = m^2$ for some integer m. Multiply by 4 to complete the square:

$$4m^2 = 4p^4 + 4p^3 + 4p^2 + 4p + 4.$$

We bound this expression between consecutive squares. Consider $(2p^2 + p)^2 = 4p^4 + 4p^3 + p^2$. Comparing coefficients: $4m^2 > (2p^2 + p)^2$ because $3p^2 + 4p + 4 > 0$. Now consider $(2p^2 + p + 2)^2 = (2p^2 + p)^2 + 4(2p^2 + p) + 4 = 4p^4 + 4p^3 + 9p^2 + 4p + 4$. Comparing with $4m^2$, we see $4m^2 < (2p^2 + p + 2)^2$ because $4p^2 < 9p^2$. Thus, the only possible integer square between them is $(2p^2 + p + 1)^2$.

$$4m^2 = (2p^2 + p + 1)^2 = (2p^2 + p)^2 + 2(2p^2 + p) + 1 = 4p^4 + 4p^3 + 5p^2 + 2p + 1.$$

Equating the two expressions for $4m^2$:

$$4p^4 + 4p^3 + 4p^2 + 4p + 4 = 4p^4 + 4p^3 + 5p^2 + 2p + 1.$$

Simplifying:

$$4p^2 + 4p + 4 = 5p^2 + 2p + 1 \implies p^2 - 2p - 3 = 0.$$

Factorising: $(p - 3)(p + 1) = 0$. Since p is prime, $p = 3$. Indeed, $\sigma(3^4) = 1 + 3 + 9 + 27 + 81 = 121 = 11^2$.

範例

We conclude with a structural property of numbers whose divisor sum is prime.

Proposition 3.3. ***Structure of Pre-images of Primes.***
If $\sigma(m)$ is a prime number greater than 3, then m must be of the form p^{2k} (a perfect square of a prime), where $2k + 1$ does not divide $p - 1$.

命題

We proceed by eliminating forms of m that force $\sigma(m)$ to be composite.

m must be a prime power.

Suppose m has at least two distinct prime factors. We can write $m = ab$ with $\gcd(a, b) = 1$ and $a, b > 1$. By the multiplicative property of σ, we have $\sigma(m) = \sigma(a)\sigma(b)$. Since $a, b > 1$, the sums of their divisors satisfy $\sigma(a) > 1$ and $\sigma(b) > 1$. Thus $\sigma(m)$ is the product of

two integers greater than 1, making it composite. Therefore, m must be a prime power, say $m = p^e$.

証明終

The exponent e must be even.

Suppose e is odd. Let $e = 2k+1$ for $k \geq 0$. We can factor the sum of divisors:

$$\sigma(p^{2k+1}) = 1 + p + \cdots + p^{2k+1} = (1+p)(1+p^2+p^4+\cdots+p^{2k}).$$

If $k = 0$, $m = p$, so $\sigma(m) = p+1$. For this to be a prime > 3, $p+1$ must be odd, implying p is even. But $p = 2 \implies \sigma(2) = 3$, which is not greater than 3. If $k \geq 1$, both factors $(1+p)$ and the remaining sum are greater than 1. Thus $\sigma(p^e)$ is composite. Therefore, e must be even. Let $m = p^{2k}$ with $k \geq 1$.

証明終

The condition on $p-1$.

We prove the contrapositive: if $(2k+1) \mid (p-1)$, then $\sigma(m)$ is composite. Assume $p \equiv 1 \pmod{2k+1}$. Evaluating the sum modulo $2k+1$:

$$\sigma(p^{2k}) = \sum_{i=0}^{2k} p^i \equiv \sum_{i=0}^{2k} 1^i \equiv \underbrace{1+1+\cdots+1}_{2k+1 \text{ times}} \equiv 0 \pmod{2k+1}.$$

Thus $(2k+1)$ divides $\sigma(p^{2k})$. Since $p \geq 2$ and $k \geq 1$, clearly $\sigma(p^{2k}) > 2k+1$. Therefore, $\sigma(m)$ has a non-trivial factor $2k+1$, so it is composite. Consequently, for $\sigma(m)$ to be prime, we must have $(2k+1) \nmid (p-1)$.

証明終

3.3 *Exercises*

1. **Floor Identities.** Let $n > 2$ be an integer. Prove that:
$$\left\lfloor \frac{n(n+1)}{4n-2} \right\rfloor = \left\lfloor \frac{n+1}{4} \right\rfloor.$$

2. **Summation with Floors.** For any positive integer n, calculate the sum:
$$S_n = \sum_{k=0}^{n} \left\lfloor \frac{n+2^k}{2^{k+1}} \right\rfloor.$$

3. **Solving for Real Variables.** Find a positive real number x satisfying the equation:
$$\lfloor x \rfloor^2 = x\{x\}.$$

4. **Floor Inequality.** Let n be a positive integer and x be a real number. Verify that:
$$\lfloor nx \rfloor \geq \lfloor x \rfloor + \left\lfloor \frac{2x}{2} \right\rfloor + \cdots + \left\lfloor \frac{nx}{n} \right\rfloor.$$

5. **Primality of a Floor Sum.** Let $f(n) = \sum_{k=1}^{n} \lfloor k^2/3 \rfloor$. Prove that in the sequence $f(n)$, the only values that are prime numbers are $f(5) = 17$ and $f(6) = 29$.

6. **Infinite Floor Series.** Let $t > 1$ be an integer and x be a real number. Prove that:
$$\sum_{k=0}^{\infty} \left(\left\lfloor \frac{x + t^k}{t^{k+1}} \right\rfloor + \cdots + \left\lfloor \frac{x + (t-1)t^k}{t^{k+1}} \right\rfloor \right)$$
equals either $\lfloor x \rfloor$ or $\lfloor x \rfloor + 1$.

7. **Condition for Inequality.** Let m, n be positive integers and α, β be real numbers. Prove that the inequality
$$\lfloor (m+n)\alpha \rfloor + \lfloor (m+n)\beta \rfloor \geq \lfloor m\alpha \rfloor + \lfloor m\beta \rfloor + \lfloor n\alpha + n\beta \rfloor$$
holds for all α, β if and only if $m = n$.

8. **Decimal Expansion Bounds.** Determine the digit immediately before and the digit immediately after the decimal point of $(\sqrt{2} + \sqrt{3})^{1999}$.

9. **Recursive Sequence.** Define $G(0) = 0$ and $G(n) = n - G(G(n-1))$ for $n \geq 1$. Prove that $G(n) = \lfloor (n+1)\alpha \rfloor$, where $\alpha = \frac{\sqrt{5}-1}{2}$ (the inverse of the Golden Ratio).

10. **Factorials and Valuations.**
    (a) Find the exponent of 7 in the standard factorisation of 300!.
    (b) Determine the standard prime factorisation of 30!.
    (c) Determine the number of trailing zeros in the decimal representation of 2000!.

11. **Combinatorial Divisibility.**
    (a) Prove that $\binom{2n}{n}^2$ is divisible by 4 for all $n \geq 1$.
    (b) Prove that $2^n \mid \binom{2^n-1}{n}$ but $2^{n+1} \nmid \binom{2^n-1}{n}$.
    (c) Prove that $\binom{2n}{n}$ divides $\operatorname{lcm}(1, 2, \ldots, 2n)$.

12. **Powers of 2 dividing Factorials.** Prove that $2^{n-1} \mid n!$ if and only if n is a power of 2.

13. **GCD of Binomial Coefficients.** Find the greatest common divisor of the set of binomial coefficients:
$$\left\{ \binom{2n}{1}, \binom{2n}{3}, \ldots, \binom{2n}{2n-1} \right\}.$$

14. Divisor Function Calculations.

(a) Compute $d(1125)$.

(b) Find the smallest positive integer n such that $d(n) = 8$. Do the same for $d(n) = 10$.

(c) Find a number less than 10,000 that has exactly 60 divisors.

15. Product of Divisors. Let $P(n) = \prod_{d|n} d$. Prove that if $P(x) = P(y)$ for positive integers x, y, then $x = y$.

16. Sum of Divisors.

(a) Compute $\sigma(232848)$.

(b) Find all n such that $\sigma(n)$ is odd.

(c) Find all n such that $\sigma(n)$ is a power of 2.

17. Generalised Divisor Sums. Let $\sigma_k(n) = \sum_{d|n} d^k$. Prove the formula:

$$\sigma_k(n) = \prod_{i=1}^{r} \frac{p_i^{(a_i+1)k} - 1}{p_i^k - 1},$$

where $n = \prod p_i^{a_i}$.

18. Average Order of Sigma. Let $f(n) = \sum_{k=1}^{n} \sigma(k)$. Prove that for $n \geq 4$:

$$f(n) > \frac{25}{36} n(n+1).$$

4
Perfect and Amicable Numbers

Having established the properties of the divisor functions $d(n)$ and $\sigma(n)$, we turn our attention to integers that possess specific structural relationships with their divisors. The study of these numbers dates back to Pythagorean mysticism, yet their complete characterisation remains an open problem in modern number theory.

4.1 Perfect Numbers

The most elementary relationship between a number and its divisors occurs when the sum of the proper divisors equals the number itself.

Definition 4.1. ***Perfect Number.***
A positive integer n is called a **perfect number** if it is equal to the sum of its positive divisors excluding itself. Equivalently, n is perfect if and only if $\sigma(n) = 2n$.

定義

Example 4.1. Small Perfect Numbers.

- For $n = 6$, the divisors are $\{1, 2, 3, 6\}$. The sum is $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2(6)$. Thus, 6 is perfect.
- For $n = 28$, the divisors are $\{1, 2, 4, 7, 14, 28\}$. The sum is $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2(28)$. Thus, 28 is perfect.

範例

Even Perfect Numbers

The history of perfect numbers is inextricably linked to Mersenne primes. Euclid proved that Mersenne primes generate even perfect numbers, and two millennia later, Euler proved that all even perfect numbers arise this way.

Theorem 4.1. ***Euclid's Condition for Perfect Numbers.***
If $2^p - 1$ is a prime number, then $n = 2^{p-1}(2^p - 1)$ is a perfect number.

定理

Proof

Let $q = 2^p - 1$. Since q is prime, $\sigma(q) = q + 1 = 2^p$. Because q is odd, $(2^{p-1}, q) = 1$. Using the multiplicative property of σ:

$$\begin{aligned}\sigma(n) &= \sigma(2^{p-1}q) \\ &= \sigma(2^{p-1})\sigma(q).\end{aligned}$$

Using the formula for $\sigma(p^k)$, we have $\sigma(2^{p-1}) = \frac{2^{(p-1)+1}-1}{2-1} = 2^p - 1 = q$. Substituting these values:

$$\sigma(n) = q \cdot 2^p = (2^p - 1)2^p = 2 \cdot [2^{p-1}(2^p - 1)] = 2n.$$

Therefore, n is a perfect number.

■

Theorem 4.2. ***Euler's Converse.***
If n is an even perfect number, then n must be of the form $2^{p-1}(2^p - 1)$, where $2^p - 1$ is a prime number.

定理

Proof

Let n be an even perfect number. We factor out the powers of 2 from the standard factorisation:

$$n = 2^k u,$$

where $k \geq 1$ (since n is even) and u is odd. Since $\sigma(n) = 2n$, we have:

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

By the multiplicativity of σ and the fact that $(2^k, u) = 1$:

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

We rearrange this to express $\sigma(u)$ in terms of u:

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

Since $\sigma(u)$ is an integer, the fraction $D = \frac{u}{2^{k+1}-1}$ must be an integer. Thus, $2^{k+1} - 1$ is a divisor of u. Write

$$u = (2^{k+1} - 1)t$$

for some integer $t \geq 1$. Then

$$\sigma(u) = u + \frac{u}{2^{k+1} - 1} = u + t.$$

So the sum of the proper divisors of u is t. Since t divides u, both 1 and t are proper divisors of u when $t > 1$, giving a sum at least $1 + t$, which is impossible. Hence $t = 1$. Then $u = 2^{k+1} - 1$ and $\sigma(u) = u + 1$, so u is prime. Thus $n = 2^k(2^{k+1} - 1)$ where $2^{k+1} - 1$ is prime. By the properties of Mersenne primes, if $2^{k+1} - 1$ is prime, the exponent $k + 1$ must be prime. Let $p = k + 1$. Then $n = 2^{p-1}(2^p - 1)$, as required.

■

Properties of Perfect Numbers

The structure imposed by $\sigma(n) = 2n$ leads to several elegant arithmetic properties.

Example 4.2. Reciprocal Sum of Divisors. Prove that a positive integer n is perfect if and only if the sum of the reciprocals of its positive divisors is 2.

$$\sum_{d|n} \frac{1}{d} = 2.$$

We expand the sum. As d iterates through all divisors of n, the term n/d also iterates through all divisors of n.

$$\sum_{d|n} \frac{1}{d} = \sum_{d|n} \frac{1}{n/d} = \frac{1}{n} \sum_{d|n} d = \frac{\sigma(n)}{n}.$$

The condition $\sum \frac{1}{d} = 2$ is equivalent to $\frac{\sigma(n)}{n} = 2$, or $\sigma(n) = 2n$, which is the definition of a perfect number.

範例

Example 4.3. Squarefree Perfect Numbers. Prove that if a perfect number n is squarefree, then $n = 6$.
Let $n = p_1 p_2 \dots p_k$ be a product of distinct primes with $p_1 < p_2 < \cdots < p_k$. Then $\sigma(n) = \prod_{i=1}^{k}(p_i + 1)$. The perfect condition $\sigma(n) = 2n$ becomes:

$$(p_1 + 1)(p_2 + 1) \dots (p_k + 1) = 2p_1 p_2 \dots p_k.$$

We analyse the cases for k:

Case $k = 1$. $p_1 + 1 = 2p_1 \implies p_1 = 1$, which is impossible.

Case $k = 2$. We have $(p_1 + 1)(p_2 + 1) = 2p_1 p_2$. If n is odd, both p_1, p_2 are odd, so $p_1 + 1$ and $p_2 + 1$ are even. Thus $4 \mid \sigma(n) \implies 4 \mid 2n \implies 2 \mid n$. This contradicts n being odd. Thus n must be even, so $p_1 = 2$. The equation becomes $3(p_2 + 1) = 4p_2 \implies 3p_2 + 3 = 4p_2 \implies p_2 = 3$. This yields $n = 2 \times 3 = 6$.

Case $k \geq 3$. As shown above, n must be even, so $p_1 = 2$. The equation implies $3\prod_{i=2}^{k}(p_i+1) = 4\prod_{i=2}^{k} p_i$. This simplifies to $\frac{3}{2}\prod_{i=2}^{k}\left(1+\frac{1}{p_i}\right) = 2$. However, for $k = 3$, the minimum possible primes are 2, 3, 5. LHS $= \frac{3}{2}\left(1+\frac{1}{3}\right)\left(1+\frac{1}{5}\right) = \frac{3}{2}\cdot\frac{4}{3}\cdot\frac{6}{5} = \frac{12}{5} = 2.4 > 2$. Adding more primes only increases the product, so there are no solutions for $k \geq 3$.

Thus, $n = 6$ is the unique squarefree perfect number.

範例

Example 4.4. Triangular Structure. Prove that every even perfect number is a triangular number.
Recall that the k-th triangular number is $T_k = \frac{k(k+1)}{2}$. Let $n = 2^{p-1}(2^p-1)$ be an even perfect number. Let $k = 2^p - 1$. Then:

$$T_k = \frac{(2^p-1)((2^p-1)+1)}{2} = \frac{(2^p-1)2^p}{2} = (2^p-1)2^{p-1} = n.$$

Thus n is the (2^p-1)-th triangular number. For example, $6 = T_3$ and $28 = T_7$.

範例

Example 4.5. Last Digits of Even Perfect Numbers. Prove that every even perfect number ends in 6 or 8.
Let n be an even perfect number. Then $n = 2^{p-1}(2^p-1)$, where p is a prime and $2^p - 1$ is also prime. We observe that for any integer $k \geq 1$, powers of 16 always end in 6. Thus, we can write $16^k = 10m+6$ for some positive integer m. We consider the possible forms of the prime p:

1. If $p = 2$, then $n = 2^1(2^2-1) = 2(3) = 6$. This ends in 6.
2. If $p > 2$, p must be odd. Thus p is of the form $4k+1$ or $4k+3$.

Case 1: $p = 4k+1$ for some integer $k \geq 1$. Then $n = 2^{4k}(2^{4k+1}-1) = 16^k(2\cdot 16^k - 1)$. Substituting $16^k = 10m+6$:

$$\begin{aligned} n &= (10m+6)(2(10m+6)-1) \\ &= (10m+6)(20m+12-1) \\ &= (10m+6)(20m+11) \\ &= 200m^2 + 110m + 120m + 66 \\ &= 10(20m^2+23m+6)+6. \end{aligned}$$

Since $10(20m^2+23m+6)$ is a multiple of 10, adding 6 results in a number ending in 6.

Case 2: $p = 4k+3$ for some integer $k \geq 0$. Then $n = 2^{4k+2}(2^{4k+3} - 1) = 2^2 \cdot 2^{4k}(2^3 \cdot 2^{4k} - 1) = 4 \cdot 16^k(8 \cdot 16^k - 1)$. Substituting $16^k = 10m + 6$:

$$\begin{aligned} n &= 4(10m+6)(8(10m+6)-1) \\ &= (40m+24)(80m+48-1) \\ &= (40m+24)(80m+47) \\ &= 3200m^2 + 1880m + 1920m + 1128 \\ &= 10(320m^2 + 380m + 112) + 8. \end{aligned}$$

Since the first term is a multiple of 10, adding 8 results in a number ending in 8.

In all cases, n ends in either 6 or 8.

範例

Note

If $k = 0$, then $p = 3$, and $n = 2^2(7) = 28$, which ends in 8 and fits this form.

Example 4.6. Product of Divisors of Perfect Numbers. Let n be an even perfect number generated by the prime p. Prove that the product of the positive divisors of n is n^p.
Let $P(n) = \prod_{d|n} d$. From the properties of the divisor function, $P(n) = n^{d(n)/2}$. For $n = 2^{p-1}(2^p - 1)$, the prime factors are 2 (with exponent $p-1$) and $q = 2^p - 1$ (with exponent 1). Using the formula for $d(n)$:

$$d(n) = ((p-1)+1)(1+1) = p \cdot 2 = 2p.$$

Substituting this into the product formula:

$$P(n) = n^{2p/2} = n^p.$$

範例

4.2 *Amicable Numbers*

While perfect numbers relate to themselves, amicable numbers relate to each other. They occur in pairs where the sum of the proper divisors of one number equals the other.

Definition 4.2. ***Amicable Numbers.***
Two positive integers m and n form an **amicable pair** if:

$$\sigma(m) - m = n \quad \text{and} \quad \sigma(n) - n = m.$$

Equivalently, $\sigma(m) = \sigma(n) = m + n$.

定義

Example 4.7. The Classical Pair. The smallest amicable pair is $(220, 284)$.

- $220 = 2^2 \cdot 5 \cdot 11$. $\sigma(220) = (1+2+4)(1+5)(1+11) = 7 \cdot 6 \cdot 12 = 504$. Sum of proper divisors: $504 - 220 = 284$.
- $284 = 2^2 \cdot 71$. $\sigma(284) = (1+2+4)(1+71) = 7 \cdot 72 = 504$. Sum of proper divisors: $504 - 284 = 220$.

範例

In the 9th century, Thabit ibn Qurra discovered a rule to generate amicable pairs, similar to Euclid's rule for perfect numbers.

Theorem 4.3. ***Thabit ibn Qurra's Theorem.***
Let $e \geq 2$ be an integer. Define:

$$p = 3 \cdot 2^{e-1} - 1, \quad q = 3 \cdot 2^e - 1, \quad r = 9 \cdot 2^{2e-1} - 1.$$

If p, q, and r are all prime numbers, then $M = 2^e pq$ and $N = 2^e r$ form an amicable pair.

定理

Proof

We compute $\sigma(M)$ and $\sigma(N)$. Note that p, q, r are distinct odd primes (since $e \geq 2$).

$$\begin{aligned}\sigma(M) &= \sigma(2^e)\sigma(p)\sigma(q) \\ &= (2^{e+1} - 1)(p+1)(q+1) \\ &= (2^{e+1} - 1)(3 \cdot 2^{e-1})(3 \cdot 2^e) \\ &= (2^{e+1} - 1)(9 \cdot 2^{2e-1}).\end{aligned}$$

Similarly for N:

$$\begin{aligned}\sigma(N) &= \sigma(2^e)\sigma(r) \\ &= (2^{e+1} - 1)(r+1) \\ &= (2^{e+1} - 1)(9 \cdot 2^{2e-1}).\end{aligned}$$

Thus $\sigma(M) = \sigma(N)$. We must now show this common sum equals

$M + N$.

$$\begin{aligned} M + N &= 2^e pq + 2^e r \\ &= 2^e(pq + r) \\ &= 2^e[(3 \cdot 2^{e-1} - 1)(3 \cdot 2^e - 1) + (9 \cdot 2^{2e-1} - 1)] \\ &= 2^e[(9 \cdot 2^{2e-1} - 3 \cdot 2^{e-1} - 3 \cdot 2^e + 1) + 9 \cdot 2^{2e-1} - 1] \\ &= 2^e[18 \cdot 2^{2e-1} - 3 \cdot 2^{e-1}(1 + 2)] \\ &= 2^e[9 \cdot 2^{2e} - 9 \cdot 2^{e-1}] \\ &= 9 \cdot 2^{2e-1}(2^{e+1} - 1). \end{aligned}$$

This matches the value of $\sigma(M)$ derived above. Thus M and N are amicable.

■

Note

For $e = 2$, we obtain primes $p = 5, q = 11, r = 71$, yielding the pair $(220, 284)$.

Properties and Non-Existence Results

Example 4.8. Reciprocal Sums for an Amicable Pair. Prove that if m and n are amicable, then

$$\left(\sum_{d|m} \frac{1}{d}\right)^{-1} + \left(\sum_{k|n} \frac{1}{k}\right)^{-1} = 1.$$

Recall that $\sum_{d|x} \frac{1}{d} = \frac{\sigma(x)}{x}$. Let $K = \sigma(m) = \sigma(n) = m + n$. Then the sum of inverses is:

$$\left(\frac{\sigma(m)}{m}\right)^{-1} + \left(\frac{\sigma(n)}{n}\right)^{-1} = \frac{m}{K} + \frac{n}{K} = \frac{m+n}{K} = \frac{K}{K} = 1.$$

範例

Example 4.9. Primes cannot be Amicable. Prove that a prime number p cannot belong to an amicable pair.
Suppose (p, n) is an amicable pair. Then $\sigma(p) = p + n$. Since p is prime, $\sigma(p) = p + 1$. The equation becomes $p + 1 = p + n$, which implies $n = 1$. If $n = 1$, the pair is $(p, 1)$. This requires $\sigma(1) = 1 + p$. But $\sigma(1) = 1$. Thus $1 = 1 + p \implies p = 0$, which is not prime. Contradiction.

範例

Example 4.10. Squares of Primes cannot be Amicable. Prove that p^2 (where p is a prime) cannot belong to an amicable pair.
Suppose (p^2, n) is an amicable pair. Then $\sigma(p^2) = p^2 + n$. We calculate $\sigma(p^2) = 1 + p + p^2$. So $1 + p + p^2 = p^2 + n \implies n = p + 1$. The condition for amicable numbers requires $\sigma(n) = \sigma(p^2) = 1 + p + p^2$. Substituting $n = p + 1$:

$$\sigma(p+1) = p^2 + p + 1.$$

We estimate the growth of $\sigma(k)$. Generally, $\sigma(k) < k^2$ for $k > 1$. For $k = p + 1$, we consider the maximum possible sum of divisors.

$$\sigma(p+1) \leq \sum_{i=1}^{p+1} i = \frac{(p+1)(p+2)}{2} = \frac{p^2+3p+2}{2} = \frac{1}{2}p^2 + \frac{3}{2}p + 1.$$

We compare this upper bound with the required value $p^2 + p + 1$. For $p \geq 2$, $p^2 + p + 1 > \frac{1}{2}p^2 + \frac{3}{2}p + 1 \iff \frac{1}{2}p^2 - \frac{1}{2}p > 0 \iff p(p-1) > 0$. Since $p \geq 2$, this inequality strictly holds. Thus $\sigma(p+1) < p^2 + p + 1$. This contradicts the requirement for being an amicable pair.

範例

4.3 *Exercises*

1. **Perfect Squares and Perfect Numbers.** Prove: A square number cannot be a perfect number.

2. **Perfect Numbers and Division by 9.** Let n be an even perfect number greater than 6. Prove that when n is divided by 9, the remainder is 1.

   Remark.

   Use the form $2^{p-1}(2^p - 1)$ and list the possible remainders of cubes upon division by 9.

3. **Verifying Amicable Pairs.** Prove that 9,363,584 and 9,437,056 are an amicable pair.

   Remark.

   This pair was discovered by Descartes.

4. **Power Condition for Amicable Pairs.** Suppose a prime power p^a is one of an amicable pair. Prove that:

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

5. **Structure of Odd Perfect Numbers.** Prove: Any odd perfect number must be of the form $p^{4a+1}Q^2$, where p is an odd prime, a is a nonnegative integer, and Q is a positive integer.

Analyse the parity of $\sigma(n)$ factors. Since n is odd, $\sigma(n) = 2n$ is even but not divisible by 4. How does $\sigma(p^e)$ behave when p is odd?

5
The Principle of Stepwise Elimination

A recurring theme in the previous chapters has been the need to count integers satisfying specific divisibility properties. For instance, the Sieve of Eratosthenes systematically removes multiples of primes to isolate the remaining prime numbers.
We now formalise this counting technique. Known in combinatorics as the Inclusion-Exclusion Principle, and in number theory as the Principle of Stepwise Elimination, this tool allows us to enumerate objects that do *not* satisfy a set of properties by systematically adding and subtracting counts of objects that do.

5.1 *The Inclusion-Exclusion Principle*

We consider a finite set of objects and a collection of properties that these objects may possess. We wish to count the number of objects that possess none of these properties.

Theorem 5.1. ***Principle of Stepwise Elimination.***
Let S be a finite set of N objects. Let $\alpha_1, \alpha_2, \ldots, \alpha_s$ be a set of s distinct properties. For any subset of indices $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, s\}$, let $N_{\alpha_{i_1} \ldots \alpha_{i_k}}$ denote the number of objects in S that possess **all** the properties $\alpha_{i_1}, \ldots, \alpha_{i_k}$ simultaneously. The number of objects in S that possess **none** of the properties $\alpha_1, \ldots, \alpha_s$ is given by:

$$E = N - \sum_{1 \le i \le s} N_{\alpha_i} + \sum_{1 \le i < j \le s} N_{\alpha_i \alpha_j} - \sum_{1 \le i < j < k \le s} N_{\alpha_i \alpha_j \alpha_k} + \cdots + (-1)^s N_{\alpha_1 \ldots \alpha_s}$$
$$= N + \sum_{k=1}^{s} (-1)^k \left(\sum_{1 \le i_1 < \cdots < i_k \le s} N_{\alpha_{i_1} \ldots \alpha_{i_k}} \right).$$

定理

We determine the contribution of an arbitrary object $x \in S$ to the total sum on the right-hand side.

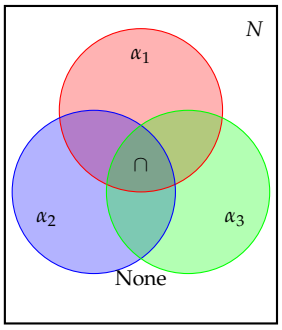


Figure 5.1: Visualisation for $s = 3$. To count the region outside the circles ("None"), we start with the total N, subtract single circles, add back pairwise intersections, and subtract the triple intersection.

x possesses none of the properties.

The object x is counted once in the term N. It does not appear in any N_{α_i} or subsequent terms because it has no properties. Total contribution: 1. This is correct.

証明終

x possesses exactly k properties ($1 \leq k \leq s$).

Assume x possesses properties $\alpha_{j_1}, \ldots, \alpha_{j_k}$.

- In the term N, x is counted 1 time (coefficient $\binom{k}{0}$).
- In the sum $\sum N_{\alpha_i}$, x is counted $\binom{k}{1}$ times (once for each of its k properties).
- In the sum $\sum N_{\alpha_i \alpha_j}$, x is counted $\binom{k}{2}$ times (once for each pair of its properties).
- Generally, in the m-th summation, x is counted $\binom{k}{m}$ times.

The total contribution of x to the alternating sum is:

$$C = \binom{k}{0} - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \cdots + (-1)^k \binom{k}{k}.$$

By the Binomial Theorem, this sum corresponds to the expansion of $(1-1)^k$:

$$C = (1-1)^k = 0.$$

Thus, any object possessing at least one property contributes 0 to the total.

証明終

Since only objects with no properties are counted (exactly once), the formula yields the number of such objects.

Applications to Divisibility

In number theory, the "properties" are typically divisibility conditions. Recall from the previous chapter that the number of multiples of an integer b not exceeding x is $\lfloor x/b \rfloor$. This allows us to calculate N_{α_i} and intersections explicitly.

Example 5.1. Counting Integers with Missing Factors. Find the number of positive integers not exceeding 100 that are not divisible by 2, 3, 5, or 7.

Let $S = \{1, 2, \ldots, 100\}$, so $N = 100$. We define four properties: α_1: divisible by 2; α_2: divisible by 3; α_3: divisible by 5; α_4: divisible by 7. We seek the number of elements with none of these properties. The count of numbers divisible by a set of coprime integers is

determined by the floor of N divided by their product.

$$\begin{aligned}\text{Count} = 100 &- \left(\left\lfloor\frac{100}{2}\right\rfloor + \left\lfloor\frac{100}{3}\right\rfloor + \left\lfloor\frac{100}{5}\right\rfloor + \left\lfloor\frac{100}{7}\right\rfloor\right) \\ &+ \left(\left\lfloor\frac{100}{6}\right\rfloor + \left\lfloor\frac{100}{10}\right\rfloor + \left\lfloor\frac{100}{14}\right\rfloor + \left\lfloor\frac{100}{15}\right\rfloor + \left\lfloor\frac{100}{21}\right\rfloor + \left\lfloor\frac{100}{35}\right\rfloor\right) \\ &- \left(\left\lfloor\frac{100}{30}\right\rfloor + \left\lfloor\frac{100}{42}\right\rfloor + \left\lfloor\frac{100}{70}\right\rfloor + \left\lfloor\frac{100}{105}\right\rfloor\right) \\ &+ \left\lfloor\frac{100}{210}\right\rfloor.\end{aligned}$$

Evaluating these terms:

$$\begin{aligned}\text{Count} &= 100 - (50 + 33 + 20 + 14) \\ &\quad + (16 + 10 + 7 + 6 + 4 + 2) \\ &\quad - (3 + 2 + 1 + 0) \\ &\quad + 0 \\ &\quad = 100 - 117 + 45 - 6 = 22.\end{aligned}$$

There are 22 such integers.

範例

The principle extends beyond simple counting; it is a linear operator that can be applied to summations.

Example 5.2. Summation of Non-Multiples. Calculate the sum of all positive integers not exceeding 100 that are not divisible by 2, 3, 5, or 7.

Let A be the set of integers $\{1, \ldots, 100\}$ satisfying the condition. We compute $\sum_{n \in A} n$. Using the Stepwise Elimination Principle, we replace the count of elements $\lfloor 100/k \rfloor$ with the sum of multiples of k. The sum of multiples of k up to N is:

$$S(N, k) = \sum_{j=1}^{\lfloor N/k \rfloor} jk = k\frac{\lfloor N/k \rfloor(\lfloor N/k \rfloor + 1)}{2}.$$

Applying the formula:

$$\begin{aligned}\text{Sum} = &\ S(100, 1) \\ &- (S(100, 2) + S(100, 3) + S(100, 5) + S(100, 7)) \\ &+ (S(100, 6) + S(100, 10) + S(100, 14) + S(100, 15) + S(100, 21) + S(100, 35)) \\ &- (S(100, 30) + S(100, 42) + S(100, 70)).\end{aligned}$$

Calculating individual terms:

- Total sum: $\frac{100 \times 101}{2} = 5050$.
- Singles: $2\frac{50 \times 51}{2} + 3\frac{33 \times 34}{2} + 5\frac{20 \times 21}{2} + 7\frac{14 \times 15}{2} = 2550 + 1683 + 1050 + 735 = 6018$.

· Pairs: $6(136) + 10(55) + 14(28) + 15(21) + 21(10) + 35(3) = 816 + 550 + 392 + 315 + 210 + 105 = 2388$.

· Triples: $30(6) + 42(3) + 70(1) = 180 + 126 + 70 = 376$.

Total Sum $= 5050 - 6018 + 2388 - 376 = 1044$.

範例

Counting Permutations (Derangements)

To demonstrate the versatility of *theorem* 5.1 beyond strictly arithmetic progressions, we consider a classical combinatorial problem involving permutations. This structure mirrors the divisibility problems: we subtract cases that violate a condition, then add back the overlaps.

Example 5.3. The Derangement Problem. A **derangement** of n elements is a permutation σ of the set $\{1, 2, \ldots, n\}$ such that $\sigma(i) \neq i$ for all i (i.e., no element remains in its original position). Find the number of derangements D_n.

Let S be the set of all $n!$ permutations. Let property α_i be the condition that $\sigma(i) = i$. We seek the number of permutations possessing none of the properties $\alpha_1, \ldots, \alpha_n$.

· $N = n!$.

· N_{α_i}: The number of permutations where i is fixed. The remaining $n - 1$ elements can be permuted in $(n - 1)!$ ways. There are $\binom{n}{1}$ such choices for i. Sum $= \binom{n}{1}(n-1)!$.

· $N_{\alpha_i \alpha_j}$: The number of permutations where i and j are fixed ($i \neq j$). The remaining $n - 2$ elements can be permuted in $(n - 2)!$ ways. There are $\binom{n}{2}$ such pairs. Sum $= \binom{n}{2}(n-2)!$.

· Generally, for k fixed points, the sum is $\binom{n}{k}(n-k)!$.

Applying *theorem* 5.1:

$$\begin{aligned} D_n &= n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \cdots + (-1)^n \binom{n}{n}(n-n)! \\ &= n! - \frac{n!}{1!(n-1)!}(n-1)! + \frac{n!}{2!(n-2)!}(n-2)! - \cdots + (-1)^n \frac{n!}{n!0!}0! \\ &= n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right). \end{aligned}$$

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

範例

5.2 *Counting Primes*

The Sieve of Eratosthenes is an algorithm. By applying the Principle of Stepwise Elimination, we can convert this algorithm into an explicit formula for $\pi(N)$, the prime-counting function.

Theorem 5.2. ***Legendre's Formula for*** $\pi(N)$**.**
Let N be a positive integer. Let $p_1, p_2, \ldots, p_s$ be the distinct prime numbers not exceeding $\sqrt{N}$. Then:

$$\pi(N) = N + s - 1 - \sum_i \left\lfloor \frac{N}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{N}{p_i p_j} \right\rfloor - \sum_{i<j<k} \left\lfloor \frac{N}{p_i p_j p_k} \right\rfloor + \cdots + (-1)^s \left\lfloor \frac{N}{p_1 \ldots p_s} \right\rfloor.$$

定理

Proof

Consider the set of integers $S = \{1, 2, \ldots, N\}$. An integer $x \in S$ is composite if and only if it is divisible by some prime $p \leq \sqrt{x} \leq \sqrt{N}$. Conversely, if $x > 1$ is not divisible by any prime $p \leq \sqrt{N}$, then x must be a prime number greater than $\sqrt{N}$.
We define the property α_i as "being divisible by p_i", for $i = 1, \ldots, s$. We apply the Principle of Stepwise Elimination to count integers in S not divisible by any p_i. Let M be this count.

$$M = N - \sum \left\lfloor \frac{N}{p_i} \right\rfloor + \sum \left\lfloor \frac{N}{p_i p_j} \right\rfloor - \ldots$$

The set of numbers counted by M contains:

1. The number 1 (which has no prime factors).
2. All primes q such that $\sqrt{N} < q \leq N$.

The primes $p_1, \ldots, p_s$ are **not** included in M because they are divisible by themselves (property α_i). Therefore, the total count of primes up to N is the number of primes in the "sieved" set (which is $M - 1$) plus the s small primes we used for sieving.

$$\pi(N) = (M - 1) + s.$$

Substituting the formula for M yields the result.

■

Example 5.4. Calculating $\pi(100)$. We find the number of primes up to 100. The primes not exceeding $\sqrt{100} = 10$ are 2, 3, 5, 7. Thus $s = 4$. We use the calculation from the first example in this chapter, where we found that the number of integers up to 100 not divisible

by 2, 3, 5, or 7 is 22. Thus $M = 22$. Using Legendre's Formula:

$$\pi(100) = M - 1 + s = 22 - 1 + 4 = 25.$$

This matches the actual count of primes up to 100.

範例

Structure of Coprime Integers

We can generalize Legendre's formula to count integers coprime to any general number n, not just the product of primes up to $\sqrt{N}$. This leads to the formula for Euler's Totient Function, which will be central to later chapters.

Example 5.5. Counting Coprimes to a Composite Number. Let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Find the number of integers $x \in \{1, \dots, n\}$ such that $(x, n) = 1$.

An integer x is coprime to n if and only if x is not divisible by any of the prime factors $p_1, \dots, p_k$. We apply Stepwise Elimination with $N = n$ and properties α_i: divisible by p_i. The number of such integers is:

$$\phi(n) = n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<l} \frac{n}{p_i p_j p_l} + \dots$$

Notice that we do not need the floor function symbols $\lfloor \dots \rfloor$ because we are dividing n by its own divisors; the results are always integers. We can factor the expression. Consider the expansion of the product:

$$n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = n \left(1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \dots\right).$$

Multiplying n through the brackets yields exactly the inclusion-exclusion sum derived above. Thus, the number of coprime integers is:

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

For example, if $n = 12 = 2^2 \cdot 3$, then $\phi(12) = 12(1 - 1/2)(1 - 1/3) = 12(1/2)(2/3) = 4$. The coprime integers are $\{1, 5, 7, 11\}$.

範例

5.3 *The Drawer Principle*

We now turn our attention to a fundamental logical tool used to prove the *existence* of mathematical objects without necessarily constructing them. This principle, often attributed to Dirichlet, posits a simple combinatorial truth: if one distributes a sufficiently large number of items into a fixed number of containers, at least one container must hold multiple items. Despite its apparent simplicity, this "Drawer Principle" (or Pigeonhole Principle) allows us to demonstrate the existence of complex number-theoretic structures.
We begin by formalising the simplest case.

Theorem 5.3. ***The First Drawer Principle.***
If $n+1$ or more objects are placed into n drawers, then at least one drawer must contain 2 or more objects.

定理

Proof

We proceed by contradiction. Assume that $n + 1$ objects are distributed into n drawers such that no drawer contains more than 1 object. Then every drawer contains either 0 or 1 object. Consequently, the total number of objects S satisfies:

$$S \leq \underbrace{1+1+\cdots+1}_{n \text{ times}} = n.$$

This contradicts the hypothesis that there are at least $n + 1$ objects. Thus, the assumption is false, and at least one drawer contains 2 or more objects.

■

This concept generalises naturally when the number of objects far exceeds the number of drawers.

Theorem 5.4. ***The Generalised Drawer Principle.***
If m objects are placed into n drawers, then at least one drawer contains at least $\lfloor \frac{m-1}{n} \rfloor + 1$ objects.

定理

Proof

Let $k = \lfloor \frac{m-1}{n} \rfloor$. The largest multiple of n strictly less than m is nk. We wish to show some drawer has at least $k + 1$ objects. Assume for the sake of contradiction that every drawer contains at most k objects. Since there are n drawers, the total number of objects S satisfies:

$$S \leq nk = n \left\lfloor \frac{m-1}{n} \right\rfloor \leq n \left(\frac{m-1}{n} \right) = m - 1.$$

This implies the total number of objects is strictly less than m, a contradiction. Therefore, at least one drawer holds $k + 1$ or more objects.

■

The Drawer Principle is particularly effective when the "drawers" represent remainders or structural partitions of the integers.

Example 5.6. Parity Subsets. Prove that among any 3 integers, there are at least 2 whose sum is a multiple of 2.
We classify integers by their parity. There are 2 possible categories ("drawers"): odd and even. We are given 3 integers. By *theorem* 5.3, since $3 > 2$, at least 2 integers must belong to the same category. Let these two integers be a and b.

1. If both are even, $a = 2k$ and $b = 2j$. Then $a + b = 2(k + j)$, which is a multiple of 2.
2. If both are odd, $a = 2k + 1$ and $b = 2j + 1$. Then $a + b = 2k + 2j + 2 = 2(k + j + 1)$, which is a multiple of 2.

In either case, the sum is divisible by 2.

範例

We can extend the logic of remainders to general divisors.

Example 5.7. Subset Sum Divisibility. Prove that among any set of n positive integers $a_1, a_2, \ldots, a_n$, there exists a non-empty subset whose sum is a multiple of n.
Consider the n partial sums:

$$S_1 = a_1, \quad S_2 = a_1 + a_2, \quad \ldots, \quad S_n = a_1 + a_2 + \cdots + a_n.$$

We examine the remainders of these sums when divided by n. By the Division Algorithm, the possible remainders are $\{0, 1, \ldots, n-1\}$.

- **Case 1:** If any sum S_k has a remainder of 0, then S_k is a multiple of n, and the subset $\{a_1, \ldots, a_k\}$ satisfies the condition.
- **Case 2:** If no sum S_k has a remainder of 0, then the n values $S_1, \ldots, S_n$ must map to the $n - 1$ non-zero remainders $\{1, \ldots, n-1\}$.

By *theorem* 5.3, placing n sums into $n - 1$ remainder classes implies that at least two sums, say S_k and S_m (with $k > m$), leave the same remainder. It follows that their difference is a multiple of n:

$$S_k - S_m = (a_1 + \cdots + a_k) - (a_1 + \cdots + a_m) = a_{m+1} + a_{m+2} + \cdots + a_k.$$

Thus, the sum of the subset $\{a_{m+1}, \ldots, a_k\}$ is divisible by n.

範例

Example 5.8. Divisibility in Intervals. Prove that for any integer $n \geq 1$, if one selects $n+1$ integers from the set $\{1, 2, \ldots, 2n\}$, then at least one selected integer divides another.
Every positive integer x can be written uniquely in the form $x = 2^k \cdot q$, where $k \geq 0$ and q is an odd integer. For any $x \in \{1, \ldots, 2n\}$, the odd part q must also be in the range $1 \leq q < 2n$. The possible odd parts in this range are the odd integers $\{1, 3, 5, \ldots, 2n - 1\}$. The number of such odd integers is exactly n. We define these n odd integers as our "drawers". We are given $n + 1$ numbers. By the Drawer Principle, two distinct numbers x and y must share the same odd part q. Let $x = 2^a \cdot q$ and $y = 2^b \cdot q$. Since x and y are distinct, we must have $a \neq b$. If $a < b$, then $x \mid y$ (since $y = 2^{b-a}x$). If $b < a$, then $y \mid x$. Thus, one number divides the other.

範例

Geometric and Additive Applications

The principle applies equally to coordinate geometry and sequence construction.

Example 5.9. Midpoints of Lattice Points. Prove that among any 5 integer points in the Cartesian plane, there exist 2 points whose midpoint is also an integer point.
A point (x, y) is an integer point if $x, y \in \mathbb{Z}$. The midpoint of $A(x_1, y_1)$ and $B(x_2, y_2)$ is:

$$M = \left(\frac{x_1 + x_2}{2}, \frac{y_1 + y_2}{2} \right).$$

For M to be an integer point, $x_1 + x_2$ and $y_1 + y_2$ must both be even. This occurs if and only if x_1 and x_2 have the same parity, and y_1 and y_2 have the same parity. We classify integer points by the parity of their coordinates. There are 4 such classes:

$$(\text{odd, odd}), \quad (\text{odd, even}), \quad (\text{even, odd}), \quad (\text{even, even}).$$

We are selecting 5 points. By *theorem* 5.3, since $5 > 4$, at least two points A and B must belong to the same parity class. Consequently, their midpoint is an integer point.

範例

Example 5.10. Additive Relations in Sets. Let n be a positive integer. Prove that given any set of $n + 1$ distinct positive integers each strictly less than $2n$, there exist three elements x, y, z in the set such that $x + y = z$.

Let the set of integers be $A = \{a_0, a_1, \ldots, a_n\}$. Sort the elements such that:

$$1 \leq a_0 < a_1 < \cdots < a_n < 2n.$$

We define a new sequence of n numbers based on A:

$$b_1 = a_1 - a_0, \quad b_2 = a_2 - a_0, \quad \ldots, \quad b_n = a_n - a_0.$$

Note that $b_i > 0$ for all i. Also, since $a_n < 2n$ and $a_0 \geq 1$:

$$b_n = a_n - a_0 < 2n - 1.$$

Consider the combined collection of numbers:

$$C = \{a_1, \ldots, a_n\} \cup \{b_1, \ldots, b_n\}.$$

There are n numbers in the first set and n in the second, totalling $2n$ numbers. However, all elements of C are positive integers strictly less than $2n$ (the maximum possible value is $2n - 1$). By the Drawer Principle (placing $2n$ items into $2n - 1$ values), at least two numbers in C must be equal. Since the sequence a_i is strictly increasing, all a_i are distinct. Similarly, all b_i are distinct. Thus, the equality must be between an element of the first set and an element of the second. There exist indices j and k such that $a_k = b_j$. Substituting the definition of b_j:

$$a_k = a_j - a_0 \implies a_k + a_0 = a_j.$$

Let $x = a_0, y = a_k, z = a_j$. These are elements of the original set satisfying $x + y = z$.

範例

The Averaging Principle

A variation of the Drawer Principle deals with sums and averages. If a total resource is distributed among n consumers, someone must possess at least the average amount.

Theorem 5.5. ***The Weighted Drawer Principle.***
Let $q_1, \ldots, q_n$ be positive integers. If

$$S = q_1 + q_2 + \cdots + q_n - n + 1$$

objects are placed into n drawers, then either the first drawer contains at least q_1 objects, or the second contains at least q_2, ..., or the n-th contains at least q_n.

定理

Proof

Assume the contrary: that for every drawer i, the number of objects o_i satisfies $o_i \leq q_i - 1$. Summing over all drawers:

$$\text{Total Objects} = \sum_{i=1}^{n} o_i \leq \sum_{i=1}^{n} (q_i - 1) = \left(\sum_{i=1}^{n} q_i \right) - n = S - 1.$$

This contradicts the fact that there are S objects.

■

Corollary 5.1. *The Average Principle.* Let $m_1, \ldots, m_n$ be integers. If their arithmetic mean is greater than $r-1$, then at least one integer is greater than or equal to r.

$$\frac{1}{n} \sum_{i=1}^{n} m_i > r - 1 \implies \exists k, m_k \geq r.$$

推論

Example 5.11. Sums on a Circle. The integers from 1 to 10 are arranged in a circle in an arbitrary order. Prove that there exist 3 adjacent numbers whose sum is at least 17.
Let the arrangement be $a_1, a_2, \ldots, a_{10}$ in clockwise order. We form the 10 sums of 3 adjacent numbers:

$$S_1 = a_1 + a_2 + a_3, \quad S_2 = a_2 + a_3 + a_4, \quad \ldots, \quad S_{10} = a_{10} + a_1 + a_2.$$

We calculate the sum of these sums. In the total $\sum S_i$, each number a_k appears exactly 3 times (once as the first element, once as the second, once as the third).

$$\sum_{i=1}^{10} S_i = 3(a_1 + a_2 + \cdots + a_{10}).$$

Since the numbers are a permutation of $1, \ldots, 10$, their sum is 55.

$$\sum_{i=1}^{10} S_i = 3(55) = 165.$$

The average value of the sums is:

$$\bar{S} = \frac{165}{10} = 16.5.$$

Since the average is 16.5, by the Average Principle (with $r = 17$, noting $16.5 > 17 - 1$), at least one sum S_k must be greater than or equal to 17.

範例

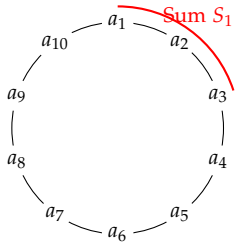


Figure 5.2: Ten integers arranged on a circle. We consider sums of triplets like (a_1, a_2, a_3).

Example 5.12. Decimal Expansions. Prove that for any integer $n > 0$, the decimal expansion of $\frac{1}{n}$ is eventually repeating.
Consider the process of long division of 1 by n. At each step k, we obtain a remainder r_k when dividing by n. By the Division Algorithm, the possible values for the remainder r_k are $\{0, 1, \ldots, n-1\}$. There are only n possible values for these remainders. Consider the sequence of $n+1$ remainders generated by the division process: $r_1, r_2, \ldots, r_{n+1}$. By the Drawer Principle, since there are $n+1$ remainders and only n possible values, at least two remainders must be identical. Let $r_i = r_j$ with $i < j$. Since the algorithm for long division is deterministic (the next digit and next remainder depend entirely on the current remainder), the sequence of digits generated after r_i will be identical to the sequence generated after r_j. Thus, the decimal expansion repeats with a period of length at most $j - i$.

範例

5.4 *Exercises*

1. **Sieve Count.** Find the number of positive integers not exceeding 500 that are **not** divisible by any of 5, 7, or 11.
2. **Sieve Sum.** Calculate the sum of all positive integers not exceeding 500 that are **not** divisible by any of 5, 7, or 11.
3. **Divisibility by Sets.** Consider the integers from 1 to 2000.
   (a) How many are divisible by at least two of the numbers 2, 3, 5?
   (b) How many are divisible by exactly one of the numbers 2, 3, 5?
4. **Counting Primes.** Use Legendre's Formula (*theorem* 5.2) to calculate $\pi(150)$, the number of primes not exceeding 150.
5. **Bertrand's Postulate.** Prove that for any real number $x \geq 1$, there exists at least one prime number in the interval $(x, 2x]$.

   Remark.
   This is a deep theorem; try to prove a weaker version first, you may use the properties of binomial coefficients $\binom{2n}{n}$.

6. **Parity and Difference.** Prove that among any 4 integers, there are at least 2 whose difference is divisible by 3.
7. **Sum Divisibility.** Prove that among any 5 integers, there are at least 3 integers whose sum is divisible by 3.
8. **Divisor Existence.** Prove that if $n+1$ integers are selected from

the set $\{1, 2, \ldots, 2n\}$, there must exist two integers such that one divides the other.

9. **Maximising the Minimum.** Let $m > n > 0$. Suppose m books are placed into n drawers. Let r be the maximum integer such that we can guarantee at least one drawer contains r books. Determine r in terms of m and n.

10. **Sum Matching.** Let A and B be two sets of distinct positive integers such that every element in $A \cup B$ is strictly less than n. Suppose $|A| + |B| \geq n$. Prove that there exists $a \in A$ and $b \in B$ such that $a + b = n$.

6
Congruence

Having established the properties of divisibility and prime factorisation in the preceding chapters, we now turn to one of the most powerful tools in elementary number theory: the theory of congruences. Developed systematically by Carl Friedrich Gauss in his *Disquisitiones Arithmeticae* (1801), this theory formalises the arithmetic of remainders. It provides a natural framework for treating divisibility problems as algebraic equations, greatly simplifying arguments that would otherwise require cumbersome manipulation of linear combinations.

6.1 The Concept of Congruence

The notion of congruence is an extension of the divisibility relation. It classifies integers based on their remainders when divided by a fixed positive integer.

Definition 6.1. ***Congruence.***
Let m be a fixed positive integer, termed the **modulus**. Two integers a and b are said to be **congruent modulo** m if they leave the same remainder when divided by m. This relationship is denoted by:

$$a \equiv b \pmod{m}.$$

If the remainders are distinct, a and b are said to be **incongruent modulo** m, denoted by $a \not\equiv b \pmod{m}$.

定義

While the definition relies on the Euclidean Division Algorithm, it is often more operationally convenient to express congruence in terms of divisibility.

Theorem 6.1. ***Characterisation of Congruence.***
Let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if m divides the difference $a - b$.

定理

Necessity.

Suppose $a \equiv b \pmod{m}$. By *theorem* 0.4, we can write $a = mq_1 + r$ and $b = mq_2 + r$, where $0 \leq r < m$. Subtracting the two equations yields:

$$a - b = (mq_1 + r) - (mq_2 + r) = m(q_1 - q_2).$$

Since $q_1 - q_2$ is an integer, $m \mid (a - b)$.

証明終

Sufficiency.

Suppose $m \mid (a - b)$. Then $a - b = mk$ for some integer k. Let $b = mq + r$ with $0 \leq r < m$. Substituting this into the expression for a:

$$a = b + mk = (mq + r) + mk = m(q + k) + r.$$

Thus, a leaves the same remainder r as b when divided by m, so $a \equiv b \pmod{m}$.

証明終

This theorem establishes the bridge between the notation of congruence and the theory of linear Diophantine equations. The expression $a \equiv b \pmod{m}$ is equivalent to the existence of an integer k such that $a = b + mk$.

Properties of Congruence

The utility of congruence lies in its structural similarity to equality. We begin by verifying that congruence behaves as an equivalence relation.

Theorem 6.2. ***Equivalence Relation.***
Congruence modulo m is an equivalence relation on the set of integers. That is, for all integers a, b, c:

1. **Reflexivity:** $a \equiv a \pmod{m}$.
2. **Symmetry:** If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
3. **Transitivity:** If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

定理

Proof

1. $a - a = 0 = m \cdot 0$, so $m \mid (a - a)$.
2. If $m \mid (a - b)$, then $a - b = mk$. Thus $b - a = m(-k)$, so $m \mid (b - a)$.
3. If $m \mid (a - b)$ and $m \mid (b - c)$, then $a - b = mk$ and $b - c = mj$. Adding these yields $(a - b) + (b - c) = a - c = m(k + j)$. Thus $m \mid (a - c)$.

■

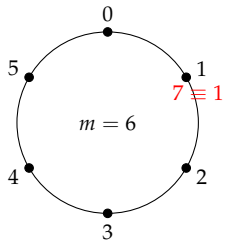


Figure 6.1: Visualising congruence modulo 6. Integers map to points on the circle; 1 and 7 occupy the same position.

Crucially, congruences preserve the basic arithmetic operations of addition and multiplication. This allows us to perform arithmetic on "remainders" without converting back to the original integers.

Theorem 6.3. ***Arithmetic Properties.***
If $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then:
1. $a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$.
2. $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

定理

Proof

By hypothesis, there exist integers k and j such that $a_1 - b_1 = mk$ and $a_2 - b_2 = mj$.
1. Consider the sum (or difference):

   $$(a_1 \pm a_2) - (b_1 \pm b_2) = (a_1 - b_1) \pm (a_2 - b_2) = mk \pm mj = m(k \pm j).$$

   Since $k \pm j$ is an integer, m divides the difference.
2. Consider the product. We use the identity $a_1 a_2 - b_1 b_2 = a_2(a_1 - b_1) + b_1(a_2 - b_2)$.

   $$a_1 a_2 - b_1 b_2 = a_2(mk) + b_1(mj) = m(a_2 k + b_1 j).$$

   Since $a_2 k + b_1 j$ is an integer, $m \mid (a_1 a_2 - b_1 b_2)$.

■

The following corollaries are immediate consequences of *theorem 6.3* and are used frequently in calculation.

Corollary 6.1. *Congruence Operations.* Let a, b, k be integers and m, n be positive integers. If $a \equiv b \pmod{m}$, then:
1. $a \pm k \equiv b \pm k \pmod{m}$.
2. $ak \equiv bk \pmod{m}$.
3. $a^n \equiv b^n \pmod{m}$.

推論

These properties extend to polynomials with integer coefficients.

Corollary 6.2. Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be a polynomial with integer coefficients. If $a \equiv b \pmod{m}$, then $P(a) \equiv P(b) \pmod{m}$. Furthermore, if two polynomials $f(x)$ and $g(x)$ have coefficients that are congruent modulo m term-by-term, then $f(x) \equiv g(x) \pmod{m}$.

推論

Example 6.1. Divisibility by 9. Using the polynomial property, we can derive the standard test for divisibility by 9. Let n be a positive integer with decimal representation $d_k d_{k-1} \dots d_1 d_0$. Then $n = \sum_{i=0}^{k} d_i 10^i$. Consider the polynomial $P(x) = \sum_{i=0}^{k} d_i x^i$. Then

$n = P(10)$. Since $10 \equiv 1 \pmod 9$, we have:

$$P(10) \equiv P(1) \pmod 9.$$

Calculating $P(1)$:

$$P(1) = \sum_{i=0}^{k} d_i (1)^i = d_0 + d_1 + \cdots + d_k.$$

Thus, $n \equiv$ sum of digits of $n \pmod 9$. An integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

範例

6.2 *Simplification and Cancellation*

While addition and multiplication behave intuitively, division requires care. The congruence $ac \equiv bc \pmod m$ does not necessarily imply $a \equiv b \pmod m$. For example, $2 \cdot 3 \equiv 2 \cdot 1 \pmod 4$, but $3 \not\equiv 1 \pmod 4$.
However, we can cancel a factor if it is coprime to the modulus.

Theorem 6.4. ***Cancellation Law.***
If $ac \equiv bc \pmod m$ and $(c, m) = 1$, then $a \equiv b \pmod m$.

定理

Proof

The congruence $ac \equiv bc \pmod m$ implies $m \mid (ac - bc)$, or equivalently $m \mid c(a - b)$. Since $(c, m) = 1$, Euclid's Lemma (established in the chapter on Divisibility) implies that m must divide the other factor, $a - b$. Thus $a \equiv b \pmod m$.

■

We can now apply these tools to solve specific number-theoretic problems.

Example 6.2. Roots of Quadratic Congruences. Let p be a prime not dividing a, and let $k \geq 1$. Determine the solutions to $n^2 \equiv an \pmod{p^k}$.
We seek n such that $p^k \mid (n^2 - an)$, or $p^k \mid n(n - a)$.

Case $k = 1$: Since p is prime, $p \mid n(n - a)$ implies $p \mid n$ or $p \mid (n - a)$. Thus $n \equiv 0 \pmod p$ or $n \equiv a \pmod p$.

Case $k \geq 2$: Suppose p divides both factors. Then $p \mid n$ and $p \mid (n - a)$. By linearity, $p \mid n - (n - a) \implies p \mid a$. But we assumed $p \nmid a$. This is a contradiction. Therefore, the prime power p^k cannot be "split" between the two factors; it must divide one

entirely. Let $v_p(x)$ denote the exponent of p in the prime factorisation of x. Since $p^k \mid n(n-a)$, we have $v_p(n) + v_p(n-a) \geq k$. The argument above shows at most one of $v_p(n), v_p(n-a)$ is positive, so one is 0 and the other is at least k. This leaves two solutions: $n \equiv 0 \pmod{p^k}$ or $n \equiv a \pmod{p^k}$.

範例

Example 6.3. Non-Existence of Integer Roots. Prove that the equation $x^2 + y^2 = 4k + 3$ has no integer solutions.
We analyse the equation modulo 4. The right-hand side is congruent to 3 modulo 4. For any integer z, we check the possible values of $z^2 \pmod 4$:
· If z is even ($z = 2m$), $z^2 = 4m^2 \equiv 0 \pmod 4$.

· If z is odd ($z = 2m+1$), $z^2 = 4m^2 + 4m + 1 \equiv 1 \pmod 4$.
Thus, squares modulo 4 are always 0 or 1. The sum of two squares $x^2 + y^2 \pmod 4$ can therefore only take the values:

$$0+0=0, \quad 0+1=1, \quad 1+0=1, \quad 1+1=2.$$

The value 3 is impossible. Thus, no integers x, y satisfy the equation.

範例

Composite Numbers and Factorials

Congruences provide elegant tests for primality and properties of composite numbers. The following result complements Wilson's Theorem (which we shall prove in a later section).

Example 6.4. Factorials of Composite Numbers. Let $n > 4$ be a composite integer. Prove that $(n-2)! \equiv 0 \pmod n$.
Since n is composite, we can write $n = d_1 d_2$ with $1 < d_1 \leq d_2 < n$. We consider the term $(n-2)! = 1 \cdot 2 \cdot \cdots \cdot (n-2)$.

Case 1: $d_1 \neq d_2$. Since n is composite, its smallest divisor $d_1 \leq \sqrt{n}$. If $n > 4$, then $d_2 = n/d_1 < n-1$. Since d_2 is an integer and $d_2 < n-1$, we have $d_2 \leq n-2$. Thus both d_1 and d_2 are distinct integers appearing in the product $1 \times \cdots \times (n-2)$. Their product $d_1 d_2 = n$ divides $(n-2)!$.

Case 2: $d_1 = d_2$. Here $n = d_1^2$ is a perfect square. Since $n > 4$, we have $d_1 > 2$. We need to find two factors in $(n-2)!$ that multiply to n. We use d_1 and $2d_1$. We check if $2d_1 \leq n-2$. Since $d_1 \geq 3$, $d_1(d_1-2) \geq 3(1) = 3 > 0$, so $d_1^2 > 2d_1$. Also $n = d_1^2$. Is $2d_1 \leq d_1^2 - 2$? For $d_1 \geq 3$, $d_1^2 - 2d_1 - 2 = (d_1-1)^2 - 3$. If $d_1 = 3$, $n = 9$.

$(n-2)! = 7!$. $d_1 = 3, 2d_1 = 6$. Both are in $7!$. $3 \times 6 = 18$, which is divisible by 9. Generally for $d_1 \geq 3$, $2d_1 < d_1^2 - 2 = n - 2$. Thus both d_1 and $2d_1$ appear in the product $(n-2)!$. Since $n = d_1^2$ divides $d_1 \cdot 2d_1 = 2d_1^2$, it follows that $n \mid (n-2)!$.

Conversely, if $(n-2)! \equiv 0 \pmod{n}$ and $n > 4$, n must be composite. If n were prime, then from $n \mid (n-2)!$ we would have $n \mid k$ for some $k \in \{1, \ldots, n-2\}$, because a prime dividing a product divides a factor. This is impossible, so n cannot be prime.

範例

6.3 *Applications to Periodicity and Sums*

The cyclical nature of modular arithmetic makes it ideal for detecting patterns in powers and calendars.

Example 6.5. Mersenne Numbers and Modulo 7. Find all positive integers n such that $2^n - 1$ is divisible by 7.
We observe the powers of 2 modulo 7:

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 = 8 \equiv 1 \pmod{7}.$$

Since $2^3 \equiv 1$, the powers repeat with period 3. We express n in terms of its remainder modulo 3. Let $n = 3k + r$, where $r \in \{0, 1, 2\}$.

$$2^n - 1 = 2^{3k+r} - 1 = (2^3)^k \cdot 2^r - 1 \equiv 1^k \cdot 2^r - 1 \equiv 2^r - 1 \pmod{7}.$$

We test the possible values of r:
· If $r = 0$, $2^0 - 1 = 0 \equiv 0$.
· If $r = 1$, $2^1 - 1 = 1 \not\equiv 0$.
· If $r = 2$, $2^2 - 1 = 3 \not\equiv 0$.
Thus, $2^n - 1$ is divisible by 7 if and only if n is a multiple of 3.

範例

Example 6.6. Calendar Cycles. February 1996 had 5 Thursdays. Determine the next years before 2100 in which this occurs.
February usually has 28 days (4 weeks exactly). In a non-leap year, days of the week do not shift within the month, and there are exactly 4 of each weekday. For a February to have 5 Thursdays, it must have 29 days. Thus, the year must be a leap year, and February 1st must be a Thursday (so that the 1st, 8th, 15th, 22nd, and 29th are Thursdays). We track the shift in weekdays for February 1st between consecutive leap years. A normal year has 365 days, which is $52 \times 7 + 1$ days. (Shift of $+1$). A leap

year has 366 days. (Shift of $+2$). The interval between one leap year's February 1st and the next (4 years later) consists of three normal years and one leap year (the current one). Total days = $3(365) + 366 = 3(52 \times 7 + 1) + (52 \times 7 + 2) = 1461$.

$$1461 \equiv 3(1) + 2 \equiv 5 \pmod 7.$$

The day of the week for Feb 1st shifts forward by 5 days (or backwards by 2) every 4 years. Let 1996 correspond to day 0 (Thursday). The sequence of shifts modulo 7 for subsequent leap years is:

- 1996: 0 (Thursday)
- 2000: $0 + 5 \equiv 5$
- 2004: $5 + 5 \equiv 10 \equiv 3$
- 2008: $3 + 5 \equiv 8 \equiv 1$
- 2012: $1 + 5 \equiv 6$
- 2016: $6 + 5 \equiv 11 \equiv 4$
- 2020: $4 + 5 \equiv 9 \equiv 2$
- 2024: $2 + 5 \equiv 7 \equiv 0$ (Thursday again)

The cycle repeats every 7 leap years (28 years). The years are $1996 + 28 = 2024$, $2024 + 28 = 2052$, and $2052 + 28 = 2080$.

範例

Example 6.7. Sum of Fourth Powers. Prove that the sum of the 4th powers of four consecutive integers cannot be the 4th power of an integer.

We examine 4th powers modulo 4. For any integer x:

- If x is even ($x = 2k$), $x^4 = 16k^4 \equiv 0 \pmod 4$.
- If x is odd ($x = 2k + 1$), $x^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$. Squaring again: $x^4 \equiv 1^2 \equiv 1 \pmod 4$.

Any set of four consecutive integers $\{n, n+1, n+2, n+3\}$ contains two even numbers and two odd numbers. Let S be the sum of their 4th powers.

$$S \equiv 0 + 1 + 0 + 1 \equiv 2 \pmod 4.$$

However, we have just shown that any perfect 4th power must be congruent to 0 or 1 modulo 4. Since $S \equiv 2 \pmod 4$, S cannot be a 4th power.

範例

6.4 *Modulus Transformations*

Many number-theoretic problems require us to manipulate the modulus itself — scaling it, dividing it, or combining multiple moduli. This flexibility is essential for solving systems of linear congruences and for analysing the structure of composite numbers.
We begin by establishing how the congruence relation behaves when the modulus is multiplied by an integer.

Theorem 6.5. ***Modulus Scaling.***
Let a, b, m be integers with $m > 0$. If $a \equiv b \pmod{m}$, then for any positive integer k,

$$ak \equiv bk \pmod{mk}.$$

定理

Proof

Since $a \equiv b \pmod{m}$, there exists an integer q such that $a - b = mq$. Multiplying both sides by k, we obtain:

$$k(a-b) = k(mq) \implies ak - bk = (mk)q.$$

Since q is an integer, mk divides $ak - bk$, which implies $ak \equiv bk \pmod{mk}$.

■

Conversely, we can reduce the modulus by dividing out a common factor, provided that factor also divides the integers involved in the congruence.

Theorem 6.6. ***Modulus Division.***
Let $a \equiv b \pmod{m}$. If d is a positive common divisor of a, b, and m, then

$$\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

定理

Proof

Let $a = b + mq$ for some integer q. Since d divides a, b, and m, we can divide the entire equation by d:

$$\frac{a}{d} = \frac{b}{d} + \frac{m}{d}q.$$

Since a/d and b/d are integers, and m/d is an integer, this equation represents a valid congruence relation modulo m/d.

■

Often, we encounter a fixed relationship $a \equiv b$ that holds for several distinct moduli. The following theorem allows us to combine these

into a single congruence involving the least common multiple.

Theorem 6.7. ***LCM of Moduli.***
Let $m_1, m_2, \ldots, m_k$ be positive integers. If $a \equiv b \pmod{m_i}$ for all $i = 1, \ldots, k$, then

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]},$$

where $[m_1, \ldots, m_k]$ denotes the least common multiple of the moduli.

定理

Proof

By definition, $a \equiv b \pmod{m_i}$ implies that $m_i \mid (a - b)$ for each i. From the properties of divisibility, if an integer N is divisible by several integers, it is divisible by their least common multiple. Thus, $[m_1, \ldots, m_k] \mid (a - b)$, which is equivalent to the stated congruence.

■

Corollary 6.3. *Coprime Moduli.* If $a \equiv b \pmod{m_i}$ for pairwise coprime integers $m_1, \ldots, m_k$, then

$$a \equiv b \pmod{m_1 m_2 \ldots m_k}.$$

This follows immediately because the LCM of pairwise coprime numbers is their product.

推論

Finally, we observe that congruence is preserved when the modulus is replaced by any of its divisors.

Theorem 6.8. ***Modulus Reduction.***
If $a \equiv b \pmod{m}$ and d is a positive divisor of m, then $a \equiv b \pmod{d}$.

定理

Proof

We are given that $m \mid (a - b)$. Since $d \mid m$, the transitivity of divisibility implies $d \mid (a - b)$.

■

Proposition 6.1. ***GCD Invariance.***
If $a \equiv b \pmod{m}$, then $(a, m) = (b, m)$.

命題

Proof

Let $(a, m) = d_1$ and $(b, m) = d_2$. Since $a \equiv b \pmod{m}$, we have $a = b + mk$ for some integer k. Because $d_2 \mid b$ and $d_2 \mid m$, it follows

that $d_2 \mid (b + mk)$, so $d_2 \mid a$. Thus d_2 is a common divisor of a and m, implying $d_2 \leq d_1$. By symmetry, writing $b = a - mk$, we deduce that $d_1 \mid b$, so $d_1 \leq d_2$. Therefore, $d_1 = d_2$.

■

Applications of Modulus Properties

We now demonstrate the power of these theorems in establishing divisibility results for general algebraic expressions.

Example 6.8. A Large Divisibility Problem. Let n be any positive integer. Prove that the expression

$$E = 2000^n + 855^n - 572^n - 302^n$$

is divisible by 1981.
First, we calculate the prime factorisation of the modulus: $1981 = 7 \times 283$. Since 7 and 283 are prime (and thus coprime), it suffices to show that $E \equiv 0 \pmod 7$ and $E \equiv 0 \pmod{283}$.

Modulo 7: We reduce the bases modulo 7:

$$2000 \equiv 5, \quad 855 \equiv 1, \quad 572 \equiv 5, \quad 302 \equiv 1.$$

Substituting these into E:

$$E \equiv 5^n + 1^n - 5^n - 1^n \equiv 0 \pmod 7.$$

Modulo 283: We reduce the bases modulo 283:

$$\begin{aligned} 2000 &= 7 \times 283 + 19 \implies 2000 \equiv 19 \pmod{283}. \\ 855 &= 3 \times 283 + 6 \implies 855 \equiv 6 \pmod{283}. \\ 572 &= 2 \times 283 + 6 \implies 572 \equiv 6 \pmod{283}. \\ 302 &= 1 \times 283 + 19 \implies 302 \equiv 19 \pmod{283}. \end{aligned}$$

Substituting these into E:

$$E \equiv 19^n + 6^n - 6^n - 19^n \equiv 0 \pmod{283}.$$

Since E is divisible by both 7 and 283, and $(7, 283) = 1$, *theorem 6.7* implies E is divisible by $7 \times 283 = 1981$.

範例

Example 6.9. Fourth Powers and Modulo 240. Prove that if p is a prime greater than 5, then $p^4 \equiv 1 \pmod{240}$.
The prime factorisation of the modulus is $240 = 2^4 \cdot 3 \cdot 5 = 16 \cdot 3 \cdot 5$.

We verify the congruence for each factor separately.

Modulo 3: Since $p > 5$, p is not divisible by 3. Thus $p \equiv \pm 1 \pmod 3$. Squaring gives $p^2 \equiv 1 \pmod 3$, so $p^4 \equiv 1 \pmod 3$.

Modulo 5: Since $p > 5$, $p \not\equiv 0 \pmod 5$. The possible residues for p are $\{1, 2, 3, 4\}$. Calculating fourth powers:

$$1^4 = 1, \quad 2^4 = 16 \equiv 1, \quad 3^4 = 81 \equiv 1, \quad 4^4 = 256 \equiv 1.$$

Thus $p^4 \equiv 1 \pmod 5$.

Modulo 16: Since p is an odd prime, let $p = 2k + 1$.

$$p^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1.$$

Notice that $k(k+1)$ is the product of two consecutive integers, so it is always even. Let $k(k+1) = 2m$.

$$p^2 = 4(2m) + 1 = 8m + 1.$$

Now we calculate p^4:

$$p^4 = (p^2)^2 = (8m+1)^2 = 64m^2 + 16m + 1.$$

Since $16 \mid 64m^2$ and $16 \mid 16m$, we have $p^4 \equiv 1 \pmod{16}$.

Since $p^4 \equiv 1$ modulo 3, 5, and 16, and these moduli are pairwise coprime,

$$p^4 \equiv 1 \pmod{3 \times 5 \times 16} \implies p^4 \equiv 1 \pmod{240}.$$

範例

Example 6.10. Cyclic System of Congruences. Find all triples of positive integers (a, b, c) satisfying the system:

$$a \equiv b \pmod c, \quad b \equiv c \pmod a, \quad c \equiv a \pmod b.$$

Without loss of generality, assume an ordering $a \leq b \leq c$. From the first congruence, $c \mid (a - b)$. Since $a \leq b$, the difference $a - b \leq 0$. However, the absolute difference $|a - b| = b - a$ must be a multiple of c. Since $b \leq c$ and $a \geq 1$, we have $b - a < c$. The only non-negative multiple of c strictly less than c is 0. Thus $b - a = 0 \implies a = b$.
Substituting $a = b$ into the remaining conditions:

$$a \equiv c \pmod a \implies a \mid (c - a) \implies a \mid c.$$

$$c \equiv a \pmod a \implies a \mid (c - a) \implies a \mid c.$$

Let $c = ka$ for some integer k. The solutions are of the form (a, a, ka) for any positive integers a, k. The coprime solutions (where $(a, b, c) = 1$) occur when $a = 1$, yielding the triple $(1, 1, k)$.

範例

6.5 *Divisibility Criteria*

The decimal representation of an integer is a polynomial in powers of 10. By analysing the properties of 10 modulo m, we can derive efficient criteria for divisibility. Let N be a positive integer with decimal expansion:

$$N = a_n a_{n-1} \dots a_1 a_0 = \sum_{i=0}^{n} a_i 10^i,$$

where $0 \leq a_i \leq 9$ are the digits. Let $P(x) = \sum_{i=0}^{n} a_i x^i$, so that $N = P(10)$. If $10 \equiv k \pmod{m}$, then by the polynomial property of congruences, $N = P(10) \equiv P(k) \pmod{m}$.

Theorem 6.9. ***Divisibility by powers of 2 and 5.***
Let m be a positive integer. An integer N is divisible by 2^m (respectively 5^m) if and only if the number formed by its last m digits is divisible by 2^m (respectively 5^m).

定理

Proof

Note that $10 \equiv 0 \pmod{2}$ and $10 \equiv 0 \pmod{5}$. Consequently, for $i \geq m$, $10^i \equiv 0 \pmod{2^m}$ and $10^i \equiv 0 \pmod{5^m}$. We can separate the summation for N:

$$N = \sum_{i=m}^{n} a_i 10^i + \sum_{i=0}^{m-1} a_i 10^i \equiv 0 + \overline{a_{m-1} \dots a_0} \pmod{2^m \text{ or } 5^m}.$$

Thus N is congruent to the number formed by its last m digits.

■

Theorem 6.10. ***Divisibility by 3 and 9.***
An integer N is divisible by 3 (respectively 9) if and only if the sum of its digits is divisible by 3 (respectively 9).

定理

Proof

We observe that $10 \equiv 1 \pmod{3}$ and $10 \equiv 1 \pmod{9}$. Therefore, $10^i \equiv 1^i \equiv 1$ for all $i \geq 0$.

$$N = \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i (1) \equiv \sum_{i=0}^{n} a_i \pmod{3 \text{ or } 9}.$$

■

Theorem 6.11. ***Divisibility by 11.***
An integer N is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. Specifically, the difference between the sum of digits in even positions and the sum of digits in odd positions must be a multiple of 11.

定理

Proof

We observe that $10 \equiv -1 \pmod{11}$. Thus $10^i \equiv (-1)^i \pmod{11}$.

$$N = \sum_{i=0}^{n} a_i 10^i \equiv \sum_{i=0}^{n} a_i (-1)^i \equiv a_0 - a_1 + a_2 - a_3 + \dots \pmod{11}.$$

■

Block Divisibility Tests

For divisors that do not divide 10 or 10 ± 1 simply, we can often find a power of 10 that provides a clean residue.

Theorem 6.12. ***Divisibility by 7, 11, and 13.***
Partition the digits of N into blocks of three, starting from the right: A_0 (last 3 digits), A_1 (next 3), etc. N is divisible by 7, 11, or 13 if and only if the alternating sum of these blocks $S = A_0 - A_1 + A_2 - \dots$ is divisible by 7, 11, or 13 respectively.

定理

Note

$7 \cdot 11 \cdot 13 = 1001$.

Proof

Since $1000 \equiv -1 \pmod{1001}$, it follows that $1000 \equiv -1$ modulo 7, 11, and 13. We write N in base 1000:

$$N = \sum_{k=0}^{m} A_k (1000)^k.$$

Taking the modulus $d \in \{7, 11, 13\}$:

$$N \equiv \sum_{k=0}^{m} A_k (-1)^k \equiv A_0 - A_1 + A_2 - \dots \pmod{d}.$$

■

Theorem 6.13. ***Divisibility by 37.***
N is divisible by 37 if and only if the sum of its 3-digit blocks is divisible by 37.

定理

$N = \dots A_2 A_1 A_0$

A_2	A_1	A_0

Groups of 3 digits

Figure 6.2: Visualisation of block decomposition for Theorem 2.15.

Proof

We observe that $3 \times 37 = 111$ and $27 \times 37 = 999$. Thus $1000 \equiv 1 \pmod{37}$.

$$N = \sum_{k=0}^{m} A_k (1000)^k \equiv \sum_{k=0}^{m} A_k (1)^k \equiv \sum_{k=0}^{m} A_k \pmod{37}.$$

■

Example 6.11. Application of Block Rules. Is the number $N = 75,312,289$ divisible by 13?
We split N into 3-digit blocks: $A_0 = 289$, $A_1 = 312$, $A_2 = 75$. Compute the alternating sum:

$$S = A_0 - A_1 + A_2 = 289 - 312 + 75 = 52.$$

Since $52 = 4 \times 13$, S is divisible by 13. Therefore, N is divisible by 13.

範例

While the block method is powerful for large numbers, a recursive test exists for divisibility by 7 using only the last digit.

Proposition 6.2. ***The "Osculation" Test for 7.***
An integer $N = 10a + b$ is divisible by 7 if and only if $a - 2b$ is divisible by 7.

命題

Note

$10 \equiv 3 \pmod{7}$.

Proof

We require a condition equivalent to $10a + b \equiv 0 \pmod{7}$. Since $(10, 7) = 1$, we can multiply the congruence by the modular inverse of 10. We seek an inverse x such that $3x \equiv 1 \pmod{7}$. Testing values: $3 \times (-2) = -6 \equiv 1 \pmod{7}$. Thus, the inverse is -2. Multiplying by -2:

$$-2(10a + b) \equiv -2(0) \implies -20a - 2b \equiv 0 \pmod{7}.$$

Since $-20 \equiv 1 \pmod{7}$, this simplifies to:

$$a - 2b \equiv 0 \pmod{7}.$$

■

Remark (Application).

Test 392. $a = 39, b = 2$. Check $39 - 2(2) = 35$. Since 35 is divisible by 7, 392 is divisible by 7.

Example 6.12. Reconstructing Missing Digits. The number $N = 341d52$ is known to be divisible by 8 and 9. Determine the digit d.

Divisibility by 8. N is divisible by 8 if and only if the number formed by the last three digits, $100d + 52$, is divisible by 8. We check values for d. Note $100 \equiv 4 \pmod 8$.

$$100d + 52 \equiv 4d + 52 \equiv 4d + 4 \pmod 8.$$

We require $4(d+1)$ to be a multiple of 8. This implies $d+1$ must be even, so d must be odd. Possible values for $d \in \{1, 3, 5, 7, 9\}$.

Divisibility by 9. The sum of digits must be divisible by 9.

$$\text{Sum} = 3 + 4 + 1 + d + 5 + 2 = 15 + d.$$

We require $15 + d \equiv 0 \pmod 9$, which implies $6 + d \equiv 0 \pmod 9$. Thus $d \equiv -6 \equiv 3 \pmod 9$. The only digit satisfying this is $d = 3$.

Verification: Since $d = 3$ is odd, it satisfies the condition derived from the modulo 8 check. The number is 341352. $341352/8 = 42669$ and $341352/9 = 37928$.

範例

Example 6.13. Smallest Multiple with Distinct Digits. Find the smallest six-digit number with distinct digits that is divisible by 5 and 11.

Let the number be N. For N to be minimal:

(i) The leading digit should be as small as possible (1).

(ii) The subsequent digits should be small (0, then 2, 3...).

Let's try the form $N = 10abcd$. The digits used so far are $\{0, 1\}$. For divisibility by 5, the last digit d must be 0 or 5. Since 0 is already used, $d = 5$. So $N = 10abc5$. The remaining digits a, b, c must be distinct and chosen from $\{2, 3, 4, 6, 7, 8, 9\}$. For divisibility by 11:

$$(1 + a + c) - (0 + b + 5) \equiv 0 \pmod{11} \implies a + c - b - 4 \equiv 0 \pmod{11}.$$

So $a + c - b = 4$ or $a + c - b = 15$ (since digits sum to at most $9 + 8 = 17$).

To minimise N, we want smallest a, then smallest b. Try to satisfy $a + c - b = 4$ with small a.

· Try $a = 2$. Then $2 + c - b = 4 \implies c - b = 2 \implies c = b + 2$. We need small b. If $b = 3$, then $c = 5$. But 5 is used for the last digit. Reject. If $b = 4$, then $c = 6$. Digits used: $\{0, 1, 2, 4, 6, 5\}$. All distinct. This gives the number 102465.

> Let's check if we could have obtained a smaller number with $a + c - b = 15$. This would require large a or c, which contradicts minimality. Is there a solution with $a = 2$ and $b < 4$? If $b = 3, c = 5$ (Fail). If $b < 3$, say $b = 2$ (Fail, $a \neq b$). Thus, 102465 is the smallest solution.
>
> 範例

6.6 Exercises

1. **The Freshman's Dream.** Let p be a prime. Prove that for any integers a and b:
$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$
> *Remark.*
>
> Expand the binomial and consider the divisibility of the coefficient $\binom{p}{k}$.

2. **Divisibility Conditions on Exponents.** Find all positive integers n such that $5^{2n} + 3^{2n}$ is divisible by 17.

3. **Calendar Calculation.** The 30th National Day (October 1st) in 1979 was a Monday. Determine the day of the week for the 100th National Day in 2049.

Account for the leap years between 1979 and 2049.

4. **Cubes Modulo 5.** Prove that the difference of the cubes of two consecutive integers cannot be divisible by 5.

5. **Sum of Powers.** Prove that $1^n + 2^n + 3^n + 4^n$ is divisible by 5 if and only if n is not a multiple of 4.

6. **Non-Existence of Perfect Powers.** An integer is a perfect power if it can be written as a^k for $a > 1, k > 1$. Prove that for any prime p, the number $2^p + 3^p$ is not a perfect power.

7. **Power Towers Modulo Powers of 2.** Let a be an odd positive integer. Prove that for any $n \geq 1$:
$$a^{2^n} \equiv 1 \pmod{2^{n+2}}.$$

8. **Solitary Numbers.** A number n is solitary if no $m \neq n$ satisfies $\sigma(m)/m = \sigma(n)/n$. Prove that any power of 2, $n = 2^r$, is solitary. Note: The text exercise defined solitary differently ($\sigma(n) = \sigma(m) = n + m$), but this is the standard definition related to friendly numbers. Stick to the text's definition if required: prove no m exists such that $\sigma(n) = \sigma(m) = n + m$.

9. **Composite Divisibility.** Let n be a positive integer. Prove that $330 \mid (6^{2n} - 5^{2n} - 11)$.

10. **Square of Primes Modulo 24.** Prove that for any prime $p > 3$, $p^2 \equiv 1 \pmod{24}$.

11. **Non-Existence of Special Integers.** Let $p_1, \ldots, p_n$ be distinct odd primes ($n \geq 2$) and $N = \prod p_j$. Let $m_j = N/p_j$. Prove that it is impossible for $p_j^2 \mid (m_j - 1)$ to hold for all $j = 1, \ldots, n$.

12. **Divisibility Verification.** Verify explicitly using congruence criteria:
    (a) 237293 is divisible by 7.
    (b) 4553294 is divisible by 37.

13. **Criterion for 101.** Derive a divisibility criterion for the number 101 based on blocks of digits.

14. **Palindromes and 11.**
    (a) Prove that every four-digit palindrome is divisible by 11.
    (b) Is every six-digit palindrome divisible by 11? Prove or provide a counterexample.

15. **Digit Reconstruction.** The eight-digit number $141x28y3$ is divisible by 99. Find the digits x and y.

16. **Smallest 3-7 Number.** Find the smallest positive integer composed entirely of the digits 3 and 7 such that both the number itself and the sum of its digits are divisible by both 3 and 7.

7
Residue Classes and Complete Systems

Building upon the theory of congruence, we now formalise the classification of integers based on their remainders. This leads to the concept of residue classes, which partition the set of integers into disjoint sets. By selecting representatives from these sets, we form complete residue systems—fundamental structures that allow us to reduce infinite problems over $\mathbb{Z}$ to finite computations.

7.1 Residue Classes

The congruence relation modulo m is an equivalence relation, and like any equivalence relation, it partitions the underlying set into equivalence classes.

Definition 7.1. ***Residue Class.***
Let m be a positive integer. For any integer r where $0 \leq r < m$, the **residue class** corresponding to r is the set of all integers congruent to r modulo m:

$$S_r = \{mq + r \mid q \in \mathbb{Z}\}.$$

The set of integers is the disjoint union of the m residue classes $S_0, S_1, \ldots, S_{m-1}$.

定義

For instance, modulo 2 partitions the integers into two classes: the evens (S_0) and the odds (S_1).
To perform arithmetic modulo m, we typically select a single representative from each class.

Definition 7.2. ***Complete Residue System.***
A set of m integers is called a **complete residue system** modulo m if it contains exactly one element from each residue class $S_0, \ldots, S_{m-1}$. Equivalently, a set A is a complete residue system modulo m if $|A| = m$ and for every integer n, there exists a unique $a \in A$ such that $n \equiv a \pmod{m}$.

定義

While any set of representatives suffices, two specific systems are standard due to their symmetry and simplicity.

Definition 7.3. ***Standard Residue Systems.***

1. The **least non-negative complete residue system** modulo m is the set:
$$\{0, 1, 2, \ldots, m-1\}.$$
2. The **absolute least complete residue system** modulo m balances representatives around zero to minimise their absolute values.
   - If m is odd, the system is:
   $$\left\{-\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2}\right\}.$$
   - If m is even, one typically chooses:
   $$\left\{-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2}\right\} \quad \text{or} \quad \left\{-\frac{m}{2}, \ldots, -1, 0, 1, \ldots, \frac{m}{2}-1\right\}.$$

定義

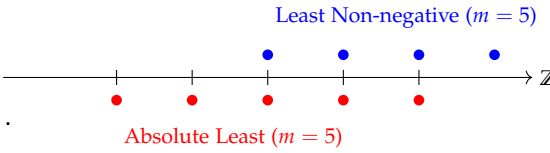


Figure 7.1: Comparison of residue systems for $m = 5$. The least non-negative system corresponds to standard division remainders, while the absolute least system minimises magnitude.

Example 7.1. Verifying a System. Verify that the set $A = \{-10, -6, -1, 2, 10, 12, 14\}$ is a complete residue system modulo 7. We compute the least non-negative residue of each element modulo 7:

$$\begin{aligned} -10 &\equiv 4 \pmod 7 \\ -6 &\equiv 1 \pmod 7 \\ -1 &\equiv 6 \pmod 7 \\ 2 &\equiv 2 \pmod 7 \\ 10 &\equiv 3 \pmod 7 \\ 12 &\equiv 5 \pmod 7 \\ 14 &\equiv 0 \pmod 7 \end{aligned}$$

The set of remainders is $\{4, 1, 6, 2, 3, 5, 0\}$. Rearranging these yields $\{0, 1, 2, 3, 4, 5, 6\}$, which is the standard least non-negative system. Since A contains 7 elements that map to distinct residue classes, A is a complete residue system.

範例

Arithmetic Applications

The choice of residue system often simplifies divisibility proofs. The absolute least system is particularly useful when evaluating

polynomials, as it keeps the base values small.

Example 7.2. Quadratic Residues and Factorials.

1. **Squares modulo 5:** Prove that an integer congruent to 2 or 3 modulo 5 cannot be a perfect square.

   Let x be an integer. We test x using the absolute least complete residue system modulo 5: $\{0, \pm 1, \pm 2\}$.

   · If $x \equiv 0$, then $x^2 \equiv 0$.

   · If $x \equiv \pm 1$, then $x^2 \equiv 1$.

   · If $x \equiv \pm 2$, then $x^2 \equiv 4$.

   The possible residues of a square modulo 5 are $\{0, 1, 4\}$. Thus, no square is congruent to 2 or 3 modulo 5.

2. **Sums of Factorials:** Prove that for $n > 3$, the sum $S_n = \sum_{k=1}^{n} k!$ is not a perfect square.

   For $n = 4$, $S_4 = 1! + 2! + 3! + 4! = 1 + 2 + 6 + 24 = 33$. This is not a square. For $n \geq 5$, we observe that $k! \equiv 0 \pmod 5$ for all $k \geq 5$. Thus, for $n \geq 5$:

   $$S_n = S_4 + \sum_{k=5}^{n} k! \equiv 33 + 0 \equiv 3 \pmod 5.$$

   From part (1), we established that a perfect square cannot be congruent to 3 modulo 5. Therefore, S_n is never a perfect square for $n > 3$.

範例

Example 7.3. Divisibility of Cubic Products. Prove that the product of three consecutive integers, where the middle term is a perfect cube, is divisible by 504. Let the integers be $n^3 - 1, n^3, n^3 + 1$. The product is $N = (n^3 - 1)n^3(n^3 + 1)$. We observe that $504 = 7 \times 8 \times 9$. Since these factors are pairwise coprime, it suffices to show divisibility by 7, 8, and 9 individually.

Modulo 7: We consider n in the absolute least residue system modulo 7: $\{0, \pm 1, \pm 2, \pm 3\}$.

· If $n \equiv 0$, then $n^3 \equiv 0$, so $7 \mid N$.

· If $n \equiv \pm 1$, then $n^3 \equiv \pm 1$, so $n^3 \mp 1 \equiv 0$, implying $7 \mid N$.

· If $n \equiv \pm 2$, then $n^3 \equiv \pm 8 \equiv \pm 1$, so $n^3 \mp 1 \equiv 0$, implying $7 \mid N$.

· If $n \equiv \pm 3$, then $n^3 \equiv \pm 27 \equiv \pm 6 \equiv \mp 1$, so $n^3 \pm 1 \equiv 0$, implying $7 \mid N$.

In all cases, $7 \mid N$.

Modulo 9: Similar to the modulo 7 case, the cubes modulo 9

are $0^3 = 0$, $(\pm 1)^3 = \pm 1$, $(\pm 2)^3 = \pm 8 \equiv \mp 1$, $(\pm 3)^3 \equiv 0$, $(\pm 4)^3 \equiv \pm 64 \equiv \pm 1$. The residues of n^3 modulo 9 are restricted to $\{0, 1, 8\}$. Thus, one of the factors n^3 (if 0), $n^3 - 1$ (if 1), or $n^3 + 1$ (if 8) is divisible by 9.

Modulo 8: If n is even, n^3 is divisible by 8. If n is odd, then n^3 is odd. The neighbours $n^3 - 1$ and $n^3 + 1$ are consecutive even integers. One is divisible by 2 and the other by 4, so their product is divisible by 8.

Since N is divisible by 7, 8, and 9, it is divisible by 504.

範例

Structural Properties

We now establish criteria for determining whether a set of integers forms a complete residue system without manually calculating every remainder.

Theorem 7.1. ***Characterisation of Complete Residue Systems.***
Let m be a positive integer. A set of m integers $\{a_1, a_2, \ldots, a_m\}$ forms a complete residue system modulo m if and only if the integers are pairwise incongruent modulo m.

定理

Proof

Since there are m distinct residue classes modulo m, a set of m integers constitutes a complete system if and only if each integer belongs to a distinct class. This is equivalent to the condition that no two integers are congruent modulo m.

■

A powerful feature of residue systems is their invariance under affine transformations, provided the scaling factor is coprime to the modulus.

Theorem 7.2. ***Affine Transformations.***
Let m be a positive integer and let a be an integer such that $(a, m) = 1$. If x runs through a complete residue system modulo m, then for any integer b, the expression $ax + b$ also runs through a complete residue system modulo m.

定理

Proof

Let $\{x_1, \ldots, x_m\}$ be a complete residue system. By *theorem 7.1*, it suffices to show that the m values $\{ax_1 + b, \ldots, ax_m + b\}$ are pairwise incongruent. Suppose, for the sake of contradiction, that for

some $i \neq j$:

$$ax_i + b \equiv ax_j + b \pmod{m}.$$

Subtracting b from both sides gives $ax_i \equiv ax_j \pmod{m}$. Since $(a, m) = 1$, *theorem 6.4* implies $x_i \equiv x_j \pmod{m}$. This contradicts the hypothesis that the x_k are distinct modulo m. Thus, the transformed values are pairwise incongruent and form a complete residue system.

■

Example 7.4. Generating a New System. Let $m = 12$. The set $S = \{0, 1, \ldots, 11\}$ is the standard system. Let $a = 5$ and $b = 7$. Since $(5, 12) = 1$, the set $\{5x + 7 \mid x \in S\}$ is also a complete residue system. For example, if $x = 2$, the element is $17 \equiv 5$. If $x = 3$, the element is $22 \equiv 10$. This transformation permutes the residue classes.

範例

Another fundamental property concerns the sum of the elements in a complete residue system.

Theorem 7.3. ***Sum of Residues.***
Let $S = \{y_1, \ldots, y_m\}$ be a complete residue system modulo m.

1. If m is odd, $\sum_{i=1}^{m} y_i \equiv 0 \pmod{m}$.
2. If m is even, $\sum_{i=1}^{m} y_i \equiv \frac{m}{2} \pmod{m}$.

定理

Proof

Since S is a complete residue system, its elements are congruent (in some order) to the least non-negative system $\{0, 1, \ldots, m-1\}$. Thus,

$$\sum_{i=1}^{m} y_i \equiv \sum_{k=0}^{m-1} k = \frac{m(m-1)}{2} \pmod{m}.$$

(m is odd). Since m is odd, $m - 1$ is even, so $(m-1)/2$ is an integer k. The sum is $mk \equiv 0 \pmod{m}$.

(m is even). Let $m = 2k$. Then $m - 1$ is odd. The sum is

$$\frac{2k(2k-1)}{2} = k(2k-1) = 2k^2 - k = mk - \frac{m}{2}.$$

Modulo m, this is congruent to $-m/2$, which is equivalent to $m/2$.

■

This theorem imposes a strong constraint on the structure of sums of residue systems.

Example 7.5. Additive Incompatibility. Let n be an even positive integer. Let $A = \{a_1, \ldots, a_n\}$ and $B = \{b_1, \ldots, b_n\}$ be two complete residue systems modulo n. Prove that the set of sums $C = \{a_1 + b_1, \ldots, a_n + b_n\}$ cannot be a complete residue system modulo n.
We sum the elements of the sets. By *theorem 7.3*, since n is even:

$$\sum a_i \equiv \frac{n}{2} \pmod{n} \quad \text{and} \quad \sum b_i \equiv \frac{n}{2} \pmod{n}.$$

If C were a complete residue system, its sum would also satisfy:

$$\sum (a_i + b_i) \equiv \frac{n}{2} \pmod{n}.$$

However, by linearity:

$$\sum (a_i + b_i) = \sum a_i + \sum b_i \equiv \frac{n}{2} + \frac{n}{2} = n \equiv 0 \pmod{n}.$$

This leads to the contradiction $\frac{n}{2} \equiv 0 \pmod{n}$, which is impossible for $n > 0$. Thus, C cannot be a complete residue system.

範例

Example 7.6. Sum Constraint Verification. Consider $m = 6$. Suppose we form a set $S = \{x, x+2, x+4, x+6, x+8, x+10\}$. Can S be a complete residue system for any integer x? The elements are an arithmetic progression with difference 2. Since $(2, 6) = 2 \neq 1$, *theorem 7.2* does not apply. Let us calculate the sum of elements in S:

$$\Sigma = 6x + (2 + 4 + 6 + 8 + 10) = 6x + 30.$$

Modulo 6, $\Sigma \equiv 0 + 30 \equiv 0 \pmod{6}$. However, by *theorem 7.3*, the sum of a complete residue system modulo 6 (even) must be congruent to $6/2 = 3$. Since $0 \not\equiv 3 \pmod{6}$, S is never a complete residue system.

範例

Composite Moduli Constructions

When the modulus is composite, we can construct complete residue systems by combining systems modulo the factors. This is the foundation for the Chinese Remainder Theorem, which we will treat fully in a later chapter.

Theorem 7.4. ***Coprime Linear Combination.***
Let m_1, m_2 be coprime positive integers. If x_1 runs through a complete residue system modulo m_1 and x_2 runs through a complete residue sys-

tem modulo m_2, then the linear combination

$$m_2x_1 + m_1x_2$$

runs through a complete residue system modulo m_1m_2.

定理

Proof

The set of values generated is of size m_1m_2, which matches the modulus size. By *theorem 7.1*, we need only show that these values are distinct modulo m_1m_2. Assume:

$$m_2x_1 + m_1x_2 \equiv m_2x_1' + m_1x_2' \pmod{m_1m_2}.$$

This implies divisibility by both m_1 and m_2.

1. Modulo m_1: $m_2x_1 \equiv m_2x_1' \pmod{m_1}$. Since $(m_2, m_1) = 1$, we cancel m_2 to get $x_1 \equiv x_1' \pmod{m_1}$. Since x_1, x_1' are from a CRS mod m_1, $x_1 = x_1'$.
2. Modulo m_2: $m_1x_2 \equiv m_1x_2' \pmod{m_2}$. Similarly, $(m_1, m_2) = 1$ implies $x_2 \equiv x_2' \pmod{m_2}$, so $x_2 = x_2'$.

Since the components are identical, the values are distinct.

■

Note

$(3, 4) = 1$.

Example 7.7. Constructing a System Modulo 12. Let $m_1 = 3$ and $m_2 = 4$. Let $S_3 = \{0, 1, 2\}$ and $S_4 = \{0, 1, 2, 3\}$. We form the set $S = \{4x_1 + 3x_2 \mid x_1 \in S_3, x_2 \in S_4\}$. For instance:

· $x_1 = 0, x_2 = 1 \implies 3$.

· $x_1 = 1, x_2 = 0 \implies 4$.

· $x_1 = 2, x_2 = 3 \implies 4(2) + 3(3) = 17 \equiv 5 \pmod{12}$.

This construction generates exactly 12 distinct integers modulo 12, providing a structured way to decompose the modulus.

範例

This principle generalizes to products of arbitrary length.

Theorem 7.5. ***Polyadic Expansion.***

Let $m_1, \ldots, m_k$ be positive integers. If x_i runs through a complete residue system modulo m_i for each i, then the sum

$$x_1 + m_1x_2 + m_1m_2x_3 + \cdots + (m_1 \ldots m_{k-1})x_k$$

runs through a complete residue system modulo $M = m_1m_2 \ldots m_k$.

定理

Proof

We proceed by induction or direct uniqueness verification. The expression is analogous to a mixed-radix representation. Consider two such sums S and S' being congruent modulo M.

$$\sum_{j=1}^{k} P_{j-1} x_j \equiv \sum_{j=1}^{k} P_{j-1} x'_j \pmod{M},$$

where $P_0 = 1$ and $P_j = m_1 \dots m_j$. Considering the congruence modulo m_1:

$$x_1 \equiv x'_1 \pmod{m_1}.$$

Thus $x_1 = x'_1$. We subtract this term and divide by m_1:

$$x_2 + m_2 x_3 + \cdots \equiv x'_2 + m_2 x'_3 + \dots \pmod{m_2 \dots m_k}.$$

Repeating the argument modulo m_2 yields $x_2 = x'_2$, and so forth. All coefficients must be identical, proving distinctness.

■

Corollary 7.1. *Base-n Representation.* By setting $m_1 = m_2 = \cdots = m_k = n$, we recover the standard base-n expansion. If $x_i \in \{0, \dots, n-1\}$, the sum

$$x_1 + n x_2 + \cdots + n^{k-1} x_k$$

generates the complete residue system $\{0, 1, \dots, n^k - 1\}$ modulo n^k.

推論

Advanced Examples

We conclude with two results illustrating the interaction between residue systems and real analysis or combinatorics.

Example 7.8. Sum of Fractional Parts. Let $m > 0$ and $(a, m) = 1$. Prove that if x runs through a complete residue system modulo m, then

$$\sum_{x} \left\{ \frac{ax + b}{m} \right\} = \frac{m-1}{2},$$

where $\{y\} = y - \lfloor y \rfloor$ denotes the fractional part.
By *theorem 7.2*, the values $z = ax + b$ form a complete residue system modulo m. Modulo m, the set $\{z\}$ is congruent to $\{0, 1, \dots, m-1\}$. For each z, the term $\frac{z}{m}$ can be written as $I + \frac{r}{m}$, where I is an integer and $r \in \{0, \dots, m-1\}$. The fractional part is simply $\frac{r}{m}$. Summing over the system:

$$\sum_{r=0}^{m-1} \frac{r}{m} = \frac{1}{m} \sum_{r=0}^{m-1} r = \frac{1}{m} \frac{(m-1)m}{2} = \frac{m-1}{2}.$$

範例

Example 7.9. Legendre's Property for Binomial Coefficients. Let p be a prime. Verify that

$$\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \pmod{p}.$$

Consider the set of p consecutive integers $S = \{n, n-1, \ldots, n-p+1\}$. By *theorem 7.1*, S is a complete residue system modulo p. Thus, exactly one element in S is divisible by p. Let this element be $n - i$, where $0 \leq i \leq p-1$. We can express the floor function as:

$$\left\lfloor \frac{n}{p} \right\rfloor = \frac{n-i}{p}.$$

Now consider the binomial coefficient:

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

Rearranging terms to isolate the multiple of p:

$$p!\binom{n}{p} = n(n-1)\ldots(n-p+1).$$

Let $M = \prod_{j \neq i}(n-j)$. This product contains $p-1$ integers forming a reduced residue system (excluding the multiple of p), so it is a permutation of $\{1, \ldots, p-1\}$ modulo p. Hence $M \equiv (p-1)! \pmod{p}$. Substituting $n - i = p\lfloor n/p \rfloor$:

$$p!\binom{n}{p} = M \cdot p \left\lfloor \frac{n}{p} \right\rfloor.$$

Dividing by p:

$$(p-1)!\binom{n}{p} = M \left\lfloor \frac{n}{p} \right\rfloor.$$

Modulo p, since $M \equiv (p-1)! \pmod{p}$:

$$(p-1)!\binom{n}{p} \equiv (p-1)! \left\lfloor \frac{n}{p} \right\rfloor \pmod{p}.$$

Since $(p-1)!$ is coprime to p, we can cancel it to obtain:

$$\binom{n}{p} \equiv \left\lfloor \frac{n}{p} \right\rfloor \pmod{p}.$$

範例

7.2 *Euler's Totient Function*

Lets now restrict our attention to integers that are coprime to the modulus. This restriction isolates the multiplicative structure of the integers modulo m, leading to the definition of Euler's Totient Function and Reduced Residue Systems.
We denote the count of positive integers up to a given integer m that are relatively prime to m by $\varphi(m)$.

Definition 7.4. ***Euler's Totient Function.***
For a positive integer m, Euler's function $\varphi(m)$ is defined as the cardinality of the set of integers $\{k \in \mathbb{Z} \mid 1 \leq k \leq m, (k,m) = 1\}$.

定義

For example, if $m = 10$, the integers in the range $[1,10]$ coprime to 10 are $\{1,3,7,9\}$. Thus $\varphi(10) = 4$. By convention, $\varphi(1) = 1$.
If p is a prime, every positive integer less than p is coprime to p. Consequently, $\varphi(p) = p - 1$.
To calculate $\varphi(m)$ for composite m, we rely on the *theorem* 5.1 (Inclusion-Exclusion) established in the previous chapter.

Theorem 7.6. ***Euler's Product Formula.***
Let the canonical factorisation of a positive integer m be $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Then:

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

定理

Proof

Let $S = \{1, 2, \dots, m\}$. We wish to count the elements of S that share no prime factors with m. The prime factors of m are exactly $p_1, \dots, p_k$. Let property α_i be that an integer is divisible by p_i. We seek the number of elements satisfying none of these properties. The number of multiples of a divisor d in S is exactly m/d. By *theorem* 5.1:

$$\begin{aligned}\varphi(m) &= m - \sum \frac{m}{p_i} + \sum \frac{m}{p_i p_j} - \dots + (-1)^k \frac{m}{p_1 \dots p_k} \\ &= m \left(1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \dots\right).\end{aligned}$$

This alternating sum factors exactly into the product:

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

Multiplying $m = \prod p_i^{a_i}$ into the product term-wise yields the second

form:

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

■

Corollary 7.2. *Multiplicativity of φ.* If m and n are coprime positive integers, then $\varphi(mn) = \varphi(m)\varphi(n)$.

推論

Example 7.10. Calculating Totients. We compute $\varphi(2008)$. The prime factorisation is $2008 = 8 \times 251 = 2^3 \times 251$.

$$\varphi(2008) = 2008 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{251}\right) = 2008 \cdot \frac{1}{2} \cdot \frac{250}{251} = 1000.$$

範例

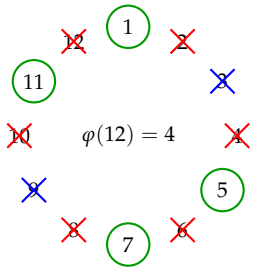


Figure 7.2: Visualisation of $\varphi(12)$. We eliminate multiples of 2 (red) and 3 (blue). The remaining integers $\{1, 5, 7, 11\}$ are circled.

The Sum of Coprime Integers

While $\varphi(m)$ counts the integers coprime to m, we can also determine their sum using the symmetry of the greatest common divisor.

Theorem 7.7. ***Sum of Coprimes.***
Let $\varepsilon(m)$ denote the sum of positive integers not exceeding m that are coprime to m. For $m \geq 2$:

$$\varepsilon(m) = \frac{m}{2}\varphi(m).$$

定理

Proof

Let $K = \{k_1, k_2, \ldots, k_{\varphi(m)}\}$ be the set of integers in $[1, m]$ coprime to m. We observe that $(k, m) = 1$ if and only if $(m - k, m) = 1$. Let $d = (m, m - k)$. Then $d \mid m$ and $d \mid (m - k)$, which implies $d \mid k$. Since $(m, k) = 1$, we must have $d = 1$. Thus, the set K is invariant under the mapping $k \mapsto m - k$. We can express the sum $\varepsilon(m)$ in two ways:

$$\varepsilon(m) = \sum_{i=1}^{\varphi(m)} k_i$$

$$\varepsilon(m) = \sum_{i=1}^{\varphi(m)} (m - k_i) = m\varphi(m) - \sum_{i=1}^{\varphi(m)} k_i.$$

Adding these equations yields $2\varepsilon(m) = m\varphi(m)$, from which the result follows.

■

Example 7.11. Sum Calculation. Calculate $\varepsilon(420)$. First, factorise $420 = 42 \times 10 = 2^2 \cdot 3 \cdot 5 \cdot 7$. Compute $\varphi(420)$:

$$\varphi(420) = 420\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 420 \cdot \frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7} = 96.$$

Then calculate the sum:

$$\varepsilon(420) = \frac{420}{2} \times 96 = 210 \times 96 = 20160.$$

範例

7.3 *Reduced Residue Systems*

Analogous to the complete residue system, which contains representatives for all residue classes, the reduced residue system focuses solely on the classes coprime to the modulus.

Definition 7.5. ***Reduced Residue System.***
A **reduced residue system** modulo m is a set of $\varphi(m)$ integers such that:
1. Each integer in the set is coprime to m.
2. No two integers in the set are congruent modulo m.

Equivalently, it is a set containing exactly one representative from each residue class coprime to m.

定義

For $m = 8$, the complete system is $\{0,1,2,3,4,5,6,7\}$. Removing those sharing factors with 8 (evens) leaves $\{1,3,5,7\}$, which is a reduced residue system.

Theorem 7.8. ***Preservation under Multiplication.***
Let $(a,m) = 1$. If $\{x_1,\ldots,x_{\varphi(m)}\}$ is a reduced residue system modulo m, then the set $\{ax_1,\ldots,ax_{\varphi(m)}\}$ is also a reduced residue system modulo m.

定理

Proof

Since $(x_i,m) = 1$ and $(a,m) = 1$, it follows that $(ax_i,m) = 1$. Thus, the new elements are coprime to m. To check distinctness, assume $ax_i \equiv ax_j \pmod m$. Since $(a,m) = 1$, *theorem 6.4* implies $x_i \equiv x_j \pmod m$. As the original set was distinct modulo m, so is the new set. Being a set of $\varphi(m)$ distinct residues coprime to m, it is a reduced residue system.

■

We can also construct reduced systems for composite moduli using linear combinations of systems for the factors.

Theorem 7.9. ***Composite Construction.***
Let m_1 and m_2 be coprime positive integers. If x_1 runs through a reduced residue system modulo m_1 and x_2 runs through a reduced residue system modulo m_2, then

$$m_2x_1 + m_1x_2$$

runs through a reduced residue system modulo m_1m_2.

定理

Proof

There are $\varphi(m_1)$ choices for x_1 and $\varphi(m_2)$ choices for x_2. The total number of generated values is $\varphi(m_1)\varphi(m_2) = \varphi(m_1m_2)$ (by multiplicativity). By *theorem 7.4*, linear combinations of this form are pairwise incongruent modulo m_1m_2. It remains to show that each value is coprime to m_1m_2. Let $N = m_2x_1 + m_1x_2$. Since $(x_1, m_1) = 1$ and $(m_2, m_1) = 1$, we have $(m_2x_1, m_1) = 1$. Thus:

$$(N, m_1) = (m_2x_1 + m_1x_2, m_1) = (m_2x_1, m_1) = 1.$$

Similarly, $(x_2, m_2) = 1$ implies $(N, m_2) = 1$. Since N is coprime to both m_1 and m_2, and $(m_1, m_2) = 1$, N is coprime to m_1m_2. Thus, the values form a reduced residue system.

■

Applications and Examples

Example 7.12. Power Properties of Totients. Prove that $\varphi(n^k) = n^{k-1}\varphi(n)$ for any integer $n \geq 1$ and $k \geq 1$.
Using *theorem 7.6*, let the prime factorisation of n be $\prod p_i^{e_i}$. Then $n^k = \prod p_i^{ke_i}$.

$$\begin{aligned}\varphi(n^k) &= n^k \prod_{p|n} \left(1 - \frac{1}{p}\right) \\ &= n^{k-1} \cdot n \prod_{p|n} \left(1 - \frac{1}{p}\right) \\ &= n^{k-1}\varphi(n).\end{aligned}$$

This identity is useful for simplifying totient calculations of powers.

範例

Proposition 7.1. ***Primality Conditions.***
Let $n \geq 2$. Prove that n is prime if and only if $\varphi(n) \mid (n-1)$ and $(n+1) \mid \sigma(n)$.

命題

Necessity.

If n is prime, $\varphi(n) = n - 1$ (divides itself) and $\sigma(n) = n + 1$ (divides itself). The conditions hold.

証明終

Sufficiency.

Assume $\varphi(n) \mid (n-1)$ and $(n+1) \mid \sigma(n)$ for $n \geq 3$. Since $\varphi(n)$ is even for $n > 2$, $n - 1$ must be even, so n is odd.
Suppose n is not square-free, i.e., $p^2 \mid n$. Then $p \mid \varphi(n)$, which implies $p \mid (n-1)$. But $p \mid n$, so $p \mid 1$, a contradiction. Thus n is square-free, $n = p_1 p_2 \dots p_k$. Then $\varphi(n) = \prod(p_i - 1)$ and $\sigma(n) = \prod(p_i + 1)$.
If $k > 1$, then $\varphi(n)$ is divisible by 2^k. Since $\varphi(n) \mid (n-1)$, $n - 1$ is divisible by 2^k. Consequently, $n + 1 = (n-1) + 2$ is not divisible by 4, only by 2.
We are given $(n+1) \mid \sigma(n)$. Since $\sigma(n)$ is divisible by 2^k (product of k even terms), and $n + 1$ is only divisible by 2, consider the ratio $R = \sigma(n)/(n+1)$. We have $2^{k-1} \mid R$.
However,

$$R = \frac{\sigma(n)}{n+1} < \frac{\sigma(n)}{n} = \prod \left(1 + \frac{1}{p_i}\right).$$

Since $p_i \geq 3$, $1 + 1/p_i \leq 4/3$. Thus $R < (4/3)^k$. We require $2^{k-1} \leq (4/3)^k$. But $\frac{(4/3)^k}{2^{k-1}} = 2\left(\frac{2}{3}\right)^k \leq \frac{8}{9}$ for $k \geq 2$, so the inequality fails for all $k \geq 2$. Thus $k = 1$, and n is prime.

証明終

Example 7.13. Sum of Powers. Let p be an odd prime and m be a positive integer such that $2^m \not\equiv 1 \pmod{p}$. Verify that $\sum_{i=1}^{p-1} i^m \equiv 0 \pmod{p}$.
The set $S = \{1, 2, \dots, p-1\}$ is a reduced residue system modulo p. Since $(2, p) = 1$, the set $2S = \{2, 4, \dots, 2(p-1)\}$ is also a reduced residue system (by preservation under multiplication). The sum of m-th powers must be congruent modulo p:

$$\sum_{x \in S} x^m \equiv \sum_{x \in 2S} x^m \pmod{p}.$$

Substituting the elements:

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

Let $\Sigma = \sum i^m$. Then $\Sigma \equiv 2^m \Sigma \pmod{p}$, or $\Sigma(2^m - 1) \equiv 0 \pmod{p}$. Since $2^m \not\equiv 1 \pmod{p}$, p does not divide $2^m - 1$. By *corollary* 1.5, $p \mid \Sigma$, so the sum is congruent to 0.

範例

Example 7.14. Sum of Fractional Parts. Let $m > 1$ and $(a, m) = 1$. Prove that if y runs through a reduced residue system modulo m, then

$$\sum_{y} \left\{ \frac{ay}{m} \right\} = \frac{1}{2}\varphi(m).$$

The set $\{ay\}$ forms a reduced residue system modulo m. Let the residues modulo m be $r_1, \ldots, r_{\varphi(m)}$. Then $\{\frac{ay}{m}\} = \{\frac{r_i}{m}\} = \frac{r_i}{m}$ (since $0 < r_i < m$). The sum is $\frac{1}{m}\sum r_i$. This is exactly $\frac{1}{m}\varepsilon(m)$. Using *theorem 7.7*:

$$\text{Sum} = \frac{1}{m}\left(\frac{m}{2}\varphi(m)\right) = \frac{1}{2}\varphi(m).$$

Alternatively, observe that residues in a reduced system pair up as r and $m - r$. Then $\frac{r}{m} + \frac{m-r}{m} = 1$. There are $\varphi(m)/2$ such pairs.

範例

Example 7.15. Totient Lower Bound. Show that if a composite integer n has k distinct prime factors, then $\varphi(n) \geq 2^k$. Note that this is a loose bound for large primes but illustrative for structure.

範例

Proof

Let $n = p_1^{a_1} \ldots p_k^{a_k}$.

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

Since each $(p_i - 1) \geq 2$, we have $\varphi(n) \geq \prod_{i=1}^{k}(p_i - 1) \geq 2^k$. If n is odd, each p_i is odd, so $p_i - 1$ is even and the product contains at least k factors of 2. Hence $2^k \mid \varphi(n)$. This confirms the structural result used in the primality test example earlier.

■

7.4 *Euler's Theorem and Fermat's Little Theorem*

We now arrive at two of the most significant results in elementary number theory. By exploiting the structure of reduced residue systems, we can generalise the periodic behaviour of powers modulo m.

Theorem 7.10. ***Euler's Theorem.***
Let m be an integer greater than 1. If a is an integer coprime to m, then

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

定理

Proof

Let $R = \{r_1, r_2, \ldots, r_{\varphi(m)}\}$ be a reduced residue system modulo m. Since $(a, m) = 1$, the set $aR = \{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ is also a reduced residue system modulo m (as proved in the previous section). Consequently, the product of elements in aR must be congruent to the product of elements in R modulo m:

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

Factoring out a from each term on the left:

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

Let $P = \prod r_i$. Since each r_i is coprime to m, their product P is also coprime to m. By the Cancellation Law, we can divide both sides by P:

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

■

In the special case where the modulus is a prime p, we have $\varphi(p) = p - 1$. This yields Fermat's result, dating back to 1640.

Theorem 7.11. ***Fermat's Little Theorem.***
If p is a prime number and $p \nmid a$, then

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

定理

Proof

This follows immediately from *theorem 7.10* with $m = p$ and $\varphi(p) = p - 1$.

■

Corollary 7.3. *Fermat's Theorem (Alternative Form).* If p is a prime number, then for any integer a:

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

推論

Proof

If $p \nmid a$, we multiply the congruence $a^{p-1} \equiv 1 \pmod{p}$ by a to get $a^p \equiv a \pmod{p}$. If $p \mid a$, then $a \equiv 0 \pmod{p}$, so $a^p \equiv 0 \equiv a \pmod{p}$.

■

Computational Applications

These theorems are indispensable for reducing large exponents.

Example 7.16. Calculating Remainders of Towers. Find the last three digits of 243^{402}. This is equivalent to finding $243^{402} \pmod{1000}$. We first compute $\varphi(1000)$. Since $1000 = 2^3 \times 5^3$:

$$\varphi(1000) = 1000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400.$$

Note that $(243, 1000) = 1$ (as $243 = 3^5$). By Euler's Theorem, $243^{400} \equiv 1 \pmod{1000}$. Thus:

$$243^{402} = 243^{400} \cdot 243^2 \equiv 1 \cdot 243^2 \pmod{1000}.$$

Calculating the square:

$$243^2 = (200+43)^2 = 40000 + 2(200)(43) + 43^2 \equiv 17200 + 1849 \equiv 49 \pmod{1000}.$$

The last three digits are 049.

範例

Example 7.17. Date Calculation. If today is Monday, what day of the week will it be after $10^{10^{10}}$ days? We compute $10^{10^{10}} \pmod 7$. By Fermat's Little Theorem, since $(10, 7) = 1$, we have $10^6 \equiv 1 \pmod 7$. The exponent we need to reduce is $E = 10^{10}$ modulo 6.

$$10 \equiv 4 \pmod 6 \implies 10^{10} \equiv 4^{10} \pmod 6.$$

Notice that $4^1 = 4$, $4^2 = 16 \equiv 4 \pmod 6$. By induction, $4^k \equiv 4 \pmod 6$ for all $k \geq 1$. Thus $E \equiv 4 \pmod 6$, so $E = 6k + 4$ for some integer k.

$$10^E = 10^{6k+4} = (10^6)^k \cdot 10^4 \equiv 1^k \cdot 3^4 \equiv 81 \equiv 4 \pmod 7.$$

Monday + 4 days is Friday.

範例

Example 7.18. Large Divisibility. If a, b are coprime to 2730, prove that $a^{12} - b^{12}$ is divisible by 2730. Factorising the modulus: $2730 = 2 \times 3 \times 5 \times 7 \times 13$. The factors are distinct primes. We show $N = a^{12} - b^{12} \equiv 0$ modulo each prime $p \in \{2, 3, 5, 7, 13\}$.

- $p = 13$: By Fermat, $a^{12} \equiv 1$ and $b^{12} \equiv 1 \pmod{13}$. Thus $N \equiv 1 - 1 = 0$.
- $p = 7$: By Fermat, $a^6 \equiv 1$. Thus $a^{12} = (a^6)^2 \equiv 1$. Similarly $b^{12} \equiv 1$. $N \equiv 0$.
- $p = 5$: $a^4 \equiv 1 \implies a^{12} = (a^4)^3 \equiv 1$. $N \equiv 0$.

· $p = 3$: $a^2 \equiv 1 \implies a^{12} \equiv 1$. $N \equiv 0$.

· $p = 2$: a is odd, so $a^{12} \equiv 1$. $N \equiv 0$.

Since N is divisible by all pairwise coprime factors, it is divisible by their product 2730.

範例

Primality Testing and Pseudoprimes

Fermat's Little Theorem provides a necessary condition for primality. If $a^{N-1} \not\equiv 1 \pmod{N}$ for some $(a, N) = 1$, then N is composite. However, the converse is not true; there exist composite numbers that satisfy the congruence.

Definition 7.6. ***Pseudoprime*.**
A composite integer n is called a **pseudoprime to base** a if $a^{n-1} \equiv 1 \pmod{n}$. If n satisfies $a^n \equiv a \pmod{n}$ for all integers a, it is called an **absolute pseudoprime** or **Carmichael number**.

定義

Example 7.19. Verifying Composition. Show that $N = 91$ is composite using Fermat's test with base 2. We calculate $2^{90} \pmod{91}$. Powers of 2 modulo 91:

$$2^6 = 64$$
$$2^7 = 128 \equiv 37$$
$$2^8 = 74 \equiv -17$$
$$2^{16} \equiv (-17)^2 = 289 \equiv 16 \quad (289 - 3(91) = 289 - 273 = 16)$$
$$2^{32} \equiv 16^2 = 256 \equiv 74 \equiv -17$$
$$2^{64} \equiv (-17)^2 \equiv 16.$$

Decompose the exponent: $90 = 64 + 16 + 8 + 2$.

$$2^{90} = 2^{64} \cdot 2^{16} \cdot 2^8 \cdot 2^2 \equiv 16 \cdot 16 \cdot (-17) \cdot 4 \pmod{91}.$$

$$\equiv 256 \cdot (-68) \equiv 74 \cdot (-68) \pmod{91}.$$

Since $74 \equiv -17$, the product is $(-17)(-68) = 1156$. $1156 = 12 \times 91 + 64$. Thus $2^{90} \equiv 64 \not\equiv 1 \pmod{91}$. N is composite.

範例

Despite the existence of pseudoprimes, we can formulate a partial converse to Fermat's Little Theorem under stronger assumptions.

Theorem 7.12. ***Lucas' Primality Test*.**
If there exists an integer a such that:

1. $a^{m-1} \equiv 1 \pmod{m}$,
2. For every prime factor q of $m-1$, $a^{(m-1)/q} \not\equiv 1 \pmod{m}$,

then m is a prime number.

定理

Proof

Let d be the order of a modulo m (the smallest exponent such that $a^d \equiv 1$). Condition (1) forces $(a, m) = 1$; otherwise a prime $p \mid (a, m)$ would give $a^{m-1} \equiv 0 \pmod{p}$, contradicting $a^{m-1} \equiv 1 \pmod{m}$. Thus the order is well-defined, and from condition (1) we have $d \mid (m-1)$. Suppose $d < m-1$. Write $m-1 = dk$ with $k > 1$, and let q be any prime divisor of k. Then $d \mid (m-1)/q$, so $a^{(m-1)/q} \equiv 1 \pmod{m}$. This contradicts condition (2). Therefore, the order of a is exactly $m-1$. Since $(a, m) = 1$, Euler's Theorem applies and the order d divides $\varphi(m)$. Thus $(m-1) \mid \varphi(m)$. Since $\varphi(m) \leq m-1$ for all m, we must have $\varphi(m) = m-1$. This equality holds if and only if m is prime.

■

This theorem underpins proofs for the infinity of primes of certain forms.

Example 7.20. Primes of the Form $4k+1$. Prove there are infinitely many primes of the form $4k+1$.

範例

Proof

Consider the number $N = (m!)^2 + 1$ for $m > 1$. Let p be any prime divisor of N. Then $(m!)^2 \equiv -1 \pmod{p}$. Squaring gives $(m!)^4 \equiv 1 \pmod{p}$. Since N is odd, $p \neq 2$. Let $a = m!$. Then $a^2 \equiv -1 \not\equiv 1 \pmod{p}$, so the order of a is not 1 or 2. Because $a^4 \equiv 1 \pmod{p}$, the order of a modulo p is 4. By Fermat's Little Theorem (equivalently, by the size of $(\mathbb{Z}/p\mathbb{Z})^\times$), the order divides $p-1$. Thus $4 \mid (p-1)$, implying $p \equiv 1 \pmod{4}$. Since $N > 1$, it has at least one prime factor, and all such factors are of the form $4k+1$. To show there are infinitely many, assume there are finitely many and set m to be the product of all such primes. Any prime factor p of $(m!)^2 + 1$ cannot divide $m!$, so $p > m$. This yields a new prime of the form $4k+1$, a contradiction.

■

7.5 *Exercises*

1. **Pythagorean Triples and Moduli.** Let a, b, c be integers satisfying $a^2 + b^2 = c^2$. Prove that at least one of a, b, c is divisible by 5.

2. **Non-Divisibility of Series.** Let $a_n = \sum_{k=0}^{n} 2^{3k}\binom{2n+1}{2k+1}$. Prove that for any positive integer n, a_n is not divisible by 5.

3. **Reciprocity Sum.** Let $m > 0$ and $(a, m) = 1$. Verify the identity:

$$\sum_{x=1}^{m-1} \left\lfloor \frac{ax}{m} \right\rfloor = \frac{1}{2}(m-1)(a-1).$$

4. **Prime Power CRS Construction.** Let p be a prime. Verify that the set of integers of the form $x = u + p^{s-t}v$, where $u \in \{0, \ldots, p^{s-t} - 1\}$ and $v \in \{0, \ldots, p^t - 1\}$, forms a complete residue system modulo p^s for any $0 \leq t \leq s$.

5. **Polyadic CRS.** Let $m_1, \ldots, m_k$ be pairwise coprime integers. Let $M_i = m/m_i$ where $m = \prod m_j$. Verify that if x_i runs through a complete residue system modulo m_i, then $\sum M_i x_i$ runs through a complete residue system modulo m.

6. **Squares are not CRS.** Prove that for any integer $m > 2$, the set of squares $\{0^2, 1^2, \ldots, (m-1)^2\}$ cannot form a complete residue system modulo m.

7. **Arithmetic Function Calculations.** Calculate:
   (a) $\varphi(1963)$.
   (b) $\varphi(25296)$.
   (c) $\varepsilon(1001)$.

8. **Parity of Totient.** Prove that for any integer $m > 2$, $\varphi(m)$ is even.

9. **Gauss's Sum.** Prove that $\sum_{d|n} \varphi(d) = n$.

10. **Additive Totient Equation.** Find all pairs of positive integers (m, n) such that $\varphi(mn) = \varphi(m) + \varphi(n)$.

11. **Euclid via Euler.** Use the properties of Euler's totient function to provide an alternative proof that there are infinitely many primes.

12. **Inverse Totient Problems.** Find all positive integers n such that:
    (a) $\varphi(n) = 24$.
    (b) $\varphi(n) = 64$.

13. **Divisibility by Totient.** Find all positive integers n such that $\varphi(n) \mid n$.

14. **Arithmetic Identity for Primes.** Prove that a positive integer n is prime if and only if $\sigma(n) + \varphi(n) = n \cdot d(n)$.

15. **Shifted Totient Equation.** Let n be a positive integer satisfying $\varphi(n+3) = \varphi(n) + 2$. Prove that n must be of the form $2p^r$ or $2p^r - 3$, where p is a prime congruent to 3 modulo 4.

16. **Reduced System Floor Sum.** Let $m > 1$ and $(a, m) = 1$. Verify that if y runs through the least positive reduced residue system

modulo m, then:

$$\sum_{y} \left\lfloor \frac{ay}{m} \right\rfloor = \frac{1}{2}\varphi(m)(a-1).$$

17. **Polyadic Reduced System.** Let $m_1, \ldots, m_k$ be pairwise coprime. Let $M_i = m/m_i$. If ξ_i runs through a reduced residue system modulo m_i, verify that $\sum M_i \xi_i$ runs through a reduced residue system modulo m.

18. **Product of Reduced Residues.** Let $r_1, \ldots, r_{\varphi(m)}$ be a reduced residue system modulo m. Let $A = \prod r_i$. Verify that $A^2 \equiv 1 \pmod{m}$.

19. **Calendar Prediction.** If today is Sunday, determine the day of the week after 3^{2008} days.

20. **Power Calculation.** Calculate the remainder when 1777^{1855} is divided by 41.

21. **Decimal Endings.** Find the last two digits of 7^{355}.

22. **Factorial Divisibility.** For any positive integer n, prove that $n^7 + 720n$ is divisible by 7.

23. **Binomial Difference.**

    (a) Let p be a prime. Prove that for any integer k:

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

    (b) Use this identity to derive Fermat's Little Theorem.

24. **Verifying Pseudoprimality.** Prove that the composite number 161038 is a pseudoprime to base 2.

    Check $2^{n-1} \pmod{n}$.

25. **Wieferich Primes.** An odd prime p satisfies $a^{p-1} \equiv 1 \pmod{p^2}$ for base a if a is a Fermat solution for p. Prove that 2 is a Fermat solution for $p = 1093$.

    This is a computationally intensive verification historically significant for Fermat's Last Theorem.

26. **Symmetric Exponents.** Let p and q be distinct odd primes such that $(p, q-1) = 1$ and $(q, p-1) = 1$. Prove that:

    $$(p-1)^{q-1} \equiv (q-1)^{p-1} \pmod{pq}.$$

27. **Euler's Sum.** Let m, n be coprime positive integers. Prove that:

    $$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}.$$

28. **Power Stabilisation.** Let $m = p_1^{k_1} \ldots p_s^{k_s}$ and $k = \max(k_1, \ldots, k_s)$. Prove that for any integer a:

    $$a^{k+\varphi(m)} \equiv a^k \pmod{m}.$$

29. Erdős-Ginzburg-Ziv Theorem. Let $n \geq 2$. Prove that from any set of $2n - 1$ integers, one can always select exactly n integers whose sum is divisible by n.

> *Remark.*
>
> Consider the remainders modulo n.

8
Finite Decimal Expansions

We investigate the conditions under which a fraction admits a finite representation in a positional numeral system. While our primary focus remains on the decimal system (base 10), we will also consider general bases, applying the divisibility properties established in earlier chapters.

8.1 Finite Decimals

We begin by formalising the fractions under consideration. A fraction $\frac{a}{b}$ with $0 < a < b$ is termed a **proper fraction**. If the numerator and denominator are coprime, that is $(a, b) = 1$, the fraction is said to be **irreducible**. Since any proper fraction can be reduced to an irreducible form by dividing out common factors, we restrict our analysis to irreducible proper fractions without loss of generality. We seek a necessary and sufficient condition for such a fraction to be expressible as a finite decimal.

Theorem 8.1. ***Condition for Finite Decimal Expansion.***
Let $\frac{a}{b}$ be an irreducible proper fraction. The fraction can be converted into a finite decimal if and only if the prime factorisation of the denominator is of the form $b = 2^\alpha \cdot 5^\beta$, where α and β are non-negative integers. Furthermore, the number of decimal places in the expansion is $\max\{\alpha, \beta\}$.

定理

Sufficiency.

Assume $b = 2^\alpha \cdot 5^\beta$. We consider two cases based on the relative magnitude of the exponents.

- If $\alpha \geq \beta$, we multiply the numerator and denominator by $5^{\alpha-\beta}$:

$$\frac{a}{b} = \frac{a}{2^\alpha \cdot 5^\beta} = \frac{a \cdot 5^{\alpha-\beta}}{2^\alpha \cdot 5^\beta \cdot 5^{\alpha-\beta}} = \frac{a \cdot 5^{\alpha-\beta}}{2^\alpha \cdot 5^\alpha} = \frac{a \cdot 5^{\alpha-\beta}}{10^\alpha}.$$

  Since $\alpha \geq \beta$, the term $a \cdot 5^{\alpha-\beta}$ is an integer. Thus, $\frac{a}{b}$ is a finite decimal with α decimal places.

- If $\alpha < \beta$, we multiply by $2^{\beta-\alpha}$:

$$\frac{a}{b} = \frac{a}{2^\alpha \cdot 5^\beta} = \frac{a \cdot 2^{\beta-\alpha}}{2^\alpha \cdot 2^{\beta-\alpha} \cdot 5^\beta} = \frac{a \cdot 2^{\beta-\alpha}}{2^\beta \cdot 5^\beta} = \frac{a \cdot 2^{\beta-\alpha}}{10^\beta}.$$

  Here, $a \cdot 2^{\beta-\alpha}$ is an integer, yielding a finite decimal with β decimal places.

In both cases, the number of places is $\max\{\alpha, \beta\}$.

証明終

Necessity.

Conversely, suppose the irreducible fraction $\frac{a}{b}$ represents a finite decimal. Then there exists a positive integer k and an integer c such that:

$$\frac{a}{b} = \frac{c}{10^k}.$$

Assume, for the sake of contradiction, that b contains a prime factor p distinct from 2 and 5. We may write $b = b_1 p$. Substituting this into the equation:

$$\frac{a}{b_1 p} = \frac{c}{10^k} \implies a \cdot 10^k = b_1 p c.$$

Expanding the power of 10, we have $a \cdot 2^k \cdot 5^k = b_1 p c$. It follows that p divides the left-hand side: $p \mid (a \cdot 2^k \cdot 5^k)$. Since p is distinct from 2 and 5, we have $(p, 2^k \cdot 5^k) = 1$. By *corollary 1.5*, p must divide a. However, p is a factor of b. This implies p is a common divisor of a and b, contradicting the hypothesis that $\frac{a}{b}$ is irreducible. Therefore, b cannot contain any prime factors other than 2 and 5.

証明終

This theorem provides a direct method for determining the length of a decimal expansion without performing long division.

Example 8.1. Calculating Decimal Lengths. Determine the number of decimal places for the following irreducible fractions:

1. $\frac{1}{3125}$
2. $\frac{1}{1024}$
3. $\frac{97}{31250}$
4. $\frac{3947}{20480}$

範例

Solution

1. The denominator factorises as $3125 = 5^5$. Here $\alpha = 0, \beta = 5$. The number of places is $\max\{0, 5\} = 5$.
2. $1024 = 2^{10}$. Here $\alpha = 10, \beta = 0$. The number of places is 10.

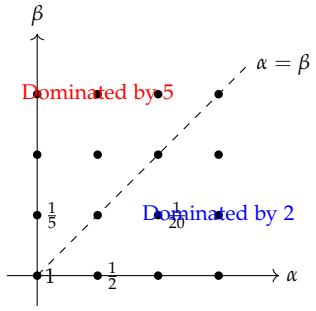


Figure 8.1: The denominators of finite decimals map to lattice points (α, β). The number of decimal places is determined by the distance from the origin in the maximum norm.

3. $31250 = 3125 \times 10 = 5^5 \times 2 \times 5 = 2^1 \cdot 5^6$. The number of places is $\max\{1, 6\} = 6$.
4. $20480 = 2048 \times 10 = 2^{11} \times 2 \times 5 = 2^{12} \cdot 5^1$. The number of places is $\max\{12, 1\} = 12$.

■

Example 8.2. Checking Finite Expansion. Determine whether $\frac{3}{40}$ and $\frac{3}{14}$ have finite decimal expansions.
For $\frac{3}{40}$, we check the prime factors of 40.

$$40 = 8 \times 5 = 2^3 \cdot 5^1.$$

The denominator contains only prime factors 2 and 5. Thus, it has a finite expansion. The length is $\max\{3, 1\} = 3$. Indeed, $\frac{3}{40} = \frac{75}{1000} = 0.075$.
For $\frac{3}{14}$, we factorise $14 = 2 \cdot 7$. The factor 7 is neither 2 nor 5. Since $(3, 14) = 1$, the fraction is irreducible. By *theorem* 8.1, it does not have a finite decimal expansion.

範例

Expansions in General Bases

The divisibility condition for finite representations generalises naturally to any base b. Just as the prime factors 2 and 5 dictate behaviour in base 10, the prime factors of the base b determine which fractions terminate in that system.

Proposition 8.1. ***Finite Expansion in Base*** b**.**
Let n and b be positive integers. Let the expansion of $\frac{1}{n}$ in base b be given by:

$$\frac{1}{n} = \frac{d_1}{b} + \frac{d_2}{b^2} + \frac{d_3}{b^3} + \dots \quad (0 \le d_k < b).$$

If this expansion is finite, then every prime factor of n is a factor of b.

命題

Proof

Suppose the expansion terminates after t terms. We can write:

$$\frac{1}{n} = \frac{d_1}{b} + \frac{d_2}{b^2} + \dots + \frac{d_t}{b^t}.$$

Multiplying the entire equation by b^t yields:

$$\frac{b^t}{n} = d_1 b^{t-1} + d_2 b^{t-2} + \dots + d_t.$$

The right-hand side is an integer composed of integer sums and products. Therefore, the left-hand side $\frac{b^t}{n}$ must be an integer. By the definition of divisibility, $n \mid b^t$. If n divides a power of b, then every prime factor of n must also divide b.

■

Example 8.3. Base 12 Expansion. Consider the fraction $\frac{1}{6}$. In base 10, this is $0.166\ldots$ (infinite) because $3 \mid 6$ but $3 \nmid 10$. In base 12, however, the denominator $n = 6$ has prime factors 2 and 3. The base $b = 12$ has prime factorisation $2^2 \cdot 3$. Since every prime factor of 6 is a factor of 12, $\frac{1}{6}$ has a finite expansion in base 12. Explicitly:

$$\frac{1}{6} = \frac{2}{12} = 0.2_{12}.$$

Conversely, $\frac{1}{5}$ is finite in base 10 but infinite in base 12, as 5 is not a factor of 12.

範例

Example 8.4. Non-Existence of Finite Representation. Prove that $\frac{1}{3}$ cannot be represented as a finite decimal in base 2 (binary).
Here $n = 3$ and the base $b = 2$. The prime factor of n is 3. Since 3 is not a factor of 2, the condition of the proposition fails. Thus, $\frac{1}{3}$ has an infinite binary expansion. Explicitly, one can verify that $\frac{1}{3} = 0.010101\ldots_2$.

範例

8.2 *Infinite Recurring Decimals*

Extending our analysis to those irreducible fractions that do not satisfy this condition, we are led to the theory of infinite recurring decimals.

Definition 8.1. ***Infinite and Recurring Decimals.***
Let x be a real number with decimal expansion $0.a_1a_2a_3\ldots$, where $0 \leq a_i \leq 9$.

1. If for every integer j, there exists $k > j$ such that $a_k \neq 0$, the representation is termed an **infinite decimal**.
2. The decimal is **recurring** (or periodic) if there exist integers $s \geq 0$ and $t > 0$ such that
$$a_{s+i} = a_{s+kt+i}$$
for all $i \in \{1, \ldots, t\}$ and $k \geq 1$. We denote this by
$$0.a_1 \ldots a_s\dot{a}_{s+1}\ldots\dot{a}_{s+t}.$$

3. If $s = 0$, the decimal is **purely recurring**.
4. If $s > 0$, the decimal is **mixed recurring**.
5. The smallest such t is the **period length**.

定義

Pure Recurring Decimals

We first determine the algebraic structure of fractions that yield purely recurring expansions.

Theorem 8.2. ***Condition for Pure Recurrence.***
Let $\frac{a}{b}$ be an irreducible proper fraction. The fraction can be converted into a pure recurring decimal if and only if $(b, 10) = 1$. Furthermore, the period length is the smallest positive integer t such that $10^t \equiv 1 \pmod{b}$.

定理

Necessity.

Suppose $\frac{a}{b}$ is a pure recurring decimal with period t. Then:

$$\frac{a}{b} = 0.\dot{a}_1 a_2 \dots \dot{a}_t.$$

Multiplying by 10^t:

$$10^t \cdot \frac{a}{b} = a_1 a_2 \dots a_t.\dot{a}_1 a_2 \dots \dot{a}_t = N + \frac{a}{b},$$

where N is the integer formed by the repeating block. Rearranging terms:

$$\frac{a}{b}(10^t - 1) = N \implies a(10^t - 1) = bN.$$

Since $(a, b) = 1$, it follows that $b \mid (10^t - 1)$. This implies $10^t - 1 = bk$ for some integer k, so $10^t \equiv 1 \pmod{b}$. If a prime p divides both b and 10, then $p \mid 10^t$ and $p \mid (10^t - 1)$, so $p \mid 1$, a contradiction. Hence $(b, 10) = 1$.

証明終

Sufficiency.

Assume $(b, 10) = 1$. By *theorem 7.10*, $10^{\varphi(b)} \equiv 1 \pmod{b}$. Thus, there exists a smallest positive integer t such that $10^t \equiv 1 \pmod{b}$. Consequently, $b \mid (10^t - 1)$, so there exists an integer N such that $10^t - 1 = bN$. Multiplying by a:

$$\frac{a}{b}(10^t - 1) = aN \implies \frac{a}{b} = \frac{aN}{10^t - 1}.$$

Since $a < b$, we have $aN < bN = 10^t - 1$. The term aN is an integer strictly less than $10^t - 1$, so it can be represented as a t-digit integer (padding with leading zeros if necessary). Division of aN by $10^t - 1$

yields the geometric series sum corresponding to $0.\dot{q}_1 \dots \dot{q}_t$, where $q_1 \dots q_t$ are the digits of aN. Thus, $\frac{a}{b}$ is purely recurring with period t.

証明終

The period length is tied intrinsically to the order of 10 modulo b. This relationship allows us to bound the period length using the totient function.

Theorem 8.3. ***Period Length Divisibility.***
Let b be a positive integer with $(b, 10) = 1$. If t is the period length of $\frac{1}{b}$, then $t \mid \varphi(b)$.

定理

Proof

By *theorem 8.2*, t is the smallest integer satisfying $10^t \equiv 1 \pmod{b}$. By *theorem 7.10*, $10^{\varphi(b)} \equiv 1 \pmod{b}$. Applying the Division Algorithm, we write $\varphi(b) = qt + r$ with $0 \leq r < t$.

$$1 \equiv 10^{\varphi(b)} \equiv (10^t)^q \cdot 10^r \equiv 1^q \cdot 10^r \equiv 10^r \pmod{b}.$$

Since t is the *smallest* positive integer with this property, r must be 0. Thus $t \mid \varphi(b)$.

■

Example 8.5. Calculating Period Lengths. Determine the period lengths of the decimals for $\frac{1}{7}$ and $\frac{1}{13}$.

1. For $b = 7$, $\varphi(7) = 6$. We test divisors of 6.

$$10^1 \equiv 3, \quad 10^2 \equiv 2, \quad 10^3 \equiv 6 \equiv -1 \pmod{7}.$$

   Since $10^3 \equiv -1$, it follows $10^6 \equiv (-1)^2 \equiv 1$. The order is 6. Indeed, $\frac{1}{7} = 0.\dot{1}42857\dot{}$.

2. For $b = 13$, $\varphi(13) = 12$. We compute powers of 10 modulo 13:

$$10^1 \equiv 10, \quad 10^2 \equiv 100 \equiv 9, \quad 10^3 \equiv 90 \equiv 12 \equiv -1.$$

   Since $10^3 \equiv -1$, we have $10^6 \equiv 1 \pmod{13}$. The period length is 6. Note that $6 \mid 12$. (Fact: $\frac{1}{13} = 0.\overline{076923}$.)

範例

Mixed Recurring Decimals

If the denominator shares factors with 10, the decimal expansion is not purely recurring. However, we can reduce this case to the pure case by shifting the decimal point.

Theorem 8.4. ***Structure of Mixed Recurring Decimals.***
Let $\frac{a}{b}$ be an irreducible proper fraction where $b = 2^\alpha \cdot 5^\beta \cdot b_1$, with $b_1 > 1$ and $(b_1, 10) = 1$. The decimal expansion of $\frac{a}{b}$ is mixed recurring.

1. The length of the non-recurring part is $s = \max\{\alpha, \beta\}$.
2. The length of the recurring part is the multiplicative order of 10 modulo b_1.

定理

Proof

Let $s = \max\{\alpha, \beta\}$. We can write:

$$\frac{a}{b} = \frac{a}{2^\alpha 5^\beta b_1} = \frac{1}{10^s} \cdot \frac{a \cdot K}{b_1},$$

where K is the integer required to equate the powers of 2 and 5 to 10^s. Let $A = a \cdot K$. We perform Euclidean division of A by b_1: $A = qb_1 + r$, with $0 < r < b_1$.

$$\frac{a}{b} = \frac{1}{10^s}\left(q + \frac{r}{b_1}\right) = \frac{q}{10^s} + \frac{1}{10^s} \cdot \frac{r}{b_1}.$$

The term $\frac{q}{10^s}$ represents a terminating decimal. The term $\frac{r}{b_1}$ is a proper fraction with $(b_1, 10) = 1$. By *theorem 8.2*, $\frac{r}{b_1}$ is a purely recurring decimal with period length t equal to the order of 10 modulo b_1. Multiplying a pure recurring decimal by 10^{-s} simply shifts the digits s places to the right, creating a non-recurring prefix of length s.

■

Example 8.6. Analysis of Denominators. Analyze the decimal structure of fractions with denominators 12 and 808.

1. $12 = 2^2 \cdot 3$. Here $\alpha = 2, \beta = 0$, so $s = 2$. $b_1 = 3$. Order of 10 modulo 3: $10 \equiv 1 \pmod 3$, so $t = 1$. Structure: 2 non-recurring digits, period 1. Check: $\frac{1}{12} = 0.08\dot{3}$.
2. $808 = 8 \cdot 101 = 2^3 \cdot 101$. Here $s = 3$. $b_1 = 101$. We determine the order of 10 modulo 101. $10^2 = 100 \equiv -1 \pmod{101}$. $10^4 \equiv (-1)^2 \equiv 1 \pmod{101}$. Period length is 4. Structure: 3 non-recurring digits, period 4. Check: $\frac{1}{808} \approx 0.00123762376\cdots = 0.001\overline{2376}$.

範例

Properties of the Period

The digits within a period often exhibit surprising symmetry. A famous result, often attributed to Midy, describes the sum of the digits in the two halves of a period of even length.

Theorem 8.5. ***Sum of Half-Periods.***
Let $\frac{a}{b}$ be an irreducible proper fraction forming a pure recurring decimal with period length $t = 2k$. Let the period be $q_1 q_2 \dots q_k t_1 t_2 \dots t_k$. If $(b, 10^k - 1) = 1$, then:

$$q_i + t_i = 9 \quad \text{for all } i = 1, \dots, k.$$

定理

Proof

We have $10^{2k} \equiv 1 \pmod{b}$. Factorising the difference of squares:

$$b \mid (10^{2k} - 1) \implies b \mid (10^k - 1)(10^k + 1).$$

Given the condition $(b, 10^k - 1) = 1$, Euclid's Lemma implies $b \mid (10^k + 1)$. Thus $10^k + 1 = b \cdot M$ for some integer M. From the decimal expansion $\frac{a}{b} = 0.\dot{q}_1 \dots t_k$, we can write:

$$\frac{a}{b} = \frac{N}{10^{2k} - 1},$$

where N is the integer $q_1 \dots t_k$. Then $a(10^{2k} - 1) = bN$. Substituting $10^{2k} - 1 = (10^k - 1)(10^k + 1) = (10^k - 1)bM$:

$$a(10^k - 1)bM = bN \implies N = aM(10^k - 1).$$

We have $\frac{a}{b} \cdot 10^k = \text{integer} + 0.\dot{t}_1 \dots t_k q_1 \dots q_k$. The sum of the fraction and its shifted version shifted by k places corresponds to:

$$\frac{a}{b}(10^k + 1) = \frac{a}{b} \cdot bM = aM.$$

This is an integer. In terms of the decimal parts, let $X = 0.\dot{q}_1 \dots t_k$ and $Y = 0.\dot{t}_1 \dots q_k$. $X + Y$ must be an integer. Since $0 < X < 1$ and $0 < Y < 1$, their sum must be exactly 1 (the expansion is purely recurring, so it cannot terminate).

$$0.\dot{q}_1 \dots t_k + 0.\dot{t}_1 \dots q_k = 0.\dot{9}9 \dots 9 = 1.$$

Write the period as a pair of k-digit blocks: $N = Q \cdot 10^k + T$ with $0 \le T < 10^k$. Since $N = aM(10^k - 1)$ and $0 < aM < 10^k$ (otherwise the period would collapse to $0.\dot{9}$), we have

$$N = aM \cdot 10^k - aM = (aM - 1)10^k + (10^k - aM).$$

Thus $Q = aM - 1$ and $T = 10^k - aM$, so $Q + T = 10^k - 1$. This forces digit-wise summation $q_i + t_i = 9$ with no carries.

■

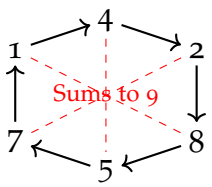


Figure 8.2: The period of 1/7 is 142857. Pairing digits separated by $k = 3$ positions $(1+8, 4+5, 2+7)$ yields 9.

Example 8.7. Midy's Theorem on $1/7$. Consider $\frac{1}{7} = 0.\dot{1}4285\dot{7}$. The period length is $t = 6$, so $k = 3$. Check the condition: $(7, 10^3 - 1) = (7, 999)$. Since $999 = 27 \times 37$, the gcd is 1. The theorem applies. The first half is 142; the second half is 857.

$$1 + 8 = 9, \quad 4 + 5 = 9, \quad 2 + 7 = 9.$$

範例

Finally, we present an algorithmic method for generating the digits of the period of $\frac{1}{b}$ in reverse order, which is particularly computationally efficient for large periods.

Theorem 8.6. ***Reverse Digit Algorithm.***
Let b be a positive integer with $(b, 10) = 1$, and let b_1 be the units digit of b. The expansion $\frac{1}{b} = 0.\dot{a}_1 a_2 \ldots \dot{a}_t$ can be computed from right to left (a_t down to a_1) as follows:

1. The last digit a_t is determined by $a_t \cdot b_1 \equiv 9 \pmod{10}$.
2. Let $M = \frac{a_t b + 1}{10}$. This integer M serves as a multiplier.
3. Each subsequent digit (moving left) is the units digit of the product of the previous digit and M, plus any carry from the previous step.

定理

Proof

The relationship stems from the identity derived in the expansion:

$$a_t b \equiv -1 \equiv 9 \pmod{10}.$$

This uniquely determines a_t because b is coprime to 10. The recursive step a_{t-k} incorporates the modular arithmetic of the long division process run in reverse. Specifically, if R_k is the remainder at step k, the reverse process reconstructs the dividend using the multiplier M.

■

Example 8.8. Generating $1/19$. We compute the period of $\frac{1}{19}$. Here $b = 19$, so $b_1 = 9$.

1. Find a_t: $9 \times a_t \equiv 9 \pmod{10} \implies a_t = 1$.
2. Find Multiplier M: $M = \frac{1 \cdot 19 + 1}{10} = \frac{20}{10} = 2$.
3. Generate sequence (multiply by 2, add carry):
   - $a_{18} = 1$. (Carry 0)
   - $1 \times 2 + 0 = 2. \implies a_{17} = 2$.
   - $2 \times 2 + 0 = 4. \implies a_{16} = 4$.

- $4 \times 2 + 0 = 8. \implies a_{15} = 8.$
- $8 \times 2 + 0 = 16. \implies a_{14} = 6.$ (Carry 1)
- $6 \times 2 + 1 = 13. \implies a_{13} = 3.$ (Carry 1)
- $3 \times 2 + 1 = 7. \implies a_{12} = 7.$
- $7 \times 2 + 0 = 14. \implies a_{11} = 4.$ (Carry 1)
- $4 \times 2 + 1 = 9. \implies a_{10} = 9.$

At this point, we have the second half of the period: 947368421. By *theorem* 8.5, since 19 is prime, the first half is the 9-complement of this sequence: 052631578. Thus

$$\frac{1}{19} = 0.\dot{0}52631578947368421\dot{}.$$

範例

8.3 *Wilson's Theorem*

In 1770, Edward Waring published a conjecture of his student John Wilson, stating that if p is a prime number, then p divides $(p-1)! + 1$. This elegant condition was proven later that year by Lagrange. We now present this fundamental result and its converse.

Theorem 8.7. ***Wilson's Theorem.***
An integer $p > 1$ is a prime number if and only if

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

定理

Necessity.

For $p = 2$, $(2-1)! = 1 \equiv -1 \pmod 2$.
For $p = 3$, $(3-1)! = 2 \equiv -1 \pmod 3$.
Assume $p > 3$. Consider the set of integers $S = \{2, 3, \ldots, p-2\}$. Since $\mathbb{Z}_p$ is a field, for every $x \in S$, there exists a unique inverse $y \in \{1, \ldots, p-1\}$ such that $xy \equiv 1 \pmod p$. Since $x \in S$, $x \neq 1$ and $x \neq -1$. The only elements that are their own inverses are the solutions to $x^2 \equiv 1 \pmod p$, namely 1 and $p-1$. Thus, for every $x \in S$, its inverse y is distinct from x and also belongs to S (since $y \neq 1, p-1$). We can therefore partition S into $(p-3)/2$ disjoint pairs $\{x, x^{-1}\}$. The product of each pair is congruent to 1.

$$\prod_{x \in S} x \equiv 1^{(p-3)/2} \equiv 1 \pmod{p}.$$

Including the boundary terms 1 and $p-1$:

$$(p-1)! = 1 \cdot \left(\prod_{x \in S} x \right) \cdot (p-1) \equiv 1 \cdot 1 \cdot (-1) \equiv -1 \pmod{p}.$$

証明終

Sufficiency.

Assume p is composite. Then p has a proper divisor d with $1 < d < p$. Since $d \leq p-1$, d appears as a factor in the product $(p-1)!$. Thus $d \mid (p-1)!$. If the congruence $(p-1)! \equiv -1 \pmod{p}$ holds, then $(p-1)! = kp - 1$. Since $d \mid p$ and $d \mid (p-1)!$, it follows that d divides their difference:

$$d \mid (kp - (p-1)!) \implies d \mid 1.$$

This implies $d = 1$, contradicting the assumption that d is a proper divisor. Thus p must be prime.

証明終

Example 8.9. Generalised Factorial Product. Let p be an odd prime. Verify that

$$1^2 \cdot 3^2 \cdot \cdots \cdot (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

Consider the factorial $(p-1)!$. We can write the even terms $2k$ as $-(p-2k) \pmod{p}$. Specifically, observe the symmetry in the product:

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \\ &= \prod_{k=1}^{(p-1)/2} (2k-1)(2k).\end{aligned}$$

Modulo p, we have $2k \equiv -(p-2k)$. Note that as k runs from 1 to $(p-1)/2$, the values $p-2k$ run through the odd integers $\{p-2, p-4, \ldots, 1\}$ in reverse order. However, it is simpler to rearrange the terms of $(p-1)!$ into odds and evens directly.

$$(p-1)! = [1 \cdot 3 \cdot \cdots \cdot (p-2)] \cdot [2 \cdot 4 \cdot \cdots \cdot (p-1)].$$

The second bracket contains $(p-1)/2$ even terms. We can write $2j \equiv -(p-2j)$. Let $m = (p-1)/2$. The even terms are $2, 4, \ldots, 2m$.

$$\prod_{j=1}^{m} (2j) = 2 \cdot 4 \cdot \cdots \cdot (p-1).$$

This does not immediately yield the square form. Let us use the

reflection property $x \equiv -(p-x)$.

$$(p-1)! = \prod_{k=1}^{(p-1)/2} k \cdot \prod_{k=1}^{(p-1)/2} (p-k) \equiv \prod_{k=1}^{(p-1)/2} k \cdot \prod_{k=1}^{(p-1)/2} (-k) \equiv (-1)^{(p-1)/2} \left[\left(\frac{p-1}{2} \right)! \right]^2.$$

This is the standard corollary. To obtain the specific result for odd squares, let us pair k with $-(p-k)$. The product of odd numbers is $O = 1 \cdot 3 \cdot \cdots \cdot (p-2)$. The product of even numbers is $E = 2 \cdot 4 \cdot \cdots \cdot (p-1)$. Notice $E = (-1)^{(p-1)/2} \cdot O \pmod{p}$ because $p-1 \equiv -1, p-3 \equiv -3$, etc. Thus $(p-1)! = O \cdot E \equiv O \cdot (-1)^{(p-1)/2} O \equiv (-1)^{(p-1)/2} O^2$. By Wilson's Theorem, $(p-1)! \equiv -1$.

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

Multiplying by $(-1)^{(p-1)/2}$:

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

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

範例

Twin Primes

Wilson's Theorem can be adapted to characterise pairs of primes.

Theorem 8.8. ***Clement's Theorem for Twin Primes.***
Let p be a positive integer with $p \neq 1$. The integers p and $p+2$ are twin primes if and only if

$$4((p-1)!+1) + p \equiv 0 \pmod{p(p+2)}.$$

定理

Necessity.

Assume p and $p+2$ are primes. Since p is part of a pair (and $p \neq 1$), p must be odd. By Wilson's Theorem:

1. $(p-1)! \equiv -1 \pmod{p}$. Thus $4((p-1)!+1) + p \equiv 4(0) + 0 \equiv 0 \pmod{p}$.
2. $(p+1)! \equiv -1 \pmod{p+2}$.

We manipulate the expression modulo $p+2$:

$$4(p-1)! + 4 + p = 4(p-1)! + p + 4.$$

Note that $(p+1)! = (p+1)p(p-1)! \equiv (-1)(-2)(p-1)! = 2(p-1)! \pmod{p+2}$. Since $2(p-1)! \equiv (p+1)! \equiv -1 \pmod{p+2}$, we

have:

$$4(p-1)! = 2[2(p-1)!] \equiv 2(-1) = -2 \pmod{p+2}.$$

Substituting this back:

$$4(p-1)! + p + 4 \equiv -2 + p + 4 = p + 2 \equiv 0 \pmod{p+2}.$$

Since the expression is divisible by p and $p+2$, and $(p, p+2) = 1$ (as p is odd), it is divisible by $p(p+2)$.

証明終

Sufficiency.

Assume the congruence holds. This implies $4((p-1)!+1) \equiv 0 \pmod{p}$, so $(p-1)! \equiv -1 \pmod{p}$. By *theorem 8.7*, p is prime. Now consider modulo $p+2$. The congruence implies:

$$4(p-1)! + p + 4 \equiv 0 \pmod{p+2} \implies 4(p-1)! \equiv -(p+4) \equiv -2 \pmod{p+2}.$$

We multiply by the invertible elements to reconstruct the factorial. Multiply by $p(p+1) = p^2 + p$. Note $p \equiv -2 \pmod{p+2}$, so $p(p+1) \equiv (-2)(-1) = 2$.

$$2 \cdot 4(p-1)! \equiv 2(-2) \implies 4[2(p-1)!] \equiv -4 \pmod{p+2}.$$

Recall $2(p-1)! \equiv p(p+1)(p-1)! = (p+1)! \pmod{p+2}$.

$$4(p+1)! \equiv -4 \pmod{p+2}.$$

For $p > 2$, $p+2$ is odd and coprime to 4. We can cancel 4:

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

By *theorem 8.7*, $p+2$ is prime.

証明終

Prime-Generating Functions

A remarkable theoretical application of *Wilson's Theorem* is the construction of functions that generate prime numbers. While computationally inefficient, these formulae demonstrate that primes are the solution set of Diophantine equations.

Theorem 8.9. ***A Prime-Generating Function.***
For positive integers n and m, let

$$Q = m(n+1) - (n! + 1).$$

Define the function

$$f(m,n) = \frac{n-1}{2}\left(|Q^2-1| - (Q^2-1)\right) + 2.$$

Then the set of values taken by $f(m,n)$ is exactly the set of prime numbers.

定理

Proof

We analyse the term $T = |Q^2-1| - (Q^2-1)$.

- If $Q^2 \geq 1$ (i.e., $Q \neq 0$), then $|Q^2-1| = Q^2-1$. Thus $T = 0$, and $f(m,n) = 2$.
- If $Q = 0$, then $Q^2 - 1 = -1$, so $|-1| - (-1) = 2$. Thus $f(m,n) = \frac{n-1}{2}(2) + 2 = n+1$.

The condition $Q = 0$ is equivalent to $m(n+1) = n! + 1$. This equality holds for some integer m if and only if $n+1$ divides $n!+1$, or equivalently:

$$n! \equiv -1 \pmod{n+1}.$$

By *theorem 8.7*, this occurs if and only if $n+1$ is prime.
Thus:

- If $n+1$ is composite or $Q \neq 0$, $f(m,n) = 2$ (which is prime).
- If $n+1$ is prime and m is chosen to make $Q = 0$, $f(m,n) = n+1$.

By varying n, we can generate every odd prime $p = n+1$ (by setting $n = p-1$ and $m = \frac{(p-1)!+1}{p}$). Thus, the range of the function is exactly the set of prime numbers.

■

Example 8.10. Non-Existence of Factorial Solutions. Find all pairs of positive integers (n,k) such that $(n-1)! = n^k - 1$.

· For $n = 1$, $0! = 1 \neq 0$.

· For $n = 2$, $1! = 1$, $2^k - 1 = 1 \implies 2^k = 2 \implies k = 1$. Solution $(2,1)$.

· For $n = 3$, $2! = 2$, $3^k - 1 = 2 \implies k = 1$. Solution $(3,1)$.

· For $n = 4$, $3! = 6$, $4^k - 1$ is odd (impossible).

· For $n = 5$, $4! = 24$, $5^k - 1 = 24 \implies k = 2$. Solution $(5,2)$.

Assume $n > 5$. From $(n-1)! = n^k - 1$, we have $(n-1)! \equiv -1 \pmod{n}$. By *theorem 8.7*, n must be prime. Since $n > 5$, $n-1$ is composite and greater than 4. Thus $n-1$ has a divisor d with $1 < d < n-1$, or $n-1$ is a square of a prime. In any case, $n-1$ divides

$(n-2)!$. We rewrite the equation:

$$(n-1)(n-2)! = n^k - 1 = (n-1)(n^{k-1} + n^{k-2} + \cdots + 1).$$

Dividing by $n-1$:

$$(n-2)! = n^{k-1} + \cdots + 1 = \frac{n^k - 1}{n-1}.$$

Since $n > 5$, we have $n - 1 < (n-2)!$. Also $n \equiv 1 \pmod{n-1}$, so:

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

Since $n - 1 \mid (n-2)!$ (for $n > 5$), we must have $k \equiv 0 \pmod{n-1}$. Let $k = m(n-1)$ for $m \geq 1$. Then $n^k - 1 = (n^{n-1})^m - 1 \geq n^{n-1} - 1$. However, it is easily shown by induction that for $n > 5$, $(n-1)! < n^{n-1} - 1$. Contradiction. Thus there are no solutions for $n > 5$.

範例

8.4 *Exercises*

1. **Finite Decimal Lengths.** Determine the number of decimal places for the following irreducible proper fractions:
   (a) $\frac{1}{128}$
   (b) $\frac{17}{320}$
   (c) $\frac{81}{800}$
2. **General Base Expansion.** Prove that in base b, the expansion of $\frac{1}{n}$ terminates if and only if every prime factor of n divides b.
3. **Period Length Calculation.** Determine the period length of the decimal expansions for:
   (a) $\frac{1}{7}$
   (b) $\frac{1}{19}$
   (c) $\frac{1}{27}$
4. **Classification of Decimals.** For irreducible fractions with the following denominators, classify them as finite, pure recurring, or mixed recurring decimals. Calculate the number of non-recurring digits and the period length.
   (a) 11
   (b) 14
   (c) 16

5. **Decimal Construction.** Write out the full recurring decimal expansion for:
   (a) $\frac{5}{17}$
   (b) $\frac{1}{23}$
6. **Wilson's Theorem Variations.** Let p be an odd prime. Prove that:
   (a) $2^2 \cdot 4^2 \cdots (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.
   (b) $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.
7. **Unified Congruence.**
   (a) Let p be a prime and a be any integer. Prove that $a(p-1)! \equiv -a \pmod{p}$.
   (b) Deduce that $a^p(p-1)! \equiv a(p-1)! \equiv -a \pmod{p}$, and use this to derive Fermat's Little Theorem and the sufficiency condition of Wilson's Theorem.
8. **Factorial Reflection.** Let p be an odd prime. Prove that if there exists an integer r such that $(-1)^r r! \equiv 1 \pmod{p}$, then
$$(p-r-1)! + 1 \equiv 0 \pmod{p}.$$
   Use this to show that $61! + 1 \equiv 0 \pmod{71}$ and $63! + 1 \equiv 0 \pmod{71}$.
9. **Quadratic Factorials.** Let $p = 2n+1$ be a prime. Prove that:
$$(n!)^2 + (-1)^n \equiv 0 \pmod{p}.$$

9
Indefinite Equations

Having developed the properties of divisibility and the greatest common divisor in the preceding chapters, we now apply these tools to the study of indefinite equations. Historically known as Diophantine equations these are polynomial equations for which we seek integer solutions.
The study of such equations is one of the oldest branches of number theory, with significant early contributions from ancient Chinese mathematicians. In this chapter, we focus on linear equations in two variables, establishing criteria for solvability and methods for constructing general solutions.

Diophantine Equations are named after the Greek mathematician Diophantus of Alexandria (c. 3rd century AD)

9.1 Linear Indefinite Equations in Two Variables

We begin by defining the class of equations under consideration.

Definition 9.1. ***Linear Indefinite Equation.***
A linear indefinite equation in two variables is an equation of the form

$$ax + by = c,$$

where a, b are non-zero integers and c is an arbitrary integer. A solution is a pair of integers (x, y) satisfying the equation.

定義

The solvability of such an equation is strictly determined by the greatest common divisor of the coefficients.

Theorem 9.1. ***Existence of Solutions.***
The linear indefinite equation $ax + by = c$ has integer solutions if and only if (a, b) divides c.

定理

Necessity.

Let $(a, b) = d$. By the definition of the greatest common divisor, there exist integers q_1, q_2 such that $a = dq_1$ and $b = dq_2$. Sup-

pose the equation has an integer solution (x_0, y_0). Substituting the expressions for a and b:

$$c = ax_0 + by_0 = (dq_1)x_0 + (dq_2)y_0 = d(q_1x_0 + q_2y_0).$$

Since q_1, x_0, q_2, y_0 are integers, their linear combination is an integer. Thus $d \mid c$.

証明終

Sufficiency.

Suppose $(a, b) = d$ and $d \mid c$. Then $c = dm$ for some integer m. From the properties of the greatest common divisor (specifically the linear combination property established in the previous chapter), there exist integers u, v such that:

$$au + bv = d.$$

Multiplying this identity by m:

$$a(um) + b(vm) = dm = c.$$

Let $x_0 = um$ and $y_0 = vm$. Then (x_0, y_0) is an integer solution to the equation.

証明終

This theorem yields two immediate consequences regarding the existence of solutions.

Corollary 9.1. If $(a, b) \nmid c$, the equation $ax + by = c$ has no integer solutions.

推論

Corollary 9.2. If $(a, b) = 1$, the equation $ax + by = c$ always possesses integer solutions.

推論

Consequently, when seeking solutions, we may divide the entire equation by (a, b) to obtain an equivalent equation with coprime coefficients. We henceforth assume $(a, b) = 1$ unless stated otherwise.

Method of Solution

To find a particular solution, one may employ the Euclidean Algorithm to express the GCD as a linear combination of a and b. Alternatively, for coefficients of manageable size, an algebraic "trial method" is often efficient. This involves isolating one variable and interpreting the resulting fraction as an integer condition.

Example 9.1. Basic Solution via Algebraic Manipulation. Find a set of integer solutions for the equation $3x + 4y = 23$.
We express x in terms of y:

$$3x = 23 - 4y \implies x = \frac{23 - 4y}{3}.$$

We separate the integer part of the quotient:

$$x = \frac{21 + 2 - 3y - y}{3} = 7 - y + \frac{2 - y}{3}.$$

For x to be an integer, 3 must divide $2 - y$. Let $2 - y = 3k$ for some integer k. Then $y = 2 - 3k$. Setting $k = 0$, we obtain $y = 2$. Substituting back into the expression for x:

$$x = 7 - 2 + 0 = 5.$$

Thus, $(5, 2)$ is a solution. Verification: $3(5) + 4(2) = 15 + 8 = 23$.

範例

Once a single solution is found, the complete set of solutions follows a predictable structure.

Theorem 9.2. ***General Solution Structure.***
Let a, b be coprime non-zero integers. If (x_0, y_0) is a particular integer solution to the equation $ax + by = c$, then the general integer solution is given by:

$$\begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases} \quad \text{for any } t \in \mathbb{Z}.$$

定理

Proof

Let (x, y) be any integer solution. Since $ax + by = c$ and $ax_0 + by_0 = c$, we have:

$$ax + by = ax_0 + by_0 \implies a(x - x_0) = -b(y - y_0).$$

Thus b divides $a(x - x_0)$. Since $(a, b) = 1$, Euclid's Lemma implies $b \mid (x - x_0)$. Therefore, $x - x_0 = bt$ for some integer t, yielding $x = x_0 + bt$. Substituting this back into the relation:

$$a(bt) = -b(y - y_0).$$

Since $b \neq 0$, we divide by b to get $at = -(y - y_0)$, or $y = y_0 - at$. Conversely, substituting these expressions into the original equation verifies they are solutions for any t.

■

Example 9.2. General Solution Construction. Find the general solution of $11x + 15y = 7$.
Since $(11, 15) = 1$, solutions exist. Isolate x (the variable with the smaller coefficient):

$$x = \frac{7 - 15y}{11} = \frac{7 - 4y - 11y}{11} = -y + \frac{7 - 4y}{11}.$$

We require $11 \mid (7 - 4y)$. We test small values for y:
· $y = 1 \implies 7 - 4 = 3$ (No).
· $y = -1 \implies 7 - 4(-1) = 11$ (Yes).
Using $y_0 = -1$, we find $x_0 = -(-1) + 1 = 2$. The particular solution is $(2, -1)$. Applying *theorem* 9.2, the general solution is:

$$\begin{cases} x = 2 + 15t \\ y = -1 - 11t \end{cases} \qquad t \in \mathbb{Z}.$$

範例

Example 9.3. Constrained Solutions. Find the smallest positive integer solution to $5x - 14y = -11$.
We isolate x:

$$5x = 14y - 11 \implies x = \frac{14y - 11}{5} = \frac{15y - y - 10 - 1}{5} = 3y - 2 - \frac{y + 1}{5}.$$

For x to be an integer, $5 \mid (y + 1)$. Let $y + 1 = 5k$, so $y = 5k - 1$. Substituting back:

$$x = 3(5k - 1) - 2 - k = 15k - 3 - 2 - k = 14k - 5.$$

The general solution is $x = 14k - 5$ and $y = 5k - 1$. We seek the smallest positive solution, so $x > 0$ and $y > 0$.

$$14k - 5 > 0 \implies k > 5/14, \quad \text{and} \quad 5k - 1 > 0 \implies k > 1/5.$$

The smallest integer k satisfying these is $k = 1$.

$$x = 14(1) - 5 = 9, \quad y = 5(1) - 1 = 4.$$

The smallest positive solution is $(9, 4)$.

範例

We now consider a problem requiring the formulation of such an equation from a text description.

Example 9.4. Partitioning an Integer. Divide the integer 239 into two positive parts, such that one part is divisible by 17 and the other by 24.

Let the two parts be $17x$ and $24y$, where x, y are positive integers.
The condition is:

$$17x + 24y = 239.$$

We solve for x:

$$17x = 239 - 24y \implies x = \frac{239 - 24y}{17} = \frac{238 + 1 - 17y - 7y}{17} = 14 - y + \frac{1 - 7y}{17}.$$

We require $17 \mid (1 - 7y)$. Testing values:

$$1 - 7(5) = 1 - 35 = -34 = 17(-2).$$

Thus $y_0 = 5$ is a solution. Substituting $y_0 = 5$ into the expression for x:

$$x_0 = 14 - 5 + (-2) = 7.$$

The general solution is:

$$x = 7 + 24t, \quad y = 5 - 17t.$$

Since the parts must be positive, we require $x > 0$ and $y > 0$:

$$7 + 24t > 0 \implies t > -7/24, \quad 5 - 17t > 0 \implies t < 5/17.$$

The only integer t in the interval $(-0.29, 0.29)$ is $t = 0$. Thus the solution is unique: $x = 7, y = 5$. The two parts are $17(7) = 119$ and $24(5) = 120$. Note that $119 + 120 = 239$.

範例

Often, Diophantine equations appear in geometric contexts involving integer coordinates or lattice points.

Example 9.5. Lattice Points on a Line. Determine the number of integer coordinate points (x, y) lying on the line $12x + 25y = 331$ in the first quadrant (i.e., $x > 0, y > 0$).
First, we find a particular solution. Isolate x:

$$x = \frac{331 - 25y}{12} = \frac{324 + 7 - 24y - y}{12} = 27 - 2y + \frac{7 - y}{12}.$$

We set $7 - y = 12k$, so $y = 7 - 12k$. For $k = 0$, $y_0 = 7$. Then $x_0 = 27 - 2(7) + 0 = 13$. The particular solution is $(13, 7)$. The general solution is:

$$x = 13 + 25t, \quad y = 7 - 12t.$$

For the points to lie in the first quadrant:

$$\begin{cases} 13 + 25t > 0 \implies t > -13/25 = -0.52 \\ 7 - 12t > 0 \implies t < 7/12 \approx 0.58 \end{cases}$$

The only integer satisfying $-0.52 < t < 0.58$ is $t = 0$. Thus, there is exactly one such point: $(13, 7)$.

範例

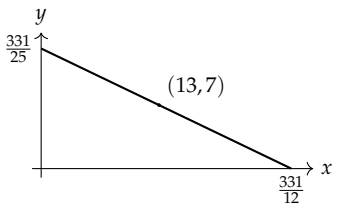


Figure 9.1: The line $12x + 25y = 331$. The unique integer solution in the positive quadrant is marked.

9.2 *The Frobenius Number for* $n = 2$

A classic problem in the theory of indefinite equations asks for the largest integer that cannot be expressed as a linear combination of two coprime positive integers a and b with non-negative coefficients. This value is known as the Frobenius number of the set $\{a, b\}$.

Theorem 9.3. ***The Coin Problem Bound.***
Let a, b be coprime positive integers greater than 1.

1. The equation $ax + by = N$ has non-negative integer solutions for all integers $N > ab - a - b$.
2. The equation $ax + by = ab - a - b$ has no non-negative integer solutions.

定理

Proof

1. Let $N > ab - a - b$. The general integer solution to $ax + by = N$ is:
$$x = x_0 + bt, \quad y = y_0 - at.$$
We can choose an integer t such that the y-value falls in the interval $[0, a - 1]$. Specifically, since the values of y form an arithmetic progression with step $-a$, there exists a unique y such that $0 \leq y \leq a - 1$. With this specific y, we examine the corresponding x. From the equation $ax = N - by$:
$$ax > (ab - a - b) - b(a - 1) = ab - a - b - ab + b = -a.$$
Thus $ax > -a$. Since $a > 0$, this implies $x > -1$. Since x is an integer, $x \geq 0$. Therefore, a solution exists with both $x \geq 0$ and $y \geq 0$.

2. Assume, for the sake of contradiction, that $ax + by = ab - a - b$ has a solution with $x \geq 0$ and $y \geq 0$. Rearranging the equation:
$$ax + by = ab - a - b \implies ax + a + by + b = ab \implies a(x+1) + b(y+1) = ab.$$
Since $(a, b) = 1$, we must have $a \mid b(y + 1)$, which implies $a \mid (y + 1)$. So $y + 1 \geq a$. Similarly, $b \mid a(x + 1)$ implies $b \mid (x + 1)$. So $x + 1 \geq b$. Substituting these inequalities back into the derived equation:
$$a(x + 1) + b(y + 1) \geq a(b) + b(a) = 2ab.$$

Thus $ab \geq 2ab$. Since $a, b > 1$, $ab > 0$, so this inequality is impossible. Hence, no non-negative solution exists.

■

Example 9.6. Non-Representable Amounts. Consider stamps of value 5 and 7. What is the largest postage value that cannot be formed using only these stamps?
Here $a = 5$ and $b = 7$. They are coprime. The largest non-representable integer is:

$$N = 5(7) - 5 - 7 = 35 - 12 = 23.$$

Any integer greater than 23 can be written as $5x + 7y$ with $x, y \geq 0$. For instance, $24 = 5(2) + 7(2)$. However, 23 cannot be so expressed. If $23 = 5x + 7y$, possible values for $7y$ are $0, 7, 14, 21$.

- $7y = 0 \implies 5x = 23$ (No solution).
- $7y = 7 \implies 5x = 16$ (No solution).
- $7y = 14 \implies 5x = 9$ (No solution).
- $7y = 21 \implies 5x = 2$ (No solution).

範例

Example 9.7. Rectangle Dissection. Consider a rectangle partitioned into squares of unequal sizes. Let the smallest two squares have side lengths x and y. By analyzing the geometry of the specific spiral dissection described in Example 5 of the source text, one derives the condition:

$$9x - 16y = 0.$$

Determine the smallest integer dimensions for such a dissection.
The general solution is $x = 16t, y = 9t$. For the smallest positive dimensions, let $t = 1$. Then $x = 16, y = 9$. These values correspond to the side lengths of the initiating squares in the dissection.

範例

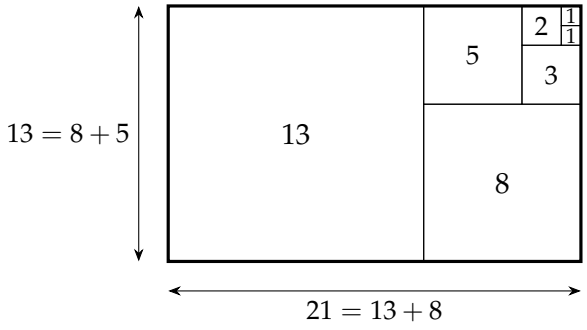


Figure 9.2: A Fibonacci squared rectangle (21×13). The side lengths satisfy the recurrence $F_n = F_{n-1} + F_{n-2}$, illustrating how geometric tiling constraints impose Diophantine conditions on square dimensions.

9.3 *Solvability and General Theory*

We extend our study of Diophantine equations to linear equations involving three or more variables. These equations typically take the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c,$$

where $n \geq 3$, the coefficients a_i are non-zero integers, and c is an integer. While the increase in variables introduces more degrees of freedom, the fundamental solvability criteria remain rooted in the theory of the greatest common divisor.
The existence of integer solutions is governed by the collective divisibility of the coefficients.

Theorem 9.4. ***Existence of Solutions for n Variables.***
The linear indefinite equation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

has integer solutions if and only if $(a_1, a_2, \ldots, a_n) \mid c$.

定理

Necessity.

Let $d = (a_1, a_2, \ldots, a_n)$. By definition, $d \mid a_i$ for all $i = 1, \ldots, n$. If integers $k_1, \ldots, k_n$ satisfy the equation, then:

$$c = \sum_{i=1}^{n} a_i k_i.$$

Since d divides every term in the sum, $d \mid c$.

証明終

Sufficiency.

We proceed by induction on n. For $n = 2$, the result holds by *theorem 9.1*. Assume the condition is sufficient for equations in $n - 1$ variables. Consider the equation:

$$a_1x_1 + \cdots + a_nx_n = c.$$

Let $d_2 = (a_1, a_2)$. The equation can be viewed as

$$(a_1x_1 + a_2x_2) + a_3x_3 + \cdots + a_nx_n = c.$$

Since any integer linear combination of a_1 and a_2 is a multiple of d_2, we introduce an auxiliary variable y such that $a_1x_1 + a_2x_2 = d_2y$. This auxiliary equation is solvable for any integer y because $(a_1, a_2) = d_2$. Substituting this into the original equation yields a new equation in $n - 1$ variables:

$$d_2y + a_3x_3 + \cdots + a_nx_n = c.$$

The greatest common divisor of the coefficients is $(d_2, a_3, \ldots, a_n) = ((a_1, a_2), a_3, \ldots, a_n) = (a_1, \ldots, a_n)$. By hypothesis, since $(a_1, \ldots, a_n) \mid c$, this reduced equation has integer solutions for $y, x_3, \ldots, x_n$. Once y is determined, we solve $a_1x_1 + a_2x_2 = d_2y$ for x_1 and x_2. Thus, the original equation has integer solutions.

証明終

Corollary 9.3. If $(a_1, \ldots, a_n) = 1$, the equation always possesses integer solutions.

推論

Methods of Solution

We present three distinct approaches for constructing the general solution.

Method 1: Iterative Reduction

Following the logic of the induction proof, we can reduce an n-variable equation to a system of 2-variable equations.

Example 9.8. Iterative Reduction. Find the general solution of $9x + 24y - 5z = 1000$.
First, observe that $(9, 24) = 3$. We introduce a parameter t such that:

$$9x + 24y = 3t.$$

This allows us to rewrite the original equation as:

$$3t - 5z = 1000.$$

We now solve these two equations sequentially.

1. **Solve** $9x + 24y = 3t$**:** Dividing by 3 gives $3x + 8y = t$. Since $(3, 8) = 1$, we can express t as a linear combination. A particular solution for $t = 1$ is $x = -5, y = 2$ (since $3(-5) + 8(2) = 1$). For a general t, a particular solution is $x = -5t, y = 2t$. Using *theorem* 9.2, the general solution for x, y in terms of t and an arbitrary integer u is:

   $$x = -5t + 8u, \quad y = 2t - 3u.$$

   (Note: The choice of particular solution is flexible. The source uses $3x + 8y = t \implies x = 3t + 8u, y = -t - 3u$, which is also valid).

2. **Solve** $3t - 5z = 1000$**:** Since $(3, 5) = 1$, solutions exist. Particular solution: $3(1000) - 5(400) = 3000 - 2000 = 1000$. So $t_0 = 1000, z_0 = 400$. General solution in terms of parameter v:

   $$t = 1000 + 5v, \quad z = 400 + 3v.$$

Substituting the expression for t into the solutions for x and y:

$$\begin{aligned} x &= -5(1000 + 5v) + 8u = -5000 - 25v + 8u \\ y &= 2(1000 + 5v) - 3u = 2000 + 10v - 3u \\ z &= 400 + 3v \end{aligned}$$

Here u, v are arbitrary integers.

範例

Method 2: Coefficient Reduction

Similar to the single-variable trial method, we can isolate variables with small coefficients to reduce the complexity of the constraints.

Example 9.9. Coefficient Reduction. Find the general solution of $25x - 13y + 7z = 4$.

We isolate z, the variable with the coefficient of smallest magnitude (excluding the sign), and split the right-hand side into a multiple of 7 plus a remainder:

$$7z = 13y - 25x + 4 = 7(-4x + 2y) + (3x - y + 4),$$

so

$$z = -4x + 2y + \frac{3x - y + 4}{7}.$$

Let $3x - y + 4 = 7t_1$. Then $y = 3x + 4 - 7t_1$. Substitute y back into the expression for z:

$$z = -4x + 2(3x + 4 - 7t_1) + t_1 = -4x + 6x + 8 - 14t_1 + t_1 = 2x - 13t_1 + 8.$$

Now x can be chosen arbitrarily. Let $x = t_2$. The general solution is:

$$\begin{cases} x = t_2 \\ y = 4 - 7t_1 + 3t_2 \\ z = 8 - 13t_1 + 2t_2 \end{cases}$$

where t_1, t_2 are arbitrary integers.

範例

Method 3: Parametric Construction

If a particular solution is known, one can construct a general solution using homogeneous generators. Specifically, if $\mathbf{x}_0$ is a solution to $\sum a_i x_i = c$, and we can find $n - 1$ linearly independent vectors $\boldsymbol{\eta}_j$ such that $\sum a_i (\eta_j)_i = 0$, then $\mathbf{x}_0 + \sum t_j \boldsymbol{\eta}_j$ generates solutions.

A simple set of generators can be formed by coupling the last variable x_n with each x_i ($i < n$). The vectors $\boldsymbol{\eta}_i$ where the i-th component

is a_n, the n-th component is $-a_i$, and others are 0, satisfy the homogeneous equation.

Example 9.10. Parametric Formula. Find the general solution of $2x_1 + 3x_2 + 5x_3 + 7x_4 = 19$.
By inspection, a particular solution is $x_1 = 5, x_2 = -1, x_3 = 1, x_4 = 1$. $(2(5) + 3(-1) + 5(1) + 7(1) = 10 - 3 + 5 + 7 = 19)$. We construct the general solution by varying x_1, x_2, x_3 independently with step $a_4 = 7$, and adjusting x_4 to compensate.

$$\begin{cases} x_1 = 5 + 7t_1 \\ x_2 = -1 + 7t_2 \\ x_3 = 1 + 7t_3 \\ x_4 = 1 - (2t_1 + 3t_2 + 5t_3) \end{cases}$$

Checking the sum:

$$2(7t_1) + 3(7t_2) + 5(7t_3) + 7(-2t_1 - 3t_2 - 5t_3) = 0.$$

This form captures integer solutions generated by this specific basis of the null space.

範例

9.4 *Systems of Indefinite Equations*

Many problems, particularly those of historical significance, involve systems of linear Diophantine equations. These can be solved by eliminating variables to reduce the system to a single indefinite equation.

Example 9.11. The Hundred Fowls Problem. A classic problem from 5th-century China states:
"A rooster is worth 5 coins, a hen 3 coins, and 3 chicks 1 coin. 100 coins buy 100 fowls. How many of each are there?"
Let x, y, z be the number of roosters, hens, and chicks respectively. The constraints are:

$$\begin{cases} x + y + z = 100 & \text{(Quantity)} \\ 5x + 3y + \frac{1}{3}z = 100 & \text{(Value)} \end{cases}$$

Multiply the second equation by 3 to clear the fraction:

$$15x + 9y + z = 300.$$

We subtract the first equation $(x + y + z = 100)$ from this new equation to eliminate z:

$$(15x + 9y + z) - (x + y + z) = 300 - 100 \implies 14x + 8y = 200.$$

Dividing by 2:

$$7x + 4y = 100.$$

This is a standard 2-variable indefinite equation. Isolating y:

$$4y = 100 - 7x \implies y = 25 - \frac{7x}{4} = 25 - x - \frac{3x}{4}.$$

For y to be an integer, x must be a multiple of 4. Let $x = 4t$. Then $y = 25 - 7t$. Substituting x and y back into $z = 100 - x - y$:

$$z = 100 - 4t - (25 - 7t) = 75 + 3t.$$

The general integer solution is:

$$x = 4t, \quad y = 25 - 7t, \quad z = 75 + 3t.$$

Since the quantities must be non-negative:

$$\begin{cases} 4t \geq 0 \implies t \geq 0 \\ 25 - 7t \geq 0 \implies t \leq 3.57 \\ 75 + 3t \geq 0 \implies t \geq -25 \end{cases}$$

The possible integer values for t are $\{0, 1, 2, 3\}$. The solutions (x, y, z) are:

- $t = 0 : (0, 25, 75)$
- $t = 1 : (4, 18, 78)$
- $t = 2 : (8, 11, 81)$
- $t = 3 : (12, 4, 84)$

範例

Example 9.12. Egyptian Fraction Decomposition. Express $\frac{77}{60}$ as a sum of three proper irreducible fractions with denominators 4, 3, and 5.

We set:

$$\frac{77}{60} = \frac{x}{4} + \frac{y}{3} + \frac{z}{5}.$$

Multiplying by 60:

$$15x + 20y + 12z = 77.$$

We use Method 2 (Coefficient Reduction). Isolate z:

$$12z = 77 - 15x - 20y \implies z = \frac{77 - 15x - 20y}{12} = 6 - x - y + \frac{5 - 3x - 8y}{12}.$$

We need $12 \mid (5 - 3x - 8y)$. Let us test small integers. Try $x = 3$: $5 - 9 - 8y = -4 - 8y$. We need $12 \mid (-4 - 8y)$, or $3 \mid (-1 - 2y)$. If $y = 1$, $-1 - 2 = -3$ (divisible by 3). So $x = 3, y = 1$ works. Substitute back

to find z:

$$12z = 77 - 15(3) - 20(1) = 77 - 45 - 20 = 12 \implies z = 1.$$

The solution is $(3, 1, 1)$.

$$\frac{77}{60} = \frac{3}{4} + \frac{1}{3} + \frac{1}{5}.$$

範例

Example 9.13. Making Change. Find the general non-negative integer solution to the equation $6x + 10y + 15z = 31$.
Note $(6, 10, 15) = 1$, so solutions exist. We simplify modulo 5 (since two coefficients are multiples of 5).

$$6x + 0 + 0 \equiv 31 \pmod 5 \implies x \equiv 1 \pmod 5.$$

Let $x = 1 + 5t$. Since $x \geq 0$ and $6x \leq 31 \implies x \leq 5$, possible values for x are restricted. If $x = 1$: $6(1) + 10y + 15z = 31 \implies 10y + 15z = 25 \implies 2y + 3z = 5$. This simple 2-variable equation has non-negative solutions $(y, z) \in \{(1, 1)\}$. $(2(1) + 3(1) = 5)$. If $x = 6$: $36 > 31$, impossible. Thus the unique non-negative solution is $(1, 1, 1)$.

範例

Geometric Dissection

We conclude with an application to geometric tiling, where a rectangle is partitioned into squares of unequal integer sides.

Example 9.14. Rectangle Dissection. Consider a rectangle partitioned into 9 squares with side lengths determined by three initial parameters x, y, z as shown in *figure* 9.3. The side lengths of the squares are derived from the geometric adjacency as:

$$x, y, z, x + y, 2x + y, y - z, y - 2z, y - 3z, 2y - 5z.$$

By equating the lengths of opposite sides of the composite rectangle, one derives the homogeneous system:

$$\begin{cases} 3x - 2y + 8z = 0 \\ x - 4z = 0 \end{cases}$$

Substituting $x = 4z$ into the first equation:

$$3(4z) - 2y + 8z = 0 \implies 20z = 2y \implies y = 10z.$$

The general integer solution is $(4t, 10t, t)$. For the smallest positive solution, we take $t = 1$, yielding $x = 4, y = 10, z = 1$. This gener-

ates a rectangle of size 33 × 32. The side lengths of the component squares are $\{4, 10, 1, 14, 18, 9, 8, 7, 15\}$.

範例

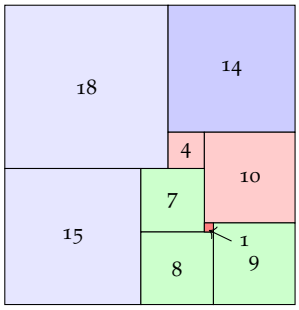


Figure 9.3: Decomposition of a 32 × 33 rectangle into squares. The squares labelled 4, 10, and 1 correspond to x, y, z.

9.5 *Exercises*

1. **General Solutions of Linear Diophantine Equations.** Find the general integer solution for each of the following equations. If no solution exists, state why.
   (a) $11x - 13y = 8$
   (b) $6x + 17y = -5$
   (c) $34x + 109y = 20$
   (d) $31x - 127y = 53$
   (e) $54x + 37y = 20$
   (f) $306x - 360y = 630$
2. **Constrained Solutions.** Find all positive integer solutions (x, y) such that $x < 100$ for the equation:
$$8x - 5y = -200.$$
3. **Logistics Optimisation.** A logistics company needs to transport exactly 46 tons of goods. They have two types of vehicles: trucks with a 4-ton capacity and vans with a 2.5-ton capacity. Every vehicle used must be fully loaded. Determine the number of trucks and vans required if the company wants to use the fewest vehicles.
4. **Counting Non-Negative Solutions.** Let a, b be coprime positive integers. Prove that the number of non-negative integer solutions to $ax + by = N$ is either $\lfloor \frac{N}{ab} \rfloor$ or $\lfloor \frac{N}{ab} \rfloor + 1$.
5. **Frobenius Bound for Three Variables.** Let a, b, c be pairwise coprime positive integers. Consider the equation:
$$bcx + cay + abz = N.$$
   (a) Prove that if $N = 2abc - ab - bc - ca$, there are no non-negative integer solutions.
   (b) Prove that if $N > 2abc - ab - bc - ca$, there exists at least one non-negative integer solution.
6. **Solvability of Systems.** Determine whether the following equations possess integer solutions:
   (a) $12x + 6y + 9z = 83$

(b) $-7x + 28y + 91z - 35t = 161$

7. **General Solutions for Systems.** Find the general integer solution for:

   (a) $25x - 13y + 7z = 4$

   (b) $39x - 24y + 9z = 78$

8. **The Generalised Coin Problem.** Let $a_1, \ldots, a_n$ be pairwise coprime positive integers. Let $A = \prod a_i$ and $A_i = A/a_i$. Consider the linear form $L = \sum A_i x_i$ with $x_i \geq 0$. Prove that the largest integer not representable in this form is:

$$(n-1)A - \sum_{i=1}^{n} A_i.$$

9. **Egyptian Fraction Decomposition.** Express the fraction $\frac{181}{180}$ as a sum of three proper irreducible fractions with pairwise coprime denominators.

10. **The Monkey and the Coconuts.** Five sailors and a monkey are stranded on an island with a pile of coconuts. During the night, the first sailor wakes up, divides the pile into 5 equal shares, finds 1 coconut left over, gives it to the monkey, hides his share, and recombines the rest. The second sailor wakes up and does the same (divides remaining into 5, 1 left for monkey, hides share). This continues for the third, fourth, and fifth sailors. In the morning, the remaining pile is divided into 5 equal shares with **no** coconuts left over. Find the smallest possible number of original coconuts and the total number each sailor received.

10
Pythagorean Triples

Following our investigation of linear indefinite equations, we now turn our attention to the quadratic case. The most fundamental of these is the homogeneous equation

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

which governs the side lengths of right-angled triangles. Historically, integer solutions to this equation have been studied since antiquity. In this chapter, we derive a complete parameterisation of the integer solutions to this equation and extend our methods to related non-linear Diophantine problems.

10.1 The Structure of Solutions

We seek all integer triples (x, y, z) satisfying the Pythagorean equation. We may assume without loss of generality that x, y, z are positive.

Definition 10.1. ***Pythagorean Triples.***
A set of positive integers x, y, z satisfying

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

is called a **Pythagorean triple**. If $(x, y, z) = 1$, the triple is termed **primitive**.

定義

We first observe that it suffices to determine the primitive triples. If $(x, y) = d$, then $d^2 \mid (x^2 + y^2)$, implying $d^2 \mid z^2$ and thus $d \mid z$. Writing $x = dx_1, y = dy_1, z = dz_1$, we obtain the reduced equation $x_1^2 + y_1^2 = z_1^2$ with $(x_1, y_1) = 1$. Consequently, any Pythagorean triple is a scalar multiple of a primitive one.
For a primitive triple (x, y, z), the integers x, y, z are pairwise coprime. It is impossible for both x and y to be even, as $(x, y) = 1$. Suppose both x and y are odd. Then $x^2 \equiv 1 \pmod 4$ and $y^2 \equiv 1$

$(\text{mod } 4)$, yielding:

$$z^2 = x^2 + y^2 \equiv 1 + 1 \equiv 2 \pmod 4.$$

However, a perfect square must be congruent to 0 or 1 modulo 4. This contradiction implies that x and y must have opposite parity. Without loss of generality, we assume x is even and y is odd. Consequently, z must be odd.
To classify these solutions, we require a preliminary lemma regarding the factorization of squares.

Lemma 10.1. ***Square Product of Coprime Integers.***
Let u, v, w be positive integers such that $uv = w^2$ and $(u, v) = 1$. Then u and v are both perfect squares. That is, there exist integers a, b such that

$$u = a^2, \quad v = b^2, \quad \text{and} \quad w = ab.$$

引理

Proof

Consider the prime factorisation of u and v:

$$u = \prod p_i^{e_i}, \quad v = \prod q_j^{f_j}.$$

Since $(u, v) = 1$, the sets of primes $\{p_i\}$ and $\{q_j\}$ are disjoint. The equation $uv = w^2$ implies

$$\prod p_i^{e_i} \prod q_j^{f_j} = w^2.$$

By the Fundamental Theorem of Arithmetic, the exponent of every prime factor in w^2 must be even. Since the prime sets are disjoint, each e_i and f_j must be even. Let $e_i = 2k_i$ and $f_j = 2m_j$. Then

$$u = \left(\prod p_i^{k_i}\right)^2 \quad \text{and} \quad v = \left(\prod q_j^{m_j}\right)^2.$$

Thus u and v are perfect squares.

■

We now present the classical parameterisation of primitive Pythagorean triples.

Theorem 10.1. ***Classification of Primitive Triples.***
All primitive Pythagorean triples x, y, z with x even are given by the formulae:

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2,$$

where a, b are integers satisfying:
1. $a > b > 0$,
2. $(a, b) = 1$,

3. a and b have opposite parity (one is even, the other odd).

定理

Proof

Let (x, y, z) be a primitive triple with x even. Then y and z are odd, so $z + y$ and $z - y$ are both even integers. We can rewrite the Pythagorean equation as:

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

Dividing by 4, we obtain:

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right).$$

Let $u = \frac{z+y}{2}$ and $v = \frac{z-y}{2}$. Note that u and v are integers. Let $d = (u, v)$. Then d divides their sum $u + v = z$ and their difference $u - v = y$. Since $(y, z) = 1$, we must have $d = 1$. Thus $uv = (x/2)^2$ with $(u, v) = 1$. By *lemma* 10.1, u and v are perfect squares. We write

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2,$$

for some coprime positive integers a, b. Solving for z and y:

$$z = a^2 + b^2, \quad y = a^2 - b^2.$$

Since $y > 0$, we require $a > b$. Also, $x/2 = ab$, so $x = 2ab$. It remains to satisfy the parity condition. Since $z = a^2 + b^2$ is odd, a^2 and b^2 must have opposite parity, which implies a and b have opposite parity. Conversely, substituting these expressions into $x^2 + y^2$ verifies the equation. One can also check that these conditions ensure $(x, y, z) = 1$.

■

This result extends naturally to the rational numbers, providing a correspondence between Pythagorean triples and rational points on the unit circle.

Corollary 10.1. *Rational Points on the Unit Circle.* Every rational point (X, Y) on the unit circle $X^2 + Y^2 = 1$ (excluding $(-1, 0)$) can be expressed as

$$\left(\frac{a^2 - b^2}{a^2 + b^2}, \frac{2ab}{a^2 + b^2}\right) \quad \text{or} \quad \left(\frac{2ab}{a^2 + b^2}, \frac{a^2 - b^2}{a^2 + b^2}\right),$$

for some coprime integers a, b.

推論

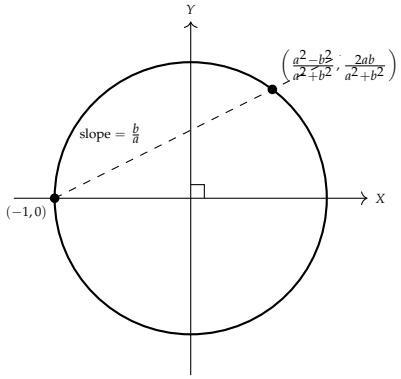


Figure 10.1: The line from $(-1, 0)$ with slope b/a intersects the unit circle at the rational point corresponding to the primitive triple.

Proof

Let $X, Y \in \mathbb{Q}$ satisfy $X^2 + Y^2 = 1$. We restrict our attention to the first quadrant ($X, Y > 0$). Write $X = q/p$ and $Y = r/p$ with a common denominator p. The condition becomes $q^2 + r^2 = p^2$. This is an integer Pythagorean triple. Applying *theorem* 10.1, we substitute the parametric forms of q, r, p to obtain the result. Symmetry handles the other quadrants.

■

Properties and Applications

We illustrate the utility of the classification theorem with several examples relating to divisibility and geometric constraints.

Example 10.1. Divisibility by 60. Let x, y, z be a primitive Pythagorean triple. Prove that $60 \mid xyz$.
We use the parameterisation $x = 2ab, y = a^2 - b^2, z = a^2 + b^2$. The product is $xyz = 2ab(a^4 - b^4)$. We analyse the prime factors of 60: 3, 4, and 5.

Divisibility by 4 Since one of a, b is even, $2ab$ is divisible by 4. Thus $4 \mid xyz$.

Divisibility by 3 If $3 \mid a$ or $3 \mid b$, then $3 \mid xyz$. If neither is divisible by 3, then $a^2 \equiv 1 \pmod 3$ and $b^2 \equiv 1 \pmod 3$. Thus $a^2 - b^2 \equiv 0 \pmod 3$. In all cases, $3 \mid xyz$.

Divisibility by 5 If $5 \mid a$ or $5 \mid b$, then $5 \mid xyz$. If not, by Fermat's Little Theorem, $a^4 \equiv 1 \pmod 5$ and $b^4 \equiv 1 \pmod 5$. Thus $a^4 - b^4 \equiv 0 \pmod 5$.

Since 3, 4, and 5 are pairwise coprime, their product 60 divides xyz.

範例

Example 10.2. Inradius of Pythagorean Triangles. Determine the primitive Pythagorean triples with an inradius of $r = 3$.
The inradius r of a right-angled triangle with legs x, y and hypotenuse z is given by $r = \frac{x+y-z}{2}$. Substituting the parametric forms:

$$r = \frac{2ab + (a^2 - b^2) - (a^2 + b^2)}{2} = \frac{2ab - 2b^2}{2} = b(a - b).$$

We are given $b(a - b) = 3$. Since b is an integer, b must be a factor of 3.

1. $b = 1$: Then $a - 1 = 3 \implies a = 4$. Check conditions: $(4, 1) = 1$ and opposite parity. Valid. Triple: $x = 2(4)(1) = 8$, $y = 16 - 1 = 15$, $z = 16 + 1 = 17$.

2. $b = 3$: Then $a - 3 = 1 \implies a = 4$. Check conditions: $(4, 3) = 1$ and opposite parity. Valid. Triple: $x = 2(4)(3) = 24$, $y = 16 - 9 = 7$, $z = 16 + 9 = 25$.

The solutions are $(8, 15, 17)$ and $(24, 7, 25)$.

範例

Example 10.3. Fixed Hypotenuse. Find all Pythagorean triples (primitive and non-primitive) with hypotenuse $z = 65$.

We solve $k(a^2 + b^2) = 65$. The divisors of 65 are 1, 5, 13, 65.

· $k = 1 \implies a^2 + b^2 = 65$. Solutions: $8^2 + 1^2$ and $7^2 + 4^2$. For $(8, 1)$: $x = 16, y = 63, z = 65$. (Primitive) For $(7, 4)$: $x = 56, y = 33, z = 65$. (Primitive)

· $k = 5 \implies a^2 + b^2 = 13$. Solution: $3^2 + 2^2$. For $(3, 2)$ scaled by 5: $x = 5(12) = 60, y = 5(5) = 25, z = 65$.

· $k = 13 \implies a^2 + b^2 = 5$. Solution: $2^2 + 1^2$. For $(2, 1)$ scaled by 13: $x = 13(4) = 52, y = 13(3) = 39, z = 65$.

The set of solutions is $\{(16, 63, 65), (33, 56, 65), (25, 60, 65), (39, 52, 65)\}$.

範例

Example 10.4. Fixed Perimeter. Find the primitive Pythagorean triple with perimeter $P = 40$.

The perimeter is $P = x + y + z = 2ab + a^2 - b^2 + a^2 + b^2 = 2a^2 + 2ab = 2a(a + b)$. We require $2a(a + b) = 40 \implies a(a + b) = 20$. Since $a < a + b$, $a^2 < 20$, so $a \in \{1, 2, 3, 4\}$. We test values for a:

· If $a = 1$, $1 + b = 20 \implies b = 19$. Both odd (invalid).

· If $a = 2$, $2 + b = 10 \implies b = 8$. Not coprime (invalid).

· If $a = 3$, $3(3 + b) = 20$ has no integer solution.

· If $a = 4$, $4 + b = 5 \implies b = 1$. Even/odd, coprime. Valid.

This yields the triple $x = 2(4)(1) = 8$, $y = 15$, $z = 17$.

範例

Example 10.5. Leg and Hypotenuse Difference. Prove that if the difference between the hypotenuse and a leg of a primitive Pythagorean triangle is 1, the sides are of the form $2b + 1, 2b^2 + 2b, 2b^2 + 2b + 1$.

Note that $z - y = 2b^2$ cannot equal 1, so the leg must be the even one. Let $z - x = 1$. Since z is odd (in a primitive triple), x must be even. Using the parameterisation:

$$z - x = (a^2 + b^2) - 2ab = (a - b)^2 = 1.$$

Thus $a - b = 1$, or $a = b + 1$. Substituting $a = b + 1$ into the formu-

lae:

$$x = 2(b+1)b = 2b^2 + 2b$$
$$y = (b+1)^2 - b^2 = 2b + 1$$
$$z = (b+1)^2 + b^2 = 2b^2 + 2b + 1$$

範例

Generalised Quadratic Equations

The method of descent and parameterisation can be applied to higher-degree variations of the Pythagorean equation.

Proposition 10.1. ***Solutions to*** $x^2 + y^2 = z^4$**.**
All primitive positive integer solutions to $x^2 + y^2 = z^4$ with x even are given by:

$$x = 4ab(a^2 - b^2), \quad y = |a^4 + b^4 - 6a^2b^2|, \quad z = a^2 + b^2,$$

where a, b are coprime integers of opposite parity.

命題

Proof

If $(x, y) = 1$, then (x, y, z^2) is a primitive Pythagorean triple. Thus:

$$x = 2rs, \quad y = r^2 - s^2, \quad z^2 = r^2 + s^2,$$

for coprime r, s of opposite parity. The equation $r^2 + s^2 = z^2$ indicates that (r, s, z) is itself a Pythagorean triple (ignoring parity of r, s for a moment). However, since r, s are coprime and one is even, (r, s, z) is primitive. We consider two cases based on parity:

s ***is even.*** We can write $s = 2ab, r = a^2 - b^2$ (since r is odd). Then $x = 2(a^2 - b^2)(2ab) = 4ab(a^2 - b^2)$. And $y = (a^2 - b^2)^2 - (2ab)^2 = a^4 - 2a^2b^2 + b^4 - 4a^2b^2 = a^4 + b^4 - 6a^2b^2$.

r ***is even.*** We write $r = 2ab, s = a^2 - b^2$. Then $y = (2ab)^2 - (a^2 - b^2)^2 = -(a^4 + b^4 - 6a^2b^2)$.

Combining these yields the magnitude form for y.

■

Example 10.6. Sum of Sides is a Square. Determine the form of primitive triples where $x + y + z$ is a perfect square.
Using the parameterisation $x = 2ab, y = a^2 - b^2, z = a^2 + b^2$:

$$x + y + z = 2ab + 2a^2 = 2a(a + b).$$

Since $(a, b) = 1$, we have $(a, a + b) = 1$. For $2a(a + b)$ to be a square, the factors must complement each other to form squares. Because

a and b have opposite parity, $a+b$ is odd, so $(2a, a+b) = 1$. Thus both factors must be squares. Hence

$$2a = (2m)^2 \quad \text{and} \quad a+b = n^2,$$

with n odd. This gives $a = 2m^2$ and $b = n^2 - 2m^2$ (with $n^2 > 2m^2$). There are no solutions with a odd because then $2a$ cannot be a square.

範例

Finally, we consider a weighted quadratic form involving an odd prime p.

Theorem 10.2. ***The Equation*** $x^2 + py^2 = z^2$**.**
Let p be an odd prime. The positive integer solutions to $x^2 + py^2 = z^2$ with $(x, y) = 1$ fall into two classes:

1. $x = \frac{1}{2}|a^2 - pb^2|$, $y = ab$, $z = \frac{1}{2}(a^2 + pb^2)$, where a, b are coprime odd integers.
2. $x = |a^2 - pb^2|$, $y = 2ab$, $z = a^2 + pb^2$, where a, b are coprime integers of opposite parity.

定理

Proof

The equation implies $z^2 - x^2 = py^2$, so $(z-x)(z+x) = py^2$. Since p is prime, $p \mid (z-x)$ or $p \mid (z+x)$. Replacing x by $-x$ if necessary (absorbed by the absolute values), we may assume $p \mid (z-x)$ and write $z = x + pk$. Then $y^2 = k(2x + pk)$. Because $(x, y) = 1$, we cannot have $p \mid x$ (otherwise $p \mid z$ and hence $p \mid y$). Thus $(x, k) = 1$ and

$$(k, 2x + pk) = (k, 2x) \in \{1, 2\}.$$

If $(k, 2x) = 1$, then k is odd and the two factors are coprime squares. Write $k = b^2$ and $2x + pk = a^2$ with $(a, b) = 1$. Then a, b are odd and

$$x = \frac{1}{2}|a^2 - pb^2|, \quad y = ab, \quad z = \frac{1}{2}(a^2 + pb^2).$$

If $(k, 2x) = 2$, write $k = 2b^2$ and $2x + pk = 2a^2$ with $(a, b) = 1$. Then

$$x = |a^2 - pb^2|, \quad y = 2ab, \quad z = a^2 + pb^2.$$

Since x is odd, a and b must have opposite parity.

■

10.2 *Fermat's Last Theorem and Infinite Descent*

In 1637, Pierre de Fermat famously noted in the margin of his copy of Diophantus' *Arithmetica* that the equation $x^n + y^n = z^n$ possesses no non-zero integer solutions for $n \geq 3$. While his "truly marvelous proof" for the general case remains a historical mystery, Fermat did leave a rigorous proof for the case $n = 4$.

The theorem was not fully proven until 1994 by Andrew Wiles

The method he developed, known as the **Method of Infinite Descent**, is a powerful tool in number theory. The logical foundation is the well-ordering principle introduced in Chapter 0 of the positive integers. To show that a Diophantine equation has no solutions, we assume the existence of a solution and construct a strictly smaller positive integer solution. Repeating this process generates an infinite sequence of decreasing positive integers, which is impossible.

The Case $n = 4$

We begin by establishing Fermat's Last Theorem for the exponent 4. In fact, we prove a stronger result: the sum of two fourth powers cannot be a perfect square.

Theorem 10.3. ***Fermat's Last Theorem for*** $n = 4$**.**
The Diophantine equation

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

has no solutions in positive integers.

定理

Proof

Suppose, for the sake of contradiction, that there exists a positive integer solution. Let u be the smallest positive integer such that $x^4 + y^4 = u^2$ for some positive integers x, y. We may assume $(x, y) = 1$; otherwise, we could divide by the common factor to obtain a smaller solution.

The equation can be written as $(x^2)^2 + (y^2)^2 = u^2$. Thus, (x^2, y^2, u) is a primitive Pythagorean triple. Since x^2 and y^2 cannot both be odd (as their sum $u^2 \equiv 2 \pmod 4$ is impossible for a square), one is even and one is odd. Without loss of generality, let x^2 be even. By *theorem* 10.1, there exist coprime integers a, b of opposite parity such that:

$$x^2 = 2ab, \quad y^2 = a^2 - b^2, \quad u = a^2 + b^2.$$

Consider the equation $y^2 = a^2 - b^2$, or $y^2 + b^2 = a^2$. Since $(a, b) = 1$, this forms a primitive Pythagorean triple (y, b, a). Since y is odd (from the first triple), b must be even and a must be odd. We apply

the parameterisation of Pythagorean triples again to $y^2 + b^2 = a^2$. There exist coprime integers p, q of opposite parity such that:

$$b = 2pq, \quad y = p^2 - q^2, \quad a = p^2 + q^2.$$

Substituting these back into the expression for x^2:

$$x^2 = 2ab = 2(p^2 + q^2)(2pq) = 4pq(p^2 + q^2).$$

Since $(p, q) = 1$, the terms p, q, and $p^2 + q^2$ are pairwise coprime. For their product to be a perfect square ($x^2/4$), each term must be a perfect square. Let

$$p = r^2, \quad q = s^2, \quad p^2 + q^2 = t^2.$$

Substituting the first two into the third yields:

$$(r^2)^2 + (s^2)^2 = t^2 \implies r^4 + s^4 = t^2.$$

Thus, (r, s, t) is a positive integer solution to the original equation. We observe the size of t:

$$t^2 = p^2 + q^2 = a \leq a^2 + b^2 = u.$$

Since u is a sum of squares of positive integers, $u > a$, so $t^2 < u$, which implies $t < \sqrt{u} < u$. This contradicts the minimality of u. Hence, no such solution exists.

■

Corollary 10.2. The equation $x^4 + y^4 = z^4$ has no positive integer solutions.

推論

Proof

If $x^4 + y^4 = z^4$, then $x^4 + y^4 = (z^2)^2$. This would provide a solution to $x^4 + y^4 = w^2$ with $w = z^2$, which is impossible by *theorem* 10.3.

■

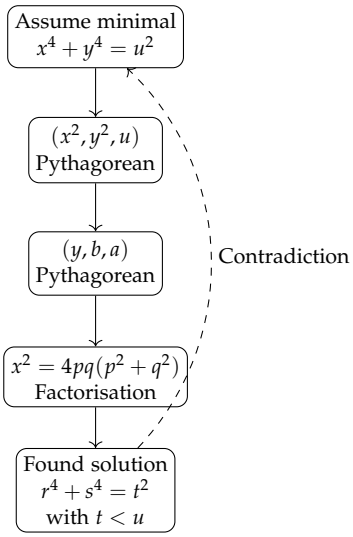


Figure 10.2: The descent process for $x^4 + y^4 = u^2$.

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

The method of infinite descent can be applied to variations of the quartic equation.

Theorem 10.4. ***Non-existence for Difference of Fourth Powers.*** The indefinite equation

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

has no solutions in positive integers with $(x, y) = 1$.

定理

Proof

We proceed by infinite descent. Let x be the smallest positive integer in any such solution. Since $(x, y) = 1$, x and y cannot both be even. If they are both odd, $x^4 - y^4 \equiv 1 - 1 \equiv 0 \pmod 2$, while z^2 is divisible by a high power of 2, leading to parity constraints. More directly, we rewrite the equation as:

$$(y^2)^2 + z^2 = (x^2)^2.$$

Thus (y^2, z, x^2) is a primitive Pythagorean triple. Since $(x, y) = 1$, x^2 is odd, so y^2 and z have opposite parity.

y is odd. Then z is even. By *theorem* 10.1, there exist coprime a, b $(a > b > 0)$ such that:

$$y^2 = a^2 - b^2, \quad z = 2ab, \quad x^2 = a^2 + b^2.$$

Multiplying the expressions for x^2 and y^2:

$$x^2y^2 = (a^2 + b^2)(a^2 - b^2) = a^4 - b^4.$$

This yields $a^4 - b^4 = (xy)^2$. This is an instance of the original equation with solution (a, b, xy). However, $x^2 = a^2 + b^2 > a^2$, so $x > a$. This contradicts the minimality of x.

y is even. Then z is odd. By the structure of Pythagorean triples:

$$z = a^2 - b^2, \quad y^2 = 2ab, \quad x^2 = a^2 + b^2.$$

Since $y^2 = 2ab$ and $(a, b) = 1$, one of a, b is even. If a is odd and b is even, $x^2 = a^2 + b^2 \equiv 1 \pmod 4$. This is consistent. If a is even and b is odd, $x^2 = a^2 + b^2 \equiv 1 \pmod 4$. However, looking at $y^2 = 2ab$, let $a = 2u^2$ and $b = v^2$ (or vice versa). Then $x^2 = 4u^4 + v^4$. Thus $(v^2, 2u^2, x)$ is a primitive Pythagorean triple:

$$v^2 = r^2 - s^2, \quad 2u^2 = 2rs, \quad x = r^2 + s^2.$$

From $u^2 = rs$ with $(r, s) = 1$, we have $r = m^2, s = n^2$. Then $v^2 = m^4 - n^4$. This is $m^4 - n^4 = v^2$, another instance of the original equation. We check the size: $m = \sqrt{r} \leq \sqrt{u^2} = u < \sqrt{2u^2} \leq \sqrt{a} < x$. Thus $m < x$, contradicting the minimality of x.

■

This theorem allows us to resolve the area problem for right-angled triangles.

Example 10.7. Fermat's Right Triangle Theorem. Prove that the area of a right-angled triangle with integer sides cannot be a perfect square.
Let the sides be u, v, w with $u^2 + v^2 = w^2$. The area is $A = \frac{1}{2}uv$. Assume $A = k^2$ for some integer k. Then $uv = 2k^2$. We may assume $(u, v) = 1$ (otherwise divide out the common factor), so (u, v, w) is primitive and w is odd. Any prime divisor of w cannot divide k, so $(w, 2k) = 1$. We have a system:

$$u^2 + v^2 = w^2, \quad 2uv = 4k^2.$$

Adding and subtracting these equations:

$$(u + v)^2 = w^2 + 4k^2, \quad (u - v)^2 = w^2 - 4k^2.$$

Multiplying them:

$$(u^2 - v^2)^2 = (u + v)^2(u - v)^2 = w^4 - 16k^4.$$

Let $X = w, Y = 2k, Z = |u^2 - v^2|$. Then $X^4 - Y^4 = Z^2$. By *theorem* 10.4, this equation has no integer solutions, so the area cannot be a square.

範例

Descent by Divisibility

Infinite descent does not always require the Pythagorean structure. It often arises from divisibility properties, particularly when a prime factor must divide variables to infinite order.

Example 10.8. A Cubic Equation. Prove that $x^3 = 2y^3 + 4z^3$ has no positive integer solutions.
Assume a solution (x_0, y_0, z_0) exists. The equation implies x_0^3 is even, so x_0 is even. Let $x_0 = 2x_1$. Substituting: $8x_1^3 = 2y_0^3 + 4z_0^3$. Dividing by 2:

$$4x_1^3 = y_0^3 + 2z_0^3.$$

This implies y_0^3 is even, so $y_0 = 2y_1$. Substituting: $4x_1^3 = 8y_1^3 + 2z_0^3$. Dividing by 2:

$$2x_1^3 = 4y_1^3 + z_0^3.$$

This implies z_0^3 is even, so $z_0 = 2z_1$. Substituting: $2x_1^3 = 4y_1^3 + 8z_1^3$. Dividing by 2:

$$x_1^3 = 2y_1^3 + 4z_1^3.$$

Thus (x_1, y_1, z_1) is a solution with $x_1 < x_0$. This process can be repeated indefinitely ($x_n = x_0/2^n$), which is impossible for integers.

範例

We present a geometric application of this divisibility argument.

Example 10.9. Diophantine Constraints on Coordinates. Prove that the equation $x^2 + y^2 = 3z^2$ has no non-zero integer solutions.
Assume a minimal positive solution (x, y, z). Consider the equation modulo 3.

$$x^2 + y^2 \equiv 3z^2 \equiv 0 \pmod 3.$$

The quadratic residues modulo 3 are 0 and 1. If $x^2 \equiv 1$, then $x^2 + y^2 \equiv 1 + 0$ or $1 + 1$, neither of which is $0 \pmod 3$. Thus, we must have $x^2 \equiv 0$ and $y^2 \equiv 0$. This implies $3 \mid x$ and $3 \mid y$. Let $x = 3x_1$ and $y = 3y_1$. Substituting back:

$$(3x_1)^2 + (3y_1)^2 = 3z^2 \implies 9x_1^2 + 9y_1^2 = 3z^2 \implies 3(x_1^2 + y_1^2) = z^2.$$

This implies $3 \mid z^2$, so $3 \mid z$. Let $z = 3z_1$.

$$3(x_1^2 + y_1^2) = 9z_1^2 \implies x_1^2 + y_1^2 = 3z_1^2.$$

We have constructed a solution (x_1, y_1, z_1) where $z_1 = z/3 < z$. This contradicts the minimality of the original solution.

範例

Constructing Solutions via Reverse Descent

While infinite descent is typically used to prove non-existence, the logic can be reversed to find solutions. If we can reduce a complex equation to a simpler form (descent), we can sometimes solve the simple form and retrace our steps (ascent) to generate large solutions. We examine the equation:

$$z^2 + 2(2xy)^2 = (x^2 - y^2 + 2xy)^2.$$

Let $X = x^4 + y^4 - 6x^2y^2$ and $Y = 4x^3y - 4xy^3$. The equation is equivalent to $X + Y = z^2$, and one checks that $X^2 + Y^2 = (x^2 + y^2)^4$. Let $s = x^2 + y^2$. Let $t = X - Y$. The system becomes:

$$\begin{cases} X + Y = z^2 \\ X^2 + Y^2 = s^4 \end{cases}$$

Substituting $X = \frac{1}{2}(z^2 + t)$ and $Y = \frac{1}{2}(z^2 - t)$ into the second equation yields:

$$\frac{1}{4}((z^2 + t)^2 + (z^2 - t)^2) = s^4 \implies \frac{1}{2}(2z^4 + 2t^2) = s^4 \implies 2s^4 - z^4 = t^2.$$

This is a reduced equation of the form $2s^4 - z^4 = t^2$.
From the original equation, $(z, 2xy, x^2 - y^2 + 2xy)$ satisfies

$$U^2 + 2V^2 = W^2.$$

For primitive solutions, we may write

$$U = |a^2 - 2b^2|, \quad V = 2ab, \quad W = a^2 + 2b^2,$$

where a, b are coprime positive integers and a is odd. Hence

$$z = |a^2 - 2b^2|, \quad 2xy = 2ab, \quad x^2 - y^2 + 2xy = a^2 + 2b^2.$$

From $2xy = 2ab$ we obtain $\frac{x}{a} = \frac{b}{y}$. Let the reduced fraction be $\frac{d}{c}$, and set

$$x = Kd, \quad a = Kc, \quad b = Ld, \quad y = Lc,$$

with integers $K, L \neq 0$. Substituting into $x^2 - y^2 + 2xy = a^2 + 2b^2$ gives

$$(c^2 + 2d^2)\left(\frac{L}{K}\right)^2 - 2cd\left(\frac{L}{K}\right) + (c^2 - d^2) = 0.$$

Since $\frac{L}{K}$ is rational, the discriminant must be a square:

$$\Delta = 4c^2d^2 - 4(c^2 + 2d^2)(c^2 - d^2) = 4(2d^4 - c^4) = (2e)^2,$$

so

$$2d^4 - c^4 = e^2.$$

Then

$$\frac{L}{K} = \frac{cd \pm e}{c^2 + 2d^2}.$$

The smallest solution to $2d^4 - c^4 = e^2$ is $c = d = e = 1$, which yields $\frac{L}{K} = \frac{2}{3}$. Taking $L = 2, K = 3$ gives

$$x = 3, \quad y = 2, \quad z = 1,$$

and indeed $1^2 + 2(12)^2 = 17^2$. For the next solution, note that $2(13)^4 - 1 = 239^2$, so $c = 1$, $d = 13$, $e = 239$. Then

$$\frac{L}{K} = -\frac{2}{3} \quad \text{or} \quad \frac{84}{113}.$$

Taking $L = 84$ and $K = 113$ yields

$$x = 1469, \quad y = 84, \quad z = 2372159,$$

which also satisfies the equation.

Example 10.10. Solving $x^4 - 2y^4 = 1$. Prove that $x^4 - 2y^4 = 1$ has no positive integer solutions.

範例

Proof

Assume a positive integer solution exists. Then x is odd, so $x^2 \pm 1$

are even. Write

$$x^2 - 1 = 2u, \quad x^2 + 1 = 2v,$$

so $uv = y^4$ and $(u, v) = 1$ because $(x^2 - 1, x^2 + 1) = 2$. Since uv is a fourth power and u and v are coprime, each of u and v is a fourth power. Indeed, in the prime factorization of u and v, the exponents add to multiples of 4 and the prime sets are disjoint, so each exponent is a multiple of 4. Thus

$$u = a^4, \quad v = b^4$$

for some positive integers a, b. Then

$$x^2 - 1 = 2a^4, \quad x^2 + 1 = 2b^4,$$

so subtracting gives

$$b^4 - a^4 = 1.$$

Factor:

$$(b^2 - a^2)(b^2 + a^2) = 1.$$

The only positive integer factorization of 1 is $1 \cdot 1$, which forces $b^2 - a^2 = 1$ and $b^2 + a^2 = 1$, hence $a = 0$, a contradiction to positivity. Therefore no positive integer solutions exist.

■

10.3 *Exponential Diophantine Equations*

Following our investigation of the quadratic Pythagorean equation $x^2 + y^2 = z^2$, we naturally extend our inquiry to higher powers. The general exponential equation

$$x^n + y^n = z^n, \quad n \geq 3$$

stands as one of the most famous problems in the history of mathematics. Known as Fermat's Last Theorem, its study has driven the development of algebraic number theory for over three centuries. In this chapter, we explore the solvability of this and related exponential Diophantine equations, establishing criteria for the existence of solutions and methods for their construction.

Fermat's Last Theorem

The study of the equation $x^n + y^n = z^n$ traditionally begins with a reduction of the exponent.

Claim 10.1. Reduction to Prime Exponents. If the equation $x^n + y^n = z^n$ has no positive integer solutions for $n = 4$ and for all odd primes

p, then it has no positive integer solutions for any integer $n \geq 3$.

主張

Proof

Any integer $n \geq 3$ is either divisible by 4 or by an odd prime p. If $n = kr$, the equation can be rewritten as:

$$(x^k)^r + (y^k)^r = (z^k)^r.$$

If n is a multiple of 4, we set $r = 4$. As established in the previous chapter (*Fermat's Last Theorem for $n = 4$*), the case $r = 4$ has no solutions, implying the general case has no solutions. If n is not divisible by 4, it possesses an odd prime factor p. Setting $r = p$, if the equation $X^p + Y^p = Z^p$ has no solutions, then neither does the original equation.

■

Historically, proofs were attempted prime by prime. Euler (1770) provided a proof for $p = 3$, though it required later refinement. The case $p = 5$ was settled independently by Legendre and Dirichlet (1825), with Lamé (1839) resolving $p = 7$. A significant advance occurred in 1847 when Kummer proved the theorem for all "regular" primes, covering all primes less than 100 except 37, 59, and 67. Kummer later resolved the cases for 59 and 67 in 1857.

The bounds on n were pushed progressively higher—Mirimanoff ($p = 37$, 1892), Wagstaff ($p < 125,000$, 1976), and Rosser ($n < 41,000,000$, 1985). The topological nature of the solution space was clarified by Faltings (1983), who proved that for $n \geq 3$, the equation has at most finitely many primitive solutions.

The complete resolution was finally announced by Andrew Wiles in 1993 at the Newton Institute in Cambridge. After correcting a subtle flaw with his student Richard Taylor, the proof was published in 1995, establishing that $x^n + y^n = z^n$ has no solution in positive integers for $n \geq 3$.

Solvable Exponential Equations

While the equation $x^n + y^n = z^n$ permits no solutions, relaxing the constraints on the exponents yields rich families of solutions. We consider equations of the form $x^n + y^n = z^m$.

Theorem 10.5. ***Existence of Solutions for Coprime Exponents.*** Let n, m be coprime positive integers. The Diophantine equation

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

possesses at least one family of positive integer solutions.

定理

Proof

We construct a solution using the method of common bases. Let $x = (ac)^u$ and $y = (bc)^u$, where a, b, c, u are positive integers to be determined. Substituting these into the equation:

$$(ac)^{nu} + (bc)^{nu} = c^{nu}(a^{nu} + b^{nu}) = z^m.$$

We set $z = c^v$ for some integer v. The equation becomes:

$$c^{nu}(a^{nu} + b^{nu}) = c^{mv}.$$

We impose the condition $a^{nu} + b^{nu} = c$. Then the left-hand side becomes $c^{nu} \cdot c = c^{nu+1}$. We require $c^{nu+1} = c^{mv}$, which implies:

$$mv - nu = 1.$$

Since $(m, n) = 1$, the linear Diophantine equation $mv - nu = 1$ has positive integer solutions for u and v (refer to the theory of the GCD from previous chapters). Once u is determined, we choose arbitrary positive integers a, b, set $c = a^{nu} + b^{nu}$, and derive x, y, z accordingly.

■

This theorem allows us to generate solutions for exponents that are close in value.

Corollary 10.3. The indeterminate equations $x^n + y^n = z^{n+1}$ and $x^n + y^n = z^{n-1}$ (for $n > 1$) always possess positive integer solutions.

推論

Example 10.11. Parametrising $x^n + y^n = z^{n+1}$. We apply the construction from *theorem* 10.5 with $m = n + 1$. The condition on the exponents is

$$(n+1)v - nu = 1.$$

Taking $u = n^2$ and $v = n^2 - n + 1$ satisfies this, since

$$(n+1)(n^2 - n + 1) - n(n^2) = n^3 + 1 - n^3 = 1.$$

Let a, b be any positive integers and set

$$c = a^{n^3} + b^{n^3}, \quad x = a^{n^2} c^{n^2}, \quad y = b^{n^2} c^{n^2}, \quad z = c^{\,n^2-n+1}.$$

Then

$$x^n + y^n = a^{n^3} c^{n^3} + b^{n^3} c^{n^3} = (a^{n^3} + b^{n^3}) c^{n^3} = c^{n^3+1}.$$

Also,

$$z^{n+1} = \left(c^{\,n^2-n+1}\right)^{n+1} = c^{(n^2-n+1)(n+1)} = c^{n^3+1}.$$

Hence this provides a family of positive integer solutions.

範例

Inductive Constructions

Mathematical induction can be utilized to extend solutions from small exponents to arbitrary ones.

Example 10.12. Sums of Squares as Powers. Prove that the equation $x^2 + y^2 = z^n$ has positive integer solutions for all $n \in \mathbb{Z}^+$.

範例

Base Cases.

For $n = 1$, $3^2 + 4^2 = 25 = 25^1$. For $n = 2$, $3^2 + 4^2 = 5^2$.

証明終

Inductive Step.

Assume there exist integers x_0, y_0, z_0 such that $x_0^2 + y_0^2 = z_0^k$. We construct a solution for $n = k + 2$. Let $x_1 = x_0 z_0$, $y_1 = y_0 z_0$, and $z_1 = z_0$. Substituting these into the sum of squares:

$$x_1^2 + y_1^2 = (x_0 z_0)^2 + (y_0 z_0)^2 = z_0^2 (x_0^2 + y_0^2).$$

Using the inductive hypothesis:

$$z_0^2 (z_0^k) = z_0^{k+2} = z_1^{k+2}.$$

Thus, the existence of a solution for k implies existence for $k + 2$. Since solutions exist for $n = 1, 2$, they exist for all positive integers n.

証明終

Solutions with Prime Constraints

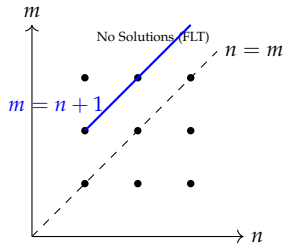
When exponents are variables or results are constrained to be prime, we rely on congruences and parity arguments.

Example 10.13. Variable Exponents with Prime Sum. Find all solutions in primes x, y, z to the equation $x^y + y^x = z$.

範例

Solution

Since z is prime, x and y cannot both be odd; otherwise $x^y + y^x$ is even and greater than 2. Thus one of x, y is even. Because x and y are primes, this forces $x = 2$ or $y = 2$. Without loss of generality, let $x = 2$ and y be an odd prime.



Solvability Space

Figure 10.3: The line $m = n$ represents Fermat's Last Theorem (no solutions). The adjacent diagonals $m = n \pm 1$ permit infinite families of solutions.

If $y = 2$, then $z = 2^2 + 2^2 = 8$ is not prime. If $y = 3$, then $z = 2^3 + 3^2 = 17$ is prime. Now assume $y \geq 5$ is an odd prime. Then

$$2^y + y^2 = (2^y + 1) + (y^2 - 1) = 3(2^{y-1} - 2^{y-2} + \cdots + 1) + (y-1)(y+1).$$

Since $y \neq 3$, the product $(y-1)(y+1)$ is divisible by 3, and so is the alternating sum. Hence $3 \mid (2^y + y^2)$, and z cannot be prime. Therefore $y = 3$ is the only possibility.
Thus the only prime solutions are $(x, y, z) = (2, 3, 17)$ and $(3, 2, 17)$.
■

Modular Constraints and Diophantine Systems

For equations involving fixed constants and powers, modulo arithmetic often restricts the possible exponents, reducing the problem to a finite set of cases.

Example 10.14. The Equation $x^2 + 615 = 2^y$. Find all positive integer solutions to $x^2 + 615 = 2^y$.

範例

Solution

We analyze the equation modulo 5. Powers of 2 modulo 5 follow the cycle: $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 3, 2^4 \equiv 1$. The term 615 is a multiple of 5, so $x^2 \equiv 2^y \pmod 5$. Quadratic residues modulo 5 are $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1$. Thus $x^2 \in \{0, 1, 4\} \pmod 5$. Comparing this with the cycle of 2^y:

- If $y \equiv 1 \pmod 4$, $2^y \equiv 2$ (Not a residue).
- If $y \equiv 3 \pmod 4$, $2^y \equiv 3$ (Not a residue).

Therefore, y must be even. Let $y = 2z$. The equation becomes $x^2 + 615 = (2^z)^2$, or:

$$2^{2z} - x^2 = 615 \implies (2^z - x)(2^z + x) = 615.$$

We factor $615 = 3 \times 5 \times 41$. We must find factors u, v such that $uv = 615$ and $v > u$. Then $2^z + x = v$ and $2^z - x = u$. Adding the equations yields $2^{z+1} = u + v$. Possible pairs (u, v):

1. $(1, 615) : u + v = 616$. $2^{z+1} = 616$. No integer solution ($512 < 616 < 1024$).
2. $(3, 205) : u + v = 208$. $2^{z+1} = 208$. No integer solution ($128 < 208 < 256$).
3. $(5, 123) : u + v = 128 = 2^7$. Thus $z + 1 = 7 \implies z = 6$. If $z = 6$, $2^6 - x = 5 \implies 64 - x = 5 \implies x = 59$. Check: $59^2 + 615 = 3481 + 615 = 4096 = 2^{12}$. This is a valid solution.

4. $(15, 41) : u + v = 56$. No integer solution ($32 < 56 < 64$).

The unique solution is $x = 59, y = 12$.

■

We conclude with two additional examples illustrating the application of these techniques to similar Diophantine problems.

Example 10.15. Constraint by Modulo 3. Prove that the equation $x^2 + 5 = 3^y$ has only one positive integer solution.

範例

Proof

We consider the equation modulo 3 and modulo 4. Modulo 3:

$$x^2 + 2 \equiv 0 \pmod 3 \implies x^2 \equiv 1 \pmod 3.$$

This is consistent for any x not divisible by 3. Modulo 4:

$$x^2 + 1 \equiv 3^y \equiv (-1)^y \pmod 4.$$

If y is odd, $x^2 + 1 \equiv -1 \equiv 3 \pmod 4$, which implies $x^2 \equiv 2 \pmod 4$. This is impossible for any integer square. Thus y must be even. Let $y = 2k$. Rearranging the equation:

$$5 = 3^{2k} - x^2 = (3^k - x)(3^k + x).$$

Since 5 is prime, the only factors are 1 and 5.

$$\begin{cases} 3^k - x = 1 \\ 3^k + x = 5 \end{cases}$$

Adding the equations: $2 \cdot 3^k = 6 \implies 3^k = 3 \implies k = 1$. Substituting back, $3^1 - x = 1 \implies x = 2$. Then $y = 2k = 2$. Verification: $2^2 + 5 = 4 + 5 = 9 = 3^2$. The unique solution is $(x, y) = (2, 2)$.

■

Example 10.16. Construction for $x^3 + y^3 = z^4$. Find a non-trivial integer solution to $x^3 + y^3 = z^4$ using the common factor method.

範例

Solution

We use the strategy from *theorem* 10.5 with exponents $n = 3, m = 4$. Let $x = c^u a$ and $y = c^u b$ (where we simplify the form $(ac)^u$ to just scaling by c^u). Substitute into $x^3 + y^3 = z^4$:

$$c^{3u}(a^3 + b^3) = z^4.$$

We choose a, b arbitrarily, say $a = 1, b = 1$. Then $a^3 + b^3 = 2$. The

equation becomes $2c^{3u} = z^4$. We need to choose c and u such that the left side is a perfect fourth power.
Let $c = 2$. The expression becomes $2 \cdot 2^{3u} = 2^{3u+1}$. We require $3u + 1$ to be a multiple of 4.
Let $3u + 1 = 4k$. For $k = 1$, $3u = 3 \implies u = 1$. Then $z^4 = 2^4 \implies z = 2$. And $x = 2^1(1) = 2$, $y = 2^1(1) = 2$. Check: $2^3 + 2^3 = 8 + 8 = 16 = 2^4$.
For distinct x, y, choose $a = 1, b = 2$. Then $a^3 + b^3 = 1 + 8 = 9$. Equation: $9c^{3u} = z^4$.
Let $c = 3$. Then $3^2 \cdot 3^{3u} = 3^{3u+2} = z^4$. We need $3u + 2$ divisible by 4.
Let $u = 2$. Then $3(2) + 2 = 8$. $z^4 = 3^8 \implies z = 3^2 = 9$. $x = 3^2(1) = 9$, $y = 3^2(2) = 18$. Check: $9^3 + 18^3 = 729 + 5832 = 6561$. $z^4 = 9^4 = 6561$. Solution: $(9, 18, 9)$.

■

10.4 *Exercises*

1. **Small Primitive Triples.** Find all primitive Pythagorean triples (x, y, z) satisfying $z < 30$.

2. **Odd-Odd Parameterisation.** Prove that all positive integer solutions to $x^2 + y^2 = z^2$ with $(x, y) = 1$ and x odd can be expressed as:
$$x = uv, \quad y = \frac{u^2 - v^2}{2}, \quad z = \frac{u^2 + v^2}{2},$$
where u, v are coprime odd positive integers with $u > v$.

3. **Weighted Quadratic Form 1.** Prove that all positive integer solutions to $x^2 + 2y^2 = z^2$ with $(x, y) = 1$ are given by:
$$x = |a^2 - 2b^2|, \quad y = 2ab, \quad z = a^2 + 2b^2,$$
where $a, b > 0$, $(a, b) = 1$, and a is odd.

4. **Weighted Quadratic Form 2.** Prove that all positive integer solutions to $x^2 + y^2 = 2z^2$ with $(x, y) = 1$ and $x > y$ are given by:
$$x = m^2 - n^2 + 2mn, \quad y = |m^2 - n^2 - 2mn|, \quad z = m^2 + n^2,$$
where $m > n > 0$, $(m, n) = 1$, and m, n have opposite parity.

5. **Quartic-Quadratic Equation.** Find all positive integer solutions to $x^4 + y^2 = z^2$ where x, y, z are pairwise coprime.

6. **Generalised Pell-Type Forms.** Let m be square-free.
   (a) If $m \equiv 1$ or $3 \pmod 4$ ($m = 2k - 1$), prove that solutions to $x^2 + my^2 = z^2$ take two forms involving parameters $m_1 m_2 = m$.

(b) If $m \equiv 2 \pmod 4$ ($m = 4k-2$), prove that solutions take the form $x = |m_1a^2 - 2m_2b^2|, y = 2ab, z = m_1a^2 + 2m_2b^2$ where $m = 2m_1m_2$.

7. **Counting Special Triples.** Let $p_1 < p_2 < \cdots < p_s$ be odd primes. Prove that the number of primitive Pythagorean triples (x, y, z) satisfying
$$2p_1p_2 \dots p_s(x + y + z) = xy$$
is exactly $4 \cdot 3^s$.

8. **Sum of Inverse Squares.** Prove that all positive integer solutions to $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$ with $(x, y, z) = 1$ and y even are given by:
$$x = r^4 - s^4, \quad y = 2rs(r^2 + s^2), \quad z = 2rs(r^2 - s^2),$$
where $r > s > 0$, $(r, s) = 1$, and r, s have opposite parity.

9. **Congruent Numbers.** A positive integer n is a congruent number if it is the area of a right triangle with rational sides. Prove:
   (a) n is congruent if and only if there exists a rational x such that $x, x + n, x - n$ are all squares of rationals.
   (b) n is congruent if and only if the system $a^2 + nb^2 = c^2$ and $a^2 - nb^2 = d^2$ has an integer solution (a, b, c, d) with $b \neq 0$.

10. **Infinite Descent Proofs.** Use infinite descent to prove that the following equations have no positive integer solutions:
    (a) $x^2 + y^2 + z^2 = 2xyz$.
    (b) $x^4 + 27y^4 = z^2$ with $(x, y) = 1$.

11. **Sum of Squares Product.** Find all integer solutions to $x^2 + y^2 + z^2 = x^2y^2$.

12. **Negative Pell Equation.** Find all positive integer solutions to $x^4 - 2y^2 = -1$.

13. **Higher Power Non-Existence.** Prove that $x^4 + 4y^4 = z^2$ has no positive integer solutions. Deduce that $x^4 + y^2 = z^4$ has no positive integer solutions.

14. **Fermat's Triangle Problem.** Find a right-angled triangle with integer legs x, y and hypotenuse z such that $x + y$ and z are both perfect squares.

This is a problem posed by Fermat in a letter to Mersenne in 1643.

15. **General Solutions for Shifted Powers.** Let $n > 1$ be an integer. Construct a parametric family of positive integer solutions to the equation:
$$x^n + y^n = z^{n-1}.$$

16. **Parity Conditions on Exponents.** Consider the equation $x^2 + 3y^2 = 2^n$. Prove that:

(a) If n is even, there exist positive integer solutions.

(b) If n is odd, there are no positive integer solutions.

17. Consecutive Product and Squares. Prove that the product of five consecutive integers is never a perfect square. That is, the equation

$$(x-2)(x-1)x(x+1)(x+2) = y^2$$

has no integer solutions.

18. Polynomial Diophantine Equation. Find all integer solutions to:

$$x^4 + x^3 + x^2 + x + 1 = y^2.$$

Bound the polynomial between squares of quadratic expressions.

19. Prime Variables. Find all solutions to $x^y + 1 = z$ where x, y, z are all prime numbers.

20. Infinite Families for Mixed Powers. Prove that the equation $x^2 + y^5 = z^3$ possesses infinitely many solutions in positive integers.

21. Fermat-Type Non-Existence. Let $n \geq 2$. Prove that the equation $x^{2n} + y^{2n} = z^2$ has no positive integer solutions.

Reduce this to the case $X^4 + Y^4 = Z^2$.

22. Unique Solution for Specific Primes. Let p be a prime such that $p \equiv 3 \pmod 4$. Prove that the only positive integer solution (x, y, z) to the equation

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

is $x = y = z = 2$.

11
Methods for Indefinite Equations

We now broaden our scope to general indeterminate equations. Unlike linear or Pythagorean equations, which possess systematic algorithms for their complete solution, general Diophantine equations often require a diverse toolbox of heuristic methods.
In this chapter, we systematise these approaches into four primary categories: algebraic factorisation, modular constraints, analytic estimation, and constructive techniques.

11.1 The Factorisation Method

A fundamental strategy in solving non-linear Diophantine equations is to convert a sum of terms into a product. If an equation can be manipulated into the form

$$f(x_1, \dots, x_n) = K,$$

where K is a constant or a simple term, the Fundamental Theorem of Arithmetic allows us to equate factors of f with divisors of K.
We begin with a classical application to reciprocal equations, often arising in geometric contexts.

Example 11.1. The Symmetric Reciprocal Equation. Find all positive integer solutions to the equation

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n},$$

where n is a fixed positive integer.
Multiplying through by nxy, we obtain the algebraic form $ny + nx = xy$. Rearranging terms to group variables:

$$xy - nx - ny = 0.$$

To factorise the left-hand side, we add n^2 to both sides, completing the rectangle:

$$xy - nx - ny + n^2 = n^2 \implies (x - n)(y - n) = n^2.$$

Since $x, y > 0$, we must have $\frac{1}{x} < \frac{1}{n}$ and $\frac{1}{y} < \frac{1}{n}$, which implies $x > n$ and $y > n$. Thus $x - n$ and $y - n$ are positive integers. The solutions correspond to the divisor pairs of n^2. For each divisor $d \mid n^2$, we obtain a solution:

$$\begin{cases} x - n = d \\ y - n = n^2/d \end{cases} \implies \begin{cases} x = n + d \\ y = n + n^2/d \end{cases}$$

The number of solutions is exactly $\tau(n^2)$, the number of divisors of n^2.

範例

This technique extends to higher-degree equations where factorization over the integers restricts the possible values of variables.

Example 11.2. Quartic-Quadratic constraints. Prove that the equation $x^4 - 2y^2 = 1$ has only the integer solutions $(x, y) = (\pm 1, 0)$. Rearranging the equation implies $x^4 - 1 = 2y^2$. We factor the difference of squares:

$$(x^2 - 1)(x^2 + 1) = 2y^2.$$

Since x must be odd (if x were even, $x^4 - 1$ would be odd, but $2y^2$ is even), let $x = 2k + 1$. The greatest common divisor of the two factors is:

$$(x^2 - 1, x^2 + 1) = (x^2 - 1, 2) = 2.$$

We can rewrite the equation as:

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

Note that y must be even. Let $y = 2Y$. The equation becomes:

$$\frac{x^2 - 1}{2} \cdot \frac{x^2 + 1}{2} = 2Y^2.$$

The two factors on the left are coprime integers. Their product is twice a square. Thus, one factor is a square and the other is twice a square. Since $\frac{x^2+1}{2} = \frac{(2k+1)^2+1}{2} = 2k^2 + 2k + 1$ is odd, it must be the square term.

$$\begin{cases} \frac{x^2+1}{2} = u^2 \\ \frac{x^2-1}{2} = 2v^2 \end{cases}$$

From the second equation, $x^2 - 1 = 4v^2$, or $x^2 - (2v)^2 = 1$. The only consecutive perfect squares are 0 and 1, so we must have $2v = 0 \implies v = 0$. Consequently, $x^2 = 1 \implies x = \pm 1$. Substituting back, $y = 0$. The solutions are $(1, 0)$ and $(-1, 0)$.

範例

Pythagorean Quadruples

We can generalize the parameterisation of Pythagorean triples (*Classification of Primitive Triples*) to sums of three squares using factorisation in the Gaussian integers or simple algebraic manipulation.

Theorem 11.1. ***Parametrisation of Pythagorean Quadruples.*** The primitive integer solutions to $x^2 + y^2 + z^2 = w^2$ are generated by the formulae:

$$\begin{aligned} x &= 2ac/d, \\ y &= 2bc/d, \\ z &= (c^2 - a^2 - b^2)/d, \\ w &= (c^2 + a^2 + b^2)/d, \end{aligned}$$

where a, b, c are integers and d is a scaling factor chosen to ensure coprimality.

定理

Proof

Let $x = tA$ and $y = tB$. Then

$$t^2(A^2 + B^2) = w^2 - z^2 = (w - z)(w + z).$$

Choose a rational parameter $\lambda = \frac{c}{u}$ with $(c, u) = 1$ and set

$$w + z = \lambda t, \quad w - z = \frac{t}{\lambda}(A^2 + B^2).$$

Then

$$u(w + z) = ct, \quad c(w - z) = ut(A^2 + B^2).$$

Since $(c, u) = 1$, we have $u \mid t$; write $t = ut_1$. Substituting gives

$$w + z = ct_1, \quad c(w - z) = t_1\big((uA)^2 + (uB)^2\big).$$

Let $a = uA$ and $b = uB$. Solving for w and z yields

$$2cw = t_1(c^2 + a^2 + b^2), \quad 2cz = t_1(c^2 - a^2 - b^2),$$

and $x = t_1 a$, $y = t_1 b$. Clearing the common factor $2ct_1$ gives

$$x : y : z : w = 2ac : 2bc : (c^2 - a^2 - b^2) : (c^2 + a^2 + b^2).$$

Choosing d to clear common factors yields the stated parametrisation.

■

Sometimes, factorisation requires assumption of coprimality to isolate powers.

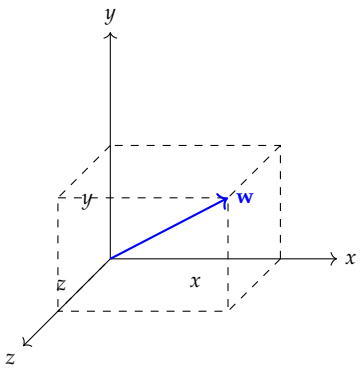


Figure 11.1: The Pythagorean Quadruple represents the integer diagonal of an integer cuboid.

Example 11.3. Coprimality and Powers. Prove that the equation $x(x+1)^n = y^{n+1}$ has only the integer solutions $(0,0)$ and $(-1,0)$ for any integer $n \geq 1$.
When $x = 0$ or $x = -1$, we have $y = 0$, so $(0,0)$ and $(-1,0)$ are solutions. Now assume $x \neq 0, -1$, so $y \neq 0$. Since $(x, x+1) = 1$, we can write

$$x = a^{n+1}, \quad (x+1)^n = b^{n+1}, \quad y = ab,$$

with integers a, b and $(a,b) = 1$. Because $(n, n+1) = 1$, the second equation implies $b = c^n$ for some integer c, hence

$$x + 1 = c^{n+1}.$$

Substituting gives

$$a^{n+1} + 1 = c^{n+1}.$$

If $a > 0$, then $c > a$ and

$$1 = c^{n+1} - a^{n+1} = (c-a)(c^n + c^{n-1}a + \cdots + a^n) \geq n+1,$$

which is impossible. If $a < 0$ and $n+1$ is even, the left-hand side is positive while the right-hand side is nonpositive. If $a < 0$ and $n+1$ is odd, then $a < -1$ and $c < 0$, and taking absolute values gives

$$|c|^{n+1} + 1 = |a|^{n+1},$$

which contradicts the previous argument. Therefore no solutions occur when $x \neq 0, -1$, and the only solutions are $(0,0)$ and $(-1,0)$.

範例

11.2 *Modular Constraints and Valuation*

When algebraic manipulation fails, examining the equation modulo n or analyzing the powers of prime factors (valuation) can reveal contradictions.

Congruence Obstructions

Example 11.4. Factorial Sums. Find all positive integer solutions to $\sum_{s=1}^{n}(s!)^m = \sum_{t=1}^{m}(t!)^n$.
It is clear that $n = m$ is a solution. Suppose $m < n$. Then

$$2^n - 2^m = 2^m(2^{n-m} - 1) = \sum_{s=3}^{n}(s!)^m - \sum_{t=3}^{m}(t!)^n.$$

The right-hand side is divisible by 3, so $3 \mid (2^{n-m} - 1)$, and hence

$n-m$ is even. Thus $n \geq m+2$. Now

$$\sum_{t=2}^{m}(t!)^n = 2^n + 6^n + \sum_{t=4}^{m}(t!)^n = 2^n(1+3^n) + \sum_{t=4}^{m}(t!)^n.$$

Since $n \geq m+2$, each term $(t!)^n$ with $t \geq 4$ is divisible by 2^{m+3}, and $2^n(1+3^n)$ is also divisible by 2^{m+3}. Hence

$$\sum_{t=2}^{m}(t!)^n \equiv 0 \pmod{2^{m+3}}.$$

If the original equation holds, then

$$\sum_{s=1}^{n}(s!)^m \equiv 0 \pmod{2^{m+3}}.$$

But modulo 8 we have

$$\sum_{s=1}^{n}(s!)^m \equiv 1 + 2^m + 6^m \equiv 1 \pmod{8},$$

contradiction. Thus there are no solutions with $m < n$. Similarly, there are no solutions with $m > n$, and therefore the only solutions are $m = n$.

範例

Example 11.5. Sum of Factorials as a Power. Find all positive integer solutions to $1! + 2! + \cdots + x! = y^z$ for $z \geq 2$.
For $x = 1$, $S_x = 1$, so $y = 1$ and any $z \geq 2$ works. For $x = 2$, $S_x = 3$ is not a perfect power. For $x = 3$, $S_x = 9 = 3^2$ gives $(x, y, z) = (3, 3, 2)$.
Now assume $x \geq 4$. Since 4! is divisible by 8, we have

$$S_x \equiv 1 + 2 + 6 \equiv 1 \pmod{8},$$

so y is odd. If $x \geq 5$, then $S_x \equiv 33 \equiv 3 \pmod{5}$, so z must be odd. For $x \geq 8$, note that $8! \equiv 9 \pmod{27}$ and $k! \equiv 0 \pmod{27}$ for $k \geq 9$, while $S_7 = 5913 \equiv 0 \pmod{27}$. Hence

$$S_x \equiv 9 \pmod{27},$$

so $v_3(S_x) = 2$. If $z \geq 3$, then y^z is divisible by 27, contradiction. Thus $z = 2$, but this contradicts $S_x \equiv 3 \pmod{5}$. Hence there are no solutions for $x \geq 8$.
For $x = 4, 5, 6, 7$, direct checks give

$$S_4 = 33, \quad S_5 = 153, \quad S_6 = 873, \quad S_7 = 5913.$$

For $x = 4$, $5^2 < 33 < 6^2$ and $3^3 < 33 < 4^3$, so S_4 is not a perfect power. For $x = 5$, $12^2 < 153 < 13^2$, $5^3 < 153 < 6^3$, and $3^4 < 153 <$

4^4. For $x = 6$, $29^2 < 873 < 30^2$, $9^3 < 873 < 10^3$, and $5^4 < 873 < 6^4$. For $x = 7$, $76^2 < 5913 < 77^2$, $18^3 < 5913 < 19^3$, and $8^4 < 5913 < 9^4$. Thus none of these is a perfect power with exponent ≥ 2. Therefore the only solutions are

$$(x, y, z) = (1, 1, z) \text{ for } z \geq 2, \quad \text{and} \quad (3, 3, 2).$$

範例

Comparing Powers of Primes

A powerful variation of the modular method is to compare the exponent of the highest power of a prime p dividing both sides of an equation. We denote the exponent of p in the prime factorisation of n as $v_p(n)$.

Theorem 11.2. ***The Quotient of Fermat Differences.***
Let p be an odd prime and $k > 1$ be an integer. The equation

$$\frac{x^p - y^p}{x - y} = p^k z, \quad \text{with } (x, y) = 1$$

has no integer solutions.

定理

Proof

Assume a solution exists. From $x^p - y^p = p^k z(x - y)$, we see that $x^p \equiv y^p \pmod{p}$. By Fermat's Little Theorem, $x \equiv y \pmod{p}$. Let $x = y + mp$. Since $(x, y) = 1$, $p \nmid y$. We expand the numerator using the Binomial Theorem:

$$x^p - y^p = (y + mp)^p - y^p = \sum_{i=1}^{p} \binom{p}{i} y^{p-i} (mp)^i.$$

The first term of the sum (for $i = 1$) is $\binom{p}{1} y^{p-1}(mp) = p \cdot y^{p-1} \cdot mp = mp^2 y^{p-1}$. The second term (for $i = 2$) is $\binom{p}{2} y^{p-2}(mp)^2 = \frac{p(p-1)}{2} y^{p-2} m^2 p^2$, which is divisible by p^3 (since p is odd). Higher order terms are divisible by p^3 or higher. Thus, the sum is dominated by the first term modulo p^3:

$$x^p - y^p \equiv mp^2 y^{p-1} \pmod{p^3}.$$

Dividing by $x - y = mp$:

$$\frac{x^p - y^p}{x - y} \equiv \frac{mp^2 y^{p-1}}{mp} \equiv py^{p-1} \pmod{p^2}.$$

The valuation of the LHS is therefore exactly $v_p(\text{LHS}) = 1$. However, the RHS is $p^k z$ with $k > 1$, so its valuation is at least 2. This contradiction implies no solution exists.

■

11.3 *Analytic Methods: Estimation and Cases*

When discrete methods yield ambiguous results, analytic constraints—such as inequalities and magnitude estimates—can narrow the search space to a finite set of cases.

Classification Discussion

Example 11.6. Cyclic Exponential Equation. Find all integer solutions to $x^y + y^z + z^x = 0$.
Let (x, y, z) be a solution. Clearly $xyz \neq 0$ and at least one of x, y, z is negative. Since the equation is cyclic in x, y, z, we discuss the following cases.

1. **Case** $x > 0$, $y > 0$, $z < 0$**.** The equation becomes

$$x^y + z^x = -\frac{1}{y^{-z}}.$$

This holds if and only if $y = 1$. Then $x + z^x = -1$, which yields $x = 1$ and $z = -2$. Hence $(x, y, z) = (1, 1, -2)$. Permuting x, y, z gives the three solutions

$$(-2, 1, 1),\ (1, -2, 1),\ (1, 1, -2).$$

2. **Case** $x > 0$, $y < 0$, $z < 0$**.** Then

$$\frac{1}{x^{-y}} + \frac{1}{y^{-z}} = -z^x.$$

This holds only if $|z^x| \leq 2$. Hence $z = -2$, $x = 1$ or $z = -1$. When $z = -2$ and $x = 1$, we have $y = -1$, so $(x, y, z) = (1, -2, -1)$, and permuting x, y, z gives

$$(1, -1, -2),\ (-1, -2, 1),\ (-2, 1, -1).$$

When $z = -1$, the equation becomes

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

If $y = -2k$ with $k > 0$, then

$$x^{2k} = \frac{2k}{1 + (-1)^{x+1} \cdot 2k},$$

which is impossible. If $y = -(2k - 1)$ with $k > 0$, then

$$x^{2k-1} = \frac{2k - 1}{1 + (-1)^{x+1} \cdot (2k - 1)},$$

which is also impossible.

3. **Case** $x < 0$, $y < 0$, $z < 0$. Then

$$\frac{1}{x^{-y}} + \frac{1}{y^{-z}} + \frac{1}{z^{-x}} = 0.$$

If x, y, z are all odd, the left side is negative; if all even, the left side is positive, both contradictions. If exactly one of x, y, z is even, say x even and y, z odd, then

$$y^{-z}z^{-x} + z^{-x}x^{-y} + x^{-y}y^{-z} = 0,$$

whose left-hand side is odd while the right-hand side is even, a contradiction. Hence exactly two of x, y, z are even. Without loss of generality, let $2 \mid x$, $2 \mid y$, and $2 \nmid z$. Write

$$x = 2^s a, \quad y = 2^t b, \quad M = z^{-x},$$

where $s, t \geq 1$, a, b are negative integers, and $2 \nmid abM$. Substituting gives

$$(2^t b)^{-z}\left(M + (2^s a)^{-2^t b}\right) = -M(2^s a)^{-2^t b}.$$

Comparing the powers of 2 on both sides yields $tz = 2^t sb$, which is impossible since $2 \nmid z$.

Therefore the equation has exactly six solutions:

$$(-2,1,1),\ (1,-2,1),\ (1,1,-2),\ (1,-1,-2),\ (-1,-2,1),\ (-2,1,-1).$$

範例

Estimation

Inequalities are particularly effective for sums of reciprocals, as the value of the function drops rapidly.

Example 11.7. Factorial Reciprocals. Find positive integers satisfying $\frac{4}{w!} = \frac{1}{x!} + \frac{1}{y!} + \frac{1}{z!}$.

Since the equation is unchanged by permuting x, y, z, assume $x \leq y \leq z$. Then

$$\frac{4}{w!} = \frac{1}{x!} + \frac{1}{y!} + \frac{1}{z!} \leq \frac{3}{x!},$$

so $w > x$. If $w \geq x + 2$, then

$$\frac{4}{(x+2)!} - \frac{1}{x!} \geq \frac{4}{w!} - \frac{1}{x!} = \frac{1}{y!} + \frac{1}{z!} > 0,$$

which implies

$$4 > \frac{(x+2)!}{x!} = (x+2)(x+1) \geq 6,$$

a contradiction. Hence $w = x + 1$.
Since $x \le y \le z$, we have

$$\frac{4}{(x+1)!} \ge \frac{3}{z!},$$

so $z \le x + 1$. Thus $z = x$ or $z = x + 1$.
If $z = x$, then $\frac{4}{(x+1)!} = \frac{3}{x!}$, giving $x = \frac{1}{3}$, impossible. If $z = x + 1$, the equation becomes

$$\frac{4}{(x+1)!} = \frac{2}{x!} + \frac{1}{(x+1)!} \quad \text{or} \quad \frac{4}{(x+1)!} = \frac{1}{x!} + \frac{2}{(x+1)!}.$$

The first gives $x = \frac{1}{2}$, impossible, while the second gives $x = 1$.
Hence

$$(x, y, z, w) = (1, 2, 2, 2),$$

and by permuting x, y, z the solutions are

$$(1, 2, 2, 2),\ (2, 1, 2, 2),\ (2, 2, 1, 2).$$

範例

11.4 Constructive Methods

When an equation has infinitely many solutions, we can often construct them by identifying a pattern or an identity.

Construction via Identities

Example 11.8. Sums of Fourth Powers. Prove that $x^4 + y^4 + z^4 = w^2$ has infinitely many integer solutions.
Let $w = z^2 + m$. Then

$$w^2 - z^4 = m^2 + 2z^2 m.$$

Since

$$(u + v)^4 + (u - v)^4 = 2(u^2 - v^2)^2 + 16u^2v^2,$$

we obtain

$$16u^2v^2\big((u + v)^4 + (u - v)^4\big) = 2(u^2 - v^2)^2(16u^2v^2) + (16u^2v^2)^2.$$

Comparing with $m^2 + 2z^2 m$, take

$$m = 16u^2v^2, \quad z = u^2 - v^2.$$

Then

$$w^2 - (u^2 - v^2)^4 = 16u^2v^2\big((u + v)^4 + (u - v)^4\big).$$

Let $u = s^2$ and $v = t^2$. This gives

$$((s^4 - t^4)^2 + 16s^4t^4)^2 - (s^4 - t^4)^4 = (2st(s^2 + t^2))^4 + (2st(s^2 - t^2))^4.$$

Hence the equation has infinitely many solutions:

$$x = 2st(s^2 + t^2), \quad y = 2st(s^2 - t^2), \quad z = s^4 - t^4, \quad w = (s^4 - t^4)^2 + 16s^4t^4.$$

範例

Rational Parametrisation

Just as the unit circle $x^2 + y^2 = 1$ can be parametrised by rational points to solve $a^2 + b^2 = c^2$, higher degree surfaces can sometimes be projected to finding rational points.

Example 11.9. Weighted Fourth Powers. Find infinitely many integer solutions to $x^4 + y^4 + 4z^4 = w^4$.
Divide by w^4 to work with rational numbers X, Y, Z:

$$X^4 + Y^4 + 4Z^4 = 1.$$

We set $X^2 + 2YZ = 1$. This reduces the degree of freedom. Substituting $X^2 = 1 - 2YZ$ into the equation:

$$(1 - 2YZ)^2 + Y^4 + 4Z^4 = 1.$$

$$1 - 4YZ + 4Y^2Z^2 + Y^4 + 4Z^4 = 1.$$

$$Y^4 + 4Y^2Z^2 - 4YZ + 4Z^4 = 0.$$

Note that $Y^4 + 4Z^4 + 4Y^2Z^2 = (Y^2 + 2Z^2)^2$. So $(Y^2 + 2Z^2)^2 = 4YZ$. This relates the square of a quadratic to a linear term. Let $Y = t^2Z$. Then $(t^4Z^2 + 2Z^2)^2 = 4t^2Z^2$.

$$Z^4(t^4 + 2)^2 = 4t^2Z^2.$$

Assuming $Z \neq 0$, we divide by Z^2 to get

$$Z(t^4 + 2) = 2t,$$

so

$$Z = \frac{2t}{t^4 + 2}, \quad Y = \frac{2t^3}{t^4 + 2}.$$

Moreover,

$$(Y^2 - 2Z^2)^2 = 4YZ(1 - 2YZ) = 4t^2Z^2X^2,$$

so

$$X = \frac{Y^2 - 2Z^2}{2tZ} = \frac{t^4 - 2}{t^4 + 2}.$$

Let $t = a/b$ with integers a, b and $b \neq 0$. Clearing denominators gives

$$x = a^4 - 2b^4, \quad y = 2a^3b, \quad z = 2ab^3, \quad w = a^4 + 2b^4.$$

範例

Exponential Constructions

We now consider equations where the exponents themselves are part of the variable structure.

Example 11.10. Self-Exponent Product. Prove that

$$\prod_{i=1}^{k} x_i^{x_i} = z^z \quad (k \geq 2,\ x_i > 1)$$

has infinitely many sets of positive integer solutions:

$$\begin{aligned}
x_1 &= k^{n(k^{n+1}-2n-k)+2n}(k^n-1)^{2(k^n-1)},\\
x_2 &= k^{n(k^{n+1}-2n-k)}(k^n-1)^{2(k^n-1)+2},\\
x_3 &= \cdots = x_k = k^{n(k^{n+1}-2n-k)+n}(k^n-1)^{2(k^n-1)+1},\\
z &= k^{n(k^{n+1}-2n-k)+n+1}(k^n-1)^{2(k^n-1)+1},
\end{aligned}$$

where $k = 2$, $n > 1$ or $k \geq 3$, $n > 0$.
Let $d = (x_1, \ldots, x_k, z)$ and write

$$x_i = dt_i \ (i = 1, \ldots, k), \quad z = du.$$

Substituting gives

$$d^{\sum_{i=1}^{k} t_i - u} \prod_{i=1}^{k} t_i^{t_i} = u^u.$$

If $\sum_{i=1}^{k} t_i - u = 1$ and $\prod_{i=1}^{k} t_i^{t_i} \mid u^u$, then

$$d = \frac{u^u}{\prod_{i=1}^{k} t_i^{t_i}}$$

produces a solution. Take

$$t_1 = k^{2n}, \quad t_2 = (k^n-1)^2, \quad t_3 = \cdots = t_k = (k^n-1)k^n, \quad u = k^{n+1}(k^n-1).$$

Then

$$\sum_{i=1}^{k} t_i - u = k^{2n} + (k^n-1)^2 + (k-2)(k^n-1)k^n - k^{n+1}(k^n-1) = 1.$$

Moreover,

$$\frac{u^u}{\prod_{i=1}^{k} t_i^{t_i}} = k^h(k^n-1)^l,$$

where

$$h = k^n(k^{n+1} - k - 2n), \quad l = 2(k^n - 1).$$

For $k = 2$, $n > 1$ or $k \geq 3$, $n > 0$, we have $h > 0$ and $l > 0$, so

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

Substituting gives the stated family of solutions.

範例

11.5 *Generating Functions and Counting Solutions*

While the methods discussed earlier focus on the existence or construction of specific solutions, a frequent question in number theory concerns the *quantity* of solutions. For linear indeterminate equations, this counting problem connects number theory with combinatorics. The most powerful tool for this analysis is the method of generating functions.

Formal Power Series

To count solutions systematically, we map sequences of numbers to analytic objects.

Definition 11.1. ***Generating Function.***
The generating function of a finite sequence $a_0, a_1, \ldots, a_n$ is the polynomial

$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

For an infinite sequence $a_0, a_1, \ldots$, the generating function is the formal power series

$$A(x) = \sum_{n=0}^{\infty} a_n x^n.$$

定義

We use the term "formal" because we are not initially concerned with the convergence of the series for specific values of x. Instead, we treat the series as an algebraic object where the position of a coefficient (the exponent of x) serves as a label.

Definition 11.2. ***Operations on Formal Power Series.***
Let $A(x) = \sum a_n x^n$ and $B(x) = \sum b_n x^n$. We define:

1. **Equality**: $A(x) = B(x)$ if and only if $a_n = b_n$ for all $n \geq 0$.
2. **Sum**: $A(x) + B(x) = \sum_{n=0}^{\infty}(a_n + b_n)x^n$.
3. **Product**: $A(x)B(x) = \sum_{n=0}^{\infty} c_n x^n$, where c_n is the Cauchy product

$c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

定義

The fundamental identity for our purposes is the expansion of the geometric series and its powers.

Theorem 11.3. ***Geometric Series Expansion.***
In the ring of formal power series:

$$\frac{1}{1-x} = \sum_{r=0}^{\infty} x^r.$$

定理

Proof

Let $\frac{1}{1-x} = \sum_{n=0}^{\infty} c_n x^n$. By definition of the quotient, we have:

$$1 = (1-x)\sum_{n=0}^{\infty} c_n x^n = \sum_{n=0}^{\infty} c_n x^n - \sum_{n=0}^{\infty} c_n x^{n+1}.$$

Shift the index of the second sum ($k = n+1$):

$$1 = c_0 + \sum_{n=1}^{\infty} (c_n - c_{n-1}) x^n.$$

Comparing coefficients, $c_0 = 1$ and $c_n - c_{n-1} = 0$ for $n \geq 1$. Thus $c_n = 1$ for all n.

■

Using mathematical induction, we can generalize this to negative integer powers.

Theorem 11.4. ***Negative Binomial Expansion.***
For any positive integer n,

$$\frac{1}{(1-x)^n} = \sum_{r=0}^{\infty} \binom{n+r-1}{n-1} x^r.$$

定理

Proof

For $n = 1$, the coefficient is $\binom{r}{0} = 1$, which matches the geometric series. Assume the formula holds for $n = k$. Then for $n = k+1$:

$$\frac{1}{(1-x)^{k+1}} = \frac{1}{(1-x)^k} \cdot \frac{1}{1-x} = \left(\sum_{j=0}^{\infty} \binom{k+j-1}{k-1} x^j\right)\left(\sum_{m=0}^{\infty} x^m\right).$$

The coefficient of x^r in the product is the sum of coefficients $a_j b_{r-j}$:

$$c_r = \sum_{j=0}^{r} \binom{k+j-1}{k-1} \cdot 1.$$

We apply the combinatorial identity $\sum_{i=r}^{n} \binom{i}{r} = \binom{n+1}{r+1}$ (often called the Hockey-stick identity).

$$\sum_{j=0}^{r} \binom{k+j-1}{k-1} = \binom{k-1}{k-1} + \binom{k}{k-1} + \cdots + \binom{k+r-1}{k-1} = \binom{k+r}{k}.$$

Thus, the coefficient is $\binom{(k+1)+r-1}{(k+1)-1}$, satisfying the inductive step.

■

Linear Equations with Unit Coefficients

We now apply this machinery to the counting of integer solutions.

Theorem 11.5. ***Solutions to*** $x_1 + \cdots + x_n = r$**.**
The number of non-negative integer solutions to the linear indeterminate equation

$$x_1 + x_2 + \cdots + x_n = r$$

is given by $\binom{n+r-1}{n-1}$.

定理

Proof

Let a_r be the number of solutions. Consider the product of n geometric series:

$$P(x) = \left(\sum_{k=0}^{\infty} x^k \right)^n = (1 + x + x^2 + \dots) \dots (1 + x + x^2 + \dots).$$

A term x^r in this expansion is formed by choosing x^{m_1} from the first factor, x^{m_2} from the second, ..., and x^{m_n} from the n-th, such that $\sum m_i = r$. Thus, the coefficient of x^r in $P(x)$ is exactly the number of solutions to $m_1 + \cdots + m_n = r$ in non-negative integers. Since $P(x) = \frac{1}{(1-x)^n}$, by *theorem* 11.4, the coefficient is $\binom{n+r-1}{n-1}$.

■

Corollary 11.1. The number of **positive** integer solutions to $x_1 + \cdots + x_n = r$ is $\binom{r-1}{n-1}$ (provided $r \geq n$).

推論

Proof

Let $x_i = y_i + 1$ where $y_i \geq 0$. The equation becomes:

$$(y_1 + 1) + \cdots + (y_n + 1) = r \implies y_1 + \cdots + y_n = r - n.$$

By *theorem* 11.5, the number of non-negative solutions for y_i is:

$$\binom{n + (r-n) - 1}{n-1} = \binom{r-1}{n-1}.$$

■

Stars and Partitions

Figure 11.2: Combinatorial representation of a solution to $x_1 + x_2 + x_3 = 5$. The arrangement corresponds to $(2, 1, 2)$. The number of arrangements is $\binom{5+3-1}{3-1}$.

This result can also be visualised combinatorially. To partition r identical items into n distinct bins, we arrange r items and $n-1$ dividers (partitions) in a line. The total number of positions is $r+n-1$, and we choose $n-1$ positions for the dividers.

Example 11.11. Constraints and Transformations. Find the number of integer solutions to $x+y+z=24$ subject to:

1. $x, y, z > 1$.
2. $x > 1, y > 2, z > 3$.

1. Let $x = X+2, y = Y+2, z = Z+2$ where $X, Y, Z \geq 0$. The equation becomes $X+Y+Z = 24-6 = 18$. The number of solutions is $\binom{3+18-1}{3-1} = \binom{20}{2} = 190$.
2. Let $x = X+2, y = Y+3, z = Z+4$ where $X, Y, Z \geq 0$. The equation becomes $X+Y+Z = 24-(2+3+4) = 15$. The number of solutions is $\binom{3+15-1}{2} = \binom{17}{2} = 136$.

範例

General Linear Equations

Consider the equation with coefficients $s_i \in \mathbb{Z}^+$:

$$s_1x_1 + s_2x_2 + \cdots + s_nx_n = r.$$

Following the logic of *theorem* 11.5, a term x^{s_i} contributes to the sum m_i times, resulting in a term $(x^{s_i})^{m_i}$. The generating function for the number of solutions b_r is:

$$B(x) = \frac{1}{(1-x^{s_1})(1-x^{s_2})\dots(1-x^{s_n})}.$$

This formulation allows us to solve problems with complex upper bound constraints by manipulating polynomials.

Example 11.12. Solutions with Upper Bounds. Find the number of positive integer solutions to $x_1 + x_2 + x_3 + x_4 = 23$ subject to the constraints:

$$x_1 \leq 9, \quad x_2 \leq 8, \quad x_3 \leq 7, \quad x_4 \leq 6.$$

Since we require positive integers ($x_i \geq 1$), the generating function for each variable x_i with upper bound U_i is the polynomial:

$$P_i(x) = x + x^2 + \cdots + x^{U_i} = x\frac{1-x^{U_i}}{1-x}.$$

The generating function for the system is the product $\prod_{i=1}^{4} P_i(x)$:

$$G(x) = x^4\frac{(1-x^9)(1-x^8)(1-x^7)(1-x^6)}{(1-x)^4}.$$

We seek the coefficient of x^{23}. Let $f(x) = x^4(1-x^9)(1-x^8)(1-x^7)(1-x^6)\sum_{k=0}^{\infty}\binom{k+3}{3}x^k$. Factoring out x^4, we look for the coefficient of x^{19} in the expansion of

$$H(x) = (1-x^9)(1-x^8)(1-x^7)(1-x^6)(1-x)^{-4}.$$

Expanding the numerator (keeping terms with degree ≤ 19):

$$Num(x) = 1 - (x^6 + x^7 + x^8 + x^9) + (x^{13} + x^{14} + 2x^{15} + x^{16} + x^{17}) - \dots$$

The coefficient of x^{19} in $H(x)$ is formed by pairing terms x^j from the numerator with x^{19-j} from the series $(1-x)^{-4}$ (which has coefficient $\binom{(19-j)+3}{3}$).

$$\begin{aligned} N = &\binom{22}{3}\cdot 1 \\ &- \left[\binom{16}{3} + \binom{15}{3} + \binom{14}{3} + \binom{13}{3}\right] \\ &+ \left[\binom{9}{3} + \binom{8}{3} + 2\binom{7}{3} + \binom{6}{3} + \binom{5}{3}\right]. \end{aligned}$$

Calculation: $1540 - (560 + 455 + 364 + 286) + (84 + 56 + 2(35) + 20 + 10) = 115$. Thus, there are 115 such solutions.

範例

Approximation via Partial Fractions

For equations with unequal coefficients, exact formulas can be derived using partial fraction decomposition over the complex roots of unity.

Example 11.13. The Frobenius-Type Problem. Find the number of non-negative integer solutions b_r to $x_1 + 2x_2 + 3x_3 = r$.
The generating function is $G(x) = \frac{1}{(1-x)(1-x^2)(1-x^3)}$. We factor the denominators using roots of unity. Let $\omega = e^{i2\pi/3}$.

$$(1-x^3) = (1-x)(1-\omega x)(1-\omega^2 x).$$

$$(1-x^2) = (1-x)(1+x).$$

The decomposition is:

$$G(x) = \frac{1}{6(1-x)^3} + \frac{1}{4(1-x)^2} + \frac{17}{72(1-x)} + \frac{1}{8(1+x)} + \frac{1}{9(1-\omega x)} + \frac{1}{9(1-\omega^2 x)}.$$

The coefficient b_r is the sum of the coefficients of each term:

$$b_r = \frac{1}{6}\binom{r+2}{2} + \frac{1}{4}\binom{r+1}{1} + \frac{17}{72} + \frac{(-1)^r}{8} + \frac{\omega^r + \omega^{2r}}{9}.$$

Using $\omega^r + \omega^{2r} = 2\cos(2\pi r/3)$, and expanding the binomials:

$$b_r = \frac{(r+3)^2}{12} - \frac{7}{72} + \frac{(-1)^r}{8} + \frac{2}{9}\cos\frac{2\pi r}{3}.$$

While this formula is exact, the oscillatory terms are small.

$$\left| -\frac{7}{72} + \frac{(-1)^r}{8} + \frac{2}{9}\cos\frac{2\pi r}{3} \right| \leq \frac{7}{72} + \frac{1}{8} + \frac{2}{9} = \frac{32}{72} < \frac{1}{2}.$$

Therefore, b_r is simply the nearest integer to the dominant quadratic term:

$$b_r = \left\lfloor \frac{(r+3)^2}{12} + \frac{1}{2} \right\rfloor.$$

範例

11.6 Exercises

Factorise the expression $x^3 + y^3 + z^3 - 3xyz$.

1. **Cubic Identity.** Find all integer solutions to the equation $x^3 + y^3 + z^3 = 3xyz$.
2. **Factorials and Mersenne Numbers.** Find all positive integer solutions (n, m) to $\sum_{k=1}^{n} k! = 2^m - 1$.
3. **Exponential Commutativity.** Find all integer solutions to the equation $x^y = y^x$.
4. **Unique Positive Solutions.**
   (a) Prove that the equation $4x^4 - 3y^2 = 1$ has the unique positive integer solution $(x, y) = (1, 1)$.
   (b) Deduce that $x^3 + 1 = 2y^2$ has only the positive integer solutions $(1, 1)$ and $(23, 78)$.
5. **Quartic-Quadratic Non-Existence.** Prove that $x^4 - 3y^2 = 1$ has only the integer solutions $(x, y) = (\pm 1, 0)$.
6. **Sum of Squares as a Square.** Find all integer solutions to $\sum_{i=1}^{n} x_i^2 = y^2$ for $n \geq 2$, satisfying the condition $\gcd(x_1, \ldots, x_n) = 1$.
7. **Exponential Inequality.** Prove that $(x+2)^{2y} = x^z + 2$ has no positive integer solutions.
8. **Sums of Fourth Powers.** Prove that $x^4 + y^4 = z^4 + w^4$ possesses infinitely many integer solutions.
9. **Reciprocal Sum with Product Term.** Prove that $\frac{1}{x} = \frac{1}{y} + \frac{1}{z} + \frac{1}{w} + \frac{1}{xyzw}$ has infinitely many positive integer solutions.
10. **Cubic Sum equal to Cube.** Construct a parametric family of positive integer solutions to $x^3 + y^3 + z^3 = t^3$.

11. **Arbitrary Powers.** Provide a method to find infinitely many positive integer solutions to $x^2 + y^2 = z^n$ for any $n \geq 2$.

12. **Generalised Coprime Powers.** Let l, m, n be positive integers with $\gcd(nl, m) = 1$. Prove that $x^l + y^m = z^n$ has infinitely many positive integer solutions.

13. **Catalan-type Equation.** Find all positive integer solutions to $3^x - 2^y = 1$.

14. **Self-Power Product.** Find a family of positive integer solutions to $x^y y^x = z^z$ with variables greater than 1.

15. **Polynomial Product Constraints.** Let p be an odd prime and $k \geq 1$. Prove that the equation

$$y(y+1)(y+2)(y+3) = p^{2k}x(x+1)(x+2)(x+3)$$

has no positive integer solutions.

16. **Quartic Difference with Prime.** Let p be an odd prime such that $p \equiv 3 \pmod 8$. Prove that $x^4 - y^4 = pz^2$ has no positive integer solutions.

17. **Sums of Four Cubes.** Prove that $x^3 + y^3 + z^3 + w^3 = n$ has integer solutions for n in the forms $18k, 18k \pm 1, \ldots, 18k \pm 9$.

18. **Cubic Form Solvability.** Let $n = 2^r \prod p_i^{r_i}$ with odd primes $p_1 < \cdots < p_k$. Prove that $x^3 + y^3 + z^3 - 3xyz = n$ has non-negative integer solutions if and only if $p_1 \neq 3$ or ($p_1 = 3$ and $r_1 \geq 2$). Find a solution for $n = 123480$.

19. **Shifted Linear Solutions.** Find the number of integer solutions to $x + y + z = 1$ such that $x, y, z > -5$.

20. **Combinatorial Equivalence.** Prove that the number of non-negative integer solutions to $\sum_{i=1}^{7} x_i = 13$ equals the number of such solutions to $\sum_{j=1}^{14} y_j = 6$.

21. **Lower Bounded Solutions.** Determine the number of integer solutions to $\sum_{i=1}^{n} x_i = r$ subject to $x_i > a_i$.

22. **Box Constraints.** Find the number of integer solutions to $x + y + z = 24$ subject to $1 \leq x \leq 5$, $12 \leq y \leq 18$, and $-1 \leq z \leq 12$.

23. **Weighted Linear Count.** Find the number of non-negative integer solutions to $x + 2y = r$.

24. **System Count.** Find the number of non-negative integer solutions to $5x + 2y + z = 10n$ for a positive integer n.