Elementary Number Theory

An Invitation to The World of Integers

Author: Kui Liu & Jiong Yang

Institute: Qingdao University

Date: September 1st, 2025

Victory won't come to us unless we go to it.

Contents

Introduction

Number theory is a branch of pure mathematics dedicated to the study of integers. Regarded as one of the most fundamental areas of mathematics, it has deep connections with other disciplines such as analysis, algebra, and geometry. In modern times, number theory has found widespread applications, particularly in cryptography, where it plays a vital role in ensuring information security. Due to its profound theoretical significance and foundational importance, number theory is often hailed as the "Queen of Mathematics."

Elementary number theory is a fundamental branch of number theory that mainly studies integers and their basic properties using elementary methods. It traces back to ancient civilizations like the Egyptians and Babylonians who had basic number - related knowledge for practical needs. However, the ancient Greeks, particularly Pythagoras and his school, were among the first to study numbers for their own sake, exploring prime and perfect numbers. Euclid's "Elements" was a landmark, presenting the Euclidean algorithm and proving the infinity of prime numbers. During the Middle Ages, Arab mathematicians preserved and expanded on Greek works, while in Europe, Fibonacci introduced the Fibonacci sequence with number - theoretic implications. In the modern era, Fermat's theorems and conjectures, Euler's numerous contributions including the totient function, and Gauss's systematization in "Disquisitiones Arithmeticae" with concepts like congruences and quadratic reciprocity, significantly advanced the field.

In this note, we use $\mathbb{Z}$, $\mathbb{N}$ and $\mathbb{Z}_{\geq 0}$ to denote the set of integers, positive integers and non-zero integers, respectively. We also call positive integers natural numbers and non-negative integers whole numbers.

Chapter 1 Greatest Common Divisor

1.1 Exact Division

Definition 1.1 (Exact Division)

For $m, n \in \mathbb{Z}$ with $m \neq 0$, if there exists $q \in \mathbb{Z}$ such that $n = qm$, we say that m divides n, denoted by $m \mid n$. Otherwise, we say that m does not divide n, denoted by $m \nmid n$.

♣

Example 1.1 We have $3 \mid 12$, $5 \nmid 12$, and $m \mid 0$ for any $m \in \mathbb{Z}$ with $m \neq 0$.

Proposition 1.1 (Mutual Divisibility Implies Equality)

If $m \mid n$ and $n \mid m$, then $m = \pm n$.

♠

Proof Since $m \mid n$ and $n \mid m$, then $n = km$ and $m = ln$ for some $k, l \in \mathbb{Z}$. Combining these two equations, we have $n = kln$, which implies $kl = 1$. Since k, l are integers, the only possibilities are $k = l = 1$ and $k = l = -1$, which gives $m = \pm n$. □

Proposition 1.2 (Transitivity of Divisibility)

If $d \mid m$ and $m \mid n$, then $d \mid n$.

♠

Example 1.2 $3 \mid 6$ and $6 \mid 18$ imply $3 \mid 18$.

Proof Since $d \mid m$ and $m \mid n$, there exist $m', n' \in \mathbb{Z}$ such that $m = m'd$ and $n = n'm$. It follows that $n = (m'n')d$. Note that $m', n' \in \mathbb{Z}$ implies $m'n' \in \mathbb{Z}$, then we obtain $d \mid n$. □

Proposition 1.3 (Divisibility of Linear Combination)

If $d \mid m$ and $d \mid n$, then $d \mid am + bn$ for any $a, b \in \mathbb{Z}$.

♠

Example 1.3 $3 \mid 6$ and $3 \mid 12$ imply $3 \mid 84 = 4 \cdot 6 + 5 \cdot 12$.

Proof Since $d \mid m$ and $d \mid n$, there exist $m', n' \in \mathbb{Z}$ such that $m = dm'$ and $n = dn'$. It follows that

$$am + bn = a(dm') + b(dn') = (am' + bn')d.$$

Note that $a, b, m', n' \in \mathbb{Z}$, then we also have $am' + bn' \in \mathbb{Z}$, which yields $d \mid am + bn$. □

Proposition 1.4 (Bound of Divisors)

If $m \mid n$ and $n \neq 0$, then $|m| \leq |n|$.

♠

Proof Since $m \mid n$, there exists $q \in \mathbb{Z}$ such that $n = qm$. Note that $n \neq 0$, then we must have $q \neq 0$, which implies $|q| \geq 1$, since $q \in \mathbb{Z}$. It follows that $|n| = |qm| = |q| \cdot |m| \geq |m|$. □

Remark The condition $n \neq 0$ is necessary; otherwise, the statement fails. For example, although $3 \mid 0$ holds, the inequality $3 \leq 0$ is false.

Corollary 1.1 (Divisibility with Restriction Forces Zero)

If $m \mid n$ and $|n| < |m|$, then $n = 0$.

♡

Proof This is a contrapositive of Proposition 1.4. □

Problem 1.1 $m, n \in \mathbb{Z}$ with $m \neq 0$, how can we determine whether $m \mid n$ or not?

1.2 Division with remainder

Theorem 1.1 (Division with remainder)

For $m, n \in \mathbb{Z}$ with $m \neq 0$, there exists a unique pair of integers q and r such that

$$n = qm + r \quad \text{and} \quad 0 \leq r < |m|.$$

Here $q = \lfloor n/m \rfloor$ is called the quotient, and r is called the remainder. ♡

Example 1.4 We have $12 = 4 \cdot 3 + 0$ and $12 = 2 \cdot 5 + 2$, which gives $3 \mid 12$ and $5 \nmid 12$, respectively.

Proof To show the existence, define

$$S := \{n - km : k \in \mathbb{Z}\}$$

and consider the subset

$$S_{\geq 0} := S \cap \mathbb{Z}_{\geq 0}.$$

Since $m \neq 0$, choose $k = \lfloor n/m \rfloor - 1$. then $n - km \geq 0$. Hence, $S_{\geq 0}$ is non-empty. Let r be the smallest element in $S_{\geq 0}$. Thus, $S_{\geq 0}$ has the smallest integer, say r. By definition, $r \geq 0$ and can be written as $r = n - qm$ for some $q \in \mathbb{Z}$.

In addition, we must have $r < |m|$. To see this, suppose in contradiction that $r \geq |m|$, then $r - |m| \geq 0$. Note that

$$r - |m| = n - qm - |m| = n - (q \pm 1)m,$$

where the sign depends on the positivity of m. This implies $r - |m| \in S_{\geq 0}$, contradicting the minimality of r, forcing $r < |m|$. This completes the proof of existence.

For the uniqueness, suppose $n = qm + r = mq' + r'$ with $0 \leq r, r' < |m|$. Subtracting these equations yields $r - r' = (q' - q)m$, which gives $m \mid r - r'$. Since $0 \leq r, r' < |m|$, the difference satisfies $-|m| < r - r' < |m|$. This forces $r - r' = 0$, i.e. $r = r'$. Then from $qm + r = q'm + r'$, we obtain $qm = q'm$, which implies $q = q'$, since $m \neq 0$. This completes the proof of uniqueness. □

✍ **Exercise 1.1(Generalized Division with remainder)** For $m, n \in \mathbb{Z}$ with $m \neq 0$, there exists a unique pair of integers q and r such that $n = qm + r$, where $a \leq r < b$ and $b - a = |m|$.

1.3 Greatest Common Divisor

Definition 1.2
If $d \mid n$, then d is called a divisor of n.

Example 1.5 The divisors of 6 are $\pm 1, \pm 2, \pm 3$ and ± 6.

Definition 1.3
For $m, n \in \mathbb{Z}$, if an integer d satisfies $d \mid m$ and $d \mid n$, then d is called a common divisor of m and n.

Example 1.6 2 is a common divisor of 12 and 18, but 4 is not.

Definition 1.4
For $m, n \in \mathbb{Z}$, not both zero, the greatest common divisor of m and n, denoted by $\gcd(m, n)$, is the largest positive common divisor of m and n.

Example 1.7 We have $\gcd(12, 18) = \max\{1, 2, 3, 6\} = 6$.

Proposition 1.5
- $\gcd(m, n) = \gcd(n, m)$.
- *If $m \mid n$, then $\gcd(m, n) = m$. In particular, $\gcd(m, 0) = m$ for any $m \in \mathbb{Z}$ with $m \neq 0$.*

Proof Leave to the reader. □

Definition 1.5
For $m, n \in \mathbb{Z}$, if $\gcd(m, n) = 1$, then m and n are called coprime.

Example 1.8 6 and 35 are coprime, but 10 and 35 are not, since $\gcd(6, 35) = 1$, while $\gcd(10, 35) = 5$.

Exercise 1.2 Please compute $\gcd(18, 48)$.

Problem 1.2 For large integers m and n, how can we efficiently compute $\gcd(m, n)$?

1.4 Bézout's Identity

Theorem 1.2 (Bézout's Identity)

For $m, n \in \mathbb{Z}$, not both zero, there exist $a, b \in \mathbb{Z}$ such that $\gcd(m, n) = am + bn$. ♡

Example 1.9 $\gcd(6, 15) = 3 \cdot 6 + (-1) \cdot 15$.

Proof Define the set

$$S := \{xm + yn : x, y \in \mathbb{Z}\}.$$

We aim to $\gcd(m, n)$ is the the smallest positive integer in S.

Consider the set $S \cap \mathbb{N}$. Since m and n are not both zero, without loss of generality, suppose $m \neq 0$. Then $1 \cdot m + 0 \cdot n$ or $(-1) \cdot m + 0 \cdot n$ is in S, and one of these is positive. Thus, $S \cap \mathbb{N}$ is non-empty. Let d be the smallest integer in $S \cap \mathbb{N}$. By definition of S, there exist $a, b \in \mathbb{Z}$ such that

$$d = am + bn.$$

Since $\gcd(m, n)$ divides both m and n, by Proposition 1.3, we obtain $\gcd(m, n) \mid d$.

Now we show $d \mid \gcd(m, n)$. By the division algorithm, there exist $q, r \in \mathbb{Z}$ such that

$$m = qd + r \quad \text{and} \quad 0 \leq r < d.$$

It follows that

$$r = m - qd = (1 - qa)m + (-qb)n \in S \cap \mathbb{N}$$

This shows $r \in \mathbb{S}$. If $r > 0$, then $r \in S \in \mathbb{N}$, contradicting the minimality of d. Hence, $r = 0$, so $d \mid m$. A symmetric argument shows $d \mid n$. Thus, by Proposition 1.6, we have $d \mid \gcd(m, n)$.

Since both $\gcd(m, n)$ and d are positive, by Proposition 1.1, we have $\gcd(m, n) = d = am + bn$. □

Proposition 1.6 (Characterization of GCD via Divisibility)

$d \mid \gcd(m, n)$ if and only if $d \mid m$ and $d \mid n$. ♠

Example 1.10 $3 \mid \gcd(30, 42)$ is equivalent to $3 \mid 30$ and $3 \mid 42$.

Proof We first prove the forward direction. Suppose $d \mid \gcd(m, n)$. Since $\gcd(m, n)$ divides both m and n, by Proposition 1.2, we have $d \mid m$ and $d \mid n$.

Now we prove the reverse direction. Suppose $d \mid m$ and $d \mid n$. By Bézout's identity, we have $\gcd(m, n) = am + bn$ for some $a, b \in \mathbb{Z}$. Then by Proposition 1.3, we have $d \mid \gcd(m, n)$. □

✍ **Exercise 1.3(Coprime Preservation under Multiplication)** If $\gcd(a, m) = 1$ and $\gcd(b, m) = 1$, then $\gcd(ab, m) = 1$.

Problem 1.3 For $m, n \in \mathbb{Z}$, not both zero, how can we efficiently find integers a, b such that $(m, n) = am + bn$?

1.5 Euclid's Algorithm

Lemma 1.1 (GCD Preservation in the Division Algorithm)

For $a, b, c, q \in \mathbb{Z}$ with $b \neq 0$, if $a = qb + c$, then $\gcd(a, b) = \gcd(b, c)$.

♡

Example 1.11 Since $1988 = 2 \cdot 929 + 130$, it follows that $\gcd(1988, 929) = \gcd(929, 130)$.

Proof Since $\gcd(b, c)$ divides both b and c, by Proposition 1.3, we have

$$\gcd(b, c) \mid a = q \cdot b + 1 \cdot c.$$

Thus, $\gcd(b, c)$ divides both a and b. By Proposition 1.6, we have $\gcd(b, c) \mid \gcd(a, b)$.

On the other hand, since $\gcd(a, b)$ divides both a and b, by Proposition 1.3, we have

$$\gcd(a, b) \mid c = 1 \cdot a + (-q) \cdot b.$$

Thus $\gcd(a, b)$ divides both b and c. By Proposition 1.6, we have $\gcd(a, b) \mid \gcd(b, c)$.

Combining the above two results, by Proposition 1.1 and the positivity of the greatest common divisor, we conclude that $\gcd(a, b) = \gcd(b, c)$. □

Theorem 1.3 (Euclid's Algorithm)

For integers $0 < r_1 \leq r_0$, define quotients $q_1, q_2, \cdots, q_k \in \mathbb{N}$ and remainders $r_2, \cdots, r_{k+1} \in \mathbb{Z}_{\geq 0}$ by

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 q_2 + r_3, & 0 < r_3 < r_2,\\
&\vdots\\
r_{k-2} &= r_{k-1} q_{k-1} + r_k, & 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k q_k + r_{k+1}, & r_{k+1} = 0.
\end{aligned}$$

Then we have $\gcd(r_0, r_1) = r_k$.

♡

Example 1.12 Let $r_0 = 1988$ and $r_1 = 929$. Applying the Euclid's algorithm, we have

$$\begin{aligned}
1988 &= 929 \cdot 2 + 130,\\
929 &= 130 \cdot 7 + 19,\\
130 &= 19 \cdot 6 + 16,\\
19 &= 16 \cdot 1 + 3,\\
16 &= 3 \cdot 5 + 1,\\
3 &= 1 \cdot 3 + 0.
\end{aligned}$$

From this we conclude that

$$\gcd(1988, 929) = \gcd(929, 130) = \gcd(130, 19) = \gcd(19, 16) = \gcd(16, 3) = \gcd(3, 1) = 1.$$

Proof By Lemma 1.1, we obtain

$$\gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k) = \gcd(r_k, 0) = r_k,$$

which is our desired result. □

✍ **Exercise 1.4** Please compute $\gcd(2017, 823)$.

1.6 Extended Euclid's Algorithm

Theorem 1.4 (Extended Euclid's Algorithm)

For integers $0 < r_1 \leq r_0$, define the quotients $q_1, q_2, \cdots, q_k \in \mathbb{N}$ and the remainders $r_2, \cdots, r_{k+1} \in \mathbb{Z}_{\geq 0}$ as in Theorem 1.3. Additionally, define $s_0, \cdots, s_{k+1}$ and $t_0, \cdots, t_{k+1}$ by the following recurrence relations:

$$s_0 = 1,\ s_1 = 0,\ s_{i+1} = s_{i-1} - s_i q_i \quad \text{for} \quad i = 1, \cdots, k,$$
$$t_0 = 0,\ t_1 = 1,\ t_{i+1} = t_{i-1} - t_i q_i \quad \text{for} \quad i = 1, \cdots, k.$$

Then, for each $i = 0, 1, \cdots, k+1$, we have

$$r_i = s_i r_0 + t_i r_1.$$

In particular, the greatest common divisor of r_0 and r_1 is given by

$$\gcd(r_0, r_1) = r_k = s_k r_0 + t_k r_1.$$

♡

Example 1.13 For $r_0 = 1988$ and $r_1 = 929$, applying the extended Euclid's algorithm, we obtain

$$\begin{aligned} s_0 &= 1, & t_0 &= 0 \\ s_1 &= 0, & t_1 &= 1 \\ s_2 &= 1, & t_2 &= -2 \\ s_3 &= -7, & t_3 &= 15 \\ s_4 &= 43, & t_4 &= -92 \\ s_5 &= -50, & t_5 &= 107 \\ s_6 &= 293, & t_6 &= -627 \end{aligned}$$

Then we have

$$\gcd(1988, 929) = 293 \times 1988 + (-627) \times 929 = 1.$$

Proof Leave to the reader. □

✍ **Exercise 1.5** Find integers a, b such that $\gcd(2019, 414) = a \cdot 2019 + b \cdot 414$.

Chapter 2 Prime Numbers

2.1 Prime Numbers

Definition 2.1

An integer $p \geq 2$ is called a prime number (or simply a prime) if it has no positive divisors other than 1 and itself. In contrast, if an integer $n \geq 2$ has divisors other than 1 and itself, then n is called a composite number.

Example 2.1 19 is a prime number, while 39 is a composite number. The integer 1 is neither a prime number nor a composite number.

Exercise 2.1(Equivalence of Prime Non-Divisibility and Coprimality) Let p be a prime number and n be an non-zero integer, then $p \nmid n$ if and only if $\gcd(p, n) = 1$.

Problem 2.1 How can we efficiently determine whether a large positive integer is a prime number?

Proposition 2.1 (Existence of Prime Divisors)

Every integer $n \geq 2$ must have a prime divisor.

Example 2.2 35 has a prime divisor 5.

Proof If n is a prime number, the statement holds trivially. Now suppose n is composite. Let p be its smallest divisor with $p > 1$, then $1 < p < n$. Assume for contradiction that p is not a prime number. Then exists an integer d such that $d \mid p$ and $1 < d < p$. Since $p \mid n$, it follows that $d \mid n$. This contradicts the minimality of p as the smallest divisor of n greater than 1. Therefore, p must be a prime number. □

Corollary 2.1 (Prime Divisor Bound for Composites)

A composite number $n \geq 2$ must have a prime divisor p with $p \leq \sqrt{n}$.

Proof Let p be the smallest prime divisor of n, then we have $1 < p < n$. Thus $n/p > 1$ is also a divisor of n. By the minimality of p, we have $p \leq n/p$, which yields $p \leq \sqrt{n}$. □

Note *To determine whether an integer $n \geq 2$ is a prime number, it suffices to check the divisibility by all prime numbers p satisfying $2 \leq p \leq \sqrt{n}$. If n is divisible by such a prime number, then n is a composite number; otherwise, n is a prime. Let's take 37 as an example. Note that $\sqrt{37} = 6.082\ldots$, then all prime numbers less than or equal to $\sqrt{37}$ are $2, 3, 5$. It is easy to check that none of these prime numbers divides 37. Hence 37 is a prime number.*

Exercise 2.2 Determine whether 2017 is a prime or not.

Corollary 2.2 (Uniqueness of 1 in Prime Divisibility)

If $n \in \mathbb{N}$ cannot be divided by any prime number, then $n = 1$.

Proof This is a contrapositive of Proposition 2.1. □

Problem 2.2 How many prime numbers are there in $\mathbb{N}$?

2.2 Prime Number Theorem

Lemma 2.1 (Euclid's Lemma)

For a prime number p, if $p \mid mn$ with $m, n \in \mathbb{Z}$, then $p \mid m$ or $p \mid n$.

Example 2.3 Since 3 is a prime number and 3 divides $45 = 5 \cdot 9$, then 3 must divide either 5 or 9. In fact, $3 \mid 9$.

Proof If $p \mid m$, the result is immediate. Suppose $p \nmid m$. By Exercise 2.1, we have $\gcd(p, m) = 1$. By Bézout's Identity, there exists integers $a, b \in \mathbb{Z}$ such that $ap + bm = 1$. It follows that

$$n = 1 \cdot n = (ap + bm)n = (an)p + b(mn).$$

Since p divides both p and mn, by Proposition 1.3, we obtain $p \mid n$. □

Exercise 2.3(Generalized Euclid's Lemma) Show that if $a \mid mn$ and $\gcd(a, m) = 1$, then $a \mid n$.

Exercise 2.4(Coprimality of Product) Show that if $\gcd(m, a) = \gcd(n, a) = 1$, then $\gcd(mn, a) = 1$.

Theorem 2.1 (Euclid's Theorem)

There are infinitely many prime numbers.

Proof Assume that there are only finitely many prime numbers, listed as $p_1, p_2, \ldots, p_k$. Consider the integer

$$n := p_1 p_2 \cdots p_k + 1.$$

Observe that n leaves a remainder of 1 when divided by each prime p_i. Then n cannot be divided by any prime number. By Corollary 2.2, we derive $n = 1$, which is impossible. Hence, our initial assumption is false. There are infinitely many prime numbers. □

Exercise 2.5 Show that there are infinitely many prime numbers in the arithmetic progression $3n + 2$, $n = 1, 2, \ldots$.

Note *For $x \geq 2$, Let $\pi(x)$ denote the number of prime numbers less than or equal to x. For example, $\pi(10) = 4$, since the prime numbers less than or equal to 10 are $2, 3, 5, 7$. Then Theorem 2.1 can be formulated as*

$$\pi(x) \to +\infty \quad \text{as} \quad x \to +\infty.$$

In the late 18th century, Gauss and Legendre independently made a more precise conjecture about the asymptotic formula of $\pi(x)$. This landmark result is now known as the prime number theorem. In 1896, Hadamard and de la Vallée Poussin proved the prime number theorem independently, building on foundational work in complex analysis.

Theorem 2.2 (Prime Number Theorem)

We have

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

Problem 2.3 Are there infinitely many primes in the arithmetic progression $qn+a$, $n = 1, 2, \ldots$ for any coprime $q, a \in \mathbb{N}$?

2.3 Fundamental Theorem of Arithmetic

Theorem 2.3 (Fundamental Theorem of Arithmetic)

Any integer $n \geq 2$ can be expressed uniquely (up to ordering) as a product of prime numbers:

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

where each p_i $(i = 1, 2, \ldots, k)$ is a prime number. ♡

Proof We first prove the existence. We proceed by induction on n. The base case $n = 2$ holds trivially as 2 is a prime number. Assume $n > 2$ and that all integers m with $2 \leq m < n$ can be expressed as a product of prime numbers. If n is a prime number, the existence follows immediately. If n is a composite number, by Proposition 2.1, there exists a prime $p \geq 2$ such that $n = pn'$ with $n' < n$. By the induction hypothesis, n' has a prime factorization, hence $n = pn'$ does as well.

Now we prove the uniqueness. We proceed by induction on n again. The base case $n = 2$ is trivial. Assume $n > 2$ and uniqueness holds for all integers less than n. Suppose

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l,$$

where each p_i and q_j is a prime number.

Since p_1 is a prime number and $p_1 \mid q_1 q_2 \cdots q_l$, by Lemma 2.1, p_1 must divide some q_j. As q_j is also a prime number, we have $q_1 = q_j$. Without loss of generality, we may reorder $q_1, q_2, \ldots, q_l$ so that $p_1 = q_1$. Let

$$n' := n/p_1 = n/q_1.$$

Dividing both sides by $p_1 = q_1$, we obtain

$$n' = p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_l.$$

Note that $n' < n$. Then by the induction hypothesis, we derive $k - 1 = l - 1$, i.e. $k = l$, and $p_2, p_3, \ldots, p_k$ is a permutation of $q_2, q_3 \ldots, q_l$. This completes the proof of uniqueness. □.

Note *By the Fundamental Theorem of Arithmetic, every integer $n \geq 2$ can be uniquely expressed (up to the order of primes) as*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where $p_1, p_2, \ldots, p_k$ are distinct prime numbers, and each exponent $e_i \in \mathbb{N}$. For example, $60 = 2^1 \cdot 3^1 \cdot 5^1$ and $72 = 2^3 \cdot 3^2$.

✍ **Exercise 2.6** Decompose 2019 into prime factors.

✍ **Exercise 2.7** Suppose $n^2 = uv$ with $n, u, v \in \mathbb{N}$ and $\gcd(u, v) = 1$. Show that there exist $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$ such that $u = a^2$ and $v = b^2$.

2.4 p-adic Valuation

Definition 2.2

Let p be a prime. For any non-zero integer n, the p-adic valuation of n at p, denoted by $v_p(n)$, is defined as the largest integer k such that $p^k \mid n$.

Example 2.4 $v_2(72) = v_2(2^3 \cdot 9) = 3$, $v_3(72) = v_3(3^2 \cdot 8) = 2$, and $v_p(1) = 0$ for every prime number p.

Note *According to the Fundamental Theorem of Arithmetic, any $n \in \mathbb{N}$ can be uniquely written as*

$$n = \prod_p p^{v_p(n)},$$

where the product takes over all prime numbers, and all but finitely many $v_p(n)$ are zero.

Proposition 2.2 (Additivity of p-adic Valuation)

Let p be a prime, then for any $m, n \in \mathbb{N}$, we have

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

Example 2.5 We have $v_2(4 \cdot 18) = v_2(72) = 3$ and $v_2(4) + v_2(18) = 2 + 1 = 3$.

Proof Suppose $m = p^{v_p(m)}m'$ and $n = p^{v_p(n)}n'$, where $p \nmid m'$ and $p \nmid n'$. Observe that

$$mn = (p^{v_p(m)}m')(p^{v_p(n)}n') = p^{v_p(m)+v_p(n)}m'n'$$

and $p \nmid m'n'$. Then by the definition of the p-adic valuation, we have $v_p(mn) = v_p(m) + v_p(n)$. □

Proposition 2.3 (Ultrametric Inequality)

Let p be a prime, then for any $m, n \in \mathbb{N}$, we have

$$v_p(m+n) \geq \min\big(v_p(m), v_p(n)\big),$$

with equality if $v_p(m) \neq v_p(n)$.

Example 2.6 We have $v_3(15 + 21) = 2$, which is larger than $\min\big(v_3(15), v_3(21)\big) = \min(1, 1) = 1$, and $v_3(15 + 36) = v_3(51) = 1$ which is equal to $\min\big(v_3(15), v_3(36)\big) = \min\big(1, 2\big) = 1$.

Proof Without loss of generality, we suppose $v_p(m) \leq v_p(n)$. Write $m = p^{v_p(m)}m'$ and $n = p^{v_p(n)}n'$, where $p \nmid m'$ and $p \nmid n'$. We have

$$m + n = p^{v_p(m)}m' + p^{v_p(n)}n' = p^{v_p(m)}(p^{v_p(n)-v_p(m)}m' + n').$$

Since $v_p(m) \leq v_p(n)$, it follows that $p^{v_p(n)-v_p(m)}m' + n'$ is an integer. By the definition of p-adic valuation, we have

$$v_p(m+n) \geq v_p(m) = \min\big(v_p(m), v_p(n)\big),$$

which is our desired result.

If $v_p(m) \neq v_p(n)$, without loss of generality, we suppose $v_p(m) < v_p(n)$. Write $m = p^{v_p(m)}m'$ and $n = p^{v_p(n)}n'$, where $p \nmid m'$ and $p \nmid n'$. We have

$$m + n = p^{v_p(m)}m' + p^{v_p(n)}n' = p^{v_p(m)}(p^{v_p(n)-v_p(m)}m' + n').$$

Since $v_p(m) < v_p(n)$, then we have $v_p(n) - v_p(m) \geq 1$, which yields $p \mid p^{v_p(m)} - p^{v_p(n)}m'$. Note that $p \nmid n'$, then we must have $p \nmid p^{v_p(m)-v_p(n)}m' + n'$. This indicates that

$$v_p(m+n) = v_p(m) = \min(v_p(m), v_p(n)).$$

This completes the proof. □

✍ **Exercise 2.8(Legendre's Formula)** Let $n \in \mathbb{N}$ and p be a prime. Show that

$$v_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right],$$

where $[x]$ with $x \in \mathbb{R}$ denotes the largest integer less than or equal to x.

Chapter 3 Congruences

3.1 Congruences

Definition 3.1

Let $a, b \in \mathbb{Z}$ and m be a non-zero integer. If there exists $k \in \mathbb{Z}$ such that $a = b + km$, then we say a and b are congruent (or a is congruent to b) modulo m, denoted by $a \equiv b \pmod{m}$. Here, m is called the modulus of the congruence.

Example 3.1 $17 \equiv 11 \pmod{3}$, since $17 = 11 + 3 \cdot 2$. But $17 \not\equiv 11 \pmod{4}$, since we cannot find an integer k such that $17 = 11 + k \cdot 4$.

Proposition 3.1 (Modulus Scaling Property)

Let k be a non-zero integer, then $ka \equiv kb \pmod{km}$ if and only if $a \equiv b \pmod{m}$.

Example 3.2 $9 \equiv 24 \pmod{15}$ is equivalent to $3 \equiv 8 \pmod{5}$.

Proof Note that $a \equiv b \pmod{m}$ if and only if there exists an integer $l \in \mathbb{Z}$ such that $a - b = lm$. This is equivalent to the statement that there exists an integer $l \in \mathbb{Z}$ such that $ka - kb = klm$, since k is a non-zero integer. By the definition of congruence, this statement is equivalent to $ka \equiv kb \pmod{km}$. □

Proposition 3.2 (Fundamental Congruence Criterion)

For a non-zero integer m, we have $a \equiv b \pmod{m}$ if and only if $m \mid a - b$.

Example 3.3 $17 \equiv 11 \pmod{3}$, since $2 \mid 6 = 17 - 11$. But $17 \not\equiv 11 \pmod{4}$, since $4 \nmid 6 = 17 - 11$.

Proof This follows immediately from the definitions of congruence and exact division.

Exercise 3.1(Congruence Induced by Divisibility) Show that if $a \equiv b \pmod{m}$ and $d \mid m$, then we have $a \equiv b \pmod{d}$. □

Proposition 3.3 (Congruence Modulo m as an Equivalence Relation)

Let m be a non-zero integer. For any $a, b, c \in \mathbb{Z}$, the following properties hold:

(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* $a \equiv c \pmod{m}$.

Example 3.4 $3 \equiv 10 \pmod{7}$ and $10 \equiv 24 \pmod{7}$ imply $3 \equiv 24 \pmod{7}$.

Proof The reflexivity follows from $m \mid a - a = 0$. The symmetry follows from the fact that $m \mid a - b$ implies $m \mid (-1)(a - b) = b - a$. For the transitivity, since $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, we have $m \mid a - b$ and $m \mid b - c$. Then by Proposition 1.3, we conclude that $m \mid (a - b) + (b - c) = a - c$. This implies $a \equiv c \pmod{m}$. □

Proposition 3.4 (Congruence Preservation under Addition and Multiplication)

Let m be a non-zero integer. We have the following statements:

- *If* $a_1 \equiv b_1 \pmod{m}$ *and* $a_2 \equiv b_2 \pmod{m}$, *then* $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.
- *If* $a_1 \equiv b_1 \pmod{m}$ *and* $a_2 \equiv b_2 \pmod{m}$, *then* $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

Example 3.5 We have

- $3 \equiv 8 \pmod 5$ and $13 \equiv 18 \pmod 5$ implies $3 + 13 \equiv 8 + 18 \pmod 5$, that is $16 \equiv 26 \pmod 5$.
- $3 \equiv 7 \pmod 4$ and $2 \equiv 6 \pmod 4$ imply $2 \cdot 3 \equiv 6 \cdot 7 \pmod 4$, that is $6 \equiv 42 \pmod 4$.

Proof The proof is left to the reader as an exercise. □

Corollary 3.1 (Congruence Preservation under Scaling and Exponentiation)

Let m be a non-zero integer. We have the following statements:

(i) *If $a \equiv b \pmod m$, then $ka \equiv kb \pmod m$ for any $k \in \mathbb{Z}$.*

(ii) *If $a \equiv b \pmod m$, then $a^l \equiv b^l \pmod m$ for any $l \in \mathbb{N}$.*

♡

Example 3.6 If $a \equiv 2 \pmod 5$, then we have

$$7a^4 + 8 \equiv 7a^4 + 3 \equiv 2a^4 + 3 \equiv 2 \cdot 2^4 + 3 \equiv 2 \cdot 16 + 3 \equiv 2 \cdot 1 + 3 \equiv 0 \pmod 5.$$

✍ **Exercise 3.2(Polynomial Congruence Preservation)** Let $f(x)$ be a polynomial with coefficients being integers. Show that if $a \equiv b \pmod m$, then $f(a) \equiv f(b) \pmod m$.

For $a, m \in \mathbb{Z}$ with $m \neq 0$, if there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod m$, then we say that a is invertible modulo m and b is an inverse of a modulo m.

Example 3.7 6 is invertible modulo 11, since $6 \cdot 2 \equiv 1 \pmod{11}$. Moreover, 2 is the inverse of 6 modulo 11.

Proposition 3.5 (Invertibility Criterion modulo m)

Let $a, m \in \mathbb{Z}$ with $m \neq 0$. Then a is invertible modulo m if and only if $\gcd(a, m) = 1$.

♠

Example 3.8 6 is invertible modulo 11, since $\gcd(6, 11) = 1$, while 6 is not invertible modulo 15, since $\gcd(6, 15) = 3 \neq 1$.

Proof We first prove the forward direction. Suppose a is invertible modulo m. Then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod m$. Then there exists $k \in \mathbb{Z}$ such that $ab = 1 + km$. Since $\gcd(a, m)$ divides both a and m, then $\gcd(a, m) \mid ab - km = 1$, which implies $\gcd(a, m) = 1$.

Now we prove the reverse direction. Suppose $\gcd(a, m) = 1$. Then by Bézout's identity, there exists integers $k, l \in \mathbb{Z}$ such that $\gcd(m, n) = ka + lm = 1$. Thus, $ka = 1 + (-l)m$, which yields $ka \equiv 1 \pmod m$. Hence, a is invertible modulo m. □

Corollary 3.2 (Cancellation Law for Congruence)

If $ka \equiv kb \pmod m$ and $\gcd(k, m) = 1$, then $a \equiv b \pmod m$.

♡

Example 3.9 $5 \cdot 7 \equiv 5 \cdot 13 \pmod 6$ implies $7 \equiv 13 \pmod 6$, since $\gcd(5, 6) = 1$.

Proof Since $\gcd(k, m) = 1$, there exist $l \in \mathbb{Z}$ such that $kl \equiv 1 \pmod m$. By $ka \equiv kb \pmod m$, we have $lka \equiv lkb \pmod m$, which yields $a \equiv b \pmod m$ by (ii) of Proposition 3.4. □

✍ **Exercise 3.3** Show that the equation $x^2 + y^2 - 15z^2 = 7$ has no integer solutions. Hint: consider both sides modulo 8.

3.2 Wilson's Theorem

Theorem 3.1 (Wilson's Theorem)

A positive integer $n > 1$ is a prime if and only if $(n-1)! + 1 \equiv 0 \pmod{n}$.

Example 3.10 $(7-1)!+1 = 721 \equiv 0 \pmod{7}$, because 7 is a prime number. On the other hand, $(6-1)!+1 = 121 \not\equiv 0 \pmod{6}$ since 6 is a composite number.

Proof First, suppose $(n-1)! \equiv -1 \pmod{n}$ for some integer $n > 1$. Assume n is a composite number. Then there exists a prime number p with $2 \leq p \leq n-1$ such that $p \mid n$. Since $p \leq n-1$, $p \mid (n-1)!$, implying $(n-1)! \equiv 0 \pmod{p}$. However, from $(n-1)! \equiv -1 \pmod{n}$, by Exercise 3.1, we have $(n-1)! \equiv -1 \pmod{p}$. This contradiction forces n to be a prime number.

Conversely, let p be a prime number. If $p = 2$, then $(2-1)! = 1 \equiv -1 \pmod{2}$. For odd p, observe that each $a \in \{1, 2, \ldots, p-1\}$ has a unique multiplicative inverse $a^{-1} \in \{1, 2, \ldots, p-1\}$ satisfying $aa^{-1} \equiv 1 \pmod{p}$. If $a \equiv a^{-1} \pmod{p}$, then $p \mid (a-1)(a+1)$, which implies $a \equiv 1 \pmod{p}$ or $a \equiv p-1 \pmod{p}$. Thus for $a = 2, 3, \ldots, p-2$, we have $a \neq a^{-1}$. These numbers can be paired into $(p-3)/2$ pairs such that each pair's product is congruent to 1 modulo p. Multiplying all terms together, we obtain

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

which is our desired result. □

3.3 Euler's Theorem

Definition 3.2

For $n \in \mathbb{N}$, Euler's function $\varphi(n)$ counts the number of integers that are coprime to n in the set $\{1, 2, \ldots, n\}$. ♣

Example 3.11 All the integers that are coprime to 12 in $\{1, 2, \ldots, 12\}$ are $\{1, 5, 7, 11\}$, so $\varphi(12) = 4$.

Theorem 3.2 (Euler's Theorem)

If $a, m \in \mathbb{N}$ are coprime, then $a^{\varphi(m)} \equiv 1 \pmod{m}$. ♡

Example 3.12 We have $5^{\varphi(12)} = 5^4 = 625 \equiv 1 \pmod{12}$.

Proof The case $m = 1$ is trivial. Now suppose $m \geq 2$. Let

$$R := \{r_1, r_2, \ldots, r_{\varphi(m)}\}$$

be the set of integers in $\{1, 2, \ldots, m\}$ that are coprime to m. Since $\gcd(m, m) = m \geq 2$, we have $m \notin R$, hence $1 \leq r_i < m$ for all i.

Define the scaled set

$$aR := \{ar_1, ar_2, \cdots, ar_{\varphi(m)}\}.$$

Since both a and r_i are coprime to m, by Exercise 1.3, each ar_i remains coprime to m. For each i, let r_i' be the remainder given by $ar_i = qm + r_i'$ with $0 \leq r_i' < m$, and define

$$R' = \{r_1', r_2', \ldots, r_{\varphi(m)}'\}.$$

Claim: $R' = R$ as sets (up to reordering).

First, we show $R' \subset R$. Let r_i' be any element of R'. By Lemma 1.1, the equality $ar_i = qm + r_i'$ implies $\gcd(r_i', m) = \gcd(ar_i, m) = 1$. It follows that $r_i' \neq 0$, and then $1 \leq r_i' < m$. Thus, $r_i' \in R$, which implies $R' \subset R$.

Next, we prove $|R'| = |R|$ by showing all the r_i's are distinct. To this aim, assume for contradiction that $r_i' = r_j'$ for some $i \neq j$. Then $ar_i = q_1 m + r_i'$ and $ar_j = q_2 m + r_j'$ imply $ar_i \equiv ar_j \pmod{m}$. Since $\gcd(a, m) = 1$, by Corollary 3.2, we have $r_i \equiv r_j \pmod{m}$. As $0 \leq r_i', r_j' < m$, we have $-m < r_i - r_j < m$, which forces $r_i - r_j = 0$, i.e. $r_i = r_j$. This contradicts the distinctness of the r_is. Thus, the assumption is false, and the $r_i's$ are distinct. Thus, $|R'| = |R| = \varphi(m)$.

Combining the above two results, we conclude that $R' = R$.

Now we prove the statement of the theorem. By definition of the r_i's, we have $ar_i \equiv r_i' \pmod{m}$ for $i = 1, 2, \ldots, \varphi(m)$. It follows that

$$(ar_1)(ar_2)\cdots(ar_{\varphi(m)}) \equiv r_1' r_2' \cdots r_{\varphi(m)}' \pmod{m}.$$

The left side of the congruence

$$(ar_1)(ar_2)\cdots(ar_{\varphi(m)}) = a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)}.$$

Since $R' = R$, the right side of the congruence

$$r_1' r_2' \cdots r_{\varphi(m)}' = r_1 r_2 \cdots r_{\varphi(m)}.$$

Thus we have

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}.$$

Since each r_i is coprime to m, by Corollary 1.3, the product $r_1 r_2 \cdots r_{\varphi(m)}$ is also coprime to m. Then by Corollary 3.2, we obtain

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

which is our desired result. □

Corollary 3.3 (Fermat's Little Theorem)

Let p be a prime number. For any integer a with $p \nmid a$, we have

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

♡

Proof This follows from Euler's theorem and the fact that $\varphi(p) = p - 1$ for any prime number p. □

✍ **Exercise 3.4** Compute $11^{2025} \pmod{20}$.

Chapter 4 Linear Congruence Equation

4.1 Algebraic Congruence Equation

Definition 4.1

Given a non-zero integer $m \in \mathbb{N}$, let $f(x) \in \mathbb{Z}[x]$ be a polynomial with leading coefficient not divided by m. Consider the algebraic congruence equation

$$f(x) \equiv 0 \pmod{m}.$$

From Exercise 3.2, we can infer that if $f(a) \equiv 0 \pmod{m}$, then $f(b) \equiv 0 \pmod{m}$ for every $b \equiv a \pmod{m}$. Thus, we can consider the entire congruence class modulo m containing a as a single solution to $f(x) \equiv 0 \pmod{m}$, denoted by $x \equiv a \pmod{m}$.

♣

Example 4.1 For example,

$$2x^2 + 3x + 4 \equiv 0 \pmod{9}$$

has two solutions $x \equiv 1 \pmod{9}$ and $x \equiv 2 \pmod{9}$, while

$$2x^2 + 3x + 4 \equiv 0 \pmod{5}$$

has no solutions. It is clear that an algebraic congruence $f(x) \equiv 0 \pmod{m}$ has at most m solutions.

Problem 4.1 For an algebraic congruence equation, we typically hope to answer the following three fundamental questions:

- Does it have solutions?
- If it has solutions, how many solutions does it have?
- Can we find all of its solutions?

4.2 Linear Congruence Equation

Proposition 4.1 (Linear Congruence Equation)

The congruence equation

$$ax \equiv b \pmod{m} \tag{4.1}$$

has solutions if and only if $\gcd(a, m) \mid b$. *If this condition is satisfied, let* $d := \gcd(a, m)$ *and define* a_0, b_0, m_0 *by* $a = da_0$, $b = db_0$ *and* $m = dm_0$, *then* (4.1) *has* d *solutions*

$$x \equiv a_0^{-1}b_0 + km_0 \pmod{m}, \quad k = 0, 1, 2, \cdots, d-1,$$

where $a_0^{-1} \in \mathbb{Z}$ *satisfies* $a_0a_0^{-1} \equiv 1 \pmod{m_0}$.

Example 4.2 $6x \equiv 9 \pmod{21}$ has solutions, since $\gcd(6, 21) = 3 \mid 9$. Moreover, it has exactly 3 solutions, which are $x \equiv 5,\ 12,\ 19 \pmod{21}$. While $6x \equiv 9 \pmod{14}$ does not have solutions, since $\gcd(6, 14) = 2 \nmid 9$.

Proof Suppose (4.1) has a solution $x \equiv x_0 \pmod{m}$ with $x_0 \in \mathbb{Z}$. Then $ax_0 \equiv b \pmod{m}$, which implies $ax_0 + qm = b$ for some $q \in \mathbb{Z}$. Since $\gcd(a, m)$ divides both a and m, by Proposition 1.3, we have $\gcd(a, m) \mid b$.

Conversely, suppose $\gcd(a, m) \mid b$. Let $d = \gcd(a, m)$, then we can write $a = da_0$, $b = db_0$, and $m = dm_0$ with $\gcd(a_0, m_0) = 1$. Then (4.1) reduces to

$$a_0x \equiv b_0 \pmod{m_0}.$$

Since $\gcd(a_0, m_0) = 1$, there exists an integer $a_0^{-1} \in \mathbb{Z}$ such that $a_0a_0^{-1} \equiv 1 \pmod{m_0}$. Multiplying both sides by a_0^{-1} gives

$$x \equiv a_0^{-1}b_0 \pmod{m_0}.$$

Thus (4.1) has a solution.

Now we lift the above solution modulo m_0 to solutions modulo m, and show that

$$x \equiv a_0^{-1}b_0 + km_0 \pmod{m}, \quad k = 0, 1, 2, \cdots, d-1,$$

are all the solutions to (4.1), which are pairwise incongruent modulo m.

First, suppose two solutions corresponding to $k = k_1$ and $k = k_2$ are congruent modulo m, where $0 \le k_1 < k_2 \le d-1$. Then

$$a_0^{-1}b_0 + k_1m_0 \equiv a_0^{-1}b_0 + k_2m_0 \pmod{m}.$$

It follows that $(k_2 - k_1)m_0 \equiv 0 \pmod{m}$. Since $m = dm_0$, this implies $k_1 \equiv k_2 \pmod{d}$, and then $d \mid k_1 - k_2$. Observe that $|k_2 - k_1| < d$. By Corollary 1.1, we have $k_1 - k_2 = 0$, which contradicts $k_1 < k_2$. Therefore, the d solutions listed above are pairwise incongruent modulo m.

Next, let x' be any solution to $ax \equiv b \pmod{m}$. Then x' must satisfy $a_0x' \equiv b_0 \pmod{m_0}$, which implies $x' \equiv a_0^{-1}b_0 \pmod{m_0}$. Thus, $x' = a_0^{-1}b_0 + tm_0$ for some integer t. By the division algorithm, we can write $t = qd + k$, where $q \in \mathbb{Z}$ and $0 \le k \le d-1$. Then we have

$$x' = a_0^{-1}b_0 + (qd + k)m_0 = a_0^{-1}b_0 + km_0 + qm.$$

Therefore, $x' \equiv a_0^{-1}b_0 + km_0 \pmod{m}$, showing that x' is congruent to one of the d solutions listed above. Hence, (4.1) has exactly d solutions modulo m. □

Problem 4.2 Given integers a, b, c, m such that $m \nmid a$, how can we solve the quadratic congruence equation $ax^2 + bx + c \equiv 0 \pmod{m}$?

4.3 Chinese Remainder Theorem

Theorem 4.1 (Chinese Remainder Theorem)

If non-zero integers $m_1, m_2, \cdots, m_k$ are pairwise coprime non-zero integers, then the system of congruences

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{4.2}$$

has integer solutions, which form a residue class modulo $m_1 m_2 \cdots m_k$. ♡

Proof Define M_i as the product

$$M_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$$

for each i. Let each M_i^{-1} be the multiplicative inverse of M_i modulo m_i, i.e.,

$$M_i^{-1} M_i \equiv 1 \pmod{m_i}$$

for $i = 1, 2, \cdots, k$. Consider a candidate solution of the form

$$x \equiv a_1 M_1 M_1^{-1} + \cdots + a_k M_k M_k^{-1} \pmod{m_1 m_2 \cdots m_k}. \tag{4.3}$$

By construction, this x satisfies each individual congruence in the system. Specifically, for each i, the terms not involving a_i will vanish modulo m_i, leaving $x \equiv a_i \pmod{m_i}$.

If another integer x' satisfies all the congruences in the system, then for each i, $x \equiv x' \pmod{m_i}$. This implies $x \equiv x' \pmod{m_1 \cdots m_k}$. Hence (4.3) gives all the solutions of the system. □

Example 4.3 Consider

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7}. \end{cases} \tag{4.4}$$

Take

$$a_1 = 2,\ a_2 = 3,\ a_3 = 2$$

and

$$m_1 = 3,\ m_2 = 5,\ m_3 = 7.$$

We have

$$M_1 = 5 \cdot 7 = 35,\ M_2 = 3 \cdot 7 = 21,\ M_3 = 3 \cdot 5 = 15$$

and

$$M_1^{-1} = 2,\ M_2^{-1} = 1,\ M_3^{-1} = 1.$$

By CRT, we obtain

$$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 23 \pmod{105}.$$

Chapter 5 Quadratic congruence equation modulo a prime

5.1 Quadratic Residues

Definition 5.1

Let p be an odd prime. An integer a is called a quadratic residue modulo p if there exists an integer x such that

$$x^2 \equiv a \pmod{p}.$$

Otherwise, a is called a quadratic non-residue modulo p.

♣

Example 5.1 All quadratic residues modulo 7 are 1, 2 and 4, because

$$\begin{aligned}
1^2 &\equiv 1 \pmod{7},\\
2^2 &\equiv 4 \pmod{7},\\
3^2 &\equiv 9 \equiv 2 \pmod{7},\\
4^2 &\equiv 16 \equiv 2 \pmod{7},\\
5^2 &\equiv 25 \equiv 4 \pmod{7},\\
6^2 &\equiv 36 \equiv 1 \pmod{7}.
\end{aligned}$$

✍ **Exercise 5.1** Please list all the quadratic residues and nonresidues for modulus 13.

✍ **Exercise 5.2** Given an arbitrary odd prime number p, please show that the number of quadratic residues and the number of quadratic non-residues are equal.

5.2 Legendre symbol

Definition 5.2

Given an odd prime p, the Legendre symbol modulo p is a function on $\mathbb{Z}$, defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo } p. \\ -1, & \text{if } a \text{ is a quadratic nonresidue modulo } p. \\ 0, & \text{if } p \mid a. \end{cases}$$

♣

Example 5.2 We have $\left(\frac{2}{7}\right) = 1$, $\left(\frac{3}{7}\right) = -1$ and $\left(\frac{21}{7}\right) = 0$. It is also clear that $\left(\frac{1}{p}\right) = 1$ for any odd prime number p.

Problem 5.1 What is the time complexity of computing the Legendre symbol using its definition?

Theorem 5.1 (Euler's criterion)

Let p be an odd prime and a be an integer, then we have

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

which determines the value of the Legendre symbol.

♡

Proof If $p \mid a$, then by the definition of the Legendre symbol, we have $\left(\frac{a}{p}\right) = 0$. Additionally, in this case, we have $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$. Thus, the desired result holds in this situation.

Now we suppose $p \nmid a$. By Euler's Theorem, we have

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

It follows that $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, since p is a prime. We claim that a is a quadratic residue if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. If a is a quadratic residue, there exists $n \in \mathbb{Z}$ with $p \nmid n$ such that $n^2 \equiv a \pmod{p}$. Hence, we have

$$a^{\frac{p-1}{2}} \equiv n^{p-1} \equiv 1 \pmod{p},$$

which is just our claim.

Conversely, if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, we consider the set

$$S = \left\{ -\frac{p-1}{2}, \cdots, -1, 1, \cdots, \frac{p-1}{2} \right\}.$$

For each $d \in S$, there exists $x_d \in S$ such that $dx_d \equiv a \pmod{p}$. Now assume that a is not a quadratic residue. Then for every d, we have $d \neq x_d$, and the set S can be partitioned into pairs of the form d, x_d. This leads to

$$-1 \equiv (p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv d^{\frac{p-1}{2}} \pmod{p},$$

which contradicts the assumption. Hence, a must be a quadratic residue modulo p. □

Example 5.3 Consider $p = 7$ and $a = 3$. Using Euler's criterion to compute the Legendre symbol, we find

$$\left(\frac{a}{p}\right) = 3^{\frac{7-1}{2}} \equiv 3^3 \equiv -1 \pmod{p}.$$

This indicates that $\left(\frac{a}{p}\right) = -1$, which means 3 is a quadratic nonresidue modulo 7.

Corollary 5.1 (Special value of Legendre's symbol at -1)

For an odd prime p, we have

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

♡

Proof By Euler's criterion, we have

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

Since the Legendre symbol $\left(\frac{-1}{p}\right)$ and $(-1)^{\frac{p-1}{2}}$ take values only in $\{-1, 1\}$, and $p \geq 3$ is an odd prime, the congruence implies the equality

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

The cases for $p \equiv 1$ or $3 \pmod 4$ follow immediately by evaluating the exponent modulo 2. □

Problem 5.2 What is the time complexity of computing the Legendre symbol using Euler's criterion?

Theorem 5.2 (Properties of the Legendre symbol)

Let p be an odd prime. Then for any $a, b \in \mathbb{Z}$, we have

- $\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$.
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

♡

Proof By Euler's criterion, we have

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

Similarly, for the product, we have

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

Thus, we have established the stated properties. □

Example 5.4 We have $\left(\frac{9}{7}\right) = \left(\frac{2}{7}\right) = 1$ and $\left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = -1$.

Problem 5.3 Is 67 a quadratic residue modulo 109?

5.3 Law of quadratic reciprocity

Theorem 5.3 (Law of Quadratic Reciprocity)

Let p and q be distinct odd primes. Then we have

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

♡

Proof Refer to the next section. □

Example 5.5 Consider the primes $q = 67$ and $p = 109$. Using properties of the Legendre symbol, we can express

$$\left(\frac{67}{109}\right) = \left(\frac{109}{67}\right) = \left(\frac{42}{67}\right) = \left(\frac{2\cdot 3\cdot 7}{67}\right) = \left(\frac{2}{67}\right)\left(\frac{3}{67}\right)\left(\frac{7}{67}\right).$$

From the law of quadratic reciprocity, we observe

$$\left(\frac{2}{67}\right) = -1, \qquad \left(\frac{3}{67}\right) = -\left(\frac{67}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

and

$$\left(\frac{7}{67}\right) = -\left(\frac{67}{7}\right) = -\left(\frac{4}{7}\right) = -1.$$

Thus, combining these results, we obtain

$$\left(\frac{67}{109}\right) = (-1)\cdot(-1)\cdot(-1) = -1.$$

This indicates that 67 is not a quadratic residue modulo 109, which means the congruence equation

$$x^2 \equiv 69 \pmod{p}$$

has solutions.

✍ **Exercise 5.3** Is the congruence equation the congruence equation

$$3x^2 + 5x + 8 \equiv 0 \pmod{101}$$

solvable?

✍ **Exercise 5.4** Is the congruence equation $3x^2 + 2x + 1 \equiv 0 \pmod{106}$ solvable?

5.4 Proof of the law of quadratic reciprocity

Lemma 5.1 (Gauss's Lemma)

Given an odd prime p and an integer a with $(a, p) = 1$, define N as the number of pairs of integers (j, r) with $1 \le j \le \frac{p-1}{2}$ and $\frac{p}{2} < r < p$ for which $aj \equiv r \pmod{p}$. Then we have

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

♡

Proof For every integer $1 \le j \le \frac{p-1}{2}$, there exists a unique integer r_j with $1 \le r_j < p$ such that $aj \equiv r_j \pmod{p}$. It is not difficult to see that all these integers r_j are distinct. Multiplying these congruences both sides, we obtain

$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv r_1 r_2 \cdots r_{\frac{p-1}{2}} \pmod{p}.$$

For convenience, let

$$S = \left\{r_1, r_2, \cdots, r_{\frac{p-1}{2}}\right\}.$$

We claim that

$$r_1 r_2 \cdots r_{\frac{p-1}{2}} \equiv (-1)^N \left(\frac{p-1}{2}\right)! \pmod{p},$$

where n is the number of all the integers in S such that $\frac{p}{2} < r_j < p$. Accepting this claim momentarily, we deduce

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

As p is a prime, $\left(\frac{p-1}{2}\right)!$ is coprime to p, it follows that

$$a^{\frac{p-1}{2}} \equiv (-1)^N \pmod{p}.$$

This result, combined with Euler's criterion, gives the desired lemma.

To prove the above claim, label the integers larger than $p/2$ in S as $s_1, s_2, \cdots, s_N$ and the positive integers in S as $t_1, t_2, \cdots, t_M$, respectively. Clearly, $M + N = \frac{p-1}{2}$. Our aim is to show that

$$\left\{p - s_1, p - s_2, \cdots, p - s_N, t_1, t_2, \cdots, t_M\right\} = \left\{1, 2, \cdots, \frac{p-1}{2}\right\}.$$

Observe that the set on the left-hand side is a subset of the set on the right hand side. So we only need to prove that the integers in the left-hand side are distinct. This requires to prove $p - s_k \neq t_l$ for any k and l, which is sufficient. By the definition of s_k and t_l, there exist integers $1 \leq j_k, j_l \leq \frac{p-1}{2}$ such that $aj_k \equiv s_k$ and $aj_l \equiv t_l$. Assume that $p - s_k = t_l$, then we have

$$a(j_k + j_l) \equiv s_k + t_l \equiv 0 \pmod{p}.$$

As $(a, p) = 1$, we have $j_k + j_l \equiv 0 \pmod{p}$, which is impossible according to the ranges of j_k and j_l. Thus, our assumption is false, leading to the desired result. Hence,

$$(p - s_1)(p - s_2) \cdots (p - s_N) t_1 \cdots t_M = \left(\frac{p-1}{2}\right)!,$$

which gives

$$r_1 r_2 \cdots r_{\frac{p-1}{2}} = s_1 s_2 \cdots s_N t_1 t_2 \cdots t_M \equiv (-1)^N \left(\frac{p-1}{2}\right)! \pmod{p}$$

This completes our proof. □

Corollary 5.2 (Special value of Legendre's symbol at -2)

For an odd prime p, we have

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

♡

Proof We use Gauss's Lemma to compute $\left(\frac{2}{p}\right)$. Let $S = \{1, 2, \ldots, (p-1)/2\}$, and let μ be the number of integers in S multiplied by 2 that exceed $p/2$. By Gauss's Lemma, we have

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

For each $1 \leq k \leq \frac{p-1}{2}$, consider $2k$. The condition $2k > p/2$ is equivalent to $k > p/4$. It follows that

$$\mu = \left[\frac{p-1}{2}\right] - \left[\frac{p}{4}\right].$$

Observe that:

- If $p \equiv 1 \pmod{8}$, let $p = 8k + 1$ for some integer k, then $\mu = \left[\frac{(8k+1)-1}{2}\right] - \left[\frac{8k+1}{4}\right] = 2k$ is even.

- If $p \equiv 3 \pmod 8$, let $p = 8k+3$ for some integer k, then $\mu = \left[\frac{(8k+3)-1}{2}\right] - \left[\frac{8k+3}{4}\right] = 2k+1$ is odd.
- If $p \equiv 5 \pmod 8$, let $p = 8k+5$ for some integer k, then $\mu = \left[\frac{(8k+5)-1}{2}\right] - \left[\frac{8k+5}{4}\right] = 2k+1$ is odd.
- If $p \equiv 7 \pmod 8$, let $p = 8k+7$ for some integer k, then $\mu = \left[\frac{(8k+7)-1}{2}\right] - \left[\frac{8k+7}{4}\right] = 2k+2$ is even.

These imply that

$$\mu \equiv \frac{p^2-1}{8} \pmod 2,$$

which gives our desired result. □

Lemma 5.2 (Counting lemma for quadratic reciprocity)

Given two distinct odd primes p, q, define N as the number of pairs of integers (j, r) with $1 \le j \le \frac{p-1}{2}$ and $\frac{p}{2} < r < p$ for which $qj \equiv r \pmod p$. Then we have

$$N \equiv \sum_{j=1}^{(p-1)/2} \left[\frac{jq}{p}\right] \pmod 2.$$

♡

Proof For each $1 \le j \le \frac{p-1}{2}$, by division with remainder, we have

$$qj = p\left[\frac{qj}{p}\right] + r_j, \quad 1 \le r_j < p.$$

Under the notations in the proof of the Gauss's lemma, sum up these equations both sides, we obtain

$$q\sum_{j=1}^{(p-1)/2} j = p\sum_{j=1}^{(p-1)/2}\left[\frac{qj}{p}\right] + s_1 + s_2 \cdots + s_N + t_1 + t_2 \cdots + t_M$$

Recall that

$$\left\{p - s_1, p - s_2, \cdots, p - s_N, t_1, t_2, \cdots, t_M\right\} = \left\{1, 2, \cdots, \frac{p-1}{2}\right\}.$$

Then we have

$$\begin{aligned} q\sum_{j=1}^{(p-1)/2} j &= p\sum_{j=1}^{(p-1)/2}\left[\frac{qj}{p}\right] + (p - s_1) + (p - s_2)\cdots(p - s_N) \\ &\quad + t_1 + t_2 \cdots + t_M + 2(s_1 + s_2 \cdots + s_N) - pN \\ &= p\Big(\sum_{j=1}^{(p-1)/2}\left[\frac{qj}{p}\right] - N\Big) + \sum_{j=1}^{(p-1)/2} j + 2(s_1 + s_2 \cdots + s_N). \end{aligned}$$

which gives

$$\frac{(p^2-1)(q-1)}{8} = p\Big(\sum_{j=1}^{(p-1)/2}\left[\frac{qj}{p}\right] - N\Big) + 2(s_1 + s_2 \cdots + s_N).$$

Note that p and q are both odd primes, then we conclude that

$$N \equiv \sum_{j=1}^{(p-1)/2} \left[\frac{qj}{p}\right] \pmod 2,$$

which is our desired result.

Now we are ready to prove the law of quadratic reciprocity. Consider a rectangle whose vertices are at the points $(0,0)$, $(p/2, 0)$, $(0, q/2)$ and $(p/2, q/2)$.

First, let's determine the number of integer points strictly inside this rectangle. The count of these points is

$$\frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Next, consider the diagonal connecting $(0,0)$ to $(p/2, q/2)$, whose equation is $py - qx = 0$. Since p and

q are distinct primes, the only integer lattice point on this diagonal within the rectangular region $0 \le x \le p/2$, $0 \le y \le q/2$ is $(0,0)$. To see this, suppose (x,y) is another integer solution to $py = qx$. By the primality and distinctness of p and q, it follows that q divides y and p divides x. Writing $y = qk$ and $x = p\ell$ for integers k, ℓ, substitution yields $p(qk) = q(pl)$, which gives $k = l$. Thus, all integer solutions are of the form (pl, ql). However, for $l \ge 1$, these points violate the boundary conditions since $pl > p/2$ and $ql > q/2$.

Then, let's compute the number of integer points below this diagonal: For given $x = j$, where $0 < j < (p-1)/2$, the valid range for y is $0 < y < qj/p$. Thus, the number of suitable values of y is $\lfloor qj/p \rfloor$. Summing over j, the total count of lattice points below the diagonal is

$$N = \sum_{j=1}^{(p-1)/2} \left[\frac{qj}{p}\right].$$

Similarly, the number of integer points above the diagonal is equal to

$$N' =: \sum_{j=1}^{(q-1)/2} \left[\frac{pj}{q}\right].$$

Finally, by the relation

$$N + N' = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

and Lemma 5.2, we derive the law of quadratic reciprocity. □

5.5 Jacobi symbol

Definition 5.3

The Jacobi symbol is a generalization of the Legendre symbol. If a is an integer and m is an odd positive integer, then the Jacobi symbol is defined as the product of Legendre symbols for the prime factors of m. Specifically, let $m = p_1 p_2 \cdots p_k$ be the prime factorization of m, where p_i are odd primes (not necessarily distinct). The Jacobi symbol is given by

$$\left(\frac{a}{m}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right),$$

where each $\left(\frac{a}{p_i}\right)$ is the Legendre symbol.

Example 5.6 For example,

$$\left(\frac{2}{45}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = -1.$$

Note *Clearly, when n is a prime, the Jacobi symbol is the Legendre symbol. By definition, the values of the Jacobi symbol can be only -1, 0 or 1. It is clear that $\left(\frac{1}{m}\right) = 1$. Furthermore, if $\gcd(a,m) > 1$, then $\left(\frac{a}{m}\right) = 0$.*

Proposition 5.1 (Periodicity of the Jacobi symbol)

For any positive odd integer m, if $a \equiv b \pmod m$, then $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$.

Proof Let $m = p_1 p_2 \cdots p_k$ be the prime factorization of m, where p_i are odd primes (not necessarily distinct). Since $a \equiv b \pmod m$, it follows that $a \equiv b \pmod{p_i}$ for each i. By the periodicity of the Legendre symbol,

if $a \equiv b \pmod{p_i}$, then $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$. Multiplying over all prime factors of m yields

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right) = \prod_{i=1}^{k} \left(\frac{b}{p_i}\right) = \left(\frac{b}{m}\right),$$

which is our desired result. □

Proposition 5.2 (Multiplicity of the Jacobi symbol)

Let m and n be positive odd integers, and let a and b be any integers. Then

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

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

♠

Proof For property (i), let $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime factorization of m. By the multiplicative property of the Legendre symbol, for each i, we have $\left(\frac{ab}{p_i}\right) = \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)$, which gives $\left(\frac{ab}{p_i}\right)^{k_i} = \left(\frac{a}{p_i}\right)^{k_i}\left(\frac{b}{p_i}\right)^{k_i}$. Multiplying over all prime factors of m gives

$$\left(\frac{ab}{m}\right) = \prod_{i=1}^{r} \left(\frac{ab}{p_i}\right)^{k_i} = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{k_i} \cdot \prod_{i=1}^{r} \left(\frac{b}{p_i}\right)^{k_i} = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right).$$

For property (ii), let $m = \prod_{i=1}^{r} p_i^{k_i}$ and $n = \prod_{j=1}^{s} q_j^{l_j}$. The factorization $mn = \prod_{i=1}^{r} p_i^{k_i} \prod_{j=1}^{s} q_j^{l_j}$ implies

$$\left(\frac{a}{mn}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{k_i} \cdot \prod_{j=1}^{s} \left(\frac{a}{q_j}\right)^{l_j} = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right).$$

This completes the proof of the properties. □

Proposition 5.3 (Special values of Jacobi symbol at -1 and 2)

Let m be a positive odd integer. Then

(i) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.

(ii) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.

♠

Proof For identity (i), let $m = \prod_{i=1}^{k} p_i$ where p_i are odd primes (not necessarily distinct). By the definition of the Jacobi symbol and the property of Legendre symbol, we have

$$\left(\frac{-1}{m}\right) = \prod_{i=1}^{k} \left(\frac{-1}{p_i}\right) = \prod_{i=1}^{k} (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^{k} \frac{p_i-1}{2}}.$$

It suffices to show that

$$\sum_{i=1}^{k} \frac{p_i - 1}{2} \equiv \frac{m-1}{2} \pmod{2}. \tag{5.1}$$

Observe that for each prime p_i, we can write

$$p_i = 1 + 2 \cdot \frac{p_i - 1}{2}.$$

Taking the product over all p_i, we obtain

$$m \equiv \prod_{i=1}^{k} \left(1 + 2 \cdot \frac{p_i - 1}{2}\right) \equiv 1 + 2 \sum_{i=1}^{k} \frac{p_i - 1}{2} \pmod{4},$$

which implies (5.1). This completes the proof of identity (i).

For identity (ii), let $m = \prod_{i=1}^{k} p_i$. Using the Legendre symbol's property, we have

$$\left(\frac{2}{m}\right) = \prod_{i=1}^{k}\left(\frac{2}{p_i}\right) = \prod_{i=1}^{k}(-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum_{i=1}^{k}\frac{p_i^2-1}{8}}.$$

It suffices to show that

$$\sum_{i=1}^{k}\frac{p_i^2-1}{8} \equiv \frac{m^2-1}{8} \pmod 2. \tag{5.2}$$

Note that for any odd integer p, we have $p^2 \equiv 1 \pmod 8$. Therefore

$$m^2 = \prod_{i=1}^{k} p_i^2 \equiv 1 \pmod 8 \quad \text{and} \quad \frac{m^2-1}{8} \in \mathbb{Z}.$$

By expanding

$$m^2 = \prod_{i=1}^{k}(1 + 8\cdot\frac{p_i^2-1}{8})$$

and considering the terms modulo 16, we obtain

$$m^2 \equiv 1 + 8\sum_{i=1}^{k}\frac{p_i^2-1}{8} \pmod{16},$$

which implies (5.2). This completes the proof of identity (ii). □

Proposition 5.4 (Reciprocity Law for the Jacobi Symbol)

Let m, n be positive odd integers, then we have

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

♠

Proof Let $m = \prod_{i=1}^{k} p_i$ and $n = \prod_{j=1}^{\ell} q_j$ be the prime factorizations of m and n respectively (where primes may repeat). By definition of the Jacobi symbol, we have

$$\left(\frac{n}{m}\right) = \prod_{i=1}^{k}\left(\frac{n}{p_i}\right) = \prod_{i=1}^{k}\prod_{j=1}^{\ell}\left(\frac{q_j}{p_i}\right),$$

and

$$\left(\frac{m}{n}\right) = \prod_{j=1}^{\ell}\left(\frac{m}{q_j}\right) = \prod_{j=1}^{\ell}\prod_{i=1}^{k}\left(\frac{p_i}{q_j}\right).$$

For each pair (p_i, q_j), by the reciprocity of quadratic law, we have

$$\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right) = (-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.$$

Thus the product becomes

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

It suffices to show that

$$\sum_{i=1}^{k}\frac{p_i-1}{2} \equiv \frac{m-1}{2} \pmod 2 \quad \text{and} \quad \sum_{j=1}^{\ell}\frac{q_i-1}{2} \equiv \frac{n-1}{2} \pmod 2.$$

This holds because

$$m = \prod_{i=1}^{k} p_i \equiv \prod_{i=1}^{k}(1 + 2\cdot\frac{p_i-1}{2}) \equiv 1 + 2\sum_{i=1}^{k}\frac{p_i-1}{2} \pmod 4,$$

and similarly for n. Therefore

$$\Big(\sum_{i=1}^{k}\frac{p_i-1}{2}\Big)\Big(\sum_{j=1}^{l}\frac{q_j-1}{2}\Big)\equiv\frac{m-1}{2}\cdot\frac{n-1}{2}\pmod 2.$$

Combining all the above steps yields

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

as desired. □

Note *In general, the Jacobi symbol* $\left(\frac{a}{m}\right)=1$ *does not mean that the congruence equation* $x^2\equiv a\pmod m$ *is solvable!*

Example 5.7 The congruence equation $x^2\equiv -1\pmod{49}$ has no solution, but $\left(\frac{-1}{49}\right)=1$.

Problem 5.4 Given an integer a and a large prime p, how can we quickly find a solution to the congruence equation $x^2\equiv a\pmod p$?

Chapter 6 Congruence Equation of Higher Power

6.1 Lagrange's Theorem

Theorem 6.1 (Lagrange's Theorem)

Let p be a prime and $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $d \geq 1$ with leading coefficient not divisible by p, then the algebraic congruence

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

has at most d solutions modulo p. ♡

Proof We proceed by induction on d. The base case $d = 1$ follows from Proposition 4.1. Now assume the result holds for all polynomials of degree $d-1$ with $d > 1$. Suppose $x \equiv a \pmod{p}$ is a solution modulo p, i.e. $f(a) \equiv 0 \pmod{p}$. By polynomial division with remainder, we can write

$$f(x) = q(x)(x-a) + r,$$

where $q(x) \in \mathbb{Z}[x]$ is a polynomial of degree $d-1$ and $r \in \mathbb{Z}$. Substituting $x = a$, we obtain

$$r = f(a) \equiv 0 \pmod{p}.$$

Now let $x \equiv b \pmod{p}$ is any solution modulo p, i.e. $f(b) \equiv 0 \pmod{p}$. Then

$$f(b) \equiv q(b)(b-a) \equiv 0 \pmod{p}.$$

Since p is a prime number, this implies that either $b \equiv a \pmod{p}$ or $q(b) \equiv 0 \pmod{p}$. By the induction hypothesis, the congruence equation $q(x) \equiv 0 \pmod{p}$ has at most $d-1$ solutions modulo p. Including the possibility $b \equiv a \pmod{p}$, the total number of solutions is at most at most $d - 1 + 1 = d$. This completes the induction. □

Example 6.1 For example, all solutions of congruence equation

$$x^3 + x^2 + x + 1 \equiv 0 \pmod{5}$$

are $x \equiv 2, 3, 4$, and the number of all solutions are not greater than 3, the degree of the above polynomial.

6.2 Hensel's Lemma

Theorem 6.2 (Hensel's Lemma)

Let $f(x) \in \mathbb{Z}[x]$, p be a prime and $k \in \mathbb{N}$. Suppose that $x \equiv r \pmod{p^k}$ satisfies

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

with

$$f'(r) \not\equiv 0 \pmod{p}.$$

Then there exists a unique lift $x \equiv s \pmod{p^{k+1}}$ such that

$$f(s) \equiv 0 \pmod{p^{k+1}}$$

and

$$s \equiv r \pmod{p^k}.$$

♡

Proof Existence: We seek for an integer t such that $s = r + tp^k$ satisfies

$$f(s) \equiv 0 \pmod{p^{k+1}}. \tag{6.1}$$

By Taylor expansion (since f is polynomial), we have

$$f(r + tp^k) = f(r) + f'(r)tp^k + \text{higher-order terms in } p^{k+1}.$$

Since $f(r) \equiv 0 \pmod{p^k}$, we write $f(r) = up^k$ for some $u \in \mathbb{Z}$. The condition $f(s) \equiv 0 \pmod{p^{k+1}}$ reduces to

$$up^k + f'(r)tp^k \equiv 0 \pmod{p^{k+1}}.$$

Dividing by p^k, we obtain

$$u + f'(r)t \equiv 0 \pmod{p}.$$

By hypothesis, $f'(r)$ is invertible modulo p , this has a unique solution t, proving the existence of s.

Uniqueness: Suppose s_1 and s_2 both satisfy $f(s_i) \equiv 0 \pmod{p^{k+1}}$ and $s_i \equiv r \pmod{p^k}$ $(i = 1, 2)$. Write $s_1 = r + t_1p^k$ and $s_2 = r + t_2p^k$. Then,

$$f(s_1) - f(s_2) \equiv f'(r)(t_1 - t_2)p^k \pmod{p^{k+1}}.$$

Since $f(s_1) \equiv f(s_2) \equiv 0 \pmod{p^{k+1}}$, we have

$$f'(r)(t_1 - t_2)p^k \equiv 0 \pmod{p^{k+1}}.$$

Dividing by p^k, we obtain

$$f'(r)(t_1 - t_2) \equiv 0 \pmod{p}.$$

But $f'(r) \not\equiv 0 \pmod{p}$, so $t_1 \equiv t_2 \pmod{p}$, implying $s_1 \equiv s_2 \pmod{p^{k+1}}$. □

Example 6.2 Let's consider the congruence equation

$$f(x) = x^2 - 2 \equiv 0 \pmod{7^2}. \tag{6.2}$$

We start by choosing an initial solution $x \equiv 3 \pmod{7}$ to

$$f(x) = x^2 - 2 \equiv 0 \pmod{7}.$$

Now we will show how to lift this solution to a solution of the above congruence equation modulo 7^2.

Note that $f'(x) = 2\dot{x}$ and $f'(3) = 6 \not\equiv 0 \pmod{7}$. According to the above proof of Hensel's lemma, we

need to find an integer t such that

$$f(3+t\cdot 7)=(3+t\cdot 7)^2-2\equiv 0 \pmod{7^2}.$$

Unfolding the square, this congruence equation is equivalent to

$$9+2\cdot 3\cdot 7\cdot t-2\equiv 0 \pmod{7^2},$$

which simplifies to

$$1+6t\equiv 0 \pmod{7}.$$

Solving this congruence equation, we obtain

$$t\equiv 1 \pmod{7}.$$

Therefore, $x\equiv 3+1\cdot 7\equiv 10 \pmod{7^2}$ is a solution to (6.2).

✍ **Exercise 6.1** Please lift the solution $x\equiv 10 \pmod{7^2}$ to (6.2) and find a solution to the congruence equation $x^2-2\equiv 0 \pmod{7^3}$.