Number Theory I

Bojue Wang

July 25, 2025

Contents

1 Introduction

Number theory is, at its most basic level, the study of the properties of the integers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

or the natural numbers

$$\mathbb{N} = \{0, 1, 2, \dots\}.$$

In some ways, it is the most fundamental piece of mathematics: one can build virtually everything else from the natural numbers via

$$\mathbb{N} \xrightarrow{\text{negation}} \mathbb{Z} \xrightarrow{\text{division}} \mathbb{Q} \xrightarrow{\text{Dedekind cut}} \mathbb{R} \xrightarrow{\text{adjoin } \sqrt{-1}} \mathbb{C},$$

and from there to calculus, topology, etc.

1.1 Classification of Number Theory

Number theory can be divided into several interrelated branches:

- *Elementary/Combinatorial* Number Theory: basic divisibility, congruences, Pell's equation, etc.
- *Analytic* Number Theory: distribution of primes, zeta and L-functions.
- *Algebraic* Number Theory: arithmetic of algebraic number fields, class groups, units.
- *Geometric* Number Theory: geometry of numbers, lattices, Diophantine approximation.
- *Computational* Number Theory: algorithms for primality testing, integer factorization, cryptography.

2 Diophantine Equations

Given an equation, one seeks integer solutions. Classic examples include:

$$a^2 + b^2 = c^2,$$

yielding Pythagorean triples $(3, 4, 5), (5, 12, 13), \dots$. Generalizations lead to Fermat's Last Theorem

$$a^n + b^n = c^n, \quad n > 2,$$

and to open problems such as the existence of a perfect cuboid, where all of

$$a^2 + b^2 + c^2,\ a^2 + b^2,\ a^2 + c^2,\ b^2 + c^2$$

are perfect squares.

Remark 2.1. Try to write a complete generating function for Pythagorean triples.

3 Basic Properties of N

3.1 Successor Operation

$$s(n) = n + 1.$$

Addition is repeated *successor*, and **multiplication** is repeated *addition*, **exponential** is repeated *multiplication*.

3.2 Principle of Mathematical Induction

If a property $P(n)$ satisfies:

(i) $P(1)$ is true,

(ii) $P(n) \implies P(n+1)$ for all n,

then $P(n)$ holds for all $n \in \mathbb{N}$.

3.3 Well–Ordering Principle

Every nonempty subset of $\mathbb{N}$ has a least element.

Remark 3.1. PMI and WOP are equivalent (each implies the other).

3.4 Divisibility

Definition 3.1. For $a, b \in \mathbb{Z}$, $a \neq 0$, we say $a \mid b$ if there exists $x \in \mathbb{Z}$ such that $b = ax$.

Basic facts:

(i) For all $n \in \mathbb{N}$, $n \mid 0$.

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

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

Theorem 3.1 (Division Algorithm of $\mathbb{Z}$)**.** Given $a, b \in \mathbb{Z}$ with $a > 0$, there exist unique $q, r \in \mathbb{Z}$ such that

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

Proof. Let

$$S = \{\, b + ka : k \in \mathbb{Z},\, b + ka \geq 0\}.$$

By choosing k large/small, S is nonempty, so by WOP it has a least element $r = b + ka$. Set $q = -k$. Then $r \geq 0$ and if $r \geq a$, then $b + (k-1)a < r$ would lie in S, contradicting minimality. □

Definition 3.2. If a, b are not both zero, the *greatest common divisor* $\gcd(a, b)$, denoted (a, b), is the largest positive integer dividing both.

Remark 3.2. By convention, use (a, b) to denote the greatest common divisor of a, b; $[a, b]$ to denote the least common multiple of a, b; furthermore, there is a relation

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

[Hint: use fundamental theorem of Arithmetic to prove it.]

Theorem 3.2 (Bézout's Identity/Expansion)**.** Let $g = \gcd(a, b)$. Then there exist $x_0, y_0 \in \mathbb{Z}$ such that

$$g = ax_0 + by_0.$$

Proof. Consider

$$S = \{\, ax + by : x, y \in \mathbb{Z},\ ax + by > 0\}.$$

By WOP S has a minimal element g. One shows $g \mid a$ and $g \mid b$ by the division algorithm and minimality, and that any common divisor of a, b must divide g. □

Remark 3.3. The motivation of Bézout's theorem is to try to figure out the coordinates of gcd under the basis of components. If the gcd is not 1, then essentially, we can factor out the constant such that the reduced components are coprime. So we can just consider the case of coprime components. Coprime has similarity to independence in linear algebra, so it can serve as basis for the unity element 1.

Remark 3.4. The positive minimal element of $\{ax + by | x, y \in \mathbb{Z}\}$ is $\gcd(a, b)$.

Remark 3.5. The **Bezout's coefficients** (the coordinate of 1 under the basis of components) is not unique since there is perturbation term affected each of the coordinates, but there is a unique *principal* Bezout's coefficients formed by Euclidean algorithm.

Definition 3.3. a and b are *coprime* if $\gcd(a, b) = 1$.

Proposition 1.

(a) If $\gcd(a, m) = \gcd(b, m) = 1$, then $\gcd(ab, m) = 1$.

(b) If $c \mid ab$ and $\gcd(c, a) = 1$, then $c \mid b$.

(c) $(1, a) = 1$, and $(0, b) = |b|$.

3.5 The Euclidean Algorithm

(i) If $a < 0$ or $b < 0$, replace (a, b) with $(|a|, |b|)$.

(ii) If $a > b$, swap the values so that $a \leq b$.

(iii) If $a = 0$, $\gcd(a, b) = b$; terminate.

(iv) Otherwise write

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

then replace (a, b) with (r, a) and return to step (ii).

Theorem 3.3. The above algorithm terminates after finitely many steps and correctly computes $\gcd(a, b)$.

Proof. At each iteration we replace (a, b) by (r, a) with $0 \leq r < a$. Hence the first entry strictly decreases in the well-ordered set $\mathbb{N}$, so the process cannot continue indefinitely and must eventually reach the case $a = 0$.

To see correctness, observe that when $b = a\,q + r$, any common divisor of a and b also divides

$$b - a\,q = r,$$

and conversely any common divisor of a and r divides b. Hence

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

Upon termination we have $a = 0$ and so $\gcd(a, b) = b$, which by the above equality is the same as the original gcd. □

Remark 3.6. Bézout's theorem and Euclidean algorithm provide a pattern of coordinate calculation.

Example 3.1. Compute $\gcd(252, 105)$:

$$\begin{aligned} 252 &= 105 \cdot 2 + 42, \\ 105 &= 42 \cdot 2 + 21, \\ 42 &= 21 \cdot 2 + 0. \end{aligned}$$

Since the last nonzero remainder is 21, we conclude $\gcd(252, 105) = 21$.

3.6 Generalization of Bezout's Identity

For (a, b), there is a Bezout's expansion

$$(a, b) = ax + by.$$

What about $(a_1, ..., a_n)$? Is there an expansion $(a_1, ..., a_n) = a_1x_1 + \cdots + a_nx_n$? Try to prove it. [Hint: the operation of gcd satisfies the property of *meet* in a structure called **lattice**.]

4 Primes and the Fundamental Theorem

Definition 4.1. A *prime* p is an integer > 1 whose only positive divisors are 1 and p.

Theorem 4.1 (Fundamental Theorem of Arithmetic)**.** Every integer $n > 1$ can be represented uniquely (up to ordering) as a product of primes.

Sketch of existence. Let S be numbers not expressible as prime products; by WOP let n be its least element. Then $n = ab$ with $1 < a, b < n$, each of which factors into primes, so n does too—a contradiction. □

Sketch of uniqueness. Use the fact that if a prime $p \mid ab$ then $p \mid a$ or $p \mid b$, and argue by cancellation and minimal counterexample. □

Theorem 4.2 (Euclid)**.** There are infinitely many primes.

Proof. Assume finitely many $p_1, \ldots, p_n$; consider $N = p_1 \cdots p_n + 1$. Any prime divisor of N is new, contradiction. □

Theorem 4.3 (Euler)**.** The sum of reciprocals of the primes diverges, hence there are infinitely many.

Sketch. Expand the Euler product for the Riemann zeta function at $s = 1$ and observe divergence. □

4.1 Famous Conjectures

Conjecture 1 (Goldbach's Conjecture)**.** Every even integer > 2 is the sum of two primes.

Conjecture 2 (Twin Prime Conjecture)**.** Infinitely many primes p with $p + 2$ also prime.

Conjecture 3 (Mersenne Primes)**.** Primes of the form $2^n - 1$; conjecturally infinitely many.

5 Lattice Structure

Recall the definition of an algebraic structure called a lattice, i.e.

Definition 5.1 (Lattice — order-theoretic)**.** A *lattice* is a partially ordered set $(L, \leq)$ such that for every pair of elements $x, y \in L$:

- The *meet* (greatest lower bound) $x \wedge y = \inf\{x, y\}$ exists in L.
- The *join* (least upper bound) $x \vee y = \sup\{x, y\}$ exists in L.

Definition 5.2 (Lattice — algebraic)**.** Equivalently, a lattice can be given as an algebraic structure $(L, \wedge, \vee)$ satisfying, for all $x, y, z \in L$:

(i) **Commutativity:**

$$x \wedge y = y \wedge x, \quad x \vee y = y \vee x.$$

(ii) **Associativity:**

$$(x \wedge y) \wedge z = x \wedge (y \wedge z), \quad (x \vee y) \vee z = x \vee (y \vee z).$$

(iii) **Absorption:**

$$x \wedge (x \vee y) = x, \quad x \vee (x \wedge y) = x.$$

(iv) **Idempotence:**

$$x \wedge x = x, \quad x \vee x = x.$$

Proposition 2. The order-theoretic and algebraic definitions of a lattice are equivalent.

Proposition 3. $(\mathbb{Z}, \gcd, \operatorname{lcm})$ is a lattice but is not a complete lattice.

Proof. (1) *lattice structure.* For any two integers a, b, define

$$a \wedge b := \gcd(a, b), \qquad a \vee b := \operatorname{lcm}(a, b).$$

We must check these satisfy the meet/join axioms:

- (gcd is greatest lower bound)
  - (i) $\gcd(a, b)$ divides both a and b, so $\gcd(a, b) \leq a$ and $\gcd(a, b) \leq b$ in the divisibility order.
  - (ii) If d divides both a and b, then d also divides $\gcd(a, b)$. Hence $\gcd(a, b)$ is the greatest such divisor.
- (lcm is least upper bound)
  - (i) Both a and b divide $\operatorname{lcm}(a, b)$.
  - (ii) If m is any integer divisible by both a and b, then $\operatorname{lcm}(a, b)$ divides m. Hence $\operatorname{lcm}(a, b)$ is the least such multiple.

Thus $\big(\mathbb{Z},\ |\ \big)$ is a lattice with meet gcd and join lcm.

(2) *Not complete.* Completeness would require that *every* subset $S \subset \mathbb{Z}$ (possibly infinite) has both a gcd-style meet $\bigwedge S$ and an lcm-style join $\bigvee S$ in $\mathbb{Z}$. But:

$$S = \{2, 3, 5, 7, 11, \dots\}$$

the set of all primes, has no least common multiple in $\mathbb{Z}$: any common multiple must be divisible by *infinitely* many distinct primes, hence is not a (finite) integer. Therefore $\bigvee S \notin \mathbb{Z}$, and completeness fails.

□

Definition 5.3. A subset $L \subset \mathbb{R}^n$ is called a *lattice* if any (hence all) of the following equivalent conditions hold:

(i) L is a discrete subgroup of $(\mathbb{R}^n, +)$ that spans $\mathbb{R}^n$ as a real vector space.

(ii) L is a free $\mathbb{Z}$-module of rank n and

$$L \otimes_{\mathbb{Z}} \mathbb{R} \;=\; \mathbb{R}^n.$$

(iii) There exist $\mathbb{R}$-linearly independent vectors $v_1, \dots, v_n \in \mathbb{R}^n$ such that

$$L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n.$$

Proposition 4. The subgroup $(\mathbb{Z}^2, +) \subset (\mathbb{R}^2, +)$ is a (geometric) lattice in $\mathbb{R}^2$.

Proof. Here "lattice" means a *discrete* subgroup of full rank in a real vector space.

(1) *Subgroup of full rank.* $\mathbb{Z}^2$ is generated (over $\mathbb{Z}$) by the two $\mathbb{R}$-linearly independent vectors

$$e_1 = (1, 0), \quad e_2 = (0, 1).$$

Hence it spans $\mathbb{R}^2$ over $\mathbb{R}$.

(2) *Discreteness.* $\mathbb{Z}^2$ is discrete in $\mathbb{R}^2$ because there is a neighborhood of the origin, say the open ball of radius $1/2$, which contains no nonzero lattice points. More formally:

$$\forall\, 0 \neq v \in \mathbb{Z}^2, \quad \|v\| \geq 1,$$

so only the origin lies in the $\frac{1}{2}$-ball.

A discrete full–rank subgroup of $\mathbb{R}^2$ is by definition a (geometric) lattice. □

Proof. Recall that a *lattice* in $\mathbb{R}^n$ is a subgroup $L \subset \mathbb{R}^n$ such that

(i) L is a free $\mathbb{Z}$-module of rank n,

(ii) L spans $\mathbb{R}^n$ over $\mathbb{R}$,

(iii) L is discrete in the usual topology of $\mathbb{R}^n$.

Let

$$e_1 = (1, 0), \quad e_2 = (0, 1).$$

(i) Every element of $\mathbb{Z}^2$ can be uniquely written as $k_1 e_1 + k_2 e_2$ with $k_1, k_2 \in \mathbb{Z}$, so $\{e_1, e_2\}$ is a $\mathbb{Z}$-basis.

(ii) Over $\mathbb{R}$ the same two vectors span $\mathbb{R}^2$, since any $(x, y) \in \mathbb{R}^2$ is $x\, e_1 + y\, e_2$.

(iii) To see discreteness, note that the distance between any two distinct points of $\mathbb{Z}^2$ is at least 1, so there is an open neighborhood around each lattice point containing no other lattice points.

Hence $\mathbb{Z}^2$ is a discrete, full-rank $\mathbb{Z}$-module in $\mathbb{R}^2$, i.e. a lattice. $\square$

6 Modulo Arithmetic

Definition 6.1 (Complete Residue System)**.** A *complete residue system* modulo m is a collection of integers

$$a_1, a_2, \ldots, a_m$$

such that

(i) $a_i \not\equiv a_j \pmod{m}$ for $i \neq j$, and

(ii) every integer n is congruent to some a_i modulo m.

Definition 6.2 (Reduced Residue System)**.** A *reduced residue system* modulo m is a collection of integers

$$a_1, a_2, \ldots, a_k$$

such that

(i) $a_i \not\equiv a_j \pmod{m}$ for $i \neq j$,

(ii) $\gcd(a_i, m) = 1$ for all i, and

(iii) every integer n with $\gcd(n, m) = 1$ is congruent to some a_i modulo m.

Example 6.1. Let $m = 12$. A complete residue system is

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\},$$

and a reduced residue system is

$$\{1, 5, 7, 11\}.$$

Definition 6.3 (Euler's Totient Function)**.** The number of elements in a reduced residue system modulo m is called *Euler's totient function*, denoted $\phi(m)$. Equivalently,

$$\phi(m) = \big|\{\, 1 \leq k \leq m : \gcd(k, m) = 1\}\big|.$$

Theorem 6.1 (Euler's Theorem)**.** If $\gcd(a, m) = 1$, then

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

Proof.

Lemma 1. If $\gcd(a, m) = 1$ and $r_1, \ldots, r_k$ is a reduced residue system mod m, where $k = \phi(m)$, then

$$ar_1,\ ar_2,\ \ldots,\ ar_k$$

is also a reduced residue system mod m.

Proof. Since $\gcd(r_i, m) = 1$ and $\gcd(a, m) = 1$, we have $\gcd(ar_i, m) = 1$ for each i. If

$$ar_i \equiv ar_j \pmod{m},$$

then $m \mid a(r_i - r_j)$. Because $\gcd(a, m) = 1$, it follows that $m \mid (r_i - r_j)$, so $r_i \equiv r_j \pmod{m}$, and hence $i = j$. Thus the ar_i are distinct mod m. □

Now, let $r_1, \ldots, r_k$ be a reduced residue system mod m.

$$ar_1, \ldots, ar_k$$

is a permutation of $r_1, \ldots, r_k$ modulo m. Hence

$$r_1 r_2 \cdots r_k \equiv (ar_1)(ar_2) \cdots (ar_k) = a^k (r_1 r_2 \cdots r_k) \pmod{m}.$$

Since $\gcd(r_1 \cdots r_k, m) = 1$, we can cancel $r_1 \cdots r_k$ to obtain

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

□

Corollary 1 (Fermat's Little Theorem)**.** For any prime p and integer a,

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

Proof. If $p \nmid a$, then $\phi(p) = p-1$ and Euler's Theorem gives $a^{p-1} \equiv 1 \pmod{p}$, hence $a^p \equiv a \pmod{p}$. If $p \mid a$, both sides are $0 \pmod{p}$. □

Lemma 2 (Freshman's Dream)**.** For a prime p and integers x, y,

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

Proof. By the Binomial Theorem,

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^p,$$

and for $1 \le k \le p-1$, $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$ is divisible by p. □

Proposition 5 (Inverses mod m)**.** If $\gcd(a, m) = 1$, then there is a unique integer b modulo m such that

$$ab \equiv 1 \pmod{m}.$$

This integer is denoted $a^{-1} \pmod{m}$.

Existence. Since $\gcd(a, m) = 1$, Bézout's identity gives $ax + my = 1$ for some $x, y \in \mathbb{Z}$, whence $ax \equiv 1 \pmod{m}$. Take $b = x$. □

Uniqueness. If b_1, b_2 both satisfy $ab_i \equiv 1 \pmod{m}$, then $a(b_1 - b_2) \equiv 0 \pmod{m}$. Since $\gcd(a, m) = 1$, it follows $b_1 \equiv b_2 \pmod{m}$. □

Theorem 6.2 (Wilson's Theorem)**.** For a prime p,

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

Proof. For odd p, the only solutions to $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1$. In the product

$$1 \cdot 2 \cdots (p-1),$$

pair each $a \not\equiv \pm 1$ with its inverse $a^{-1} \neq a$, leaving only 1 and $p-1$ unpaired, so

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

□

Theorem 6.3. The congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

Proof. If $p \equiv 3 \pmod{4}$ and $x^2 \equiv -1$, then raising both sides to the $(p-1)/2$ power gives $1 \equiv -1 \pmod{p}$, impossible. If $p \equiv 1 \pmod{4}$, one shows via Wilson's theorem that $x = \big((p-1)/2\big)!$ satisfies $x^2 \equiv -1 \pmod{p}$. □

Theorem 6.4. There are infinitely many primes of the form $4k+1$.

Proof. Analogous to Euclid's proof: assume $p_1, \ldots, p_n$ are all the primes $\equiv 1 \pmod{4}$. Consider

$$N = \big(2p_1 p_2 \cdots p_n\big)^2 + 1.$$

Any prime divisor q of N satisfies $q \equiv 1 \pmod{4}$, contradicting completeness. □

The Möbius function $\mu(n)$ is defined as:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is divisible by a square prime}, \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes}. \end{cases}$$

6.1 Properties of Totient Function

- **Product formula.**

$$n = \prod_{i=1}^{r} p_i^{e_i} \quad \Longrightarrow \quad \phi(n) \;=\; n \prod_{i=1}^{r} \Big(1 - \tfrac{1}{p_i}\Big) \;=\; \prod_{i=1}^{r} \big(p_i^{e_i} - p_i^{e_i - 1}\big).$$

  Proof. An integer $1 \le k \le n$ fails to be coprime to n exactly when it is divisible by at least one prime p_i. By inclusion–exclusion, the count of those not divisible by any p_i is

$$n \;-\; \sum_{i} \frac{n}{p_i} \;+\; \sum_{i<j} \frac{n}{p_i p_j} \;-\; \cdots \;+\; (-1)^r \frac{n}{p_1 \cdots p_r} \;=\; n \prod_{i=1}^{r} \Big(1 - \tfrac{1}{p_i}\Big).$$

  Factoring each term $p_i^{e_i}\big(1 - 1/p_i\big) = p_i^{e_i} - p_i^{e_i - 1}$ gives the alternate form. □

- **Sum over divisors.**

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

Proof. Partition the set $\{1, 2, \ldots, n\}$ by $\gcd(k, n) = d$. For each divisor d of n, there are $\phi(n/d)$ integers k with $\gcd(k, n) = d$. Hence

$$n \;=\; \sum_{d|n} \phi\big(n/d\big) \;=\; \sum_{d|n} \phi(d).$$

□

- **Möbius inversion.**

$$\phi(n) = \sum_{d|n} \mu(d)\, \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Proof. From $\sum_{d|n} \phi(d) = n$, apply the Möbius inversion formula:

$$\phi(n) = \sum_{d|n} \mu(d)\, \big(\sum_{e|(n/d)} \phi(e) \big) = \sum_{d|n} \mu(d)\, \tfrac{n}{d}.$$

□

- **Parity.** For $n > 2$, $\phi(n)$ is even.

Proof. If $n > 2$, then among the $\phi(n)$ units mod n, each a with $a \neq a^{-1}$ pairs off with its inverse. The only fixed points $a = a^{-1}$ satisfy $a^2 \equiv 1 \pmod{n}$, i.e. $a \equiv \pm 1$, giving at most two. Hence $\phi(n) - 2$ is even, so $\phi(n)$ itself is even. □

- **Bounds.** For $n > 1, n \neq 2, 6$,

$$\sqrt{n} \;\leq\; \phi(n) \;\leq\; n - 1.$$

Remark 6.1. The proof is from HW5.

- **Average order.**

$$\sum_{k \leq x} \phi(k) \sim \frac{3}{\pi^2}\, x^2.$$

Sketch. One shows $\sum_{k \leq x} \phi(k) = \sum_{d \leq x} d \sum_{\substack{k \leq x \\ d|k}} \mu(k/d) = \sum_{d \leq x} d\big(\frac{x}{d} + O(1)\big)\mu * 1(1) = \frac{3}{\pi^2} x^2 + O(x \log x)$. □

- **Group-theoretic interpretation.** $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Proof. By definition, $(\mathbb{Z}/n)^\times$ is the set of residue classes invertible mod n, which are exactly those coprime to n. □

7 A Glimpse on Chinese Remainder Theorem

A linear congruence

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

has a solution if and only if $g = \gcd(a, m)$ divides b. We distinguish two cases:

Case 1 $\gcd(a, m) = 1$

Then a is invertible mod m. Find integers x_0, y_0 such that

$$ax_0 + my_0 = 1$$

via the Euclidean Algorithm. Then $ax_0 \equiv 1 \pmod{m}$, so $x_0 = a^{-1}$, and

$$x \equiv a^{-1}b = x_0\, b \pmod{m}$$

is the unique solution mod m.

Case 2 $\gcd(a, m) = g > 1$

- If $g \nmid b$, there is no solution.
- If $g \mid b$, write

$$a = ga', \quad b = gb', \quad m = gm'.$$

Then the congruence becomes

$$a'x \equiv b' \pmod{m'},$$

where $\gcd(a', m') = 1$. By Case 1, there is a unique solution x mod m'. All solutions mod m are then

$$x + k\, m', \quad k = 0, 1, \ldots, g - 1,$$

giving g distinct solutions mod m.

Remark 7.1. Intrinsically, we can directly assume a, m coprime, since otherwise, we can factor out their gcd then investigate the principal pair of components, which is coprime, denoted by (a_0, m_0).

Example 7.1. Solve $35x \equiv 14 \pmod{28}$. Here $\gcd(35, 28) = 7$. Divide by 7:

$$5x \equiv 2 \pmod{4} \implies x \equiv 2 \pmod{4}.$$

Thus the solutions mod 28 are

$$x \equiv 2,\ 6,\ 10,\ 14,\ 18,\ 22,\ 26 \pmod{28}.$$

7.1 Chinese Remainder Theorem

Consider the system

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \quad \vdots \\ x \equiv a_k \pmod{m_k}. \end{cases}$$

Compatibility/consistency is not guaranteed in general (e.g. $x \equiv 3 \pmod 8$ and $x \equiv 1 \pmod{12}$).

But we have the following conclusion:

Theorem 7.1 (Chinese Remainder Theorem)**.** If the moduli $m_1, \ldots, m_k$ are pairwise coprime, then the system has a unique solution modulo $M = m_1 m_2 \cdots m_k$.

Uniqueness. If x and y both satisfy all congruences, then $m_i \mid (x - y)$ for each i. Since the m_i are pairwise coprime, their product M divides $x - y$, so $x \equiv y \pmod M$. □

Existence. Define **auxiliary indices**

$$A_i = \frac{M}{m_i}, \quad \text{and choose } B_i \text{ such that } B_i A_i \equiv 1 \pmod{m_i},$$

where B_i is the **Bézout's coefficient** of A_i.

Then set

$$C_i = A_i B_i,$$

so that $C_i \equiv 1 \pmod{m_i}$ and $C_i \equiv 0 \pmod{m_j}$ for $j \neq i$. The solution is

$$x \;=\; \sum_{i=1}^{k} C_i \, a_i \;\equiv\; a_i \pmod{m_i} \quad \text{for each } i.$$

□

Remark 7.2. From the statement of Chinese remainder theorem, we only know there is unique solution, but we have no idea about the algorithm to figure out the solution. Actually, the proof of a theorem contains much more information than the plain statement of theorem, since within the proof, there are concrete constructions to achieve the conclusion regularly, so try not skip the proof when we are studying new stuffs.

Remark 7.3. From the proof of Chinese remainder theorem, in the step to calculate B_i, which is the Bézout's coefficient of A_i, computationally, we can construct an intermediate index, which is called **reduced auxiliary index**, denoted by R_i, and $R_i = (A_i)_{m_i}$, where $(A_i)_{m_i}$ is the integer in interval $[-\frac{m_i}{2}, \frac{m_i}{2})$ congruent to $A_i \mod m_i$.

Example 7.2. Solve

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

Here $M = 105$. Compute

$$N_1 = 35 \equiv 2 \pmod 3,\ H_1 = 2, \quad N_2 = 21 \equiv 1 \pmod 5,\ H_2 = 1, \quad N_3 = 15 \equiv 1 \pmod 7,\ H_3 = 1.$$

Thus

$$x = 2 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 3 + 1 \cdot 15 \cdot 5 \equiv 278 \equiv 68 \pmod{105}.$$

7.2 Solving System of Normalized Linear Congruence Equations

Suppose there is a system

$$\{x = b_i \mod m_i : i = 1, 2, ..., k\},$$

then the general steps to solve it follows:

Step 1 Set **modulo index** $M = m_1 \cdots m_k$, **auxiliary indices** $A_i = \frac{M}{m_i}$

Step 2 Since $(A_i, m_i) = 1$, then find the **Bézout's coefficient** of A_i, denoted by B_i

Step 3 Construct the general solution $x = b_1(A_1B_1) + \cdots + b_k(A_kB_k) \mod M$, which is unique (guaranteed by Chinese Remainder Theorem)

7.3 Solving System of Linear Congruence Equations

Consider linear congruence system $\{a_i x = b_i \mod m_i\}$, and suppose it is compatible, then we can simplify it by

$$\{a_{i0}x = b_{i0} \mod m_{i0}\},$$

such that $(a_{i0}, m_{i0}) = 1$. Therefore, there is multiplicative inverse of $a_{i0} \mod m_{i0}$, so we simplify the original system to the normalized system.

8 Primality Testing

Given n, we wish to determine if it is prime or composite. An algorithm is *efficient* if it runs in time polynomial in the input size, i.e. polynomial in $\log n$.

8.1 Square Root Test

Let n be a positive integer. Compute the integer part of $\sqrt{n}$, denoted by $\lfloor \sqrt{n} \rfloor$. Then test all prime numbers p with $p \leq \lfloor \sqrt{n} \rfloor$.

- If there exists a prime divisor $p \leq \lfloor \sqrt{n} \rfloor$ such that $p \mid n$, then n is composite.
- **If no such prime divisor exists, then n is prime.**

8.2 Fermat's Little Theorem Test

If n is prime and $\gcd(a, n) = 1$, then

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

(i) Choose $a \in \{2, \ldots, n-1\}$.

(ii) If $\gcd(a, n) > 1$, then n is composite.

(iii) Otherwise compute $a^{n-1} \bmod n$. If $\not\equiv 1$, then n is composite; if $\equiv 1$, the test is *inconclusive*.

8.3 Factorization Techniques

The naive trial division runs in time $O(\sqrt{n})$. More advanced methods include:

- **Pollard's Rho:** iterate $x_{k+1} = f(x_k) \bmod n$, e.g. $f(x) = x^2 + 1$. Use Floyd's cycle detection and take $\gcd(x_i - x_j, n)$ to find small factors in expected $O(\sqrt{p})$ time where p is the smallest prime divisor.
- **Elliptic Curve Factorization:** heuristic $\exp(O(\sqrt{\log p \log \log p}))$ time.
- **Number Field Sieve:** currently the fastest for large n, runtime

$$\exp\big((c + o(1))(\log n)^{1/3}(\log \log n)^{2/3}\big)$$

.

8.4 RSA Cryptography

(i) Choose large primes p, q and set $N = pq$. Compute $\phi(N) = (p-1)(q-1)$.

(ii) Choose e with $\gcd(e, \phi(N)) = 1$ and compute $d \equiv e^{-1} \pmod{\phi(N)}$.

(iii) Public key: (N, e); private key: d.

(iv) Encryption: $c \equiv m^e \pmod{N}$, Decryption: $m \equiv c^d \pmod{N}$.

Example 8.1. Security relies on the hardness of factoring N.

(a) Choose primes $p = 61$, $q = 53$, compute $N = pq = 3233$ and $\phi(N) = (p-1)(q-1) = 3120$.

(b) Choose public exponent $e = 17$, since $\gcd(17, 3120) = 1$, then compute private exponent $d \equiv 17^{-1} \pmod{3120} = 2753$.

(c) **Public key:** $(N, e) = (3233, 17)$; **Private key:** $d = 2753$.

(d) **Example Encryption:** let message $m = 65$. Compute

$$c \equiv m^e \;=\; 65^{17} \mod 3233 = 2790.$$

(e) **Example Decryption:** recover

$$m \equiv c^d \;=\; 2790^{2753} \mod 3233 = 65.$$

9 Congruent Equations

9.1 Exponential Modulo

Modular exponentiation refers to the process of computing

$$a^b \mod m$$

where a, b, m are integers with $m > 0$.

Key points:

- The goal is to find the remainder when a^b is divided by m, without directly computing the potentially huge number a^b.
- Modular exponentiation is fundamental in number theory, cryptography (e.g., RSA encryption), and computational algorithms.
- Efficient computation methods such as **binary exponentiation** (also called exponentiation by squaring) are used to compute $a^b \mod m$ in $O(\log b)$ time.
- Euler's theorem and Fermat's little theorem are useful tools in the simplification process of modular exponentiation.

Basic properties:

- $(a \cdot b) \bmod m = [(a \bmod m) \cdot (b \bmod m)] \bmod m$
- Therefore,
$$a^b \bmod m = \left((a^{b_1} \bmod m) \cdot (a^{b_2} \bmod m) \cdots\right) \bmod m,$$
where the exponent b can be decomposed as $b = b_1 + b_2 + \cdots$.

Algorithm (Binary Exponentiation):

- Express b in binary: $b = \sum_{i=0}^{k} b_i 2^i$, with each $b_i \in \{0, 1\}$.
- Initialize result $= 1$, base $= a \bmod m$.
- For each bit b_i from least significant to most significant:
  - If $b_i = 1$, update result $\leftarrow$ (result $\times$ base) $\bmod m$.
  - Update base $\leftarrow$ (base $\times$ base) $\bmod m$.
- Return result.

Applications:

- Cryptography: Secure key exchange, encryption, digital signatures.
- Primality testing algorithms (e.g., Fermat, Miller-Rabin tests).
- Computing powers in modular arithmetic systems.

9.2 Congruence Systems

Definition 9.1 (Congruence)**.** A *congruence* of degree n is an equation

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0 \mod m,$$

where $a_i \in \mathbb{Z}$. Solutions are integers (or residue classes) satisfying the congruence.

Remark 9.1. Concisely, we use notation

$$f(t) \in \mathbb{Z}[t]$$

to denote the meaning $f(t)$ is a polynomial in variable t with coefficients in integers.

Remark 9.2. For $f(t) \in \mathbb{Z}[t]$,

$$f(t) = 0 \mod m$$

is a congruence of degree $\deg f$.

Definition 9.2 (Linear Congruence)**.** A *linear congruence* has the form

$$ax = b \mod m.$$

Theorem 9.1. Let $g = \gcd(a, m)$. The congruence $ax = b \mod m$ has a solution if and only if $g \mid b$. In that case, there are exactly g solutions modulo m.

Proof. Write $a = a_0 g$, $m = m_0 g$ with $\gcd(a_0, m_0) = 1$. If $ax = b$, then $g \mid b$. Conversely, if $b = b_0 g$, Bézout gives $a_0 x_0 + m_0 y_0 = 1$, so

$$a(b_0 x_0) = b \mod m.$$

Distinct solutions differ by multiples of m_0, yielding exactly g residue classes. □

Remark 9.3. For linear congruence $ax = b \mod m$, if $d = (a, m)$ divides b, then $ax = b \mod m$ is equivalent to $a_0 x = b_0 \mod m_0$, where $(-)_0 = \frac{(-)}{d}$ here.

9.3 Solution of Polynomial Congruence

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \mod m, \quad a_i \in \mathbb{Z}.$$

Write the factorization of m as

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

By the CRT, solving the congruence modulo m is equivalent to solving it modulo each prime power $p_i^{e_i}$. More precisely:

- If x satisfies the congruence modulo m, then it satisfies it modulo each $p_i^{e_i}$.
- Conversely, given solutions $x_i \mod p_i^{e_i}$ for each i, there is a unique $x \mod n$ with $x = x_i \mod p_i^{e_i}$ for all i.

This bijection implies that the total number of solutions modulo m is

$$\prod_{i=1}^{r} \big(\#\{\text{solutions mod } p_i^{e_i}\}\big).$$

Remark 9.4. Consider $f(t) \in \mathbb{Z}[t]$, m is a fixed integer, and $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ is its prime factorization.

- denote the set of solutions of $f(t) = 0 \mod m$ by S_m
- denote the set of solutions of $f(t) = 0 \mod p_i^{e_i}$ by S_{p_i}
- there is a one to one correspondence (bijection)

$$S_m \to S_{p_1} \times \cdots \times S_{p_r}$$

Remark 9.5. The concrete construction of the bijection above is from the proof of CRT, and it provides a tool to break down a congruence modulo a composite number into a system of congruence modulo its divisors of power of primes.

Example 9.1. We want to solve the congruence

$$x^2 = 1 \mod 45.$$

Step 1 Factor the modulus

Write

$$45 = 3^2 \times 5.$$

We solve the congruence separately modulo 9 and modulo 5.

Step 2 Solve modulo 9

Solve

$$x^2 = 1 \mod 9.$$

Check $x = 0, 1, \ldots, 8$:

$$1^2 = 1 = 1 \mod 9, \quad 8^2 = 64 = 1 \mod 9.$$

No other squares are congruent to 1 modulo 9, so the solutions mod 9 are

$$x = 1, \quad 8 \mod 9.$$

Step 3 Solve modulo 5

Solve

$$x^2 = 1 \mod 5.$$

Check $x = 0, 1, 2, 3, 4$:

$$1^2 = 1 = 1, \quad 4^2 = 16 = 1 \mod 5.$$

Solutions mod 5 are

$$x = 1, \quad 4 \mod 5.$$

Step 4 Combine solutions via the Chinese Remainder Theorem

Total solutions modulo 45 correspond to pairs $(x \bmod 9, x \bmod 5)$ where

$$x = 1 \text{ or } 8 \mod 9, \quad x = 1 \text{ or } 4 \mod 5.$$

Thus, the total number of solutions modulo 45 is

$$2 \times 2 = 4.$$

We find the explicit solutions by solving each system:

(a) $x = 1 \mod 9$, $x = 1 \mod 5$

Write $x = 1 + 9k$. Substitute into modulo 5 condition:

$$1 + 9k = 1 \mod 5 \implies 9k = 0 \mod 5.$$

Since $9 = 4 \mod 5$,

$$4k = 0 \mod 5 \implies k = 0 \mod 5.$$

Taking $k = 0$, we get

$$x = 1.$$

(b) $x = 1 \mod 9$, $x = 4 \mod 5$
Again $x = 1 + 9k$, and

$$1 + 9k = 4 \mod 5 \implies 9k = 3 \mod 5.$$

With $9 = 4 \mod 5$,

$$4k = 3 \mod 5.$$

Multiply both sides by the inverse of 4 modulo 5, which is 4:

$$k = 3 \times 4 = 12 = 2 \mod 5.$$

So $k = 2$, and

$$x = 1 + 9 \times 2 = 19.$$

(c) $x = 8 \mod 9$, $x = 1 \mod 5$
Write $x = 8 + 9k$, then

$$8 + 9k = 1 \mod 5 \implies 9k = -7 = 3 \mod 5.$$

Again $9 = 4 \mod 5$, so

$$4k = 3 \mod 5.$$

Multiplying by 4:

$$k = 2 \mod 5.$$

Thus,

$$x = 8 + 9 \times 2 = 26.$$

(d) $x = 8 \mod 9$, $x = 4 \mod 5$
$x = 8 + 9k$,

$$8 + 9k = 4 \mod 5 \implies 9k = -4 = 1 \mod 5.$$

With $9 = 4$,

$$4k = 1 \mod 5.$$

Multiply both sides by 4:

$$k = 4 \mod 5.$$

Hence,

$$x = 8 + 9 \times 4 = 44.$$

Step 5 Final solutions modulo 45

The four solutions are

$$\boxed{x = 1, \quad 19, \quad 26, \quad 44 \mod 45.}$$

9.4 Solving Congruence of Product of Linear Factors

Consider the congruence equation

$$(xb_1)(xb_2)\cdots(xb_k) = 0 \mod m.$$

If this were an algebraic equation over a field, the solutions would be exactly the union of solutions to each linear factor, i.e.

$$\bigcup_{i=1}^{k} \{x : x = b_i\}.$$

However, working modulo m is more subtle, because zero divisors may appear, and the factorization behaves differently.

Using the Chinese Remainder Theorem (CRT), we can reduce the problem modulo m to solving modulo prime powers p^e:

$$m = \prod_j p_j^{e_j}.$$

Therefore, to solve

$$(xb_1)(xb_2)\cdots(xb_k) = 0 \mod m,$$

it suffices to solve, for each prime power p^e,

$$(xb_1)(xb_2)\cdots(xb_k) = 0 \mod p^e.$$

The solutions modulo p^e can be described as

$$\bigcup_{\substack{e_1,e_2,\ldots,e_k \geq 0 \\ e_1+e_2+\cdots+e_k=e}} \bigcap_{i=1}^{k} \{x : x = b_i \mod p^{e_i}\},$$

where the exponents e_i indicate the power of p dividing each factor xb_i.

Remark 9.6. In other words, for the product to be divisible by p^e, the factors' divisibilities by powers of p must sum at least to e, and the solutions are the intersection of the corresponding congruences for each factor.

Problem: Solve the congruence

$$(xb_1)(xb_2) = 0 \mod p^e,$$

where p is a prime, $e \geq 1$, and $b_1, b_2 \in \mathbb{Z}$.

Idea: For the product to be divisible by p^e, the sum of the powers of p dividing each factor must be at least e:

$$v_p(xb_1) + v_p(xb_2) \geq e,$$

where $v_p(y)$ denotes the p-adic valuation, i.e., the highest power of p dividing y.

This means there exist nonnegative integers e_1, e_2 such that

$$e_1 + e_2 = e,$$

and

$$x = b_1 \mod p^{e_1}, \quad x = b_2 \mod p^{e_2}.$$

Thus the solution set is the union over all such pairs (e_1, e_2) of

$$S_{e_1,e_2} = \{x : x = b_1 \mod p^{e_1} \text{ and } x = b_2 \mod p^{e_2}\}.$$

Step 1: Enumerate all pairs (e_1, e_2) with $e_1 + e_2 = e$. For example, if $e = 2$, the pairs are:

$$(0, 2), (1, 1), (2, 0).$$

Step 2: Solve each system of congruences: Each S_{e_1,e_2} is the solution set of

$$\begin{cases} x = b_1 \mod p^{e_1}, \\ x = b_2 \mod p^{e_2}. \end{cases}$$

By the Chinese Remainder Theorem (CRT), this system has a unique solution modulo $p^{\max(e_1,e_2)}$ if it is compatible, i.e., if

$$b_1 = b_2 \mod p^{\min(e_1,e_2)}.$$

If this compatibility fails, S_{e_1,e_2} is empty.

Step 3: Take the union:

$$\bigcup_{e_1+e_2=e} S_{e_1,e_2}$$

gives the full solution set modulo p^e.

Concrete Example: Solve

$$(x1)(x3) = 0 \mod 8$$

with $p = 2, e = 3$.

- Possible pairs (e_1, e_2) with $e_1 + e_2 = 3$:

$$(0, 3), (1, 2), (2, 1), (3, 0).$$

- For each pair, write the system:

$$\begin{cases} x = 1 \mod 2^{e_1} \\ x = 3 \mod 2^{e_2} \end{cases}$$

and check compatibility.

  - $(0, 3)$:

$$x = 1 \mod 1 \text{ (always true)}, \quad x = 3 \mod 8.$$

So

$$S_{0,3} = \{x = 3 \mod 8\}.$$

  - $(1, 2)$:

$$x = 1 \mod 2, \quad x = 3 \mod 4.$$

Check compatibility modulo $2^{\min(1,2)} = 2$:

$$1 = 3 \mod 2 \iff 1 = 1,$$

compatible.

Solve via CRT modulo 4: Numbers congruent to 3 mod 4 are 3, 7, 11, ... Numbers congruent to 1 mod 2 are odd numbers: 1, 3, 5, 7, 9, ... Intersection modulo 4 is $x = 3 \mod 4$.

So

$$S_{1,2} = \{x = 3 \mod 4\}.$$

  - $(2, 1)$:

$$x = 1 \mod 4, \quad x = 3 \mod 2.$$

Check compatibility modulo $2^{\min(2,1)} = 2$:

$$1 = 3 \mod 2 \iff 1 = 1,$$

compatible.

Numbers congruent to 1 mod 4 are $1, 5, 9, \ldots$, numbers congruent to 3 mod 2 are odd numbers (since 3 mod 2 = 1 mod 2). Intersection modulo 4 is $x = 1 \mod 4$.

So

$$S_{2,1} = \{x = 1 \mod 4\}.$$

  - $(3, 0)$:

$$x = 1 \mod 8, \quad x = 3 \mod 1 \text{ (always true)}.$$

So

$$S_{3,0} = \{x = 1 \mod 8\}.$$

Final solution set modulo 8 is the union:

$$\begin{aligned} S =& S_{0,3} \cup S_{1,2} \cup S_{2,1} \cup S_{3,0} \\ =& \{x = 3 \mod 8\} \cup \{x = 3 \mod 4\} \cup \{x = 1 \mod 4\} \cup \{x = 1 \mod 8\}. \end{aligned}$$

Note that $\{x = 3 \mod 4\}$ and $\{x = 1 \mod 4\}$ cover all odd numbers modulo 8 except those congruent to 3 mod 8 and 1 mod 8. Combining carefully,

$$S = \{x : x = 1, 3, 5, 7 \mod 8\} = \{\text{all odd numbers modulo } 8\}.$$

Indeed, any odd number x satisfies

$$(x1)(x3) = 0 \mod 8.$$

Check with $x = 5$:

$$(5-1)(5-3) = 4 \times 2 = 8 = 0 \mod 8.$$

Summary: The decomposition splits the exponent e into all possible sums $e_1 + \cdots + e_k = e$. For each distribution, solve the simultaneous congruences $x = b_i \mod p^{e_i}$. The full solution set is the union of all such intersections. Compatibility conditions determine if solutions exist for each system. This method works due to the valuation property of prime powers dividing the product.

9.5 General Proof for Uniqueness and Completeness of the Decomposition

Setup: Let p be a prime and $e \geq 1$. Consider the congruence

$$(xb_1)(xb_2) \cdots (xb_k) \equiv 0 \pmod{p^e},$$

where $b_1, \ldots, b_k \in \mathbb{Z}$.

Goal: Show that the solutions modulo p^e are exactly

$$\bigcup_{\substack{e_1,\ldots,e_k \geq 0 \\ e_1+\cdots+e_k=e}} \bigcap_{i=1}^{k} \{x : x \equiv b_i \pmod{p^{e_i}}\}.$$

Proof: Step 1: (Valuation and divisibility)
Recall the p-adic valuation $v_p(y)$ is the highest exponent α such that $p^\alpha \mid y$. The product

$$\prod_{i=1}^{k} (xb_i)$$

is divisible by p^e if and only if

$$v_p\left(\prod_{i=1}^{k}(xb_i)\right) = \sum_{i=1}^{k} v_p(xb_i) \geq e.$$

Thus there exist nonnegative integers $e_1, \ldots, e_k$ such that

$$e_1 + e_2 + \cdots + e_k \geq e,$$

with

$$v_p(xb_i) \geq e_i, \quad \forall i = 1, \ldots, k.$$

Since valuations are integers, the condition

$$v_p(xb_i) \geq e_i$$

is equivalent to

$$x \equiv b_i \pmod{p^{e_i}}.$$

Step 2: (Restriction on the sum of e_i)
If

$$\sum_{i=1}^{k} e_i > e,$$

then clearly

$$p^e \mid \prod_i (xb_i).$$

Since $v_p(\cdot)$ is discrete, the condition $v_p(\prod_i (xb_i)) \geq e$ is equivalent to $\sum e_i \geq e$.

In fact, solutions with $\sum e_i > e$ are also solutions with $\sum e_i = e$ if we relax to inequalities; but for the purposes of counting modulo p^e, the solutions with $\sum e_i > e$ coincide with those with $\sum e_i = e$ because of modulo reduction.

Hence it suffices to consider

$$e_1 + \cdots + e_k = e,$$

as any larger sum reduces modulo p^e to a solution with equality.

Step 3: (Equivalence of solutions and intersections)
Each tuple $(e_1, \ldots, e_k)$ with sum e defines a system of congruences

$$x \equiv b_i \pmod{p^{e_i}}, \quad i = 1, \ldots, k.$$

The set of solutions to this system is

$$S_{(e_1,\ldots,e_k)} = \bigcap_{i=1}^{k} \{x : x \equiv b_i \pmod{p^{e_i}}\}.$$

By the Chinese Remainder Theorem (CRT), if this system is *compatible* — that is, the congruences agree modulo

$$p^{\min(e_i, e_j)} \quad \forall i, j,$$

then there exists a unique solution modulo

$$p^{\max(e_1,\ldots,e_k)}.$$

If incompatible, the solution set is empty.

Step 4: (Completeness)
Any solution x modulo p^e satisfies

$$v_p(xb_i) = e_i' \geq 0,$$

and since the product is divisible by p^e,

$$\sum_i e_i' \geq e.$$

Reducing if necessary, x also satisfies

$$x \equiv b_i \pmod{p^{e_i}},$$

for some tuple $(e_1, \ldots, e_k)$ with

$$\sum_i e_i = e,$$

by lowering the exponents if they exceed the minimal condition modulo p^e.

Therefore, every solution is contained in at least one of the sets

$$S_{(e_1,\ldots,e_k)},$$

and thus the union over all such tuples covers the entire solution set modulo p^e.

Step 5: (Uniqueness and non-overlap)
Distinct tuples $(e_1, \ldots, e_k)$ can give overlapping sets $S_{(e_1,\ldots,e_k)}$ since one congruence system can imply another with weaker divisibility.

However, the decomposition is unique in the sense that the full solution set modulo p^e is exactly the union of these intersections, and no solution lies outside this union.

In practical terms, the union is a minimal covering by sets corresponding to divisibility patterns of the factors.

Conclusion: The decomposition

$$\boxed{\{x : (xb_1)(xb_2)\cdots(xb_k) \equiv 0 \pmod{p^e}\} = \bigcup_{\substack{e_1,\ldots,e_k \geq 0 \\ e_1+\cdots+e_k=e}} \bigcap_{i=1}^{k} \{x : x \equiv b_i \pmod{p^{e_i}}\}}$$

is *complete* (covers all solutions) and *unique* (no solution is left out).

This result relies on the additive property of valuations on products and the CRT for simultaneous congruences.

Theorem 9.2. Let p be prime. Then a congruence $f(x) = 0 \mod p$ of degree n has at most n solutions.

Proof. We proceed by induction on n. For $n = 0$ and $n = 1$ the statements are clear. Now assume the result holds for all degrees $< n$, and let $\deg f = n \geq 2$. If f has no root modulo p, the claim is trivial. Otherwise, let α be one root of $f(x) = 0 \mod p$. Perform polynomial long division in $\mathbb{Z}[x]$:

$$f(x) = g(x)\,(x - \alpha) + r, \quad g \in \mathbb{Z}[x],\ r \in \mathbb{Z}.$$

Evaluating at $x = \alpha$ gives $f(\alpha) = r$, and since α is a root we have $r = 0 \mod p$. Now if $\beta \neq \alpha$ is any other root of f, then

$$0 = f(\beta) = g(\beta)\,(\beta - \alpha) + r = g(\beta)\,(\beta - \alpha) \mod p,$$

and $\beta \neq \alpha$ forces $g(\beta) = 0 \mod p$. Hence all other roots of f are roots of g, which has degree $n - 1$, and by the inductive hypothesis $g = 0 \mod p$ has at most $n - 1$ solutions. Including α, f has at most n solutions. □

Corollary 2. If

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0 \mod p$$

has more than n solutions modulo p, then each $a_i = 0 \mod p$.

Theorem 9.3. Let

$$f(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x].$$

Then $f(x) = 0 \mod p$ has exactly n distinct solutions modulo p if and only if $f(x)$ divides $x^p - x$ in $\mathbb{F}_p[x]$, i.e. there is $g(x) \in \mathbb{Z}[x]$ with

$$f(x)\,g(x) = x^p x \mod p.$$

Proof. Suppose first that f has n distinct roots modulo p. Since $\deg f = n \leq p$, divide in $\mathbb{F}_p[x]$:

$$x^p x = f(x)\,g(x) + r(x), \quad \deg r < n.$$

If α is any root of f, then

$$\alpha^p \alpha = f(\alpha)\,g(\alpha) + r(\alpha) = r(\alpha) \mod p,$$

so $r(\alpha) = 0$. Thus r has n roots but $\deg r < n$, so $r = 0$ and $f \mid (x^p - x)$.

Conversely, suppose $f \mid (x^p - x)$ in $\mathbb{F}_p[x]$. Write $x^p - x = f(x)\,g(x)$ with $\deg f = n$ and $\deg g = p - n$.g has at most $p - n$ roots. For any $\alpha \in \{0, 1, \ldots, p-1\}$ not a root of g, we get

$$0 = \alpha^p \alpha = f(\alpha)\,g(\alpha) \mod p,$$

and $g(\alpha) \neq 0$ forces $f(\alpha) = 0$. There are at least $p - (p - n) = n$ such α, so f has at least n roots; it has exactly n. □

Corollary 3. If $d \mid (p - 1)$ then $x^d = 1 \mod p$ has exactly d solutions modulo p.

Proof. Write $p-1=kd$, so

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

Hence $x^d-1 \mid x^p-x$, and by Theorem 30 the congruence $x^d=1$ has exactly d solutions. □

Corollary 4 (Wilson's Theorem)**.** Let p be an odd prime. Then

$$(x)(x-1)\cdots(x-(p-1)) = x^p - x \mod p$$

and in particular $(p-1)! = -1 \mod p$.

Proof. The polynomial $f(x)=\prod_{k=0}^{p-1}(x-k)$ has degree p and p roots modulo p, so $f \mid (x^p-x)$ and since both are monic of degree p they are equal in $\mathbb{F}_p[x]$. Comparing the coefficient of x gives

$$(-1)^{p-1}(p-1)! = -1\cdot(p-1)! = -1 \mod p,$$

as claimed (since p is odd). □

If $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$ then expanding gives

$$f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n,$$

where the σ_i are the elementary symmetric polynomials in the roots:

$$\sigma_1 = \sum_i \alpha_i, \quad \sigma_2 = \sum_{i<j} \alpha_i\alpha_j, \quad \ldots, \quad \sigma_n = \prod_i \alpha_i.$$

9.6 Hensel's Lifting Lemma

Setup: Let p be a prime and $f(x)\in\mathbb{Z}[x]$ be a polynomial. Suppose we know a solution a_0 to the congruence

$$f(a_0) \equiv 0 \pmod p,$$

and the derivative satisfies

$$f'(a_0) \not\equiv 0 \pmod p.$$

Goal: Lift the solution $a_0 \pmod p$ to a solution $a_e \pmod{p^e}$ such that

$$f(a_e) \equiv 0 \pmod{p^e},$$

and

$$a_e \equiv a_0 \pmod p.$$

Statement of Hensel's Lemma (Simplified Version): If $a_0\in\mathbb{Z}$ satisfies

$$f(a_0) \equiv 0 \pmod p,$$

and

$$f'(a_0) \not\equiv 0 \pmod p,$$

then for each $e\geq 1$, there exists a unique $a_e\in\mathbb{Z}$ modulo p^e such that

$$f(a_e)\equiv 0 \pmod{p^e}, \quad a_e \equiv a_0 \pmod p.$$

Method (Constructive Proof Sketch): Given $a_e \bmod p^e$, construct $a_{e+1} = a_e + tp^e$ for some integer t to satisfy

$$f(a_{e+1}) \equiv 0 \pmod{p^{e+1}}.$$

Using Taylor expansion,

$$f(a_e + tp^e) \equiv f(a_e) + tp^e f'(a_e) \pmod{p^{e+1}}.$$

Because $f(a_e) \equiv 0 \pmod{p^e}$, write $f(a_e) = p^e m$, so

$$f(a_{e+1}) \equiv p^e m + tp^e f'(a_e) = p^e(m + tf'(a_e)) \pmod{p^{e+1}}.$$

For $f(a_{e+1}) \equiv 0 \pmod{p^{e+1}}$, we need

$$m + tf'(a_e) \equiv 0 \pmod{p}.$$

Since $f'(a_e) \not\equiv 0 \pmod{p}$, t can be chosen uniquely modulo p.

Application Example: Solve

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

given a solution modulo p (e.g., $p = 7, e = 1$, $x \equiv 3$).

Using Hensel's lemma, the solution modulo 7 can be lifted step-by-step to modulo 7^2, 7^3, etc., as long as $2x \not\equiv 0 \pmod 7$ (the derivative condition).

Summary: Hensel's lemma allows lifting solutions of polynomial congruences from modulo p to modulo p^e. Requires the derivative at the root mod p to be invertible modulo p. Uniqueness and existence of the lifted solution are guaranteed. Essential in computational number theory, factorization algorithms, and solving modular equations involving prime powers.

9.7 Concrete Example of Hensel Lifting

Problem: Solve the congruence

$$x^2 \equiv 2 \pmod{7^3}.$$

Step 1: Find a solution modulo 7. First, solve

$$x^2 \equiv 2 \pmod 7.$$

Test $x = 1, 2, \ldots, 6$:

$$1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9 \equiv 2, \quad 4^2 = 16 \equiv 2, \quad 5^2 = 25 \equiv 4, \quad 6^2 = 36 \equiv 1.$$

So solutions modulo 7 are

$$x \equiv 3 \pmod 7 \quad \text{and} \quad x \equiv 4 \pmod 7.$$

Choose $a_1 = 3$.

Step 2: Lift solution from modulo 7 to modulo $7^2 = 49$. We want to find $a_2 = a_1 + t \cdot 7$ such that

$$a_2^2 \equiv 2 \pmod{49}.$$

Write

$$a_2 = 3 + 7t.$$

Compute

$$a_2^2 = (3 + 7t)^2 = 9 + 2 \cdot 3 \cdot 7t + 49t^2 = 9 + 42t + 49t^2.$$

Modulo 49, the term $49t^2$ vanishes, so

$$a_2^2 \equiv 9 + 42t \pmod{49}.$$

We want

$$9 + 42t \equiv 2 \pmod{49} \implies 42t \equiv 29 = -7 \equiv 42 \pmod{49}.$$

Solve

$$42t \equiv 42 \pmod{49}.$$

Note $\gcd(42, 49) = 7$. Divide both sides by 7:

$$6t \equiv 6 \pmod{7}.$$

Since $\gcd(6, 7) = 1$, inverse of 6 mod 7 is 6 (because $6 \times 6 = 36 \equiv 1 \pmod{7}$), so

$$t \equiv 6 \times 6 = 36 \equiv 1 \pmod{7}.$$

So the solution for t modulo 7 is

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

Choose $t = 1$. Then

$$a_2 = 3 + 7 \times 1 = 10.$$

Check:

$$10^2 = 100 \equiv 1002 \times 49 = 10098 = 2 \pmod{49}.$$

Step 3: Lift solution from modulo 49 to modulo $7^3 = 343$. Set

$$a_3 = a_2 + s \cdot 49 = 10 + 49s.$$

We want

$$a_3^2 \equiv 2 \pmod{343}.$$

Calculate

$$a_3^2 = (10 + 49s)^2 = 100 + 2 \cdot 10 \cdot 49s + 49^2 s^2 = 100 + 980s + 2401s^2.$$

Modulo 343, note

$$2401s^2 = 7^4 s^2 \equiv 0 \pmod{343},$$

so

$$a_3^2 \equiv 100 + 980s \pmod{343}.$$

We want

$$100 + 980s \equiv 2 \pmod{343} \implies 980s \equiv 2100 = -98 \equiv 245 \pmod{343}.$$

Divide by 7 (since $\gcd(980, 343) = 7$):

$$140s \equiv 35 \pmod{49}.$$

Again divide by 7:

$$20s \equiv 5 \pmod{7}.$$

Reduce $20 \equiv 6 \pmod{7}$, so

$$6s \equiv 5 \pmod{7}.$$

Multiply both sides by inverse of 6 modulo 7, which is 6:

$$s \equiv 5 \times 6 = 30 \equiv 2 \pmod{7}.$$

Choose $s = 2$.
Thus,

$$a_3 = 10 + 49 \times 2 = 10 + 98 = 108.$$

Check:

$$108^2 = 11664.$$

Divide 11664 by 343:

$$343 \times 34 = 11662, \quad 1166411662 = 2,$$

so

$$108^2 \equiv 2 \pmod{343}.$$

Final answer: The solution lifted to modulo 7^3 is

$$x \equiv 108 \pmod{343}.$$

Similarly, the other root modulo 7, $x \equiv 4$, can also be lifted.

Summary: Start with solution modulo p. Use Hensel's lemma to iteratively find solutions modulo p^e. At each step, solve a linear congruence for the correction term. This method ensures a unique lift exists when the derivative condition is met.

10 Discrete Logarithm

Let $n = 35$. Euler's theorem says if $(a, 35) = 1$ then $a^{\phi(35)} = 1 \mod 35$, i.e. $a^{24} = 1 \mod 35$. Can 24 be replaced by a smaller exponent? Equivalently, what is the smallest $N > 0$ such that $a^N = 1 \mod 35$ for all $(a, 35) = 1$?
Answer: The smallest positive integer N such that

$$a^N = 1 \mod 35$$

for all $(a, 35) = 1$ is $N = 12$.

Definition 10.1 (Order)**.** If $(a, m) = 1$ and h is the least positive integer with $a^h = 1 \mod m$, we write $\mathrm{ord}_m(a) = h$.

Example 10.1. Consider $a = 2$ and $m = 7$. Since $\gcd(2, 7) = 1$, the order of 2 modulo 7, denoted $\mathrm{ord}_7(2)$, is the smallest positive integer h such that

$$2^h = 1 \mod 7.$$

Let's compute powers of 2 modulo 7:

$$2^1 = 2 \neq 1 \mod 7,$$

$$2^2 = 4 \neq 1 \mod 7,$$

$$2^3 = 8 = 1 \mod 7.$$

Since $h = 3$ is the smallest positive integer with this property, we have

$$\mathrm{ord}_7(2) = 3.$$

Remark 10.1. By Euler's theorem, $\phi(7) = 6$, then $2^6 = 1 \mod 7$. But here we can decrease 6 to 3 as the order of 2 in the sense of modulo 7.

Lemma 3. Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ such that $\gcd(a, m) = 1$. Then the order of a modulo m, denoted $\mathrm{ord}_m(a)$, divides Euler's totient $\phi(m)$. That is,

$$\mathrm{ord}_m(a) \mid \phi(m).$$

Proof. Recall that $\mathrm{ord}_m(a)$ is defined as the smallest positive integer k such that

$$a^k \equiv 1 \pmod m.$$

Since $\gcd(a, m) = 1$, a is a unit in the multiplicative group $U(m)$ of integers modulo m. Euler's theorem states that

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

By the definition of order, the order $\mathrm{ord}_m(a) = k$ divides any exponent n for which $a^n \equiv 1 \pmod m$.

Since $a^{\phi(m)} \equiv 1 \pmod m$, it follows that

$$k = \mathrm{ord}_m(a) \mid \phi(m).$$

Thus, the order of a modulo m divides $\phi(m)$. □

Remark 10.2. We can use symbol $\langle h \rangle$ to denote all multiples of h, then $\phi(m) \in \langle h \rangle$.

Lemma 4. If $h = \mathrm{ord}_m(a)$ then $\mathrm{ord}_m(a^k) = \frac{h}{\gcd(h,k)}$.

Proof. One checks that $(a^k)^j = 1 \mod m \iff h \mid kj \iff \frac{h}{\gcd(h,k)} \mid j$. □

Lemma 5. If $\mathrm{ord}_m(a) = h$ and $\mathrm{ord}_m(b) = k$ with $\gcd(h,k) = 1$, then $\mathrm{ord}_m(ab) = hk$.

Proof. Since $\gcd(h,k) = 1$ we have

$$(ab)^{hk} = a^{hk}b^{hk} = (a^h)^k(b^k)^h = 1 \cdot 1 = 1 \mod m,$$

and minimality arguments show no smaller exponent works. □

Definition 10.2 (Primitive Root)**.** If $\mathrm{ord}_p(g) = \phi(p) = p - 1$, we say g is a *primitive root* modulo p.

Example 10.2. Consider the prime $p = 7$. Since $\phi(7) = 6$, a primitive root modulo 7 is an integer g such that $g^6 \equiv 1 \pmod 7$ and no smaller positive exponent $k < 6$ satisfies $g^k \equiv 1 \pmod 7$.

Check $g = 3$:

$$3^1 = 3 \not\equiv 1 \pmod 7, \quad 3^2 = 9 \equiv 2 \pmod 7, \quad 3^3 = 3 \cdot 3^2 = 3 \cdot 2 = 6 \not\equiv 1 \pmod 7,$$

$$3^4 = 3^3 \cdot 3 = 6 \cdot 3 = 18 \equiv 4 \pmod 7, \quad 3^5 = 3^4 \cdot 3 = 4 \cdot 3 = 12 \equiv 5 \pmod 7,$$

$$3^6 = 3^5 \cdot 3 = 5 \cdot 3 = 15 \equiv 1 \pmod 7.$$

Since the order of 3 modulo 7 is 6, which equals $\phi(7)$, 3 is a primitive root modulo 7.

Lemma 6. Let p be a prime and suppose

$$p - 1 = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$$

is its prime factorization. Then there exists a primitive root modulo p.

Proof. The multiplicative group $U(p) = (\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p - 1$.

By the fundamental theorem of finite cyclic groups, for each divisor d of $p-1$, the group $U(p)$ contains exactly $\phi(d)$ elements of order d.

In particular, for each prime divisor q_i of $p - 1$, there exist elements in $U(p)$ of order $q_i^{e_i}$.

To find an element of order $p - 1$, one can pick elements g_i of order $q_i^{e_i}$ for each i. Since $U(p)$ is cyclic, these elements generate cyclic subgroups of coprime orders (powers of distinct primes). Consider the element

$$g = g_1 g_2 \cdots g_r.$$

Because the orders $q_i^{e_i}$ are pairwise coprime, the order of g is the product of these orders:

$$\mathrm{ord}_p(g) = \mathrm{lcm}(\mathrm{ord}_p(g_1), \mathrm{ord}_p(g_2), \ldots, \mathrm{ord}_p(g_r)) = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r} = p - 1.$$

Thus, g is a primitive root modulo p. □

Let p be a prime. Then there exists a primitive root g modulo p, whose order is

$$\operatorname{ord}_p(g) = p - 1 = \prod_{i=1}^{r} q_i^{e_i},$$

where q_i are distinct primes and e_i their respective exponents.

We showed that for each i, there exists an element $g_i \in U(p)$ such that

$$\operatorname{ord}_p(g_i) = q_i^{e_i}.$$

By setting

$$g = \prod_{i=1}^{r} g_i,$$

and noting that the orders $q_i^{e_i}$ are powers of distinct primes (hence pairwise coprime), it follows from the properties of cyclic groups that

$$\operatorname{ord}_p(g) = \operatorname{lcm}\big(\operatorname{ord}_p(g_1), \operatorname{ord}_p(g_2), \ldots, \operatorname{ord}_p(g_r)\big) = \prod_{i=1}^{r} q_i^{e_i} = p - 1.$$

Thus, g is a primitive root modulo p.

10.1 Number of Primitive Roots

Suppose m admits a primitive root g. Then the elements

$$1, g, g^2, \ldots, g^{\phi(m)-1}$$

are all coprime to m and distinct modulo m. Hence, they form a complete reduced residue system modulo m.

If a is any primitive root modulo m, then there exists an integer k such that

$$a \equiv g^k \pmod{m}.$$

The order of a satisfies

$$\operatorname{ord}_m(g^k) = \frac{\operatorname{ord}_m(g)}{\gcd(k, \operatorname{ord}_m(g))} = \frac{\phi(m)}{\gcd(k, \phi(m))}.$$

Thus, g^k is a primitive root modulo m if and only if

$$\gcd(k, \phi(m)) = 1.$$

The number of such integers k with $1 \le k \le \phi(m)$ and $\gcd(k, \phi(m)) = 1$ is exactly $\phi(\phi(m))$.

Therefore, the number of primitive roots modulo m is

$$\phi\big(\phi(m)\big).$$

In particular, when $m = p$ is prime, the number of primitive roots modulo p is

$$\phi(p - 1).$$

10.2 Artin's Conjecture

Conjecture 4 (Artin)**.** Let a be an integer that is not a perfect square and not equal to -1. Then there exist infinitely many primes p for which a is a primitive root modulo p.

This conjecture predicts that any "non-degenerate" integer a generates a cyclic subgroup of maximal order modulo infinitely many primes.

Significant progress on this conjecture includes:

- Hooley (1967) proved Artin's conjecture conditional on the Generalized Riemann Hypothesis (GRH).
- Heath-Brown (1986) showed unconditionally that for any prime a, the conjecture fails for at most two primes p.

10.3 Discrete Logarithm

Definition 10.3 (Discrete Logarithm)**.** Let p be a prime and g a primitive root modulo p. For any $a \not\equiv 0 \pmod{p}$, there exists a unique integer k, $0 \leq k \leq p-2$, such that

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

The integer k is called the *index* or *discrete logarithm* of a to the base g, denoted

$$k = \log_g a.$$

Computing the discrete logarithm k given a, g, and p is known as the *discrete logarithm problem*, which is computationally hard in general. This hardness forms the basis for many cryptographic protocols, including Diffie–Hellman key exchange and the ElGamal encryption scheme.

10.3.1 Example of Discrete Logarithm

Consider the prime $p = 11$ and the primitive root $g = 2$ modulo 11. The powers of 2 modulo 11 are:

$$2^0 \equiv 1 \pmod{11}, \quad 2^1 \equiv 2 \pmod{11}, \quad 2^2 \equiv 4 \pmod{11}, \quad 2^3 \equiv 8 \pmod{11}, \quad 2^4 \equiv 5 \pmod{11},$$

$$2^5 \equiv 10 \pmod{11}, \quad 2^6 \equiv 9 \pmod{11}, \quad 2^7 \equiv 7 \pmod{11}, \quad 2^8 \equiv 3 \pmod{11}, \quad 2^9 \equiv 6 \pmod{11},$$

Suppose we want to find the discrete logarithm of $a = 7$ to the base $g = 2$ modulo 11. From above,

$$2^7 \equiv 7 \pmod{11}.$$

Hence,

$$\log_2 7 \equiv 7 \pmod{11}.$$

10.3.2 Applications of Discrete Logarithms

The discrete logarithm problem is computationally hard in sufficiently large groups and underpins the security of many cryptographic protocols, such as:

- **Diffie–Hellman key exchange:** Enables two parties to establish a shared secret over an insecure channel.
- **ElGamal encryption:** A public-key cryptosystem relying on discrete logs.
- **Digital signatures:** Such as the Digital Signature Algorithm (DSA).

The hardness assumption means that, given g, p, and $a = g^k \mod p$, it is computationally infeasible to find k for large p.

10.3.3 Connection to the Continuous Logarithm

The discrete logarithm in modular arithmetic can be viewed as an analogue of the regular logarithm function in real numbers:

- **Continuous logarithm:** For positive real x, b, $\log_b x$ is the exponent k such that $b^k = x$.
- **Discrete logarithm:** For integers modulo p, the discrete log $\log_g a$ is the exponent k such that $g^k \equiv a \pmod{p}$.

However, unlike the continuous logarithm, the discrete logarithm is defined in a finite cyclic group, making it a *discrete* function with fundamentally different computational properties—most notably, the absence of efficient algorithms for inversion in large groups (without special structure), which is the source of its cryptographic strength.

10.4 Index Calculus Method

To solve the congruence

$$x^d \equiv 1 \pmod{p},$$

where p is prime and g is a primitive root modulo p, write $x = g^k$. Then

$$g^{kd} \equiv 1 \pmod{p} \iff p-1 \mid kd \iff \frac{p-1}{\gcd(d, p-1)} \mid k.$$

Thus, the solutions are precisely those

$$x = g^k$$

where k is a multiple of $\frac{p-1}{\gcd(d,p-1)}$. Hence, there are exactly $\gcd(d, p-1)$ distinct solutions.

More generally, to solve

$$x^d \equiv a \pmod{p},$$

write

$$a = g^{\ell}, \quad x = g^{k},$$

so that

$$g^{kd} \equiv g^{\ell} \pmod{p} \implies kd \equiv \ell \pmod{p-1}.$$

This linear congruence in k has a solution if and only if

$$\gcd(d, p-1) \mid \ell,$$

and in that case, there are $\gcd(d, p-1)$ solutions k modulo $p-1$, corresponding to $\gcd(d, p-1)$ solutions $x = g^{k} \pmod{p}$.

This method reduces solving $x^{d} = a \pmod{p}$ to solving a linear congruence in the exponent, utilizing the cyclic structure of the multiplicative group modulo p.

10.5 Existence of Primitive Roots

Theorem 10.1. There exists a primitive root modulo m if and only if

$$m \in \{1, 2, 4, p^{e}, 2p^{e}\},$$

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

Outline. We focus on the case when $m = p^{e}$ with p an odd prime:

(i) For $e = 1$, the existence of a primitive root modulo p is classical.

(ii) For $e = 2$, one can *lift* a primitive root modulo p to a primitive root modulo p^{2} using Hensel's Lemma or explicit construction.

(iii) Assuming g is a primitive root modulo p^{2}, one can prove by induction that g remains a primitive root modulo p^{e} for all $e \geq 2$.

The other cases follow by direct verification for small moduli and by using the multiplicative structure of the group $(\mathbb{Z}/m\mathbb{Z})^{\times}$, especially for $m = 2, 4$ and $2p^{e}$. □

11 Quadratic Residues and Quadratic Reciprocity

11.1 Quadratic Congruences

Consider the quadratic congruence modulo an odd prime p:

$$ax^2 + bx + c \equiv 0 \pmod{p}, \quad a \not\equiv 0 \pmod{p}.$$

By completing the square, we rewrite it as:

$$\left(x + \frac{b}{2a}\right)^2 \equiv \frac{b^2 - 4ac}{4a^2} \pmod{p}.$$

Set the discriminant $\Delta = b^2 - 4ac$. Then there are two cases:

- If $\Delta \equiv 0 \pmod{p}$, the congruence has a unique solution:

$$x \equiv -\frac{b}{2a} \pmod{p}.$$

- If $\Delta \not\equiv 0 \pmod{p}$, then the number of solutions depends on whether Δ is a quadratic residue modulo p:

$$x^2 \equiv \Delta \pmod{p} \implies \begin{cases} \text{no solution if } \Delta \text{ is a non-residue,} \\ \text{two distinct solutions } x \equiv \pm\sqrt{\Delta} \pmod{p} \text{ if } \Delta \text{ is a residue.} \end{cases}$$

11.2 Quadratic Residues Modulo a Prime

Definition 11.1. Let p be an odd prime and $a \in \mathbb{Z}$ with $p \nmid a$. We say a is a *quadratic residue modulo p* if there exists x such that

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

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

Examples:

- For $p = 5$, residues are $1, 4$.
- For $p = 7$, residues are $1, 2, 4$.
- For $p = 11$, residues are $1, 3, 4, 5, 9$.
- For $p = 13$, residues are $1, 3, 4, 9, 10, 12$.

11.3 Legendre Symbol

Definition 11.2 (Quadratic Non-Residue)**.** Let p be an odd prime. An integer a is called a *quadratic non-residue modulo p* if

$$\gcd(a, p) = 1$$

and the congruence

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

has **no** solution x in integers.

Example 11.1. Consider $p = 7$. The quadratic residues modulo 7 are:

$$1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 2, \quad 4^2 \equiv 2, \quad 5^2 \equiv 4, \quad 6^2 \equiv 1 \pmod{7}.$$

Thus, the quadratic residues modulo 7 are $\{1, 2, 4\}$.

For example, 3 is a quadratic non-residue modulo 7 since there is no integer x such that

$$x^2 \equiv 3 \pmod{7}.$$

Definition 11.3 (Legendre symbol)**.** For an odd prime p and integer a, the *Legendre symbol* is defined as

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

Remark 11.1. An integer g is a *primitive root* modulo p if its powers

$$\{g, g^2, \ldots, g^{p-1}\}$$

are distinct modulo p. Writing $a = g^k$, one has

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & k \text{ even}, \\ -1, & k \text{ odd}. \end{cases}$$

Remark 11.2 (Multiplicativity)**.** For $\gcd(a, p) = \gcd(b, p) = 1$,

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

Remark 11.3 (Congruence)**.**

$$\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right).$$

11.4 Characterization of Quadratic Residues

Lemma 7. Let p be an odd prime and $a \not\equiv 0 \pmod{p}$. Then

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

Proof. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \pmod{p}$. If $a = g^k$ for a primitive root g, then

$$a^{\frac{p-1}{2}} = (g^k)^{\frac{p-1}{2}} = g^{k\frac{p-1}{2}} \equiv \begin{cases} 1, & k \text{ even}, \\ -1, & k \text{ odd}. \end{cases}$$

Hence the lemma. □

11.5 Gauss's Lemma

Lemma 8 (Gauss)**.** Let p be an odd prime and $\gcd(a, p) = 1$. For $1 \le k \le \frac{p-1}{2}$, let $(ka)_p$ denote the least residue of ka modulo p in the interval $\left(-\frac{p}{2}, \frac{p}{2}\right]$. Let n be the number of such residues which are negative. Then

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

Sketch. One shows

$$\prod_{k=1}^{\frac{p-1}{2}} (ka)_p \equiv (-1)^n \prod_{k=1}^{\frac{p-1}{2}} ka \equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p},$$

and also

$$\prod_{k=1}^{\frac{p-1}{2}} (ka)_p \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Comparing, this yields

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

which equals $\left(\frac{a}{p}\right)$. □

11.6 Supplementary Laws

Theorem 11.1. For an odd prime p,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Sketch. Apply Gauss's Lemma to $a = -1$ and $a = 2$, counting the number of negative residues among $\{k \cdot (-1)\}_p$ and $\{2k\}_p$, respectively. □

11.7 Quadratic Reciprocity

Theorem 11.2 (Quadratic Reciprocity)**.** Let p, q be distinct odd primes. Then

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

Sketch. One classical proof uses counting lattice points inside the rectangle

$$[1, \tfrac{p-1}{2}] \times [1, \tfrac{q-1}{2}],$$

and relates the parity of the number of lattice points below the line $y = \frac{q}{p}x$ to the product of the Legendre symbols $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$. □

Theorem 11.3 (Quadratic Reciprocity Law (Restated))**.** Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol.

Equivalently,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4,$$

and

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \quad \text{if } p \equiv q \equiv 3 \pmod 4.$$

Example 11.2. Let $p = 3$ and $q = 11$, both odd primes.

Calculate $\left(\frac{3}{11}\right)$ and $\left(\frac{11}{3}\right)$:

- Since $3 \equiv 3 \pmod 4$ and $11 \equiv 3 \pmod 4$, the reciprocity law gives
$$\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right).$$
- Compute $\left(\frac{11}{3}\right) = \left(\frac{2}{3}\right)$ since $11 \equiv 2 \pmod 3$.
- Because 2 is a quadratic non-residue modulo 3, $\left(\frac{2}{3}\right) = -1$.
- Therefore,
$$\left(\frac{3}{11}\right) = -(-1) = 1.$$

Hence, 3 is a quadratic residue modulo 11.

11.8 Jacobi Symbol

Definition 11.4 (Jacobi Symbol)**.** Let $n > 1$ be an odd positive integer with prime factorization

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

For any integer a, the *Jacobi symbol* $\left(\frac{a}{n}\right)$ is defined by

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{e_i},$$

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

Remarks:

- Multiplicative in numerator and denominator:

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right), \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right).$$

- Trivial cases:

$$\left(\frac{a}{n}\right) = 0 \iff \gcd(a, n) > 1, \quad \left(\frac{1}{n}\right) = 1.$$

- Congruence property:

$$a \equiv b \pmod{n} \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$

- **Note:** $\left(\frac{a}{n}\right) = 1$ does *not* imply that a is a quadratic residue modulo n.

Remark 11.4. The Jacobi symbol value $\left(\frac{a}{n}\right) = 1$ does *not* guarantee that a is a quadratic residue modulo n. In other words, it is possible to have $\left(\frac{a}{n}\right) = 1$ even when the congruence

$$x^2 \equiv a \pmod{n}$$

has no solution.

If n is composite (odd and > 1), the Jacobi symbol $\left(\frac{a}{n}\right)$ is not a definitive test for a being a quadratic residue modulo n.

Specifically, if

$$\left(\frac{a}{n}\right) = -1,$$

then no solution exists for

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

But if

$$\left(\frac{a}{n}\right) = 1,$$

the equation may or may not have solutions.

In other words, the Jacobi symbol only gives a **necessary** condition for a to be a square modulo n, not a sufficient one.

11.9 Quadratic Reciprocity for Jacobi Symbol

If m, n are odd positive integers with $\gcd(m, n) = 1$, then

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

Combined with the supplements,

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}, \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}},$$

this provides a fast algorithm to compute $\left(\frac{a}{n}\right)$ by repeated reciprocity steps.

11.10 Computation Algorithm for Jacobi Symbol

To compute $\left(\frac{a}{n}\right)$ for odd $n > 1$:

(i) Reduce a modulo n.

(ii) If $a = 0$, return 0; if $a = 1$, return 1.

(iii) Factor out powers of 2: write $a = 2^k a'$ with a' odd, then

$$\left(\frac{a}{n}\right) = \left(\frac{2}{n}\right)^k \left(\frac{a'}{n}\right),$$

using the supplement for $\left(\frac{2}{n}\right)$.

(iv) Apply quadratic reciprocity:

$$\left(\frac{a'}{n}\right) = (-1)^{\frac{a'-1}{2}\frac{n-1}{2}} \left(\frac{n \bmod a'}{a'}\right).$$

(v) Repeat the above steps until the denominator becomes 1 or prime.

Example:

$$\left(\frac{127}{233}\right) = (-1)^{63\cdot 116}\left(\frac{233 \bmod 127}{127}\right) = -\left(\frac{21}{127}\right) = \cdots = -1.$$

11.11 Zolotareff's Definition

Definition 11.5 (Zolotareff)**.** Let n be odd. Multiplication by a modulo n induces a permutation

$$\pi_a : \{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n-1\}, \quad \pi_a(x) \equiv ax \pmod{n}.$$

Then the Jacobi symbol equals the sign of the permutation:

$$\left(\frac{a}{n}\right) = \operatorname{sgn}(\pi_a) = \begin{cases} +1, & \pi_a \text{ is an even permutation,} \\ -1, & \pi_a \text{ is an odd permutation.} \end{cases}$$

Example 11.3.

$$Q = 7, \quad P = 4: \quad (0)(1\,4\,2)(3\,5\,6) \implies e = 0, \quad \left(\frac{4}{7}\right) = 1,$$

$$Q = 7, \quad P = 5: \quad (0)(1\,5\,4\,6\,2\,3) \implies e = 1, \quad \left(\frac{5}{7}\right) = -1.$$

12 Higher Power Residues

12.1 Definition

Let p be a prime, and $k \geq 2$ an integer. An integer a is called a *k-th power residue modulo p* if the congruence

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

has a solution $x \in \mathbb{Z}$.

If no such x exists, then a is called a *k-th power non-residue modulo p*.

12.2 Basic Properties

- When $k = 2$, this reduces to the classical quadratic residue problem.
- The set of all k-th power residues modulo p forms a subgroup of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$.
- The size of this subgroup is $\frac{p-1}{d}$, where $d = \gcd(k, p-1)$.

12.3 Higher Residue Symbols

Generalizations of the Legendre symbol exist for higher residues, such as:

- **Cubic Residue Symbol** for $k = 3$.
- **Quartic Residue Symbol** for $k = 4$.
- These symbols satisfy reciprocity laws similar in spirit to quadratic reciprocity, but more intricate.

12.4 Higher Reciprocity Laws

Cubic reciprocity and **quartic reciprocity** laws generalize quadratic reciprocity to higher powers. Their proofs often require the use of *cyclotomic fields* and algebraic number theory.

12.5 Applications

Higher power residue theory is fundamental in advanced number theory and cryptography. It appears in the study of:

- Kummer extensions.
- Reciprocity laws in algebraic number fields.
- Cryptographic protocols relying on higher residue problems.

12.6 Example

For a prime $p \equiv 1 \pmod 3$, the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order divisible by 3, so cubic residues modulo p form a subgroup of size $\frac{p-1}{3}$.

$$a \text{ is a cubic residue mod } p \iff a^{\frac{p-1}{3}} \equiv 1 \pmod p.$$