MAT422: Theory of Numbers

Notes taken by Mahmudul Hasan Turjoy
Based on the lectures of Arnab Chakraborty

Last Updated: March 14, 2025

Preface

These lecture notes were taken in the course *MAT422: Theory of Numbers* taught by *Arnab Chakraborty* at BRAC University as part of the BSc. in Mathematics program Spring 2025.

These notes are not endorsed by the lecturer, and I often modified them after lectures. They are not accurate representations of what was actually lectured, and in particular, all errors are surely mine. If you find anything that needs to be corrected or improved, please inform me at: mh.turjoy@yahoo.com.

— Mahmudul Hasan Turjoy

Contents

1
Preliminaries

§ 1.1 Number Systems

The most natural and familiar number system is the set of *natural numbers*,

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

However, solving equations using only natural numbers is often challenging. To address this, we extend $\mathbb{N}$ by introducing 0 and additive inverses, forming the set of *integers*,

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

$\mathbb{Z}$ allows for systematic techniques in algebra, particularly in solving linear equations. In $\mathbb{Z}$, we can add, subtract, and multiply, but division is not always possible. To allow division, we extend $\mathbb{Z}$ to the set of *rational numbers*,

$$\mathbb{Q} = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0, gcd(p, q) = 1 \right\}.$$

However, $\mathbb{Q}$ is still not sufficient to solve all equations. For example, $\sqrt{2}$ is not a rational number but a solution to the equation $x^2 = 2$. To include such numbers, we extend $\mathbb{Q}$ to the set of *real numbers*, $\mathbb{R}$. Yet even $\mathbb{R}$ is not enough for certain equations, such as $x^2 + 1 = 0$ have no solutions in $\mathbb{R}$. To resolve this, we introduce the *complex numbers*,

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R},\ i^2 = -1\}.$$

According to the *Fundamental Theorem of Algebra*, $\mathbb{C}$ is *algebraically closed*, meaning every polynomial equation with complex coefficients has a solution in $\mathbb{C}$. Thus, $\mathbb{C}$ is the most comprehensive number system we need for solving polynomial equations, and we do not extend it further in this context. Notice,

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

§ 1.2 Well-Ordering Principle

In Peano Arithmetic, the *Principle of Mathematical Induction (PMI)* is assumed as an axiom. And from this axiom, we can derive a fundamental result known as the *Well-Ordering Principle*.

Well-Ordering Principle. Every non-empty subset of $\mathbb{N}$ has a least element.

§ 1.3 Goals and Motivation for doing NT

To be written once I figure out myself. Hopefully, at the end of this course I will be able to write something here. :3

2
Divisibility and Primes

§ 2.1 Basics of Divisibility

Definition 2.1 (Divisibility)**.** Let $a, b \in \mathbb{Z}$. We say that $a \neq 0$ divides b if there exists an integer c such that $b = ac$. We write $a \mid b$ if a divides b.

We say a is a divisor of b if $a \mid b$. The set of all divisors of b is denoted by $Div(b)$.

$$Div(b) := \{a \in \mathbb{Z} : a \mid b\}.$$

We can also say $a \mid b$ implies there is a solution in $\mathbb{Z}$ to the equation $ax = b$.

Proposition 2.1. 1. For all $a \in \mathbb{Z} \setminus 0$, $a \mid 0$.

2. $a \mid b$ and $b \mid c$ implies $a \mid c$.

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

Proof. 1. $a \mid 0$ since $0 = a \cdot 0$.

2. $a \mid b$ implies $b = ax$ and $b \mid c$ implies $c = by = axy = a(xy)$ implies $a \mid c$.

3. $a \mid b$ implies $b = ax$ and $a \mid c$ implies $c = ay$. So, $bx + cy = a(x^2 + y^2)$ implies $a \mid (bx + cy)$.

□

Theorem 2.1 (Division Algorithm)**.** Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers q, r such that $a = qb + r$ and $0 \leq r < b$.

Proof. Consider the set

$$S = \{a - xb \mid x \in \mathbb{Z}, a - xb \geq 0\}.$$

The set is nonempty because $a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$. According to the Well-Ordering Principle, S has a least element, say r. So, $r = a - qb$ for some $q \in \mathbb{Z}$. We will show that $0 \leq r < b$. $0 \leq r$ by the construction of S. We argue that $r < b$. If this were not the case, then $r \geq b \Rightarrow r - b \geq 0$. But

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

Hence, $a - (q + 1)b = r - b \in S$ which contradicts the minimality of r. Hence, $0 \leq r < b$. This completes the proof of existence.

Now, we will show the uniqueness of q and r. Suppose there exist q_1, q_2, r_1, r_2 such that $a = q_1 b + r_1$, $a = q_2 b + r_2$, $0 \leq r_1, r_2 < b$. Subtracting the two equations, we get

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

Since $0 \leq r_1, r_2 < b$, we have $-b < r_2 - r_1 < b$, or,

$$|r_2 - r_1| < b.$$

Therefore, $|q_1 - q_2|b < b$, which implies,

$$0 \leq |q_1 - q_2| < 1$$

So, $r_2 - r_1 = 0 \Rightarrow r_1 = r_2$ and $q_1 = q_2$. This completes the proof of uniqueness. □

§ 2.2 Primes & Related Theorems

Definition 2.2 (Prime Number)**.** An element $p \in \mathbb{N}$ and $p > 1$ is called a prime number if for all $q \in \mathbb{N}$, $q \mid p \Rightarrow q = 1$ or $q = p$.

Equivalently, $p > 1$ is prime if $Div(p) = \{\pm 1, \pm p\}$.

Example 2.1. $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59$ etc. are primes. ◇

Example 2.2 (Biggest Prime)**.** As of writing this note, the biggest known prime number is

$$2^{136279841} - 1.$$

◇

Theorem 2.2 (Existence of Prime Factorization)**.** Every positive integer greater than 1 can be written as a product of primes.

Proof. Assume for the sake of contradiction, that there exits a positive integer greater than 1 that cannot be written as a product of primes. By well-ordering principle, we will have a least n of this sort. If n is prime, then it is already a product of primes (just itself), which is a contradiction.

If n is composite, then it can be written as $n = a \cdot b$, for some $a, b \in \mathbb{N}$ where $1 < a, b < n$. Since $a, b < n$, they can be written as a product of primes. So, $n = a \cdot b$ can also be written as a product of primes, which is again a contradiction.

Hence, every positive integer greater than 1 can be written as a product of primes. □

We can extend this concept to negative integers as well by including -1 as a

factor. For any integer $n \neq 0$,

$$n = (-1)^{\varepsilon(n)} \prod_{i=1}^{k} p_i^{a(p_i)},$$

where $\varepsilon(n) = 0$ if $n > 0$ and 1 otherwise. And $a(p_i)$ is called *order of* n *at* p_i which is a non-negative integer such that $p^a \mid n$ but $p^{a+1} \nmid n$.

Next lemma requires a theorem which we will just state but not prove.

Theorem 2.3 (Bezout's Identity)**.** Given two integers a and b, not both of which are zero, there exist $x, y \in \mathbb{Z}$ such that

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

Lemma 2.1. If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. If $p \mid a$, then we are done. So, assume $p \nmid a$. Let $g = gcd(a, p)$. Since, p is a prime $g = 1$ or $g = p$ (which is not possible). Hence, $g = 1$. By Bezout's Identity, there exist $x, y \in \mathbb{Z}$ such that $px + ay = 1$. Multiplying both sides by b, we get

$$bpx + aby = b.$$

In the equation, left side is divisible by p, so is the right side. Hence, $p \mid b$. □

Corollary 2.1. If p is a prime and $p \mid a_1 a_2 \dots a_n$, then $p \mid a_i$ for some i.

Proof. We will prove this by induction on n. For $n = 1$, the statement is trivial. When $n = 2$, the result is the content of Lemma 2.1. Assume the result is true for $n = k$. We will show that it is true for $n = k + 1$. By Lemma 2.1, $p \mid a_1 a_2 \dots a_k$ or $p \mid a_{k+1}$. Let $p \mid a_1 a_2 \dots a_{k+1}$. By induction hypothesis, $p \mid a_1 a_2 \dots a_k$ implies $p \mid a_i$ for some i and we are done. Otherwise, $p \mid a_{k+1}$. This completes the proof. □

Theorem 2.4 (Fundamental Theorem of Arithmetic)**.** Every positive integer greater than 1 can uniquely be written as a product of primes (upto reordering).

Proof. Existence is already proved in theorem 2.2. We will now show uniqueness. Assume for the sake of contradiction that there exists a positive integer greater than 1 that can be written as a product of primes in two different ways. Let n be the smallest such number. Let $n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$ where p_i, q_i are primes. Since $p_1 \mid q_1 q_2 \dots q_l$, by Corollary 2.1, $p_1 \mid q_i$ for some i. WLOG, let $p_1 \mid q_1$. Since q_1 is prime, $p_1 = q_1$. Let, $n' =$

$p_2p_3 \dots p_k = q_2q_3 \dots q_l$. Clearly, $n > n'$ which contradicts the minimality of n. Hence, every positive integer greater than 1 can uniquely be written as a product of primes. □

Theorem 2.5. There are infinitely many primes.

Proof. Assume for the sake of contradiction that there are finitely many primes, say $p_1, p_2, \dots, p_n$. Consider the number $N = p_1p_2 \dots p_n + 1$. Since $N > 1$, it can be written as a product of primes. But none of $p_1, p_2, \dots, p_n$ divides N as N leaves a remainder of 1 when divided by any of p_i. Hence, N is a prime which is not in the list $p_1, p_2, \dots, p_n$. This contradicts the assumption that there are finitely many primes. □

Definition 2.3 (Riemann Zeta Function)**.** The Riemann Zeta function is defined as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

where the function is defined for $s \in \mathbb{R}$ (in this context) and $s > 1$.

Theorem 2.6 (Euler's Product Formula)**.** For $s > 1$, we have

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

Proof. The geometric series formula gives us,

$$\frac{1}{1 - p^{-s}} = \sum_{m=0}^{\infty} \frac{1}{p^{ms}}.$$

So,

$$\prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} = \prod_{p \text{ prime}} \sum_{m=0}^{\infty} \frac{1}{p^{ms}} = \sum_{n=1}^{\infty} a_n \frac{1}{n^s}.$$

By Fundamental Theorem of Arithmetic, $a_n = 1$ for all n. Hence, the product is equal to $\zeta(s)$. □

Now, set $s = 1$ in Euler's Product Formula to get

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

Left side is the harmonic series which diverges to ∞. So, the product on the right side must also diverge to ∞ which requires the product on the right side to be over infinite index. This implies that we must have infinitely many primes.

§ 2.3 Distribution of Primes

Gauss conjectured that the density of primes is approximately given by:

$$\frac{1}{\log x}$$

Let $\pi(x)$ denote the number of primes less than or equal to x. Then, an asymptotic estimate for $\pi(x)$ is:

$$\pi(x) \sim \frac{x}{\log x}$$

In asymptotic notation, if $f(x) \sim g(x)$, it means:

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

A more refined approximation is given by the logarithmic integral:

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

The **Prime Number Theorem (PNT)** states that:

$$\pi(x) \sim \mathrm{Li}(x),$$

which was proven in 1896.

Von Mangoldt's Explicit Formula: Von Mangoldt's explicit formula connects the sum of the von Mangoldt function $\Lambda(n)$ to the nontrivial zeros of the Riemann zeta function. It is a key result in analytic number theory, particularly in understanding the distribution of prime numbers.

Define the von Mangoldt function $\Lambda(n)$ as:

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

The Chebyshev function $\psi(x)$ is given by:

$$\psi(x) = \sum_{n\leq x} \Lambda(n).$$

Von Mangoldt's explicit formula states:

$$\psi(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \log 2\pi - \frac{1}{2}\log(1 - x^{-2}),$$

where the sum runs over all the nontrivial zeros ρ of the Riemann zeta function $\zeta(s)$.

3
Abstract Algebra Review

§ 3.1 Groups

Definition 3.1 (Binary Operation)**.** A binary operation $*$ on a set G is a function $* : G \times G \longrightarrow G$. For any $a, b \in G$, we will write $a * b$ for $*(a, b)$.

Definition 3.2 (Group)**.** A group is an ordered pair $(G, *)$, where G is a set and $*$ is a binary operation on G satisfying the following axioms:

- **Associativity:** $(a * b) * c = a * (b * c)$; for all $a, b, c \in G$.
- **Identity:** There exists an element $e \in G$, called identity of G, such that for all $a \in G, a * e = e * a = a$.
- **Inverse:** For all $a \in G$, there exists $b \in G$ such that $a * b = b * a = e$. We call b is the inverse of a and write $b = a^{-1}$.

Informally, we say G *is a group under* $*$, if $(G, *)$ is a group, or just G *is a group* when the operation $*$ is clear from the context.

Example 3.1. $(\mathbb{Q}, +), (\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Q} \setminus \{0\}, \times)$. ◇

Example 3.2. Define

$$M_{2\times 2}(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}.$$

Then with usual matrix addition $+$, $(M_{2\times 2}(\mathbb{R}), +)$ forms a group. ◇

Proof. We check the group axioms:

1. **Closure:** Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ be two elements of $M_{2\times 2}(\mathbb{R})$. Then, $A + B = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$ is also an element of $M_{2\times 2}(\mathbb{R})$. So, $M_{2\times 2}(\mathbb{R})$ is closed under addition.
2. **Associativity:** Matrix addition is associative.
3. **Identity:** The zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ is the identity element.
4. **Inverses:** For any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the inverse is $-A = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$. So, inverses exist.

Hence, $(M_{2\times 2}(\mathbb{R}), +)$ is a group. □

Non-example. Define

$$M_{2\times 2}(\mathbb{N}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{N} \right\}.$$

Then, $(M_{2\times 2}(\mathbb{N}), +)$ is not a group because inverses do not exist.

Definition 3.3. A group G is called *abelian* (or *commutative*) if $a * b = b * a$, for all $a, b \in G$. Otherwise, it is called *non-abelian* (or *non-commutative*).

Example 3.3. $(R, +), (M_{2\times 2}(\mathbb{R}), +)$ are abelian groups. ◇

Definition 3.4 (Cycilc Group & Generators)**.** A group G is called *cyclic* if there exists an element $g \in G$ such that $G = \{g^n : n \in \mathbb{Z}\}$. Moreover, g is called a *generator* of G.

§ 3.2 Rings

We add additional structure on abelian groups and define rings.

Definition 3.5 (Ring)**.** A set R together with two binary operations $+$ and $\times$ (called addition and multiplication respectively) is a ring denoted by $(R, +, \times)$ if the following axioms are satisfied:

1. $(R, +)$ is an abelian group.
2. $\times$ **is associative:** $(a \times b) \times c = a \times (b \times c)$ for all $a, b \in R$.
3. **Distributive Law:** $(a + b) \times c = (a \times c) + (b \times c)$ and $a \times (b + c) = (a \times b) + (a \times c)$ for all $a, b, c \in R$.

Example 3.4. We can easily check that $(\mathbb{Z}, +, \times), (\mathbb{Q}, +, \times), (\mathbb{R}, +, \times)$ are all rings. ◇

Example 3.5. Define $M_{2\times 2}(\mathbb{R})$ as before. Then, $(M_{2\times 2}(\mathbb{R}), +, \times)$ is a ring. ◇

Proof. We have seen earlier, $(M_{2\times 2}(\mathbb{R}), +)$ is an abelian group. So we left to check the closure, associative and distributive law (over addition) of $\times$.

2. Closure: Let $A, B, C \in M_{2\times 2}(\mathbb{R})$.

The (i, j)-th entry of AB is given by:

$$(ab)_{ij} = \sum_{m=1}^{2} a_{im} b_{mj} \in \mathbb{R}; 1 \leq i, j \leq 2.$$

Both i, j runs from 1 to 2, so we again get a 2×2 matrix and hence, multiplication is closed.

Now we prove that

$$(AB)C = A(BC).$$

The (i,j)-th entry of $(AB)C$ is given by:

$$[(ab)c]_{ij} = \sum_{m=1}^{2} (ab)_{im} C_{mj}.$$

Expanding $(ab)_{im}$:

$$(ab)_{im} = \sum_{k=1}^{2} a_{ik} b_{km},$$

substituting it back:

$$[(ab)c]_{ij} = \sum_{m=1}^{2} \left(\sum_{k=1}^{2} a_{ik} b_{km} \right) c_{mj}$$

$$= \sum_{k=1}^{2} a_{ik} \left(\sum_{m=1}^{2} b_{km} c_{mj} \right) = \sum_{k=1}^{2} a_{ik} (bc)_{kj} = [a(bc)]_{ij}.$$

Thus, $(AB)C = A(BC)$, proving associativity.

2. Distributive Law: The (i,j)-th entry of $A(B+C)$ is:

$$[a(b+c)]_{ij} = \sum_{k=1}^{2} a_{ik} (b+c)_{kj}.$$

By definition of matrix addition:

$$(b+c)_{kj} = b_{kj} + c_{kj},$$

substituting:

$$[a(b+c)]_{ij} = \sum_{k=1}^{2} a_{ik} (b_{kj} + c_{kj}) = \sum_{k=1}^{2} a_{ik} b_{kj} + \sum_{k=1}^{2} a_{ik} c_{kj} = (ab)_{ij} + (ac)_{ij},$$

which proves

$$A(B+C) = AB + AC.$$

Similarly, we can prove $(B+C)A = BA + CA$.

Matrix multiplication is closed, associative and distributes over addition, therefore the proof is complete.

□

A ring not necessarily has a multiplicative identity.

Example 3.6. $(2\mathbb{Z}, +, \times)$ is a ring (an easy check!) but does not have a multiplicative identity. ◇

However, when it does have a multiplicative identity, we call it a *ring with identity*.

Definition 3.6 (Ring with Identity)**.** A ring is said to *have an identity* if there is an element $1 \neq 0$ such that

$$1 \times a = a \times 1 = a, \text{ for all } a \in R.$$

We call R a *ring with identity.*

Definition 3.7 (Commutative Ring)**.** A ring is said to be *commutative* if multiplication $\times$ is commutative.

Examples given earlier include rings with identity and commutative rings.

Example 3.7 (Direct Product of Rings)**.** Let R_1 and R_2 be rings. Then, the set $R_1 \times R_2$ with component-wise addition and multiplication is a ring. ◇

Proof. We check the ring axioms:

1. **Closure:** Let $(a_1, a_2), (b_1, b_2) \in R_1 \times R_2$. Then, $(a_1 + b_1, a_2 + b_2) \in R_1 \times R_2$.
2. **Associativity:** Component-wise multiplication is associative.
3. **Distributive Law:** Distributive law holds for component-wise addition and multiplication.

Hence, $R_1 \times R_2$ is a ring. □

Definition 3.8 (Polynomial Ring)**.** Let R be a ring, x be an indeterminate and define $R[x]$ be the set of all formal sums

$$R[x] := a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum a_i x^i.$$

Given two polynomials $f = \sum a_i x^i$ and $g = \sum b_i x^i$ in $R[x]$, the sum of f and g is defined as

$$f + g = \sum (a_i + b_i) x^i,$$

(where we have implicitly assumed that $m \leq n$ and we set $b_i = 0$ for $i > m$). And the product of f and g as

$$f \cdot g = \sum_i (\sum_j a_j b_{i-j}) x^i.$$

With this rule of addition and multiplication, $R[x]$ becomes a ring, called *polynomial ring.*

In the definition above, each $a_i \in R$ is called the coefficients of the polynomial; a_i is the coefficient of x^i and the zero element given as the polynomial with zero coefficients.

§ 3.3 Ring Homomorphism

Definition 3.9 (Ring Homomorphisms)**.** Let R and S be two rings. A *ring homomorphism* $\varphi : R \to S$ is a map satisfying the following:

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$ for all $a, b \in R$,
2. $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in R$.

Definition 3.10 (Isomorphism)**.** A bijective ring homomorphism is called an *isomorphism*.

Definition 3.11 (Kernel and Image of Ring)**.** For rings, the *kernel* is the set of all elements in R that get mapped to $0 \in S$. In symbols,

$$\ker \varphi = \{r \in R : \varphi(r) = 0\}.$$

The *image* of φ is the set of all elements in S that are mapped from R. In symbols,

$$\operatorname{Im} \varphi = \{s \in S : s = \varphi(r) \text{ for some } r \in R\}.$$

Theorem 3.1. Let R and S be rings and let $\varphi : R \to S$ be a ring homomorphism. Then φ is injective if and only if *ker* $\varphi = \{0\}$.

Proof. ($\Rightarrow$) Suppose φ is injective. Let $r \in \ker \varphi$. Then, $\varphi(r) = 0 = \varphi(0)$. Since φ is injective, $r = 0$. Hence, $\ker \varphi = \{0\}$.

($\Leftarrow$) Suppose $\ker \varphi = \{0\}$. Let $r_1, r_2 \in R$ such that $\varphi(r_1) = \varphi(r_2)$. Then, $\varphi(r_1 - r_2) = 0$. Since $\ker \varphi = \{0\}$, $r_1 - r_2 = 0 \Rightarrow r_1 = r_2$. Hence, φ is injective. □

§ 3.4 Fields

Definition 3.12 (Division Ring)**.** A ring with identity 1, where $1 \neq 0$, is called a *division ring*, if every element $a \neq 0 \in R$ has a multiplicative inverse, that is, there exists $b \in G$ such that

$$a \times b = b \times a = 1.$$

Definition 3.13 (Field)**.** A commutative division ring is called *field*.

Example 3.8. $\mathbb{Z}, \mathbb{Q}, \mathbb{C}, \mathbb{R}$ are all examples of ring and commutative ring. Excluding $\mathbb{Z}$, all of them are division ring, so are fields. ◇

4
Congruences

"If mathematics is the queen of sciences and number theory the queen of mathematics as Gauss said, then we may add that the *Disquisitiones Arithmeticae* is the Magna Charta of number theory"

— Moritz Cantor

Theory of Congruences is another approach to the divisibility problems. The concept and the notation that makes it such a powerful tool, was first introduced by Carl Friedrich Gauss in his book *Disquisitiones Arithmeticae*.

Definition 4.1 (Congruence modulo m)**.** If $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$, we say a *is congruent to* b *modulo* m if $m \mid (a - b)$ and write it as

$$a \equiv b \pmod{m}.$$

Example 4.1. Let $m = 5$. Then 2 and 7 are congruent modulo 5 because $5 \mid (7 - 2)$. ◇

Example 4.2 (Why congruence is a useful tool)**.** Prove that the following equation has no integral solution:

$$x^2 - 3y^3 - 2 = 0.$$

◇

Proof. A useful technique to prove non-existence of integral solution is to consider the equation modulo some well-chosen integer n; because if there are no solution modulo n, then there are no solution over the integers. Let's consider the equation modulo 3.

Taking both sides modulo 3, we get

$$x^2 - 2 \equiv 0 \pmod{3}.$$

The possible remainders when divided by 3 are $0, 1, 2$. But

$$0^2 - 2 \not\equiv 0 \pmod{3},\ 1^2 - 2 \not\equiv 0 \pmod{3},\ 2^2 - 2 \not\equiv 0 \pmod{3}.$$

Hence, this equation has no solution modulo 3 implying there's no integral solution either. □

§ 4.1 Basic Properties of Congruences

Proposition 4.1. Let $a, b, c, d \in \mathbb{Z}$ and fix $m \in \mathbb{N}$. Then the following are true:

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

Proof. 1. $a \equiv a \pmod{m}$ because $m \mid (a - a)$.

2. If $a \equiv b \pmod{m}$, then $m \mid (a - b)$ implies $m \mid (b - a)$, so $b \equiv a \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m \mid (a-b)$ and $m \mid (b-c)$ implies $m \mid (a - b + b - c) = (a - c)$, so $a \equiv c \pmod{m}$.

□

Furthermore,

Proposition 4.2 (Operations with Congruences)**.** Congruences are preserved under addition, multiplication, and exponentiation, i.e., given that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, the following also hold:

1. $a + c \equiv b + d \pmod{m}$, $\quad ac \equiv bd \pmod{m}$.
2. $a + c \equiv b + c \pmod{m}$, $\quad ac \equiv bc \pmod{m}$.
3. $a^n \equiv b^n \pmod{m}$ $\quad$ for all $n \in \mathbb{N}$.

Proof. Using basic divisibility properties and division algorithm, these properties are easy to verify. □

Congruence makes certain types of computations easier to carry out.

Example 4.3. Show that 41 divides $2^{20} - 1$. ◇

Proof. We begin by

$$2^5 \equiv -9 \pmod{41}.$$

Using Proposition 4.2 we have

$$(2^5)^4 \equiv (-9)^4 \pmod{41} \Rightarrow 2^{20} \equiv 81^2 \pmod{41}.$$

But

$$81 \equiv -1 \pmod{41} \Rightarrow 81^2 \equiv 1 \pmod{9}.$$

Therefore, we have

$$2^{20} \equiv 81^2 \equiv 1 \pmod{41}.$$

Which means $41 \mid 2^{20} - 1$. □

Theorem 4.1. If $ac \equiv bc \pmod{m}$ then $a \equiv b \left(\frac{m}{\gcd(m,c)}\right)$. The converse also holds.

Proof. Let $d = \gcd(m, c)$. Then there exist m', c' such that $m = dm'$ and $c = dc'$ with $\gcd(m', c') = 1$.

From $ac \equiv bc \pmod{m}$, we have $m \mid (ac - bc)$ which implies $m \mid c(a - b)$ which is $dm' \mid dc'(a - b)$ which implies $m' \mid c'(a - b)$. Since $\gcd(m', c') = 1$, we have $m' \mid (a - b)$ which is equivalent to

$$a \equiv b \left(\frac{m}{gcd(m, c)}\right),$$

since $m' = \frac{m}{d} = \frac{m}{gcd(m,c)}$. This completes the proof of the first part.

For the converse, if $a \equiv b \left(\frac{m}{\gcd(m,c)}\right)$, then for some $k, (a - b) = k\frac{m}{gcd(m,c)} \Rightarrow ac - bc = m\left(k\frac{c}{gcd(m,c)}\right) = m \times l$ for some $l \in \mathbb{Z}$ which is $ac \equiv bc \pmod{m}$. This completes the proof. □

Corollary 4.1 (Cancellation Law)**.** If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

§ 4.2 $\mathbb{Z}/m\mathbb{Z}$ & Its Algebraic Structure

Definition 4.2 (Congruence modulo m)**.** Fix $m \in \mathbb{Z}$. Define a relation $\sim$ on $\mathbb{Z}$ called *congruence modulo* m. For $a, b \in \mathbb{Z}$ we say

$$a \sim b \text{ if } a \equiv b \pmod{m}$$

Lemma 4.1. Congruence modulo m defines an equivalence relation on $\mathbb{Z}$. Furthermore, it partitions $\mathbb{Z}$ into m equivalence classes we will call them *residue classes*.

Proof. As proven in proposition 4.1 congruence modulo m satisfies reflexive, symmetric and transitive property. Hence it is an equivalence relation.

We know an equivalence relation partitions a set into disjoint equivalence classes.

$a, b \in \mathbb{Z}$ are in the same equivalence class if and only if $m \mid (a - b)$ which is equivalent to saying a and b have the same remainder when divided by m.

Since there are m possible remainders when divided by m and remainder is unique, hence there are exactly m equivalence classes. □

Definition 4.3 ($\mathbb{Z}/m\mathbb{Z}$)**.** Define the equivalence class of a modulo m as

$$[a]_m = \{a + km : k \in Z\}.$$

The set of all equivalence classes modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$.

Furthermore, define two operations addition (denoted by $+$) and multiplication (denoted by $\cdot$) on $\mathbb{Z}/m\mathbb{Z}$ as follows:

For $a, b \in \mathbb{Z}/m\mathbb{Z}$,

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

Notation. $[a]_m$ is simply written as $[a]$ or $\overline{a}$ when m is clear from the context.

Proposition 4.3. $(\mathbb{Z}/m\mathbb{Z}, +, \times)$ forms a commutative ring with identity.

Proof. Firstly, we will prove $(\mathbb{Z}/m\mathbb{Z}, +)$ is an abelian group.

1. **Closure:** By definition, for all $[a], [b] \in \mathbb{Z}/m\mathbb{Z}, [a + b] \in \mathbb{Z}/m\mathbb{Z}$.
2. **Associativity:** Let $[a], [b], [c] \in \mathbb{Z}/m\mathbb{Z}$. Then

   $$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c].$$

   Since, addition is associative in $\mathbb{Z}$, we have

   $$[(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c]).$$

3. **Additive Identity:** For all $[a] \in \mathbb{Z}/m\mathbb{Z}$, we have $[0] \in \mathbb{Z}/m\mathbb{Z}$ such that

   $$[a] + [0] = [a + 0] = [a].$$

   And Similarly,

   $$[0] + [a] = [0 + a] = [a].$$

4. **Inverse:** For all $[a] \in \mathbb{Z}/m\mathbb{Z}$, we have $[m - a] \in \mathbb{Z}/m\mathbb{Z}$ such that

   $$[a] + [m - a] = [a + m - a] = [m] = [0].$$

   Similarly,

   $$[m - a] + [a] = [0].$$

5. **Commutativity:** Since addition in integer is commutative, for all $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$,

   $$[a] + [b] = [a + b] = [b + a] = [b] + [a].$$

Hence, $(\mathbb{Z}/m\mathbb{Z}, +)$ is indeed an abelian group.

Using similar arguments, we can show multiplication in $\mathbb{Z}/m\mathbb{Z}$ is **closed, associative, commutative** and **multiplicative identity** exists.

6. **Distributive Law:** From distributive law in $\mathbb{Z}$ it follows that for all $[a], [b], [c] \in \mathbb{Z}/m\mathbb{Z}$,

$$[a]([b]+[c]) = [a]\times[b+c] = [a(b+c)] = [ab+ac] = [ab]+[ac] = [a][b]+[a][c].$$

Similarly,

$$([b] + [c])[a] = [b][a] + [c][a].$$

Hence, $(\mathbb{Z}/m\mathbb{Z}, +, \times)$ forms a commutative ring with identity. □

Definition 4.4 (Unit in $\mathbb{Z}/m\mathbb{Z}$)**.** An element $a \in \mathbb{Z}/m\mathbb{Z}$ is called a *unit* if there exists $b \in \mathbb{Z}/m\mathbb{Z}$ such that

$$a \cdot b = 1.$$

Definition 4.5 (Group of Units of $\mathbb{Z}/m\mathbb{Z}$)**.** The set of all units of $\mathbb{Z}/m\mathbb{Z}$ is called the *Group of Units of* $\mathbb{Z}/m\mathbb{Z}$. In symbol, group of units of $\mathbb{Z}/m\mathbb{Z}$

$$U(\mathbb{Z}/m\mathbb{Z}) = \{a \in \mathbb{Z}/m\mathbb{Z} : gcd(a, m) = 1\}.$$

Lemma 4.2. $U(\mathbb{Z}/m\mathbb{Z})$ forms a group under multiplication modulo m.

Example 4.4 (Not every element of $\mathbb{Z}/m\mathbb{Z}$ is a unit)**.** Consider $\mathbb{Z}/6\mathbb{Z}$. The element $[5]$ is a unit because

$$[5] \cdot [5] = [25] = [1].$$

However, $[2]$ is not a unit. To see this, we check its products with all elements in $\mathbb{Z}/6\mathbb{Z}$:

$$[2] \cdot [0] = [0], \quad [2] \cdot [1] = [2], \quad [2] \cdot [2] = [4],$$
$$[2] \cdot [3] = [0], \quad [2] \cdot [4] = [2], \quad [2] \cdot [5] = [4].$$

Hence, $[2]$ is not a unit in $\mathbb{Z}/m\mathbb{Z}$. ◇

This example shows that not every element in $\mathbb{Z}/m\mathbb{Z}$ is a unit. But, an element $a \in \mathbb{Z}/m\mathbb{Z}$ is a unit if and only if the equation

$$a \cdot x \equiv 1 \pmod{m}$$

has a solution. Equations of this form are called *linear congruences*, and we will study them in the next section and prove results that will tell when equations of this form has a solution.

§ 4.3 Linear Congruences

Definition 4.6 (Linear Congruence)**.** An equation of the form

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

is called a *linear congruence*. An integer x_0 is called a solution to this equation if $ax_0 \equiv b \pmod{m}$.

Notice, x_0 is a solution to $ax \equiv b \pmod{m}$ is equivalent to $m \mid (ax_0 - b)$, which is equivalent to $my_0 = ax_0 - b$, for some $y_0 \in \mathbb{Z}$.

Theorem 4.2. The linear congruence $ax \equiv b \pmod{m}$ has a solution if and only if $d \mid b$, where $d = gcd(a, m)$. Furthermore, if $d \mid b$, then it has d mutually incongruent solutions modulo m.

Proof. ($\Rightarrow$) Say the equation $ax \equiv b \pmod{m}$ has a solution x_0. Then there exists $y_0 \in \mathbb{Z}$ such that

$$my_0 = ax_0 - b \Rightarrow ax_0 - my_0 = b.$$

Here, $d \mid a, d \mid m$, so $d \mid ax_0 - my_0$. Hence, $d \mid b$.

($\Leftarrow$) Conversely, suppose $d \mid b$. Then there is $c \in \mathbb{Z}$ such that $c = b/d$.

Since $d = gcd(a, m)$, there exists x_0, y_0 such that

$$ax_0 - my_0 = d.$$

Multiplying both sides with c, we have

$$a(cx_0) - m(cy_0) = dc = b.$$

Which is equivalent to saying cx_0 is a solution to the equation $ax \equiv b \pmod{m}$.

Now we will prove there are exactly d incongruent solutions. Let x_0 be a solution to this equation. It is clear that $x_0 + \frac{m}{d}t, t \in \mathbb{Z}$ is a solution to this equation also. Let x' be any other solution to this equation. Then there exists $y_0, y' \in \mathbb{Z}$ such that

$$ax_0 - my_0 = b = ax' - my'$$

$$\Rightarrow a(x_0 - x') = y' - y_0$$

$$\Rightarrow \frac{a}{d}(x_0 - x') = \frac{m}{d}(y' - y_0)$$

Since $gcd(a/d, m/d) = 1, \frac{m}{d} \mid x_0 - x'$.

Hence, for $t \in \mathbb{Z}$, we have $x' = x_0 + \frac{m}{d}t$. So any solution to this congruence has this form.

Now, we will argue the solutions we get for the values $t = 0, 1, \cdots, d-1$ are all incongruent and all other such integers x' are congruent to one of former solutions.

If it happened that

$$x_0 + \frac{m}{d}t_1 \equiv x_0 + \frac{m}{d}t_2 \pmod{m},$$

where $0 \leq t_1 < t_2 \leq (d-1)$, then we would have

$$\frac{m}{d}t_1 \equiv \frac{m}{d}t_2 \pmod{m}.$$

Since $gcd(m/d, m) = m/d$, therefore previous congruence implies

$$t_1 \equiv t_2 \pmod{d} \Rightarrow d \mid t_2 - t_1,$$

which is impossible in view of the inequality $0 < t_2 - t_1 < d$. So, we have d incongruent solutions so far. It remains to argue that any other solution $x_0 + \frac{n}{d}t, t \geq d$ is congruent modulo m to one of these d integers. The Division Algorithm permits us to write t as $t = qd + r$, where $0 \leq r \leq d-1$. Hence

$$\begin{aligned} x_0 + \frac{m}{d}t &= x_0 + \frac{m}{d}(qd + r) \\ &= x_0 + mq + \frac{m}{d}r \\ &\equiv x_0 + \frac{m}{d}r \pmod{m} \end{aligned}$$

with $x_0 + \frac{m}{d}r$ being one of our d selected solutions. This ends the proof. □

Corollary 4.2. The linear congruence $ax \equiv b \pmod{m}$ has a unique solution mod m if and only if $gcd(a, m) = 1$

Now, coming back to the question "When $a \in \mathbb{Z}/m\mathbb{Z}$ is a unit?", we can now state the following proposition.

Proposition 4.4. An element a of $\mathbb{Z}/m\mathbb{Z}$ is a unit iff $gcd(a, m) = 1$.

Corollary 4.2 has an equivalent from in terms of maps from $\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$.

Corollary 4.3 (Equivalent to corrolary 4.2)**.** Define $\varphi_a : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ such that

$$\varphi_a(x) = ax \pmod{m}$$

The map is bijective if and only if $gcd(a, m) = 1$.

Proof. ($\Leftarrow$) Let $gcd(a, m) = 1$, we have to prove φ_a is bijective.

Let $x_1, x_2 \in \mathbb{Z}/m\mathbb{Z}$. And

$$\varphi_a(x_1) = \varphi_a(x_2)$$

$$\Rightarrow ax_1 \equiv ax_2 \pmod{m}$$

Since, $gcd(a, m) = 1$ using cancellation law,

$$\Rightarrow x_1 \equiv x_2 \pmod{m}.$$

Hence, φ_a is injective.
Choose $b\mathbb{Z}/m\mathbb{Z}$. Since, $gcd(a, m) = 1$ there exist $x_0, y_0 \in \mathbb{Z}$ such that

$$ax_0 + my_0 = 1$$

$$\Rightarrow abx_0 + mby_0 = b.$$

Reduce this equation mod m, then we get

$$abx_0 \equiv b \pmod{m}.$$

Hence, we have $[bx_0] \in \mathbb{Z}/m\mathbb{Z}$ such that $\varphi_a([bx_0]) = b$, which prove φ_a is surjective[a] and completes verifying bijectivity of φ_a.
($\Rightarrow$) Let φ_a be bijective. We will prove $gcd(a, m) = 1$.
Since $[1] \in \mathbb{Z}/m\mathbb{Z}$, surjectivity of φ_a implies there exists $x_0 \in \mathbb{Z}/m\mathbb{Z}$ such that $ax_0 = [1]$ which is equivalent to saying $ax_0 \equiv 1 \pmod{m}$, which means there is $y_0 \in \mathbb{Z}$ such that

$$ax_0 - my_0 = 1,$$

where $gcd(a, m)$ divides left side of the equation, so is the right side. Which means $gcd(a, m) \mid 1$, and that implies $gcd(a, m) = 1$. Which proves the forward direction. □

[a] We could do even better. Here domain and co-domain are finite and are of same cardinality, so injectivity implies surjectivity (automatically).

Similarly we could prove

Corollary 4.4. If $gcd(a, m) = 1$, then the map $\varphi_a : U(\mathbb{Z}/m\mathbb{Z}) \to U(\mathbb{Z}/m\mathbb{Z})$ such that $\varphi(x) = ax \pmod{m}$ is a bijection.

Proposition 4.5. If p is a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof. If p is prime, then for all $a \neq 0 \in \mathbb{Z}/p\mathbb{Z}$, $gcd(a, p) = 1$. Hence, each nonzero $a \in \mathbb{Z}/p\mathbb{Z}$ has multiplicative inverse. So $\mathbb{Z}/p\mathbb{Z}$ is a division ring, which is also commutative as previously proven. Therefore $\mathbb{Z}/p\mathbb{Z}$ is a field. □

$\mathbb{Z}/p\mathbb{Z}$ is an example of a finite field.

§ 4.4 Wilson's, Euler's & Fermat's Theorems

Theorem 4.3 (Wilson's Theorem). $p > 1$ is a prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

Proof. Consider the set $S = \{1, 2, \ldots, p-1\}$ of integers modulo p. Since p is prime, every $a \in S$ has a unique inverse a^{-1} modulo p, satisfying $aa^{-1} \equiv 1 \pmod{p}$.

If $a^2 \equiv 1 \pmod{p}$, then $(a-1)(a+1) \equiv 0 \pmod{p}$, implying $a \equiv \pm 1 \pmod{p}$. Thus, all elements in $S \setminus \{1, p-1\}$ pair up with their distinct inverses, contributing a product congruent to 1 modulo p, i.e.,

$$(p-2)! \equiv 1 \pmod{p}$$

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

Conversely, assume p has a non-trivial divisor $d > 1$. Then

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

But

$$-1 \equiv (p-1)! \equiv 0 \pmod{d},$$

which implies $d = 1$ (contradiction!). Hence, We conclude p cannot have non-trivial divisors and hence it is prime. □

Example 4.3 motivates us to find some trick to calculate integer raised to some power modulo m. i.e., we want to find properties of $a, a^2, a^3, \ldots$ modulo m. In number theory, it is often fruitful to reduce a problem to prime cases and then solve for those prime cases, or vice-versa. With respect to this approach, we set $m = p$ where p is a prime and state the following theorem.

Theorem 4.4 (Fermat's Little Theorem)**.** Let p be a prime, and let a be any number with $a \not\equiv 0 \pmod{p}$. Then

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

Proof. Define the map $\varphi_a : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ such that

$$\varphi_a(x) = ax \pmod{p}.$$

Since $gcd(a, p) = 1$, using corollary 4.3, we know φ_a is a bijection and so φ_a is just a permutation.

Then the numbers

$$1, 2, 3, ..., (p-1) \pmod{p}$$

are the same as the numbers

$$a, 2a, 3a, ..., (p-1)a \pmod{p},$$

although they might be in a different order. Which means

$$1, 2, 3, ..., (p-1) \equiv a, 2a, 3a, ..., (p-1)a \pmod{p}$$

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

But p and $(p-1)!$ are co-prime. Hence, we conclude

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

□

And then we have the following generalization of Fermat's Little Theorem.

Theorem 4.5 (Euler's Theorem)**.** If a and n are relatively prime then

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

where $\phi(n) = \#\{u : 1 \leq u \leq n \text{ and } gcd(a, n) = 1\}$.

Proof. The proof is identical to the previous one. Let $A = \{a_1, a_2, ..., a_{\phi(n)}\}$ be the set of all numbers coprime to a. Then the map $\varphi_a : A \to A$ such that $\varphi(x) = ax$ is a bijection according to corollary 4.4.

Since φ_a is a permutation, the numbers

$$a_1, a_2, ..., a_{\phi(n)} \pmod{n}$$

are the same as the numbers

$$aa_1, aa_2, ..., aa_{\phi(n)} \pmod{n},$$

although they might be in a different order. Which means

$$a_1, a_2, \cdots, a_{\phi(n)} \equiv (aa_1)(aa_2)\cdots, (aa_{\phi(n)}) \pmod{n}.$$

Cancelling out all the a_i's from both sides, we get

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

as required. □

We already know group of units $U(\mathbb{Z}/n\mathbb{Z})$ has group structure under multiplication mod n. We can exploit this and provide an alternative proof to Euler's theorem.

Proof (Using group theory)**.** Order of $U(\mathbb{Z}/n\mathbb{Z})$ is $\phi(n)$.

Since $[a] \in U(\mathbb{Z}/n\mathbb{Z})$, Lagrange's theorem states that the order of any element in a finite group divides the order of the group. That is, the order of $[a]$ (i.e., the smallest integer d such that $[a]^d = [1]$) divides $\phi(n)$. This implies:

$$[a]^{\phi(n)} = [1].$$

Rewriting this in terms of modular arithmetic we get

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

completing the proof. □

§ 4.5 Euler's Totient Function & Chinese Remainder Theorem

Definition 4.7 (Euler's Totient Function)**.** Euler's totient function, denoted by $\phi(n)$, is defined as

$$\phi(n) = \#\{k \in \mathbb{Z} \mid 1 \leq k \leq n, \gcd(k, n) = 1\}.$$

That is, $\phi(n)$ counts the number of integers from 1 to n that are coprime to n.

Euler's theorem

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

is a beautiful and powerful result. But it won't be of much use unless we can find an efficient way to compute $\phi(n)$. As usual, we first try to solve for primes.

Proposition 4.6. If p is prime and $\alpha \geq 1$, then

1. $\phi(p) = p - 1$.
2. $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Proof.

1. Since p is prime, the only number in $\{1, 2, \ldots, p\}$ that is not coprime to p is p itself. Thus, all $p - 1$ numbers from 1 to $p - 1$ are coprime to p, giving $\phi(p) = p - 1$.
2. The numbers in $\{1, 2, \ldots, p^\alpha\}$ that are not coprime to p^α are precisely the multiples of p, i.e., $p, 2p, \ldots, p^{\alpha-1}p$. There are $p^{\alpha-1}$ such multiples. Since there are p^α numbers in total, we obtain

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

□

Having established results for $\phi(p)$ and $\phi(p^\alpha)$, we now aim to compute $\phi(n)$ based on the prime factorization of n. This brings us to the multiplicative property of $\phi(n)$.

Theorem 4.6. If $gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Proof. As proven in Example 3.7, direct product of two rings form a ring. Consider the map $h : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ defined by

$$h(x \pmod{mn}) = (x \pmod{m}, x \pmod{n}).$$

We claim h is an isomorphism. h is a homomorphism because for $x, y \in \mathbb{Z}/mn\mathbb{Z}$,

$$h(x+y) = (x+y \pmod m, x+y \pmod n)$$

$$= (x \pmod m + y \pmod m, x \pmod n + y \pmod n)$$

$$= (x \pmod m, x \pmod n) + (y \pmod m, y \pmod n)$$

$$= h(x \pmod{mn}) + h(y \pmod{mn}).$$

Similarly (and tediously), $h(xy) = h(x)h(y)$.

By Theorem 3.1, h is injective iff $\ker h = \{0\}$. Let $x \in \ker h$. Then, $h(x) = (0,0)$. This implies $x \equiv 0 \pmod m$ and $x \equiv 0 \pmod n$. Since $gcd(m,n) = 1$, $x \equiv 0 \pmod{mn}$. Hence, $\ker h = \{0\}$ and h is injective.

To check surjectivity, let $(b \pmod m, c \pmod n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. We have to find $a \pmod{mn}$ such that

$$h(a \pmod{mn}) = (b \pmod m, c \pmod n).$$

So we are basically want to solve the following system of congruences modulo mn:

$$a \equiv b \pmod m$$

$$a \equiv c \pmod n.$$

Our next theorem will ensure that such an a exists.

Hence h is an isomorphism and

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

Then it is immediate that

$$U(\mathbb{Z}/mn\mathbb{Z}) \cong U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z}),$$

via the group isomorphism induced from h. Which means they have the same cardinality, that is

$$|U(\mathbb{Z}/mn\mathbb{Z})| = |U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z})|.$$

But $|U(\mathbb{Z}/mn\mathbb{Z})| = \phi(mn)$ and $|U(\mathbb{Z}/m\mathbb{Z}| \times |\mathbb{Z}/n\mathbb{Z})| = \phi(m)\phi(n)$, therefore we have

$$\phi(mn) = \phi(m)\phi(n),$$

as required. □

Theorem 4.7 (Chinese Remainder Theorem)**.** Let m and n be integers satisfying $gcd(m,b) = 1$, and let $b, c \in \mathbb{Z}$. Then the simultaneous congruences

$$x \equiv b \pmod m \text{ and } x \equiv c \pmod n$$

have a unique solution modulo mn.

Proof. $x \equiv b \pmod{m}$ is equivalent to

$$x = b + my,$$

for some $y \in \mathbb{Z}$. Then the second congruence is the same as

$$b + my \equiv c \pmod{n}$$

$$\Rightarrow my \equiv c - b \pmod{n}.$$

Since $gcd(m, n) = 1$, there exists m' such that $mm' \equiv 1 \pmod{n}$. Multiplying both sides by m', we get

$$y \equiv m'(c - b) \pmod{n},$$

equivalently,

$$y = m'(c - b) + nz$$

for some $z \in \mathbb{Z}$.

substituting y in $x = b + my$, we get

$$x = b + m(m'(c - b) + nz)$$

$$= b + m'm(c - b) + m^2 z$$

$$= b + m'm(c - b) + mnz.$$

Any x satisfies the original two congruences must have this form. We will check if this x satisfies the two congruences.

$$x = b + m'm(c - b) + mnz \equiv b + 0 + 0 = b \pmod{m}$$

and

$$x = b + m'm(c - b) + mnz \equiv b + 1(c - b) + 0 = c \pmod{n}$$

as required.

To prove uniqueness, let $x = x_1$ and $x = x_2$ both satisfy the congruences

$$x \equiv b \pmod{m} \text{ and } x \equiv c \pmod{n}.$$

Then,

$$x_1 \equiv x_2 \pmod{m} \text{ and } x_1 \equiv x_2 \pmod{n}.$$

This implies

$$m \mid x_1 - x_2 \text{ and } n \mid x_1 - x_2.$$

Since $gcd(m, n) = 1$, $mn \mid x_1 - x_2$. Hence, $x_1 \equiv x_2 \pmod{mn}$, proving the uniqueness. □

Remark. We have shown that if $gcd(m, n) = 1$ then Theorem 4.7 (Chinese Remainder Theorem) implies

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

The converse also holds, that is

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

implies the congruences

$$x \equiv b \pmod{m} \text{ and } x \equiv c \pmod{n}$$

have a unique solution modulo mn.

Theorem 4.8 (Generalized Chinese Remainder Theorem)**.** For $k \geq 2$, let $m_1, m_2, \ldots, m_k$ be nonzero integers that are pairwise relatively prime: $(m_i, m_j) = 1$ for $i \neq j$. Then, for all integers $a_1, a_2, \ldots, a_k$, the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_r \pmod{m_k}, \end{aligned}$$

has a solution modulo $M = m_1 m_2 \cdots m_k$.

Proof (Rough)**.** Using ring theory,

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

through the isomorphism

$$x \pmod{M} \mapsto (x \pmod{m_1}, x \pmod{m_2}, \ldots, x \pmod{m_k}),$$

hence the system of congruences has a unique solution modulo M. □

Corollary 4.5. If $m_1, m_2, \ldots, m_k$ are pairwise relatively prime, then

$$\phi(m_1 m_2 \cdots m_k) = \phi(m_1)\phi(m_2)\cdots\phi(m_k).$$

Corollary 4.6. $\phi(n) = n\prod_{i=1}^{k}(1 - p_i^{-1})$, where $p_1, p_2, \ldots, p_k$ are distinct prime factors of n.

Proof.

$$\begin{aligned} \phi(n) &= \phi\left(p_1^{a_1} \cdots p_k^{a_k}\right) \\ &= \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) \\ &= (p_1^{a_1} - p_1^{a_1-1}) \cdots (p_k^{a_k} - p_k^{a_k-1}) \\ &= p_1^{a_1-1}(p_1 - 1) \cdots p_k^{a_k-1}(p_k - 1) \end{aligned}$$

$$= \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1)$$

$$= \prod_{i=1}^{k} p_i^{a_i} \cdot \prod_{i=1}^{k} p_i^{-1}(p_i - 1)$$

$$= n \prod_{i=1}^{k} (1 - p_i^{-1})$$

□

These results allow us to compute congruence related problems for any large power of n by prime factorizing n.

Example 4.5. Compute $(102^{73} + 55)^{37} \pmod{111}$. ◇

Solution. Let $x \equiv (102^{73} + 55)^{37} \pmod{111}$.

We know $111 = 3 \times 37$. Since $gcd(3, 37) = 1$, by Chinese Remainder Theorem, we can compute x modulo 3 and 37 separately.

First, we compute $x \pmod 3$. Since $102 \equiv 0 \pmod 3$, we have

$$102^{73} \equiv 0^{73} = 0 \pmod 3,$$

and $55 \equiv 1 \pmod 3$. Hence,

$$102^{73} + 55 \equiv 0 + 1 = 1 \pmod 3.$$

Therefore,

$$x \equiv (102^{73} + 55)^{37} \equiv 1^{37} = 1 \pmod 3.$$

Next, we compute $x \pmod{37}$.

$102^{73} \equiv (102^{36})^2 \cdot 102 \equiv 1 \cdot 102 \equiv 28 \pmod{37}$ by Fermat's Little Theorem. Replacing this to

$$x \equiv (102^{73} + 55)^{37} \equiv (28 + 55) \equiv 9 \pmod{37}.$$

By procedure used in Theorem 4.7, we solve $x \equiv 1 \pmod 3$ and $x \equiv 9 \pmod{37}$ to get $x \equiv 46 \pmod{111}$.

Proposition 4.7.

1. When $gcd(m, n) \neq 1$, $\phi(mn) = \phi(m)\phi(n)\frac{d}{\phi(d)}$, where $d = gcd(m, n)$.
2. $a \mid b$ implies $\phi(a) \mid \phi(b)$.

Proof. □

§ 4.6 Addendum: Primality Test

A primality test is an algorithm for determining whether an input number is prime. Result's of this chapter can be used to design primality tests.

Wilson's theorem gives a definitive test for primality since it is a biconditional statement. For a prime n,

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

If this condition is not satisfied, n is composite. However, computing $(n-1)! \pmod{n}$ is impractical for large n.

Fermat's Little Theorem provides a faster, probabilistic primality test. It states that if n is prime, for any a such that $\gcd(a, n) = 1$,

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

If this fails for any a, n is composite. If it holds for many a, n is *probably prime*.

Definition 4.8 (Carmichael Number)**.** A composite number n is a *Carmichael number* if it satisfies Fermat's test for all a coprime to n, i.e.,

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

for all a such that $\gcd(a, n) = 1$.

Carmichael numbers, like 561, are composite yet pass Fermat's test for all bases a, making Fermat's test unreliable.

Wilson's and Euler's criteria suggest that primality testing for large numbers is infeasible within a reasonable amount of time, particularly within polynomial time. However, in 2002, three Indian computer scientists—Agrawal, Kayal, and Saxena created a general, polynomial-time, deterministic and unconditionally correct algorithm for primality testing, known as the AKS primality test. Previous algorithms, developed for centuries, achieved three of these properties at most. Hence, primality testing is fundamentally easier than one might expect.

Given that primality testing is in P (class of problems solvable in polynomial time), a natural question arises: can we also factorize a number in polynomial time? The answer remains unknown. It is an important question because modern cryptography assumes that factorization is not in P. This problem can be formulated using mathematics and is now one of the central open problems in computational complexity and mathematics. No formal discipline is close to resolving this question, highlighting the gaps in our fundamental understanding of computation.

5
Structure of $U(\mathbb{Z}/n\mathbb{Z})$

If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then as was shown in the previous chapter,

$$U(\mathbb{Z}/n\mathbb{Z}) \cong U(\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times U(\mathbb{Z}/p_2^{a_2}\mathbb{Z}) \times \cdots \times U(\mathbb{Z}/p_k^{a_k}\mathbb{Z}).$$

Thus to determine the structure of $U(\mathbb{Z}/n\mathbb{Z})$, it is enough to determine the structure of $U(\mathbb{Z}/p^{a_k}\mathbb{Z})$ for p prime and $a \in \mathbb{N}$. We will simplest case of $U(\mathbb{Z}/p\mathbb{Z})$.

§ 5.1 Polynomial ring $\mathbb{Z}/p\mathbb{Z}[x]$

Lemma 5.1. Let $K[x]$ be a polynomial ring over the field K. If $p(x) \in K[x]$ is a non-zero polynomial of degree n, then $p(x)$ has at most n distinct roots in K.

Proof. We use induction. For $n = 1, p(x) = a_0 + a_1 x$ has at most one root given by $x = -a_0 a_1^{-1}$.

Assume the lemma is true for degree $(n-1)$. If $p(x)$ has no roots in K, we are done.

Otherwise, let a be a root of $p(x)$. Then, we can write

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

where $q(x)$ is a polynomial of degree $(n-1)$ and $deg\ r(x) < deg\ (x-a)$.

Furthermore, $r(x) = r_0$, for some $r_0 \in K$. Then we have $r_0 = p(a) - (a-a)q(a) = 0$, since a is a root of $p(x)$. Rewriting $p(x)$ we have,

$$p(x) = (x-a)q(x).$$

By the induction hypothesis, the polynomial $q(x)$ has at most $(n-1)$ roots.

Clearly, any root of $q(x)$ is a root of $p(x)$. And if $b \neq a$ is a root of $p(x)$ then

$$(b-a)q(b) = p(b) = 0 \Rightarrow q(b) = 0,$$

meaning b is also a root of $q(x)$. Thus, $p(x)$ has at most $1 + (n-1) = n$ roots, which completes the proof of the lemma. □

Corollary 5.1. Let $f(x), g(x) \in K[x]$ be two polynomials of degree n. If $f(\alpha_i) = g(\alpha_i)$ for $(n+1)$ distinct $\alpha_1, \alpha_2, ..., \alpha_{n+1} \in K$, then $f = g$.

Proof. Define $h(x) = f(x) - g(x)$. Then $h(\alpha_i) = 0$ for $(n+1)$ distinct α_i. Since $h(x)$ is a polynomial of degree at most n, it has at most n roots. But we have $(n+1)$ roots. Hence, it must be the case that $h(x) = 0$ which implies $f = g$. □

Theorem 5.1. If p is prime, then

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}.$$

Proof. Let $K = \mathbb{Z}/p\mathbb{Z}$. Then we know K is a field. Let $f(x) \in K[x]$ be given by

$$f(x) = x^{p-1} - 1 - (x-1)(x-2)\cdots(x-(p-1)).$$

$f(x)$ has degree less than $(p-1)$.

But according to Fermat's Little Theorem, $x^{p-1} - 1 = 0$ for all $x \in \{1, 2, ..., p-1\}$ and hence $f(x) = 0$ for all $x \in \{1, 2, ..., p-1\}$.

Since $f(x)$ has degree less than $(p-1)$ but has $(p-1)$ roots, it must be the zero polynomial. Hence,

$$0 = x^{p-1} - 1 - (x-1)(x-2)\cdots(x-(p-1)).$$

Rewriting this in terms of congruence, we have

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}.$$

□

Corollary 5.2 (Wilson's Theorem Fowards Direction)**.** p is prime and set $x = 0$ in the above theorem to get

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

Proposition 5.1. If $d \mid p-1$, then $x^d \equiv 1 \pmod{p}$ has exactly d solutions in $\mathbb{Z}/p\mathbb{Z}$.

Proof. Let $dd' = p - 1$. Then

$$\frac{x^{p-1} - 1}{x^d - 1} = \frac{(x^d)^{d'} - 1}{x^d - 1}.$$

Let $y = x^d$. Then we have

$$\begin{aligned}\frac{y^{d'}-1}{y-1} &= \frac{(y-1)(1+y+y^2+\cdots+y^{d'-1})}{y-1}\\ &= 1+y+y^2+\cdots+y^{d'-1}\\ &= 1+x^d+(x^d)^2+\cdots+(x^d)^{d'-1}\\ &= g(x).\end{aligned}$$

Let $f(x) = x^{p-1}-1 = g(x)(x^d-1)$. Reducing this modulo p, we get

$$f(x) \equiv g(x)(x^d-1) \pmod{p}.$$

From Theorem 5.1 We know that $f(x) = x^{p-1}-1$ has $(p-1)$ roots modulo p, which means $g(x)(x^d-1)$ has $(p-1)$ roots modulo p.

Now, $g(x)$ is a polynomial of degree $d(d'-1) = dd'-d = (p-1-d)$. So, it has at most $(p-1-d)$ roots. Since $f(x)$ has $(p-1)$ roots, so does $g(x)(x^d-1)$, hence x^d-1 must have at least d roots modulo p. But we know that x^d-1 has at most d roots in $\mathbb{Z}/p\mathbb{Z}$. Hence, it must have exactly d roots in $\mathbb{Z}/p\mathbb{Z}$, which completes the proof. □

§ 5.2 Group Structure of $U(\mathbb{Z}/n\mathbb{Z})$ & Primitive Roots

Consider the group of units of $\mathbb{Z}/5\mathbb{Z}$, $U(\mathbb{Z}/5\mathbb{Z})$.

Notice the following exponentiation table for $U(\mathbb{Z}/5\mathbb{Z})$:

a	a^1	a^2	a^3	a^4
2	2	4	3	1
3	3	4	2	1

We can see elements of $U(\mathbb{Z}/5\mathbb{Z})$ can be generated by 2 or 3 by raising powers to them, i.e.,

$$U(\mathbb{Z}/5\mathbb{Z}) = (\mathbb{Z}/5\mathbb{Z})^* = \{2^\alpha : \alpha \in \mathbb{N}\} = \{3^\alpha : \alpha \in \mathbb{N}\}.$$

Such a group is called cyclic group.

In the above example, 2 or 3 generates the group $U(\mathbb{Z}/5\mathbb{Z})$, but 4 does not.

Definition 5.1 (Primitve Root)**.** An integer a is called a *primitive root* modulo n if $\overline{a}$ generates the group $U(\mathbb{Z}/n\mathbb{Z})$. Equivalently, an integer a is a *primitive root* modulo n if $\phi(n)$ is the smallest positive integer such that $a^{\phi(n)} \equiv 1 \pmod{n}$.

One can explicitly check that $U(\mathbb{Z}/5\mathbb{Z}), U(\mathbb{Z}/7\mathbb{Z})$ etc. have primitive roots but $U(\mathbb{Z}/8\mathbb{Z})$ for example do not have primitive roots.

Theorem 5.2. If p is prime then $U(\mathbb{Z}/p\mathbb{Z})$ is a cyclic group.

Proof. To be written. □

The theorem above shows existence of primitive roots modulo all prime numbers.

6
Quadratic Reciprocity

When does

$$x^m \equiv b \pmod{n},$$

have a solution? From Theorem 5.1, we know when n is prime, $m \mid n-1$ and $b = 1$, we have exactly m solutions. But that is a special case. In this section, we will resolve when the congruence

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

has a solution. This answer is provided by the law of Quadratic Reciprocity, which was first conjectured by Euler and Legendre and later proved by Gauss. Gauss was extremely proud of this result that he called it the **Theorema Aureum**, the golden theorem. This is probably his most favorite theorem as he provided 6 different proofs for it in his lifetime.

§ 6.1 Quadratic Residues

Definition 6.1 (Quadratic Residue)**.** Let p be an odd prime and $a \in \mathbb{Z}$ with $gcd(a, p) = 1$. We call a a *quadratic residue* if

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

has a solution. Otherwise, we call a a *quadratic non-residue*.

Example 6.1. Let $p = 3$. Then 1 is a quadratic residue modulo 3 as $1^2 \equiv 1 \pmod{3}$. But 2 is a quadratic non-residue modulo 3 as $x^2 \equiv 2 \pmod{3}$ has no solutions.

Explicitly, we can check that $0^2 \equiv 0 \pmod{3}$, $1^2 \equiv 1 \pmod{3}$, and $2^2 \equiv 1 \pmod{3}$. ◇

Example 6.2. Let $p = 5$. Then quadratic residues are: $1, 4$ as $1^2 \equiv 1 \pmod{5}$ and $2^2 \equiv 4 \pmod{5}$.

And quadratic non-residues are: $2, 3$. ◇

Example 6.3. Let $p = 7$. Then quadratic residues are: $1, 2, 4$.

And quadratic non-residues are: $3, 5, 6$. ◇

Example 6.4. Let $p = 11$. Then quadratic residues are: $1, 3, 4, 5, 9$.

And quadratic non-residues are: $2, 6, 7, 8, 10$. ◇

So we state the following proposition.

Proposition 6.1 (# of QR/QNR)**.** There are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues modulo p.

Proof. The quadratic residues modulo p are the numbers $a^2 \pmod{p}$ where $a \in \{1, 2, \cdots p-1\}$. Since

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

we have at most $\frac{p-1}{2}$ distinct quadratic residues, namely $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$.

But in order to show that there are exactly $\frac{p-1}{2}$ quadratic residues, we need to show that the number $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$ are all distinct modulo p. Let $a, b \in \{1, 2, \cdots, \frac{p-1}{2}\}$ such that $a^2 \equiv b^2 \pmod{p}$. Then

$$a^2 - b^2 \equiv 0 \pmod{p} \Rightarrow (a-b)(a+b) \equiv 0 \pmod{p}.$$

Which implies $p \mid (a-b)(a+b) \Rightarrow p \mid (a-b)$ or $p \mid (a+b)$. But $1 \leq a, b \leq \frac{p-1}{2}$, so $2 \leq a+b \leq p-1$. Hence, $p \nmid (a+b)$. So, $p \mid (a-b) \Rightarrow a \equiv b \pmod{p}$. Hence, the numbers $1^2, 2^2, ..., \left(\frac{p-1}{2}\right)^2$ are all distinct modulo p. Therefore, there are exactly $\frac{p-1}{2}$ quadratic residues modulo p.

Since there are $p-1$ nonzero numbers in $\mathbb{Z}/p\mathbb{Z}$ and exactly $\frac{p-1}{2}$ of them are quadratic residues, the remaining $\frac{p-1}{2}$ numbers are quadratic non-residues. □

7
References

1. *An Introduction to the Theory of Numbers* by Ivan Niven, Herbert S. Zuckerman & Hugh L. Montgomery,

2. *A Classical Introduction to Modern Number Theory* by Kenneth F. Ireland & Michael Wayne Rosen.