MAT422: Theory of Numbers

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

Last Updated: February 26, 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 **3**
- 1.1 Number Systems . . . 3
- 1.2 Well-Ordering Principle . . . 3
- 1.3 Goals and Motivation for doing NT . . . 3

2 Divisibility and Primes **4**
- 2.1 Basics of Divisibility . . . 4
- 2.2 Primes & Related Theorems . . . 5
- 2.3 Distribution of Primes . . . 8

3 Abstract Algebra Review **9**
- 3.1 Groups . . . 9
- 3.2 Rings . . . 10
- 3.3 Fields . . . 12

4 Congruences **13**
- 4.1 Basic Properties of Congruences . . . 14
- 4.2 $\mathbb{Z}/m\mathbb{Z}$ & Its Algebraic Structure . . . 15
- 4.3 Linear Congruences . . . 17

5 References **21**

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

Example (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, $n' = p_2 p_3 \dots p_k = q_2 q_3 \dots q_l$. 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 $p_1, p_2, \ldots, p_n$. Consider the number $N = p_1 p_2 \ldots p_n + 1$. Since $N > 1$, it can be written as a product of primes. But none of $p_1, p_2, \ldots, p_n$ 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 $p_1, p_2, \ldots, p_n$. 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. $(\mathbb{Q}, +), (\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{Q} \setminus \{0\}, \times)$. ◇

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

§ 3.2 Rings

We add additional structure on abelian groups and define rings.

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

Example. 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. $(2\mathbb{Z}, +, \times)$ 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 3.5 (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 3.6 (Commutative Ring)**.** A ring is said to be *commutative* if multiplication $\times$ is commutative.

Examples given earlier include rings with identity and commutative rings.

§ 3.3 Fields

Definition 3.7 (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 3.8 (Field)**.** A commutative division ring is called *field*.

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

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

◇

Example (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. □

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

$$a \cdot b = 1.$$

Example (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 4.5 (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

$$\begin{aligned} ax_0 - my_0 = b = ax' - my' \\ \Rightarrow a(x_0 - x') = y' - y_0 \\ \Rightarrow \frac{a}{d}(x_0 - x') = \frac{m}{d}(y' - y_0) \end{aligned}$$

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).

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.

5
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.