BRAC
UNIVERSITY

Inspiring Excellence

MAT422: Theory of Numbers

Lecture notes

Last updated on February 28, 2025

Preface

These notes summarize key concepts from the *MAT422: Theory of Numbers* course taught by *Arnab Chakraborty* at BRAC University in Spring 2025. They provide a structured and precise version of the material discussed in class but do not serve as an exact transcription of the lectures. While every effort has been made to ensure accuracy, errors or omissions may still be present. If you identify any inaccuracies, please feel free to reach out via email:
nafisanazlee3@gmail.com

Nafisa Karim Nazlee

References

- *An Introduction to the Theory of Numbers*, by Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery
- *A Classical Introduction to Modern Number Theory*, by Kenneth F. Ireland and Michael Wayne Rosen

Contents

1

Preliminaries

1.1 Sets of Numbers

The most familiar set of numbers is the set of *natural numbers*, denoted as

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}.$$

The set of natural numbers, $\mathbb{N}$, is sufficient for counting, but it lacks the ability to represent differences. For instance, the equation

$$3 + x = 1$$

has no solution in $\mathbb{N}$, necessitating the introduction of negative numbers, forming the set of integers, $\mathbb{Z}$. By considering the negation of $\mathbb{N}$, we extend our number system to include the *integers*, forming the set

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

However, even $\mathbb{Z}$ is not sufficient. Consider the equation

$$2x = 5$$

This equation has no solution in $\mathbb{Z}$, leading to the need for fractions or *rational numbers*, defined as

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

For example,

$$\mathbb{Q} = \left\{ -\frac{3}{4}, 0, \frac{1}{2}, 2, \frac{5}{3}, \dots \right\}.$$

It can also be expressed as

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z} / \sim$$

where $\sim$ is the equivalence relation given by $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$.
Despite this, $\mathbb{Q}$ is still not sufficient.

Theorem 1.1.1

There is no rational number whose square is 2.

Proof. If x were rational, we could write $x = \frac{p}{q}$ with $p, q \in \mathbb{Z}$ and $\gcd(p, q) = 1$. Substituting, we get

$$\left(\frac{p}{q}\right)^2 = 2 \quad \Rightarrow \quad p^2 = 2q^2.$$

This implies p^2 is even, so p must also be even, say $p = 2k$. Substituting,

$$(2k)^2 = 2q^2 \quad \Rightarrow \quad 4k^2 = 2q^2 \quad \Rightarrow \quad 2k^2 = q^2.$$

Thus, q^2 is also even, meaning q is even. But this contradicts our assumption that $\gcd(p, q) = 1$, proving that no rational number satisfies $x^2 = 2$. $\square$

This leads to the discovery of *irrational numbers*, numbers that cannot be expressed as a fraction of integers. To accommodate such numbers, we construct the real number system, $\mathbb{R}$. The rationals $\mathbb{Q}$ form a subset of the *real numbers*, $\mathbb{R}$, which is obtained as the *completion* of $\mathbb{Q}$ using *Cauchy sequences*. The real numbers include both rationals and irrationals, such as

$$\mathbb{R} = \left\{-\sqrt{5}, -1, 0, \frac{1}{2}, \pi, e, \sqrt{2}, \dots\right\}.$$

Even $\mathbb{R}$ is not enough to solve all equations. Consider

$$x^2 + 1 = 0.$$

Rearranging,

$$x^2 = -1.$$

There is no real number whose square is negative. To resolve this, we introduce a new number i, called the imaginary unit, defined by

$$i^2 = -1.$$

We then extend our number system further by introducing the *complex numbers*, denoted as $\mathbb{C}$, which include all numbers of the form

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

Examples include

$$\mathbb{C} = \{2 + 3i, -1 - i, \pi + i, 0, \dots\}.$$

The hierarchy of number sets follows the subset relation:

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

However, complex numbers are not the end. Beyond $\mathbb{C}$, we encounter the *quaternions*, denoted as $\mathbb{H}$, which extend the number system further. But for now, we conclude our discussion here.

1.2 Well-Ordering Principle

The *Well-Ordering Principle* states that every non-empty subset of the natural numbers $\mathbb{N}$ has a least element. That is, if S is a non-empty subset of $\mathbb{N}$, then there exists an element $m \in S$ such that for all $s \in S$, we have $m \leq s$. Formally:

$$\forall S \subseteq \mathbb{N}, (S \neq \emptyset) \Rightarrow \exists m \in S \, \text{such that} \, \forall s \in S, m \leq s$$

This principle implies that the natural numbers are well-ordered, as every subset of $\mathbb{N}$ has a minimum. The Well-Ordering Principle is closely related to the *Axiom of Choice* in axiomatic set theory, and in fact, it can be derived from it.

1.3 Number Theory

Number Theory is *loosely* the study of the properties of the natural numbers $\mathbb{N}$ and integers $\mathbb{Z}$. It is one of the oldest branches of mathematics, focusing on the relationships between numbers, particularly concerning their divisibility, primality, and arithmetic properties.
Key topics in number theory include the study of prime numbers, divisibility, congruences, Diophantine equations, and number-theoretic functions. Number theory also explores more advanced subjects like quadratic forms, modular forms, and the distribution of prime numbers.

2

Divisibility

2.1 Basics

Definition 2.1.1: Divisibility

We say that an integer a divides another integer b, written as $a \mid b$, $a, b \in \mathbb{Z}$ with $a \neq 0$, if $\exists\, x \in \mathbb{Z}$ such that

$$b = ax.$$

We then say that a is a divisor of b.

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

In another words, $a \mid b \implies \exists$ a solution x to the equation $ax - b = 0$ over $\mathbb{Z}$.

Theorem 2.1.1

1. $\forall\, x \in \mathbb{N}, x \mid 0$.
2. $a \mid b \;\&\; b \mid c \implies a \mid c$.
3. $a \mid b \;\&\; b \mid c \implies a \mid (bx + cy) \,\forall\, x, y \in \mathbb{Z}$

Proof.

1. By definition, $x \mid 0$ means there exists $k \in \mathbb{Z}$ such that $0 = xk$. Choosing $k = 0$, we get $0 = x \cdot 0$, which holds for all $x \in \mathbb{N}$.
2. Since $a \mid b$, there exists $m \in \mathbb{Z}$ such that $b = am$. Similarly, since $b \mid c$, there exists $n \in \mathbb{Z}$ such that $c = bn$. Substituting $b = am$ into $c = bn$, we get $c = a(mn)$, implying $a \mid c$.
3. Since $a \mid b$, we write $b = am$ for some $m \in \mathbb{Z}$. Similarly, $a \mid c$ implies $c = an$ for some $n \in \mathbb{Z}$. Then,

$$bx + cy = (am)x + (an)y = a(mx + ny),$$

where $mx + ny \in \mathbb{Z}$, so $a \mid (bx + cy)$.

$\square$

Theorem 2.1.2: The Division Algorithm

Given $a, b \in \mathbb{Z}$ with $a > 0$, there exist unique integers $q, r \in \mathbb{Z}$ such that

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

Proof. Consider a set

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

if $b > 0$, $k = 0$ & S is non-empty.
If $b < 0$, add a enough times to set $b + ka > 0$. By Well-Ordering Principle (WOP), S has a smallest element $r = b + ka$, for some k.
If we set $q = -k$, then we have:

$$r = b - qa \implies b = aq + r$$

Obviously, $r \geq 0$ since $r \in S$. Also, $r < a$, as otherwise, $b + (k-1)a > 0$ but $b + (k-1)a < r$, and therefore contradicts minimality of r.

$$\therefore 0 \leq r < a$$

□

2.2 Primes

Definition 2.2.1: Prime Number

An element $p \in \mathbb{N}$, $p > 1$, is prime if $q \mid p \implies q = 1$ or $q = p$. Equivalently,

$$Div(p) = \{\pm 1, \pm q\}$$

Example.

> 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 - how many primes are there? The biggest prime found till now is $2^{136,279,841} - 1$. Mersenne primes are primes of the form $2^p - 1$, where p is also a prime.

Theorem 2.2.1: Prime Factorization

Every positive integer greater than 1 can be written as a product of primes.

Proof. Let S to be the set of positive integers that cannot be written as a product of primes. Let N be the smallest element, $N > 1$, and N is not prime. $\therefore N = mn$ for some $1 < m, n < N$.
Since $m, n < N$, they have to be prime, as otherwise they contradict the minimality of N.

□

$$n = (-1)^{\varepsilon(n)} \prod_p p^{a(p)}$$

Where, $\varepsilon(n) = \begin{cases} 1 & \text{if } n < 0 \\ 0 & \text{if } n > 0 \end{cases}$

$a(p) =$ order of n at p. a is the smallest non-negative integer such that $p^a \mid n$ but $p^{a+1} \nmid n$.

Theorem 2.2.2: Bézout's Identity

For any integers a and b, there exist integers x and y such that

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

We will use this theorem for the next lemma.

Lemma 2.2.1

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

Proof. Assume $p \nmid a$. $g = gcd(a, p)$. Since p is a prime, $g = 1$ or p. But if $g = p$, then $p \mid a$, which is so $g = 1$.
From Theorem 2.2.2, $\exists\, x, y \in \mathbb{Z} : ax + py = 1$
$\implies b = bax + pby$
We have that $p \mid (bax + pby)$. Since $p \mid ab \therefore p \mid b$ □

Corollary 2.2.1

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

Proof. $n = 1$ is obvious.
$n = 2$ is what we proved in Lemma 2.2.1.
Assume that this is true for $n = k$. For $n = k + 1$
assume

$$p \mid \underbrace{a \ldots a_k}_{A}\, \underbrace{a_{k+1}}_{B}$$

So, $p \mid AB \implies p \mid A$ or $p \mid B$
If $p \mid A \implies p \mid a_1 \ldots a_k \implies p \mid a_i$ for some $1 \leq i \leq k$
or else, $p \mid B \implies p \mid a_{k+1} \therefore p \mid a_i$ for some $1 \leq i \leq k + 1$ □

Theorem 2.2.3: Fundemental Theorem of Arithmetic or Unique Factorization Theorem

Every positive integer can be written *uniquely* as a product of primes *upto reordering*.

Proof. The existence of prime factorization is already proved in Theorem 2.2.1. Now, we have to prove the uniqueness.
Suppose that there is an integer n with two different factorings.

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$$

Now,

$$p_1 \mid n$$

$$\implies p_1 \mid q_1 \dots q_s$$

Means $p_1 \mid q_i$ for some i.
Since p_1 and q_i are primes, $p_1 = q_i$.

$$p_1 \dots p_r = q_1 \dots q_{i-1} p_1 q_{i+1} \dots q_s$$

$$\implies n' = p_2 \dots p_r = q_1 \dots q_{i-1} q_{i+1} \dots q_s$$

n' is not in the set of counterexamples. $[n' < n]$
Therefore, $r - 1 = s - 1 \implies r = s$
Also, $p_2 \dots p_r$ is a permutation of $q_{i-1} q_{i+1} \dots q_s$. □

Theorem 2.2.4: Euclid

There are infinitely many primes.

Proof. Assume that there are finitely many primes, $p_1 \dots p_n$
define $p = p_1 p_2 \dots p_n + 1$
$p_i \nmid p \, \forall i$
p must have a prime divisor since p is not prime. But we have a contradiction.

$$\therefore p_1 \dots p_n p \text{ are } n+1 \text{ distinct primes.}$$

□

Definition 2.2.2: Riemann Zeta Function

The Riemann Zeta Function is defined as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{for } \Re(s) > 1.$$

For its *Euler product formula*, valid for $\Re(s) > 1$:

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

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

Using the geometric series sum

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

So,

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

$$= (1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \dots)(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \dots)(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \dots)$$
$$= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots$$

We set,

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

By the *fundemental theorem of arithmetic*, $\forall n, a_n = 1$

$$\sum_{n=1}^{\infty} n^{-s} = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$$

We set $s = 1$ to get

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

$\sum \frac{1}{n}$ is the harmonic series which diverges.
$\therefore$ The product on the R.H.S. should be over an infinite index, as otherwise it will converge.
Which implies that there are infinitely many primes!

2.3 Distribution of Primes

Gauss conjectured that the distribution of prime numbers can be approximated by

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

$\pi(x) =$ the number of primes less than or equal to x. Then,

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

In asymptotic notations, if $f(x) \sim g(x)$, then

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

A more precise approximation is provided 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 independently by *Jacques Hadamard* & *Charles Jean de la Vallée Poussin* in 1896.

von Mangoldt's Explicit Formula relates the sum of the *Von Mangoldt function* $\Lambda(n)$ to the nontrivial zeros of the *Riemann Zeta Function.*

We 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 that

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

ρ is the sum running over all the nontrivial zeros of the *Riemann Zeta function* $\zeta(s)$.

2.4 The Riemann Hypothesis!

The *Riemann Hypothesis*, proposed by Bernhard Riemann in 1859, is one of the most important unsolved problems in mathematics. It states that all nontrivial zeros of the *Riemann Zeta function* $\zeta(s)$, defined for $\Re(s) > 1$ by the series

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

and analytically continued elsewhere, lie on the *critical line* $\Re(s) = \frac{1}{2}$. That is, if $\zeta(s) = 0$ and s is not a negative even integer (trivial zero), then $s = \frac{1}{2} + it$ for some real t. The hypothesis has deep implications in number, particularly in the distribution of prime numbers, as the nontrivial zeros of $\zeta(s)$ appear in explicit formulas for the prime counting function $\pi(x)$. Extensive numerical calculations confirm that the first trillions of nontrivial zeros lie on the critical line, but no general proof is known. The *Riemann Hypothesis* remains one of the *Millennium Prize Problems*, with a \$1 million reward for a correct proof or disproof.

The Error Term in the Prime Number Theorem

In earlier estimates of the error term, it was suggested that the deviation of $\pi(x)$ from its leading asymptotic term is at most on the order of $\sqrt{x}$. Although this bound is not optimal, it provides insight into the distribution of prime numbers.

Connection to the Riemann Hypothesis

A much sharper result states that if the *Riemann Hypothesis* holds, then:

$$\pi(x) = \mathrm{Li}(x) + O(\sqrt{x} \log x).$$

This significantly improves the error term and highlights the deep connection between the *zeros of the Riemann zeta function* and the *distribution of primes*.

3

Abstract Algebra Review

3.1 Groups

Definition 3.1.1: Group

A *group* is a set G equipped with a binary operation $*$ satisfying the following properties:

- **Closure**: For all $a, b \in G$, the result of the operation $a * b$ is also in G:
$$a * b \in G, \quad \forall\, a, b \in G.$$
- **Associativity**: The operation is associative, meaning that for all $a, b, c \in G$,
$$(a * b) \cdot c = a * (b * c).$$
- **Identity Element**: There exists an element $e \in G$ such that for all $a \in G$,
$$e * a = a * e = a.$$
- **Inverse Element**: For each $a \in G$, there exists an element $a^{-1} \in G$ such that
$$a * a^{-1} = a^{-1} * a = e.$$

A set G together with a binary operation satisfying these four properties is called a *group*.

Example.

$$(\mathbb{Q}, +),\ (\mathbb{Z}, +),\ (\mathbb{R}, +),\ (\mathbb{Q}\backslash\{0\}, \times)$$

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 want to verify the *group* axioms

1. **Closure:** Let $A = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ and $B = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$ be two elements of $M_{2\times 2}(\mathbb{R})$. Then,
$$A + B = \begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ c_1 + c_2 & d_1 + d_2 \end{pmatrix}$$
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.

□

but, $M_{2\times 2}(\mathbb{N}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{N} \right\}$ is not a group because the inverse axiom does not satisfy.

Are groups necessarily commutative?

No, but if they are commutative they are a special type of group, namely *Abelian* group.

Definition 3.1.2: Abelian Group

A group G is called an *Abelian group* if it satisfies the commutative property:
$$a \cdot b = b \cdot a, \quad \forall a, b \in G.$$
That is, the binary operation is commutative for all elements in the group.

Example.

> $(\mathbb{Z}, +)$ is an *abelian* group.

3.2 Rings

Definition 3.2.1: Ring

A *ring* is a set R equipped with two binary operations, usually called addition $(+)$ and multiplication $(\times)$, such that:

1. $(R, +)$ is an abelian group.
2. Multiplication is associative: for all $a, b, c \in R$,
$$(a \times b) \times c = a \times (b \times c).$$
3. Multiplication distributes over addition: for all $a, b, c \in R$,
$$a \times (b + c) = (a \times b) + (a \times c), \quad \text{and} \quad (a + b) \times c = (a \times c) + (b \times c).$$

Example.

> $(\mathbb{Z}, +, \times)$ is a ring. (We have previously seen that $(\mathbb{Z}, +)$ is an *abelian* group.)
> A more general example could be for some fixed n,
> $$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$
> $$(n\mathbb{Z}, +, \times) \text{ is a } \textit{ring}.$$

Example.

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

Proof. We look at the definition again,

- $M_{2\times 2}(\mathbb{R})$ is an *abelian* group under $+$,
- We show that $M_{2\times 2}(\mathbb{R})$ is closed under matrix multiplication.

  Let $A = (a_{ij})$ and $B = (b_{ij})$ be two arbitrary matrices in $M_{2\times 2}(\mathbb{R})$, where
$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}.$$

The product of A and B is defined as

$$(AB)_{ij} = \sum_{k=1}^{2} a_{ik} b_{kj}.$$

Expanding this for a 2×2 matrix

$$AB = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Since the entries of A and B are real numbers, each entry in the resulting matrix is also a real number. Thus, AB is an element of $M_{2\times2}(\mathbb{R})$.

- We need to show that for any three matrices $A, B, C \in M_{2\times2}(\mathbb{R})$, the following holds

$$\underbrace{(A \times B)}_{D} \times C = A \times \underbrace{(B \times C)}_{E}.$$

Let

$$A = (a_{ij}), \quad B = (b_{ij}), \quad C = (c_{ij})$$

be three arbitrary 2×2 matrices, where their elements are real numbers.

Now,

$$\begin{aligned} \text{L.H.S} &= D \times C \\ &= \sum_{l=1}^{2} (A \times B)_{il} c_{lj} \\ &= \sum_{l=1}^{2} \left(\sum_{k=1}^{2} a_{ik} b_{kl} \right) c_{lj} \\ &= \sum_{l,k} a_{ik} b_{kl} c_{lj} \end{aligned}$$

$$\begin{aligned} \text{R.H.S.} &= A \times E \\ &= \sum_{k=1}^{2} a_{ik} (B \times C)_{kj} \\ &= \sum_{k=1}^{2} a_{ik} \left(\sum_{l=1}^{2} b_{kl} b_{lj} \right) \\ &= \sum_{k,l} a_{ik} b_{kl} c_{lj} \\ &= \sum_{l,k} a_{ik} b_{kl} c_{lj} \end{aligned}$$

Both sides yield the same result.
Thus, associativity of the operation $\times$ is shown.

The given 2×2 matrix is a *ring*.

$\square$

Definition 3.2.2: Unitary Ring

A *unitary ring* (or unital ring) is a ring R that contains a multiplicative identity element 1 such that for all $a \in R$,

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

That is, a unitary ring has a *multiplicative identity* distinct from zero.

Definition 3.2.3: Commutative Ring

A *commutative ring* is a ring R where the multiplication operation is *commutative*, meaning that for all $a, b \in R$,

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

If a commutative ring also has a multiplicative identity, it is called a *commutative unitary ring* or simply a *commutative ring with unity*.

4

Congruences

4.1 Basics of Congruences

Congruences are a fundamental concept in number theory, primarily dealing with divisibility properties and modular arithmetic. They provide a structured way to classify integers based on their remainders when divided by a fixed integer.

Definition 4.1.1: Congruence Relation

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$. We say that a is *congruent* to b mod m, written as:

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

if and only if m divides the difference $a - b$, i.e.,

$$m \mid (a - b).$$

This means that a and b leave the same remainder when divided by m.

Example.

- $17 \equiv 5 \pmod{6}$ because $17 - 5 = 12$ is divisible by 6.
- $23 \equiv 3 \pmod{10}$ since $23 - 3 = 20$ is a multiple of 10.
- $-7 \equiv 2 \pmod{3}$ because $-7 - 2 = -9$ is divisible by 3.

Theorem 4.1.1

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

1. Addition is preserved: $a + c \equiv b + d \pmod{m}$.
2. Subtraction is preserved: $a - c \equiv b - d \pmod{m}$.
3. Multiplication is preserved: $ac \equiv bd \pmod{m}$.
4. Exponentiation is preserved: $a^n \equiv b^n \pmod{m}$.

Proof. Since $a \equiv b \pmod{m}$, there exists an integer k such that

$$a = b + km.$$

Similarly, since $c \equiv d \pmod{m}$, there exists an integer l such that

$$c = d + lm.$$

1. Proof for Addition
Adding the two congruences,

$$\begin{aligned} a + c &= (b + km) + (d + lm) \\ &= (b + d) + (k + l)m. \end{aligned}$$

Since $(k + l)m$ is a multiple of m, we conclude that

$$a + c \equiv b + d \pmod{m}.$$

2. Proof for Subtraction
Subtracting the congruences,

$$\begin{aligned} a - c &= (b + km) - (d + lm) \\ &= (b - d) + (k - l)m. \end{aligned}$$

Since $(k - l)m$ is a multiple of m, we get

$$a - c \equiv b - d \pmod{m}.$$

3. Proof for Multiplication
Multiplying the two expressions,

$$\begin{aligned} ac &= (b + km)(d + lm) \\ &= bd + blm + dkm + klm^2. \end{aligned}$$

Since $blm + dkm + klm^2$ is a multiple of m, it follows that

$$ac \equiv bd \pmod{m}.$$

4. Proof for Exponentiation We use induction on n.
Base Case: For $n = 1$, we have $a^1 = a$ and $b^1 = b$, so

$$a^1 \equiv b^1 \pmod{m},$$

which holds by assumption.
Inductive Step: Assume for some $k \geq 1$ that

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

using the multiplication property, $a^k \cdot a \equiv b^k \cdot b \pmod{m}$, it follows that

$$a^{k+1} \equiv b^{k+1} \pmod{m}.$$

Thus, by induction, the statement holds for all $n \geq 1$. □

Theorem 4.1.2

If $ra \equiv rb \pmod{m}$, then it follows that $a \equiv b \pmod{\frac{m}{\gcd(m,r)}}$.

Proof. Given that $ra \equiv rb \pmod{m}$, we have

$$m \mid r(a-b)$$

which implies that there exists some integer k such that

$$r(a-b) = km.$$

Define $d = \gcd(m, r)$. Since d divides both m and r, we can write:

$$m = dm_1, \quad r = dr_1$$

for some integers m_1 and r_1, where $\gcd(m_1, r_1) = 1$.
Rewriting the congruence condition in terms of these factors

$$dr_1(a-b) = kdm_1.$$

Dividing both sides by d gives

$$r_1(a-b) = km_1.$$

Since $\gcd(r_1, m_1) = 1$, r_1 is coprime to m_1, which implies that m_1 must divide $a-b$, i.e.,

$$a - b \equiv 0 \pmod{m_1}.$$

Thus, we conclude

$$a \equiv b \pmod{\frac{m}{\gcd(m,r)}}.$$

□

Corollary 4.1.1

If $ra \equiv rb \pmod{m}$ and $\gcd(r, m) = 1$, then it follows that $a \equiv b \pmod{m}$. This is also called the *Cancellation Law*.

4.2 Equivalence Relations and Equivalence Classes

An *equivalence relation* on a set S is a binary relation $\sim$ that satisfies the following three properties:

1. **Reflexivity**: For all elements $a \in S$, $a \sim a$. This means every element is related to itself.

2. **Symmetry**: For all $a, b \in S$, if $a \sim b$, then $b \sim a$. This means the relation is mutual.

3. **Transitivity**: For all $a, b, c \in S$, if $a \sim b$ and $b \sim c$, then $a \sim c$. This means the relation can be "passed" from one element to another.

If a relation $\sim$ on S satisfies all three properties, it is called an *equivalence relation*.

Given an equivalence relation $\sim$ on a set S, the *equivalence class* of an element $a \in S$ is the set of all elements in S that are equivalent to a. The equivalence class of a is denoted by

$$[a] = \{b \in S : b \sim a\}$$

This equivalence class consists of all elements b that are related to a under the equivalence relation.

Equivalence relations induce a partition of the set S into disjoint equivalence classes. In other words, the set S can be decomposed into distinct subsets, where each subset consists of elements that are equivalent to each other. Each element of S belongs to exactly one equivalence class.

4.3 Congruences as an Equivalence Relation

Proof. We verify that the congruence relation satisfies the three properties of reflexivity, symmetry, and transitivity.

1. **Reflexivity**: For any integer $a \in \mathbb{Z}$, we have

$$a - a = 0,$$

and since $m \mid 0$ for all m, we conclude that

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

Thus, the relation is reflexive.

2. **Symmetry**: If $a \equiv b \pmod{m}$, then by definition, $m \mid (a-b)$. Since $m \mid (a-b)$ implies $m \mid (b-a)$ (because $b-a = -(a-b)$), we conclude that

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

   Thus, the relation is symmetric.

3. **Transitivity**: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then by definition, $m \mid (a-b)$ and $m \mid (b-c)$. Adding these two relations

$$(a-b) + (b-c) = a - c,$$

   and since n divides both $a-b$ and $b-c$, it follows that $m \mid (a-c)$, and therefore

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

   Thus, the relation is transitive.

Since congruence modulo n satisfies all three properties—reflexivity, symmetry, and transitivity—it is an equivalence relation on $\mathbb{Z}$. $\square$

An equivalence relation partitions a set into disjoint equivalence classes. $a, b \in \mathbb{Z}$ are in the same equivalence class iff $m \mid (a-b)$, 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 the remainder is unique, there are exactly m equivalence classes.
The equivalence class of an integer a modulo m, denoted by $[a]_m$, is defined as:

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

This represents the set of all integers that are congruent to a modulo m, meaning they have the same remainder when divided by m. Explicitly, this set includes:

$$[a]_m = \{a, a+m, a-m, a+2m, a-2m, \dots\}.$$

Each integer in this set belongs to the same equivalence class because their difference is always a multiple of m.
For simplicity, the notation $[a]_m$ is often abbreviated as $[a]$ or $\overline{a}$, whenever the modulus m is clear from the context. The set of all such equivalence classes modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$, and it consists of the following m distinct classes:

$$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], [2], \dots, [m-1]\}.$$

Addition on $\mathbb{Z}/m\mathbb{Z}$

For $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$, addition is defined as:

$$\overline{a} + \overline{b} = \overline{a+b}.$$

Example in $\mathbb{Z}/5\mathbb{Z}$:

$$\overline{3} + \overline{4} = \overline{7} = \overline{2}.$$

Multiplication on $\mathbb{Z}/m\mathbb{Z}$

Multiplication is defined as:

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Example in $\mathbb{Z}/5\mathbb{Z}$:

$$\overline{3} \cdot \overline{4} = \overline{12} = \overline{2}.$$

Proposition 4.3.1

$\mathbb{Z}/m\mathbb{Z}$ is a commutative ring with identity.

Proof. First, we want to show that $(\mathbb{Z}/m\mathbb{Z}, +)$ is an Abelian Group.

1. Closure

For any $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$, their sum is:

$$\overline{a} + \overline{b} = \overline{a + b}.$$

Since $a + b$ is an integer, $\overline{a + b} \in \mathbb{Z}/m\mathbb{Z}$, so the set is closed under addition.

2. Associativity

For any $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/m\mathbb{Z}$:

$$(\overline{a} + \overline{b}) + \overline{c} = \overline{(a + b)} + \overline{c} = \overline{(a + b) + c}.$$

Since addition in $\mathbb{Z}$ is associative:

$$\overline{(a + b) + c} = \overline{a + (b + c)} = \overline{a} + (\overline{b} + \overline{c}).$$

3. Identity Element

The element $\overline{0}$ is the additive identity since:

$$\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}.$$

4. Additive Inverses

For each $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$, the element $\overline{-a}$ satisfies:

$$\overline{a} + \overline{-a} = \overline{a + (-a)} = \overline{0}.$$

5. Commutativity

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

$$\overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a}.$$

Now we need to show that $(\mathbb{Z}/m\mathbb{Z}, +, \times)$ is a Commutative Ring with Identity.

1. Closure under Multiplication

For any $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$, we define multiplication as:

$$\overline{a} \times \overline{b} = \overline{a \times b}.$$

Since $a \times b$ is an integer, $\overline{a \times b} \in \mathbb{Z}/m\mathbb{Z}$, so the set is closed under multiplication.
2. Associativity of Multiplication
For any $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/m\mathbb{Z}$:

$$(\overline{a} \times \overline{b}) \times \overline{c} = \overline{(a \times b)} \times \overline{c} = \overline{(a \times b) \times c}.$$

Since multiplication in $\mathbb{Z}$ is associative:

$$\overline{(a \times b) \times c} = \overline{a \times (b \times c)} = \overline{a} \times (\overline{b} \times \overline{c}).$$

3. Distributive Property
For all $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}/m\mathbb{Z}$:

$$\overline{a} \times (\overline{b} + \overline{c}) = \overline{a} \times \overline{(b + c)} = \overline{a \times (b + c)}.$$

By the distributive law in $\mathbb{Z}$:

$$\overline{a \times (b + c)} = \overline{a \times b + a \times c} = \overline{a} \times \overline{b} + \overline{a} \times \overline{c}.$$

4. Commutativity of Multiplication
For any $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$:

$$\overline{a} \times \overline{b} = \overline{a \times b} = \overline{b \times a} = \overline{b} \times \overline{a}.$$

5. Multiplicative Identity
The element $\overline{1}$ is the multiplicative identity since:

$$\overline{a} \times \overline{1} = \overline{a \times 1} = \overline{a}.$$

Since $(\mathbb{Z}/m\mathbb{Z}, +, \times)$ satisfies all the axioms of a commutative ring with identity, it forms a commutative ring with identity. □

Definition 4.3.1: Unit in $\mathbb{Z}/n\mathbb{Z}$

An element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is called a **unit** if there exists $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ such that

$$\overline{a} \times \overline{b} = \overline{1}.$$

Equivalently, $\overline{a}$ is a unit if and only if a has a multiplicative inverse modulo n, meaning there exists an integer b such that

$$a \times b \equiv 1 \pmod{n}.$$

This is true if and only if $\gcd(a, n) = 1$, meaning a is coprime to n.
The set of all units in $\mathbb{Z}/n\mathbb{Z}$ forms a group under multiplication, denoted by

$$(\mathbb{Z}/n\mathbb{Z})^{\times}$$

Example.

Consider $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

The element $\overline{5}$ is a unit because $\gcd(5, 6) = 1$, and its inverse is $\overline{5}$ itself since:

$$5 \times 5 \equiv 25 \equiv 1 \pmod{6}.$$

The element $\overline{2}$ is **not** a unit because $\gcd(2, 6) = 2 \neq 1$, meaning 2 does not have an inverse modulo 6.

Thus, $\overline{5}$ is a unit in $\mathbb{Z}/6\mathbb{Z}$, but $\overline{2}$ is not.

4.4 Linear Congruences

Definition 4.4.1: Linear Congruence

A *linear congruence* is a congruence of the form

$$ax \equiv b \pmod{n},$$

Theorem 4.4.1: Existence and Number of Solutions of a Linear Congruence

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 the congruence has exactly d mutually incongruent solutions modulo m.

Proof. $(\implies)$

Suppose x_0 is a solution to the congruence, i.e.,

$$ax_0 \equiv b \pmod{m}.$$

This means that m divides $ax_0 - b$, so there exists some integer y_0 such that:

$$ax_0 - b = my_0.$$

Since $d = \gcd(a, m)$, we know d divides both a and m. Therefore, d must also divide the right-hand side of the equation:

$$d \mid (ax_0 - my_0).$$

Thus, $d \mid b$, proving the necessary condition.
$(\Longleftarrow)$
Since $d \mid b$, we can write $b = dc$ for some integer c. By Bézout's identity, there exist integers x_0 and y_0 such that:

$$ax_0 - my_0 = d.$$

Multiplying both sides by $c = \frac{b}{d}$, we obtain:

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

Setting $x' = cx_0$, we see that x' is a solution:

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

Thus, at least one solution exists.
Number of distinct solutions
Now, suppose x_0 and x_1 are two solutions to the congruence:

$$ax_0 \equiv b \pmod{m}, \quad ax_1 \equiv b \pmod{m}.$$

Subtracting these two congruences:

$$a(x_0 - x_1) \equiv 0 \pmod{m}.$$

This means m divides $a(x_0 - x_1)$, i.e.,

$$m \mid a(x_0 - x_1).$$

Dividing by d, we get:

$$\frac{m}{d} \mid \frac{a}{d}(x_0 - x_1).$$

Since $\gcd(a/d, m/d) = 1$, it follows that:

$$\frac{m}{d} \mid (x_0 - x_1).$$

Thus, any two solutions differ by a multiple of m/d, meaning the solutions are of the form:

$$x_k = x_0 + k\frac{m}{d}, \quad \text{for } k = 0, 1, 2, \ldots, d-1.$$

Since these values are distinct modulo m, there are exactly d incongruent solutions. $\square$

Corollary 4.4.1

If a & m are coprime, then $ax \equiv b \pmod{m}$ has exactly one solution.

The following is equivalent to Corollary 4.4.1,

Corollary 4.4.2

Define the map:

$$\varphi_a : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

such that

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

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

Proof. **Injectivity**

To prove injectivity, suppose $\varphi_a(x_1) = \varphi_a(x_2)$, i.e.,

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

Rearranging, we get:

$$a(x_1 - x_2) \equiv 0 \pmod{m}.$$

This means that m divides $a(x_1 - x_2)$, i.e.,

$$m \mid a(x_1 - x_2).$$

If $\gcd(a, m) = 1$, then a has a multiplicative inverse modulo m, so we can cancel a from both sides, giving:

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

Thus, φ_a is injective.

Surjectivity
$\exists\, ax_0 + my_0 = 1$ (From Bézout's Identity)
Choose $b \in \mathbb{Z}/m\mathbb{Z}$

$$abx_0 + myb = b$$

Reduce $\mod m$
$abx_0 \pmod{m} = b \pmod{m}$
$x = bx_0$ gives $\varphi_a(x) \equiv b \pmod{m}$

In other sense,
Since $\mathbb{Z}/m\mathbb{Z}$ is a finite set of m elements, an injective function must also be surjective. Hence, φ_a is bijective when $\gcd(a, m) = 1$.
If $d = \gcd(a, m) > 1$, then a and m share a common divisor. In this case, the equation $ax \equiv b \pmod{m}$ does not have a solution for all b, meaning φ_a is not surjective. This shows that φ_a fails to be bijective. Thus, φ_a is bijective if and only if $\gcd(a, m) = 1$. □

Proposition 4.4.1

An element a in $\mathbb{Z}/m\mathbb{Z}$ is a unit if and only if $\gcd(a, m) = 1$.

Proof. ($\Longrightarrow$)
$\varphi_a(x) \equiv ax \pmod{m}$, φ_a is surjective.
$\forall\, b \in \mathbb{Z}/m\mathbb{Z}$, $x : ax_0 \equiv b \pmod{m}$
Take $b = 1$

$$ax_0 = 1 \pmod{n}$$

$$\exists\, y_0 : ax_0 - my_0 = 1$$

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

(From Bézout's Identity)
($\Longleftarrow$)
if $m = p$ (prime)

$$\forall\, a \in \mathbb{Z}/m\mathbb{Z}$$

$$\gcd(a, m) = 1 \implies a \text{ is a unit,}$$

meaning $a \neq 0$ has a multiplicative inverse. □

Theorem 4.4.2

If p is a prime number, then the ring $\mathbb{Z}/p\mathbb{Z}$ is a field.

Proof. If p is prime, then for all $a \neq 0 \in \mathbb{Z}/p\mathbb{Z}$, we have $\gcd(a, p) = 1$. Hence, each nonzero $a \in \mathbb{Z}/p\mathbb{Z}$ has a 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.

Theorem 4.4.3: Wilson's Theorem

Let p be a prime number. Then,

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