Inspiring Excellence

MAT422: Theory of Numbers

Lecture notes

Last updated on March 12, 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 $x^2 = 2$. □

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 $a \mid (bx + cy)$.

□

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 $p \mid a_1 a_2 \dots a_n$, 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

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

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

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

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

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 $a, b, c \in G$,

$$(a * b) * c = a * (b * c).$$

- **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 $M_{2\times 2}(\mathbb{R})$.

- We need to show that for any three matrices $A, B, C \in M_{2\times 2}(\mathbb{R})$, 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*.

□

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 $\mathbb{Z}$. □

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. ($\Longrightarrow$)

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. □

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. ($\implies$)
$\varphi_a(x) \equiv ax \pmod{m}$, 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)
($\impliedby$)
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,

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

Proof. ($\implies$)
For a prime p, the set $\{1, 2, \ldots, p-1\}$ forms a multiplicative group under modulo p arithmetic, meaning each integer a has a unique modular inverse a^{-1} such that:

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

Each element a in $\{1, 2, \ldots, p-1\}$ can be paired with its inverse a^{-1}, except for those that are their own inverses

$$a^2 \equiv 1 \pmod{p}.$$

Which means, $p \mid a^2 - 1 \implies p \mid (a+1)(a-1)$
Which implies either $p \mid (a+1)$ or $p \mid a-1$

$$\therefore a = \pm 1 \pmod{p}$$

Multiply $1, 2 \ldots p-2$ to get

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

Multiply by $p-1$ to get

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

($\impliedby$)
Conversely assume p has a non-trivial divisor d
We have $(p-1)! \equiv -1 \pmod{p} \implies (p-1)! \equiv -1 \pmod{d}$
We also have $(p-1)! \equiv 0 \pmod{d}$
But d cannot be 1 as it is a non-trivial solution. Thus this is a contradiction, implying that p is a prime. □

Theorem 4.4.4: Fermat's Little Theorem

Let p be a prime number. Then for any integer a such that p does not divide a, we have:

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

Equivalently, for any integer a, we have

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

Proof.

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

such that

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

This map is a bijection.
Consider the set of integers $\{1, 2, \ldots, p-1\}$, which forms a complete set of nonzero residues modulo p. Since a is coprime to p, multiplication by a permutes these elements modulo p.

Thus, multiplying each element by a gives

$$a \cdot 1, \quad a \cdot 2, \quad \ldots, \quad a \cdot (p-1).$$

Since this is just a rearrangement of the same elements modulo p, we obtain

$$(a \cdot 1) \cdot (a \cdot 2) \cdot \cdots \cdot (a \cdot (p-1)) \equiv (1 \cdot 2 \cdot \cdots \cdot (p-1)) \pmod{p}$$

Rewriting the right-hand side

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

Since $(p-1)!$ is nonzero modulo p, we cancel it out, yielding

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

This completes the proof. □

Definition 4.4.2: Carmichael Numbers

Carmichael numbers are composite numbers that falsely satisfy *Fermat's Little Theorem.*

Example.

> The smallest Carmichael number is:
>
> $$561 = 3 \times 11 \times 17.$$
>
> Other examples include:
>
> $$1105 = 5 \times 13 \times 17, \quad 1729 = 7 \times 13 \times 19, \quad 2465 = 5 \times 17 \times 29.$$

Definition 4.4.3: Euler's Theorem

Euler's Theorem is a generalization of *Fermat's Little Theorem.* It states that:

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \quad \text{for any integer } a \text{ such that } \gcd(a, n) = 1.$$

Here, $\varphi(n)$ is *Euler's totient function*, which counts the number of integers from 1 to n that are coprime to n.
$\varphi(n) = \#\{0 \leq m \leq n : \gcd(m, n) = 1\}$

Proof. The set of integers that are coprime to n modulo n forms a multiplicative group

$$A = \{a_1, a_2, \ldots, a_{\varphi(n)}\}, \quad \text{where } \gcd(a_i, n) = 1 \text{ for all } a_i.$$

$A \to A$, $\varphi_a(x) = ax \pmod{n}$
Since $\gcd(a, n) = 1$, multiplication by a preserves coprimality. That is, the new set

$$A' = \{aa_1, aa_2, \ldots, aa_{\varphi(n)}\} \pmod{n}$$

is simply a permutation of A.
Since A' is just a rearrangement of A, their products must be congruent modulo n

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

Factoring out $a^{\varphi(n)}$ from the right-hand side

$$a_1 a_2 \cdots a_{\varphi(n)} \equiv a^{\varphi(n)} \cdot (a_1 a_2 \cdots a_{\varphi(n)}) \pmod{n}.$$

Since $x_1 x_2 \cdots x_{\varphi(n)}$ is coprime to n, we can cancel it

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

Thus, we have proved *Euler's Theorem.* □

Definition 4.4.4: Euler's Totient Function

Euler's totient function, denoted $\varphi(n)$, counts the number of positive integers less than or equal to n that are coprime to n. In other words, $\varphi(n)$ counts how many integers between 1 and n share no common factors with n other than 1.

The Euler totient function $\varphi(n)$ is defined by the following properties

- For a prime p
$$\varphi(p) = p - 1.$$
- For a prime power p^α
$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

Proof. Let p be a prime and α a positive integer. We aim to prove the formula for Euler's totient function for a prime power p^α, that is:

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

The total number of integers from 1 to p^α is p^α.
The numbers divisible by p are $p, 2p, 3p, \ldots, p^{\alpha-1}p$, and there are $p^{\alpha-1}$ such numbers.
The numbers that are not divisible by p are the integers that are coprime with p^α.
Therefore, the number of integers from 1 to p^α that are coprime to p^α is

$$p^\alpha - p^{\alpha-1}.$$

This completes the proof. □

- If $\gcd(m, n) = 1$, then φ is multiplicative:

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Proof. The group of units modulo mn, denoted as $U(\mathbb{Z}/mn\mathbb{Z})$, consists of integers modulo mn that are coprime to mn.
By the *Chinese Remainder Theorem*, we have an isomorphism:

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

Taking the group of units on both sides, we get

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

Since the groups $U(\mathbb{Z}/mn\mathbb{Z})$ and $U(\mathbb{Z}/m\mathbb{Z}) \times U(\mathbb{Z}/n\mathbb{Z})$ are isomorphic, they must have the same number of elements. That is,

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

By definition, the size of these groups corresponds to Euler's totient function

$$\varphi(mn) = \varphi(m)\varphi(n).$$

□

- If $a \mid b$, then the totient function satisfies:

$$\varphi(a) \mid \varphi(b).$$

General Formula for Euler's Totient Function

There is a general formula

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right),$$

where $p_1, p_2, \ldots, p_k$ are the distinct prime factors of n.

Proof. As we have proved before, the number of integers that are coprime to p^α is

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

Now, let n be a general integer with the prime factorization

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}.$$

Using the multiplicativity of $\varphi(n)$, we have

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \ldots \varphi(p_k^{\alpha_k}).$$

Now, we substitute $\varphi(p^\alpha)$

$$\varphi(n) = \left(p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)\right) \times \left(p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)\right) \times \cdots \times \left(p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right)\right).$$

Rearranging the terms

$$\varphi(n) = (p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) \times \left(1-\frac{1}{p_1}\right) \times \left(1-\frac{1}{p_2}\right) \times \cdots \times \left(1-\frac{1}{p_k}\right).$$

Since $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, we obtain:

$$\varphi(n) = n \prod_{i=1}^{k} \left(1-\frac{1}{p_i}\right).$$

□

We can write $\varphi(n)$ as a product

$$\varphi(n) = n \prod_{p|n} \left(1-\frac{1}{p}\right)$$

over primes. Using this identity, we have

$$\varphi(mn) = mn \prod_{p|mn} \left(1-\frac{1}{p}\right) = mn \frac{\prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{p|n}\left(1-\frac{1}{p}\right)}{\prod_{p|d}\left(1-\frac{1}{p}\right)} = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$$

Definition 4.4.5: Group of Units

The *group of units* of the ring $\mathbb{Z}/n\mathbb{Z}$, denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$, is the set of all integers modulo n that have a multiplicative inverse. That is,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n) = 1\}.$$

This set forms a group under multiplication modulo n.

Example.

Consider $n = 12$. The elements of $\mathbb{Z}/12\mathbb{Z}$ are

$$\mathbb{Z}/12\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}\}.$$

To find $(\mathbb{Z}/12\mathbb{Z})^\times$, we need to select elements that have a multiplicative inverse, i.e., numbers that are coprime to 12.

The numbers less than 12 that are coprime to 12 are:

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

These numbers form the group $(\mathbb{Z}/12\mathbb{Z})^\times$ under multiplication modulo 12.

- $1 \mod 12$ is its own inverse.
- $5 \times 5 \equiv 25 \equiv 1 \pmod{12}$, so $5^{-1} \equiv 5$.
- $7 \times 7 \equiv 49 \equiv 1 \pmod{12}$, so $7^{-1} \equiv 7$.
- $11 \times 11 \equiv 121 \equiv 1 \pmod{12}$, so $11^{-1} \equiv 11$.

Thus, the group $(\mathbb{Z}/12\mathbb{Z})^\times$ consists of $\{1, 5, 7, 11\}$, which has 4 elements.

The *Euler totient function*, $\varphi(n)$, counts the number of integers between 1 and n that are coprime to n.

Since $(\mathbb{Z}/n\mathbb{Z})^\times$ consists of elements that are coprime to n, the order of this group is given by

$$|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n).$$

For $n = 12$, we compute

$$\phi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12 \times \frac{1}{2} \times \frac{2}{3} = 4.$$

This matches the number of elements in $(\mathbb{Z}/12\mathbb{Z})^\times$.

From now on, we will use $U(\mathbb{Z}/M\mathbb{Z})$ notation for *group of units*.

$$U(\mathbb{Z}/M\mathbb{Z}) \cong U(\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times U(\mathbb{Z}/m_k\mathbb{Z})$$

$$\varphi(M) = |U(\mathbb{Z}/M\mathbb{Z})|$$

Application of Euler's Theorem

$$ax \equiv 1 \pmod{n}$$

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

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

We want to derive the formula

$$x \equiv ba^{\varphi(n)-1} \pmod{n}$$

Since $\gcd(a, n) = 1$, the integer a has a *multiplicative inverse modulo* n, meaning there exists some a^{-1} such that

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

From *Euler's theorem*, we know

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

Multiplying both sides by a^{-1}, we obtain

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

Thus, the inverse of a is

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

Multiplying both sides by a^{-1}, we get

$$x \equiv b \cdot a^{-1} \pmod{n}$$

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

we obtain

$$x \equiv b \cdot a^{\varphi(n)-1} \pmod{n}.$$

Thus, we have derived the desired result:

$$x \equiv ba^{\varphi(n)-1} \pmod{n}.$$

4.5 The Chinese Remainder Theorem

Definition 4.5.1: The Chinese Remainder Theorem

If $\gcd(m, n) = 1$ & $u, v \in \mathbb{N}$ such that $mu - nv = 1$ then

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

$$x \equiv b \pmod{n}$$

has solution $x = bmu - anv$ and the solution is unique modulo mn.

Proof. We are given that $\gcd(m, n) = 1$, which implies that the integers m and n are coprime. By the properties of linear Diophantine equations, there exist integers u and v

such that

$$mu - nv = 1$$

Now, consider the expression $x = bmu - anv$, where b and a are the residues in the system of congruences. We want to show that this satisfies both congruences.
We first check the congruence $x \equiv b \pmod{n}$. We compute

$$x = bmu - anv$$

Taking this modulo n, we get

$$x \pmod{n} = (bmu - anv) \pmod{n}$$

Since $mu \equiv 1 \pmod{n}$ by the assumption $mu - nv = 1$, we have

$$x \pmod{n} = b \cdot 1 - a \cdot 0 \equiv b \pmod{n}$$

Thus, $x \equiv b \pmod{n}$, as required.
Now, we check the congruence $x \equiv a \pmod{m}$. We compute

$$x = bmu - anv$$

Taking this modulo m, we get

$$x \pmod{m} = (bmu - anv) \pmod{m}$$

Since $nv \equiv 1 \pmod{m}$ (again, by the assumption $mu - nv = 1$), we have

$$x \pmod{m} = b \cdot 0 - a \cdot 1 \equiv a \pmod{m}$$

Thus, $x \equiv a \pmod{m}$, as required.
Suppose there is another solution y that satisfies both congruences

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

$$y \equiv b \pmod{n}$$

This implies

$$x \equiv y \pmod{m} \quad \text{and} \quad x \equiv y \pmod{n}$$

We now show that $x = y \pmod{mn}$. From the fact that $x \equiv y \pmod{n}$, we know that

$$n \mid (x - y)$$

Similarly, from $x \equiv y \pmod{m}$, we know that

$$m \mid (x - y)$$

Thus, $x - y$ is divisible by both m and n. Since $\gcd(m, n) = 1$, by the *Chinese Remainder*

Theorem, we conclude that

$$mn \mid (x - y)$$

Therefore, $x \equiv y \pmod{mn}$, proving the uniqueness of the solution modulo mn.

□

We now will try to simplify an expression.

$$x = (102^{73} + 55)^{37} \mod 111$$

To solve this, we will first break down the expression using moduli 3, 37, and 111, and then combine the results using the *Chinese Remainder Theorem*.
We start by analyzing the powers of 102 and 55 modulo 3.
• $102 \mod 3$
Since $102 = 3 \times 34$, we have $102 \equiv 0 \mod 3$.
• $55 \mod 3$
Similarly, $55 = 3 \times 18 + 1$, so $55 \equiv 1 \mod 3$.
Now, let's compute $102^{73} + 55 \mod 3$.
Since $102 \equiv 0 \mod 3$, we know that $102^{73} \equiv 0^{73} = 0 \mod 3$
Thus, we have

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

Finally, we have

$$x \equiv 1^{37} = 1 \mod 3$$

So, $x \equiv 1 \mod 3$, which matches the result given in the problem.
Next, let's compute $102^{73} \mod 37$.
• $102 \mod 37$
We first reduce 102 modulo 37

$$102 \div 37 = 2 \quad \text{with remainder} \quad 102 - 37 \times 2 = 102 - 74 = 28.$$

So, $102 \equiv 28 \mod 37$.
Now, we need to compute $102^{73} \mod 37$, which is equivalent to $28^{73} \mod 37$.
By *Fermat's Little Theorem*, since 37 is prime, we know that

$$28^{36} \equiv 1 \mod 37.$$

Therefore, we reduce the exponent 73 modulo 36

$$73 \div 36 = 2 \quad \text{with remainder} \quad 73 - 36 \times 2 = 73 - 72 = 1.$$

Thus, we have

$$28^{73} \equiv 28^1 = 28 \mod 37.$$

So, we conclude that

$$102^{73} \equiv 28 \mod 37.$$

Now, let's compute $(102^{73}+55)^{37} \mod 37$.
We already know that $102^{73} \equiv 28 \mod 37$.
• $55 \mod 37$
We calculate $55 \mod 37$ by subtracting

$$55 - 37 = 18, \quad \text{so} \quad 55 \equiv 18 \mod 37.$$

Thus, we have

$$102^{73} + 55 \equiv 28 + 18 = 46 \mod 37$$

Now reduce $46 \mod 37$

$$46 - 37 = 9, \quad \text{so} \quad 102^{73} + 55 \equiv 9 \mod 37.$$

Now, we compute $9^{37} \mod 37$.
By *Fermat's Little Theorem* , since 37 is prime, we know that:

$$9^{36} \equiv 1 \mod 37.$$

Thus

$$9^{37} = 9^{36} \times 9 \equiv 1 \times 9 = 9 \mod 37.$$

So, we conclude

$$(102^{73} + 55)^{37} \equiv 9 \mod 37.$$

Now, we need to compute the final expression modulo 111. We use the fact that $111 = 3 \times 37$, so we can apply the *Chinese Remainder Theorem* to combine the results we found modulo 3 and modulo 37.
We already know
$x \equiv 1 \mod 3$
$x \equiv 9 \mod 37$
We now solve this system of congruences

$$x \equiv 1 \mod 3$$

$$x \equiv 9 \mod 37$$

$37 \cdot 1 - 3 \cdot 12 = 1$, so
$x \equiv 37 \cdot 1 \cdot 1 - 3 \cdot 12 \cdot 9 \pmod{37 \cdot 3} = -65 \pmod{111} = 46 \pmod{111}$
Thus, the solution to the given expression is

$$x \equiv 46 \mod 111.$$

Definition 4.5.2: Ring Homomorphism

Let R and S be two rings. A function $f : R \to S$ is called a *ring homomorphism* if it satisfies the following properties

1. **Preservation of addition:** For all $a, b \in R$, we have
$$f(a +_R b) = f(a) +_S f(b).$$
2. **Preservation of multiplication:** For all $a, b \in R$, we have
$$f(a \times_R b) = f(a) \times_S f(b).$$
3. **Preservation of the multiplicative identity:** If 1_R is the multiplicative identity in R, then
$$f(1_R) = 1_S,$$
where 1_S is the multiplicative identity in S.
If the ring homomorphism $f : R \to S$ is also bijective, then f is called a *ring isomorphism*. In this case, R and S are said to be *isomorphic* as rings, and we write
$$R \cong S.$$

Chinese Remainder Theorem with Ring Isomorphism

Let m, n be two coprime integers, i.e., $\gcd(m, n) = 1$. Then, there exists a ring isomorphism

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

We define the mapping
$$\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
by
$$\varphi(x) = (x \mod m, x \mod n).$$

This function takes an integer modulo mn and maps it to its residues modulo m and n.
We now verify that φ is a ring homomorphism.

1. **Addition Preservation:**

$\varphi(x+y) = ((x+y) \mod m, (x+y) \mod n) = (x \mod m + y \mod m, x \mod n + y \mod n) = \varphi(x) + \varphi(y).$

2. **Multiplication Preservation:**

$\varphi(xy) = (xy \mod m, xy \mod n) = ((x \mod m)(y \mod m), (x \mod n)(y \mod n)) = \varphi(x) \cdot \varphi(y).$

Thus, φ is a ring homomorphism.

Injectivity

The kernel of φ consists of all $x \in \mathbb{Z}$ such that

$$(x \mod m, x \mod n) = (0, 0),$$

which means x is divisible by both m and n. Since m and n are coprime, this implies x is divisible by their product mn. Thus,

$$\ker(\varphi) = mn\mathbb{Z}.$$

By the First Isomorphism Theorem,

$$\mathbb{Z}/\ker(\varphi) \cong \varphi(\mathbb{Z}/mn\mathbb{Z}).$$

Since the codomain has the same number of elements as the domain, φ is injective.

Surjectivity

For any pair $(a, b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, we need to find an x such that

$$\varphi(x) = (a, b),$$

meaning

$$x \equiv a \pmod{m}, \quad x \equiv b \pmod{n}.$$

By the *Chinese Remainder Theorem*, such an x always exists. Therefore, φ is surjective. Since φ is a bijective ring homomorphism, it is a ring isomorphism. Thus, we conclude:

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

General Form of the Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_k$ be pairwise coprime positive integers, and let $M = m_1 m_2 \cdots m_k$. Then, the system of simultaneous congruences

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_k \pmod{m_k}$$

has a unique solution modulo M. That is, there exists an integer x satisfying all congruences, and any two solutions are congruent modulo M.
Additionally, the ring isomorphism

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

follows from the *Chinese Remainder Theorem*. Under this isomorphism, the equivalence class of x modulo M corresponds to the tuple

$$(x \mod m_1, x \mod m_2, \ldots, x \mod m_k),$$

meaning

$$x \mod M = (x \mod m_1, x \mod m_2, \ldots, x \mod m_k).$$

This establishes a one-to-one correspondence between elements of $\mathbb{Z}/M\mathbb{Z}$ and the product $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$.

4.6 Polynomial Ring $K[x]$

Lemma 4.6.1

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

Proof. We proceed by induction on n.

For the base case $n = 1$, consider the polynomial

$$f(x) = a_0 + a_1 x.$$

This is a linear polynomial and has at most one root, as required.
Now, assume that for a polynomial of degree $n-1$, the lemma holds. That is, any polynomial of degree $n-1$ has at most $n-1$ distinct roots in K.
Now, consider a polynomial $f(x)$ of degree n.
If $f(x)$ has no roots in K, we are done. Otherwise, suppose α is a root of $f(x)$. By the division algorithm in $K[x]$, we can write

$$f(x) = q(x)(x - \alpha) + r(x),$$

where $\deg r < \deg(x - \alpha) = 1$, so $r(x)$ is a constant.
Since α is a root,

$$f(\alpha) = 0 \implies q(\alpha)(\alpha - \alpha) + r = 0 \implies r = 0.$$

Thus,

$$f(x) = q(x)(x - \alpha).$$

Since $f(x)$ has degree n, it follows that $q(x)$ has degree $n - 1$.

Now, assume $f(x)$ has another root β with $\beta \neq \alpha$. Then,

$$f(\beta) = 0 \implies q(\beta)(\beta - \alpha) = 0.$$

Since $\beta \neq \alpha$, we must have $q(\beta) = 0$, meaning β is a root of $q(x)$.
By the induction hypothesis, $q(x)$ (which has degree $n - 1$) has at most $n - 1$ roots. Since α was already counted separately, $f(x)$ has at most n roots.
Thus, by induction, the lemma holds for all n. □

Corollary 4.6.1

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 $\alpha_1, \alpha_2, \ldots, \alpha_{n+1} \in K$, 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 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 4.6.1

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 that K is a field.
Let $f(x) \in K[x]$

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

Since $f(x)$ is defined this way, it has degree less than $(p - 1)$.
By Fermat's Little Theorem, we know

$$x^{p-1} - 1 = 0, \quad \text{for all } x \in \{1, 2, \ldots, p - 1\}.$$

Thus,

$$f(x) = 0, \quad \text{for all } x \in \{1, 2, \ldots, p - 1\}.$$

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

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

Rewriting this in terms of congruence, we get

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

□

Corollary 4.6.2

Let p be prime and set $x = 0$ in the above theorem to get

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

which is the *Wilson's Theorem.*

Proposition 4.6.1

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

Proof. We consider the polynomial

$$f(x) = x^{p-1} - 1$$

in the ring $\mathbb{Z}/p\mathbb{Z}[x]$. We can express it in terms of its coefficients as

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

where $a_1 \in \mathbb{Z}/p\mathbb{Z}$.
Since we are in $\mathbb{Z}/p\mathbb{Z}$, we know from Fermat's theorem that for any $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$,

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

Thus, the equation $x^{p-1} \equiv 1 \pmod{p}$ has exactly $p-1$ roots.
We assume $d \mid (p-1)$, meaning there exists an integer d' such that

$$dd' = p - 1.$$

Now, consider the polynomial division

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

Let $y = x^d$, then the expression simplifies to

$$\frac{y^{d'} - 1}{y - 1}.$$

Using the factorization,

$$\frac{y^{d'} - 1}{y - 1} = (y-1)\frac{1 + y + y^2 + \cdots + y^{d'-1}}{y-1} = 1 + y + y^2 + \cdots + y^{d'-1}.$$

Substituting $y = x^d$, we define

$$g(x) = 1 + x^d + (x^d)^2 + \cdots + (x^d)^{d'-1}.$$

The polynomial $g(x)$ has degree $d(d'-1)$, simplifying to

$$\deg(g(x)) = p - 1 - d.$$

Since $f(x)$ has $p-1$ roots in $\mathbb{Z}/p\mathbb{Z}$, we write

$$f(x) = g(x)(x^d - 1).$$

Reducing modulo p, we obtain

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

Since $f(x)$ has exactly $p-1$ roots, the product $g(x)(x^d-1)$ also has $p-1$ roots. Since $g(x)$ has at most $p-1-d$ roots, it follows that $x^d - 1$ must have exactly d roots in $\mathbb{Z}/p\mathbb{Z}$. □

4.7 Primitve Roots & Quadratic Residues

Cayley Table for $U(\mathbb{Z}/5\mathbb{Z})$

The group of units of $\mathbb{Z}/5\mathbb{Z}$, denoted as $U(\mathbb{Z}/5\mathbb{Z})$, consists of the nonzero elements of $\mathbb{Z}/5\mathbb{Z}$ under multiplication modulo 5. The elements are $\{1, 2, 3, 4\}$, and we construct the Cayley table for multiplication modulo 5:

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Cyclic Groups

Definition 4.7.1: Cyclic Group

A group G is called **cyclic** if there exists an element $g \in G$ such that every element of G can be written as g^k for some integer k. Such an element g is called a **generator** of the group.

Example.

For example, in $U(\mathbb{Z}/5\mathbb{Z})$, the elements 2 and 3 generate the entire group

$$2^1 \equiv 2 \pmod 5, \quad 2^2 \equiv 4 \pmod 5, \quad 2^3 \equiv 3 \pmod 5, \quad 2^4 \equiv 1 \pmod 5,$$
$$3^1 \equiv 3 \pmod 5, \quad 3^2 \equiv 4 \pmod 5, \quad 3^3 \equiv 2 \pmod 5, \quad 3^4 \equiv 1 \pmod 5.$$

However, 4 is not a generator, since

$$4^1 \equiv 4 \pmod 5, \quad 4^2 \equiv 16 \equiv 1 \pmod 5.$$

Primitive Roots Modulo p

Definition 4.7.2: Primitive Root Modulo p

A number g is called a **primitive root** modulo p if the smallest integer k such that $g^k \equiv 1 \pmod p$ is exactly $\varphi(p) = p-1$, meaning g generates the entire multiplicative group $U(\mathbb{Z}/p\mathbb{Z})$.

Example.

For example, in $U(\mathbb{Z}/5\mathbb{Z})$, the numbers 2 and 3 are primitive roots since they generate all elements of the group.

The unit group $U(\mathbb{Z}/4\mathbb{Z})$ consists of the elements $\{1, 3\}$ under multiplication modulo 4

$$3^1 \equiv 3 \pmod 4, \quad 3^2 \equiv 9 \equiv 1 \pmod 4$$

Since 3 has order 2 (not 2, which is $|U(\mathbb{Z}/4\mathbb{Z})|$), it is not a generator. Therefore, $U(\mathbb{Z}/4\mathbb{Z})$ is not cyclic.

Similarly, for $U(\mathbb{Z}/8\mathbb{Z}) = \{1, 3, 5, 7\}$, we compute the orders

$$3^1 \equiv 3 \pmod 8, \quad 3^2 \equiv 9 \equiv 1 \pmod 8$$

$$5^1 \equiv 5 \pmod 8, \quad 5^2 \equiv 25 \equiv 1 \pmod 8$$

$$7^1 \equiv 7 \pmod 8, \quad 7^2 \equiv 49 \equiv 1 \pmod 8$$

Since all elements have order 2, there is no generator. Hence, $U(\mathbb{Z}/8\mathbb{Z})$ is not cyclic.

Some notions regarding order

- Let G be a group and $g \in G$. The **order** of g, denoted by $\text{ord}(g)$, is the smallest positive integer d such that
$$g^d = e$$

where e is the identity element of the group. If no such d exists, we say that g has infinite order.

- If an element has order equal to the size of the group, it generates the entire group.
- For cyclic groups, there exists at least one element whose order is the same as the group order.

U(Z/pZ) is cyclic if p is prime.

Proof. Left as an exercise. □

For a prime p, the multiplicative group of units modulo p is given by

$$|U(\mathbb{Z}/p\mathbb{Z})| = p - 1.$$

If a is a primitive root modulo p, then the elements of $U(\mathbb{Z}/p\mathbb{Z})$ can be written as

$$a, a^2, \ldots, a^{p-1} \pmod{p}.$$

The smallest positive integer n such that

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

is called the *order* of a in $U(\mathbb{Z}/p\mathbb{Z})$. If a is a primitive root, this order is exactly $p - 1$.
For a general modulus n, the group of units modulo n is denoted as:

$$U(\mathbb{Z}/n\mathbb{Z}).$$

An element a is called a *primitive root modulo* n if the smallest integer m such that

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

is given by

$$m = |U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n),$$

where $\varphi(n)$ is the Euler totient function.

Solvability of $x^m \equiv b \pmod{n}$

We investigate when the equation

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

has a solution.
$n = p$ (Prime Modulus)
If n is a prime p, then the equation

$$x^m \equiv b \pmod{p}$$

has a solution if

- $m \mid (p-1)$, ensuring that exponentiation by m stays within the cyclic structure of $U(\mathbb{Z}/p\mathbb{Z})$.
- $b = 1$, which always admits a solution (e.g., $x = 1$).

Solving $ax \equiv b \pmod{n}$
The linear congruence

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

has a solution if and only if $\gcd(a, n)$ divides b.

4.8 Quadratic Congruences Modulo p

Now, consider the quadratic congruence

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

Example.

$p = 3, a = 2$
We check for solutions to

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

Testing $x \in \{0, 1, 2\}$:

- $x = 0 \Rightarrow 0^2 \equiv 0 \not\equiv 2 \pmod{3}$.
- $x = 1 \Rightarrow 1^2 \equiv 1 \not\equiv 2 \pmod{3}$.
- $x = 2 \Rightarrow 2^2 \equiv 4 \equiv 1 \not\equiv 2 \pmod{3}$.

Thus, $x^2 \equiv 2 \pmod{3}$ has no solutions.

Solving $x^2 \equiv 1 \pmod{3}$

Now, we solve

$$x^2 \equiv 1 \pmod{3}.$$

Checking $x \in \{0, 1, 2\}$

- $x = 1 \Rightarrow 1^2 \equiv 1 \pmod{3}$ (solution).
- $x = 2 \Rightarrow 2^2 \equiv 4 \equiv 1 \pmod{3}$ (solution).

Thus, $x^2 \equiv 1 \pmod{3}$ has solutions $x \equiv 1, 2 \pmod{3}$.

4.9 Quadratic Residue modulo p

Definition 4.9.1: Quadratic Residue modulo p

Let p be an odd prime, and a be an integer with $\gcd(a, p) = 1$.
We call a a quadratic residue modulo p if

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

has a solution.

For a prime p, we determine the quadratic residues (QR) and quadratic non-residues (QNR).

Case: $p = 5$

The quadratic residues modulo 5 are given by solving $x^2 \equiv a \pmod 5$

$$x^2 \equiv 1 \pmod 5 \quad \Rightarrow \quad x = \pm 1$$

$$x^2 \equiv 4 \pmod 5 \quad \Rightarrow \quad x = \pm 2$$

Thus, the quadratic residues modulo 5 are

$$\{1, 4\}$$

The quadratic non-residues are

$$\{2, 3\}$$

Case: $p = 7$

By computing $x^2 \mod 7$, we find
Quadratic residues (QR):

$$\{1, 2, 4\}$$

Quadratic non-residues (QNR):

$$\{3, 5, 6\}$$

Case: $p = 11$

Computing $x^2 \mod 11$, we get
Quadratic residues (QR):

$$\{1, 3, 4, 5, 9\}$$

Quadratic non-residues (QNR):

$$\{2, 6, 7, 8, 10\}$$

Proposition 4.9.1

There are exactly $\frac{p-1}{2}$ quadratic residues modulo p.

Proof. Let p be an odd prime. We show that there are exactly $\frac{p-1}{2}$ distinct quadratic residues modulo p.
The quadratic residues modulo p are the values of $a^2 \mod p$ for integers a in the set

$$\{1, 2, \ldots, p-1\}.$$

Since squaring is a symmetric operation, we observe that

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

Thus, each quadratic residue appears at most twice.
To count the number of distinct quadratic residues, consider distinct values $a, b \in \{1, \ldots, p-1\}$ such that

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

Rearranging gives

$$a^2 - b^2 \equiv 0 \pmod{p},$$

which factors as

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

Since p is prime, it must divide one of the factors

$$p \mid (a-b) \quad \text{or} \quad p \mid (a+b).$$

This implies

$$a \equiv b \pmod{p} \quad \text{or} \quad a \equiv -b \pmod{p}.$$

Since a, b are chosen from $\{1, 2, \ldots, p-1\}$, each quadratic residue corresponds to exactly two values of a, namely a and $p-a$.
Since there are $p-1$ values in the set $\{1, \ldots, p-1\}$, and each quadratic residue is counted twice, the number of distinct quadratic residues is

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