BRAC
UNIVERSITY

Inspiring Excellence

MAT422: Theory of Numbers

Lecture notes

Last updated on February 15, 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,

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

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

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*.