MAT422: Theory of Numbers

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

Last Updated: February 9, 2025

Preface

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

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

— Mahmudul Hasan Turjoy

Contents

1
Preliminaries

§ 1.1 Number Systems

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

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

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

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

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

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

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

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

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

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

§ 1.2 Goals and Motivation for doing NT

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

2
References

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

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