# MAS4203
# Notes

Oliver Deng

January 15, 2025

# Contents

## 0.1 Introduction

What is number theory? It is the study of the properties of integers, and functions defined on integers. It is also the study of how real and complex numbers are related to integers.

Number theory is full of simple statements that are very difficult to prove. For example, the Goldbach Conjecture and the Twin Primes Conjecture.

**Conjecture 0.1.1** Goldbach Conjecture

Every even integer $\geq 6$ is a sum of two primes.

**Conjecture 0.1.2** Twin Primes Conjecture

There exist infinitely many primes $p$ for which $p+2$ exists and is also prime.

**Theorem 0.1.1** Euclid's Theorem

There are infinitely many primes.

# Chapter 1

# Divisibility

## 1.1 Notation and Terminology

$$\mathbb{Z} = \{0, \pm 1, \pm 2 \ldots\}$$
$$\mathbb{Z}^+ = \{1, 2, 3 \ldots\}$$
$$\mathbb{N} = \{0, 1, 2, 3 \ldots\}$$
$$\mathbb{Q} = \{x = \frac{a}{b} : a, b \in \mathbb{Z}, b \notin \mathbb{Z}\}$$
$$\mathbb{R} = \text{Real numbers, which are the limits of sequences of rational numbers}$$
$$\mathbb{C} = \{z = x + iy : x, y \in \mathbb{R}, i = \sqrt{-1}\}$$

Recall that $(\mathbb{Z}, +)$ is a group. Also notice that it is commutative (i.e. $a + b = b + a, a, b \in \mathbb{Z}$), and is thus an **abelian group**.

Notice that $(\mathbb{Z}, \times)$ is not a group since there is no multiplicative inverse. However, it is associative, and it distributes over addition (i.e. $a \times (b + c) = (a \times b) + (a \times c)$. What this means is that $(\mathbb{Z}, +, \times)$ is a **ring**.

Two other axioms of $\mathbb{Z}$:

1. Integers are discrete: If $a \in \mathbb{Z}$ and $a \neq 0$, then $|a| \geq 1$
2. Well-ordering principle: Every non-empty subset of $\mathbb{Z}^+$ has a least element. I.e. suppose $S \subset \mathbb{Z}^+, S \neq \varnothing$, then there exists $l \in S$ such that $l \leq a, \forall a \in S$

## 1.2 Divisibility

**Definition 1.2.1: Divisibility**

If $a, b \in \mathbb{Z}$, we say $a$ divides $b$ if there exists $x \in \mathbb{Z}$ such that $ax = b$.

**Note**

If $a$ divides $b$, we write

$$a \mid b$$

If $a$ does not divide $b$, we write

$$a \nmid b$$

**Example 1.2.1** $(5 \mid (-10)$ )

$$5 \times (-2) = -10$$

Immediate consequences:

1. For any $a \in \mathbb{Z}$, we have $a \mid 0$
2. For any $a \in \mathbb{Z}$, we have $1 \mid a$, because $1 \times a = a$

### 1.2.1 Properties of Divisibility

**Theorem 1.2.1**

1. If $a \mid b$, then $a \mid bc, \forall c \in \mathbb{Z}$

   ***Proof:*** Let $a \mid b \implies \exists x \in \mathbb{Z}$ such that $ax = b \therefore axc = bc$ i.e. $a(xc) = bc \implies a \mid bc$ because $xc \in \mathbb{Z}$ (closure under multiplication). 😄

2. If $a \mid b$ and $b \mid c$, then $a \mid c$ (divisibility is transitive)

   ***Proof:*** Let $a \mid b \implies \exists x \in \mathbb{Z}$ such that $ax = b$. Next, let $b \mid c$, so $\exists y \in \mathbb{Z}$ such that $by = c \therefore axy = by = c$ with $xy \in \mathbb{Z}$ (closure under multiplication). Hence $a \mid c$. 😄

3. If $a \mid b$ and $a \mid c$, then $a \mid (ax + cy), \forall x, y \in \mathbb{Z}$

   ***Proof:*** Let $a \mid b \implies \exists x' \in \mathbb{Z} \ni ax' = b$. Let $a \mid c \implies \exists y' \in \mathbb{Z} \ni ay' = c$. Then for $x, y \in \mathbb{Z}$, we have $bx + cy = ax'x + ay'y = a(x'x + y'y)$ (by distributive law) $\therefore a \mid (bx + cy)$ because $x'x + y'y \in \mathbb{Z}$ (closure under multiplication and addition). 😄

4. If $a \mid b$ and $b \mid a$, then $a = \pm b$, or equivalently $|a| = |b|$

   ***Proof:*** Let $a \mid b \implies \exists x \in \mathbb{Z} \ni ax = b$. Next let $b \mid a \implies \exists y \in \mathbb{Z} \ni by = a \therefore axy = by = a$. We now have 2 cases:

   (a) If $a = 0$, then $b = 0$

   (b) $a \neq 0$ and $b \neq 0 \therefore xy = 1 \implies \begin{cases} x = y = 1 \\ x = y = -1 \end{cases} \quad \therefore a = \pm b.$

   😄

5. If $a \mid b$ and $a > 0, b > 0$, then $a \leq b$

   ***Proof:*** Let $a \mid b$, so $\exists x \ni ax = b, x \in \mathbb{Z}$. If $a > 0, b > 0$, then $x > 0 \therefore$ by Axiom 1, $x \geq 1$. Then $b = ax \geq a * 1 = a$. 😄

6. If $a \mid b$, then $ma \mid mb, \forall m \in \mathbb{Z}$

   ***Proof:*** Let $a \mid b$, then $\exists x \in \mathbb{Z} \ni ax = b \therefore max = mb, x \in \mathbb{Z} \therefore ma \mid mb$. 😄

**Theorem 1.2.2** The Division Algorithm

Given any pair of integers $a, b$ with $b > 0, \exists$ a unique pair of integers $q, r \ni a = bq + r$ and $0 \leq r < b$. Also, $b \mid a \iff r = 0$.

***Proof:*** First, we must prove the existence of the pair, and then the uniqueness of the pair. 😄