Math 4573: Number Theory

Lecturer: **James Cogdell**
Notes by: Farhan Sadeek

Spring 2025

1 January 8, 2025

Dr. Cogdell explained the logistics of the class and also took attendance.

1.1 Conjectures in Number Theory

- A number is divisible by 3 if the sum of its digits is divisible by 3.
- **Fermat's Last Theorem**: There are no three positive integers a, b, and c that satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2.
- There are infinitely many primes.
- $\sqrt{2}$ is irrational.
- π is irrational.
- Every number can be written as the sum of four squares (Lagrange's Four Square Theorem). For example, $1000 = 10^2 + 30^2 + 0^2 + 0^2$ and $999 = 30^2 + 9^2 + 3^2 + 3^2$.
- The polynomial $n^2 - n + 41$ produces prime numbers for $n = 0, 1, 2, \ldots, 40$, but not for $n = 41$.
- Euler conjectured that no n^{th} power can be written as the sum of two n^{th} powers for $n > 2$. This was proven false by the counterexample $144^5 = 27^5 + 84^5 + 110^5 + 133^5$.
- **Goldbach's Conjecture**: Every even integer greater than 2 can be written as the sum of two primes. For example, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 5 + 5$, $12 = 5 + 7$, $14 = 7 + 7$, $16 = 3 + 13$, $18 = 7 + 11$. This has been verified for numbers up to 100,000 but remains unproven.

Number theory is related to **Abstract Algebra**, but also intersects with other domains such as **Combinatorics, Analysis, and Topology**. We will accept a few fundamental facts about **Number Theory**.

> **Fact 1**
> If $\mathcal{S}$ is a non-empty set of positive integers, then $\mathcal{S}$ contains a smallest element. This is known as the Well-Ordering Principle.

1.2 Divisibility

This concept has been known since the time of Euclid.

Definition 2

An integer b is divisible by an integer $a \neq 0$ if there is an integer x such that $b = ax$. We write this as $a \mid b$. If b is not divisible by a, we write $a \nmid b$.

There are two derivative notions:

- If $0 < a < b$, then a is called a **proper divisor** of b.
- If $a^k \mid\mid b$, it means $a^k \mid b$ and $a^{k+1} \nmid b$.

Theorem 3

Let a, b, and c be integers. Then the following are true:

- If $a \mid b$, then $a \mid bc$.
- If $a \mid b$, then $a \mid b + c$.
- If $a \mid b$ and $a \mid c$, then $a \mid b + c$.
- If $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.
- If $a \mid b$ and $a > 0$ and $b > 0$, then $a \leq b$.
- If $m \neq 0$ and $a \mid b$, then $am \mid bm$.
- If $a \mid b_1, a \mid b_2, \ldots, a \mid b_n$, then $a \mid \sum_{i=1}^{n} b_i x_i$ for any integers x_i.

Theorem 4 (The Division Algorithm)

Given integers a and b with $a > 0$, there exist unique integers q and r such that $0 \leq r < a$ and $b = aq+r$.

Proof. Consider the arithmetic progression $\ldots, b-3a, b-2a, b-a, b, b+a, b+2a, b+3a, \ldots$. In this sequence, select the smallest non-negative member. This defines r and satisfies the inequalities of the theorem. Since r is in the sequence, it can be written as $b - qa$. To prove the uniqueness of q and r, suppose there is another pair q_1 and r_1 that satisfies the same conditions. We first prove that $r = r_1$. If not, assume $r < r_1$, so $0 < r_1 - r < a$. But $r_1 - r = a(q - q_1)$, meaning $a \mid (r_1 - r)$, which contradicts the fact that $0 < r_1 - r < a$. Thus, $r = r_1$ and $q = q_1$. $\square$

Fact 5

If $a \mid b$, then r satisfies the stronger inequality $0 \leq r < a$.

Fact 6

The Division Algorithm can be stated without the assumption $a > 0$. Given integers a and b with $a \neq 0$, there exist integers q and r such that $b = qa + r$ with $0 \leq |r| < |a|$.