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

- Every number is divisible by 3 if the sum of its digits are deivisimble by 3.
- **Fermat's last theorem**: Every number is a solution to $x^2 + y^2 = z^2$.
- There are infinitely many primes.
- $\sqrt{2}$ is irrational.
- π is irrational.
- Every number can be written as the sum of 4 squares (Lagrange). e.g. $1000 = 10^2 + 30^2 + 0^2 + 0^2$ and $999 = 30^2 + 9^2 + 3^2 + 3^2$.
- $n^2 - n + 41$ is a prime. [This is proven to be false if $n = 41$]. There is a counterexample to this.
- Euler conjectured that no n^{th} power can be written as the sum of two n^{th} powers for $n > 2$. [This is proben to be false] e.g. $144^5 = 27^5 + 84^5 + 10^5 + 133^5$
- **Goldbach's Conjecture** : Every even integer greater than 2 can be written as the sum of two primes. e.g. $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 5+5$, $12 = 5+7$, $14 = 7+7$, $16 = 3+13$, $18 = 7+11$. [Yet to be proven if it's true or false, but this has been verified till 100,000]

The theory of number is related to **Abstract Algebra**. But also, in other domains like **Combinatorics, Analysis, Topology**. We will accept a few facts about **Number Theory**.

Fact 1
However, if SSis a set of positive integers, not empty then SScontains a member such that $s \leq a$. This is stated as follows: If SSis a set of positive integers that contains 1 and contains $n+1$ then SScontains all positive integers.

1.2 Divisibility

This has been known since the time of Euclid.

Definition 2
An integer b is divisible by an integer a, not zero, if there is an integer x so that $b = ax$. So we will write as $a \mid b$. In case, n isn't divisible by b, we write as $a \nmid b$.

There are two derivative notion.

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

Theorem 3
- 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 $a = b$.
- 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 $a \mid b_1, a \mid b_2, \ldots, a \mid b_n \to \sum_{i=1}^{n} b_i X_i$

Theorem 4 (The division algorithm)
Given integers a b, with $a > 0$, then there exists 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 the sequence, select the sequence if the smallest non-negative member. So this definition of r is satifies the inequalities of the theorem. But also, the being in the sequence of the form

$$b - qa$$

This is defined in terms of qr. To prove the uniqueness of q and r, suppose there is another r pair q_1, and r_1 satiesfies the same conditions.
We first prove that $r = r_1$. For if not, we may assume $r < r_1$, so $0 < r_1 - r < a$. But we see that $r - 1 = a(q - q_1)$ meaning $a \mid (r_1 - r)$ so it's a contradiction to to the theorem 1, part 5. So $q = q_1$ and $r = r_1$. $\square$

Fact 5

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

Fact 6

If we stated the theorem, with the assumption, $a > 0$. However, this hypothesis is not necessary. We may formulate the theorem without a, given integers a and b such that $a \neq 0$ there then exists q and r such that $b = qa + r$ wich $0 \leq |a|$.