A Bad Introduction to Number Theory

Albert Ye

August 23, 2023

1 Lecture 1

Definition 1

An integer $p \neq 0, 1, -1$ is **prime** if the only integers which divide p are ± 1 and $\pm p$.

Recall that the integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

Theorem 2 (Twin Prime Conjecture)

There are infinitely many $p \in \mathbb{N}$ such that p is prime and $p + 2$ is prime.

Yitang Zhang proved bounded gaps between primes, so there are infinitely many prime $p, p + N$.

Theorem 3 (Goldbach Conjecture)

Every even number can be written as the sum of two primes.

Vinagradar proved that every odd number can be written as the sum of 3 primes. The proof should use something called sieves.

Proposition 4

There are infinitely many primes.

Proof. Suppose not and $p_1, \ldots, p_n$ are all the primes. Then, let $p_1 \cdots p_n + 1 = N$.

As we will see, every integer admits a unique decomposition into a product of primes. □

1.1 Counting Primes

Let $\pi(x) : N \to \mathbb{N}$ return the number of primes p such that $0 < p < x$.

Then, $\pi(x)$ is unbounded: $\lim_{x\to\infty} \pi(x) = \infty$.

Theorem 5 (Prime Number Theorem)

$$\lim \frac{\pi(x)}{x/\log x} = 1.$$

In other words, $\pi(x) \to \frac{x}{\log x}$¿

A better approximation is $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$. The error for $\mathrm{Li}(x)$ is $|\pi(x) - \mathrm{Li}(x)| = O(\log x\sqrt{x})$.

Theorem 6 (Uniqueness of Prime Factorization)
Every integer $0 \neq n \in \mathbb{Z}$ can be written as

$$n = (-1)^{Z(n)} \prod_{p \text{ prime}} p^{a_p} \qquad a_p \in \mathbb{N},$$

where all but finitely many a_p are zero, $\epsilon(n) = \begin{cases} 0 & n > 0 \\ 1 & n < 0 \end{cases}$.

To prove this, we first look at a lemma:

Lemma 1.1.1
If $a, b \in \mathbb{Z}$ and $b > 0$, there exist integers q, r such that $a = qb + r$ and $0 \leq r < b$.

Proof. Consider the set of integers of the form $\{a - xb | x \in \mathbb{Z}\} = S$. The set S contains infinitely many positive integers, so contains a least positive integer $r = a - qb$.

Remark 7
This property does not hold for $S \subset \mathbb{Q}$. Consider $S = \{1, \frac{1}{2}, \frac{1}{4}, \ldots\}$.

□

The rest of the proof will follow later.

Definition 8
Let $a_1, \ldots, a_n$ be integers. Denote $(a_1, \ldots, a_n)$ to be the set $\{b_1 a_1 + \cdots + b_n a_n | b_i \in \mathbb{Z}\}$.