Lecture 1. Introduction to Numbers *July 18, 2025*

1 Introduction to Numbers

1.1 Numbers

Leopold Kronecker story: *God gave us the natural numbers, everything else is man's handiwork.*

This course introduces abstraction

> **Definition 1** (Abstraction). Abstraction means that we want to use a single symbol to represent various things. Example: 2 oranges and 2 elephants; the elephants and oranges do not matter, only the 2.

Mathematics as we know it is currently the language of set theory.

Set Theory really starts with Georg Cantor. He begins with the set of natural numbers: $\mathbb{N} = \{1, 2, 3, \ldots\}$. Interestingly enough, Kronecker, the advisor of Cantor, did not appreciate the concept of infinity in the way that Cantor did. We may use $\hat{\mathbb{N}} = \{0\} \cup \mathbb{N}$.

Zahl means number in German, which is how we get the $\mathbb{Z}$ set as the representation for the integers. Of course, from there we have the rational numbers ($\mathbb{Q}$) constructed from $r = \frac{p}{q}$, s.t. $p, q \in \mathbb{Z}$ and $q \neq 0$.

Hippasus, student of Pythagoras, was the original person to conceptualize of irrational numbers through his studies in geometry; he found that for a right triangle, whose a and b sides are both equal to 1, the hypotenuse was then equal to $\sqrt{2}$. Hippasus then proved that $\sqrt{2}$ could not be represented by any rational number. The Pythagoreans (the cult of Pythagoas) were so aghast that this was the case that they killed Hipparchus for his blasphemous discovery, throwing him into the sea. We may use various symbols for the irrational numbers, but here we will use $\mathbb{Q}^c$, i.e., $\mathbb{Q}$-compliment.

The union between the rational and irrational numbers, finally, compose the set of reals (the set of real numbers), $\mathbb{R}$.

A set that is worth study and rather important is the set of prime numbers, $\mathbb{P}$. All natural numbers have a unique prime factorization, let $n \in \mathbb{N}$, then $\forall n$, $n = p_1^{q_1} \ldots p_r^{q_r}$. One cannot be a prime number, by convention, for the very reason that every $p_r^{q_r}$ is unique, and if $1 \in \mathbb{P}$, then there exists infinitely many cases of m s.t. $1^m = 1$, which contradicts the uniqueness of a given prime factor (e.x.: $20 = 2^2 \cdot 5 = 1 \cdot 2^2 \cdot 5 = 1^{99} \cdot 2^2 \cdot 5 = \ldots$).

1.2 Induction

If you have a mathematical statement involving the symbol n, say $P(n)$, the statement $P(n)$ may or may not be true. Thus, we take the following steps to see if $P(n)$ is true:

1. $P(1)$ is true;
2. $P(n+1)$ is true;

then $P(n)$ holds for all $n \in \mathbb{N}$.

A classic example is of the well known result $1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$.

Proof. Let $P(n)$ be the statement $1+2+\ldots+n=\frac{n(n+1)}{2}$, then

$$P(1)=1=\frac{1(1+1)}{2}=\frac{2}{2}=1;$$

$$P(n+1)=1+2+\ldots+n+(n+1)=\frac{n(n+1)}{2}+(n+1)=\frac{(n+2)(n+1)}{2}=\frac{(n+1)((n+1)+1)}{2};$$

thus, $P(n)$ is true. □

Using induction, we may prove the most famous result in all of proofs: the proof that there exists infinitely many primes. First, however, we need to introduce some more information pertinent to the proof. Additionally, we will not be using the original proof by Euclid, instead using a more modern proof.

Definition 2 (Fermat Numbers)**.** A Fermat number is an number in the form of $F_n=2^{2^n}+1$. Notice that any F_n is odd.

There are infinitely many Fermat numbers (since there are infintiely many numbers), and for any two Fermat numbers, the prime divisors are relatively coprime, i.e., they have no shared prime factors.

Theorem 1.

$$\prod_{k=0}^{n-1} F_k = F_n - 2,\ \forall 1 \leq n \in \mathbb{N}$$

Proof. We will use induction to show that this identity holds:

Base case:

$$\prod_{k=0}^{n-1} F_k = F_0 = 2^{2^0} = 2$$
$$F_1 - 2 = 2^{2^1} - 2 = 2.$$

Thus, the base case holds. Then for $n+1$:

$$\begin{aligned}
F_{n+1}-2 &= \prod_{k=0}^{n} F_k \\
F_{n+1}-2 &= \left(\prod_{k=0}^{n-1} F_k\right) F_n \\
F_{n+1}-2 &= (F_n-2)(F_n) \\
2^{2^{n+1}}+1-2 &= (2^{2^n}+1-2)2^{2^n}+1 = (2^{2^n}-1)(2^{2^n}+1) \\
2^{2^{n+1}}-1 &= (2^{2^n})^2-1 \\
2^{2^{n+1}} &= 2^{2^1 2^n} \\
2^{2^{n+1}} &= 2^{2^{n+1}}.
\end{aligned}$$

□

Theorem 2. There exists no two Fermat numbers that are coprime.

Proof. We begin with an identity regarding Fermat numbers:

$$\prod_{k=0}^{n-1} F_k = F_n - 2, \forall 1 \leq n \in \mathbb{N}.$$

Let q be a divisor of F_k and F_n (i.e., a common divisor); note by definition, $k < n$. Thus both sides must be divisible by q. This additionally means that 2 must also be divisible by q; the divisors of 2 are $1, 2$; note that 1 is not a prime number, thus, we only need to check 2. But notice that $F_n - 2$ being divisible by 2 means that F_n is divisible by 2; this cannot be, since, by definition, F_n must always be odd! Thus we have a contradiction. □

Fermat had *assumed* that all Fermat numbers are Fermat primes, however Euler refuted that in 1732, showing that $F_5 = 4294967297 = 641 \cdot 6700417$. The question as to if there are infintely many Fermat primes (conjected by Eistenstein in 1844) has yet to be proven or refuted. This also begs the question if there are infintely many composite Fermat numbers and if F_n is composite for all $n > 4$, both of which are still open problems.

We may finally begin our proof that there exists infintely many primes.

Theorem 3 (Existence of Infinitely Many Primes)**.** There are infinitely many primes.

Proof. Let us imagine a product that is the product of all prime numbers:

$$\prod_{k=0}^{n} p_k = \mathcal{P}$$

where k is the number of primes. I will finish this proof later. □

There are two types of decimal numbers: those represented by terminating decimals, and those represented by infinite decimals. Note, that infinite decimals does not mean irrational. A famous example is $1 = 0.999\ldots$ or $\frac{1}{3} = 0.333\ldots$. We ask ourselves when does $\frac{p}{q}$, $q \neq 0$ give me a terminating decimal? Every non-terminating decimal that is not irrational has a periodic pattern within it.

kk

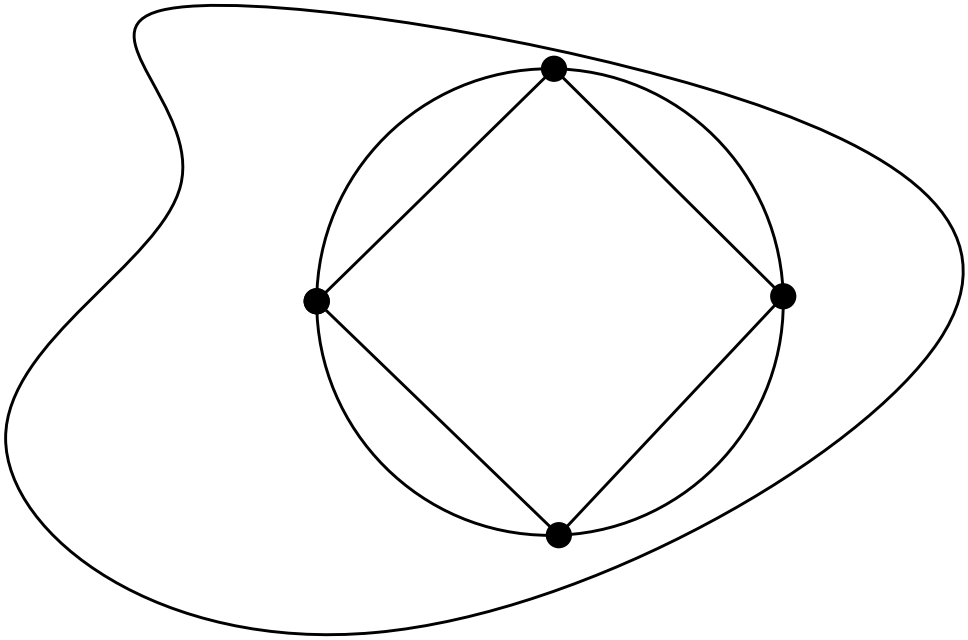

Figure 1: Untitled