CS 173 Lecture 36: Prime Numbers

Prime Numbers:

- Fascinating. Spurred developments in:
  - Abstract Algebra
  - Complex Function Theory
  - Algebraic Geometry & Topology
  - Deep Connections between these
- Form the basis of modern crypto.

Definition: An integer $q \geq 2$ is <u>prime</u> if its only positive factors are 1 & q.

(a is a factor of b $\Leftrightarrow a|b$.)

otherwise, q is <u>composite</u>.

Definition: For an integer $q > 1$, its <u>prime factorization</u> is the expression of q as a product of its prime factor.

$18 = 2 \cdot 3 \cdot 3 = 2 \cdot 3^2$

$70 = 2 \cdot 3 \cdot 5$

$187 = 11 \cdot 17$

Theorem (Fundamental Theorem of Arithmetic) Every integer greater than 1 has a unique prime factorization

(up to rearrangement of factors)

Proof? (Later, requires induction)

Theorem (Infinitude of primes). There are infinitely many prime numbers.

(Euclid's Theorem): There are infinitely many prime numbers.

Proof. We will prove that there is no finite set of prime numbers that contains all of them.

Let P be any finite set of prime numbers, say $P = \{p_1, \dots, p_n\}$

Consider $q = 1 + \prod_{i=1}^{n} p_i$.

Then for all $p_i \in P$, $p_i \nmid q$. $\nexists\, k$ s.t. $q = kp_i$

This means that the prime factorization of q contains a prime number not in P. $\square$