Prime numbers

Def

An integer $p > 1$ is **prime** if its only positive divisors are $1, p$.

n not prime $\Leftrightarrow$ n **composite**

(prime $\Leftrightarrow$ irreducible).

Def.

In a commutative ring A with unity.

$I \subseteq A$ is prime if.

$$ab \in I \Rightarrow a \in I \quad b \in I.$$

In $\mathbb{Z}$:

Theorem $n \in \mathbb{Z}$ $n > 1$

n prime $\Leftrightarrow$ (n) is a prime ideal.

Pf.

$\boxed{\Leftarrow}$ (n) prime ideal

$n = ab \Rightarrow n \in (n)$ ← prime

$\Rightarrow a \in (n)$ or $b \in (n)$

$\Rightarrow n \mid a$ or $n \mid b$

$\Rightarrow a = n$ or $b = n$

(because $a, b \geq 1$)

$\boxed{\Rightarrow}$ n irreducible

$n \mid ab$, $n \nmid a$ $\Rightarrow$ $\gcd(a, n) = 1$

Bézout identity

$1 = ax + ny \quad x, y \in \mathbb{Z}$

$b = abx + nby \Rightarrow n \mid b.$ ∎

n divides

FUNDAMENTAL THEOREM OF ARITHMETIC

Every positive integer > 1 can be written as a product of primes.

This representation is unique, apart from the order of the factors.

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \qquad k_i > 0$$

p_i distinct primes

Proof $\Rightarrow$ 2 parts

1. primes are irreducible
2. uniqueness of factorisation.

Primes are infinitely many

Define: $\pi : \mathbb{R}_{>0} \longrightarrow \mathbb{N}$

$\pi(x) = |\{p \text{ prime} \mid p \leq x\}|$

Examples

$\pi(10) = |\{2, 3, 5, 7\}| = 4$

$\pi(12,7) = |\{2, 3, 5, 7, 11\}| = 5$

Primes are infinitely many $\iff$

$$\lim_{x \to \infty} \pi(x) = \infty$$

Euclid proof

Assume that $S = \{p_1, \dots, p_2\}$ finite set of primes.

Consider $N = p_1 \cdots p_2 + 1$

$\rightsquigarrow$ FTA: $\exists p$ prime such that $p \mid N$.

$p \neq p_i$ for every i, because

$p_i \mid p_1 \cdots p_2$

so if $p_i \mid N$ then

$p_i \mid N - p_1 \cdots p_2 = 1$ $\rightsquigarrow$ impossible.

$\rightsquigarrow$ the set of primes cannot be finite. ∎

Euler proof

Let p_n be the n-th prime number

$p_1 = 2 \qquad p_2 = 3 \qquad p_3 = 5 \dots$

$\forall_2$ let

$$N_2 = \{ n \in \mathbb{N} \mid n = p_1^{k_1} \cdots p_2^{k_2},\ k_1, \dots, k_2 \geq 0 \}$$

$$\sum_{n=0}^{\infty} \frac{1}{n} = \lim_{2 \to \infty} \sum_{n \in N_2} \frac{1}{n}$$

diverges

$$= \lim_{2 \to \infty} \sum_{k_1, \dots, k_2} \frac{1}{p_1^{k_1}} \cdots \frac{1}{p_2^{k_2}}$$

$$= \lim_{2 \to \infty} \prod_{i=1}^{2} \sum_{k=0}^{\infty} \frac{1}{p_i^{k}}$$

$$= \lim_{2 \to \infty} \prod_{i=1}^{2} \left(1 - \frac{1}{p_i}\right)^{-1}$$

$$= \prod_{p} \left(1 - \frac{1}{p}\right)^{-1}$$

$\Downarrow$

INFINITELY MANY
BECAUSE $\sum \frac{1}{n}$ diverges

Consequences

① $\sum_{p} \frac{1}{p}$ diverges

Proof

We have $\sum_{n \le N} \frac{1}{n} \le \prod_{p \mid N} \left(1 - \frac{1}{p}\right)^{-1}$

Take log

$$\log\left(\sum_{n \le N} \frac{1}{n}\right) \le -\sum_{p \le N} \log\left(1 - \frac{1}{p}\right)$$

(in general for $0 < x \le \frac{1}{2}$

$-\log\left(1 - \frac{1}{x}\right) < x + x^2$)

$$\le \sum_{p \le N} \frac{1}{p} + \frac{1}{p^2}$$

$$\log\left(\sum_{n \le N} \frac{1}{n}\right) \le \sum_{p \le N} \frac{1}{p} + \sum_{p \le N} \frac{1}{p^2}$$

$\Rightarrow$ divergent

$\Rightarrow$ convergent

$\Downarrow$

DIVERGES

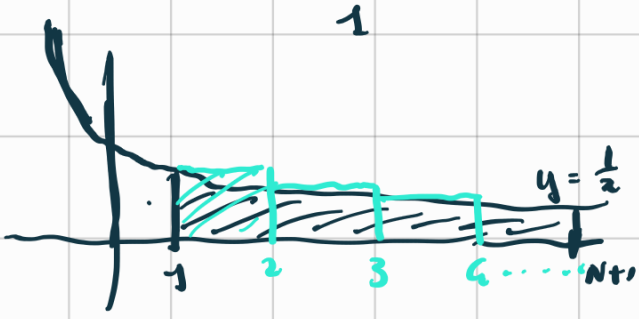
(2) $\pi(x) > \log\log x$

Pf:

$$\sum_{n \le N} \frac{1}{n} < \prod_{p \mid N} \left(1 - \frac{1}{p}\right)^{-1}$$

every $\left(1 - \frac{1}{p}\right) \ge \frac{1}{2}$ so $\cdot$ r.s.h $\le 2^{\pi(N)}$

l.s.h. $\sum_{n \le N} \frac{1}{n} > \int_1^{N+1} \frac{dx}{x} = \log(N+1)$



Therefore $\log(N+1) < 2^{\pi(N)}$ when $N \ge 2$

For $x \ge 2$ let $N \le x < N+1$ $N = [x]$ ← integer part of x

Then

$$\log(x) < \log(N+1) < 2^{\pi(N)} \le 2^{\pi(x)} \le e^{\pi(x)}$$

Take logarithms.

$$\log\log(x) \le \pi(x) \quad \blacksquare$$

Hadamard, de la Vallée-Poussin (1896)

PRIME NUMBER THEOREM.

$$\pi(x) \sim \frac{x}{\log x}$$