Defn: Let $n \in \mathbb{N} \setminus \{0, \pm 1\}$

We say n is a **COMPOSITE** integer if we can write $n = a \cdot b$, where $a, b \in \mathbb{Z}$, $a, b \neq \pm 1$ $\iff$

$\iff |a| \cdot |b| \geq 2 \iff |a| \cdot |b| < |n|$

If $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ is not composite, we say n is **prime** number.

Ex: n prime $\iff -n$ is prime

$2, 3, 5, 7$ primes

$8, 4, 6$ composite

Mersenne

$M_n = 2^n - 1$

$M_2 = 2^2 - 1 = 3$ prime

$M_3 = 2^3 - 1 = 7$ prime

$M_4 = 2^4 - 1 = (2^2-1)(2^2+1)$ not prime

$n = a \cdot b \nearrow (2^a - 1)/(2^n - 1)$
$\neq \pm 1$

n prime

$M_5 = 2^5 - 1 = 31$ prime

But: $M_{11} = 2047 = 23 \cdot 89 =$ not prime

G i M P S

Great Internet Mersenne Prime Search

$M_{82.589.933}$ is prime

Oct 2024: $M_{136.279.841} \simeq 41 \cdot 10^6$ digits

Only 52 Mersenne primes are known so far.

Q: How can you decide if a number is prime?

Eratosthenes' Sieve

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~

Given n → test if $d \leq \sqrt{n}$ is a factor for n

Probabilistic methods to test primality

→ Fermat's test

→ Miller-Rabin Algorithm

Rmk: p prime

For $a \in \mathbb{Z}$ $\gcd(a,p) = \begin{cases} 1 \iff p \nmid a \\ p \iff p \mid a \end{cases}$

Theorem: Let $p \in \mathbb{Z} \setminus \{0, \pm 1\}$. Then

p prime $\Leftrightarrow \forall a, b \in \mathbb{Z}$ s.t.
$p \mid a \cdot b \Rightarrow p \mid a$ or $p \mid b$

Proof: "$\Rightarrow$" Assume p prime and $p \mid a \cdot b$

If $p \mid a$ ✓

If $p \nmid a \Rightarrow \gcd(p, a) = 1$ $\Rightarrow p \mid b$

"$\Leftarrow$" Assume $p \mid a \cdot b \Rightarrow p \mid a$ or $p \mid b$

We prove that p is prime.

Assume, by contradiction, that p is composite.

$p = a \cdot b \Rightarrow p \mid a \cdot b \Rightarrow p \mid a$ or $p \mid b$

$\Rightarrow |a| \geq |p|$ and $|b| \geq |p|$ } Contradiction

$2 \leq |a|, |b| < |p|$

$p \neq 0 \Rightarrow a, b \neq 0$

Theorem (Euclid): Any $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ can be written as a product of prime numbers. Moreover, this decompositions is unique, up to reordering the therms and sign changes.

For $\forall n \in \mathbb{Z} \setminus \{0, \pm 1\}$

$$n = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$$; with $p_1, p_2, \ldots, p_r > 0$ distinct primes, $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}^*$

Proof: E.T. work with $n \geq 2$

Complete induction on n.

- If n is prime $\Rightarrow$ the decomposition is $n = n$
- Assume n is not prime $\Rightarrow$ we may write

$$n = a \cdot b, \text{ where } 2 \leq a, b < n$$

by the induction hypotheses:

a = product of primes
b = product of primes
$\Rightarrow a \cdot b$ = product of primes

Uniqueness: by complete induction on n

- n prime ✓ $n = n$
- n composite $n = p_1 \cdot p_2 \cdot \ldots \cdot p_t$ as prod. of primes
  $n = q_1 \cdot q_2 \cdot \ldots \cdot q_s$

$p_1 \mid n = q_1 \cdot q_2 \cdot \ldots \cdot q_n$

$\Rightarrow p_1 \mid q_i$ for some $i = \overline{1,s}$

q_i prime $\Rightarrow p_1 = q_i$

$\frac{n}{p_1} = \frac{n}{q_i} < n$

By the induction hypothesis they have a unique decomposition into primes: $t-1 = s-1$

Up to rearrangement

$p_2, \dots, p_t = q_1, \dots, \cancel{q_i}, \dots, q_s$

Theorem: There are infinitely many primes

Pf: If we assume that, $p_1, p_2 \dots, p_n$ are all the prime integers (1)

Let $t = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$

Then $\gcd(t, p_i) = 1 \Rightarrow p_i \nmid t \ \forall i = \overline{1,n}$

t is a product of primes $\Rightarrow \exists i \ \ p_j \mid t$ (2)

(1) and (2) are in contradiction

Let $x \in \mathbb{N}$ call $\pi(x) =$ nr. of primes in $[0, x]$

Theorem (Hadamard, de la Vallée-Poussin, 1890)

$$\pi(x) \sim \frac{x}{\ln x} \quad \text{as} \quad x \to \infty$$

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1 \rightsquigarrow \text{Prob}(x \text{ is prime}) \simeq \frac{1}{\ln x}$$

Prop: If n has the primary decomposition $n = \pm p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_t^{a_t}$, then any division $d \mid n$ is of the form:

$$d = \pm p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_t^{b_t} \quad \text{where } 0 \leq b_i \leq a_i \ \forall i = \overline{1,t}$$

Pb: For any $d \mid n$, its prime factors also are prime factors for n

Consequence: $\mathbb{N}$

$$n = \pm p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$$

$$m = \pm p_1^{b_1} p_2^{b_2} \cdots p_t^{b_t}$$

where $0 \leq a_i, b_i$

$$\gcd(n, m) = \prod_{i=1}^{t} p_i^{\min\{a_i, b_i\}}$$

$$\operatorname{lcm}(n, m) = \prod_{i=1}^{t} p_i^{\max\{a_i, b_i\}}$$