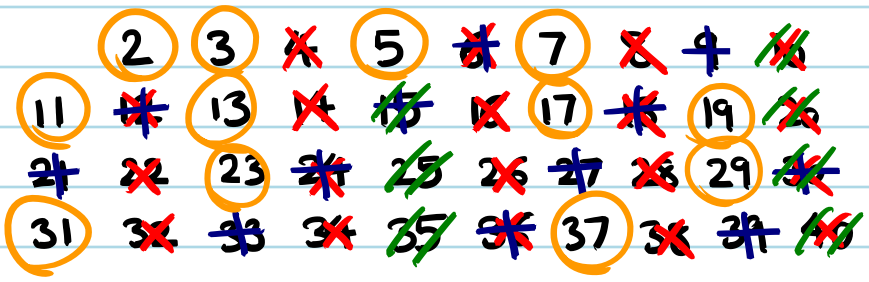
Lecture 5 : Primes, Congruence.

How can we find all the prime numbers $\leq n$?

In the previous lecture we proved:

Lemma A integer $n > 1$ is either prime or it has a divisor $1 < a \leq \sqrt{n}$.

This means among the numbers $1, 2, \ldots, N$ it is enough to cross out numbers that are (non-trivial) multiples of a number $\leq \sqrt{N}$. So to list all the primes ≤ 40 , we need to cross out multiples of numbers ≤ 6.



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

$$\Rightarrow \lim_{x \to \infty} \frac{\pi(x)}{x / \ln x} = 1 . \quad \text{(Prime number theorem)}$$

If one understands the error term $\left| \pi(x) - \frac{x}{\ln x} \right|$, she gets a 1,000,000 $ prize and definitely a Fields

medal.

Thm (The Fundmental theorem of Arithmetic)

Every integer >1 can be uniquely written as

$$p_1^{k_1} \cdot \cdots \cdot p_m^{k_m},$$

where $p_1 < p_2 < \cdots < p_m$ are prime numbers and $k_1, \ldots, k_m$ are positive integers.

Remark. ① FTA tells us that primes are building blocks of integers with respect to multiplication.

② If we have the factorization of a number to its prime factors, we can easily list the set of it divisors and compute the value of many arithmetic functions (called multiplicative functions) e.g.

$d(n) :=$ number of its positive divisors,

$\sigma(n) :=$ sum of its positive divisors,

$\mu(n) :=$ the Möbius function,

$\varphi(n) := |\{a \mid 1 \le a \le n, \ \gcd(a,n)=1\}|.$

③ So far there is no effective algorithm to decompose a positive integer into its prime factors. And at the moment credit card companies rely on this:

> If p and q are huge prime numbers, it takes for ever to decompose pq into prime factors.

Pf of FTA It has two parts: existence and uniqueness. For both parts, we proceed by contradiction and use the well-ordering principle

Existence. Suppose this is NOT true, i.e.

$$\Sigma_1 := \{ n \in \mathbb{Z}^{>1} \mid n \text{ cannot be written as product of primes} \}$$

is non-empty. So by the well-ordering principle Σ_1 has a smallest element n_1.

Since n_1 cannot be written as product of primes, it is NOT prime. So $n_1 = ab$ where $1 < a, b < n_1$.

Since n_1 is the smallest element of Σ_1 and

$1 < a, b < n_1$, $\underline{a, b}$ can be written as product of primes. Therefore $n_1 = a\,b$ can be written as product of primes. This contradicts the fact that $n_1 \in \Sigma_1$.

Uniqueness. Again suppose to the contrary that

$$\Sigma_2 := \{ n \in \mathbb{Z}^{>1} \mid n \text{ can be decomposed in at least two (genuinely) different ways} \}$$

is non-empty. So by the well-ordering principle, Σ_2 has a smallest element n_2. So

$$n_2 = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m} = q_1^{l_1} \cdot \ldots \cdot q_s^{l_s}$$

where $p_1 < \ldots < p_m$ and $q_1 < \ldots < q_s$ are primes, and $k_1, \ldots, k_m$ and $l_1, \ldots, l_s$ are positive integers.

And these are NOT the same decompositions.

$p_1 \mid \text{LHS} = \text{RHS} \xrightarrow[\text{lemma}]{\text{Euclid's}} p_1 \mid q_i$ for some $\underline{i} \Rightarrow p_1 = q_i$.

$q_1 \mid \text{RHS} = \text{LHS} \Rightarrow q_1 \mid p_j$ for some $\underline{j} \Rightarrow q_1 = p_j$

$\Rightarrow \quad p_1 = q_{j_2} \geq q_{j_1} = p_j \geq p_1 \quad \Rightarrow \quad p_1 = q_{j_1}$.

$\Rightarrow$ (suppose $k_1 \leq \ell_1$)

$$n' := p_2^{k_2} \cdots p_m^{k_m} = p_1^{\ell_1 - k_1} q_{j_2}^{\ell_2} \cdots q_{j_s}^{\ell_s} < n$$

if $n' = 1$ $\Rightarrow$ $m = s = 1$, $p_1 = q_{j_1}$ and $k_1 = \ell_1$

which means they are the same decomposition.

which is a contradiction.

$n' > 1$

$n > n'$

n smallest in Σ_2 $\Rightarrow$ n' has a unique factorization into primes $\Rightarrow$

- $\ell_1 - k_1 = 0$
- $m - 1 = s - 1$
- $p_2 = q_{j_2}$, $p_3 = q_{j_3}$, $\cdots$, $p_m = q_{j_m}$
- $k_2 = \ell_2, \ldots, k_m = \ell_m$

$\Rightarrow$ the starting decompositions are the same,

which is a contradiction. ∎

Cor. (Euclid) There are infinitely many primes.

Pf. Suppose to the contrary that there are only finitely

many primes $p_1 < p_2 < \cdots < p_n$. Consider $N = p_1 \cdots p_n + 1$.

Let p be a prime factor of N. So $p = p_i$ for some i.

Hence $\left.\begin{array}{l} p_i \mid p_1 \cdots p_n + 1 \\ p_i \mid p_1 \cdots p_n \end{array}\right\} \Rightarrow p_i \mid 1$ which is a contradiction. ■

Cor. Let $n = p_1^{k_1} \cdots p_m^{k_m}$ and $d \in \mathbb{Z}^{>0}$. Then

$$d \mid n \iff d = p_1^{l_1} \cdot p_2^{l_2} \cdots p_m^{l_m} \text{ where } 0 \le l_i \le k_i.$$

(as before $p_1 < \cdots < p_m$ are primes and $k_1, \ldots, k_m$ are positive integers.)

Pf ($\Leftarrow$) This is clear: $n = \prod p_i^{k_i} = \underbrace{\left(\prod p_i^{k_i - l_i}\right)}_{\in \mathbb{Z}} \underbrace{\left(\prod p_i^{l_i}\right)}_{d}$.

($\Rightarrow$) $d \mid n \Rightarrow n = dd'$ for some positive integer d'

$d = \prod p^{v_p(d)}$ (notice that $v_p(d)$'s are zero except

$d' = \prod p^{v_p(d')}$ for finitely many prime p.)

$\Rightarrow d \cdot d' = \prod p^{v_p(d) + v_p(d')}$.

$\Rightarrow$ For any prime p, $v_p(n) = v_p(d) + v_p(d') \ge v_p(d)$

$\Rightarrow d = \prod p_i^{l_i}$ where $l_i = v_{p_i}(d) \le v_{p_i}(n) = k_i$. ■

Cor. $d(\prod p_i^{k_i}) := |\{ d \mid \prod p_i^{k_i} \mid 1 \le d \}|$

$= \prod (k_i + 1)$.

Pf. A positive number is a divisor of $p_1^{k_1} \cdots p_m^{k_m}$

if and only if it is of the form

$$p_1^{l_1} \cdots p_m^{l_m}$$

where $0 \le l_1 \le k_1$, $0 \le l_2 \le k_2$, $\cdots$, $0 \le l_m \le k_m$.

So for l_1 we have $k_1 + 1$ choices, ... Hence by the multiplication principle we have

$$(k_1+1)(k_2+1) \cdots (k_m+1)$$

possibilities for $l_1, \ldots, l_m$. And by uniqueness of prime decomposition any such possibility gives us a different divisor. ■

Exp. $\sqrt{2}$ is irrational.

Pf. If not, $\exists\, m, n \in \mathbb{Z}^+$ s.t. $\frac{m}{n} = \sqrt{2}$.

$\Rightarrow m^2 = 2n^2$

$\Rightarrow \quad v_2(m^2) = v_2(2n^2)$

$\Rightarrow \quad 2\, v_2(m) = 1 + 2\, v_2(n)$

$\Rightarrow \quad 2 \mid 1$ which is a contradiction. ∎

Def. For a positive integer n and a prime p, let $v_p(n)$ be the power of p in the prime decomposition of n.

Exp. · $v_2(10) = 1$; $v_3(10) = 0$; $v_5(10) = 1$.

· $v_p(n) = 0$ if p is large enough depending on n.

Basic properties : • $n = \prod p^{v_p(n)}$.

• $v_p(n_1 n_2) = v_p(n_1) + v_p(n_2)$.