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 $\leq 40$, we need to cross out multiples of numbers $\leq 6$.

\[ \begin{array}{cccccccc}
2 & 3 & 5 & 7 & 11 & 13 & 17 & 19 \\
23 & 29 & 31 & 37 & 41 & 43 & 47 & 53 \\
\end{array} \]

\[ \pi(x) := \left\{ p \mid p \leq x; \ p \text{ prime} \right\} \]

\[ \lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1. \] (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 Fundamental theorem of Arithmetic)

Every integer \( \geq 1 \) can be uniquely written as

\[ p_1^{k_1} \cdots p_m^{k_m} , \]

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 its divisors and compute the value of many arithmetic functions (called multiplicative functions) e.g.

\[ d(n) := \text{number of its positive divisors}, \]

\[ \sigma(n) := \text{sum of its positive divisors}, \]

\[ \mu(n) := \text{the Möbius function}, \]

\[ \varphi(n) := |\{ a \leq n, \gcd(a,n)=1 \}|. \]
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 forever to decompose \( pq \) into prime factors.

\textbf{Pf of FTA} It has two parts: existence and uniqueness.

For both parts, we proceed by contradiction and use the well-ordering principle.

\textbf{Existence}. Suppose this is NOT true, i.e.

\[ \Sigma_1 := \{ n \in \mathbb{Z}^+ \mid n \text{ cannot be written as product of primes} \} \]

is non-empty. So by the well-ordering principle \( \Sigma_1 \) 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 \( \Sigma_1 \) and

\[ \Sigma_1 := \{ n \in \mathbb{Z}^+ \mid n \text{ cannot be written as product of primes} \} \]
$1 < a, b < n_q, \quad a, b$ can be written as product of primes. Therefore $n_q = a \cdot b$ can be written as product of primes. This contradicts the fact that $n_q \in \Sigma_1$.

Uniqueness. Again suppose to the contrary that

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

is non-empty. So by the well-ordering principle, $\Sigma_2$ has a smallest element $n_2$. So

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

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.

$$p_1 \mid \text{LHS} = \text{RHS} \implies p_1 \mid q_i \quad \text{for some } i \implies p_1 = q_i \quad \text{Euclid's lemma}$$

$$q_1 \mid \text{RHS} = \text{LHS} \implies q_1 \mid p_j \quad \text{for some } j \implies q_1 = p_j$$
\[
p_1 = q_1 \geq q_2 = p_j \geq p_1 \implies p_1 = q_i.
\]

\[\implies \text{(Suppose } k_1 \leq l_1)\]

\[n' := p_2 \cdots p_m = p_1 \cdot q_2 \cdots q_s < n\]

If \(n' = 1\) \(\implies m = s = 1\), \(p_1 = q_1\) and \(k_1 = l_1\),

which means they are the same decomposition.

which is a contradiction.

\[n' > 1 \implies n' \text{ has a unique factorization into primes.} \implies \]

\[n \text{ smallest in } \Sigma_2\]

\[\cdot l_1 - k_1 = 0\]

\[\cdot m - 1 = s - 1\]

\[\cdot p_2 = q_2, p_3 = q_3, \ldots, p_m = q_m\]

\[\cdot k_2 = l_2, \ldots, k_m = l_m\]

\[\implies \text{the starting decompositions are the same,}\]

which is a contradiction.

\[\Box\]

Cor. (Euclid) There are infinitely many primes.

Pr. 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 $p_i | p_1 \cdots p_n + 1 \Rightarrow p_i | 1$ which is a contradiction. \hfill \blacksquare

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

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

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

**Proof (\iff)** This is clear: $n = \prod p_i^{k_i} = (\prod p_i^{k_i - l_i})(\prod p_i^{l_i})$. \hfill \in \mathbb{Z} \quad \text{\text{d}}$  

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

$$d = \prod p v_p(d) \quad \text{(notice that $v_p(d)$'s are zero except for finitely many prime $p$.)}$$  

$$d' = \prod p v_p(d')$$  

$\Rightarrow d d' = \prod p v_p(d) + v_p(d')$.

$\Rightarrow$ For any prime $p$, $v_p(n) = v_p(d) + v_p(d') \geq v_p(d)$.
\[ d = \prod p_i^{l_i} \quad \text{where} \quad l_i = v_{p_i}(d) \leq v_{p_i}(m) = k_i. \]  

**Cor.** \( d(\prod p_i^{k_i}) = \prod d_i \mid d_i \mid \prod p_i^{k_i} \mid d \leq d \left| \prod p_i^{k_i} \right| \)

\[ = \prod (k_i + 1). \]

**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 \( 0 \leq l_1 \leq k_1, 0 \leq l_2 \leq k_2, \ldots, 0 \leq l_m \leq k_m. \)

So for \( l_i \) we have \( k_i + 1 \) choices. \( \ldots \) 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. \( \frac{m}{n} = \sqrt{2} \).

\[ \Rightarrow m^2 = 2n^2 \]
\[ v_2(m^2) = v_2(2n^2) \]
\[ \Rightarrow 2v_2(m) = 1 + 2v_2(n) \]
\[ \Rightarrow 2 \mid 1 \text{ which is a contradiction.} \]

**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:**

\[ n = \prod p^{v_p(n)} \]

\[ v_p(n_1n_2) = v_p(n_1) + v_p(n_2) \]