LECTURE 25

(Wed. MAR. 11, 2020)

Def. An integer $p > 1$ is a *prime number* if it has no non-trivial factors.
I.e., if $p = ab$ with $a, b \in \mathbb{N}$, then $a = 1$ or $b = 1$.
["non-primes" $n > 1$ are called *composite* — they admit a factorization $n = ab$ with $1 < a, b < n$.]

- First few primes:

$2, 3, 5, 7, 11, 13, \ldots$

Thm. Every $n \in \mathbb{N}$ can be factored into primes (say n *has* a "prime factorization"):

$$n = p_1 p_2 \cdots p_r$$

the p_i are primes — possibly with repetitions.

Ex $n = 60 = 2 \cdot 2 \cdot 3 \cdot 5$

○ *Convention*: We allow the empty product ($r=0$) when $n=1$, and the one-factor product ($r=1$) when n is already prime.

PROOF (Thm.): Strong induction on n.

(1) *Base step* ($n=1$): Allow $r=0$ by convention.

(2) *Ind. step*: Let $n \in \mathbb{N}$ and suppose every $m < n$ admits a prime factorization.

<u>Show:</u> n has a prime factorization.

- If n is prime, we're done since $r=1$ allowed by convention.
- If n is composite, write $n=ab$ with $1<a,b<n$.

By <u>induction hypothesis</u> both a and b have prime factorizations — say:

$$a = p_1 p_2 \cdots p_r \quad \text{and} \quad b = q_1 q_2 \cdots q_s .$$

Therefore so does $n = ab = (p_1 \cdots p_r)(q_1 \cdots q_s)$. $\square$

★ <u>FACT</u>: Prime factorization is <u>unique</u> up to <u>reordering</u> the factors. ($60 = 2\cdot 2\cdot 3\cdot 5 = 3\cdot 2\cdot 5\cdot 2$ etc.)

— the key to proving this is the characteristic property that: (p = prime)

$$p \mid ab \Rightarrow p \mid a \vee p \mid b.$$

(we omit the proof)

This fails if p <u>not</u> prime.

<u>EX</u>: $6 \mid 2\cdot 3$ but $6 \nmid 2$ and $6 \nmid 3$.

<u>Thm</u>. (Euclid) There are <u>infinitely</u> many primes.

PROOF. Suppose, on the contrary, that $p_1, p_2, \dots, p_r$ is a complete (finite) list of <u>all</u> primes.

Trick: Consider the number $n = (p_1 p_2 \cdots p_r) + 1$.
— it has a prime factorization, so certainly some prime p divides n. That p also divides $p_1 p_2 \cdots p_r$ since $p = p_i$ for some i. But then p divides their difference:

$$n - (p_1 p_2 \cdots p_r) = 1.$$

$p \mid 1$ is a contradiction (the only divisors of 1 are ± 1, but $p > 1$). $\square$

Euclid's argument shows:

If we list the primes in increasing order,

$$\begin{array}{cccccc} p_1, & p_2, & p_3, & \ldots, & p_n, & \ldots \\ \parallel & \parallel & \parallel & & & \\ 2 & 3 & 5 & & & \end{array}$$

Then $p_{n+1} \leq (p_1 p_2 \cdots p_n) + 1$.

(Why? Some p divides $(p_1 p_2 \cdots p_n) + 1$. In particular

$$p \leq (p_1 p_2 \cdots p_n) + 1.$$

On the other hand p is not among $p_1, p_2, \ldots, p_n$ so it must be at least the next prime: $p_{n+1} \leq p$.)

Thm $p_n < 2^{2^n}$.

PROOF. Strong induction on n.

(1) $n=1$: $2 = p_1 < 2^2 = 4$ ok.

(2) Ind. step: Assume inequality holds for $p_1, p_2, \dots, p_n$.

(Let $n \in \mathbb{N}$) — Show: $p_{n+1} < 2^{2^{n+1}}$.

From above,

$$
\begin{aligned}
p_{n+1} &\leq (p_1 p_2 \cdots p_n) + 1 \\
&< \left(2^2 \cdot 2^4 \cdots 2^{2^n}\right) + 1 \quad \leftarrow \text{by ind. hypothesis.} \\
&= 2^s + 1, \text{ where } s = 2+4+8+\dots+2^n \\
&= \tfrac{1}{4} \cdot 2^{2^{n+1}} + 1. \\
&< 2^{2^{n+1}}
\end{aligned}
$$

$$
\begin{aligned}
s &= 2+4+8+\dots+2^n \\
&= 2(1+2+4+\dots+2^{n-1}) \\
&= 2(2^n - 1) = 2^{n+1} - 2.
\end{aligned}
$$

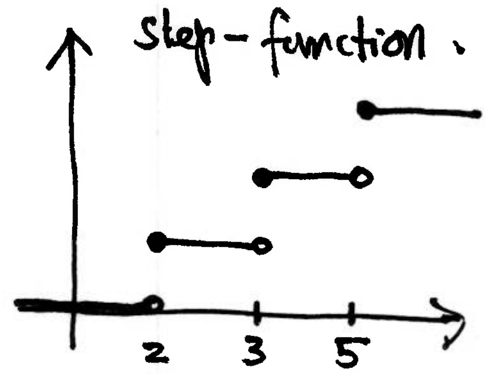
geometric sum formula ($x=2$).

just check that $\frac{1}{4}t + 1 < t \iff t > \frac{4}{3}$. $\square$

($t = 2^{2^{n+1}}$)

Reformulation: Prime — counting function

$$\pi(x) = \#\{\text{primes } p \leq x\}$$



By Euclid, $\pi(x)$ unbounded. Can do better:

Given $x \geq 4$ find the n s.t. $2^{2^n} \leq x < 2^{2^{n+1}}$.

Then:

$$\pi(x) \geq \pi(2^{2^n}) \geq \pi(p_n) = n.$$

previous Thm.

On the other hand,

$$\ln x < 2^{n+1} \cdot \ln 2, \qquad \ln\ln x < (n+1)\ln 2 + \ln\ln 2$$

$$= n\ln 2 + (\ln 2 + \ln\ln 2)$$

$$< n$$

check this ($\ln 2 \approx 0.69$)

Combined:

Corollary

$\pi(x) > \ln\ln x$.

— the true asymptotics:

THE Prime Number Thm: $\pi(x) \sim \dfrac{x}{\ln x}$

(meaning $\dfrac{\pi(x)}{x/\ln x} \to 1$ as $x \to \infty$)