Plan for today

- Chebyshev's theorem on the density of prime numbers.

LAST TIME: PROBABILISTIC PRIME TESTS
THIS TIME: DENSITY OF PRIMES
$\Rightarrow$ EFFICIENT PROBABILISTIC ALGORITHM TO OBTAIN A PRIME

Notation, statements and some history

- $\mathbb{P} := \{p \in \mathbb{N} : p \text{ is prime}\}$.
- For $x \in \mathbb{R}_+$, $\pi(x) := |\{p \in \mathbb{P} \,:\, p \le x\}|$.

Theorem (Prime Number Theorem)

$\pi(x) \sim \frac{x}{\ln x} \iff \lim_{x \to +\infty} \frac{\pi(x)}{x/\ln x} = 1$

(CONJECTURED BY GAUß, LEGENDRE ≈ 1800
PROVED BY HADAMARD, DE LA VALLÉE POUSSIN 1896)

Theorem (Chebyshev's Theorem) (≈ 1850)

$\pi(x) = \vartheta(\frac{x}{\ln x}) \iff \exists\, c_1, c_2 \in \mathbb{R}_+, \exists\, \bar{x} \in \mathbb{R}_+ :\ c_1 \frac{x}{\ln x} \le \pi(x) \le c_2 \frac{x}{\ln x}$ $\forall\, x \ge \bar{x}$

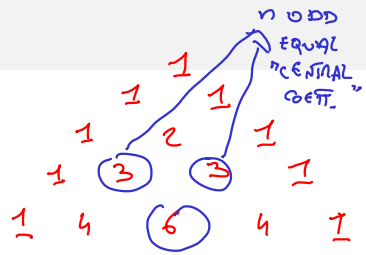
we prove this

A basic fact on binomial coefficients

Fact

For each $m \in \mathbb{N}$, one has $\frac{2^{2m}}{2m} \le \binom{2m}{m} \le \binom{2m+1}{m} \le 2^{2m}$. (1) ✓ (2)

$n = 0$
$= 1$
$= 2$
$= 3$
$= 4$



$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

↳ i-TH COEFFICIENT OF THE n-TH ROW OF THE PASCAL TRIANGLE

↳ n EVEN, UNIQUE BIGGEST "CENTRAL" COEFFICIENT

(1)

$$2^{2m} = (1+1)^{2m} = \sum_{i=0}^{2m} \binom{2m}{i} = 1+1 + \sum_{i=1}^{2m-1} \binom{2m}{i} \le 2 + \binom{2m}{m}(2m-1) \le 2m\binom{2m}{m}$$

$$\Rightarrow \frac{2^{2m}}{2m} \le \binom{2m}{m}$$ ✓

(2)

$$2^{2m+1} \ge \sum_{i=0}^{2m+1} \binom{2m+1}{i} \ge \binom{2m+1}{m} + \binom{2m+1}{m+1} = 2\binom{2m+1}{m}$$ ✓ □

The p-adic order of an integer

Definition

Given $p \in \mathbb{P}$ and $n \in \mathbb{N}$, we let $\mathrm{ord}_p(n)$ to be the biggest k such that $p^k \mid n$.

$\mathrm{ord}_2(18) = 1$ $\quad 18 = 3 \cdot 3 \cdot 2$ $\qquad \mathrm{ord}_3(54) = 3$ $\quad 54 = 3 \cdot 3 \cdot 2 \cdot 3$

Fact

For $p \in \mathbb{P}$ and $n \in \mathbb{N}$, one has $\mathrm{ord}_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.

$a, b \in \mathbb{N}$, $p \in \mathbb{P}$ $\quad \mathrm{ord}_p(a \cdot b) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b) \Rightarrow \mathrm{ord}_p(n!) = \sum_{i=1}^{n} \mathrm{ord}_p(i)$

$p^k \cdot \blacksquare \qquad p^c \cdot \bullet$

$a/b \in \mathbb{N}$ $\quad \mathrm{ord}_p(a/b) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$. Let $t_{p,i} = \begin{cases} 1 & \text{if } p^p \mid i \\ 0 & \text{oth.} \end{cases}$.

$p^k \mid i \iff p^{k-1} \mid i, p^{k-2} \mid i, \ldots, p^1 \mid i$ $\quad p^{k+1} \nmid i$

$t_{k,i} = 1, t_{k-1,i} = 1, \ldots, t_{1,i} = 1$ AND OTHERS ARE 0

$\Rightarrow \sum_{p \geq 1} t_{p,i} = \mathrm{ord}_p(i)$

CONTINUES...

$$\boxed{\operatorname{ord}_p(i)} = \sum_{\ell \geq 1} t_{\ell i}$$

BOTH SUMMATIONS ARE FINITE

$$(*) = \operatorname{ord}_p(n!) = \sum_{i=1}^{n} \operatorname{ord}_p(i) = \sum_{i=1}^{n} \sum_{\ell \geq 1} t_{\ell i} = \sum_{\ell \geq 1} \boxed{\sum_{i=1}^{n} t_{\ell i}}$$

$$\sum_{i=1}^{n} t_{\ell i} = \left[\#\text{ OF MULTIPLES OF } p^{\ell} \text{ THAT ARE} \leq n \right] = \left\lfloor \frac{n}{p^{\ell}} \right\rfloor \quad \Rightarrow (*) = \sum_{\ell \geq 1} \left\lfloor \frac{n}{p^{\ell}} \right\rfloor \quad \square$$

$i = 1, 2, 3, \ldots, p^{\ell}, \ldots, 2p^{\ell}, \ldots, 3p^{\ell}, \ldots \left\lfloor \frac{n}{p^{\ell}} \right\rfloor \ldots n$

$t_{\ell i} = 0\ 0\ 0 \ldots 0, \underset{1}{1}, 0 \ldots, 0, 1, 0 \ldots 1, 0 \ldots$

$\pi(\text{🐰}) = \Omega(\frac{n}{\ln n})$

Fact

For each $n \in \mathbb{N}$, one has $\pi(n) \geq (\frac{1}{2}\ln 2) \cdot \frac{n}{\ln n}$.

PF. FIRST WE PROVE IT FOR n EVEN $\Rightarrow n = 2m$, $m \in \mathbb{N}$ $\quad N := \binom{2m}{m} = \frac{(2m)!}{(m!)(m!)}$

FOR $p \in \mathbb{P}$, $\operatorname{ord}_p(N) = \operatorname{ord}_p\left(\frac{(2m)!}{(m!)(m!)}\right) = \operatorname{ord}_p((2m)!) - \operatorname{ord}_p((m!)(m!))$ (seen in the previous slides)

(also from previous slides) $= \operatorname{ord}_p((2m)!) - 2\operatorname{ord}_p(m!) = \sum_{k \geq 1} \left\lfloor \frac{2m}{p^k} \right\rfloor - 2\left\lfloor \frac{m}{p^k} \right\rfloor \leq \frac{\ln(2m)}{\ln(p)}$ (*)

- ALL SUMMANDS $> K$ ARE 0
- ALL OTHERS ARE 0 OR 1

$\left\lfloor \frac{2m}{p^k} \right\rfloor = 0$ IF $p^k > 2m \Leftrightarrow k \ln p > \ln(2m) \Leftrightarrow k > \frac{\ln(2m)}{\ln(p)}$

$\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0, 1\} \Rightarrow (*) \in \{0, 2\}$

(TWICE THE FRACTIONAL PART OF A NUMBER IS < 2)

JUST PROVE: $\operatorname{ord}_p(N) \le \frac{\ln(2m)}{\ln(p)}$

CONTINUES...

n EVEN, $n = 2m$

$$N = \binom{2m}{m} = \frac{2m!}{(m!)(m!)}$$

$$\pi(2m)\,\ln(2m) = \sum_{\substack{p \in \mathbb{P} \\ p \le 2m}} \ln(2m) = \sum_{\substack{p \in \mathbb{P} \\ p \le 2m}} \frac{\ln(2m)}{\ln(p)} \cdot \ln(p) \ge \sum_{\substack{p \in \mathbb{P} \\ p \le 2m}} \operatorname{ord}_p(N) \cdot \ln(p)$$

$\ge$ TO SHOW

$\ln N$

$$N = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_K^{e_K}$$

ALL PRIMES DIVIDING N ARE $\le 2m$

$$\sum_{\substack{p \in \mathbb{P} \\ p \le 2m}} \operatorname{ord}_p(N) \cdot \ln(p) = \sum_{i=1}^{K} e_i \ln(p_i) = \sum_{i=1}^{K} \ln\left(p_i^{e_i}\right) = \ln\left(\prod_{i=1}^{K} p_i^{e_i}\right) = \ln N$$

CONTINUES (2)

$$\pi(2m)\ln(2m) \geq \ln(N)$$

$$N = \binom{2m}{m} \geq \frac{2^{2m}}{2m} \geq 2^m \Rightarrow \ln(N) \geq m \cdot \ln(2)$$

$$\Rightarrow \pi(2m)\ln(2m) \geq m\ln(2) \Rightarrow \pi(2m) \geq \left(\frac{1}{2}\ln 2\right)\frac{2m}{\ln(2m)} \Rightarrow \pi(n) \geq (\dots)\frac{n}{\ln(n)}$$ ✓

$\frac{x}{\ln x}$ INCREASING FOR $x \geq 3$

n ODD: $\pi(n) = \pi(n+1) \geq \left(\frac{1}{2}\ln 2\right)\frac{n+1}{\ln(n+1)} \geq \left(\frac{1}{2}\ln 2\right)\frac{n}{\ln n}$ □

↑ NO EVEN NUMBER >2 IS PRIME

EASY EXERCISE:

EXTEND TO ALL $x \in \mathbb{R}_+$ THAT $\exists\, c, \bar{x} \in \mathbb{R}_+ : \pi(x) \geq c\frac{x}{\ln x} \quad \forall x \geq \bar{x}$

More basics

Fact

For all $x \in \mathbb{R}_+$, one has

$$(*) = \prod_{p \le x,\, p \in \mathbb{P}} p < 4^x.$$

PF.

WLOG $x \in \mathbb{N}$: $\prod_{p \le x,\, p \in \mathbb{P}} p = \prod_{p \le \lfloor x \rfloor,\, p \in \mathbb{P}} p \overset{<1}{\le} 4^{\lfloor x \rfloor} \le 4^x$ ✓

INDUCTION ON $x \in \mathbb{N}$

$x = 1$ $(*) = 1 < 4^1$ ✓ $\quad x = 2$ $(*) = 2 < 4^2$ ✓

EVEN $x \ge 4$ $\prod_{p \le x,\, p \in \mathbb{P}} p = \prod_{p \le x-1,\, p \in \mathbb{P}} p \overset{(\text{IND.})}{<} 4^{x-1} < 4^x$ ✓

ODD $x \ge 3$ $x = 2m+1$

$$\prod_{p \le x,\, p \in \mathbb{P}} p = \underbrace{\prod_{p \le m+1,\, p \in \mathbb{P}} p}_{A} \cdot \underbrace{\prod_{m+2 \le p \le 2m+1,\, p \in \mathbb{P}} p}_{B}$$

More basics

Fact

For all $x \in \mathbb{R}_+$, one has

$$\prod_{p \le x,\, p \in \mathbb{P}} p < 4^x.$$

$$\prod_{\substack{p \le x \\ p \in \mathbb{P}}} p = \prod_{\substack{p \le m+1 \\ p \in \mathbb{P}}} p \cdot \prod_{\substack{m+2 \le p \le 2m+1 \\ p \in \mathbb{P}}} p < 4^{m+1} \cdot 4^{m} = 4^{2m+1} = 4^{x}$$

A

B

$$B \mid \binom{2m+1}{m} = \frac{(2m+1)!}{(m!)(m+1)!}$$

NO PRIME $\ge m+2$ CAN BE IN THE DENOMINATOR, AND ALL OF THEM ARE IN THE NUMERATOR

(A) $< 4^{m+1}$

INDUCTION

$$\Rightarrow B \le \binom{2m+1}{m} \le 2^{2m}$$

$\pi(n) = O(\frac{n}{\ln n}) \equiv \exists\, c \in \mathbb{R}_+, \bar{x} \in \mathbb{N} : \pi(x) \le c \cdot \frac{x}{\ln x} \quad \forall x \ge \bar{x}$

PF: Let $x \in \mathbb{R}_+$

$2^{2x} = 4^x > \prod_{\substack{p \le x \\ p \in \mathbb{P}}} p \ge \prod_{\substack{\sqrt{x} \le p \le x \\ p \in \mathbb{P}}} p \ge \prod_{\substack{\sqrt{x} \le p \le x \\ p \in \mathbb{P}}} \sqrt{x} = \sqrt{x}^{\pi(x) - \pi(\sqrt{x})}$

$\longrightarrow \frac{1}{2}\ln(x)$

TAKING THE $\ln$: $2x \ln 2 \ge (\pi(x) - \pi(\sqrt{x}))\, \ln(\sqrt{x})$

$\pi(x) \le (4 \ln 2)\frac{x}{\ln x} + \pi(\sqrt{x})$ — we need to upper bound this!

$\pi(\sqrt{x}) \le \sqrt{x}$

$\pi(x) \ge c \frac{x}{\ln x}$

For some $c \in \mathbb{R}_+$, $x > 0$, $x \ge \bar{x} \in \mathbb{R}_+$

$\frac{\pi(\sqrt{x})}{\pi(x)} \le c' \frac{\sqrt{x}}{x/\ln(x)} = c' \frac{\ln(x)}{\sqrt{x}} \xrightarrow{x \to +\infty} 0 \equiv \forall c'' \in \mathbb{R}_+ \; \exists \bar{x} : \pi(\sqrt{x}) \le c'' \cdot \pi(x) \; \forall x \ge \bar{x}$

CONTINUES ...

$\Rightarrow$ FOR x BIG ENOUGH $\quad \pi(\sqrt{x}) \leq \frac{1}{2}\pi(x)$

$\pi(x) \leq K\frac{x}{\ln x} + \pi(\sqrt{x}) \leq K\frac{x}{\ln x} + \frac{1}{2}\pi(x)$ FOR SOME $K \in \mathbb{R}_+$

$\Rightarrow \frac{1}{2}\pi(x) \leq K\frac{x}{\ln x} \Rightarrow \pi(x) \leq 2K\frac{x}{\ln x}$ $\forall x$ BIG ENOUGH

$\square$

NEW CONSTANT