Distribution of primes

① Gaps between primes can be arbitrarily large

$$(n+1)!+2,\ (n+1)!+3,\ \dots,\ (n+1)!+(n+1)$$

are all not prime

② Gaps between primes cannot be arbitrarily large

Bertrand's Postulate: There's always a prime between n and $2n$.

Ex The first prime gap ≥ 20 occurs after the prime 1129.
There's a prime $\leq 2 \cdot 1129 = 2258$ (e.g. 1151)

The Prime Number Theorem

For real $x > 0$ we define the prime counting function

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

Ex $\pi(2) = 1$, $\pi(3) = 2$, $\pi(\pi) = \pi(3,141\dots) = \pi(3) = 3$.

Theorem (PNT; Hadard / de la Vallée Poussin 1896)
we have

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log(x)} = 1$$

$\left(\pi(x) - \frac{x}{\log(x)} \text{ does not go to } 0!\right)$

$\left(\pi(x) = \frac{x}{\log(x)} + R(x)\right)$

We want to prove the elementary estimates

$$\frac{2}{3}\frac{x}{\log(x)} \leq \pi(x) \leq 2\frac{x}{\log(x)} \qquad (x \geq 3)$$

Start with the lower bound:

Lemma For all $n, k \in \mathbb{N}$, $k \leq n$ we have

$$\binom{n}{k} \leq n^{\pi(n)}$$

Proof First show

$$v_p\left(\binom{n}{k}\right) \leq \frac{\log(n)}{\log(p)} \quad \checkmark$$

Indeed, by Legendre's Theorem, we have

$$v_p\left(\binom{n}{k}\right) = v_p\left(\frac{n!}{k!(n-k)!}\right) = v_p(n!) - v_p(k!) - v_p((n-k)!)$$

Legendre $$\sum_{j=1}^{\infty}\left(\left\lfloor \frac{n}{p^j}\right\rfloor - \left\lfloor \frac{k}{p^j}\right\rfloor - \left\lfloor \frac{n-k}{p^j}\right\rfloor\right)$$

$\to 0$ for $p^j > n \iff j > \frac{\log(n)}{\log(p)}$

$\to$ all terms for $j \leq \frac{\log(n)}{\log(p)}$ are either 0 or 1

$$\leq \frac{\log(n)}{\log(p)}$$

Exponentiate e^x:

$$p^{v_p\left(\binom{n}{k}\right)} \leq n$$

Now

$$\binom{n}{k} = \prod_{p \leq n} p^{v_p\left(\binom{n}{k}\right)} \leq \prod_{p \leq n} n = n^{\pi(n)}. \quad \blacksquare$$

Prop For $n \in \mathbb{N}$ with $n \geq 2$ we have

$$\pi(n) > \frac{2}{3}\frac{n}{\log(n)}$$

$\binom{n}{0} = \binom{n}{n} = 1$

Proof $$2^n = (1+1)^n = \sum_{k=0}^{n}\binom{n}{k} \leq 1 + (n-1)n^{\pi(n)} + 1 < n^{\pi(n)+1}$$

($2 < n^{\pi(n)}$ if $n \geq 2$)

Take logarithms:

$$\pi(n) > n\frac{\log(2)}{\log(n)} - 1$$

For $n > 200$ we have

$$\log(2)\frac{n}{\log(n)} - 1 \geq \frac{2}{3}\frac{n}{\log(n)}$$

and for $n \leq 200$ $\pi(n) > \frac{2}{3}\frac{n}{\log(n)}$ can be checked directly. ▨

For the upper bound:

Lemma For $n \in \mathbb{N}$, $n \geq 2$, we have

$$\underbrace{\pi(2n) - \pi(n)}_{\text{number of primes } n < p \leq 2n} < \log(4)\frac{n}{\log(n)}$$

Proof ① $\prod_{n < p \leq 2n} p \leq \binom{2n}{n}$ $\left(\binom{2n}{n} = \frac{(2n)!}{n!n!}\right.$, these primes appear in $(2n)!$ but not in $n!$ $\left.\right)$

② $\binom{2n}{n} \leq 4^n$ $\left(4^n = 2^{2n} = (1+1)^{2n} = \sum_{k=0}^{2n}\binom{2n}{k}\right)$

$$\Rightarrow n^{\pi(2n)-\pi(n)} = \underbrace{n \cdot n \cdot n \cdot \ldots \cdot n}_{\text{one factor for each } n < p \leq 2n}$$

$$\leq \prod_{n < p \leq 2n} p \overset{①}{\leq} \binom{2n}{n} \overset{②}{\leq} 4^n$$

Taking logarithms gives the result. ▨

Prop For $n \geq 2$,

$$\pi(n) < 2\frac{n}{\log(n)}$$

Proof By induction. Check it for $n \leq 256 = 2^8$.

Assume that it's true for all $k < n$ for some $n \geq 256$.

(1) $n = 2m$ even:

$$\pi(n) = \pi(2m) - \pi(m) + \pi(m)$$

Lemma
$$\leq \pi(m) + \log(4)\frac{m}{\log(m)}$$

IH
$$\leq 2\frac{m}{\log(m)} + \frac{\log(4)}{2\log(2)}\frac{m}{\log(m)}$$

$$= \frac{n}{\log(n)-\log(2)} + \log(2)\frac{n}{\log(n)-\log(2)}$$

For $n \geq 2^8$ we have

$$\frac{1}{\log(n)-\log(2)} \leq \frac{8}{7}\frac{1}{\log(n)}, \quad \text{and} \quad (1+\log(2))\frac{8}{7} < 2.$$

$$\Rightarrow \pi(n) \leq (1+\log(2))\frac{8}{7}\frac{n}{\log(n)} < 2\frac{n}{\log(n)} \quad \checkmark$$

(2) $n = 2m+1$ similar ✓ ▨

Twin Prime Conjecture

Twin primes: $(3,5), (11,13), \ldots (101, 103)$

Conjecture There are infinitely many twin primes.

Known results:

① Yitang Zhang 2013: Infinitely many primes with gap ≤ 70 million

② Terence Tao, James Maynard brought this down to 246
(Fields medal)

Goldbach's conjecture

Conjecture (Strong form) Every even number >2 can be written as a sum of 2 primes

Olivier Ramaré 1995: ≤ 6 primes are enough

Conjecture (weak form) Every odd number >5 can be written as a sum of three primes.

Strong $\Rightarrow$ weak, $n-3 = p+q \Rightarrow n = p+q+3$

T. Tao (2013): ≤ 5 primes is enough
Harald Helfgott (2013): full proof.