$\boxed{L\,10}$ $\boxed{\text{Thm. (P. L. Čebyšev) } \doteq 1850}$ $\exists c_1 > c_2 > 0\ \forall x \geq 2$: (1)

Dec 7, 2020

$$\frac{c_2 x}{\log x} < \underbrace{\pi(x)}_{|\{p \in \mathbb{N} \mid p \text{ is a prime and } p \leq x\}|} < \frac{c_1 x}{\log x}.$$

<u>Proof.</u> $n \in \mathbb{N}$, then a) $\underline{\dfrac{4^n}{2n+1} \overset{①}{\leq} \dbinom{2n}{n} \overset{②}{\leq} 4^n}$. This follows from the binomial expansion $4^n = 2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i}$ and the inequalities $\binom{2n}{i} \geq 0$ and $\binom{2n}{i} \leq \binom{2n}{n}$. Also, b) $\underline{\prod_{n < p \leq 2n} p \overset{①'}{\leq} \dbinom{2n}{n} \overset{②'}{\leq} (2n)^{\pi(2n)}}$.

The first $\leq$ follows from the fact that $\binom{2n}{n} = \frac{(2n)!}{n!\,n!}$, so in fact $\left(\prod_{n<p\leq 2n} p\right) \mid \binom{2n}{n}$. The second $\leq$ was proven in the previous lecture (the 2nd proof of P. Erdős): if $\binom{2n}{n} = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ then $p_i \leq 2n$ and even $p_i^{a_i} \leq 2n$. Combining $\overset{①}{\leq}$ and $\overset{②'}{\leq}$ (which we did already in ) we get $\frac{4^n}{2n+1} \leq (2n)^{\pi(2n)}$, thus $\forall n \in \mathbb{N}$: $\underline{\pi(2n) \geq \frac{2n \log 2}{\log(2n)} - \frac{\log(2n+1)}{\log(2n)}}$

$\underline{> (\log 2)\,\frac{2n}{\log(2n)} - 2.}$ $\boxed{\text{Exercise for you:}}$ deduce from this that indeed for some $c_2 > 0$ and every real $x \geq 2$, $\pi(x) > \frac{c_2 x}{\log x}$

Combining 1 and 2 we get that $\forall n\in\mathbb{N}$:

$\prod_{n<p\le 2n} p \le 4^n \rightsquigarrow \sum_{n<p\le 2n}\log p \le n\log 4$. For real $x\geq 2$ we take (unique) $q\in\mathbb{N}$ s.t. $2^q \le x \le 2^{q+1}$. Then $\sum_{p\le x}\log p \le$

$$\le \sum_{j=0}^{q}\sum_{2^j<p\le 2^{j+1}}\log p \le \sum_{j=0}^{q} 2^j\log 4 = (2^{q+1}-1)\log 4 < 2\cdot 2^q\log 4 \le (2\log 4)x.$$

$\boxed{\text{So } \forall x\geq 2: \sum_{p\le x}\log p < (2\log 4)\,x.}$

$x\geq 2$:

$$\rightsquigarrow (2\log 4)x > (-\shortparallel-) \geq \sum_{\sqrt{x}<p\le x}\log p \geq \Big(\pi(x)-\underbrace{\pi(\sqrt{x})}_{0\le\ \ \le\sqrt{x}}\Big)\log(\sqrt{x})$$

$$\rightsquigarrow \pi(x)\le \frac{(2\log 4)\,x}{\log(\sqrt{x})}+\sqrt{x} = \frac{(4\log 4)\,x}{\log x}+\underbrace{\sqrt{x}}_{\lll \frac{x}{\log x}}.$$

$\boxed{\text{Exercise for you:}}$ deduce from this that indeed for some $c_1>0$ and every real $x\geq 2$:

$$\pi(x)<\frac{c_2\,x}{\log x}$$

☒

I mention some further classical results from the theory of prime numbers, without proofs (almost).

$\boxed{\text{PNT - The Prime Number Theorem (1896, J. Hadamard; de la Vallée-Poussin)}}$ For real $x\to+\infty$,

$$\pi(x)\sim\frac{x}{\log x}, \text{ i.e. } \pi(x)=(1+o(1))\frac{x}{\log x}.$$

• Jacques Hadamard (1865–1963),

• Charles J. de la Vallée Poussin (1866–1962)

$Li(x) := \int_2^x \frac{dt}{\log t}$. Then, more precisely than above, $\pi(x) = \underbrace{Li(x)}_{\sim \frac{x}{\log x}} + O\left(x e^{-\frac{A(\log x)^{3/5}}{(\log\log x)^{1/5}}}\right)$, where

$A = 0.2098$ (K. Ford, 2002)

• Kevin Ford (1967), | the Riemann Hypothesis

$\boxed{(RH)}$: $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} : \mathbb{C} \setminus \{1\} \to \mathbb{C}$, $\zeta(s) = 0$ with $Re(s) > 0 \Rightarrow Re(s) = \frac{1}{2}$. Explicit formula for $\pi(x)$:

H. von Koch (1901): $RH \Rightarrow \pi(x) = Li(x) + O(\sqrt{x}\log x)$

---

three formulas of • Franz Mertens (1840–1927) ($x \to +\infty$) ($\doteq 1874$)

(1) $\sum_{p \le x} \frac{\log p}{p} = \log x + O(1)$. Proofs: see my LNA.

(2) $\sum_{p \le x} \frac{1}{p} = \log(\log x) + c + O(1/\log x)$, where $c$ is a constant.

(3) $\prod_{p \le x} \left(1 - \frac{1}{p}\right) = \frac{d}{\log x}\left(1 + O(1/\log x)\right)$, where $d > 0$ is a constant.

(4)

For $\mathbb{N} \ni n = p_1^{a_1} \cdots p_k^{a_k}$ we define $\omega(n) := k$, $\Omega(n) := a_1 + a_2 + \cdots + a_k$, $\tau(n) = (1+a_1)(1+a_2)\cdots(1+a_k)$ (# of divisors of $n$). For real $x \geq 2$,

- $$\sum_{n \leq x} \omega(n) = x \cdot \log(\log x) + c_1 x + O(x/\log x)$$
- $$\sum_{n \leq x} \Omega(n) = x \cdot \log(\log x) + c_2 x + O(x/\log x)$$ where $c_i$, $i = 1, 2$, are constants.

Almost everywhere in $\mathbb{N}$ holds $(\log n)^{\log 2 - \varepsilon} < \tau(n) < (\log n)^{\log 2 + \varepsilon}$.
× the divisor pr.

$\boxed{\text{theorem (Hardy–Ramanujan, 1917)}}$

$\forall \varepsilon > 0 \; \exists x_0 = x_0(\varepsilon) > 0$ s.t.

$$x > x_0 \Rightarrow \#\{n \leq x \mid |\omega(n) - \log(\log x)| < \varepsilon \log(\log x)\} > (1-\varepsilon)x.$$

$\boxed{\text{• the multiplic. table result. LNs}}$ ⟸

or $\log(\log n)$, does not matter.

~~Also~~ holds ~~for~~ with $\Omega(n)$ too.

- Godfrey H. Hardy (1877–1947)
- Srinivasa Ramanujan (1887–1920)

• Zhang's theorem !

Proof (see my LNs) by the 2nd moment method by • Paul Turán (1910–1976) (Pál) | • or in Alon–Spencer, The Probab. Method

# $\boxed{\text{Chapter 5 — Congruences}}$ (theory of quadratic residues)

$a \not\equiv 0\ (p)$

$a \in \mathbb{Z}$, $p \in \mathbb{P}$: $a$ is a <u>(quadratic) residue mod $p$</u> if $x^2 \equiv a \pmod p$ has a solution $x \in \mathbb{Z}$. Else $a$ is a <u>(quadratic) non-residue mod $p$</u>. For example, for $p = 11$ the residues (q.r.) are $1, 4, 9, 5, 3$. The rest — $2, 6, 7, 8, 10$ — are q. non-residues. For $p = 2$, $1$ is a q.r. and there is no q. non-residue.

$\boxed{\text{Proposition}}$ For any prime $p > 2$, the # of q.r. mod $p$ = the # of q. non-r. mod $p$ $= \frac{p-1}{2}$.

$\boxed{\text{Proof.}}$ $\mathbb{Z}_p^\times := \mathbb{Z}_p \setminus \{0\}$. The map $\mathbb{Z}_p^\times \ni x \mapsto x^2 \in \mathbb{Z}_p^\times$ is two-to-one: $x^2 \equiv y^2 \pmod p \Leftrightarrow (x-y)(x+y) \equiv 0 \pmod p$ $\Leftrightarrow x \equiv \pm y$ and $x \not\equiv -x \pmod p$ as $p > 2$. $\boxtimes$

---

Standard notation: $a \in \mathbb{Z}$, $p > 2$ a prime

- <u>Legendre's symbol</u>: $\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{.. } a \text{ is q.r. mod } p \\ -1 & \text{.. '' q. non-r. mod } p \\ 0 & \text{.. p\mid a.} \end{cases}$

<u>Trivially</u>: $a \equiv b\ (p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right), \quad (b \not\equiv 0 \bmod p).$$

**Proposition** (Euler's criterion) $\forall a \in \mathbb{Z}\ \forall p > 2$:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

**Proof.** Recall the little theorem of Fermat: $a \not\equiv 0 \Rightarrow a^{p-1} \equiv 1$. So $(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) \equiv 0$ and $a^{\frac{p-1}{2}} \equiv \pm 1$. If $a \equiv 0$ then $0 \equiv 0\ (p)$ ✓. If $a \not\equiv 0$ and is a q.r. then $b^2 \equiv a\ (p)$, so $a^{\frac{p-1}{2}} = (b^2)^{\frac{p-1}{2}} = b^{p-1} \equiv 1$ (by FLT).
It remains to prove that if $a$ is a q. non-r., $\left(\frac{a}{p}\right)$ ✓. then $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. This follows from a theorem in algebra that $\forall f(x) \in F[x]$, $f \neq 0$ and $F$ is a field, $\#\{a \in F \mid f(a) = 0_F\} \leq \deg(f)$. In our case

$$f(x) = x^{\frac{p-1}{2}} - 1 \text{ and } F = \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z},$$

$x^{\frac{p-1}{2}} - 1 = 0$ has $\frac{p-1}{2}$ solutions in $\mathbb{Z}_p$ (namely the q. r. (see ? and the previous Prop.) $\Rightarrow x^{\frac{p-1}{2}} = -1$ if $x$ is a q. non-r. $\boxtimes$

**Proposition** $\forall a, b \in \mathbb{Z}\ \forall p > 2$: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

P. $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, hence ✓. $\boxtimes$