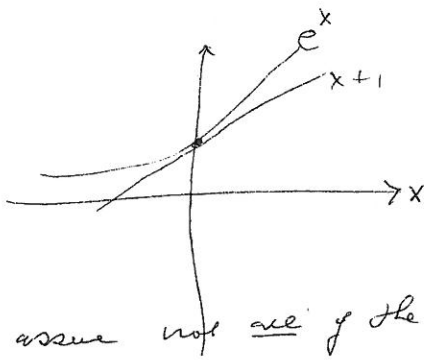
## 1.10 Basic inequalities

**Prop 1.16** (Arithmetic Geometric Mean Inequality)

If $x_1, \dots x_r$ are positive ($x_i > 0$) then

$$G := (x_1 \dots x_r)^{\frac{1}{r}} \leq \frac{x_1 + \dots + x_r}{r} =: A$$

with equality $\Leftrightarrow$ $x_1 = x_2 = \dots = x_r$.




**Proof** $\forall x \in \mathbb{R}$, $1 + x \leq e^x$

and $1 + x = e^x \Leftrightarrow x = 0$.

If $x_1 = \dots = x_r$, $G = x_1 = A$, so assume not all of the $x_i$ are the same.

Set $x = \frac{x_i}{A} - 1$ so $e^{\frac{x_i}{A} - 1} \geq \frac{x_i}{A}$ for $1 \leq i \leq r$.

At least one $x_i > A$ so $\frac{x_i}{A} - 1 > 0 \Rightarrow e^{x_i/A - 1} > \frac{x_i}{A}$ for that $i$ $\Rightarrow$

$$\prod_{i=1}^{r} e^{\frac{x_i}{A} - 1} > \prod_{i=1}^{r} \frac{x_i}{A} \Rightarrow e^{\frac{\sum x_i}{A} - r} > \prod_{i=1}^{r} x_i / A^r \Rightarrow e^0 > \frac{G^r}{A^r}$$

$\Rightarrow A > G$. //

**Theorem 17 (Euler Summation)** *If $f$ has a continuous derivative $f'$ on $[y,x] \in \mathbb{R}$ where $0 < y < x$, then*

$|t - \lfloor t \rfloor| \leq 1$

$$S = \sum_{y<n\leqslant x} f(n) = \int_y^x f(t)\,dt + \int_y^x (t - \lfloor t \rfloor) f'(t)\,dt + f(x)(\lfloor x \rfloor - x) - f(y)(\lfloor y \rfloor - y) \tag{3}$$

*Proof.* Let $m = \lfloor y \rfloor$, $k = \lfloor x \rfloor$. If $n, n-1 \in [y,x]$:

$$\begin{aligned}
\int_{n-1}^{n} \lfloor t \rfloor f'(t)\,dt &= \int_{n-1}^{n} (n-1) f'(t)\,dt \\
&= (n-1)(f(n) - f(n-1)) \\
&= \{nf(n) - (n-1)f(n-1)\} - f(n)
\end{aligned}$$

Summing from $n = m+2$ to $n = k$, the sum in braces ($\{\cdots\}$) telescopes to give

$$\begin{aligned}
\int_{m+1}^{k} \lfloor t \rfloor f'(t)\,dt &= kf(k) - (m+1)f(m+1) - \sum_{n=m+2}^{k} f(n) \\
&= kf(k) - mf(m+1) - \sum_{y<n\leqslant x} f(n) = S.
\end{aligned}$$

$f(m+1)$

Hence

$$\begin{aligned}
S &= -\int_{m+1}^{k} \lfloor t \rfloor f'(t)\,dt + kf(k) - mf(m+1) \\
&= -\int_{y}^{x} \lfloor t \rfloor f'(t)\,dt + kf(x) - mf(y).
\end{aligned} \tag{4}$$

Integrating $\int_y^x f(t)\,dt$ (by parts) gives

$$\int_y^x f(t)\,dt = xf(x) - yf(y) - \int_y^x tf'(t)dt. \tag{5}$$

Then (4) − (5) $\Rightarrow$ (3). $\square$

# Prime Numbers

## §2.1 Formulas for primes – recall

## §2.2. $\exists\ \infty$ many primes, $|\mathbb{P}| = \infty$.

$\{2<3<5<7<11<\dots\}$

**Theorem 2.1.** (Euclid) Suppose $\exists$ a finite number of primes $\{p_1<p_2<\dots<p_n\}$ (??)

and consider $N := p_1 \dots p_n + 1$. Then $N > p_n$ so $N$ is not prime.

Thus $N$ is composite so must be divisible by a prime, $p_j$ say, where $1 \le j \le n$.

Hence $p_j \mid N - p_1 \dots p_n \Rightarrow p_j \mid 1$ (!!). Hence $|\mathbb{P}| = \infty$. //

## §2.3. The prime counting function $\pi(x)$

Let $\pi(x) = |\{n \le x;\ n \in \mathbb{P}\}| = \sum_{\substack{n \le x \\ n \in \mathbb{P}}} 1$.

How big is $\pi(x)$? How does it go with $x$? Find a nice (approx) formula for $\pi(x)$? Find a nice (approx.) formula for $p_n$ the $n^{th}$ prime. $p_1 = 2$, $p_2 = 3$, ..

**Claim** $p_k \le 2^{2^{k-1}}$, $k = 1, 2, \dots$ (*) Proof by induction.

$k = 1$: $2 = p_1$ $\quad 2^{2^{1-1}} = 2^1 = 2$ & $2 \le 2$ ✓

so let $k \ge 1$ and assume (*) is true for $j = 1, \dots, k$.

By Thm 2.1 $\quad p_{k+1} \le p_1 \dots p_k + 1 \le 2^{2^0 + 2^1 + \dots + 2^{k-1}} + 1 = 2^{2^k - 1} + 1 < 2^{2^k}$

$(\le 2 \cdot 2^{2^k - 1})$

$\therefore$ (*) is true $\forall n \in \mathbb{N}$

**Claim** $\forall x \ge 2$ $\quad \boxed{\log_2 x < \pi(x)}$

$\exists\ \ell \in \mathbb{N}$ so $\quad 2^{2^{\ell-1}} \le x < 2^{2^\ell}$

By (*) $\quad p_\ell \le 2^{2^{\ell-1}} \Rightarrow p_\ell \le x \Rightarrow \pi(x) \ge \ell$ {since $p_1, \dots, p_\ell$ are $\le x$}.

But $\quad x < 2^{2^\ell} \Rightarrow \log x < 2^\ell \log 2 \Rightarrow \frac{\log x}{\log 2} < 2^\ell \Rightarrow \frac{\log(\log x / \log 2)}{\log 2} < \ell$

Hence $\pi(x) \ge \ell > \frac{\log_2 x - \log_2 2}{\log 2 = 0.6} > \log_2 x$. //

**Definition** If $p = 2^n - 1 \in \mathbb{P}$ we say $p$ is a **Mersenne Prime**.

**Theorem 6** *If $n > 1$ and $a^n - 1$ is prime then $a = 2$ and $n$ is prime.*
*Proof.* If $a > 2$ then $a - 1 \,|\, a^n - 1$ $(a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + 1))$ so $a^n - 1 \notin \mathbb{P}$. If $a = 2$ and $n = j\ell$, where $j$ is a proper divisor of $n$, then $2^n - 1 = (2^j)^\ell - 1$ is divisible by $2^j - 1$ ($a = 2^j$ in the equation above). Hence $n \in \mathbb{P}$. $\square$

$= a^\ell - 1 = (a-1)(\ldots)$
$\overset{\shortparallel}{2^j}$

web: `http://www.utm.edu/research/primes/mersenne.shtml`

**Theorem 7** *If $2^m + 1 \in \mathbb{P}$ then $m = 2^n$.*

$\mp (-1)^q = 1.$

*Proof.* If $m = qr$, where $q$ is odd, then $r \neq 1$
$2^{qr} + 1 = (2^r)^q + 1 = (2^r + 1)(2^{r(q-1)} - 2^{r(q-2)} + \cdots + 1)$ and $1 < 2^r + 1 < 2^{qr} + 1$ so $2^{qr} + 1$ cannot be prime. Hence $m$ has no odd prime factor. Hence $m = 2^n$, $n \in \mathbb{N}$. $\square$

*Note* The factorization

$r = \frac{a}{b}$ in J.P.

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1})$$

works here for *odd* $n$ since

$$\begin{aligned} a^n + 1 &= a^n - (-1)^n \\ &= (a - (-1))(a^{n-1} + a^{n-2}(-1) + a^{n-3}(-1)^2 + \cdots (-1)^{n-1}) \\ &= (a+1)(a+1)(a^{n-1} - a^{n-2} + a^{n-3} - \cdots + 1) \end{aligned}$$

## Fermat Numbers

**Definition** The $n^{\text{th}}$ Fermat number, $F_n = 2^{2^n} + 1$

$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537.$ $\in \mathbb{P}$

$F_i \in \mathbb{P}$ for $0 \leqslant i \leqslant 4$. *No* other Fermat prime is known.

$F_5 \notin \mathbb{P}$.

$2^7 = 128.$

(Euler, 1732): $641 \,|\, 2^{2^5} + 1 = 641 \cdot 6700417$.
*Proof.* Let

$$\begin{aligned} a &= 2^7 \\ b &= 5 \\ a - b^3 &= 3 \\ 1 + ab - b^4 &= 1 + 5 \cdot 3 = 2^4 \end{aligned}$$

$2^5 = 2 \cdot 2^2$ $\quad n = p_1^{\lambda_1} \cdots p_m^{\lambda_m}$

Therefore

$$\begin{aligned}
2^{2^5}+1 &= (2^8)^4+1 \\
&= (2a)^4+1 \\
&= 2^4a^4+1 \\
&= (1+ab-b^4)a^4+1 \\
&= (1+ab)a^4+1-a^4b^4 \\
&= (1+ab)a^4+(1-a^2b^2)(1+a^2b^2) \\
&= (1+ab)[a^4+(1-ab)(1+a^2b^2)]
\end{aligned}$$

and $1+ab=641$. $\square$

**Theorem 8 (Lagrange)** *If $p \in \mathbb{P}$, the exact power $\alpha$ of $p$ dividing $n!$ ($p^\alpha \| n!$) is*

$$\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

*Proof.*

$$\begin{aligned}
n! &= 1 \cdot 2 \cdots (p-1) \\
&\quad \cdot p(p+1)\cdots 2p \cdots (p-1)p \\
&\quad \cdot p^2 \\
&\quad \cdots
\end{aligned}$$

There are $\left\lfloor \frac{n}{p} \right\rfloor$ multiples of $p$, $\left\lfloor \frac{n}{p^2} \right\rfloor$ multiples of $p^2$, etc.

Each multiple of p contributes 1 to $\alpha$. Each multiple of $p^2$ has already contributed 1, being a multiple of $p$, so contributes 1 more to $\alpha$ leading to

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor$$

etc. Hence

$$\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^r} \right\rfloor$$

where $r$ is the first $\mathbb{N}$ such that $p^{r+1} > n$. So $\left\lfloor \frac{n}{p^\beta} \right\rfloor = 0 \ \ \forall \beta \geqslant r+1$. $\square$

**Ex** $n=12,\ p=3$ so

$$\begin{aligned}
\alpha &= \left\lfloor \frac{12}{3} \right\rfloor + \left\lfloor \frac{12}{9} \right\rfloor + \left\lfloor \frac{12}{27} \right\rfloor \\
&= 4+1+0 \\
&= 5.
\end{aligned}$$

## 2.4 Fermat Numbers

$F_n := 2^{2^n} + 1 \qquad n \geq 0 \qquad$ so all are odd.

$F_0 = 3, \; F_1 = 5, \; F_2 = 17, \; F_3 = 257, \; F_4 = 65537 \in \mathbb{P}$

$641 \mid F_5. \qquad$ (Euler 1732) $\qquad F_5 \notin \mathbb{P}$.

(Read)

<u>Thm 2.2</u> $\quad 0 \leq n < m \Rightarrow (F_n, F_m) = 1$

<u>Proof</u> $\quad F_m - 2 = 2^{2^m} - 1 = (2^{2^{m-1}})^2 - 1 = (2^{2^{m-1}} + 1)(2^{2^{m-1}} - 1)$

$= F_{m-1}(2^{2^{m-1}} - 1)$

$= \cdots = F_{m-1} F_{m-2} \cdots F_0$

$\Rightarrow F_{m-1} \cdots F_0 \mid F_m - 2$

so $F_n \mid F_m - 2$.

If a prime $p \mid (F_n, F_m) \Rightarrow p \mid F_m$ and $p \mid F_m - 2 \Rightarrow p \mid 2 \Rightarrow p = 2$

But $F_m$ is odd(!!). Hence $(F_n, F_m) = 1$. //

<u>Note</u>: An $F_n$ might not be prime, but must have a different (new) prime factor to earlier prime divisors of $F_j$ for $0 \leq j < n$. and $2 \nmid F_n \; \forall n$.

so

$p_0 = 2 < F_0 = 3$

$p_1 = 3 \leq F_0 = 3$

$p_2 = 5 \leq F_1 = 5$

$p_3 = 7 \leq F_2 = 17$

$\vdots$

$p_n \leq F_{n-1} \quad \forall n \geq 3 \Rightarrow p_n < 2^{2^{n-1}} + 1$

$p_n \leq 2^{2^{n-1}} \ldots$

Since $|\mathbb{N}| = \infty$ and $|\{F_n : n \geq 0\}| = \infty \Rightarrow |\mathbb{P}| = \infty$.

## §2.5 A better lower bound for $\pi(x)$

**Thm 2.4** for $x \geq 2$ $\quad \pi(x) \geq \dfrac{\log(x)}{2\log 2}$ and $p_n \leq 4^n \quad \forall n \geq 1$.

**Proof** Let $x \in \mathbb{N}$ & $j \in \mathbb{N}$ such that.

$2 = p_1 < p_2 \dots < p_j \leq x$ suppose all of the primes in $[2, x]$.

If $n \leq x$ write $n = m \cdot l^2$ where $m$ is squarefree.

Ex. $24 = 6 \cdot 2^2 \implies m = p_1^{\varepsilon_1} \dots p_j^{\varepsilon_j}$, $\varepsilon_i \in \{0, 1\}$.

There are $\lfloor x \rfloor$ possible values for $n$.

and each $l^2 \leq x \implies l \leq \sqrt{x} \implies \exists \lfloor \sqrt{x} \rfloor$ possible values for $l$.

There are $2^j$ possible values for $m$, hence at most $\lfloor \sqrt{x} \rfloor \cdot 2^j$ possible value for $n \implies \lfloor x \rfloor \leq \lfloor \sqrt{x} \rfloor 2^j \quad \otimes$

$$\implies \pi(x) = j \geq \frac{\log\left(\frac{\lfloor x \rfloor}{\lfloor \sqrt{x} \rfloor}\right)}{\log 2} \overset{\text{Ex}}{\geq} \frac{\log \lfloor x \rfloor}{2 \log 2}$$

To see this write
$$\begin{aligned} \sqrt{x} &\geq \lfloor \sqrt{x} \rfloor \\ x &\geq \lfloor \sqrt{x} \rfloor^2 \\ \lfloor x \rfloor &\geq \lfloor \sqrt{x} \rfloor^2 \\ \lfloor x \rfloor^2 &\geq \lfloor \sqrt{x} \rfloor^2 \lfloor x \rfloor \\ \lfloor x \rfloor &\geq \lfloor \sqrt{x} \rfloor \sqrt{\lfloor x \rfloor} \\ 2^j \geq \Big) \quad \frac{\lfloor x \rfloor}{\lfloor \sqrt{x} \rfloor} &\geq \sqrt{\lfloor x \rfloor} \qquad \otimes \quad \lfloor x \rfloor \leq 2^{2j} \end{aligned}$$

Let $x = p_n$ so $j = n$ & $\otimes \implies p_n \leq 4^n$. //

**Thm 2.6** : (Chebyshev's Estimate)
$$\left(\frac{3\log 2}{8}\right) \frac{x}{\log x} < \pi(x) < (6\log 2) \frac{x}{\log x}.$$

## §2.7 (Bertrand's Hypothesis) $\forall n \; \exists p \in [n, 2n)$

Thm 2.10.

## §2.8 Distance between consecutive primes.

$\forall n \in \mathbb{N}$: $n! + 2, \dots, n! + n$ gives $n-1$ composites

so $p_{n+1} - p_n$ can be large.

## §2.8 Distance between consecutive primes

| $p_1$ | $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | $p_7$ | $p_8$ | $p_9$ | $\cancel{p_{10}}$ | $p_{10}$ | $p_{11}$ | $p_{12}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | ~~27~~ | 29 | 31 | 37 |

1 2 2 4 2 4 2 4 ~~8~~ 6 ~~8~~ 2 6.

Since $\exists\ p \in [p_n, 2p_n) \Rightarrow p_{n+1} < 2p_n. \Rightarrow \underline{p_{n+1} - p_n < p_n}.$

Cramer's conj (1936) $\dfrac{p_{n+1} - p_n}{(\log p_n)^2} \leq 1 + \varepsilon \quad \forall\, n \geq n_\varepsilon.$

Baker, Harman, Pintz (2001). $p_{n+1} - p_n < p_n^{0.525}$

Small gaps? $p_{n+1} - p_n = 2$ so $(p_n, p_{n+1})$ are twin primes.

unknown if or if not an $\infty$ number of them.

similarly $p_{n+1} - p_n = 4$ or even $p_{n+1} - p_n = 2k$, $k$ fixed.

Read the rest of §2.8 note if $(a_n)$ is a bounded sequence

$$\liminf_{n\to\infty} a_n = \lim_{n\to\infty} (\inf\{a_n, a_{n+1}, \dots\})$$

$$\& \quad \limsup_{n\to\infty} a_n = \lim_{n\to\infty} (\sup\{a_n, a_{n+1}, \dots\})$$

the smallest and, respectively, largest limit of any subsequence. So

roughly. $\displaystyle\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0$ means. $\exists\,(n_j)$ so $\forall\, \varepsilon > 0$

$p_{n_j+1} - p_{n_j} \leq \varepsilon \log n_j \quad j \in \mathbb{N}.$

a result of Goldston, Pintz and Yildirim, 2005.

## 42.9 Mersenne primes

Cleric Marin Mersenne (1588 – 1648) $p \le 257$ $p \in \mathbb{P}$ with $2^p - 1 \in \mathbb{P}$

where $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$

$2^{67} - 1 = 193707721 \times 761838257287$ &

$2^{61} - 1$, $2^{89} - 1$, $2^{107} - 1$ $\in \mathbb{P}$ [1947].

$2^{257} - 1 =$

Know $x = 2^a - 1 \in \mathbb{P} \Rightarrow a \in \mathbb{P}$.

$23 \times 89 = 2^{11} - 1$ $\not\Leftarrow$ $a = 11$

$M_p := 2^p - 1$ Mersenne numbers. If $M_p \in \mathbb{P}$ get a Mersenne prime

Largest known prime are Mersenne.

– very sparse on the number line

so impossible to study easily.

– only 47 known $M_p \in \mathbb{P}$.

$M_2 = 3$ ) 4
$M_3 = 7$ ) 24
$M_5 = 31$ ) 96
$M_7 = 127$

Problem: $\exists ?$ $\infty$ no. of Mersenne primes

## 42.10 Conjectures on primes

– better than dek/L see introduction to Apostol, Hardy & Wright.

(1) Twin prime conjecture (3,5), (5,7), (11,13) (17,19), (41,43) ....

(2) $\exists$ $p$ in $(n^2, (n+1)^2)$ $\forall n \in \mathbb{N}$.

(3) Goldbach's conjecture $2n = p + q$ $\forall n$ $\exists p, q \in \mathbb{P}$.

(4) RH $\pi(x) = \dfrac{x}{\log x} + O(x^{\frac{1}{2}+\varepsilon})$ $x \to \infty$ $\forall \varepsilon > 0$.

but usually posed in terms of the Riemann Zeta Function

(5) odd perfect no. problem $N$ odd & $\sigma(N) = 2N$ where $\sigma(N) := \sum_{d|N} d$

then $N > 10^{1500}$ (2011)