**Theorem** (Euclid)

There are infinitely many prime numbers

Proof. Toward a contradiction, assume there are only finitely many prime numbers

$$p_1 = 2, \ p_2 = 3, \ \cdots, \ p_N$$ ← largest prime number

Consider $M = p_1 \cdot p_2 \cdot \dots \cdot p_N + 1$.

Since $M > p_N$, it is a composite number.

Hence, there is a prime number $p_i$ such that $p_i \mid M$.

On the other hand $p_i \mid p_1 \cdot p_2 \cdot \dots \cdot p_N$. ← prod of ALL prime numbers

By 2-out-of-3. $p_i \mid 1$, which is a contradiction! $\boxed{\not\!\!\!\!\ \ }$

So the Hasse diagrame of all positive integers is an INFINITE-dimensional network !!

But, the # of "primes $\leq$ a given bound $x$" is finite

<u>Def</u>: For any real number $x > 0$,

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

e.g. $\pi(\frac{3}{2}) = 0$ no prime number is $\leq \frac{3}{2}$

$\pi(3\sqrt{5}) = \pi(6) = 3$ $\{2, 3, 5\}$

$6 < \sqrt{45} < 7$

$\pi(24) = 9$ $\{2, 3, 5, 7, 11, 13, 17, 19, 23\}$

## Open Question:

Do we have an asymptotic formula for $\pi(x)$?

Namely, can we have a simpler function $f(x)$ s.t.

$$\pi(x) \sim f(x) \ ?$$

means: $\displaystyle \lim_{x\to\infty} \frac{\pi(x)}{f(x)} = 1.$

If so, can we bound the "error" $|\pi(x) - f(x)|$ in terms of $x$?

**Thm** (Prime Number Theorem, 1896, J. Hadamard and C. J. de la Vallée Poussin)

$$\pi(x) \sim \frac{x}{\log(x)}$$

$$\mathrm{Li}(x) := \int_2^x \frac{dt}{\log(t)}$$ offset logarithmic integral

$$\mathrm{li}(x) := \int_0^x \frac{dt}{\log(t)}$$ logarithmic integral

$$\pi(x) \sim \mathrm{Li}(x)$$

**Coro of RH** (by Lowell Schoenfeld 1976)

Assuming RH, then $\left|\pi(x) - \mathrm{li}(x)\right| < \frac{\sqrt{x}\log x}{8\pi}$ for $x \geqslant 2657$.

Riemann's Hypothesis

# Gaps between primes

- How large could $P_n - P_{n-1}$ be? Arbitorily large.
- Smallest gap: 1 (2 & 3) the only case. ; 2 (e.g. 3 & 5)

⇝ **Twin Prime** $p$ & $q$ are twin primes if they are primes and $|p-q|=2$

Open Question:

Are there infinitely many twin primes?

**Thm**: There are infinitely many pairs of primes $(p, q)$ s.t

(~2013, Y. Zhang) $|p-q| < 70$ million.

(~2014, PolyMath8) $|p-q| < 246$.

# The set of divisors

$$\mathcal{D}(n) := \{ d \text{ is an positive integer} \mid d \text{ is a divisor of } n \}$$

$$\sigma_0(n) := \# \mathcal{D}(n)$$

$$\sigma_k(n) := \sum_{d \in \mathcal{D}(n)} d^k$$

$k=0$: $\sum_{d \in \mathcal{D}(n)} 1 = \# \mathcal{D}(n)$

$= \sigma_0(n)$

**Prop.** (Multiplicativity of divisor sets / $\sigma$)

$$\begin{array}{ccccc} \mathcal{D}(m) & \times & \mathcal{D}(n) & \xrightarrow{\Phi} & \mathcal{D}(mn) \\ u & & v & & u \cdot v \end{array}$$

If $m$, $n$ are coprime, then $\Phi$ is bijective.

$GCD(m, n) = 1$

proof: $\Phi$ is well-defined since:

$$u \mid m \ \& \ v \mid n \Rightarrow u \cdot v \mid mn$$

$$\left( m = u \cdot d_1 \ , \ n = v \cdot d_2 \Rightarrow mn = u \cdot v \cdot d_1 d_2 \right)$$

Surjectivity of $\Phi$: $w \mid mn \Rightarrow u \mid m \ \& \ v \mid n$

If $w \mid mn$, then for every prime $p$, we have

$$v_p(w) \leq v_p(mn) = v_p(m) + v_p(n).$$

But $m$ & $n$ are coprime, so either $v_p(m) = 0$ or $v_p(n) = 0$.

Define $u, v$ as follows

$$u := GCD(w, m) \quad \& \quad v := GCD(w, n)$$

In particular, $u \mid m$ and $v \mid n$. Remains to show $w = uv$

For every prime number $p$, we have.

$$v_p(u) = \min\{v_p(w), v_p(m)\}$$
$$v_p(v) = \min\{v_p(w), v_p(n)\}$$

Then $v_p(u \cdot v) = v_p(u) + v_p(v)$

$$= \underbrace{\min\{v_p(w), v_p(m)\}}_{①} + \underbrace{\min\{v_p(w), v_p(n)\}}_{②}$$

Since either $v_p(m) = 0$ or $v_p(n) = 0$

$v_p(m) = 0 \Rightarrow ① = 0,\ ② = v_p(w)$

$v_p(n) = 0 \Rightarrow ① = v_p(w),\ ② = 0$.

$\Rightarrow v_p(u \cdot v) = v_p(w)$.

Therefore $u \cdot v = w$.

## Injectivity of $\Phi$:

Suppose $u \mid m$, $v \mid n$ and $u \cdot v = w$.

Then for every prime $p$, we have

$$v_p(u) \le v_p(m), \quad v_p(v) \le v_p(n)$$

and $v_p(u) + v_p(v) = v_p(w)$

Since either $v_p(m) = 0$ or $v_p(n) = 0$, (by $\gcd(m,n)=1$)

If $v_p(m) = 0 \Rightarrow v_p(u) = 0 = \min\{v_p(m), v_p(w)\}$ & $v_p(v) = v_p(w) = \min\{v_p(n), v_p(w)\}$

If $v_p(n) = 0 \Rightarrow v_p(v) = 0 = \min\{v_p(n), v_p(w)\}$ & $v_p(u) = v_p(w) = \min\{v_p(m), v_p(w)\}$

we have $\begin{cases} v_p(u) = \min\{v_p(w), v_p(m)\} \\ v_p(v) = \min\{v_p(w), v_p(n)\} \end{cases} \Rightarrow \begin{array}{l} u = \mathrm{GCD}(w, m) \\ v = \mathrm{GCD}(w, n) \end{array}$

$\square$

**Def.** An *Arithmetic function* is a function whose domain is the set of positive integers.

An arithmetic function $f(z)$ is *multiplicative* if for any coprime positive integers $m$, $n$,

$$f(mn) = f(m) \cdot f(n).$$

**Remark**: If we remove the restriction of being coprime, then the property is called "*complete multiplicative*".

**Coro**: $\sigma_k$ is multiplicative. I.e.

$$\sigma_k(mn) = \sigma_k(m)\cdot\sigma_k(n)$$

**Proof**: $LHS = \sum_{d\mid mn} d^k$

$d \in D(mn)$

Bec of $\Phi$ is bijective

$(u,v) \in D(m) \times D(n)$

$$\overset{\circledast}{=} \sum_{u\mid m,\, v\mid n} (u\cdot v)^k$$

$$= \left(\sum_{u\mid m} u^k\right)\cdot\left(\sum_{v\mid n} v^k\right) = RHS.$$

∎

<u>Coro</u>. If $n = p_1^{e_1} \cdots p_r^{e_r}$, then

$$\sigma_0(n) = (e_1+1)\cdots(e_r+1)$$

Proof: By multiplicativity,

$$\sigma_0(n) = \sigma_0(p_1^{e_1}) \cdot \cdots \cdot \sigma_0(p_r^{e_r}).$$

For each prime $p$, we have

$$\sigma_0(p^e) = \#\{1, p, p^2, \cdots, p^e\}$$
$$= e+1.$$

Thus the coro is proved.

**Lemma**: If $x \neq 1$ is a real number and $e$ a natural number, then

$$1 + x + x^2 + \cdots + x^e = \frac{x^{e+1} - 1}{x - 1}$$

Proof: Let $S = 1 + x + x^2 + \cdots + x^e$.

Then $xS = x + x^2 + \cdots + x^e + x^{e+1}$.

Hence $(x-1)S = x^{e+1} - 1$.

Since $x \neq 1$, dividing both side by $x - 1$ shows the identity.

∎

**Prop.** If $n = p_1^{e_1} \cdots p_r^{e_r}$, then

$$\boxed{\sigma_k(n) = \frac{(p_1^{e_1+1})^k - 1}{p_1^k - 1} \cdot \cdots \cdot \frac{(p_r^{e_r+1})^k - 1}{p_r^k - 1}}$$

**Proof**: By multiplicativity of $\sigma_k$, it suffices to show

$$\sigma_k(p^e) = \frac{(p^{e+1})^k - 1}{p^k - 1}.$$

$$\sigma_k(p^e) = \sum_{i=0}^{e} (p^i)^k = \sum_{i=0}^{e} (p^k)^i \qquad x = p^k$$

$\{1, p, p^2, \cdots, p^e\}$

$$= \frac{(p^k)^{e+1} - 1}{p^k - 1} = RHS$$

$\blacksquare$

# After-Class :

- There are many ways to prove *Euclid's theorem on infiniteness of prime numbers*. Please check this wiki page or this wiki article for more information. It is worth mentioning that one method is to show the series $\sum \frac{1}{p}$ of reciprocals of prime numbers *diverges* (see the beginning of this note).
- See this wiki page for Prime number theorem. It is worth mentioning that the proof relies on the Riemann zeta function $\zeta(s)$.
- The method people used to attack the *twin prime conjecture* as well as many other questions in number theory is called the *Sieve theory*. James Maynard, one of the Fields Medal winner this year, showed that there are infinitely many pairs of primes with gap no larger than 600 in 2013.
- The first **Glossary** submission is due **tonight**, be aware of it.
- HW 2 is **due Monday**, be aware of it.
- We will finish Chapter 2 in one or 1.5 lectures. Please read the rest of Chapter 2 preparing next meeting.