Section 3.1

Def: A <u>prime number</u> is an integer $p > 1$ which has exactly two positive divisors. Every other integer greater than 1 is called <u>composite</u>.

Facts

Thm: Every integer $n > 1$ has a prime divisor.

Pf: Consider: $S = \{d > 1 : d \mid n\}$

Note $n > 1$ and $n \mid n$, so $n \in S \rightarrow S \neq \emptyset$

S has a least elt., p, by well-ordering

If p isn't prime, it has at least 3 divisors: $1, p, d$

$\rightarrow d \mid p,\ p \mid n \Rightarrow \underline{d \mid n}$

also, $\underline{d > 1} \longrightarrow d \in S$

But $d < p$ b/c $d \mid p$, $d \neq p$

This contradicts the minimality of p

Hence, p is prime!

Thm: There are infinitely many primes

Pf: Suppose not.

Let $P = \{p > 1 : p \text{ is prime}\}$

↳ set of $\underline{\text{all}}$ primes

Define $k := \prod_{x \in P} x$ ← \prod

↳ "multiply all elts. of P"

\sum

$\sum_{x \in P} x$ ← "add all elts. of P"

By prev. thm, $k+1$ has a prime divisor, p.

Q: is $p \in P$?

A: yes - P is the set of all primes

$\rightarrow$ $p \mid k$

$p \mid k+1$

$\Rightarrow p \mid (k+1) - k = 1$

Contradiction: no prime number divides 1.

So there are inf. many primes.

Ex: $3 \cdot 5 = 15$ $\qquad 15 + 1 = 16$

$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p_n$ is called a <u>primorial number</u>

Q: Is a primorial $+1$ always prime?

Another pf:

Prop: For every $n > 1$, if p is a prime divisor of $n!+1$, then $p > n$.

Cor: For every $n > 1$, there exits a prime $p > n$.

Pf of Cor: Pick n, so $n!+1$ has prime divisor, $p > n$

Pf of prop: Let $n > 1$, p be a prime divisor of $n!+1$

By $\oint$, assume $p \leq n$.

$\rightarrow p \mid n!$

$p \mid n!+1$

$\Rightarrow p \mid (n!+1) - n! = 1$

Contradiction

Hence, $p > n$.

Ex: $n = 4 \rightarrow n!+1 = 25$

every $p \mid 25 \rightarrow p = 5 > n$

Thm: If n is composite, then n has a prime divisor $\leq \sqrt{n}$

Pf: Since n is composite, $n = ab$ where $1 < a \leq b < n$

Suppose by $\lightning$ $a > \sqrt{n}$

So $b \geq a$, $b > \sqrt{n}$

Hence $\underline{n} = ab \underline{>} \sqrt{n} \cdot \sqrt{n} = \underline{n}$

Contradiction

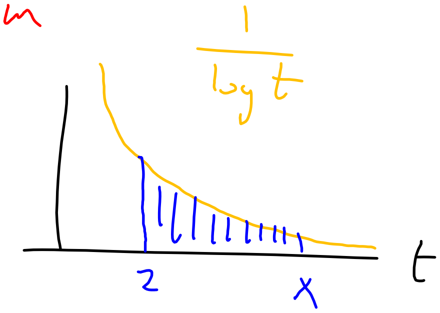
So $a \leq \sqrt{n}$

Q: Where do the primes live?

- How many primes end in 1? 3? 5? 7?
  ↳ can answer
- Are infinitely many twin primes?
  ↳ p, $p+2$ (both prime)
  ↳ Open
- Given a number n, how far do I have to look to find a prime?
- Are there inf. many primes of the form n^2+1? ↳ open

- How many primes are there $\leq x$?
  - ↳ Prime Number Theorem

Def: $Li(x) = \int_2^x \frac{1}{\log t}\, dt$



$\log(x)$ means "natural log of x"

$\pi(x)$ = number of primes $\leq x$

Thm (Prime Number Theorem): $\lim_{x \to \infty} \frac{\pi(x)}{Li(x)} = 1$

Examine $Li(x)$

$$Li(x) = \int_2^x \frac{1}{\log t}\, dt = uv\Big|_2^x - \int_2^x v\, du$$

$(\log t)^{-1}$

$u = \frac{1}{\log t} \qquad dv = dt$

$du = \frac{-1}{t \log^2 t}\, dt \qquad v = t$

$$= \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{t}{t \log^2 t}\, dt$$

$$= \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{1}{\log^2 t}\, dt$$

Claim: $\lim_{x \to \infty} \dfrac{Li(x)}{\int_2^x \frac{1}{\log^2 t}\,dt} = \infty$

Pf: Check $Li(x) \xrightarrow[x \to \infty]{} \infty$

$$Li(x) = \int_2^x \frac{1}{\log t}\,dt \geq \int_2^x \frac{1}{t}\,dt \xrightarrow[x \to \infty]{} \infty$$

Check $\int_2^x \frac{1}{\log^2 t}\,dt \xrightarrow[x \to \infty]{} \infty$

(Same comparison)

Apply L'Hôpital:

$$\lim_{x \to \infty} \frac{\int_2^x \frac{1}{\log t}\,dt}{\int_2^x \frac{1}{\log^2 t}\,dt} = \lim_{x \to \infty} \frac{\frac{d}{dx}\int_2^x \frac{1}{\log t}\,dt}{\frac{d}{dx}\int_2^x \frac{1}{\log^2 t}\,dt}$$

$$\overset{FTC}{=} \lim_{x \to \infty} \frac{\left(\frac{1}{\log x}\right)}{\left(\frac{1}{\log^2 x}\right)}$$

$$= \lim_{x \to \infty} \log x = \infty$$

Meaningfully $Li(x)$ is bigger than $\int_2^x \frac{1}{\log^2 t} dt$

$$Li(x) = \underbrace{\frac{x}{\log x}}_{\text{main contributor}} - \frac{2}{\log 2} + \int_2^x \frac{1}{\log^2 t} dt$$

$$\rightarrow \quad Li(x) \simeq \frac{x}{\log x}$$

$$\approx$$

$$\pi(x)$$

Probability of randomly picking a prime $\leq x$

$$\rightarrow \quad \frac{\pi(x)}{x} \simeq \frac{\left(\frac{x}{\log(x)}\right)}{x} = \frac{1}{\log x}$$

Cor: There are inf. many primes

Pf: $\pi(x) \approx \frac{x}{\log x} \rightarrow \lim_{x\to\infty} \pi(x)$

$\approx \lim_{x\to\infty} \frac{x}{\log x}$

$= \infty$

Q: How many primes end in 3?

$\updownarrow$

How many primes have the form $\underline{10k+3}$?

$\downarrow$

arithmetic progression

13, 23, 33, 43, ...

Q: How many primes end in 5?

A: One: $p = 5$

$\updownarrow$

How many primes have the form $10k+5$?
$\quad\quad = 5(2k+1)$

Thm (Dirichlet): If $a, b \in \mathbb{Z}_{\geq 1}$, $(a,b)=1$, then there are inf. primes of the form $a + bk$

Cor: Inf. many primes ending in 3

Q: How far do you have to look to find a prime?

So far: $\forall n$, $\exists$ prime p: $n < p \leq n! + 1$

Thm (Betrand-Chebyshev): $\forall n$: $\exists$ prime p:

$$n < p < 2n$$

(Legendre's)
Conjecture: $\forall n$ $\exists$ prime p: $n^2 < p < (n+1)^2$