Math 321

Primes $\cdot, \cdot\cdot, \cdot\cdot\cdot, \cdot\cdot\cdot\cdot, \ldots$

$(1)_2 \quad (1,0)_2 \quad (1,1)_2 \quad (1,0,0)_2$

1 2 3 4

Def - if $n \geq 2$ is a prime if its only factors are 1 and n.

- call n composite otherwise.

6 $2\overline{|\cdot\cdot\cdot}$ 3

Finding Primes (Prime Sieve)

if n is a prime then $n \cdot k$, $k = 2, 3, 4, \ldots$ is a composite

1 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ...

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

Fundamental Thm of Arithmetic

For every $n \geq 2$, it is prime or it can be written as a uniq. prod of primes in non-dec. order.

Note: if you say (2) to be a product (no multiplication) then you can just say "uniq prod. of primes"

Note: proof is "hidden" in the textbook.

$1, (2), (3), (2^2), (5), (2\cdot3), (7), (2^3), (3^2)$
$1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \ldots$

How to factor numbers?

check all primes from 2 up to $\sqrt{n}$

$n = 101 \quad \leq \sqrt{101} \approx 10.x$

check: 2, 3, 5, 7 — $n=101$ is prime

$2 \nmid 101$

$3 \nmid 101$

$5 \nmid 101$

$7 \nmid 101$

$7 \overline{)101}$ (1, remainder 7; 7, remainder 31)

How many primes? Thm: ∞ primes

PF (by contradiction) all primes are $\{p_1, p_2, \ldots, p_n\}$ finite.

Consider: $(p_1 \cdot p_2 \cdot \ldots \cdot p_n) + 1 = Q$

all numbers have some prime that divides it.

OK call p^* the prime that divides $p^* \mid Q$

p^* is prime so $p^* \in \{p_1, p_2, \ldots, p_n\}$

$\rightarrow$ so $p^* \mid (p_1 \cdot p_2 \cdot \ldots p^* \cdot \ldots p_n)$

Know: Q

1) $p^* \mid \overline{(p_1 \cdot p_2 \cdot \ldots p_n) + 1}$

2) $p^* \mid (p_1 \cdot p_2 \cdot \ldots p_n)$

we have: $a \mid b \wedge a \mid c \rightarrow a \mid m \cdot b + n \cdot c$

$\Rightarrow p^* \mid (1)Q + (-1)(p_1 \cdot p_2 \cdot \ldots p_n)$

$\rightarrow p^* \mid 1 \equiv F$

---

rare?

$x \rightarrow \infty$ primes are always here

but are they rare?

Thm

Define: $\pi(x)$ is the prime counting function. $\pi(x) = \#$ of primes $\leq x$

Ex

$\pi(7) = 4$ $\pi(10) = 4$ $\pi(13) = 6$

$\pi(8) = 4$ $\pi(11) = 5$

$\pi(9) = 4$ $\pi(12) = 5$

$$\pi(x) \sim \frac{x}{\ln(x)} \quad \text{as} \quad x \rightarrow +\infty$$

① $\lim_{x\to+\infty} \pi(x) = \lim_{x\to+\infty} \frac{x}{\ln(x)} = \lim_{x\to+\infty} \frac{1}{\ln x} \cdot \lim_{x\to+\infty} x = +\infty$

② <u>% of primes</u> $\frac{\pi(x)}{x} \sim \frac{x/\ln x}{x} = \frac{1}{\ln x}$

% of primes from 1 to $10^{10} \approx \frac{1}{\ln 10^{10}} = \frac{1}{10\ln 10}$

$\approx \frac{1}{20}$

$\approx 5\%$

<u>Prime factorization</u> $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ (ex) $12 = 2^2 \cdot 3^1 \cdot 5^0$

$b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ (ex) $15 = 2^0 \cdot 3^1 \cdot 5^1$

$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$

$\gcd(12,15) = 2^0 3^1 5^0 = \boxed{3}$

$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdots p_n^{\max(a_n,b_n)}$

$\operatorname{lcm}(12,15) = 2^2 3^1 5^1 = \boxed{60}$

Thm $\boxed{a \cdot b = \gcd(a,b) \cdot \operatorname{lcm}(a,b)}$

gcd — Euclidean Algorithm

gcd(a, b)

$$a = b \cdot q + r$$

$$a - b \cdot q = r$$

$d = \gcd(a, b)$ means $d \mid a$ and $d \mid b$

so $d \mid (a - b \cdot q)$

$\Rightarrow d \mid r$

$$\gcd(a, b) = \gcd(b, r)$$

$$a = b \cdot q + r$$

gcd(15, 12)

$15 = 1 \cdot 12 + 3$

$12 = 4 \cdot 3 + 0$