Last time: FTA

$\forall n \in \mathbb{Z}, n > 0, \Rightarrow n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$

where $p_1 < \dots < p_k$ are primes
$a_i \geq 0$

where $\alpha_i \neq 0$, this decomposition is unique

Let $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \dots p_k^{\beta_k}$

- Lemma: $a \mid b \iff \alpha_i \leq \beta_i, \forall i$

- Thm: $gcd(a,b) = p_1^{\min(\alpha,\beta)} \dots p_k^{\min(\alpha_k,\beta_k)}$
  ↳ prove

Proof: Let $d = p_1^{s_1} \dots p_k^{s_k}$ where $s_i = \min(\alpha_i, \beta_i)$

Goal: show $d = gcd(a,b)$

① d is common divisor:

$s_i = \min(\alpha_i, \beta_i) \leq \alpha_i \ \forall i$

$\Rightarrow d \mid a$ by lemma similarly $d \mid b$

② It's greatest:

Let $c \mid a$ and $c \mid b$ where $c = p_1^{\gamma_1} \dots p_k^{\gamma_k}$

Goal: $c \leq d$

$c \mid a \Rightarrow \gamma_i \leq \alpha_i \ \forall i$ (by lemma)

$c \mid b \Rightarrow \gamma_i \leq \beta_i \ \forall i$

So $\gamma_i \leq \min(\alpha_i, \beta_i) = s_i$

$\Rightarrow c \mid d \Rightarrow c \leq d$ □

Distribution of prime numbers:
Hardest problem in number theory...

Primes are distributes on the number line in a strange and irregular way. Figuring this out is related to the Riemann Hypothesis (The hardest problem of all mathematics)

But we know a few things...

Theorem: There are infinitely many primes

Proof by contradiction:

Assume that the set of all prime is finite

$$P = \{p_1, p_2, p_3, \ldots, p_k\}$$

Let $n = p_1 p_2 p_3 \ldots p_k + 1$

n is not a prime number!

Because $n > p_i$, $i = 1 \ldots k$ $\Rightarrow$ n is composite

$\Rightarrow$ n is divisible by some prime p;

$p_i \mid n$ and $p_i \mid p_1 p_2 \ldots p_k$

$\Rightarrow p_i \mid n - p_1 p_2 \ldots p_k \Rightarrow p_i \mid 1$ CONTRADICTION

Sometimes, primes are very close and sometimes they are very far apart...

Thm (Very far apart): For any n > 0, there are consecutive primes p and q, with q-p>n

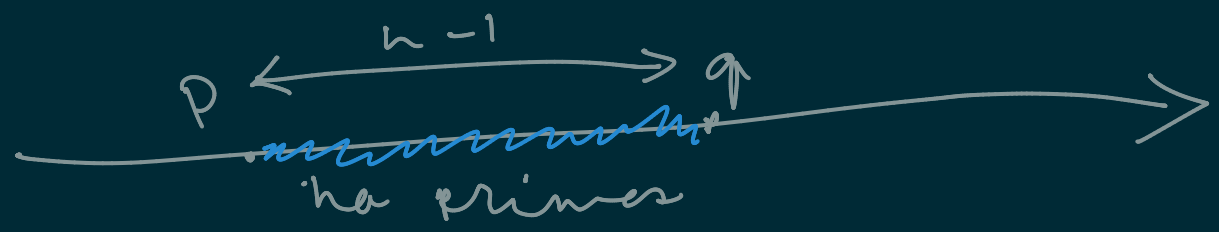
Proof: Consider following numbers

$n! + 2, n! + 3, n! + 4, \ldots n! + n$

This is a list of $n-1$ consecutive numbers

None are prime!

If $2 \le k \le n$ then $k \mid n! + k \Rightarrow n! + k$ is composite



About "very close" primes, there is a famous conjecture...

Def: Primes p and q are called twin primes if $p = q \pm 2$

Ex: 3 and 5

11 and 13

4291 and 4293

Twin primes conjecture (open since 1846):
There are infinitely many pairs of twin primes

One way to describe the distribution of primes is "on average"

Let $\pi(n)$ = The amount of primes $\le n$

Ex: $\pi(42) = ? = 13$

Primes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29,
31, 37, 41

Prime number theorem:

Asymptotically, $\pi(n) \sim \frac{n}{\log(n)}$

That means $\lim_{n \to \infty} \frac{\pi(n)}{\left(\frac{n}{\log(n)}\right)} = \text{constant}$

Modular Arithmetic

Ex: 12-hour clock. It is now 10:00

What time will it be in 42 hours?

"Dumb solution": start at 10 and count in head 42 steps, check where you land

More clever: Note that every 12 steps, you return to the original point...

$$42 = 3 \cdot 12 + 6$$

$$\Rightarrow 10 + 42 = 10 + 3 \times 12 + 6 = 16$$

$16 = 4$ (differ by 12)

Answer: 4

This is not true in $\mathbb{Z}$, but it's true on the clock
We should have written:

$$16 \equiv 4 \pmod{12}$$

Def: Let $a, b, n \in \mathbb{Z}$, $n > 1$

We say a is congruent to b modulo n, written

$$a \equiv b \pmod{n}$$

if a and b differ by a multiple of n

i.e: $a = b + kn$ $(k \in \mathbb{Z})$

equivalently: $n \mid (a - b)$

Another notation: $a \equiv_n b$ ← relation

ex: $42 \equiv 6 \pmod{12}$ $\quad 42 = 3 \times 12 + 6$

$6 \equiv 42 \pmod{12}$ $\quad 6 = (-3) \times 12 + 42$

$3 \equiv -2 \pmod{5}$

$n \equiv 0 \pmod{n}$ $\quad$ because $n = 1 \times n + 0$

In programming: modulo is a function

modulo: $x \,\%.\, n$ = remainder of division of x by n

$x \,\%.\, n$ = the unique r, $0 \leq r \leq n-1$

such that $x = qn + r$

ex: $42 \,\%.\, 12 = 6$

$6 \,\%.\, 12 = 6$

Thm: $a \equiv b \pmod{n}$

$\iff a \,\%.\, n = b \,\%.\, n$

Proof :

⇐ Suppose $a \,\%\, n = b \,\%\, n = r$

then $a = q_1 n + r$

$b = q_2 n + r$

$\Rightarrow a - b = (q_1 - q_2) n$

$n \mid a - b \Rightarrow a \equiv b \pmod n$

⇒ Suppose $a \equiv b \pmod n$

$\Rightarrow a - b = k n \quad (k \in \mathbb{Z})$

Let $r = a \,\%\, n$

Goal : Show $r = b \,\%\, n$

$\Rightarrow a = q n + r, \quad 0 \le r \le n - 1$

$b + k n = q n + r$

$b = (q - k) n + r$

By uniqueness of remainder :

$r = b \,\%\, n$ □

Corollary $\equiv_n$ is an equivalence relation.

Proof : Show that $\equiv_n$ is reflexive, symmetric, transitive

In terms of "%" that means :

① reflexive : $x \,\%\, n = x \,\%\, n$

→ of course ! same expression

② symmetry : $x \,\%\, n = y \,\%\, n \Rightarrow y \,\%\, n = x \,\%\, n$

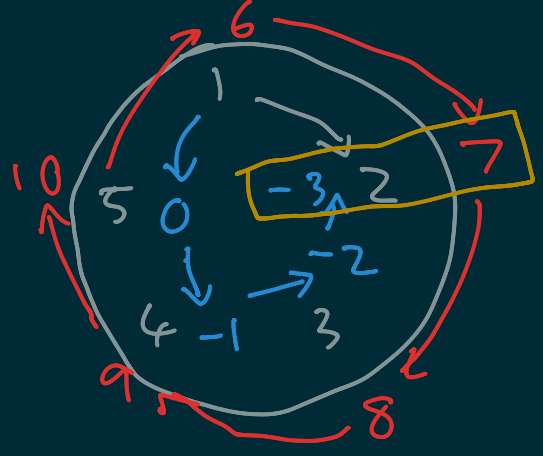
③ transitivity : $x \,\%\, n = y \,\%\, n$ and $y \,\%\, n = z \,\%\, n$

$\Rightarrow x \,\%\, n = z \,\%\, n$

All are true because $\equiv_5$ is an equivalence relation on $\mathbb{Z}$

⇒ <u>Consequence</u> : $\mathbb{Z}$ can be split into equivalence classes, mod 5

Ex : 5 hour clock



← equivalence class

$$[1]_{\equiv_5} = [\ldots -9, -4, 1, 6, 11, \ldots]$$

5 classes !.

$$\mathbb{Z}/\equiv_5 = \{[0], [1], [2], [3], [4]\}$$