Motivating example

Q6 from chapter 3.

Claim for all primes $p \geq 5$

p^2+2 is never prime.

$2^2+2=6$, $3^2+2=11$, $5^2+2=27$ $= 3\times 9$,

$7^2+2=51$ $=3\times 17$, $11^2+2=123$ $=3\times 41$, ...

Consider a prime $p \geq 5$

and $p = 6q + r$

where $r = \cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5$

$11 = 1\times 6+5$

$31 = 5\times 6 + 1$

The remainders $0, 2, 3, 4$ can not occur as p is a prime ≥ 5.

So we have two cases

$p = 6q+1$ **OR** $p = 6q+5$.

$p^2+2 = 36q^2+12q+3$

$= 3(12q^2+4q+1)$

So this is composite.

$p^2+2 = 36q^2+60q+27$

$= 3(12q^2+20q+9)$

which is composite.

Therefore if $p \geq 5$ is prime then p^2+2 is not prime.

In fact: using a divisor 3, instead of 6 would also work.

$$p = 3q + r$$

$$r = \not{0}, 1, 2$$

From this we see utility in ~~fo~~ fixing a divisor and focussing on how the remainders behave.

<u>Def 4.1</u> Congruence relation.

"a is congruent to b modulo n"

iff $n \mid a-b$. $a \equiv b \pmod{n}$

if $n \nmid a-b$ we say $a \not\equiv b \pmod{n}$

eg. $10 \equiv 17, 38 \pmod{7}$

$10 - 17 = -7$ and $7 \mid -7$

$10 - 38 = -28$ and $7 \mid -28$

$10 \not\equiv 37. \pmod{7}.$

Theorem 4.1

$a \equiv b \pmod{n} \iff$ a, b leaving the same remainder after division by n.

$a = q_1 n + r$

$b = q_2 n + r$

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

$\Rightarrow n \mid a - b.$

Congruence modulo n is a binary relation on $\mathbb{Z}$.

$a \equiv b \pmod{n}$

OR $a \not\equiv b \pmod{n}$

Def 4.2

A relation $\sim$ on a set X is an equivalence relation iff.

- $\sim$ is reflexive on X

  $\forall x \in X \quad x \sim x$

- $\sim$ is symmetric on X

  $\forall x, y \in X \quad x \sim y \Rightarrow y \sim x$

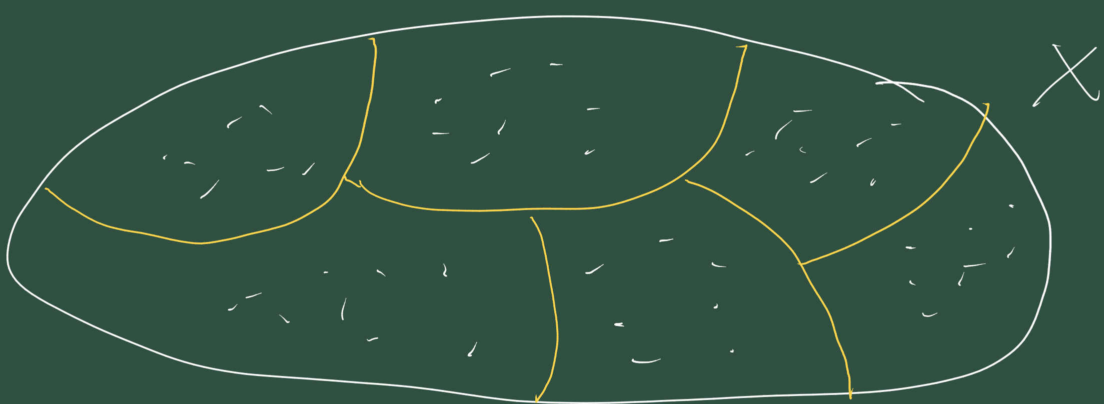
- $\sim$ is transitive on X.

$\forall x, y, z$

$(x \sim y \ \& \ y \sim z) \Rightarrow x \sim z.$

For an element $x \in X$ the equivalence class of x (wrt $\sim$) is $[x] = \{ y \in X : x \sim y \}$

When $\sim$ is an equivalence relation on X then X is partitioned by the equivalence classes.



Any partition X is associated to an equivalence relation on X and vice versa.

<u>Theorem 4.2</u> Congruence modulo n is an equivalence relation on $\mathbb{Z}$.

<u>Proof</u> Fix a ~~nonz~~ positive modulus n.

<u>Reflexive.</u> Let $z \in \mathbb{Z}$.

$n \mid 0$ so $n \mid z - z$.

$$\Rightarrow z \equiv z \pmod{n}$$

Symmetry.

If $x \equiv y \pmod{n}$

$\Rightarrow n \mid x - y$

$\Rightarrow n \mid y - x$, $y - x = -(x-y)$.

$\Rightarrow y \equiv x \pmod{n}$

Transitive.

Assume $x \equiv y$ & $y \equiv z \pmod n$

$\Rightarrow n \mid x-y$ & $n \mid y-z$.

$\Rightarrow n \mid (x-y)+(y-z)$

$\Rightarrow n \mid x-z$

$\Rightarrow x \equiv z \pmod n$.

So an equivalence relation as required. ∎

What's the partition look like?

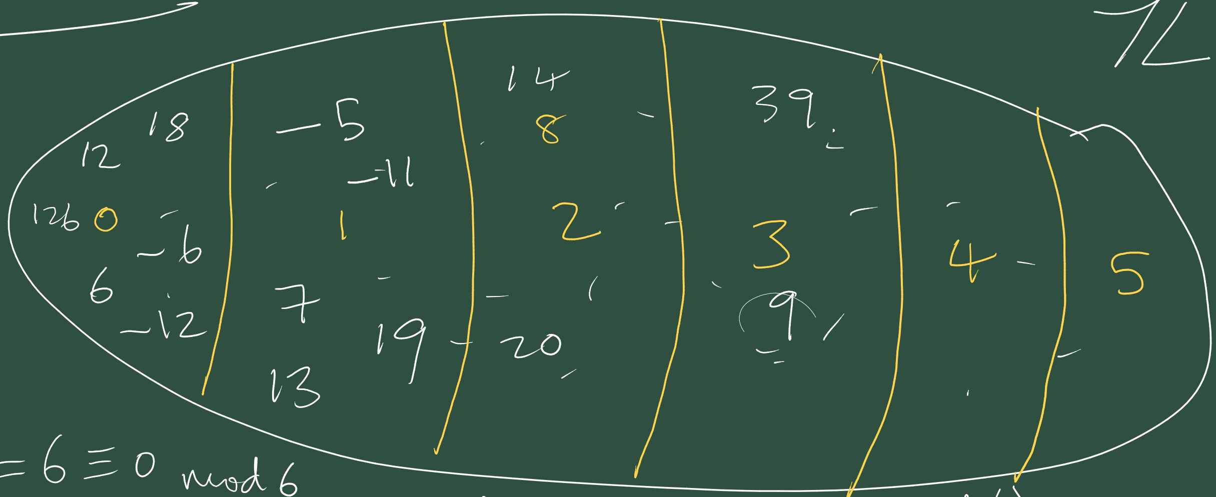
The equivalence classes are called congruence classes.

$[x] = \{ y \in \mathbb{Z} : x \equiv y \pmod n \}$.

eg $n=6$

$1+2=3 \equiv$
$19+20=39 \equiv 3 \pmod 6$

$\mathbb{Z}$.

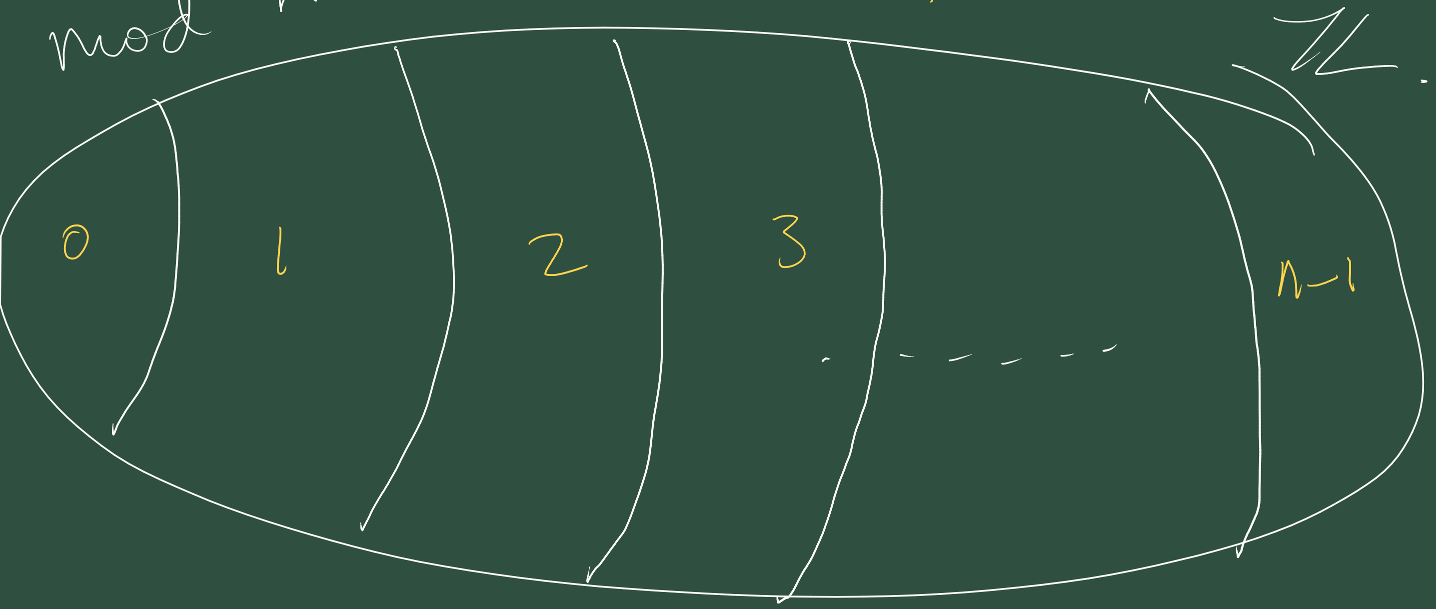


$2 \times 3 = 6 \equiv 0$ mod 6.

$14 \times 9 = 126 \equiv 0 \pmod 6$

The smallest non-negative remainders $0, \ldots, 5$ are regarded as the "cananoical" representatives / remainders / residues mod n

$1+2=3$.



In exercise 4.1 we have a sequence of results that say that ops $+ / \times$ work consistently with $\equiv \pmod n$.

<u>Ex 4.1</u> Let $a, b, a', b' \in \mathbb{Z}$.
assume $a \equiv a'$, $b \equiv b' \pmod n$.

Q1. Claim: $a+b \equiv a'+b' \pmod n$.

We know $n \mid a-a'$ & $n \mid b-b'$

$\Rightarrow n \mid a-a'+b-b'$

$\Rightarrow n \mid (a+b)-(a'+b')$

$\Rightarrow a+b \equiv a'+b' \pmod n$

Q2. Claim: $ab \equiv a'b' \pmod n$

Again. $n \mid a-a'$, $n \mid b-b'$

use a suitable linear combination.

$\Rightarrow n \mid [\underline{b}(a-a') + \underline{a'}(b-b')]$

, by the div. of lin. combs.

$\Rightarrow n \mid ab - a'b'$

$\Rightarrow ab \equiv a'b' \pmod n$

These Q1, 2. allow us to speak about adding or multiplying congruence classes using the rules.

$[a] + [b] := [a+b]$

$[a] \cdot [b] := [ab]$

and it doesn't matter which representatives are used.

Caution: not all arithmetic rules will pass across to $\mathbb{Z}_n$ = set of cong. classes. mod n

if $a \equiv a' \pmod n$

Q4. $\forall c \in \mathbb{Z}$. $ac \equiv a'c \pmod n$

But what about going the other direction

Q? If $ac \equiv a'c \pmod{n}$
does this imply that
$a \equiv a' \pmod{n}$ <u>NO.</u>

Consider.

$$20 \equiv 35 \pmod{15}.$$

does this $\Rightarrow$ $4 \equiv 7 \pmod{15}$?.

NO. $15 \nmid 4-7$. $4 \equiv 7 \pmod{3}$

However, we can cancel factors but the modulus may change.

<u>Theorem 4.3</u>.

If $xc \equiv yc \pmod{m}$

then $x \equiv y \pmod{m/d}$

where $d = \gcd(c, m)$.

So in particular if $\gcd(c, m) = 1$
then $x \equiv y \pmod{m}$

Return to this concept next week in group theory.

Theorem 4.4 Exercise

Dealing with large integers

Ex4.1

Q1. Show that $41 \mid 2^{20} - 1$

i.e. show that $2^{20} - 1 \equiv 0 \pmod{41}$

$$2^5 = 32 \equiv -9 \pmod{41}$$

$$2^{10} \equiv (2^5)^2 \equiv (-9)^2 \equiv 81 \equiv 40 \pmod{41}$$
$$\equiv -1 \pmod{41}$$

$$2^{20} \equiv (2^{10})^2 \equiv (-1)^2 \equiv 1 \pmod{41}$$

$$\Rightarrow \quad 2^{20} - 1 \equiv 0 \pmod{41}.$$

Q2 What remainder is left after dividing $\sum_{n=1}^{100} n!$ by 12?

i.e. $$\sum_{n=1}^{100} n! \equiv r \pmod{12}$$

$$1! + 2! + 3! + 4! + 5! + 6! + \cdots + 100! = r \pmod{12}$$

$$1 + 2 + 6 + \underset{2\times 12}{\underset{\uparrow}{24}} + \underset{10\times 12}{\underset{\uparrow}{120}} + \dots + 100! \equiv$$

$$\equiv 1 + 2 + 6 + 0 + 0 + 0 \dots 0 \; 0$$

$$\equiv 9 \pmod{12}$$, as all $n!$ for $n \geq 4$ contains a factor of 12.

Q.

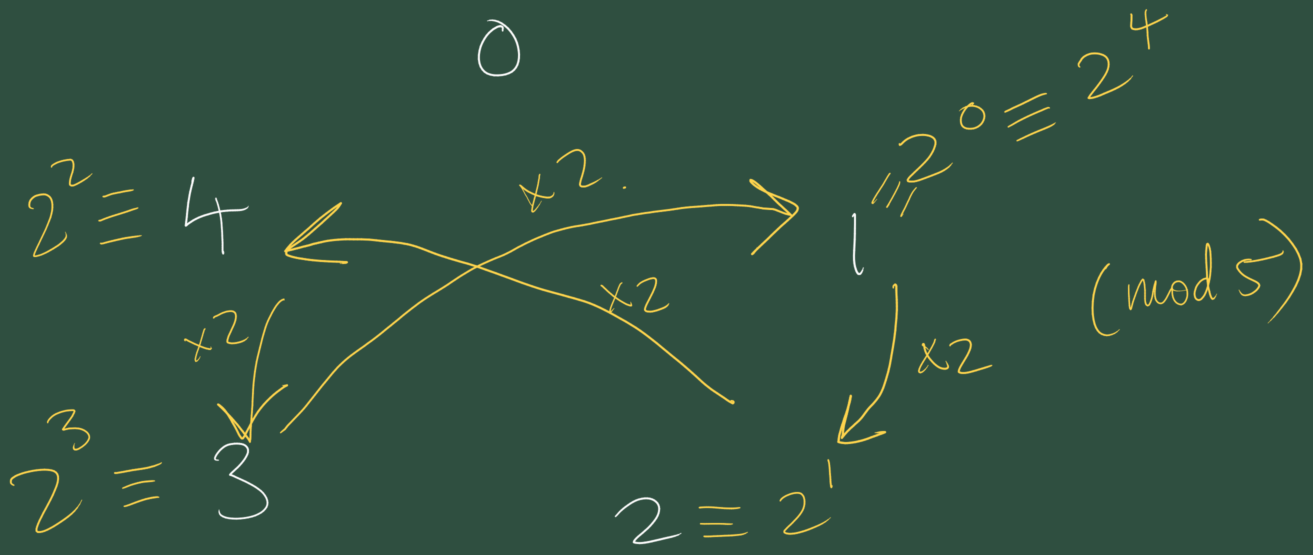
What remainder is left after dividing 2027^{2026} by 5?

$$2027^{2026} \equiv ? \pmod 5.$$

$$2027^{2026} \equiv 2^{2026} \pmod 5$$

, since $2027 \equiv 2 \pmod 5$

0



$$2027^{2026} \equiv 2^{2026} \pmod 5$$

$$\equiv 2^{\underline{2}} \equiv 4 \pmod{5}.$$

since $2026 \equiv \underline{2} \pmod 4$