Congruence relation and modular arithmetic.

Motivating example

Chap 3.

Q6. Claim: For prime numbers $p \geq 5$.

p^2+2 is never prime.

p 5, 7, 11, ...

p^2+2 27, 51, 123, ... all seem composite.

How to prove this?

Hint: Consider dividing p by 6.

Let p be a prime ≥ 5 what effect does this condition have?

$p = 6q + r$

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

$r = 0, 2, 4$ would imply $2 | p$

$r=3$ " " $3 \mid p$

So $\boxed{p = 6q + r}$, $r = 1$ or 5.

By focusing on the remainders, we've represented the infinite number of possibilities for prime numbers by just two case

We can prove the claim using this

If $p = 6q+1$ then

$$p^2+2 = (6q+1)^2+2$$
$$= 36q^2+12q+3$$
$$= 3(12q^2+4q+1)$$

So p^2+2 is not prime.

Similarly. If $p = 6q+5$

$$p^2+2 = 36q^2+60q+27$$
$$= 3(12q^2+20q+9).$$

So p^2+2 is not prime.

Treating integers according to

their remainders after division by 6 is known as "modular arithmetic modulo 6."

<u>Def 4.1</u> Congruence relation.
$a, b, n \in \mathbb{Z}, \quad n > 0$

"a is congruent to b modulo n"

means $\quad n \mid a-b$

and the notation

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

modulos

<u>Theorem 4.1.</u>

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

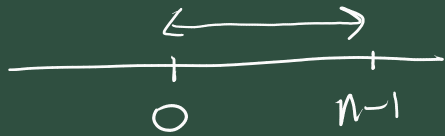
$a = q_1 n + \boxed{r}$ same.
$b = q_2 n + \boxed{r}$

<u>Proof</u> Assume $a \equiv b \pmod{n}$

i.e. $n \mid a-b$

$n \mid (q_1 n + r_1) - (q_2 n + r_2)$

$$\iff n \mid \underbrace{(q_1-q_2)n} + (r_1-r_2)$$



$$\iff n \mid r_1 - r_2, \quad \text{but } 0 \le r_1, r_2 < n$$

$$\iff r_1 = r_2$$

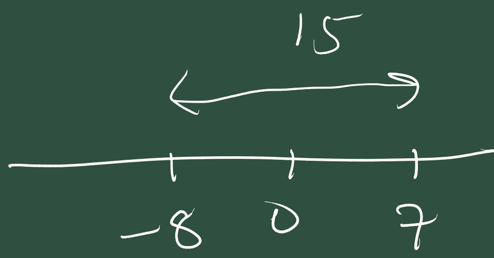
<u>Examples</u>

$7 \equiv 1 \pmod 6$ & $7 \equiv 1 \pmod 3$

$27 \equiv 3 \pmod 6$

but $7 \not\equiv 1 \pmod 5$

$7 \equiv 2 \pmod 5$



$7 \equiv -8 \pmod 5$

Congruence modulo n is a <u>binary relation</u> on $\mathbb{Z}$.

in fact its an <u>equivalence</u>

relation on $\mathbb{Z}$

Def 4.2 A binary relation $\sim$ on X (so this forms statements $x \sim y$ for $x, y \in X$). is an equivalence relation iff its reflexive, symmetric, and transitive.

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

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

Transitivity $\forall x, y, z \in X$

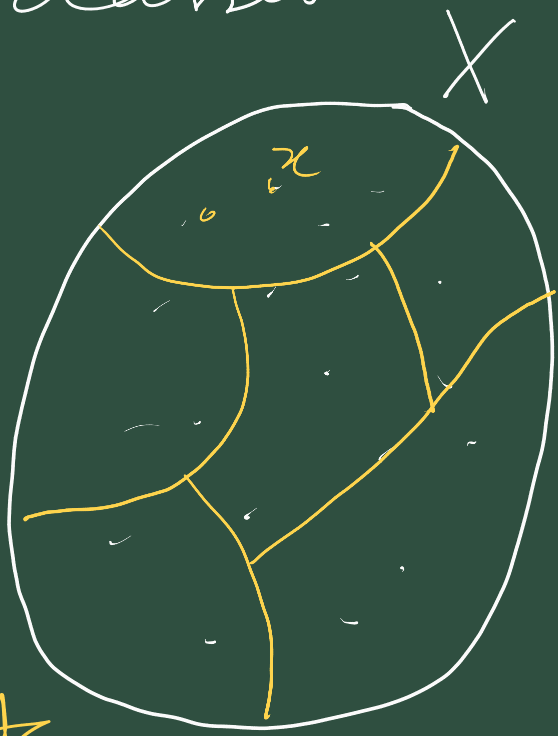
$$(x \sim y,\ y \sim z) \Rightarrow x \sim z$$

Equivalence relations allow us to group the elements of X into equivalence classes (subsets of X)

$$[x] = \{ y \in X : x \sim y \}$$

the equivalence class of x.

and in fact X is <u>partitioned</u> by these equivalence classes.



A partition of X is a system P of non-empty subsets of X

- $\bigcup_{S \in P} S = X$
- P consists of disjoint sets.

$\forall\, S, T \in P \quad S = T$ or $S \cap T = \phi$

<u>Theorem 4.2</u>

For a fixed modulus n, congruence modulo n is an equivalence relation on $\mathbb{Z}$.

<u>Proof</u>: <u>Reflexivity</u>:

Remember $\quad n \mid 0$

$\Rightarrow n \mid z - z \quad$, for any $z \in \mathbb{Z}$.

so $\quad z \equiv z \pmod{n.}$

<u>Symmetry</u>

Assume $\underline{x \equiv y}$ $(\bmod n)$

$\implies n \mid x-y$

$\implies n \mid -(x-y)$

$\implies n \mid y-x$

$\implies \underline{y \equiv x \pmod{n}}$.

<u>Transitivity</u> Assume $x \equiv y$, $y \equiv z \pmod{n}$

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

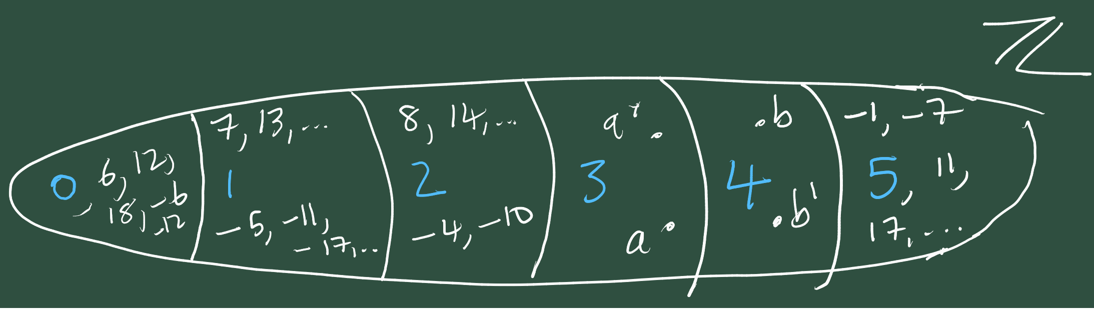
$\implies n \mid (x-y)+(y-z)$,

$\implies n \mid x-z$

$\implies x \equiv z \pmod{n}$

So $\equiv \pmod{n}$ is an equivalence relation. It's equivalence classes are called congruence classes.

eg. modulus $n=6$.



Gives a way making infinite integers into a finite set, in a sense.

Ex 4.1 The existing arithmetic on $\mathbb{Z}$, its addition and multiplication, "fits well" with the congruence relation.

For a fixed modulus m. Let $a, a', b, b' \in \mathbb{Z}$ satisfy $a \equiv a'$, $b \equiv b' \pmod{m}$

1. $a+b \equiv a'+b' \pmod{m}$.

Assume $a \equiv a'$, $b \equiv b' \pmod{m}$

$\Rightarrow m \mid a - a'$, $m \mid b - b'$

$$(a+b) - (a'+b') = (a-a') + (b-b')$$

$\Rightarrow m \mid (a+b) - (a'+b')$, as it is a lin. comb. of things divisible by m.

2. $ab \equiv a'b' \pmod{m}$

Pf:

$$ab - a'b' = (a-a')(b-b') - 2a'b' + ab' + a'b$$

$$= (a-a')(b-b') + b'(a-a')$$

$+ a'(b-b')$.

This RHS is clearly divisible by m, as it's a combination $a-a'$, $b-b'$

so $m \mid ab - a'b'$

$\Longrightarrow ab \equiv a'b' \pmod{m}$

Similar proof techniques can be given for 3–6.

Consider 6. Let $c \in \mathbb{Z}$.

$$a \equiv a' \Longrightarrow ac \equiv a'c \pmod{m}$$

$\overset{?}{\underset{?}{\Longleftarrow}}$ NO.

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

but $4 \not\equiv 7 \pmod{15}$

In fact, factors can be cancelled from a congruence, but the modulus may have to change.

<u>Theorem 4.3</u>

If $xc \equiv yc \mod m$.

then $x \equiv y \mod \left(\frac{m}{d}\right)$

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

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

$5 \cdot 4 \equiv 5 \cdot 7$

$\gcd(5, 15) = 5 = d$

$\Rightarrow \quad 4 \equiv 7 \pmod 3$

In particular if $\gcd(c, m) = 1$

then $xc \equiv yc \pmod m$

$\Rightarrow x \equiv y \pmod m$

<u>Example 4.1</u>.

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

Congruence relation can allow us to show things about large integers without directly evaluating them.

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

$$(2^5)^2 = 2^{10}$$

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

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

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

---

2. What remains after dividing

$$\sum_{n=1}^{100} n! \quad \text{by } 12 \text{ ?}$$

$$\sum_{n=1}^{100} n! = 12q + r \quad , \quad r = 0, 1, \dots, 11$$

$$\Leftrightarrow \quad \sum_{n=1}^{100} n! \equiv r \pmod{12}$$
$$0 \le r < 12$$

Solve for r.

$$\sum_{n=1}^{100} n! = 1! + 2! + 3! + 4! + 5! + 6! + \dots + 99! + 100!$$

$$\equiv 1 + 2 + 6 + 0 + 0 + \dots + 0 + 0 \pmod{12}$$

$$\equiv 9 \pmod{12}$$

, since $m!$ for $m \geq 4$, has factors 4 and 3 and so divisible by 12.

<u>Ex4.2</u>

Q5. Consider 2012^{2012}, divided by 5.

What's the remainder?

$$2012^{2012} = 5q + r, \quad r = 0, 1, 2, 3, 4.$$

$$2012^{2012} \equiv r \pmod 5$$

$0 \leq r < 5$

What's r?

$$2012^{2012} \equiv \underline{2^{2012}} \pmod 5$$

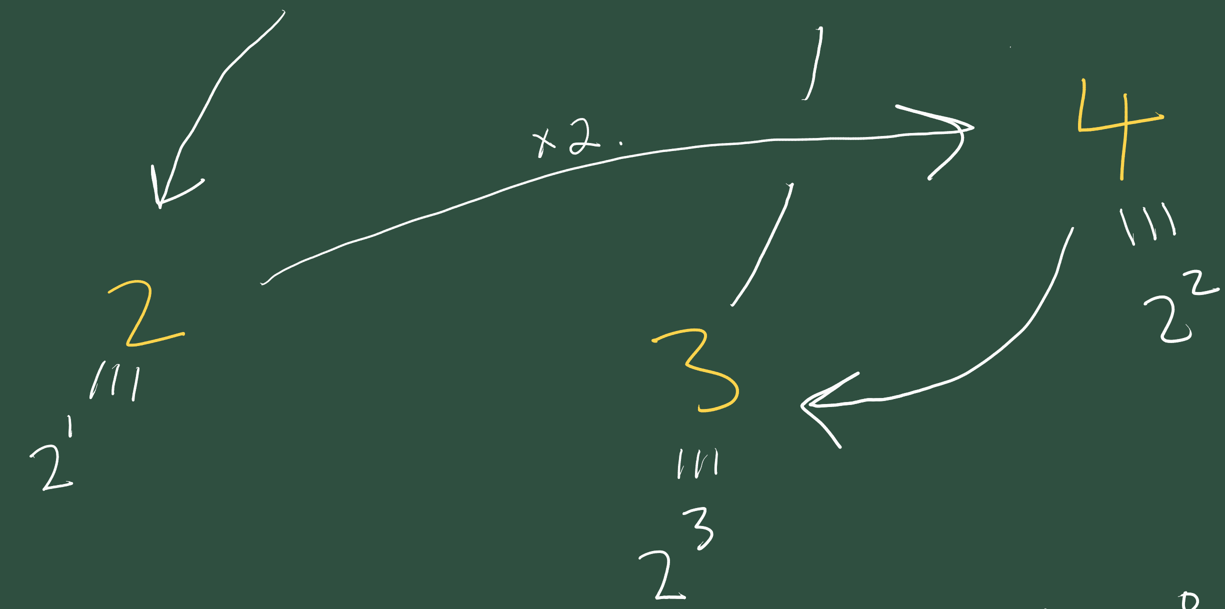
, since $2012 \equiv 2 \pmod 5$

$\times 2$

$1 \equiv 2^0 \equiv 2^4$

O

(mod 5)



Taking 2012 steps, starting from $1 \equiv 2^0$, around this diagram, will finish at $1 \equiv 2^{2012}$, because

$$2012 \equiv 0 \pmod 4$$

$$\Rightarrow 2^{2012} \equiv 1 \pmod 5$$