Section 4.1 - Congruences

- $\underbrace{6x + 15y}_{\text{LHS is mult. of 3}} = \underbrace{83}_{\text{RHS is not}}$ → no solns.

- Show that no integer in the seq.

  $$11, 111, 1111, 11111, \dots$$

  is a perfect square

Definition / Exs

Def: Let $m \in \mathbb{Z}_{>0}$. For any $a, b \in \mathbb{Z}$, we say that <u>a is congruent to b modulo m</u> if $m \mid (a-b)$

Notation: if a is congruent to b modulo m we write $a \equiv b \mod m$

\equiv   \mod or \pmod

Exs: $22 \equiv 7 \mod 15$ because $15 \mid (22-7)$

$-3 \equiv 30 \mod 11$ because $11 \mid (-3-30)$

$91 \equiv 0 \mod 13$ because $13 \mid (91-0)$

Aside: In other fields/classes, you may have seen "mod m" as a function

This is not how mod is used in this class/math in general

Avoid writing "9 mod 4" in this class

Ex: $a \equiv 1 \mod 4$ iff $4 \mid a-1$

iff $\exists k : 4k = a-1$

$a = 1+4k$

Previously: "a is of the form $1+4k$"

Now: $a \equiv 1 \mod 4$

$1+4k \longrightarrow$ arithmetic progression

Equivalence Properties

Thm. Let $m > 0$. Then for all $a, b, c \in \mathbb{Z}$

① (Reflexive property): $a \equiv a \mod m$

② (Symmetric property): if $a \equiv b \mod m$
then $b \equiv a \mod m$

③ (Transitive property): if $a \equiv b \mod m$
and $b \equiv c \mod m$, then $a \equiv c \mod m$

Pf: Worksheet (week 6)

Def: This means that congruence mod m is
an "equivalence relation"

above 3 props.

Thm: Let $m > 0$, $a, b, c \in \mathbb{Z}$. Suppose
$a \equiv b \mod m$. Then

① $a + c \equiv b + c \mod m$

② $a - c \equiv b - c \mod m$

③ $ac \equiv bc \mod m$

Pf of 3 : Suppose $a \equiv b \mod m$

Then $m \mid a-b$ so there exists $k \in \mathbb{Z}$

with $mk = a-b$

Goal Show $m \mid ac - bc$

Note $ac - bc = c(a-b) = cmk$

So $m \mid ac - bc \rightarrow ac \equiv bc \mod m$

Q : How do we divide? (mod m)

Answer should look something like,

"if $ac \equiv bc \mod m$, then $a \ ? \ b$"

Ex: $100 \equiv 20 \mod 10$

Note $5 \, 20 \equiv 5 \cdot 4 \mod 10$

Q1: Can we cancel 5?

is $20 \equiv 4 \mod 10$?

No - $20 - 4 = 16$ not div. by 10

Note: $20 \equiv 4 \mod 2$

Why is $100 \equiv 20 \mod 10$?

$$100 - 20 = 8 \cdot 10$$

$$\downarrow$$

$$\frac{100 - 20}{5} = \frac{8 \cdot 10}{5}$$

$$20 - 4 = 8 \cdot \frac{10}{5}$$

More generally: Suppose $ac \equiv bc \mod m$

Then $ac - bc = mk$ for some $k \in \mathbb{Z}$

So $$a - b = \frac{mk}{c} = \underbrace{\frac{m}{(m,c)}}_{\in \mathbb{Z}} \cdot \frac{(m,c)}{c} \underbrace{k}_{\in \mathbb{Z}}$$

$$\rightarrow \frac{c}{(m,c)} \cdot (a - b) = \frac{m}{(m,c)} k$$

Observe that $\frac{c}{(m,c)}$ and $\frac{m}{(m,c)}$ are rel. prime

Ex: $c = 2^3 \cdot 3^5 \cdot 7 \qquad m = 2^1\, 3^2 \cdot 11$

$$(m,c) = 2^1 \cdot 3^2$$

$$\frac{c}{(m,c)} = 2^2 \cdot 3^3 \cdot 7 \qquad \frac{m}{(m,c)} = 11$$

In particular, $\frac{m}{(m,c)} \,\Big|\, a-b$

Hence $a \equiv b \mod \frac{m}{(m,c)}$

Thm: If $ac \equiv bc \mod m$, then
$$a \equiv b \mod \frac{m}{(m,c)}$$

Ex: $100 \equiv 20 \mod 10$

$$5 \cdot 20 \equiv 5 \cdot 4 \mod 10$$

$m = 10,\ c = 5 \longrightarrow (m,c) = 5$

$20 \equiv 4 \mod 2$

Note: If c and m are rel. prime you can always divide by c modulo m.

Addendum: $21 \equiv 9 \mod 4 \longrightarrow 7 \equiv 3 \mod 4 \longrightarrow$ Q. $\div 3$ again?

If $(c, m) = 1$, so now we have

$$ac \equiv bc \mod m \longrightarrow a \equiv b \mod m$$

The Point

Classify integers into easier-to-understand categories

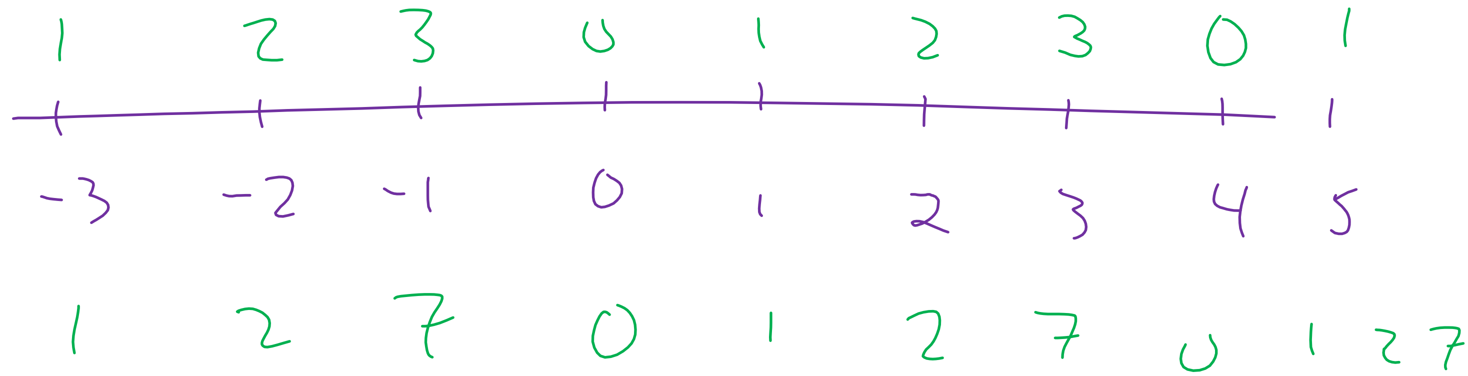
Ex: mod 4

$\dots \equiv -8 \equiv -4 \equiv 0 \equiv 4 \equiv 8 \dots \mod 4$

$-7 \equiv -3 \equiv 1 \equiv 5 \equiv 9 \dots \mod 4$

$-6 \equiv -2 \equiv 2 \equiv 6 \equiv 10 \dots \mod 4$

$-5 \equiv -1 \equiv 3 \equiv 7 \equiv 11, \dots \mod 4$



Note: every integer n has exactly one of the following:

$$n \equiv 0 \mod 4$$
$$n \equiv 1 \mod 4$$
$$n \equiv 2 \mod 4$$
$$n \equiv 7 \mod 4$$

Def: A set S is a <u>complete set of residues modulo m</u> if every $n \in \mathbb{Z}$ has $n \equiv x \mod m$ for exactly one $x \in S$

Exs: $\{0, 1, 2, 3\}$ is a complete set of residues mod 4

$\{0, 1, 2, 7\}$ " "

Nonex: $\{0, 1, 2, 5\}$ is not a complete set of residues mod 4

7 is not congruent to any of 0, 1, 2, or 5 mod 4

Non ex: $\{0, 1, 2, 3, 7\}$ is not a complete set of residues mod 4

Note: $11 \equiv 7 \mod 4$

$11 \equiv 3 \mod 4$

$0 + 4\mathbb{Z} = 4 + 4\mathbb{Z}$

Def $\bar{n}$ to be $n + 4\mathbb{Z} \to \bar{0} = \bar{4}$

Ex: $\{0, 1, 2, \ldots, m-1\} = \mathbb{Z}/m\mathbb{Z}$ is a complete set of residues mod m

Ex: $\left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}\right\}$ is a complete set of residues mod m if m is odd.

Ex: $\{-3, -2, -1, 0, 1, 2, 3\}$ is a complete set of residues mod 7

Analogy: If U is a finite dimensional vector space, V has a basis $v_1, \dots, v_n$.

"You can get to every $v \in U$ uniquely using $v_1, \dots, v_n$"

Complete sets of residues: "You can get to every $n \in \mathbb{Z}$ uniquely using your set of residues mod m"

Fact: If S is a complete set of residues mod m, then there is a unique function $f : \mathbb{Z} \to S$ s.t. $f(n) = f(j)$ if and only if $n \equiv j \mod m$