Warm-Up: Find integers x and y such that

$$51x - 13y = 1$$

Last time: $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$

$a \equiv b \mod m \iff$ a and b leave the same remainder when divided by m.

$\hookrightarrow m \mid (b-a)$

Cor: Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$.

(a) There is a unique integer r such that $0 \le r \le m-1$ and $a \equiv r \mod m$. Specifically, r is the remainder left upon dividing a by m.

(b) $a \equiv 0 \mod m$ if and only if $m \mid a$.

Properties

Thm: Let $m \in \mathbb{N}$.

(a) For all $a \in \mathbb{Z}$, $a \equiv a \bmod m$ [Reflexive]

(b) For all $a, b \in \mathbb{Z}$, if $a \equiv b \bmod m$, then $b \equiv a \bmod m$. [Symmetric]

(c) For all $a, b, c \in \mathbb{Z}$, if $a \equiv b \bmod m$ and $b \equiv c \bmod m$, then $a \equiv c \bmod m$ [Transitive]

Proof: HW 15.

Together, these properties say that congruence mod m is an <u>equivalence relation</u>.

Equivalence relations give a notion of "sameness."

<u>Other examples</u>:
- Equality (of integers, real numbers, functions, ...)
- Congruence of triangles
- Similarity of triangles

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

(a) $a + c \equiv b + d \mod m$.
(b) $a - c \equiv b - d \mod m$.
(c) $ac \equiv bd \mod m$.

Proof: HW 15.

Ex: When $m = 2$, every $a \in \mathbb{Z}$ satisfies exactly one of

- $a \equiv 0 \mod 2 \iff a$ is even
- $a \equiv 1 \mod 2 \iff a$ is odd

So when we do arithmetic mod 2, we can replace every integer by 0 or 1.

We have

$0 + 0 = 0$	$0 \cdot 0 = 0$
$0 + 1 = 1$	$0 \cdot 1 = 0$
$1 + 0 = 1$	$1 \cdot 0 = 0$
$1 + 1 = 2 \equiv 0 \mod 2$	$1 \cdot 1 = 1$

So we have the following + and · tables:

$+$ mod 2	0	1
0	0	1
1	1	0

$\cdot$ mod 2	0	1
0	0	0
1	0	1

This recovers

$+$	even	odd
even	even	odd
odd	odd	even

$\cdot$	even	odd
even	even	even
odd	even	odd

<u>Ex</u>: What is the remainder when $22 \cdot 19$ is divided by 3?

<u>Recall</u>: Remainder is the unique $r \in \mathbb{Z}$ such that $0 \leq r \leq 2$ and $22 \cdot 19 \equiv r \mod 3$.

$$22 \equiv 1 \mod 3, \quad 19 \equiv 1 \mod 3,$$

So
$$\begin{aligned} 22 \cdot 19 &\equiv 1 \cdot 1 \mod 3 \\ &\equiv 1 \mod 3, \end{aligned}$$

meaning $22 \cdot 19$ leaves a remainder of 1 when divided by 3.

<u>Ex</u>: What is the remainder when
$$(754 + 1083) \cdot 17$$
is divided by 5?

$$\begin{aligned} (754 + 1083) \cdot 17 &\equiv (4 + 3) \cdot 2 \mod 5 \\ &\equiv 7 \cdot 2 \mod 5 \\ &\equiv 2 \cdot 2 \mod 5 \\ &\equiv 4 \mod 5 \end{aligned}$$

So the remainder is 4.