Warm-Up: Find integers x and y such that

$$58x - 13y = 1$$

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 $0 \leq r \leq m-1$ 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 $m \mid a$.

Ex: $m = 8$, $a = 29$.

Then $29 \equiv 5 \mod 8$.

Warning: "mod m" has no meaning outside of the sentence $a \equiv b \mod m$.

Properties

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

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

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

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

Proof: HW 14.

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, ...)
- Logical equivalence of sentences
- Congruence of triangles
- Similarity of triangles

<u>Thm</u>: Let $m \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$.
Suppose $a \equiv b \bmod m$ and $c \equiv d \bmod m$.
Then

(a) $a + c \equiv b + d \bmod m$.

(b) $a - c \equiv b - d \bmod m$.

(c) $ac \equiv bd \bmod m$.

<u>Proof</u>: HW 14.