Modular arithmetic

congruence mod k: Let k be any positive integer.
$a, b \in \mathbb{Z}$ are congruent mod k ($a \equiv b \pmod{k}$)
iff $k \mid (a-b)$.

they differ by a factor of k.

not operation

~~$a \equiv b \cdot \mod k$~~

$a \equiv_k b$ congruent under mod k.

ex) $17 \equiv 5 \pmod{12}$ true because $12 \mid 17-5$
$5 \equiv 17 \pmod{12}$ $12 \mid 5-17$

order doesn't matter.

$38 \equiv 3 \pmod{7}$ $7 \mid 38-3$

$38/7$ gives remainder of 3.

↓

not remainder we saw yesterday

$b > k$

ex) For integers a, b, c, d, k with $k > 0$,
if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$, then
prove $ac \equiv bd \pmod{k}$.

Let $a, b, c, d \in \mathbb{Z}$, $k \in \mathbb{Z}^+$.

Suppose $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$.

then, by the defn of congruence mod k, $k \mid a-b$ and $k \mid c-d$.

if $k \mid a-b$, $k \mid c(a-b) = k \mid ac-bc$

if $k \mid c-d$, $k \mid b(c-d) = k \mid bc-bd$

} not super intuitive, takes practice.

then, $k \mid [ac - bc + bc - bd) = k \mid ac - bd$. So $ac \equiv bd \pmod{k}$

Goal: $ac \equiv bd \pmod{k} \leftrightarrow$ $k \mid ac - bd$.

equivalence classes

$17 \equiv 5 \pmod{12}$

$29 \equiv 5 \pmod{12}$

$41 \equiv 5 \pmod{12}$

$5 \equiv 5 \pmod{12}$

$-7 \equiv 5 \pmod{12}$

$\vdots$

in $\mathbb{Z}_{12}$ (we're looking at arithmetic congruent to mod 12)

12 classes:

$[0] = \{12, 24, 36, -12 \dots\}$

$[1]$

$\vdots$

$[5] = \{41, 17, -7, 29 \dots\}$

$\vdots$

$[11]$

all $\mathbb{Z}$ in one of these classes

compute $41 \cdot 36$ in $\mathbb{Z}_{12}$.

$[5] \cdot [0] = [5 \cdot 0] = [0]$

$[x] + [y] = [x+y]$

$[x] \cdot [y] = [xy]$