On HW you proved:

<u>Prop'n</u> ("Modular arithmetic lemma")

Fix $n \in \mathbb{N}$, $a, b, k, k' \in \mathbb{Z}$. Assume $a \equiv b$, $k \equiv k' \pmod{n}$

<u>Then</u>: ① $a + k \equiv b + k' \pmod{n}$

② $ak \equiv bk' \pmod{n}$

<u>Ex's</u> ① $6 \equiv 21 \pmod{5}$ and $12 \equiv 2 \pmod{5}$

<u>So must be</u>: $6 + 12 \equiv 21 + 2 \pmod{5}$

and indeed can check $18 \equiv 23 \pmod{5}$

$\equiv 3 \pmod{5}$

Also: $6 \cdot 12 \equiv 21 \cdot 2 \pmod{5}$ by prop'n

and indeed: $72 \equiv 42 \pmod{5}$

$\equiv 2$

② Prop'n says we can manipulate congruences w/ $\equiv$ like equations w/ $=$ with respect to $+$ and $\times$.

e.g. if $x, y \in \mathbb{Z}$ and $x \equiv y \pmod{7}$

<u>then</u> $x + 3 \equiv y + 3 \pmod{7}$

and $3x \equiv 3y \pmod{7}$

or even $x + 3 \equiv y + 10 \pmod{7}$ since $3 \equiv 10 \pmod{7}$

$3x \equiv 10y \pmod{7}$

③ Can also "reduce expressions mod n"

e.g. $17x + 23 \equiv 2x + 3 \pmod 5$ for any $x \in \mathbb{Z}$

since $17 \equiv 2$ and $23 \equiv 3 \pmod 5$

④ Using these various manipulations we can "solve congruency"

e.g: Find all $x \in \mathbb{Z}$ s.t.

$$652x \equiv x + 23 \pmod 5$$

Sol'n: reduces to: $2x \equiv x + 3 \pmod 5$

(since $652x \equiv 2x$
$x + 23 \equiv x + 3 \pmod 5$)

$\Leftrightarrow 2x + (-x) \equiv x + 3 + (-x) \pmod 5$

$\Leftrightarrow x \equiv 3 \pmod 5$

so set of solutions is $[3]_5 = \{\ldots, -2, 3, 8, \ldots\}$

(note: shows why subtraction is legal too: just adding a negative).

OTOH, division on both sides of $\equiv$ is not allowed in general.

ex: ① Fix $x \in \mathbb{Z}$. Sps $2x \equiv 1 \pmod 3$

writing $x \equiv 1/2 \pmod 3$

is meaningless ($1/2 \notin \mathbb{Z}$)

② Observe: $15 \equiv 21 \pmod 6$ (15)

but if we "divide both sides by 3" we get:

$$5 \equiv 7 \pmod 6$$

which is false.

③ Observe: $8 \equiv 22 \pmod 7$

if we divide both sides by 2, we get: $4 \equiv 11 \pmod 7$

which is true

What gives? Reason is: 2 has a multiplicative inverse in $\mathbb{Z}/7\mathbb{Z}$ whereas 3 has no such inverse in $\mathbb{Z}/6\mathbb{Z}$.

$\rightsquigarrow$ more later.

Exponentiation also allowed over $\equiv$:

Prop'n: Fix $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$ and $k \in \mathbb{N}$.

if $a \equiv b \pmod n$

then $a^k \equiv b^k \pmod n$

Pf: follows immediately from mod arithmetic lemma + induction.

__why__: if $a \equiv b \pmod{n}$

then $a^2 \equiv b^2 \pmod{n}$

$\vdots$

$a^k \equiv b^k \pmod{n}$. ✓

__Ex's__: ① Since $7 \equiv 2 \pmod{5}$

$\Rightarrow 7^3 \equiv 2^3 \pmod{5}$

$\equiv 8 \pmod{5}$

$\equiv 3 \pmod{5}$

get this w/o actually computing 7^3.

② Find the last digit of $2033 \cdot 719 + 27$.

__sol'n__ last digit is exactly the remainder when divided by 10.

__Observe__: $2033 \cdot 719 + 27 \equiv 3 \cdot 9 + 7 \pmod{10}$

$\equiv 27 + 7 \pmod{10}$

$\equiv 34 \pmod{10}$

$\equiv 4 \pmod{10}$

$\Rightarrow$ last digit is 4

And indeed: $2033 \cdot 719 + 27 = 1{,}461{,}754$.

(3) Find the remainder of 2^{37} when divided by 47. (20)

Sol'n: $2, 4, 8, 16, 32, 64 = 47 + 17$

$$64 = 2^6$$

So $2^6 \equiv 17 \pmod{47}$

$$\Rightarrow 2^{12} = (2^6)^2 \equiv (17)^2 \pmod{47}$$

$$(17)^2 = 289 = 47 \cdot 6 + 7$$

$$\equiv 7 \pmod{47}$$

$$\Rightarrow 2^{24} = (2^{12})^2 \equiv 7^2 \pmod{47}$$

$$\equiv 49 \pmod{47}$$

$$\equiv 2 \pmod{47}$$

now: $2^{37} = 2^{24} \cdot 2^{12} \cdot 2$

$$\equiv 2 \cdot 7 \cdot 2 \pmod{47}$$

$$\equiv 28 \pmod{47}$$

So 28 is the remainder

Multiplicative inverses in $\mathbb{Z}/n\mathbb{Z}$

Def'n Fix $n \in \mathbb{N}$, $a \in \mathbb{Z}$. We say a has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$ iff $\exists b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$

If such a b exists, we sometimes write $b = a^{-1}$.

not unique, but unique up to $\equiv$-class.

ex: 3 has a multiplicative inverse in $\mathbb{Z}/7\mathbb{Z}$ since $3 \cdot 5 = 15 \equiv 1 \pmod{7}$

Prop'n Fix $n \in \mathbb{N}$, $a \in \mathbb{Z}$. Then a has a mult. inv. in $\mathbb{Z}/n\mathbb{Z}$ iff $\gcd(a,n) = 1$

Pf. ($\Rightarrow$) assume $\exists b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$

- then $n \mid 1 - ab$
- i.e. $\exists k \in \mathbb{Z}$ $kn = 1 - ab$
- so $kn + ab = 1$
- hence 1 is a linear combo of a, n

$\Rightarrow \gcd(a,n) = 1$ by Bezout.

($\Leftarrow$) Now suppose $\gcd(a,n)=1$.
Then, by Bezout, $\exists b,k \in \mathbb{Z}$ s.t.

$$ab + nk = 1$$

so $nk = 1-ab$

$\Rightarrow n \mid 1-ab \Rightarrow ab \equiv 1 \pmod{n}$

Ex's ① $5x \equiv 1 \pmod{21}$
has a solution, since $\gcd(5,21)=1$.
indeed $x = 17$ works since
$5 \cdot 17 = 85 = 84+1 \equiv 1 \pmod{21}$

↳ any $x \in \mathbb{Z}$ congruent to 17 must also work, e.g. $x = -4, 38, \ldots$ work too.

Check: $5(-4) = -20 = 21(-1)+1$
$\equiv 1 \pmod{21}$.

↳ in fact: set of solutions must be exactly: $[17]_{21}$: if $x \in [17]_{21}$
then $5x \equiv 5 \cdot 17 \equiv 1 \pmod{21}$
and if $5x \equiv 1 \pmod{21}$ then $5x \equiv 5 \cdot 17 \pmod{21}$
$\Rightarrow 17 \cdot 5x \equiv 17 \cdot 5 \cdot 17 \Rightarrow x \equiv 17$

So might write:

$$[5]_{21} \cdot [17]_{21} \text{ " = " } [1]_{21}$$

in the sense that

$\forall a \in [5]_{21}$; $\forall b \in [17]_{21}$

we have $ab \equiv 1 \pmod{21}$

i.e. $ab \in [1]_{21}$

(2) The congruence $6x \equiv 1 \pmod{21}$ has <u>no</u> sol'n: such an x would be a mult inverse for 6 in $\mathbb{Z}/21\mathbb{Z}$: but $\gcd(6,21) = 3 \neq 1$ so no such inverse exists.

(3) Find all sol'ns to:

$$4x \equiv 5 \pmod{7}$$

<u>Sol'n</u>: since 7 is prime and $7 \nmid 4$ we have $\gcd(4,7) = 1$. Hence 4 has a mult. inv. in $\mathbb{Z}/7\mathbb{Z}$. Indeed 2 works: $4 \cdot 2 = 8 \equiv 1 \pmod{7}$.

<u>Idea</u>: instead of "dividing both sides" of $4x \equiv 5 \pmod 7$ by 4, can multiply by 2:

$$4x \equiv 5 \pmod 7$$
$$\Rightarrow 2 \cdot 4x \equiv 2 \cdot 5 \pmod 7$$
$$\Rightarrow x \equiv 10 \pmod 7$$
$$\equiv 3 \pmod 7$$

(and the $\Rightarrow$'s can be reversed - why?)

hence $[3]_7$ is the set of solutions!

<u>Prop'n</u>: For a given $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$, there is a sol'n to $ax \equiv b \pmod n$ iff $\gcd(a, n) \mid b$.

<u>Pf</u>: Let $\gcd(a, n) = d$

($\Rightarrow$) Assume there is a sol'n $x = l$ to $ax \equiv b \pmod n$, i.e. $al \equiv b \pmod n$

then $n \mid b - al$

$\Rightarrow \exists k \in \mathbb{Z}$ $\quad b - al = ak$

$\Rightarrow b = al + nk$

$\Rightarrow$

but a, n are both divisible by d, hence b is too.

i.e. $d \mid b$, i.e. $\gcd(a,n) \mid b$.

($\Leftarrow$) Now assume $d \mid b$, i.e. $\exists l$ s.t. $b = ld$.

By Bezout $\exists k, k'$ s.t.

$$ak + nk' = d$$

$$\Rightarrow \quad akl + nk'l = ld = b$$

$$\Rightarrow \quad nk'l = b - akl$$

$$\Rightarrow \quad n \mid b - akl$$

$$\Rightarrow \quad akl \equiv b \pmod{n}$$

$$\Rightarrow \quad x = kl \text{ is a sol'n to } ax \equiv b \pmod{n}$$

<u>Ex</u>: ① There <u>is</u> a sol'n to

$$6x \equiv 4 \pmod{8}$$

since $\gcd(6,8) = 2$ and $2 \mid 4$.

indeed $x = 2$ works: $6 \cdot 2 = 12 \equiv 4 \pmod{8}$

② There is <u>no</u> solution to $4x \equiv 3 \pmod{8}$ since $\gcd(4,8) = 4$ and $4 \nmid 3$.