Oh! How you proved:

Prop'n ("Modular arithmetic lemma")

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

Then:
1. \( a + k \equiv b + k' \pmod{\! n} \)
2. \( a k \equiv b k' \pmod{\! n} \)

Ex's:
- \( 0 \equiv 21 \pmod{\! 5} \) and \( 12 \equiv 2 \pmod{\! 5} \)
- So must be: \( 0 + 12 \equiv 21 + 2 \pmod{\! 5} \)
- and indeed can check \( 14 \equiv 23 \pmod{\! 5} \)
- \( 0 \cdot 12 \equiv 21 \cdot 2 \pmod{\! 5} \) by prop'n
- and indeed: \( 0 \equiv 42 \pmod{\! 5} \)
- \( 1 \equiv 2 \)

Prop'n says: We can manipulate congruences \( \equiv \) like equations \( = \)

with respect to + and \( \cdot \).

E.g. if \( x, y \in \mathbb{Z} \) and \( x \equiv y \pmod{\! 7} \)

Then:
1. \( x + 3 \equiv y + 3 \pmod{\! 7} \)
2. \( 3x \equiv 3y \pmod{\! 7} \)
3. \( x + 3 \equiv y + 10 \pmod{\! 7} \) since \( 3 \equiv 10 \pmod{\! 7} \)
(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.
   \[62x \equiv x + 23 \pmod{5}\]
   **Solv'n:** reduce to: \(2x \equiv x + 3 \pmod{5}\)
   (since \(62x \equiv 2x\)
   \[x + 23 \equiv x + 3 \pmod{5}\])
   \[\Rightarrow 2x + (-x) \equiv x + 3 + (-x) \pmod{5}\]
   \[\Rightarrow x \equiv 3 \pmod{5}\]
   So set of solutions is \(\mathbb{Z}_5 = \{\ldots, -2, 3, 8, \ldots\}\)
   (Note: shows why subtractions are legal too: just adding a negative).

**Note:** division on both sides of \(=\) is not allowed in general.

**Ex:** \(\circ \) Fix \(x \in \mathbb{Z}\). Sps \(2x \equiv 1 \pmod{3}\)
   writing \(x \equiv \frac{1}{2} \pmod{3}\)
   is meaningless (\(\frac{1}{2} \notin \mathbb{Z}\))
2. Observe: $15 \equiv 21 \pmod{6}$

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

We'll see more later.

Exponentiation also obeys congruence:

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

If $a \equiv b \pmod{n}$

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

Def: follows immediately from mod arithmetic lemma + induction.
why: if \( a \equiv b \pmod{n} \)
then \( a^2 \equiv b^2 \pmod{n} \)

\[ a^k \equiv b^k \pmod{n} \] \( \checkmark \)

**Ex. 5**: (i) Since \( 7 \equiv 2 \pmod{5} \)
\[ 7^3 \equiv 2^3 \pmod{5} \]
\[ = 8 \pmod{5} \]
\[ = 3 \pmod{5} \]

get this we actually
computing \( 7^3 \).

(ii) Find the last digit of \( 2033 \cdot 719 + 27 \).

So the last digit is exactly the
remainder when divided by 10.

**Observe**: \( 2033 \cdot 719 + 27 \equiv 39 + 7 \pmod{10} \)
\[ = 27 + 7 \pmod{10} \]
\[ = 34 \pmod{10} \]
\[ = 4 \pmod{10} \]

= 4 \text{ last digit is 4.}

And indeed: \( 2033 \cdot 719 + 27 = 1,461,754 \)
Find the remainder of $2^{34}$ when divided by 47.

\[
\text{So}\; \text{r} \equiv 2, 4, 8, 16, 32, 64 \equiv 47 + 17 \\
\implies 26
\]

So $26 \equiv 17 \; (\text{mod} \; 47)$

\[
\implies 2^{12} \equiv (26)^2 \equiv (17)^2 \; (\text{mod} \; 47)
\]

\[
\implies 289 \equiv 47 \cdot 6 + 7
\]

\[
\equiv 7 \; (\text{mod} \; 47)
\]

\[
\implies 2^{24} \equiv (2^{12})^2 \equiv 7^2 \; (\text{mod} \; 47)
\]

\[
\equiv 49 \; (\text{mod} \; 47)
\]

\[
\equiv 2 \; (\text{mod} \; 47)
\]

Now:

\[
2^{34} = 2^{24} \cdot 2^{12} \cdot 2
\]

\[
\equiv 2 \cdot 7 \cdot 2 \; (\text{mod} \; 47)
\]

\[
\equiv 28 \; (\text{mod} \; 47)
\]

So 28 is the remainder.
**Multiplicative inverses in \( \mathbb{Z}/n\mathbb{Z} \)**

**Defn** 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 \( 3 \cdot 5 = 15 \equiv 1 \pmod{7} \).

**Propn** 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.
\(\iff\) Now suppose \(\gcd(a, n) = 1\).

Then, by Bezout, \(\exists b, k \in \mathbb{Z}\) s.t.
\[ab + nk = 1\]
so
\[nk = 1 - ab\]
\[\Rightarrow n \mid 1 - ab \Rightarrow ab \equiv 1 \pmod{n}\]

\text{Ex's:} \(\iff 5x \equiv 1 \pmod{21}\)

has a solution, since \(\gcd(5, 21) = 1\).

Indeed \(x = 17\) works since
\[5 \cdot 17 = 85 = 34 + 1 \equiv 1 \pmod{21}\]

Any \(x \equiv 17 \pmod{21}\) must also work, e.g. \(x = -4, 38\) - work too.

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

\(\iff\) In fact: \(\{17\}\) must be exactly: \([17]_n\): if \(x \in [17]_{21}\)

then \(5x \equiv 5 \cdot 17 \equiv 1 \pmod{21}\)

and if \(5x \equiv 1 \pmod{21}\) then \(5x = 5 \cdot 17 \pmod{21}\)
\[\Rightarrow 17 \cdot 5x \equiv 17 \cdot 5 \cdot 17 \Rightarrow x \equiv 17\)
So might work:
\[ (5)_{21} \cdot (7)_{21} = (1)_{21} \]
In the sense that
\[ a \in (5)_{21}, \quad b \in (7)_{21}, \quad \text{we have } ab \equiv 1 \pmod{21} \]
i.e. \( ab \equiv 1_{21} \)

2 The congruence \( 6x \equiv 1 \pmod{21} \)
has no solution: 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 solutions to:
\[ 4x \equiv 5 \pmod{7} \]
Solution: 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: \( 4 \cdot 2 = 8 \equiv 1 \pmod{7} \).
Idea: Instead of "dividing both sides" of \(4x \equiv 5 \pmod{7}\) by \(4\),

\(\) can multiply by \(2\):

\[
4x \equiv 5 \pmod{7}
\]

\[
2 \cdot 4x \equiv 2 \cdot 5 \pmod{7}
\]

\[
x \equiv 10 \pmod{7}
\]

\[
\equiv 3 \pmod{7}
\]

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

Hence \(\{3\}\) is the set of solutions.

Prop'n: For a given \(n \in \mathbb{N}\) and \(a,b \in \mathbb{Z}\),

\(\) there is a sol'n to \(ax \equiv b \pmod{n}\)

If \(\gcd(a,n) \mid b\).

PF: Let \(\gcd(a,n) = d\)

\(\) Assume there is a sol'n \(x = e\)

to \(ax \equiv b \pmod{n}\), i.e. \(ae \equiv b \pmod{n}\)

then \(n \mid b - ae\)

\(\) \(\exists k \in \mathbb{Z} \quad b - ae = ak\)

\(\) \(b = ae + nk\)
but a, n are both divisible by d, hence b is too.

i.e. d | b, i.e. gcd(a, n) | b.

(\Rightarrow) Now assume d | b, i.e. \exists k \in \mathbb{Z},

b = kd.

By Bezout's \textit{Th,} k \in \mathbb{Z},

ak + nk'k = d

\Rightarrow ak + nk'k = ld = b

\Rightarrow nk'k = b - ak

\Rightarrow n | b - ak

\Rightarrow n | b - ak

\Rightarrow \text{gcd}(n) | b

\Rightarrow x = k \in \mathbb{Z} \text{ s.t. } \text{gcd}(n) | b \Rightarrow x = b \text{ (mod } n)\]