Integer congruence

MTH 350 -- Module 2B

If $x \equiv y \bmod 9$, then

$9|(y - x)$

$9|(x - y)$

$x|(9 - y)$

$x/y \equiv 1 \bmod 9$

To 0

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Which of these is the smallest, nonnegative integer that is congruent to 100 mod 12?

- -8
- 0
- 4
- 8
- 16
- 100
- No such number exists
- The number exists but it's not one of the above

Tc 0

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

If a, b are integers and n is a natural number, then $a \equiv b \bmod n$ if and only if

- $a|b$
- $n|a$
- a and b are both multiples of n
- a and b have the same remainder when divided by n
- None of the above

To 0

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

If $a \equiv 0 \mod n$, then

- $a | n$
- $n | a$
- $a = 0$
- $a = n$

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Proving properties of integer congruence

(a) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $(a + c) \equiv (b + d) \pmod{n}$.

Solution: *Using the definition of congruence, the given result is equivalent to the following:*

If $n \mid (a - b)$ *and* $n \mid (c - d)$*, then* $n \mid [(a + c) - (b + d)]$.

Thus, assume that $n \mid (a - b)$ *and* $n \mid (c - d)$. *Then there exist integers* j *and* k *such that* $a - b = nj$ *and* $c - d = nk$. *Simple algebra (in particular, the associative and distributive axioms) then implies that*

$$
\begin{aligned}
(a + c) - (b + d) &= (a - b) + (c - d) \\
&= nj + nk \\
&= n(j + k).
\end{aligned}
$$

Thus, $n \mid [(a + c) - (b + d)]$*, as desired.*

If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $ac \equiv bd \bmod n$.

Use a direct proof. So assume…

By definition of congruence, we can rephrase this as....

We want to show that $ac \equiv bd \bmod n$. By definition of congruence, we can rephrase this as....

[Now take the last statement and do some math!]

For every integer a, a ≡ a mod n. (I.e. integer congruence is a relation that satisfies the **reflexive property.**)

Use a direct proof. So assume…

By definition of congruence, we can rephrase this as....

We want to show that...

[Now complete the proof]

For all integers a and b, if a ≡ b mod n then b ≡ a mod n . (I.e. integer congruence is a relation that satisfies the **symmetric property.**)

Use a direct proof. So assume…

By definition of congruence, we can rephrase this as....

We want to show that...

[Now complete the proof]

For all integers a, b, and c, if a ≡ b mod n and b ≡ c mod n, then a ≡ c mod n. (I.e. integer congruence is a relation that satisfies the **transitive property.**)

Use a direct proof. So assume…

By definition of congruence, we can rephrase this as....

We want to show that...

[Now complete the proof]

BONUS PROOF

For all integers a,b and natural numbers m, if $a \equiv b \bmod n$, then $a^m \equiv b^m \bmod n$.

Question: What method of proof should we use? Can you make an outline of the proof once you've selected the method?

Recap

- **Definition of integer congruence:** Integers that are congruent mod n aren't necessarily *equal* but their difference is divisible by n.
- **Properties of integer congruence:** We proved some potentially useful algebra properties of integer congruence.
- **Equivalence relation:** We proved that "congruence mod n" is an equivalence relation on the set of integers (reflexive, symmetric, transitive).

NEXT UP: Greatest common divisors

Feedback:

http://gvsu.edu/s/1zN