CSE 311 Section 4

English Proofs & Number Theory

Announcements & Reminders

- HW2
  - Regrades open a day or two after

- HW3 due yesterday @ 11:00PM on Gradescope
  - Use late days if you need to!
  - Make sure you tagged pages on gradescope correctly

- HW4
  - Releases tonight
  - Due Friday 4/26 @11:00 PM
- Book One-on-Ones on the course homepage!

English Proofs

Writing a Proof (symbolically or in English)

- Don't just jump right in!

1. Look at the **claim**, and make sure you know:
   - What every word in the claim means
   - What the claim as a whole means

2. Translate the claim in predicate logic.

3. Next, write down the **Proof Skeleton**:
   - Where to **start**
   - What your **target** is

4. Then once you know what claim you are proving and your starting point and ending point, you can finally write the proof!

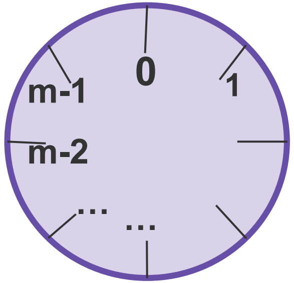
Helpful Tips for English Proofs

- Start by introducing your assumptions
  - Introduce variables with “let”
    - “Let x be an arbitrary prime number…”
  - Introduce assumptions with “suppose”
    - “Suppose that $y \in A \land y \notin B$…”
- When you supply a value for an existence proof, use “Consider”
  - “Consider $x = 2$…”
- **ALWAYS** state what type your variable is (integer, set, etc.)
- Universal Quantifier means variable must be arbitrary
- Existential Quantifier means variable can be specific

Mod

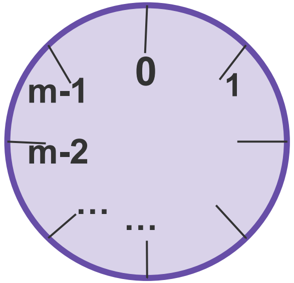
$a \equiv b \pmod{m}$

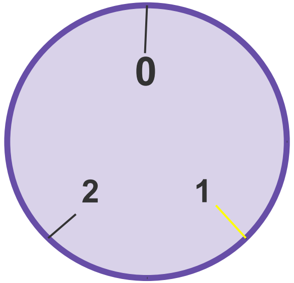
Imagine a clock with m numbers



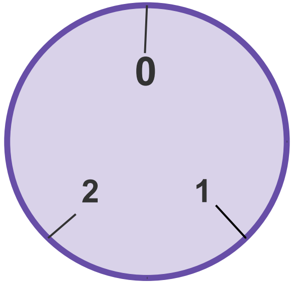
a ≡ b (mod m)

Imagine a clock with m numbers





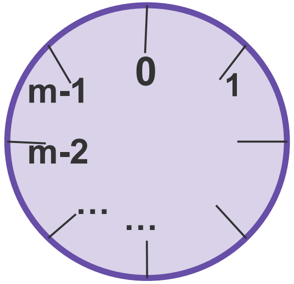
≡

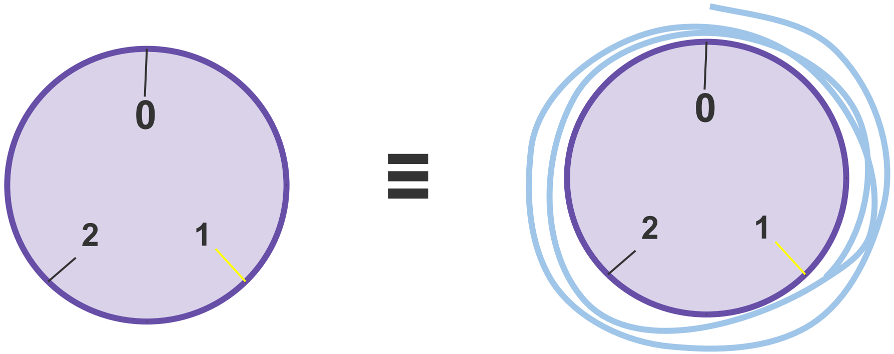


1 (mod 3) **VS** 10 (mod 3)

a ≡ b (mod m)

Imagine a clock with m numbers

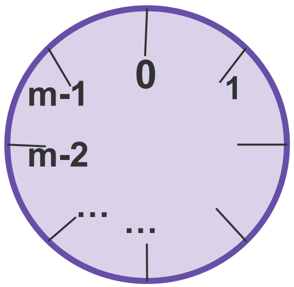


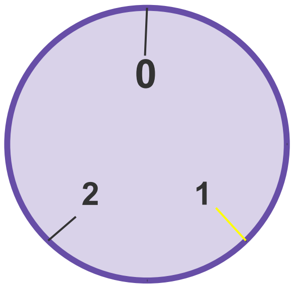


1 (mod 3) **VS** 10 (mod 3)

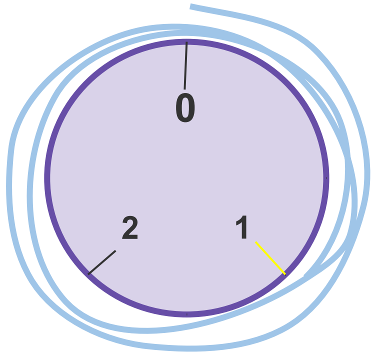
$a \equiv b \pmod{m}$

Imagine a clock with m numbers





$\equiv$



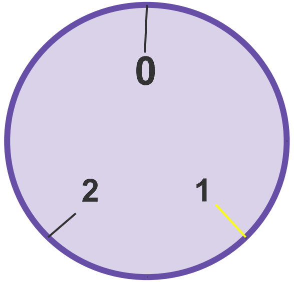
1 (mod 3) **VS** 10 (mod 3)

So we can say that **$a \equiv b \pmod{m}$** where a and b are in the same position in the mod clock

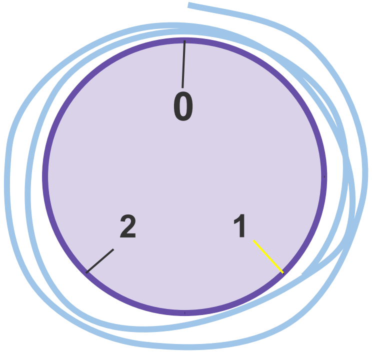
$1 \equiv 10 \pmod{3}$

Divides

What if we "unroll" this clock?



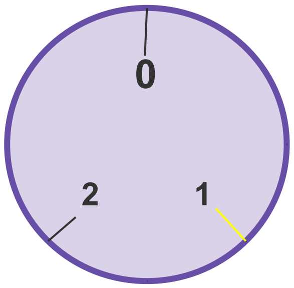
$\equiv$



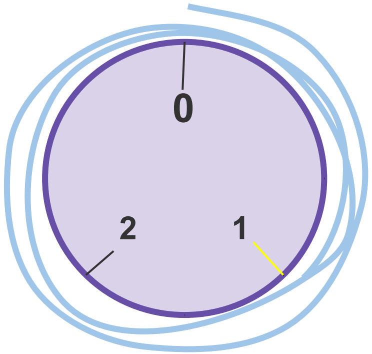
1 (mod 3) **VS** 10 (mod 3)

Divides

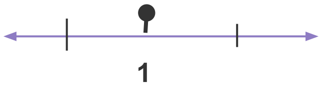
What if we “unroll” this clock?



≡

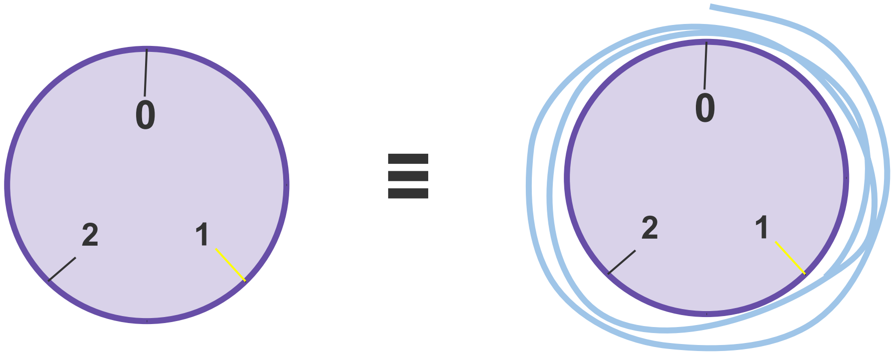


1 (mod 3) **VS** 10 (mod 3)

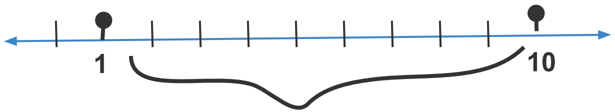


Divides

What if we “unroll” this clock?



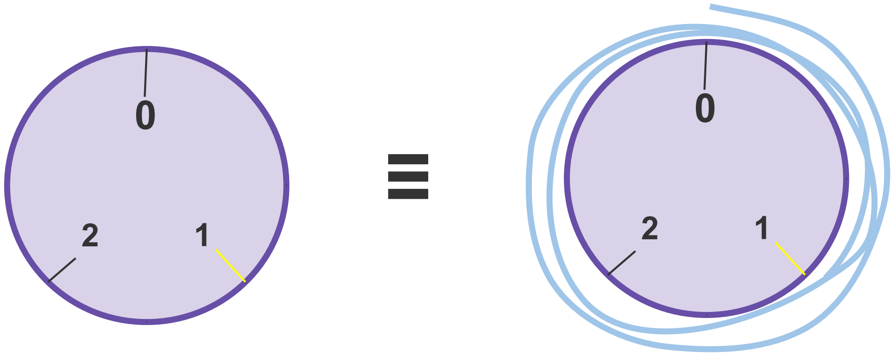
1 (mod 3) **VS** 10 (mod 3)



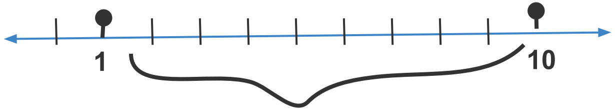
Anything interesting?

Divides

What if we “unroll” this clock?



1 (mod 3) **VS** 10 (mod 3)



(10-1) = 9

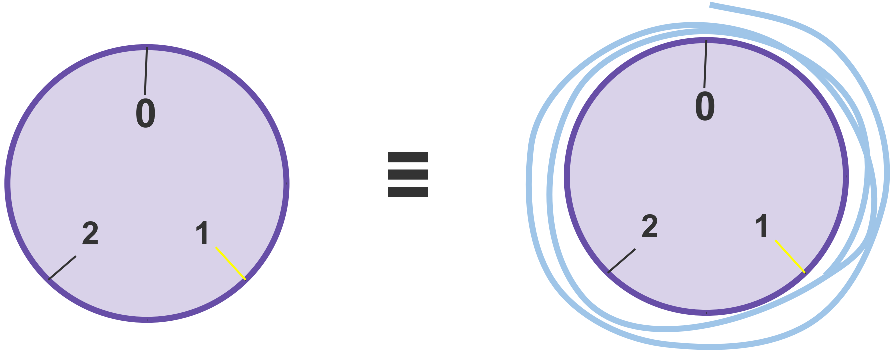
9 ÷ 3 = 3 so 3 | 9

Anything interesting?

$3 \nmid 10$ and $3 \nmid 1$ BUT $3 \mid 9$

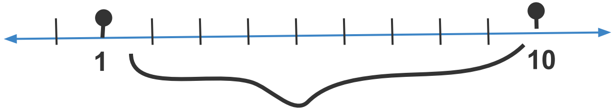
Divides

What if we “unroll” this clock?



1 (mod 3) **VS** 10 (mod 3)

So m divides the <u>difference</u> between a and b!



$(10-1) = 9$

$9 \div 3 = 3$ so $3 \mid 9$

Anything interesting?

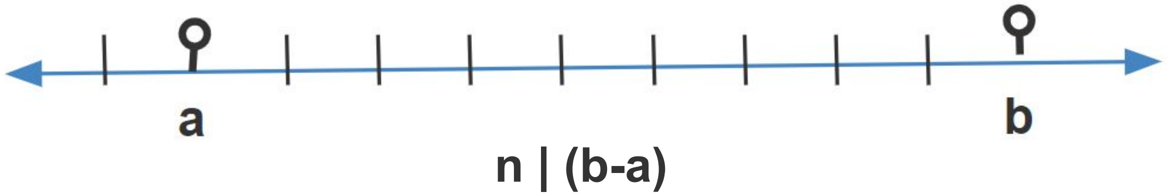
$3 \nmid 10$ and $3 \nmid 1$ BUT $3 \mid 9$

Formalizing Mod and Divides

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.

We say $a \equiv b \ (mod\ n)$ if and only if $n|(b-a)$



Problem 1

(b) Identify the statements that are true for mod using the equivalence definition!

(i) $-3 \equiv 3 \pmod 3$

(ii) $0 \equiv 9000 \pmod 9$

(iii) $44 \equiv 13 \pmod 7$

(iv) $-58 \equiv 707 \pmod 5$

(v) $58 \equiv 707 \pmod 5$

Problem 1

(b) Identify the statements that are true for mod using the equivalence definition!

(i) $-3 \equiv 3 \pmod 3$

(ii) $0 \equiv 9000 \pmod 9$

(iii) $44 \equiv 13 \pmod 7$

(iv) $-58 \equiv 707 \pmod 5$

(v) $58 \equiv 707 \pmod 5$

i. True: $3|(3+3) = 3|6$

Problem 1

(b) Identify the statements that are true for mod using the equivalence definition!

(i) $-3 \equiv 3 \pmod 3$

(ii) $0 \equiv 9000 \pmod 9$

(iii) $44 \equiv 13 \pmod 7$

(iv) $-58 \equiv 707 \pmod 5$

(v) $58 \equiv 707 \pmod 5$

i. True: $3|(3+3) = 3|6$

ii. True: $9|(9000-0) = 9|9000$

Problem 1

(b) Identify the statements that are true for mod using the equivalence definition!

(i) $-3 \equiv 3 \pmod 3$

(ii) $0 \equiv 9000 \pmod 9$

(iii) $44 \equiv 13 \pmod 7$

(iv) $-58 \equiv 707 \pmod 5$

(v) $58 \equiv 707 \pmod 5$

i. True: $3|(3+3) = 3|6$

ii. True: $9|(9000-0) = 9|9000$

iii. False: $7\nmid(13-44) = 7\nmid-31$

Problem 1

(b) Identify the statements that are true for mod using the equivalence definition!

(i) $-3 \equiv 3 \pmod 3$

(ii) $0 \equiv 9000 \pmod 9$

(iii) $44 \equiv 13 \pmod 7$

(iv) $-58 \equiv 707 \pmod 5$

(v) $58 \equiv 707 \pmod 5$

i. True: $3|(3+3) = 3|6$
ii. True: $9|(9000-0) = 9|9000$
iii. False: $7\nmid(13-44) = 7\nmid -31$
iv. True: $5|(707+58) = 5|765$

Problem 1

(b) Identify the statements that are true for mod using the equivalence definition!

(i) $-3 \equiv 3 \pmod{3}$

(ii) $0 \equiv 9000 \pmod{9}$

(iii) $44 \equiv 13 \pmod{7}$

(iv) $-58 \equiv 707 \pmod{5}$

(v) $58 \equiv 707 \pmod{5}$

i. True: $3|(3+3) = 3|6$
ii. True: $9|(9000-0) = 9|9000$
iii. False: $7\nmid(13-44) = 7\nmid-31$
iv. True: $5|(707+58) = 5|765$
v. False: $5|(707-58) = 5\nmid649$

Proving Divisibility

“Unwrapping”

a ≡ b (mod n) ⟺ n|(b-a) ⟺ (b-a) = n * k

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b\ (mod\ n)$ if and only if $n|(b-a)$

Divides

For integers x, y we say $x|y$ (“x divides y”) iff there is an integer z such that $xz = y$.

"Unwrapping"

This expression is generally easier to deal with

a ≡ b (mod n) ⟺ **n|(b-a)** ⟺ **(b-a) = n * k**

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b - a)$

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

Problem

Problem 2

Problem 2

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$. You can find this on cozy here: https://bit.ly/section4_2a. Then, translate it into an English proof.

Problem 2

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$. You can find this on cozy here: `https://bit.ly/section4_2a`. Then, translate it into an English proof.

Let x, y be arbitrary.

Suppose that $x \equiv y \pmod 7$.

Problem 2

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$. You can find this on cozy here: https://bit.ly/section4_2a. Then, translate it into an English proof.

Let x, y be arbitrary.

Suppose that x ≡ y (mod 7). By definition of congruence, we get that 7 | x - y,

Problem 2

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$. You can find this on cozy here: https://bit.ly/section4_2a. Then, translate it into an English proof.

Let x, y be arbitrary.

Suppose that x ≡ y (mod 7). By definition of congruence, we get that 7 | x - y, which through the definition of divides is 7k = x - y for some integer k.

Problem 2

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$. You can find this on cozy here: https://bit.ly/section4_2a. Then, translate it into an English proof.

Let x, y be arbitrary.

Suppose that $x \equiv y \pmod 7$. By definition of congruence, we get that $7 \mid x - y$, which through the definition of divides is $7k = x - y$ for some integer k.

Multiplying both sides by -1 gives $7(-k) = y - x$.

Problem 2

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$. You can find this on cozy here: https://bit.ly/section4_2a. Then, translate it into an English proof.

Let x, y be arbitrary.

Suppose that x ≡ y (mod 7). By definition of congruence, we get that 7 | x - y, which through the definition of divides is 7k = x - y for some integer k.

Multiplying both sides by -1 gives 7(-k) = y - x.

Since (-k) is an integer, through the definition of divides, 7 | y - x holds

Problem 2

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$. You can find this on cozy here: https://bit.ly/section4_2a. Then, translate it into an English proof.

Let x, y be arbitrary.
Suppose that x ≡ y (mod 7). By definition of congruence, we get that 7 | x - y, which through the definition of divides is 7k = x - y for some integer k.
Multiplying both sides by -1 gives 7(-k) = y - x.
Since (-k) is an integer, through the definition of divides, 7 | y - x holds, which, through the definition of congruence, means that y ≡ x (mod 7).

Problem 2

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$. You can find this on cozy here: https://bit.ly/section4_2a. Then, translate it into an English proof.

Let x, y be arbitrary.
Suppose that x ≡ y (mod 7). By definition of congruence, we get that 7 | x - y, which through the definition of divides is 7k = x - y for some integer k.
Multiplying both sides by -1 gives 7(-k) = y - x.
Since (-k) is an integer, through the definition of divides, 7 | y - x holds, which, through the definition of congruence, means that y ≡ x (mod 7).
Since x and y were arbitrary, the claim holds

Problem 2

b) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers and $a \neq 0$, then $a = b$ or $a = -b$.

Problem 2

(b) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers and $a \neq 0$, then $a = b$ or $a = -b$.

(1) Understand what this claim means
(2) Write your start and end goal
(3) Write the skeleton
(4) Fill in the skeleton

Problem 2

(b) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

(1) Understand what this claim means

$3 \mid 3$ and $3 \mid 3$ so $3 = 3$

Or

$3 \mid -3$ and $-3 \mid 3$ so $3 = -(-3)$

(1) Write your start and end goal

(1) Write the skeleton

(1) Fill in the skeleton

Problem 2

Prove that if a | b and b | a, where a and b are integers, then a = b or a = −b.

(1) Understand what this claim means

3 | 3 and 3 | 3 so 3 = 3

Or

3 | -3 and -3 | 3 so 3 = -(-3)

(1) Write your start and end goal

Start: some a and b where a | b and b | a

End: show that a = b or a = −b

(1) Write the skeleton

(1) Fill in the skeleton

Problem 2

Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

(3) Write the skeleton

Problem 2

Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

(3) Write the skeleton

Suppose that for some arbitrary integers a and b where $a|b$ and $b|a$

…

…

…

So we get $b = -a$ or $b = a$

Since a and b were arbitrary, the claim holds

Problem 2

Prove that if a | b and b | a, where a and b are integers, then a = b or a = −b.

(4) Fill in the skeleton

Suppose that for some arbitrary integers a and b where a|b and b|a

By the definition of divides, we have b = ka and **a** = jb, for some integers k, j

…

…

…

So we get b = -a or b = a

Since a and b were arbitrary, the claim holds

Problem 2

Prove that if a | b and b | a, where a and b are integers, then a = b or a = −b.

(4) Fill in the skeleton

Suppose that for some arbitrary integers a and b where a|b and b|a

By the definition of divides, we have b = ka and **a** = jb, for some integers k, j

…

…

…

So we get b = -a or b = a

Since a and b were arbitrary, the claim holds

Can we prove something about k and j to get to b = -a or b = a ?

Problem 2

Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

(4) Fill in the skeleton

Suppose that for some arbitrary integers a and b where $a|b$ and $b|a$

By the definition of divides, we have $b = ka$ and $\mathbf{a} = jb$, for some integers k, j

Substituting b, $a= j(ka)$

…

…

So we get $b = -a$ or $b = a$

Since a and b were arbitrary, the claim holds

Problem 2

Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

(4) Fill in the skeleton

Suppose that for some arbitrary integers a and b where $a|b$ and $b|a$
By the definition of divides, we have $b = ka$ and **a** $= jb$, for some integers k, j
Substituting b, $a= j(ka)$
Dividing both sides by a, we get $1 = jk$.

…

So we get $b = -a$ or $b = a$
Since a and b were arbitrary, the claim holds

What do we need to say about k and j to get to $b = -a$ or $b = a$?

Problem 2

Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

(4) Fill in the skeleton

Suppose that for some arbitrary integers a and b where $a|b$ and $b|a$

By the <u>definition of divides</u>, we have $b = ka$ and $a = jb$, for some integers k, j.

Substituting b, $a= j(ka)$

Dividing both sides by a, we get $1 = jk$.

We can say that $1/j = k$

This expression only holds when j and k are <u>either -1 or 1</u>

$1/3 \neq$ Integer

$1/1 =$ Integer

So we get $b = -a$ or $b = a$

Since a and b were arbitrary, the claim holds

Problem 2

(a) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers greater than 0, then $a = b$ or $a = -b$.

(4) Fill in the skeleton

Suppose that for some arbitrary integers a and b where $a|b$ and $b|a$

By the definition of divides, we have $b = ka$ and **a** $= jb$, for some integers k, j

Substituting b, $a= j(ka)$

Dividing both sides by a, we get $1 = jk$.

We can say that $1/j = k$

k must be an integer and we must get an integer from $1/j$

We know that j and k must be either 1 or -1

So we get $b = -a$ or $b = a$

Since a and b were arbitrary, the claim holds

Problem 3

Problem 3

Let n and m be integers greater than 1, and suppose that $n|m$.
Give an English proof that for any integers a and b, if $a \equiv b \pmod{m}$, then $a \equiv b \pmod{n}$.

Problem 3

Let n and m be integers greater than 1, and suppose that n|m.
Give an English proof that for any integers a and b, if a ≡ b (mod m), then a ≡ b (mod n).

Let a and b be arbitrary integers and n > 1 and m > 1. Suppose that a ≡ b (mod m).

…

…

Since a and b were arbitrary, the claim holds

Problem 3

Let n and m be integers greater than 1, and suppose that $n|m$.
Give an English proof that for any integers a and b, if $a \equiv b \pmod{m}$, then $a \equiv b \pmod{n}$.

Let a and b be arbitrary integers and $n > 1$ and $m > 1$. Suppose that $a \equiv b \pmod{m}$.

Then, by definition of mod, $m \mid (a-b)$, so there exists an integer k such that $a-b = mk$.

…

Since a and b were arbitrary, the claim holds

Problem 3

Let n and m be integers greater than 1, and suppose that n|m.
Give an English proof that for any integers a and b, if a ≡ b (mod m), then a ≡ b (mod n).

Let a and b be arbitrary integers and n > 1 and m > 1. Suppos
(mod m).
Then, by definition of mod, m | (a-b) , so there exists an integ
a-b = mk.

…

…

…

Since a and b were arbitrary, the claim holds

Try to work a step backwards when you can!

Problem 3

Let n and m be integers greater than 1, and suppose that n|m.
Give an English proof that for any integers a and b, if a ≡ b (mod m), then a ≡ b (mod n).

Let a and b be arbitrary integers and n > 1 and m > 1. Suppos
(mod m).
Then, by definition of mod, m | (a-b) , so there exists an integ
a-b = mk.
…
…
So, by definition of mod equivalence, n | (a-b) so a ≡ b (mod m)
Since a and b were arbitrary, the claim holds

Try to work a step backwards when you can!

Problem 3

Let n and m be integers greater than 1, and suppose that n|m.
Give an English proof that for any integers a and b, if a ≡ b (mod m), then a ≡ b (mod n).

Let a and b be arbitrary integers and n > 1 and m > 1. Suppose that a ≡ b (mod m).
Then, by definition of mod, m | (a-b) , so there exists an integer k such that a-b = mk.
Also, since n | m, there is an integer j such that m = jn. Thus, we have.
a-b = (jn)k
a-b = (kj)n
So, by definition of mod equivalence, n | (a-b) so a ≡ b (mod m)
Since a and b were arbitrary, the claim holds

Proof By Cases

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(1) Understand what this claim means
(2) Write your start and end goal
(3) Write the skeleton
(4) Fill in the skeleton

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(1) Understand what this claim means

$(3)^2 \equiv 1 \pmod 4$

$(2)^2 \equiv 0 \pmod 4$

*If you square an **even** integer, you get **0** (mod 4)*

*If you square an **odd** integer, you get **1** (mod 4)*

(1) Write your start and end goal

(2) Write the skeleton

(3) Fill in the skeleton

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(1) Understand what this claim means

$(3)^2 \equiv 1 \pmod 4$

$(2)^2 \equiv 0 \pmod 4$

*If you square an **even** integer, you get **0** (mod 4)*

*If you square an **odd** integer, you get **1** (mod 4)*

(1) Write your start and end goal

Start: Some integer

End: Prove the integer^2 will be either ***0*** *(mod 4) or* ***1*** *(mod 4)*

(1) Write the skeleton

(2) Fill in the skeleton

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(3) Write the skeleton

Let n be an arbitrary integer. We go by cases.

Case 1: n is even … $n^2 \equiv 0 \pmod 4$

Case 2: n is odd … $n^2 \equiv 1 \pmod 4$

…

…

In <u>all cases</u> $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

Since n was arbitrary, the claim holds

(4) Fill in the skeleton

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(4) Fill in the skeleton

Let n be an arbitrary integer

Case 1: n is even

Then $n = 2k$ for some integer k

…

…

Then by the definition of congruence, $\mathbf{n^2 \equiv 0 \pmod 4}$

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(4) Fill in the skeleton

Let n be an arbitrary integer

Case 1: n is even

Then n = 2k for some integer k

…

By the definition of divides so $4 | n^2$

Then by the definition of congruence, $\mathbf{n^2 \equiv 0 \pmod 4}$

Work one step backwards to "unwrap"

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(4) Fill in the skeleton

Let n be an arbitrary integer

Case 1: n is even

Then n = 2k for some integer k

…

By the definition of divides so $4 | n^2$

Then by the definition of congruence, $\mathbf{n^2 \equiv 0 \pmod 4}$

So we need to get something like:
$k * 4 = n^2$

Work one step backwards to "unwrap"

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(4) Fill in the skeleton

Let n be an arbitrary integer

Case 1: n is even

Then $n = 2k$ for some integer k

Then $n^2 = (2k)^2 = 4k^2$

Since k is an integer, k^2 is an integer.

By the definition of divides, $4 \mid 4k^2$ so $4 \mid n^2$

Then by the definition of congruence, $\mathbf{n^2 \equiv 0 \pmod 4}$.

Thus $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(4) Fill in the skeleton

Let n be an arbitrary integer

Case 2: n is odd

Then $n = 2k+1$ for some integer k

…

…

…

…

$\mathbf{n^2 \equiv 1 \pmod 4}$

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(4) Fill in the skeleton

Let n be an arbitrary integer

Case 2: n is odd

Then $n = 2k+1$ for some integer k

…

…

…

…

By the definition of divides, **$4 \mid n^2-1$**

Then by the definition of congruence, **$n^2 \equiv 1 \pmod 4$**

Thus $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Work one step backwards to "unwrap"

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(4) Fill in the skeleton

Let n be an arbitrary integer

Case 2: n is odd

Then n = 2k+1 for some integer k

…

…

…

So we can say that 4 * j = $\mathbf{n^2}$ **- 1**

By the definition of divides, **4|** $\mathbf{n^2}$**-1**

Then by the definition of congruence, $\mathbf{n^2 \equiv 1 \pmod 4}$

Thus $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Work one step backwards to "unwrap"

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(4) Fill in the skeleton

Let n be an arbitrary integer

Case 2: n is odd

Then $n = 2k+1$ for some integer k

Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$

…

…

So we can say that $4 * j = \mathbf{n^2 - 1}$

By the definition of divides, $\mathbf{4 | n^2\text{-}1}$

Then by the definition of congruence, $\mathbf{n^2 \equiv 1 \pmod 4}$

Thus $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(4) Fill in the skeleton

Let n be an arbitrary integer

Case 2: n is odd

Then $n = 2k+1$ for some integer k

Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$

So $\mathbf{n^2 - 1} = 4(k^2 + k)$

Since k is an integer, we can say $j = k^2 + k$ where j is an integer.

So we can say that $4 * j = \mathbf{n^2 - 1}$

By the definition of divides, $\mathbf{4 | n^2-1}$

Then by the definition of congruence, $\mathbf{n^2 \equiv 1 \pmod 4}$

Thus $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Problem 4:

(a) Prove that for all integers n, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

(4) Fill in the skeleton

Let n be an arbitrary integer

Case 1: n is even

Then $n = 2k$ for some integer k

Then $n^2 = (2k)^2 = 4k^2$

Since k is an integer, k^2 is an integer.

By the definition of divides, $4 \mid 4k^2$ so $4 \mid n^2$

Then by the definition of congruence, $n^2 \equiv 0 \pmod 4$

Thus $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

Case 2: n is odd

Then $n = 2k+1$ for some integer k

Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$

So $\mathbf{n^2 - 1} = 4(k^2 + k)$

Since k is an integer, we can say $j = k^2 + k$ where j is an integer.

So we can say that $4 * j = \mathbf{n^2 - 1}$

By the definition of divides, $\mathbf{4 \mid n^2-1}$

Then by the definition of congruence, $\mathbf{n^2 \equiv 1 \pmod 4}$

Thus $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

In either case, $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$. Since n was arbitrary, the claim holds

That’s All Folks

Written by Aruna & Jacob