CSE 311 Section 4

English Proofs & Number Theory

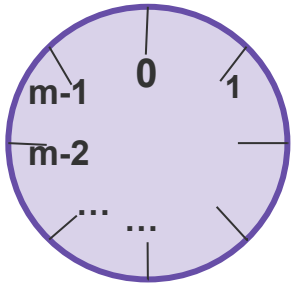
Announcements & Reminders

- HW2
  - Regrades will open soon
- 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

Mod

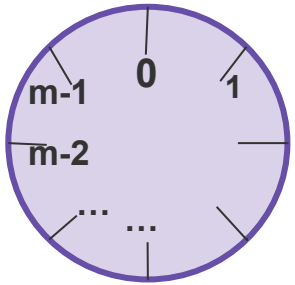
$a \equiv b \pmod{m}$

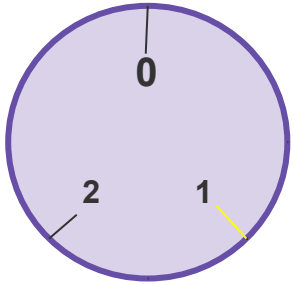
Imagine a clock with m numbers



$a \equiv b \pmod{m}$

Imagine a clock with m numbers

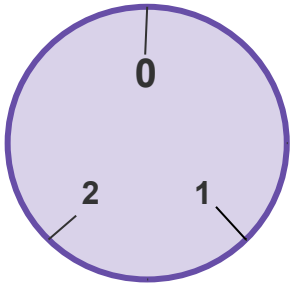




1 (mod 3)

≡

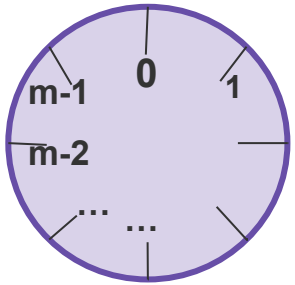
VS

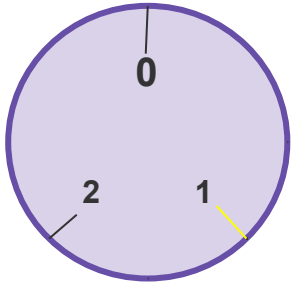


10 (mod 3)

$a \equiv b \pmod{m}$

Imagine a clock with m numbers

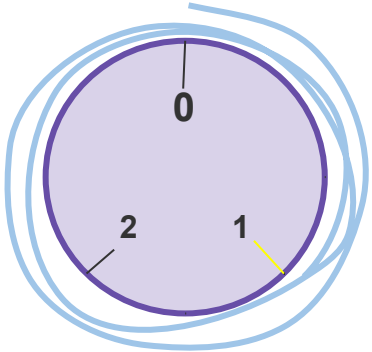




1 (mod 3)

≡

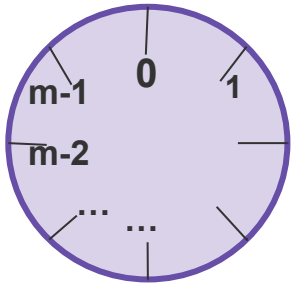
VS

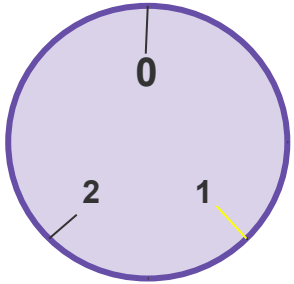


10 (mod 3)

a ≡ b (mod m)

Imagine a clock with m numbers

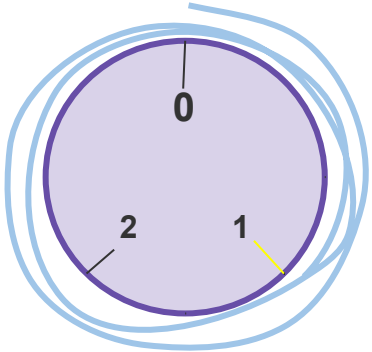




1 (mod 3)

≡

VS



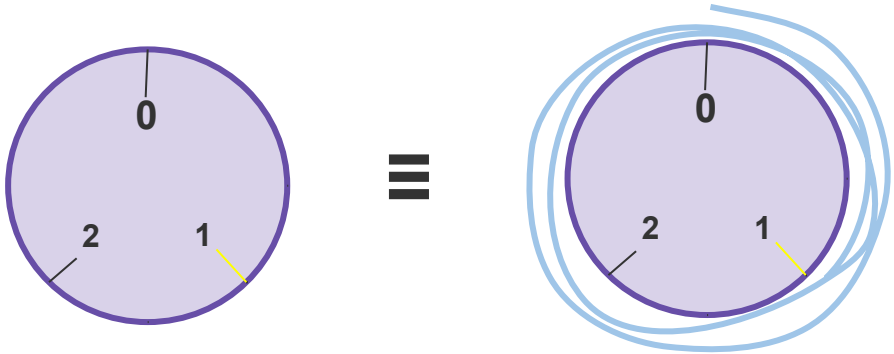
10 (mod 3)

So we can say that **a ≡ b (mod m)** where a and b are in the same position in the mod clock

1 ≡ 10 (mod 3)

Divides

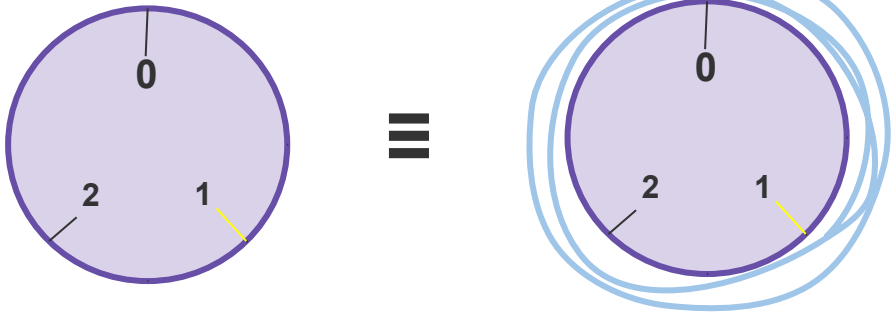
What if we “unroll” this clock?



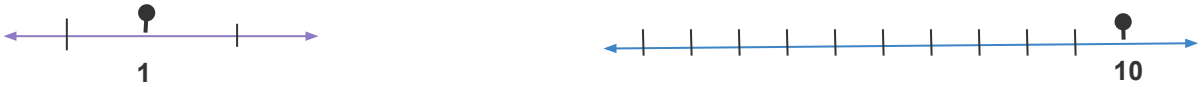
1 (mod 3) **VS** 10 (mod 3)

Divides

What if we “unroll” this clock?

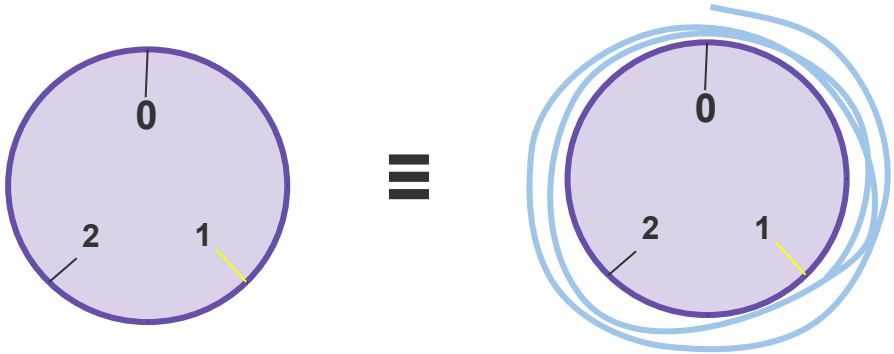


1 (mod 3) **VS** 10 (mod 3)

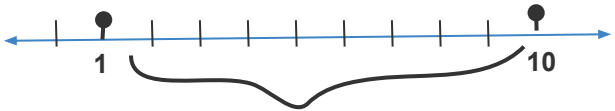


Divides

What if we “unroll” this clock?



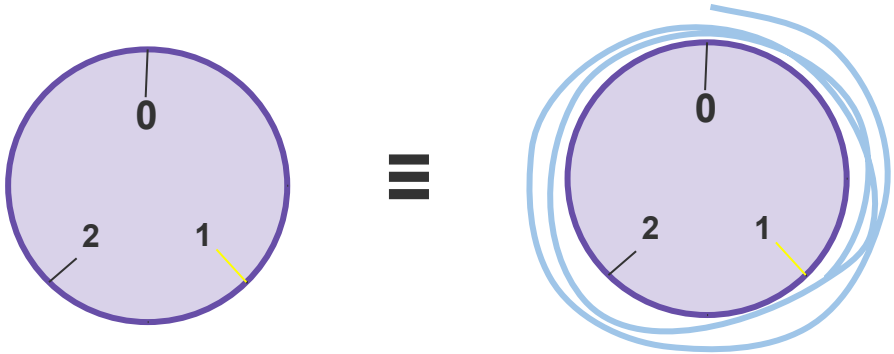
1 (mod 3) **VS** 10 (mod 3)



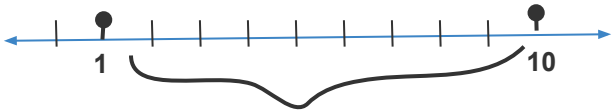
Anything interesting?

Divides

What if we “unroll” this clock?



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



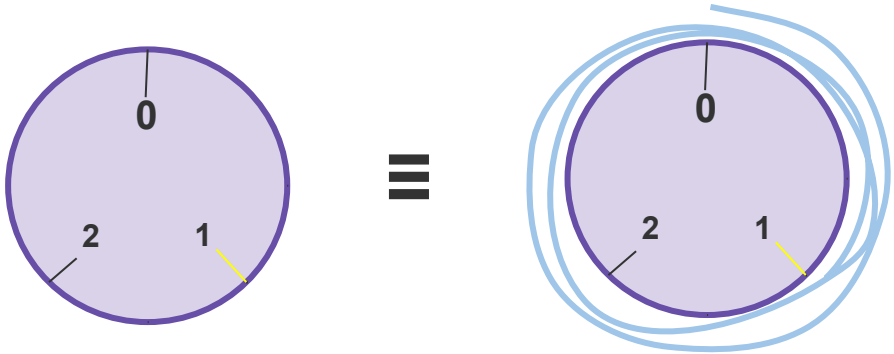
(10-1) = 9
9 ÷ 3 = 3 so 3 | 9

Anything interesting?

3 ∤ 10 and 3 ∤ 1 BUT 3 | 9

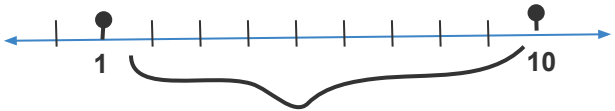
Divides

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 ÷ 3 = 3 so 3 | 9

Anything interesting?

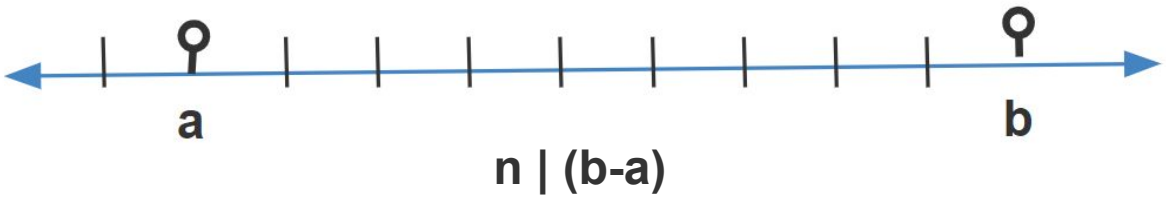
3∤10 and 3∤1 BUT 3|9

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 $n|(b - a)$



Review

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) $58 \equiv 707 \pmod 5$

Review

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: $3|(3+3) = 3|6$

Review

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: $9|(9000-0) = 9|9000$

Review

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

Review

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: $5|(707+58) = 5|765$

Review

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”

$a \equiv b \pmod{n}$  $n \mid (b-a)$  $(b-a) = n * k$

Equivalence in modular arithmetic

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

Divides

For integers x, y we say $x \mid y$ (“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 2: Division of Labor

Problem 2

In this problem, we will use the predicate "Divides", defined by $\text{Divides}(x, y) := \exists k\,(y = k \cdot x)$. We can use this definition via these two rules:

Def of Divides

$$\frac{\text{Divides}(x, y)}{\therefore\ \exists k\,(y = k \cdot x)}$$

Undef Divides

$$\frac{\exists k\,(y = k \cdot x)}{\therefore\ \text{Divides}(x, y)}$$

Note that, in math, we write $\text{Divides}(x, y)$ with the nicer notation "$x \mid y$".

Let domain of discourse be the integers. Consider the following claim: $\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$. In English, this says that if an integer b divides an integer a, then the square of b will divide the cube of a.

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

We can verify this:

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

We can verify this:
3 | 9 so

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

We can verify this:
3 | 9 so
$3^2 \mid 9^3 = 9 \mid 729$

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

We can verify this:
3 | 9 so
3^2 | 9^3 = 9 | 729
We know: 729/9 = 81

Cool!

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

Attempt proving this with a formal proof!

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

Problem 2

$$\forall a \forall b((b \mid a) \to (b^2 \mid a^3))$$

Let a, b be arbitrary.

Let's get started!

1. $\forall a \forall b \left((b \mid a) \to (b^2 \mid a^3)\right)$ Intro $\forall$

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

Let a, b be arbitrary.

Let's get started!

We can use intro forall twice (though we will state it just once)

1. $\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$ Intro $\forall$

Problem 2

$$\forall a \forall b((b \mid a) \to (b^2 \mid a^3))$$

Let a, b be arbitrary.

1.1.1. $(b \mid a)$ Assumption

Now we just unroll definitions…

$b^2 \mid a^3$

1.1. $(b \mid a) \to (b^2 \mid a^3)$ Direct Proof

1. $\forall a \forall b \left((b \mid a) \to (b^2 \mid a^3)\right)$ Intro $\forall$

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

Let a, b be arbitrary.

1.1.1. $(b \mid a)$ Assumption

1.1.2. $\exists k(a = kb)$ Def of Divides: 1.1.1

$b^2 \mid a^3$

1.1. $(b \mid a) \rightarrow (b^2 \mid a^3)$ Direct Proof

1. $\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$ Intro $\forall$

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2

$$b^2 \mid a^3$$

1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	Direct Proof
1.	$\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$	Intro $\forall$

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3

$$b^2 \mid a^3$$

1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	Direct Proof
1.	$\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$	Intro $\forall$

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3

…I am not sure where to go… lets work a step backward!

$$b^2 \mid a^3$$

1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	Direct Proof
1.	$\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$	Intro $\forall$

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3

Since k is an integer, what if it became (bj^3) ?

	$\exists k(a^3 = kb^2)$	
	$b^2 \mid a^3$	Undef of Divides: 1.1.6
1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	Direct Proof
1.	$\forall a \forall b\,((b \mid a) \rightarrow (b^2 \mid a^3))$	Intro $\forall$

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3
1.1.5.	$a^3 = (bj^3)b^2$	Algebra : 1.1.4
	$\exists k(a^3 = kb^2)$	
	$b^2 \mid a^3$	Undef of Divides: 1.1.6
1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	Direct Proof
1.	$\forall a \forall b\,((b \mid a) \rightarrow (b^2 \mid a^3))$	Intro $\forall$

Nice! Now just fill in the remaining definitions…

Problem 2

$$\forall a \forall b((b \mid a) \rightarrow (b^2 \mid a^3))$$

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3
1.1.5.	$a^3 = (bj^3)b^2$	Algebra : 1.1.4
1.1.6.	$\exists k(a^3 = kb^2)$	Intro $\exists$: 1.1.5
1.1.7.	$b^2 \mid a^3$	Undef of Divides: 1.1.6

1.1. $(b \mid a) \rightarrow (b^2 \mid a^3)$ Direct Proof

1. $\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$ Intro $\forall$

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 $y \in A \wedge y \notin B$…”
- 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

Problem 2

Translating to English…

Let's use the skeleton of the formal proof to help us:

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3
1.1.5.	$a^3 = (bj^3)b^2$	Algebra : 1.1.4
1.1.6.	$\exists k(a^3 = kb^2)$	Intro $\exists$: 1.1.5
1.1.7.	$b^2 \mid a^3$	Undef of Divides: 1.1.6
1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	
1.	$\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$	

Problem 2

Translating to English…

Let a and b be arbitrary integers

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3
1.1.5.	$a^3 = (bj^3)b^2$	Algebra : 1.1.4
1.1.6.	$\exists k(a^3 = kb^2)$	Intro $\exists$: 1.1.5
1.1.7.	$b^2 \mid a^3$	Undef of Divides: 1.1.6
1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	
1.	$\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$	

As a and b were arbitrary, our claim holds

Problem 2

Translating to English…

Let a and b be arbitrary integers

Suppose that a | b

As a and b were arbitrary, our claim holds

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3
1.1.5.	$a^3 = (bj^3)b^2$	Algebra : 1.1.4
1.1.6.	$\exists k(a^3 = kb^2)$	Intro $\exists$: 1.1.5
1.1.7.	$b^2 \mid a^3$	Undef of Divides: 1.1.6
1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	
1.	$\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$	

Problem 2

Translating to English…

Let a and b be arbitrary integers

Suppose that a | b

By the def of divides, we have for some integer j, a = jb

As a and b were arbitrary, our claim holds

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3
1.1.5.	$a^3 = (bj^3)b^2$	Algebra : 1.1.4
1.1.6.	$\exists k(a^3 = kb^2)$	Intro $\exists$: 1.1.5
1.1.7.	$b^2 \mid a^3$	Undef of Divides: 1.1.6
1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	
1.	$\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$	

Problem 2

Translating to English…

Let a and b be arbitrary integers

Suppose that a | b

By the def of divides, we have for some integer j, a = jb

Cubing both sides, we have that $a^3 = (jb)^3$
Factoring bj^3, we see that $a^3 = (bj^3)b^2$

As a and b were arbitrary, our claim holds

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3
1.1.5.	$a^3 = (bj^3)b^2$	Algebra : 1.1.4
1.1.6.	$\exists k(a^3 = kb^2)$	Intro $\exists$: 1.1.5
1.1.7.	$b^2 \mid a^3$	Undef of Divides: 1.1.6
1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	
1.	$\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$	

Problem 2

Translating to English…

Let a and b be arbitrary integers

Suppose that a | b

By the def of divides, we have for some integer j, a = jb

Cubing both sides, we have that $a^3 = (jb)^3$
Factoring bj^3, we see that $a^3 = (bj^3)b^2$

As integers are closed under multiplication, we have that (bj^3) is an integer
So for **some** integer k, $a^3 = k\,b^2$

As a and b were arbitrary, our claim holds

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3
1.1.5.	$a^3 = (bj^3)b^2$	Algebra : 1.1.4
1.1.6.	$\exists k(a^3 = kb^2)$	Intro $\exists$: 1.1.5
1.1.7.	$b^2 \mid a^3$	Undef of Divides: 1.1.6
1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	
1.	$\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$	

Problem 2

Translating to English…

Let a and b be arbitrary integers

Suppose that a | b

By the def of divides, we have for some integer j, a = jb

Cubing both sides, we have that $a^3 = (jb)^3$
Factoring bj^3, we see that $a^3 = (bj^3)b^2$

As integers are closed under multiplication, we have that (bj^3) is an integer
So for some integer k, $a^3 = k\,b^2$

By the definition of divides, $b^2 \mid a^3$

As a and b were arbitrary, our claim holds

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3
1.1.5.	$a^3 = (bj^3)b^2$	Algebra : 1.1.4
1.1.6.	$\exists k(a^3 = kb^2)$	Intro $\exists$: 1.1.5
1.1.7.	$b^2 \mid a^3$	Undef of Divides: 1.1.6

1.1. $(b \mid a) \rightarrow (b^2 \mid a^3)$

1. $\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$

Problem 2

Translating to English…

Let a and b be arbitrary integers

Suppose that a | b

By the def of divides, we have for some integer j, a = jb

Cubing both sides, we have that $a^3 = (jb)^3$
Factoring bj^3, we see that $a^3 = (bj^3)b^2$

As integers are closed under multiplication, we have that (bj^3) is an integer
So for some integer k, $a^3 = k\,b^2$

By the definition of divides, $b^2 \mid a^3$

As a and b were arbitrary, our claim holds

Let a, b be arbitrary.

1.1.1.	$(b \mid a)$	Assumption
1.1.2.	$\exists k(a = kb)$	Def of Divides: 1.1.1
1.1.3.	$a = jb$	Elim $\exists$: 1.1.2
1.1.4.	$a^3 = (jb)^3$	Algebra: 1.1.3
1.1.5.	$a^3 = (bj^3)b^2$	Algebra : 1.1.4
1.1.6.	$\exists k(a^3 = kb^2)$	Intro $\exists$: 1.1.5
1.1.7.	$b^2 \mid a^3$	Undef of Divides: 1.1.6
1.1.	$(b \mid a) \rightarrow (b^2 \mid a^3)$	
1.	$\forall a \forall b \left((b \mid a) \rightarrow (b^2 \mid a^3)\right)$	

Problem 2

Translating to English…

Let a and b be arbitrary integers

Suppose that a | b

By the def of divides, we have for some integer j, a = jb

Cubing both sides, we have that $a^3 = (jb)^3$
Factoring bj^3, we see that $a^3 = (bj^3)b^2$

As integers are closed under multiplication, we have that (bj^3) is an integer
So for some integer k, $a^3 = k\ b^2$

By the definition of divides, $b^2 \mid a^3$

As a and b were arbitrary, our claim holds

Problem 3

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

1. $x \equiv_7 y$ Given

$y \equiv_7 x$

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

1.	$x \equiv_7 y$	Given
2.	$7 \mid x - y$	Def of Congruent: 1

$y \equiv_7 x$

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

1.	$x \equiv_7 y$	Given
2.	$7 \mid x - y$	Def of Congruent: 1
3.	$\exists\, k, x - y = k\,7$	Def of Divides: 2

$y \equiv_7 x$

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

1.	$x \equiv_7 y$	Given
2.	$7 \mid x - y$	Def of Congruent: 1
3.	$\exists\, k, x - y = k\,7$	Def of Divides: 2
4.	$x - y = k\,7$	Elim $\exists$: 3

lets work a few steps back as well!

$y \equiv_7 x$

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

1.	$x \equiv_7 y$	Given
2.	$7 \mid x - y$	Def of Congruent: 1
3.	$\exists\, k, x - y = k\,7$	Def of Divides: 2
4.	$x - y = k\,7$	Elim $\exists$: 3

lets work a few steps back as well!

	$7 \mid y - x$	
	$y \equiv_7 x$	Undef Congruent: 7

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

1.	$x \equiv_7 y$	Given
2.	$7 \mid x - y$	Def of Congruent: 1
3.	$\exists\, k, x - y = k\,7$	Def of Divides: 2
4.	$x - y = k\,7$	Elim $\exists$: 3
	$\exists\, k, y - x = k\,7$	
	$7 \mid y - x$	Undef Divides: 6
	$y \equiv_7 x$	Undef Congruent: 7

lets work a few steps back as well!

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

1.	$x \equiv_7 y$	Given
2.	$7 \mid x - y$	Def of Congruent: 1
3.	$\exists\, k, x - y = k\,7$	Def of Divides: 2
4.	$x - y = k\,7$	Elim $\exists$: 3
	$y - x = (-k)\,7$	Algebra: 4
	$\exists\, k, y - x = k\,7$	Intro $\exists$: 5
	$7 \mid y - x$	Undef Divides: 6
	$y \equiv_7 x$	Undef Congruent: 7

This gap looks easier to close!

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

1.	$x \equiv_7 y$	Given
2.	$7 \mid x - y$	Def of Congruent: 1
3.	$\exists\, k, x - y = k\,7$	Def of Divides: 2
4.	$x - y = k\,7$	Elim $\exists$: 3
5.	$y - x = (-k)\,7$	Algebra: 4
6.	$\exists\, k, y - x = k\,7$	Intro $\exists$: 5
7.	$7 \mid y - x$	Undef Divides: 6
8.	$y \equiv_7 x$	Undef Congruent: 7

Problem 3

Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

Now for the english proof!

$x \equiv_7 y$	Given
$7 \mid x - y$	Def of Congruent:
$\exists\, k, x - y = k\,7$	Def of Divides: 2
$x - y = k\,7$	Elim $\exists$: 3
$y - x = (-k)\,7$	Algebra: 4
$\exists\, k, y - x = k\,7$	Intro $\exists$: 5
$7 \mid y - x$	Undef Divides: 6
$y \equiv_7 x$	Undef Congruent:

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

Let x, y be arbitrary integers.
Suppose that x ≡ y (mod 7).

More implicit than before!

$x \equiv_7 y$	Given
$7 \mid x - y$	Def of Congruent:
$\exists\, k, x - y = k\,7$	Def of Divides: 2
$x - y = k\,7$	Elim ∃: 3
$y - x = (-k)\,7$	Algebra: 4
$\exists\, k, y - x = k\,7$	Intro ∃: 5
$7 \mid y - x$	Undef Divides: 6
$y \equiv_7 x$	Undef Congruent:

Since x and y were arbitrary, the claim holds

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

Let x, y be arbitrary integers.
Suppose that x ≡ y (mod 7).

By definition of congruence, we get that 7 | x - y

$x \equiv_7 y$	Given
$7 \mid x - y$	Def of Congruent:
$\exists\, k, x - y = k\,7$	Def of Divides: 2
$x - y = k\,7$	Elim ∃: 3
$y - x = (-k)\,7$	Algebra: 4
$\exists\, k, y - x = k\,7$	Intro ∃: 5
$7 \mid y - x$	Undef Divides: 6
$y \equiv_7 x$	Undef Congruent:

Since x and y were arbitrary, the claim holds

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

Let x, y be arbitrary integers.
Suppose that x ≡ y (mod 7).

By definition of congruence, we get that 7 | x - y
By the definition of divides is 7k = x - y for some integer k.

$x \equiv_7 y$	Given
$7 \mid x - y$	Def of Congruent:
$\exists\, k, x - y = k\,7$	Def of Divides: 2
$x - y = k\,7$	Elim ∃: 3
$y - x = (-k)\,7$	Algebra: 4
$\exists\, k, y - x = k\,7$	Intro ∃: 5
$7 \mid y - x$	Undef Divides: 6
$y \equiv_7 x$	Undef Congruent:

Since x and y were arbitrary, the claim holds

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

Let x, y be arbitrary integers.
Suppose that x ≡ y (mod 7).

By definition of congruence, we get that 7 | x - y
By the definition of divides is 7k = x - y for some integer k.
Multiplying both sides by -1 gives 7(-k) = y - x.

$x \equiv_7 y$	Given
$7 \mid x - y$	Def of Congruent:
$\exists\, k, x - y = k\,7$	Def of Divides: 2
$x - y = k\,7$	Elim ∃: 3
$y - x = (-k)\,7$	Algebra: 4
$\exists\, k, y - x = k\,7$	Intro ∃: 5
$7 \mid y - x$	Undef Divides: 6
$y \equiv_7 x$	Undef Congruent:

Since x and y were arbitrary, the claim holds

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

Let x, y be arbitrary integers.
Suppose that x ≡ y (mod 7).

By definition of congruence, we get that 7 | x - y
By 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, by the definition of divides, 7 | y - x holds

Since x and y were arbitrary, the claim holds

$x \equiv_7 y$	Given
$7 \mid x - y$	Def of Congruent:
$\exists\, k, x - y = k\,7$	Def of Divides: 2
$x - y = k\,7$	Elim ∃: 3
$y - x = (-k)\,7$	Algebra: 4
$\exists\, k, y - x = k\,7$	Intro ∃: 5
$7 \mid y - x$	Undef Divides: 6
$y \equiv_7 x$	Undef Congruent:

Problem 3

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$.

Let x, y be arbitrary integers.
Suppose that x ≡ y (mod 7).

By definition of congruence, we get that 7 | x - y
By 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, by the definition of divides, 7 | y - x holds

By the definition of Congruence, y ≡ x (mod 7).
Since x and y were arbitrary, the claim holds

$x \equiv_7 y$	Given
$7 \mid x - y$	Def of Congruent:
$\exists\, k, x - y = k\,7$	Def of Divides: 2
$x - y = k\,7$	Elim ∃: 3
$y - x = (-k)\,7$	Algebra: 4
$\exists\, k, y - x = k\,7$	Intro ∃: 5
$7 \mid y - x$	Undef Divides: 6
$y \equiv_7 x$	Undef Congruent:

Problem 4:

In this problem, we will use the theorem "DivideEqn". It says that, if you have the equation $ca = cb$ and you know that $c \neq 0$, then you can divide both sides of the equation by c to get $a = b$. We can use this theorem in a formal proof via these two rules:

Cite DivideEqn

$$\therefore \quad \forall a \, \forall b \, \forall c \, ((ca = cb \wedge \neg(c = 0)) \rightarrow a = b)$$

Apply DivideEqn

$$\frac{ca = cb \wedge \neg(c = 0)}{\therefore \quad a = b}$$

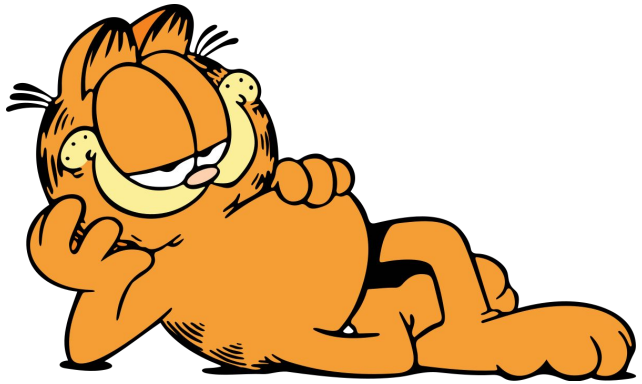
In this problem, we will use the theorem "DivideEqn". It says that, if you have the equation $ca = cb$ and you know that $c \neq 0$, then you can divide both sides of the equation by c to get $a = b$. We can use this theorem in a formal proof via these two rules:

Cite DivideEqn

$$\therefore \quad \forall a \, \forall b \, \forall c \, ((ca = cb \wedge \neg(c = 0)) \rightarrow a = b)$$

Apply DivideEqn

$$\frac{ca = cb \wedge \neg(c = 0)}{\therefore \quad a = b}$$



Simply put:

If **c** * **a** = **c** * **b**
then **a** = **b**

If **c** is non zero

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \rightarrow a \equiv_m b)$$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \to a \equiv_m b)$$

1. $\neg(5 = 0)$ — Given
2. $\forall\, a, \forall\, b, \forall\, c, c\, a = c\, b \wedge \neg(c = 0) \to a = b$ — Cite DivideEqn

   Let a, b, and m be arbitrary.

$\forall\, a, \forall\, b, \forall\, m, 5\, a \equiv_{5\, m} 5\, b \to a \equiv_m b$ — Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \to a \equiv_m b)$$

1. $\neg(5 = 0)$ — Given
2. $\forall\, a, \forall\, b, \forall\, c, c\, a = c\, b \wedge \neg(c = 0) \to a = b$ — Cite DivideEqn

   Let a, b, and m be arbitrary.

   3.1.1. $5\, a \equiv_{5\, m} 5\, b$ — Assumption

   3.1. $5\, a \equiv_{5\, m} 5\, b \to a \equiv_m b$ — Direct Proof

$\forall\, a, \forall\, b, \forall\, m, 5\, a \equiv_{5\, m} 5\, b \to a \equiv_m b$ — Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \to a \equiv_m b)$$

1. $\neg(5 = 0)$	Given
2. $\forall\, a, \forall\, b, \forall\, c, c\,a = c\,b \wedge \neg(c = 0) \to a = b$	Cite DivideEqn
Let a, b, and m be arbitrary.	
3.1.1. $5\,a \equiv_{5\,m} 5\,b$	Assumption
3.1.2. $5\,m \mid 5\,a - 5\,b$	Def of Congruent: 3.1.1
3.1. $5\,a \equiv_{5\,m} 5\,b \to a \equiv_m b$	Direct Proof
$\forall\, a, \forall\, b, \forall\, m, 5\,a \equiv_{5\,m} 5\,b \to a \equiv_m b$	Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \rightarrow a \equiv_m b)$$

1. $\neg(5 = 0)$	Given
2. $\forall a, \forall b, \forall c, ca = cb \wedge \neg(c = 0) \rightarrow a = b$	Cite DivideEqn
Let a, b, and m be arbitrary.	
3.1.1. $5a \equiv_{5m} 5b$	Assumption
3.1.2. $5m \mid 5a - 5b$	Def of Congruent: 3.1.1
3.1.3. $\exists k, 5a - 5b = k5m$	Def of Divides: 3.1.2
3.1. $5a \equiv_{5m} 5b \rightarrow a \equiv_m b$	Direct Proof
$\forall a, \forall b, \forall m, 5a \equiv_{5m} 5b \rightarrow a \equiv_m b$	Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \to a \equiv_m b)$$

1. $\neg(5 = 0)$	Given
2. $\forall a, \forall b, \forall c, ca = cb \wedge \neg(c = 0) \to a = b$	Cite DivideEqn
Let a, b, and m be arbitrary.	
3.1.1. $5a \equiv_{5m} 5b$	Assumption
3.1.2. $5m \mid 5a - 5b$	Def of Congruent: 3.1.1
3.1.3. $\exists k, 5a - 5b = k5m$	Def of Divides: 3.1.2
3.1.4. $5a - 5b = i5m$	Elim $\exists$: 3.1.3
3.1. $5a \equiv_{5m} 5b \to a \equiv_m b$	Direct Proof
$\forall a, \forall b, \forall m, 5a \equiv_{5m} 5b \to a \equiv_m b$	Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \to a \equiv_m b)$$

1. $\neg(5 = 0)$	Given
2. $\forall a, \forall b, \forall c, ca = cb \wedge \neg(c = 0) \to a = b$	Cite DivideEqn
Let a, b, and m be arbitrary.	
3.1.1. $5a \equiv_{5m} 5b$	Assumption
3.1.2. $5m \mid 5a - 5b$	Def of Congruent: 3.1.1
3.1.3. $\exists k, 5a - 5b = k5m$	Def of Divides: 3.1.2
3.1.4. $5a - 5b = i5m$	Elim $\exists$: 3.1.3

Now we work back a bit…

3.1. $5a \equiv_{5m} 5b \to a \equiv_m b$	Direct Proof
$\forall a, \forall b, \forall m, 5a \equiv_{5m} 5b \to a \equiv_m b$	Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \to a \equiv_m b)$$

1. $\neg(5 = 0)$	Given
2. $\forall a, \forall b, \forall c, ca = cb \wedge \neg(c = 0) \to a = b$	Cite DivideEqn
Let a, b, and m be arbitrary.	
3.1.1. $5a \equiv_{5m} 5b$	Assumption
3.1.2. $5m \mid 5a - 5b$	Def of Congruent: 3.1.1
3.1.3. $\exists k, 5a - 5b = k5m$	Def of Divides: 3.1.2
3.1.4. $5a - 5b = i5m$	Elim $\exists$: 3.1.3
$a \equiv_m b$	
3.1. $5a \equiv_{5m} 5b \to a \equiv_m b$	Direct Proof
$\forall a, \forall b, \forall m, 5a \equiv_{5m} 5b \to a \equiv_m b$	Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \rightarrow a \equiv_m b)$$

1. $\neg(5 = 0)$ — Given
2. $\forall a, \forall b, \forall c, ca = cb \wedge \neg(c = 0) \rightarrow a = b$ — Cite DivideEqn

   Let a, b, and m be arbitrary.

   3.1.1. $5a \equiv_{5m} 5b$ — Assumption

   3.1.2. $5m \mid 5a - 5b$ — Def of Congruent: 3.1.1

   3.1.3. $\exists k, 5a - 5b = k\,5m$ — Def of Divides: 3.1.2

   3.1.4. $5a - 5b = i\,5m$ — Elim $\exists$: 3.1.3

   $m \mid a - b$

   $a \equiv_m b$ — Undef Congruent:

   3.1. $5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Direct Proof

$\forall a, \forall b, \forall m, 5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \rightarrow a \equiv_m b)$$

1. $\neg(5 = 0)$ — Given
2. $\forall a, \forall b, \forall c, ca = cb \wedge \neg(c = 0) \rightarrow a = b$ — Cite DivideEqn

Let a, b, and m be arbitrary.

3.1.1. $5a \equiv_{5m} 5b$ — Assumption

3.1.2. $5m \mid 5a - 5b$ — Def of Congruent: 3.1.1

3.1.3. $\exists k, 5a - 5b = k\,5m$ — Def of Divides: 3.1.2

3.1.4. $5a - 5b = i\,5m$ — Elim $\exists$: 3.1.3

$\exists k, a - b = km$ — Undef Divides:

$m \mid a - b$ — Undef Congruent:

$a \equiv_m b$ — Direct Proof

3.1. $5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Intro $\forall$

$\forall a, \forall b, \forall m, 5a \equiv_{5m} 5b \rightarrow a \equiv_m b$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \rightarrow a \equiv_m b)$$

1. $\neg(5 = 0)$ — Given
2. $\forall a, \forall b, \forall c, ca = cb \wedge \neg(c = 0) \rightarrow a = b$ — Cite DivideEqn

Let a, b, and m be arbitrary.

3.1.1. $5a \equiv_{5m} 5b$ — Assumption

3.1.2. $5m \mid 5a - 5b$ — Def of Congruent: 3.1.1

3.1.3. $\exists k, 5a - 5b = k\,5m$ — Def of Divides: 3.1.2

3.1.4. $5a - 5b = i\,5m$ — Elim $\exists$: 3.1.3

$a - b = im$

$\exists k, a - b = km$ — Intro $\exists$:

$m \mid a - b$ — Undef Divides:

3.1.11. $a \equiv_m b$ — Undef Congruent:

3.1. $5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Direct Proof

$\forall a, \forall b, \forall m, 5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \rightarrow a \equiv_m b)$$

1. $\neg(5 = 0)$ — Given
2. $\forall a, \forall b, \forall c, ca = cb \wedge \neg(c = 0) \rightarrow a = b$ — Cite DivideEqn

Let a, b, and m be arbitrary.

3.1.1. $5a \equiv_{5m} 5b$ — Assumption

3.1.2. $5m \mid 5a - 5b$ — Def of Congruent: 3.1.1

3.1.3. $\exists k, 5a - 5b = k\,5m$ — Def of Divides: 3.1.2

3.1.4. $5a - 5b = i\,5m$ — Elim $\exists$: 3.1.3

3.1.5. $5(a - b) = 5\,i\,m$ — Algebra: 3.1.4

$a - b = im$

$\exists k, a - b = km$ — Intro $\exists$:

$m \mid a - b$ — Undef Divides:

3.1.11. $a \equiv_m b$ — Undef Congruent: :

3.1. $5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Direct Proof

$\forall a, \forall b, \forall m, 5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \rightarrow a \equiv_m b)$$

1. $\neg(5 = 0)$ — Given
2. $\forall a, \forall b, \forall c, ca = cb \wedge \neg(c = 0) \rightarrow a = b$ — Cite DivideEqn

Let a, b, and m be arbitrary.

3.1.1. $5a \equiv_{5m} 5b$ — Assumption

3.1.2. $5m \mid 5a - 5b$ — Def of Congruent: 3.1.1

3.1.3. $\exists k, 5a - 5b = k\,5m$ — Def of Divides: 3.1.2

3.1.4. $5a - 5b = i\,5m$ — Elim $\exists$: 3.1.3

3.1.5. $5(a - b) = 5im$ — Algebra: 3.1.4

3.1.6. $5(a - b) = 5im \wedge \neg(5 = 0)$ — Intro $\wedge$: 3.1.5, 1

$a - b = im$

$\exists k, a - b = km$ — Intro $\exists$:

$m \mid a - b$ — Undef Divides:

3.1.11. $a \equiv_m b$ — Undef Congruent:

3.1. $5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Direct Proof

$\forall a, \forall b, \forall m, 5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \rightarrow a \equiv_m b)$$

1. $\neg(5 = 0)$ — Given
2. $\forall a, \forall b, \forall c, ca = cb \wedge \neg(c = 0) \rightarrow a = b$ — Cite DivideEqn

Let a, b, and m be arbitrary.

- 3.1.1. $5a \equiv_{5m} 5b$ — Assumption
- 3.1.2. $5m \mid 5a - 5b$ — Def of Congruent: 3.1.1
- 3.1.3. $\exists k, 5a - 5b = k\,5m$ — Def of Divides: 3.1.2
- 3.1.4. $5a - 5b = i\,5m$ — Elim $\exists$: 3.1.3
- 3.1.5. $5(a - b) = 5\,im$ — Algebra: 3.1.4
- 3.1.6. $5(a - b) = 5\,im \wedge \neg(5 = 0)$ — Intro $\wedge$: 3.1.5, 1
- 3.1.7. $5(a - b) = 5\,im \wedge \neg(5 = 0) \rightarrow a - b = im$ — Elim $\forall$: 2

$a - b = im$

$\exists k, a - b = km$ — Intro $\exists$:

$m \mid a - b$ — Undef Divides:

- 3.1.11. $a \equiv_m b$ — Undef Congruent:

3.1. $5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Direct Proof

$\forall a, \forall b, \forall m, 5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Intro $\forall$

Problem 4

$$\forall a \, \forall b \, \forall m \, (5a \equiv_{5m} 5b \rightarrow a \equiv_m b)$$

1. $\neg(5 = 0)$ — Given
2. $\forall a, \forall b, \forall c, ca = cb \wedge \neg(c = 0) \rightarrow a = b$ — Cite DivideEqn

Let a, b, and m be arbitrary.

3.1.1. $5a \equiv_{5m} 5b$ — Assumption

3.1.2. $5m \mid 5a - 5b$ — Def of Congruent: 3.1.1

3.1.3. $\exists k, 5a - 5b = k5m$ — Def of Divides: 3.1.2

3.1.4. $5a - 5b = i5m$ — Elim $\exists$: 3.1.3

3.1.5. $5(a - b) = 5im$ — Algebra: 3.1.4

3.1.6. $5(a - b) = 5im \wedge \neg(5 = 0)$ — Intro $\wedge$: 3.1.5, 1

3.1.7. $5(a - b) = 5im \wedge \neg(5 = 0) \rightarrow a - b = im$ — Elim $\forall$: 2

3.1.8. $a - b = im$ — Modus Ponens: 3.1.6, 3.1.7

3.1.9. $\exists k, a - b = km$ — Intro $\exists$: 3.1.8

3.1.10. $m \mid a - b$ — Undef Divides: 3.1.9

3.1.11. $a \equiv_m b$ — Undef Congruent: 3.1.10

3.1. $5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Direct Proof

$\forall a, \forall b, \forall m, 5a \equiv_{5m} 5b \rightarrow a \equiv_m b$ — Intro $\forall$

Problem 4

1. $\neg(5 = 0)$ — Given
2. $\forall a, \forall b, \forall c, c\,a = c\,b \wedge \neg(c = 0) \rightarrow a = b$ — Cite DivideEqn

   Let a, b, and m be arbitrary.

   3.1.1. $5\,a \equiv_{5\,m} 5\,b$ — Assumption

   3.1.2. $5\,m \mid 5\,a - 5\,b$ — Def of Congruent: 3.1.1

   3.1.3. $\exists\, k, 5\,a - 5\,b = k\,5\,m$ — Def of Divides: 3.1.2

   3.1.4. $5\,a - 5\,b = i\,5\,m$ — Elim $\exists$: 3.1.3

   3.1.5. $5\,(a - b) = 5\,i\,m$ — Algebra: 3.1.4

   3.1.6. $5\,(a - b) = 5\,i\,m \wedge \neg(5 = 0)$ — Intro $\wedge$: 3.1.5, 1

   3.1.7. $5\,(a - b) = 5\,i\,m \wedge \neg(5 = 0) \rightarrow a - b = i\,m$ — Elim $\forall$: 2

   3.1.8. $a - b = i\,m$ — Modus Ponens: 3.1.6, 3.1.7

   3.1.9. $\exists\, k, a - b = k\,m$ — Intro $\exists$: 3.1.8

   3.1.10. $m \mid a - b$ — Undef Divides: 3.1.9

   3.1.11. $a \equiv_m b$ — Undef Congruent: 3.1.10

   3.1. $5\,a \equiv_{5\,m} 5\,b \rightarrow a \equiv_m b$ — Direct Proof

3. $\forall a, \forall b, \forall m, 5\,a \equiv_{5\,m} 5\,b \rightarrow a \equiv_m b$ — Intro $\forall$

Problem 4

English proof for reference…

Let a, b, and m be arbitrary integers.

Suppose that $5a \equiv_{5m} 5b$. This tells us, by definition of congruence, that $5m \mid 5a - 5b$, which means that $5a - 5b = i(5m)$ for some integer i, by definition of divides. We can rewrite that equivalently as $5(a-b) = 5(im)$. Using this and the fact that $5 \neq 0$, we can apply DivideEqn to get that $a - b = im$, which tells us that $m \mid a - b$, by the definition of divides, and the latter tells us that $a \equiv_m b$, by the definition of congruence.

Since a, b, and m were arbitrary, we proven the claim.

That's All Folks

Written by Aruna & Zareef