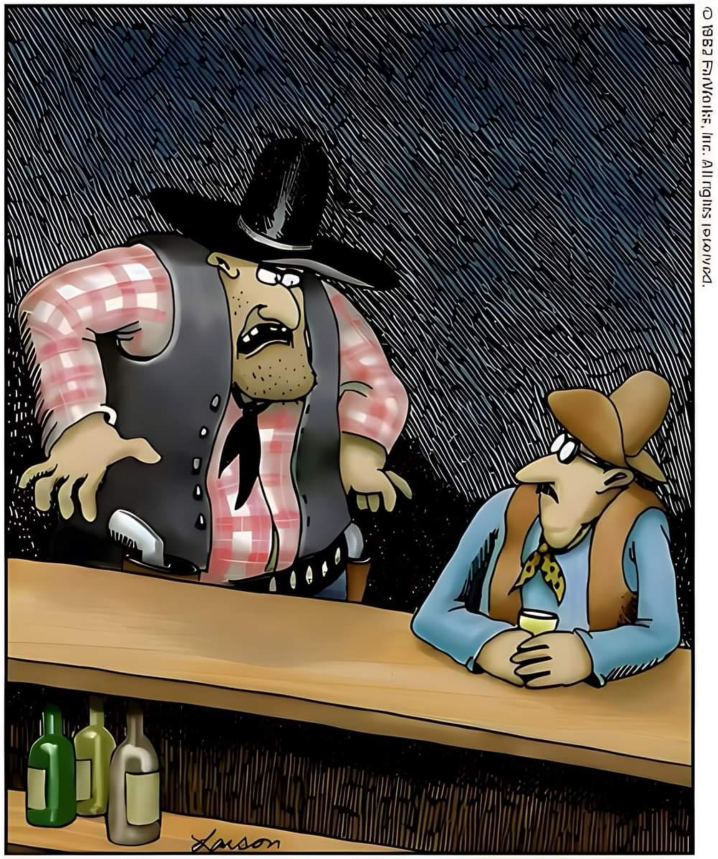
CSE 311: Foundations of Computing

Topic 4: Number Theory



"I *asked* you a question, buddy. ... What's the square root of 5,248?"

Formal Proofs

- In principle, formal proofs are the standard for what it means to be "proven" in mathematics
  - almost all math (and theory CS) done in Predicate Logic

- But they can be tedious and impractical
  - e.g., applications of commutativity and associativity
  - Russell & Whitehead's formal proof that 1+1 = 2 is *several hundred pages* long

    we allow ourselves to cite "Arithmetic", "Algebra", etc.

- *Historically*, rarely used for "real mathematics"…

English Proofs

- Vastly more common in CS and math

- High-level language that lets us work more quickly
  - not necessary to spell out *every* detail
  - reader checks that the writer is not skipping too much

    the reader is the "compiler" for English proofs

    they implement a community standard of correctness

- English proofs require understanding formal proofs
  - English proof follows the structure of a formal proof
  - we will learn English proofs by translating from formal

    eventually, we will write English directly

English Proofs

- Vastly more common in CS and math

- High-level language that lets us work more quickly
  - not necessary to spell out *every* detail
  - reader checks that the writer is not skipping too much

    the reader is the "compiler" for English proofs

    they implement a community standard of correctness

- Examples of what can be skipped (more to come):
  - Intro and Elim ∧
  - explicitly stating existence claims (Elim ∃ immediately)
  - no rule names, e.g., Direct Proof

Recall: Even and Odd

$\text{Even}(x) := \exists y\ (x=2y)$
$\text{Odd}(x) := \exists y\ (x=2y+1)$
Domain: Integers

Prove: “The square of any even number is even.”

Formal proof of: $\forall x\ (\text{Even}(x) \rightarrow \text{Even}(x^2))$

Let a be an arbitrary integer

1.1.1	$\text{Even}(\mathbf{a})$	Assumption
1.1.2	$\exists y\ (\mathbf{a} = 2y)$	Definition of Even: 1.1.1
1.1.3	$\mathbf{a} = 2\mathbf{b}$	Elim $\exists$ (**b**): 1.1.2
1.1.4	$\mathbf{a}^2 = 2(2\mathbf{b}^2)$	Algebra: 1.1.3
1.1.5	$\exists y\ (\mathbf{a}^2 = 2y)$	Intro $\exists$: 1.1.4
1.1.6	$\text{Even}(\mathbf{a}^2)$	Definition of Even: 1.1.5
1.1	$\text{Even}(\mathbf{a})\rightarrow\text{Even}(\mathbf{a}^2)$	Direct proof
1.	$\forall x\ (\text{Even}(x)\rightarrow\text{Even}(x^2))$	Intro $\forall$

English Proof: Even and Odd

Even(x) $\equiv \exists y\ (x=2y)$
Odd(x) $\equiv \exists y\ (x=2y+1)$
Domain: Integers

Prove "The square of every even integer is even."

Let a be an arbitrary integer.	Let a be an arbitrary integer		
Suppose a is even.	1.1.1	Even(a)	Assumption
Then, by definition, a = 2b for some integer b.	1.1.2 1.1.3	$\exists y\ (a = 2y)$ $a = 2b$	Definition Elim $\exists$
Squaring both sides, we get $a^2 = 4b^2 = 2(2b^2)$.	1.1.4	$a^2 = 2(2b^2)$	Algebra
So a^2 is, by definition, even.	1.1.5 1.1.6	$\exists y\ (a^2 = 2y)$ Even(a^2)	Intro $\exists$ Definition
Since a was arbitrary, we have shown that the square of every even number is even.	1.1. 1.	Even(a)$\rightarrow$Even(a^2) $\forall x$ (Even(x)$\rightarrow$Even(x^2))	Direct Proof Intro $\forall$

English Proof: Even and Odd

Even(x) ≡ ∃y (x=2y)
Odd(x) ≡ ∃y (x=2y+1)
Domain: Integers

Prove "The square of every even integer is even."

Proof: Let **a** be an arbitrary integer.

Suppose **a** is even. Then, by definition, $\mathbf{a} = 2\mathbf{b}$ for some integer b. Squaring both sides, we get $\mathbf{a}^2 = 4\mathbf{b}^2 = 2(2\mathbf{b}^2)$. So $\mathbf{a}^2$ is, by definition, is even.

Since **a** was arbitrary, we have shown that the square of every even number is even. ■

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

Prove "The sum of two odd numbers is even."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

Prove "The sum of two odd numbers is even."

Formally, prove $\forall x\ \forall y\ ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y))$

Let x and y be arbitrary integers.

Since x and y were arbitrary, the sum of any odd integers is even.

Let x and y be arbitrary integers.

1.1. $(\text{Odd}(\mathbf{x}) \land \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(\mathbf{x+y})$

1. $\forall x\ \forall y\ ((\text{Odd}(\mathbf{x}) \land \text{Odd}(\mathbf{y})) \rightarrow \text{Even}(x+y))$ Intro ∀

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

Prove "The sum of two odd numbers is even."

Formally, prove ∀x ∀y ((Odd(x) ∧ Odd(y))→Even(x+y))

Let x and y be arbitrary integers.

Suppose that both are odd.

so x+y is even.

Since x and y were arbitrary, the sum of any odd integers is even.

Let x and y be arbitrary integers

1.1.1 Odd(**x**) ∧ Odd(**y**) Assumption

1.1.9 Even(**x+y**)

1.1. (Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**) Direct..

1. ∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(x+y)) Intro ∀

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

Prove “The sum of two odd numbers is even.”

Formally, prove $\forall x\ \forall y\ ((\mathrm{Odd}(x) \land \mathrm{Odd}(y)) \rightarrow \mathrm{Even}(x+y))$

Let x and y be arbitrary integers.

Suppose that both are odd.

so x+y is even.

Since x and y were arbitrary, the sum of any odd integers is even.

Let x and y be arbitrary integers

1.1.1	Odd(**x**) ∧ Odd(**y**)	Assumption
1.1.2	Odd(**x**)	Elim ∧
1.1.3	Odd(**y**)	Elim ∧
1.1.9	Even(**x+y**)	

1.1. (Odd(**x**) ∧ Odd(**y**)) → Even(**x+y**) Direct..

1. ∀x ∀y ((Odd(**x**) ∧ Odd(**y**)) → Even(x+y)) Intro ∀

English Proof: Even and Odd

$\mathrm{Even}(x) \equiv \exists y\ (x=2y)$
$\mathrm{Odd}(x) \equiv \exists y\ (x=2y+1)$
Domain: Integers

Prove "The sum of two odd numbers is even."

Let x and y be arbitrary integers.

Suppose that both are odd.

Then, we have x = 2a+1 for some integer a and y = 2b+1 for some integer b.

so x+y is, by definition, even.

Since x and y were arbitrary, the sum of any odd integers is even.

Let x and y be arbitrary integers.

1.1.1	$\mathrm{Odd}(x) \land \mathrm{Odd}(y)$	Assumption
1.1.2	$\mathrm{Odd}(x)$	Elim ∧
1.1.3	$\mathrm{Odd}(y)$	Elim ∧
1.1.4	$\exists z\ (x = 2z+1)$	Def of Odd: 1.1.2
1.1.5	$x = 2a+1$	Elim ∃
1.1.6	$\exists z\ (y = 2z+1)$	Def of Odd: 1.1.3
1.1.7	$y = 2b+1$	Elim ∃
1.1.9	$\exists z\ (x+y = 2z)$	Intro ∃
1.1.10	$\mathrm{Even}(x+y)$	Def of Even
1.1.	$(\mathrm{Odd}(x) \land \mathrm{Odd}(y)) \rightarrow \mathrm{Even}(x+y)$	Direct..
1.	$\forall x\ \forall y\ ((\mathrm{Odd}(x) \land \mathrm{Odd}(y)) \rightarrow \mathrm{Even}(x+y))$	Intro ∀

English Proof: Even and Odd

$\text{Even}(x) \equiv \exists y\ (x=2y)$
$\text{Odd}(x) \equiv \exists y\ (x=2y+1)$
Domain: Integers

Prove "The sum of two odd numbers is even."

Let x and y be arbitrary integers.

Suppose that both are odd.

Then, we have x = 2a+1 for some integer a and y = 2b+1 for some integer b.

Their sum is x+y = ... = 2(a+b+1)

so x+y is, by definition, even.

Since x and y were arbitrary, the sum of any odd integers is even.

Let x and y be arbitrary integers.

1.1.1	$\text{Odd}(x) \land \text{Odd}(y)$	Assumption
1.1.2	$\text{Odd}(x)$	Elim ∧
1.1.3	$\text{Odd}(y)$	Elim ∧
1.1.4	$\exists z\ (x = 2z+1)$	Def of Odd: 1.1.2
1.1.5	$x = 2a+1$	Elim ∃
1.1.6	$\exists z\ (y = 2z+1)$	Def of Odd: 1.1.3
1.1.7	$y = 2b+1$	Elim ∃
1.1.8	$x+y = 2(a+b+1)$	Algebra
1.1.9	$\exists z\ (x+y = 2z)$	Intro ∃
1.1.10	$\text{Even}(x+y)$	Def of Even
1.1.	$(\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y)$	Direct..
1.	$\forall x\ \forall y\ ((\text{Odd}(x) \land \text{Odd}(y)) \rightarrow \text{Even}(x+y))$	Intro ∀

Even and Odd

Predicate Definitions

Even(x) ≡ $\exists y\ (x = 2y)$

Odd(x) ≡ $\exists y\ (x = 2y + 1)$

Domain of Discourse

Integers

Prove "The sum of two odd numbers is even."

Proof: Let x and y be arbitrary integers.

Suppose that both are odd. Then, we have x = 2a+1 for some integer a and y = 2b+1 for some integer b. Their sum is x+y = (2a+1) + (2b+1) = 2a+2b+2 = 2(a+b+1), so x+y is, by definition, even.

Since x and y were arbitrary, the sum of any two odd integers is even. ■

Formal-to-English Translation

- Document posted on website

- Use these on HW4
  - no need to match the *exact* phrasing
  - English proofs are not formal proofs

Number Theory

- Direct relevance to computing
  - everything in a computer is a number

    colors on the screen are encoded as numbers

- Many significant applications
  - Cryptography & Security
  - Data Structures
  - Distributed Systems

Recall: Elementary School Division

For a, b with $b > 0$, we can divide b into a. Suppose that

$$\frac{a}{b} = q$$

The number q is called the *quotient*.

This equation involve fractions. We want to stick to integers! Multiplying both sides by b, this becomes

$$a = qb$$

When there exists some such q, we write "$b \mid a$".

Divisibility

Domain of Discourse
Integers

Definition: "b divides a"

For a, b (usually with $b \neq 0$):

$$b \mid a \ :=\ \exists q\ (a = qb)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
1 | 5	5 | 25	0 | 5	2 | 3

Divisibility

Domain of Discourse

Integers

Definition: "b divides a"

For a, b (usually with $b \neq 0$):

$$b \mid a \; \coloneqq \; \exists q\,(a = qb)$$

Check Your Understanding. Which of the following are true?

5 | 1 5 | 1 iff 1 = 5k	25 | 5 25 | 5 iff 5 = 25k	[✓ 5 | 0] 5 | 0 iff 0 = 5k	3 | 2 3 | 2 iff 2 = 3k
[✓ 1 | 5] 1 | 5 iff 5 = 1k	[✓ 5 | 25] 5 | 25 iff 25 = 5k	0 | 5 0 | 5 iff 5 = 0k	2 | 3 2 | 3 iff 3 = 2k

Recall: Elementary School Division

For a, b with $b > 0$, we can divide b into a.

If $b \nmid a$, then we end up with a *remainder* r with $0 < r < b$.
Now,

instead of $\dfrac{a}{b} = q$ we have $\dfrac{a}{b} = q + \dfrac{r}{b}$

Multiplying both sides by b gives us $a = qb + r$

Recall: Elementary School Division

For a, b with $b > 0$, we can divide b into a.

If $b \mid a$, then we have $a = qb$ for some q.
If $b \nmid a$, then we have $a = qb + r$ for some q, r with $0 < \mathrm{r} < \mathrm{b}$.

In general, we have $a = qb + r$ for some q, r with $0 \leq r < b$, where $r = 0$ iff $b \mid a$.

Division Theorem

Domain of Discourse
Integers

Division Theorem

For a, b with $b > 0$
there exist *unique* integers q, r with $0 \leq r < b$
such that $a = qb + r$.

To put it another way, if we divide b **into** a**, we get a unique quotient** $q = a$ **div** b
and non-negative remainder $r = a$ **mod** b

$$a = (a \textbf{ div } b)\, b + (a \textbf{ mod } b)$$

$$\forall a\, \forall b\, \big((b > 0) \rightarrow \big(a = (a \textbf{ div } b)b + (a \textbf{ mod } b)\big)\big)$$

Modular Arithmetic

Modular Arithmetic

- Arithmetic over a finite domain

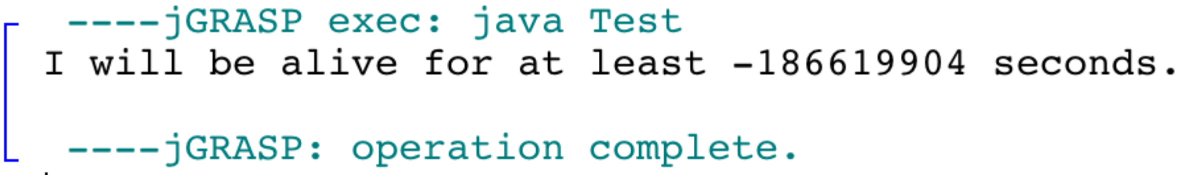
- Almost all computation is over a finite domain

I’m ALIVE!

```
public class Test {
   final static int SEC_IN_YEAR = 365*24*60*60;
   public static void main(String args[]) {
      System.out.println(
         “I will be alive for at least ” +
         SEC_IN_YEAR * 101 + “ seconds.”
      );
   }
}
```

I’m ALIVE!

```
public class Test {
   final static int SEC_IN_YEAR = 365*24*60*60;
   public static void main(String args[]) {
      System.out.println(
         “I will be alive for at least ” +
         SEC_IN_YEAR * 101 + “ seconds.”
      );
   }
}
```

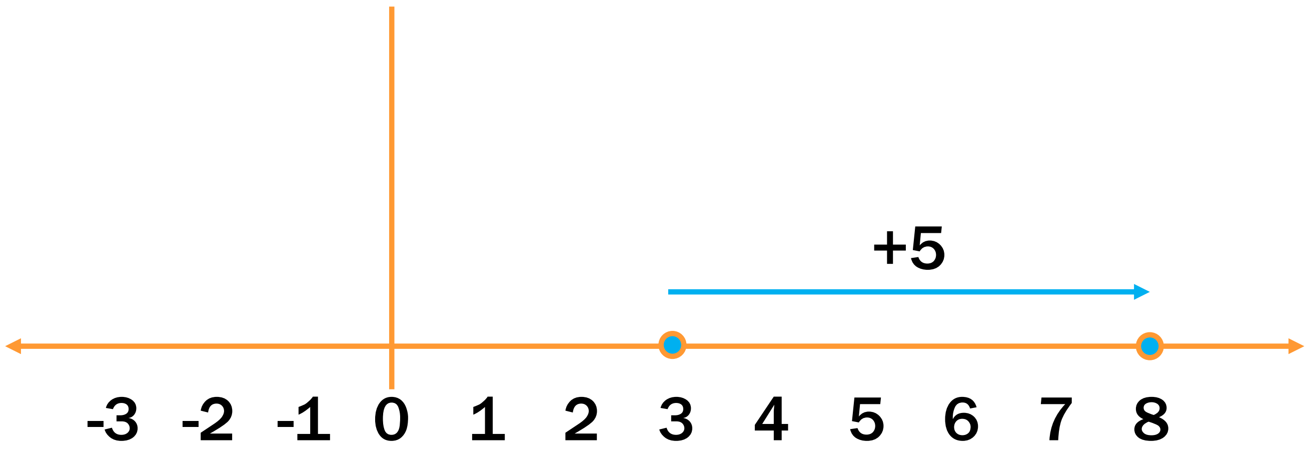


```
 ----jGRASP exec: java Test
I will be alive for at least -186619904 seconds.

 ----jGRASP: operation complete.
```

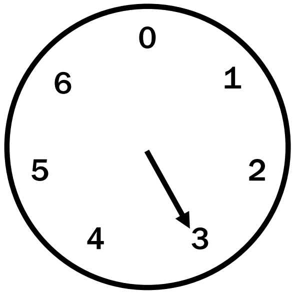
Ordinary arithmetic

3 + 5 = 8



Arithmetic on a Clock

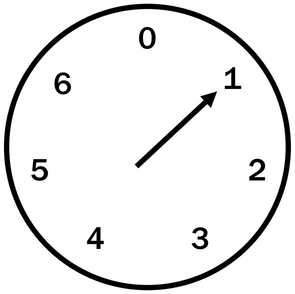
$3 + 5 = 8$



$8 = 7 \cdot 1 + 1$

$15 = 7 \cdot 2 + 1$

$22 = 7 \cdot 3 + 1$

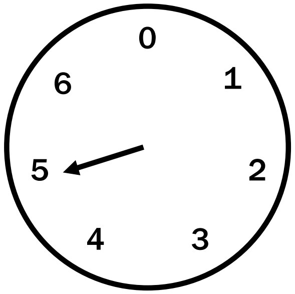


If $a = 7q + r$, then $r \ (= a \bmod b)$ is where you stop after taking a steps on the clock

Arithmetic, mod 7

$(a + b) \bmod 7$

$(a \times b) \bmod 7$



+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modular Arithmetic

Domain of Discourse

Integers

Definition: "a is congruent to b modulo m"

For a, b, m with $m > 0$

$$a \equiv_m b \ \coloneqq \ m \mid (a - b)$$

New notion of "sameness" that will help us understand modular arithmetic

Modular Arithmetic

Domain of Discourse

Integers

Definition: “a is congruent to b modulo m”

For a, b, m with $m > 0$

$$a \equiv_m b \;\; := \;\; m \mid (a - b)$$

The standard math notation is

$$a \equiv b \pmod{m}$$

A chain of equivalences is written

$$a \equiv b \equiv c \equiv d \pmod{m}$$

Many students find this confusing,
so we will use $\equiv_m$ instead.

Modular Arithmetic

Domain of Discourse
Integers

Definition: "a is congruent to b modulo m"

For a, b, m with $m > 0$

$$a \equiv_m b \ := \ m \mid (a - b)$$

Check Your Understanding. What do each of these mean? When are they true?

$-1 \equiv_5 19$

This statement is true. 19 - (-1) = 20 which is divisible by 5

$x \equiv_2 0$

This statement is the same as saying "x is even"; so, any x that is even (including negative even numbers) will work.

$y \equiv_7 2$

This statement is true for y in { ..., -12, -5, 2, 9, 16, ...}. In other words, all y of the form 2+7k for k an integer.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

Proof Plan:

1. $(\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}) \rightarrow (\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b})$ **??**
2. $(\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}) \rightarrow (\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m})$ **??**
3. $(\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}) \rightarrow (\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}) \wedge$
   $(\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}) \rightarrow (\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m})$ **Intro $\wedge$: 1, 2**
4. $(\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}) \leftrightarrow (\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m})$ **Equivalent: 3**

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \textbf{ mod } \boldsymbol{m} = \boldsymbol{b} \textbf{ mod } \boldsymbol{m}$.

1. $(\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}) \rightarrow (\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b})$??

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

1.1. $a \bmod m = b \bmod m$	Assumption
1.? $a \equiv_m b$	??
1. $(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b)$	Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

1.1. $\boldsymbol{a \bmod m = b \bmod m}$	Assumption
1.? $\boldsymbol{m \mid a - b}$	??
1.? $\boldsymbol{a \equiv_m b}$	Def of ≡
1. $\boldsymbol{(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b)}$	Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \ \mathbf{mod}\ \boldsymbol{m} = \boldsymbol{b}\ \mathbf{mod}\ \boldsymbol{m}$.

1.1. $a \bmod m = b \bmod m$ Assumption

1.? $\exists q\ (a - b = qm)$??

1.? $m \mid a - b$ Def of |

1.? $a \equiv_m b$ Def of ≡

1. $(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b)$ Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

1.1. $a \bmod m = b \bmod m$	Assumption
1.2. $a = (a \operatorname{div} m)\, m + (a \bmod m)$	Apply Division
1.3. $b = (b \operatorname{div} m)\, m + (b \bmod m)$	Apply Division
1.? $\exists q\ (a - b = qm)$	??
1.? $m \mid a - b$	Def of |
1.? $a \equiv_m b$	Def of ≡
1. $(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b)$	Direct Proof

Modular Arithmetic: A Property

Let a, b, m be integers with $m > 0$.
Then, $a \equiv_m b$ if and only if $a \bmod m\ =\ b \bmod m$.

1.1. $a \bmod m = b \bmod m$	Assumption
1.2. $a = (a \operatorname{div} m)\, m + (a \bmod m)$	Apply Division
1.3. $b = (b \operatorname{div} m)\, m + (b \bmod m)$	Apply Division
1.4. $a - b = \big((a \operatorname{div} m) - (b \operatorname{div} m)\big)\, m$	Algebra
1.5. $\exists q\ (a - b = qm)$	Intro ∃
1.6. $m \mid a - b$	Def of |
1.7. $a \equiv_m b$	Def of ≡
1. $(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b)$	Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

Suppose that $a \bmod m = b \bmod m$.

Assumption

Apply Division
Apply Division

Algebra

Intro ∃
Def of |
Def of ≡
Direct Proof

Therefore, $a \equiv_m b$.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m\ =\ b \bmod m}$.

Suppose that $a \bmod m = b \bmod m$. — Assumption

By the Division Theorem, we can write
$a = (a \operatorname{div} m)\, m + (a \bmod m)$ and — Apply Division
$b = (b \operatorname{div} m)\, m + (b \bmod m)$. — Apply Division

Algebra

Intro ∃

Def of |

Def of ≡

Therefore, $a \equiv_m b$.

Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m \ = \ b \bmod m}$.

Suppose that $a \bmod m = b \bmod m$.

Assumption

By the Division Theorem, we can write
$a = (a \operatorname{div} m)\, m + (a \bmod m)$ and
$b = (b \operatorname{div} m)\, m + (b \bmod m)$.

Apply Division
Apply Division

Subtracting these we can see that

$$\begin{aligned} a - b &= \big((a \operatorname{div} m) - (b \operatorname{div} m)\big)m + \\ &\qquad ((a \bmod m) - (b \bmod m)) \\ &= \big((a \operatorname{div} m) - (b \operatorname{div} m)\big)\, m \end{aligned}$$

Algebra

since $(a \bmod m) - (b \bmod m) = 0$.

…

Therefore, $a \equiv_m b$.

Intro ∃
Def of |
Def of ≡
Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m \ = \ b \bmod m}$.

Suppose that $a \bmod m = b \bmod m$.

Assumption

By the Division Theorem, we can write
$a = (a \operatorname{div} m)\, m + (a \bmod m)$ and
$b = (b \operatorname{div} m)\, m + (b \bmod m)$.

Apply Division
Apply Division

Subtracting these we can see that

$$\begin{aligned} a - b &= \big((a \operatorname{div} m) - (b \operatorname{div} m)\big)m + \\ &\qquad ((a \bmod m) - (b \bmod m)) \\ &= \big((a \operatorname{div} m) - (b \operatorname{div} m)\big)\, m \end{aligned}$$

since $(a \bmod m) - (b \bmod m) = 0$.

Algebra

Therefore, by definition of divides, $m \mid (a - b)$
and so $a \equiv_m b$, by definition of congruent.

Intro ∃
Def of |
Def of ≡
Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \mathbf{\ mod\ } \boldsymbol{m} = \boldsymbol{b} \mathbf{\ mod\ } \boldsymbol{m}$.

2. $(\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}) \rightarrow (\boldsymbol{a} \mathbf{\ mod\ } \boldsymbol{m} = \boldsymbol{b} \mathbf{\ mod\ } \boldsymbol{m})$??

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

2.1. $a \equiv_m b$ Assumption

2.? $a \bmod m = b \bmod m$??

2. $(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$ Direct Proof

Modular Arithmetic: A Property

Let a, b, m be integers with $m > 0$.
Then, $a \equiv_m b$ if and only if $a \bmod m = b \bmod m$.

2.1. $a \equiv_m b$	Assumption
2.2. $m \mid a - b$	Def of |
2.? $a \bmod m = b \bmod m$	??
2. $(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$	Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

2.1. $a \equiv_m b$	Assumption
2.2. $m \mid a - b$	Def of ≡
2.3. $\exists q\ (a - b = qm)$	Def of |
2.? $a \bmod m = b \bmod m$	??
2. $(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$	Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

2.1. $a \equiv_m b$	Assumption
2.2. $m \mid a - b$	Def of ≡
2.3. $\exists q\ (a - b = qm)$	Def of |
2.4. $a - b = km$	Elim ∃
2.? $a \bmod m = b \bmod m$	??
2. $(a \equiv_m b) \to (a \bmod m = b \bmod m)$	Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} \ = \ \boldsymbol{b} \bmod \boldsymbol{m}$.

2.1. $a \equiv_m b$	Assumption
2.2. $m \mid a - b$	Def of ≡
2.3. $\exists q\ (a - b = qm)$	Def of |
2.4. $a - b = km$	Elim ∃
2.5. $a = (a \operatorname{div} m)\, m + (a \bmod m)$	Apply Division
2.? $a \bmod m = b \bmod m$	??
2. $(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$	Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

2.1. $\boldsymbol{a \equiv_m b}$ Assumption

2.2. $\boldsymbol{m \mid a - b}$ Def of ≡

2.3. $\boldsymbol{\exists q\ (a - b = qm)}$ Def of |

2.4. $\boldsymbol{a - b = km}$ Elim ∃

2.5. $\boldsymbol{a = (a \operatorname{div} m)\, m + (a \bmod m)}$ Apply Division

2.6. $\boldsymbol{b = (a \operatorname{div} m - k)\, m + (a \bmod m)}$ Algebra

2.? $\boldsymbol{a \bmod m = b \bmod m}$??

2. $\boldsymbol{(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)}$ Direct Proof

Modular Arithmetic: A Property

Let a, b, m be integers with $m > 0$.
Then, $a \equiv_m b$ if and only if $a \bmod m = b \bmod m$.

2.1. $a \equiv_m b$	Assumption
2.2. $m \mid a - b$	Def of ≡
2.3. $\exists q\ (a - b = qm)$	Def of |
2.4. $a - b = km$	Elim ∃
2.5. $a = (a \operatorname{div} m)\, m + (a \bmod m)$	Apply Division
2.6. $b = (a \operatorname{div} m - k)\, m + (a \bmod m)$	Algebra
2.7. $b \operatorname{div} m = (a \operatorname{div} m - k) \wedge$ $b \bmod m = a \bmod m$	Apply DivUnique
2.? $a \bmod m = b \bmod m$	??
2. $(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$	Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

2.1. $a \equiv_m b$	Assumption
2.2. $m \mid a - b$	Def of ≡
2.3. $\exists q\ (a - b = qm)$	Def of |
2.4. $a - b = km$	Elim ∃
2.5. $a = (a \operatorname{div} m)\, m + (a \bmod m)$	Apply Division
2.6. $b = (a \operatorname{div} m - k)\, m + (a \bmod m)$	Algebra
2.7. $b \operatorname{div} m = (a \operatorname{div} m - k) \land$ $b \bmod m = a \bmod m$	Apply DivUnique
2.8. $a \bmod m = b \bmod m$	Elim ∧
2. $(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$	Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

Suppose that $a \equiv_m b$.

Assumption

Def of ≡
Def of |
Elim ∃

Apply Division

Algebra

Apply DivUnique
Elim ∃

Therefore, $a \bmod m = b \bmod m$.

Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

Suppose that $a \equiv_m b$.

Then, $m \mid (a - b)$ by the definition of congruence.
So, $a - b = km$ for some integer k by the definition of divides. Equivalently, $a = b + km$.

Therefore, $a \bmod m = b \bmod m$.

Assumption

Def of ≡
Def of |
Elim ∃

Apply Division

Algebra

Apply DivUnique
Elim ∃

Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

Suppose that $a \equiv_m b$.

Assumption

Then, $m \mid (a - b)$ by the definition of congruence.
So, $a - b = km$ for some integer k by the definition of divides. Equivalently, $a = b + km$.

Def of ≡
Def of |
Elim ∃

By the Division Theorem, we have $a = (a \operatorname{div} m)\, m + (a \bmod m)$, with $0 \leq (a \bmod m) < m$.

Apply Division

Algebra

Apply DivUnique
Elim ∃

Therefore, $a \bmod m = b \bmod m$.

Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m \ = \ b \bmod m}$.

Suppose that $a \equiv_m b$.

Assumption

Then, $m \mid (a - b)$ by the definition of congruence.
So, $a - b = km$ for some integer k by the definition of divides. Equivalently, $a = b + km$.

Def of ≡
Def of |
Elim ∃

By the Division Theorem, we have $a = (a \operatorname{div} m)\ m + (a \bmod m)$, with $0 \leq (a \bmod m) < m$.

Apply Division

Combining these, we have $(a \operatorname{div} m)m + (a \bmod m) = a = b + km$. Solving for b gives $\mathrm{b} = (a \operatorname{div} m)\ m + (a \bmod m) - km = \big((a \operatorname{div} m) - k\big)m + (a \bmod m)$.

Algebra

Apply DivUnique
Elim ∃

Therefore, $a \bmod m = b \bmod m$.

Direct Proof

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

Suppose that $a \equiv_m b$.

Assumption

Then, $m \mid (a - b)$ by the definition of congruence.
So, $a - b = km$ for some integer k by the definition of divides. Equivalently, $a = b + km$.

Def of ≡
Def of |
Elim ∃

By the Division Theorem, we have $a = (a \operatorname{div} m)\, m + (a \bmod m)$, with $0 \leq (a \bmod m) < m$.

Apply Division

Combining these, we have $(a \operatorname{div} m)m + (a \bmod m) = a = b + km$. Solving for b gives b $= (a \operatorname{div} m)\, m + (a \bmod m) - km = \big((a \operatorname{div} m) - k\big)m + (a \bmod m)$.

Algebra

By the uniqueness property in the Division Theorem, we must have $b \bmod m = a \bmod m$ (and, although we don't need it, also $b \operatorname{div} m = a \operatorname{div} m - k$).

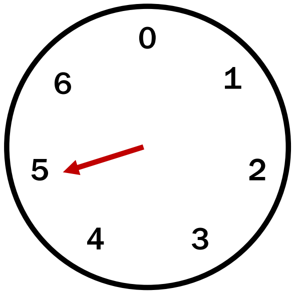
Apply DivUnique
Elim ∃

Direct Proof

The $\text{mod}\ m$ function vs the $\equiv_m$ predicate

– **The $\text{mod}\ m$ function maps any integer a to a remainder $a \text{ mod } m \in \{0,1,..,m-1\}$.**

Tells you where it lands on the clock.



– **Imagine grouping together all integers that have the same value of the $\text{mod}\ m$ function.**

They must differ by a multiple of m ($q_1 m + r$ vs $q_2 m + r$)

– **The $\equiv_m$ predicate compares integers a, b to see if if they differ by a multiple of m.**

If they differ by a multiple of m, then walking from one to the other leaves you at the same spot on the clock.

Recall: Familiar Properties of "="

- **If $a = b$ and $b = c$, then $a = c$.**
  - **i.e., if $a = b = c$, then $a = c$**

- **If $a = b$ and $c = d$, then $a + c = b + d$.**
  - **since $c = c$ is true, we can "$+ c$" to both sides**

- **If $a = b$ and $c = d$, then $ac = bd$.**
  - **since $c = c$ is true, we can "$\times c$" to both sides**

These facts allow us to use algebra to solve problems

The Algebra Rule

$$\boxed{\text{Algebra}}\ \frac{x_1 = y_1 \quad \dots \quad x_n = y_n}{\therefore\ x = y}$$

- **Algebra rule applies these properties:**
  - **adding equations**
  - **multiplying equations by a *constant***

Note: no division (since domain is integers)

- **But also uses knowledge of**
  - **arithmetic with constants**
  - **commutativity of multiplication (e.g.,** $yx = xy$**)**
  - **distributivity (e.g.,** $a(b+c) = ab + bc$**)**

Recall: Familiar Properties of “=”

- If $a = b$ and $b = c$, then $a = c$.
  - i.e., if $a = b = c$, then $a = c$

- If $a = b$ and $c = d$, then $a + c = b + d$.
  - since $c = c$ is true, we can “$+\ c$” to both sides

- If $a = b$ and $c = d$, then $ac = bd$.
  - since $c = c$ is true, we can “$\times\ c$” to both sides

Same facts apply to “≤”

with non-negative numbers

What about “$\equiv_{\boldsymbol{m}}$”?

Modular Arithmetic: Basic Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m} > \boldsymbol{0}$.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

Modular Arithmetic: Basic Property

Let $\boldsymbol{a, b, c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m > 0}$.
If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{b \equiv_m c}$, then $\boldsymbol{a \equiv_m c}$.

1. $\boldsymbol{(a \equiv_m b \wedge b \equiv_m c) \rightarrow (a \equiv_m c)}$??

Modular Arithmetic: Basic Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

2.1. $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b} \wedge \boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$ Assumption

2.?. $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$??

1. $(\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b} \wedge \boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}) \rightarrow (\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c})$ Direct Proof

Modular Arithmetic: Basic Property

Let $\boldsymbol{a, b, c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m > 0}$.
If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{b \equiv_m c}$, then $\boldsymbol{a \equiv_m c}$.

2.1. $\boldsymbol{a \equiv_m b \land b \equiv_m c}$	Assumption
2.2. $\boldsymbol{a \equiv_m b}$	Elim $\land$: 2.1
2.3. $\boldsymbol{b \equiv_m c}$	Elim $\land$: 2.1
2.?. $\boldsymbol{a \equiv_m c}$	??
1. $\boldsymbol{(a \equiv_m b \land b \equiv_m c) \rightarrow (a \equiv_m c)}$	Direct Proof

Modular Arithmetic: Basic Property

Let a, b, c and m be integers with $m > 0$.
If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

2.1. $a \equiv_m b \wedge b \equiv_m c$	Assumption
2.2. $a \equiv_m b$	Elim $\wedge$: 2.1
2.3. $b \equiv_m c$	Elim $\wedge$: 2.1
2.4. $m \mid a - b$	Def of ≡: 2.2
2.5. $m \mid b - c$	Def of ≡: 2.3
2.?. $a \equiv_m c$	??
1. $(a \equiv_m b \wedge b \equiv_m c) \rightarrow (a \equiv_m c)$	Direct Proof

Modular Arithmetic: Basic Property

Let $\boldsymbol{a, b, c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m > 0}$.
If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{b \equiv_m c}$, then $\boldsymbol{a \equiv_m c}$.

2.1. $a \equiv_m b \wedge b \equiv_m c$	Assumption
2.2. $a \equiv_m b$	Elim $\wedge$: 2.1
2.3. $b \equiv_m c$	Elim $\wedge$: 2.1
2.4. $m \mid a - b$	Def of ≡: 2.2
2.5. $m \mid b - c$	Def of ≡: 2.3
2.6. $\exists q\ (a - b = qm)$	Def of |: 2.4
2.7. $\exists q\ (b - c = qm)$	Def of |: 2.5
2.?. $a \equiv_m c$	??
1. $(a \equiv_m b \wedge b \equiv_m c) \rightarrow (a \equiv_m c)$	Direct Proof

Modular Arithmetic: Basic Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

2.1. $a \equiv_m b \wedge b \equiv_m c$	Assumption
2.2. $a \equiv_m b$	Elim $\wedge$: 2.1
2.3. $b \equiv_m c$	Elim $\wedge$: 2.1
2.4. $m \mid a - b$	Def of ≡: 2.2
2.5. $m \mid b - c$	Def of ≡: 2.3
2.6. $\exists q\ (a - b = qm)$	Def of |: 2.4
2.7. $\exists q\ (b - c = qm)$	Def of |: 2.5
2.8. $a - b = km$	Elim $\exists$: 2.6
2.9. $b - c = jm$	Elim $\exists$: 2.7
2.?. $a \equiv_m c$	??
1. $(a \equiv_m b \wedge b \equiv_m c) \rightarrow (a \equiv_m c)$	Direct Proof

Modular Arithmetic: Basic Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

2.1. $\boldsymbol{a \equiv_m b \land b \equiv_m c}$	Assumption
…	
2.8. $\boldsymbol{a - b = km}$	Elim ∃: 2.6
2.9. $\boldsymbol{b - c = jm}$	Elim ∃: 2.7
2.?. $\boldsymbol{a \equiv_m c}$	??
1. $\boldsymbol{(a \equiv_m b \land b \equiv_m c) \rightarrow (a \equiv_m c)}$	Direct Proof

Modular Arithmetic: Basic Property

Let a, b, c and m be integers with $m > 0$.
If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

2.1. $a \equiv_m b \land b \equiv_m c$	Assumption
…	
2.8. $a - b = km$	Elim $\exists$: 2.6
2.9. $b - c = jm$	Elim $\exists$: 2.7
2.?. $m \mid a - b$	??
2.?. $a \equiv_m c$	Def of $\equiv$
1. $(a \equiv_m b \land b \equiv_m c) \rightarrow (a \equiv_m c)$	Direct Proof

Modular Arithmetic: Basic Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

2.1. $a \equiv_m b \land b \equiv_m c$	Assumption
…	
2.8. $a - b = km$	Elim ∃: 2.6
2.9. $b - c = jm$	Elim ∃: 2.7
2.?. $\exists q\ (a - c = qm)$	??
2.?. $m \mid a - c$	Def of |
2.?. $a \equiv_m c$	Def of ≡
1. $(a \equiv_m b \land b \equiv_m c) \rightarrow (a \equiv_m c)$	Direct Proof

Modular Arithmetic: Basic Property

Let a, b, c and m be integers with $m > 0$.
If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

2.1. $a \equiv_m b \land b \equiv_m c$	Assumption
…	
2.8. $a - b = km$	Elim ∃: 2.6
2.9. $b - c = jm$	Elim ∃: 2.7
2.10. $a - c = (k + j)m$	Algebra
2.11. $\exists q\ (a - c = qm)$	Intro ∃: 2.10
2.12. $m \mid a - c$	Def of |: 2.11
2.13. $a \equiv_m c$	Def of ≡: 2.12
1. $(a \equiv_m b \land b \equiv_m c) \rightarrow (a \equiv_m c)$	Direct Proof

Modular Arithmetic: Basic Property

Let $\boldsymbol{a, b, c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m > 0}$.
If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{b \equiv_m c}$, then $\boldsymbol{a \equiv_m c}$.

Suppose that $a \equiv_m b$ and $b \equiv_m c$.

Therefore, $a \equiv_m c$.

Assumption

Elim ∧

Def of ≡

Def of |

Elim ∃

Algebra

Intro ∃

Def of |

Def of ≡

Direct Proof

Modular Arithmetic: Basic Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m} > \boldsymbol{0}$.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

Suppose that $a \equiv_m b$ and $b \equiv_m c$.

By the definition of congruence, we know that $m \mid (a - b)$ and $m \mid (b - c)$. By the definition of divides, we know that $a - b = km$ and $b - c = jm$ for some integers k and j.

Therefore, $a \equiv_m c$.

Assumption

Elim ∧

Def of ≡

Def of |

Elim ∃

Algebra

Intro ∃

Def of |

Def of ≡

Direct Proof

Modular Arithmetic: Basic Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

Suppose that $a \equiv_m b$ and $b \equiv_m c$.

By the definition of congruence, we know that $m \mid (a - b)$ and $m \mid (b - c)$. By the definition of divides, we know that $a - b = km$ and $b - c = jm$ for some integers k and j.

Adding these, gives $a - c = km + jm = (k + j)m$.

Therefore, $a \equiv_m c$.

Assumption

Elim ∧
Def of ≡
Def of |
Elim ∃

Algebra

Intro ∃
Def of |
Def of ≡
Direct Proof

Modular Arithmetic: Basic Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}$ and $\boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

Suppose that $a \equiv_m b$ and $b \equiv_m c$.

By the definition of congruence, we know that $m \mid (a - b)$ and $m \mid (b - c)$. By the definition of divides, we know that $a - b = km$ and $b - c = jm$ for some integers k and j.

Adding these, gives $a - c = km + jm = (k + j)m$.

Therefore, by the definition of divides, we have shown that $m \mid (a - c)$, and then, $a \equiv_m c$ by the definition of congruence.

Assumption

Elim ∧
Def of ≡
Def of |
Elim ∃

Algebra

Intro ∃
Def of |
Def of ≡
Direct Proof

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

1. $\boldsymbol{(a \equiv_m b \land c \equiv_m d) \rightarrow (a + c \equiv_m b + d)}$??

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

2.1. $\boldsymbol{a \equiv_m b \land c \equiv_m d}$ **Assumption**

2.?. $\boldsymbol{a + c \equiv_m b + d}$ **??**

1. $\boldsymbol{(a \equiv_m b \land c \equiv_m d) \rightarrow (a + c \equiv_m b + d)}$ **Direct Proof**

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

2.1. $a \equiv_m b \land c \equiv_m d$	Assumption
2.2. $a \equiv_m b$	Elim $\land$: 2.1
2.3. $c \equiv_m d$	Elim $\land$: 2.1
2.?. $a + c \equiv_m b + d$	??
1. $(a \equiv_m b \land c \equiv_m d) \rightarrow (a + c \equiv_m b + d)$	Direct Proof

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

2.1. $\boldsymbol{a \equiv_m b \land c \equiv_m d}$	Assumption
2.2. $\boldsymbol{a \equiv_m b}$	Elim $\land$: 2.1
2.3. $\boldsymbol{c \equiv_m d}$	Elim $\land$: 2.1
2.4. $\boldsymbol{m \mid a - b}$	Def of ≡: 2.2
2.5. $\boldsymbol{m \mid c - d}$	Def of ≡: 2.3
2.?. $\boldsymbol{a + c \equiv_m b + d}$	??
1. $\boldsymbol{(a \equiv_m b \land c \equiv_m d) \rightarrow (a + c \equiv_m b + d)}$	Direct Proof

Modular Arithmetic: Addition Property

Let m be a positive integer. If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$.

2.1. $a \equiv_m b \wedge c \equiv_m d$	Assumption
2.2. $a \equiv_m b$	Elim ∧: 2.1
2.3. $c \equiv_m d$	Elim ∧: 2.1
2.4. $m \mid a - b$	Def of ≡: 2.2
2.5. $m \mid c - d$	Def of ≡: 2.3
2.6. $\exists q\ (a - b = qm)$	Def of |: 2.4
2.7. $\exists q\ (c - d = qm)$	Def of |: 2.5
2.?. $a + c \equiv_m b + d$	??
1. $(a \equiv_m b \wedge c \equiv_m d) \rightarrow (a + c \equiv_m b + d)$	Direct Proof

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

2.1. $\boldsymbol{a \equiv_m b \land c \equiv_m d}$	Assumption
2.2. $\boldsymbol{a \equiv_m b}$	Elim $\land$: 2.1
2.3. $\boldsymbol{c \equiv_m d}$	Elim $\land$: 2.1
2.4. $\boldsymbol{m \mid a - b}$	Def of ≡: 2.2
2.5. $\boldsymbol{m \mid c - d}$	Def of ≡: 2.3
2.6. $\boldsymbol{\exists q\ (a - b = qm)}$	Def of |: 2.4
2.7. $\boldsymbol{\exists q\ (c - d = qm)}$	Def of |: 2.5
2.8. $\boldsymbol{a - b = km}$	Elim $\exists$: 2.6
2.9. $\boldsymbol{c - d = jm}$	Elim $\exists$: 2.7
2.?. $\boldsymbol{a + c \equiv_m b + d}$	??
1. $\boldsymbol{(a \equiv_m b \land c \equiv_m d) \rightarrow (a + c \equiv_m b + d)}$	Direct Proof

Modular Arithmetic: Addition Property

Let m be a positive integer. If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$.

2.1. $a \equiv_m b \land c \equiv_m d$	Assumption
…	
2.8. $a - b = km$	Elim ∃: 2.6
2.9. $c - d = jm$	Elim ∃: 2.7
2.?. $m \mid (a + c) - (b + d)$	??
2.?. $a + c \equiv_m b + d$	Def of ≡
1. $(a \equiv_m b \land c \equiv_m d) \rightarrow (a + c \equiv_m b + d)$	Direct Proof

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

2.1. $a \equiv_m b \wedge c \equiv_m d$	Assumption
…	
2.8. $a - b = km$	Elim ∃: 2.6
2.9. $c - d = jm$	Elim ∃: 2.7
2.?. $\exists q\ ((a + c) - (b + d) = qm)$	??
2.?. $m \mid (a + c) - (b + d)$	Def of |
2.?. $a + c \equiv_m b + d$	Def of ≡
1. $(a \equiv_m b \wedge c \equiv_m d) \rightarrow (a + c \equiv_m b + d)$	Direct Proof

Modular Arithmetic: Addition Property

Let m be a positive integer. If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$.

2.1. $a \equiv_m b \land c \equiv_m d$	Assumption
…	
2.8. $a - b = km$	Elim ∃: 2.6
2.9. $c - d = jm$	Elim ∃: 2.7
2.10. $(a + c) - (b + d) = (k + j)m$	Algebra
2.11. $\exists q\ ((a + c) - (b + d) = qm)$	Intro ∃: 2.10
2.12. $m \mid (a + c) - (b + d)$	Def of |: 2.11
2.13. $a + c \equiv_m b + d$	Def of ≡: 2.12
1. $(a \equiv_m b \land c \equiv_m d) \rightarrow (a + c \equiv_m b + d)$	Direct Proof

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

Assumption

Elim ∧

Def of ≡

Def of |

Elim ∃

Algebra

Intro ∃

Def of |

Def of ≡

Direct Proof

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$.

Therefore, $a + c \equiv_m b + d$.

Assumption

Elim ∧

Def of ≡

Def of |

Elim ∃

Algebra

Intro ∃

Def of |

Def of ≡

Direct Proof

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$.

By the definition of congruence, we know that $m \mid (a - b)$ and $m \mid (c - d)$. By the definition of divides, we know that $a - b = km$ and $c - d = jm$ for some integers k and j.

Therefore, $a + c \equiv_m b + d$.

Assumption

Elim ∧

Def of ≡

Def of |

Elim ∃

Algebra

Intro ∃

Def of |

Def of ≡

Direct Proof

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$. Assumption

By the definition of congruence, we know that $m \mid (a - b)$ and $m \mid (c - d)$. By the definition of divides, we know that $a - b = km$ and $c - d = jm$ for some integers k and j.

Elim ∧
Def of ≡
Def of |
Elim ∃

Adding these, gives $(a + c) - (b + d) = (a - b) + (c - d) = km + jm = (k + j)m$. Algebra

Intro ∃
Def of |
Def of ≡

Therefore, $a + c \equiv_m b + d$.

Direct Proof

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b} + \boldsymbol{d}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$.

Assumption

By the definition of congruence, we know that $m \mid (a - b)$ and $m \mid (c - d)$. By the definition of divides, we know that $a - b = km$ and $c - d = jm$ for some integers k and j.

Elim ∧

Def of ≡

Def of |

Elim ∃

Adding these, gives $(a + c) - (b + d) = (a - b) + (c - d) = km + jm = (k + j)m$.

Algebra

Therefore, by the definition of divides, we have shown $m \mid (a + c) - (b + d)$, and then, we have $a + c \equiv_m b + d$ by the definition of congruence.

Intro ∃

Def of |

Def of ≡

Direct Proof

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

1. $(\boldsymbol{a \equiv_m b \land c \equiv_m d}) \rightarrow (\boldsymbol{ac \equiv_m bd})$??

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

2.1. $\boldsymbol{a \equiv_m b \land c \equiv_m d}$ **Assumption**

2.?. $\boldsymbol{ac \equiv_m bd}$ **??**

1. $\boldsymbol{(a \equiv_m b \land c \equiv_m d) \rightarrow (ac \equiv_m bd)}$ **Direct Proof**

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

2.1. $\boldsymbol{a \equiv_m b \wedge c \equiv_m d}$	Assumption
2.2. $\boldsymbol{a \equiv_m b}$	Elim $\wedge$: 2.1
2.3. $\boldsymbol{c \equiv_m d}$	Elim $\wedge$: 2.1
2.?. $\boldsymbol{ac \equiv_m bd}$	??
1. $\boldsymbol{(a \equiv_m b \wedge c \equiv_m d) \rightarrow (ac \equiv_m bd)}$	Direct Proof

Modular Arithmetic: Multiplication Property

Let m be a positive integer. If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.

2.1. $a \equiv_m b \wedge c \equiv_m d$	Assumption
2.2. $a \equiv_m b$	Elim $\wedge$: 2.1
2.3. $c \equiv_m d$	Elim $\wedge$: 2.1
2.4. $m \mid a - b$	Def of ≡: 2.2
2.5. $m \mid c - d$	Def of ≡: 2.3
2.?. $ac \equiv_m bd$	??
1. $(a \equiv_m b \wedge c \equiv_m d) \rightarrow (ac \equiv_m bd)$	Direct Proof

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

2.1. $a \equiv_m b \wedge c \equiv_m d$	Assumption
2.2. $a \equiv_m b$	Elim $\wedge$: 2.1
2.3. $c \equiv_m d$	Elim $\wedge$: 2.1
2.4. $m \mid a - b$	Def of ≡: 2.2
2.5. $m \mid c - d$	Def of ≡: 2.3
2.6. $\exists q\ (a - b = qm)$	Def of |: 2.4
2.7. $\exists q\ (c - d = qm)$	Def of |: 2.5
2.?. $ac \equiv_m bd$	??
1. $(a \equiv_m b \wedge c \equiv_m d) \rightarrow (ac \equiv_m bd)$	Direct Proof

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

2.1. $a \equiv_m b \wedge c \equiv_m d$	Assumption
2.2. $a \equiv_m b$	Elim $\wedge$: 2.1
2.3. $c \equiv_m d$	Elim $\wedge$: 2.1
2.4. $m \mid a - b$	Def of ≡: 2.2
2.5. $m \mid c - d$	Def of ≡: 2.3
2.6. $\exists q\ (a - b = qm)$	Def of |: 2.4
2.7. $\exists q\ (c - d = qm)$	Def of |: 2.5
2.8. $a - b = jm$	Elim $\exists$: 2.6
2.9. $c - d = km$	Elim $\exists$: 2.7
2.?. $ac \equiv_m bd$	??
1. $(a \equiv_m b \wedge c \equiv_m d) \rightarrow (ac \equiv_m bd)$	Direct Proof

Modular Arithmetic: Addition Property

Let m be a positive integer. If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.

2.1. $a \equiv_m b \wedge c \equiv_m d$	Assumption
…	
2.8. $a - b = jm$	Elim ∃: 2.6
2.9. $c - d = km$	Elim ∃: 2.7
2.?. $ac \equiv_m bd$	??
1. $(a \equiv_m b \wedge c \equiv_m d) \rightarrow (ac \equiv_m bd)$	Direct Proof

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

2.1. $\boldsymbol{a \equiv_m b \wedge c \equiv_m d}$	Assumption
…	
2.8. $\boldsymbol{a - b = jm}$	Elim ∃: 2.6
2.9. $\boldsymbol{c - d = km}$	Elim ∃: 2.7
2.?. $\boldsymbol{m \mid ac - bd}$	??
2.?. $\boldsymbol{ac \equiv_m bd}$	Def of ≡
1. $\boldsymbol{(a \equiv_m b \wedge c \equiv_m d) \rightarrow (ac \equiv_m bd)}$	Direct Proof

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

2.1. $a \equiv_m b \wedge c \equiv_m d$	Assumption
…	
2.8. $a - b = jm$	Elim ∃: 2.6
2.9. $c - d = km$	Elim ∃: 2.7
2.?. $\exists q\ (ac - bd = qm)$	??
2.?. $m \mid ac - bd$	Def of |
2.?. $ac \equiv_m bd$	Def of ≡
1. $(a \equiv_m b \wedge c \equiv_m d) \rightarrow (ac \equiv_m bd)$	Direct Proof

Modular Arithmetic: Addition Property

Let m be a positive integer. If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.

2.1. $a \equiv_m b \wedge c \equiv_m d$ Assumption

…

2.8. $a - b = jm$ Elim ∃: 2.6

2.9. $c - d = km$ Elim ∃: 2.7

2.10. $ac - bd = (bk + dj + jkm)m$ Algebra

2.11. $\exists q\ (ac - bd = qm)$ Intro ∃: 2.10

2.12. $m \mid ac - bd$ Def of |: 2.11

2.13. $ac \equiv_m bd$ Def of ≡: 2.12

1. $(a \equiv_m b \wedge c \equiv_m d) \rightarrow (ac \equiv_m bd)$ Direct Proof

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$.

Assumption

Therefore, $ac \equiv_m bd$.

??

Direct Proof

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$.

Assumption

By the definition of congruence, we know that $m \mid (a - b)$ and $m \mid (c - d)$.

Def of ≡

Therefore, $ac \equiv_m bd$.

??

Direct Proof

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$.

Assumption

By the definition of congruence, we know that $m \mid (a - b)$ and $m \mid (c - d)$. By the definition of divides, we know that $a - b = jm$ and $c - d = km$ for some integers j and k.

Def of ≡
Def of |
Elim ∃

Therefore, $ac \equiv_m bd$.

??

Direct Proof

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$.

Assumption

By the definition of congruence, we know that $m \mid (a - b)$ and $m \mid (c - d)$. By the definition of divides, we know that $a - b = jm$ and $c - d = km$ for some integers j and k.

Def of ≡

Def of |

Elim ∃

Equivalently, $a = b + jm$ and $c = d + km$. Multiplying these gives $ac = (b + jm)(d + km) = bd + bkm + djm + jkm = bd + (bk + dj + jk)m$, so $ac - bd = (bk + dj + jk)m$.

Algebra

Intro ∃

Def of |

Def of ≡

… Therefore, $ac \equiv_m bd$.

Direct Proof

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$.

Assumption

By the definition of congruence, we know that $m \mid (a - b)$ and $m \mid (c - d)$. By the definition of divides, we know that $a - b = jm$ and $c - d = km$ for some integers j and k.

Def of ≡

Def of |

Elim ∃

Equivalently, $a = b + jm$ and $c = d + km$. Multiplying these gives $ac = (b + jm)(d + km) = bd + bkm + djm + jkm = bd + (bk + dj + jk)m$, so $ac - bd = (bk + dj + jk)m$.

Algebra

Therefore, $m \mid ac - bd$ by the definition of divides, so $ac \equiv_m bd$ by the definition of congruence.

Intro ∃

Def of |

Def of ≡

Direct Proof

Modular Arithmetic: Properties

If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{b \equiv_m c}$, then $\boldsymbol{a \equiv_m c}$.

If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

Corollary: If $\boldsymbol{a \equiv_m b}$, then $\boldsymbol{a + c \equiv_m b + c}$.

If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

Corollary: If $\boldsymbol{a \equiv_m b}$, then $\boldsymbol{ac \equiv_m bc}$.

Recall: Familiar Properties of “=”

- If $a = b$ and $b = c$, then $a = c$.
  - i.e., if $a = b = c$, then $a = c$

- If $a = b$ and $c = d$, then $a + c = b + d$.
  - since $c = c$ is true, we can “$+ c$” to both sides

- If $a = b$ and $c = d$, then $ac = bd$.
  - since $c = c$ is true, we can “$\times c$” to both sides

These facts allow us to use algebra to solve problems

The Arithmetic Rule

$$\frac{\boxed{\text{Arithmetic}}}{\therefore x = y}$$

we won't use this…

if this follows by standard properties

- **Equation must be true with no outside information**
- **Use only these properties of arithmetic operators:**
  - **commutativity** ($x+y = y+x$ **and** $yx = xy$)
  - **associativity** ($x+(y+z) = (x+y)+z$ **and** $x(yz) = (xy)z$)
  - **distributivity** ($a(b+c) = ab + bc$)
  - **identity** ($x+0 = x$ **and** $1 \cdot x = x$)
  - **arithmetic with constants** ($7 - 5 = 2$)
  - **…**

The Arithmetic Rule

Arithmetic ——————————— we won't use this…

∴ x = y

if this follows by standard properties

- **Examples:**

1. $7 = 7$ **Arithmetic**
2. $7 - 4 = 3$ **Arithmetic**
3. $5x - 3x = 2x$ **Arithmetic**

…

Recall: Properties of "=" Used in Algebra

If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{b} = \boldsymbol{c}$, then $\boldsymbol{a} = \boldsymbol{c}$	"Transitivity"
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} = \boldsymbol{b} + \boldsymbol{d}$	"Add Equations"
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{ac} = \boldsymbol{bd}$	"Multiply Equations"

We need these facts to do algebra…

Example: **given** $5x + 4 = 2x + 25$**,**
prove that $3x = 21$**.**

Recall: Properties of “=” Used in Algebra

If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{b} = \boldsymbol{c}$, then $\boldsymbol{a} = \boldsymbol{c}$	“Transitivity”
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} = \boldsymbol{b} + \boldsymbol{d}$	“Add Equations”
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{ac} = \boldsymbol{bd}$	“Multiply Equations”

1. $5x + 4 = 2x + 25$	**Given**
2. $-4 = -4$	**Arithmetic**
3. $5x + 4 - 4 = 2x + 25 - 4$	**Add Equations: 1, 2**
4. $5\mathrm{x} = 5x + 4 - 4$	**Arithmetic**
5. $5x = 2x + 25 - 4$	**Transitivity: 4, 3**
6. $2x + 25 - 4 = 2x + 21$	**Arithmetic**
7. $5x = 2x + 21$	**Transitivity: 5, 6**

Recall: Properties of “=” Used in Algebra

If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{b} = \boldsymbol{c}$, then $\boldsymbol{a} = \boldsymbol{c}$	“Transitivity”
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} = \boldsymbol{b} + \boldsymbol{d}$	“Add Equations”
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{ac} = \boldsymbol{bd}$	“Multiply Equations”

…

7. $5x = 2x + 21$	**Transitivity: 5, 6**
8. $-2x = -2x$	**Arithmetic**
9. $5x - 2x = 2x + 21 - 2x$	**Add Equations: 7, 8**
10. $3\mathrm{x} = 5x - 2x$	**Arithmetic**
11. $3\mathrm{x} = 2x + 21 - 2x$	**Transitivity: 10, 9**
12. $2x + 21 - 2x = 21$	**Arithmetic**
13. $3\mathrm{x} = 21$	**Transitivity: 11, 12**

Recall: The Algebra Rule

$$\boxed{\text{Algebra}}\ \frac{x_1 = y_1 \quad \dots \quad x_n = y_n}{\therefore x = y}$$

- Algebra rule accepts equation if it follows by
  - multiplying equations by a *constant*
  - adding them
  - and *then* doing some arithmetic

- Example:

1. $5x = 15$
2. $2x = 6$
3. $3x = 9$

(Line 1) + –1 (Line 2) gives

$$5x - 2x = 15 - 6$$

Algebra: 1, 2

Recall: The Algebra Rule

$$\boxed{\text{Algebra}}\ \frac{x_1 = y_1 \quad \dots \quad x_n = y_n}{\therefore\ x = y}$$

- **Algebra rule accepts equation if it follows by**
  - **multiplying equations by a *constant***
  - **adding them**
  - **and *then* doing some arithmetic**

- **Note: the Algebra rule works on equations**
  - **what about congruences? (“$\equiv_m$” instead of "$=$")**

Modular Arithmetic: Properties

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b} + \boldsymbol{c}$.

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$, then $\boldsymbol{ac} \equiv_{\boldsymbol{m}} \boldsymbol{bc}$.

These properties are sufficient to allow us to do algebra with congruences

Properties of “$\equiv_m$” Used in Algebra

If $\boldsymbol{a} \equiv_m \boldsymbol{b}$ and $\boldsymbol{b} \equiv_m \boldsymbol{c}$, then $\boldsymbol{a} \equiv_m \boldsymbol{c}$ “Transitivity”

If $\boldsymbol{a} \equiv_m \boldsymbol{b}$ and $\boldsymbol{c} \equiv_m \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_m \boldsymbol{b} + \boldsymbol{d}$ “Add Congruences”

If $\boldsymbol{a} \equiv_m \boldsymbol{b}$ and $\boldsymbol{c} \equiv_m \boldsymbol{d}$, then $\boldsymbol{ac} \equiv_m \boldsymbol{bd}$ “Multiply Congruences”

Example: **given that** $5x + 4 \ \equiv_{\mathrm{m}} 2x + 25$**,**
prove that $3x \equiv_{\mathrm{m}} 21$

Properties of "$\equiv_m$" Used in Algebra

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$ "Transitivity"

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b} + \boldsymbol{d}$ "Add Congruences"

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{ac} \equiv_{\boldsymbol{m}} \boldsymbol{bd}$ "Multiply Congruences"

1. $5x + 4 \equiv_{\mathrm{m}} 2x + 25$	**Given**
2. $-4 = -4$	**Algebra**
3. $5x \equiv_{\mathrm{m}} 2x + 21$	**Add Congruences: 2, 1 ??**

Line 2 says "=" not "$\equiv_{\mathrm{m}}$"

But "=" implies "$\equiv_{\mathrm{m}}$" !
(equality is a special case)

Properties of “$\equiv_m$” Used in Algebra

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$ “Transitivity”

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b} + \boldsymbol{d}$ “Add Congruences”

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{ac} \equiv_{\boldsymbol{m}} \boldsymbol{bd}$ “Multiply Congruences”

If $\boldsymbol{a} = \boldsymbol{b}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$. “To Modular”

1. $5x + 4 \equiv_{\mathrm{m}} 2x + 25$ **Given**

2. $-4 = -4$ **Algebra**

3. $-4 \equiv_{\mathrm{m}} -4$ **To Modular: 2**

4. $5x + 4 - 4 \equiv_{\mathrm{m}} 2x + 25 - 4$ **Add Congruences: 3, 1**

Properties of "$\equiv_m$" Used in Algebra

If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{b \equiv_m c}$, then $\boldsymbol{a \equiv_m c}$ "Transitivity"

If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$ "Add Congruences"

If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$ "Multiply Congruences"

If $\boldsymbol{a = b}$, then $\boldsymbol{a \equiv_m b}$. "To Modular"

…

4. $5x + 4 - 4 \equiv_{\mathrm{m}} 2x + 25 - 4$ **Add Congruences: 3, 1**

5. $5x = 5x + 4 - 4$ **Arithmetic / Algebra**

6. $5x \equiv_{\mathrm{m}} 5x + 4 - 4$ **To Modular: 5**

7. $5x \equiv_{\mathrm{m}} 2x + 25 - 4$ **Transitivity: 6, 4**

Properties of "$\equiv_m$" Used in Algebra

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$	"Transitivity"
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b} + \boldsymbol{d}$	"Add Congruences"
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{ac} \equiv_{\boldsymbol{m}} \boldsymbol{bd}$	"Multiply Congruences"
If $\boldsymbol{a} = \boldsymbol{b}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$.	"To Modular"

…

7. $5x \equiv_{\mathrm{m}} 2x + 25 - 4$	**Transitivity: 6, 4**
8. $2x + 25 - 4 = 2x + 21$	**Arithmetic / Algebra**
9. $2x + 25 - 4 \equiv_{\mathrm{m}} 2x + 21$	**To Modular: 8**
10. $5x \equiv_{\mathrm{m}} 2x + 21$	**Transitivity: 7, 9**

… continue by adding $-2x$ to both sides …

Properties of "$\equiv_m$" Used in Algebra

If $\boldsymbol{a} \equiv_m \boldsymbol{b}$ and $\boldsymbol{b} \equiv_m \boldsymbol{c}$, then $\boldsymbol{a} \equiv_m \boldsymbol{c}$ "Transitivity"

If $\boldsymbol{a} \equiv_m \boldsymbol{b}$ and $\boldsymbol{c} \equiv_m \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_m \boldsymbol{b} + \boldsymbol{d}$ "Add Congruences"

If $\boldsymbol{a} \equiv_m \boldsymbol{b}$ and $\boldsymbol{c} \equiv_m \boldsymbol{d}$, then $\boldsymbol{ac} \equiv_m \boldsymbol{bd}$ "Multiply Congruences"

We don't want to do all that!

Example: **given that** $5x + 4 \equiv_{\mathrm{m}} 2x + 25$,
prove that $3x \equiv_{\mathrm{m}} 21$

These properties are sufficient to allow us to do algebra with congruences:

- move terms from one side to the other
- simplify either side

Properties of "$\equiv_m$" Used in Algebra

If $\boldsymbol{a} \equiv_m \boldsymbol{b}$ and $\boldsymbol{b} \equiv_m \boldsymbol{c}$, then $\boldsymbol{a} \equiv_m \boldsymbol{c}$ "Transitivity"

If $\boldsymbol{a} \equiv_m \boldsymbol{b}$ and $\boldsymbol{c} \equiv_m \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_m \boldsymbol{b} + \boldsymbol{d}$ "Add Congruences"

If $\boldsymbol{a} \equiv_m \boldsymbol{b}$ and $\boldsymbol{c} \equiv_m \boldsymbol{d}$, then $\boldsymbol{ac} \equiv_m \boldsymbol{bd}$ "Multiply Congruences"

We don't want to do all that!

Example: **given that** $5x + 4 \equiv_\mathrm{m} 2x + 25$,
prove that $3x \equiv_\mathrm{m} 21$

Careful: **proved** $5x + 4 = 2x + 25 \Rightarrow 3x = 21$

not $3x = 21 \Rightarrow 5x + 4 = 2x + 25$

the second is a "*backward proof*"

Another Property of “=” Used in Algebra

Can “plug in” (a.k.a. substitute)
the known value of a variable

Example: **given** $2y + 3x = 25$ **and** $x = 7y$,
follows that $2y + 21y = 25$**.**

The Substitute Rule

$$\boxed{\text{Substitute}}\quad \frac{\mathrm{P(x)} \qquad \mathrm{x = y}}{\therefore\ \mathrm{P(y)}}$$

- **If** x = y**, then anything true of** x **is true of** y
- **Note that** y **can be any expression**
  - **e.g., if** x = 7y + 3**, then we get** P(7y + 3)
- **Note that equations are also predicates**
  - **can think of** $2y + 3x = 25$ **as** $\mathrm{Equal}(2y + 3x, 25)$

    better to use the nicer notation though…

Another Property of "=" Used in Algebra

Can "plug in" (a.k.a. substitute)
the known value of a variable

Example: given $2y + 3x = 25$ and $x = 7y$,
follows that $2y + 21y = 25$.

This is also true of *congruences*!

(But we don't have the tools to prove it yet....)

Example: given $2y + 3x \equiv_{\mathrm{m}} 25$ and $x \equiv_{\mathrm{m}} 7y$,
follows that $2y + 21y \equiv_{\mathrm{m}} 25$.

Substitution vs Other Properties

If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{b} = \boldsymbol{c}$, then $\boldsymbol{a} = \boldsymbol{c}$	“Transitivity”
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} = \boldsymbol{b} + \boldsymbol{d}$	“Add Equations”
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{ac} = \boldsymbol{bd}$	“Multiply Equations”

Can prove "Add Equations" by Substitution...

$$\begin{aligned} a + c &= a + c && \textbf{Arithmetic} \\ &= b + c && \textbf{Substitute } a = b \\ &= b + d && \textbf{Substitute } c = d \end{aligned}$$

"Add Equations" follows by Transitivity.

Substitution vs Other Properties

If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{b} = \boldsymbol{c}$, then $\boldsymbol{a} = \boldsymbol{c}$	“Transitivity”
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} = \boldsymbol{b} + \boldsymbol{d}$	“Add Equations”
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{ac} = \boldsymbol{bd}$	“Multiply Equations”

Can prove "Multiply Equations" by Substitution...

$$\begin{aligned} ac &= ac && \textbf{Arithmetic} \\ &= bc && \textbf{Substitute } a = b \\ &= bd && \textbf{Substitute } c = d \end{aligned}$$

"Multiply Equations" follows by Transitivity.

Substitution vs Other Properties

If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{b} = \boldsymbol{c}$, then $\boldsymbol{a} = \boldsymbol{c}$	“Transitivity”
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} = \boldsymbol{b} + \boldsymbol{d}$	“Add Equations”
If $\boldsymbol{a} = \boldsymbol{b}$ and $\boldsymbol{c} = \boldsymbol{d}$, then $\boldsymbol{ac} = \boldsymbol{bd}$	“Multiply Equations”

- **Substitution is an alternative for solving problems**
  - **we will try this out on HW4**
  - **will be heavily used in *future* homework**

Recall: Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \textbf{ mod } \boldsymbol{m} = \boldsymbol{b} \textbf{ mod } \boldsymbol{m}$.

What numbers a and b did we **prove** this for?

We don't know anything about these numbers.

I.e., they were **arbitrary**.

That means our proof could be changed…

Recall: Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m \ = \ b \bmod m}$.

1.1. $a \bmod m = b \bmod m$ Assumption

...

1.7. $a \equiv_m b$ Def of ≡

1. $(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b)$ Direct Proof

2.1. $a \equiv_m b$ Assumption

...

2.8. $a \bmod m = b \bmod m$ Elim ∧

2. $(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$ Direct Proof

3. $(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b) \land$
$(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$ Intro ∧

4. $(a \equiv_m b) \leftrightarrow (a \bmod m = b \bmod m)$ Equivalent

Recall: Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m \ = \ b \bmod m}$.

Let $\boldsymbol{a}$ and $\boldsymbol{b}$ be arbitrary integers.

1.1.1. $\boldsymbol{a \bmod m = b \bmod m}$ Assumption

...

1.1.7. $\boldsymbol{a \equiv_m b}$ Def of ≡

1.1. $\boldsymbol{(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b)}$ Direct Proof

1.2.1. $\boldsymbol{a \equiv_m b}$ Assumption

...

1.2.8. $\boldsymbol{a \bmod m = b \bmod m}$ Elim ∧

1.2. $\boldsymbol{(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)}$ Direct Proof

1.3. $\boldsymbol{(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b) \land}$
$\boldsymbol{(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)}$ Intro ∧

1.4. $\boldsymbol{(a \equiv_m b) \leftrightarrow (a \bmod m = b \bmod m)}$ Equivalent

1. $\boldsymbol{\forall a \, \forall b \, ((a \equiv_m b) \leftrightarrow (a \bmod m = b \bmod m))}$ Intro ∀

Recall: Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m \;=\; b \bmod m}$.

This is stated as

$$(\mathrm{a} \equiv_{\mathrm{m}} \mathrm{b}) \leftrightarrow (\mathrm{a} \bmod \mathrm{m} \;=\; \mathrm{b} \bmod \mathrm{m})$$

but it is **really**

$$\forall \mathrm{a}\, \forall \mathrm{b}\;\; ((\mathrm{a} \equiv_{\mathrm{m}} \mathrm{b}) \leftrightarrow (\mathrm{a} \bmod \mathrm{m} \;=\; \mathrm{b} \bmod \mathrm{m}))$$

This is a fact we can apply to **any**
integers $\boldsymbol{a}$ and $\boldsymbol{b}$ (and $\boldsymbol{m > 0}$).

Rule: unquantified variables are *implicitly* ∀-quantified

(will see one exception later…)

Recall: Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

But the proof **stays** as is!

Rule: structure of the proof follows the structure of the claim

Recall: Properties of "$\equiv_m$" Used in Algebra

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$ "Transitivity"

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b} + \boldsymbol{d}$ "Add Congruences"

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{ac} \equiv_{\boldsymbol{m}} \boldsymbol{bd}$ "Multiply Congruences"

If $\boldsymbol{a} = \boldsymbol{b}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$. "To Modular"

1. $5x + 4 \equiv_{\mathrm{m}} 2x + 25$	**Given**
2. $-4 = -4$	**Algebra**
3. $-4 \equiv_{\mathrm{m}} -4$	**To Modular: 2**
4. $5x + 4 - 4 \equiv_{\mathrm{m}} 2x + 25 - 4$	**Add Congruences: 3, 1**

Lines 3 & 4 are *applying* the **theorems** above!

Using Theorems

If $\boldsymbol{a} = \boldsymbol{b}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$. “To Modular”

$\forall a\ \forall b\ ((a = b) \rightarrow (a \equiv_m b))$

- First way to use theorems in a proof:

Cite T

$\therefore \forall x\ P(x)$

where T is a well-known theorem that says $\forall x\ P(x)$

Using Theorems

If $\boldsymbol{a} = \boldsymbol{b}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$. “To Modular”

$$\forall \mathrm{a}\ \forall \mathrm{b}\ ((\mathrm{a} = \mathrm{b}) \rightarrow (\mathrm{a} \equiv_{\mathrm{m}} \mathrm{b}))$$

1. $5x + 4 \equiv_{\mathrm{m}} 2x + 25$	**Given**
2. $-4 = -4$	**Algebra**
3. $\forall a\ \forall b\ ((a = b) \rightarrow (a \equiv_m b)$	**Cite "To Modular"**
4. $\forall b\ ((-4 = b) \rightarrow (-4 \equiv_m b)$	**Elim ∀: 3**
5. $(-4 = -4) \rightarrow (-4 \equiv_m -4)$	**Elim ∀: 4**
6. $-4 \equiv_{\mathrm{m}} -4$	**MP: 2, 5**

Using Theorems

If $\boldsymbol{a = b}$, then $\boldsymbol{a \equiv_m b}$. “To Modular”

$$\underbrace{\forall a\ \forall b\ ((a = b) \rightarrow (a \equiv_m b))}$$

most theorems look like this...
(some ∀s and then →)

- Second way to use theorems in a proof...

Apply T

$$\frac{P(c)}{\therefore Q(c)}$$

where T is a well-known theorem
that says $\forall x\ (P(x) \rightarrow Q(x))$

Using Theorems

If $\boldsymbol{a} = \boldsymbol{b}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$. “To Modular”

$$\forall \mathrm{a}\ \forall \mathrm{b}\ ((\mathrm{a} = \mathrm{b}) \rightarrow (\mathrm{a} \equiv_{\mathrm{m}} \mathrm{b}))$$

1. $5x + 4 \equiv_{\mathrm{m}} 2x + 25$	Given
2. $-4 = -4$	Algebra
3. $\forall a\ \forall b\ ((a = b) \rightarrow (a \equiv_m b)$	Cite "To Modular"
4. $\forall b\ ((-4 = b) \rightarrow (-4 \equiv_m b)$	Elim ∀: 3
5. $(-4 = -4) \rightarrow (-4 \equiv_m -4)$	Elim ∀: 4
6. $-4 \equiv_{\mathrm{m}} -4$	MP: 2, 5
3. $-4 \equiv_{\mathrm{m}} -4$	Apply "To Modular": 2

applying the theorem with
$\mathrm{a} = -4$ and $\mathrm{b} = -4$