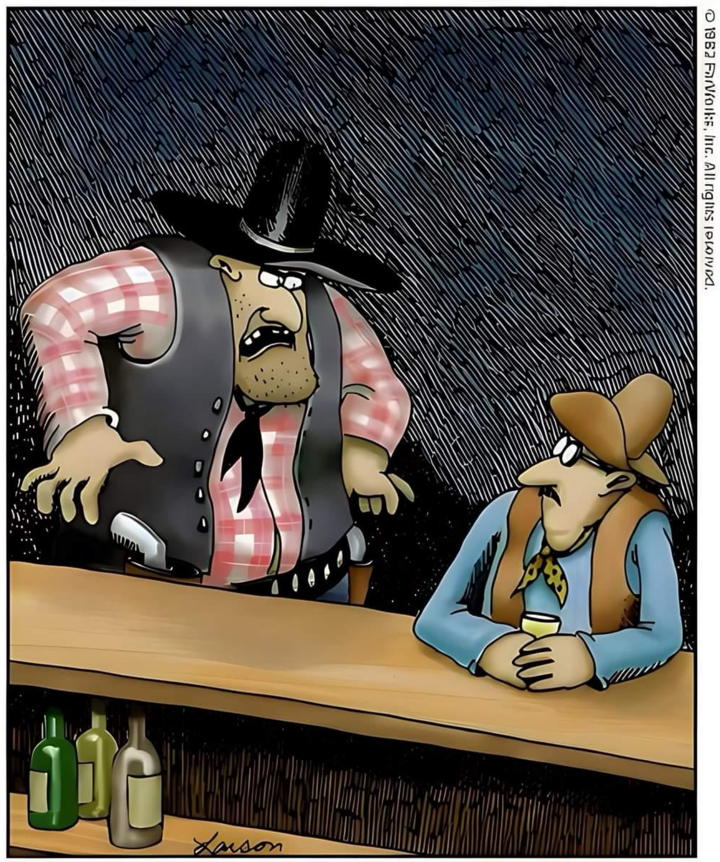
CSE 311: Foundations of Computing

Topic 4: Number Theory



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

Mechanical vs Creative Predicate Logic

- We've done examples with "meaningless" predicates such as $\forall x\, P(x) \rightarrow \exists x\, P(x)$
  - Saw how to (often) *mechanically* solve by looking at "shape" of the goal.
  - We'll need these skills in all domains!

- When we enter "interesting" domains of discourse, we will use domain knowledge.
  - We will see how to *creatively* solve goals, especially with rules like Intro $\vee$, Intro $\exists$, Elim $\wedge$, Elim $\forall$.

Applications of Predicate Logic

- Remainder of the course will use predicate logic to prove <u>important</u> properties of <u>interesting</u> objects
  - start with math objects that are widely used in CS
  - eventually more CS-specific objects

- Encode domain knowledge in predicate definitions
- Then apply predicate logic to infer useful results

Domain of Discourse
Integers

Predicate Definitions
$\text{Even}(x) \equiv \exists y\ (x = 2 \cdot y)$
$\text{Odd}(x) \equiv \exists y\ (x = 2 \cdot y + 1)$

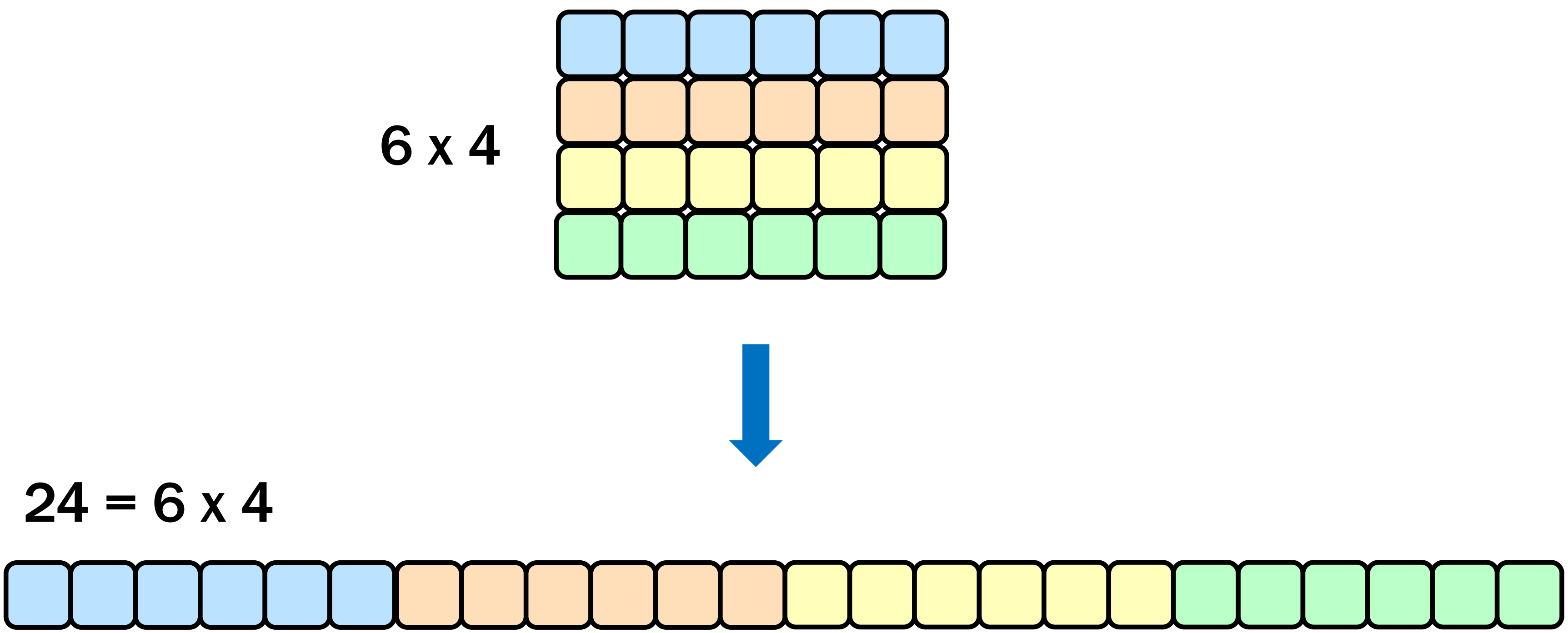
Number Theory

- **Direct relevance to computing**
  - **everything in a computer is a number**
    - colors on the screen are encoded as numbers

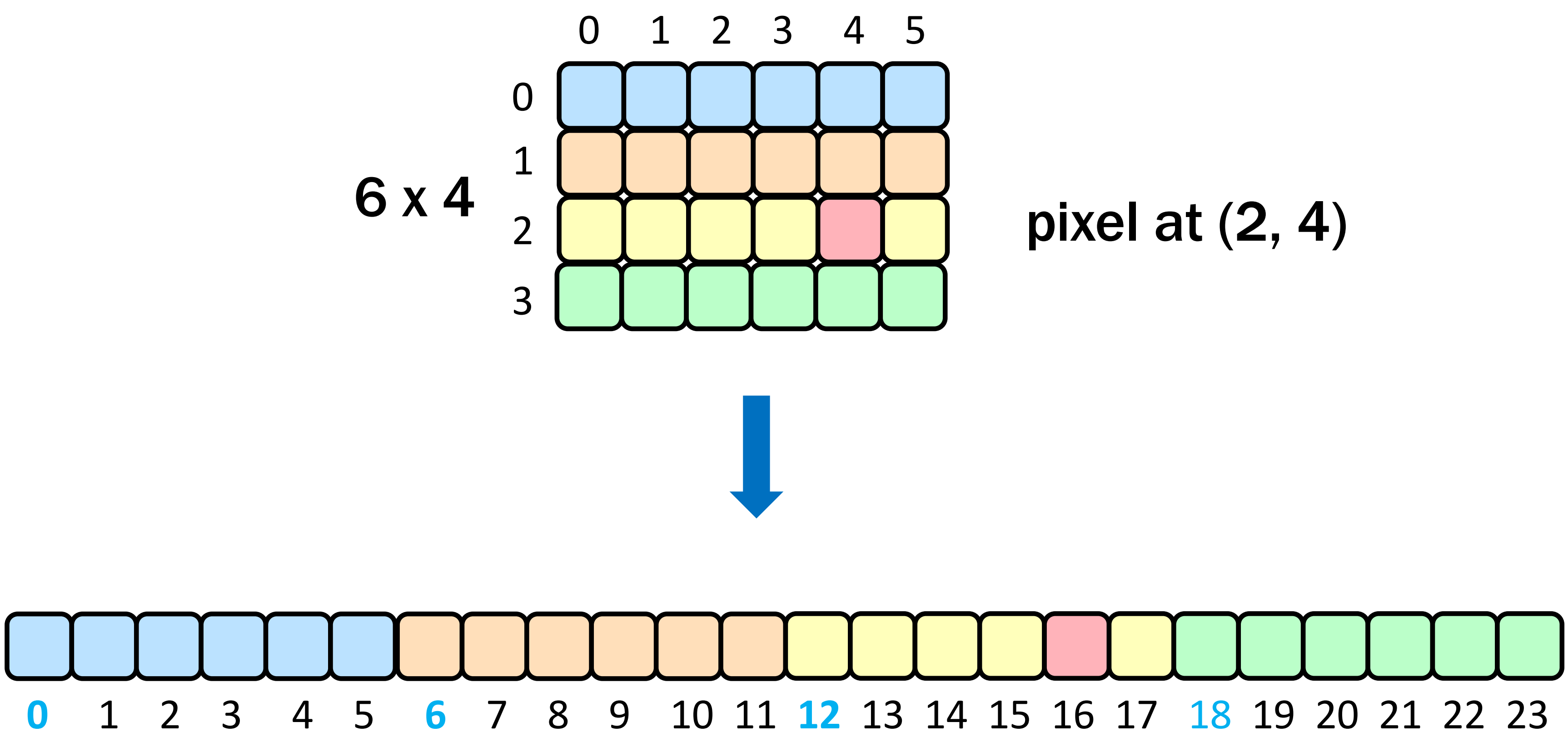
- **Many significant applications in CS…**

Pixels in Memory

- Memory is an array, so
  pixel positions must be mapped to array indexes



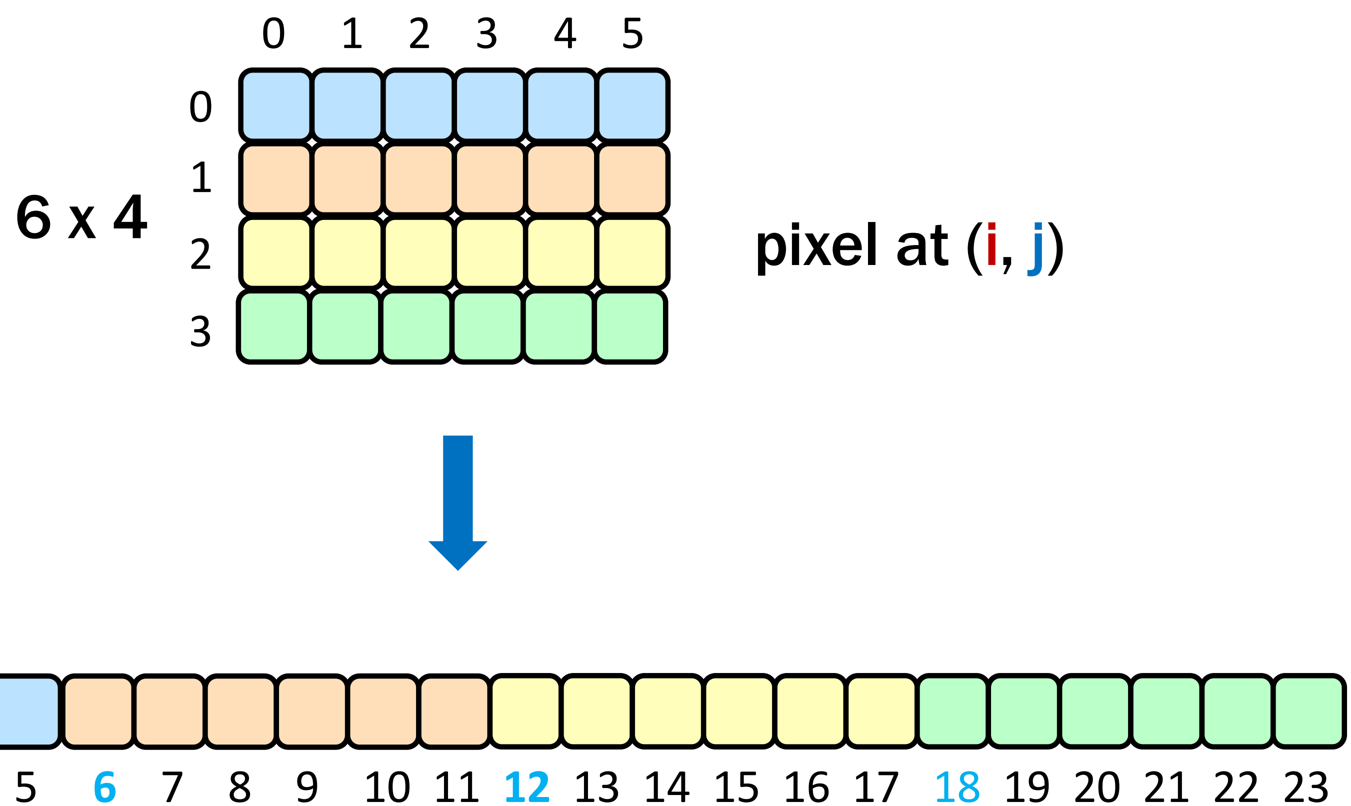
Pixels in Memory



stored at index 16 $= 12 + 4$

$= 2 \cdot 6 + 4$

Pixels in Memory



Stored at index n.
How do we calculate n from i and j?

$$n = i \cdot 6 + j$$

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 with $b \neq 0$:

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

Check Your Understanding. Which of the following are true?

$5 \mid 1$ $\quad$ $25 \mid 5$ $\quad$ $5 \mid 0$ $\quad$ $3 \mid 2$

$1 \mid 5$ $\quad$ $5 \mid 25$ $\quad$ $0 \mid 5$ $\quad$ $2 \mid 3$

Divisibility

Domain of Discourse
Integers

Definition: "b divides a"

For a, b with $b \neq 0$:

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

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
5 | 1 iff 1 = 5k	25 | 5 iff 5 = 25k	5 | 0 iff 0 = 5k	3 | 2 iff 2 = 3k
1 | 5	5 | 25	0 | 5	2 | 3
1 | 5 iff 5 = 1k	5 | 25 iff 25 = 5k	0 | 5 iff 5 = 0k	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 $\frac{a}{b} = q$ we have $\frac{a}{b} = q + \frac{r}{b}$

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

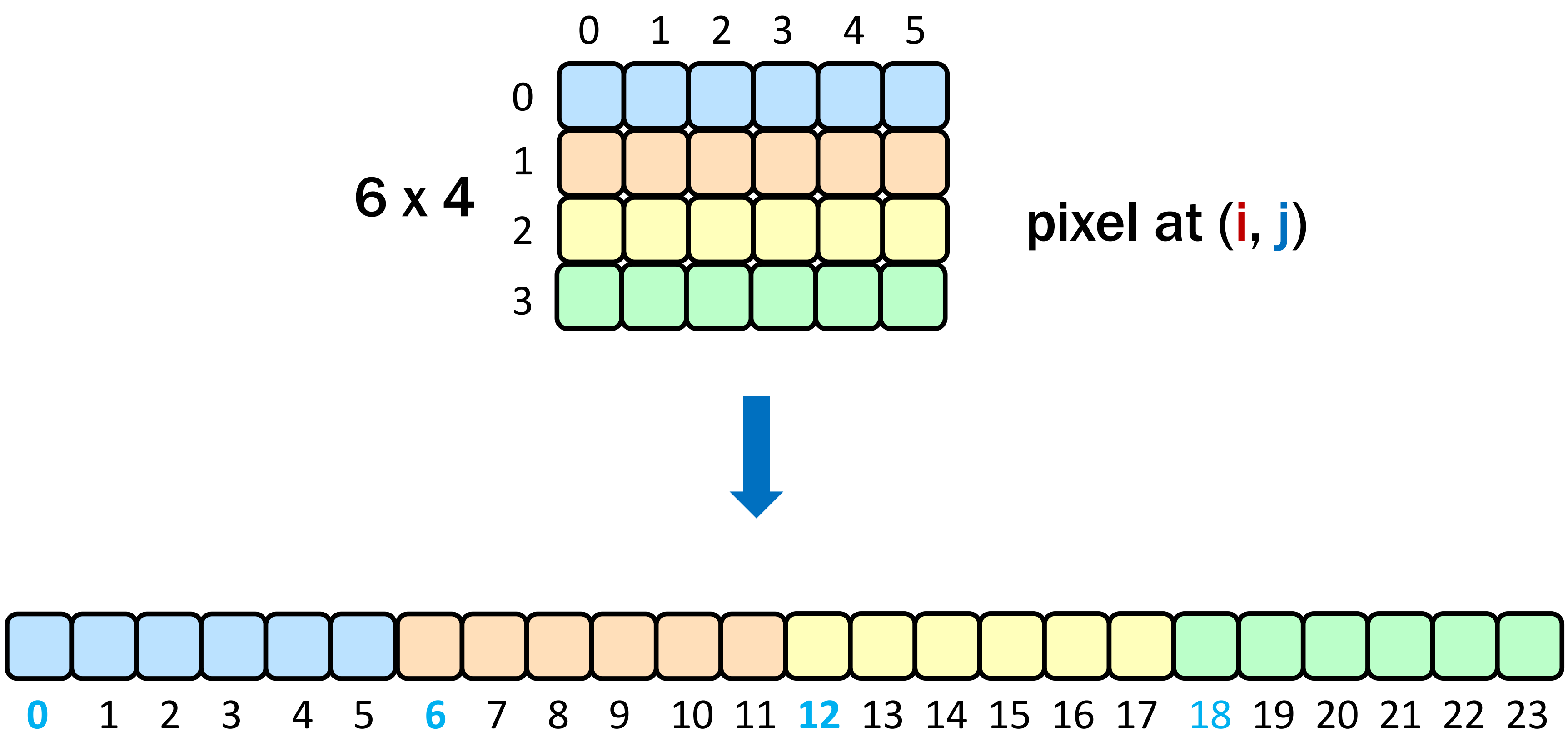
For a, b with $b > 0$
there exist *unique* integers q, r with $0 \leq r < b$
such that $a = qb + r$.

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* **div** *b*) *b* + (*a* **mod** *b*)

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

Pixels in Memory

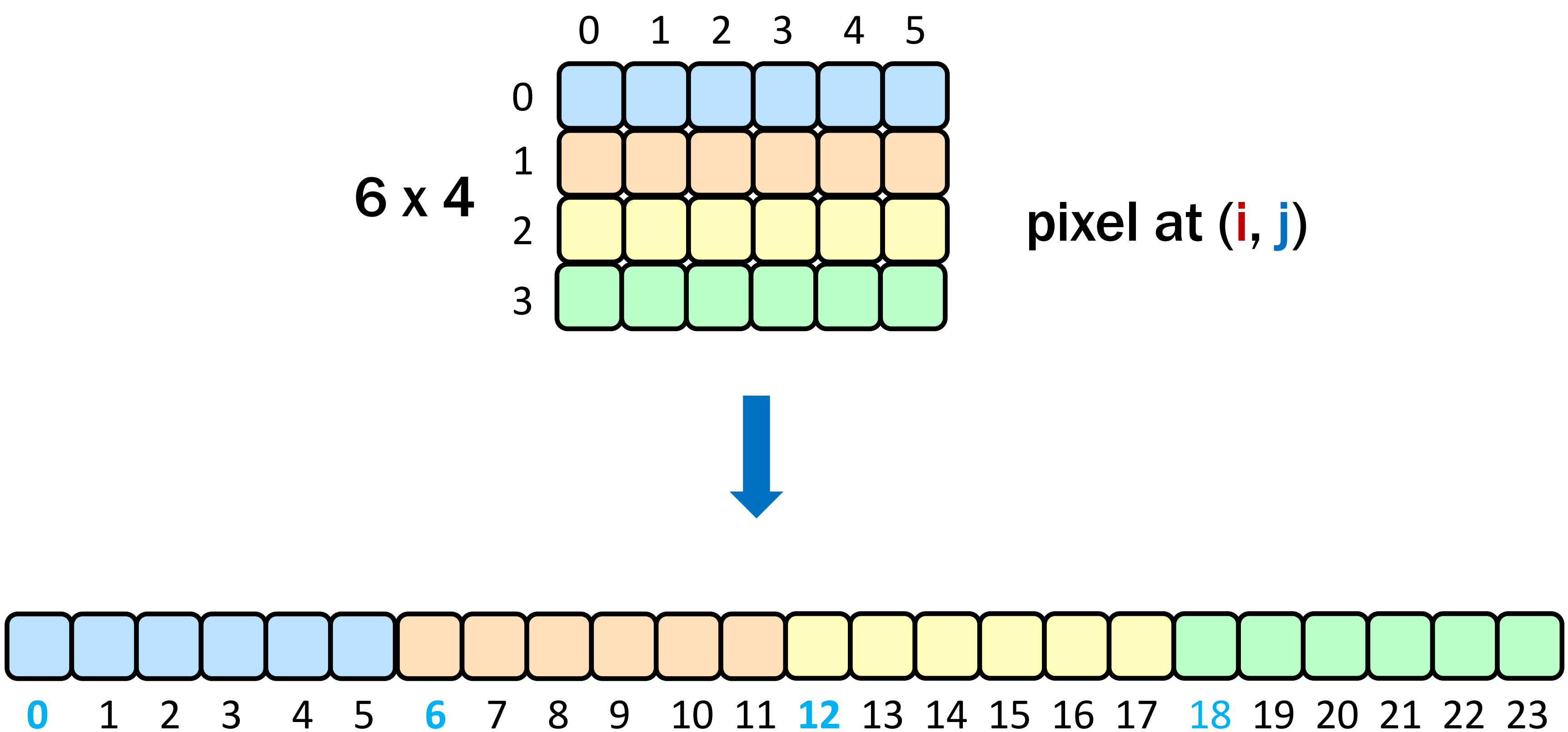


pixel at (i, j)

Stored at index n.
How do we calculate n from i and j?

$$n = i \cdot 6 + j$$

Pixels in Memory



Stored at index n.
How do we calculate i and j from n?

i = n div 6
j = n mod 6

Number Theory

- Direct relevance to computing
  - important toolkit for programmers

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

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!

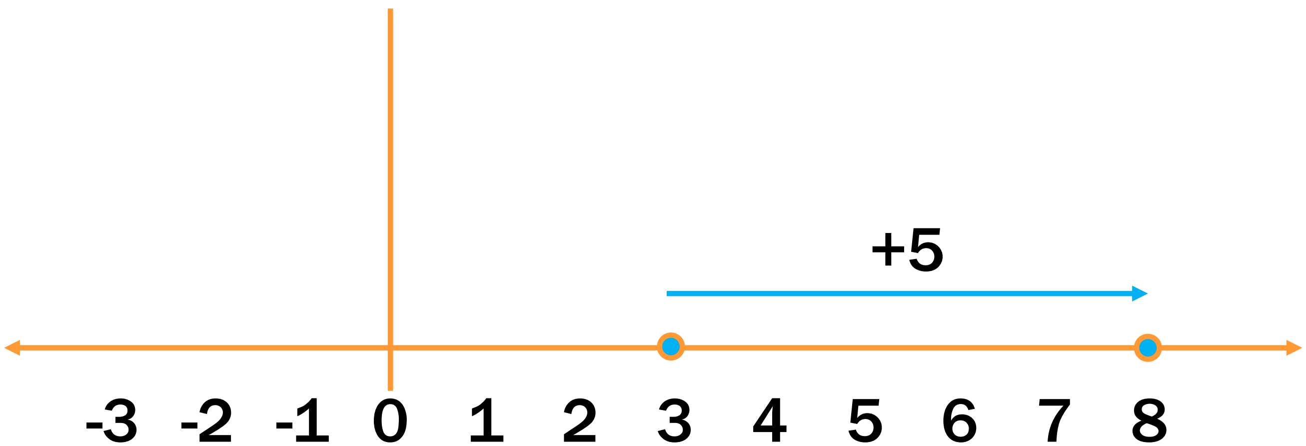
```
public class Test {
    final static int SEC_IN_YEAR = 365*24*60*60;
    public static void main(String args[]) {
        System.out.println(
            "I will be alive for at least " +
            SEC_IN_YEAR * 101 + " seconds."
        );
    }
}
```

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

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

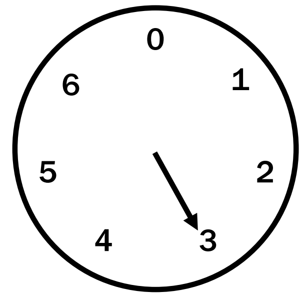
Ordinary arithmetic

$$3 + 5 = 8$$



Arithmetic on a Clock

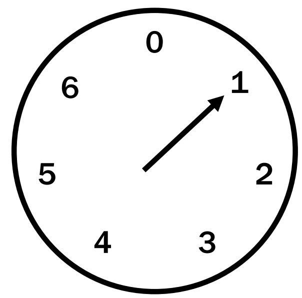
$3 + 5 = 8$



$8 = 7 \cdot 1 + 1$

$15 = 7 \cdot 2 + 1$

$22 = 7 \cdot 3 + 1$

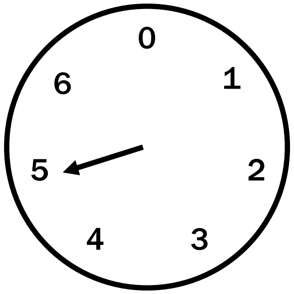


If $a = 7q + r$, then $r \ (= a \bmod b)$ is where you <u>stop</u> after taking a steps on the clock

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 $m > 0$

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

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?

$x \equiv_2 0$

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

$-1 \equiv_5 19$

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

$y \equiv_7 2$

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

Proof Plan:

1. $(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b)$??
2. $(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$??
3. $(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b) \wedge$
   $(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$ Intro $\wedge$: 1, 2
4. $(a \equiv_m b) \leftrightarrow (a \bmod m = b \bmod m)$ Equivalent: 3

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. $(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b)$??

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.? $a \equiv_m b$??

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

1.? $m \mid a - b$ — ??

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.? $\exists q\ (a - b = qm)$	??
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 $\boldsymbol{a, b, m}$ 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
1.2. $a = (a \operatorname{div} m)\, m + (a \bmod m)$	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 $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \ \mathbf{mod}\ \boldsymbol{m} = \boldsymbol{b} \ \mathbf{mod}\ \boldsymbol{m}$.

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

Apply Division
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 — Apply Division
$b = (b \operatorname{div} m)\, m + (b \bmod m)$. — 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 $\boldsymbol{m} > \boldsymbol{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \textbf{ mod } \boldsymbol{m} = \boldsymbol{b} \textbf{ mod } \boldsymbol{m}$.

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

Subtracting these we can see that

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

Algebra

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

…

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 — Apply Division
$b = (b \operatorname{div} m)\, m + (b \bmod m)$. — Apply Division

Subtracting these we can see that

$$a - b = \big((a \operatorname{div} m) - (b \operatorname{div} m)\big) m + ((a \bmod m) - (b \bmod m))$$
$$= \big((a \operatorname{div} m) - (b \operatorname{div} m)\big)\, m$$

— Algebra

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

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

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 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.? $a \bmod m = b \bmod m$ — ??

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

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ 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.? $a \bmod m = b \bmod m$	??
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 ≡
2.3. $\exists q\ (a - b = qm)$ — 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 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.? $a \bmod m = b \bmod m$	??
2. $(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$	Direct Proof

Modular Arithmetic: A Property

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

2.1. $a \equiv_m b$	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. $a = (a \text{ div } m)\, m + (a \bmod m)$	Apply Division
2.6. $b = (a \text{ div } m - k)\, m + (a \bmod m)$	Algebra
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 ≡
2.3. $\exists q\ (a - b = qm)$	Def of |
2.4. $a - b = km$	Elim ∃
2.5. $a = (a \text{ div } m)\, m + (a \bmod m)$	Apply Division
2.6. $b = (a \text{ div } m - k)\, m + (a \bmod m)$	Algebra
2.7. $b \text{ div } m = (a \text{ div } m - k) \wedge$ $b \bmod m = a \bmod m$	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 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. $a = (a \text{ div } m)\, m + (a \bmod m)$	Apply Division
2.6. $b = (a \text{ div } m - k)\, m + (a \bmod m)$	Algebra
2.7. $b \text{ div } m = (a \text{ div } m - k) \wedge$ $b \bmod m = a \bmod m$	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 $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

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

Suppose that $a \equiv_m b$. — Assumption

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

Then, $m \mid (a - b)$ by the definition of congruence. — Def of ≡
So, $a - b = km$ for some integer k by the definition of divides. Equivalently, $a = b + km$. — Def of | / Elim ∃

By the Division Theorem, we have $a = (a \text{ div } m)\, m + (a \bmod m)$, 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 $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

Suppose that $a \equiv_m b$. — Assumption

Then, $m \mid (a - b)$ by the definition of congruence. — Def of ≡
So, $a - b = km$ for some integer k by the definition of divides. Equivalently, $a = b + km$. — Def of | ; Elim ∃

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

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

Apply DivUnique
Elim ∃

Therefore, $a \bmod m = b \bmod m$. — Direct Proof

Modular Arithmetic: A Property

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

Suspose that $a \equiv_m b$. — Assumption

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

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

Combining these, we have $(a \text{ div } m)m + (a \bmod m) = a = b + km$. Solving for b gives $\mathrm{b} = (a \text{ div } m)\, m - km + (a \bmod m) = \big((a \text{ div } m) - k\big)m + (a \bmod m)$. — 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 $b \text{ div } m = a \text{ div } m - k$). — Apply DivUnique, Elim ∃

Direct Proof

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

- What we have just shown
  - The $\text{mod}\ m$ function maps any integer a to a remainder $a \bmod m \in \{0,1,..,m-1\}$.
  - Imagine grouping together all integers that have the same value of the $\text{mod}\ m$ function

    That is, the same remainder in $\{0,1,..,m-1\}$.
  - The $\equiv_m$ predicate compares integers a, b. It is true if and only if the $\text{mod}\ m$ function has the same value on a and on b.

    That is, a and b are in the same group.

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

Recall: Properties of "=" Used in Algebra

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

These are **Theorems** that
we use *implicitly* in Algebra

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

Let's see how to do this in **formal** logic…

Recall: Properties of "=" Used in Algebra

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

1. $5x + 4 = 2x + 25$	**Given**
2. $-4 = -4$	**Algebra**
3. $5x = 2x + 21$	**Add Equations: 1, 2**
4. $-2x = -2x$	**Algebra**
5. $3x = 21$	**Add Equations: 3, 4**

Recall: Properties of "=" Used in Algebra

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

1. $5x + 4 = 2x + 25$ **Given**

...

5. $3x = 21$ **Transitivity**

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

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

the second is a "backward" proof

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 "$\equiv_m$"?

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

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

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.?. $a \equiv_m c$??

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
2.2. $a \equiv_m b$	Elim $\land$: 2.1
2.3. $b \equiv_m c$	Elim $\land$: 2.1
2.?. $a \equiv_m c$	??
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
2.2. $a \equiv_m b$	Elim $\land$: 2.1
2.3. $b \equiv_m c$	Elim $\land$: 2.1
2.4. $m \mid a - b$	Def of $\equiv$: 2.2
2.5. $m \mid b - c$	Def of $\equiv$: 2.3
2.?. $a \equiv_m c$	??
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. $a \equiv_m b \wedge b \equiv_m c$	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 $\equiv$: 2.2
2.5. $m \mid b - c$	Def of $\equiv$: 2.3
2.6. $\exists q\ (a - b = qm)$	Def of $\mid$: 2.4
2.7. $\exists q\ (b - c = qm)$	Def of $\mid$: 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 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 $\equiv$: 2.2
2.5. $m \mid b - c$	Def of $\equiv$: 2.3
2.6. $\exists q\ (a - b = qm)$	Def of $\mid$: 2.4
2.7. $\exists q\ (b - c = qm)$	Def of $\mid$: 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 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
…	
2.8. $a - b = km$	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 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

...

2.8. $a - b = km$ Elim ∃: 2.6

2.9. $b - c = jm$ Elim ∃: 2.7

2.?. $m \mid a - b$??

2.?. $a \equiv_m c$ Def of ≡

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
...	
2.8. $a - b = km$	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. $(a \equiv_m b \wedge b \equiv_m c) \rightarrow (a \equiv_m c)$	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
...	
2.8. $a - b = km$	Elim $\exists$: 2.6
2.9. $b - c = jm$	Elim $\exists$: 2.7
2.10. $a - c = (k + j)m$	Algebra
2.11. $\exists q\ (a - c = qm)$	Intro $\exists$: 2.10
2.12. $m \mid a - c$	Def of |: 2.11
2.13. $a \equiv_m c$	Def of $\equiv$: 2.12
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 $\boldsymbol{m > 0}$.
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 $\wedge$
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 $\boldsymbol{m > 0}$.
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 $b \equiv_m c$. — Assumption

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. — Elim ∧, Def of ≡, Def of |, Elim ∃

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

Intro ∃

Def of |

Def of ≡

Therefore, $a \equiv_m c$. — Direct Proof

Modular Arithmetic: Basic Property

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

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

1. $(\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b} \wedge \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}) \rightarrow (\boldsymbol{a}+\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b}+\boldsymbol{d})$??

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 $\boldsymbol{a} + \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b} + \boldsymbol{d}$.

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

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

1. $(\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b} \wedge \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}) \rightarrow (\boldsymbol{a} + \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b} + \boldsymbol{d})$ 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 $\wedge$: 2.1
2.3. $c \equiv_m d$ Elim $\wedge$: 2.1

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 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
2.2. $a \equiv_m b$	Elim $\land$: 2.1
2.3. $c \equiv_m d$	Elim $\land$: 2.1
2.4. $m \mid a - b$	Def of ≡: 2.2
2.5. $m \mid c - d$	Def of ≡: 2.3
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. $a \equiv_m b \wedge c \equiv_m d$	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 $\equiv$: 2.2
2.5. $m \mid c - d$	Def of $\equiv$: 2.3
2.6. $\exists q\ (a - b = qm)$	Def of $\mid$: 2.4
2.7. $\exists q\ (c - d = qm)$	Def of $\mid$: 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 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 $\wedge$: 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. $a - b = km$	Elim $\exists$: 2.6
2.9. $c - d = jm$	Elim $\exists$: 2.7
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. $a \equiv_m b \land c \equiv_m d$	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 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.?. $\exists q\, ((a + c) - (b + d) = qm)$	??
2.?. $m \mid (a + c) - (b + d)$	Def of |
2.?. $a + c \equiv_m b + d$	Def of ≡
1. $(a \equiv_m b \land c \equiv_m d) \rightarrow (a + c \equiv_m b + d)$	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
...	
2.8. $a - b = km$	Elim $\exists$: 2.6
2.9. $c - d = jm$	Elim $\exists$: 2.7
2.10. $(a + c) - (b + d) = (k + j)m$	Algebra
2.11. $\exists q\ ((a + c) - (b + d) = qm)$	Intro $\exists$: 2.10
2.12. $m \mid (a + c) - (b + d)$	Def of $\mid$: 2.11
2.13. $a + c \equiv_m b + d$	Def of $\equiv$: 2.12
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 $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b} + \boldsymbol{d}$.

Assumption

Elim $\wedge$

Def of $\equiv$

Def of |

Elim $\exists$

Algebra

Intro $\exists$

Def of |

Def of $\equiv$

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 $c \equiv_m d$.

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

Assumption

Elim $\wedge$

Def of $\equiv$

Def of $|$

Elim $\exists$

Algebra

Intro $\exists$

Def of $|$

Def of $\equiv$

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 $\wedge$, Def of $\equiv$, Def of $\mid$, Elim $\exists$

Algebra

Intro $\exists$

Def of $\mid$

Def of $\equiv$

Therefore, $a + c \equiv_m b + d$. — 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 $\boldsymbol{a + c \equiv_m b + d}$.

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 $\wedge$, Def of $\equiv$, Def of $\mid$, Elim $\exists$

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

Intro $\exists$

Def of $\mid$

Therefore, $a + c \equiv_m b + d$. — Def of $\equiv$

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

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 $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{ac} \equiv_{\boldsymbol{m}} \boldsymbol{bd}$.

Modular Arithmetic: Multiplication Property

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

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 ∃

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

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 $\boldsymbol{ac \equiv_m bd}$.

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 ∃

Intro ∃
Def of |
Def of ≡

Show: $\exists k\,(ac - bd = km)$

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

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 $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

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

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

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

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

Modular Arithmetic: Properties

If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

If $a \equiv_m b$, then $a + c \equiv_m b + c$.

If $a \equiv_m b$, then $ac \equiv_m bc$.

"$\equiv_m$" allows us to solve problems in modular arithmetic, e.g.

- **add / subtract numbers from both sides of equations**
- **chains of "$\equiv_m$" values shows first and last are "$\equiv_m$"**
- **substitute "$\equiv_m$" values in equations (not proven yet)**

Properties of "$\equiv_m$" Used in Algebra

If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$	"Transitivity"
If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$	"Add Equations"
If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$	"Multiply Equations"

These are **Theorems** that
we use *implicitly* in Algebra

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

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 Equations"
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 Equations"

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

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

3. $5x \equiv_{\mathrm{m}} 2x+21$ **Add Equations: 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 Equations"
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 Equations"

1. $5x + 4 \equiv_{\mathrm{m}} 2x + 25$	**Given**
2. $-4 = -4$	**Algebra**
3. $-4 \equiv_{\mathrm{m}} -4$	**To Modular: 2**
4. $5x \equiv_{\mathrm{m}} 2x + 21$	**Add Equations: 3, 1**
5. $-2x = -2x$	**Algebra**
6. $-2x \equiv_{\mathrm{m}} -2x$	**To Modular**
7. $3x \equiv_{\mathrm{m}} 21$	**Add Equations: 4, 6**

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

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

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

This is also true of congruences!
(We just don't have the tools to prove it yet.)

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

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

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

1.1.1. $a \bmod m = b \bmod m$	Assumption
...	
1.1.7. $a \equiv_m b$	Def of ≡
1.1. $(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b)$	Direct Proof
1.2.1. $a \equiv_m b$	Assumption
...	
1.2.8. $a \bmod m = b \bmod m$	Elim ∧
1.2. $(a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$	Direct Proof
1.3. $(a \bmod m = b \bmod m) \rightarrow (a \equiv_m b) \wedge (a \equiv_m b) \rightarrow (a \bmod m = b \bmod m)$	Intro ∧
1.4. $(a \equiv_m b) \leftrightarrow (a \bmod m = b \bmod m)$	Equivalent
1. $\forall a\, \forall b\, ((a \equiv_m b) \leftrightarrow (a \bmod m = b \bmod m))$	Intro ∀

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 $\boldsymbol{a} \mathbf{\ mod\ } \boldsymbol{m} = \boldsymbol{b} \mathbf{\ mod\ } \boldsymbol{m}$.

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 $\boldsymbol{m} > \mathbf{0}$).

Rule: unquantified variables are *implicitly* ∀-quantified
(will see one exception later…)

Recall: Modular Arithmetic: A Property

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

But the proof **stays** as is!

<u>Rule</u>: structure of the proof follows the structure of the claim