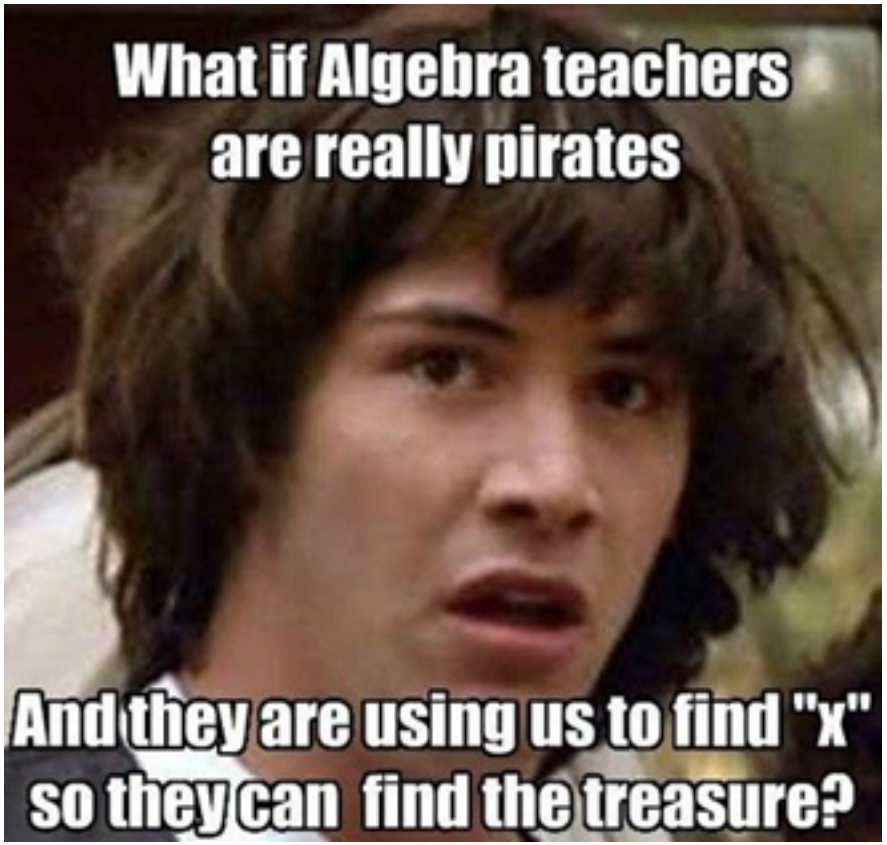
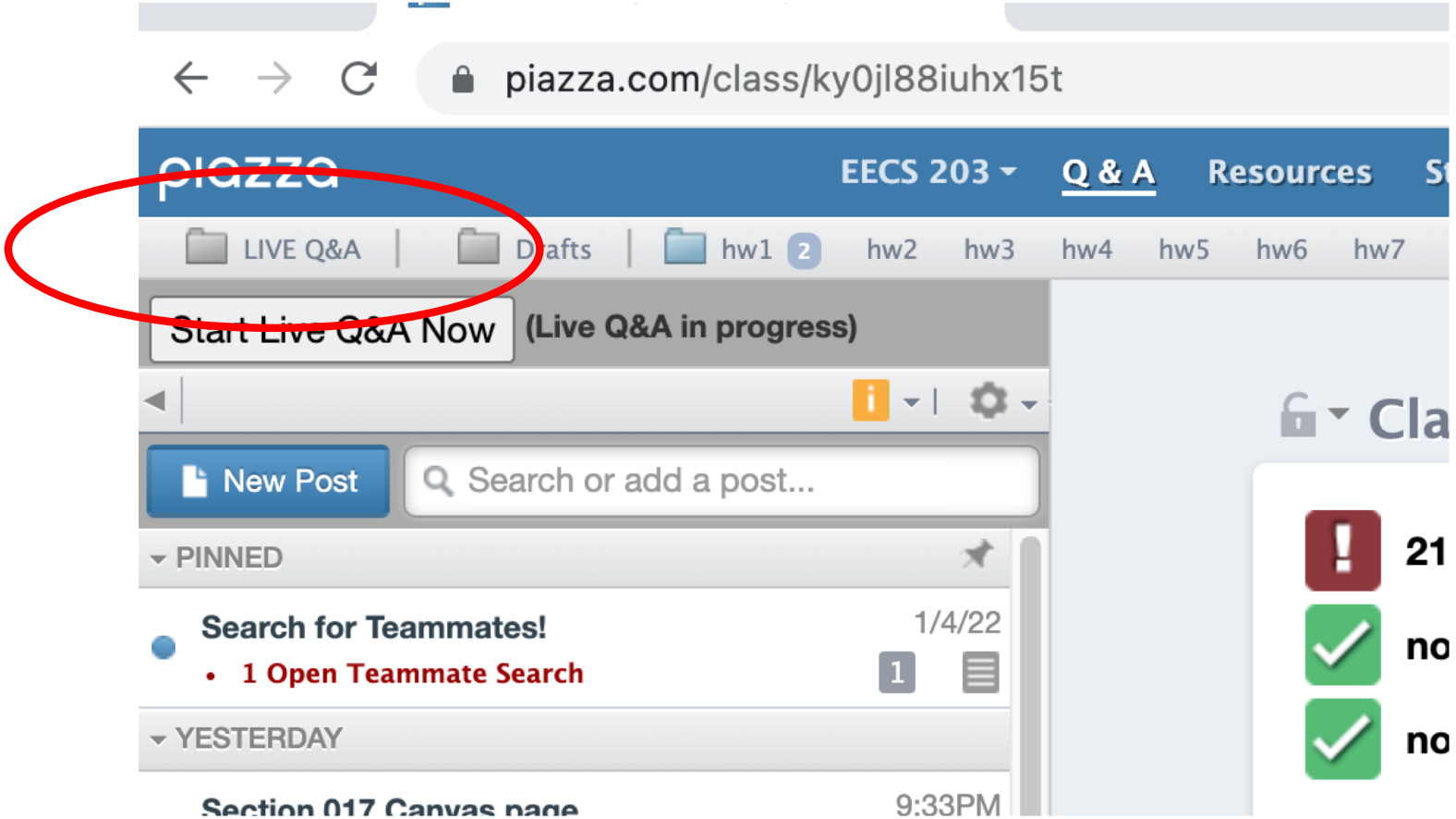
Modular Arithmetic



EECS 203 Lecture 2

Questions during lecture (Prof. Diaz's sections)

- Raise your hand any time
- Ask via Piazza's "Live Q&A"
  - If you're on Zoom or if you're in person



Learning Objectives: Lec 2

After today's lecture (and the associated readings, discussion, & homework), you should be able to:

- **Know Technical Vocab:** $a \equiv b \pmod{m}$, $a \pmod{m}$, equivalence/congruence, inverses, relatively prime
- Reduce any integer (mod m) to an integer in $\{0, \ldots, m-1\}$
- Translate statements about the integers into the language of modular arithmetic
- Determine whether x has an inverse (mod m), and find it by guess-and-check if so
- Solve equivalences of the form $ax + b \equiv c \pmod{m}$, or recognize that there is not a unique solution

Outline

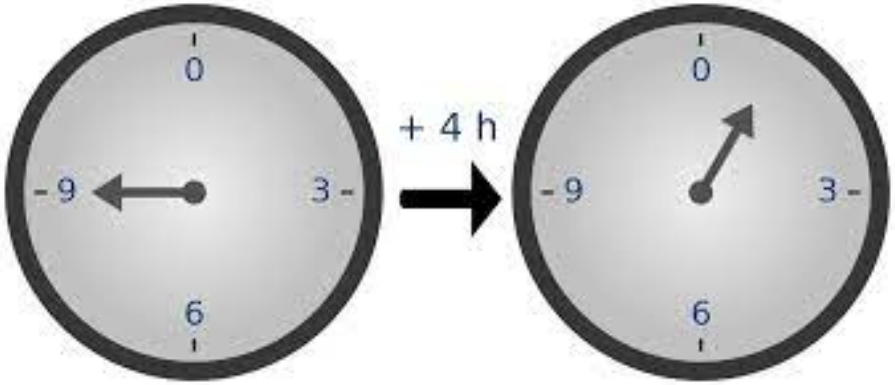
- **Intro to modular arithmetic**
  - Examples of modular arithmetic
  - Equivalence mod m
  - (x mod m)
  - Translating propositions into modular arithmetic
- Addition/subtraction
- Multiplication
- Division and inverses

Modular Arithmetic

- Sometimes, we want to do arithmetic **"with rollover"**

- The clock shows 9:00 right now. What time will it show in 4 hours?

- $9 + 4 = 13 \rightarrow$ **1**



"Clocks use arithmetic **mod 12**"

Modular Arithmetic

- Sometimes, we want to do arithmetic **"with rollover"**

- unsigned int_8 x = 129
- What value will the computer assign $\mathbf{2}^{*}\boldsymbol{x}$?
- (Max value is 255; 256 rolls back over to 0)

- $2x = 258 \rightarrow$ **2**

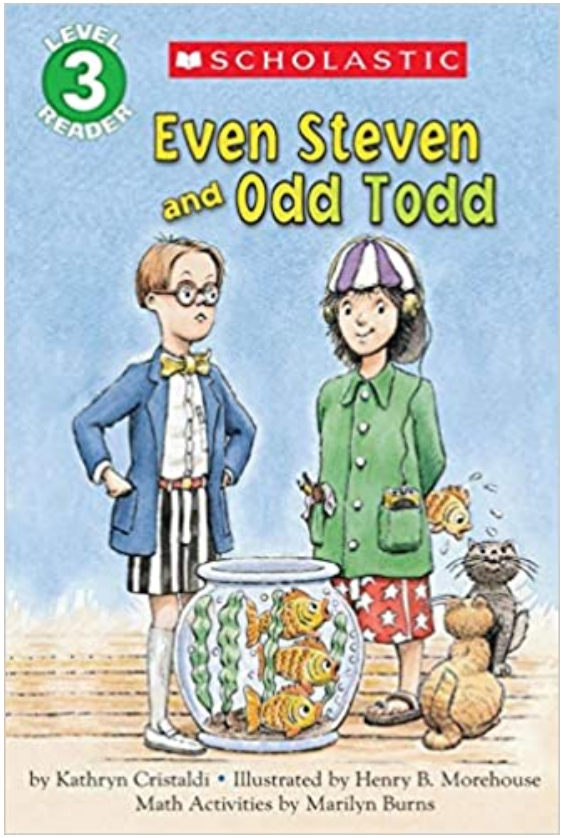
"unsigned int_8's use arithmetic **mod 256**"

Modular Arithmetic

- Sometimes, we want to do arithmetic **"with rollover"**

- Is 203+281 even or odd?
  - When you divide it by 2, is the remainder 0 or 1?

- $203 + 281 = 484 \rightarrow$ **0**



"Even/odd calculations use arithmetic **mod 2**"

Why are we studying this?

- Simple, semi-familiar example of a discrete structure
- Modular arithmetic is the foundation for number theory
- Number theory is critical in cryptography
  - Advanced cryptosystems (e.g., RSA encryption) also are based on number theory

- Also: more exposure to reading/writing proofs

Recall some basics from Algebra

In **Algebra (over the reals)**, you add or multiply terms from equations while preserving **equality**. We often solve for an unknown x.

Modular Arithmetic

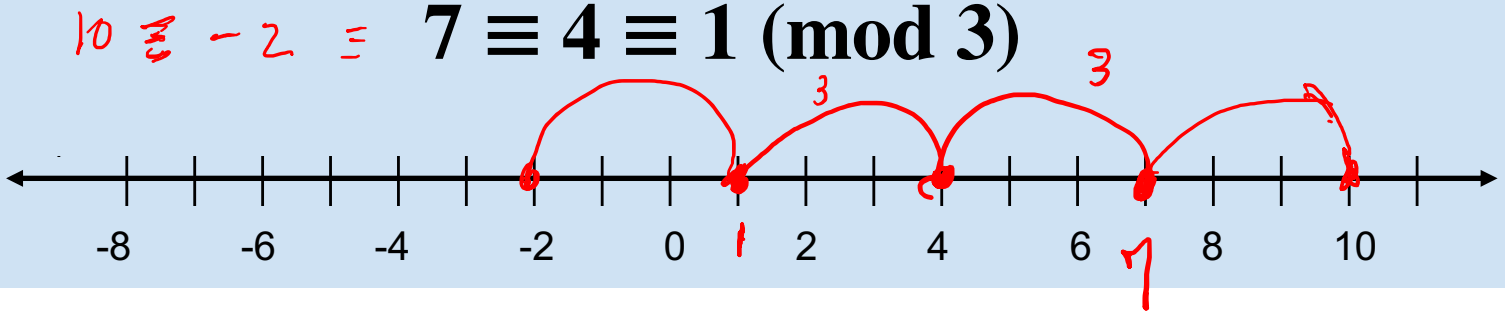
In **modular arithmetic**, we make a few changes:

- We work over the **integers**, not the reals.
  - So **x = 4/3** is not valid.
- We only care about the **remainder** when divided by **m**
  - m > 1
- We talk about **equivalence (mod m)**, not equality.

a ≡ b (mod m)
means that **a** and **b** have the same remainder when divided by **m**.

Example:

$10 \equiv -2 \equiv 7 \equiv 4 \equiv 1 \pmod 3$



Modular Arithmetic

In **modular arithmetic**, we make a few changes:

- We work over the **integers**, not the reals.
  - So **x = 4/3** is not valid.
- We only care about the **remainder** when divided by m
  - m > 1
- We talk about **equivalence (mod m)**, no

Read: "equivalent to" or "congruent to"
here: "4 is congruent to 1, mod 3"

"mod 3" modifies the entire equation, not the 1 specifically

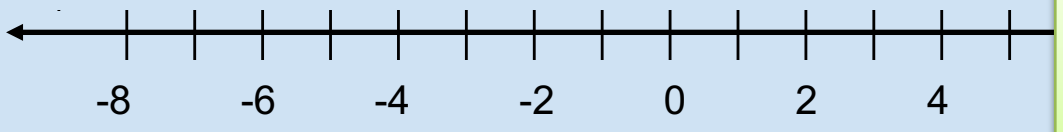
…od m)

means that **a** and **b** have the same remainder when divided by **m**.

$4 \equiv 1 \pmod 3$

Example:

$$7 \equiv 4 \equiv 1 \pmod 3$$



m is called the *modulus*. Here the modulus is 3.

Definition of Modular Equivalence

Definition: $a \equiv b \pmod{m}$ means
There exists an integer **k** such that $a = b + mk$
a = b + mk

Read: "a is **equivalent to** b mod m"
or "a is **congruent to** b mod m"
The (mod m) modifies the entire equivalence, not just the b, even though it's written at the end.

$a \equiv b \pmod{m}$

Example: $1 \equiv 7 \pmod{3}$

Because $1 = 7 + 3 \cdot (-2)$

$k = -2$

$1 = 7 + 3k$

Definition of Modular Equivalence

Definition: **$a \equiv b \pmod{m}$** means
There exists an integer **k** such that
a = b + mk

Read: "a is **equivalent to** b mod m"
or "a is **congruent to** b mod m"
The (mod m) modifies the entire equivalence, not just the b, even though it's written at the end.

Non-Example: $107 \not\equiv 3 \ (mod\ 10)$ $\updownarrow$ $107 \neq 3 + 10k$

Because $107 = 3 + 10k$ solves to
$k = 10.4$ (not an integer)

The Other "mod"

The statement **a ≡ b (mod m)** is a **proposition** involving three integers

The statement **a mod m** is an **integer** in $\{0, \ldots, m-1\}$, which is the remainder when we divide a by m.

- Written a%m in C++
- (Examples) 13 mod 5 = 3, 7 mod 3 = 1

a ≡ b (mod m)

can be equivalently defined as

(a mod m) = (b mod m)

a ≡ b (mod m) means a mod m = b mod m

"a and b have the same remainder when divided by m"

Alternate Defs of Mod Equivalence

a ≡ b (mod m) means

a and **b** have the same remainder when divided by m
(i.e., **a mod m = b mod m**)

Or, equivalently

a - b is a multiple of **m**
(i.e., **a - b = mk** for some integer **k**)

Or, equivalently

There exists an integer **k** such that
a = b + mk

"main" definition

7 ≡ 10 (mod 3), because:

7 ≡ 10 (mod 3) because

- 7÷3 has a remainder of 1
- 10÷3 also has a remainder of 1

7 – 10 = -3, which is a multiple of 3

$7 = 10 + 3(-1)$
here $k = -1$

Lecture 2 Handout: Modular Arithmetic

Definitions of Mod:

- **a ≡ b (mod m):** There exists an integer **k** such that $a = b + mk$
- **a mod m:** The integer in $\{0, 1, \ldots, m-1\}$ which is the remainder when we divide a by m.

Alternate definitions of a ≡ b (mod m):

- a and b have the same remainder
- $a - b$ is an integer multiple of m

The "range" of mod

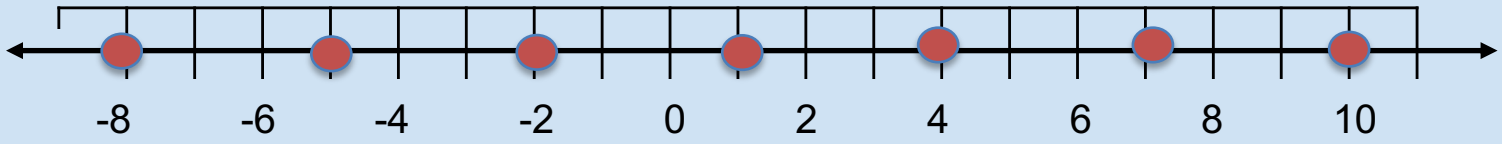
- Every integer x is equivalent to infinitely many other integers (mod m)
- But x is always equivalent to **exactly one** integer in the range $\{0, \ldots, m-1\}$.

in mod m

Example:

$$\ldots \equiv 7 \equiv 4 \equiv 1 \equiv \cdots \pmod 3$$

$$(\text{But } 7 \not\equiv 0, 7 \not\equiv 2 \pmod 3)$$



Translation

Last lecture, we saw:

Proposition
For all integers **x**, if **x** is even, then **x+2** is even.

Alt Definition: An integer x is "**even**" if $x \equiv 0 \ (mod\ 2)$

Rephrased Proposition
For all integers x, if $x \equiv 0 \ (mod\ 2)$, then $x + 2 \equiv 0 \ (mod\ 2)$

Translation

Last lecture, we saw:

Proposition:
There exists an integer x for which $4x$ is not even.

Alt Definition: An integer x is "**even**" if $x \equiv 0 \ (mod\ 2)$

Rephrased Proposition
There exists an integer x for which $4x \not\equiv 0 \pmod 2$.

Translation

Last lecture, we saw:

Proposition:
For all integers x, $3x$ is a multiple of 9.

Alt Definition: An integer x is a "**multiple**" of another integer y if $x \equiv 0 \ (mod \ y)$

Rephrased Proposition
For all integers x, $3x \equiv 0 \ (mod \ 9)$

Warm Up Exercises

Handout

1. (a) $8 \bmod 5 =$ 3

   (b) $(25 \bmod 7)^2 =$ $4^2 = 16$

2. T / F $27 \equiv 32 \pmod 5$

   T / F $27 \equiv 2 \pmod 5$

   T / F $27 \equiv -3 \pmod 5$

   T / F $-17 \equiv 1 \pmod 9$

$27 = 2 + 5k$ works $k=5$

b/c $27 \div 5 \Rightarrow$ rem $= 2$

$2 \div 5 \Rightarrow$ rem $= 2$

$27 - (-3) = 30$

$= 5k$ ✓

$-17 - 1 = -18$

$= 9 \cdot k$ ✓ $k = -2$

3. Find 3 numbers, including at least one negative number, that are equivalent to 30 (mod 9):

39, -6, 3, 12, 21, 84

Check-in

Slido.com
#203203

- How many of the T/F equivalences are true?

A. None are true

B. 1

C. 2

D. 3

E. All are true

Modular Arithmetic

Main goal today:
Can we do basic solve-for-x type algebra problems in the world of modular arithmetic?

In **algebra (over real numbers)**, we add or multiply terms to both sides of equations, solving for an unknown x.

Example:
Given $\mathbf{3x + 8 = 4}$, we can uniquely solve for **x**:

(Subtract 8 from both sides) $\boldsymbol{3x = -4}$

(Multiply both sides by 3^{-1}) $\boldsymbol{x = -\frac{4}{3}}$

In algebra over the reals, $3^{-1} = 1/3$.

Modular Arithmetic

In **modular arithmetic**, we make two changes:

- ***x* must be an integer.** So **x = 4/3** is not valid.
- We talk about **equivalence (mod m)**, not equality.

Example:

Given $\mathbf{3}\boldsymbol{x} + \mathbf{8} \equiv \mathbf{4}\ (\boldsymbol{mod}\ \mathbf{5})$,

- Is there an **integer solution *x*?**
- If so, is there a **unique** integer solution x, or do several choices work?

If $x = 2$ works
Then $x = 7$ also works
And $x = 12$ also works
And $x = 17$ also works …

To avoid this, **"unique"** should mean unique choice of x in $\{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{4}\}$.

Modular Arithmetic

In **modular arithmetic**, we make two changes:

- ***x* must be an integer.** So **x = 4/3** is not valid.
- We talk about **equivalence (mod m)**, not equality.

Example:

$$\mathbf{3}\boldsymbol{x} + \mathbf{8} \equiv \mathbf{4}\ (\boldsymbol{mod}\ \mathbf{5}),$$

- By guess-and-check (for now): → {0, 1, 2, 3, 4}

$x = 2$ is the unique solution with x in $\{0,1,2,3,4\}$

$$x = 0: \quad 3(0) + 8 = 8 \equiv 3\ (mod\ 5)$$
$$x = 1: \quad 3(1) + 8 = 11 \equiv 1\ (mod\ 5)$$
$$x = 2: \quad 3(2) + 8 = 14 \equiv 4\ (mod\ 5)$$
$$x = 3: \quad 3(3) + 8 = 17 \equiv 2\ (mod\ 5)$$
$$x = 4: \quad 3(4) + 8 = 20 \equiv 0\ (mod\ 5)$$

Or: This equivalence reduces to $x \equiv 2\ (mod\ 5)$

Modular Arithmetic

Example:

$$\mathbf{3}\boldsymbol{x} + \mathbf{8} \equiv \mathbf{4}\ (\boldsymbol{mod}\ \mathbf{5}),$$

- Can we solve this using standard algebra?

Do the basic operations work:

Add/subtract something on both sides?

Multiply something on both sides?

Divide something on both sides?

Outline

- Intro to modular arithmetic
  - Examples of modular arithmetic
  - Equivalence mod m
  - (x mod m)
  - Translating propositions into modular arithmetic
- **Addition/subtraction**
- Multiplication
- Division and inverses

Modular Addition/Subtraction

$x + 12 \equiv 3 \pmod 5$

Is there a unique solution with x in {0,1,2,3,4}?

Slido.com
#203203

A. Yes, unique solution $x \equiv 1 \pmod 5$
B. No, several possible solutions
C. No, no solutions
D. I don't understand the question.
E. I understand the question but I'm not sure.

Modular Addition/Subtraction

$x + 12 \equiv 3 \pmod 5$

Is there a unique solution with x in $\{0,1,2,3,4\}$?

A. Yes, unique solution
B. No, several possible solutions
C. No, no solutions
D. I don't understand the question.
E. I understand the question but I'm not sure.

Modular Addition/Subtraction

x + 12 ≡ 3 (mod 5)

Is there a unique solution with x in $\{0,1,2,3,4\}$?

The Dream Solution

- **(subtract 12 from both sides)** $x \equiv -9 \ (mod\ 5)$
- **(find equivalent x in range)** $x \equiv 1\ (mod\ 5)$

Main question: is this operation valid?

- From algebra: subtracting c from both sides preserves **equalities**
- But does subtracting c from both sides also preserve **modular equivalences?**

Modular Addition/Subtraction

Proposition:

For all integers a, b, c, d, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

"Adding **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Def: $\boldsymbol{a \equiv b \pmod{m}}$ means there exists an integer k such that $a = b + mk$

Proof:

- There is an integer k_1 such that $a = b + mk_1$.

Uses definition of modular equivalence

Modular Addition/Subtraction

Proposition:

For all integers a, b, c, d, if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $a + c \equiv b + d \ (mod\ m)$.

"Adding **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Def: $\boldsymbol{a \equiv b \ (mod\ m)}$ means there exists an integer k such that $a = b + mk$

Proof:

- There is an integer k_1 such that $a = b + mk_1$.
- There is an integer k_2 such that $c = d + mk_2$.

$a = b + mk_1$

$c = d + mk_2$

Uses definition of modular equivalence (again)

Modular Addition/Subtraction

Proposition:
For all integers a, b, c, d, if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $a + c \equiv b + d \ (mod\ m)$.

"Adding **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Def: $\boldsymbol{a \equiv b \ (mod\ m)}$ means there exists an integer k such that $a = b + mk$

Proof:
- There is an integer k_1 such that $a = b + mk_1$.
- There is an integer k_2 such that $c = d + mk_2$.
- So $a + c = b + mk_1 + d + mk_2$

Uses laws of algebra

Modular Addition/Subtraction

Proposition:
For all integers a, b, c, d, if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $a + c \equiv b + d \ (mod\ m)$.
"Adding **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Def: $\boldsymbol{a \equiv b \ (mod\ m)}$ means there exists an integer k such that $a = b + mk$

Proof:
- There is an integer k_1 such that $a = b + mk_1$.
- There is an integer k_2 such that $c = d + mk_2$.
- So $a + c = b + mk_1 + d + mk_2$
- So $a + c = b + d + m(k_1 + k_2)$

Uses laws of algebra (again)

Modular Addition/Subtraction

Proposition:
For all integers a, b, c, d, if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $a + c \equiv b + d \ (mod\ m)$.
"Adding **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Def: $\boldsymbol{a \equiv b \ (mod\ m)}$ means there exists an integer k such that $a = b + mk$

Proof:
- There is an integer k_1 such that $a = b + mk_1$.
- There is an integer k_2 such that $c = d + mk_2$.
- So $a + c = b + mk_1 + d + mk_2$
- So $a + c = b + d + m(k_1 + k_2)$
- Since k_1, k_2 are both integers, $k_1 + k_2$ is an integer

Uses closure of integers under addition

Modular Addition/Subtraction

Proposition:
For all integers a, b, c, d, if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $a + c \equiv b + d \ (mod\ m)$.
"Adding **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Def: $\boldsymbol{a \equiv b \ (mod\ m)}$ means there exists an integer k such that $a = b + mk$

Proof:
- There is an integer k_1 such that $a = b + mk_1$.
- There is an integer k_2 such that $c = d + mk_2$.
- So $a + c = b + mk_1 + d + mk_2$
- So $a + c = b + d + m(k_1 + k_2)$
- Since k_1, k_2 are both integers, $k_1 + k_2$ is an integer
- So $a + c \equiv b + d \ (mod\ m)$

Uses def of mod equivalence (done!)

Modular Addition/Subtraction

$x + 12 \equiv 3 \pmod 5$

What is **x (mod 5)**? Is there a **unique** answer?

The Dream Solution

- **(subtract 12 from both sides)** $x \equiv -9 \pmod 5$
- **(find equivalent x in range)** $x \equiv 1 \pmod 5$

This is legit!

By previous proof, adding/subtracting c from both sides preserves an equivalence.

(subtracting c is the same as adding $-c$)

Modular Arithmetic

Do the basic operations work:

✓Add/subtract something on both sides?

Multiply something on both sides?

Divide something on both sides?

You can add (or subtract) the same number (or an equivalent number) to both sides

Outline

- Intro to modular arithmetic
  - Examples of modular arithmetic
  - Equivalence mod m
  - (x mod m)
  - Translating propositions into modular arithmetic
- Addition/subtraction
- **Multiplication**
- Division and inverses

Modular Multiplication

Next question: Can we **multiply** both sides of an equivalence by c?

- From algebra: multiplying c on both sides preserves **equalities**
- But does it also preserve **modular equivalences?**

Example:

Say $x \equiv 2 \ (mod\ 7)$
Does that imply that $3x \equiv 6 \ (mod\ 7)$?

Modular Multiplication

Proposition:

For all integers a, b, c, d, if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $ac \equiv bd \ (mod\ m)$.

"Multiplying **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Example:

- $\mathbf{8 \equiv -2 \ (mod\ 5)}$ and also $\mathbf{4 \equiv 9 \ (mod\ 5)}$.
- Can we multiply both sides? Is $\mathbf{8 \cdot 4 \equiv (-2) \cdot 9 \ (mod\ 5)?}$
- This gives: $\mathbf{32 \equiv -18 \ (mod\ 5)}$. This is true!

This is not a proof! It's just one example.

To prove the proposition, we need to show that it holds for *all* values of a, b, c, d, m.

Modular Multiplication

Proposition:

For all integers a, b, c, d, if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $ac \equiv bd \ (mod\ m)$.

"Multiplying **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Def: $\boldsymbol{a \equiv b \ (mod\ m)}$ means there exists an integer k such that $a = b + mk$

Proof:

- There is an integer k_1 such that $a = b + mk_1$.
- There is an integer k_2 such that $c = d + mk_2$.

Uses definition of modular equivalence (twice)

Modular Multiplication

Proposition:

For all integers a, b, c, d, if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $ac \equiv bd \ (mod\ m)$.

"Multiplying **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Def: $\boldsymbol{a \equiv b \ (mod\ m)}$ means there exists an integer k such that $a = b + mk$

Proof:

- There is an integer k_1 such that $a = b + mk_1$.
- There is an integer k_2 such that $c = d + mk_2$.
- So $ac = (b + mk_1)(d + mk_2)$

Uses laws of algebra

Modular Multiplication

Proposition:

For all integers a, b, c, d, if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $ac \equiv bd \ (mod\ m)$.

"Multiplying **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Def: $\boldsymbol{a \equiv b \ (mod\ m)}$ means there exists an integer k such that $a = b + mk$

Proof:

- There is an integer k_1 such that $a = b + mk_1$.
- There is an integer k_2 such that $c = d + mk_2$.
- So $ac = (b + mk_1)(d + mk_2)$
- So $ac = bd + m(bk_2 + dk_1 + mk_1k_2)$

Uses algebra to refactor equation

Modular Multiplication

Proposition:

For all integers a, b, c, d, if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $ac \equiv bd \ (mod\ m)$.

"Multiplying **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Def: $\boldsymbol{a \equiv b \ (mod\ m)}$ means there exists an integer k such that $a = b + mk$

Proof:

- There is an integer k_1 such that $a = b + mk_1$.
- There is an integer k_2 such that $c = d + mk_2$.
- So $ac = (b + mk_1)(d + mk_2)$
- So $ac = bd + m(bk_2 + dk_1 + mk_1k_2)$
- Since b, d, k_1, k_2 are all integers, $(bk_2 + dk_1 + mk_1k_2)$ is also an integer

Uses closure of integers under addition and multiplication

Modular Multiplication

Proposition:

For all integers a, b, c, d, if $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $ac \equiv bd \ (mod\ m)$.

"Multiplying **equivalent integers** to both sides of an **equivalence** preserves the equivalence."

Def: $\boldsymbol{a \equiv b \ (mod\ m)}$ means there exists an integer k such that $a = b + mk$

Proof:

- There is an integer k_1 such that $a = b + mk_1$.
- There is an integer k_2 such that $c = d + mk_2$.
- So $ac = (b + mk_1)(d + mk_2)$
- So $ac = bd + m(bk_2 + dk_1 + mk_1k_2)$
- Since b, d, k_1, k_2 are all integers, $(bk_2 + dk_1 + mk_1k_2)$ is also an integer
- So $ac \equiv bd \ (mod\ m)$

Uses def of mod equivalence (and done!)

Modular Arithmetic

Do the basic operations work:

✓ Add/subtract something on both sides?

✓ Multiply something on both sides?

Divide something on both sides?

You can add (or subtract) the same number (or an equivalent number) to both sides

You can multiply the same number (or an equivalent number) to both sides

Outline

- Intro to modular arithmetic
  - Examples of modular arithmetic
  - Equivalence mod m
  - (x mod m)
  - Translating propositions into modular arithmetic
- Addition/subtraction
- Multiplication
- **Division and inverses**

Does Division Work?

Let's explore some examples.

Solve the following for **x**: (via guess and check, for now)

(a) $2x - 7 \equiv 3 \pmod 6$

(b) $2x - 7 \equiv 3 \pmod 7$

(c) $2x \equiv 3 \pmod 6$

For each equivalence, answer options will be:

A. Unique solution (in $\{0, \ldots, m-1\}$)
B. Several possible solutions
C. No solutions
D. Not sure

Does Division Work? Examples

For each equivalence, what is **x mod m**? Is there a **unique** answer?

(a) **$2x - 7 \equiv 3 \pmod 6$**

try 0, 1, 2, 3, 4, 5

$2x \equiv 10 \pmod 6$

$x \equiv 5 \pmod 6$

$2x \equiv 4 \pmod 6$

$x \equiv 2 \pmod 6$

(b) **$2x - 7 \equiv 3 \pmod 7$**

$x \equiv 5 \pmod 7$

(c) **$2x \equiv 3 \pmod 6$**

No solution

Does Division Work?

(a) $2x - 7 \equiv 3 \pmod 6$

What is **x**? Is there a **unique** answer?

Slido.com
#203203

A. Unique solution (in $\{0, \ldots, 5\}$)
B. Several possible solutions
C. No solutions
D. Not sure

Does Division Work?

(a) $2x - 7 \equiv 3 \pmod 6$

What is **x**? Is there a **unique** answer?

A. Unique solution (in $\{0, \ldots, 5\}$)
B. Several possible solutions
C. No solutions
D. Not sure

Does Division Work?

(a) $2x - 7 \equiv 3 \pmod 6$

What is **x**? Is there a **unique** answer?

One possibility:

x = 2

$2x - 7 = -3$

$-3 \equiv 3 \pmod 6$

Another possibility:

x = 5

$2x - 7 = 3$

$3 \equiv 3 \pmod 6$

Does Division Work?

(a) $2x - 7 \equiv 3 \pmod 6$

Several possible solutions ($x = 2$ or $x = 5$)

Why can't we do algebra? What went wrong?

(add 7 to both sides) $2x \equiv 10 \pmod 6$

(adjust right-hand side) $2x \equiv 4 \pmod 6$

$$\mathbf{(2^{-1})}2x \equiv \mathbf{(2^{-1})}4 \pmod 6$$

Does Division Work?

(a) $2x - 7 \equiv 3 \pmod 6$

Several possible solutions ($x = 2$ or $x = 5$)

do al

(2^{-1}) under (mod 6) DOES NOT EXIST!

So algebra doesn't work the way we're used to (i.e., there's not a single solution)

sides

nd s

2^{-1} ("inverse of 2") needs to be an integer such that

$(2^{-1})2 \equiv 1 \pmod 6$

Similar to how in algebra over reals,

$(2^{-1})2 = (1/2)2 = 1$

$$(2^{-1})2x \equiv (2^{-1})4 \pmod 6$$

Does Division Work?

(b) $2x - 7 \equiv 3 \pmod 7$

What is **x**? Is there a **unique** answer?

A. Unique solution (in $\{0, \ldots, 6\}$)
B. Several possible solutions
C. No solutions
D. Not sure

Does Division Work?

(b) $2x - 7 \equiv 3 \pmod 7$

What is **x**? Is there a **unique** answer?

A. Unique solution (in $\{0, \ldots, 6\}$)

B. Several possible solutions

C. No solutions

D. Not sure

Does Division Work?

(b) $2x - 7 \equiv 3 \pmod 7$

U

(add 7 to

(adjust rig

2^{-1} (**"inverse of 2"**) needs to be an integer such that

$$(2^{-1})2 \equiv 1 \pmod 7$$

Inverse exists! $2^{-1} = 4$

because $(4)2 = 8 \equiv 1\ (mod\ 7)$

$$(2^{-1})2x \equiv (2^{-1})3 \pmod 7$$

Does Division Work?

(b) $2x - 7 \equiv 3 \pmod 7$

Unique solution for x

(add 7 to both sides) $2x \equiv$

(adjust right-hand side) $2x$

Note: this time the inverse existed and there **was** a *unique* answer

$$(\mathbf{2^{-1}})2x \equiv (\mathbf{2^{-1}})3 \pmod 7$$

$$(\mathbf{4})2x \equiv (\mathbf{4})3 \pmod 7$$

$$8x \equiv 12 \pmod 7$$

(reduce both sides) $x \equiv 5 \pmod 7$

Does Division Work?

(c) $2x \equiv 3 \pmod 6$

What is **x**? Is there a **unique answer**?

A. Unique solution (in $\{0, \ldots, 5\}$)
B. Several possible solutions
C. No solutions
D. Not sure

Does Division Work?

(c) $2x \equiv 3 \pmod 6$

What is **x**? Is there a **unique answer**?

A. Unique solution (in $\{0, \ldots, 5\}$)
B. Several possible solutions
C. No solutions
D. Not sure

Why no answers? Proof sketch:

- **2x** is always even
- The only possible values for **2x mod 6** are 0, 2, or 4

Modular Arithmetic

Do the

Add/subtract

Multiply son

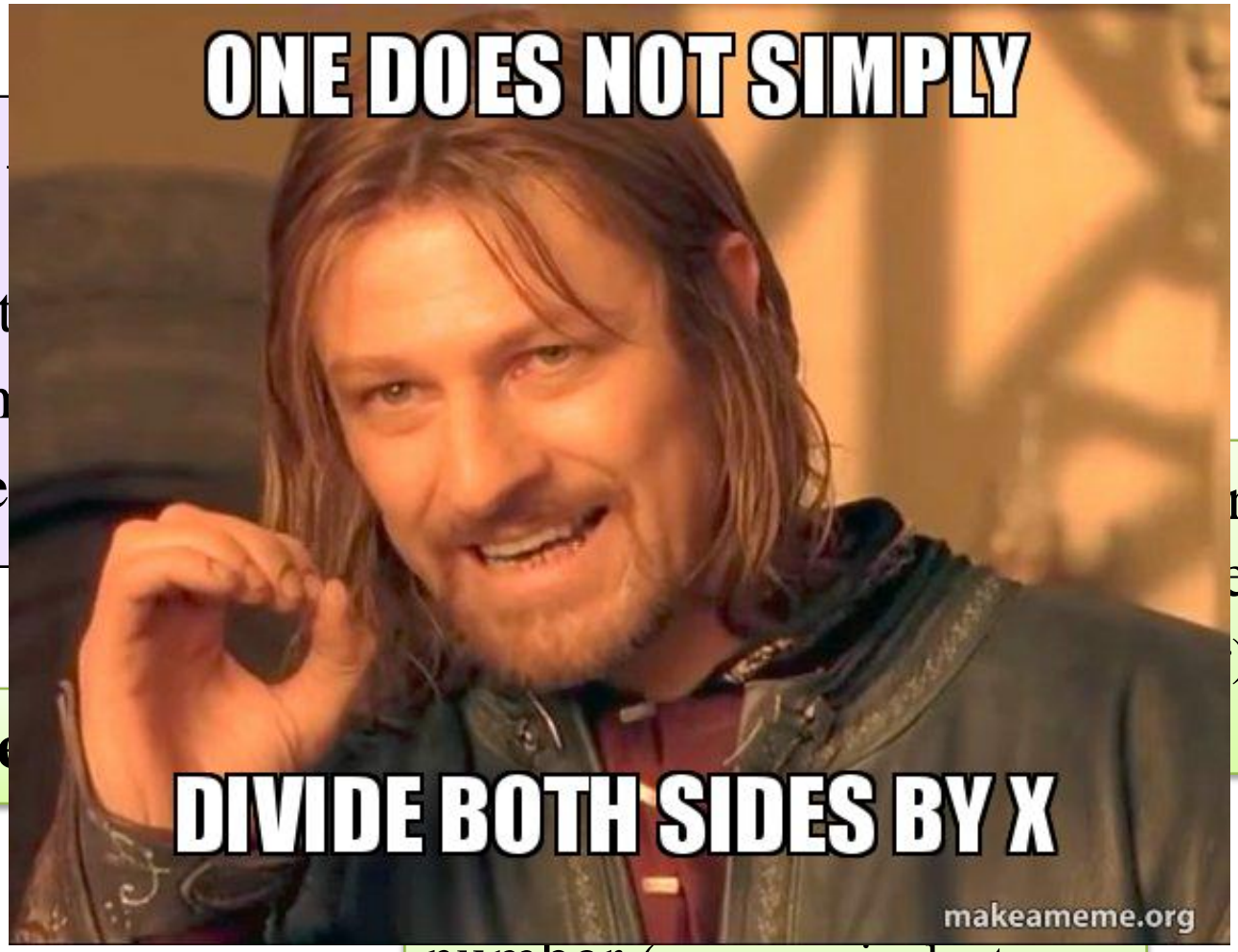
Divide some

r subtract)

er (or an

) to both

Works **some**



number (or an equivalent number) to both sides

Modular Inverses

- "Division by a" is really multiplying by a^{-1}.
  - But a^{-1} is **not** $\frac{1}{a}$, like in algebra.
  - a^{-1} is an integer in $\{0,1,\ldots,m-1\}$, such that $(a^{-1})(a) \equiv 1 \ (mod\ m)$

Beware: a^{-1} may or may not exist!

- **If it doesn't exist**, $ax + b \equiv c \ (mod\ m)$ won't have a **unique** solution
  - Either no solutions or multiple solutions with x in $\{0,\ldots,m-1\}$.
- **If it does exist**: a^{-1} is unique we will have a unique solution.

Theorem (but we won't prove it):

a has an inverse (mod m) if and only if a, m are **relatively prime**.

(meaning they have no common factor > 1)

Modular Inverses

Beware: a^{-1} may or may not exist!

- **If it doesn't exist**, $ax + b \equiv c \ (mod\ m)$ won't have a **unique** solution
  - Either no solutions or multiple solutions.
- **If it does exist**: a^{-1} is unique we will have a unique solution.

Theorem:

a has an inverse (mod m) if and only if a, m are relatively prime

(meaning they have no common factors > 1)

Examples: Finding a^{-1} "By Observation"

a^{-1} is the value that makes $a \cdot a^{-1} \equiv 1 \pmod{m}$

- For example: $7^{-1} \equiv 4 \pmod{9}$
  because $7 \cdot 7^{-1} \equiv 7 \cdot 4 \equiv 28 \equiv \mathbf{1} \pmod{9}$

- Find the following inverses, if they exist:

$1^{-1} \equiv \_\_\_\_\_ \pmod{5}$
$2^{-1} \equiv \_\_\_\_\_ \pmod{5}$
$3^{-1} \equiv \_\_\_\_\_ \pmod{5}$
$4^{-1} \equiv \_\_\_\_\_ \pmod{5}$
$5^{-1} \equiv \_\_\_\_\_ \pmod{5}$

$1^{-1} \equiv \_\_\_\_\_ \pmod{6}$
$2^{-1} \equiv \_\_\_\_\_ \pmod{6}$
$3^{-1} \equiv \_\_\_\_\_ \pmod{6}$
$4^{-1} \equiv \_\_\_\_\_ \pmod{6}$
$5^{-1} \equiv \_\_\_\_\_ \pmod{6}$

Finding a^{-1} "By Observation"

Handout

1. Find the following inverses, if they exist:

$1^{-1} \equiv \_\_\_\_\_ \pmod 5$

$2^{-1} \equiv \_\_\_\_\_ \pmod 5$

$3^{-1} \equiv \_\_\_\_\_ \pmod 5$

$4^{-1} \equiv \_\_\_\_\_ \pmod 5$

$5^{-1} \equiv \_\_\_\_\_ \pmod 5$

$1^{-1} \equiv \_\_\_\_\_ \pmod 6$

$2^{-1} \equiv \_\_\_\_\_ \pmod 6$

$3^{-1} \equiv \_\_\_\_\_ \pmod 6$

$4^{-1} \equiv \_\_\_\_\_ \pmod 6$

$5^{-1} \equiv \_\_\_\_\_ \pmod 6$

Finding a^{-1} "By Observation"

Handout

1. Find the following inverses, if they exist:

$1^{-1} \equiv \_\_1\_\_ \pmod 5$ $\quad$ $1^{-1} \equiv \_\_\_\_\_ \pmod 6$

$2^{-1} \equiv \_\_3\_\_ \pmod 5$ $\quad$ $2^{-1} \equiv \_\_\_\_\_ \pmod 6$

$3^{-1} \equiv \_\_2\_\_ \pmod 5$ $\quad$ $3^{-1} \equiv \_\_\_\_\_ \pmod 6$

$4^{-1} \equiv \_\_4\_\_ \pmod 5$ $\quad$ $4^{-1} \equiv \_\_\_\_\_ \pmod 6$

$5^{-1} \equiv \_\_DNE\_\_ \pmod 5$ $\quad$ $5^{-1} \equiv \_\_\_\_\_ \pmod 6$

Try $aj \equiv 1 \pmod 5$, for $j = 1, \ldots, 4$.

$\boldsymbol{a = 1}$: $1 \cdot 1 \equiv 1 \pmod 5$ $\rightarrow$ $1^{-1} \equiv 1 \pmod 5$

$\boldsymbol{a = 2}$: $2 \cdot 3 \equiv 6 \equiv 1 \pmod 5$ $\rightarrow$ $2^{-1} \equiv 3 \pmod 5$

$\boldsymbol{a = 3}$: $3 \cdot 2 \equiv 6 \equiv 1 \pmod 5$ $\rightarrow$ $3^{-1} \equiv 2 \pmod 5$

$\boldsymbol{a = 4}$: $4 \cdot 4 \equiv 16 \equiv 1 \pmod 5$ $\rightarrow$ $4^{-1} \equiv 4 \pmod 5$

$\boldsymbol{a = 5}$: $5 \cdot j \equiv 1 \pmod 5$; But $5j \equiv 0 \pmod 5$ always, so 5^{-1} DNE

Finding a^{-1} "By Observation"

Handout

1. Find the following inverses, if they exist:

$1^{-1} \equiv \_\_1\_\_ \pmod 5$	$1^{-1} \equiv \_\_1\_\_ \pmod 6$
$2^{-1} \equiv \_\_3\_\_ \pmod 5$	$2^{-1} \equiv \_\_DNE\_\_ \pmod 6$
$3^{-1} \equiv \_\_2\_\_ \pmod 5$	$3^{-1} \equiv \_\_DNE\_\_ \pmod 6$
$4^{-1} \equiv \_\_4\_\_ \pmod 5$	$4^{-1} \equiv \_\_DNE\_\_ \pmod 6$
$5^{-1} \equiv \_\_DNE\_\_ \pmod 5$	$5^{-1} \equiv \_\_5\_\_ \pmod 6$

Try $aj \equiv 1 \pmod 6$, for $j = 1, \ldots, 5$.

$\boldsymbol{a = 1}$: $1 \cdot 1 \equiv 1 \pmod 6$ $\rightarrow$ $1^{-1} \equiv 1 \pmod 6$

$\boldsymbol{a = 2}$: $2 \cdot j \equiv 1 \pmod 6$; But $2j \bmod 6$ is in $\{0,2,4\}$, so 2^{-1} DNE

$\boldsymbol{a = 3}$: $3 \cdot j \equiv 1 \pmod 6$; But $3j \bmod 6$ is in $\{0,3\}$, so 3^{-1} DNE

$\boldsymbol{a = 4}$: $4 \cdot j \equiv 1 \pmod 6$; But $4j \bmod 6$ is in $\{0,2,4\}$, so 4^{-1} DNE

$\boldsymbol{a = 5}$: $5 \cdot 5 \equiv 25 \equiv 1 \pmod 6$ $\rightarrow$ $5^{-1} \equiv 5 \pmod 6$

$2j \bmod 6$ is **never** 1

"Is there a unique solution" Blitz

Handout

Determine whether there is a unique solution (mod m) for each of the following.

- **Don't find the solution**, just decide if there **is** a unique solution

a) $6x - 10 \equiv 2 \pmod{13}$

b) $11x + 3 \equiv 14 \pmod{16}$

c) $15x + 3 \equiv 14 \pmod{16}$

d) $15x + 3 \equiv 14 \pmod{18}$

Hint:
Does $\mathbf{a^{-1}}$ exist **(mod m)** for the given equivalence? If so, there is a unique solution.

"Is there a unique solution" Blitz

Handout

Determine whether there is a unique solution (mod m) for each of the following.

- **Don't find the solution**, just decide if there **is** a unique solution

a) $6x - 10 \equiv 2 \pmod{13}$

b) $11x + 3 \equiv 14 \pmod{16}$

c) $15x + 3 \equiv 14 \pmod{16}$

d) $15x + 3 \equiv 14 \pmod{18}$

Solution:

a) a = 6: factors are 1, 2, 3, 6
m = 13: factors are 1, 13
no common factors > 1, so unique solution

b) a = 11: factors are 1, 11
m = 16: factors are 1, 2, 4, 8, 16
no common factors > 1, so unique solution

c) a = 15: factors are 1, 3, 5, 15
m = 16: factors are 1, 2, 4, 8, 16
no common factors > 1, so unique solution

d) a = 15: factors are 1, 3, 5, 15
m = 18: factors are 1, 2, 3, 6, 9, 18
common factor of 3, so **no** unique solution

Summary: Algebra vs. Modular Arithmetic

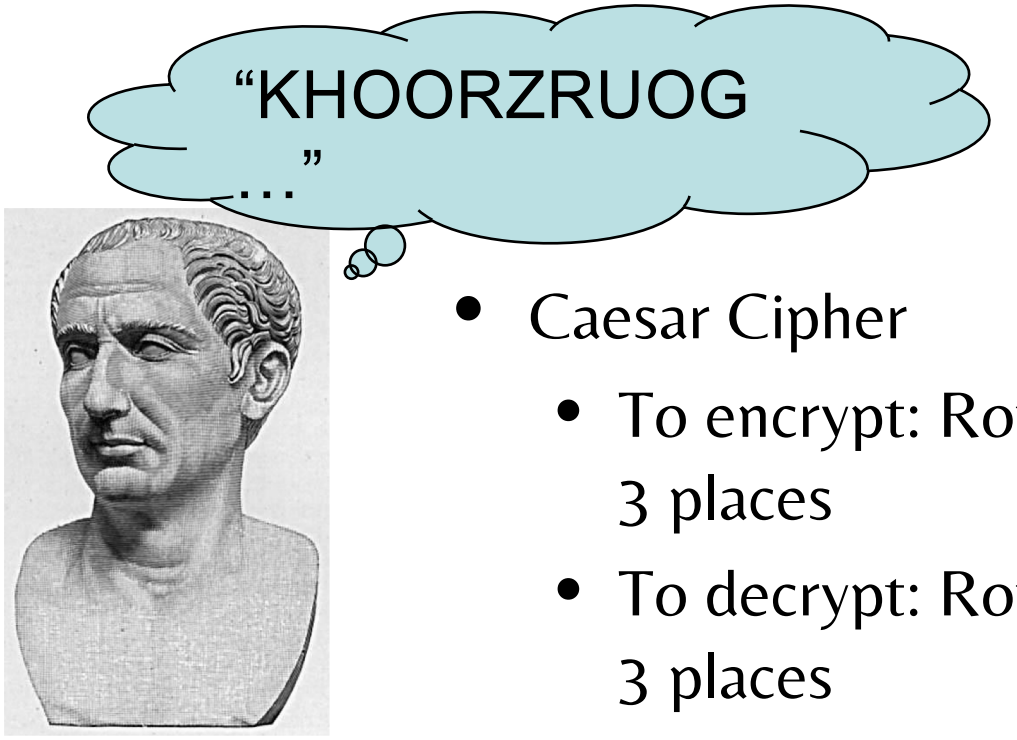
	Algebra	**Modular Arithmetic**
Domain	real numbers	_____
We care about	Equality ex: x = y	Equivalence with respect to a modulus m ex: $x \equiv y \pmod{m}$
How many unique numbers?	Infinitely many ex: -153.21, 76, $\sqrt{2}$	There are only _____ numbers in (mod m): _____
Multiplicative Inverse, a^{-1} Defn: $a^{-1}a \equiv 1$	For $a \neq 0$, $a^{-1} = 1/a$	Even for $a \neq 0$, $\mathbf{a^{-1}}$ may or may not exist

Summary: Algebra vs. Modular Arithmetic

	Algebra	Modular Arithmetic
Domain	real numbers	**integers**
We care about	Equality ex: x = y	**Equivalence** with respect to a modulus **m** ex: **x ≡ y (mod m)**
How many unique numbers?	Infinitely many ex: -153.21, 76, $\sqrt{2}$	There are *only* **m** numbers with all pairs non-equivalent in **(mod m)**: **{0, 1, 2, …., m-1}**
Multiplicative Inverse	For $a \neq 0$, $a^{-1} = 1/a$	Even for $a \neq 0$, $\mathbf{a^{-1}}$ **may or may not exist**

Wrapup

- Next lecture: leveraging the power of modular arithmetic for fancier proofs
- This is all useful in cryptography!



- Caesar Cipher
  - To encrypt: Rotate the alphabet to the right by 3 places
  - To decrypt: Rotate the alphabet to the left by 3 places

HELLOWORLD + 3 (mod 26) = KHOORZRUOG