Modular Arithmetic I

CS 70 Discussion 3A

Raymond Tsao

2025-02-12

Note: These slides are unofficial course materials. Please use the notes as the only single source of truth.

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1 \ (mod\ 10)$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1 \ (mod\ 10)$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1 \ (mod\ 10)$

$$11^1 \equiv 1 \quad (mod\ 10)$$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1 \; (mod\; 10)$
- $11^2 \equiv 121 \equiv 1 \; (mod\; 10)$
- $11^3 \equiv 1331 \equiv 1 \; (mod\; 10)$

$$11^1 \cdot 11 \equiv 1 \cdot 11 \; (mod\; 10)$$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1 \ (mod\ 10)$

$$11^1 \cdot 11 \equiv 1 \cdot 11 \ (mod\ 10)$$

$$\Downarrow$$

$$11^2 \equiv 11 \quad (mod\ 10)$$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1 \ (mod\ 10)$

$$11^2 \equiv 1 \quad (mod\ 10)$$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1 \ (mod\ 10)$

$$11^2 \cdot 11 \equiv 1 \cdot 11 \ (mod\ 10)$$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1 \ (mod\ 10)$

$$11^2 \cdot 11 \equiv 1 \cdot 11 \ (mod\ 10)$$

$$\Downarrow$$

$$11^3 \equiv 11 \quad (mod\ 10)$$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1 \ (mod\ 10)$

$$11^2 \cdot 11 \equiv 1 \cdot 11 \ (mod\ 10)$$

$$\Downarrow$$

$$11^3 \equiv 11 \quad (mod\ 10)$$

Trick: Take mod to the base

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1\ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1\ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1\ (mod\ 10)$

$$11^2 \cdot 11 \equiv 1 \cdot 11\ (mod\ 10)$$

$$\Downarrow$$

$$11^3 \equiv 11 \quad (mod\ 10)$$

Trick: Take mod to the base

$$11^{3142} \equiv (11\ mod\ 10)^{3142} \equiv 1^{3142} \equiv 1\ (mod\ 10)$$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1 \ (mod\ 10)$

$$11^2 \cdot 11 \equiv 1 \cdot 11 \ (mod\ 10)$$

$$\Downarrow$$

$$11^3 \equiv 11 \quad (mod\ 10)$$

Trick: Take mod to the base

$$11^{3142} \equiv (11\ mod\ 10)^{3142} \equiv 1^{3142} \equiv 1 \ (mod\ 10)$$

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1 \ (mod\ 10)$

$$11^2 \cdot 11 \equiv 1 \cdot 11 \ (mod\ 10)$$

$$\Downarrow$$

$$11^3 \equiv 11 \quad (mod\ 10)$$

Trick: Take mod to the base

$$11^{3142} \equiv (11\ mod\ 10)^{3142} \equiv 1^{3142} \equiv 1 \ (mod\ 10)$$

$$a^b \equiv (a\ mod\ m)^b \ (mod\ m)$$

This is something you CAN do!

Problem 1: Party Tricks

a) Last digit of 11^{3142}

Look for patterns

Need to reevaluate the whole thing!

- $11^1 \equiv 11 \equiv 1 \ (mod\ 10)$
- $11^2 \equiv 121 \equiv 1 \ (mod\ 10)$
- $11^3 \equiv 1331 \equiv 1 \ (mod\ 10)$

$$11^2 \cdot 11 \equiv 1 \cdot 11 \ (mod\ 10)$$

$$\Downarrow$$

$$11^3 \equiv 11 \quad (mod\ 10)$$

Trick: Take mod to the base

$$11^{3142} \equiv (11\ mod\ 10)^{3142} \equiv 1^{3142} \equiv 1 \ (mod\ 10)$$

$$a^b \equiv (a\ mod\ m)^b \ (mod\ m)$$

This is something you CAN do!

$$a^b \not\equiv a^{b\ (mod\ m)} \ (mod\ m)$$

You CANNOT do this to exponents!

Problem 1: Party Tricks

b) Last digit of 9^{9999}

Look for patterns

- $9^1 \equiv 9 \equiv 9 \ (mod\ 10)$
- $9^2 \equiv 9 \cdot 9 \equiv 1 \ (mod\ 10)$
- $9^3 \equiv 9 \cdot 1 \equiv 9 \ (mod\ 10)$

Enters a cycle of length 2

Apply mod to the base?

$$9^{9999} \equiv (9\ mod\ 10)^{9999} \equiv (-1)^{9999} \equiv -1 \equiv 9 \ (mod\ 10)$$

$-3 \quad -2 \quad \boxed{-1} \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad \boxed{9} \quad 10 \quad 11 \quad 12 \quad 13 \quad 14 \quad 15 \quad 16 \quad 17 \quad 18 \quad \boxed{19}$

Gap of 10

Gap of 10

Problem 1: Party Tricks

c) Last digit of 3^{641}

Look for patterns

- $3^1 \equiv 3 \equiv 3 \ (mod\ 10)$
- $3^2 \equiv 3 \cdot 3 \equiv 9 \ (mod\ 10)$
- $3^3 \equiv 3 \cdot 9 \equiv 7 \ (mod\ 10)$
- $3^4 \equiv 3 \cdot 7 \equiv 1 \ (mod\ 10)$
- $3^5 \equiv 3 \cdot 1 \equiv 3 \ (mod\ 10)$

Enters a cycle of length 4

So

$$3^{641} \equiv 3 \ (mod\ 10)$$

Problem 3: Modular Inverses

a) Is 3 an inverse of 5 modulo 14?

$$3 \cdot 5 \equiv 15 \equiv 1 \ \ (mod\ 14)$$

So yes

b) Is 3 an inverse of 5 modulo 10?

$$3 \cdot 5 \equiv 15 \equiv 5 \ \ (mod\ 10)$$

So no

c) Is $3 + 14n$ an inverse of 5 modulo 14?

$$\boxed{(3 + 14n)} \cdot 5 \equiv 15 + 14 \cdot 5n \equiv 15 \ \ (mod\ 14)$$

So yes

Equivalence class!

Problem 3: Modular Inverses

d) Does 4 has an inverse modulo 8?

Brute force:

- $4 \cdot 1 \equiv 4 \pmod 8$
- $4 \cdot 2 \equiv 0 \pmod 8$
- $4 \cdot 3 \equiv 4 \pmod 8$
- $4 \cdot 4 \equiv 0 \pmod 8$ .....

Cycle of length 2

Bad idea if we're dealing with modulo 10000!

Finding inverse (solving mod equation) is the same as solving linear diophantine equation

Solve for x		Find integer solution x, y
$4x \equiv 1 \pmod 8$	$\Longleftrightarrow$	$4x + 8y = 1$

Problem 3: Modular Inverses

Finding inverse (solving mod equation) is the same as solving diophantine equation

Solve for x		Find integer solution x, y
$4x \equiv 1 \ (mod\ 8)$	$\Leftrightarrow$	$4x + 8y = 1$

Why?

$$4x \equiv 1 \ (mod\ 8) \quad \Leftrightarrow \quad 8 \mid 4x - 1$$ Definition on mod

$$\Leftrightarrow \quad 4x - 1 = -8y$$ Definition of divisibility

$$\Leftrightarrow \quad \boxed{4x + 8y} = \boxed{1}$$

Divisible by 4   Not divisible by 4

Does not have any solutions!

Problem 3: Modular Inverses

Finding inverse (solving mod equation) is the same as solving diophantine equation

Solve for x		Find integer solution x, y
$\mathrm{a}x \equiv k \pmod{b}$	$\Leftrightarrow$	$\mathrm{a}x + by = k$

Problem 3: Modular Inverses

Finding inverse (solving mod equation) is the same as solving diophantine equation

Solve for x		Find integer solution x, y
$\mathrm{a}x \equiv k \ \ (mod\ b)$	$\Leftrightarrow$	$\mathrm{a}x + by = k$

Why is this helpful?

Problem 3: Modular Inverses

Finding inverse (solving mod equation) is the same as solving diophantine equation

Solve for x		Find integer solution x, y
$ax \equiv k \pmod{b}$	$\Longleftrightarrow$	$ax + by = k$

Why is this helpful?

A: We know when the solution and how to find them for linear diophantine equation!

Problem 3: Modular Inverses

Finding inverse (solving mod equation) is the same as solving diophantine equation

Solve for x		Find integer solution x, y
$\mathrm{a}x \equiv k \ \ (mod\ b)$	$\Longleftrightarrow$	$\mathrm{a}x + by = k$

$\mathrm{a}x + by = k$ has a solution

if and only if $\mathbf{gcd}(a, b)\ |k$

Problem 3: Modular Inverses

Finding inverse (solving mod equation) is the same as solving diophantine equation

Solve for x		Find integer solution x, y
$\mathrm{a}x \equiv k \ \ (mod\ b)$	$\Longleftrightarrow$	$\mathrm{a}x + by = k$

$\mathrm{a}x \equiv k\ (mod\ b)$ has a solution if and only if $\mathbf{gcd}(a, b)\ |k$ $\Longleftrightarrow$ $\mathrm{a}x + by = k$ has a solution if and only if $\mathbf{gcd}(a, b)\ |k$

Problem 3: Modular Inverses

Finding inverse (solving mod equation) is the same as solving diophantine equation

Solve for x

$$ax \equiv k \pmod b$$

$\Longleftrightarrow$

Find integer solution x, y

$$ax + by = k$$

$ax \equiv k \ (mod\ b)$ has a solution if and only if $\gcd(a, b) \mid k$

$\Longleftrightarrow$

$ax + by = k$ has a solution if and only if $\gcd(a, b) \mid k$

$ax \equiv \boxed{1}\ (mod\ b)$ has a solution if and only if $\gcd(a, b) \mid \boxed{1}$

Problem 3: Modular Inverses

Finding inverse (solving mod equation) is the same as solving diophantine equation

Solve for x		Find integer solution x, y
$ax \equiv k \pmod{b}$	$\Leftrightarrow$	$ax + by = k$

$ax \equiv k \pmod{b}$ has a solution if and only if $\gcd(a, b) \mid k$ $\Leftrightarrow$ $ax + by = k$ has a solution if and only if $\gcd(a, b) \mid k$

$ax \equiv \boxed{1} \pmod{b}$ has a solution if and only if $\gcd(a, b) \mid \boxed{1}$

Condition for whether an inverse exists!

Problem 3: Modular Inverses

Finding inverse (solving mod equation) is the same as solving diophantine equation

Solve for x		Find integer solution x, y
$ax \equiv k \pmod{b}$	$\Leftrightarrow$	$ax + by = k$

The only missing puzzle!

$ax \equiv k \ (mod\ b)$ has a solution
if and only if $\gcd(a, b) \mid k$

$\Leftrightarrow$

$ax + by = k$ has a solution
if and only if $\gcd(a, b) \mid k$

$ax \equiv 1 \ (mod\ b)$ has a solution
if and only if $\gcd(a, b) \mid 1$

Condition for whether an inverse exists!

Problem 3: Modular Inverses

e) Can $ax \equiv ax' \pmod{m}$

$$a(x - x') \equiv 0 \pmod{m}$$

$$x \cdot a(x - x') \equiv x \cdot 0 \pmod{m}$$

$$(x - x') \equiv 0 \pmod{m}$$

$$x \equiv x' \pmod{m}$$

This tells us that inverses are unique in mod space!

Problem 2: Modular Potpourri

a) There exists some x such that $x \equiv 3 \ (mod\ 16)$ and $x \equiv 4 \ (mod\ 6)$

Solving modular equation is the same as solving linear diophantine equation

$$x \equiv 3 \ \ (mod\ 16) \quad \Longrightarrow \quad x \equiv 3 + 16k_1$$

$$x \equiv 4 \ \ (mod\ 6) \quad \Longrightarrow \quad x \equiv 4 + 6k_2$$

$$3 + 16k_1 = 4 + 6k_2$$

$$\boxed{16k_1 - 6k_2} = \boxed{1}$$

Divisible by 2 Not divisible by 2

Problem 2: Modular Potpourri

b, c) $2x \equiv 4 \ \ (mod\ 12) \quad \Leftrightarrow \quad x \equiv 2 \ \ (mod\ 12)$

$$2x \equiv 4 \ \ (mod\ 12) \quad \Leftrightarrow \quad 2x = 4 + 12y$$

$$\Downarrow$$

$$x \equiv 2 \ \ (mod\ 6) \quad \Leftrightarrow \quad x = 2 + 6y$$

False, counter-example: $x = 8$