Modular Arithmetic II

CS 70 Discussion 3B

Raymond Tsao

2025-02-14

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

Problem 1: Extended Euclid: Two Ways

(a) Solving mod equation is equivalent as finding integer solution to linear equation

Solve for x		Find integer solution x, y
$17x \equiv 1 \pmod{54}$	$\Leftrightarrow$	$17x + 54y = 1$
Problem 1		**Problem 2**

If I can solve Problem 1 (i.e. I can find x^* satisfying $17x^* \equiv 1 \pmod{54}$)

$$54 \mid 17x^* - 1 \implies y^* = (17x^* - 1)/54$$

If I can solve Problem 2 (i.e. I can find x^*, y^* s.t. $17x^* + 54y^* = 1$)

$$17x^* + \underbrace{\boxed{54y^*}}_{0} \equiv 1 \pmod{54} \implies 17x^* \equiv 1 \pmod{54}$$

Problem 1: Extended Euclid: Two Ways

Solving mod equation is equivalent as finding integer solution to linear equation

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

$\Longrightarrow$: Suppose $ax + by = k$ has integer solution

$\gcd(a, b)$ divides a, b, so $\gcd(a, b)$ divides k

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

$\Longleftarrow$: Suppose $\gcd(a, b) \mid k$, how to find a solution?

Step 1: We can always solve $ax + by = \gcd(a, b)$ — Extended Euclid Algorithm

Step 2: $a(mx) + b(my) = \mathrm{m} \cdot \gcd(a, b)$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

$$\mathrm{a} = q \cdot b + r$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient

$$a = q \cdot b + r$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient, remainder

$$\mathrm{a} = q \cdot b + r$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$\mathrm{a} = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$\mathrm{a} = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient, remainder

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient   remainder

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$

Backward

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$ → 1

Backward

$$3 = 54 - 3 \cdot 17$$

$$2 = 17 - 5 \cdot 3$$

$$1 = 3 - 1 \cdot 2$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$

Backward

$$3 = 54 - 3 \cdot 17$$

$$2 = 17 - 5 \cdot 3$$

$$1 = 3 - 1 \cdot 2$$

$$1 = 3 - 1 \cdot 2$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$

Backward

$$3 = 54 - 3 \cdot 17$$

$$2 = 17 - 5 \cdot 3$$

$$1 = 3 - 1 \cdot 2$$

$$1 = 3 - 1 \cdot 2$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$

Backward

$$3 = 54 - 3 \cdot 17$$

$$2 = 17 - 5 \cdot 3$$

$$1 = 3 - 1 \cdot 2$$

$$1 = 3 - 1 \cdot (17 - 5 \cdot 3)$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$\mathrm{a} = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$

Backward

$$3 = 54 - 3 \cdot 17$$

$$2 = 17 - 5 \cdot 3$$

$$1 = 3 - 1 \cdot 2$$

$$1 = 3 - 1 \cdot (17 - 5 \cdot 3)$$

$$= -1 \cdot 17 + 6 \cdot 3$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$

Backward

$$3 = 54 - 3 \cdot 17$$

$$2 = 17 - 5 \cdot 3$$

$$1 = 3 - 1 \cdot 2$$

$$1 = -1 \cdot 17 + 6 \cdot 3$$

$$1 = 3 - 1 \cdot (17 - 5 \cdot 3)$$

$$= -1 \cdot 17 + 6 \cdot 3$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$

Backward

$$3 = 54 - 3 \cdot 17$$

$$2 = 17 - 5 \cdot 3$$

$$1 = 3 - 1 \cdot 2$$

$$1 = -1 \cdot 17 + 6 \cdot 3$$

$$1 = 3 - 1 \cdot (17 - 5 \cdot 3)$$

$$= -1 \cdot 17 + 6 \cdot 3$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$

Backward

$$3 = 54 - 3 \cdot 17$$

$$2 = 17 - 5 \cdot 3$$

$$1 = 3 - 1 \cdot 2$$

$$1 = -1 \cdot 17 + 6 \cdot (54 - 3 \cdot 17)$$

$$1 = 3 - 1 \cdot (17 - 5 \cdot 3)$$

$$= -1 \cdot 17 + 6 \cdot 3$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient → q, remainder → r

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$

Backward

$$3 = 54 - 3 \cdot 17$$

$$2 = 17 - 5 \cdot 3$$

$$1 = 3 - 1 \cdot 2$$

$$1 = -1 \cdot 17 + 6 \cdot (54 - 3 \cdot 17)$$

$$= -19 \cdot 17 + 6 \cdot 54$$

$$1 = 3 - 1 \cdot (17 - 5 \cdot 3)$$

$$= -1 \cdot 17 + 6 \cdot 3$$

Problem 1: Extended Euclid: Two Ways

(b, c) Method 1: Recursive Approach

quotient, remainder

$$a = q \cdot b + r$$

$$\gcd(a, b) = \gcd(b, r)$$

Forward: Find $\gcd(54, 17)$

$$54 = 3 \cdot 17 + 3$$

$$17 = 5 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$\gcd(54, 17)$

Backward

$$3 = 54 - 3 \cdot 17$$

$$2 = 17 - 5 \cdot 3$$

$$1 = 3 - 1 \cdot 2$$

$$1 = -1 \cdot 17 + 6 \cdot (54 - 3 \cdot 17)$$

$$= -19 \cdot 17 + 6 \cdot 54$$

$$1 = 3 - 1 \cdot (17 - 5 \cdot 3)$$

$$= -1 \cdot 17 + 6 \cdot 3$$

This method allows us to solve $ax + by = \gcd(a, b)$

Problem 1: Extended Euclid: Two Ways

(d) Method 2: Iterative Approach

$$54 = 1 \cdot 54 + 0 \cdot 17 \qquad (E_1)$$

$$17 = 0 \cdot 54 + 1 \cdot 17 \qquad (E_2)$$

$$3 = 1 \cdot 54 + -3 \cdot 17 \qquad (E_3) = (E_1) - 3(E_2)$$

$$2 = -5 \cdot 54 + 16 \cdot 17 \qquad (E_4) = (E_2) - 5(E_3)$$

$$1 = 6 \cdot 54 + -19 \cdot 17 \qquad (E_5) = (E_3) - (E_4)$$

Problem 1: Extended Euclid: Two Ways

Solving mod equation is equivalent as finding integer solution to linear equation

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

$$54x \equiv 2 \pmod{32} \quad \Leftrightarrow \quad 54x + 32y = 2$$

- Check: $\gcd(54, 32) \mid 2$, so there exists a solution
- Use Extended Euclid to find the solution
- $54(3) + 32(-5) = 2$
- $54(3) \equiv 2 \pmod{32}$

$$54 = 1 \cdot 54 + 0 \cdot 32 \qquad E_1$$
$$32 = 0 \cdot 54 + 1 \cdot 32 \qquad E_2$$
$$22 = 1 \cdot 54 - 1 \cdot 32 \qquad E_3 = E_1 - E_2$$
$$10 = -1 \cdot 54 + 2 \cdot 32 \qquad E_4 = E_2 - E_3$$
$$2 = 3 \cdot 54 - 5 \cdot 32 \qquad E_5 = E_3 - 2E_4$$

Problem 2: Chinese Remainder Theorem Practice

a)

$$x \equiv 1 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 7)$$
$$x \equiv 4 \ (mod\ 11)$$

$$x \equiv \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \begin{matrix} (mod\ 3) \\ (mod\ 7) \\ (mod\ 11) \end{matrix}$$

Suppose we have three "basis" solution

$$\underbrace{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \begin{matrix} (mod\ 3) \\ (mod\ 7) \\ (mod\ 11) \end{matrix}}_{a} \qquad \underbrace{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \begin{matrix} (mod\ 3) \\ (mod\ 7) \\ (mod\ 11) \end{matrix}}_{b} \qquad \underbrace{\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \begin{matrix} (mod\ 3) \\ (mod\ 7) \\ (mod\ 11) \end{matrix}}_{c}$$

Problem 2: Chinese Remainder Theorem Practice

a)

$$x \equiv 1 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 7)$$
$$x \equiv 4 \ (mod\ 11)$$

$$x \equiv \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \begin{matrix} (mod\ 3) \\ (mod\ 7) \\ (mod\ 11) \end{matrix}$$

Problem 2: Chinese Remainder Theorem Practice

a)

$$x \equiv 1 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 7)$$
$$x \equiv 4 \ (mod\ 11)$$

$$x \equiv \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \begin{matrix} (mod\ 3) \\ (mod\ 7) \\ (mod\ 11) \end{matrix}$$

$$\boxed{?} \underbrace{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}}_{a} + \boxed{?} \underbrace{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}}_{b} + \boxed{?} \underbrace{\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}}_{c} = \underbrace{\begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix}}_{x}$$

Problem 2: Chinese Remainder Theorem Practice

a)

$$x \equiv 1 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 7)$$
$$x \equiv 4 \ (mod\ 11)$$

$$x \equiv \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \begin{matrix} (mod\ 3) \\ (mod\ 7) \\ (mod\ 11) \end{matrix}$$

$$\boxed{1} \underbrace{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}}_{a} + \boxed{?} \underbrace{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}}_{b} + \boxed{?} \underbrace{\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}}_{c} = \underbrace{\begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix}}_{x}$$

Problem 2: Chinese Remainder Theorem Practice

a)

$$x \equiv 1\ (mod\ 3)$$
$$x \equiv 3\ (mod\ 7)$$
$$x \equiv 4\ (mod\ 11)$$

$$x \equiv \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \begin{matrix} (mod\ 3) \\ (mod\ 7) \\ (mod\ 11) \end{matrix}$$

$$\boxed{1} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \boxed{3} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + \boxed{?} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix}$$

$$a \qquad\qquad b \qquad\qquad c \qquad\qquad x$$

Problem 2: Chinese Remainder Theorem Practice

a)

$$x \equiv 1 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 7)$$
$$x \equiv 4 \ (mod\ 11)$$

$$x \equiv \begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix} \begin{matrix} (mod\ 3) \\ (mod\ 7) \\ (mod\ 11) \end{matrix}$$

$$\boxed{1} \underset{a}{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}} + \boxed{3} \underset{b}{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}} + \boxed{4} \underset{c}{\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}} = \underset{x}{\begin{bmatrix} 1 \\ 3 \\ 4 \end{bmatrix}}$$

Problem 2: Chinese Remainder Theorem Practice

b) Solve

$$a \equiv 1 \ (mod\ 3) \qquad (1)$$

$$a \equiv 0 \ (mod\ 7) \qquad (2)$$

$$a \equiv 0 \ (mod\ 11) \qquad (3)$$

Step 1: From (2) and (3)

$$a = 7 \cdot 11 \cdot k$$

Step 2: Plug in (1)

$$7 \cdot 11 \cdot k \equiv 1 \ (mod\ 3) \quad \Longrightarrow \quad 2k \equiv 1 \ (mod\ 3)$$

Step 3: Solve!

$$k \equiv 2 \ (mod\ 3) \quad \Longrightarrow \quad k \equiv 3m + 2$$

Step 4:

$$a = 7 \cdot 11 \cdot (3m + 2) = 3 \cdot 7 \cdot 11m + 154$$

Problem 2: Chinese Remainder Theorem Practice

c) Solve

$$b \equiv 0 \ (mod\ 3) \qquad (1)$$

$$b \equiv 1 \ (mod\ 7) \qquad (2)$$

$$b \equiv 0 \ (mod\ 11) \qquad (3)$$

Step 1: From (1) and (3)

$$b = 3 \cdot 11 \cdot k$$

Step 2: Plug in (2)

$$3 \cdot 11 \cdot k \equiv 1 \ (mod\ 7) \quad \Longrightarrow \quad 5k \equiv 1 \ (mod\ 7)$$

Step 3: Solve!

$$k \equiv 3 \ (mod\ 7) \quad \Longrightarrow \quad k \equiv 7m + 3$$

Step 4:

$$b = 3 \cdot 11 \cdot (7m + 3) = 3 \cdot 7 \cdot 11m + 99$$

Problem 2: Chinese Remainder Theorem Practice

e) Now we have

$$a = 3 \cdot 7 \cdot 11m + 154 \equiv 154 \pmod{3 \cdot 7 \cdot 11}$$

$$b = 3 \cdot 7 \cdot 11m + 99 \equiv 99 \pmod{3 \cdot 7 \cdot 11}$$

$$c = 3 \cdot 7 \cdot 11m + 210 \equiv 210 \pmod{3 \cdot 7 \cdot 11}$$

$$x = a + 3b + 4c = (154) + 3(99) + 4(210) \equiv 1291 \pmod{3 \cdot 7 \cdot 11}$$

Problem 2: Chinese Remainder Theorem Practice

In general

$$x \equiv a_1 \ (mod \ n_1) \quad (1)$$

$$x \equiv a_2 \ (mod \ n_2) \quad (2)$$

$$x \equiv a_3 \ (mod \ n_3) \quad (3)$$

$$\boxed{a_1} \underbrace{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}}_{b_1} + \boxed{a_2} \underbrace{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}}_{b_2} + \boxed{a_3} \underbrace{\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}}_{b_3} = \underbrace{\begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}}_{x}$$

$$x = a_1 b_1 + a_2 b_3 + a_3 b_3 = \sum_{i=1}^{3} a_i b_i$$

Problem 2: Chinese Remainder Theorem Practice

Solve

$$a \equiv 1 \ (mod\ 3) \quad (1)$$
$$a \equiv 0 \ (mod\ 7) \quad (2)$$
$$a \equiv 0 \ (mod\ 11) \quad (3)$$

Step 1: From (2) and (3)

$$a = 7 \cdot 11 \cdot k$$

Step 2: Plug in (1)

$$(N/n_1)\ k \equiv 1 \ (mod\ n_1)$$

$$7 \cdot 11 \cdot k \equiv 1 \ (mod\ 3)$$

Step 3: Solve!

$$k \equiv 2 \ (mod\ 3) \quad \Longrightarrow \quad k \equiv 3m + 2$$

Step 4:

$$a = 7 \cdot 11 \cdot (3m + 2) = \underbrace{3 \cdot 7 \cdot 11}_{N} m + \underbrace{7 \cdot 11}_{N/n_1} \cdot 2$$

$$k = \left(\frac{N}{n_1}\right)^{-1} \ (mod\ n_1)$$