CSCI 220 | Spring 2022

Discrete Structure

Solving Linear Congruences

Discrete Mathematics and its Application

Section 4.4, 4.5

Solving Linear Congruences

- Find x such that
  - $3x \equiv 2 \ (mod\ 5)$

$3(4) \equiv 12 \equiv 2 \pmod 5$ $\quad x \equiv 4 \pmod 5$

  - $3x \equiv 2 \ (mod\ 6)$

No solution.

  - $4x \equiv 2 \ (mod\ 6)$

$4(2) \equiv 8 \equiv 2 \pmod 6$ $\quad x \equiv 2, 5 \pmod 6$.

$4(5) \equiv 20 \equiv 2 \pmod 6$

Solving Linear Congruences

- Find x such that $56x \equiv 2\ (mod\ 79)$.

$$\frac{1}{56} \cdot 56x = 2 \cdot \frac{1}{56}$$

Inverse

- If $x \cdot x^{-1} \equiv 1 \pmod{m}$, then x^{-1} is the multiplicative inverse of $x \pmod{m}$.

Inverse

- If $x \cdot x^{-1} \equiv 1 \pmod{m}$, then x^{-1} is the multiplicative inverse of $x \pmod{m}$.
- Exercises: Find the inverses of the follow modulus.
  - $2 \pmod{5}$

$2(3) \equiv 6 \equiv 1 \pmod{5}$ $\quad 2^{-1} \equiv 3 \pmod{5}$

$\gcd(2,5) = 1$

  - $3 \pmod{6}$

DNE

$\gcd(3,6) = 3$

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

$\underbrace{3 \cdot 3^{-1} + 6k}_{\text{multiple of } 3} = \underbrace{1}_{\text{is NOT.}}$

  - $4 \pmod{6}$

DNE

$\gcd(4,6) = 2$

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

$\underbrace{4 \cdot 4^{-1} + 6k}_{\text{even}} = \underbrace{1}_{\text{odd}}$.

  - $5 \pmod{6}$

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

$\gcd(5,6) = 1$

$5(5) = 25 \equiv 1 \pmod{6}$

Inverse

- If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m.
  (That is, there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.)

$a^{-1} \pmod{m}$ exists only when $\gcd(a, m) = 1$.

Inverse

- Which of following modulus has inverse?
  - [A] $3 \pmod{12}$, No
  - [B] $4 \pmod{12}$, No
  - [C] $5 \pmod{12}$, Yes
  - [D] $6 \pmod{12}$, No
  - [E] $7 \pmod{12}$. Yes

Inverse

- Find inverse of $13\ (mod\ 27)$.

$$\boxed{13^{-1} \equiv 25 \pmod{27}}$$

$$13 \cdot 13^{-1} \equiv 1 \pmod{27}$$

W

$$\gcd(13, 27) = 1$$

$$13w \equiv 1 \pmod{27}$$

$$\downarrow$$

$$27 = 13(2) + 1$$

$$13w + 27k = 1$$

$$1 = 27(1) + 13(-2) \rightarrow 13(-2) + 27(1) = 1$$

w

$$13^{-1} \equiv -2 \equiv 25 \pmod{27}$$

Solving Linear Congruences

- Find x such that $13x \equiv 11\ (mod\ 27)$.

$13^{-1} \equiv 25 \pmod{27}$

$13x \equiv 11 \pmod{27}$

$13^{-1} * \qquad 13^{-1} *$

$x \equiv 11 * 13^{-1}$

$\equiv 11 * 25$

$\equiv 11 * (-2)$

$\equiv -22$

$\boxed{x \equiv 5 \pmod{27}}$

Solving Linear Congruences

- Find x such that $56x \equiv 2\ (mod\ 79)$.

$\boxed{x \equiv 48 \pmod{79}}$

① Find $56^{-1} \pmod{79}$

$56w + 79k = 1$

$79 = 56(1) + 23$

$56 = 23(2) + 10$

$23 = 10(2) + 3$

$10 = 3(3) + 1$

$\gcd(56, 79) = 1$

$1 = 10(1) + 3(-3)$

$= 10(1) + [23(1) + 10(-2)](-3)$

$= 10(7) + 23(-3)$

$= [56(1) + 23(-2)](7) + 23(-3)$

$= 23(-17) + 56(7)$

$= [79(1) + 56(-1)](-17) + 56(7)$

$1 = 56(24) + 79(-17)$

w ↑ , k ↑

$56^{-1} \equiv 24 \pmod{79}$

$56x \equiv 2 \pmod{79}$

$56^{-1} *$ ... $56^{-1} *$

$x \equiv 2 * 56^{-1} \equiv 2 * 24 \equiv 48 \pmod{79}$

Solving Linear Congruences

- Find x such that $9x \equiv 6 \ (mod\ 15)$.

$3x \equiv 2 \pmod 5$

$\boxed{x \equiv 4 \pmod 5}$

$\equiv 9 \equiv 14 \equiv 19$

① find $9^{-1} \pmod{15}$

$15 = 9(1) + 6$

$9 = 6(1) + 3$

gcd

$6 = 3(2) + 0$

$\gcd(9, 15) = 3$

$9^{-1} \pmod{15}$ DNE.

$9x + 15k = 6$

$9s + 15t = 3$

x2

$3 = 9(1) + 6(-1) = 9(1) + [15(1) + 9(-1)](-1)$

$3 = 9(2) + 15(-1)$

$\downarrow \times 2 \quad \downarrow \times 2 \quad \downarrow \times 2$

$6 = 9(4) + 15(-2)$

$$\boxed{\begin{aligned} x &\equiv 4 \pmod{15} \\ x &\equiv 9 \pmod{15} \\ x &\equiv 14 \pmod{15} \end{aligned}}$$

$x \equiv \text{LNR} \left(\bmod \dfrac{m}{\gcd(a,m)} \right)$

Solving Linear Congruences

- Find x such that $14x \equiv 10 \ (mod\ 35)$.

① $\gcd(14, 35) = 7$

$35 = 14(2) + 7$

$14 = 7(2) + 0$

$14s + 35t = 7$

$14x + 35k = 10$

No integer scaling.

$7 \nmid 10$

No solution!

Summary of Solving Linear Congruences

- Every congruence can be written as a linear combination.

1
- $ax \equiv b \ (mod\ m) \Leftrightarrow ax + mk = b$
- Given $ax \equiv b \ (mod\ m)$, x has solution if and only if $\gcd(a, m) | b$.

2 Use Euclidean Alg. to solve gcd (a, m)

C1: $\gcd(a, m) = 1$

(inverse exists)

3 Use Extended Euclidean Alg. to solve $as + mt = 1$.

$a^{-1} \equiv s \ (mod\ m)$

4 Solve for x by multiply a^{-1} on both sides.

$ax \equiv b \ (mod\ m)$

$*a^{-1} \quad a^{-1}*$

$x \equiv b * a^{-1} \equiv b * s \equiv LNR \ (mod\ m)$

C2: $\gcd(a, m) = d \neq 1$

3 Check $\gcd(a,m) = d \ | \ b$?

→ No → No solution! stop

→ Yes → keep going.

4 Use Extended Euclidean Alg. to solve $as + mt = d$. ($= \gcd(a,m)$)

5 Scale the linear combination from 4 to $ax + mk = b$. ($d | b$)

put the answer in LNR form.

$x \equiv LNR \ (mod\ \frac{m}{d})$ ($d = \gcd(a,m)$)

Solving Linear Congruences

- Find x such that $34x \equiv 6 \ (mod\ 58)$. $\rightarrow$ ① $34x + 58k = 6$

② $\gcd(34, 58) = 2$

$$58 = 34(1) + 24$$
$$34 = 24(1) + 10$$
$$24 = 10(2) + 4$$
$$10 = 4(2) + 2$$
$$4 = 2(2) + 0$$

③ $2 \mid 6$

$$\boxed{\begin{array}{l} x \equiv 7 \pmod{58} \\ x \equiv 36 \pmod{58} \end{array}}$$

④ $34s + 58t = 2$

$$2 = 10(1) + 4(-2) = 10(1) + [24(1) + 10(-2)](-2)$$
$$= 10(5) + 24(-2) = [34(1) + 24(-1)](5) + 24(-2)$$
$$= 24(-7) + 34(5) = [58(1) + 34(-1)](-7) + 34(5)$$

$$2 = 34(12) + 58(-7)$$

$\downarrow \times 3$ $\quad \downarrow \times 3$ $\quad \downarrow \times 3$

$$6 = 34(36) + 58(-21)$$

x

$$x \equiv 36 \pmod{\tfrac{58}{2}} \rightarrow x \equiv 36 \pmod{29}$$

$$\boxed{x \equiv 7 \pmod{29}}$$

Exercise

- Can you find an integer x that when divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2?

$$\left.\begin{array}{l} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \equiv 23 \\ x \equiv 2 \pmod{7} \end{array}\right\} \quad \begin{array}{l} x \equiv 2 \pmod{21} \\ x \equiv 23 \pmod{21} \end{array}$$

$$x \equiv 23 \pmod{105}$$

Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_n \pmod{m_n}. \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

Chinese Remainder Theorem

- Can you find an integer x that when divided by 5, the remainder is 3; when divided by 8, the remainder is 5; and when divided by 9, the remainder is 7?

$x \equiv 3 \pmod{5} \equiv 13$

$x \equiv 5 \pmod{8} \equiv 13$

$x \equiv 7 \pmod{9} \equiv 133$

$>$

$x \equiv 13 \pmod{40}$

$\equiv 53$

$\equiv 93$

$\equiv 133$

$$\boxed{x \equiv 133 \pmod{360}}$$

Chinese Remainder Theorem

- Find x such that when x divided by 3, the remainder is 2; when x divided by 4, the remainder is 3; and when x divided by 5, the remainder is 4.

$$x \equiv 2 \pmod{3} \equiv -1$$

$$x \equiv 3 \pmod{4} \equiv -1$$

$$x \equiv 4 \pmod{5} \equiv -1$$

$$x \equiv -1 \pmod{60} \equiv \boxed{59 \pmod{60}}$$

Exercises

- Reduce the following Modulus
  - $3^4 \pmod 5$ $\equiv 81 \equiv 1 \pmod 5$
  - $3^5 \pmod 6$ $\equiv 3\cdot3\cdot3\cdot3\cdot3 \equiv 9\cdot9\cdot3 \equiv 3\cdot3\cdot3 \equiv 9\cdot3 \equiv 3\cdot3 \equiv 9 \equiv 3 \pmod 6$
  - $3^6 \pmod 7$ $\equiv (3^2)^3 \equiv 9^3 \equiv 2^3 \equiv 8 \equiv 1 \pmod 7$
  - $3^7 \pmod 8 \equiv (3^2)^3\cdot 3 \equiv 9^3\cdot 3 \equiv 1^3\cdot 3 \equiv 3 \pmod 8$
  - $3^8 \pmod 9$ $\equiv 3^2\cdot 3^6 \equiv 9\cdot 3^6 \equiv 0\cdot 3^6 \equiv 0 \pmod 9$
  - $3^{10} \pmod{11}$ $\equiv (3^2)^5 \equiv (9)^5 \equiv (-2)^5 \equiv -32 \equiv 1 \pmod{11}$
  - $3^{12} \pmod{13}$ $\equiv (3^3)^4 \equiv (27)^4 \equiv 1^4 \equiv 1 \pmod{13}$

Fermat's Little Theorem

If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

$\gcd(a, p) = 1$

$a \not\equiv 0 \pmod{p}$

$a^{p-1} \equiv 1 \pmod{p}$

prime

Fermat’s Little Theorem

If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$.

Exercises on Fermat's Little Theorem

- Reduce the following Modulus
  - $7^{222} \pmod{11}$

    prime

    FLT: $7^{10} \equiv 1 \pmod{11}$

    $7^{222} \equiv (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 7^2 \equiv 49 \equiv \boxed{5 \pmod{11}}$

  - $2^{123} \pmod{31}$

    prime

    FLT: $2^{30} \equiv 1 \pmod{31}$

    $2^{123} \equiv (2^{30})^4 \cdot 2^3 \equiv 1^4 \cdot 2^3 \equiv \boxed{8 \pmod{31}}$

  - $36^{400} \pmod{37}$

    prime

    FLT: $36^{36} \equiv 1 \pmod{37}$

    $36^{400} \equiv (-1)^{400} \equiv 1 \pmod{37}$