Lecture 40

06 December 2021 14:39

Lemma 2:

If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Lemma 3:

If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

Linear Congruences

A congruence of the form $ax \equiv b \bmod m$

$x = ?$

$+_m$

a^{-1}

$x \equiv ? \pmod{m}$

$m \mid (ax - b)$

$a \cdot_m 1 = a$

$a \cdot_m a^{-1} = 1$

$m \mid a a^{-1} - 1$

Theorem 11:

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 $\overline{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\overline{a}$ modulo m.)

Q19. Find inverse by inspection method

(i) 4 modulo 9. $\longrightarrow$ R. Prime

$9 \mid 4a^{-1} - 1$

$a^{-1} \{0, 1, 2, 3, \ldots 8\}$

$a^{-1} = 7$

$a = 7$

Inverse of 4 modulo 9 = 7

(ii) 2 modulo 17

$17 \mid (2\bar{a}^{1}-1)$, $\bar{a}^{1} = 9$

Q20. Find inverse by using Bezout coefficients

(i) 4 modulo 9

$9 = 4(2)+1$, $1 = 9-4(2)$

$4 = 1(4)+0$

$1 = 9(1)+4(-2)$

Inverse of 4 modulo 9 = -2, $-2+9=7$

(ii) 7 modulo 26

$26 = 7(3)+5$

$7 = 5(1)+2$

$5 = 2(2)+1$

$2 = 1(2)+0$

$1 = 5-2(2)$

$1 = 5-(7-5(1))(2)$, $1 = 5(3)-7(2)$

$1 = (26-7(3))(3)-7(2)$

$1 = 26(3)-7(11)$, $1 = 26(3)+7(-11)$

Inverse of 7 modulo 26 = $-11+26 = 15$

(iii) 200 modulo 1001

$1001 = 200(5)+1$

$200 = 1(200)+0$

$1 = 1001(1)+200(-5)$

Inverse of 200 modulo 1001 = -5

Inverse of 200 modulo 1001 = −5

$-5 + 1001 = 996$

Q21. Solve the linear congruence equation

$ax \equiv b \bmod m$

$\gcd(a, m) \mid b \Rightarrow$ soln. exist

a^{-1} ?? $\gcd(a, m) = 1$

(i) $3x \equiv 4 \ (mod\ 7)$

$a = 3, \ m = 7, \quad b = 4$

$\gcd(a, m) = 1, \quad 1 \mid 4$ ✓

$\downarrow$

a^{-1} exists

$a \equiv b \bmod m$

$ac \equiv bc \bmod m$

Inverse of 3 modulo 7 = 5

$7 \mid 3a^{-1} - 1$

Multiply with Inverse = 5

$15x \equiv 20 (\bmod 7)$

$15 \equiv 1 \bmod (7) \qquad 20 = 6 \bmod (7)$

$1 \cdot x \equiv 6 \bmod 7, \qquad x \equiv 6 \bmod 7$

(ii) $19x \equiv 4 \ (mod\ 141)$

$\gcd(19, 141) = 1, \quad 1 \mid 4$

$141 = 19(7) + 8 \qquad 1 = 19(3) - (141 - 19(7))(7)$

$1 = 19(3) - 8(7)$

$141 = 19(7) + 8$ $\quad 1 = 19(3) - (141 - 19(7))(7)$

$19 = 8(2) + 3$ $\quad 1 = (19 - 8(2))(3) - 8(1)$, $1 = 19(3) - 8(7)$

$8 = 3(2) + 2$ $\quad 1 = 3 - (8 - 3(2))(1)$, $1 = 3(3) - 8(1)$

$3 = 2(1) + 1$ $\quad 1 = 3 - 2(1)$

$$1 = 19(52) - 141(7)$$

$$1 = 19(52) + 141(-7)$$

Inverse of 19 modulo 141 = 52

Multiply 52

$$988x \equiv 208 \pmod{141}$$

$988 \equiv 1 \bmod (141)$ $\quad 208 \equiv 67 \pmod{141}$

$$x \equiv 67 \bmod (141)$$

(iii) $55x = 34(mod\ 89)$

$\gcd(55, 89) = 1$, $1 | 34$ soln exist

$\downarrow$

a^{-1} exist

$1 = 55(34) + 89(-21)$

Inverse of 55 modulo 89 = 34

$(55 \cdot 34)x \equiv (34 \cdot 34) \bmod 89$, $\quad 1870x \equiv 1156 \pmod{89}$

$1x \equiv 88 \pmod{89}$

(iv) Solve $6x \equiv 33\ mod\ 81$

(iv) Solve $6x \equiv 33 \bmod 81$

$\gcd(6, 81) = 3$, $3 | 33$ soln. exist

$ac \equiv bc \bmod mc$

$\Downarrow$

$a \equiv b \bmod m$

$2x \equiv 11 \pmod{27}$

Inverse of 2 modulo 27 = 14

$28x \equiv 154 \pmod{27}$

$1 \cdot x \equiv 19 \pmod{27}$

Three solns

19, 19+27, 19+27+27

19, 46, 73