Class Work

Date 26/April/2023
Page

Unit-6 (Number Theory & its Applications)

coprime ⇒ gcd = 1

gcd(a,b) = 1

gcd(3,5) = 1

(3,8) = 1

(8,9) = 1

Formula :→ gcd (24,36)

$24 = 6 \times 4 = 2^3 \times 3^1$

$36 = 6 \times 6 = 2^2 \times 3^2$

$\gcd(24,36) = 2^{\min(3,2)} \cdot 3^{\min(1,2)}$

$= 2^2 \cdot 3^1 = 4 \times 3 = 12$

$lcm = 2^{\max(3,2)} \cdot 3^{\max(1,2)}$

$= 2^3 \cdot 3^2 = 8 \times 9 = 72$

$\therefore \gcd = p_1^{\min(n_1, n_1')} \cdots p_k^{\min(n_k, n_k')}$

$lcm = p_1^{\max(n_1, n_1')} \cdots p_k^{\max(n_k, n_k')}$

Que (1) $2^3 3^5 7^2$ & $2^4 3^3$

$\gcd = 2^3 \times 3^3 \times 7^0 = 8 \times 27 \times 49 =$

$lcm = 2^4 \times 3^5 \times 7^2 =$

gcd = hcf

Date
Page

(2) $3^7 5^3 7^3$, $2^{11} 3^9 5^9$

gcd $= 3^7 \times 2^0 \times 5^3 \times 7^0$

lcm $= 2^{11} \times 3^9 \times 5^9 \times 7^3$

(3) $2^2 3^3 5^5$ $\quad 2^5 3^3 5^2$

gcd $2^2 3^3 5^2$

lcm $2^5 3^3 5^5$

Q1 Find gcd 252 & 198

198) 252 (1
198
54) 198 (3
162
36) 54 (1
36
18) 36 (2
36
x

252 = 198(1) + 54

198 = 54(3) + 36

54 = 36(1) + 18

36 = 18(2) + 0

hcf = 18 (gcd)

(A) 21, 55

$55 = 21(2) + 13$

$21 = 13(1) + 8$

$13 = 8(1) + 5$

$8 = 5(1) + 3$

$5 = 3(1) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

gcd = 1

(B) 414, 662

$662 = 414(1) + 248$

$414 = 248(1) + 166$

$248 = 166(1) + 82$

$166 = 82(2) + 2$

$82 = 2(41) + 0$

gcd = 2

gcd = 2

Date
Page

(4) 101, 111

101) 111 (1
101
10) 101 (10
100
1) 10 (10
10
X

gcd = 1

(5) 1001, 1331

1001) 1331 (1
- 1001
330) 1001 (3
990
110) 330 (30
330
X

gcd = 11

(6) 124, 323

124) 323 (2
248
75) 124 (1
75
49) 75 (1
49
26) 49

$23\overline{)29}\ (1$
$\quad 23$
$\quad\overline{\quad 6\overline{)23}\ (3}$
$\quad\quad 18$
$\quad\quad\overline{\quad 5\overline{)6}\ (1}$
$\quad\quad\quad 5$
$\quad\quad\quad\overline{\quad 1\overline{)5}\ (5}$
$\quad\quad\quad\quad 5$
$\quad\quad\quad\quad\overline{\quad x}$

gcd = 1

Bezout's Theorem

If gcd (d) of a, b, can be written as linear combination of a & b then d

$d = gcd(a,b)$

i.e $d = ax + by$

Eg:- $(662, 414) = 2$ (two equations)

$2 = 166 - 82(2)$
$= 166 - (248 - 166(1))(2)$
$= 166(3) + 248(2)$
$= (414 - 248(1))(3) + -248(2)$
$= 414(3) - 248(5)$
$= 414(3) - (662 - 414(1))5$
$= 662(-5) + 414(8)$
$2 = 662x + 414y \Rightarrow x = -5, y = 8$

Q. 21, 55

gcd (21, 55) = 1

$1 = 3 - 2(1)$

$= 3 - [5 - 3(1)]1$

$= 8 - 5(1) - (5(1)) + 3(1)$

$= 8 - 5(2) + 3(1)$

$= 8 - (13 - 8)(2) + 3(1)$

$= 8 - 13(2) + 8(2) + 3(1)$

$= 8(3) - 13(2) + 3(1)$

$21(3) - 13(3) - 13(2) + 3(1)$

$= 21(3) - 13(6) + 3(1)$

$= 21(3) - (55 - 21(2))(3) + 3(1)$

$= 21(5) \cdot$

$= 21(3) - 55(5) + 21(10) + 3(1)$

$= 21(13) - 55(5) + 3$

Ques. : 124 & 323

$124 \overline{)323}\ 2$

248

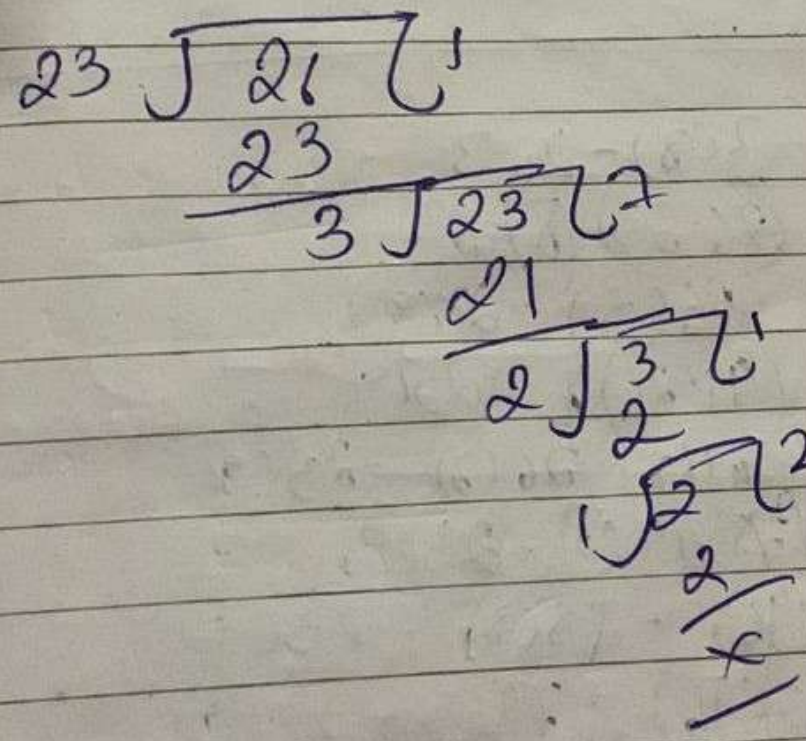
$75 \overline{)124}\ 1$

75

$49 \overline{)75}\ 1$

49

$26 \overline{)49}\ 1$



$323 = 124(2) + 75$

$124 = 75(1) + 49$

$75 = 49(1) + 26$

$49 = 26(1) + 23$

$26 = 23(1) + 3$

$23 = 3(7) + 2$

$3 = 2(1) + 1$

$2 = 1(2) + 0$

Begin with $\Rightarrow$

$1 = 3 - 2(1)$

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

$= 3 - 23 + 3(7)$

$= 3(8) - 23$

$= 26 - 23(1) - 23$

$= 26 - 23(2)$

$= 26 - [49 - 26]2$

MTH401

Unit-6 Continued

Quer fried of 4999, 1109

$1109 \overline{)4999}\ (4$
4436
$563 \overline{)1109}\ (1$
563
$546 \overline{)563}\ (1$
546
$17 \overline{)546}\ (32$
544
$2 \overline{)17}\ (8$
16
$1 \overline{)2}\ (2$
2
0

$4999 = 1109(4) + 563$
$1109 = 563(1) + 546$
$563 = 546(1) + 17$
$546 = 17(32) + 2$
$17 = 2(8) + 1$
$2 = 1(2) + 0$

$1 = 17 - 2(8)$
$17(1) - [546 - 17(32)](8)$
$17(1) - 546(8) - 17(32)(8)$
$17(1) - 546(8) - 17(256)$

ThinkBIG

$-546(8) - [563 - 546(1)](257)$
$= -546(8) - 563(257) + 546(257)$
$= -546(265) - 563(257)$
$= -(1109 - 563)\,265 - 563(257)$
$= -1109(265) + 563(265) + 563(257)$
$= -1109(265) + 563(522)$
$= -1109(265) + 4999 - 1109(4)(522)$
$= -1109(265) + 4999(522) - 1109(4)(522)$
$= -1109(2653) + 4999(522)$

$x = -2353$
$y = 522$

Division Algorithm

Let a be an integer and d be a +ve integer.
Then there are unique integers q & r with $0 \le r < d$

such that $a = dq + r \Rightarrow \frac{r-a}{d}$ or $\frac{a-r}{d}$

or

$r = a \bmod d$

If 'a' and 'b' are integers and m is a positive integer then a is congruent to b modulo m

i.e. $a \equiv b \bmod m$

iff $a-b$ is divisible by m

Ex: Determine whether 17 is congruent to 5 modulo 6

$17 \equiv 5 \bmod 6$

$\Rightarrow \frac{17-5}{6} = \frac{12}{6} = 2$ Yes

24 & 14 are congruent modulo to 6

~~6 | 24 mod 6~~
~~6 - 24~~
~~18~~

$24 = 14 \bmod 6$

$\neq$

$\frac{24-14}{6} \neq$

Let m be a +ve integer. If $a \equiv b$ modulo m & $c \equiv d \bmod m$

then $a+c \equiv (b+d) \bmod m$

(1)

(2) $ac = bd \bmod m$

Q: find an inverse of 3 modulo 7

3 mod 7

$7 = 3(2) + 1$
$3 = 1(3) + 0$

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

Ans $\Rightarrow -2$

$3 \overline{)7} \; (2$
6
$1 \overline{)3} \; (3$
3
0

2 Find an inverse of 4 mod 9

$$4 \overline{)9}\ (2$$
$$\underline{8}$$
$$1 \overline{)4}\ (4$$
$$\underline{4}$$
$$0$$

$9 = 4(2) + 1$

$4 = 1(4) + 0$

$9 - 4(2) \Rightarrow 9 + 4(-2)$ Ans $\rightarrow -2$

3 Inverse of 2 mod 17

$$2 \overline{)17}\ (8$$
$$\underline{16}$$
$$1 \overline{)2}\ (2$$
$$\underline{2}$$
$$0$$

$17 = 2(8) + 1$

$1 = 17 + 2(-8)$

19 mod 141

ThinkBIG

Ques Show that 15 is an inverse of 7 modulo 26

$7 \overline{)26}\ 3$
-21
$5 \overline{)7}\ 1$
5
$2 \overline{)5}\ 2$
4
$1 \overline{)2}\ 2$
2
X

GCD = 1

$26 = 7(3) + 5$
$7 = 5(1) + 2$
$[5 = 2(2) + 1]$
$2 = 1(2) + 0$

$5 - 2(2)$
$5 - (7-5)(2)$
$5 - 7(2) + 5(2)$
$5(3) - 7(2)$
$(26 - 7(3))(3) - 7(2)$
$26(3) + 7(-11)$

$x \in (-26, 26)$

32

ThinkBIG

7 modulo 26 $= -11 + 26$
$= 15$ //

[-ve में add करना है]

First Positive Answer

Ques $4x \equiv 5 \pmod 9$

$4x - 5$
9

Ans -1
8

$-1, 8$

Ques $2x \equiv 7 \bmod 17$

Ans $= -5$
12

$2x - 7$
17

Chinese Remainder Theorem..

Ques
$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 1$

$(3,5) = 1$

$(5,7) = 1$

$(3,7) = 1$

$(3,5,7) = 1$

$a_1 = 2, \quad a_2 = 3, \quad a_3 = 2$

$m_1 = 3, \quad m_2 = 5, \quad m_3 = 7$

$M = m_1 \cdot m_2 \cdot m_3$

$= 3 \cdot 5 \cdot 7$

$= 105$

$M_1 = \frac{M}{m_1} = \frac{m_1 \cdot m_2 \cdot m_3}{m_1} = 5 \cdot 7 = 35$

$M_2 = \frac{M}{m_2} = 3 \cdot 7 = 21$

$M_3 = \frac{M}{m_3} = 3 \cdot 5 = 15$

$M_1 y_1 \equiv 1 \pmod{m_1}$

$35 y_1 \equiv 1 \pmod 3$

$2 y_1 \equiv 1 \pmod 3$

$y_1 = 2$

$M_2 y_2 \equiv 1 \pmod{m_2}$

$21 y_2 \equiv 1 \pmod 5$

$1 y_2 \equiv 1 \pmod 5$

$y_2 = \frac{1}{5} \Rightarrow y_2 = 1$

$M_3 y_3 \equiv 1 \pmod{m_3}$

$15 y_3 \equiv 1 \pmod 7$

$1 y_3 \equiv 1 \pmod 7$

$y_3 = \frac{1}{7} \Rightarrow y_3 = 1$

$x = a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3$

$= 2 \cdot 2 \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 5 \cdot 1$

$\Rightarrow 233 \equiv 23 \bmod 105$

Qu 2

$x = 1 \bmod (3)$

$x = 2 \pmod 5$

$x = 3 \pmod 7$

Ans → $157 \equiv 52 \bmod (105)$

Q3

$x \equiv 7 \pmod 9 \rightarrow 3 \times 3$

$x \equiv 14 \pmod{12} \rightarrow 2 \times 2 \times 3$

$x = 16 \pmod{21} \rightarrow 3 \times 7$

(1) $x \equiv 7 \pmod 3$

$x \equiv 7 \pmod 3$

$x \equiv 1 \pmod 3$ — (1)

(2) $x \equiv 4 \pmod 2$

$x \equiv 4 \pmod 2$

$x \equiv 4 \pmod 3$

$x = 1 \pmod 3$ ✗

$x = 4 \pmod 2$ — (2)

(3) $x = 16 \pmod 3 \longrightarrow x = 1 \pmod 3$ ✗

$x = 16 \pmod 7$

$x = 2 \pmod 7$ — (3)

Ans $x = 1 \pmod 3$ →

$x = 4 \pmod 2$

$x = 2 \pmod 7$

ThinkBIG

3, 2, 7,

$a_1 = 1 \quad a_2 = 4 \quad a_3 = 2$

$m_1 = 3 \quad m_2 = 2 \quad m_3 = 7$

$m = 3 \times 2 \times 7$

Que

$x = 5 \pmod 6$ 2×3
$x = 3 \pmod{10}$ 2×5
$x = 8 \pmod{15}$ 3×5

$a_1 = 5 \quad a_2 = 3 \quad a_3 = 8$
$m_1 = 6 \quad m_2 = 10 \quad m_3 = 15$

$m = 6 \times 10 \times 15$
$= 900$

$\frac{60}{15}$

$5 \pmod 2 = 1 \pmod 2$ — (1)
$5 \pmod 3 = 3 \pmod 2$

$3 \bmod 2 = 1 \bmod 2$
$3 \bmod 5$ — (2)

ThinkBIG

$3 \bmod 15 \quad 8 \bmod 3 = 2 \bmod 3$
$5 \bmod 15 \quad 8 \bmod 5 =$

$1 \pmod 2$ — (1)
$3 \pmod 5$ — (2)
$2 \pmod 3$ — (3)

$a_1 = 1 \quad a_2 = 3 \quad a_3 = 2$

$m_1 = 2 \quad m_2 = 5 \quad m_3 = 3$

$m = 2 \times 5 \times 3$
$= 30$

$M_1 = \frac{m}{m_1} = 15$

$M_2 = \frac{30}{5} = 6$

$M_3 = 10$

$M_1 y_1 = 1 \pmod{m_1}$
$15 y_1 = 1 \pmod 2$

$y_1 = 1 \pmod 2$

$\frac{y_1 - 1}{2} \Rightarrow \boxed{y_1 = 1}$

$y_2 = 1$

$y_3 = 1$

$x = 1(1)(15) + 3(1)(6) + 2(1)(4)$

$= 15 + 18 + 20$

$= 53$

$\therefore 53 \equiv 23 \pmod{30}$

So $\boxed{53}$

$2x \equiv 6 \pmod{14}$

$3x \equiv 9 \pmod{15}$

$5x \equiv 20 \pmod{60}$

$x = 3 \pmod 7$

$x = 3 \pmod 5$

$x = 4 \pmod{12}$

$7,5 = 1$ $\quad 5,12 = 1$ $\quad 7,12 = 1$

$a_1 = 3$ $\quad a_2 = 3$ $\quad a_3 = 4$

$m_1 = 7$ $\quad m_2 = 5$ $\quad m_3 = 12$

$M = 7 \times 5 \times 12$

$= 420$

$M_1 = 5 \times 12 = 60$

$M_2 = 7 \times 12 = 84$

$M_3 = 7 \times 5 = 35$

$M_i y_i = 1 \pmod{m_i}$

$\Rightarrow 4y_1 = 1 \pmod 7$

$\frac{4y=1}{7}$ $y_1=2$

$y_2=4$

$35y_3 \equiv 1 \pmod{12}$

$11y_3 = 1 \pmod{12}$

$\frac{11y_3-1}{12}$ $\frac{-12}{12}$ $= \frac{-1}{-1} = 11$

$y_3=11$

$x = 3\times60\times2 + 3\times84\times4$

$+ 4\times11\times35$

$= 360 + 1008 + 1540$

$= 2908$

2980 $\equiv$ 388 mod 420

Cryptology

A	-0	R	-17
B	-1	S	-18
C	-2	T	-19
D	-3	U	-20
E	-4	V	-21
F	-5	W	-22
G	-6	X	-23
H	-7	Y	-24
I	-8	Z	-25
J	-9		
K	-10		
L	-11		
M	-12		
N	-13		
O	-14		
P	-15		
Q	-16		

What is the secret Message produced from the message

"MEET YOU IN THE PARK"

$12+3=15$ → +3

Using Caesar's Cipher.

⇒ PHHW BRX LQ WKH SDUN

(2) Shift Cipher → +K

Encrypt the message "do not pass" K = 13 using shift cipher with

DO NOT PASS

QB AB GNFF

(3) Affine Transport

↓

$ap+b$

$3K+7$