Modular Arithmetic.

Divisibility:-

The set of integers consists of all positive integers, all negative integers and zero. It is denoted by I or Z.

I or Z = { .... -3, -2, -1, 0, 1, 2, 3 --- }

= { 0, ±1, ±2, ±3, ±4, ±5, ----- }

Consider 2 integers a and b where $a \neq 0$, a divides b if there exists an integer k such that $b = k.a$.

Eg:- 9 divides 54 ; there is the integer 6 such that

$54 = 6 \times 9$.

'a divides b' is written as a|b (the symbol '|' stands for divides).

Eg:- i) 13|-52 ∵ $-52 = -4 \times 13$

ii) 9∤78 (9 does not divide 78)

78 ≠ (an integer) 9

Division Algorithm:-

Given two integers a and b where $a > 0$, two unique integers q and r can always be found such that $b = qa + r$, where $0 \leq r < a$. This is known as division algorithm. q is called the quotient and r is called the remainder.

The process of division is as follows:

a) b (q

qa

b - qa = r, where $0 \leq r < a$.

i.e $b = qa + r$, $0 \leq r < a$.

In case $r = 0$, $b = qa \Rightarrow a|b$.

Dr. Sreelakshmi
BMSIT&M

Q:-

1) $a=25,\ b=18$

$$25\overline{)18}\,(0$$
$$\underline{00}$$
$$18$$

$\therefore q=0,\ r=18$ $\quad\therefore 18 = 0\times 25 + 18.$

2) $a=17,\ b=2589$

$$17\overline{)2589}\,(152$$
$$\underline{17}$$
$$88$$
$$\underline{85}$$
$$39$$
$$\underline{34}$$
$$5$$

$\therefore q=152,\ r=5$ $\quad\therefore 2589 = 152\times 17 + 5.$

3) $a=17,\ b=-245$

$$17\overline{)-245}\,(-15$$
$$\underline{-255}$$
$$10$$

$\therefore q=-5,\ r=10$ $\quad\therefore -245 = -15\times 17 + 10.$

*Note:-

In all divisions q may be positive or negative or zero; but r is always positive (or zero) and less than the divisor.

* Greatest Common Divisor (G.C.D) OR Highest Common Factor (H.C.F).

The G.C.D of two integers a and b (both of them are not zero) is a unique positive integer d such that

i) d is the common divisor of both a and b,
   i.e, $d|a$, $d|b$.

ii) every common divisor of a and b divides d
   i.e $x|a$ and $x|b \Rightarrow x|d$.

The G.C.D of 2 numbers a and b is written as
(a,b) i.e, $d = (a,b)$.

Eg:- Consider the integers 12 and 18.
The positive divisors of 12 are 1, 2, 3, 4, 6, 12.
The positive divisors of 18 are 1, 2, 3, 6, 9, 18.
the common divisors of 12 and 18 are 1, 2, 3, 6
clearly 6 is the G.C.D of 12 and 18.

i) 6 is the common divisor of 12 and 18
   i.e., $6|12$, $6|18$.

ii) every common division of 12 and 18 divides 6.
   i.e $1|6$, $2|6$, $3|6$ and $6|6$.

* Euclid's Algorithm method to find the G.C.D of 2 given numbers a and b and to express the G.C.D as ax+by.

A method of finding the greatest common divisor of two numbers by dividing the larger by the smaller, the smaller, the smaller by the remainder, the first reminder by the second remainder, and so on until exact division is obtained hence the greatest common divisor is the exact divisor.

Steps to find gcd using Eudidian Algorithm for any two integers a and b with a>b.

Step 1: Let a, b be the two numbers.
Step 2: a mod b = R.
Step 3: Let a = b and b = R.
Step 4: Repeat steps 2 and 3 until a mod b is greaterthan 0.

---

1) Find the G.C.D of 32 and 54 and express it in the form 32x+54y.

$$32\overline{)54}\,(1 \quad \underline{32} \quad 22$$

$22 = 54 - 1(32) \rightarrow (1)$

$$22\overline{)32}\,(1 \quad \underline{22} \quad 10$$

$10 = 32 - 1(22) \rightarrow (2)$

$$10\overline{)22}\,(2 \quad \underline{20} \quad 2$$

$2 = 22 - 2(10) \rightarrow (3)$

$$2\overline{)10}\,(5 \quad \underline{10} \quad 0$$

The last non zero remainder is 2.

$\therefore$ G.C.D is 2.

From (3),

$2 = 22 - 2(10)$

$2 = [54 - 1(32)] - 2[32 - 1(22)]$

$2 = 54 - 3(32) + 2(22)$

$= 54 - 3(32) + 2[54 - 1(32)]$

$= 3(54) - 5(32)$

$= 54(3) + 32(-5)$

i.e $2 = 54x + 32y$ Where $x = 3, y = 5$.

Find the G.C.D of 25520 and 19314 and express it in the form $25520x + 19314y$.

$$19314\overline{)25520}\,(1 \quad 19314 \quad \underline{6206}$$

$$6206 = 25520 - 1(19314) \rightarrow (1)$$

$$6206\overline{)19314}\,(3 \quad 18618 \quad \underline{696}$$

$$696 = 19314 - 3(6206) \rightarrow (2)$$

$$696\overline{)6206}\,(8 \quad 5568 \quad \underline{638}$$

$$638 = 6206 - 8(696) \rightarrow (3)$$

$$638\overline{)696}\,(1 \quad 638 \quad \underline{58}$$

$$58 = 696 - 1(638) \rightarrow (4)$$

$$58\overline{)638}\,(11 \quad 638 \quad \underline{0}$$

$\therefore$ The last non-zero remainder is 58.

$\therefore$ G.C.D is 58.

From (4),

$$58 = 696 - 1(638)$$
$$58 = 696 - 1[6206 - 8(696)]$$
$$58 = 9 \times 696 - 6206$$
$$58 = 9[19314 - 3(6206)] - 6206$$
$$58 = 9 \times 19314 - 28 \times 6206$$
$$58 = 9 \times 19314 - 28[25520 - 1(19314)]$$
$$58 = 37 \times 19314 - 28 \times 25520$$
$$58 = (-28)25520 + (37)19314$$

i.e $58 = 25520x + 19314y$ Where

$x = -28$, $y = 37$.

Relatively Prime numbers:

Two numbers a and b are said to be relatively prime or co-prime if and only if $(a,b)=1$, i.e the g.c.d of a and b is 1.

Eg: $(8,15)=1$ $\therefore$ 8 and 15 are relatively prime.

---

* Congruences:

Let m be a positive integer (>1). If a and b are any integers then a is said to be congruent to b modulo m if and only if $m \mid a-b$.

'a is congruent to b modulo m' is written as

$a \equiv b \pmod{m}$.

Thus if $a \equiv b \pmod{m}$ then $m \mid a-b$ and conversely if $m \mid a-b$ then $a \equiv b \pmod{m}$.

Eg: i) $25 \equiv 3 \pmod{11}$ $\quad 11 \mid 25-3$ i.e, $11 \mid 22$.

ii) $-69 \equiv -5 \pmod{16}$ $\quad 16 \mid -69+5$ i.e, $16 \mid 64$

iii) $79 \not\equiv 8 \pmod{9}$ $\quad 9 \nmid 79-8$.

* Consider the congruence: $134 \equiv 108 \pmod{13}$ which is true.

```
13)134(10        13)108(8
   130               104
   ---               ---
     4                 4.
```

When 134 and 108 are divided by 13, the same remainder 4 is obtained. This gives the alternate definition of the congruence.

Def^n:- If m is a positive integer (>1) and a and b are any integers then 'a' is said to be congruent to b modulo m if and only if a and b leave the same remainder when divided by m.

Eg:- i) $45 \equiv 3 \pmod 4$

$45 - 3 = 42$, $4 \mid 42$ ∴ It is false.

ii) $-124 \equiv -172 \pmod{12}$

$-124 + 172 = 48$, $12 \mid 48$ ∴ It is true.

iii) $2^8 \equiv 1 \pmod{17}$

$2^8 - 1 = (2^4)^2 - 1 = 256 - 1 = 255$, $17 \mid 255$ ∴ It is true.

Problems:

1) Solve $5x = 4 \pmod{13}$

$\Rightarrow 13 \mid 5x - 4$

$\Rightarrow 5x - 4 = 13k$ Where $k \in z$

$\Rightarrow 5x = 13k + 4$

$\Rightarrow x = \frac{13k+4}{5}$

By inspection, $k = 2$ gives the integral value of x.

i.e, $x = \frac{13(2)+4}{5} = 6$.

i.e $x \equiv 6 \pmod{13}$ ∴ The general solution is $x = 6 + 13t$ where $t \in z$.

---

2).

If $2^8 \equiv a \pmod{13}$ find a.

$2^8 = (2^4)^2 = 256$

$\therefore 256 \equiv 9 \pmod{13}$

i.e, $2^8 \equiv 9 \pmod{13}$ ∴ $a = 9$

13)256(19
13
126
117
9

---

3) Solve $7x \equiv 9 \pmod{15}$

$\Rightarrow 15 \mid 7x - 9$

$\Rightarrow 7x - 9 = 15k$

$\Rightarrow 7x = 15k + 9$ Where $k \in z$

$\Rightarrow x = \frac{15k+9}{7}$

By inspection, $k = 5$ gives the integral value of x.

i.e $x = \frac{15(5)+9}{7} = \frac{75+9}{7} = 12$.

$\therefore x \equiv 12 \pmod{15}$

4) Find the least positive values of x such that

i) $71 \equiv x \pmod 8$

$$8)71(8$$
$$\underline{64}$$
$$7$$

The value of $x = 7$

ii) $78 + x \equiv 3 \pmod 5$

$78 + x - 3 = 5n$ (n is any integer)

$75 + x = 5n$

Let $x = 5$

$75 + 5 = 80$ (80 is multiple of 5)

∴ The least value of x is 5

iii) $89 \equiv (x + 3) \pmod 4$

$89 - x - 3 \equiv 4n$

$86 - x = 4n$

Let $x = 2$

$86 - 2 = 84$ (84 is multiple of 4)

∴ The least value of x is 2.

iv) $96 \equiv \left(\frac{x}{7}\right) \bmod 5$.

$96 - \frac{x}{7} = 5n$

$672 - x = 35n$

$672 - 7 = 665$ (multiple of 35 is 665)

∴ The value of $x = 7$

4) $5x \equiv 4 \pmod 6$

$5x - 4 = 6n$

$5x = 6n + 4$

$x = \frac{6n+4}{5}$

Substitute the value of n as 1, 6, 11, 16 --- as n values in $x = (6n+4)/5$ which is divisible by 2, 8, 14, 20 --

$\therefore$ The least positive value is 2.

---

5) If $2x \equiv 3 \pmod 7$ find x such that $9 \leq x \leq 30$.

$x = 5$ satisfies the congruence because $10 \equiv 3 \pmod 7$ is true.

$\therefore x \equiv 5 \pmod 7$ is the solution.

Solution set = $\{ \ldots -9, -2, 5, 12, 19, 26, 33, \ldots \}$

The required values of x are 12, 19, 26.

---

6) Find the least positive remainder when 2^{301} is divided by 5.

$2^4 \equiv 16 \equiv 1 \pmod 5$

$(2^4)^{75} \equiv 1 \pmod 5$

$2^{300} \equiv 1 \pmod 5 \rightarrow (1)$

$2 \equiv 2 \pmod 5 \rightarrow (2)$

$(1) \times (2)$

$2^{301} \equiv 2 \pmod 5$

$\therefore$ Remainder is 2

4)301(75
28
21
20
1

---

7) Find the unit digit in the number 7^{289}. (10)

$7^2 \equiv 9 \pmod{10}$

$7^4 \equiv 81 \equiv 1 \pmod{10}$

$(7^4)^{72} \equiv 81 \pmod{10}$

$7^{288} \equiv 1 \pmod{10}$

$7 \equiv 7 \pmod{10}$

$7^{289} \equiv 7 \pmod{10}$

$\therefore$ unit digit in 7^{289} is 7.

$$\begin{array}{r|l} 4 & 289 \\ \hline & 28 \\ \hline & 9 \\ & 8 \\ \hline & 1 \end{array} \quad 72$$

---

8) Find the last digit of 7^{2013}.

$7^2 \equiv 9 \pmod{10}$

$7^4 \equiv 81 \equiv 1 \pmod{10}$

$(7^4)^{503} \equiv 1 \pmod{10}$

$7^{2012} \equiv 1 \pmod{10}$

$7 \equiv 7 \pmod{10}$

$\therefore 7^{2013} \equiv 7 \pmod{10}$

$\therefore$ Last digit is 7

$$\begin{array}{r|l} 4 & 2013 \\ \hline & 20 \\ \hline & 13 \\ & 12 \\ \hline & 1 \end{array} \quad 503$$

---

1) Find the unit (last) digit in the number 7^{126}.

$7^2 \equiv 9 \pmod{10}$

$7^4 \equiv 81 \equiv 1 \pmod{10}$

$(7^4)^{31} \equiv 1 \pmod{10}$

$7^{124} \equiv 1 \pmod{10}$

$7^2 \equiv 9 \pmod{10}$

$7^{126} \equiv 9 \pmod{10}$.

$\therefore$ 9 is the unit digit in 7^{126}.

4) 126 (31
12
6
4
2

---

10) Find the last digit of 13^{37}.

$13 \equiv 13 \pmod{10}$

$13 \equiv 3 \pmod{10}$

$13^2 \equiv 3^2 \pmod{10}$

$13^2 \equiv 9 \pmod{10}$

$\equiv -1 \pmod{10}$

$13^4 \equiv (-1)^2 \pmod{10}$

$13^4 \equiv 1 \pmod{10}$

$(13)^{37} \equiv 13^{4\times 9+1} = 13^{4\times 9} \cdot 13$

$= (13^4)^9 \cdot 13$

$= 1 \bmod 10 \times 13$

$(13)^{27} = 13 \bmod 10$

$= 3 \bmod 10$

$\therefore$ 3 is the last digit in 13^{37}.

11) What is the remainder in the division of 2^{50} by 7 ?.

$2^3 \equiv 8 \equiv 1 \pmod 7$

$(2^3)^{16} \equiv 1^{16} \pmod 7 \rightarrow (1)$

$2^2 \equiv 4 \pmod 7 \rightarrow (2)$

$2^{48} \cdot 2^2 \equiv 1 \cdot 4 \pmod 7$

$\therefore 2^{50} \equiv 4 \pmod 7$

$\therefore$ the remainder is 4.

---

*12) Find the remainder when 2^{23} is divided by 47.

$2^8 \equiv 256 \equiv 21 \pmod{47}$

$(2^8)^2 \equiv (21)^2 \pmod{47}$

$2^{16} \equiv 441 \pmod{47}$

$2^{16} \equiv 18 \pmod{47} \rightarrow (1)$

47)256(5
235
21

47)441(9
423
18

$2^7 \equiv 128 \equiv 34 \pmod{47} \rightarrow (2)$

47)128(2
94
34

(1) × (2)

$2^{16} \times 2^7 = 18 \times 34 \pmod{47}$

$2^{23} \equiv 612 \pmod{47}$

$2^{23} \equiv 1 \pmod{47}$

47)612(13
47
142
141
1

$\therefore$ the remainder is 1.

Find the remainder when $135 \times 74 \times 48$ is divided by 7.

$$7)135(19$$
$$\underline{7}$$
$$65$$
$$\underline{63}$$
$$2$$

$135 \equiv 2 \pmod 7 \rightarrow (1)$

$$7)74(10$$
$$\underline{70}$$
$$4$$

$74 \equiv 4 \pmod 7 \rightarrow (2)$

$$7)48(6$$
$$\underline{42}$$
$$6$$

$48 \equiv 6 \pmod 7 \rightarrow (3)$

$(1) \times (2) \times (3)$

$135 \times 74 \times 48 \equiv 48 \pmod 7 \equiv 6 \pmod 7$

$\therefore$ the remainder is 6

---

14) Find the remainder obtained when $64 \times 65 \times 66$ is divided by 67.

$64 \equiv -3 \pmod{67} \rightarrow (1)$

$65 \equiv -2 \pmod{67} \rightarrow (2)$

$66 \equiv -1 \pmod{67} \rightarrow (3)$

$(1) \times (2) \times (3)$

$64 \times 65 \times 66 \equiv -6 \pmod{67}$

$\equiv 61 \pmod{67}$

$\therefore$ the remainder is 61

---

15) Find the remainder when $349 \times 74 \times 36$ is divided by 3.

$$3)349(116$$
$$\underline{3}$$
$$49$$
$$\underline{3}$$
$$19$$
$$\underline{18}$$
$$1$$

$349 \equiv 1 \pmod 3 \rightarrow (1)$

3) 74 (24
   6
   14
   12
   2

$74 \equiv 2 \pmod 3 \rightarrow (2)$

3) 36 (12
   36
   0

$36 \equiv 0 \pmod 3 \rightarrow (3)$

① × ② × ③

$349 \times 74 \times 36 \equiv 0 \pmod 3$

∴ the remainder is 0.

---

16) Find the reminder when $175 \times 113 \times 53$ is divided by 11.

11) 175 (15
    11
    65
    55
    10

$175 \equiv 10 \pmod{11} \rightarrow (1)$

11) 113 (10
    110
    3

$113 \equiv 3 \pmod{11} \rightarrow (2)$

11) 53 (4
    44
    9

$53 \equiv 9 \pmod{11} \rightarrow (3)$

① × ② × ③

$175 \times 113 \times 53 = 10 \times 3 \times 9 \equiv 270 \pmod{11}$

$\equiv 6 \pmod{11}$

∴ the remainder is 6

**17) Find the remainder when the number 2^{1000} is divided by 13.

$2 = 2$; $2^2 = 4$; $2^3 = 8$, $2^4 = 16 \equiv 3 \pmod{13}$

$2^5 = 32$, $2^6 \equiv 64 \equiv -1 \pmod{13}$

$2^{1000} = 2^{6\times166+4}$.

$= (2^6)^{166} * 2^4$.

$\equiv (-1)^{166} \bmod 13 \cdot 3 \bmod 13$

$= 1 \bmod 13 \cdot 3 \bmod 13$

$2^{1000} \equiv 3 \bmod 13$

$\therefore$ The remainder is 3.

$$\begin{array}{r|l} 6 & 1000 \\ \hline & 6 \\ \hline & 40 \\ & 36 \\ \hline & 40 \\ & 36 \\ \hline & 4 \end{array}$$ 166 .

* Rules for finding x in linear congruence:

General format : $ax \equiv b \pmod n$.

1) Find gcd $(a, n) = d$ (let)
2) $b/d \rightarrow$ if possible $\rightarrow$ solution exist.
3) Find $d \bmod n \rightarrow$ There no. of sol^n are possible.
4) Divide both sides by d.
5) Multiply both sides by 'Mul. inverse of a'.
   i.e $(a a^{-1}) x = b.a^{-1} \pmod n$
6) General sol^n eq^n is

$$x_k = x_0 + k\left(\frac{n}{d}\right),$$

Where $k = \{0, 1, 2 \text{ --- } (d-1)\}$.

---

1) $14x \equiv 12 \pmod{18}$

$ax \equiv b \pmod n$

$a = 14, b = 12, n = 18$.

1) gcd $(a, n) \rightarrow d$
   gcd $(14, 18) = 2$ (d)
2) $b/d = 12/2 = 6 \rightarrow$ Sol^n exist.
3) $d \bmod n = 2 \bmod 18 = 2 \rightarrow 2$ sol^n exist.
4) Divide both the sides by d.

$$\frac{14}{2}x \equiv \frac{12}{2} \pmod{\frac{18}{2}}$$

$$7x \equiv 6 \pmod 9$$

5) Multiply both sides by mul. inverse of a.

$$7 \cdot 7^{-1} x = 6 \cdot 7^{-1} \pmod 9$$

$$x = 6 \cdot 7^{-1} \pmod 9$$

$(7 \times c) \bmod n = 1$

$(7 \times c) \bmod 9 = 1$

$c=1)\ 7 \bmod 9 \neq 1$

$c=2)\ 14 \bmod 9 \neq 1$

$c=3)\ 21 \bmod 9 \neq 1$

$\boxed{c=4)}\ 28 \bmod 9 = 1$ ✓

$x \equiv 6.4 \bmod 9$

$x = 24 \bmod 9$

$\boxed{x_0 = 6}$

6) General sol^n eq^n is

$x_k = x_0 + k\left(\frac{n}{d}\right)$

$x_1 = 6 + 1\left(\frac{18}{2}\right) = 6 + 9 = \underline{15}$.

---

2) Solve $9x \equiv 12 \pmod{15}$

Sol^n $\gcd(9, 15) = 3$.

∴ The no of possible sol^n are 3.

The given congruence is equivalent to

$3x \equiv 4 \pmod 5$

$5 \mid 3x - 4$

$\Rightarrow 3x - 4 = 5k$

$\Rightarrow x = \frac{5k+4}{3}$

If $k=1$; $x = 3$

$x \equiv 3 \pmod 5$

The q.s is

$x_k = x_0 + k\left(\frac{m}{d}\right)$

$x_k = 3 + k\left(\frac{15}{3}\right)$

$x_k = 3 + 5k$

∴ $x = \underline{3, 8, 13}$.

* The chinese Remainder Theorem :—

The chinese Remainder Theorem (CRT) is used to solve a set of different Congruent equations with one variable but different moduli which are relatively prime as shown below:

$X \equiv a_1 \pmod{m_1}$; $X \equiv a_2 \pmod{m_2}$; $X \equiv a_3 \pmod{m_3}$

- - - - $X \equiv a_n \pmod{m_n}$.

CRT states that the above equations have a unique solution of the moduli are relatively prime.

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \text{- - - - -} + a_n M_n M_n^{-1}) \bmod M$$

1) Solve the following equations using CRT

$X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$

Soln: $X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

Given		To find		
$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$M_1^{-1} = 2$	$M = 105$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$M_2^{-1} = 1$	
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$M_3^{-1} = 1$	

$M = m_1 \times m_2 \times m_3 = 3 \times 5 \times 7 = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$; $M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$; $M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

$M_1 \times M_1^{-1} = 1 \bmod m_1$

↑ Multiplicative inverse

$35 \times M_1^{-1} = 1 \bmod 3$; $M_2 \times M_2^{-1} = 1 \bmod m_2$; $M_3 \times M_3^{-1} = 1 \bmod m_3$

By inspection, $M_1^{-1} = 1$ ✓ (Re-(1))

$21 \times M_2^{-1} = 1 \bmod 5$

$15 \times M_3^{-1} = 1 \bmod 7$

$35 \times 2 = 1 \bmod 3$

$21 \times 1 = 1 \bmod 5$

$15 \times 1 = 1 \bmod 7$

$M_1^{-1} = 2$

$M_2^{-1} = 1$

$M_3^{-1} = 1$.

$\therefore X = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$X = 233 \bmod 105$

$X = 23$.

$105) 233 (2$
210
23

---

2) Solve the following equations using CRT:

$4X \equiv 5 \pmod 9$

$2X \equiv 6 \pmod{20}$.

Soln: $4X \equiv 5 \pmod 9$; $2X \equiv 6 \pmod{20}$

$\div$ by $2^{2\times3}$

$X \equiv 3 \pmod{10}$

X^{th} by 4^{-1} on both sides.

$4^{-1} \times 4X \equiv 4^{-1} \times 5 \pmod 9$

$X \equiv 4^{-1} \pmod 9 \times 5 \pmod 9$

↑ multiplicative inverse

1 as the remainder

$X = 7 \times 5 \pmod 9$

$X \equiv 35 \pmod 9$

$X \equiv 8 \pmod 9$

$\therefore X \equiv 8 \pmod 9$

$X \equiv 3 \pmod{10}$

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_1^{-1})$

Given		To Find		
$a_1 = 8$	$m_1 = 9$	$M_1 = 10$	$M_1^{-1} = 1$	$M = 90$
$a_2 = 3$	$m_2 = 10$	$M_2 = 9$	$M_2^{-1} = 9$	

$M = m_1 \times m_2 = 9 \times 10 = 90$

$M_1 = \frac{M}{m_1} = \frac{90}{9} = 10$; $M_2 = \frac{M}{m_2} = \frac{90}{10} = 9$

$M_1 \times M_1^{-1} = 1 \bmod m_1$ | $M_2 \times M_2^{-1} \equiv 1 \bmod m_2$

$10 \times M_1^{-1} \equiv 1 \bmod 9$ | $9 \times M_2^{-1} \equiv 1 \bmod 10$

$10 \times 1 \equiv 1 \bmod 9$ | $9 \times 9 \equiv 1 \bmod 10$

$M_1^{-1} = 1$ | $M_2^{-1} = 9$

$\therefore X = (8 \times 20 \times 1 + 3 \times 9 \times 9) \bmod 180$

$X \equiv 403 \bmod 180.$

$X \equiv 43$

---

3) Solve the following equations using CRT:

$X \equiv 5 \pmod 3$

$X \equiv 2 \pmod 5$

$X \equiv 1 \pmod{11}$.

Soln : $X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$.

Given		To find		
$a_1 = 5$	$m_1 = 3$	$M_1 = 55$	$M_1^{-1} = 1$	$M = 165$
$a_2 = 2$	$m_2 = 5$	$M_2 = 33$	$M_2^{-1} = 2$	
$a_3 = 1$	$m_3 = 11$	$M_3 = 15$	$M_3^{-1} = 3$	

$M = m_1 \times m_2 \times m_3 = 3 \times 5 \times 11 = 165$

$M_1 = \frac{M}{m_1} = \frac{165}{3} = 55$; $M_2 = \frac{M}{m_2} = \frac{165}{5} = 33$; $M_3 = \frac{M}{m_3} = \frac{165}{11} = 15$

$M_1 \times M_1^{-1} \equiv 1 \bmod m_1$; $M_2 \times M_2^{-1} \equiv 1 \bmod m_2$; $M_3 \times M_3^{-1} \equiv 1 \bmod m_3$

$55 \times M_1^{-1} \equiv 1 \bmod 3$ | $33 \times M_2^{-1} \equiv 1 \bmod 5$ | $15 \times M_3^{-1} \equiv 1 \bmod m_3$

$55 \times 1 \equiv 1 \bmod 3$ | $33 \times 2 \equiv 1 \bmod 5$ | $15 \times 3 \equiv 1 \bmod 11$

$M_1^{-1} = 1$ | $M_2^{-1} = 2$ | $M_3^{-1} = 3$

$\therefore X = (5\times55\times1 + 2\times33\times2 + 1\times15\times3) \bmod 165$

$X = 452 \bmod 165$

$X = 122$

---

4) Solve $3^{302} \bmod 5005$ using CRT.

$M = 5005$

$M = 5\times7\times11\times13$.

$m_1 = 5,\ m_2 = 7,\ m_3 = 11,\ m_4 = 13$.

$M_1 = \frac{M}{m_1} = \frac{5005}{5} = 1001$; $M_2 = \frac{M}{m_2} = \frac{5005}{7} = 715$

$M_3 = \frac{M}{m_3} = \frac{5005}{11} = 455$; $M_4 = \frac{M}{m_4} = \frac{5005}{13} = 385$.

To find a_i values:

$a_i = 3^{302} \bmod m_i$.

$a_1 = 3^{302} \bmod m_1(5) = 4$.

$a_2 = 3^{302} \bmod 7 = 2$

$a_3 = 3^{302} \bmod 11 = 9$

$a_4 = 3^{302} \bmod 13 = 9$

$3^{302} \bmod 5 = 3^{60\times5+2} \bmod 5$

$= (3^5)^{60}.3^2 \bmod 5$

$= (3)^{60}.3^2 \bmod 5$ $(a^p \bmod p = a)$.

$= 3^{62} \bmod 5$

$= 3^{12\times5+2} \bmod 5$

5) 302 (60
300
2

(OR)

302 as multiple of 4

$= (3^5)^{12}.3^2 \bmod 5$

$= (3)^{12}.3^2 \bmod 5$

$= 3^{14} \bmod 5$

$= 3^{5\times2+4} \bmod 5$

$= (3^5)^2.3^4 \bmod 5$

$= 3^5 \bmod 5$

$= 3^{5\times1+1} \bmod 5$

$= (3^5)3 \bmod 5$

$= 3.3 \bmod 5 = 4$

$M_1 \times M_1^{-1} = 1 \bmod m_1$; $M_2 \times M_2^{-1} = 1 \bmod 7$; $M_3 \times M_3^{-1} = 1 \bmod 11$

$1001 \times M_1^{-1} \equiv 1 \bmod 5$ $\quad 715 \times M_2^{-1} \equiv 1 \bmod 7$ $\quad 455 \times M_3^{-1} = 1 \bmod 11$

$1001 \times 1 \equiv 1 \bmod 5$ $\quad 715 \times 1 = 1 \bmod 7$ $\quad 455 \times 3 = 1 \bmod 11$

$M_1^{-1} = 1$ $\quad M_2^{-1} = 1$ $\quad M_3^{-1} = 3$.

$M_4 \times M_4^{-1} \equiv 1 \bmod 13$

$385 \times M_4^{-1} \equiv 1 \bmod 13$

$385 \times 5 \equiv 1 \bmod 13$

$M_4^{-1} = 5$.

$\therefore X = (4 \times 1 \times 1001 + 2 \times 1 \times 715 + 9 \times 3 \times 455 + 5 \times 9 \times 385) \bmod 5005$

$X = 35044 \bmod 5005$

$X = 9$.

---

5) Solve the following equations using CRT

a) $x \equiv 3 \bmod 4$
$x \equiv 2 \bmod 3$
$x \equiv 4 \bmod 5$

b) $2x \equiv 6 \pmod{14} \div 2$.
$3x \equiv 9 \pmod{15} \div 3$
$5x \equiv 20 \pmod{60} \div 5$
$\gcd(2,14) = 2$.

---

6) Find a number having remainder 2, 3, 4, 5 when divided by 3, 4, 5, 6 respectively.

Soln:
$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 4$
$x \equiv 4 \pmod 5$
$x \equiv 5 \pmod 6$

Linear Diophantine Equation :-

An equation of the form $ax+by+c=0$ where $a\neq 0, b\neq 0$ and c is an integers is called a linear diophantine eq^n in two variables x & y.

Eg:- i) $8x+17y=7$ ii) $2x+3y=12$.

Solution of Linear Diophantine Equation :-

A pair (x_0, y_0) of integers is called a sol^n of linear Diophantine equation $ax+by=c$ if $ax_0+by_0=c$, and $(a,b)=d$.

then the general solution is given by

$$\boxed{x_1 = x_0 - \frac{b}{d}t \; ; \; y_1 = y_0 + \frac{a}{d}t}$$

---

1. Which of the following Diophantine Equation cannot be solved.

i) $6x+51y=22 \rightarrow (1)$

By Euclidean Algorithm.

$51 = 3+6\times 8$.

$6 = 0+3\times 2$.

gcd of $(6,51)=3$.

$3 \nmid 22$.

$\therefore$ eq^n (1) is not solvable.

6)51(8
48
3)6(2
6
0

---

ii) $33x+14y=115 \rightarrow (1)$

$33 = 5+14\times 2$

$14 = 4+5\times 2$

$5 = 1+4\times 1$

$4 = 0+1\times 4$

$\gcd(14,33)=1$ &

$1/115$

So, eqn (1) is solvable.

14) 33 (2
28
5) 14 (2
10
4) 5 (1
4
1) 4 (4
4
0

---

2. Determine all the solution in +ve integers of the linear Diophantine equation, $54x+21y=906$.

Sol^n:- Given L.D. eq^n

$54x+21y=906$.

By Euclidean Algorithm

$54 = 12+21\times 2$

$21 = 9+12\times 1$

$12 = 3+9\times 1$

$9 = 0+3\times 3$

$\gcd(21,54)=3$ &

$3/906$.

So, eq^n(1) is solvable.

21) 54 (2
42
12) 21 (1
12
9) 12 (1
9
3) 9 (3
9
0

---

3) Find the general sol^n of the eq^n

$70x + 112y = 168$.

Soln :- $\gcd(70, 112) =$

$112 = 70 \times 1 + 42$

$70 = 42 \times 1 + 28$

$42 = 28 \times 1 + 14$

$28 = 14 \times 2 + 0$.

$\therefore \gcd(70, 112) = 14$.

$70)112(1$
70
$42)70(1$
42
$28)42(1$
28
$14)28(2$
28
0

Now $14 / 168 = 12$.

$\therefore$ Linear Diophantine eq^n $70x + 112y = 168$ has a solution.

By reverse,

$14 = 42 - 28$

$= 42 - (70 - 42)$

$= 42 - 70 + 42$

$= 2(42) - 70$

$= 2(112 - 70) - 70$

$= 2(112) - 2(70) - 70$

$14 = 2(112) - 3(70)$

Multiply by 12.

$14(12) = (2(12)112 - 3(12)70$.

$168 = 24 \cdot 112 - 36 \cdot 70 \Rightarrow 168 = -36 \cdot 70 + 24 \cdot 112$

Thus $x_0 = 24$ & $y_0 = -36$ is a particular sol^n of the given eq^n.

The general sol^n is given by

$x_1 = x_0 + \frac{b}{d}t$ $\qquad$ $y_1 = y_0 - \frac{a}{d}t$

(put both +)

$x_1 = -36 + \left(\frac{112}{14}\right)t$; $y_1 = 24 - \left(\frac{70}{14}\right)t$

$x_1 = -36 + 8t$; $y_1 = 24 - 5t$.

Hence, $x_1 = -36 + 8t$ & $y_1 = 24 - 5t$, t is an integer.

---

4) $39x - 56y = 11$.

$56 = 39 \times 1 + 17$

$39 = 17 \times 2 + 5$

$17 = 5 \times 3 + 2$

$5 = 2 \times 2 + 1$

$2 = 1 \times 2 + 0$

39)56(1
39
17)39(2
34
5)17(3
15
2)5(2
4
1)2(2
2
0

Hence gcd(39, 56) = 1

Now $1 / 11 = \underline{11}$.

∴ Linear Diophantine eqⁿ $39x - 56y = 11$ has a solution.

By reverse,

$1 = 5 - 2(2)$

$1 = 5 - 2(17 - 3(5))$

$1 = 5 - 2(17) + 6(5)$

$1 = 7(5) - 2(17)$

$1 = 7(39 - 2(17)) - 2(17)$

$1 = 7(39) - 14(17) - 2(17)$

$1 = 7(39) - 16(17)$

$1 = 7(39) - 16(56 - 1(39))$

$1 = 7(39) - 16(56) + 16(39)$

$1 = 23(39) - 16(56)$

Multiply by 11

$1.(11) = 23(11)(39) - 16(11)(56)$

$11 = \frac{253}{x_0}(39) - \frac{176}{y_0}(56)$.

Thus $x_0 = 253$, $y_0 = 176$. is a particular sol^n of the given eq^n.

Its general sol^n is

$x_1 = x_0 + \frac{b}{d}t$; $y_1 = y_0 - \frac{a}{d}t$ (put both +)

$x_1 = 253 + (-\frac{56}{1})t$; $y_1 = 176 - (\frac{39}{1})t$

$x_1 = 253 - 56t$; $y_1 = 176 - 39t$

Hence $x_1 = 253 - 56t$ & $y_1 = 176 - 39t$;

t is an integer.

---

5) Solve: $7x + 13y = 208$. $x_0 = -1040$; $y_0 = 416$

6) Solve: $56x + 72y = 40$. $x_0 = 20$; $y_0 = -15$

7) Solve: $172x + 20y = 1000$.

---

8) A certain number of sixes and nines is added a sum of 126. if the number of sixes and is interchanged, the new sum is 114. How many each were there originally?

Soln:- Let x be no of sixes

y be no of nines.

$6x + 9y = 126$.

$9x + 6y = 114$.

$9 = 3 + 6 \times 1$

$6 = 0 + 3 \times 2$

$\uparrow$

$\gcd(6, 9) = 3$.

$3 \mid 126 = \underline{42}$.

6) 9 (1
6
3) 6 (2
6
0

Reverse.

$3 = 9 - 6 \times 1$

$3 = 6(-1) + 9(1)$

$3 \cdot 42 = 6((-1)(42)) + 9((1)(42))$

$126 = 6(-42) + 9(42)$

$x = -42 + 3t \geq 0$ $\quad y = 42 - 2t \geq 0$.

$3t \geq 42$ $\quad -2t > -42$

$t \geq 14$ $\quad 2t < 42$

$t < 21$.

$14 < t < 21$.

$x = x_0 + y_d t$ $\quad y = y_0 - x_d t$

$x = 3t$ $\quad y = 14 - 2t$.

t	x	y
14	0	14

Initial value

To Find the value of t S.T

$6y + 9x = 114$.

$6(14 - 2t) + 9(3t) = 114$.

$15t - 30 = 0$

$15t = 30$

$t = 2$.

$x_0 = 3t$ $\quad y_0 = 14 - 2t$

$x_0 = 6$ $\quad y_0 = 10$.

RSA Algorithm:-

↓

Ron Rivest, Adi Shamir and Leonard Adleman in 1978.

It is an asymmetric cryptographic algorithm.
(2 keys) i.e public and private key

Public key → Known to all users in N/W.
Private Key → Kept secret, not shareable to all.

If public key of user A is used for encryption, we have to use the private key of some user for decryption.

The RSA scheme is a block cipher (→ Secret code) in which the plain text and ciphertext are integers b/w 0 and n-1 for some value n.

---

1. Key Generation: [RSA ALGORITHM]

i) Select 2 large prime numbers 'P' and 'q'.

ii) Calculate $n = P * q$.

iii) Calculate $\phi(n) = (p-1) * (q-1)$ // Euler's toitient function.

iv) choose value of e

$1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$.

v) calculate

$d = e^{-1} \bmod \phi(n)$.

$ed = 1 \bmod \phi(n)$.

vi) Public key = $\{e, n\}$

vii) Private key = $\{d, n\}$.

2. Encryption.

$C = M^e \bmod n$.

plaintext = $M < n$.
C → Ciphertext.

3. Decryption

$M = C^d \bmod n$

Problems:-

1: Using RSA algorithm find public key and Private key w.r.to $p = 3$, $q = 11$ and $M = 31$

Soln: Let $p = 3$, $q = 11$

$n = p * q = 3 * 11 = 33$

$\phi(n) = (p-1) * (q-1) = 2 * 10 = 20$.

so, let $e = 7$ as $1 < 7 < 20$ & $\gcd(7, 20) = 1$

Now $d = e^{-1} \bmod \phi(n)$.

$de \equiv 1 \bmod \phi(n)$.

$7 * d \equiv 1 \bmod 20$. (Solve by using Euclidean Algorithm also)

$\therefore d = 3$

Since $e = 7$, $d = 3$

Public Key = $\{e, n\} = \{7, 33\}$

Private Key = $\{d, n\} = \{3, 33\}$.

Encryption: $C = M^e \bmod n$ Let $M = 31$.

$C = 31^7 \bmod 33$

$31 \equiv -2 \bmod 33$

$(31)^7 \equiv (-2)^7 \bmod 33$

$(31)^7 \equiv -128 \pmod{33}$

$(31)^7 \equiv -(-4) \bmod 33$

$(31)^7 \equiv 4 \pmod{33}$ [A B C D E - - - - 26 → 0 1 2 3 4]

$\Rightarrow C = 04 = AE$.

$\Rightarrow M = 31 = DB$ (plaintext) $\Rightarrow C = 04 = AE$ (ciphertext).

Decryption:

$M = c^d \bmod n$.

$M = 4^3 \bmod 33$

$4^3 \equiv 64 \bmod 33$

$M \equiv 31 \bmod 33$.

$\therefore M = 31 = DB$.

---

2) In RSA algorithm if $p = 7$, $q = 11$ and $e = 13$ then what will be the value of d?

Soln: $p = 7$, $q = 11$

$n = pq = 7 \times 11 = 77$.

$\phi(n) = (p-1)(q-1) = 6 \times 10 = 60$.

Given $e = 13$.

$\Rightarrow 1 < 13 < 60$; $\gcd(60, 13) = 1$.

To find d:

$d \equiv e^{-1} \bmod (\phi(n))$.

$ed \equiv 1 \bmod (\phi(n))$

$13d \equiv 1 \bmod 60$.

$\Rightarrow 60 \mid 13d - 1 \Rightarrow 13d - 1 = 60K$

$\Rightarrow d = \frac{60K + 1}{13}$.

If $K = 8$, $d = 37$.

$\therefore$ public key = $\{e, n\} = \{13, 77\}$

Private key = $\{d, n\} = \{37, 77\}$.

---

3) Encode STOP using RSA algorithm with key $(n, e) = (2537, 13)$ and $P=43$, $q=59$.

Public key

Soln:- $P=43$, $q=59$.

$n = Pq = 2537$.

$\phi(n) = (P-1)(q-1) = 42 \times 58 = 2436$.

Given $e=13$, $1 < e < 2436 \Rightarrow 1 < 13 < 2436$.

$\therefore \gcd(2436, 13) = 1$.

$M = \text{STOP} = 18191415$ (0 1 2 3 4 5 / A B C D E F ----)

Let $M_1 = 1819$ $M_2 = 1415$.

Encryption:

$C = M^e \bmod n$

$C_1 = M_1^e \bmod n \Rightarrow C_1 = (1819)^{13} \bmod 2537$.

$(1819)^2 \equiv 3308761$.

$C_1 = 2081$

$C_2 = M_2^e \bmod n \Rightarrow C_2 = (1415)^{13} \bmod 2537$.

$C_2 = 2182$.

$C = C_1 C_2 = 20812182$

$C = UHBYHC$.

4) If $p=3$, $q=11$ and private key $d=7$ find the public key using RSA algorithm and hence encrypt the number 19.

Soln: $n = p \times q = 33$, $d = 7$.

$\phi(n) = (p-1)*(q-1) = 2*10 = 20$.

To find e:

$1 < e < \phi(n)$

$\Rightarrow 1 < e < 20$.

$\Rightarrow \gcd[e, 20] = 1$

W.K.T $ed \equiv 1 \pmod{\phi(n)}$

$7e \equiv 1 \pmod{20}$

$\Rightarrow 20 / 7e-1$

$\Rightarrow 7e-1 = 20K$.

$\Rightarrow e = \frac{20K+1}{7}$

$\Rightarrow \underline{e=3}$

Given $M = 19 = BJ$.

Encryption: $C = M^e \bmod n$.

$C = 19^3 \bmod 33$.

$C = -2 \times 19 \bmod 33$ $(\because 19^2 \equiv -2 \pmod{33})$

$C = -38 \bmod 33 \equiv -5 \bmod 33$

$C = 28 \bmod 33$

$\therefore C = 28 = CI$

5) Using RSA Algorithm decrypt 09810461 using d=937 and p=43, q=59.

Soln: $n = p*q = 43*59 = 2537$.

$\phi(n) = 42*58 = 2436$.

$C = \underline{0981}\,\underline{0461}$

$C_1 = 0981 \quad C_2 = 0461$.

∴ Required plain text is

$M = C^d \pmod n$

$M_1 = C_1^{937} \pmod{2537}$

$M_1 = (0981)^{937} \pmod{2537}$

$M_1 = 0704$.

$M_2 = C_2^d \pmod{2537}$

$M_2 = (0461)^{937} \pmod{2537}$

$M_2 = 1115$

$M = \underline{07}\,\underline{04}\,\underline{11}\,\underline{15}$

$M = \underline{HELP}$.

** To find powers in Calculator.

Eg:- $5^7 \bmod 33 = 14$

$5\times5\times5\times5\times5\times5\times5 = 78{,}125 \div 33$

$= \underline{2367}.424242 - 2367$

$= 0.424242 \times 33$

$= 13.999$

$= \underline{14}$.