Mathematical and Statistical Foundations

UNIT-1

Greatest common Divisors and prime factorization

1.1 Objectives:

- To Understand the greatest common divisor and identify the greatest common divisor using prime factorization.
- To Identify the common factors, greatest common factor, common multipliers.
- To Apply the Euclidean Algorithm and compute the Gcd of two or larger integers.
- To Understands the Fundamental Theorem of arithmetic.
- To Understand the concept of Fermat Numbers.
- To Understands the concept of Congruence and use various results related to Congruence including the Chinese Remainder Theorem.

1.2 Introduction to Greatest common Divisors:

This chapter continues to deal with divisibility in Number Theory. we begin exploring the common factors of two or more positive integers. Explain what it means to say that a non-zero integers 'a'

divides an integer b. Remember That we use the notation a/b to indicate that the non zero integer 'a' divides The integer 'b'. Let 'a' and 'b' are integers with a≠0. That is to say That 'a' does not divide b. we establish The fundamental Theorem of arithmetic, one of the fundamental results in number Theory. Then we can turn to the common multiples of two or more positive integers. Some positive integers have exactly two positive factors and some have more than two. prime factorization is a process of factoring a number interms of prime numbers. prime factorization is finding which prime numbers multiply together to make The original number. It would be pretty difficult to perform prime factorization. The prime number is number that can only be divided by '1' and itself. The method of prime factorization is used to break down (or) express a given number as a product of prime numbers. The Greatest common

divisor (GCD) of two non-zero integers 'a' and 'b' is the greatest positive integers 'd' such that 'd' is a divisor of both 'a' and 'b'; That is There are integers 'e' and 'f' such that $a=de$ and $b=df$, and 'd' is the largest such integers. The GCD of 'a' and 'b' is generally denoted by $gcd(a,b)$. This definition also applies when one of 'a' and 'b' is zero. In this case, the GCD is the absolute value of the non-zero integers that is

$$gcd(a,0) = gcd(0,a) = |a|.$$

This case is important as the terminating step the Euclidean algorithm.

1.21 Peano's Axioms:

The basic mathematical system is the set N of positive integers. The positive integers can be defined by a set of axioms, are known as peano's axioms. In this we have three axioms that are

Axiom-I : There exists a natural number '1' i.e $n \in N$

Axiom-II : There exist an injective mapping $f: N \to N$.

If $n \in N$, Then $f(n) = n+1$ is said to be successor of n.

Axiom-III : There exist no $n \in N$ such that $f(n) = 1$

where Axiom-I gives that N is non-empty.

Axiom-II gives that $f(m) = f(n) \Rightarrow m = n$.

Axiom-III state that the natural number '1' is a non-successor.

1.22 Basic properties of Integers:

we denote the set of positive integers by N and the set of integers by Z.

i.e $N = \{1, 2, 3 \cdots\}$ & $Z = \{\cdots, -2, -1, 0, 1, 2, 3 \cdots\}$

The simple rules associated with addition and multiplication of these integers are given below.

- Commutative laws: For all $a, b \in \mathbb{Z}$ Then

$$a+b = b+a,$$

$$a \cdot b = b \cdot a$$

- Associative laws: For all $a, b, c \in \mathbb{Z}$ then

$$a+(b+c) = (a+b)+c,$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

- Additive inverse: For each integer 'a', $\exists$ an integer $-a$ s.t $a+(-a) = 0 = (-a)+a$. The integer '$-a$' is called the additive inverse of a.

- Identity elements: $\forall\ a \in \mathbb{Z}$ then $a+0 = a = 0+a$

$$a \cdot 1 = a = 1 \cdot a$$

Here the element '0' is called the additive identity and the element '1' is called the multiplicative identity

- Distribution laws: $\forall\ a, b, c \in \mathbb{Z}$ then

$$a \cdot (b+c) = a \cdot b + a \cdot c,$$

$$(b+c) \cdot a = b \cdot a + c \cdot a$$

- Well-ordering principle: Any non-empty subset of non-negative integers has a least element.
i.e If 'S' is a non-empty subset of non-negative integers Then $\exists\ n \in S$ s.t $n \leq m$ for all $m \in S$.

Divisibility: Let 'a' and 'b' be two integers with $a \neq 0$. If there exists an integer 'x' s.t $b = ax$, then 'a' is said to divide 'b' (or) 'b' is divisible by a. and it is denoted by the notation a/b.

when a divides b, then 'a' is called a divisor of 'b' (or) factor of 'b' and 'b' is called a multiple of a.

if 'b' is not divisible by 'a', then we use the notation $a \times b$. Ex: 99 is divisible by 11, since $99 = 11 \times 9$.

Note: when a divides b, then $-a$ also divides b, since $b = ax = (-a)(-x)$.

1.2.3 Division theorem (or) division algorithm:

Theorem: Let 'a' and 'b' be any two integers, $b > 0$. Then $\exists$ unique integers q and r such that $a = bq + r$, $0 \leq r < b$.

If $a \times b$, then 'r' satisfies the stronger inequalities $0 < r < b$.

proof:- consider an ~~infinite~~ infinite sequence of multiples of b, namely, $\cdots, -2b, -b, 0, b, 2b, 3b \cdots$

clearly $a = qb$ (or) $qb < a < (q+1)b$ for some q.

i.e 'a' is equal to one of the multiples of b say qb in

The sequence then qb and $(q+1)b$.

[It lies b/w two consecutive multiples]

In either case we have $qb \le a < (q+1)b$, for some q.

$$\Rightarrow \quad 0 \le a - qb < b \rightarrow (1)$$

Let $r = a - qb \Rightarrow$ [illegible], $(\because 0 \le r < b)$

$$\Rightarrow a = qb + a - qb \Rightarrow a = ab + r$$

This proves the existence of two integers q and r.

To prove the uniqueness of q and r let us assume that a can be expressed in the given form in two ways (i) Let $a = q_1 b + r_1$, $0 \le r_1 < b \rightarrow (2)$ and

$$a = q_2 b + r_2, \quad 0 \le r_2 < b \rightarrow (3)$$

For some integers q_1, r_1, q_2 and r_2.

from (2) & (3) we have $q_1 b + r_1 = q_2 b + r_2$

$$r_1 - r_2 = (q_2 - q_1) b \rightarrow (4)$$

$\Rightarrow$ Here 'b' divides $r_1 - r_2$

which is a contradiction since both r_1 and r_2 are positive and less than 'b'. Hence $r_1 = r_2$ and also $q_1 = q_2$

$\therefore$ 'q' and 'r' are unique.

Note:

(i) When 'a' is divided by b, the integer 'q' is called the quotient and the integer 'r' is called the remainder.

(ii) When $r=0$, then $a=qb$ and hence 'a' is a multiple of 'b'.

(iii) When b is any integer, the above result can be stated as $a=qb+r$, where $0 \le r < |b|$.

(iv) qb is the largest multiple of 'b' which does not exceed 'a'.

Ex:- Let $a=21$, $b=5$ Then $21 = 4\times5+1$, $0<1<5$.

Here 4×5 is the largest multiple of '5' which does not exceed 21: 1 is the remainder of 21 when divided by 5; '4' is the quotient.

Greatest common Divisor:

Greatest common divisor is another concept related to integers. The greatest common divisor of two integers 'a' and 'b', not both zero, is the largest positive integer that divides both 'a' and 'b'; it is denoted by (a,b).

Consider the integers 12 and 18. Now 2/12 and 2/18; 3/12 and 3/18; and 6/12 and 6/18

i.e The integers 12 and 18 are divisible by 2, 3 and 6. Then The integers 2, 3 and 6 are called The common divisors of 12 and 18.

- Definition of common divisor: A non-zero integer 'd' is said to be a common divisor of integers 'a' and 'b' if d/a and d/b.

For example, The integers 2, 3 and 6 divides both 12 & 18.
Hence 2, 3, 6 are called common divisors of 12 and 18.
However, 6 is The largest positive integer That divides both 12 and 18. such integer is called a greatest common divisor.

- Definition of Greatest common divisor: A non-zero integer 'd' is said to be a greatest common divisor(gcd) of 'a' and 'b' (i) if 'd' is a common divisor of a & b; and (ii) if 'c' is a common divisor of 'a' and 'b', Then 'c' is a divisor of d,

In other-words, if 'd' is the largest of all common divisors, then 'd' is called the greatest common divisor of a & b and it is denoted by gcd(a,b).

(1) Ex:- Find the Greatest common divisor of the integers 12 and 14.

Sol: Here the divisors of '12' are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$, and the divisors of 14 are $\pm 1, \pm 2, \pm 7, \pm 14$.

∴ The common divisors of 12 and 14 are $\pm 1, \pm 2$.

Hence the greatest common divisor is '2'.

i.e $\gcd(12,14) = 2$.

(2) Ex:- Find the greatest common divisor of 8 and 12

Sol Here the divisors of '8' are $\pm 1, \pm 2, \pm 4 \pm 8$

and the divisors of '12' are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$

∴ The common divisors of 8 and 12 are $\pm 1, \pm 2, \pm 4$.

Hence the greatest common divisor is '4'.

∴ $\gcd(8,12) = 4$.

Note:- ① A positive integers $p>1$ is called prime, if The. only positive integers that divide p are p and 1. If +ve integers $m>1$ is not prime, then 'm' is said to be composite.

② The positive integers '1' is neither prime nor composite.

③ The positive integers 'm' is composite, if ∃ +ve integers 'a and b' s.t $m=ab$, where $a>1$ & $b<m$.

Ex:- The integers 2, 3, 5, 7, 11, 13 and 17 are prime, whereas the integers 4, 6, 9, 10 and 15 are composite,

since $4=2\times2$, $6=2\times3$, $9=3\times3$, $10=2\times5$ and $15=3\times5$.

- Relatively prime integers: If $\gcd(a,b)=1$, then 'a and b' are said to be relatively prime. (or) co-prime. (or) each is said to be prime to other.

If $\gcd(a_1, a_2, a_3 \ldots a_n)=1$, then the integers $a_1, a_2 \ldots a_n$ are said to be pairwise relatively prime. i.e $a_1, a_2 \ldots a_n$ are relatively prime in pairs if $\gcd(a_i, a_j)=1$ for $1\le i<j\le n$.

Ex:- Find wheather the integers 9, 13, 85, 92 are pairwise relatively prime (or) not.

Sol Given integers 9, 13, 85, 92.

$\gcd(9,13)=1$, $\gcd(13,85)=1$

$\gcd(9,85)=1$, $\gcd(13,92)=1$

$\gcd(9,92)=1$, $\gcd(85,92)=1$

∴ The integers 9, 13, 85, 92 are pairwise relatively prime.

(2) Consider the integers 6, 10, 17.

$\gcd(6,10,17)=1$ But $\gcd(6,10)=2\neq 1$

∴ The integers 6, 10, 17 are not pairwise relatively prime.

Note:- The greatest common divisor is unique.

- Linear combination: A linear combination of the integers 'a' and 'b', that is a sum of the form $\alpha a+\beta b$, where α and β are integers.

For example, $2\cdot 3+5\cdot 7$ is linear combination of 3 and 7.

So is $(-4)\cdot 3 + 0\cdot 7$. its proof is an elegant application of the well-ordering principle.

Note: gcd of the +ve integers 'a' and 'b' is a linear combination of 'a' and 'b'.

② Two positive integers 'a' and 'b' are relatively prime if and only if there are integers 'α' and 'β' s.t $\alpha a + \beta b = 1$

③ Let a, b and c be any +ve integers. Then $(ac, bc) = c(a,b)$.

① Example: Express the gcd of 28 and 12 as a linear combination of their gcd.

Sol: gcd of (12, 28) are 4

i.e The divisor's of 12 is $\pm 1, \pm 2, \pm 4, \pm 6, \pm 12$

The divisor's of 28 is $\pm 1, \pm 2, \pm 4, \pm 7$.

∴ The greatest common divisor of $(28, 12) = 4$

Next we need to find integers 'α' and 'β' such that

$\alpha \cdot 28 + \beta \cdot 12 = 4$ By trial and error, $\alpha = 1$ & $\beta = -2$

Work $1 \cdot 28 + (-2)12 = 4$.

Note That the values of 'α' and 'β' in the linear combination need not be unique. For instance in this example, you may remember that $(-5)\cdot 28 - 12 \times 12 = 4$

Ex② Find the gcd of (a) (12, 18, 28) (b) (15, 28, 50)

Sol (a) divisor's of 12 are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$

divisor's of 18 are $\pm 1, \pm 2, \pm 3, \pm 6 \pm 9, \pm 18$

divisor's of 28 are $\pm 1, \pm 2, \pm 4 \pm 7, \pm 14, \pm 28$

∴ The greatest common divisor of (12, 18, 28) is = 2

∴ gcd(12, 18, 28) = 2

(b) divisors of 15 are $\pm 1, \pm 3, \pm 5, \pm 15$

divisor's of 28 are $\pm 1, \pm 2, \pm 4, \pm 7, \pm 14, \pm 28$

divisor's of 50 are $\pm 1, \pm 2, \pm 5, \pm 10, \pm 50$.

∴ The greatest common divisors of (15, 28, 50) is 1

∴ The Largest common factor of 15, 28, 50 is 1.

i.e gcd (15, 28, 50) = 1.

Note: one way to find the such linear combination is by using trial error method i.e especially when a, & b are small.

3) Express the gcd of each pair as a linear combination of the numbers (i) 24, 28 (ii) 15, 28

i) Sol: Given numbers 24, 28

The divisor's of 24 is $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24$

The divisor's of 28 is $\pm 1, \pm 2, \pm 4 \pm 7 \pm 14 \pm 28$

∴ The greatest common divisor of $(24, 28) = 4$

Next we need to find the integers α and β such that

$$\alpha \cdot 24 + \beta \cdot 28 = 4$$

By trial and error, $\alpha = -1$ & $\beta = 1$

$$\therefore (-1)\, 24 + 1\,(28) = 4$$

∴ The values of α and β in the linear combination need not be unique.

(ii) 15, 18 left for student exercise.

- Gcd of 'n' positive integers :- The gcd of 'n' positive integers $a_1, a_2, \ldots a_n$ is the largest +ve integer that divides each a_i. It is denoted by $(a_1, a_2, \ldots a_n)$.

A linear combination of 'n' positive integers:

A linear combination of 'n' +ve integers $a_1, a_2 \cdots a_n$ is a sum of the form $\alpha_1 a_1 + \alpha_2 a_2 + \alpha_3 a_3 + \cdots + \alpha_n a_n$, where $\alpha_1, \alpha_2 \cdots \alpha_n$ are integers.

Note: ① The gcd of the +ve integers $a_1, a_2 \cdots a_n$ is the least +ve integer that is a linear combination of $a_1, a_2, \cdots a_n$.

① Ex:- Express (12, 15, 21) as a linear combination of 12, 15 & 21

Sol First find gcd (12, 15, 21)

The divisor's of 12 are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$

The divisor's of 15 are $\pm 1, \pm 3, \pm 5, \pm 15$

The divisor's of 21 are $\pm 1, \pm 3, \pm 7, \pm 21$

$\therefore$ The gcd (12, 15, 21) = 3

Now to find the integers α, β & γ

By trial error method (for small +ve integers) s.t

$\alpha \cdot 12 + \beta \cdot 15 + \gamma \cdot 21 = 3$

$(-1)\, 12 + 1\,(15) + 0\,(21) = 3$

$\therefore \alpha = -1, \beta = 1$ & $\gamma = 0$ is such a combination of 12, 15, 21.

(2) Express the gcd of the given numbers as a linear combination of the numbers: (a) 15, 18, 24 (b) 12, 18, 20, 24

Sol (a) First find the gcd of 15, 18, 24

The divisors of 15 are $\pm 1, \pm 3, \pm 5, \pm 15$

The divisors of 18 are $\pm 1, \pm 3, \pm 6, \pm 9, \pm 18$

The divisors of 24 are $\pm 1, \pm 3, \pm 4 \pm 6 \pm 12 \pm 24$

$\therefore$ The gcd $(15, 18, 24) = 3$

Now to find the integers α, β & γ

By trial error method we have

$$\alpha \cdot 15 + \beta \cdot 18 + \gamma 24 = 3$$

Put

$\alpha = -1, \beta = 1$ & $\gamma = 0$

$\therefore (-1)\,15 + (1)(18) + 0 \times 24 = 3$

Hence $\alpha = -1, \beta = 1$ & $\gamma = 0$ are such combination of 15, 18, 24.

b) First find the gcd of 12, 18, 20 & 24.

The divisors of 12 are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6 \pm 12$

The divisors of 18 are $\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18$

The divisors of 20 are $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20$

The divisors of 24 are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm 24$

$\therefore$ The gcd of $(12, 18, 20, 24) = 2$

Now to find the integers of α, β, γ & μ

By trial error method we have

$$\alpha \cdot 12 + \beta \cdot 18 + \gamma \cdot 20 + \mu \cdot 24 = 2$$

Put $\alpha = 0, \beta = -1, \gamma = 1$ & $\mu = 0$ then

$$0 \times 12 + (-1)18 + 1 \times 20 + 0(24) = 2$$

Hence $\alpha = 0, \beta = -1, \gamma = 1$ & $\mu = 0$ are the linear combinati

of 12, 18, 20 & 24.

③ Express the gcd of the given numbers as a linear combination of the numbers (or) not

(i) ⓐ (12, 18, 28) ⓑ (12, 36, 60, 108) and ⓒ (15, 28, 50)

Sol ⓐ The largest positive integer that divides 12, 18 and 28 is 2

so $(12, 18, 28) = 2$. i.e $\gcd(12, 18, 28) = 2$

in this no linear combination

ⓑ 12 is the largest factor of 12 and 12 is a factor of 12, 36, 60 and 108;

Then the $\gcd(12, 36, 60, 108) = 12$.

∴ The linear combination 12, 36, 60, 108 are $\alpha = 1, \beta = 0, \gamma = 0$ & $\delta = 0$

ⓒ we have the largest common factor of 15, 28, 50 is 1 Then $(15, 28, 50) = 1$

∴ $\gcd(15, 28, 50) = 1$

Then is no linear combination

1.3 Euclidean Algorithm for finding the GCD:-

There are several procedures for finding gcd of two positive integers.

An efficient method for finding the greatest common divisor of two integers based on the quotient and remainder technique is called the Euclidean algorithm. The following Theorem provides the key to this algorithm.

Theorem: If $a = qb + r$, where a, b, q and r are integers, then $gcd(a, b) = gcd(b, r)$

proof:- Consider $a = qb + r$ where a, b, q, r are integers

Let $d_1 = gcd(a, b) \rightarrow ①$ and $d_2 = gcd(b, r) \rightarrow ②$

Now, $d_1 = gcd(a, b)$

$\Rightarrow$ d_1 divides both 'a' and b.

d_1 also divides $r = a - bq$ also

Hence any common divisor of 'a' and 'b' is also a common divisor of b and r.

Since $d_2 = \gcd(b, r)$,

we have $d_1 \leq d_2 \rightarrow (3)$

Ily, $d_2 = \gcd(b, r)$

$\Rightarrow$ d_2 divides both 'b' and 'r'.

$\Rightarrow$ d_2 also divides $a = bq + r$.

Hence any common divisor of 'b' and 'r' is also common divisor of 'a' and 'b'. Since $d_1 = \gcd(a, b)$,

we have $d_2 \leq d_1 \rightarrow (4)$

from eqn (3) & (4) we get

$$d_1 = d_2$$

$\therefore$ $\gcd(a, b) = \gcd(b, r)$ ($\because$ from (1) & (2))

- Theorem :- when 'a' and 'b' any two integers such that $a \geq b > 0$, if r_1 is the remainder when 'a' is divided by b, r_2 is the remainder when 'b' is divided by r_1, r_3 is the remainder when r_1 is divided by r_2 and so on and if $r_{n+1} = 0$, Then the last non-zero

remainder r_n is the gcd (a,b).

Proof :- Let 'a' and 'b' be any two integers s.t $a > b > 0$.

By the division algorithm, $\exists$ integers q_1 and r_1 s.t

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b.$$

Now consider 'b' and r_1. Suppose $r_1 \neq 0$, Then by the division algorithm, $\exists$ integers q_2 and r_2 s.t

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1$$

Next consider r_1 and r_2. If $r_2 \neq 0$, Then the divison algorithm, $\exists$ integers q_3 and r_3 such that

$$r_1 = q_3 r_2 + r_3, \quad 0 \leq r_3 < r_2.$$

Continuing this process we get $a = bq_1 + r_1, \quad 0 \leq r_1 < b$

If $r_1 \neq 0$, divide b by r_1 : $b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1$

If $r_2 \neq 0$, divide r_1 by r_2 : $r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2$

If $r_3 \neq 0$, divide r_2 by r_1 : $r_2 = r_3 q_4 + r_4, \quad 0 \leq r_4 < r_3$

If $r_{n-1} \neq 0$, divides r_{n-2} by r_{n-1} : $r_{n-2} = r_{n-1} q_n + r_n$,

$0 \leq r_n < r_{n-1}$

If $r_n \neq 0$, divide r_{n-1} by r_n: $r_{n-1} = r_n q_{n+1} r_{n+1}$,

$0 \leq r_{n+1} < r_n$

Since $r_1, r_2, r_3 \cdots$ form a decreasing set of non-negative integers, there must exist an r_{n+1} equal to zero.

By the above Theorem we have

$$gcd(a,b) = gcd(b,r_1) = gcd(r_1, r_2) \cdots = gcd(r_1,r_2) \cdots$$
$$= gcd(r_{n-1}, r_n) = gcd(r_n, 0) = r_n.$$

Hence the greatest common divisor of 'a' and 'b' is r_n, which is the last non-zero remainder.

- Theorem :- $gcd(a,b)$ can be expressed as an integral linear combination of 'a' and b.

  i.e $gcd(a,b) = ua + vb$, where 'u' and 'v' are integers.

Proof :- Euclid's algorithm can also be used to express $gcd(a,b) = x$ in the form $x = ua + vb$, where u and v are integers.

By The Euclidean Algorithm we have

$$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 \le r_n < r_{n-1}$$

$$r_n = r_{n-2} + (-q_n) r_{n-1}$$

$$= r_{n-2} + (-q_n)(r_{n-3} + (-q_{n-1}) r_{n-2})$$

in similar way

$$= r_{n-3}(-q_n) + r_{n-2} + q_n q_{n-1} r_{n-2}$$

$$= r_{n-3}(-q_n) + (r_{n-2})(1 + q_{n-1} \times q_n)$$

Here substitute $r_{n-4} + (-q_{n-2}) r_{n-3}$ for r_{n-2} and

Continue The process until we reach $r_n = ua + vb$

for some integers u and v.

• Examples:

1) Use The Euclidean algorithm to find The gcd of 42823 and 6409.

Sol Here $42823 > 6409$

Applying The division algorithm repeatedly

$$42823 = 6 \times 6409 + 4369$$

$$6409 = 1 \times 4369 + 2040$$

$$4369 = 2 \times 2040 + 289$$

$$2040 = 7 \times 289 + 17$$

$$289 = 17 \times 17 + 0$$

Since the last non-zero remainder is 17,

$$\gcd(42823, 6409) = 17$$

2) Apply Euclidean Algorithm to find the gcd of 4076, 1024.

Sol By the successive application of the division algorithm, we get

$$4076 = 3 \times 1024 + 1004$$

$$1024 = 1 \times 1004 + 20$$

$$1004 = 50 \times 20 + 4 \leftarrow \text{last non-zero remainder}$$

$$20 = 5 \times 4 + 0$$

Since the last non-zero remainder is 4

$$\therefore \gcd(4076, 1024) = 4.$$

3) Find the gcd of 615 and 1080, and find the integers u and v such that $\gcd(615, 1080) = 615u + 1080v$

Sol: By the division algorithm, we get ($\because 615 > 1080$)

$$1080 = 1 \times 615 + 465$$

$$615 = 1 \times 465 + 150$$

$465 = 3 \times 150 + 15$ ← last non-zero remainder

$150 = 10 \times 15 + 0$ ← zero remainder

Since the last non-zero remainder is 15,

$\therefore \gcd(615, 1080) = 15.$

Now $465 = 1080 - 1 \times 615 \rightarrow (1)$

$150 = 615 - 1 \times 465$

$= 615 - 1 \times (1080 - 1 \times 615)$

$= 2 \times 615 - 1 \times 1080$ and

Also $15 = 465 - 3 \times 150$

$= 465 - 3(2 \times 615 - 1 \times 1080)$

$= (1080 - 1 \times 615) - 3(2 \times 615 - 1 \times 1080)$

↓ from (1)

$= (-7)\,615 + 4 \times 1080$

$= 615\,u + 1080\,v$

Thus $u = -7$ and $v = 4$

(or)

we can also determine another way.

$15 = 465 - 3 \times 150$

$= 465 - 3 \times (615 - 1 \times 465)$

$= 4 \times 465 - 3 \times 615$

$= 4(1080 - 1 \times 615) - 3 \times 615$

$= 615(-7) + 1080 \times 4$

Hence $u = -7$ and $v = 4$.

Note: The Necessary and sufficient condition for $\gcd(a,b) = 1$ is the existence of integers u and v such that $au + bv = 1$

Explanation:- If $\gcd(a,b) = 1$, Then $au + bv = 1$

The converse is true. for Example, $5 \cdot 5 + 8(-3) = 1$

(i.e $au + bv = 1$)

Here $u = 5$ & $v = -3$

$$\gcd(5, 8) = 1$$

i.e divisor of 5 is $\pm 1, \pm 5$

divisor of 8 is $\pm 1, \pm 2, \pm 4, \pm 8$

$\therefore$ The greatest common divisor is 1.

1.3.1 Properties of The Greatest common divisor:-

① Show that

If $\gcd(a,b) = 1$ and $\gcd(a,c) = 1$, Then $\gcd(a, bc) = 1$.

i.e If a and b are co-prime and a and c are co-prime, Then a and b are co-prime.

Proof:- Let $\gcd(a,b) = 1$

There exists integers u_1 and v_1 such that

$u_1 a + v_1 b = 1 \rightarrow (1)$

also $\gcd(a,c) = 1$ $\exists$ integers u_2 and v_2 such that

$u_2 a + v_2 c = 1 \rightarrow (2)$

from eqn (1) & (2) we have

$(u_1 a + v_1 b)(u_2 a + v_2 c) = 1$

$(u_1 u_2 a + u_1 v_2 c + v_1 u_2 b)a + (v_1 v_2)bc = 1$

which is of the form $ua + vbc = 1$, where u and v are integers.

$\therefore \gcd(a, bc) = 1$

$\Rightarrow$ a & b are co-prime.

Property

② If a, b are any integers which are not simultaneously zero and if k is any integer, then $\gcd(ka, kb) = |k| \cdot \gcd(a,b)$

Proof:- Let $d = \gcd(a,b) \rightarrow (1)$

Then $ua + vb = d \rightarrow (2)$, where 'u' and 'v' are integers

multiplying by +ve integer k on both sides then we get

$uak + vbk = dk$

i.e. $u(ka) + v(kb) = dk$

$\therefore \gcd(ka, kb) = dk$

$\gcd(ka, kb) = k \gcd(a,b)$ from (1)

If 'k' is any integer, then $\gcd(ka, kb) = |k| \cdot \gcd(a,b)$

3. If $a_1, a_2 -- a_n$ are relatively prime to 'b' then their product $a_1 \cdot a_2 \cdot a_3 \cdot \cdots \cdot a_n$ is also prime to b.

proof :-

- Property ③ : If $\gcd(a,b)=1$, Then for any integers c, then

$$\gcd(ac,b) = \gcd(c,b)$$

Proof: Assume that $\gcd(a,b)=1$ then

$\Rightarrow$ $u_1 a + v_1 b = 1$, for u_1, v_1 $\rightarrow$ ①

Let $\gcd(ac,b) = d$ $\rightarrow$ ② then

$u_2 ac + v_2 b = d$ $\rightarrow$ ③ for any integers u_2 and v_2

from ① & ③ we have

$(u_1 a + v_1 b)(u_2 ac + v_2 b) = d$

$u_1 u_2 a^2 c + (u_1 v_2 a + u_2 v_1 ac + v_1 v_2 b) b = d$

i.e $u_3 c + v_3 b = d$

where $u_3 = u_1 u_2 a^2$ and $v_3 = u_1 v_2 a + u_2 v_1 ac + v_1 v_2 b$

$\therefore \gcd(c,b) = d$ $\rightarrow$ ④

Thus. $\gcd(ac,b) = \gcd(c,b)$

- property ④ : If $a_1, a_2 \cdots a_n$ are relatively prime to be 'b'

Then their product $a_1, a_2 \cdots a_n$ is also prime to 'b'.

Proof:- a_1 is relative prime to b. Then $\therefore \gcd(a_1, b) = 1$

By property ③ $\gcd(a_1 a_2, b) = \gcd(a_2, b)$

$= 1$

since a_2 is relative prime to b.

again by property (3)

$$\gcd(a_1 a_2 a_3, b) = \gcd(a_3, b)$$
$$= 1,$$

since a_3 is relative prime to b

Ily $\gcd(a_1 a_2 a_3 a_4, b) = \gcd(a_4, b)$
$= 1$, since a_4 is relative prime to b.

continuing this process we get

$$\gcd(a_1 a_2 a_3 \cdots a_n, b) = \gcd(a_n, b) = 1$$

i.e $a_1, a_2 a_3 \cdots a_n$ and 'b' are co-prime.

Least common multiple:-

Let 'a' and 'b' be two non-zero integers, A non zero integers 'm' is said to be a least common multiple (lcm) of 'a' and 'b'. Then

(i) if m is a common multiple of 'a' and b

means if a/m and b/m ✗

(ii) If 'c' is a common multiple of 'a' and 'b', Then 'c' is a multiple of m. means if a/c and b/c then m/c'

(or)

Def: If 'a' and 'b' are +ve integers, Then the smallest positive integers that is divisible by both 'a' and 'b' is called the least common ~~divi~~ multiple of 'a' and 'b' and it is denoted by lcm(a,b).

Note: If either or ✗ both 'a' and 'b' are negative then

for example. lcm(8, 18) = lcm(-8, 18) = lcm(-8, -18) = 72

1.3.3 Testing for prime Numbers:

Prime testing is a common task for computers for deciding whether a number 'n' is prime or composite. Prime testing have become important in the applications of number theory to cryptography. Now, given a particular integers, how can we test whether it is prime or not? also if it is a composite integers, how can we determine non-trivial divisors of n?

Theorem: Every integers $n \geq 2$ has a prime factor.

proof: Let S(n) denote the sentence

S(n): If 'n' is an integers ≥ 2, then 'n' has a prime factor

we have to prove that $\forall n\, S(n)$ is true in the domain D

we have to prove this by using mathematical induction. $\forall n \geq 2$

Initially If $n = 2$, then 2 is a prime factor of n.

Hence, the result holds for $n \geq 2$

Inductive hypothesis: Suppose 'm' is a +ve integers s.t $m \geq 2$ & each of statements S(2), S(3), S(4) --, S(m) is true. i.e each of the integers 2, 3, 4 -- m has a prime factor.

Inductive step:

Consider the integer $m+1 \geq 2$. Then we S.T $S(m+1)$ is true.

If $m+1$ is prime, Then $m+1$ is a prime factor of $m+1$

Suppose $m+1$ is composite, Then $\exists$ integers q and r such that $m+1 = qr$, where $1 < q < m+1$ and

$$1 < r < m+1$$

Hence By inductive hypothesis 'q' and 'r' has a prime factor, which is also prime factor of $m+1$.

Thus $m+1$ has a prime factor.

∴ By The principle of mathematical induction

Every integers $n \geq 2$ has a prime factor.

Note:- If $n > 1$ be a composite integer, Then there exist a prime 'p' such that p/n and $p \leq \sqrt{n}$. (or) $p^2 \leq n$

Working rule Algorithm to test whether an integer $n > 1$ is a Prime.

Step①: Verify whether n is 2. If n is 2, Then n is prime:

step②: verify whether '2' divides n. If '2' divides n, Then 'n' is not prime. If '2' does not divide n, Then go forward

Step③: Find all odd primes $p \leq \sqrt{n}$. If there is no such odd prime, Then 'n' is prime otherwise go for next

Step④: Verify whether 'p' divides n, where 'p' is a prime obtained in step③.

If p divides n, Then 'n' is not a prime.

If p does not divides 'n' for any prime 'p' obtained in step③. Then 'n' is prime.

- Examples:-

① Determine whether the integer 133 is prime or not

Sol) Given integer is 133 i.e $n=133$

Here we know that '2' does not divide 133.

Now we find all odd primes 'p' such that $p^2 \leq 133$

These primes are 3, 5, 7 and 11.

Since $11^2 \leq 133 < 13^2$

None of these primes divide 133.

Hence $n=133$ is a prime integer.

② Determine whether the integers 287 is prime or not.

Sol Given $n = 287$

2 does not divide 287.

Now we find all odd primes such that $p^2 < 287$.

These primes are 3, 5, 7, 11 and 13

7 divides 287.

Hence 287 is a composite integer.

1.4 Fundamental Theorem of Arthmetic :-

Theorem : Every integer $n > 1$ can be expressed uniquely as a product of primes up to the order of the factors. more precisely, any integer $n > 1$ can be expressed as $n = p_1 p_2 \cdots p_u$ where $p_1, p_2, p_3 \cdots p_u$ are primes. moreover, if $n = p_1 p_2 \cdots p_u$ and $n = q_1 q_2 \cdots q_v$ are two factorisations of n as a product of primes, then $u = v$ and the q_j can be related so that $p_i = q_i$ $\forall$ $i = 1, 2, 3 \cdots u$

Proof :- we divide the proof into two parts. First, we will show by strong induction that either n is a prime or can be expressed as a product of primes. The

factorization into primes is unique except for the order of the factors. (i.e existence and uniqueness)

Part-2)

(i) Existence: Let S(n) denote the statement

S(n): 'n' can be expressed as a product of primes.

we prove that $\forall n$ S(n) is true in the domain of all integers ≥ 2.

By the principle of mathematical induction.

Initial step: If $n=2$, then $2=2$ is a prime.

$\Rightarrow$ S(2) is true.

- Inductive hypothesis: Assume that is a +ve integer, $k \geq 2$ and each of the statement S(2), S(3), S(4), S(5) ---, S(k) is true i.e each of the integers 2, 3, 4 --- k-1, k can be expressed as a product of primes.

Inductive step: To prove that S(k+1) is true.

- i.e to prove that the integer k+1 can be expressed as a product of primes.

If k+1 is a prime, then S(k+1) is true.

Suppose that (k+1) is composite. Then $\exists$ integers x and z

such that $k+1 = uv$, where $2 \le u \le k$ and $2 \le v \le k$.

By the indective hypothesis, both u and v can be expressed as a product of primes.

Hence let $u = p_1 p_2 \cdots p_i$ and $v = q_1 q_2 \cdots q_j$

where $p_1, p_2, \cdots p_i, q_1, q_2, q_3 \cdots q_j$ are primes.

Thus, we have $k+1 = uv = p_1 p_2 \cdots p_i q_1 q_2 \cdots q_j$

Which is product of primes.

Hence, $P(k+1)$ is true.

Thus by the principle of mathematical induction that any integers $n \ge 2$ can be expressed as a product primes.

(ii) Uniqueness: Now, we prove the uniqueness part.

Let $B(n)$ denote the statement

$B(n)$: If $n = p_1 p_2 \cdots p_u$ and $n = q_1 q_2 q_3 \cdots q_v$ are two factorisations of n as a product of primes, then $u = v$ and q_j can be related so that $p_i = q_i$ forall $i = 1, 2 \cdots r$

we prove that forall n $B(n)$ is true the domain of all integers ≥ 2.

Let us use the principle of mathematical induction

Initial Step: If $n=2$ then $2=2 \Rightarrow B(2)$ is true.

Inductive hypothesis: Assume 'k' is a +ve integers, $k \geq 2$, and each of the statements $B(2), B(3), B(4) \cdots B(k)$ is true.

i.e each of the integers $2,3,4,5, \cdots, k-1, k$ can be expressed as a product of primes uniquely.

Inductive step: Now to show that $B(k+1)$ is true.

if $k+1$ is a prime integers, then the result is true.

Assume that $k+1$ is not a prime integers and can be expressed as a product of primes in two ways

$$k+1 = p_1 p_2 \cdots p_i = q_1 q_2 \cdots q_j \text{ (say)} \rightarrow (1)$$

Now p_1 divides $k+1$,

$\Rightarrow$ p_1 divides ~~one~~ $q_1 q_2 q_3 \cdots q_j$,

p_1 divides one of $q_1 q_2 \cdots, q_j$

Since the result, "If a prime p divides $p_1 p_2 \cdots p_n, n>1$, then p divides one of the integers $p_1, p_2, \cdots p_n$".

Let us assume that p_1 divides q_k.

Now, p_1 and q_k are both primes and p_1 / q_k. ∎

Thus we must have $p_1 = q_k$.

Cancelling this common factor, we get

$$p_2 p_3 \cdots p_i = q_1 q_2 \cdots q_{k-1} q_{k+1} q_{k+2} \cdots q_j \rightarrow (2)$$

Let $m = p_2 p_3 \cdots p_i = q_1 q_2 \cdots q_{k-1} q_{k+1} \cdots q_j \rightarrow (3)$

Now $m \in \{2, 3, \cdots k\}$

Hence by the induction hypothesis, $B(m)$ is true.

∴ The above two factorizations of m are the same and hence the two factorisations of $(k+1)$ are the same.

Hence By the principle of mathematical induction,

$B(n)$ is true for every n.

Hence Fundamental Theorem of Arithmetic says that every integers greater than 1 can be factored uniquely into a product of primes.

• Def:- Every integer greater than 1 can be written in the form

$$n = p_1^{n_1} p_2^{n_2} p_3^{n_3} \cdots p_k^{n_k}$$

where $n_i \geq 0$ and the p_i's are distinct primes. for $i = 1, 2, 3 \cdots k$

and i.e $p_i \neq p_j$ for $i \neq j$

each p_i is a prime integer, The factorization is unique, except possibly for the order of factors is called standard (Prime) factorization of n.

· For Example The Standard factorization of 4312 is

$4312 = 2 \times 2156 = 2 \times 2 \times 1078 = 2 \times 2 \times 2 \times 539$

$= 2 \times 2 \times 2 \times 7 \times 77$

$= 2 \times 2 \times 2 \times 7 \times 7 \times 11$

$= 2^3 \cdot 7^2 \cdot 11$

· Examples:

① Find the prime factorization of 100, 289 & 630.

Sol Given integers are 100, 289 & 630

100 can be written as ⇒

$100 = 2 \times 2 \times 5 \times 5 = 2^2 \cdot 5^2$ ∴ Prime factorization of $100 = 2^2 \cdot 5^2$

Now $289 = 17 \times 17 = 17^2$ ⇒ P.f. of $289 = 17^2$

Now $630 = 2 \times 315$

$= 2 \times 3 \times 105$

$= 2 \times 3 \times 3 \times 35$

$= 2 \times 3 \times 3 \times 7 \times 5$

$= 2^1 \cdot 3^2 \cdot 7^1 \cdot 5^1 = 2 \times 3^2 \times 7 \times 5$

∴ Prime factorization of $630 = 2 \times 3^2 \times 5 \times 7$

② Find the prime factorization of 250 and 400

Sol prime factorization $250 = 2 \times 5 \times 25$

$= 2 \times 5 \times 5 \times 5$

$= 2 \times 5^3$

My prime factorization of $400 = 2 \times 200$

$= 2 \times 2 \times 100$

$= 2 \times 2 \times 2 \times 50$

$= 2 \times 2 \times 2 \times 2 \times 25$

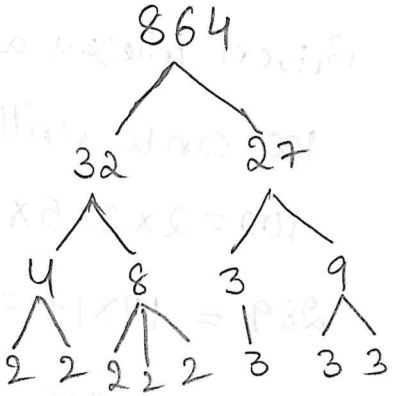
$= 2^4 \times 5 \times 5$

$= 2^4 \cdot 5^2$ //

③ Find the prime factorization of 864

Sol Given $n = 864$

or use this factor tree



$n = 864 = 2 \times 432$

$= 2 \times 2 \times 216$

$= 2 \times 2 \times 2 \times 108$

$= 2 \times 2 \times 2 \times 2 \times 54$

$= 2 \times 2 \times 2 \times 2 \times 2 \times 27$

$= 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 9$

$= 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 3$

$864 = 2^5 \cdot 3^3$

∴ Prime factorization of $864 = 2^5 \cdot 3^3$

Def:- A prime number 'p' is an integer greater than 1, that has no other positive integer divisors then '1' and p.

Def: The composite number 'n' is a positive integer, $n > 1$ which is not a prime

(i.e which has factors other than '1' and itself)

Canonical Decomposition:-

The canonical decomposition of a +ve integer 'n' is of the form $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ where $p_1, p_2 \cdots p_k$ are distinct Primes with $p_1 < p_2 < p_3 < \cdots < p_r$ and each exponent a_i is a positive integer. There are two commonly used techniques for finding the canonical decomposition of a composite number.

→ The first method involves finding all prime factors, beginning with the smallest prime. This method can be quite consuming if the number 'n' is fairly large

→ The second method, which is generally more efficient, involves splitting 'n' as the product of two positive integers not necessarily prime numbers, and continuing to split each factor into further factors until all factors are prime.

Examples:

(1) Find the canonical decomposition of 2520

Sol First we start with smallest prime '2'

Since $2520 = 2 \times 1260$

Now '2' is a factor of 1260,

So

$2520 = 2 \cdot 2 \cdot 630$;

again '2' is a factor of 630, so

$2520 = 2 \cdot 2 \cdot 2 \cdot 315$ Here 2 is a not factor of 315 But

3 is a factor of 315 then

$2520 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 105$

Now '3' is a factor of 105 also, so

$2520 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 35$ and Here '3' is not a factor of '35'

But 5 is a factor of 35, Then

$2520 = 2 \times 2 \times 2 \times 3 \times 3 \times 5 \times 7$

$\therefore$ Canonical decomposition of $2520 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1$

which is the required solution.

Alternately (method-2)

Sol Here $n = 2520$

$2520 = 40 \times 63$,

Since none of the factors are primes,

Split them again

$40 = 4 \times 10$ and

$63 = 7 \times 9$

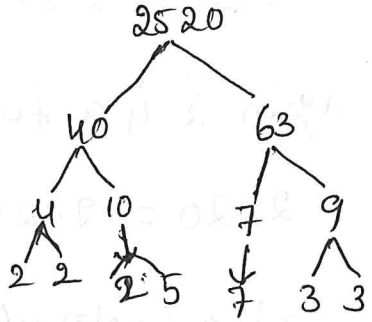
Now

$2520 = (4 \times 10) \cdot (7 \times 9)$

Since 4, 10 and 9 are composites again split each of them

i.e $2520 = (2 \times 2)(2 \times 5)(7)(3 \times 3)$

factor tree



Now all the factors are primes then stop the procedure.

Hence the canonical decomposition of $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$

- **Note①:-** The canonical decomposition of a composite number can be used to find its positive factors.

- **Note②:-** Let $m = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_u^{a_u} \rightarrow ①$ and

$n = p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots p_v^{b_v} \rightarrow ②$ then

$$\gcd(m,n) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_u^{\min(a_u,b_v)}$$

(or)

$$\gcd(m,n) = p^{\min(a,b)},$$ where $\min(a,b)$ represents the minimum of the two numbers 'a' and b.

which is called canonical decomposition of +ve integer their gcd. (or) gcd by using prime factorization method.

- **Note③:-** Let $m = p^a$ and $n = p^b$ then

$$\text{lcm}(m,n) = p^{\max(a,b)}$$ (lcm = least common multiple)

where $\max(a,b)$ represents the maximum of the two numbers 'a' and 'b'.

- Examples:

① Use prime factorization to find the greatest common divisor of 16 and 30.

(or)

Use the canonical decompositions of 18 and 30 to find their gcd.

Sol Given $m = 18$ and

$n = 30$

∴ prime factorization of 18 and 30 are

$18 = 2 \times 9$

$18 = 2 \times 3^2 \times 5^0$

and

$30 = 2^1 \times 15$

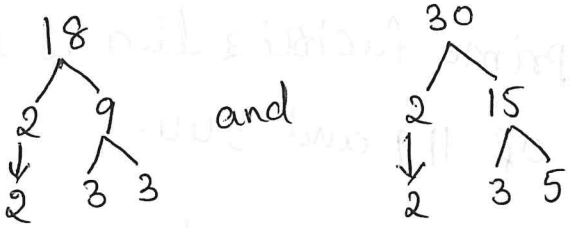
$30 = 2^1 \times 3^1 \times 5^1$

$\therefore \gcd(18, 30) = 2^{\min(1,1)} \times 3^{\min(2,1)} \times 5^{(0,1)}$

$= 2^1 \times 3^1 \times 5^0 = 2 \times 3 \times 1 = 6$

$\therefore \gcd(18, 30) = 6$

factor tree



② Use Prime factorization to find the gcd(120, 360)

(or)

Use the canonical decomposition of 120 and 360 to find their gcd.

Sol Given $m = 120$ and $n = 360$

Prime factorization of $120 = 2^3 \times 3^1 \times 5^1$

Prime factorization of $360 = 2^3 \times 3^2 \times 5^1$

$\therefore \gcd(120, 360) = 2^{\min(3,3)} \times 3^{\min(1,2)} \times 5^{\min(1,1)}$

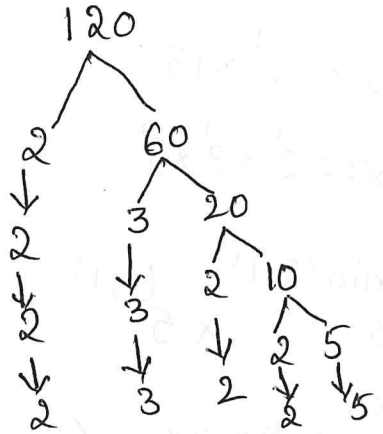
$= 2^3 \times 3^1 \times 5^1$

$= 8 \times 3 \times 5$

$= 120$

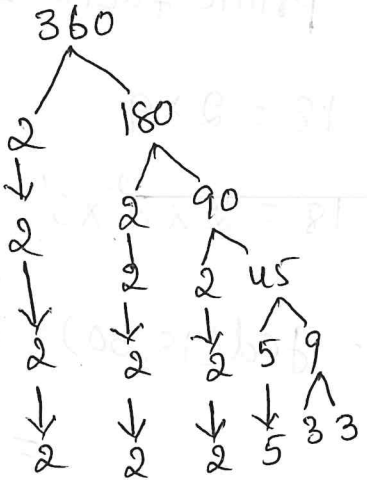
$\therefore \gcd(120, 360) = 120$

factor tree



$120 = 2^3 \cdot 3^1 \cdot 5^1$

factor tree



$\therefore 360 = 2^3 \cdot 3^2 \cdot 5^1$

③ Use prime factorization to find the least common multiple of 119 and 544.

Sol Given $m = 119$ and $n = 544$

prime factorization of $119 = 2^0 \times 7^1 \times 17^1$ and

Prime factorization of 544 is

$544 = 2^5 \times 7^0 \times 17^1$

∴ least common multiple of (119, 544)

i.e $\text{Lcm}(119,544) = 2^{\max(0,5)} \times 7^{\max(1,0)} \times 17^{\max(1,1)}$

$= 2^5 \times 7^1 \times 17^1$

∴ $\text{Lcm}(119,544) = 3808$

(4) Use prime factorization to find the least common multiple of 4410 and 51450

Sol Prime factorization of $4410 = 2 \times 3^2 \times 7^2 \times 5^1$

Prime factorization of $51450 = 2 \times 3 \times 7^3 \times 5^2$

∴ The $\text{Lcm}(4410, 51450) = 2^{\max(1,1)} \times 2^{\max(2,1)} \times 7^{\max(2,3)} \times 5^{\max(1,2)}$

$= 2^1 \times 3^2 \times 7^3 \times 5^2$

$= 2 \times 9 \times 343 \times 25$

$= 154,350$

∴ $\text{Lcm}(4410, 51450) = 154,350$.

⑤ Use the canonical decomposition of 1050 and 2574 to find their lcm.

Sol: Given $m = 1050$ and $n = 2574$

Prime factorization of $1050 = 2 \times 3 \times 5^2 \times 7 \times 11^0$ and

Prime factorization of $2574 = 2 \times 3^2 \times 11 \times 13 \times 7^0$

$\therefore \text{lcm}(1050, 2574) = 2^{\max(1,1)} \times 3^{\max(1,2)} \times 5^{\max(2,0)} \times 7^{\max(1,0)} \times 11^{\max(0,1)} \times 13^{\max(0,1)}$

$= 2^1 \times 3^2 \times 5^2 \times 7^1 \times 11^1 \times 13^1$

$\therefore \text{lcm}(1050, 2574) = 450,450$.

1.5 Fermat Numbers :- A Fermat number is a natural number which is of the form $2^{2^n} + 1$, where $n = 0, 1, 2 \ldots$

It is denoted by f_n.

$\therefore f_n = 2^{2^n} + 1$

The first four fermat numbers are

$$f_0 = 2^{2^0}+1 = 2^1+1 = 3$$

$$f_1 = 2^{2^1}+1 = 2^2+1 = 5$$

$$f_2 = 2^{2^2}+1 = 2^4+1 = 16+1 = 17$$

$$f_3 = 2^{2^3}+1 = 2^8+1 = 257 \text{ etc}$$

- Note: (1) Let f_n denote the n^{th} Fermat number. Then

$$f_n = f_{n-1}^2 - 2f_{n-1} + 2, \text{ where } n \geq 1$$

If $n=1$ Then $f_1 = f_0^2 - 2f_0 + 2$

$$f_1 = (3)^2 - 2(3) + 2 = 9 - 6 + 2 = 5$$

$$f_2 = f_1^2 - 2f_1 + 2$$

$$= 25 - 10 + 2$$

$$f_2 = 17 \text{ etc}$$

The first '5' Fermat numbers 3, 5, 17, 257, 65537. are primes and f_5 is a composite number and it is divisible by 641. [i.e $f_5 = 4294967297$]

Note②: Every prime factor of f_n is of the form $k \cdot 2^{n+2} + 1$, where $n \geq 2$, if f_n has no prime factor of the form $k \cdot 2^{n+2} + 1$, then f_n must be a prime.

Here $f_4 = 2^{16} + 1 = 65,537$ is the largest fermat number.

• Properties of Fermat numbers:

① The sum of the reciprocals of all the Fermat numbers are irrational.

② No Fermat prime can be expressed as the difference of two p^{th} powers, where 'p' is an odd prime

③ If 'n' is a positive integers then

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^k b^{n-1-k}$$

Generalized Fermat numbers:- the numbers of the form $a^{2^n} + b^{2^n}$, where a, b are co-prime integers $a > b > 0$ are called generalized fermat numbers. An odd prime 'p' is a generalized Fermat number $\Leftrightarrow$ 'p' is a congruent to $1 \pmod 4$.

- Theorem :- If 2^k+1 is an odd prime, then 'k' is a power of 2.

Proof: Let 'k' is a positive integers but not a power of 2. Then it must have an odd prime factor, $t > 2$ and we may write

$$k = rt \quad \text{where } 1 \leq r < k$$

By property no (3) we have for +ve integers m

$$(a-b) \mid a^m - b^m$$

it means "evenly divides".

Substituting $a = 2^r$, and $b = -1$, and $m = t$

Here using 't' is odd.

$$\therefore (2^r+1) \mid 2^{rt}+1 = 2^r+1 \mid 2^k+1$$

$$\therefore 1 < 2^r+1 < 2^k+1$$

i.e 2^k+1 is not prime.

By contraposition 'k' must be a power of 2.

• Examples:

① Show that $641 | f_5$ (or)

Show that f_5 is divisible by 641.

Sol Given integer is $n = 641$ and $n = 5$

By the defination of Fermat number we have

$$f_5 = 2^{2^n} + 1 = 2^{2^5} + 1$$

$$= 2^{32} + 1$$

$$= 2^4 \cdot 2^{28} + 1$$

$$= 16 \cdot 2^{28} + 1$$

$$= (641 - 5^4)\, 2^{28} + 1 \quad [\because 5^4 = 625]$$

$$= 641 \cdot 2^{28} - 5^4 \cdot 2^{28} + 1$$

$$= 641 \cdot 2^{28} - (5 \times 2^7)^4 + 1$$

$$= 641 \cdot 2^{28} - (641 - 1)^4 + 1 \quad [\because 5 \times 2^7 = 640]$$

$$= 641 \cdot 2^{28} - ((641)^4 - 4 \cdot (641)^3 + 6(641)^2 - 4(641) + 1) + 1$$

$$\therefore f_5 = 641\,(2^{28} - (641)^3 + 4(641)^2 - 6(641) + 4)$$

Thus f_5 is divisible by 641.

1.5) Fermats method of factorization: suppose we know that 'n' number is composite, writing $n = ab$, where 'a' and 'b' are practically unknown quantity.

Now we can use the identity $n = ab$

$$n = ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

if n is odd then a, b → odd

$$= t^2 - s^2 \quad \text{where } t = \frac{a+b}{2},\ s = \frac{a-b}{2}$$

(t, s are non-ve integers)

$$\therefore n = ab = t^2 - s^2 = (t+s)(t-s)$$

i.e $n = t^2 - s^2$

$$s^2 = t^2 - n$$

Here take $t = [\sqrt{n}] + 1$

where [ ] is greatest integer function,

If $t^2 - n$ is a perfect square then our problem completed

If $t^2 - n$ is not a perfect square Then

take $t = (\sqrt{n}) + 2$ and continue this process

until we get perfect square i.e $t = \sqrt{n} + 3$ etc

- Examples

① Factorise 809009 using Fermat method of factorization.

Sol Given $n = 809009$

First we have to find $\sqrt{n}$

ie $\sqrt{n} = \sqrt{809009} = 899.44$

Now w.k.t $t = \sqrt{n} + 1 = 899.44 + 1$

$t = 899 + 1 = 900$

Now $t^2 = (900)^2 = 810000$

$t^2 - n = 810000 - 809009 = 991$

if it is a perfect square (or) not check

$\sqrt{991} = 31.48$ it is not a perfect square, Then

$t = \sqrt{n} + 2 = 899 + 2 = 901$

Here $t = 901$ we have to find $t^2 - n$

$t^2 - n = (901)^2 - 809009$

$t^2 - n = 811801 - 809009 = 2792$

again check $\sqrt{2792} = 52.83$ This is also not a perfect square

go for the next step

$t = \sqrt{n} + 3 = 902$

Now $t^2 - n = (902)^2 - 809009$

$= 813604 - 809009$

$t^2 - n = 4595$ which is also not perfect square

again $t = \sqrt{n} + 4 = 903$

$t^2 - n = (903)^2 - 809009$

$= 815409 - 809009$

$= 815409 - 809009$

$= 6400$

$t^2 - n = (80)^2$

which is a perfect square.

$\therefore t^2 - n = (80)^2 = s^2$

$(903)^2 - (809009) = (80)^2$

where $t = 903$, $s = 80$

By using the above values to find 'a' & b

$n = t^2 - s^2 = (t+1)(t-1)$

$= (903 + 80)(903 - 80)$

$n = 983 \times 823$.

$\therefore 809009 = 983 \times 823$

where $a = 983$ & $b = 823$.

$\therefore 809009 = 983^2$

② Use Fermat's factorization method to factorize 119143

Sol Given $n = 119143$

First we have to find $\sqrt{n} = \sqrt{119143} = 345.170$

Now we have $t = \sqrt{n} + 1 = 345 + 1 = 346$

Now $t^2 = (346)^2 = 119716$

$t^2 - n = 119716 - 119143 = 573$

which is not perfect square

Now check $\sqrt{573} = 23.93$ ✗ Then

$t = \sqrt{n} + 2 = 345 + 2 = 347$

Here $t = 347$. Then find $t^2 - n$

$t^2 - n = (347)^2 - 119143 = 120409 - 119143 = 1266$

Now check $\sqrt{1266} = 35.5$ it is not perfect square

Then check next

$t = \sqrt{n} + 3 = 348$

Now $t^2 - n = (348)^2 - 119143 = 121104 - 119143 = 1961$

which is also not perfect square ($\because \sqrt{1961}$)

Now $t = \sqrt{n} + 4 = 349$

$t^2 - n = (349)^2 - 119143$

$= 121801 - 119143 = 2658$

Here $\sqrt{2658}$ is also not perfect square

Now $t = \sqrt{n} + 5 = 350$

$\Rightarrow t^2 - n = (350)^2 - 119143 = 122500 - 119143 = 3357$

it is also not perfect square

~~the~~ take $t = \sqrt{n} + 6 = 351$

$t^2 - n = 123201 - 119143 = 4058$

which has no perfect square

check again

$t = \sqrt{n} + 7 = 352$

$\therefore t^2 - n = (352)^2 - 119143$

$= 123904 - 119143$

$= 4761$

$t^2 - n = 69^2 \rightarrow (1)$

we have $t^2 - n = s^2$ Then here $s^2 = 69^2$

$s = 69$

Now to find n, a, b

and $t = 352$

$\therefore n = t^2 - s^2 = (t+s)(t-s)$

$n = ((352) + 69)(352 - 69)$

$n = 421 \times 283$

$n = 119,143$ which is satisfied

clearly $a = 421$ and $b = 283$

③ Use Fermat's factorization method to factorize 23449.

Sol Given $n = 23449$

First to find $\sqrt{n} = \sqrt{23449} = 153.1$

Now $t = \sqrt{n} + 1 = 154$

$t^2 - n = (154)^2 - 23449 = 23716 - 23449 = 267$

which has no perfect square

Now check again

take $t = \sqrt{n} + 2$

$t = 153 + 2 = 155$

Now $t^2 - n = (155)^2 - 23449$

$= 24025 - 23449$

$= 576$

$t^2 - n = (24)^2 = s^2$ which is perfect square

$\therefore n = t^2 - s^2$

$n = (155)^2 - (24)^2$ which is pero

where $t = 155 \rightarrow s = 24$

$n = (t+s)(t-s)$

$= (155+24)(155-24)$

$n = (179)(131)$

$\therefore n = 23449$. which is the solution

$a = 179$ and $b = 131$.

1.6 Introduction to Congruences:-

One of the most remarkable relation in number Theory is the congruence relation. Introduced and developed by the German mathematician Karl Friedrich Gauss. The congruence relation, as well will see shortly. shares many interesting properties with the equality relation, so that the congruence symbol can be written as '$\equiv$'. The congruence symbol facilities the study of divisibility Theory and has many interesting applications. Let us begin our discussion with a definition. Congruences containing variables, such as $3x \equiv 4 \pmod 5$, $x^2 \equiv 1 \pmod 8$, and $x^2 + 2 \equiv 3x \pmod 5$. The simplest of such congruences is the linear congruence i.e $ax \equiv b \pmod m$. we will now see that linear congruence and diophantine equations are interlinked. we will also learn a necessary and sufficient condition for a linear congruence to be solvable. we use congruence in every day life. As with so many concepts we will see, Congruence is

is simple, perhaps familiar to you, it is commonly useful and powerful in the study of number theory. If 'n' is a positive integers, we say that the integers 'a' and 'b' are congruent modulo n, and we write this as $a \equiv b \pmod{n}$, if they have the same remainder on division by n. This notation is much of the elementary theory of congruence

- Def: If 'a' and 'b' are integers and 'm' is a positive integers, then 'a' is said to be congruent to b module m, if 'm' divides (a-b) (or) a-b is a multiple of m. (i.e $m \mid a-b$)

It is denoted by $a \equiv b \pmod{m}$ is called the modulus of the congruence. and 'b' is called the residue of $a \pmod{m}$. i.e $(m \mid a-b)$

Here 'a' is not congruent to be module m, then it is denoted by $a \not\equiv b \pmod{m}$

it is also called as incongruent.

(i.e a is incongruent to b madulo m)

Examples:-

① $5/_{23-3} \Rightarrow 23 \equiv 3 \pmod 5$

(i.e $23-3 = 20$ is divisible by 5)

Hence '3' is the residue of 23 (mod 5) and '5' is the modules of the congruent.

② $\underset{28-(-4)}{16} \Rightarrow 28 \equiv -4 \pmod{16}$

i.e $28+4 = 32$ is divisible by 16

Hence -4 is the residue of 28 (mod 16) and 16 is the modules of the congruent.

③ $\frac{5}{20-3} \Rightarrow 20 \not\equiv 3 \pmod 5$,

since $20-3 = 18$ is not divisible by 5.

Hence '20' and '3' are incongruent module 5.

(4) $\frac{4}{20-3} \Rightarrow 20 \not\equiv 3 \pmod 4$

Since $20-3 = 18$ is not divisible by 4

Hence 20 and 3 are incongruent modulo 4.

- **Note:** If $a \equiv b \pmod m \iff a = b + km \ \forall k$

(or)

$\iff a - b = km \ \forall k$

(i.e k is some integers)

Ex: $23 \equiv 3 \pmod 5$ and $23 = 3 + 4 \times 5$

Ily $49 \equiv -5 \pmod 6$ (or) $49 = -5 + 9 \times 6$.

- **Basic properties of congruence:-**

(1) The congruence relation is an equilance relation

i.e for all integers a, b and c, Then the relation congruence is (i) $a \equiv a \pmod m$

(ii) If $a \equiv b \pmod m$, Then $b \equiv a \pmod m$ (symmetric)

(iii) If $a \equiv b \pmod m$ and $b \equiv c \pmod m$ Then

$a \equiv c \pmod{m}$ [Transitive]

- Proofs

(1) Show That The congruence relation is reflexive

(or) $a \equiv a \pmod{m}$

Proof:- W.K.T $a-a=0$ is divisible by m

(i.e $m/a-a$)

Hence $a \equiv a \pmod{m}$

∴ The congruence relation is reflexive.

Ex:- $6 \equiv 6 \pmod{5}$ i.e $5/6-6$ means $6-6=0$ is divisible by 5

(2) Show That The congruence relation is symmetric.

[i.e if $a \equiv b \pmod{m}$ Then $b \equiv a \pmod{m}$]

Proof: By The Def of congruence we have

$a \equiv b \pmod{m}$

That means $a-b$ is divisible by m.

i.e $(a-b)$ is a multiple of m and

clearly $b-a$ is also a multiple of m.

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

Hence The congruence relation is symmetric.

Ex: $3 \equiv 5 \pmod{2}$, i.e $2/3-5$ means $3-5=-2$ is divisible by 2. and also $5 \equiv 3 \pmod{2}$

③ Show that $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then

$a \equiv c \pmod m$

Proof:- Given that L.H.S $a \equiv b \pmod m$ → ①

That means $a-b$ is divisible by m and

$b \equiv c \pmod m$ → ② means that $(b-c)$ is divisible by m.

Hence $a-b+b-c = a-c$ is also divisible by m

(i.e ~~$a-b = mx = by$~~)

i.e $a \equiv c \pmod m$

∴ The congruence relation is transitive.

Hence the congruence relation is an equivalence relation. Ex: $7 \equiv -5 \pmod 4$ and $-5 = 15 \pmod 4$, $7 \equiv 15 \pmod 4$

- Congruence arithmetic properties:

① If $a \equiv b \pmod m$ and 'c' is any integer, then

(i) $a \pm c \equiv b \pm c \pmod m$

(ii) $ac \equiv bc \pmod m$

Proof: (i) we know that $a \equiv b \pmod{m}$ means

$a-b$ is divisible by m.

Now $(a \pm c) - (b \pm c) = a+c-b-c = a-b$

(or)

$= a-c-b+c = a-b$

$\therefore (a \pm c) - (b \pm c) = a-b$ is divisible by m.

$\therefore (a \pm c) \equiv (b \pm c) \pmod{m}$

(ii) we have $a \equiv b \pmod{m}$,

i.e $a-b$ is divisible by m.

$\therefore (a-b)c = ac-bc$ is also divisible by m.

$\therefore ac \equiv bc \pmod{m}$.

• Note: The converse of (ii) is not always true.

Ex:- If we take $ac \equiv bc \pmod{m}$ then 'a' need not be congruent to b mod m always.

(2) If $ac \equiv bc \pmod{m}$, Then $a \equiv b \pmod{m}$, only if $\gcd(c, m) = 1$. In fact, if c is an integers which divides m, and if $ac \equiv bc \pmod{m}$ Then

$$a \equiv b \left[\mod\left(\frac{m}{\gcd(c,m)}\right)\right]$$

Proof: we have $ac \equiv bc \pmod{m}$ means that

$ac - bc$ is divisible by m (or)

$ac - bc$ is a multiple of m.

i.e $ac - bc = pm$, where 'p' is an integers.

$\therefore (a-b)c = pm$

$a - b = p/c\, m$

$a - b = p(m/c)$

$a \equiv b \pmod{(m/c)}$, provided that m/c is an integers

$\therefore$ 'c' divides m, $\gcd(c, m) = c$

Hence $a \equiv b \left[\mod \frac{m}{\gcd(c,m)}\right]$

- given $\gcd(c, m) = 1$ Then $a \equiv b \pmod{m}$

③ If a, b, c, d are integers and m is a positive integer such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

(i) $a \pm c \equiv (b \pm d) \pmod{m}$

(ii) $ac \equiv bd \pmod{m}$

(iii) $a^n \equiv b^n \pmod{m}$, where n is a +ve integer.

Proof: ① Since $a \equiv b \pmod{m}$

i.e $a-b$ is divisible by m.

Similarly $c \equiv d \pmod{m}$

means $c-d$ is divisible by m.

$(a-b) \pm (c-d)$ is also divisible by m

i.e $(a \pm c) - (b \pm d)$ is divisible by m.

i.e $a \pm c \equiv (b \pm d) \pmod{m}$

Hence $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ Then $a \pm c \equiv (b \pm d) \pmod{m}$.

(ii) W.K.T $a \equiv b \pmod{m}$, $(a-b)$ is divisible by m.

and $(a-b)c$ is divisible by m. $\rightarrow$ ①

Since $c \equiv d \pmod{m}$, means $c-d$ is divisible by m.

$\therefore (c-d)b$ is also divisible by m

$\therefore (a-b)c + (c-d)b = ac - bc + bc - bd$

$= ac - bd$ is divisible by m $\rightarrow$ (2)

i.e $ac \equiv bd \pmod{m}$

Hence $ac \equiv bd \pmod{m}$ $\rightarrow$ (3)

(iii) Now Here we have to show That

$a^n = b^n \pmod{m}$

sub $c = a$ and $d = b$ in eq^n (3) we get

$a^2 = b^2 \pmod{m}$ $\rightarrow$ (4)

also $a \equiv b \pmod{m}$ $\rightarrow$ (5)

By using the above (ii) in eq^n (4) & (5)

we get $a^3 = b^3 \pmod{m}$

Continuing this process we get

$a^n = b^n \pmod{m}$, where n is positive integer

(or) $a^n = b^n \pmod{m}$, where n is a +ve integer

• A complete set of Residues modulo m:-

A set of 'm' integers is a complete set of residues modulo 'm' if every integer is congruent modulo 'm' to exactly one of them.

Thus the set of integers $(a_1, a_2 \cdots a_m)$ is a complete set of residues modulo m if they are congruent 'm' to the least residues $0, 1, 2, \cdots (m-1)$ in some order.

for Ex: The set $\{-12, 9, 6, 23\}$ is a complete set of residues modulo 4

$\because -12 \equiv 0 \pmod 4$, $9 \equiv 1 \pmod 4$, $6 \equiv 2 \pmod 4$

and $23 \equiv 3 \pmod 4$ so by the above properties shows that the congruences with the same modules can be added and multiplied, just as with equality.

Examples

① Find the remainder when $1! + 2! + 3! + \cdots + 100!$ is divided by 15.

Sol Let K is any integer.

when $K \geq 5$, $K! \equiv 0 \pmod{15}$

$\therefore 1! + 2! + 3! + \cdots + 100! \equiv (1! + 2! + 3! + 4! + 0 + \cdots + 0) \pmod{15}$

$\equiv 1 + 2 + 6 + 24 \pmod{15}$

$\equiv 1 + 2 + 0 \pmod{15}$ ($\because$ 30 is divisible by 15)

$1! + 2! + \cdots + 100! \equiv 3 \pmod{15}$

Hence when the given sum is divided by 15, and the remainder is 3.

(2) Find the positive integers n for which $\sum_{1}^{n} k!$ is a square.

Sol when $k \geq 5$, $k! \equiv 0 \pmod{10}$ why because

let $n \geq 5$, and let 's' denote the given sum then.

$S \equiv$ ones digit in $\sum_{1}^{n} k! \pmod{10}$

$\equiv (1! + 2! + 3! + 4!) \pmod{10}$

$\equiv (1 + 2 + 6 + 24) \pmod{10}$

$S \equiv 3 \pmod{10}$

Thus the ones digit in 's' is 3, if $n \geq 5$.

But $0^2 \equiv 0 \pmod{10}$, $1^2 \equiv 1 \pmod{10}$, $2^2 \equiv 4 \pmod{10}$,

$3^2 \equiv 9 \pmod{10}$, $4^2 \equiv 6 \pmod{10}$, $5^2 \equiv 5 \pmod{10}$.

$6^2 \equiv 6 \pmod{10}$, $7^2 \equiv 9 \pmod{10}$, $8^2 \equiv 4 \pmod{10}$, and

$9^2 \equiv 1 \pmod{10}$

Consequently, the square of every integer must end in 0, 1, 4, 5, 6, or 9.

Thus, if $n \geq 5$'s' cannot be a square.

when $n = 1$, then $S = 1$ and when $n = 3$, $S = 9$, both perfect squares.

But 'S' is not a square when $n = 2$ or 4.

Thus there are exactly two +ve integers 'n' for which 'S' is square, namely, 1 and 3.

③ Find the remainder when 16^{53} is divided by 7.

Sol First, reduce the base to its least residue:

$16 \equiv 2 \pmod{7}$

So by property ③ we have $a^n \equiv b^n \pmod{m}$

$$16^{53} \equiv 2^{53} \pmod 7$$

Now we can express 2 as a suitable power of 2 congruent modulo 7 to a number less than 7:

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

$$2^{53} = 2^{3\times 17+2} = (2^3)^{17} \cdot 2^2$$

$$\equiv 1^{17} \cdot 4 \pmod 7$$

$$\equiv 4 \pmod 7$$

So $16^{53} \equiv 4 \pmod 7$. (By transitive property)

Thus when 16^{53} is divided by 7, and the remainder is 4.

(4) Find the remainder when 3^{247} is divided by 17.

Sol We have $3^3 = 27 \equiv 10 \pmod{17}$

Squaring on both sides

$$(3^3)^2 \equiv (10)^2 \bmod(17)$$

$$3^6 \equiv 100 \pmod{17}$$

$$\equiv -2 \pmod{17}$$

take both sides 4th powers

$$(3^6)^4 \equiv (-2)^4 \pmod{17}$$

$$3^{24} \equiv -1 \pmod{17}$$

Now applying division algorithm with 24 of the divisor $3^{247} = 3^{24\times 10+7} = (3^{24})^{10} \cdot 3^6 \cdot 3$

$$\equiv (-1)^{10} \cdot (-2)\ 3 \pmod{17}$$

$$\equiv -6 \pmod{17}$$

change -6 to its least residue:

$$\equiv 11 \pmod{17}$$

Thus the remainder is 11.

(5) Compute the remainder when 3^{247} is divided by 25.

sol First to find the least residues of 3^2 and its successive squares modulo 25.

$3^2 \equiv 9 \pmod{25}$

$3^4 = 9^2 \equiv 6 \pmod{25}$

$3^8 = 6^2 = 11 \pmod{25}$

$3^{16} \equiv 11^2 \equiv 21 \pmod{25}$

$3^{32} \equiv (21)^2 \equiv 16 \pmod{25}$

$3^{64} \equiv 16^2 \equiv 6 \pmod{25}$

$3^{128} \equiv 6^2 \equiv 11 \pmod{25}$.

128 is the largest power of 2 contained in 247. Then

$3^{247} = 3^{128+64+32+16+4+2+1}$

$= 3^{128} \cdot 3^{64} \cdot 3^{32} \cdot 3^{16} \cdot 3^4 \cdot 3^2 \cdot 3^1$

$3^{247} \equiv 11 \cdot 6 \cdot 16 \cdot 21 \cdot 6 \cdot 9 \cdot 3 \pmod{25}$

$\equiv 11 \cdot (6 \cdot 16) \cdot 21 \cdot (6 \cdot 9) \cdot 3 \pmod{25}$

$\equiv 11 \cdot (-4) \cdot (-4) \cdot 4 \cdot 3 \equiv 6 \cdot 9 \cdot 3 \equiv (6 \cdot 9) \cdot 3 \pmod{25}$

$\equiv 4 \cdot 3$

$3^{247} \equiv 12 \pmod{25}$.

Thus 12 is the desired remainder.

1.6 Fermat's Theorem :

If 'p' is a prime and 'a' is an integers such that p does not divide a, then $a^{p-1} \equiv 1 \pmod{p}$, for every integers a,

$a^p \equiv a \pmod{p}$.

proof: Let us consider the first (p-1) positive multiples of 'a'

i.e The integers $1 \cdot a, 2 \cdot a, 3 \cdot a, 4 \cdot a, \ldots, (p-1)a$

since 'p' does not divide a, the above set of integers no two integers are congruent module p (or) congruent to zero.

Suppose if possible

Let $ra \equiv va \pmod{p}$, where $r, v \in \{1, 2, 3 \ldots p-1\}, r \neq v$

then $(r-v)a \equiv 0 \pmod{p}$

Thus 'p' divides $(r-v)a$.

Since p is a prime, either 'p' divides $r-v$ (or) p divides a.

But, $r, v \in \{1, 2, 3, \ldots p-1\}$ and $r \neq v$

$\therefore$ p does not divided $r-v$ and also

from the hypothesis we have p does not divide a.

Hence $ra \equiv va \pmod{p}$ and also $ra \equiv 0 \pmod{p}$

for $r = 1, 2, 3 \ldots p-1$

∴ the above set of integers must be congruent modulo p to 1, 2, 3 - - - , p-1, taken in some order.

multiplying all these congruences together. we have to find that

$$a \cdot 2a \cdot 3a \cdot \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots (p-1) \pmod{p}$$

i.e $(p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$

∴ $\gcd(p, (p-1)!) = 1$

we can cancelate $(p-1)!$ on both sides

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

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

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

Hence proved.

• Note: Fermat's theorem is also called Fermat's little theorem.

• Example: ① Using Fermat's Theorem, prove that $4^{13,332} \equiv 16 \pmod{13,331}$. Also, give an example to show that the Fermat's Theorem is true for a composite integer.

Sol We know that 13,331 is a prime number and 4 does not divide 13,331.

by Fermat Theorem we have

$$4^{13,331-1} \equiv 1 \bmod (13,331)$$

i.e $4^{13,330} \equiv 1 \bmod (13,331)$

$$4^{13,331} \equiv 4 \bmod (13,331)$$

$$4^{13,332} \equiv 16 \bmod (13,331) \rightarrow ①$$

Since 11 is a prime and 2 does not divide 11,

By Fermat's Theorem we have

$$2^{11-1} \equiv 1 \pmod{11} \rightarrow ②$$

$$2^{10} \equiv 1 \pmod{11}$$

$$2^5 \equiv 1 \pmod{31}$$

$$(2^5)^{66} \equiv 1^{68} \pmod{31} \rightarrow ③$$

$$2^{340} \equiv 1 \pmod{31}$$

from ② & ③ we have

$2^{340} - 1$ divisible by 11×31

since $\gcd(11, 31) = 1$

i.e $2^{340} \equiv 1 \pmod{341}$

Thus even though 341 is not prime, Hence Fermat's Theorem is satisfied.

② prove that $\log_3 7$ is irrational

Sol] let $\log_3 7 = u/v$, where u and v are +ve integers

take exponential on both sides

$$7 = 3^{u/v}$$

(∴ take 'v' powers on both sides)

$$7^v = 3^u = m \text{ (say)}$$

This means that the integer $m > 1$ is expressed as a product of prime number in two ways. This contradicts the fundamental theorem of arithmetic

∴ $\log_3 7$ is irrational.

③ prove that $\sqrt{11}$ is irrational.

Sol If possible, let $\sqrt{11} = p/q$ → ① where p and q are +ve integers prime to each other.

Then take square on both sides

$$(\sqrt{11})^2 = (p/q)^2$$

$$11 = p^2/q^2$$

$$p^2 = 11q^2 \rightarrow ②$$

$\therefore p^2$ is divide by 11

$\therefore p$ is divisible by 11.

$\therefore p = 11k \rightarrow ③$

sub ③ in ② we get

$$(11k)^2 = 11q^2$$

$$121k^2 = 11q^2$$

$$q^2 = 11k^2$$

Now q^2 is divisible by 11

i.e q is divisible by 11

Hence $q = 11m$

from (2) & (3) we find that 'u' and 'v' have a common factor 11, which contradicts the assumption.
Hence $\sqrt{11}$ is an irrational number.

- Def: A reduced residue system module m is a set of integers r_i, such that $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod m$ if $i \neq j$, and such that every 'n' prime to m is congruent module m to some member r_i, of the set.

- modular exponentiation: modular exponentiation is a less efficient method for determining the remainder when b^n is divided by m. It is based on the binary representation of $n = (n_k, n_{k-1}, n_{k-2} \cdots n_1, n_0)$. Successive Square The least residue of b^{n_i}, where $0 \le i \le k$

from proof the above properties i.e $ac \equiv bd \pmod m$ and if $a^n \equiv b^n \pmod m$ we have

$$b^n = b^{n_k 2^k + n_{k-1} 2^{k-1} + \cdots + n_0}$$

$$\equiv b^{n_k 2^k} \cdot b^{n_{k-1} 2^{k-1}} \cdots b^{n_0} \pmod m.$$

1.7 Linear congruence :- Let a, b are positive integers and $n \in \mathbb{Z}$, a solution $x \in \mathbb{Z}$ to the linear congruence $ax \equiv b \pmod{n}$ is called a linear congruence, where x is unknown. Here the linear congruence and linear diophantine equations are interlinked.

- Examples :-

① solve the linear congruence $131x \equiv 21 \pmod{77}$

Sol) we have $1 = (131, 77)/21$

There is a unique solution modulo 77. and we have $5 \cdot 4x \equiv 21 \pmod{77}$ it is dividing by 3.

and $18x \equiv 7 \pmod{77}$

next multiplying '4' on both sides Then we get

$$72x \equiv 28 \pmod{77} \text{ and}$$

$$-5x \equiv 28 \equiv 105 \pmod{77}$$

$$\therefore x \equiv -21 \equiv 56 \pmod{77}.$$

② Determine if the congruences (i) $8x \equiv 10 \pmod 6$

(ii) $2x \equiv 3 \pmod 4$

Sol (i) $(8,6) = 2$ and $2 \mid 10$.

So the congruence $8x \equiv 10 \pmod 6$

it is solvable and it has two incongruent solutions modulo 6.

(ii) $(2,4) = 2$, but $2 \nmid 3$

so the congruence $2x \equiv 3 \pmod 4$ has no solution.

③ solve the linear congruence $91x \equiv 98 \pmod{119}$

Sol Since $7 = (91, 119) \mid 98$ there are '7' incongruent solutions modulo 119.

we can cancellation and simplify the congruence to

$$13x \equiv 14 \pmod{17}$$

we have $-4x \equiv -3 \equiv -20 \pmod{17}$

∴ in terms of the original modulus, the solutions are $x = 5, 22, 39, 56, 73, 90, 107 \pmod{119}$.

(4) Solve the linear congruence $6x \equiv (10)^k \pmod{21}$

Sol Here it has no solutions because

$(6, 21) = 3$ it does not divide $2^k, 5^k$.

for all +ve integer k.

(5) Solve the linear congruence $31x \equiv 12 \pmod{24}$

Sol Since $(31, 24) = 1$ and $1 \mid 12$

There is exactly one incongruent solutions modulo 24.

for finding that solution we can use

$31 \equiv 7 \pmod{24}$

multiplying 'x' on both sides we get

$31x \equiv 7x \pmod{24}$

which means we have to solve the linear congruence

$7x \equiv 12 \pmod{24}$

next we multiply by '7' on both sides then we get

$$49x \equiv 84 \pmod{24}$$

$\because 49 \equiv 1 \pmod{24}$ and $84 \equiv 12 \pmod{24}$

Now we have $x \equiv 12 \pmod{24}$

which is required solution to the linear congruence.

$$13x \equiv 12 \pmod{24}.$$

- Inverse of a integers modulo n: To solve a linear congruence eqn $ax \equiv b \pmod{n}$, if possible first we find an integer 'k' such that $ak \equiv 1 \pmod{n}$ and then using k, we solve by multiplying by k, and then find $x \equiv kb \pmod{n}$

- Def:- Let 'a' be an integers with $(a,n) = 1$ then a solution of the linear congruence $ax \equiv 1 \pmod{n}$ is called an inverse of a.

• Note: Let 'p' is a prime, the positive integers 'a' is its own inverse integers modulo $p \Leftrightarrow a \equiv 1 \pmod{p}$

(or)

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

• Examples:-

① Solve the linear congruence $78x \equiv 12 \pmod{240}$ by finding an inverse.

Sol we have $(78, 240) = 6$ and $6 \mid 12$

There are exactly six incongruent solution modulo 240.

To find this solution by using congruence definition.

$240 \mid (78x - 12)$ which means $\exists$ an integer 'y' s.t

$78x - 12 = 240y$ and

now we will solve this By linear Diophantine eqn

$78x + 240(-y) = 12$ B'

By using Euclidean algorithm

$$240 = 3(78) + 6 \text{ ; with } 0 \leq 7 < 2$$

Here '6' as a linear combination of '78' and 240,

i.e $6 = (-3)78 + (1)(240)$

multiplying '2' on both sides and taken particular solution

$x_0 = -6$ Then

$$12 = (-6)(78) + (2)(240)$$

The all solution to the linear diophantine equation

$78x - 12 = 240y$ are given

$$x = -6 + \frac{240}{6}t$$

$$x = -6 + 40t$$

Put $t = 1, 2, 3, 4, 5, 6, 7$ we get '6' incongruent solutions modulo 240.

i.e $x = 34, 74, 114, 154, 194, 234 \pmod{240}$

which is the desired solution.

(2) solve the linear congruence $37x \equiv b \pmod{53}$ by finding an inverse.

Sol we first solve $37x \equiv 1 \pmod{53}$

Now we have $-16x \equiv 1 \equiv 54 \pmod{53}$

dividing by '2' on both sides we get

$$-8x \equiv 27 \pmod{53}$$

$$8x \equiv -27 \equiv 26 \equiv 132 \pmod{53}$$

again dividing by 2 and simplify

we have $2x \equiv 33 \equiv 86 \pmod{53}$

$\therefore x \equiv 43 \pmod{53} \rightarrow (1)$

Now to solve $37x \equiv b \pmod{53}$

multiplying '43' on both sides

$$(43)\ 37x = 43b \pmod{53}$$

Thus $x \equiv 43b \pmod{53}$

which is the required solution.

③ By finding an inverse, solve the linear congruence

$31x \equiv 12 \pmod{24}$

Sol Since $(31, 24) = 1$ and $1 \mid 12$

there is exactly one incongruent solution modulo 24.

By the def of congruence

$24 \mid (31x - 12)$.

i.e $\exists$ an integer y such that

$31x - 12 = 24y$ and so we will solve

the linear system of Diophantine eqn

$31x + 24(-y) = 12$

But we need solution of x.

First we find the particular solution to this linear Diophantine eqn.

By using Euclidean algorithm

$31 = 1(24) + 7$ with $0 \leq 7 < 24$

$24 = 3(7) + 3$, with $0 \leq 2 < 7$

$7 = 2(3) + 1$, with $0 \leq 1 < 2$

so $(31, 24) = 1$

which we already knew.

Now we can take backward substitutions to find 1 as a linear combination of 31 and 24.

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

$$1 = 7 - 2(24 - 3(7))$$

$$1 = 7(7) + (-2)(24)$$

$$1 = 7(31 - 1(24) + (-2)(24))$$

$$1 = 7(31) + (-9)(24)$$

multiplying 12 on both sides and take $x_0 = 84$

$$\therefore 12 = (31)(84) + 24(-108)$$

So all the solutions of linear Diophantine eqn

$$31x + 24(-y) = 12$$

given $x = 84 + 24t$ where t is an integer

Sub $t = -3$ Then $x \equiv 12 \pmod{24}$ (we can find)

• Linear Diophantine equations: The simplest class of diophantine equations is the class of linear diophantine equations. A linear dipphantine equation in two variables 'x' and 'y' is of the form

$ax+by=c$ where a, b and c are integers

Solving such linear diophantine eqn involves the euclidean algorithm.

Note: The linear diophantine equation $ax+by=c$ is solvable if and only if d/c, where $d=(a,b)$, if x_0, y_0 is a particular solution of the linear diophantine equation, Then all its solutions are given by

$$x = x_0 + (b/d)t \quad \text{and} \quad y = y_0 - (a/d)t$$

where 't' is an arbitrary integer.

Note ②: If $(a,b)=1$, Then the linear diophantine equation $ax+by=c$ is solvable and the general solution is

$x = x_0 + bt$, $y = y_0 - at$ where x_0, y_0 is a particular solution

Ex: ① Determine if the linear diophantine equations $12x+18y=30$, $2x+34y=4$ and $6x+8y=25$ are solvable.

Sol Here $(12,18)=6$ and, $6/30$

Then the linear diophantine $12x+18y=30$ has a solution.

next take second equation

Here $(2,3)=1$, by the above note ②

the diophantine equation has a solution

next the third eqn

$(6,8)=2$, but $2/25$ so the linear diophantine equation $6x+8y=25$ is not solvable.

Note: The modern linear congruence $ax \equiv b \pmod{m}$ $\forall a,b \in \mathbb{Z}$ and $m \in \mathbb{N}$, is equivalent to the linear diophantine equation $ax - my = b$ in the two unknowns x and y.

Ex:- Use The congruence to solve $63x - 23y = 7$

Sol we have $63x - 23y = -7$ This linear diophantine equation creates two linear congruences.

$$63x \equiv -7 \pmod{23} \text{ and}$$

$$-23y \equiv -7 \pmod{63}$$

first one yields $-6x \equiv -7 \pmod{23}$

i.e $6x \equiv 7 \pmod{23}$ where $(6, 23) = 1$

multiplying 'u' on both sides

$u(6x) \equiv u(7) \pmod{23} \Rightarrow x \equiv 5 \pmod{23}$

∴ The general solution of The congruence is $63x \equiv 7 \pmod{23}$

i.e $x = 5 + 23t$

Substituting 'x' in The linear diophantine eqn and solve for 'y'

$$63(5 + 23t) - 23y = -7$$

$$315 + 1449t - 23y = -7$$

$$\therefore y = 14 + 63t$$

Hence The General solution of this linear diophantine is

$x = 5 + 23t$, $y = 14 + 63t$ where 't' is any arbitrary integer

1.8 System of linear congruences:

The system of linear congruence with one unknown is of the form $a_1 x \equiv b_1 \pmod{m_1}$,

$a_2 x \equiv b_2 \pmod{m_2}$

in this first solve one of them and then find its solutions that also satisfy the another.

1.9 The Chinese remainder Theorem:

Statement:- The linear system of congruences $x \equiv a_i \pmod{m_i}$ where the module are pairwise relatively prime and $1 \le i \le k$ has a unique solution modulo

$m_1, m_2, m_3 \dots m_k$

(or)

Let $m_1, m_2, m_3 \dots m_k$ be non-zero integers, that are pairwise relatively prime, then, for any integers $a_1, a_2, a_3 \dots a_k$, The system of congruency $x_1 \equiv a_1 \pmod{m_1}$, $x_2 \equiv a_2 \pmod{m_2}$, $x_3 \equiv a_3 \pmod{m_3} \dots x \equiv a_k \pmod{m_k}$

has a solution. If x_0 is the one solution, then all solutions are $x \equiv x_0 \pmod{m_1, m_2 \cdots m_r}$.

Proof: Let $m = m_1, m_2, m_3 \cdots m_r$ and and

$$M_i = \frac{M}{m_j} \text{ for } j = 1, 2, 3 \cdots r.$$

Then $\gcd(m_j, m_j) = 1$

Let y_j be an inverse of M_j modulo m_j, then

we have $M_j y_j \equiv 1 \pmod{m_j}$,

By the defination of the inverse modulo

we have

$$x = \sum_{j=1}^{r} a_r M_r x_r$$

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 + a_3 M_3 x_3 + \cdots + a_r M_r x_r.$$

Then 'x' is a simultaneous solution to the given system of linear congruences.

If 'x' and 'y' are two simultaneous solutions

Then $x \equiv y \pmod{m_j}$

where $j = 1, 2, 3 \cdots r$

and m_j are pairwise relatively prime.

Now we calculate that $x \equiv y \pmod{M}$

i.e The solution is a unique congruence class modulo M, and the value of x obtained.

• Examples: ① Solve the following system of congruences.

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Sol The modules are pairwise relatively prime,

∴ we can use the chinese remainder theorem.

we have $m_1 = 3$, $m_2 = 5$, and $m_3 = 7$

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

and $M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

$$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$$

$$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15.$$

Now the linear congruences

$$M_1 y_1 \equiv 1 \pmod 3 \Rightarrow 35 y_1 \equiv 1 \pmod 3$$

$$M_2 y_2 \equiv 1 \pmod 5 \Rightarrow 21 y_2 \equiv 1 \pmod 5,$$

and

$$M_3 y_3 \equiv 1 \pmod 7 \Rightarrow 15 y_3 \equiv 1 \pmod 7.$$

are satisfied by $y_1 = -1$, $y_2 = 1$ and $y_3 = 1$ respectively.

Thus, a solution to the given system is given by

$$x = (2 \cdot 35 \cdot (-1) + (3 \cdot 21) \cdot 1) + (2 \cdot 15 \cdot 1)$$

$$= -70 + 63 + 30$$

$$= 23$$

Madulo 105. So, the solution of the form congruence class of 23 modulo 105,

i.e the General solution is

$$x = 23 + 105k, \quad k \in \mathbb{Z}$$

Hence the chinese remainder theorem gives us an algorithm for solving a system of linear congruences with one unknown.

(2) Solve the system of congruences:

$$x \equiv 3 \pmod{10},\ x \equiv 8 \pmod{15},\ x \equiv 5 \pmod{84}$$

Sol the module in this problem are not pairwise relatively prime so we can not apply the chinese remainder theorem directly, and it is possible that such a system has no solution

Since $10 = 2 \cdot 5$, $15 = 3 \cdot 5$ & $84 = 2 \times 2 \times 3 \times 7$

The first congruence is equivalent to

$$x \equiv 3 \pmod{2},\ x \equiv 3 \pmod{5}$$

The second congruence is equal to

$$x \equiv 2 \pmod{3},\ x \equiv 3 \pmod{5}$$

and the third congruence is equal to

$x \equiv 5 \pmod 4$, $x \equiv 5 \pmod 3$, $x \equiv 5 \pmod 7$

∴ in general system is equal to

$$x \equiv 1 \pmod 4,$$
$$x \equiv 2 \pmod 3,$$
$$x \equiv 3 \pmod 5,$$
$$x \equiv 5 \pmod 7.$$

Now we can apply Chinese remainder theorem.

We have $m_1 = 4$, $m_2 = 3$, $m_3 = 5$ & $m_4 = 7$

∴ $M = 4 \times 3 \times 5 \times 7 = 420$

∴ $M_1 = \frac{M}{m_1} = \frac{420}{4} = 105$

$M_2 = \frac{M}{m_2} = \frac{420}{3} = 104$

$M_3 = \frac{M}{m_3} = \frac{420}{5} = 84$

$m_4 = \frac{M}{m_4} = \frac{420}{7} = 60.$

Now the linear congruences

$$105\, y_1 \equiv 1 \pmod 4,$$

$$140\, y_2 \equiv 1 \pmod 3,$$

$$84\, y_3 \equiv 1 \pmod 5$$

and

$$60\, y_4 \equiv 1 \pmod 7$$

Solving the above eqn which is satisfies by

$y_1 = 1$, $y_2 = 2$, $y_3 = -1$ and $y_4 = 2$

Thus the solutions are

$$x = (1 \cdot 105 \cdot 1) + (2 \cdot 140 \cdot 2) + (3 \cdot 84 \cdot (-1)) + (5 \cdot 60 \cdot 2)$$

$$\equiv 105 + 4 \times 140 - 3 \times 84 + 10 \times 60$$

$$\equiv 1013$$

$$x \equiv 173 \pmod{420}.$$

③ Solve the system of congruences

$$x \equiv 1 \pmod 3,\ x \equiv 2 \pmod 5 \text{ \& } x \equiv 3 \pmod 7$$

Sol given $m_1 = 3$, $m_2 = 5$ \& $m_3 = 7$ are pairwise relatively prime.

by the chinese Remainder Theorem

linear system has a unique solution.

to find it, first we find $m_1, m_2, m_3; y_1, y_2 \& y_3$

$$M_1 = \frac{M}{m_1} = \frac{3\times5\times7}{3} = 35$$

$$M_2 = \frac{M}{m_2} = \frac{3\times5\times7}{5} = 21$$

$$M_3 = \frac{M}{m_3} = \frac{3\times5\times7}{7} = 15$$

Now to find $y_1, y_2 \& y_3$

y_1 is the solution of the congruence

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

i-e $35\, y_1 \equiv 1 \pmod 3$

$(-1)\, y_1 \equiv 1 \pmod 3$

$y_1 \equiv 2 \pmod 3$

lly $M_2 y_2 = 1 \pmod{m_2}$

$\Rightarrow$ $21 y_2 \equiv 1 \pmod 5$

$y_2 \equiv 1 \pmod 5$

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

$15 y_3 \equiv 1 \pmod 7$

$y_3 \equiv 1 \pmod 7$

∴ By chinese Remainder Theorem we have

$$x \equiv \sum_1^3 a_i M_i y_i \pmod M$$

$$\equiv 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1 \pmod{105}$$

$$x \equiv 52 \pmod{105}$$

∴ 52 is the unique solution of the linear system modulo 105.

Hence the general solution is

$$x = 52 + 105t.$$

(4) Solve The linear system

$$x \equiv 1 \pmod 3, \quad x \equiv 2 \pmod 4 \text{ \& } x \equiv 3 \pmod 5$$

Sol Given $m_1 = 3, m_2 = 4$ \& $m_3 = 5$

First to find M_1, M_2 \& M_3

$$M_1 = \frac{M}{m_1} = \frac{3 \cdot 4 \cdot 5}{3} = 20$$

$$M_2 = \frac{M}{m_2} = \frac{3 \cdot 4 \cdot 5}{4} = 15$$

$$M_3 = \frac{M}{m_3} = \frac{3 \cdot 4 \cdot 5}{5} = 12$$

∴ the unique sol of The congruence is

$$M_1 y_1 \equiv 1 \pmod{m_1}, \quad M_2 y_2 \equiv 1 \pmod{m_2}$$

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

i.e $20 y_1 \equiv 1 \pmod 3$, $15 y_2 \equiv 1 \pmod 4$

and

$$12 y_3 \equiv 1 \pmod 5$$

which are satisfy when $y_1 = 2$, $y_2 = 3$ \& $y_3 = 3$ Ans

By chines remainder Theorem

$$x \equiv \sum_{1}^{3} a_i M_i y_i \pmod{M}$$

$$\equiv 1 \times 20 \times 2 + 2 \times 15 \times 3 + 3 \times 12 \times 3 \pmod{60}$$

$$x \equiv 58 \pmod{60}$$

Hence the result.

(5) Solve the system of congruence

$$x \equiv 3 \pmod{7}$$
$$x \equiv 7 \pmod{12}$$
$$x \equiv 4 \pmod{17}$$

Ans This solution is left for students exercise.

General linear systems: The chinese Remainder Theorem establishes a solution to a linear system with pairwise relatively prime moduli and it shows the solution is unique. If it does not unique however, indicate anything about a system where

The moduli are not necessarily pairwise relatively prime. We will establish a necessary and sufficient condition for such system to be solvable.

Note: The linear system of congruence

$x \equiv a \pmod{m}$

$x \equiv b \pmod{n}$ is solvable $\Leftrightarrow (m,n) / (a-b)$.

when it is solvable then the solution is modulo (m,n).

Ex: Determine if the following linear systems are solvable. (i) $x \equiv 3 \pmod 6$, $x \equiv 5 \pmod 8$ (ii) $x \equiv 7 \pmod 9$, $x \equiv 11 \pmod{12}$

Sol (i) Since $(6,8) = 2$ and $2 / 3-5$ the first linear system has a solution.

(ii) we have $(9,12) = 3$ but $3 / 7-11$

so the second system is not solvable.

② Determine if the following linear systems aresdvable.

(i) $x \equiv 4 \pmod 6$
$x \equiv 2 \pmod 8$
$x \equiv 1 \pmod 9$

(ii) $x \equiv 3 \pmod 4$
$x \equiv 5 \pmod 9$
$x \equiv 8 \pmod{12}$

Sol ① we have $(6,8) \mid (4-2), (8,9) \mid (2-1)$; and

$(6,9) \mid 4-1$

∴ The first linear system has a solution

② we have $(4,9) \mid (3-5), \nmid (9,12) \mid (5-9)$, but

$(4,12) = 4$ and $4 \mid (3-8)$.

so The second system is not solvable.

System of linear congruence for two variables.

P. In previous we discused linear congruence for single variable, Now we demonstrated in detail detail how to solve system of linear congruence for two variables with same modules 'm'.

The linear congruence for two variables of the form

$$ax+by \equiv e \pmod{m}$$

$$cx+dy \equiv f \pmod{m}$$

A solution of the linear system is a pair $x \equiv x_0 \pmod{m}$, $y \equiv y_0 \pmod{m}$ that satisfies both congruences.

Examples:

① Show that $x \equiv 12 \pmod{13}$ and $y \equiv 2 \pmod{13}$ is a solution of the 2×2 linear system (or) (two variables)

$$2x+3y \equiv 4 \pmod{13}$$

$$3x+4y \equiv 5 \pmod{13}$$

Sol When $x \equiv 12 \pmod{13}$ and $y \equiv 2 \pmod{13}$

$$2x+3y \equiv 2(12)+3(2) \equiv 4 \pmod{13}$$

$$3x+4y \equiv 3(12)+4(2) \equiv 5 \pmod{13}$$

$\therefore$ every pair $x \equiv 12 \pmod{13}$, $y \equiv 2 \pmod{13}$ is a solution of the system.

∴ The general solution of the system is

$$x = 12 + 13t \quad \& \quad y = 2 + 13t$$

where 't' is an arbitrary integer.

② Use the method of elimination to solve the linear system $2x + 3y \equiv 4 \pmod{13}$

$$3x + 4y \equiv 5 \pmod{13}$$

Sol Given linear system of congruences are

$$2x + 3y \equiv 4 \pmod{13} \quad \rightarrow ①$$

$$3x + 4y \equiv 5 \pmod{13} \quad \rightarrow ②$$

To eliminating 'y', multiplying eq^n ① with '4' and multiplying eq^n no ② with '3'.

$$8x + 12y \equiv 3 \pmod{13}$$

$$9x + 12y \equiv 2 \pmod{13}$$

Substracting we get $-x \equiv 1 \pmod{13}$

$$x \equiv 12 \pmod{13}$$

for finding 'y' substitute 'x' in eqn ①

$$2 \times 12 + 3(y) \equiv 4 \pmod{13}$$

$$3y \equiv -7 \pmod{13}$$

$$y \equiv 2 \pmod{13}$$

Hence $x \equiv 12 \pmod{13}$ and

$$y \equiv 2 \pmod{13}$$