Chapter # III
THEORY OF PRIMES

Primes: (book P#41)

Definition:-3.1

An integer $p>1$, is called a prime Number, if ± 1 and $\pm p$ are Its only divisors.

Example:

The integers 2, 3, 5, 11 and 13 are primes.

Definition:-3.2

An integer $n>1$, which is not a prime, is called a Composite Number.

We note that n is composite if and only if n can written as a product of two integers $n_1, n_2 > 1$

Example:

The integers 4, 6, 8, 9, 10 and 12 are Composite.

Notes:-

(1) The integer 1 is neither prime nor Composite.
(2) 2 is the only even prime number.
(3) Throughout this chapter, we will consider only positive divisors of positive integers.

Definition:-3.3

Any prime number p which divides an integer n is called prime divisor of n.

The greatest prime number is $2^{77,232,917}-1$ a number with 23,249,425 digits it was found in 2016 by Great Internet Mersenne search (GIMPS). It is also known as M74,207,281. It is almost 5 million digits larger than the previous record prime number. Mersenne prime number is of 2^p-1

Theorem:- 3.1 (book P#:42)

Every integer $n>1$ has a prime divisor.

Proof:-

Since $n>1$, so it is either prime or Composite.

Case I:-

Let 'n' is prime then n/n

$\Rightarrow$ 'n' has a prime divisor which is itself 'n'

Case II:-

Let 'n' be Composite and 'd' is the least divisor of 'n' then we claim that 'd' is prime.

Suppose that 'd' is Composite then

$$d = d_1 d_2$$

Where

$$1 < d_1, d_2 < d$$

Since $d_1, d_2 / d$ and d/n then d_1/n & d_2/n.

Where $1 < d_1, d_2 < d$

Which is contradiction to the choice that 'd' is the least divisor of 'n'. Hence our Supposition is Wrong. This proves the truthness of our claim that 'd' is prime.

So this proves that every integer $n>1$ has a prime divisor.

Hence if P/ab

then P/a or P/b. "Proved."

Theorem #3.3 (book P#=12)

If 'P' is a prime and $P/a_1a_2\ldots a_m$, then P/a_i for some i $(1 \leq i \leq m)$

PROOF:-

It is given that

1. P is a prime.
2. $P/a_1a_2\ldots a_m$

We prove that P/a_i for some i $(1 \leq i \leq m)$. We prove this theorem by Mathematical Induction.

Case I:-

When $m=2$

then P/a_1a_2

$\Rightarrow$ P/a_1 or P/a_2

Which is true.

Case II:-

Let us suppose that it is true for $m=k$.

i.e

if $P/a_1a_2\ldots a_k$

then

P/a_1 or P/a_2 ..... or P/a_k

THEOREM #3.2 (book P#:42)

If 'p' is a prime and $p \mid ab$ where $a, b \in z$ then either $p \mid a$ or $p \mid b$.

PROOF

It is given that

(i) p is prime

(ii) $p \mid ab$ where $a, b \in z$

We have to prove that $p \mid a$ or $p \mid b$

Let $p \nmid b$ then

$\Rightarrow (p, b) = 1$

$\Rightarrow \exists\ x, y \in z$ such that

$$px + by = 1$$

Multiplying by 'a'

$$apx + aby = a \rightarrow (1)$$

Since

$$p \mid apx$$

and

$$p \mid aby \qquad \therefore p \mid ab$$

$\Rightarrow p \mid apx + aby$

$\Rightarrow p \mid a \rightarrow$ by (1)

i.e

If $p \nmid b$ then $p \mid a$

Similarly

If $p \nmid a$ then we can prove that $p \mid b$.

Case III:-

Now we prove that the result is true for $m=k+1$

$\Rightarrow P/(a_1a_2\ldots\ldots a_k)a_{k+1}$

$\Rightarrow P/a_1a_2\ldots\ldots a_k$ or P/a_{k+1} by (C-I)

$\Rightarrow P/a_1$ or $P/a_2\ldots\ldots P/a_k$ or P/a_{k+1} by (C-2)

$\Rightarrow P/a_1$ or $P/a_2\ldots\ldots$ or P/a_{k+1}

The result is true for $m=k+1$.

Hence by mathematical induction we conclude that the theorem is true for every positive integer 'm'

i.e

if $P/a_1a_2\ldots\ldots a_m$

then P/a_i for some $i\ (1\leq i\leq m)$

Where 'P' is a prime.

(Proved)

Theorem:- 3.4 (book P#43)

This theorem is named as

"FUNDAMENTAL THEOREM OF ARITHMETIC"

OR

"UNIQUE FACTORIZATION THEOREM"

Statement:-

Every integer $n>1$ can be represented as a product of primes and this representation is Unique except for the order in which they are written.

PROOF:-

We prove this theorem by "Mathematical Induction"

Case I:-

When $n=2$

then $2=2$

Which is true.

Case II:-

Let us Suppose that the theorem is true for

$n=3, 4, 5, \ldots k-1$

Case III:-

Now we prove that the result is true for $n=k$

i) C-1

Where 'k' is prime then k/k.

ii) C-2

Where 'k' is Composite then

$k = k_1 k_2$

Where $(1 < k_1, k_2 < k)$

Since $1 < k_1, k_2 < k$

So by case II k_1 and k_2 can be expressed as product of primes.

Since 'k' is the product of 'k_1' and 'k_2' so, We conclude that 'k' is expressed as a product of primes.

Hence by Mathematical Induction we Conclude that every integer $n>1$ can be expressed as a product of primes.

Uniqueness:-

Now we prove that the representation of 'n' as a product of primes is unique.

Let there be two different representation of 'n'

(1) $n = P_1 \cdot P_2 \cdot P_3 \ldots P_i$

(2) $n = q_1 \cdot q_2 \ldots q_j$

$\Rightarrow P_1 \cdot P_2 \ldots P_i = q_1 \cdot q_2 \ldots q_j \rightarrow (4)$

We cancel the common primes on both sides (if any) and get.

$P_1 \cdot P_2 \ldots P_k = q_1 \cdot q_2 \ldots q_t \rightarrow (2)$

Where 'P's and 'q's are all different primes. $\longrightarrow (3)$

From expression (2) We conclude that

$P_1 \mid q_1 q_2 \ldots q_t$

$\Rightarrow$

$P_1 \mid q_1$ or $P_1 \mid q_2 \ldots$ or $P_1 \mid q_t$

For definiteness we ~~conclude~~ Suppose

$P_1 \mid q_1 \Rightarrow P_1 = q_1$

Which is contradiction to the theorem Statement given in (3)

Hence our supposition that 'n' has two representation is wrong. This proves that the representation of $n > 1$ as a product of primes is unique except for the order in which primes are written.

Example:- (book P#-45)

Show that none of the following (n-1) consective integers is prime.

$n!+2, n!+3, n!+4, \ldots\ldots n!+n$

Hence show that given a positive integer N, it is always possible to find N consective Composite integers.

Solution:-

The integer $n!+2 = 1.2.3\ldots\ldots n+2$ is obviously divisible by 2. Similarly the integer $n!+3$ is divisible by 3 and so on. Finally $n!+n$ is divisible by n. Hence the given integers are not prime.

If N is a given integer, then the following N consective integers are Composite.

$(N+1)!+2, (N+1)!+3, \ldots\ldots (N+1)!+N+1$

FOR KNOWLEDGE

The greatest prime number is $2^{74,207,281}$ a number with 22,338,618 digits. It was found in 2016 by Great Internet Mersenne prime search (GIMPS). It is also known as M74,207,281. It is almost 5 million digits larger than the previous record prime number. Mersenne prime number is of the form $2^p - 1$.

EXERCISE # 1 (book Pg. 115)

1) If 'p' is a prime such that $p \mid a^2+b^2$, and $p \mid a$, then $p \mid b$

Solution:-

It is given that

① $p \mid a^2+b^2$

② $p \mid a$ where 'p' is prime.

then We have to prove that

$p \mid b$

Since

$p \mid a$ so $p \mid a^2$

Since

$p \mid a^2$ and $p \mid a^2+b^2$

So $p \mid b^2 \Rightarrow p \mid b.b$

$\Rightarrow$ $p \mid b$ or $p \mid b$

$\Rightarrow p \mid b$ "Proved"

2) Show that all the primes except 2, are of the form $4n-1$ or $4n+1$.

Solution:-

We have to show that all the primes except 2 are of the form $4n-1$ or $4n+1$.

Let $a, b \in Z$ such that

① a is any integer

② $b > 0$

An expression in Euclid theorem is

$a = bq + r \rightarrow (1) \qquad 0 \leq r < b$

We put

$a = a$, $q = n$

$b = 4$ and $r = r$ in (1)

$\therefore a = 4n + r \quad ; \quad 0 \leq r < 4$

i.e $r = 0, 1, 2, 3$ then

$a = 4n$, $4n+1$, $4n+2$, $4n+3$

When $4n$, $4n+2$ are even integers. Prime 2 is of the form $4n+2$ at $n=0$

$4n+1$ and $4n+3$ are odd integers.

So every integer (prime) except 2 is of the form $4n-1$ or $4n+1$.

"Hence it is proved"

(7) Show that every positive integer of the form $3n+2$ has a prime divisor of the form $3n+2$.

Solution:-

We have to show that every +ive integer of the form $3n+2$ has a prime divisor of the form $3n+2$.

Case (1)

Let (n') is prime then $n' | n'$

Hence (n') is a prime divisor of the form $3n+2$ which is itself.

Case ②

Let (n') be Composite. We know that all primes except 3 are of the form $3n+1$ or $3n+2$.

When (n') is expressed as a product of primes then these primes are of the form $3n+1$, $3n+2$.

Let us Suppose that the primes in the standard form of (n') are of the form $3n+1$. Then their product will also of the form $3n+1$.

Which is contradiction to the fact that (n') is of the form $3n+2$. Hence our Supposition is Wrong. This proves that there exist at least one prime divisor of (n') Which is also of the form $3n+2$.

(Proved).

Theorem 3.5: (book P#46)

Every Composite number n has a prime divisor $\leq \sqrt{n}$

Proof:

Since 'n' is composite number & it has a least prime divisor P.

We claim that $P \leq \sqrt{n}$

OR We want to Prove that $P \leq \sqrt{n}$

Where $n = Pn_1 \rightarrow (1)$ $n_1 \in Z$

Let us contrary suppose that

$P \nleq \sqrt{n}$

then

$P > \sqrt{n}$ then from (1)

We get

$n_1 < \sqrt{n}$

and $n_1 < P$ $(\because n_1 < \sqrt{n} < P)$

Since $n = Pn_1$ and $n_1 < P$ so 'P' is not the least divisor of 'n' which is contradiction to the choice that 'P' is the least prime divisor of 'n'.

Hence Our supposition is Wrong, this proves the truthness of our claim that

$P \leq \sqrt{n}$

Hence this Completes the Proof.

Example:- (book p#47)

Find all the primes less than or equal to 30.

Solution:- 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30.

Therefore the primes ≤ 30 are
2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Note:- (FOR KNOWLEDGE)
With the help of Eratosthenes, many tables of primes have been constituted. Recently, Baker and Gruenberger have found all primes ≤ 109,395,301 which are 6,000,000 in number. These tables indicate that the series of primes is infinite. In fact one can prove the following theorem which is due to Euclid.

Theorem (3.6) (book p#47)
The number of primes is infinite.

Proof:-
We want to prove that number of primes is infinte and these primes are
2, 3, 5, 7, 11, ... P
Where P is last prime number.
Now Contrary Suppose that number of primes is finite.

$2 \cdot 3 \cdot 5 = 30 + 1 = 31$ Prime

$2 \cdot 3 \cdot 5 \cdot 7 = 210 + 1 = 211$ Prime

2, 3, 5, 7 Prime

i can be divided by 1 and in itself only

$n' = (2.3.5.7.\ldots\ldots P)+1$

We see that

$2 \nmid n'$, $3 \nmid n'$, $5 \nmid n'$, $\ldots\ldots P \nmid n'$

this shows that n' has no prime divisor which is contradiction to the fact that every integer $n>1$ has a prime divisor.

Hence our supposition is Wrong, this proves that number of prime is infinite.

(Proved).

Theorem 3.7 (book P#48)

There exist infinitely many primes of the form $4n-1$ or $4n+3$.

Proof:-

Let us contrary suppose that the number of the primes of the form $4n-1$ is finite and these primes are

$3, 7, 11, \ldots P$

Where P is the last prime of the form $4n-1$.

Now consider a number

$n' = 4(3.7.11\ldots\ldots P)-1 \rightarrow (1)$

We know that all the primes except '2' of the form $4n-1$ or $4n+1$.

When 'n' is expressed as a product of primes then these primes are of the form $4n-1$ or $4n+1$.

We see that
$3 \nmid n'$, $7 \nmid n'$, ... $P \nmid n'$

Which shows that the primes of the form $4n-1$ are not the divisor of 'n'.

Then we conclude that all the prime factors of (n') are of the form $4n+1$.

The product of primes is also of the form $4n+1$ but n' is not of the form $4n+1$.

Hence our supposition is Wrong. So we conclude that the primes of the form $4n-1$ or $4n+3$ are infinite.

"Proved"

CHAPTER #4

THEORY OF NUMBER

Definition:

(i) **CONGORENCES:-**

Let m be a fixed positive integer then 'a' is said to be congurent to 'b' if $m|a-b$

It is represented as

$a \equiv b \pmod{m}$

(ii) $a \equiv b \pmod{m}$ iff a, b leave the same remainder after division by 'm' then 'a' is congurent to 'b'.

For example:-

(i) $-8 \equiv 2 \pmod{5}$

(ii) $5 \equiv 2 \pmod{3}$

(iii) $15 \equiv 1 \pmod{7}$

RESIDUE:-

If $a \equiv b \pmod{m}$ then 'a' is called residue of 'b' and 'b' is called residue of 'a'

CONGURENCE RELATIONS:-

(i) If 'a' and 'b' such that $a \equiv b \pmod{m}$ then relation between 'a' and 'b' is called congurance relations.

(ii) Let 'm' be a fixed positive integer then the statement "$a \equiv b \pmod{m}$" is either true or false for any ordered pair $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. So it is defined as relation in $\mathbb{Z}$ called the congurance relation or simply called

congurance modulus 'm'.

EQUIVALENCE RELATION:

A relation is said to be equivalence if it satisfy following three properties.

(i) Reflexive Property
(ii) Symmetric Property
(iii) Transitive Property

For Example:

Congurance relation is an equivalence relation in Z.

THEOREM 1:

Prove that congurance relation is an equivalence relation in Z.

PROOF:

To prove this theorem we show that three properties of an equivalence relations are satisfied by the relation $a \equiv b \pmod m$.

(i) Reflexive property:-

Since $m/a-a$ therefore $a \equiv a \pmod m$

(ii) Symmetric property:-

If $m/a-b$ then $m/b-a$

If $a \equiv b \pmod m$

then $b \equiv a \pmod m$.

(iii) Transitive property:-

If $m/a-b$ and $m/b-c$ then

$m/a-b+(b-c)$ or $m/a-c$

If $a \equiv b \pmod m$ and $b \equiv c \pmod m$ then $a \equiv c \pmod m$

Hence it is proved that the congurance relation is an equivalence relation.

THEOREM 3:-

Statement

If a, b, c, d are integers such that $a \equiv b \pmod m$ and $c \equiv d \pmod m$ then

(i) $a+c \equiv b+d \pmod m$

(ii) $a-c \equiv b-d \pmod m$

(iii) $ac \equiv bd \pmod m$

Proof:-

(i) Since $a \equiv b \pmod m$

and $c \equiv d \pmod m$

$\therefore m/a-b$ and $m/c-d$

Then $\exists$ unique integers q_1, q_2 such that

$a-b = mq_1 \longrightarrow (i)$

$c-d = mq_2 \longrightarrow (ii)$

By adding eq (i) and (ii) We get

$(a+c)-(b+d) = m(q_1+q_2)$

$\Rightarrow m/(a+c)-(b+d)$ ($\because$ m is factor of $(a+c)-(b+d)$.

$\Rightarrow a+c \equiv b+d \pmod m$

Which is required result.

(ii) Since $a \equiv b \pmod m$

$c \equiv d \pmod m$

$\therefore m/a-b$ & $m/c-d$

There exist unique integers q_1, q_2 such

that

$a-b = mq_1 \rightarrow (i)$

$c-d = mq_2 \rightarrow (ii)$

By subtracting eq (i) and (ii)

$(a-c)-(b-d) = m(q_1-q_2)$

$\Rightarrow m/(a-c)-(b-d)$ $\because$ (m is factor of $(a-c)-(b-d)$)

$\Rightarrow a-c \equiv b-d \pmod m$

Which is required result.

iii) Since $a \equiv b \pmod m$

and $c \equiv d \pmod m$

$\therefore m/a-b$ and $m/c-d$

Then $\exists$ unique integers q_1, q_2 such that

$a-b = mq_1 \rightarrow (i)$

$c-d = mq_2 \rightarrow (ii)$

From eq (i) and (ii)

$a = b+mq_1$

$c = d+mq_2$

By xing both equations

$ac = (b+mq_1)(d+mq_2)$

$ac = bd+mbq_2+mdq_1+m^2q_1q_2$

$ac-bd = m(bq_2+dq_1)+m^2q_1q_2$

So $\because$ m is factor of ac-bd

$m/ac-bd$

$\Rightarrow ac \equiv bd \pmod m$

Which is required Result.

COROLLARIES:-

(i) Statement:- If $a \equiv b \pmod m$ then $na \equiv nb \pmod m$ for all $n \in Z$.

Proof:- It is given that $\forall n \in Z$

$$a \equiv b \pmod m$$

$\Rightarrow m/a-b$

the $\exists\ q \in Z$ such that

$$a-b = mq$$

$\Rightarrow na-nb = nmq$ $\because$ m is factor of na-nb

$\Rightarrow m/na-nb$

$\Rightarrow na \equiv nb \pmod m$.

Which is required Result.

(ii) **Statement**:-

If $a \equiv b \pmod m$ then $a^n \equiv b^n \pmod m$ where n is positive integer.

Proof:- It is give that

If $a \equiv b \pmod m$ then

$\Rightarrow m/a-b$

then $\exists\ q \in Z$ such that

$$a-b = mq$$

$$a = b+mq$$

$$a^n = (b+mq)^n$$

$$a^n = b^n + nb^{n-1}mq + \ldots\ldots (mq)^n$$

$$a^n - b^n = m\left[nb^{n-1}q + \ldots\ldots m^{n-1}q^n\right]$$

$\Rightarrow m/a^n-b^n$ $\because$ m is factor of a^n-b^n

$\Rightarrow a^n \equiv b^n \pmod m$

Which is required Result.

THEOREM 4:- P-68

Statement:-

If $na \equiv nb \pmod{m}$ and $(n,m)=d$

then $a \equiv b \pmod{\frac{m}{d}}$

Proof:-

Since $na \equiv nb \pmod{m}$

then $m \mid na-nb$

then $\exists$ an integer q such that

$$na-nb=mq$$

$$n(a-b)=mq \longrightarrow (1)$$

As $(m,n)=d$ (g.c.d)

$\Rightarrow d \mid m$, $d \mid n$

$\Rightarrow m=m_1 d$, $n=n_1 d$ Where $(m_1,n_1)=1$ i.e relative prime

Consider eq (1)

$$n(a-b)=mq$$

putting the values of m and n

$$n_1 d(a-b)=m_1 dq$$

$$n_1(a-b)=m_1 q$$

$\Rightarrow m_1 \mid (a-b)n_1$ $\because m_1$ is factor of $n_1(a-b)$

As $m_1 \nmid n_1$ (i.e m_1 does not divide n_1) $\because (m_1,n_1)=1$

$\Rightarrow m_1 \mid (a-b)$

So $a \equiv b \pmod{m_1}$

Putting the value of m_1 $\left(\because m_1=\frac{m}{d}\right)$

$\Rightarrow a \equiv b \pmod{\frac{m}{d}}$

Which is required Result.

Exercise (book P#171)

(Q.1) Determine wether the following statements are true or false.

(i) $131 \equiv 14 \pmod{15}$

$\Rightarrow 15 \mid 131-14$

$\Rightarrow 15 \nmid 117$

Hence it is false.

(ii) $132 \equiv 2 \pmod{13}$

$\Rightarrow 13 \mid 132-2$

$13 \mid 130$

Hence it is true.

(iii) $-207 \equiv 2 \pmod{11}$

$\Rightarrow -207 \equiv 2$

$\Rightarrow 11 \mid -207-2$

$11 \mid -209$

Hence it is true.

(Q.2) If $a \equiv b \pmod{m}$ and $(a,m)=1$ then show that $(b,m)=1$.

Solution:-

It is Given that

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

(ii) $(a,m)=1$ (i.e relatively prime).

then $(b,m)=1$

Since $m \mid a-b$

then $\exists$ an integer q such that

$a-b=mq$

$\Rightarrow a=b+mq$

Let $(b,m)=d$

$\Rightarrow d \mid b$, $d \mid m$

so $d|a$

d is a Common divisor of a and m

$\therefore d=1$

$(b,m)=1$

Which is Our Required Result.

$\left.\begin{array}{l} \because d|b, d|mq \\ \Rightarrow d|b+mq \\ \Rightarrow d|a \end{array}\right\} \because (a,m)=1$

(6)) Find the Smallest +ive integer 'n' so that $3^n \equiv 1 \pmod{11}$

Solution:- Put $n=1$

$3^1 \not\equiv 1 \pmod{11}$

Put $n=2$

$3^2 \not\equiv 1 \pmod{11}$

Put $n=3$

$3^3 \not\equiv 1 \pmod{11}$

Put $n=4$

$3^4 \not\equiv 1 \pmod{11}$

Put $n=5$

$3^5 = 1 \pmod{11}$

$n=5$ is required +ive integer.

SOLUTION OF CONGURENCE:-

A congurence of the form $ax \equiv b \pmod m$ where $a \neq 0 \pmod m$ is called a Linear congurence If $(a,m)=d$ and $d|b$, the congurence has solution and if $d \nmid b$ then the congurence has no Solution. If Solutions existi they are d is number.

(1) Solve $3x \equiv 5 \pmod 7$

$\because (3,7)=1$ and $1|5$ therefore the congurence has unique solution.

We try $x = 1,2,3,4,5,6.$

$\because x=4$ satisfies the congurence

$\therefore x \equiv 4 \pmod 7$ is the required Solution

(2) $11x + 9 \equiv 0 \pmod{13}$

$11x \equiv 1-9 \pmod{13}$

~~$11x \equiv 1-9$~~

$\because (11,13)=1$ and $1|-9$

$\therefore$ Congurence has unique solution, We try

$x = \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6.$

Since $x=-2$ satisfies the Congurence

therefore $x \equiv -2 \pmod{13}$

or $x \equiv -2+13 \pmod{13}$

or $x \equiv 11 \pmod{13}$ is required solution.

(3) $17x \equiv 11 \pmod{43}$

$\because (17,43)=1$ and $1|11$

$\therefore$ Congurence has unique Solution

Let $\frac{17x-11}{43} = y$

By Euclidean Algorithm.

$157 = 4 \cdot 36 + 13$

$36 = 2 \cdot 13 + 10$

$13 = 1 \cdot 10 + 3$

$10 = 3 \cdot 3 + 1$

$3 = 1 \cdot 3$

$1 = 10 - 3 \cdot 3$

$= 10 - 3 \cdot [13 - 1 \cdot 10]$

$= 10 - 3 \cdot 13 + 3 \cdot 10$

$= 4 \cdot 10 - 3 \cdot 13$

$= 4 \cdot [36 - 2 \cdot 13] - 3 \cdot 13$

$= 4 \cdot 36 - 11 \cdot 13$

$= 4 \cdot 36 - 11 \cdot [157 - 4 \cdot 36]$

$= 4 \cdot 36 - 11 \cdot 157 + 44 \cdot 36$

$= 48 \cdot 36 - 11 \cdot 157$

$1 = 48 \cdot 36 + 11(-157)$

Xing both sides by 7

$7 = 336 \cdot 36 + 77(-157)$

$x_0 = 336$

$x \equiv 336 \pmod{157}$

OR $x \equiv 336 - 157 \pmod{157}$

or $x \equiv 179 \pmod{157}$

$x \equiv 179 - 157 \pmod{157}$

$x \equiv 22 \pmod{157}$

is the required solution.

Then $17x - 43y = 11$ is the Linear Diophantine equation.

Now $(17, -43) = 1$

By Euclidean Algorithm.

$$43 = 2 \cdot 17 + 9$$
$$17 = 1 \cdot 9 + 8$$
$$9 = 1 \cdot 8 + 1$$
$$1 = 9 - 1 \cdot 8$$
$$= 9 - 1 \cdot [17 - 1 \cdot 9]$$
$$= 9 - 1 \cdot 17 + 1 \cdot 9$$
$$= 2 \cdot 9 - 1 \cdot 17$$
$$= 2 \cdot [43 - 2 \cdot 17] - 1 \cdot 17$$
$$= 2 \cdot 43 - 4 \cdot 17 - 1 \cdot 17$$
$$= 2 \cdot 43 - 5 \cdot 17$$
$$= (-5)17 + (-2)(-43)$$

xing both sides by 11

$$11 = (-55)17 + (-22)(-43)$$
$$x_0 = -55$$
$$\therefore x \equiv -55 + 43 \pmod{43}$$
$$\equiv -12 \pmod{43}$$
$$\equiv -12 + 43 \pmod{43}$$
$$x \equiv 31 \pmod{43}$$

Which is the required solution.

(4) $36x \equiv 7 \pmod{157}$.

$\because (36, 157) = 1$ and $1 \mid 7$

$\therefore$ Congruence has unique solution.

The linear Diophantine equation is

$$36x - 157y = 1$$
$$(36, -157) = 1$$

$21x \equiv 23 \pmod{29}$

$\because \gcd(21, 29) = 1$ and $1 \mid 23$

$\therefore$ Congurence has unique solution.

The Linear Diophantine equation is

$$21x - 29y = 23$$

$$(21, -29) = 1$$

By Euclidean Algorithm.

$$24 = 1021 + 8$$

$$21 = 2 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

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

$$3 = 1 \cdot 2 + 1$$

$$2 = 1 \cdot 2$$

$$1 = 3 - 1 \cdot 2$$

$$= 3 - 1 \cdot [5 - 1 \cdot 3]$$

$$= 3 - 1 \cdot 5 + 1 \cdot 3$$

$$= 2 \cdot 3 - 1 \cdot 5$$

$$= 2 \cdot [8 - 1 \cdot 5] - 1 \cdot 5$$

$$= 2 \cdot 8 - 2 \cdot 5 - 1 \cdot 5$$

$$= 2 \cdot 8 - 3 \cdot 5$$

$$= 2 \cdot 8 - 3 \cdot [21 - 2 \cdot 8]$$

$$= 2 \cdot 8 - 3 \cdot 21 + 6 \cdot 8$$

$$= 2 \cdot 8 - 3 \cdot 21 + 6 \cdot 8$$

$$= 8 \cdot 8 - 32 \, 1$$

$$= 8 \cdot 29 - 8 \cdot 21 - 32 \, 1$$

$$= 8 \cdot 29 - 11 \cdot 21$$

$$1 = (-11)21 + (-8)(-29)$$

Xing both sides by 23

$$23 = (-253)21 + (-184)(-29)$$

$$x_0 = -253$$

$$x \equiv -253 \pmod{29}$$

OR $$x \equiv -253 + 9(29) \pmod{29}$$

$$x \equiv -253 + 261 \pmod{29}$$

or $x \equiv 8 \pmod{29}$ is the required solution.

(6) $34x \equiv 60 \pmod{98}$

$\because (34, 98) = 2$ and $2 \mid 60$

$\therefore$ Congurence has exactly two solutions.

We Solve the Congurence

$17x \equiv 30 \pmod{49}$

The Linear diophantine equation is

$17x - 49y = 30$

$\because (17, -49) = 1$

By Euclidean algorithm.

$49 = 2 \cdot 17 + 15$

$17 = 1 \cdot 15 + 2$

$15 = 2 \cdot 7 + 1$

$7 = 1 \cdot 7$

$1 = 1 \cdot 15 - 2 \cdot 7$

$= 1 \cdot 15 - 7 \cdot [17 - 1 \cdot 15]$

$= 1 \cdot 15 - 7 \cdot 17 + 7 \cdot 15$

$= 8 \cdot 15 - 7 \cdot 17$

$= 8 \cdot [49 - 2 \cdot 17] - 7 \cdot 17$

$= (-8)(-49) + (-23)(17)$

Xing both sides by 30

$30 = (-690)17 + (-240)(-49)$

$x_0 = -690$

$\therefore x \equiv -690 \pmod{49}$

or $x \equiv -690 + 15(49) \pmod{49}$

or $x \equiv 45, 94 \pmod{98}$ are required solutions.

(g) $343x \equiv 201 \pmod{1029}$

$(343, 1029) = 343$

and $343 \nmid 201$

$\therefore$ Congurence has no solution.

Ex: Solve the System of linear congurences

$x \equiv 1 \pmod 2 \longrightarrow$ (i)

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

$x \equiv 3 \pmod 5 \longrightarrow$ (iii)

From (i) $\frac{x-1}{2} = y$

$\Rightarrow x = 1 + 2y$

Put in (ii)

$1 + 2y \equiv 2 \pmod 3$

$2y = 1 \pmod 3$

$2y = 4 \pmod 3$

$y = 2 \pmod 3$

Let $\frac{y-2}{3} = z$

then $y = 2 + 3z$

$\therefore x = 1 + 2(2 + 3z)$

$= 1 + 4 + 6z$

$=$

$x = 5 + 6z \rightarrow$ (iv)

put in (iii)

$5 + 6z = 3 \pmod 5$

$6z = -2 \pmod 5$

$6z = -2 + 20 \pmod 5$

$6z = 18 \pmod 5$

$z = 3 \pmod 5$

$z = 3 + 5t$, $t \in z$

put in (iv)

$x = 5 + 6(3+5t)$

$= 5 + 18 + 30t$

$= 23 + 30t$

$\frac{x-23}{30} = t$

$x = 23 \pmod{30}$

is the required solution.