Chapter 1

Divisibility

The outstanding German Mathematician Karl Friedrich Gauss (1777 – 1855) once said " Mathematics is the queen of the sciences and number theory the queen of Mathematics". Number theory has played a central role in the development of Mathematics and as we shall see in the chapters ahead, the study of number theory is both elegant and beautiful. In this chapter, stress will be laid upon divisibility, greatest common divisor, least common multiple, division algorithm and primes.

1. DIVISIBILITY : We start with some definitions

Def. Natural Numbers : The numbers 1 , 2 , 3 , ... which are used for counting are called natural numbers.

Def. Integers : The numbers .....–3, – 2, – 1, 0, 1, 2, 3, ... are called integers.

Note : In this book we shall use the word number to represent an integer.

Def. Divisibility : A non-zero integer a is said to divide an integer b if there exists an integer c such that

$$b = ac$$

We also represent this fact by saying that a is a divisor of b or b is a multiple of a . Symbolically, we write a/b. If a does not divide b then we write $a \not/ b$.

e.g. $2/10$, because there exists an integer 5 such that $10 = 2.5$ and $2 \not/ 11$, because there does not exist an integer c such that $11 = 2.c$

Theorem 1.1 : Properties of divisibility

(i) Every non-zero integer a divides 0 i.e. $a/0$

Proof : Clearly $a.\ 0 = 0$, so by definition of divisibility , we get $a/0$.

(ii) 1 divides every integer a

Proof : Clearly $a = 1.a$, so by definition of divisibility, we get $1/a$.

(iii) Every non-zero integer divides itself i.e. for any integer a ($\neq 0$), we always have a/a

Proof : Clearly $a = a.1$, where $a \neq 0$, so by definition of divisibility, we get a/a.

(iv) If a and b are integers and a/b, then a/bc for every integer c

Proof : Given that a/b so there exists an integer d such that $b = ad$

Multiplying both sides by c, we get

$$bc = adc = a(dc)$$

So, by definition of divisibility, we obtain a/bc .

(v) If a, b, c are integers such that a/b and b/c, then a/c

Proof : Given that a/b, so by definition of divisibility, there exists an integer d such that

$$b = ad \quad \text{.....(1)}$$

Again given that b/c, so by definition of divisibility there exists an integer e such that

$$c = be \quad \text{.....(2)}$$

Putting the value of b from (1) in (2), we get

$$c = ade = a(de)$$

So, by definition of divisibility we get a/c

(vi) If a, b are natural numbers such that a/b and b/a then $a = b$

Proof : As a, b are natural numbers and a/b, so by definition , there exists a natural number c s.t.

$$b = ac \quad \text{.....(1)}$$

Again b/a so by definition, there exists a natural number d such that

$$a = bd \quad \text{.....(2)}$$

Putting the value of a from (2) in (1), we get

$$b = bdc$$

$$\Rightarrow \quad 1 = dc$$

But c , d are natural numbers and product of two natural numbers is 1 if and only if both of them are 1, so we get $c = 1$ and $d = 1$.

Using $d = 1$ in equation (2) , we get $a = b$

(vii) If a and b are integers such that a/b and b/a then $a = \pm b$

Proof : Given that a/b, so there exists an integer c such that

$$b = ac \quad \text{.....(1)}$$

Again, b/a so there exists an integer d such that

$$a = bd \quad \text{.....(2)}$$

Putting the value of a from (2) in (1), we get

$$b = bdc$$

$$\Rightarrow \quad 1 = dc$$

But c, d are integers and their product is 1 so either both of them are 1 or both of them are -1.

i.e. either $c = 1 , d = 1$ or $c = -1 , d = -1$

Thus $d = \pm 1$ and using it in (2), we get $a = \pm b$

(viii) If a and b are integers such that a/b and $|b| < |a|$, then $b = 0$

Proof : As a / b and a and b are integers so by definition, there exists an integer c such that

$$b = ac \quad \text{.....(1)}$$

We shall prove that $c = 0$. Let if possible, $c \neq 0$, then

$$|c| \geq 1 \quad \Rightarrow \quad |a||c| \geq |a| \quad \text{[Multiplying both sides by } |a|\text{]}$$

$$\Rightarrow \quad |ac| \geq |a| \quad \Rightarrow \quad |b| \geq |a| , \quad \text{which is a contradiction}$$

Hence our supposition is wrong. Therefore $c = 0$, so by (1), we get $b = 0$

(ix) If a, b, c, x, y are integers such that a/b and a/c, then $a/(bx + cy)$

Proof : Given that a / b, so there exists an integer d such that

$$b = ad \quad \text{.....(1)}$$

Again, given that a / c, so there exists an integer e such that

$$c = a e \quad \text{.....(2)}$$

Using values of b and c we have $bx + cy = adx + aey = a(dx + ey)$

So, by definition of divisibility $a /(bx + cy)$

(x) If a , b, c are integers such that a/b and a/c then $a/b+c$ and $a/b-c$ i.e. if a non-zero integer divides two integers then it also divides their sum and difference.

Proof : Taking $x = 1$ and $y = 1$ in part (ix) , we get $a / b + c$

Taking $x = 1$ and $y = -1$ in part (ix), we get $a / b - c$

Def. Even Number : A number which is divisible by 2 is called an even number. e.g. 0, 2, 4, 6, 8, 10, ...

An even number can always be expressed as $2k$, where k is any number.

Def. Odd Number : A number which is not divisible by 2 is called an odd number e.g. 1, 3, 5, 7, 9, ...

An odd number can always be expressed as $2k + 1$, where k is any number.

Remark : Out of two consecutive numbers one is always even and other is odd. e.g. 5 and 6 are consecutive numbers , here 5 is odd and 6 is even.

Also 20 and 21 are consecutive numbers, here 20 is even and 21 is odd.

Example 1 : (i) Prove that product of two even numbers is again an even number.

(ii) Prove that product of two odd numbers is again an odd number.

(iii) Prove that product of an even number and an odd number is an even number.

Solution : (i) Let a and b are two even numbers then they are of the form

$$a = 2k \text{ and } b = 2k' \quad \text{where } k \text{ and } k' \text{ are two integers.}$$

Now, $ab = 2k.2k'$

$= 2(2kk') = 2m$, where $m = 2kk'$

$\Rightarrow$ ab is an even number.

(ii) Let a and b are two odd numbers then they are of the form

$$a = 2k+1 \text{ and } b = 2k'+1 \text{ where } k \text{ and } k' \text{ are two integers}$$

Now, $ab = (2k+1)(2k'+1) = 4kk'+2k+2k'+1$

$= 2(2kk'+k+k')+1 = 2m+1$, where $m = 2kk'+k+k'$

$\Rightarrow$ ab is an odd number.

(iii) Let a be an even and b is an odd number then they are of the form

$$a = 2k \text{ and } b = 2k'+1 \quad \text{where } k \text{ and } k' \text{ are two integers.}$$

Now, $ab = 2k(2k'+1)$

$= 2(2kk'+k) = 2m$, where $m = 2kk' + k$

$\Rightarrow$ ab is an even number.

Example 8 : Prove that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9. **[K.U. 2010 (2nd Sem.)]**

Solution : Let $a = a_n.....a_3\ a_2\ a_1$ be a n-digit integer. Let $S = a_1 + a_2 + a_3 + a_4 + ... + a_n$ be the sum of the digits in the value of a.

Now, we can write
$$\begin{aligned} a &= a_1 + (10)^1 a_2 + (10)^2 a_3 + (10)^3 a_4 + ... + (10)^{n-1} a_n \\ &= a_1 + 10a_2 + 100a_3 + 1000a_4 + ... \\ &= a_1 + (a_2 + 9a_2) + (a_3 + 99a_3) + (a_4 + 999a_4) + ... \\ &= (a_1 + a_2 + a_3 + a_4 + ...) + (9a_2 + 99a_3 + 999a_4 + ...) \\ &= S + 9(a_2 + 11a_3 + 111a_4 + ...) \end{aligned}$$

$$\Rightarrow \quad a - S = 9(a_2 + 11a_3 + 111a_4 + ...)$$

$$\Rightarrow \quad 9/(a - S) \qquad .....(1)$$

Now we prove our result. First suppose that a is divisible by 9 i.e. $9/a$ .....(2)

By (1) and (2), we get, $9/[a - (a - S)] \Rightarrow 9/S$

i.e. sum of digits is divisible by 9.

Conversely, suppose S (the sum of digits) is divisible by 9 i.e. $9/S$ .....(3)

By (1) and (3), we get, $9/[(a - S) + S] \Rightarrow 9/a$

i.e. the integer a is divisible by 9.

Exercise 1.1

1. Show that product of two numbers is even if at least one of them is even.

2. Show that the difference between the square of any number and the number itself is even.

3. **(i)** If x and y are positive integers and if $(x - y)$ is even, show that $(x^2 - y^2)$ is divisible by 4.
(ii) Prove that 4 does not divide $(n^2 + 2)$ for any integer n.

4. **(i)** Show that $2^{2n} + 1$ is divisible by 5 for a positive odd integer n.
(ii) Show that $2^{2n} - 1$ is divisible by 15 for a positive even integer n.
(iii) Prove that $3^{2n} + 7$ is divisible by 8.

5. **(i)** If a and b are two natural numbers such that $(a^2 - b^2)$ is a prime number, show that $a^2 - b^2 = a + b$.
(ii) If $p > 1$ and $2^p - 1$ is prime, then prove that p is prime.

6. Show that :
(i) Every number of the form $4n - 1$ is also of the form $4n + 3$.
(ii) Every number of the form $8k - 1$ is also of the form $8k + 7$.

7. **(i)** Prove that product of two numbers of the form $4n + 1$ is of the form $4n + 1$.
(ii) Prove that product of two numbers of the form $8n + 1$ is of the form $8n + 1$.
(iii) Prove that product of two numbers of the form $8n + 1$ and $8n + 3$ is of the form $8n + 3$.

8. Prove that an integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

2. PROBLEMS ON DIVISIBILITY BY MATHEMATICAL INDUCTION

Theorem 2.1: Product of any r consecutive integers is divisible by $r!$. [M.D.U. 2011]

Proof : Let P_n denotes the product of r consecutive integers beginning with n i.e.

$$P_n = n(n+1)(n+2).....(n+r-1) \quad .....(1)$$

We shall prove the theorem by applying principle of mathematical induction on r.

For $r = 1$, by (1), $P_n = n$ which is divisible by 1! for all n.

Hence the theorem is true for $r = 1$.

As our induction hypothesis, we assume that theorem is true for $r - 1$

i.e. product of any $r - 1$ consecutive integers is divisible by $(r-1)!$ .....(2)

Replacing n by $n + 1$ in (1), we get

$$P_{n+1} = (n+1)(n+2).....(n+r-1)(n+r) \quad .....(3)$$

Subtracting (1) from (3), we get

$$\begin{aligned} P_{n+1} - P_n &= (n+1)(n+2).....(n+r-1)(n+r) - n(n+1)(n+2).....(n+r-1) \\ &= [(n+1)(n+2).....(n+r-1)](n+r-n) \\ &= r(n+1)(n+2).....(n+r-1) \\ &= r \text{ [Product of } (r-1) \text{ consecutive integers]} \end{aligned}$$

$$\Rightarrow \quad P_{n+1} - P_n = rP \quad .....(4)$$

where P denotes the product of $r - 1$ consecutive integers

Now, by (2), P must be divisible by $(r - 1)!$

i.e. $(r-1)!/P \quad \Rightarrow \quad P = m(r-1)!$ for some integer m

Putting this value of P in (4),

$$P_{n+1} - P_n = mr(r-1)! \Rightarrow r!/[P_{n+1} - P_n] \text{ for all } n \quad .....(5)$$

Putting $n = 1$, we get $r!/P_2 - P_1$. Also by (1), we have $P_1 = 1.2.3.....r = r! \Rightarrow r!/P_1$

Therefore, we have $r!/P_2 - P_1 + P_1 \Rightarrow r!/P_2$

Putting $n = 2$ in (4), we have $r!/P_3 - P_2$

So, we have $r!/P_3 - P_2 + P_2 \Rightarrow r!/P_3$

Continuing in same manner, we obtain $r!/P_n$ for all n

COR 1 : ${}^nC_r$ is an integer.

Proof : We have

$$\begin{aligned} {}^nC_r &= \frac{n!}{r!(n-r)!} \quad \text{[By def.]} \\ &= \frac{n(n-1)(n-2).....(n-r+1)(n-r)!}{r!(n-r)!} \\ &= \frac{n(n-1)(n-2).....(n-r+1)}{r!} \\ &= \frac{\text{a product of } r \text{ consecutive integer}}{r!} = \text{an integer} \end{aligned}$$

[$\because r!$ divides the product of any r consecutive integers]

COR 2 : If m, n are positive integers, show that $(m + n)!$ is divisible by $m!\, n!$.

Proof : We have $\dfrac{(m+n)!}{m!n!} = \dfrac{1.2.3.....m(m+1)(m+2)...(m+n)}{1.2.3.....m\, n!}$

$$= \frac{(m+1)(m+2)....(m+n)}{n!}$$

$$= \frac{\text{The Product of } n \text{ consecutive integers}}{n!} = \text{An integer}$$

[$\because$ Product of n consecutive integers is divisible by $n!$]

$\Rightarrow$ $(m + n)!$ is divisible by $m!$. $n!$.

Example 1 : Prove that $n(n + 1)(n + 5)$ is a multiple of 6.

Solution : We have $n(n + 1)(n + 5) = n(n + 1)[(n + 2) + 3]$

$= n(n + 1)(n + 2) + 3n(n + 1)$ .....(1)

Now $n(n+ 1)(n+ 2)$ is product of three consecutive integers so it is divisible by $3! = 6$.

Again $n(n + 1)$ is the product of two consecutive integers so it is divisible by $2! = 2$.

Thus $3n(n + 1)$ is divisible by $3 \times 2 = 6$.

Now, $n(n + 1)(n + 2)$ and $3n(n + 1)$ both are divisible by 6 and so their sum is also divisible by 6 i.e. $n(n+1)(n+2)+3n(n+1)$ is divisible by 6.

Therefore by (1), $n(n + 1)(n + 5)$ is divisible by 6.

Example 2 : For even n show that $n(n^2 + 20)$ is divisible by 48.

Solution : As n is even. Let $n = 2m$

Now, $n(n^2 + 20) = 2m(4m^2 + 20) = 8m(m^2 + 5)$

$= 8m\left[(m^2 - 1) + 6\right] = 8m(m^2 - 1) + 48m$

$= 8(m - 1)m(m + 1) + 48m$ .....(1)

Now $(m - 1)\, m\, (m + 1)$ is the product of three consecutive integers, so it divisible by $3! = 6$ and therefore $(m-1)m(m+1) = 6k$.

Using this value in (1), we get , $n(n^2 + 20) = 8.6k + 48m = 48(k + m)$

$\Rightarrow$ $n(n^2 + 20)$ is divisible by 48, for even n.

Example 3 : Prove that (i) $3^{2n+1} + 2^{n+2}$ is divisible by 7.

(ii) $3^{2n+2} - 8n - 9$ is divisible by 64.

Solution : **(i)** We shall prove the result by Principle of Mathematical Induction.

Let $f(n) = 3^{2n+1} + 2^{n+2}$

Step I. Put $n = 1$, $f(1) = 3^3 + 2^3 = 27 + 8 = 35$ which is divisible by 7.

So, the result in true for $n = 1$

Step II. As our induction hypothesis, we assume that the result in true for some n i.e., $f(n)$ is divisible by 7.

i.e. $(n) = 7k$ for some integer k.

i.e. $3^{2n+1} + 2^{n+2} = 7k$

i.e. $3^{2n+1} = 7k - 2^{n+2}$ .....(1)

Step III. Now we prove that the result is true for $n + 1$ i.e. $f(n + 1)$ is divisible by 7.

Now replacing n by $n + 1$ in $f(n)$, we have

$f(n + 1) = 3^{2(n+1)+1} + 2^{(n+1)+2}$

$= 3^{2n+3} + 2^{n+3}$

$$= 3^2.3^{2n+1} + 2^{n+3}$$
$$= 9.(7k - 2^{n+2}) + 2^{n+3} \quad [\text{By } (1)]$$
$$= 63k - 9.2^{n+2} + 2.2^{n+2}$$
$$= 63k - 7.2^{n+2}$$
$$= 7(9k - 2^{n+2}) \quad \text{which is divisible by 7.}$$

Hence by Principle of Mathematical Induction, $f(n)$ is divisible by 7 for all n.

(ii) We shall prove the result by Principle of Mathematical Induction.

Let $f(n) = 3^{2n+2} - 8n - 9$.

Step I. For $n = 1$, $f(1) = 3^4 - 8 - 9 = 64$ which is divisible by 64.

$\therefore$ The result is true for $n = 1$.

Step II. As our induction hypothesis, we assume that the result is true for n

i.e. $f(n)$ is divisible by 64.

i.e. $3^{2n+2} - 8n - 9 = 64k$

i.e. $3^{2n+2} = 64k + 8n + 9$ .....(1)

Step III. Now we prove that the result is true for $n + 1$

i.e. $f(n + 1)$ is divisible by 64.

Replacing n by $n + 1$ in $f(n)$, we have

$$f(n+1) = 3^{2(n+1)+2} - 8(n+1) - 9$$
$$= 3^{2n+4} - 8n - 17$$
$$= 3^2.3^{2n+2} - 8n - 17$$
$$= 9.3^{2n+2} - 8n - 17$$
$$= 9[64k + 8n + 9] - 8n - 17 \quad [\text{By } (1)]$$
$$= 9.64k + 72n + 81 - 8n - 17$$
$$= 64.9k + 64n + 64$$
$$= 64(9k + n + 1) \text{ which is divisible by 64.}$$

Hence by Principle of Mathematical Induction, $f(n)$ is divisible by 64 for all n.

Exercise 1.2

1. If n is an integer , then prove that

(i) $n(n^2 - 1)$ is a multiple of 6.

(ii) $n(n + 1)(2n + 1)$ is divisible by 6

(iii) $n(n - 1)(2n - 1)$ is divisible by 6.

(iv) $n^5 - 5n^3 + 4n$ is divisible by 120 for $n > 2$.

(v) $n(n^2 - 1)(3n + 2)$ is divisible by 24.

2. Prove the following :

(i) If n is even , then $n(n + 1)(n + 2)$ is divisible by 24.

(ii) If n is odd , then $n(n^2 - 1)$ is divisible by 24.

3. Prove that :

(i) $5^{2n+2} - 24n - 25$ is a multiple of 576.

(ii) $9^n - 8^n - 1$ is divisible by 8.

(iii) $2^{2n+1} - 9n^2 + 3n - 2$ is divisible by 54.

(iv) $3^{2n} - 32n^2 + 24n - 1$ is divisible by 512.

(v) $2.7^n + 3.5^n - 5$ is a multiple of 24.

(vi) $10^n + 3.4^{n+2} + 5$ is divisible by 9.

(vii) $3^{4n+2} + 5^{2n+1}$ is divisible by 14

(viii) $4^{2n+1} + 3^{n+2}$ is a multiple of 13.

---

3. DIVISION ALGORITHM [M.D.U. 2010 (2nd Sem.)]

Theorem 3.1 : Division Algorithm : For any two integers a and b where $b > 0$, there exist unique integers q and r such that $a = bq + r$, $0 \le r < b$
The integers q and r are called the quotient and remainder respectively.

Proof : We consider the following infinite sequence of multiples of b

$$\ldots\ldots -3b, -2b, -b, 0, b, 2b, 3b, \ldots\ldots$$

Now a has two possibilities : either a is equal to one of multiples of b say bq or it lie between two consecutive multiples say bq and $b(q + 1)$.

So we have, $bq \le a < b(q + 1)$ for some q.

Subtracting bq from all three sides, we get $0 \le a - bq < b$ .....(1)

Let $a - bq = r$, and using this value in (1), $0 \le r < b$

Thus , we have , $a = bq + r$, $0 \le r < b$ .....(2)

This proves the existence part.

Uniqueness : Let q_1 and r_1 be another integers such that

$$a = bq_1 + r_1 \quad , \quad 0 \le r_1 < b \qquad \ldots\ldots(3)$$

By (2) and (3), we get $bq + r = bq_1 + r_1$

$$\Rightarrow \quad b(q - q_1) = r_1 - r \qquad \ldots\ldots(6)$$

$$\Rightarrow \quad b / r_1 - r$$

But $0 \le r < b$, $0 \le r_1 < b$ so $r_1 - r$ is numerically less than b i.e. $|r_1 - r| < b$.

So, $r_1 - r = 0 \Rightarrow r_1 = r$

Putting $r_1 = r$ in (6), we get $b(q - q_1) = 0$

$$\Rightarrow \quad q - q_1 = 0 \qquad [\because b \ne 0]$$

$$\Rightarrow \quad q = q_1$$

Hence the uniqueness is proved.

Illustration (i) If $a = 22$ and $b = 6$ then $22 = 6.3 + 4$
i.e. $a = bq + r$, where $q = 3$, $r = 4$

(ii) If $a = -22$ and $b = 6$ then $-22 = 6(-4) + 2$
i.e. $a = bq + r$ where $q = -4$, $r = 2$

Def. Common divisor : A number c dividing two numbers a and b is called a common divisor of a and b. e.g. ± 1 , ± 2 , ± 4 are common divisors of 8 and 12.

Def. Greatest common divisor : The greatest common divisor (g . c . d .) of two integers a and b, not both zero, is the largest positive integer which divides both a and b. It is denoted by (a, b). e.g. $(8, 12) = 4$, $(10, 11) = 1$, $(5, 16) = 1$, $(-15, 20) = 5$, $(5, 0) = 5$

Note : The above definition of g . c . d ., although simple and clear, is not of practical use in the proofs of theorems. So we define g. c. d. symbolically as follows

Def. Greatest Common divisor : A positive integer d is the $g.c.d.$ of two integers a and b if **(i)** d/a and d/b **(ii)** If d'/a and d'/b then d'/d.

Remark : If a/b where a is positive integer then $(a, b) = a$

Proof : We know that a itself is the greatest divisor of a. Also a/b, so a is the largest positive common divisor of a and b i.e. $(a, b) = a$

Def. Co-prime Integers (or Relatively prime integers) : Two integers a and b are said to be co-prime or relatively prime if their $g.c.d.$ is 1 i.e. $(a, b) = 1$.
e.g. $(4, 9) = 1$ i.e. 4 and 9 are co-prime but $(8, 10) = 2$ and so 8 and 10 are not co-prime.

Note : Two co-prime integers need not be both prime . e.g. 4 and 9 are co-prime but they are not prime numbers.

Theorem 3.2 : If $a = bq + r$ then $(a, b) = (b, r)$.
OR The $g.c.d.$ of a and b is the same as $g.c.d.$ of b and r, where r is the remainder obtained on dividing a by b.

Proof : Given that $a = bq + r \Rightarrow a - bq = r$ .....(1)

Let $(a, b) = d$ and $(b, r) = d'$

As $(a, b) = d \Rightarrow d/a$ and d/b
$\Rightarrow d/a$ and d/bq
$\Rightarrow d/a - bq \Rightarrow d/r$ [By (1)]
$\Rightarrow d$ is a common divisor of b and r

But d' is the greatest common divisor of b and r, so by definition of $g.c.d.$, we have
d/d' .....(2)

Again, $(b, r) = d' \Rightarrow d'/b$ and d'/r
$\Rightarrow d'/bq$ and d'/r
$\Rightarrow d'/bq + r \Rightarrow d'/a$ [By (1)]
$\Rightarrow d'$ is a common divisor of a and b

But d is the greatest common divisor of a and b, so by definition of $g.c.d.$, we have
d'/d .....(3)

From (2) and (3), we have $d = d'$ i.e. $(a, b) = (b, r)$

COR: If $(a, b) = 1$, then $(b, r) = (a, b) = 1$ i.e. if a is co-prime to b, then r is co-prime to b where r is the remainder obtained on dividing a by b.

Theorem 3.3 : If $(a,b)=d$ then there exist two integers x and y such that $d=ax+by$. Further d is least positive value of the values $ax + by$ where x and y are integers.

Proof : Applying division algorithm successively, we get the following equations.

Dividing	a by b,	$a = bq_1 + r_1$	, $0 \le r_1 < b$
Dividing	b by r_1,	$b = r_1q_2 + r_2$	, $0 \le r_2 < r_1$
Dividing	r_1 by r_2,	$r_1 = r_2 q_3 + r_3$	, $0 \le r_3 < r_2$
	.....	.....	.....
	.....	.....	.....
Dividing	r_{n-2} by r_{n-1},	$r_{n-2} = r_{n-1}q_n + r_n$	, $0 \le r_n < r_{n-1}$
Dividing	r_{n-1} by r_n,	$r_{n-1} = r_n q_{n+1} + r_{n+1}$	, $0 \le r_{n+1} < r_n$

.....(1)

Thus we have obtained the following sequence of remainder

$$r_1 > r_2 > r_3 > \ldots\ldots\ldots\ldots \geq 0$$

Since the remainders are non-negative and getting smaller and smaller, this sequence must terminate after a finite number of steps . Therefore remainder after a certain stage must be zero so let $r_{n+1} = 0$.

$\therefore$ By last equation of system (1), $\quad r_{n-1} = r_n q_{n+1} + 0$

$\Rightarrow \quad r_n / r_{n-1}$

$\Rightarrow \quad (r_{n-1}, r_n) = r_n \quad [\because$ If a/b then $(a, b) = a]$

Hence by using **Theorem 3.2** on system of equations (1), we obtain

$$(a,b) = (b, r_1) = (r_1, r_2) = \ldots\ldots\ldots = (r_{n-1}, r_n) = r_n$$

$\Rightarrow \quad (a, b) = r_n = d$ (say)

Now by first equation of (1), $\quad r_1 = a - bq_1$

$= ax_1 + by_1 \quad$ where $x_1 = 1, y_1 = -q_1$

Using this value of r_1 in second equation of (1), we get

$$r_2 = b - r_1 q_2 = b - (a - bq_1)q_2$$

$$= b - aq_2 + bq_1 q_2 = a(-q_2) + b(1 + q_1 q_2)$$

$$= ax_2 + by_2$$

where $x_2 = -q_2$ and $y_2 = 1 + q_1 q_2$

Thus $\quad r_2 = ax_2 + by_2$

Continuing like this, we can obtain $\quad r_n = ax_n + by_n$

i.e. $\quad d = ax + by, \quad$ where $d = r_n, x = x_n, y = y_n$

Second Part : As $(a, b) = d \Rightarrow \quad d/a$ and d/b

$\Rightarrow \quad d / ax + by$ for all integers x and y.

$\Rightarrow \quad ax + by = kd$ for an integer k.

Now d, being a *g.c.d.*, is positive so to obtain the least positive value of $ax + by$, we must take $k = 1$. Therefore d is the least positive value of $ax + by$.

Cor : If a and b are co-prime, then $(a, b) = 1$, so by **Theorem 3.3** there exist integers x and y such that $\quad 1 = ax + by$

Remark : Converse of **Theorem 3.3** is not true in general. However converse of **COR** is always true. e.g. $2(12) + (-1)\,6 = 18$ but g.c.d of 12 and 6 is not equal to 18. In fact *g.c.d.* of 12 and 6 is 6.

Let us prove the converse of corollary i.e.

If there exist integers x and y s.t. $ax + by = 1$, then $(a, b) = 1$.

Proof : Let $\quad d = (a, b)$

$\Rightarrow \quad d/a$ and $d/b \quad \Rightarrow \quad d/(ax + by)$

$\Rightarrow \quad d/1 \quad [\because ax + by = 1]$

$\Rightarrow \quad d = 1.$

Example 1: Find the *g.c.d.* of 858 and 325 and express it in the form *m*.858+*n*.325.

Solution : $\quad 858 = 325.2 + 208 \quad \ldots\ldots(1) \quad$ (dividing 858 by 325)

$325 = 208.1 + 117 \quad \ldots\ldots(2) \quad$ (dividing 325 by 208)

$208 = 117.1 + 91$ .....(3) (dividing 208 by 117)
$117 = 91.1 + 26$ .....(4) (dividing 117 by 91)
$91 = 26.3 + 13$ .....(5) (dividing 91 by 26)
$26 = 13.2$

The last non-zero remainder in this procedure is the *g.c.d.*, so *g.c.d.* of 858 and 325 is $d = 13$.

Now from (5), $d = 13 = 91 - 26.3$
$= 91 - 3(117 - 91.1)$ [By (4), $26 = 117 - 91.1$]
$= 91 - 3.117 + 3.91$
$= 4.91 - 3.117$
$= 4(208 - 117.1) - 3.117$ [By (3), $91 = 208 - 117.1$]
$= 4.208 - 4.117 - 3.117$
$= 4.208 - 7.117$
$= 4.208 - 7(325 - 208.1)$ [By (2), $117 = 325 - 208.1$]
$= 4.208 - 7.325 + 7.208$
$= 11.208 - 7.325$
$= 11(858 - 325.2) - 7.325$ [By (1), $208 = 858 - 325.2$]
$= 11.858 - 22.325 - 7.325$
$= 11.858 - 29.325$
$= m \cdot 858 + n \cdot 325$, where $m = 11$ and $n = -29$

Theorem 3.4 : Gauss Theorem : If a/bc and $(a, b) = 1$, then a/c
[M.D.U. 1996 ; K.U. 1996]

Proof : Given that a/bc so there exists an integer d s.t. $bc = ad$ .....(1)
Now, $(a, b) = 1$ (given) so there exist integers m and n such that
$am + bn = 1$
Multiplying both sides by c, we get $acm + bcn = c$
$\Rightarrow$ $acm + adn = c$ [By (1), $bc = ad$]
$\Rightarrow$ $a(cm + dn) = c$ $\Rightarrow$ a/c

Theorem 3.5 : If a/c, b/c and $(a, b) = 1$ then ab/c
OR If two co-prime numbers divide the same number, then their product will also divide the same number.

Proof : As a/c, so there exists an integer m s.t. $c = am$ .....(1)
Again as b/c, so there exists an integer n s.t. $c = bn$ .....(2)
Now as $(a, b) = 1$, so by **Theorem 3.3** there exist two integers x and y s.t.
$ax + by = 1$ .....(3)
Multiplying both sides of (3) by c, we get
$c(ax) + c(by) = c$
$\Rightarrow$ $bn(ax) + am(by) = c$ [Using $c = am$, $c = bn$ by (1) and (2)]
$\Rightarrow$ $abnx + abmy = c$
$\Rightarrow$ $ab(nx + my) = c$
$\Rightarrow$ ab/c [By definition of divisibility]

Example 2 : If p is a prime number and a is any integer, then either p/a or $(p, a) = 1$
OR If p is a prime number and a is any integer then either p divides a or p is co-prime to a

Solution : Let $(p, a) = d$

$\Rightarrow$ d/p and d/a .....(1)

Now d/p and p is a prime number and only divisors of a prime number are 1 and p itself so either $d = 1$ or $d = p$

If $d = 1$, then $(p, a) = d = 1$ i.e. p is co-prime to a.

If $d = p$, then $d/a \Rightarrow p/a$

Thus either p divides a or p is co-prime to a.

Theorem 3.6: If p is prime, and p/ab, prove that p/a or p/b.

[M.D.U. 2010 ; K.U. 2011]

Proof : As p/ab, so by definition of divisibility, there exist an integer c s.t.

$ab = pc$ .....(1)

Now p is a prime, and a is an integer so either p divides a or p is co-prime to a i.e. p/a or $(p, a) = 1$

If p/a then there is nothing to prove.

If $(p, a) = 1$ then there exist integers m and n such that $pm + an = 1$

Multiplying both sides by b, we get $pmb + abn = b$

Putting $ab = pc$ by (1) in (2), we get $pmb + pcn = b$ .....(2)

$\Rightarrow$ $p(mb + nc) = b \Rightarrow p/b$

Generalisation of Theorem 3.6 : If p is prime and divides the product $a_1 . a_2 . \ldots\ldots a_k$; then p must divide at least one of $a_1 , a_2 , \ldots\ldots , a_k$.

Def. Least Common Multiple (l.c.m.) : The least common multiple of two integers a and b is the least positive integer divisible by both a and b ; it is denoted by $[a , b]$

OR

An integer m is called the least common multiple of a and b if

(i) a/m and b/m **(ii)** If a/c and b/c then m/c

Theorem 3.7 : Prove that the product of two numbers is equal to the product of their *l.c.m.* and *g.c.d.*

OR **If a , b are any two numbers , then $a . b = [a , b].(a , b)$**

Proof : Let a and b be any two numbers such that $(a , b) = d$ and $[a , b] = m$

As $(a , b) = d$, so d/a and d/b

$\therefore$ there exist integers a_1 and b_1 such that

$a = a_1 d$ and $b = b_1 d$ where $(a_1 , b_1) = 1$ .....(1)

Now $a = a_1 d \Rightarrow a/a_1 b_1 d$ and $b = b_1 d \Rightarrow b/a_1 b_1 d$

Therefore , $a_1 b_1 d$ is a common multiple of a and b.

Let c be any other common multiple of a and b , then a/c and b/c and therefore there exist integers c_1 and c_2 such that $c = ac_1$ and $c = bc_2$ .....(2)

$\Rightarrow$ $ac_1 = bc_2$

$\Rightarrow$ $a_1 dc_1 = b_1 dc_2$ [Using values of a and b from (1)]

$\Rightarrow$ $a_1 c_1 = b_1 c_2$

$\Rightarrow$ $a_1 / b_1 c_2$

$\Rightarrow$ a_1 / c_2 [$\because (a_1 , b_1) = 1$]

$c_2 = ka_1$ where k is an integer

Putting this value of c_2 in $c = bc_2$, we get,

$$c = bka_1 = b_1dka_1 \quad [\because b = b_1d]$$
$$= (a_1b_1d)k$$
$$\Rightarrow \quad a_1b_1d/c \qquad \text{.....(3)}$$

From (2) and (3), it is clear that a_1b_1d is the least common multiple of a and b.

$\therefore \quad a_1b_1d = m$

$\Rightarrow \quad (a_1d)(b_1d) = md$

$\Rightarrow \quad ab = [a, b](a, b)$

$\Rightarrow$ the product of two numbers is equal to the product of their *l.c.m.* and *g.c.d.*

Remark : The above theorem is useful in finding the *l.c.m.* of two given numbers as shown in the next example.

Example 3 : Find the *l. c. m.* of the following : (i) 272, 1479 (ii) 26, 195

Solution : We know that

(*l. c. m.* of a and b) × (*g. c. d* of a and b) = product of a and b.

$$\Rightarrow \quad l.\ c.\ m.\ \text{of } a \text{ and } b = \frac{\text{product of } a \text{ and } b}{g.\ c.\ d.\ \text{of } a \text{ and } b} \qquad \text{.....(1)}$$

We shall use the relation (1) to find *l. c. m.* of given numbers.

(i) To find *g. c. d.* of 272 and 1479, we have

$$1479 = 272.5 + 119$$
$$272 = 119.2 + 34$$
$$119 = 34.3 + 17$$
$$34 = 17.2$$

The last non-zero remainder in this procedure is *g.c.d.*, so *g.c.d.* of 272 and 1479 = 17

Now, using (1), *l. c. m.* of 272 and 1479 $= \frac{272 \times 1479}{17} = \frac{402288}{17} = 23664$

(ii) To find *g.c.d.* of 26 and 195, we have

$$195 = 26.7 + 13$$
$$26 = 13.2$$

The last non-zero remainder in this procedure is *g.c.d.*, so *g.c.d.* of 26 and 195 = 13.

Now, using (1), *l.c.m.* of 26 and 195 $= \frac{26 \times 195}{13} = 2 \times 195 = 390$.

Example 4 : (i) If $(a, b) = d$ then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

(ii) Find the positive integer a and b such that $(a, b) = 20$ and $[a, b] = 840$.

Solution : (i) Given that $(a, b) = d$, so d/a and d/b

$$\Rightarrow \quad a = da_1 \qquad \text{.....(1)}$$

and

$$b = db_1 \qquad \text{.....(2)}$$

Again as $(a, b) = d$, so there exist integers m and n such that

$$am + bn = d \qquad \text{.....(3)}$$

Putting the values of a and b from (1) and (2) in (3), we have

$$da_1m + db_1m = d$$

$\Rightarrow \quad a_1 m + b_1 y = 1 \quad \Rightarrow \quad (a_1, b_1) = 1 \quad \Rightarrow \quad \left(\frac{a}{d}, \frac{b}{d}\right) = 1$

(ii) Here $(a, b) = 20$

$\Rightarrow \quad 20/a$ and $20/b$

$\Rightarrow \quad a = 20x$ and $b = 20y$ .....(1)

By part (i) of this example, we have $\left(\frac{a}{20}, \frac{b}{20}\right) = 1$

$\Rightarrow \quad (x, y) = 1$ .....(2)

Further, we know that $(a, b)\,[a, b] = ab$

$\Rightarrow \quad 20.840 = 20x.20y$

$\Rightarrow \quad xy = 42$ .....(3)

The integers satisfying (2) and (3) are

$x = 1$, $y = 42$

$x = 2$, $y = 21$

$x = 3$, $y = 14$

$x = 6$, $y = 7$

Using these values of x and y in (1), the different values of a and b are

$a = 20$, $b = 840$

$a = 40$, $b = 420$

$a = 60$, $b = 280$

$a = 120$, $b = 140$

Note : In above example, if values of x and y are interchanged then the four values of a and b will also interchange. But we should not consider these values because $gcd(a, b)$ and $gcd(b, a)$ are essentially same thing.

Example 5 : (i) Prove that there are no pair of integers x, y satisfying $x + y = 100$ and $(x, y) = 7$ simultaneously.

(ii) Prove that there are infinitely many pairs of integers x, y satisfying $x + y = 100$ and $(x, y) = 5$ simultaneously.

Solution : (i) Let, if possible, there exist integers x, y satisfying

$x + y = 100$

and $(x, y) = 7$ simultaneously.

Then, $7/x$ and $7/y$

$\Rightarrow \quad 7/x + y \quad \Rightarrow \quad 7/100$, which is a contradiction.

Our supposition is wrong and therefore there are no pair of integers x, y satisfying the equations simultaneously.

(ii) The two equations are

$x + y = 100$ .....(1)

$(x, y) = 5$ .....(2)

Let m and n such that

$$mx + ny = 5$$

Putting $y = 100 - x$ from (1) in (3), we get

$$mx + n(100 - x) = 5 \quad \Rightarrow \quad mx - nx + 100n = 5$$

$$\Rightarrow \quad (m - n)x = 5 - 100n \quad \Rightarrow \quad x = \frac{5 - 100n}{m - n}$$

Since x is an integer, so we have to choose m and n in such a way so that x may be an integer. Clearly there are infinitely many such choices of m and n e.g. $m = 2, n = 1$; $m = 3, n = 2$ etc.

Thus there are infinitely many x and hence infinitely many pairs of integers x, y satisfying (1) and (2) simultaneously.

Example 6 : Prove that every two consecutive integers are co-prime.

Solution : Let n and $n + 1$ be two consecutive integers.

Let $(n, n + 1) = d \quad \Rightarrow \quad d/n$ and $d/n + 1$

We know that if a number divides two numbers then it also divides their difference, so we get

$$d/n + 1 - n \quad \Rightarrow \quad d / 1$$

$$\Rightarrow \quad d = 1 \quad \Rightarrow \quad (n, n + 1) = 1$$

i.e. n and $n + 1$ are co-prime

Example 7 : If a, m, n are non-zero integers, then $(a , mn) = 1$ iff $(a , m) = 1$ and $(a , n) = 1$. **[M.D.U. 2010 (2nd Sem.), 1997 ; K.U. 1998]**

Solution : First Part . Let $(a, m) = 1$ and $(a, n) = 1$

As $(a, m) = 1$ so there exist integers x and y s.t. $ax + my = 1$ .....(1)

and $(a, n) = 1$ so there exist integers x' and y' s.t. $ax' + ny' = 1$

Now consider $a x' + n y' . 1 = 1$

$$\Rightarrow \quad a x' + n y'(a x + m y) = 1 \qquad \text{[By (1)]}$$

$$\Rightarrow \quad ax' + a x n y' + mn y y' = 1$$

$$\Rightarrow \quad a(x' + x n y') + mn(y y') = 1$$

$$\Rightarrow \quad (a, mn) = 1$$

Converse Part. Let $(a, mn) = 1$ then there exist integers h and k s.t.

$$ah + mnk = 1$$

$$\Rightarrow \quad a(h) + m(nk) = 1 \quad \Rightarrow \quad (a, m) = 1$$

Similarly, we can show that $(a,n) = 1$

Example 8 : If a/b , c/d and $(b , d) = 1$, then prove that $(a , c) = 1$

Solution : Given that a/b , so there exists an integer m s.t. $b = am$ .....(1)

Again, given that c/d , so there exists integer n s.t. $d = cn$ .....(2)

Also, $(b, d) = 1$ so there exist integers x and y s.t. $bx + dy = 1$

From (1) and (2), putting $b = am, d = cn$ in this equation, we get

$$amx + cny = 1$$

$$\Rightarrow \quad a(mx) + c(ny) = 1$$

$$\Rightarrow \quad (a, c) = 1$$

$$p_1 p_2 p_3 \ldots\ldots p_r = q_1 q_2 q_3 \ldots\ldots q_s \quad \ldots\ldots(4)$$

Clearly, $p_1 / p_1 . p_2 p_3 \ldots . p_r$

$\Rightarrow$ $p_1 / q_1 q_2 \ldots\ldots q_s$ [By (4)]

$\Rightarrow$ p_1 must divide one prime out of $q_1, q_2, \ldots\ldots, q_s$ say q_1 i.e. p_1 / q_1

But q_1 is prime, so either $p_1 = 1$ or $p_1 = q_1$

But $p_1 \neq 1$ because p_1 is a prime so we must have $p_1 = q_1$

Putting this value in(4), and cancelling p_1(or q_1), we get

$$p_2 p_3 \ldots\ldots p_r = q_2 q_3 \ldots\ldots q_s \quad \ldots\ldots(5)$$

Again, applying the above process on (5), we obtain that p_2 must be equal to one of the primes $q_2, q_3, \ldots\ldots, q_s$.

Without loss of generality, we take $p_2 = q_2$. Then (5) becomes,

$$p_3 p_4 \ldots\ldots p_r = q_3 q_4 \ldots\ldots q_s$$

Proceeding in the same manner, we can obtain

$$p_3 = q_3, p_4 = q_4 \ldots\ldots \text{so on.}$$

Finally we prove that $r = s$. Let, if possible, $r > s$, then equation (4) can be written as

$$p_1 p_2 \ldots\ldots p_s p_{s+1} \ldots\ldots p_r = q_1 q_2 \ldots\ldots q_s$$

Putting $q_1 = p_1, q_2 = p_2, \ldots\ldots q_s = p_s$, we get

$$p_1 p_2 \ldots\ldots p_s p_{s+1} \ldots\ldots p_r = p_1 p_2 \ldots\ldots p_s$$

Cancelling $p_1 p_2 \ldots\ldots p_s$ from both sides by, we get

$$p_{s+1} \ldots\ldots \therefore p_r = 1$$, which is a contradiction because each of the prime on L.H.S. is > 1 so their product can not be equal to 1. Hence our supposition $r > s$ is wrong.

Similarly, we can prove that $s > r$ is wrong. Therefore $r = s$.

Hence the two decompositions of n namely $p_1 p_2 \ldots\ldots p_r$ and $q_1 q_2 \ldots\ldots q_s$ are identical.

Def. Standard Form (Canonical form) :

A number $n > 1$ is said to be expressed in the **Standard form or Canonical form** if $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_k^{\alpha_k}$ where $p_1, p_2, \ldots\ldots p_k$ are **distinct** prime factors of n and $\alpha_i \geq 1$ for $i = 1, 2, \ldots\ldots, k$.

Example 1 : Express 9000 in its canonical form.

Solution :

2	9000
2	4500
2	2250
3	1125
3	375
5	125
5	25
5	5
	1

$$9000 = 2 \times 2 \times 2 \times 3 \times 3 \times 5 \times 5 \times 5 = 2^3 . 3^2 . 5^3$$

Example 2 : If $(a, b) = 1$; prove that $(a^2, b^2) = 1$.

Solution : Let $(a^2, b^2) = d$. Then d/a^2 and d/b^2

Let, if possible, $d > 1$. We know that every natural number greater than 1 has at least one prime factor so d must have a prime factor, say p.

Now p/d and $d/a^2 \Rightarrow p/a^2$ or $p/a.a$

$\Rightarrow p/a$ ($\because p$ is prime)

Similarly, we can prove that p/b.

Thus p is a common divisor of a and b. But 1 is greatest common divisor of a and b, so we arrive at a contradiction as p, being a prime number, is ≥ 2.

Hence our supposition is wrong and so $d = 1$ i.e., $(a^2, b^2) = 1$

Theorem 4.3 Euclid's theorem : Prove that the number of primes is infinite.

Proof : Let , if possible, the number of primes is finite and let q be the largest prime. Then these primes can be listed as 2, 3, 5, 7, 11, ..., q.

Let b denote the product of all these primes i.e. $b = 2.3.5.....q$ .....(1)

Let $a = b + 1$ .....(2)

Clearly $a > 1$ and we know that every natural number greater than 1 has at least one prime factor and so a must have a prime factor say p i.e. p/a

But according to our assumption 2, 3, 5,....q are the only primes, so p must be one out of 2, 3, 5, ..., q.

As $b = 2.3.5.....q$, so p/b

Now p/a and $p/b \Rightarrow p/a - b$

$\Rightarrow p/1$ [By (2) , $a - b = 1$]

which is a contradiction as p, being a prime number, is ≥ 2. Hence our supposition is wrong. Therefore, the number of primes is infinite.

Note : Recall that we have proved earlier that product of the primes of the form $4k + 1$ is again of the form $4k + 1$.

Example 3 : Show that every odd prime can be put either in the form $4k + 1$ or $4k + 3$ (i.e. $4k - 1$), where k is a positive integer.

Solution : Let p be any odd prime. If we divide p by 4, then by division algorithm , we get

$p = 4k + r$ where $0 \leq r < 4$ i.e. $r = 0, 1, 2, 3$

Using these values of r , we see that p can be of following four different forms :

$p = 4k$, $p = 4k + 1$

$p = 4k + 2$, $p = 4k + 3$

We see that $4k$ is not a odd prime as it is divisible by 4 and $4k + 2 = 2(2k + 1)$ is also not a odd prime as it is divisible by 2.

But we are given that p is a odd prime so $p \neq 4k$ and $p \neq 4k + 2$.

Hence, we remain with two possibilities, namely , $p = 4k + 1$ and $p = 4k + 3$. Thus an odd prime p is either of the form $4k + 1$ or $4k + 3$.

Also a $4k + 3$ number is of the form $4k-1$, therefore we have that an odd prime p is either of the form

$4k+1$ or $4k+3$ $(\text{i.e. } 4k-1)$

Chapter 2

Congruences and Diophantine Equations

1. Congruences

Def. Congruence : If a and b are two integers and m is a positive integer, then a is said to be congruent to b modulo m if $m/a - b$ i.e. $a - b$ is a multiple of m.

Symbolically, we express it by writing

$a \equiv b \pmod{m}$ or $a - b \equiv 0 \pmod{m}$

For example, $18 \equiv 2 \pmod 4$ since $4/(18 - 2)$ i.e. $4/16$

$17 \equiv -3 \pmod 5$ since $5/(17-(-3))$ i.e. $5/20$

If m does not divide $a - b$ i.e. $m \nmid a - b$ then we say that a is incongruent or not congruent to b and we express it by writing $a \not\equiv b \pmod m$

e.g. $18 \not\equiv 3 \pmod 4$ since $4 \nmid (18 - 3)$ i.e. $4 \nmid 15$

Example 1 : Find the least positive integer (mod 11) to which 285 is congruent.

Solution : Dividing 285 by 11, we have $285 = 11.25 + 10$

$\Rightarrow \quad 285 - 10 = 11.25$

$\Rightarrow \quad 11 / 285 - 10$

$\Rightarrow \quad 285 \equiv 10 \pmod{11}$

Hence 10 is the least positive integer to which 285 is congruent.

Example 2 : Find a such that $a \equiv 7 \pmod 5$.

Solution : As $a \equiv 7 \pmod 5$, so by definition of congruence, we have $5/a - 7$

$\Rightarrow \quad a - 7 = 5k$ where k is any integer.

$\Rightarrow \quad a = 7 + 5k$ where k is any integer

Putting $k = 0, 1, 2, 3, \ldots, -1, -2, -3, \ldots$, we get

$a = 7, 12, 17, 22, \ldots, 2, -3, -8, \ldots$ .....(1)

Hence all integers given by (1) are congruent to 7 (mod 5).

Example 3 : If x is odd, show that $x^2 \equiv 1 \pmod 8$.

Solution : Given that x is odd so it must be of the form $x = 2n + 1$ for some non-negative integer n.

Then, $x^2 - 1 = (2n + 1)^2 - 1$

$= 4n^2 + 1 + 4n - 1$

$= 4n^2 + 4n = 4n(n + 1)$ .....(1)

But $n(n + 1)$ is the product of two consecutive integers, hence it is divisible by 2.
So let $n(n + 1) = 2k$ for some integer k.
Putting this value in (1), we obtain $(x^2 - 1) = 8k$ which is divisible by 8.

i.e. $8/x^2 - 1 \Rightarrow x^2 \equiv 1 \pmod 8$

Example 4 : Prove that $3^{4n+2} + 5^{2n+1} \equiv 0 \pmod{14}$

Solution : Let $f(n) = 3^{4n+2} + 5^{2n+1}$. We shall prove result by applying mathematical induction on n.

Step I. For $n = 1$, $f(1) = 3^6 + 5^3 = 729 + 125$

$= 854$ which is divisible by 14.

$\therefore$ $f(n)$ is divisible by 14 for $n = 1$. So result is true for $n = 1$

Step II. As our induction hypothesis, we assume that result is true for n i. e. $f(n)$ be divisible by 14 .

$\therefore$ $f(n) = 14k$

$\Rightarrow$ $3^{4n+2} + 5^{2n+1} = 14k$

$\Rightarrow$ $3^{4n+2} = 14k - 5^{2n+1}$ .....(1)

Step III. Changing n to $n + 1$ in $f(n)$.

$f(n + 1) = 3^{4(n+1)+2} + 5^{2(n+1)+1}$

$= 3^{4n+6} + 5^{2n+3}$

$= 3^{4n+2}.3^4 + 5^{2n+1}.5^2$

$= 3^{4n+2} . 81 + 5^{2n+1} . 25$

Putting the value of 3^{4n+2} from (1),

$f(n + 1) = \left[14k - 5^{2n+1}\right]81 + 5^{2n+1}.25$

$= 14k(81) - 81.5^{2n+1} + 25.5^{2n+1}$

$= 14k(81) - 56.5^{2n+1}$

$= 14[81k - 4.5^{2n+1}]$, which is divisible by 14.

So by Principle of Mathematical Induction , $f(n)$ is divisible by 14 for all n

i.e. $3^{4n+2} + 5^{2n+1} \equiv 0 \pmod{14}$

Theorem 1.1: Prove that two integers are congruent modulo m if and only if they leave the same remainder when divided by m. **[M.D.U. 2011]**

Proof : Let the two integers be a and b and let r_1, r_2 be the remainders when a and b are divided by m respectively.

i.e. $a = q_1 m + r_1$ $\quad 0 \le r_1 < m$ .....(1)

$b = q_2 m + r_2$ $\quad 0 \le r_2 < m$ .....(2)

First we suppose that $a \equiv b \pmod m$ and we shall prove that $r_1 = r_2$.

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

$\Rightarrow$ $m/a-b$

$\Rightarrow$ $m/[(q_1m+r_1)-(q_2m+r_2)]$ [By (1) and (2)]

$\Rightarrow$ $m/[m(q_1-q_2)+(r_1-r_2)]$

Clearly m/m and so $m/m(q_1-q_2)$

Now if an integer divides two integers then it also divides their difference and so

$m/[m(q_1-q_2)+(r_1-r_2)-m(q_1-q_2)]$

$\Rightarrow$ m/r_1-r_2

$\Rightarrow$ $r_1-r_2=0$ because $|r_1-r_2|<m$

$\Rightarrow$ $r_1 = r_2$

Hence a and b leave the same remainder when divided by m.

Conversely, Let a and b leave the same remainder when divided by m.

i.e. $r_1 = r_2 = r$ (say)

Let $a = mq_1 + r$

and $b = mq_2 + r$

Subtracting $a - b = m(q_1 - q_2)$

$\Rightarrow$ $m/a - b$

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

Theorem 1.2 : If r is the remainder on dividing a by m, prove that $a \equiv r \pmod{m}$ i.e. an integer is congruent to its remainder.

Proof : As r is the remainder obtained on dividing a by m, so

$a = mq + r$

i.e. $a - r = mq$

$\Rightarrow$ $m/(a-r)$

$\Rightarrow$ $a \equiv r \pmod{m}$

Theorem 1.3 (i) $a \equiv a \pmod{m}$ for every integer a.

(ii) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$

(iii) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

OR

The relation of congruence is an equivalence relation i.e. it is reflexive , symmetric and transitive.

Proof : (i) We know that $m/0$ where $m \neq 0$

$\Rightarrow$ $m/a - a$

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

(ii) Let $a \equiv b \pmod{m}$ $\Rightarrow$ $m/a - b$

$\Rightarrow$ $m/b - a$

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

(iii) Let $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$

$\Rightarrow \quad m/a-b$ and $m/b-c$

$\Rightarrow \quad m/(a-b)+(b-c)$

$\Rightarrow \quad m/a-c$

$\Rightarrow \quad a \equiv c \pmod{m}$

Remark : In the congruence $a \equiv b \pmod{m}$, a is called L.H.S., b is called R.H.S. and m is called modulus of congruence

Theorem 1.4 : (Addition and Multiplication by a constant) : If $a \equiv b \pmod{m}$ and c is an integer then

(i) $a + c \equiv b + c \pmod{m}$ i.e. a constant can be added on both sides of a congruence

(ii) $ac \equiv bc \pmod{m}$ i.e. a constant can be multiplied on both sides of a congruence

(iii) $ac \equiv bc \pmod{cm}$ i.e. a constant can be multiplied on both sides and the modulus of a congruence .

Proof : (i) Given that $a \equiv b \pmod{m}$

$\Rightarrow \quad m/a-b$

$\Rightarrow \quad m/(a+c)-(b+c)$

$\Rightarrow \quad (a+c) \equiv (b+c) \pmod{m}$

(ii) Given that $a \equiv b \pmod{m}$

$\Rightarrow \quad m/a-b$

$\Rightarrow \quad m/c(a-b)$

$\Rightarrow \quad m/ac-bc$

$\Rightarrow \quad ac \equiv bc \pmod{m}$

(iii) Given that $a \equiv b \pmod{m}$

$\Rightarrow \quad m/a-b$

$\Rightarrow \quad mc/(a-b)c$

$\Rightarrow \quad mc/ac-bc$

$\Rightarrow \quad ac \equiv bc \pmod{mc}$

Remark 1: The converse of part (ii) of above theorem is not true.

i. e. it is not always possible to cancel a common factor from a congruence. For example,

$16 \equiv 8 \pmod{4}$ $\quad [\because 4/16-8]$

If we cancel the common factor 8 from number 16 and 8, we get $2 \equiv 1 \pmod{4}$ which is a false result because $4 \nmid (2-1)$.

Remark 2 : The converse of part (ii) of above theorem is not true but it will be true under some conditions as given in the next theorem.

Theorem 1.5 : CANCELLATION Theorem

(i) If $ac \equiv bc \pmod m$ and $(c, m) = d$, then $a \equiv b \left(\mod \frac{m}{d}\right)$

(ii) If $ac \equiv bc \pmod m$ and $(c, m) = 1$, then $a \equiv b \pmod m$ **[K.U. 2000, 1998]**

(iii) If $ac \equiv bc \pmod{mc}$ then $a \equiv b \pmod m$

Proof : **(i)** Given that d is the greatest common divisor of c and m so there exist integers c_1 and m_1 such that $c = dc_1$, $m = dm_1$ and $(c_1, m_1) = 1$

Now $ac \equiv bc \pmod m$ is given

$\Rightarrow$ $m / ac - bc$

$\Rightarrow$ $m / (a - b)c$

Putting the values of m and c, we get $dm_1 / dc_1 (a - b)$

$\Rightarrow$ $m_1 / c_1 (a - b)$

$\Rightarrow$ $m_1 / (a - b)$ $[\because (m_1, c_1) = 1]$

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

$\Rightarrow$ $a \equiv b \left(\mod \frac{m}{d}\right)$ $\left[\because m_1 = \frac{m}{d}\right]$.

(ii) Given $ac \equiv bc \pmod m$ and $(c, m) = 1$ so by putting $d = 1$ in the above part, we have

$$a \equiv b \left(\mod \frac{m}{1}\right)$$

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

(iii) Given that $ac \equiv bc \pmod{mc}$

$\Rightarrow$ $mc / ac - bc$

$\Rightarrow$ $mc / (a - b)c$

$\Rightarrow$ $m / (a - b)$

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

Theorem 1.6 : (Addition , subtraction and multiplication of congruences) :
If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

(i) $a + c \equiv b + d \pmod m$ (i.e. two congruences of same modulo can be added)

(ii) $a - c \equiv b - d \pmod m$ (i.e. two congruences of same modulo can be subtracted)

(iii) $ac \equiv bd \pmod m$ (i.e. two congruences of same modulo can be multiplied)

Proof : **(i)** Given that $a \equiv b \pmod m$ and $c \equiv d \pmod m$

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

$\Rightarrow$ $m / [(a - b) + (c - d)]$

$\Rightarrow$ $m / ((a + c) - (b + d))$

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

(ii) Given that $a \equiv b \pmod m$ and $c \equiv d \pmod m$

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

$\Rightarrow$ $m/(a-b)-(c-d)$

$\Rightarrow$ $m/(a-c)-(b-d)$

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

(iii) Given that $a \equiv b \pmod m$ and $c \equiv d \pmod m$

$\Rightarrow$ $m/(a-b)$ and $m/(c-d)$

Then there exist integers h and k s.t.

$a-b=mh$ and $c-d=mk$

$\Rightarrow$ $a=b+mh$ and $c=d+mk$

Multiplying these two equations , we get

$$ac = (b+mh)(d+mk)$$
$$= bd+bmk+mhd+m^2hk$$
$$\Rightarrow \quad ac-bd = m(bk+hd+mkh)$$
$$\Rightarrow \quad m/(ac-bd)$$
$$\Rightarrow \quad ac \equiv bd \pmod m$$

Cor : If $a \equiv b \pmod m$, then $a^2 \equiv b^2 \pmod m$

Proof : As $a \equiv b \pmod m$

and again $a \equiv b \pmod m$

Multiplying the two congruences, we get $a^2 \equiv b^2 \pmod m$.

Theorem 1.7 (Generalization of Theorem 1.6 (iii)): If $a_1, a_2, \ldots\ldots, a_n$ are respectively congruent to $b_1, b_2, \ldots\ldots, b_n \pmod m$, then prove that

$$a_1 a_2 \ldots\ldots a_n \equiv b_1 b_2 \ldots\ldots b_n \pmod m.$$

(i.e. any finite number of congurences with same modulo can be multiplied).

Proof : As $a_1 \equiv b_1 \pmod m$

$\Rightarrow$ m/a_1-b_1

$\Rightarrow$ there exist an integer k_1 s.t. $a_1-b_1=mk_1$

$\Rightarrow$ $a_1=b_1+mk_1$

Similarly, we can obtain

$a_2=b_2+mk_2$

$\ldots\ldots\ldots\ldots\ldots$

and $a_n=b_n+mk_n$

Multiplying all these equations

$$a_1a_2\ldots\ldots a_n = (b_1+mk_1)(b_2+mk_2)\ldots\ldots(b_n+mk_n)$$
$$= b_1b_2\ldots\ldots b_n + \text{a multiple of } m$$
$$\Rightarrow \quad a_1a_2\ldots\ldots a_n - b_1b_2\ldots\ldots b_n = \text{a multiple of } m.$$
$$\Rightarrow \quad m/(a_1a_2\ldots\ldots a_n)-(b_1b_2\ldots\ldots b_n)$$
$$\Rightarrow \quad a_1a_2\ldots\ldots a_n \equiv b_1b_2\ldots\ldots b_n \pmod m.$$

COR : If $a \equiv b \pmod m$, then $a^k \equiv b^k \pmod m$ for every positive integer k.

Proof : As $a \equiv b \pmod m$ (Given). We write the given congruence k times i. e.

$a \equiv b \pmod m$, $a \equiv b \pmod m$, ... , $a \equiv b \pmod m$

Multiplying these k congruences , we get $a^k \equiv b^k \pmod m$.

Theorem 1.8 : (i) If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$ and $[m_1 , m_2] = m$, i.e. m is the l.c.m. of m_1 and m_2 then $a \equiv b \pmod m$.

(ii) If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$ and $(m_1 , m_2) = 1$ then $a \equiv b \pmod{m_1 m_2}$

(iii) If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$ and $(m_1 , m_2) = d$, then $a \equiv b \pmod d$.

Proof : (i) Given that $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$ so $m_1 / a - b$ and $m_2 / a - b$

i.e. $a - b$ is a common multiple of m_1 and m_2.

But m is given to be the least common multiple of m_1 and m_2 , so by definition of least common multiple, we must have

$$m / a - b \quad \Rightarrow \quad a \equiv b \pmod m$$

(ii) Given that $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$ so $m_1 / a - b$ and $m_2 / a - b$

But $(m_1 , m_2) = 1$ so $m_1 m_2 / a - b \quad \Rightarrow \quad a \equiv b \pmod{m_1 m_2}$

(iii) Given that $a \equiv b \pmod{m_1}$ so $m_1 / a - b$

Also $(m_1 , m_2) = d$ so d / m_1

Now d / m_1 and $m_1 / a - b \quad \Rightarrow \quad d / a - b$

$\Rightarrow \quad a \equiv b \pmod d$.

Remark : The converse of the part (i) is true but part (iii) is not true.

Proof : Converse of (i) : Let $a \equiv b \pmod m$ where m is the l.c.m. of m_1 and m_2 .

$\Rightarrow \quad m / a - b$

But m_1 / m and m_2 / m $\quad [\because [m_1 , m_2] = m]$

so, we have $m_1 / a - b$ and $m_2 / a - b$

i.e. $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$

Converse of (iii) Here we give an example to show that the converse of part (iii) is not true.

Let $m_1 = 4$ and $m_2 = 6$

$\therefore \quad d = (m_1 , m_2) = (4, 6) = 2$

Let $a = 10$ and $b = 8$

Thus, we have $10 \equiv 8 \pmod 2$ i.e. $a \equiv b \pmod d$

but $10 \not\equiv 8 \pmod 4$ i.e. $a \not\equiv b \pmod{m_1}$

and $10 \not\equiv 8 \pmod 6$ i.e. $a \not\equiv b \pmod{m_2}$

Theorem 1.9 (i) : If $a + b \equiv c \pmod m$ and $b \equiv d \pmod m$, show that $a + d \equiv c \pmod m$

(ii) If $ab \equiv c \pmod m$ and $b \equiv d \pmod m$, show that $ad \equiv c \pmod m$.

Proof : (i) Given that $a + b \equiv c \pmod m$ ..... (1)

12. (i) 4 (ii) 1 (iii) 4 (iv) 5 (v) 11
(vi) 4 (vii) 6 (viii) 12

13. (i) 9 (ii) 1

---

2. LINEAR CONGRUENCES

Def. Linear congruence : A congruence of the form

$$ax \equiv b(\text{mod } m) \quad \text{or} \quad ax + b \equiv 0(\text{mod } m)$$

where a, b, m are integers is called a linear congruence.

Def. Solution of linear congruence : An integer x_0 is called a solution of a linear congruence $ax \equiv b \pmod m$ if it satisfies this congruence i.e. $ax_0 \equiv b(\text{mod } m)$.

e.g. $x = 3$ is a solution of the linear congruence $3x \equiv 4(\text{mod } 5)$ as $3.3 \equiv 4 \pmod 5$. But $x = 4$ is not a solution of $3x \equiv 4(\text{mod } 5)$ because $3.4 \not\equiv 4(\text{mod } 5)$

Theorem 2.1 : If x_0 is a solution of $ax \equiv b(\text{mod } m)$ and x_1 is an integer such that $x_1 \equiv x_0 \pmod m$, then x_1 is a solution of $ax \equiv b(\text{mod } m)$.

Solution : As x_0 is a solution of $ax \equiv b(\text{mod } m)$, so by definition,

$$ax_0 \equiv b(\text{mod } m) \qquad \text{.....(1)}$$

Also given that $x_1 \equiv x_0 \pmod m$

Multiplying both sides by a

$$ax_1 \equiv ax_0(\text{mod } m) \qquad \text{.....(2)}$$

By (1) and(2), we get

$$ax_1 \equiv b(\text{mod } m).$$

Thus x_1 is also a solution of $ax \equiv b(\text{mod } m)$.

Remark : Another way to represent the above theorem is as follows :
"If x_0 is a solution of $ax \equiv b(\text{mod } m)$, then every integer of the form $x_0 + km$ is also a solution of $ax \equiv b(\text{mod } m)$.".

Proof : Clearly if $x_1 \equiv x_0 \pmod m$ then $m/x_1 - x_0$.

$$\Rightarrow \quad x_1 - x_0 = km \quad \text{for some integer } k$$

$$\Rightarrow \quad x_1 = x_0 + km \quad \text{for some integer } k$$

IMPORTANT NOTE : By above theorem it is clear that if a linear congruence $ax \equiv b(\text{mod } m)$ has one solution then it has infinitely many solutions. For example, we consider the linear congruence

$$3x \equiv 4(\text{mod } 5) \qquad \text{.....(1)}$$

We see that $x = 3$ is a solution of this congruence and so every integer of the form $3 + 5k$ is also a solution of (1).

Putting $k = 1, -1, 2, -2, \ldots\ldots$ in $3 + 5k$, we get that $8, -2, 13, -7, \ldots\ldots$ all are also solutions of (1). Another way to express this fact is that every integer x satisfying $x \equiv 3 \pmod 5$ is a solution of (1).

Here we also could have said that $x \equiv 8 \pmod 5$ is a solution of (1), but it is more convenient to use least positive integer modulo 5 for solution. By this discussion we once again define the solution of a linear congruence in the form of a congruence.

Def. Solution of a linear congruence : The solution of a linear congruence $ax \equiv b \pmod m$, if it exists, will be of the form

$$x \equiv x_0 \pmod m \quad \text{where} \quad 0 \le x_0 \le m-1$$

or $$x = x_0 + km \quad \text{where} \quad 0 \le x_0 \le m-1 \quad \text{and } k \text{ is any integer.}$$

Proof : Whenever it is required to find a solution of a linear congruence $ax \equiv b \pmod m$, we first search out an integer x_0 in the set $\{0, 1, 2, \ldots\ldots, m-1\}$ which satisfies the given congruence i.e., $ax_0 \equiv b \pmod m$. If such a x_0 is found then we say that $x \equiv x_0 \pmod m$ is a solution of $ax \equiv b \pmod m$ If no such integer x_0 is found in the set $\{0, 1, 2, \ldots\ldots, m-1\}$ then $ax \equiv b \pmod m$ has no solution.

Example 1 : Find the solution of the following linear congruences by inspection.

(i) $3x \equiv 5 \pmod 7$ (ii) $2x \equiv 1 \pmod 4$ (iii) $2x \equiv 6 \pmod 4$

Solution : (i) Here $m = 7$ so we have to search out a solution in the set $\{0, 1, 2, 3, 4, 5, 6\}$.

Putting	$x = 0$,	$3.0 \equiv 5 \pmod 7$	which is false
Putting	$x = 1$,	$3.1 \equiv 5 \pmod 7$	which is false
Putting	$x = 2$,	$3.2 \equiv 5 \pmod 7$	which is false
Putting	$x = 3$,	$3.3 \equiv 5 \pmod 7$	which is false
Putting	$x = 4$,	$3.4 \equiv 5 \pmod 7$	which is **true**
Putting	$x = 5$,	$3.5 \equiv 5 \pmod 7$	which is false
Putting	$x = 6$,	$3.6 \equiv 5 \pmod 7$	which is false

$\therefore$ The congruence $3x \equiv 5 \pmod 7$ has only one solution given by $x \equiv 4 \pmod 7$.

(ii) Here $m = 4$ so we have to search out a solution in the set $\{0, 1, 2, 3\}$.

Putting	$x = 0$,	$2.0 \equiv 1 \pmod 4$	which is false
Putting	$x = 1$,	$2.1 \equiv 1 \pmod 4$	which is false
Putting	$x = 2$,	$2.2 \equiv 1 \pmod 4$	which is false
Putting	$x = 3$,	$2.3 \equiv 1 \pmod 4$	which is false

$\therefore$ The congruence $2x \equiv 1 \pmod 4$ has no solution.

(iii) Here $m = 4$ so we have to search out a solution in the set $\{0, 1, 2, 3\}$.

Putting	$x = 0$,	$2.0 \equiv 6 \pmod 4$	which is false.
Putting	$x = 1$,	$2.1 \equiv 6 \pmod 4$	which is **true.**
Putting	$x = 2$,	$2.2 \equiv 6 \pmod 4$	which is false

Putting $x = 3$, $2.3 \equiv 6 \pmod 4$ which is true

$\therefore$ The congruence $2x \equiv 6 \pmod 4$ has two solutions given by

$x \equiv 1 \pmod 6$ and $x \equiv 3 \pmod 6$.

Note : By above example it is clear that a linear congruence may have no solution, unique solution or more than one solution in the set $\{0, 1, 2, \ldots\ldots, m-1\}$. Now we shall study some theorems which tell us when a linear congruence is solvable and if it solvable then how many solutions it has.

Theorem 2.2 : The linear congruence $ax \equiv b \pmod m$ has a solution if and only if (a, m) divides b. **[K.U. 1994, 95]**

Proof : Let $(a, m) = d$ and first we suppose that d/b. We shall prove that $ax \equiv b \pmod m$ has a solution.

As d/b so there exists an integer c such that $b = dc$ .....(1)

Now $(a, m) = d$ so there exist integers h and k such that $ah + mk = d$ .....(2)

Multiplying (2) by c on both sides

$$ahc + mkc = dc$$

$$\Rightarrow \quad ahc + mkc = b \qquad \text{[By (1)]}$$

$$\Rightarrow \quad ahc - b = m(-kc)$$

$$\Rightarrow \quad m / ahc - b$$

$$\Rightarrow \quad a(hc) \equiv b \pmod m$$

$$\Rightarrow \quad x = hc \text{ is a solution of } ax \equiv b \pmod m$$

Conversely, we suppose that $ax \equiv b \pmod m$ has a solution , say x_0, therefore

$$ax_0 \equiv b \pmod m$$

$$\Rightarrow \quad m / ax_0 - b$$

$$\Rightarrow \quad ax_0 - b = mt \text{ for some integer } t.$$

$$\Rightarrow \quad ax_0 - mt = b$$

Now as $(a, m) = d$ so d/a and d/m .....(3)

$$\Rightarrow \quad a = da_1 \quad \text{and} \quad m = dm_1 \text{ for some integers } a_1 \text{ and } m_1.$$

Putting these values of a and m in (3),we get

$$da_1x_0 - dm_1t = b$$

$$\Rightarrow \quad d(a_1x_0 - m_1t) = b \quad \Rightarrow \quad d/b .$$

Example 2 : Do the following congruences possess a solution.

(i) $135x \equiv 6 \pmod{10}$ **(ii) $51x \equiv 32 \pmod 7$**

(iii) $51x \equiv 6 \pmod{21}$ **(iv) $66x \equiv 8 \pmod{78}$**

Solution : (i) Given congruence is $135x \equiv 6 \pmod{10}$.

Comparing it with $ax \equiv b \pmod m$, we have $a = 125$, $b = 6$, $m = 10$.

We know that the linear congruence $ax \equiv b \pmod m$ has a solution if and only if $(a, m) = d$ divides b.

Here $(a, m) = (135, 10) = 5$ and 5 does not divide $b = 6$.

So the congruence $135x = 6 \pmod{10}$ has no solution.

(ii) Given congruence is $51x \equiv 32 \pmod{7}$
Comparing it with $ax \equiv b \pmod{m}$, we have $a = 51,\ b = 32,\ m = 7$
We know that the linear congruence $ax \equiv b \pmod{m}$ has a solution if and only if $(a, m) = d$ divides b.
Here $(a, m) = (51, 7) = 1$ and 1 divides $b = 32$.
So the congruence $51x \equiv 32 \pmod{7}$ has a solution.

(iii) Given congruence is $51x \equiv 6 \pmod{21}$
Comparing it with $ax \equiv b \pmod{m}$, we have $a = 51,\ b = 6,\ m = 21$
We know that the linear congruence $ax \equiv b \pmod{m}$ has a solution if and only if $(a, m) = d$ divides b.
Here $(a, m) = (51, 21) = 1$ and 1 divides $b = 6$.
So the congruence $51x \equiv 6 \pmod{21}$ has a solution.

(iv) Given congruence is $66x \equiv 8 \pmod{78}$
Comparing it with $ax \equiv b \pmod{m}$, we have $a = 66,\ b = 8,\ m = 78$
We know that the linear congruence $ax \equiv b \pmod{m}$ has a solution if and only if $(a, m) = d$ divides b.
Here $(a, m) = (66, 78) = 2$ and 2 divides $b = 8$.
So the congruence $66x \equiv 8 \pmod{78}$ has a solution.

Theorem 2.3 : In the linear congruence $ax \equiv b \pmod{m}$ if $(a, m) = 1$ then it has a unique incongruent solution modulo m. **[M.D.U. 1995 ; K.U. 1996]**

Proof : We know that $ax \equiv b \pmod{m}$ has a solution if and only if (a, m) divides b. Here $(a, m) = 1$ and 1 divides b so $ax \equiv b \pmod{m}$ has a solution.

Uniqueness : Let x_1 and x_2 be any two solutions of $ax \equiv b \pmod{m}$.

Then $ax_1 \equiv b \pmod{m}$ .....(1)

and $ax_2 \equiv b \pmod{m}$ .....(2)

Subtracting (2) from (1), we get

$$a(x_1 - x_2) \equiv 0 \pmod{m}$$

$$\Rightarrow \quad m / a(x_1 - x_2)$$

$$\Rightarrow \quad m / x_1 - x_2 \qquad [\because (a, m) = 1]$$

$$\Rightarrow \quad x_1 \equiv x_2 \pmod{m}$$ i.e. x_1 and x_2 are congruent modulo m. Thus $ax \equiv b \pmod{m}$ has a unique incongruent solution modulo m.

Theorem 2.4: In the linear congruence $ax \equiv b \pmod{m}$ if $(a, m) = d$ and d/b then it has exactly d incongruent solutions modulo m. **[M.D.U. 1996 ; K.U. 1994]**

Proof : Step (i) The given congruence is

$$ax \equiv b(\text{mod } m) \quad \text{.....(1)}$$

Here $(a, m) = d$ and d/b so congruence (1) must have a solution, say x_0, so that

$$ax_0 \equiv b(\text{mod } m) \quad \text{.....(2)}$$

Now $$(a,m) = d \Rightarrow \left(\frac{a}{d}, \frac{m}{d}\right) = 1 \quad \text{.....(3)}$$

Subtracting (2) from (1), we get

$$a(x - x_0) \equiv 0(\text{mod } m)$$

$$\Rightarrow \quad m / a(x - x_0)$$

$$\Rightarrow \quad \frac{m}{d} \Big/ \frac{a}{d}(x - x_0)$$

$$\Rightarrow \quad \frac{m}{d} \Big/ x - x_0 \qquad \left[\text{By (3)}, \left(\frac{m}{d}, \frac{a}{d}\right) = 1\right]$$

$$\Rightarrow \quad x - x_0 = \frac{km}{d} \qquad \text{where } k \text{ is any integer.}$$

$$\Rightarrow \quad x = x_0 + \frac{km}{d} \qquad \text{where } k \text{ is any integer} \quad \text{.....(4)}$$

Putting $k = 0, 1, 2, \ldots\ldots, d - 1$, we get following d solutions of (1)

$$x \equiv x_0, x_0 + \frac{m}{d}, \ldots\ldots\ldots\ldots, x_0 + \frac{(d-1)m}{d} \quad \text{.....(5)}$$

Step (ii) Now we prove that if any $k \geq d$ is used in (4), then we get one of the solutions in(5).

Let $k \geq d$ be any integer then by division algorithm there exist integers q and r such that

$$k = dq + r, \text{ where } 0 \leq r < d$$

Using this value of k in (4), we get

$$x = x_0 + \frac{m}{d}(dq + r)$$

$$\Rightarrow \quad x = x_0 + mq + \frac{rm}{d}$$

$$\Rightarrow \quad x - \left(x_0 + \frac{rm}{d}\right) = mq$$

$$\Rightarrow \quad m \text{ divides } x - \left(x_0 + \frac{rm}{d}\right)$$

$$\Rightarrow \quad x = x_0 + \frac{rm}{d} \text{ where } 0 \leq r \leq d - 1$$

which is one of the solutions in (5).

Step (iii) Finally, we prove that all the solutions in (5) are incongruent modulo m.

Let, if possible, two solutions in(5) are congruent modulo m

i.e., $$x_0 + \frac{k_1 m}{d} \equiv x_0 + \frac{k_2 m}{d} (\text{mod } m) \text{for } k_1 \neq k_2 \text{ and } 0 \leq k_1, k_2 \leq d - 1$$

$$\Rightarrow \quad \frac{k_1 m}{d} \equiv \frac{k_2 m}{d} (\text{mod } m)$$

Dividing by $\frac{m}{d}$ throughout, we get

$$k_1 \equiv k_2 \pmod{d} \qquad \left[\because \text{If } a \equiv b \pmod{m} \text{ then } \frac{a}{d} \equiv \frac{b}{d}\left(\text{mod}\frac{m}{d}\right)\right]$$

$$\Rightarrow \quad d / k_1 - k_2$$

which is a contradiction since k_1 and k_2 both lies between 0 and $d-1$.
Hence all solutions in (5) are incongruent modulo m.

Remark : The equation (5) in above proof will be helpful in solving the numericals. Due to its importance let us conclude it as follows :
The linear congruence $ax \equiv b \pmod{m}$ has a solution if and only if $d = (a, m)$ divides b and has exactly d incongruent solutions given by

$x = x_0 + \frac{km}{d}$ where $k = 0, 1, 2, \ldots, d-1$ and x_0 is one of the solution of $ax \equiv b \pmod{m}$.

Example 3 : Find the number of incongruent solutions of following linear congruences :

(i) $10x \equiv 15 \pmod{25}$ (ii) $3x \equiv 5 \pmod{12}$ (iii) $2x \equiv 5 \pmod{9}$

Solution : **(i)** The given congruence is $10x \equiv 15 \pmod{25}$
Comparing it with
$ax \equiv b \pmod{m}$, we have $a = 10$, $b = 15$, $m = 25$
Here $d = (a, m) = (10, 25) = 5$ and $d = 5$ divides $b = 15$.
Hence the given congruence has $d = 5$ incongruent solution modulo 25.

(ii) The given congruence is $3x \equiv 5 \pmod{12}$
Comparing it with $ax \equiv b \pmod{m}$, we have $a = 3$, $b = 5$, $m = 12$
Here $d = (a, m) = (3, 12) = 3$ and $d = 3$ does not divide $b = 5$.
Hence the given congruence has no solution .

(iii) The given congruence is $2x \equiv 5 \pmod{9}$
Comparing it with $ax \equiv b \pmod{m}$, we have $a = 2$, $b = 5$, $m = 9$
Here $d = (a, m) = (2, 9) = 1$ and $d = 1$ divides $b = 5$.
Hence the given congruence has unique incongruent solution modulo 9.

Note : Now we shall develop some methods to solve linear congruences.

Method I : Method to solve a linear congruence having unique incongruent solution.

(i) Write the given congruence in the form

$$ax \equiv b \pmod{m} \qquad \ldots\ldots(1)$$

(ii) Verify that $(a, m) = 1$ so that the given congruence has one and only one incongruent solution.

(iii) Consider the multiples of m i.e., $m, 2m, 3m$ ..... . Out of these integers select the first integer, say tm, such that $tm + b$ is divisible by a.

(iv) Take the congruence $0 \equiv tm \pmod{m}$ .....(2)

(v) Add the congruences (1) and (2), cancel out 'a' from both sides and the solution is obtained.

Example 4 : Solve the following congruences

(i) $3x + 2 \equiv 0 \pmod{7}$ **(ii) $7x \equiv 4 \pmod{10}$**

Solution : **(i)** The given congruence can be written as

$$3x \equiv -2 \pmod{7} \quad \text{.....(1)}$$

Comparing (1) with $ax \equiv b \pmod{m}$, we have $a = 3$, $b = -2$ and $m = 7$

Here $d = (a, m) = (3, 7) = 1$ which divides $b = -2$ and hence (1) has one and only one incongruent solution. Now, we consider the multiples of $m = 7$

i.e. 7 , 14 , 21 , 28 , 35 .....

and we see that

$-2 + 7 = 5$ is not divisible by $a = 3$.

$-2 + 14 = 12$ is divisible by $a = 3$

So we take the congruence $0 \equiv 14 \pmod{7}$ .....(2)

Adding (1) and (2), we get $3x \equiv 12 \pmod{7}$

Cancelling 3 as $(3, 7) = 1$, we get $x \equiv 4 \pmod{7}$ is the solution of the congruence (1).

(ii) The given congruence is $7x \equiv 4 \pmod{10}$ .....(1)

Comparing (1) with $ax \equiv b \pmod{m}$, we have $a = 7$, $b = 4$ and $m = 10$

Here $d = (a, m) = (7, 10) = 1$ which divides $b = 4$ and hence (1) has one and only one incongruent solution. Now, we consider the multiples of $m = 10$

i.e. 10 , 20 , 30 , ...

and we see that $4 + 10 = 14$ is divisible by $a = 7$.

So we take the congruence $0 \equiv 10 \pmod{10}$ .....(2)

Adding (1) and (2), we get $7x \equiv 14 \pmod{10}$

Cancelling 7 as $(7, 10) = 1$, we get $x \equiv 2 \pmod{10}$ is the solution of the congruence (1).

METHOD II : To solve a linear congruence $ax \equiv b \pmod{m}$ having unique solution where 'a' is large

(i) Write the given congruence in the form $ax \equiv b \pmod{m}$ .....(1)

(ii) Verify that $(a, m) = 1$ so that the given congruence has one and only one incongruent solution.

(iii) Divide a by m and let r be the remainder obtained and then write $a \equiv r \pmod{m}$

(iv) Multiply the above congruence both sides by x to obtain

$$ax \equiv rx \pmod{m} \quad \text{.....(2)}$$

(v) By (1) and(2), we obtain $rx \equiv b \pmod{m}$ .....(3)

(vi) Now solve the congruence (3) by **Method I**.

Alternative Method :

(i) Write the given congruence in the form $ax \equiv b(\text{mod } m)$ .....(1)

(ii) Verify that $(a, m) = 1$ so that the given congruence has one and only one incongruent solution.

(iii) Let c be the largest multiple of m which is less than or equal to a , then we write the congruence

$$cx \equiv 0(\text{mod } m)$$

(iv) Subtracting (2) from (1) we get $(a - c)x \equiv b(\text{mod } m)$ .....(2)

(v) Now the solve the congruence (3) by **Method I**. .....(3)

Example 5 : Solve the congruence $259x \equiv 5(\text{mod } 11)$. **[K.U. 2011]**

Solution : The given congruence is $259x \equiv 5 \text{ (mod } 11)$

Comparing it with $ax \equiv b(\text{mod } m)$, we have $a = 259$, $b = 5$, $m = 11$ .....(1)

Here $d = (a, m) = (259, 11) = 1$ and $d = 1$ divides $b = 5$ so (1) has one and only one incongruent solution. Now, 6 is the remainder obtained on dividing 259 by 11 so we can write

$$259 \equiv 6(\text{mod } 11)$$

Multiplying it both sides by x

$$259x \equiv 6x(\text{mod } 11)$$

By (1) and (2),we get .....(2)

$$6x \equiv 5(\text{mod } 11)$$

We consider the multiples of 11 i.e., 11, 22, 33, 44, 55, 66,..... .....(3)

Out of these we see that $55 + 5 = 60$ is divisible by 6, so we take the congruence

$$0 \equiv 55 \text{ (mod } 11)$$

Adding (3) and (4) , we get .....(4)

$$6x \equiv 60 \text{ (mod } 11)$$

Cancelling 6 as $(6, 11) = 1$, we get $x \equiv 10(\text{mod } 11)$ is the solution of (1)

Alternative Method : The given congruence is $259x \equiv 5 \text{ (mod } 11)$ .....(1)

Comparing it with $ax \equiv b(\text{mod } m)$ we have $a = 259$, $b = 5$, $m = 11$

Here $d = (a, m) = (259, 11) = 1$ and $d = 1$ divides $b = 5$ so (1) has one and only one incongruent solution. Now, 253 is the largest multiple of 11 which is less than 259 so we write

$$253x \equiv 0(\text{mod } 11)$$

Subtracting (2) from (1),we get .....(2)

$$6x \equiv 5(\text{mod } 11)$$

We consider the multiples of 11 i.e., 11, 22, 33, 44, 55, 66,..... .....(3)

Out of these we see that $55 + 5 = 60$ is divisible by 6, so we take the congruence

$$0 \equiv 55 \text{ (mod } 11)$$

Adding (3) and (4) , we get .....(4)

$$6x \equiv 60 \text{ (mod } 11)$$

Cancelling 6 as (6, 11) = 1, we get $x \equiv 10 (\text{mod } 11)$ is the solution of (1)

Method III : Method to solve the linear congruence $ax \equiv b (\text{mod } m)$ having more than one incongruent solutions modulo m.

(i) Write the given congruence in the form $ax \equiv b (\text{mod } m)$ .....(1)

(ii) Let $(a, m) = d$ and verify that d/b so that (1) has exactly d incongruent solutions modulo m.

(iii) Divide the congruence (1) throughout by d to obtain

$$\frac{a}{d}x \equiv \frac{b}{d}\left(\text{mod}\frac{m}{d}\right) \quad \text{.....(2)}$$

(iv) Now solve (2) by **Method I** and let the solution $x \equiv x_0$ is obtained.

(v) The all incongruent solutions of (1) are then given by

$$x = x_0 + \frac{km}{d} \text{ where } k = 0, 1, 2, \ldots\ldots\ldots\ldots, d-1.$$

Example 6 : Solve the linear congruence $15x \equiv 6 \pmod{21}$.

Solution : The given congruence is $15x \equiv 6 (\text{mod } 21)$ .....(1)

Comparing it with $ax \equiv b (\text{mod } m)$, we have $a = 15$, $b = 6$, $m = 21$.

Here, $d = (a,m) = (15, 21) = 3$ and $d = 3$ divides $b = 6$.

Therefore, the congruence (1) has exactly $d = 3$ incongruent solutions.

Dividing the congruence (1) throughout by $d = 3$, we get

$$5x \equiv 2 (\text{mod } 7) \quad \text{.....(2)}$$

Consider the multiples of 7 i.e., 7, 14, 21, 28, 35,.....

Out of these we see that 28 + 2 = 30 is divisible by 5 so we take the congruence

$$0 \equiv 28 (\text{mod } 7) \quad \text{.....(3)}$$

Adding (2) and (3), we get $5x \equiv 30 (\text{mod } 7)$

Cancelling 5 as (5, 7) = 1, we get $x \equiv 6 (\text{mod } 7)$ is one solution of the congruence (2).

$\therefore$ $x_0 = 6$ is a solution of congruence (2).

Therefore, all the three incongruent solutions modulo 21 of $15x \equiv 6 (\text{mod } 21)$ are given by

$$x = x_0 + \frac{km}{d}, \text{ where } k = 0, 1, 2, \ldots\ldots\ldots\ldots, d-1.$$

Here $x_0 = 6, d = 3, m = 21$

$\therefore$ $x = 6 + 7k$, where $k = 0, 1, 2$

i.e., $x = 6, 13, 20$

Thus $x = 6 (\text{mod } 21)$, $x \equiv 13 (\text{mod } 21)$ and $x \equiv 20 (\text{mod } 21)$ are three incongruent solutions modulo 21 of the linear congruence $15x \equiv 6 (\text{mod } 21)$.

Method IV : Method to solve the linear congruence $ax \equiv b (\text{mod } m)$ having more than one incongruent solution modulo m where 'a' is large.

This is just the combination of **Method II** and **Method III.**

Example 7 : Solve the congruence $222x \equiv 12 \pmod{18}$. **[M.D.U. 1997]**

Solution : The given congruence is $222x \equiv 12 \pmod{18}$ .....(1)

Comparing it with $ax \equiv b \pmod{m}$, we have $a = 222$, $b = 12$, $m = 18$

Here $d = (a, m) = (222, 18) = 6$ and $d = 6$ divides $b = 12$. Therefore the congruence (1) has exactly $d = 6$ incongruent solutions modulo 18.

Dividing the congruence (1) throughout by $d = 6$, we get

$$37x \equiv 2 \pmod{3} \quad \text{.....(2)}$$

Now 1 is the remainder obtained on dividing 37 by 3, so we can write

$$37 \equiv 1 \pmod{3}$$

Multiplying this both sides by x .

$$37x \equiv x \pmod{3} \quad \text{.....(3)}$$

By (2) and (3) , we get $x \equiv 2 \pmod{3}$ is a solution of the congruence (2). Hence $x_0 = 2$ is a solution of congruence (2).

Therefore, all the six incongruent solutions modulo 18 of $222x \equiv 12 \pmod{18}$ are given by

$$x = x_0 + \frac{km}{d}, \; k = 0, 1, 2, \ldots\ldots\ldots\ldots, d - 1$$

Here $x_0 = 2, m = 18, \quad d = 6$

$\therefore \quad x = 2 + 3k$ where $k = 0 , 1 , 2 , 3 , 4 , 5.$

i.e. $x = 2 , 5 , 8 , 11 , 14 , 17$

Hence $x \equiv 2 , 5 , 8 , 11 , 14 , 17 \pmod{18}$ are all six incongruent solutions modulo 18 of congruence $222x \equiv 12 \pmod{18}$.

Note : Methods explained earlier are not suitable for the linear congruences $ax \equiv b \pmod{m}$ in which m is large because they sometimes require difficult numerical calculations . So we develop a general method for solving linear congruences.

Method V : General method to solve linear congruence $ax \equiv b \pmod{m}$ with unique solution.

(i) Write the congruence as $ax \equiv b \pmod{m}$ .....(1)

(ii) Verify that $d = (a, m) = 1$ so that the given congruence has one and only one incongruent solution.

(iii) Express 1 in the form $1 = au + mv$

(iv) Multiply above equation by b to get $b = abu + mbv$

(v) Put this value of b in (1) to get $ax \equiv abu + mbv \pmod{m}$ .....(2)

(vi) Now write the congruence $0 \equiv -mbv \pmod{m}$ .....(3)

(vii) Adding (2) and (3) to get $ax \equiv abu \pmod{m}$

(viii) Cancel a from both sides to obtain the solution $x \equiv bu \pmod{m}$.

METHOD VI : General method to solve the linear congruence $ax \equiv b \pmod{m}$ having more than one incongruent solution.

(i) Write the given congruence as $ax \equiv b \pmod{m}$ .....(1)

(ii) Let $d = (a, m) > 1$ and d/b so that (1) has d incongruent solutions.

(iii) Divide (1) throughout by d to obtain $\frac{ax}{d} \equiv \frac{b}{d}\left(\text{mod}\frac{m}{d}\right)$ .....(2)

(iv) Solve (2) by **Method V** and let $x = x_0$ be the solution thus obtained.

(v) Now d incongruent solution of (1) are given by

$$x = x_0 + \frac{km}{d} \text{ where } k = 0, 1, 2, \ldots\ldots\ldots, d-1$$

Example 8 : Solve the congruence $7x \equiv 5(\text{mod } 256)$. **[K.U. 2010 (2nd Sem.), 95]**

Solution : The given congruence is $7x \equiv 5(\text{mod } 256)$ .....(1)

Comparing it with $ax \equiv b(\text{mod } m)$, we have $a = 7$, $b = 5$, $m = 256$

Here $d = (a, m) = (7, 256) = 1$ therefore (1) has a unique incongruent solution modulo m.

We express 1 in the form $7u + 256v$. For this we write

$256 = 7.36 + 4$ .....(i) [On dividing 256 by 7]

$7 = 4.1 + 3$ .....(ii) [On dividing 7 by 4]

$4 = 3.1 + 1$ .....(iii) [On dividing 4 by 3]

By (iii), $1 = 4 - 3.1$

$= 4 - (7 - 4)$ [$\because 3 = 7 - 4$ by (ii)]

$= 2.4 - 7$

$= 2(256 - 7.36) - 7$ [$\because 4 = 256 - 7.36$ by (i)]

$= 2.256 - 7.72 - 7$

$= 2.256 - 73.7$

$\Rightarrow \quad 1 = 7.(-73) + 2(256)$

Multiplying both sides by b = 5, we get

$5 = 5.7(-73) + 5.2(256)$

Putting this value of 5 in (1), we get

$7x = 5.7(-73) + 5.2(256) (\text{mod } 256)$

Writing $0 \equiv -5.2(256) (\text{mod } 256)$ .....(2)

Adding (2) and (3), we get $7x \equiv 5.7(-73) (\text{mod } 256)$ .....(3)

Cancelling 7 as $(7, 256) = 1$ we get $x \equiv -365 (\text{mod } 256)$

To obtain the positive solution, we write $0 \equiv 512 (\text{mod } 256)$ .....(4)

Adding (4) and (5), we get $x \equiv 147(\text{mod } 256)$ which is the required solution of (1). .....(5)

Example 9 : Solve the linear congruence $6x \equiv 3(\text{mod } 75)$

Solution : The given congruence is

$6x \equiv 3(\text{mod } 75)$

Comparing it with $ax \equiv b(\text{mod } m)$, we have $a = 6$, $b = 3$, $m = 75$ .....(1)

Here $d = (a, m) = (6, 75) = 3$ and $d = 3$ divides $b = 3$. therefore the given congruence has three incongruent solution modulo 75.

Dividing (1) throughout by $d = 3$, we get $2x \equiv 1 (\text{mod } 25)$

Comparing (2) with $a_1x \equiv b_1(\text{mod } m_1)$ we get $a_1 = 2$, $b_1 = 1$, $m_1 = 25$ .....(2)

Here $(a_1, m_1) = (2, 25) = 1$ divides $b_1 = 1$ so (2) has a unique solution.

We express 1 in the form $1 = 2u + 25v$.

For this we write $25 = 2.12 + 1$ [On dividing 25 by 2]

$\Rightarrow$ $1 = 2(-12) + 25$

Putting this value of 1 in (2), we get $2x \equiv 2(-12) + 25 \pmod{25}$ .....(3)

We write, $0 \equiv -25 \pmod{25}$ .....(4)

Adding (3) and (4), we get $2x \equiv 2(-12) \pmod{25}$

Cancelling 2 as $(2, 25) = 1$, we obtain $x \equiv -12 \pmod{25}$

To obtain a least positive solution we write

$0 \equiv 25 \pmod{25}$

Adding this and above congruence, we get

$x \equiv 13 \pmod{25}$.

Thus $x_0 \equiv 13$ is a solution of (2) as well as of (1).

Now all the three in-congruent solution modulo 75 of (1) are given by

$$x = x_0 + \frac{km}{d},\ k = 0, 1, 2, \ldots\ldots, d-1$$

i.e., $x = 13 + 25k,\ k = 0, 1, 2$

$\therefore$ $x_0 \equiv 13, 38, 63 \pmod{75}$ are the three incongruent solutions modulo 75 of the congruence (1).

Note : Although **Method V** and **Method VI** can be applied to every linear congruence (as they are general methods),we usually adopt these methods when m is large.

Exercise 2.2

1. Find the solution of the following linear congruences by inspection.

(i) $4x \equiv 2 \pmod{7}$ **(ii)** $3x \equiv 1 \pmod{8}$ **(iii)** $3x \equiv 6 \pmod{9}$

2. Do the following congruence possess a solution

(i) $4x \equiv 5 \pmod{6}$ **(ii)** $84x \equiv 16 \pmod{35}$

(iii) $12x \equiv 4 \pmod{6}$ **(iv)** $3x \equiv 7 \pmod{10}$

3. Find the number of incongruent solutions of following linear congruences

(i) $3x \equiv 5 \pmod{7}$ [K.U. 2000, M.D.U. 1996] **(ii)** $10x \equiv 3 \pmod{5}$

(iii) $15x \equiv 20 \pmod{10}$

4. Solve the following linear congruences

(i) $13x \equiv 10 \pmod{28}$ **(ii)** $4x + 3 \equiv 4 \pmod{5}$

(iii) $2x + 1 \equiv 0 \pmod{7}$ [M.D.U. 1998] **(iv)** $51x \equiv 32 \pmod{5}$

5. Solve the congruences

(i) $55x \equiv 1 \pmod{7}$ **(ii)** $51x \equiv 32 \pmod{5}$

(iii) $77x \equiv 1 \pmod{5}$ **(iv)** $342x \equiv 5 \pmod{13}$

6. Solve the following congruences

(i) $36x \equiv 27 \pmod{45}$ **(ii)** $15x \equiv 12 \pmod{36}$

Chapter 4

Euler's and Chinese Remainder Theorems

1. EULER'S ϕ-FUNCTION AND ITS PROPERTIES :

Def. Euler's ϕ-function : Let m be any positive integer, then Euler's ϕ function is defined as : [M.D.U. 2011]

$\phi(1) = 1$ and $\phi(m)$ = number of natural number less than m which are relatively prime to m.

For Example , $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(10) = 4$ etc.

Def. Multiplicative function : A function $f(n)$ is said to be multiplicative if it is not identically zero and $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$

Remark : Now, we lead to an important theorem showing that $\phi(n)$ is a multiplicative function. For this, we first give three results which are proved earlier.

1. Given integers a, b, c we have that $gcd\ (a, bc) = 1$ iff $g.c.d.(a\ ,\ b) = 1$ and $g.c.d.\ (a\ ,\ c) = 1$.
2. If $a \equiv r \pmod m$ then $(a\ ,\ m) = (r\ ,\ m)$
   This result can also be stated as if $a = qm + r\ ,\ 0 \le r < m$, then $(a\ ,\ m) = (r\ ,\ m)$
3. If $S = \{0, 1, 2, ..., n-1\}$, then no two elements of this set are congruent modulo n.

Theorem 1.1 : $\phi(n)$ is a multiplicative function

i.e. $\phi(m\ n) = \phi(m)\ \phi(n)$ where $(m\ ,\ n) = 1$. **[M.D.U. 2010 (2nd Sem.)]**

Proof : If $m = 1$ or $n = 1$, then the theorem is trivial , so let $m > 1$ and $n > 1$. Let us arrange first $m\ n$ natural numbers in n rows and m columns as

$$\begin{array}{ccccc} 1 & 2 & 3 & \ldots\ldots\ldots\ldots & m \\ m+1 & m+2 & m+3 & \ldots\ldots\ldots\ldots & 2m \\ 2m+1 & 2m+2 & 2m+3 & \ldots\ldots\ldots\ldots & 3m \\ \vdots & \vdots & \vdots & \ldots\ldots\ldots\ldots & \vdots \\ \vdots & \vdots & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \ldots\ldots\ldots\ldots & nm \end{array} \quad \ldots\ldots(1)$$

We shall prove the theorem in three steps.

Step (i) : First we prove that out of m columns in above arrangement there are $\phi(m)$ columns whose elements are co-prime to m.

In arrangement (1) , we observe that in the rth column, the numbers are of the form $qm + r$ $(0 \le q \le n - 1)$ and since $(qm + r , m) = (r , m)$ it follows that the numbers in the rth column are co-prime to m iff r itself is co-prime to m.

But in this arrangement number of such columns is $\phi(m)$ i.e. only $\phi(m)$ columns contains integers co-prime to m

Step (ii) Now we prove that each of the $\phi(m)$ columns obtained in step (i), contains $\phi(n)$ elements which are co-prime to n.

Consider the r th column. The entries in the rth column are

$$r, m + r, 2m + r, \ldots\ldots\ldots, (n-1)m + r$$

These are n numbers and we show that no two of these congruent mod n. Let , if possible,

$$km + r \equiv jm + r \pmod{n} \qquad \text{where } 0 \le k < j < n$$

$$\Rightarrow \quad km \equiv jm \pmod{n}$$

$$\Rightarrow \quad k \equiv j \pmod{n} \qquad [\because (m , n) = 1]$$

which is a contradiction , since any two elements of the set $\{0,1,2,\ldots\ldots,n-1\}$ are incongruent modulo n.

Thus the numbers in the rth column are congruent mod n to 0, 1, 2, ..., n – 1 in some order. But we know that if a ≡ b (mod n), then (a , n) =1 iff (b , n) = 1. This implies that rth column contains as many numbers which are co-prime to n as does the set $\{0, 1, 2, \ldots\ldots, n-1\}$. But the set $\{0,1,2,\ldots\ldots,n-1\}$ clearly contains $\phi(n)$ elements which are co prime to n . Hence rth column contains $\phi(n)$ numbers which are co prime to n.

Step (iii) By step (i) and (ii), we conclude that in arrangement (1), the numbers which are co prime to both m and n are $\phi(m)\ \phi(n)$. But we know that if an integer is co-prime to m and n then it is also co-prime to their product mn. Thus the number of integers in the arrangement (1) which are co-prime to mn are $\phi(m)\ \phi(n)$. But by definition of Euler's function, this number is $\phi(mn)$.

Thus, we have obtained $\phi(mn) = \phi(m)\ \phi(n)$.

Theorem 1.2 : If p is a prime and $k > 0$, then $\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$.

[M.D.U. 20

Proof : Clearly g.c.d. $(n, p^k) = 1$ iff $p \nmid n$. There are exactly p^{k-1} integers between 1 and p^k which are divisible by p namely

$$p, 2p, 3p, \ldots\ldots\ldots\ldots, p^{k-1}.p$$

Thus the set $\{1, 2, \ldots\ldots, p^k\}$ contains exactly p^{k-1} integers which are not relatively prime to p^k and so by definition of $\phi(n)$, we get

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

Theorem 1.3 : Let $n = p_1^{k_1} p_2^{k_2} \ldots\ldots\ldots p_r^{k_r}$ **be any natural number where** $p_1, p_2, \ldots\ldots, p_r$ **are prime numbers then** $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\ldots\left(1-\frac{1}{p_r}\right)$.

OR

For any positive integer $n \geq 1$ $\quad \phi(n) = n\prod_{p/n}\left(1-\frac{1}{p}\right)$. **[K.U. 2011]**

Proof : We know that , for any prime p , $\quad \phi(p^k) = p^k - p^{k-1} = p^k\left(1-\frac{1}{p}\right)$

Now let $n > 1$ be any natural number with prime power factorization given by

$$n = p_1^{k_1} p_2^{k_2} \ldots\ldots\ldots p_r^{k_r}$$

Then we have $\phi(n) = \phi\left(p_1^{k_1} p_2^{k_2} \ldots\ldots\ldots p_r^{k_r}\right)$

$= \phi(p_1^{k_1})\,\phi(p_2^{k_2})\ldots\ldots\ldots\phi(p_r^{k_r})$ [As $\phi(n)$ is a multiplicative function and $(p_i^{k_i}, p_j^{k_j}) = 1$]

$= p_1^{k_1}\left(1-\frac{1}{p_1}\right)p_2^{k_2}\left(1-\frac{1}{p_2}\right)\ldots\ldots\ldots p_r^{k_r}\left(1-\frac{1}{p_r}\right)$

$= p_1^{k_1} p_2^{k_2}\ldots\ldots\ldots p_r^{k_r}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\ldots\ldots\left(1-\frac{1}{p_r}\right)$

$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\ldots\ldots\left(1-\frac{1}{p_r}\right) = n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$ or $\phi(n) = n\prod_{p/n}\left(1-\frac{1}{p}\right)$

Example 1 : Evaluate the following :

(i) $\phi(92)$ **(ii)** $\phi(385)$ **(iii)** $\phi(1575)$

Solution : (i) We have $n = 92 = (2)^2\,(23)^1 = p_1^{k_1}\, p_2^{k_2}$

where $p_1 = 2$, $p_2 = 23$ and $k_1 = 2$, $k_2 = 1$.

We know that if $n = p_1^{k_1}\, p_2^{k_2}\ldots\ldots\ldots p_r^{k_r}$

then $\quad \phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\ldots\left(1-\frac{1}{p_k}\right)$

$\therefore \quad \phi(92) = 92\left(1-\frac{1}{2}\right)\left(1-\frac{1}{23}\right) = 92\times\frac{1}{2}\times\frac{22}{23} = 44$

(ii) Here, $\quad n = 385 = 5\,.\,7\,.\,11 = p_1^{k_1}\,.\,p_2^{k_2}\,.\,p_3^{k_3}$

where $p_1 = 5$, $p_2 = 7$, $p_3 = 11$ and $k_1 = k_2 = k_3 = 1$

Using $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)$, we get

$$\phi(385) = 385\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)$$

$$= 385\times\frac{4}{5}\times\frac{6}{7}\times\frac{10}{11} = 240$$

(iii) We have $n = 1575 = (3)^2\ (5)^2\ (7)^1 = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3}$

where $p_1 = 3,\ p_2 = 5,\ p_3 = 7$ and $k_1 = 2,\ k_2 = 2,\ k_3 = 1$

Using $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)$, we get

$$\phi(1575) = 1575\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)$$

$$= (3)^2\ (5)^2\ (7)^1\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right) = 720$$

Example 2 : (i) Find the number of positive integers ≤ 3600 that are co-prime to 3600.

(ii) Find the number of positive integers ≤ 3600 that have a factor greater than 1 in common with 3600.

Solution :(i) We have $n = 3600 = (2)^4\ (3)^2\ (5)^2 = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3}$

where $p_1 = 2,\ p_2 = 3,\ p_3 = 5$ and $k_1 = 4,\ k_2 = 2,\ k_3 = 2$

We know that number of positive integers ≤ 3600 that are coprime to 3600 is $\phi(3600)$. So we have to calculate $\phi(3600)$.

Using $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_3}\right)$, we get

$$\phi(3600) = 3600\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= (2)^4\ (3)^2\ (5)^2\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) = 960$$

(ii) In above part we have evaluated that there are 960 positive integers ≤ 3600 that are coprime to 3600. The remaining positive integers ≤ 3600 are those which are not coprime to 3600 i.e., they have a factor greater than 1 in common with 3600. So, number of such integers is 3600 – 960 = 2640.

Example 3 : For $n > 2$, $\phi(n)$ is even.

Solution : We consider two cases :

Case (i) : When n has no odd prime factor :

In this case, the only prime which divides n is 2, therefore

$$n = 2^k \text{ for some } k > 1$$

Then, $$\phi(n) = \phi(2^k) = 2^k\left(1-\frac{1}{2}\right)$$

$$= (2)^k\left(\frac{1}{2}\right) = (2)^{k-1} \text{ which is even as } k - 1 > 0.$$

Case (ii) : When n has atleast one odd prime factor, say p.

In this case, let k is the maximum power of p which occurs in factorization of n and so

$$n = p^k\ (m) \text{ where } k \geq 1 \text{ and } (p^k, m) = 1$$

Now,
$$\begin{aligned}\phi(n) &= \phi(p^k \cdot m)\\ &= \phi(p^k)\,\phi(m) && [\because \phi \text{ is multiplicative}]\\ &= (p^k - p^{k-1})\,\phi(m)\\ &= p^{k-1}(p-1)\,\phi(m)\end{aligned}$$
As p is a odd prime, $p-1$ is even. Since product of an even number with any number is even, so $\phi(n)$ is even.

Example 4 : For what values of n, $\phi(n)$ is odd.

Solution : We know that $\phi(1) = 1$ and $\phi(2) = 1$. Further, for $n > 2$, $\phi(n)$ is even as shown in above example. So $\phi(n)$ is odd only for $n = 1, 2$.

Example 5 : Find all possible values of n which satisfies $\phi(n) = 7$ (or any odd number > 1).

Solution : We know that $\phi(1) = \phi(2) = 1$ and $\phi(n) =$ even for $n \geq 3$.
Here $\phi(n) = 7$ (or any odd number > 1), so there exists no n which satisfies the given equation.

Example 6 : Characterize the set of positive integers n that satisfies $\phi(n) = 2$.

Solution : As $\phi(n) = 2$ so $n \geq 2$. We consider two cases on n.

Case (i) : When n is odd :

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$ where each prime p_i is odd i.e., $p_i \geq 3$ for all i.

$$\Rightarrow \quad \phi(n) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r})$$
$$\Rightarrow \quad 2 = \phi(p_1^{\alpha_1})\,\phi(p_2^{\alpha_2}) \ldots\ldots \phi(p_r^{\alpha_r}) \qquad [\because \phi \text{ is multiplicative}]$$
$$\Rightarrow \quad 2 = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})\,(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \ldots\ldots (p_r^{\alpha_r} - p_r^{\alpha_r - 1}) \qquad \ldots\ldots(1)$$

Now, $p_i \geq 3$ for all i.

$$\Rightarrow \quad p_i^{\alpha_i} - p_i^{\alpha_i - 1} \geq 2 \text{ for all } i$$

Therefore, to satisfy (1), there must be only one prime in the factorization of n, say, p_1. So, by (1), we have
$$2 = p_1^{\alpha_1} - p_1^{\alpha_1 - 1}$$
This is satisfied only for $p_1 = 3$ and $\alpha_1 = 1$.
$$\therefore \quad n = p_1^{\alpha_1} = 3^1 = 3 \text{ in this case.}$$

Case (ii) : When n is even :

Let k be the maximum power of 2, which appears in factorization of n.
i.e., $n = 2^k m$ where $k \geq 1$ and m is odd.

$$\Rightarrow \quad \begin{aligned}\phi(n) &= \phi(2^k \cdot m)\\ &= \phi(2^k)\,\phi(m) && [\because \phi \text{ is multiplicative}]\\ &= (2^k - 2^{k-1})\,\phi(m)\end{aligned}$$

$$= 2^{k-1} \cdot \phi(m)$$

$$\Rightarrow \quad 2 = 2^{k-1}\, \phi(m) \qquad \ldots\ldots(2)$$

By (2), it is clear that $k - 1 \leq 1$

$$\Rightarrow \quad k \leq 2 \quad \Rightarrow \quad k = 1 \text{ or } 2$$

If $k = 1$, then by (2), $\phi(m) = 2$.

Also m is odd, so by case (i), $m = 3$. Therefore $n = 2^k \cdot m = 2^1 \cdot 3 = 6$. If $k = 2$, then by (2), $\phi(m) = 1$.

Also m is odd and we know that $\phi(m) = 1$ only for $m = 1, 2$, so m must be 1.

Therefore $n = 2^k \cdot m = (2)^2 (1) = 4$.

Thus we have proved that $\phi(n) = 2$ if $n = 3, 4, 6$.

Example 7 : Prove that $\phi(n) = n$ iff $n = 1$.

Solution : We know that $\phi(1) = 1$. So $\phi(n) = n$ is satisfied for $n = 1$. Now, we shall prove that for any $n > 1$, we must have $\phi(n) \neq n$.

We have, $\phi(2) = 1$ so $\phi(n) \neq n$ for $n = 2$. So suppose $n > 2$.

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$, where $p_1, p_2, \ldots\ldots, p_r$ are the distinct primes and $k \geq 0$.

Now, let if possible, $\phi(n) = n$.

$$n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\ldots\left(1-\frac{1}{p_r}\right) = n$$

$$\Rightarrow \quad \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\ldots\left(1-\frac{1}{p_r}\right) = 1$$

which is a contradiction since each bracket on the left hand side is less than 1, so their product is also less than 1.

So, our supposition is wrong and hence $\phi(n) \neq n$.

Concluding all the above discussion, we obtain

$$\phi(n) = n \text{ iff } n = 1.$$

Example 8 : Prove that $\phi(n) = \frac{n}{2}$ iff $n = 2^k$ for some integer $k \geq 1$.

Solution : Suppose first that $\phi(n) = \frac{n}{2}$

We know that $\phi(n)$ is always an integer

$$\Rightarrow \quad \frac{n}{2} \text{ is an integer}$$

$$\Rightarrow \quad n \text{ is an even integer}$$

Let k be the maximum power of 2 which occurs in the factorization of n so that $n = 2^k (m)$ where $k \geq 1$ and m is odd

Now, given that $\phi(n) = \frac{n}{2}$

$$\Rightarrow \quad \phi(2^k \cdot m) = \frac{2^k \cdot m}{2}$$

$$\Rightarrow \quad \phi(2^k)\,\phi(m) = 2^{k-1}(m)$$

$$\Rightarrow \quad (2^k - 2^{k-1})\,\phi(m) = 2^{k-1}(m)$$

$$\Rightarrow \quad 2^{k-1}\,\phi(m) = 2^{k-1}(m)$$

$$\Rightarrow \quad \phi(m) = m$$

$$\Rightarrow \quad m = 1 \qquad \text{[By above example]}$$

Therefore, $n = 2^k\,(m) = 2^k$.

Conversely, suppose that $n = 2^k$ for $k \geq 1$.

$$\Rightarrow \quad \phi(n) = \phi(2^k) = 2^k - 2^{k-1}$$

$$= 2^{k-1} = \frac{2^k}{2} = \frac{n}{2}$$

Exercise 4.1

1. Evaluate
   (i) $\phi(800)$ **(ii)** $\phi(450)$ **(iii)** $\phi(1260)$ **(iv)** $\phi(1002)$
2. **(i)** Find the number of positive integers ≤ 1800 that are relatively prime to 1800.
   (ii) Find the number of positive integers ≤ 1800 that have a factor greater than 1 in common with 1800.
3. Show that $\phi(10^n) = 4 \times 10^{n-1}$.
4. Find all possible values of n for which $\phi(n) = 11$.
5. If p and $p + 2$ are both primes then prove that $\phi(p+2) = \phi(p) + 2$.
6. **(i)** If p and $2p + 1$ are both primes and $n = 4p$ then prove that $\phi(n+2) = \phi(n) + 2$.
   (ii) If p and $2p - 1$ are both odd primes and $n = 2(2p-1)$ then prove that $\phi(n+2) = \phi(n)$.
7. If m and n are positive integers and $(m, n) = d$ then prove that $\phi(mn) = \dfrac{d \cdot \phi(m)\,\phi(n)}{\phi(d)}$.

Answers

1. **(i)** 320 **(ii)** 120 **(iii)** 288 **(iv)** 332 **2.** **(i)** 480 **(ii)** 1320 **4.** No such n exist

2. RESIDUE SYSTEMS AND EULER'S THEOREM :

Def. : Complete Residue System : A set containing m incongruent integers modulo m is called a complete residue system modulo m i.e. the set $\{a_1, a_2, \ldots\ldots, a_m\}$ is a complete residue system modulo m if

$$a_i \not\equiv a_j \pmod{m} \text{ for } i \neq j$$

OR

A set $\{a_1, a_2, \ldots\ldots, a_m\}$ of integers is said to be complete residue system modulo m if for every integer x there is a unique a_i such that

$$x \equiv a_i \pmod{m}$$

Remark 1 : There are always infinitely many complete residue systems modulo m. Any set containing m consecutive integers is always a complete residue system modulo m.

Remark 2 : The set $\{0, 1, 2, \ldots\ldots, m-1\}$ is the most fundamental complete residue system modulo m. If $\{a_1, a_2, \ldots\ldots, a_m\}$ is any other complete residue system modulo m, then each a_i must be congruent to exactly one number of the set $\{0, 1, 2, \ldots\ldots, m-1\}$.

Thus, we have the following criteria to determine whether a given set S is a complete residue system modulo m or not :

(i) S must have m integers.

(ii) Least non-negative residues modulo m of the integers of S must be just an rearrangement (per-mutation) of the integers $0, 1, 2, \ldots\ldots, m-1$.

Example 1 : Which of the following sets form complete residue system:

(i) $\{-3, 7, 3, 12, 37, 57, -1\} \pmod 7$ **(ii)** $\{11, -3, -4, 7, 18, 22\} \pmod 6$

(iii) $\{5, 3, 2, -5, 6\} \pmod 6$

Solution : (i) The given set contains seven integers and the least non-negative residues modulo 7 of these integers are

$$4, 0, 3, 5, 2, 1, 6$$

which is an rearrangement of the integers 0, 1, 2, 3, 4, 5, 6.

Hence the given set forms a complete residue system modulo 7.

(ii) The given set contains six integers and the least non-negative residues modulo 6 of these integers are

$$5, 3, 2, 1, 0, 4$$

Which is an rearrangement of the integers 0, 1, 2, 3, 4, 5.

Hence the given sets forms a complete residue system modulo 6.

(iii) The given set does not contain six elements therefore it can not be a complete residue system modulo 6.

Theorem 2.1 : If $\{a_1, a_2, \ldots\ldots, a_m\}$ is a complete residue system modulo m and $(k, m) = 1$ then $\{ka_1, ka_2, \ldots\ldots, ka_m\}$ is also a complete residue system modulo m.

Proof : Clearly the set $\{ka_1, ka_2, \ldots\ldots, ka_m\}$ contains m incongruent integers because if $k a_i \equiv k a_j \pmod m$ for $i \neq j$ then $a_i \equiv a_j \pmod m$ $[\because (k, m) = 1]$ which is a contradiction.

Hence the set $\{ka_1, ka_2, \ldots\ldots, ka_m\}$ is a complete residue system modulo m.

Example 2 : Show that $\{2, 4, 6, \ldots\ldots, 2m\}$ is a complete residue system modulo m if m is odd.

Solution : Clearly, the set $\{1, 2, 3, \ldots\ldots, m\}$ is a complete residue system modulo m and as m is given to odd so $(2, m) = 1$. So, by above theorem $\{2, 4, 6, \ldots\ldots, 2m\}$ is also a complete residue system modulo m.

Example 3 : If m is an even positive integer then show that $\left\{-\frac{m-2}{2}, -\frac{m-4}{2}, \ldots\ldots, -1, 0, 1, \ldots\ldots, \frac{m-4}{2}, \frac{m-2}{2}, \frac{m}{2}\right\}$ is a complete residue system modulo m.

Solution : Clearly, the set has m elements. The integers $0, 1, \ldots\ldots, \frac{m-2}{2}, \frac{m}{2}$ are themselves the least non-negative residues modulo m, so let us find the least non-negative residues of the integers $-\frac{m-2}{2}, -\frac{m-4}{2}, \ldots\ldots, -1$.

For this, we see that

$$-\frac{m-2}{2} \equiv \frac{m+2}{2} \pmod m$$

$$-\frac{m-4}{2} \equiv \frac{m+4}{2} \pmod m$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$-2 \equiv m-2 \pmod m$$

$$-1 \equiv m-1 \pmod m$$

Thus, the least non-negative residues modulo m of the integers of the given set are

$$\frac{m+2}{2}, \frac{m+4}{2}, \ldots\ldots, m-2, m-1, 0, 1, 2, \ldots\ldots, \frac{m-2}{2}, \frac{m}{2}$$

which is just an rearrangement of the set $0, 1, 2, \ldots\ldots, m-1$.

Therefore the given set is a complete residue system modulo m.

Example 4 : Write a complete residue system modulo 11 composed entirely of multiples of 2.

Solution : We know that the set $\{0, 1, 2, \ldots\ldots, 10\}$ is a complete residue system modulo 11. Since $(2, 11) = 1$, by above theorem, $\{0, 2, 4, \ldots\ldots, 20\}$ is also a complete residue system modulo 11.

Def. Reduced Residue System : A set $\{r_1, r_2, \ldots\ldots, r_k\}$ of integers is said to reduced residue system mod m if

(i) $(r_i, m) = 1$, $1 = 1, 2, \ldots\ldots, k$

(ii) $r_i \not\equiv r_j \pmod{m}$ for $i \neq j$

(iii) If x is any integer which is co-prime to m, then there exists a unique r_i s.t. $x \equiv r_i \pmod{m}$

OR

Def. Reduced Residue System : A set $\{r_1, r_2, \ldots\ldots, r_k\}$ of integers is said to reduced residue system mod m if

(i) $(r_i, m) = 1$, $1 = 1, 2, \ldots\ldots, k$

(ii) $r_i \not\equiv r_j \pmod{m}$ for $i \neq j$

(iii) The set $\{r_1, r_2, \ldots\ldots, r_k\}$ has $\phi(m)$ elements i.e. $k = \phi(m)$.

Remark : The most fundamental reduced residue system modulo m is the set of positive integers $\leq m$ which are coprime to m. This set will contain $\phi(m)$ integers.

For example, if $m = 12$ then {1, 5, 7, 11} is the reduced residue system modulo 12. This set contains $\phi(12) = 4$ positive integers.

If S is any other reduced residue system modulo 12, then it must have four integers and the least positive residues of these integers must be an rearrangement of 1, 5, 7, 11.
e.g. Let $S = \{23, -11, 43, 65\}$. Here S contains four elements and the least positive residues modulo 12 are 11, 1, 7, 5
which is just an rearrangement of the integers 1, 5, 7, 11.
Therefore $S = \{23, -11, 43, 65\}$ is a reduced residue system modulo 12.

Example 5 : Show that the set $\{64, 157, -14, -28, -37, 11, 28, 104\}$ is a reduced residue system modulo 15.

Solution : The positive integers ≤ 15, which are coprime to 15 are

1, 2, 4, 7, 8, 11, 13, 14

The given set will become a reduced residue system modulo 15 if the least positive residues of its integers is just an rearrangement of above integers.

The given set {64, 157, – 14, – 28, – 37, 11, 28, 104} contains eight elements and its least positive residues are

4, 7, 1, 2, 8, 11, 13, 14

which is just an rearrangement of 1, 2, 4, 7, 8, 11, 13, 14.

Therefore the given set is a reduced residue system modulo 15.

Theorem 2.2 : Let $\{r_1, r_2, \ldots\ldots, r_k\}$ be a reduced residue system mod m and a be any integer such that $(a, m) = 1$ then $\{ar_1, ar_2, \ldots\ldots, ar_k\}$ is also a reduced residue system mod m.

Proof : To prove that $\{ar_1, ar_2, \ldots, ar_k\}$ is a reduced residue system we have to prove the following three things (according to definition of reduced residue system):

(i) $(ar_i, m) = 1$ for $1 \leq i \leq k$

(ii) $ar_i \not\equiv ar_j \pmod{m}$ for $i \neq j$

(iii) The set $\{ar_1, ar_2, \ldots\ldots, ar_k\}$ has $\phi(m)$ elements i.e. $k = \phi(m)$.

Let us prove these three things one by one.

(i) Since $\{r_1, r_2, \ldots\ldots r_k\}$ is a reduced residue system so $(r_i, m) = 1$ for $1 \le i \le k$

Also $(a, m) = 1$ (given). So, we get $(ar_i, m) = 1$

$[\because$ If $(a, m) = 1$ and $(b, n) = 1$ then $(ab, m) = 1]$

(ii) Let, if possible, $ar_i \equiv ar_j \pmod{m}$ for $i \neq j$

Then, cancelling a [as $(a, m) = 1$], we get

$$r_i \equiv r_j \pmod{m} \text{ for } i \neq j$$

which is a contradiction to the fact that $\{r_1, r_2, \ldots\ldots, r_k\}$ is a reduced residue system.

(iii) Since $\{r_1, r_2, \ldots\ldots, r_k\}$ is a reduced residue system so it contains $\phi(m)$ elements i.e. $k = \phi(m)$ and so the set $\{ar_1, ar_2, \ldots\ldots, ar_k\}$ also contains the $\phi(m)$ elements.

2.3 : Euler's Theorem : If $(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$

Proof : Let $\{r_1, r_2, \ldots\ldots, r_{\phi(m)}\}$ be reduced residue system mod m. Since $(a, m) = 1$. So by last theorem $\{ar_1, ar_2, \ldots\ldots, ar_{\phi(m)}\}$ is also a reduced residue system mod m. Hence by definition corresponding to each r_i, there is one and only one ar_j s.t.

$$r_i \equiv ar_j \pmod{m} \qquad \ldots\ldots(1)$$

Further, different r_i will have different corresponding ar_j. This implies that the numbers $ar_1, ar_2, \ldots\ldots, ar_{\phi(m)}$ are just the residue modulo m of $r_1, r_2, \ldots\ldots, r_{\phi(m)}$ but not necessarily in the same order. Thus multiplying all congruences of form (1), we obtain

$$\prod_{j=1}^{\phi(m)} (ar_j) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}$$

$$\Rightarrow \quad a^{\phi(m)} \prod_{j=1}^{\phi(m)} r_j \equiv \prod_{j=1}^{\phi(m)} r_j \pmod{m}$$

Now $(r_j, m) = 1$, so $\left(\prod_{j=1}^{\phi(m)} r_j , m \right) = 1$ and therefore cancelling $\prod_{j=1}^{\phi(m)} r_j$, we get $a^{\phi(m)} \equiv 1 \pmod{m}$

Remark : Above Theorem is also known as Euler's Generalization of Fermat's theorem.

Cor. Fermat's Theorem : Let p be a prime s.t. $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof : Since p is prime, so every natural number less than p is co-prime to p so that $\phi(p) = p - 1$.

Now given that p is prime and $p \nmid a$ $\Rightarrow$ $(p, a) = 1$

Hence by Euler' theorem $a^{\phi(p)} \equiv 1 \pmod{p}$ $\Rightarrow$ $a^{p-1} \equiv 1 \pmod{p}$

Exercise 4.2

1. Which of the following sets form a complete residue system :
   (i) $\{23, 52, 7, -6, -1, -66, 145\}$ (mod 7)
   (ii) $\{-28, -16, 18, 31, 64, 605\}$ (mod 6)
   (iii) $\{-298, -696, 100, 503, 201\}$ (mod 5)

2. Which of the following sets form a reduced residue system :
   (i) $\{17, -21, 45, -73\}$ (mod 8)
   (ii) $\{-77, 65, 25, 109\}$ (mod 12)
   (iii) $\{13, 25, 80, -8, -16, -31\}$ (mod 9)
   (iv) $\{-23, 125, 37, -5\}$ (mod 12)

3. Write a complete residue system modulo 7 composed entirely of
   (i) multiples of 2 (ii) multiples of 3.

4. Write a reduced residue system for modulo 12 and modulo 30.

5. For an odd positive integer m, prove that the sum of integers of any complete residue system modulo m is congruent to zero modulo m.

6. If $\{r_1, r_2, \ldots\ldots, r_{p-1}\}$ is any reduced residue system modulo p, where p is a prime, then prove that $\prod_{i=1}^{p-1} r_i \equiv -1 (\text{mod } p)$.

7. If m is an odd positive integer then prove that the set $\left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots\ldots, -1, 0, 1, \ldots\ldots, \frac{m-3}{2}, \frac{m-1}{2}\right\}$ is a complete residue system modulo m.

Answers

1. (i), (iii)
2. (i), (iii)
3. (i) $\{0, 2, 4, 6, 8, 10, 12\}$
   (ii) $\{0, 3, 6, 9, 12, 15, 18\}$
4. $\{1, 5, 7, 11\}$ and $\{1, 7, 11, 13, 17, 19, 23, 29\}$

3. CHINESE REMAINDER THEOREM

The following theorem is called the Chinese Remainder Theorem in honour of Chinese mathematician' early contributions to the theory of congruences.

Chinese Remainder Theorem : Let the integers $m_1, m_2, \ldots\ldots, m_n$ are relatively prime in pairs i.e., $(m_i, m_j) = 1$ for $i \neq j$ and $a_1, a_2, \ldots\ldots, a_n$ are any integers, then the congruences $x \equiv a_1 (\text{mod}\, m_1)$, $x \equiv a_2 (\text{mod}\, m_2)$, ..., $x \equiv a_n (\text{mod}\, m_n)$ have a common solution. Further any two common solutions of these congruences are congruent modulo m, where $m = m_1 m_2 \ldots\ldots m_n$. **[K.U. 2011 (Only statement)]**

Proof : The given n congruences are

$$\left.\begin{aligned} x &\equiv a_1 (\text{mod}\, m_1) \\ x &\equiv a_2 (\text{mod}\, m_2) \\ &\ldots\ldots\ldots\ldots \\ x &\equiv a_n (\text{mod}\, m_n) \end{aligned}\right] \quad \ldots\ldots(1)$$

Also, it is given that $m = m_1 . m_2 \ldots\ldots m_n$. We define n new integers as follows :

$$b_1 = \frac{m}{m_1}, \quad b_2 = \frac{m}{m_2}, \ldots\ldots\ldots\ldots, b_n = \frac{m}{m_n}$$

i.e

$$\left.\begin{aligned} b_1 &= \frac{m_1 m_2 \ldots\ldots m_n}{m_1} = m_2 m_3 \ldots\ldots m_n \\ b_2 &= \frac{m_1 m_2 \ldots\ldots m_n}{m_2} = m_1 m_3 \ldots\ldots m_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ b_n &= \frac{m_1 m_2 \ldots\ldots m_n}{m_n} = m_1 m_2 \ldots\ldots m_{n-1} \end{aligned}\right] \quad \ldots\ldots(2)$$

Now, we consider the n new congruences

$$\left.\begin{aligned} b_1 x &\equiv 1 (\text{mod}\, m_1) \\ b_2 x &\equiv 1 (\text{mod}\, m_2) \\ &\ldots\ldots\ldots\ldots \\ b_n x &\equiv 1 (\text{mod}\, m_n) \end{aligned}\right] \quad \ldots\ldots(3)$$

Out of these congruences, we consider the first congruence i.e.,

$$b_1 x \equiv 1 (\text{mod}\, m_1)$$

Given that m_1 is coprime to each of m_2, m_3, ..., m_n , so m_1 is also coprime to their product $m_2 . m_3 \ldots\ldots m_n = b_1$ i.e. $(m_1, b_1) = 1$ and therefore the congruence $b_1 x \equiv 1 \ (\text{mod}\ m_1)$ has a unique incongruent solution modulo m_1.

Let this solution be x_1 and therefore $b_1 x_1 \equiv 1 (\text{mod}\, m_1)$ .....(4)

$m_1 = 3,\ m_2 = 4,\ m_3 = 5$

Here $(m_1, m_2) = (3, 4) = 1$, $(m_2, m_3) = (4, 5) = 1$ and $(m_1, m_3) = (3, 5) = 1$

So m_1, m_2, m_3 are relatively prime in pairs and therefore congruences in (1) have common solutions.

Let $m = m_1 . m_2 . m_3 = 3.4.5 = 60$

and

$$b_1 = \frac{m}{m_1} = \frac{60}{3} = 20$$

$$b_2 = \frac{m}{m_2} = \frac{60}{4} = 15$$

$$b_3 = \frac{m}{m_3} = \frac{60}{5} = 12$$

Now we consider the three new congruences one by one.

First we consider $b_1 x \equiv 1 \pmod{m_1}$ .....(2

i.e. $20x \equiv 1 \pmod 3$

we have $18x \equiv 0 \pmod 3$

Subtracting above two, $2x \equiv 1 \pmod 3$

Also $0 \equiv 3 \pmod 3$

Adding above two, $2x \equiv 4 \pmod 3$

Cancelling 2 as $(2, 3) = 1$, we get $x \equiv 2 \pmod 3$

$\therefore$ $x_1 = 2$ is a solution of (2).

Now we consider the congruence

$b_2 x \equiv 1 \pmod{m_2}$ .....(3

i.e. $15x \equiv 1 \pmod 4$

we have $12x \equiv 0 \pmod 4$

Subtracting above two, $3x \equiv 1 \pmod 4$

Also $0 \equiv 8 \pmod 4$

Adding above two, $3x \equiv 9 \pmod 4$

Cancelling 3 as $(3, 4) = 1$, we get $x \equiv 3 \pmod 4$

$\therefore$ $x_2 = 3$ is a solution of (3)

Finally we consider the congruence $b_3 x \equiv 1 \pmod{m_3}$ .....(4

i.e. $12x \equiv 1 \pmod 5$

We have $10x \equiv 0 \pmod 5$

Subtracting above two, $2x \equiv 1 \pmod 5$

Also, $0 \equiv 5 \pmod 5$

Adding above two, $2x \equiv 6 \pmod 5$

Cancelling 2 as $(2, 5) = 1$, we get $x \equiv 3 \pmod 5$

$\therefore$ $x_3 = 3$ is a solution of (4).

By Chinese Remainder Theorem, we know that

$x_0 = b_1 a_1 x_1 + b_2 a_2 x_2 + b_3 a_3 x_3$ is a common solution of congruences in (1).

i.e. $x_0 = 20.1.2 + 15.2.3. + 12.3.3 = 40 + 90 + 108 = 238$

The least positive solution is the remainder obtained on dividing x_0 (= 238) by m (= 60

The remainder obtained is 58, therefore $x = 58$ is the least positive common solution of the given congruences.

Remark : If all the solutions are asked in the above problem then they are given by

$$x = 58 + mk$$

i.e. $x = 58 + 60\,k$ where k is any integer

Remark : Example 1 can also be put in another form as follows:
Find all integers that give the remainder 1 , 2 , 3 when divided by 3 , 4 , 5 respectively.

Exercise 4.3

1. Find the least positive common solution of the linear congruences $x \equiv 2 (\text{mod } 3)$, $x \equiv 3 (\text{mod } 5)$, $x \equiv 5 (\text{mod } 2)$

2. Solve the congruences $x \equiv 1 \pmod 4$, $x \equiv 0 \pmod 3$, $x \equiv 5 \pmod 7$ simultaneously.

3. Find the least positive integer (except $x = 1$) which satisfies the congruences $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 5$ and $x \equiv 1 \pmod 7$ simultaneously.

4. Find all integers that give the remainder 2, 6, 5 when divided by 5, 7, 11 respectively. [K.U. 2010 (2nd Sem.)]

5. Solve the congruences $2x \equiv 3 (\text{mod } 5)$, $4x \equiv 2 (\text{mod } 6)$ and $3x \equiv 2 (\text{mod } 7)$ simultaneously.

6. Find the least positive integer x such that
$x \equiv 5 (\text{mod } 7)$; $x \equiv 7 (\text{mod } 11)$; $x \equiv 3 (\text{mod } 13)$. [K.U. 2011]

Answers

1. 23 **2.** $x = 33 + 84\,k$ **3.** $x = 106$

4. $x = 27 + 385k$ **5.** $x = 59 + 105\,k$ **6.** $887 \pmod{1001}$