Chapter One

PROPERTIES OF INTEGERS

Important Points from the Chapter

1. **Divisibility** An integer a is said to be divisible by an integer b ($\neq 0$), if there exists an integer q such that $a = bq$. It is denoted by $b \mid a$. In other words, we can say that 'a' is multiple of b.
   - **Note** If b divides a, then $-b$ also divides a, because $a = bq \Rightarrow a = (-b)(-q)$.
2. **Some Important Properties of Divisibility** For integers a, b, c and d, we have
   (i) $a \mid 0$, $1 \mid a$ and $a \mid a$
   (ii) $a \mid b$ and $c \mid d \Rightarrow ac \mid bd$
   (iii) $a \mid b$ and $b \mid c \Rightarrow a \mid c$ [transitivity]
   (iv) $a \mid b$ and $b \mid a \Rightarrow a = \pm b$
   (v) $a \mid b$ and $a \mid c \Rightarrow a \mid (bx + cy)$, for all integers x, y.
3. **Division Algorithm** For given integers a and $b > 0$, there exist unique integers q and r such that
   $$a = bq + r,\ 0 \leq r < b$$
   The integers q and r are called the **quotient** and the remainder respectively. **(2016, 11, 07)**
4. **Greatest Common Divisor** (G.C.D.) Let 'a' and 'b' be any two integers in which at least one is non-zero. Then, the greatest common divisor of a and b denoted by gcd (a, b) or (a, b) is the positive integer 'd' such that
   (i) $d \mid a$ and $d \mid b$
   (ii) If $c \mid a$ and $c \mid b$, then $c \mid d$.
   e.g. gcd $(15, 25) = 5$ **(2014, 06)**
   - **Note** gcd $(a, b) = a$, if $a \mid b$.
5. **Euclid's Algorithm** The gcd of two integers 'a' and 'b' can be determined by a process known as Euclid's algorithm and which is defined below.
   Let a and b be two positive integers and $a > b$. Then, there exist integers q_1 and r_1 such that
   $$a = bq_1 + r_1, 0 \leq r_1 < b$$ [by division algorithm] ...(i)
   Again, there exist integers q_2 and r_2, such that
   $$b = r_1 q_2 + r_2, 0 \leq r_2 < r_1$$ ...(ii)

Continuing this process, we get

$$r_1 = r_2 q_3 + r_3, 0 \le r_3 < r_2 \quad \ldots(iii)$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n, r_n = 0 \quad \ldots(iv)$$

where, $q_n \ge 2$.

Thus, $a > b > r_1 > r_2 > \ldots$

Hence, these numbers form a decreasing sequence of non-negative integers. It follows that $r_n = 0$ for some integer n. This process ends at this stage. The set of equations from Eqs. (i) to (iv) is called Euclid's Algorithm for gcd (a, b). The gcd of 'a' and 'b' will be r_{n-1}. **(2012, 06)**

■ **Note**

(i) Let a and b be positive integers such that $a > b$ and $r_n = 0$ in Euclid's algorithm. Then, r_{n-1} is the gcd of a and b.

(ii) If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

(iii) If a and b are integers, p is a prime such that $p \mid ab$ and $p \nmid a$, then $p \mid b$.

6. **Prime Number** A positive integers p other than 1 is said to be prime number, if its only positive divisors are 1 and p. **(2012)**

7. **Relatively Prime** Two integers, not both zero, are said to be relatively prime (coprime), if $(a, b) = 1$.

■ **Note** Two integers a and b not both zero are relatively prime, if there exist integers x and y such that $ax + by = 1$.

8. **Fundamental Theorem of Arithmatic** Every positive integer $n > 1$ can be expressed as the product of prime factors uniquely. **(2015, 05, 02)**

9. **Congruence Modulo m** Let m be a fixed positive integer. Then, an integer a is said to be congruent to another integer b modulo m, if $m \mid (a - b)$ and it is denoted by $a \equiv b \pmod{m}$. **(2003)**

■ **Note** Above expression is called the **Congruence**, m is called the **modulo** of the congruence and b is called **residue** of a (mod m).

10. **Linear Congruence** Let $a, b \in Z$ and n be a fixed positive integer. If x is an unknown integer, then the relation $ax \equiv b \pmod{n}$ is called a linear congruence.

By a solution of this linear congruence, we mean that there exists an integer x_1 such that $ax_1 \equiv b \pmod{n}$, i.e. $n \mid ax_1 - b$.

11. **Properties of Congruence** Let $m > 0$ be fixed and a, b, c and d are integers, then the following properties hold:

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

(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 $a \equiv c \pmod{m}$.

(iv) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $(a + c) \equiv (b + d) \pmod{m}$ and $ac \equiv bd \pmod{m}$.

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

(vi) If $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$ for all $k \ge 1$.

(vii) If $a^k \equiv b^k \pmod{m}$ for $k \ge 2$, then $a \equiv b \pmod{m}$ may not be true.

Residue Classes The relation '$\equiv$' of congruence modulo a non-zero positive integer n is an equivalence relation on the set Z of all integers. This equivalence relation partitions the set of integers Z into mutually disjoint equivalence classes. Each equivalence class is called a residue class defined as the set of integer which is such that each element of it when divided by n leaves the same remainder. **(2012)**

Fermat's Theorem If p is prime and $(a, p) = 1$, then $(a^{p-1} - 1)$ is divisible by p, i.e. $a^{p-1} \equiv 1 \pmod{p}$. **(2015, 11, 08)**

Wilson's Theorem If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Note If $(m-1)! + 1$ is divisible by m, then m is a prime.

Very Short Answer Questions

Q 1. If $m \in Z$ and n is a positive integer, then prove that $m \equiv r \pmod{n}$, where r is the remainder, when m is divided by n. **(2001)**

Sol. Let $m \in Z$ and $n > 0$, then by division algorithm, there exist two unique integers q and r such that

$$m = nq + r, 0 \le r < n$$

$$\Rightarrow \quad m - r = nq \Rightarrow m \equiv r \pmod{n}$$ **Hence proved.**

Q 2. If $(a+m) \equiv (b+m) \pmod{n}$, then prove that $a \equiv b \pmod{n}$.

Sol. Given that, $a + m \equiv b + m \pmod{n}$

$$\Rightarrow \quad n \mid [(a+m) - (b+m)]$$

$$\Rightarrow \quad n \mid (a-b)$$

$$\therefore \quad a \equiv b \pmod{n}$$ **Hence proved.**

Q 3. If p is a prime integer such that $p \mid m_1 m_2$, where $m_1, m_2 \in Z$, then prove that either $p \mid m_1$ or $p \mid m_2$. **(2005)**

Sol. Let us assume that p is not a factor of m_1. Therefore, $(p, m_1) = 1$.
By Euclidean algorithm, there exist two integers x and y such that

$$px + m_1 y = 1$$

$$\Rightarrow \quad m_2 = pm_2 x + m_1 m_2 y \quad \ldots(i)$$

Now, we have $p \mid m_1 m_2 \Rightarrow m_1 m_2 = pq$, for some $q \in Z$ $\ldots(ii)$

Using Eq. (ii) in Eq. (i), we get

$$m_2 = pm_2 x + pq\, y$$

$$\Rightarrow \quad m_2 = p(m_2 x + qy) \Rightarrow p \mid m_2$$

Similarly, we can show that, if p is not a factor of m_2, then $p \mid m_1$.

Hence proved.

Q 4. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then prove that $ac \equiv bd \pmod{n}$. **(2009, 03)**

Sol. We have, $a \equiv b \pmod{n} \Rightarrow n \mid (a-b)$

$\Rightarrow$ $(a-b) = nq_1 \Rightarrow a = b + nq_1$ ...(i)

and $c \equiv d \pmod{n} \Rightarrow n \mid (c-d)$

$\Rightarrow$ $(c-d) = nq_2 \Rightarrow c = d + nq_2$ ...(ii)

We have, $ac = (b + nq_1)(d + nq_2)$

$\Rightarrow$ $ac = bd + n(q_1 d + bq_2 + nq_1 q_2)$

$\Rightarrow$ $ac = bd + nq$, where $q = q_1 d + bq_2 + nq_1 q_2$

$\Rightarrow$ $ac - bd = nq \Rightarrow n \mid (ac - bd)$

$\therefore$ $ac \equiv bd \pmod{n}$ **Hence proved.**

Q 5. If $a^2 \equiv 1 \pmod{p}$, where p is a prime, then prove that $a \equiv 1 \pmod{p}$ or $a \equiv (p-1) \pmod{p}$. **(2009, 03)**

Sol. Given that, $a^2 \equiv 1 \pmod{p} \Rightarrow a^2 - 1 \equiv 0 \pmod{p}$

$\Rightarrow$ $p \mid (a^2 - 1) \Rightarrow p \mid (a-1)(a+1)$

$\Rightarrow$ $p \mid (a-1)$ or $p \mid (a+1)$

$\Rightarrow$ $a \equiv 1 \pmod{p}$ or $a \equiv (-1) \pmod{p}$

$\Rightarrow$ $a \equiv 1 \pmod{p} \Rightarrow a \equiv (p-1) \pmod{p}$ **Hence proved.**

Q 6. Define the relation of the 'congruence modulo n' of a positive integer. If $ma \equiv mb \pmod{n}$ and $(m, n) = 1$, then prove that $a \equiv b \pmod{n}$. **(2003)**

Sol. **Part I Congruence Modulo n** Let m be a fixed integer. Then, an integer a is said to be congruent to another integer b modulo m, if $m \mid (a-b)$ and it is denoted by $a \equiv b \pmod{m}$.

- **Note** Above expression is called the **congruence**, m is called the **modulo** of the congruence and b is called **residue** of $a \pmod{m}$.

Part II Given that, $ma \equiv mb \pmod{n}$

$\Rightarrow$ $n \mid (ma - mb) \Rightarrow n \mid m(a-b)$

$\Rightarrow$ either $n \mid m$ or $n \mid (a-b)$

$\Rightarrow$ $n \mid (a-b)$ $[\because (m, n) = 1]$

$\therefore$ $a \equiv b \pmod{n}$ **Hence proved.**

Q 7. Show that 3 is reciprocal of 2 modulo 5. **(2018)**

Sol. 3 is the reciprocal of 2 modulo 5, because

$$3 \cdot 2 \pmod{5} = 6 \pmod{5} = 1 \pmod{5}$$

Q 8. If $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, then prove that $ac \equiv bd \pmod{m}$. **(2016)**

Sol. We have, $a \equiv b \pmod{m} \Rightarrow m \mid (a-b)$ ...(i)

and $c \equiv d \pmod{m} \Rightarrow m \mid (c-d)$ ...(ii)

From Eqs. (i) and (ii), we have

$$(a-b) = mq_1 \text{ and } (c-d) = mq_2$$

$$a = b + mq_1 \text{ and } c = d + mq_2$$

Now, $ac = bd + m(q_1 d + bq_2 + mq_1 q_2) = bd + mq$

where, $q = q_1 d + bq_2 + mq_1 q_2$

$m \mid (ac - bd)$

$ac \equiv bd \pmod{m}$ **Hence proved.**

Q 9. If x_1 is a solution of the congruence equation $ax \equiv b \pmod{m}$ and $x_2 \equiv x_1 \pmod{m}$, then prove that x_2 is also a solution of the congruence equation $ax \equiv b \pmod{m}$.

(2011, 03, 1993)

Sol. We have, x_1 is the solution of $ax \equiv b \pmod{m}$ ...(i)

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

Now, we have $x_2 \equiv x_1 \pmod{m}$

$\therefore$ $ax_2 \equiv ax_1 \pmod{m}$ ...(iii)

From Eqs. (ii) and (iii), we get

$ax_2 = b \pmod{m}$

Since, the relation of congruence modulo m is transitive, hence x_2 is a solution of Eq. (i). **Hence proved.**

Q 10. How many incongruent solutions modulo 21 does the congruence equation $35x \equiv 14 \pmod{21}$ have? **(2017)**

Sol. Given that, $35x \equiv 14 \pmod{21}$

On comparing with $ax \equiv b \pmod{m}$, we have

$a = 35, \quad b = 14$ and $m = 21$

Here, gcd $(35, 21) = 7$ and $7 \mid 14$, so the given equation has 7 incongruence solutions.

Short Answer Questions

Q 1. Prove that the relation of congruence modulo n is an equivalence relation on the set of integers. **(2006)**

Or Prove that the relation of congruence modulo a positive integer m is an equivalence relation on Z. **(2015)**

Sol.

(i) **Reflexivity** Let $x \in Z$. Then, we have

$n \mid (x - x) \Rightarrow x \equiv x \pmod{n}$

Therefore, 'Congruence modulo n' on Z is reflexive.

(ii) **Symmetry** Let $a \equiv b \pmod{n}$, where $a, b \in Z$

Since, $a \equiv b \pmod{n} \Rightarrow n \mid (a - b)$

$\Rightarrow$ $a - b = \lambda n, \lambda \in Z$

$\Rightarrow$ $b-a=(-\lambda)n, -\lambda \in Z$

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

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

$\therefore$ $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

Therefore, 'congruence modulo n' on Z is symmetric.

(iii) **Transitivity** Let $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, where $a, b, c, \in Z$

Since, $a \equiv b \pmod{n} \Rightarrow n \mid (a-b)$ ...(i)

and $b \equiv c \pmod{n} \Rightarrow n \mid (b-c)$ ...(ii)

From Eqs. (i) and (ii), we have

$$n \mid [(a-b)+(b-c)] \Rightarrow n \mid (a-c) \Rightarrow a \equiv c \pmod{n}$$

Therefore, 'congruence modulo n' on Z is transitive.

Hence, the relation 'congruence modulo n' on Z is an equivalence relation. **Hence proved.**

Q 2. If p is a positive prime integer, then prove that

$$(p-1)!+1 \equiv 0 \pmod{p}.$$ **(2006, 04, 01)**

Or **If p is a prime number, then prove that**

$$(p-1)! \equiv (-1) \pmod{p}.$$ **(2017, 12, 09, 06, 04, 1996, 93, 92)**

Or **State and prove Wilson's theorem.**

Sol. **Statement** If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof Consider a set $S = \{1, 2, 3, \ldots, (p-1)\}$ of $(p-1)$ integers.

If a is any element of S, then multiplying each element of S by a, we get integers $a, 2a, 3a, \ldots, (p-1)a$.

Since, $(a, p) = 1$, therefore there exists one integer $x\,(0 < x < p)$ in S such that $ax \equiv 1 \pmod{p}$, i.e. a and x are reciprocals modulo p.

Assume $a = x$.

Therefore, $a^2 \equiv 1 \pmod{p}$, i.e. $p \mid (a-1)(a+1)$

i.e. either $p \mid a-1$ or $p \mid a+1$

If $p \mid a-1$, then $a-1=0$.

Since, p is prime and $a-1 < p$. Therefore, $a = 1$, i.e. 1 is reciprocal of 1 modulo p.

If $p \mid a+1$, then either $a+1=0$, i.e. $a=-1$, not possible or $p = a+1$, i.e. $a = p-1$.

This shows that $(p-1)$ is reciprocal of itself modulo p.

Remaining elements of S are 2, 3, 4,..., $p-2$ and the number of elements is $p-3$, which is even.

Hence, these elements can be classified into $\left(\frac{p-3}{2}\right)$ pairs of distinct reciprocals modulo p. Since, product of each is congruent to 1 modulo p and so on multiplication of such pairs, we get

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

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

$(p-1)! \equiv (p-1) \pmod{p}$

$[(p-1)! + 1] \equiv p \pmod{p} \equiv 0 \pmod{p}$

$[(p-1)! + 1] \equiv 0 \pmod{p}$ **Hence proved.**

Q 3. Prove that the number of prime numbers are infinite. **(2013, 1994)**

Sol. Let if possible, there are only finite number of primes $p_1, p_2, \ldots, p_r$ in ascending order.

Let $p = p_1 p_2 \ldots p_r + 1$. Then, clearly $p > p_r$. If p is a prime, then it shows that there exists a prime, greater than p_r.

If p is a composite number, then it is not divisible by any primes $p_1, p_2, \ldots, p_r$ as such a division leaves 1 as the remainder.

This shows that if p is composite, it must be divisible by a prime greater than p_r. Thus, in either case there exists a prime greater than p_r. But this contradicts our assumption that there are only a finite number of primes.

Hence, there are infinitely many primes.

Q 4. Prove that $a \equiv b \pmod{m}$ iff a and b leave the same remainder, when divided by m. **(2014, 09, 04)**

Or **Prove that two integers a and b leave the same remainder when divided by a positive integer m if and only if $a \equiv b \pmod{m}$.** **(2012)**

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

Again, let r_1 and r_2 be the remainders of a and b respectively w.r.t. m,

i.e. $a = mq_1 + r_1, 0 \le r_1 < m$

and $b = mq_2 + r_2, 0 \le r_2 < m$ ...(i)

We have to prove that $r_1 = r_2$

Since, $a \equiv b \pmod{m}$, we have

$(mq_1 + r_1) \equiv (mq_2 + r_2) \pmod{m}$

$\Rightarrow \quad m \mid (mq_1 + r_1) - (mq_2 + r_2)$

$\Rightarrow \quad m \mid m(q_1 - q_2) + (r_1 - r_2)$

$\Rightarrow \quad m \mid (r_1 - r_2)$

$\Rightarrow \quad r_1 - r_2 = 0$

[$\because r_1$ and r_2 are positive integers less than m]

which gives $r_1 = r_2$

Conversely Let $r_1 = r_2$.

Then, Eq. (i) gives

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

$\Rightarrow \quad a \equiv b \pmod{m}$ **Hence proved.**

Q 5. Define a prime number. Prove that, if p is a positive prime, then $[(p-1)!+1] \equiv 0 \pmod{p}$. **(2012)**

Sol. **Part I Prime Number** A positive integers p other than 1 is said to be prime number, if its only positive divisors are 1 and p.

Part II See the solution of Q. 2.

Q 6. State and prove Fermat's theorem. **(2008, 05, 2000, 1998, 95, 93, 91)**

Or **If p is a prime and a is an integer not divisible by p then prove that $a^{p-1} \equiv 1 \pmod{p}$.** **(2015, 11)**

Or **If p is a prime and $(a, p) = 1$, then prove that $a^{p-1} - 1$ is divisible by p, i.e. $a^{p-1} \equiv 1 \pmod{p}$.**

Sol. **Statement** If p is prime and $(a, p) = 1$, then $(a^{p-1} - 1)$ is divisible by p, i.e. $a^{p-1} \equiv 1 \pmod{p}$.

Proof We have, $(x_1 + x_2)^p = x_1^p + {}^pC_1 x_1^{p-1} x_2 + {}^pC_2 x_1^{p-2} x_2^2 + \ldots + {}^pC_{p-1} x_1 x_2^{p-1} + x_2^p$

$= x_1^p + x_2^p +$ term divisible by p

$\equiv x_1^p + x_2^p \pmod{p}$

Similarly, we can show that

$$(x_1 + x_2 + \ldots + x_a)^p \equiv (x_1^p + x_2^p + \ldots x_a^p) \pmod{p} \quad \ldots(i)$$

On putting $x_1 = x_2 = \ldots = x_a = 1$ in Eq. (i), we get

$$a^p \equiv a \pmod{p} \quad \ldots(ii)$$

But $(a, p) = 1$. Therefore, we can cancel the common factor a in Eq. (ii).

Thus, we have $a^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow$ $a^{p-1} - 1 \equiv 0 \pmod{p}$

Hence, $(a^{p-1} - 1)$ is divisible by p. **Hence proved.**

Q 7. Define gcd of a and b, not both zero. If r is the remainder in the division of a by b, prove that $(a, b) = (b, r)$. **(2014)**

Sol. **Part I Greatest Common Divisor** (G.C.D.) Let a and b be any two integers in which at least one is non-zero. Then, the greatest common divisor of 'a' and 'b' denoted by gcd (a, b) or (a, b) is the positive integer 'd' such that

(i) $d \mid a$ and $d \mid b$

(ii) If $c \mid a$ and $c \mid b$, then $c \mid d$.

e.g. gcd $(15, 25) = 5$

Part II Do same as Q 7 of long Answer Question

Q 8. Find gcd of 143 and 481 and express it as $143a + 481b$. Also find the values of a and b. (2018)

Sol. We have, $481 = 143 \cdot 3 + 52$

$$143 = 52 \cdot 2 + 39$$
$$52 = 39 \cdot 1 + 13$$
$$39 = 13 \cdot 3 + 0$$

Therefore, gcd $(143, 481) = 13$

Now, $13 = 52 - 39 \cdot 1$

$$= 52 - [143 - 52 \cdot 2]$$
$$= 52 \cdot 3 - 143$$
$$= 3 \cdot [481 - 143 \cdot 3] - 143$$
$$= 3 \cdot 481 - 9 \cdot 143 - 143$$
$$= 3 \cdot 481 - 10 \cdot 143$$
$$= -10 \cdot 143 + 3 \cdot 481$$

Here, $a = -10$ and $b = 3$

Thus, gcd 13 has been expressed as linear combination of 143 and 481.

Q 9. Prove that the congruence $235x \equiv 54 \pmod 7$ possesses only one incongruent solution.

Sol. We have, $(235, 7) = 1$ divides 54.

Therefore, the congruence has only one incongruent solution.

Now, $235x \equiv 54 \pmod 7$ ...(i)

We know that $231x \equiv 0 \pmod 7$ ...(ii)

On subtracting Eq. (i) from Eq. (ii), we get

$$4x \equiv 54 \pmod 7$$

Also, we know that $54 \equiv 5 \pmod 7$

Hence, $4x \equiv 5 \pmod 7$

Again, $12 \equiv 5 \pmod 7$

$\Rightarrow$ $5 \equiv 12 \pmod 7$

Therefore, $4x \equiv 12 \pmod 7$

$\Rightarrow$ $x \equiv 3 \pmod 7$, since $(4,7) = 1$

Hence, the congruence has only one incongruent solution, which is $\overline{3} = \{\ldots -11, -4, 3, 10, 17, 24, \ldots\}$.

Long Answer Questions

Q 1. **Prove that the congruence equation $ax \equiv b \pmod{m}$ has a solution iff d, the gcd of a and m, divides b. Further, prove that when d divides b, the equation $ax \equiv b \pmod{m}$ has exactly d incongruent solutions modulo m.** **(2013)**

Or **Prove that the congruence $ax = b \pmod{m}$ has a solution if and only if the gcd of a and m, i.e. (a, m) divides b.** **(2010)**

Or **Prove that the linear congruence equation $ax \equiv b \pmod{m}$ has a solution iff d, the gcd of a and m, divides b.** **(2016)**

Or **Find the necessary and sufficient condition for the existence of solution of the linear congruence equation $ax \equiv b \pmod{m}$.** **(2007)**

Or **If $d = (a, m)$ divides b, then prove that the congruence $ax = b \pmod{m}$ has exactly d incongruent solutions $\pmod{m}$.** **(2010)**

Sol. Let x_1 be the solution of $ax \equiv b \pmod{n}$

Then, $ax_1 \equiv b \pmod{n}$, i.e. $n \mid ax_1 - b$

$\Rightarrow$ $ax_1 - b = kn$, i.e. $b = ax_1 - kn$ for some $k \in Z$

Now, $(a, n) = d$

$\Rightarrow$ $d \mid a$ and $d \mid n$

$\Rightarrow$ $d \mid ax_1$ and $d \mid kn$

$\Rightarrow$ $d \mid ax_1 - kn$

$\Rightarrow$ $d \mid b$

Conversely Suppose that $d \mid b$, then $b = b_1 d$ for some $b_1 \in Z$.

Now, $(a, n) = d$, so there exist integers p and q, such that

$$pa + qn = d$$

$\Rightarrow$ $pab_1 + qnb_1 = b_1 d = b$

$\Rightarrow$ $pab_1 - b = (-qb_1)n$

i.e. $n \mid a(pb_1) - b$

$\Rightarrow$ $a(pb_1) \equiv b \pmod{n}$

Hence, pb_1 is a solution of $ax \equiv b \pmod{n}$

Now, we will prove the second part of the theorem as follows

Let $d = (a, n)$, then $d \mid a$ and $d \mid n$

$a = a_1 \cdot d$, $n = n_1 d$ for some $a_1, n_1 \in Z$ and $(a_1, n_1) = 1$

Given that, $d \mid b$, i.e. $b = b_1 d$ for some $b_1 \in Z$

Let x_1 and x_0 be two solutions of the given linear congruence.

Then, $ax_1 \equiv b \pmod{n}$ and $ax_0 \equiv b \pmod{n}$

$$a_1 dx_1 \equiv b_1 d \pmod{n_1 d} \text{ and } a_1 dx_0 \equiv b_1 d \pmod{n_1 d}$$

$$a_1 x_1 \equiv b_1 \pmod{n_1} \text{ and } a_1 x_0 \equiv b_1 \pmod{n_1}$$

Therefore, $a_1 x_1 \equiv a_1 x_0 \pmod{n_1}$

$$x_1 \equiv x_0 \pmod{n_1} \qquad [\because (a_1, n_1) = 1]$$

$$x_1 = x_0 + mn_1 \text{ for some } m \in Z.$$

Hence, all the solutions of the given linear congruence belong to the residue class $x_0 \pmod{n_1}$, i.e. the set $(x_0 + mn_1)$ of integers.

Now, consider the set of d integers of residue class x_0 modulo n_1 as

$$S = \{x_0 + mn_1 ; m = 0, 1, 2, \ldots, d-1\}$$

$$= \{x_0, x_0 + n_1, x_0 + 2n_1, \ldots, x_0 + r_1 n_1, \ldots, x_0 + r_2 n_1, \ldots x_0 + (d-1)n_1\}$$

We will show that no two distinct elements of S are congruent modulo n.

If possible, let $x_0 + r_1 n_1 \equiv x_0 + r_2 n_1 \pmod{n}$

Then, $r_1 n_1 \equiv r_2 n_1 \pmod{n} \Rightarrow n \mid n_1 (r_1 - r_2)$

But $n = n_1 d$ and so $d \mid r_1 - r_2$

Since, $r_1 - r_2 < d$, therefore d cannot divide $r_1 - r_2$ unless $r_1 = r_2$.

Hence, $x_0 + r_1 n_1 \not\equiv x_0 + r_2 n_1 \pmod{n}$

Now, we will prove that any element $x_0 + mn_1$ where $m \geq d$ is congruent modulo n to some element of S.

When $m \geq d$, by division algorithm, we have $m = dq + r, 0 \leq r < d$.

Therefore, $x_0 + mn_1 = x_0 + (dq + r)n_1$

$$= x_0 + rn_1 + dqn_1 = x_0 + rn_1 + qn \qquad [\because n = n_1 d]$$

$$\Rightarrow \quad (x_0 + mn_1) - (x_0 + rn_1) = qn$$

$$\Rightarrow \quad n \mid (x_0 + mn_1) - (x_0 + r n_1)$$

$$\therefore \quad x_0 + mn_1 \equiv x_0 + rn_1 \pmod{n} \text{ and } x_0 + rn_1 \in S$$

Hence, the congruence $ax \equiv b \pmod{n}$ has exactly d incongruent solutions.

Q 2. Define residue classes of modulo n. If the modulo of the congruence is n, then prove that all the integers will be split up into n residue classes. Also, show that the n residue classes are mutually exclusive. **(2002)**

Sol. **Part I Residue Classes** The relation '$\equiv$' of congruence modulo a non-zero positive integer n is an equivalence relation on the set Z of all integers. This equivalence relation partitions the set of integers Z into mutually disjoint equivalence classes. Each equivalence class is called a residue class defined as the set of integer which is such that each element of it when divided by n leaves the same remainder.

Part II Let r be the remainder, when an integer a divided by n.

Then, $$[r] = \bar{r} = \{\ldots, r - 2n, r - n, r, r + n, r + 2n, \ldots\}$$

Every integer when divided by n has one of the n-remainders (residues), i.e. 0, 1, 2, ..., $(n-1)$.

Thus, the set Z of integers can be partitioned into n-mutually disjoint equivalence classes or residue classes as given below

$$[0] = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$$
$$[1] = \{\ldots, 1-2n, 1-n, 1, 1+n, 1+2n, \ldots\}$$
$$[2] = \{\ldots, 2-2n, 2-n, 2, 2+n, 2+2n, \ldots\}$$
$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$
$$[n-1] = \{\ldots, -n-1, -1, n-1, 2n-1, \ldots\}$$

Hence, the set of residue classes modulo n is denoted by Z_n,
i.e. $Z_n = \{[0], [1], [2], \ldots, [n-1]\}$.

Q 3. State and prove division algorithm for the division of an integer a by a non-zero integer b. **(2016, 07)**

Or **State and prove division algorithm.** **(2011)**

Or **If m is any integer and n is a positive integer, then prove that there exist two unique integers q and r such that $m = nq + r, 0 \le r < n$.** **(2002)**

Sol. **Statement** For the given integers a and $b > 0$, there exist unique integers q and r such that $a = bq + r$, $0 \le r < b$, where integers q and r are called the quotient and remainder, respectively.

Proof We consider the infinite sequence of multiples of 'b' given as

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

Then, clearly either 'a' must be equal to one of the multiples of b say bq in this sequence or it must lie between two consecutive multiples say bq and $b(q+1)$.

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

$$\Rightarrow \quad 0 \le a - bq < b$$

Let $a - bq = r$. Then, we have

$$a = bq + (a - bq) \Rightarrow a = bq + r, 0 \le r < b$$

Uniqueness Let us assume that the two different representations of a are

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

and

$$a = bq_2 + r_2, 0 \le r_2 < b \quad \ldots(ii)$$

for some integers q_1, q_2, r_1 and r_2.

From Eqs. (i) and (ii), we get

$$bq_1 + r_1 = bq_2 + r_2$$
$$\Rightarrow \quad bq_1 - bq_2 = r_2 - r_1$$
$$\Rightarrow \quad b(q_1 - q_2) = r_2 - r_1 \quad \ldots(iii)$$
$$\Rightarrow \quad r_2 - r_1 = b(q_1 - q_2)$$

which shows that b divides $(r_2 - r_1)$.

But this is possible only when $r_2 - r_1 = 0$, i.e. $r_1 = r_2$ because both r_1 and r_2 are positive integers less than b.

On putting $r_1 = r_2$ in Eq. (iii), we get

$$b(q_1 - q_2) = 0$$

$$\Rightarrow \quad q_1 - q_2 = 0 \qquad [\because b \neq 0]$$

$$\Rightarrow \quad q_1 = q_2$$

Hence, q and r must be unique. **Hence proved.**

Q 4. Define greatest common divisor. Prove that any two non-zero integers has a greatest common division. **(2012, 06)**

Or **Define greatest common divisor of two integers and prove that any two non-zero integers have a greatest common divisor.** **(2017)**

Sol. **Part I Greatest Common Divisor** Let a and b be any two integers in which at least one is non-zero. Then, the greatest common divisor of a and b denoted by gcd (a, b) or (a, b) is the positive integer 'd' such that

(i) $d \mid a$ and $d \mid b$

(ii) If $c \mid a$ and $c \mid b$, then $c \mid d$.

e.g. gcd $(15, 25) = 5$

Part II Obviously the gcd (a, b) is not affected by the signs of a and b. Therefore, we assume that both a and b are positive and $a \geq b$. By division algorithm, we have

$$a = bq_1 + r_1, 0 \leq r_1 < b \qquad \ldots(i)$$

If $r_1 = 0$, then $b \mid a$ and gcd $(a, b) = b$.

Thus, gcd (a, b) exists.

If $r_1 \neq 0$, then by division algorithm, we have

$$b = r_1 q_2 + r_2, 0 \leq r_2 < r_1 \qquad \ldots(ii)$$

If $r_2 = 0$, then $r_1 \mid b$ and therefore from Eq. (i), we get

$$a = (r_1 q_2) q_1 + r_1 = r_1 (q_2 q_1 + 1) \Rightarrow r_1 \mid a$$

Let $s \mid a, s \mid b \Rightarrow s \mid (a - bq_1) \Rightarrow s \mid r_1$

Therefore, gcd $(a, b) = r_1$. Thus, gcd (a, b) exists.

If $r_2 \neq 0$, we repeat the process. This process terminates in finite steps n. In this way, we will arrive at zero remainder after nth step. Thus, we have a sequence of integers r_i such that

$$0 \leq r_n < r_{n-1} \ldots < r_2 < r_1 < b,$$

where, $\quad r_{n-2} = r_{n-1} q_n + r_n, n \geq 3$ and $r_{n-1} = q_{n+1} r_n$

Thus, $\quad r_n \mid r_{n-1}, r_n \mid r_{n-2}, \ldots, r_n \mid b$ and $r_n \mid a$

Now, if s is a common divisor of a and b, then $s \mid a$ and $s \mid b \Rightarrow s \mid (a - bq)$

$\Rightarrow \quad s \mid r_1, s \mid r_2, \ldots, s \mid r_n$ [from Eq. (i)]

Therefore, gcd $(a, b) = r_n$.

Thus, gcd (a, b) exists. **Hence proved.**

Q 5. State and prove fundamental theorem of arithmetic. **(2005, 02)**

Or **Prove that every integer n, greater than 1, can be uniquely expressed as a product of primes.** **(2015)**

Or **Prove that every integer can be uniquely expressed as a finite product of primes. Also, explain about the exceptions.** **(2018)**

Sol. **Statement** Every integer $n > 1$ can be expressed as the product of prime factors uniquely.

Proof Let $n > 1$ be an integer. If n is prime, then the result is obvious. If n is a composite number, then there exists a prime p_1 such that $n = p_1 n_1$ for some integer n_1.

If n_1 is a prime, then n is expressed as the product of prime factors.

If n_1 is a composite number, then there exists a prime p_2 such that $n = p_1 n_1 = p_1 p_2 n_2$ for some integer n_2.

If n_2 is a prime, then n is expressed as the product of prime factors. If n_2 is a composite number, then we continue the process.

Since, $n > n_1 > n_2 > \ldots$, the process cannot continue infinitely. Therefore, after finite number of steps, we get

$$n = p_1 p_2 \ldots p_k$$

where, all p_i's are primes.

Uniqueness Suppose, if possible n can be represented as a product of primes in two ways as given below

$$n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s,\ r < s \qquad \ldots(i)$$

where p_i and q_i are primes in the increasing order, i.e.

$$p_1 \leq p_2 \leq p_3 \leq \ldots \leq p_r$$

and $$q_1 \leq q_2 \leq q_3 \leq \ldots \leq q_s$$

Since, $p_1 \mid q_1 q_2 \ldots q_s$, there exists some q_k such that $p_1 \mid q_k$.

But p_1 and q_k are both primes.

Therefore, $p_1 = q_k$.

We rearrange q_i's, such that $p_1 = q_1$.

Now, cancelling p_1 and q_1 in Eq. (i), we get

$$p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s$$

We continue the process till all p_i's are exhausted.

Also, $r < s$, we left with $1 = q_{r+1} \cdot q_{r+2} \ldots q_s$

But it is not possible as q_i's are primes.

Therefore, r cannot be less than s.

Similarly, we can show that s cannot be less than r.

Thus, $r = s$ and $p_i = q_i,\ \forall\ i$.

Hence, the representation is unique. **Hence proved.**

Q 6. If d is greatest common divisor of two non-zero integers m and n, then show that $d = am + bn$, for some $a, b \in Z$.

(2009, 04, 01)

Sol. Let m and n be the given non-zero integers.

Let us construct an infinite set A, such that

$$A = \{xm + yn : \forall x, y \in Z\}.$$

Let B denotes a subset of A, which contains all the positive integers in A, namely

$$B = \{xm + yn > 0 : \forall\, x, y \in Z\} \subseteq A$$

By well ordering principle, suppose d is the least element of B.

Then, $d = am + bn$, where $x = a$ and $y = b \in Z$.

It is obvious that d is a positive integer as it belongs to B.

We claim that $d|m$ and $d|n$, i.e. d is a common divisor of m and n.

Since, $m \in Z$ and $d > 0$, then by division algorithm, there exist two unique integers q and r such that

$$m = qd + r, 0 \le r < d \qquad \ldots(i)$$

$$\Rightarrow \quad r = m - q(am + bn) \qquad [\because d = am + bn]$$

$$\Rightarrow \quad r = (1 - aq)m + n(-bq)$$

Thus, r is of the type $(mx + ny)$. Also, if $0 < r < d$, then $r \in B$ and hence arises a contradiction of the fact that d is the least element of B.

Hence, $0 < r < d$ is not true, therefore $r = 0$.

On putting $r = 0$ in Eq. (i), we have $m = qd$ implies that $d|m$.

Similarly, by taking $n \in Z$ and $d > 0$, we can prove that $d|n$.

Hence our claim is true, i.e. d is a common divisor of m and n.

Again, we claim that if $c \mid m$ and $c \mid n$ then $c \mid d$

Now, $c \mid m \Rightarrow c \mid am$ and $c \mid n \Rightarrow c \mid bn$

$\therefore$ $c \mid (am + bn) \Rightarrow c \mid d$

Thus, we have prove that any other common divisor of m and n divides d, hence this claim is true.

Combining above claims, we can say that d is the greatest common divisor of m and n or $d = (m, n)$. **Hence proved.**

Q 7. If m, n, q_1 and r_1 are positive integers such that $m = nq_1 + r_1$, where $0 < r_1 < n$, then prove that $(m, n) = (n, r_1)$. **(2008)**

Or **Let a and b be two positive integers such that $a = bq + r$, where $q, r \in Z$ and $0 < r < b$. Prove that $(a, b) = (b, r)$.**

(2010)

Sol. If $r_1 = 0$, then $n \mid m$ and $(m, n) = n$, whereas $(n, 0) = n$.

Therefore, $n = (m, n) = (n, r_1)$

If $r_1 \neq 0$, let $d = (m, n)$ i.e. $d \mid m$ and $d \mid n$.

Then, $d \mid (m - nq_1)$ or $d \mid r_1$

Hence, 'd' is common divisor of n and r_1.

Let $d' = (n, r_1)$, then $d \mid d'$.

Since, $d' \mid n$ and $d' \mid r_1$ and so $d' \mid (nq_1 + r_1)$, i.e. $d' \mid m$

Therefore, d' is a common divisor of m and n.

Since, $d = (m, n)$ and so $d' \mid d$.

Since, $d \mid d'$ and $d' \mid d$, therefore $d = d'$

Hence, $(m, n) = (n, r_1)$

Now, we apply division alogrithm for integers n and r_1, we get

$$n = r_1 q_2 + r_2, 0 \leq r_2 < r_1$$

If $r_2 = 0$, then $(n, r_1) = r_1$

If $r_2 \neq 0$, then by similar process, we prove that $(n, r_1) = (r_1, r_2)$

Proceeding in this way, we get

$$m = nq_1 + r_1, 0 \leq r_1 < n \quad \text{...(i)}$$

$$n = r_1 q_2 + r_2, 0 \leq r_2 < r_1 \quad \text{...(ii)}$$

$$r_1 = r_2 q_3 + r_3, 0 \leq r_3 < r_2 \quad \text{...(iii)}$$

.....

.....

$$r_{n-2} = r_{n-1} q_n + r_n, 0 \leq r_n < r_{n-1} \quad \text{...(iv)}$$

Since, $b > r_1 > r_2 > \ldots$ and so this process must end after finite number of steps with remainder

$$r_{n-1} = 0 \text{ and } r_{n-1} = r_n q_{n+1}.$$

Thus, we have $(m, n) = (n, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n$

Therefore, $(m, n) = r_n$. **Hence proved.**