# Udai. Pratap. College, Varanasi

(Autonomous Institution)

NAAC Re-accredited B Grade

---

## e-content

1. Subject: **Mathematics**
2. Class: **B. Sc. I**
3. Year/ Semester: **Yearly**

1. Unit**: Three**
2. Topic**: Algebra**
3. Sub topic**: Integers**
4. Key words: **Divison algorithm,Euclidean algorithm, congurence modulo n**


**Name: Dr. Rajiv Kumar Singh**

**Department: Mathematics**

**Address: Dept. of Mathematics, U. P. College, Varanasi**

**Email: rksupc@gmail.com**

**Mobile No: 9451973531**

# Integers

Integers are denoted by Z and Z = {……, -3. -2. -1. 0. 1. 2. 3, ……}

Operation of addition, substraction and multiplication are binary operation on Z but division is not a binary operation on Z, e.g. 2 and 5 $\in Z$ to Z but $\frac{2}{5} \notin Z$.

## Divisors:

Let $m \in Z$ and n be a non-zero integer then n is defined to be a divisor of m iff there exists an integer p such that $m = np$.

P is also called a divisor of m.

When n is a divisor of m, we can write $n/m$, we can also say that m is an integral multiple of n.

- The relation divisibility in intezer is not an equivalence relation. It is reflexive , transitive but not symmetric

(i) Reflexive:

$$\text{Since} \quad m = m.1 \qquad \forall \quad m \in Z$$

$$\Rightarrow m/m \qquad \forall \quad m \in Z$$

(ii) Transitive:

If $m/n$ and $n/p \quad \Rightarrow \quad m/p$

$\Rightarrow$ m is divisor of p $\quad \forall \quad m, n.p \in Z$

Since $m/n$ i.e. m is a divisor of n $\Rightarrow \exists \quad q \in Z$ s.t. $\quad n = mp$

and $n/p$ i.e. n is a divisor of p $\Rightarrow \exists \quad r \in Z$ s.t. $\quad p = nr$

Now $\quad p = nr$

$= (mq).r$

$= m(q.r)$

i.e. $p = m.s$ where $s = qr \in Z$

i.e. m is divisor of p

i.e. $m/p$

divisibility is not symmetric i.e. if 3 is a divisor of 6 but 6 is not divisor of 2.

Prime and composite integers:

$p \in Z$ is said to be prime integer iff its only divisors are $\pm 1$ and $\pm p$ i.e. $\pm 2$, $\pm 3$, $\pm 5$. $\pm 7$, ….. etc. are prime integers.

$p \in Z$, is said to be composite integer iff it can be expressed as product of two or more prime integers e.g. $\pm 4$, $\pm 6$, $\pm 8$. $\pm 9$, ….. etc. are composite integers.

- 0 and $\pm 1$ are neither prime nor composite integers.

## Divison Algorithm:

If $p \in Z$ and n is a positive integer, there exists two integers q and r, such that

$$m = nq + r \qquad 0 \le r \prec n$$

- For $m = nq + r$, q and r are known as "quotient" and remainder respectively, when m is divided by n, in this process od divison, we arein search of a remainder, which is non-negative as well as less than n, such a remainder is always unique.

## Greatest Common Divisor :

The greatest common divisor (g.c.d.) of two integers m and n is such a positive integer d that

(1) It is common divisor of m and n,

(2) It is divisible by all other common divisors of m and n i.e. if $c \in Z$ is any common divisor of m and n, then c divides d.

If d is the g.c.d. of m and n then we write $d = (m, n)$

## Euclidean Algorithm:

Any two non-zero integers m and n have a greatest common divisor d, such that

$$d = am + bn \qquad\qquad a, b \in Z$$

**Properties:**

(1) $K(m,n) = (Km, Kn)$

(2) $(m,n) = d\,,\quad {}^{m}/_{b} \quad \Rightarrow \quad {}^{mn}/_{bd}$

(3) $(m,n) = d\,,\quad m = xd \quad , \quad n = yd \quad \Rightarrow \quad (x,y) = 1$

(4) $(m,n) = 1\,,\quad (p,n) = 1 \quad \Rightarrow \quad (mp,n) = 1$

(5) $(m,n) = 1\,,\quad {}^{n}/_{pm}\,, \quad \Rightarrow \quad {}^{n}/_{p}$

(6) $(m,n) = 1\,, \quad \Rightarrow \quad (m^k, n) = 1\,, \quad k \succ 0$

**Theorem:** If p is a prime integer such that ${}^{p}/_{(m_1.m_2)}$ then either ${}^{p}/_{m_1}$ or ${}^{p}/_{m_2}$.

**Proof:** Let p is not a factor of $m_1$ then p and $m_1$ are relatively prime

i.e. $(p, m_1) = 1$

by Eucledian algorithm, there exists two integers x and y such that

$$1 = px + m_1 y$$

or $$m_2 = pxm_2 + m_1 m_2 y \qquad (1)$$

Now ${}^{p}/_{(m_1.m_2)} \Rightarrow m_1 m_2 = p.q$ for some $q \in Z$

then by (1) $m_2 = pxm_2 + pqy$

$$m_2 = p\left(xm_2 + qy\right)$$

$$\Rightarrow \qquad {}^{p}\!/_{m_2}$$

Similarly we can show that if p is not a factor of $m_2$ then ${}^{p}\!/_{m_1}$.

Generalization of this result, we can show that if p is a prime integer and ${}^{p}\!/_{(m_1.m_2.m_3.....m_n)}$

then p divides at least one of $m_1.m_2.m_3.....m_n$.

- The set of all prime integers if infinite
- Every positive integer greater than one has at least one prime factor.

## Congurence modulo n:

Let $a, b \in Z$ and n be a positive integer, Then the relation

$$a \equiv b(\bmod n) \qquad \Leftrightarrow \qquad {}^{n}\!/_{(a-b)}$$

is called "a is congruent to b modulo n ".It is an equivalence relation.

$$\begin{aligned} a \equiv b(\bmod n) \qquad & \Leftrightarrow \quad {}^{n}\!/_{(a-b)} \\ & \Leftrightarrow \quad a-b=nk \qquad \forall \;\; k \in Z \\ & \Leftrightarrow \quad a=b+nk \end{aligned}$$

**Theorem:** Two integers a and b leave the same remainder, when divided by a positive integer n, iff $a \equiv b(\bmod n)$.

**Proof:** Let $a \in Z$ , $n \succ 0$ then by division algorithm there exists $q_1, r_1 \in Z$ ,

$$a = nq_1 + r_1 \qquad 0 \le r_1 \prec n \qquad (1)$$

Similarly for $b \in Z$ , $n \succ 0$ we have $q_2, r_2 \in Z$ as

$$a = nq_1 + r_1 \qquad 0 \le r_1 \prec n \qquad (2)$$

From (1) and (2), we get

$$a - b = n(q_1 - q_2) + (r_1 - r_2)$$

Where $r_1$ and $r_2$ are remainders when a and b are divided by n.

Now $r_1 = r_2 \quad \Leftrightarrow \quad a - b = n(q_1 - q_2)$

$$\Leftrightarrow \quad {}^{n}\!/\!_{(a-b)}$$

$$\Leftrightarrow \quad a \equiv b \pmod{n}$$

* Let $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ , then

(1) $a + c \equiv b + d \pmod{n}$

(2) $a - c \equiv b - d \pmod{n}$

(3) $ac \equiv bd \pmod{n}$

(4) $a^m \equiv b^m \pmod{n}$ , mis a positive integer.

(5) $am \equiv bm \pmod{n}$ . $m \in Z$

(6) $a + m \equiv b + m \pmod{n}$ , $m \in Z$

## Linear congruence and reciprocal:

Let $a, b \in Z$ and n be a positive integer, suppose x is some unknown quantity, then the relation $ax \equiv b(\bmod n)$ is called linear congruence modulo n and integral value of x lying between o and n , which satisfies it, is called an " Incongurent solution" of linear congruence.

Solution of $ax \equiv 1(\bmod n)$ is called " reciprocal of a modulo n". Thus reciprocal of an integer a modulo n exists iff $(a,n)=1$.

- If $(a,n)=d$, and $d/b$, then the linear congruence $ax \equiv b(\bmod n)$ has d incongruent solutions.
- If $x_1 \in Z$ is a solution of $ax \equiv b(\bmod n)$ and $x_2 \equiv x_1(\bmod n)$ then $x_2$ is also a solution of given linear congruence.
- The linear congruence $ax \equiv b(\bmod n)$ has a solution iff $(a,n)/b$, (a,n)=d.

## Fundamental theorem of arithmetic:

Every positive integer greater than one can be uniquely expressed as a finite product of positive primes.

Proof: Let m be a positive integer greater than 1.Since every positive integer gteater than 1 can be expressed as finite product of positive prime integers. So, let m be expressed as two ways as

$$m = p_1.p_2.p_3.........p_r \tag{1}$$

$$m = q_1.q_2.q_3.........q_s \tag{2}$$

where $p^{'s}$ and $q^{'s}$ are positive prime integers.

From (1) and (2), $p_1.p_2.p_3.........p_r = q_1.q_2.q_3.........q_s$ (3)

Now $p_1 / m \Rightarrow p_1 / q_1.q_2.q_3.........q_s$

$\Rightarrow$ $p_1$ is a factor of at least one $q's$ say $q_i$

$\Rightarrow p_1 / q_i$

$\Rightarrow p_i = q_i$ because a prime integer can not be a factor of another prime.

Then from (3) , $p_2.p_3.........p_r = q_1.q_2.q_3.....q_{i-1}.q_{i+1}....q_s$ repeating this method we can show that $p_i = q_j$ for $i \neq j$ . Similarly. $p_3.p_4.........$ are equal to some $q's$ .This process of cancellation will continue til one side reduces to 1,now $p's$ and $q's$ being integers the another side also must be equal to 1.Thus representation of m by (10 and (2) are same irrespective of the orders of $p's$ and $q's$ in which they have written.

## Questions :

(1) Find the greatest common divisor of 23 and 17 respectively and express it in the form of $23a + 17b$ .

(2) Show that $m \in Z$ and n be a positive integer, then $m \equiv r(\text{mod}\, n)$ where r is the remainder, when m is divided by n.

(3) If $ma \equiv mb(\text{mod}\, n)$ , $(m,n) = 1$ , then $a \equiv b(\text{mod}\, n)$

(4) Show that $a^2 \equiv 1(\text{mod}\, 8)$ , when a is an odd integers.

(5) If p is a positive prime integer and $a \in Z$ , show that $a^2 \equiv 1(\text{mod}\, p)$ implies either $a \equiv 1(\text{mod}\, p)$ or .

(6) Find the incongruent solution of

(i) $2x + 1 \equiv 2(\text{mod}\, 8)$

(ii) $x + 20 \equiv 14(\text{mod}\, 5)$

(iii) $6x \equiv 10 \pmod{16}$

(iv) $235x \equiv 54 \pmod{7}$

## References:-


1. Algebra & trigonometry by Pandey
2. Modern Algebra by A.R. Vashistha