2.1 THEORY OF NUMBER

2.1.1 Introduction.

The theory of numbers, an important branch of mathematics, is primarily concerned with the properties of the natural numbers. 1, 2, 3, 4, ..., also called the positive integers. However, the theory is not strictly confined to just the natural numbers or even to the set of all integers: $0, \pm 1, \pm 2, ...$ In fact, some theorems of number theory can easily be proved by applying the properties of real or complex numbers. Some important applications of number theory are in computer arithmetic that includes transmission, coding, manipulation of numerical data and also in cryptology– the study of secret messasges. The aim of the present chapter is to introduce the divisibility theory and properties, greatest common divisors (GCD) and some properties of GCD with applications and congruence relations with a few applications.

2.1.2 Well ordering principle

Every non–empty subset of naturals numbers has a smallest element. Thus, if S be a non–empty subset of natural numbers, then there exists $p \in S$ such that $p \leq q$ for all $q \in S$.

A set containing just one element has a smallest member, namely the element itself. Hence, the well– ordering principle is true for sets of size 1.

Now set us assume that the principle is true for sets of size n, i.e., any set of n natural numbers has a smallest number

Let us now consider a set S of $(n+1)$ numbers from which one element 'p' is removed. The remaning n numbers have a smallest element say q (by the induction hypothesis). The smaller of p and q is the smallest element of S.

Hence, by the principle of mathematical induction, it follows that any non–empty finite set of natural numbers has a smallest element.

2.1.3 Divisibility theory

Definition. An integer b is divisible by an integer $a\,(\neq 0)$, if there is an integer x such that $b = ax$, and we write $a \mid b$.

In case b is not divisible by a, we write $a \chi b$

Note. (i) when a divides b, a is called a divisor or factor at b and b is called a multiple of a

(ii) If a divides b then $-a$ also divides b because $b = ax \Rightarrow b = (-a)(-x)$

i.e., $a \mid b \Rightarrow -a \mid b$

Illustrations.

(i) 38 is divisible by 19 since $38 = 19 \times 2$

(ii) 11 is a divisor of 143 since $143 = 11 \times 13$

(iii) 0 is divisible by every integer because $0 = x \times 0$ for every value x.

2.1.4 Properties of divisibility

Some basic properties of divisibitily of integers are given in the following theorem:

Theorem–1 Let $a, b, c \in Z$, the set of integers. Then

(a) If $a \mid b$, then $a \mid b, n$, for any integer n

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

(c) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any integers x and y

(d) In $a \mid b$, $a > 0$, $b > 0$, then $a \leq b$

Proof.

(a) Since $a \mid b$, we have $b = ax$ for some integer n

$\therefore bn = anx = (nx)a$ where n, x are integers

This means that a divides bn

$$\therefore a \mid bn$$

(b) Since $a \mid b$ and $b \mid c$, we have

$b = pa$ and $c = qb$ where p, q are integers

$$\therefore c = qb = q(pa) = (pq)a$$

This means that a divides c

$$\therefore a \mid c$$

(c) Since $a \mid b$ and $a \mid c$, so we have

$b = pa$ and $c = qa$ where p, q are integers

Now $bx + cy$

$$= (pa)x + (qa)y$$

$$= (px + qy)a$$

$p \to q \cdot \sim q \to \sim p$
$q \to p \quad \sim p \to \sim q.$

This means that a divides $bx + cy$, as p, q, x and y are integers.

$$\therefore a \mid bx + cy$$

(d) Since $a \mid b$, we have

$b = pa$ for some integers p

But $a > 0, b > 0$

$$\therefore p > 0 \text{ i.e. } p \geq 1$$

Then $b = pa \Rightarrow b \geq a \ [\because p \geq 1]$

$$\therefore a \leq b.$$

Corollary. If $a \mid b$ and $a \mid c$, then

$$a \mid (b + c) \text{ and } a \mid (b - c)$$

proof follows from (c)

Note. To check if a given integer n is prime it is sufficient to see that it is not divisible by any prime less than or equal to its square root.

Illustration.

Let $n = 19$

$\therefore 4 < \sqrt{19} < 5$

Here 2 and 3 are the prime less than or equal to 4. But 19 is not divisible by 2 and 3

There 19 must be a prime.

Theorem 4 (The division algorithm)

Given any two integers a and b, with $b > 0$, there exist unique integers q and r such that $a = bq + r$, $0 \le r < b$

Proof. Consider the following infinite sequence of multiples of b:

$$\ldots. -2b, -b, 0, b, 2b, \ldots\ldots, qb, \ldots.$$

Then, obviously

$$a = qb \text{ or } qb < a < (q+1)b \text{ for some } q$$

In either case we have

$qb \le a < (q+1)b$ for some q

$$\therefore 0 \le a - qb < b \quad \ldots (1$$

Let us take $a - bq = r$

$\therefore$ From (1), we get

$\therefore 0 \le r < b$

$\therefore a = bq + r$, $0 \le r < b$

To prove the uniqueness of q and r, let us assume

$$a = bq_1 + r_1 \quad \ldots (2$$

where $0 \le r_1 < b$

i.e., $-b < r_1 \le 0$

and $a = bq_2 + r_2$ ... (3)

where $0 \le r_2 < b$

$\therefore$ (2) and (3) gives

$$bq_1 + r_1 = bq_2 + r_2$$

i.e. $(q_1 - q_2)b = r_2 - r_1$ ... (4)

Thus $r_2 - r_1$ is an integral multiple of b

But, since $-b < r_1 \le 0$ and $0 \le r_2 < b$, so we have

$$-b < r_2 - r_1 < b.$$ ... (5)

Hence the only possibility is that $r_2 - r_1$ is zero multiple of b

$$\therefore r_1 = r_2 \text{ and } q_1 = q_2$$

Thus q and r are uniqie.

Note. (1) When $b \nmid a$, r satisfies the stronger inequalities $0 < r < b$

(2) When b is any integer, the above result can be written as

$$a = bq + r,\ 0 \le r < |b|$$

(3) Here q and r are called quotient and remainder respectively

(4) bq is the largest multiple of b which does not exceed a

Illustration

(i) If $a = 57$, $b = 9$, then $57 = 6 \times 9 + 3, 0 < 3 < 9$

$$\therefore q = 6,\ r = 3$$

(ii) If $a = -57, b = 9$, then

$-57 = (-7) \times 9 + 6,\ 0 < 6 < 9$

$\therefore\ q = -7,\ r = 6$

(iii) If $a = 57, b = -9$, then

$57 = (-9)(-6) + 3,\ 0 < 3 < |-9|$

$\therefore\ q = -6,\ r = 3$

(iv) If $a = -57,\ b = -9$, then

$$-57 = (-9) \times 7 + 6,\ 0 < 6 < |-9|$$

$\therefore\ q = 7,\ r = 6.$

2.1.6 Greatest common divisor

Definition. The integer $d(\neq 0)$ is said to be the common divisor of a and b if $d|a$ and $d|b$ i.e., if d divides both a and b.

Since there is only a finite number of divisors of any non–zero integers, there is only a finite number of common divisors of a and b, except in the case $a = b = 0$. If at least one of a and b is not 0, the largest of all common divisors is called the **greatest common divison** of a and b and is denoted by $\gcd(a, b)$ or simply (a, b). Obviously $\gcd\ (a, b) \geq 1$.

If $\gcd(a, b) = 1$, then a and b are said to be **relatively prime** or **coprime** or each said to be prime to the other.

If $\gcd\ (a_1, a_2, \ldots . a_n) = 1$, then the integers $a_1, a_2, \ldots . a_n$ are said to be **pairwise relatively prime.**

Illustration.

(i) The divisors of 8 are $\pm 1, \pm 2, \pm 4, \pm 8$; the divisors of 36 are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 18, \pm 36$

Thus the common divisors of 8 and 36 are $\pm 1, \pm 2, \pm 4$

Hence the greatest common divison is 4.

$$\therefore\ gcd(8, 36) = 4$$

(ii) The divisors of 15 are $\pm 1, \pm 3, \pm 5, \pm 15$; the divisiors of 44 are $\pm 1, \pm 2, \pm 4, \pm 11$.

Hence gcd $(15, 44) = 1$.

$\therefore$ 15 and 44 are relatively prime

(iii) Consider the integers 8, 17, 35. Since gcd $(8, 17) = 1$, gcd $(8, 35) = 1$ and gcd $(17, 35) = 1$, so the integers 8, 17, 35 are pairwise relatively prime.

2.1.7 Euclidean algorithm for finding GCD

Statement : Let a and b $(a > b)$ be any two integers. If r_1 is the remainder when a is divided by b, r_2 is the remainder when b is divided by r_1, r_3 is the remainder where r_1 is divided by r_2 and so on. Thus if $r_{p+1} = 0$, then the last non–zero remainder r_p is the gcd(a, b).

Proof. Let $a = qb + r$, $0 \le r < b$

We now prove that $\gcd(a, b) = ged(b, r)$

For that, let $d_1 = \gcd(a, b)$ ... (1)

and $d_2 = \gcd(b, r)$ ... (2)

$\therefore$ From (2),

$d_2 \mid b$ and $d_2 \mid r$

$\therefore$ $d_2 \mid (qb + r)$ ie., $d_2 \mid a$

Thus d_2 is a common divisor of a and b. Since d_1 is gcd(a, b), we must have

$d_2 \le d_1$ ... (3)

Again from (1),

$$d_1 | a \text{ and } d_1 | b$$

$$\therefore d_1 | (a - qb) \text{ i.e., } d_1 | r$$

Thus d_1 is a common divisor of b and r. Since $d_2 = gcd(b, r)$, we must have

$$d_1 \leq d_2 \quad \ldots (4)$$

$\therefore$ From (3) and (4), we get

$$d_1 = d_2$$

i.e., $gcd(a, b) = gcd(b, r)$ where $a = qb + r$ ... (5)

Now, since r_1 is the remainder when a is divided by b, we have $a = q_1 b + r_1$, $0 \leq r < b$.

Similarly by the given data,

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

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

....

$$r_{p-1} = q_{p+1} r_p + r_{p+1}, \; 0 \leq r_{p+1} < r_p$$

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

$\therefore$ Using (5) we have

$$\gcd(a, b) = \gcd(b_1, r_1) = \gcd(r_1, r_2) = \ldots\ldots$$

$$= \gcd(r_{p-1}, r_p) = \gcd(r_p, 0) = r_p$$

Hince $\gcd(a, b) = r_p$ which is the last non-zero remainder.

Illustration. We now find gcd $(1120, 128)$

By division algorithm,

$1120 = 8 \times 128 + 96$

$128 = 1 \times 96 + 32$

$96 = 3 \times 32 + 0$.

Since the last non–zero remainder is 21, so

$$\gcd(1120, 128) = 21.$$

Theorem 5. Let a and b $(a > b)$ be any two integers. Then gcd (a, b) can be expressed as an integral linear combination of a and b.

i.e., gcd $(a, b) = ma + nb$, where m and n are integers.

Proof. Using the Euclid's algorithm, we have

$r_{p-2} = q_p r_{p-1} + r_p$, where $r_p = \gcd(a, b)$

$\therefore r_p = r_{p-2} + (-q_r) r_{p-1}$ ... (1)

$\therefore r_{p-1} = r_{p-3} + (-q_{p-1}) r_{p-2}$

$\therefore$ From (1),

$r_p = r_{p-2} + (-q_r)\{r_{p-3} + (-q_{p-1}) r_{r-2}\}$

$= r_{p-3} + (-q_r) + (1 + q_{p-1} q_p) r_{p-2}$

Then we substitute $r_{p-4} + (-q_{p-2}) r_{p-3}$ for r_{p-2} and continue the process Finally we will have

$r_p = gcd(a, b) = ma + nb$ for some integers m and n

Illustration. First we consider the steps used to find $gcd(1120, 128)$ as given below

$$1120 = 8 \times 128 + 96 \quad \ldots (1)$$

$$128 = 1 \times 96 + 32 \quad \ldots (2)$$

$\therefore$ From (2), we have

$$32 = 128 - 1 \times 96$$

$$= 128 - 1 \times (1120 - 8 \times 128), \text{ by (1)}$$

$$= 9 \times 128 - 1 \times 1120 \quad \ldots (3)$$

Thus $32 = ged(1120, 128) = (-1)1120 + 9 \times 128$

$$\therefore m = -1, \; n = 9$$

Note. (3) can be written as

$$gcd(1120, 128) = (9 + 1120) \times 128 - (1 + 128) \times 1120$$

$$= 1129 \times 128 - 129 \times 1120$$

$$= (-129)1120 + 1129 \times 128$$

$$\therefore m = -129, \; n = 1129$$

Thus m and n are not unique.

Hence the expression of $gcd(a, b)$ in the form $ma + nb$ is not unique.

Alternative definition of GCD

Let the prime decomposition of two integers a and b be

$$a = n_1^{a_1} \, n_2^{a_2} \, n_3^{a_3} \ldots . n_r^{a_r}$$

and

$$b = n_1^{b_1} \, n_2^{b_2} \, n_3^{b_3} \ldots . n_r^{a_r}$$

where each exponent is a non-negetive integer and all primes occuring in the prime decomposition of either a or b are included in both decomposition, with zero exponent if necessary. Then

$$\gcd(a,b) = n_1^{\min(a_1,b_1)} . n_2^{\min(a_2,b_2)} \ldots\ldots\ldots n_r^{\min(a_r,b_r)}$$

where $\min(a_i, b_i)$ means the minimum of two numbers a_i and b_i

Illustratiition.

We have

$$20 = 2^2 \cdot 5^1 \cdot 7^0$$

$$350 = 2^1 \cdot 5^2 \cdot 7^1$$

$$\therefore \gcd(20, 350) = 2^{\min(2,1)} \cdot 5^{\min(1,2)} \cdot 7^{\min(0,1)}$$

$$= 2^1 \cdot 5^1 \cdot 7^0$$

$$= 10$$

2.1.8 Some properties of GCD

A. If $c \mid ab$ and b, c are coprime , then $c \mid a$

Proof. Since b, c are coprime, so

$$\gcd(b, c) = 1 .$$

$\therefore$ By theorem 5, there exist integers m and n such that

$$mb + nc = gcd(b, c)$$

i.e. $mb + nc = 1$

i.e. $a(mb + nc) = a$

i.e. $m\,ab + n\,ac = a$ ... (1)

Now $c \mid ab \Rightarrow c \mid m\,ab$

Also $c \mid n\,ac$

$\therefore c \mid (m\,ab + n\,ac)$

$\therefore c \mid a$. by (1)

B. If a and b are coprime and a and c are coprime, then a and bc are coprime

Proof. Since a, b are coprime, so

$$gcd(a, b) = 1$$

$\therefore$ There exists integers m and n such that

$$ma + nb = 1 \quad \ldots (2)$$

Similarly, since a and c are prime, there exists integers x and y such that

$$xa + yc = 1 \quad \ldots (3)$$

$\therefore$ From (2) and (3), we get

$$(ma + nb)(xa + yc) = 1$$

i.e., $$(mxa + myc + nxb)a + (ny)bc = 1$$

which is of the form

$pa + q\,bc = 1$, where $p = mxa + myc + nxb$, $q = ny$ are integers

Hence $gcd(a, bc) = 1$

$\therefore$ a and bc are coprime

C. For any positive integer m,

$$gcd(ma, mb) = m\ gcd(a, b)$$

Proof. Let $d = gcd(a, b)$

By theorem 5, there exits integers x and y that

$$xa + yb = d$$

$$\therefore m(xa + yb) = md$$

i.e., $$x(ma) + y(mb) = md$$

$$\therefore gcd(ma, mb) = m\ gcd(a, b)$$

Note. When m is any integer, the result becomes

$$gcd(ma, mb) = |m| gcd(a, b)$$

D. If $d \mid a$ and $d \mid b$ and $d > 0$, then

$$gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d} gcd(a, b)$$

Proof. Let $gcd(a, b) = k$

$\therefore$ By theorem 5, there exists integers m and n such that

$$ma + nb = k$$

$$\therefore \frac{1}{d}(ma + nb) = \frac{k}{d}$$

$$\text{i.e. } m\left(\frac{a}{d}\right) + n\left(\frac{b}{d}\right) = \frac{1}{d}.k$$

Since $d \mid a$ and $d \mid b$, $\frac{a}{d}$ and $\frac{b}{d}$ are integers.

Hence $gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}.gcd(a, b)$

Note. If $gcd(a, b) = d$, then $gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

E. If $gcd(a, b) = 1$, then for any integer x,

$$gcd(ax, b) = gcd(x, b)$$

Proof. Since $gcd(a, b) = 1$, by theorem 5, there exists integers m, n such that

$$ma + nb = 1 \quad \ldots (1)$$

Let $gcd(ax, b) = d$.

Then there exists integers p, q such that

$$pax + qb = d \quad \ldots (2)$$

$\therefore$ From (1) and (2)

$$(ma+nb)(p\,ax+q\,b)=1\cdot d$$

i.e., $(mpa)^2x+(ma\,q+npax+nqb)b=d$

i.e., $rx+sb=d$ where $r=mpa^2, s=maq+npax+nqb$

are integers.

Hence $gcd(x,b)=d$

$\therefore gcd(ax,b)=gcd(x,b)$.

F. If $a_1, a_2, \ldots a_n$ are relatively prime b, then their product $a_1, a_2, \ldots a_n$ is also prime to b

Proof. Since a_1 is relatively prime to b, so

$$gcd(a_1,b)=1$$

$\therefore$ By property E,

$$gcd(a_1a_2,b)=gcd(a_2,b)$$

$$=1 \quad [\because a_2, b \text{ are relatively prime}]$$

Again by property E,

$$gcd(a_1a_2a_3,b)=gcd(a_3,b)$$

$$=1 \quad [\because a_3, b \text{ are relatively prime}]$$

Proceeding in this way, we get

$$gcd(a_1a_2a_3\ldots a_n,b)=1.$$

Thus $a_1\ a_2\ a_3\ldots a_n$ is prime to b.

2.1.9 Least common multiple.

Definition. Let a and b be positive integers. Then the smallest positive integer that is divisible by both a and b is called the least common multiple of a and b and is dinoted by $lcm(a, b)$ or $[a, b]$

Note. $lcm(a, b)$ is always positive even if either or both a and b are negetive.

Illustration.

$$lcm(8, 20) = lcm(-8, 20) = lcm(-8, -20) = 40$$

Alternative definition of *lcm*

Let the prime decomposition of two integers a and b be

$$a = n_1^{a_1} n_2^{a_2} \ldots\ldots n_p^{a_p}$$

and $$b = n_1^{b_1} n_2^{b_2} \ldots\ldots n_p^{a_p}$$

where each exponent is a non–negative integer and all primes occuring in the prime decomposition of either a or b are included in both decomposition, with zero exponent if necessary. Then

$$lcm(a, b) = n_1^{\max(a_1, b_1)} n_2^{\max(a_2, b_2)} \ldots\ldots n_p^{\max(a_p, b_p)}$$

where $\max(a_i, b_i)$ means the maximum of two number a_i and b_i

Illustration.

We have

$$8 = 2^3 \times 5^0$$

$$20 = 2^2 \times 5^1$$

$$\therefore lcm(8, 20) = 2^{\max(3, 2)} 5^{\max(0, 1)}$$

$$= 2^3 \cdot 5^1 = 40$$

Theorem. Let a and b be any two positive integers.

Then $gcd(a, b) \cdot lcm(a, b) = ab$

Proof. Let the prime decomposition of a and b be

$$a = n_1^{a_1} n_2^{a_2} n_3^{a_3} \ldots\ldots n_p^{a_p}$$

and $$b = n_1^{b_1} n_2^{b_2} n_3^{b_3} \ldots\ldots n_p^{a_p}$$

$$\therefore gcd(a, b) = n_1^{min(a_1, b_1)} n_2^{min(a_2, b_2)} \ldots\ldots n_p^{min(a_p, b_p)}$$

$$lcm(a, b) = n_1^{max(a_1, b_1)} n_2^{max(a_2, b_2)} \ldots\ldots n_p^{max(a_p, b_p)}$$

Note that if $\max(a_i, b_i)$ is a_i (or b_i), then $\min(a_i, b_i)$ is b_i (or, a_i), $i = 1, 2 \ldots\ldots p$

$$\therefore gcd(a, b) \times lcm(a, b)$$

$$= n_1^{\{\max(a_1, b_1) + \min(a_1, b_1)\}} \cdot n_2^{\{\max(a_2, b_2) + \min(a_2, b_2)\}}$$

$$\ldots\ldots n_p^{\{\max(a_p, b_p) + \min(a_p, b_p)\}}$$

$$= n_1^{a_1 + b_1} n_2^{a_2 + b_2} \ldots\ldots n_p^{a_p + b_p}$$

$$= \left(n_1^{a_1} n_2^{a_2} \ldots\ldots n_p^{a_p}\right) \cdot \left(n_1^{b_1} n_2^{b_2} \ldots\ldots n_p^{a_p}\right)$$

$$= ab \cdot$$

Illustration.

Since $lcm(8, 20) = 40$, so

$gcd(8, 20) \cdot lcm(8, 20) = 8 \times 20$ gives

$$ged(8, 20) = \frac{8 \times 20}{40} = 4 .$$

2.1.10 Diophantine Equations.

The general form of a linear Diophantive equation in two variables having integral coefficients is

$$ax + by = c \qquad \ldots \quad (1)$$

The solution of this equation is trivial unless neither a nor b is zero, so we can suppose $a \neq 0$, $b \neq 0$. Let $d = gcd(a, b)$. Then theorem 5 shows that there exist integers x_0 and y_0 such that

$$ax_0 + by_0 = d \qquad \ldots \quad (2)$$

Numarical values for x_0 and y_0 can be obtained conveniently by applying the Euclidean algorithm, art. 2.7 to the integers $|a|$ and $|b|$. Now if $d \mid c$, we get (x_0, y_0) as the particular integeral solution of (1). Then all integral solutions of (1) are given by

$$x = x_0 + \frac{b}{d}k, \quad y = y_0 - \frac{a}{d}k$$

where k is any integer.

But, if $d \nmid c$, then $ax + by = c$ clearly has no solutions in integers.

Illustration

(i) Consider the Diophantine equation $2x + 3y = 4$.

Here $gcd(2, 3) = 1$ and 4 is divisible by 1. So the equation $2x + 3y = 4$ has integral solution.

Now $\quad 1 = 2 \cdot (-1) + 3 \cdot 1$

$\therefore \quad 4 = 2 \cdot (-4) + 3 \cdot 4$

Thus one integral solution is $x_0 = -4$, $y_0 = 4$. Hence all integral solutions of the given equation are given by

$$x = -4 + \frac{3}{1}k, \quad y = 4 - \frac{2}{1}k \text{ for any integer } k$$

i.e., $x = -4 + 3k$, $y = 4 - 2k$ for any integer k.

(ii) Consider another Diophantine equation

$$14x + 21y = 5$$

Here $gcd(14, 21) = 7$ and 5 is not divisible by 7. Hence the given equation has no integral solution.

Illustrative Examples.

Ex. 1. If $d = gcd(x, y)$, then $\frac{x}{d}$ and $\frac{y}{d}$ are integers prime to each other.

Solution. Since $d = gcd(x, y)$, there exist integers l and m such that

$$d = lx + my$$

$$\therefore 1 = \frac{x}{d}l + \frac{y}{d}m$$

Since d is the division of x and y, there exist integers u and v such that $\frac{x}{d} = u$, $\frac{y}{d} = v$

$$\therefore 1 = ul + vm$$

$\therefore$ u and v are integers prime to each other. Thus $\frac{x}{d}$ and $\frac{y}{d}$ are integers prime to each other.

Ex. 2. If $gcd(a, 4) = 2$ and $gcd(b, 4) = 2$, proved that

$$gcd(a + b, 4) = 4$$

Solution. Since $gcd(a, 4) = 2$, so a is a multiple of 2 but not 4

$$\therefore a = 2p, \text{ for some odd integer } p$$

Similarly, since $gcd(b, 4) = 2$, we have

$$b = 2q, \text{ for some odd integer } q$$

$\therefore a+b = 2(p+q)$

$= 2 \cdot 2r$ where $p+q = 2r$, an even integer,

as, p, q are odd

$= 4r$

$\therefore gcd(a+b, 4) = gcd(4r, 4)$ where r is an integer

$= 4$

Thus $gcd(a+b, 4) = 4$.

Ex. 3. If $gcd(a, b) = 1$ prove that $gcd(a+b, a-b) = 1$ or 2

Solution Let $gcd(a+b, a-b) = d$

$\therefore a+b = k_1 d$ ... (1)

and $a-b = k_2 d$ ... (2)

where k_1, k_2 are integers

From (1) and (2), we get

$2a = (k_1 + k_2)d$ and $2b = (k_1 - k_2)d$

$\therefore d$ divides $2a$ and $2b$

$\therefore d \le gcd(2a, 2b) = 2\,gcd(a, b)$, by property (C) of at 2.8

$= 2 \cdot 1$ [$\because gcd(a, b) = 1$

$= 2$.

Hence $d = 1$ or 2

$\therefore gcd(a+b, a-b) = 1$ or 2

Ex. 4. Find the integers x and y such that $154x + 260y = 3$

Solution. Here $gcd(154, 260) = 2$. Since 3 is not divisible by 2, it follows that the given equation has no integral solution.

Ex. 5. Find the gcd of 252 and 595 and express it in the form $252x + 595y$

Solution. By division algorithm,

$595 = 2 \times 252 + 91$ (i)

$252 = 2 \times 91 + 70$ (ii)

$$91 = 1 \times 70 + 21 \quad \text{(iii)}$$

$$70 = 3 \times 21 + 7 \quad \text{(iv)}$$

$$21 = 3 \times 7 + 0 \quad \text{(v)}$$

Since the last non–zero remainder is 7, so

$$gcd(252, 595) = 7$$

To express the gcd in the form $252x + 595y$, we have, from (iv)

$$7 = 70 - 3 \times 21$$

$$= 70 - 3(91 - 1 \times 70), \text{ by (iii)}$$

$$= 4 \cdot 70 - 3 \cdot 91$$

$$= 4(252 - 2 \times 91) - 3 \cdot 91, \text{ by (ii)}$$

$$= 4 \cdot 252 - 11 \cdot 91$$

$$= 4 \cdot 252 - 11(595 - 2 \times 252), \text{ by (i)}$$

$$= 26 \cdot 252 - 11 \cdot 595$$

$\therefore 7 = 252x + 595y$ where $x = 26$, $y = -11$

Ex. 6. Find all solutions in positive integers of $5x + 3y = 52$.

Solution. Since $gcd(5, 3) = 1$ and 52 is divisible by 1, so the equation has integeral solutions.

Now $5 = 1 \cdot 3 + 2$

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

$$\therefore 1 = 3 - 1 \cdot 2 = 3 - 1(5 - 1 \cdot 3)$$

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

Hence $52 = -5 \cdot 52 + 3 \cdot 104$

Thus one integral solution of the equation is

$$x_0 = -52, \; y_0 = 104.$$

Hence all integral solutions of the equation are given by

$x = -52 + 3k$, $y = 104 - 5k$ for all integers k

As the solution will be positive, we must have

$$-52+3k>0 \text{ and } 104-5k>0$$

$$\therefore \frac{52}{3}<k<\frac{104}{5}$$

$$\therefore k=18,19,20.$$

Thus the given equation has exactly three positive solutions and these are

$$x=-52+3\cdot 18=2,\ y=104-5\cdot 18=14$$

$$x=-52+3\cdot 19=5,\ y=104-5\cdot 19=9$$

$$x=-52+3\cdot 20=8,\ y=104-5\cdot 20=4.$$

Ex. 7. Using prime factorisation, find gcd and lcm of 1300, 3575. Also verify that $gcd(a,b)\cdot lcm(a,b)=ab$.

Solution. We have

$$1300=2^2\cdot 5^2\cdot 11^0\cdot 13^1$$

$$3575=2^0\cdot 5^2\cdot 11^1\cdot 13^1$$

$$\therefore gcd(1300,3575)=2^{min(2,0)}\cdot 5^{min(2,2)}\cdot 11^{min(0,1)}\cdot 13^{min(1,1)}$$

$$=2^0\cdot 5^2\cdot 11^0\cdot 13^1$$

$$=325$$

$$lcm(1300,3575)=2^{max(2,0)}\cdot 5^{max(2,2)}\cdot 11^{max(0,1)}\cdot 13^{max(1,1)}$$

$$=2^2.5^2.11^1\,13^1$$

$$=14300$$

$$\therefore gcd(1300,3575)\cdot lcm(1300,3575)$$

$$=325\times 14300$$

$$=4647500$$

$$=1300\times 3575$$

Hence $gcd(a,b)\cdot lcm(a,b)=ab$.

Ex. 8. If a is a prime integer such that $a = n^2 - 4$ for some integer n, then show that $a = 5$.

Solution. We have $a = n^2 - 4 = (n-2)(n+2)$ for some integer n

Since a is prime, we must have, either $n-2=1$ or, $n+2=1$

But $n+2 \neq 1$ for some integer n. Hence

$$n-2=1$$

i.e., $n=3$.

$$\therefore a = n^2 - 4 = 3^2 - 4 = 5.$$

Ex. 9. Solve the Diophantine equations $158x - 47y = 9$.

Solution. Here $gcd(158, -47) = 1$ and 9 is divisible by 1.

Hence the given equation has integral solution.

Now

$$158 = (-3)(-47) + 17$$

$$-47 = (-3)17 + 4$$

$$17 = 4 \cdot 4 + 1$$

$$\therefore \quad 1 = 17 - 4 \cdot 4$$

$$= 17 - 4\{-47 - (-3) \cdot 17\}$$

$$= (-4)(-47) + (-11) \cdot 17$$

$$= (-4)(-47) + (-11) \cdot \{158 - (-3)(-47)\}$$

$$= (-11) \cdot 158 + (-37)(-47)$$

$$\therefore 9 = (-99) \cdot 158 + (-333)(-47)$$

Thus one integral solution of the given equation is $x_0 = -9$

$y_0 = -333$.

Hence all integral solutions of the equation are given by

$x = -99 - 47k$, $y = -333 - 158k$, for all integers k.

2.1.11 Congruence.

Definition. Let a and b be any two integers and m is a positive integer. Then a is said to be congruent to b modulo m, if $a-b$ is divisible by m or, $m \mid (a-b)$, and in this care we write

$$a \equiv b \mod (m)$$

Here m is called the **modulus** of the congruence, and b is called a **residue** of a mod (m).

If $a-b$ is not divisible by m, we say that a is not congruent to b module m and in this case we write $a \not\equiv b \mod (m)$.

Note. If $a \equiv b \pmod m$ then $a-b=km$ i.e., $a=b+km$ for some integer k.

Illustration.

(i) Since $57-17$ is divisible by 5, so

$57 \equiv 17 \pmod 5$

Here 5 is the modulus of the congruent and 17 is the residue of 57(mod 5)

(ii) Since $32-3=29$ is not divisible by 7, so 32 and 3 are incongruent modulo 7.

$$\therefore 32 \not\equiv 3 \pmod 7.$$

2.1.12 Properties of congruence

Let a, b, c denote integers. Then :

1. If $a \equiv b \pmod m$, then $b \equiv a \pmod m$

Proof: Since $a \equiv b \pmod m$, $a-b$ is divisible by m

i.e., $-(b-a)$ is divisible by m

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

$$\therefore b \equiv a \mod (m)$$

2. If $a \equiv b \pmod m$, then $a \pmod m = b \pmod m$

Proof: As $a \equiv b \pmod m$, so $a-b=km$, for some integer m

Let $k = k_1 - k_2$ where k_1 and k_2 are integers.

$\therefore a - b = (k_1 - k_2)\, m$

$\therefore a - k_1 m = b - k_2 m = r$, say

$\therefore a - k_1 m = r, b - k_2 m = r$

$\therefore r \equiv a \pmod m$, $r \equiv b \pmod m$

$\therefore a \pmod m = b \pmod m$

3. If $a \equiv b \pmod m$, then $a \pm c \equiv (b \pm c) m$

Proof: Since $a \equiv b \pmod m$, $a - b$ is divisible by m

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

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

$\Rightarrow a \pm c \equiv (b \pm c) m$.

4. If $a \equiv b \pmod m$, then $ac \equiv bc \pmod m$

Proof: Since $a \equiv b \pmod m$, $a - b$ is divisible by m

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

$\therefore ac \equiv bc \pmod m$

Note. The converse of the above property is not always true.

5. If $ac \equiv bc \pmod m$ then $a \equiv b \left(mod \dfrac{m}{gcd\,(c, m)} \right)$

Proof: Since $ac \equiv bc \pmod m$, $ac - bc$ is divisible by m

$\therefore ac - bc = km$ where k is an integer

$\therefore a - b = k \left(\dfrac{m}{c} \right)$

$\therefore a \equiv b \pmod{\dfrac{m}{c}}$, providesd $\dfrac{m}{c}$ is an integer.

Since $\frac{m}{c}$ is an integer, so c divides m

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

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

Note. If $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$ only if $gcd(c, m) = 1$

6. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

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

Proof : Since $a \equiv b \pmod{m}$, $a - b$ is divisible by m

Similerly $c - d$ is divisible by m.

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

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

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

Note In general $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$

$\Rightarrow ax + cy \equiv (bx + dy) \pmod{m}$ where x, y are integers.

7. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$ac \equiv bd \pmod{m}$$

Proof : Since $a \equiv b \pmod{m}$, $a - b$ is divisible by m

$\therefore (a - b)\, c$ is divisible by m

Also, since $c \equiv d \pmod{m}$, $c - d$ is divisible by m

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

Hence $(a - b)\, c + (c - d)\, b$ is divisible by m.

i.e., $ac - bd$ is divisible by m.

$\therefore ac \equiv bd \pmod{m}$

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

Proof : Obviously, statement is true for $n = 1$.

Let the statement is true for $n = k$.

$\therefore a^k \equiv b^k \pmod{m}$

Then, using property (7), we have

$a \cdot a^k \equiv b \cdot b^k \pmod{m}$

$\therefore a^{k+1} \equiv b^{k+1} \pmod{m}$

Thus the statement is true for $n = k+1$ whenever it is true for $n = k$.

Hence by induction the statement is true for any positive integer n.

Theorem. The congruence relation is an equivalence relation.

Proof. As $a - a = 0$ is divisible by m, so

$a \equiv a \pmod{m}$ for any integer a.

Thus the congruence relation is reflexive

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

$\Rightarrow a - b$ is divisible by m

$\Rightarrow -(b - a)$ is divisible by m

$\Rightarrow b - a$ is divisible by m

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

Hence the congruence relation is symmetric.

Lastly $a \equiv b \pmod{m} \Rightarrow a - b$ is divisible by m and $b \equiv c \pmod{m} \Rightarrow b - c \pmod{m}$ in divisible by m

So $(a - b) + (b - c)$ in divisible by m

i.e., $a - c$ is divisible by m

$\therefore a \equiv c \pmod{m}$

Thus $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$

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

Hence the congruence relation is transitive .

Thus the congruence relation is an equivalence relation.

2.1.13 Residue classes of integer modulo n

Definition The set of all integers b which are congruent to a modulo n is called the **congruence class of integer modulo n** or **residue classes of integer modulo n** and is denoted by $[a]_n$ or $[a]$ or, $\bar{a}$. Thus

$$[a] = \{b \in Z : b \equiv a \pmod{n}\}.$$

For example,all congruence classes of integer modulo 4 are

$$[0] = \{b \in Z : b \equiv 0 \pmod{4}\}.$$

$$= \{b \in Z : b \text{ is divisible by 4 or } b = 4k \text{ for some } k\}$$

$$= \{\cdots -8, -4, 0, 4, 8, \cdots\}$$

$$[1] = \{b \in Z : b \equiv 1 \pmod{4}\}$$

$$= \{b \in Z : b - 1 = 4k \text{ ie } b = 1 + 4k \text{ for some } k\}$$

$$= \{\cdots -7, -3, 1, 5, 9, \cdots\}$$

Similarly

$$[2] = \{\cdots -6, -2, 2, 6, 10, \cdots\}$$

$$[3] = \{-5, -1, 3, 7, 11, \cdots\}$$

$$[4] = \{\cdots -8, -4, 0, 4, 8, \cdots\} = [0]$$

Thus, there are only 4 distinct congruence classes of integer modulo 4, namely $[0], [1], [2], [3]$.

In general $[0],[1],[2],\cdots[n-1]$ are n distinct residue classes integer modulo n.

It is evident that

$$[a]=[a+n]=[a+2n]=\cdots .$$

$$[0]=[n]=[2n]=\cdots .$$

For any positive integer n, Z_n denote the set of all congruenc classes of integer modulo n. Thus

$$Z_4=\{[0],[1],[2],[3]\}$$

In general,

$$Z_n=\{[0],[1],[2],\cdots[n-1]\}$$

Theorem, The number of elements of Z_n is finits and th number is n.

Proof. left as an exercise

Arithmetic of Residue classes.

Addition and multiplication for residue classes of integer modu n are defined as given below :

$$[a]+[b]=[a+b] \text{ and } [a]\cdot[b]=[ab]$$

As an illustration, consider the residue classes of integer modu 3, namely $[0],[1],[2]$.

Then $[1]+[0]=[1]$, $[1]+[2]=[3]=[0]$

$[1]\cdot[2]=[2]$, $[2]\cdot[2]=[4]=[1]$

Following composite tables show the addition and multiplication tables for the residue classes of integer modulo 3:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

*	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Definition. An element $[b] \in Z_n$ is called an inverse of an element $[a] \in Z_n$ if $[a][b] = [1]$ in Z_n.

Definition. An element $[a] \in Z_n$ is said to be a unit element in Z_n if $[a]$ has inverse in Z_n.

Theorem Let a and n be integers with $n \geq 2$ relatively prime. Then $[a]$ has an inverse in Z_n if and only if a and n are relatively prime

Proof. Beyond the scope of this book.

Illustration.

(i) The unit elements of Z_6 are $[1], [5]$, as

$$gcd\,(1, 6) = gcd\,(5, 6) = 1$$

(ii) The inverse of $[5]$ in Z_6 is $[3]$ as $[5][3] = [1]$

Linear Congruence.

Let a, b be any two integers. Then a congruence of the form

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

Where m is a positive integer and n is an unknown integer is called a linear congruence.

An integer x_0 is called a solution of (1) if $a\,x_0 \equiv b \pmod{m}$.

Any value of x which is a solution of the congruence $ax \equiv 1 \pmod{m}$ is called an inverse of a modulo m.

Illustration (i) Consider the congruence

$$6x = 3 \pmod 9 \qquad \ldots (2)$$

Since $6 \cdot 2 \equiv 3 \pmod 9$, so $x = 9$ is a solution of (2).

(ii) Since $x = 3$ is a solution of the congruence

$3x \equiv 1 \pmod 8$, so 3 is an inverse of 3 modulo 8.

Theorum. If a and m are relatively prime, then the congruence $ax \equiv b \pmod m$ has a unique solution.

Proof : As a and m are relatively prime,

$$gcd\,(a, m) = 1.$$

$\therefore$ There exist integers p, q such that

$$pa + qm = 1.$$

Then $pab + qmb = b$

Hence $pab + qmb - b = 0$

$$\therefore pab + qmb \equiv b \pmod m$$

But $qmb \equiv 0 \pmod m$

$$\therefore pab \equiv b \pmod m$$

Hence $x_0 = pb$ is a solution of $ax \equiv b \pmod{m}$

$\therefore ax_0 = b \bmod m)$

Next let us assume that y be the another solution of $ax \equiv b \pmod{m}$

$\therefore ay_0 \equiv b \pmod{m}$ ... (2)

$\therefore$ From (1) and (2), we have.

$ax_0 - y_0 a \equiv 0 \pmod{m}$

$\therefore ax_0 \equiv y_0 a \pmod{m}$

$\therefore x_0 \equiv y_0 \pmod{m}$ [$\because$ a and m are relatively prime .]

Thus the solution of $ax \equiv b \pmod{m}$ is unique.

Note : If $gcd(a, m) \neq d$ the congruence $ax = b \pmod{m}$ has no solution when d does not divide b; but if d divides b, there are exactly d solutions.

Illustration Consider the congruence $3x \equiv 2 \pmod{8}$.

Since $gcd(3, 8) = 1$, the congruence has a unique solution.

As $gcd(3, 8) = 1$ there exists u and v such that

$$3u + 8v = 1$$

Here u, v can be found out using division algorithm as follows

$8 = 3 \times 2 + 2$

$3 = 2 \times 1 + 1$

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

$= 3 - 1 \cdot (8 - 3 \cdot 2)$

$= 3 \cdot 3 + (-1) \cdot 8$

Hence $u = 3, v = -1$

$\therefore 3 \cdot 3 + (-1) \cdot 8 = 1.$

which implies

$3 \cdot 3 \equiv 1 \pmod 8$

$\therefore\ 3 \cdot 6 \equiv 2 \pmod 8$

Thus $x = 6$ is a solution of the congruence

$3x \equiv 2 \pmod 8$

Hence the solution of the given congruence is

$$x \equiv 6 \pmod 8$$

Fermat's theorem.

If p be a prime and a is an integer such that p does not divide a, then

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

Proof : Consider the integers

$$a, 2a, 3a, \cdots (p-1)\, a \qquad \ldots (1)$$

As p is not a divison of a, none of these integers is divisible by p.

We show that no two distinct integers of (1) are congruent to each other modulo p. Suppose, if possible

$$ra \equiv sa \pmod p$$

where $1 \le s < r \le p-1$

But $gcd\,(a, p) = 1$, so must have

$$r \equiv s \pmod p$$

Which is a contradiction.

Hence the integers $a, 2a, 3a, \cdots (p-1)\, a$ are congruent modulo p to $1, 2, 3, \cdots p-1$ taken in some order.

$\therefore\ a \cdot 2a \cdot 3a \cdots (p-1)\, a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$

or $a^{p-1}(p-1)\,! \equiv (p-1)\,!\ \text{mod}\ p)$ $\qquad \ldots (2)$

Since $gcd\,(p,(p-1)!) = 1$, (2) is equivalent to

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

Corollary. If p is a prime and a is any integer, then

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

Proof : If p divides a, then p divides $a^p - a$.

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

If p does not divide a, from the above theorem, we get

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

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

Illustration 7 is a prime and 7 does not divide 5, so by Fermat's theorem, $5^6 \equiv 1 \pmod{7}$

$\therefore 5^6 - 1$ is divisible by 7.

Illustrative Examples.

Ex. 1. Show that $3^{302} \equiv 4 \pmod{5}$

Solution. By Fermat's theorem, we have

$$3^4 \equiv 1 \pmod{5}$$

$$\therefore \left(3^4\right)^{75} \equiv (1)^{75} \pmod{5}$$

$$\therefore 3^{300} \equiv 1 \pmod{5}$$

$$\therefore 3^{300}3^2 \equiv 3^2 \pmod{5}$$

$$\therefore 3^{302} \equiv 9 \pmod{5}$$

But $9 \equiv 4 \pmod{5}$

Hence $9^{302} \equiv 4 \pmod{5}$

Ex. 2. When n is a positive integer, show that

$$3^{2n+1} \equiv 3 \cdot 2^n \pmod{7}$$

Solution. We have

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

$$\therefore 3^{2n} \equiv 2^n \pmod 7$$

$$\therefore 3 \cdot 3^{2n+1} \equiv 3 \cdot 2^n \pmod 7$$

Thus $3^{2n+1} \equiv 3 \cdot 2^n \pmod 7$

Ex. 3. Find the remainder when the sum $1! + 2! + 3! + \cdots + 100!$ is divided by 5.

Solution. $1! \pmod 5 \equiv 1 \pmod 5$

$2! \pmod 5 = 2 \pmod 5$

$3! \pmod 5 = 6 \pmod 5 = 1 \pmod 5$

$4! \pmod 5 = 24 \pmod{} = 4 \pmod 5$

$5! \pmod 5 = 120 \pmod 5 = 0 \pmod 5$

When $n \geq 5$,

$$n! = 5!\ 6 \cdot 7 \cdots n$$

$$\therefore n! \pmod 5 = (5!\, 6 \cdot 7 \cdots n) \pmod 5$$

$$= (0 \cdot 1 \cdot 2 \cdots) \pmod 5$$

$$= 0 \pmod 5 \text{ when } n \geq 5$$

$$\therefore (1! + 2! + 3! + \cdots + 100!) \pmod 5$$

$$= (1 + 2 + 1 + 4 + 0 + 0 + \cdots + 0) \pmod 5$$

$$= 8 \pmod 5$$

$$= 3 \pmod 5$$

Thus the required remainder is 3.

Ex. 4. Solve the linear congruence $6x \equiv 3 \pmod 9$

Solution. Here $\gcd(6, 9) = 3$ and 3 divides 3. Hence the given congruence has 3 incongruent solutions.

Now $6x \equiv 3 \pmod 9$ is equivalent to

$$2x \equiv 1 \pmod 3$$

Since $gcd\,(2, 3) = 1$, the congruence $2x \equiv 1 \pmod 3$ has only one solution.

$\therefore$ There exist integers u and v such that

$$2u + 3v = 1$$

Thus $u = -1, v = 1$ so that

$$2 \cdot (-1) + 3 \cdot 1 = 1$$

which imples

$$2(-1) \equiv 1 \pmod 3$$

Thus $x = -1$ is a solution of congruence

$$2x \equiv 1 \pmod 3$$

Since the given congruence has 3 incongruent solution they are

$$x = -1, -1 + 3, -1 + 6 \pmod 9$$

i.e. $\quad -1, 2, 5 \pmod 9$

Ex. 5. Find all units of Z_{18}

Solution. we have

$$Z_{18} = \{ [0], [1], [2], \cdots [16], [17] \}$$

Now $gcd\,(1, 18) = gcd\,(5, 18) = gcd\,(7, 18)$

$= gcd\,(11, 8) = gcd\,(13, 18) = gcd\,(17, 18) = 1$

Hence $[1], [5], [7], [11], [13], [17]$ are the only unit elements of Z_{18}.

Ex. 6. In Z_{16} find the inverse of [9] and use it to solve

$[9]\,x = [12]$

Solution. Since (9,16) = 1, the inverse $[9]$ exists in Z_{16}. From the Euclidean algorithem, we have

$$16 = 1 \cdot 9 + 7$$

$$9 = 1 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1$$

$$\therefore 1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (9 - 1 \cdot 7)$$

$$= 4 \cdot 7 - 3 \cdot 9$$

$$= 4 \cdot (16 - 1 \cdot 9) - 3 \cdot 9$$

$$= 4 \cdot 16 - 7 \cdot 9$$

$$= 16 \cdot 4 + 9(-7)$$

Hence

$$[1] = [16][4] + [9][-7]$$

$$= [0][4] + [9][9] \qquad [\because\ 9 \equiv -7 \pmod{16} = [9][9]$$

Thus the inverse of [9] is [9]

Now $[9]\,x = [12]$

$\Rightarrow [9]\ [9]x = [12][-9]$

$\Rightarrow x = [-4][-7]$

$= [28]$

$= [12]$.

7. Find all integers $m \geq 5$ such that $7 \equiv m^2 \pmod{m}$

Solution. Since $7 \equiv m^2 \pmod{m}$, so $7 - m^2$ is divisible by m. Thus there exist integer p such that

$$7 - m^2 = mp$$

$$\therefore m^2 + mp = 7$$

i.e., $m(m + p) = 7$

Thus 7 is divisible by m. But $m \geq 5$.
Hence we must have

$$m = 7$$