Chapter 1
1.1 Divisibiliy

By Natural numbers we mean the numbers 1, 2, 3 . Integers are Natural numbers, 0 and the negative numbers ...-3,-2,-1, the set of Integers will be denoted by Z such that $\mathbf{Z} = \{,-3,-2,-1, 0, 1, 2, 3\}$.

Definition ***1.1.1***

If a and b are Integers with $a \neq 0$, we say that a divides b if there is an integer c such that b=ac.

If a divides b, then a is a divisor or factor of b.

If a divides b we write $a \mid b$, if a doesn't divide b then $a \nmid b$.

Example (1):

The following illustrate the concept of divisibility of integers:

$13 \mid 182$, $-5 \mid 30$, $6 \nmid 44$, $7 \nmid 50$ and $17 \mid 0$.

Example (2):

The divisors of 6 are $\pm1, \pm2, \pm3, \pm6$.

The divisors of 17 are $\pm1, \pm17$.

The divisors of 100 are $\pm1, \pm2, \pm4, \pm5, \pm10, \pm20, \pm25, \pm50$ and ±100.

Note that:

Every non-zero Integer is a divisor of 0 and 1 is a divisor of every Integer or equivalently every Integer is a multiple of 1.

Theorem ***1.1.2***

If a,b and c are integers with $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof :

Since $a \mid b$ so $b = k_1 a$, and $b \mid c$ so $c = k_2 b$,where k_1, k_2 are integers ,i.e. $k_1, k_2 \in \mathbf{Z}$.

Hence $c = (k_2 k_1)\, a = k_3 a$, where $k_3 = k_1 . k_2 \in \mathbf{Z}$. So $a \mid c$.

Thus the relation of divisibility is transitive.

Example (3):

Since $11 \mid 66$ and $66 \mid 198$ $\therefore$ $11 \mid 198$.

Note:

The relation of divisibility of integer is not an equivalence relation,since it is reflexive and transitive but not symmetric.

Theorem ***1.1.3***

If a,b,x and y are integers and if $d \mid a$ and $d \mid b$ then $d \mid (ax+by)$.

Proof :

Since $d \mid a \Rightarrow a = k_1 d$ and $d \mid b \Rightarrow b = k_2 d$, where $k_1 , k_2 \in \mathbf{Z}$.

$\therefore$ $ax + by = k_1 dx + k_2 dy$

$= d (k_1 x + k_2 y)$

$\Rightarrow d \mid (ax + by)$.

Example (4):

Since $3 \mid 21$ and $3 \mid 33$, $\therefore$ 3 divides $5.\ 21 - 3(33) = 105 - 99 = 6$.

Corollary ***(1)***

Taking x=y=1 we see that $d \mid a+b$.

Corollary *(2)*

Taking x=1 , y=-1 we see that d | a-b.

Thus the divisor of each of two integers is a divisor of their sum and their difference.

Example (**5**):

Show that a-b | a^n-b^n for all non-negative integral values of n.

Solution *:*

It is proved by induction.

• it is true for n = 0 i.e., a-b | a^0-b^0 i.e., a-b | 0.

• assume that it is true for n = k then a-b | a^k - b^k . . . . . (∗)

we will prove it is true n=k+1.

$a^{k+1} - b^{k+1} = a^{k+1} - a^k b + a^k b - b^{k+1}$

$= a^k (a-b) + b (a^k - b^k)$

Since a-b | a^k (a-b), and (a-b) | b (a^k - b^k) by (∗) then Theorem **1.1.3** implies that a-b | a^k (a - b) + b (a^k - b^k) i.e. a-b | a^{k+1} - b^{k+1},

and so it is true for n=k+1. So the induction is complete and

a-b | a^n - b^n for all non-negative integral values of n.

Theorem *1.1.4*

The division Algorithm or Theorem of Euclid.

If a and b are integers such that b>0 , then there are unique integers q and r such that a=bq+r with 0≤ r < b . The integers q and r are called respectively , the quotient and remainder in the division of a by b.

Proof :

We have two cases :

(I) If a is a multiple of b .

(II) If a is not a multiple of b.

In case (I): a = bq , q ∈**Z**, the reminder being zero in this case.

In case (II): a = bq + r , 0 < r < b.

For if r = b , then

$$a = bq + b$$
$$= (q + 1) b$$
$$= q' b , \ q' = q + 1,$$

which contradict the fact that a is not a multiple of b .Combing the two cases , we get

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

Now we prove the uniqueness of q and r. Suppose that a has two representations of the desired form , namely

$$a = bq + r , 0 \le r < b \text{ and } a = bq' + r' , 0 \le r' < b.$$
$$\therefore a-a = 0 = b (q-q') + (r-r').$$

The L.H.S. of the above equation is divisible by b and the first term on the R.H.S. is also divisible by b.

Hence b | | r-r'| , but r<b and r'<b and so | r-r'|<b .

Hence b | r-r'| only if | r-r'|=0 ⇒ r-r' =0 ⇒ r=r'. Consequently q=q' .

Example (**6**):

let b = 15 then

177 = 15 . 11 + 12 0 < 12 < 15

-54 = 15 . (-4) + 6 0 < 6 < 15

$105 = 15\ (7) + 0 \qquad 0 < 0 < 15.$

Note:

We can use the greatest integer function to give explicit formula for the quotient and reminder in the division algorithm.

Since q is the largest integer such that $bq \le a$, and $r = a - bq$ it follows that:

$q=[a/b]$, $r = a-b\ [\ a/b\ ]$.

Example (**7**):

let $a = 1028$ and $b = 34$, then $a = bq + r$, $0 \le r < b$,

where $q = [\ 1028/34\ ] = 30$,

$r = 1028-34\ (30) = 8$.

Example (**8**):

let $a = -380$, $b = 75$, then $a = bq + r$, $0 \le r < b$,

where $q= [\ -380 / 75\ ] = -6$,

$r = -380 - 75\ (-6) = 70$.

Definition ***1.1.5***

If $b = 2$ we get $a = 2q + r$, $0 \le r < 2$, thus $r = 0$, 1.

Thus every integer is either of the form $2q$ or $2q + 1$.

Integers of the form $2q$ are called even.

Integers of the form $2q + 1$ are called odd.

Example (**9**):

The square of any integer a leaves the reminder 0 or 1 when divided by 4.

Solution *:*

$a = 2q$ or $a = 2q + 1$

$\therefore a^2 = 4q^2$ or $a^2 = 4q^2 + 4q + 1$,

and so leaves the reminder 0 or 1 when divided by 4.

Example (**10**):

Show that if n is an odd integer then $8 \mid n^2-1$

Solution *:*

Let $n = 2q+1$, then $n^2 = 4q^2 + 4q + 1$

$\therefore n^2-1 = 4q\ (q + 1)$.

Now either q or q+1 is even , so $q\ (q + 1)$ is even so $q(q+1) =2k$, $k \in \mathbf{Z}$.

$\therefore n^2-1 = 8k \Rightarrow 8 \mid n^2-1$.

Example(**11**):

Use division algorithm to prove that the cube of any integer is either of the form qn , qn+1 or qn+8.

Solution *:*

By division algorithm every integer is either of the form 3k , 3k+1 , or 3k+2 (taking b=3 in division algorithm).

Now

$(3k)^3 = 27k^3 = 9\ (3k^3) = 9n$.

$(3k+1)^3 = 27k^3 + 9k\ (3k+1) + 1$

$= 9\ [3k^3 + k(3k + 1)\ ] + 1$

$= 9n+1$.

$(3k+2)^3 = 27k^3 + 18k\ (3k + 2) + 8$

$= 9\ [3k^3 + 2k\ (3k + 2)\ ] + 8$

$= 9n + 8$.

Example (**12**):

Prove that if n is an odd positive integer then $a+b \mid a^n+b^n$.

Solution *:*

It is true for n=1 as $a+b \mid a+b$.

Suppose it is true for n = k, so that $a+b \mid a^k + b^k$ .....(*).

Now $a^{k+2} + b^{k+2} = a^{k+2} - a^k b^2 + a^k b^2 + ak\, b2 + b^{k+2}$

$= a^k (a^2-b^2) + b^2(a^k + b^k)$.

Now $a + b \mid a^k (a^2-b^2)$ and $a+b \mid b^2(a^k + b^k)$ (from *)

$\therefore\ a+b \mid a^k (a^2-b^2) + b^2(a^k + b^k)$

i.e., $a+b \mid a^{k+2} + b^{k+2}$.

So it is true for n =k+2 and hence by induction its true for all odd positive integral value

1.2 The Greatest Common Divisor

Definition ***1.2.1***

The greatest common divisor of two integers a and b , that are not both zero , is the largest integer that divides
both a and b.

The greatest common divisor of a,b is written as (a,b),so (0,0)=0 . It is denoted by d and it satisfies the following:

(i) d>0, (ii) $d \mid a$, $d \mid b$, (iii) if c is any integer such that $c \mid a$, $c \mid b$ then $c \mid d$,

i.e. any common divisor of a,b is also a divisor of d.

Example (**1**):

The common divisors of 24 and 84 are
± 1 , ± 2 , ± 4 , ± 6 , ± 12, hence (24 , 84)=12.
(15 , 81)=3, (17 , 25)=1, (0 , 44)=44, (-6 , -15)=3.

Definition ***1.2.2:***

The integers a and b are called relatively prime if a and b have greatest common divisor (a , b)=1.

Example(**2**):

Since (25 , 42)=1 so 25 , 42 are relatively prime.

Note:

Since the divisors of -a are the same divisors of a , it follows that
(a , b)=(|a|,|b|) where |a| denotes the absolute value of a.

Theorem ***1.2.3***

The gcd of two integers a and b is unique .

Suppose d =(a , b) , c= (a, ,b) , we must prove that c=d.

Since d is gcd (a , b) , c is a common divisor (gcd is also a common divisor of a , b)

$\therefore c \mid d$ likewise , $d \mid c$.

Hence $d = \pm c$. Since both c , d are positive therefore c = d .

Theorem ***1.2.4***

Let a , b and c be integers with (a , b)=d then
(i) (a/d , b/d) = 1
(ii) (a+cb , b) = (a , b)

Proof :

(i) Let (a , b) = d such that a , $b \in Z$. We show that a/d , b/d have no common positive divisors other than 1 .

let k be a +ve integer such that $k \mid (a/d)$ and $k \mid (b/d)$ then there are k_1 and k_2 such that $a/d = k_1 k$ and $b/d = k_2 k$.

So $a = d k_1 k$, $b = d k_2 k$.

Hence dk is a common divisor of a and b.

Since d is gcd of a,b and $dk \leq d$ so that k must equal 1 so (a / d , b / d)=1.

(ii) let d = (a,b) and d_1=(a + cb , b), so $d \mid a$, $d \mid b$, by Theorem (1.1.3)

$\therefore d \mid a + cb$, $d \mid b$, $c \in Z$, so $d \mid d_1$ .....(1).

$d_1 \mid a+cb$, $d_1 \mid b$ by Theorem (1.1.3)

$\therefore d_1 \mid a + cb - cb \Rightarrow d_1 \mid a$, $d_1 \mid b$, so $d_1 \mid d$ .....(2),

from (1),(2) $d = d_1$ and (a , b) = (a + cb , b).

Theorem ***1.2.5***

If $a = bq+r$ then $(a , b) = (b , r)$.

Proof :

Let $(a , b) = d$

so $d \mid a$, $d \mid b$, by Theorem 1.1.3 $d \mid a-bq$, $q \in Z$

$\therefore d \mid r$, $d \mid b$,

$\therefore d$ is a common divisor of r,b .

If $(b , r) = d_1$

$\therefore d \mid d_1$.....(1).

Since $d_1 \mid b$, $d_1 \mid r$ by Theorem 1.1.3 $d_1 \mid bq+r \Rightarrow d_1 \mid a$, $d_1 \mid b$

$\therefore d_1$ is a common divisor of a,b.

$\therefore d_1 \mid d$ .....(2)

from (1) and (2) $d_1 = d$ $\therefore (a , b) = (b , r)$.

Theorem ***1.2.6***

Let $d = (a , b)$ then there exist integers x_0 , y_0 such that $d = ax_0 + by_0$.

Proof :

Consider the linear combination $ax + by$, where x , y range over all integers .This set of integers $\{ax + by\}$

includes positiveve and -ve values also 0 by the choice $x = y = 0$. Choosing x_0 and y_0 so that $ax_0 + by_0$ is

the least positive integer l in the set.

Thus $l = ax_0 + by_0$. We prove that $l \mid a$, $l \mid b$.

Assume that $l \nmid a$ and we obtain a contradiction.From $l \nmid a$ $\exists$ integers q and r , such that

$a = lq+r$ with $0 < r < l$,

so $r = a - lq$

$= a - q (ax_0 + by_0)$

$= a (l - q x_0) + b (- q y_0)$,

and thus r is in the set $\{ ax + by \}$. This contradicts the fact that l is the least positive integer in the

set $\{ ax + by \}$.

Thus our assumption that $l \nmid a$ is false and so $l \mid a$ .Similarly we can show that $l \mid b$.

Now since d is the gcd of a and b $a = dA$, $b = dB$ where $A,B \in Z$.Since

$l = ax_0 + by_0$

$= dAx_0 + dBy_0$

$= d (Ax_0 + By_0) \Rightarrow d \mid l \Rightarrow d \leq l$.

Now $d < l$ is impossible since d is the gcd and so $d = l = ax_0 + by_0$.

Corollary ***(1):***

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

Theorem ***1.2.7:***

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

Proof :

$(a , b) = 1 \Rightarrow$ $ax+by =1$, for $x , y \in Z$.

$\therefore$ $acx + bcy =c$.

Now $a \mid acx$, $a \mid bcy$,

$\therefore a \mid acx + bcy$ i.e., $a \mid c(ax+by)$ i.e., $a \mid c$ ($\because$ $(ax+by)=1$) .

Definition ***1.2.8***

Let $a_1 , a_2,... , a_n$ be integers not all zeros. The gcd of these integers is the

largest integer

which is a divisor of all the integers in the set .

The gcd of $a_1 , a_2,... , a_n$ is denoted by $(a_1 , a_2,... , a_n)$.

Example (3):

$(12 , 18 , 30)=6, \quad (10 , 15 , 25)=5.$

Lemma *1.2.9*

If $a_1, a_2,... ,a_n$ are integers not all zeros , then

$(a_1, a_2,... ,a_n) = (a_1, a_2,... ,a_{n-1} , (a_{n-1}, a_n))$.

Example(4):

To find gcd of 105 , 140 and 350 by lemma 1.2.9

$(105 , 140 , 350) = (105 , (140 , 350))$

$= (105 , 70)= 35.$

Example (5):

$(15 , 21 , 35) = (15 , (21 , 35)) = (15 , 7) = 1$

1.3 The Euclidean Algorithm

The gcd of two integers can be found by listing all +ve divisors and picking out the largest one common to

each , but this is not suitable for large numbers.

A more efficient process involving repeated application of the division algorithm goes by the name of

Euclidean Algorithm . The E.A. may be described as follows :

Let a , b be two integers whose gcd is desired , we can find unique integers q_1 , r_1 such that

$a = bq_1 + r_1 \quad 0 \le r_1 < b$

if $r_1 \neq 0$ we divide b by r_1 so

$b = r_1 q_2 + r_2 \quad 0 \le r_2 < r_1.$

if $r_2 \neq 0$ we divide r_1 by r_2 so

$r_1 = r_2 q_3 + r_3 \quad 0 \le r_3 < r_2.$

Similarly if $r_3 \neq 0$

$r_2 = r_3 q_4 + r_4 \quad 0 \le r_4 < r_3$

.

.

.

$r_{k-2} = r_{k-1} q_k + r_k \quad 0 < r_k < r_{k-1}$

$r_{k-1} = r_k q_{k+1} + 0 \quad r_{k+1} = 0.$

By the repeated application of Theorem 1.2.5 , we can show that r_k , the last non-zero reminder which appears in this manner is equal to (a , b),

i.e.,$(a , b) = (b , r_1) = (r_1 , r_2)$ - - - - $(r_{k-1} , r_k) = (r_k , 0) = r_k$.

Example (1):

Find (243 , 129).

$243 = 129.1 + 114$

$129 = 114.1 + 15$

$114 = 15.7 + 9$

$15 = 9.1 + 6$

$9 = 6.1 + \boxed{3}$

$6 = 3.2 + 0$

$\therefore (243 , 129) = 3$.

Example (**2**):

Find (275 , 105) and express it as a linear combination of 275 and 105 .

Solution *:*

$275 = 105.2 + 65$
$105 = 65.1 + 40$
$65 = 40.1 + 25$
$40 = 25.1 + 15$
$25 = 15.1 + 10$
$15 = 10.1 + \boxed{5}$
$10 = 5.1 + 0$

$\therefore (275 , 105) = 5.$

To express 5 as L.C. of 275 , 105 we have to begin from the second equation from the bottom

$5 = 15 - 10$
$= 15 - (25 - 15)$
$= 2(15) - 25$
$= 2(40 - 25) - 25$
$= 2(40) - 3(25)$
$= 2(40) - 3(65 - 40)$
$= 5(40) - 3(65)$
$= 5(105 - 65) - 3(65)$
$= 5(105) - 8(65)$
$= 5(105) - 8(275 - 2.105)$
$= (105) (21) + (275) (-8)$

$\therefore 5 = 275\ x + 105\ y$ where $x = -8, \quad y=21$.

Note:

The integers x and y are not unique i.e., for example 5 can be written as a L.C. of 275 and 105 for different values of x and y than those listed above.

For example: one could add and subtract (275) (105) to get

$5 = (275)(-8) + (105)(21) + (275)(105) - (275)(105)$
$= 275 (-8 + 105) + 105 (21 - 275)$
$= 275 (97) + 105 (-254)$.

Ex (**3**):

Apply the Euclidean Algorithm to find (34 , 55)

$55 = 34.1 + 21$
$34 = 21.1 + 13$
$21 = 13.1 + 8$
$13 = 8.1 + 5$
$8 = 5.1 + 3$
$5 = 3.1 + 2$
$3 = 2.1 + \boxed{1}$
$2 = 1.2 + 0$

$\therefore (34 , 55) = 1.$

Example (**4**):

Prove that for any integer a,one of the integers a , a+2 , a+4 is divisible by 3 .

Solution *:*

Every integer a is either of the form 3k or 3k+1 or 3k+2.

If a is of the form 3k then $3 \mid a$.

If a = 3k+1 then a+2 = 3k+3 $\Rightarrow$ $3 \mid a+2$.

If a = 3k+2 then a+4 = 3k+6 $\Rightarrow$ $3 \mid a+4$

Example (**5**):

Show that if a is an integer such that $2 \nmid a$ and $3 \nmid a$, then $24 \mid a^2-1$.

Solution *:*

a must be of the form 6k+1 or 6k+5.

If a = 6k+1 then $a^2 - 1 = 36k^2 + 12k$

$= 12k (3k + 1)$.

Now either k or 3k+1 is even so $k (3k + 1)=2n$

Hence $a^2 - 1=24n \Rightarrow 24 \mid a^2 - 1$.

If a = 6k+5 then $a^2 - 1 = 36k2 + 60k + 24$

$= 12k (3k + 5) + 24$.

Now either k or 3k+5 is even and so $k (3k + 5)=2n$.

Hence $a^2 - 1=24n+24=24(n+1) \Rightarrow 24 \mid a^2-1$.

1.3.1 Fibonacci Numbers:

The integers 1,2,3,5,8,13,.. in which each integer after the second is the sum of two preceding integers are

called Fibonacci Numbers.

Ex (**6**):

Prove that two consecutive Fibonacci numbers are relatively prime.

Solution *:*

The first two consecutive F.N. are 1 , 2 and (1 , 2)=1 . Let k_1 , k_2 be two consecutive F.N. which are

relatively prime i.e. $(k_1 , k_2) = 1$.

we must prove that $(k_2 , k_3) = 1$, where $k_3 = k_1+k_2$.

Let $(k_2 , k_3) = d$ i.e., $(k_2 , k_1+k_2) = d$.

$\Rightarrow d \mid k_2 , d \mid k_1+k_2$. $\therefore d \mid k_1+k_2-k_2$ i.e., $d \mid k_1$.

Thus $d \mid k_2 , d \mid k_1$, but $(k_1 , k_2) = 1$ by hypothesis .

Therefore $d \mid 1 \Rightarrow d=1$, which completes the proof.

Example (**7**):

Prove that if $a \mid c , b \mid c$ with (a , b) = 1 , then $ab \mid c$.

Solution *:*

$a \mid c \Rightarrow c = ap, \quad p \in \mathbf{Z}$.

$b \mid c \Rightarrow c = bq, \quad q \in \mathbf{Z}$.

$\because$ (a , b) = 1 so $\exists$ x , y $\in \mathbf{Z}$, such that $ax + by = 1$.

$\therefore acx + bcy = c, \Rightarrow a(bq)x + b(ap)y = c$

i.e. $ab (qx + py) = c \Rightarrow ab \mid c$.

1.4 The Least Common Multiple

Definition ***1.4.1:***

Let a , b be two non-zero integers . An integer c is said to be Common Multiple of a and b if a | c and b | c.

Definition ***1.4.2:***

Let a , b be non-zero integers . Then an integer m is called the least common multiple of a and b denoted by [a , b] or Lcm(a , b) if it has the following properties:

(1) m > 0,

(2) a | m , b | m,

(3) if c∈ Z is any common multiple of a , b then m | c.

Example(1):

Find the +ve common multiple of [-12 , 30]

-12 , 30 = 60 , 120 , 180 , ..

hence [-12 , 30] = 60

Theorem ***1.4.3:***

For any positive integers a , b we find (a , b)[a , b] = a b.

Proof :

Let d = (a , b) so that a = dr and b = ds for r,s ∈ Z .

Let $m = \frac{ab}{d}$. we verify that m satisfy the three conditions of l.c.m.

The first condition obviously satisfied as a > 0 , b > 0 , d > 0 so m > 0 .

Secondly $m = \frac{ab}{d} \Rightarrow m = as = rb$ so a | m , b | m .

To see the condition (3) let c be any positive integer such that a | c , b | c so,

c = au = bv for some u , v Z .

Since d = (a , b) , so ∃ integers x , y such that d = ax + by consequently ,

$$\frac{c}{m} = \frac{c}{\frac{ab}{d}} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = (\frac{c}{b})x+(\frac{c}{a})y=vx+uy.$$

∴ m | c, so m satisfies the third condition for l.c.m.

Thus m = [a , b] i.e. $[a , b]= \frac{ab}{d} = \frac{ab}{(a,b)}$. Hence (a , b) [a , b] = ab.

Example (2):

Find [a , b] if a = 275 , b = 105.

Solution *:*

From example before (275 , 105) = 5. By the above theorem

(275 , 105) [275 , 105] = (275)(105)

5 [275 , 105] = (275)(105)

$$[275 , 105]=\frac{(275)(105)}{5}$$

[275 , 105] = 5775.

Example (**3**):

Proof that the gcd of two positive integers always divides their lcm.

Solution *:*

Let $a , b \in \mathbf{Z}^+$ such that $(a , b) = d$, so $a = a_1 d$ and $b = b_1 d$.By Theorem1.4.3

$(a , b)[a , b] = ab$

$d[a , b] = a_1 b_1 d^2 \qquad (\div\ d)$

$[a , b] = a_1 b_1 d$

so $d \mid [a , b]$

1.5 The Linear Diophantine Equations

Consider the following problem . A man wishes to purchase $510 of travelers checks . The checks are

available only in $20 and $50 . How many of each denomination should he buy ? if we let x denotes the

number $20 checks and y the number of $50 checks , then the equation is

$20x + 50y = 510$ must be satisfied . To solve this problem we need to find all solutions of this equation ,

where x , y are non-negative integers .

From here we have a diophantine equation . Diophantine eqs. get their name from the ancient

Greek mathematician diophantus .

Definition ***1.5.1:***

An equation of the form $ax + by = c$,

where a , b , c Z and a , b are not both zero is called a Linear Diophantine equation in two

variables (unknowns) (if it is solved in integers) .

A solution of this equation is a pair of integers x0 , y0 which when substituted into the equation satisfies it .

A given Linear Diophantine equation may have a number of solutions for ex: the equation

$3x + 6y = 18$ has infinitely many solutions like:

$3.4 + 6.1 = 18$

$3(-6) + 6.6 = 18$

$3(10) + 6(-2) = 18$.

where as the equation $2x + 10y = 17$ which has no solution .

so its reasonable to ask about the conditions under which a solution is possible . The answer

is given by the following theorem .

Theorem ***1.5.2:***

Let a , b be integers with d = (a , b) . The equation $ax + by = c$ has no integral solution if $d \mid c$.

If $d \mid c$ then there are infinitely many integral solutions . Moreover , if $x = x_0$, $y = y_0$ is a particular solution of the equation , then all solutions are given by

$x = x_0 + (b/d)n$, $y = y_0 - (a/d)n$, where n is an integer .

Proof :

Assume that x and y are integers such that $ax+ by = c$. Then since $d \mid a$ and $d \mid b$ so $d \mid c$.

Hence if $d \nmid c$, there are no integral solutions of the equation.

Assume that d\c. Since (a,b)=d $\exists$ s,t Z, such that $d = as + bt$ .....(*)

Since $d \mid c$ there is $e \in Z$ such that $de = c$.

Multiply both sides of (*) by e we get

$c = de = (as + bt)\, e = a(se) + b(te)$.

Hence one solution of the eq. is given by $x=x_0$ and $y=y_0$ where $x_0=se$, $y_0=te$.

Now show that there are infinitely many solutions.

Let $x=x_0 + (b/d)n$ and $y=y_0 - (a/d)n$, $n \in Z$,

we see that the pair (x , y) is a solutions since

$ax + by = a(x_0+(b/d)n) + b(y_0-(a/d)n)$

$= ax0 + a(b/d)n + by0 - b(a/d)n$

$= ax_0 + by_0 = c.$

We now show that every solutions of this equation ax+by=c must be of the form of the theorem .

Suppose x and y are integers with ax+by=c, since $ax_0+by_0=c$, subtracting we get

$(ax+by) - (ax_0+by_0) = 0$

$a(x-x_0) + b(y-y_0) = 0$

$a(x-x_0) = b(y_0-y)$.....(**)

dividing by d

$(a/d)(x-x_0) = (b/d)(y_0-y)$

By theorem (1.2.4) (a/d , b/d)=1.

By lemma (if a,b,c Z^+ , (a , b)=1 and a | bc , then a | c),so (a/d) | (y_0-y) so there is an integer n such that

$(a/d)n = y_0-y$, so $y=y_0-(a/d)n$.

Substituting in (**)

$a(x-x_0) = b(y_0-y)$

$a(x-x_0) = b(a/d)n$,

so $x=x_0+(b/d)n$.

Corollary *1.5.3:*

If (a , b) = 1 and if x_0 , y_0 is a particular solution of the linear Diophantine equation ax+by=c then all other solutions are given by

$x = x_0+bt$, $y = y_0-at$, $t \in Z$.

Example (**1**):

Find the solution of the linear Diophantine equation 15x+6y=7.

Since (15 , 6)=3 , $3 \nmid 7$, it has no integral solution.

Example (**2**):

Find the general solution of the Diophantine equation 172x+20y=1000.

Solution *:*

We first find (127 , 20) by Euclidean Algorithm.

$172 = (20)(8) + 12$

$20 = 12.1 + 8$

$12 = 8.1 + \boxed{4}$

$8 = 4.1 + 0$

$\therefore (172 , 20) = 4.$

Since 4 | 1000 the solution exists.Now express 4 as a linear combination of 172,20, thus we get

$4 = 12-8$

$= 12-(20-12)$

$= 12(2)-20$

$= (172-20(8))(2)-20$

$4 = 172(2) + (20)(-17).$

Multiplying by 250 we get

$1000 = 127(500) + (20)(-4250)$, so $x_0=500$ and $y_0=-4250$,

this is the one particular solution of the given Diophantine equation .

The general solution is given by

$x = 500+(20/4)t = 500+5t$,

$y = -4250 -(127/4)t = -4250 -43t$, $t \in Z$.

Example (3):

Find all positive solutions of the equation $172x + 20y = 1000$

Solution *:*

In Example (2) we found the general solution of the given equation is

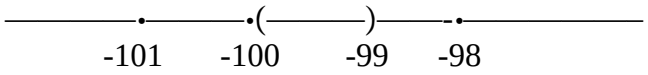
$x = 500 + 5t$ $y = -4250 - 43t,$ $t \in Z$.

For a positive solutions the inequalities

$500 + 5t > 0 \Rightarrow 5t > -500 \Rightarrow t > -100$

$-4250- 43t > 0 \Rightarrow -4250 > 43t \Rightarrow t < -98\frac{36}{43}$

thus $-100 < t < -98\frac{36}{43}$ i.e., $t \in (-100 , -98\frac{36}{43})$.



Since $t \in Z$ $\therefore t = -99.$

$x = 500 + 5(-99) = 5.$

$y = -4250 - 43(-99) = -4250 + 4257 = 7,$

is the only positive solution .

Chapter 2

Theory of Primes

Definition *2.1.1:*

A natural number p> 1 is called a prime number, or simply prime, if 1 and p are its only positive divisors.

A positive integer greater than 1 which is not a prime is called a composite number, or simply composite.

Primes less than 20 are : 2, 3, 5, 7, 11, 13, 17, 19. Note that 2 is the only even prime.Number 1 is regarded

neither prime or composite.

Any prime P which divides a natural n is called a prime divisor of n.

Theorem *2.1.2*

Every natural number n>1, has a prime divisor.

Proof :

Either n is prime or composite, if n is prime then n itself is a prime divisor of n, and there

is nothing left to prove.

If n is composite, then n has a least divisor (d).Certainly d is prime. For if d is not a prime,

then it can be factorized.

Let $d = d_1 d_2$ where $1 < d_1 < d$, $1 < d_2 < d$ and both $d_1 \mid n$,$d_2 \mid n$, this contradicts the choice of d (that it's the least divisor) hence d is a prime.

Lemma *2..1.3:*

If a,b and c are positive integers such that (a, b) = 1 and $a \mid bc$, then $a \mid c$.

Theorem *2.1.4:*

If p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof :

If $p \mid a$, then we need to go no further.

Assume that $p \nmid a$ and prove that $p \mid b$.

Since p is prime (p, a) = 1 hence $\exists$ x, y $\in$ Z, such that

px + a y = 1.

Multiply both sides by b we get

pbx + aby = b.

Since $p \mid pbx$ and $p \mid aby$,so by theorem 1.1.3

$p \mid pbx + aby \Rightarrow p \mid b(px + ay) \Rightarrow p \mid b$.

Lemma *2.1.5:*

It is an extend of more than two terms:

If p is a prime and $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_k$ for some k, where $1 \leq k \leq n$.

Proof :

We prove by induction.

If n = 1 it is obviously follows,

If n = 2 we just proved.

Suppose that n > 2 and whenever p divides a product of less than n factors, then it divides at

least one of the factors.

Let $p \mid a_1a_2 \ldots a_{n-1}a_n$, i.e , $p \mid (a_1a_2 \ldots a_{n-1})a_n$.

By the first part of the theorem, either $p \mid a_n$ or $p \mid a_1a_2 \ldots a_{n-1}$.

If $p \mid a_n$ the result is proved , if $p \mid a_1a_2 \ldots a_{n-1}$ by induction $p \mid a_i$, for some i , $1 \leq i \leq$ n-1,

so in either case if $p \mid a_1a_2 \ldots a_n$, then $p \mid a_i$ for some i where $1 \leq i \leq n$

Corollary *2.1.6:*

If p, q_1 ,q_2,.. ,q_n are primes,such that $p \mid q_1q_2 \ldots q_n$ then $p=q_i$ for some i where $1 \leq i \leq$ n.

Proof :

By theorem above if $p \mid q_1q_2 \ldots q_n$, then $p \mid q_i$ for some i, $1 \leq i \leq n$, but since q_i is prime so

it is not divisible by any natural number except 1 and q_i itself. Since p > 1, we are forced to conclude that $p = q_i$, for $1 \leq i \leq n$.

Theorem *2.1.7*

The Fundamental Theorem of Arithmetic.

Every positive integer greater than one can be written uniquely as a product of primes, with the

prime factors in the product written in order of non-decreasing size.

Proof :

If the integer n is a prime, then the integer itself stands as a product with a single factor and

the theorem is proved.

If n is a composite, then it has a least prime divisor p_i so,

$n = p_1n_1, \quad 1 < n_1 < n.$

If n_1 is a prime we have our representation.

If n_1 is composite then it has a least prime divisor p_2 ,

$n_1 = p_2n_2 , \quad 1 < n_2 < n_1.$

Thus $n = p_1 p_2 n_2 , \quad 1 < n_2 < n_1 < n.$

If n_2 is prime then again we have our representation, otherwise

$n_2 = p_3n_3$, where p_3 is the least prime divisor of n_2 , $1 < n_3 < n_2$.

Thus,

$n = p_1 p_2 p_3 n_3 , \quad 1 < n_3 < n_2 < n_1 < n.$

The decreasing sequence $n > n_1 > n_2 > n_3 > \ldots > 1$,

cannot continue indefinitely, so that after a finite number of steps, n_{k-i} is a prime say p_k .

This leads to the prime factorization, $n = p_1p_2 \ldots p_k$.

To prove uniqueness of the factorization, suppose that n has another representation as a product

of primes say

$n = q_1q_2 \ldots q_s$, so

$$p_1p_2 \ldots p_k = q_1q_2 \ldots q_s.$$

We cancel the common prime factors of any of the two sides of the above equation, remove them (if necessary) and get,

$$p_1p_2 \ldots p_i = q_1q_2 \ldots q_j \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where $i \geq 1$, $j \geq 1$, all the p's are different from the q's. Since p_1 divides the L.H.S of (1) so

it must divide the R.H.S of (1) as well i.e,

$p_1 \mid q_1 q_2 \ldots q_j \Rightarrow p_1 = q_r$ for some r where, $1 \le r \le j$ by corollary 2.1.6.

This contradicts the fact that all the p's are different from q's.

Hence the assumption that n can be represented as product of primes in two different ways

is wrong and so the representation is unique .

Note that:

It is not necessary that all primes in the factorization of n be distinct, suppose that p_1 occurs α_1 times, p_2 occurs α_2 times, ...,p_k occurs α_k times then,

$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $p_1 < p_2 < p_3 \ldots < p_k$, $\alpha_i \in Z^+$, $1 \le i \le k$.

This is called the standard form or canonical form of n.

Example (1):

Take (i) $n = 240 = 2.2.2.2.3.5 = 2^4.3.5$.

(ii) $n = 289 = 17.17 = 17^2$.

(iii) $n = 1001 = 7.11.13$

(iv) $n = 17640 = 2.2.2.3.3.5.7.7 = 2^3.3^2.5^1.7^2$.

How prime factorization can be used to find gcd.

Let min (a, b) denote the smaller or minimum of the two numbers a and b. Now let the prime factorization of a and b be

$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$.

So we note the gcd of a, b to be

$$(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \ldots p_n^{\min(a_n,b_n)}.$$

Since for each prime p_i, a and b share exactly $\min(a_i, b_i)$ factors of p_i.

Example (2):

$2484 = 2^2.3^3.23^1$, $3960 = 2^3.3^2.5.11$.

So, $(2484, 3960) = 2^2.3^2 = 36$.

Similarly the lcm of a, b is seen to be

$$[a, b] = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \ldots p_n^{\max(a_n,b_n)}.$$

Where max (a,b) denotes the larger or maximum of a and b.

Example (3):

(i) $24 = 23.3$

$36 = 22.32$

$\therefore [24, 36] = 23.32 = 72$.

(ii) $15 = 3.5$

$21 = 3.7$

$\therefore [15,21] = 3.5.7 = 105$.

Lemma *2.1.8:*

If x and y are real numbers, then max (x, y) + min (x.y) = x+y

Proof :

If $x \ge y$ then min (x, y) = y and max (x,y) = x.

So, max (x, y) + min (x,y) = x + y.

If x < y then min (x, y) = x and max (x, y) = y.

then, max (x, y) + min (x. y) = x + y.

Lemma *2.1.9*

Let m and n be relatively prime positive integers . Then if d is a positive divisor of m n, there is

a unique pair of positive divisor d_1 of m and d_2 of n such that $d = d_1 d_2$.

Conversely, if d_1 and d_2 are positive divisors of m and n respectively, then $d = d_1 d_2$ is a positive divisor of m.n .

Proof :

Let the prime power factorization of m and n be

$m = p_1^{m_1} p_2^{m_2} \ldots\ldots\ldots\ldots p_s^{m_s}$, $\quad n = q_1^{n_1} q_2^{n_2} \ldots\ldots\ldots\ldots q_t^{n_t}$.

Since (m, n) = 1, so $p_1^{m_1}, p_2^{m_2}, \ldots\ldots\ldots, p_s^{m_s}, q_1^{n_1}, q_2^{n_2}, \ldots\ldots\ldots, q_t^{n_t}$ have no common elements.

Therefore the prime factorization of mn is

$$mn = p_1^{m_1} p_2^{m_2} \ldots\ldots\ldots\ldots p_s^{m_s} q_1^{n_1} q_2^{n_2} \ldots\ldots\ldots\ldots q_t^{n_t}.$$

If d is a positive divisor of mn, then

$d = p_1^{e_1} p_2^{e_2} \ldots\ldots\ldots\ldots p_s^{e_s} q_1^{f_1} q_2^{f_2} \ldots\ldots\ldots\ldots q_t^{f_t}$,

where $0 \le e_i \le m_i$ for i = 1, 2, ., s , $0 \le f_j \le n_j$ for j = 1, 2, ...t.

Let $d_1 = (d, m)$ and d_2 (d, n) , so

$d_1 = p_1^{e_1} p_2^{e_2} \ldots\ldots\ldots\ldots p_s^{e_s}$, $d_2 = q_1^{f_1} q_2^{f_2} \ldots\ldots\ldots\ldots q_t^{f_t}$.

So, $d = d_1 d_2$ and $(d_1 , d_2) = 1$.

The uniqueness will left as an excersise .

Conversely let d_1, d_2 be positive divisors of m, n respectively then

$d_1 = p_1^{e_1} p_2^{e_2} \ldots\ldots\ldots\ldots p_s^{e_s}$, $\quad 0 \le e_i \le m_i$ $\quad$ for i = 1, 2, ...s,

$d_2 = q_1^{f_1} q_2^{f_2} \ldots\ldots\ldots\ldots q_t^{f_t}$, $0 \le f_j \le n_j$ $\quad$ for j = 1, 2, ...t.

$\therefore d = d_1 d_2 = p_1^{e_1} p_2^{e_2} \ldots\ldots\ldots\ldots p_s^{e_s} q_1^{f_1} q_2^{f_2} \ldots\ldots\ldots\ldots q_t^{f_t}$,

is clearly a divisor of m n ,where $mn = p_1^{m_1} p_2^{m_2} \ldots\ldots\ldots\ldots p_s^{m_s} q_1^{n_1} q_2^{n_2} \ldots\ldots\ldots\ldots q_t^{n_t}$,

since the power of such prime occurring in the prime power factorization of d is less than

or equal to the power of that prime in the prime power factorization of m n.

Definition ***2.1.10:***

An integer is said to be square free if it is not divisible by the square of any integer greater than 1.

This means that if

$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots\ldots p_r^{\alpha_r}$

is square free then none of the α_i is greater than 1 i.e., $0 \le \alpha_i \le 1$.

Determination of Primality:

In order to determine whether a given integer is prime or not, we make use of the following theorem:

Theorem ***2.1.11***

Every composite natural number n has a prime divisor $\le \sqrt{n}$.

Proof :

Since n is composite , it has a least prime divisor p, (Theorem 2.1.2), then

$n = n_1 p$. We must have $p \le \sqrt{n}$. For if $p > \sqrt{n}$, then $n = n_1 p$ shows that

$n_1 < \sqrt{n} < p$ i.e, $\exists$ a divisor of n less than the least, which is a contradiction hence $p \le \sqrt{n}$.

From Theorem 2.1.11, we see that in order to find out whether a given integer n is a prime or not ,

we divide it by primes 2, 3,5 ,7, ..., p where p is the largest prime $\le \sqrt{n}$, if none of these primes divide n, then n is a prime.

Example 4:

Determine whether 2093 is prime or composite.

Solution *:*

$\sqrt{2093} \simeq 45.75$

$45 < \sqrt{2093} < 46.$

Primes less than 46 are:

2,3,5,7,11,13,17,19,23,29,31,37,41,43

$2 \nmid 2093$, $3 \nmid 2093$, $5 \nmid 2093$ but $7 \mid 2093$ since $2093 = 7 \times 299 \Rightarrow$ 2093 is composite .

Example (**5**):

Determine whether 563 is prime or composite.

Solution *:*

$\sqrt{563} \simeq 23.73$

$23 < \sqrt{563} < 24.$

Primes less than 24 are: 2,3,5,7,11,13,17,19,23

none of these primes divide 563 , so 563 is prime.

2.2: The Sieve of Eratosthenes

In order to find all primes $\leq$ n where $n \in Z^+$, write down all numbers from 2 to n. Then we cancel all the proper multiples of the primes up to $\sqrt{n}$. In this process those numbers which are not cancelled are primes.

Example (6):

Find all primes less than 100.

Solution *:*

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primes up to $\sqrt{100}$ are 2, 3, 5, 7 so we cancel their multiples from the list, so only the following numbers are left :

2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97

which are primes .

Theorem ***2.2.1: Euclids theorem:***

There are an infinite number of primes.

Proof :

The proof will be by contradiction:

Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, be primes in ascending order, and suppose that there is a

last prime p_n. Consider the positive integer p such that : $p = p_1 p_2 \ldots . p_n + 1$,

since $p > 1$ by Theorem 2.1.7, then p is divisible by some prime k, but $p_1, p_2, \ldots . , p_n$ are the

only prime numbers, so that k must be equal to one of $p_1, p_2, \ldots . , p_n$ i.e.$k = p_i$,

where $1 \leq i \leq n \Rightarrow k \mid p_1, p_2, \ldots . , p_n$.

combining the relation $k \mid p_1, p_2, \ldots . , p_n$ with $k \mid p$, then

$k \mid p\text{-}p_1, p_2, \ldots . , p_n \Rightarrow k \mid 1$.The only positive divisor of 1 is 1 itself and since $p > 1$, a contradiction arises. Thus no finite list of primes is complete, so the number of primes is in infinite .

- Let p_n denotes the n^{th} prime number in their natural order. If the next prime is p_{n+1}, then it is easy to see that

$$p_{n+1} \leq p_1 p_2 \ldots . p_n + 1 < p_n^n + 1.$$

For example if n = 3 then

$p_4 = 7 < p_3^3 + 1 = 5^3 + 1 = 126$,

$7 < 31 < 126$.

Theorem ***2.2.2:***

If p_n is the n^{th} prime number, then $p_n \leq 2^{2^{n-1}}$.

Proof :

We prove the theorem by induction.
The given inequality is true for n = 1 as
$2 = p_1 = 2^{2^{1-1}} = 2^{2^0} = 2.$
Let the theorem be true for all integers up to n = k i.e. $p_k \leq 2^{2^{k-1}}$.
Now, $p_{k+1} \leq p_1 p_2 p_k + 1$

$\leq 2^1 2^2 \ldots\ldots\ldots 2^{2^{k-1}} + 1$

$\leq 2^{1+2+2^2+2^3+\ldots..2^{k-1}} + 1$

From identity $1+2+2^2+....+2^{k-1} = 2^k - 1$,

$p_{k+1} \leq 2^{2^{k-1}} + 1$

$\leq 2^{2^{k-1}} + 2^{2^{k-1}}$ (since $1 \leq 2^{2^{k-1}} \quad \forall k \in \mathbf{Z}^+$)

$\leq 2.\ 2^{2^{k-1}}$

$p_{k+1} \leq 2^{2^k}$.
Completing the induction step and the proof .

Theorem ***2.2.3:***

The number $\sqrt{2}$ is irrational.

Proof :

To prove that $\sqrt{2}$ is irrational is equivalent to proving that $\sqrt{2} \neq a/b$ for any $a,b \in Z$ i.e,
the equation $a^2 = 2b^2$, has no solution in Z. We can assume without any loss of generality
that (a,b) = 1, thus in particular both of them are not even. Both of them cannot be odd either thus one of them is odd an the other is even. Clearly a is even , b is odd , let a = 2c , $c \in Z$ then,
$4c^2 = 2b^2 \quad \Rightarrow \quad 2c^2 = b^2$
$\Rightarrow$ b^2 is even $\Rightarrow$ b is even,
which is a contradiction of the fact that b is odd.
Thus the equation $a^2 = 2b^2$ has no solution in Z , i.e. $\sqrt{2} \neq a/b$ for any $a, b \in Z$
i.e. $\sqrt{2}$ is irrational .

Lemma ***2.2.4:***

The product of two or more integers of the form 4n + 1 is of the same form.

Proof :

Let $k = 4n + 1, \quad k' = 4m + 1$
Then $kk' = (4n + 1)(4m + 1)$
$= 16\ mn + 4n + 4m + 1$
$= 4\ (4mn + n + m) + 1$
$= 4L + 1$, where $L = 4mn + n + m$.

Which is of the desired form.

Theorem *2.2.5:*

There is an infinite number of primes of the form 4n + 3.

Proof :

In anticipation of a contradiction , let us assume that there exist only finitely many primes

of the form 4n+3 , call them $q_1, q_2, \ldots\ldots, q_s$. Consider the positive integer

$N = 4\, q_1\, q_2 \ldots\ldots\, q_s - 1 = 4\,(q_1\, q_2 \ldots\ldots\, q_s - 1) + 3,$

and let $N = r_1 . r_2 \ldots\, r_t$ be its prime factorization .

Because N is an odd integer, we have $r_k \neq 2$ for all k , so that each r_k is either of the form

4n+1 or 4n+3.By the lemma above for N take the form 4n+3 as its clearly dose,

N must contain at least one prime factor r_i of the form

4n+3. But r_i cannot be found among the listing $q_1, q_2, \ldots\ldots, q_s$, for this would lead to a contradiction that $r_i \mid 1$.

The only possible conculosion is that there are infinitly many primes of the form 4n+3 .

Theorem *2.2.6: (Dirichlet)*

If a and b are relatively prime positive integers i.e (a, b) = 1 , then the arithmetic progression

a, a + b, a + 2b, a + 3 b

contains infinitely many primes.

Example(6):

(3, 4) = 1 , therefore the arithmetic progression is

3, 3 + 4 , 3+ 2(4) ,3+ 3(4) , 3 + 4(4), 3 + 5(4),.....

i.e, the arithmetic progression is 3, 7, 11, 15, 19, 23, ...

contains infinitely many primes all of them are of the form 4n + 3.

Similarly (1, 4) = 1 therefore the arithmetic progression is :

1, 1 + (4) , 1+ 2(4), 1 + 3(4), 1 + 4(4), 1 + 5(4) ,..... ,i.e. 1, 5, 9, 13, 17, 21,.....

contains infinite number of primes of the form 4n + 1 .

Theorem *2.2.7:*

No Arithmetic progression of the form a, a + b , a + 2b, contains only primes.

Proof :

Let a + nb = p where p is a prime.

If we put $n_k = n + kp$, k = 1, 2, 3,..., then the n_k^{th} term in the progression is

$$\begin{aligned} a + n_k\, b &= a + (n + kp)\, b \\ &= a + nb + kpb \\ &= p + kpb \\ &= p\,(1 + kb) \quad \Rightarrow \quad p \mid a + n_k\, b, \end{aligned}$$

$\Rightarrow a + n_k\, b$ is composite, this means that the progression must contain infinitely many composite numbers.

2.3 Fermat Factorization

Lemma *2.3.1:*

If n is an odd positive integer ,then there is a 1–1 correspondence between factorization of

n into two positive integers and difference of two squares that equal n.

Proof :

Let n be an odd positive integer and let,

$n = ab$ be a factorization of n into two positive integer.

Then n can be written as a difference of two squares since

$n = ab = s^2 - t^2$

where, $s = (a + b)/2$, $t = (a - b)/2$ are both integers, since a,b are both odd.

Conversely if n is the difference of two squares say:

$n = s^2 - t^2$ then,we can factor n to

$n = (s - t)(s + t)$.

I will leave the proof a 1-1 correspondence to you.

To carry out the method of Fermat factorization, we look for the solution of the equation

$n = x^2 - y^2$ by searching for perfect squares of the form $x^2 - n$ hence to find F.F of n we search for among the sequence of integers.

$t^2 - n, (t + 1)^2 - n, (t + 2)^2 - n,$.....,

where t is the smallest integer greater than $\sqrt{n}$ which leads to the equation

$n = (n + 1)^2/2 - (n - 1)^2/2$.

Example (8):

Use Fermat factorization to factor 6077.

$\sqrt{6077} = 77.96$

$77 < \sqrt{6077} < 78$.

So $t = 78$ then,

$$t^2 - n = (78)^2 - 6077 = 7$$
$$(t+1)^2 - n = (79)^2 - 6077 = 164$$
$$(t+2)^2 - n = (80)^2 - 6077 = 323$$
$$(t+3)^2 - n = (81)^2 - 6077 = 484 = 22^2$$

So,
$$6077 = (81)^2 - (22)^2$$
$$= (81 - 22)(81 + 22)$$
$$= 59\,(103).$$

Example (9):

Use F.F to factor 23449

$\sqrt{23449} = 153.13$

$153 < \sqrt{23449} < 154$

So $t=154$ then,

$$t^2 - n = (154)^2 - 23449 = 267$$
$$(t+1)^2 - n = (155)^2 - 23449 = 576 = (24)^2$$
$$23449 = (155)^2 - (24)^2$$
$$= (155 - 24)(155 + 24)$$
$$= 131\,(179).$$

Fermat's Numbers.

The numbers of the form :

$$F_n = 2^{2^n} + 1,$$

are known as Fermats numbers. Fermat conjectured that for $n \geq 1$, the numbers F_n are all primes and he proved that $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$

are primes. Euler , however found in 1732 that

$F_5 = 2^{2^2} + 1 = 2^{32} + 1 = 4294967297,$

$= 641 \times 6700417,$

is composite because it is divisible by 641, 6700417.

In 1880 , Landry proved that

$F_6 = 2^{2^6} + 1 = 2^{64} + 1 = 274177 \times 67280421310721.$

In fact no prime F_n has been founded beyond F_4 , so the Fermat conjecture has not proved

a happy one.An interesting property of Fermats numbers is displayed by the following theorem.

Theorem *2.3.2*

Any two Fermats numbers are relatively prime.

Proof :

Let F_n , F_{n+k} $(n, k \in Z^+)$ be two Fermats numbers and let

$m \mid F_n$, $m \mid F_{n+k}$.

Consider $$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1}$$

$$= \frac{2^{2^n 2^k} - 1}{2^{2^n} + 1}$$

$$= \frac{(2^{2^n})^{2^k} - 1}{2^{2^n} + 1}$$

$$= \frac{x^{2^k} - 1}{x + 1} \qquad \text{where } x = 2^{2^n}$$

$$= x^{2^k-1} - x^{2^k-2} + x^{2^k-3} - x^{2^k-4} + \ldots\ldots\ldots - 1$$

$\Rightarrow F_n \mid F_{n+k} - 2.$

Now since $m \mid F_n$, therefore $m \mid F_{n+k} - 2, \Rightarrow m \mid F_{n+k} - (F_{n+k} - 2)$,

$\Rightarrow m \mid 2$ but F_n, F_{n+k} are both odd numbers therefore m is odd,

and since $m \mid 2$ so, $m = 1$. Hence $(F_n , F_{n+k}) = 1$.

2.4 Mersenne Numbers

Definition *2.4.1*

If n is a positive integer and $\sigma(n) = 2n$, then n is called a prefect number.

The integers that are equal to the sum of all their proper positive divisors are called perfect numbers.

Example (10):

Since $\sigma(6) = 1 + 2 + 3 + 6 = 12$.

Also $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$,

so that 6, 28 are perfect numbers.

Theorem *2.4.2:*

The positive integer n is an even perfect number iff

$$n = 2^{m-1}(2^m - 1),$$

where m is an integer such that $m \geq 2$ and $2^m - 1$ is prime.

Theorem *2.4.3:*

If m is a positive integer and $2^m - 1$ is prime, then m must be prime.

Proof :

Assume that m is not prime, so that m = a.b where $1 < a < m$ and $1 < b < m$, then

$$2^m - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \ldots\ldots + 2^a + 1).$$

Since both factors on the R.H.S of the equation are greater than 1, we see that $2^m - 1$ is composite if m is not prime.

Therefore if $2^m - 1$ is prime, then m must be also prime .

Definition *2.4.4:*

If m is a positive integer, then $M_m = 2^m - 1$ is called the m^{th} Mersenne number, and if p is prime and $M_m = 2^p - 1$ is also prime then M_p is called a Mersenne prime.

Example (11):

The Mersenne number $M_7 = 2^7 - 1 = 127$ is prime, where the Mersenne number $M11 = 211 - 1 = 2047 = 23.89$ is composite.

Theorem *2.4.5:*

If p is an odd prime, then any divisor of the Mersenne number $M_p = 2^p - 1$ is the form $2kp + 1$ where k is a positive integer.

Example (12):

Decide whether M_{13} is prime.

Solution *:*

we look for a prime factor not exceeding $\sqrt{8191}$.

$M_{13} = 2^{13} - 1 = 8191$.

$\sqrt{8191} \simeq 90.504$

Any such divisor (by Theorem 2.4.5) will be of the form 26k + 1.The only candidates primes dividing M_{13} less than or equal to $\sqrt{M_{13}}$ are :

$26 \times 1 + 1 = 27$ not prime,

$26 \times 2 + 1 = 53$ prime, but $53 \nmid 8191$,

$26 \times 3 + 1 = 79$ prime, but $79 \nmid 8191$, so M_{13} is prime.

Example (13):

Show that a positive integer n >1 is a perfect square iff all the exponents in the standard form of n are even.

Solution *:*

Let n be a perfect square say $n = m^2$.

$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_r^{\alpha_r}$ be the standard form of m.

$\therefore n = m^2 = (p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_r^{\alpha_r})^2,$

$= p_1^{2\alpha_1} p_2^{2\alpha_2} \ldots\ldots\ldots p_r^{2\alpha_r},$

and all the exponents in the standard form of n are even.

Suppose conversely that

$n = p_1^{2\alpha_1} p_2^{2\alpha_2} \ldots\ldots\ldots p_r^{2\alpha_r},$

$n = (p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_r^{\alpha_r})^2,$

$= m^2$.

Example (14):

Use **Example (13)** to prove that $\sqrt{2}$ is irrational.

Solution *:*

As we have seen, to prove that $\sqrt{2}$ is irrational is equivalent to prove that $a^2 = 2b^2$ has no solution for $a, b \in Z$.

For if $b = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_r^{\alpha_r}$, then

$a^2 = 2^1 p_1^{2\alpha_1} p_2^{2\alpha_2} \ldots\ldots\ldots p_r^{2\alpha_r},$

is impossible since all the exponents of the prime factors on the R.H.S. of the above equation

are not even.Thus there do not exist $a, b \in Z$ such that $a^2 = 2b^2$,

i.e. such that $a^2 / b^2 = 2$ i.e. such that $a/b = \sqrt{2} \Rightarrow \sqrt{2}$ is irrational.

Example (15):

If $p \geq 5$ is a prime number, show that $p^2 + 2$ is composite.

Solution *:*

If $p \geq 5$ is prime number then its either of the form $6k + 1$ or $6k + 5$.

If $p = 6k + 1$, then,

$P^2 + 2 = (6k + 1)^2 + 2$

$= 36k^2 + 12k + 3 = 3 (12k^2 + 4k + 1)$

$\Rightarrow p^2 + 2$ is composite

If $p = 6k + 5$, then

$p^2 + 2 = (6k + 5)^2 = 36k^2 + 60k + 9 = 3 (12k^2 + 20k + 5)$

$\Rightarrow p^2 + 2$ is composite .

Example(16):

If $p = 2^k - 1$ for $k \geq 3$ is prime show that k is an odd integer.

Solution *:*

If k is even , say $k = 2n$ then $n \geq 2$.

$2^k - 1 = 2^{2n} - 1$

$= (2^n)^2 - (1)^2$

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

Since $n \geq 2$, therefore $2^n - 1 > 1, \quad 2n + 1 > 1,$

$\Rightarrow 2^k - 1$ is composite which contradicts the hypothesis that $2^k - 1$ is prime

hence k must be odd.

Example (17):

If p is prime , show that $p \mid \binom{p}{i}$, $1 \le i \le p - 1$.

Solution *:*

$$\binom{p}{i} = \frac{p!}{(p-i)!i!}$$

$$= \frac{p(p-1)(p-2)\ldots(p-(i-1))(p-i)!}{(p-i)!i!}$$

$$= \frac{p(p-1)(p-2)\ldots(p-(i-1))}{i!}$$

The numerator of the R.H.S of the above equation is the product of i consecutive integers and

so is divisible by i!.

But since p is prime and $i < p$, so $k \nmid p$ for any integer k satisfying $2 \le k \le i$,thus

$i! \mid (p - 1)(p - 2) \ldots (p - (i - 1))$,

$$\Rightarrow \binom{p}{i} = pA, \quad \text{where}$$

$$A = \frac{p(p-1)(p-2)\ldots(p-(i-1))}{i!}.$$

So, $p \mid \binom{p}{i}$, $1 \le i \le p - 1$.

Definition ***2.4.6***

Prime pairs p and p + 2 , where p is a prime are called twin primes.

For example: 3,5, 5,7, 11,13, 17,19 are twin primes.

Example (18):

Show that if 1 is added to a product of twin primes, a perfect square is always obtained.

Solution *:*

Let p, p + 2 be twin primes.

$p(p + 2) + 1 = p^2 + 2p + 1$

$= (p + 1)^2$.

Example (19):

Prove that any prime of the form 3n + 1 is also of the form 6n + 1.

Solution *:*

Let p a prime of the form 3n + 1 then n must be even for if n is odd, then 3n + 1 is even i.e , composite.

Hence $n = 2k \Rightarrow p = 3n + 1 = 6k + 1$

$= 3(2k) + 1$.

Chapter 3

The Theory of Congruences

3.1 : Introduction to Congruences.

The special language of congruences that we introduce in this chapter is extremely useful in

number theory. This language of congruences was developed at the beginning of the 19^{th}

century by Karl Friedrich Gauss. One of the most famous mathematicians in history.

Definition ***3.1.1:***

Let m be a positive integer if a and b are integer we say that a is congruent to b modulo m if m | (a- b).

If a is congruent to b modulo m, we write $a \equiv b \pmod{m}$.

If m ∤ (a - b), we write $a \equiv b \pmod{m}$, and say that a and b are incongruent module m.

Example(1):

We have $22 \equiv 4 \pmod 9$, since 9 | 22 - 4 .

Likewise $3 \equiv -6 \pmod 9$ and $200 \equiv 2 \pmod 9$. On the other hand $13 \equiv 5 \pmod 9$ since 9∤ 13 -5 .

Congruences often arise in everyday life. For instance, clocks work either modulo 12 or 24 for

hours, and modulo 60 for minutes and seconds, calendars work modulo 7 for days.

Theorem ***3.1.2:***

If a and b are integers then $a \equiv b \pmod m$ iff there is an integer k such that a = b + k m.

Proof :

If $a \equiv b \pmod m$, then m | (a - b). This means that there is an integer k with km = a - b, so that a = km + b.

Conversely if there is an integer k with a = b + km, then km = a - b, hence m | (a - b),

and consequently $a \equiv b \pmod m$.

Example(2):

We have $19 \equiv -2 \pmod 7$ and 19 = -2 +3.7 .

Remark 3.1.3

(1) Any two integers are congruent modulo 1. i.e. , $a \equiv b \pmod 1$ ∀ a, b∈ Z ,

since 1 | a - b i. e , every integer is divisible by 1.

(2) (i) $a \equiv 1 \pmod 2$ if a is odd.

(ii) $a \equiv 0 \pmod 2$ if a is even.

(iii) $a \equiv b \pmod 2$ if a & b are of the same parity i. e, both of them are odd or both of them are even.

3.2 : Congruent classes and complete Residue system:

Given an integer a , we get by division algorithm

$a = qm + r \qquad 0 \le r \le m - 1 < m.$

This mean that if the integer a is divided by m , the possible remainders are : 0 , 1 , 2 ,,m - 1.

Thus the set of integer is partitioned into m subsets

C_0 , C_1, C_2 , ..., C_{m-1} , which we call the **Congruence Classes modulo m** .

C_0 consists of all those integers which leave the remainder 0 when divided by m ,

i.e , the multiples of m . C_1 consists of all those integers which leave the remainder 1 when divided by m. They are integers of the form $mq + 1$, $q \in Z$.

In general $C_i = mq + i$, $i = 0 , 1 ,2 ,....., m- 1$.

This set { 0 , 1 , 2 , , m - 1} is called the set of least non- negative residues (mod m).

Example (3) :

Take m = 4 , then the set of integer is partitioned or divided into four congruence classes :

$C_0 = 4q + 0$ i.e. ,.....- 8 ≡ - 4 ≡ 0 ≡ 4 ≡ 8.....(mod 4)

$C_1 = 4q +1$ i.e. ,.....-7 ≡ -3 ≡ 1 ≡5 ≡ 9.....(mod 4)

$C_2 = 4q + 2$ i.e. ,.....-6 ≡-2≡ 2≡ 6≡ 10.....(mod 4)

$C_3 = 4q +3$ i.e.,.....-5 ≡ -1≡ 3≡ 7 ≡11.....(mod 4).

Here the set of least non-negative residues (mod 4) is { 0, 1 , 2, 3} .

If we take any integer ,then clearly it will belong to one of the congruences classes $C_0 , C_1 , C_2 ,.... C_{m-1}$ modulo m.

We can say that it will be congruent to either 0, 1, 2,.., or m - 1 (mod m). If we take an arbitrary element from each congruence class, $C_0, C_1 , ... C_{m-1}$ modulo m , then we have a set called the **complete residue system (mod m)**.

We formally define it as follows.

Definition ***3.2.1:***

If a_i is an arbitrary element of the congruence class C_i for $i = 0, 1 , 2 ,..,m-1$.

Then the set $A = \{ a_0,a_1,a_2, ...,a_{m-1}\}$ is called a complete residue system (mod m),and will be usually written as C.R.S. (mod m) .

It is straightforward to see that if A is a C.R.S (mod m), then it has the following properties :

i) A has m elements.

ii) No two elements of A are congruent (mod m)

(If they are then they belong to the same congruence class (mod m))

Example (4):

Take m = 7, then the congruence classes (mod 7) are:

$C_0 = 7q + 0$

$C_1 = 7q + 1$

$C_2 = 7q + 2$

$C_3 = 7q + 3$

$C_4 = 7q + 4$

$C_5 = 7q + 5$

$C_6 = 7q + 6$.

The set of least non-negative residue (mod 7) is {0, 1, 2, 3, 4, 5, 6}.

If we take an arbitrary element from each congruence class $C_0,C_1,C_2,C_3,C_4,C_5,C_6$ (mod 7),

then we have a set of C.R.S. (mod 7). One such set is A= {7, 15, 9, 24, 18, 40, 13}.

This set has seven elements & no two elements are congruent to each other (mod 7) to exactly one element of { 0 , 1 ,2, 3 ,4, 5, 6}.

Theorem ***3.2.2:***

For any two integer a and b, $a \equiv b$ (mod m) iff a & b leave the same non-negative remainder when divided by m.

Proof :

Suppose $a \equiv b$ (mod m) so $a = b + km$, $k \in Z$.

Suppose that b leaves the remainder r when divided by m so

$b = q m + r$, $q \in Z , 0 \leq r < m$.

Now $a = b + k\,m$

$= q\,m + r + k\,m$

$= (q + k)\,m + r$,

which means that a also leaves the remainder r when divided by m.

Suppose conversely, that a & b leave the same remainder after division by m. Then

$a = q_1\,m + r$ & $b = q_2\,m + r$, $0 \le r < m$, $q_1, q_2 \in Z$,

$\therefore a - b = (q_1 - q_2).m \Rightarrow m \mid a - b$,

or $a \equiv b \pmod m$.

Example (5):

Since $58 = 8.7 + 2$, $16 = 2.7 + 2$ i.e , 58 & 16 leave the same remainder 2 , after division by 7,

therefore $58 \equiv 16 \pmod 7$,

i.e, 58 & 16 are in the same congruence class (mod 7).

Theorem *3.2.3:*

Congruence is an equivalence relation.

Let $m \in Z^+$ & $a,b,c,d \in Z$. Then the following properties hold :

1) $a \equiv a \pmod m$, reflexive property.

2) If $a \equiv b \pmod m$ then $b \equiv a \pmod m$, symmetric property.

3) If $a \equiv b \pmod m$, $b \equiv c \pmod m$, then $a \equiv c \pmod m$, transitive property.

4) If $a \equiv b \pmod m$ & $c \equiv d \pmod m$, then $a - c \equiv b - d \pmod m$ and $a + c \equiv b + c \pmod m$.

5) If $a \equiv b \pmod m$, then $a + c \equiv b + c \pmod m$ and $ac \equiv bc \pmod m$ for any $c \in Z$.

6) If $a \equiv b \pmod m$, then $a^n \equiv b^n \pmod m$, for any positive integer n.

Proof :

1. For any $a \in Z$, we have $m \mid a - a$ i.e., $m \mid 0 \Rightarrow a \equiv a \pmod m$.

2. If $m \mid a - b$, then $m \mid b - a$. Therefore if $a \equiv b \pmod m$, then $b \equiv a \pmod m$.

3. $a \equiv b \pmod m \Rightarrow a - b = km$ or $a = b + km$, $k \in Z$,

$b \equiv c \pmod m \Rightarrow b - c = qm$ or $b = c + qm$, $q \in Z$.

$\therefore a = c + q\,m + k\,m$

$a = c + (q + k)\,m \Rightarrow a \equiv c \pmod m$.

4. $a \equiv b \pmod m \Rightarrow a = b + k\,m$ .....(1)

$c \equiv d \pmod m \Rightarrow c = d + q\,m$ .....(2)

subtracting (1) & (2) we get

$a - c = (b - d) + (k - q)\,m$,

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

Adding (1) & (2)

$a + c = (b + d) + (k + q)\,m$,

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

Also

$ac = (b + km)(d + qm)$,

$= bd + (bq + dk + kqm)\,m$

$\Rightarrow ac \equiv bd \pmod m$.

5. $a \equiv b \pmod m \Rightarrow a = b + k\,m$,

$\therefore a + c = b + c + km$,

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

Also

$ac = bc + ckm$,

$= bc + (ck)m$

$\Rightarrow ac \equiv bc \pmod m$.

6. It will be proved by induction given that $a \equiv b \pmod m$ i.e, the statement is true for n=1.

Let it be true for n=k i.e., $a^k \equiv b^k \pmod m$, $k \in Z^+$, $k > 1$,

then

$a^k \equiv b^k \pmod m$.

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

$\therefore$ $a^{k+1} \equiv b^{k+1} \pmod m$ by (4) in the theorem, so its true for n = k+ 1, so its true for all $n \in Z^+$.

Example (6):

Since $19 \equiv 3 \pmod 8$), then

(1) $19 + 7 \equiv 3 + 7 \pmod 8$,

$\Rightarrow$ $26 \equiv 10 \pmod 8$.

(2) $19 - 4 \equiv 3 - 4 \pmod 8$,

$\Rightarrow$ $15 \equiv -1 \pmod 8$.

(3) $19.2 \equiv 3.2 \pmod 8$,

$\Rightarrow$ $38 \equiv 6 \pmod 8$.

Example (7) :

Use congruence to show that 41 divides $2^{20} - 1$.

Solution *:*

we have to prove that, $2^{20} - 1 \equiv 0 \pmod{41}$, or $2^{20} \equiv 1 \pmod{41}$.

To begin we select a power of 2 which gives an integer near to 41. To this end we have,

$2^5 \equiv -9 \pmod{41}$

$\therefore (2^5)^4 \equiv (-9)^4 \pmod{41}$

$2^{20} \equiv (81)^2 \pmod{41}$

Also we observe that

$81 \equiv -1 \pmod{41}$

$(81)^2 \equiv (-1)^2 \pmod{41}$

$(81)^2 \equiv 1 \pmod{41}$

$2^{20} \equiv (81)^2 \pmod{41}$ & $(81)^2 \equiv 1 \pmod{41}$, by Theorem 3.2.3 part (3) we have

$2^{20} \equiv 1 \pmod{41} \Rightarrow 41 \mid 2^{20} - 1$.

Example (8):

Find the remainder obtained when the sum $1! + 2! + 3! + .. + 100!$ is divided by 12.

Solution *:*

we have $4! = 24$ & $24 \equiv 0 \pmod{12}$.

Thus for $k \geq 4$, we have

$k! = 1.2.3.4.5.....k$

$= 4!.5.6.....k$

$\equiv 0 \pmod{12}$,

$\therefore 1! + 2! + 3! + 4! + 5! + ...+100! \equiv 1! + 2! + 3! + 0 + 0 + ...+0 \pmod{12}$,

$\equiv 1 + 2 + 6 \pmod{12}$,

$\equiv 9 \pmod{12}$.

Thus the remainder is 9 when the sum $1! + 2! + 3! + .+100!$ is divided by 12.

Example (9):

We have $14 \equiv 8 \pmod 6$

$7.2 \equiv 4.2 \pmod 6$ but we cannot cancel the common factor of 2

since $7 \equiv 4 \pmod 6$.

So it is not necessarily true that we preserve a congruence when we divide both sides by an integer. The true converse of this result is the following theorem.

Theorem ***3.2.4:***

If a,b,c and m are integers such that m > 0 , d=(c,m) and $ac \equiv bc \pmod m$, then $a \equiv b \pmod{m/d}$.

Proof :

If $ac \equiv bc \pmod m$, we know that $m|(ac - bc) \Rightarrow m \mid c(a - b)$.

Hence there is an integer k with $c(a - b) = km$. Dividing both sides by d, we have

$(c/d)(a-b)=k(m/d), \quad \Rightarrow \quad m/d \mid (c/d)(a-b)$.

Since $(m/d, c/d) = 1$, by Theorem 1.2.7. it follows that $(m/d) \mid (a - b)$.

Hence $a \equiv b \pmod{m/d}$.

Example(10):

Since $50 \equiv 20 \pmod{15}$ and $(10, 15) = 5$ we see that

$50/10 \equiv 20/10 \pmod{15/5}$ or $5 \equiv 2 \pmod 3$.

Corollary ***3.2.5:***

If a , b, c & m are integers such that m > 0 , $(c, m) = 1$ and $ac \equiv bc \pmod m$, then $a \equiv b \pmod m$.

Proof :

Here d = 1 & so $a \equiv b \pmod{m/1}$ i.e., $a \equiv b \pmod m$.

Theorem ***3.2.6:***

If $a_1, a_2, \ldots, a_m$ is a complete residue system modulo m & $(a, m) = 1$, then $a a_1, a a_2, \ldots, a a_m$ is also a complete residue system modulo m.

Proof :

Let $A = \{ a a_1, a a_2, \ldots, a a_m \}$.

A has m elements. So it is only needed to prove that no two elements of A are congruent (mod m).

Suppose $a a_i \equiv a a_j \pmod m$, $i \neq j$

$\Rightarrow m \mid a(a_i - a_j)$

$\Rightarrow m \mid (a_i - a_j)$ ($\because (a, m) = 1$)

$\Rightarrow a_i \equiv a_j \pmod m$.

This contradicts the hypothesis that $a_1, a_2, \ldots a_m$ is C.R.S. (mod m).

Thus all the elements of A are incongruent (mod m) & is therefore a C.R.S.(mod m).

Theorem ***3.2.7:***

If $a \equiv b \pmod{m_1}$ & $a \equiv b \pmod{m_2}$.

Then $a \equiv b \pmod{[m_1, m_2]}$, where $[m_1, m_2]$ is the least common multiple of m_1, m_2.

Proof :

$a \equiv b \pmod{m_1} \Rightarrow m_1 \mid (a - b)$ i.e., (a- b) is a multiple of m_1.

$a \equiv b \pmod{m_2} \Rightarrow m_2 \mid (a - b)$ i.e., (a - b) is a multiple of m_2.

Since the l.c.m. of two integers divides their common multiple therefore $[m_1, m_2] \mid a - b$

$\Rightarrow a \equiv b \pmod{[m_1, m_2]}$.

Theorem ***3.2.8:***

If $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots\ldots, a \equiv b \pmod{m_k}$

whrer $a, b, m_1, m_2, \ldots\ldots, m_k \in Z$ with $m_1, m_2, \ldots, m_k$ are positive integer, then

$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$.

Corollary *3.2.9:*

If $a \equiv b(\text{mod } m_1)$ & $a \equiv b \text{ (mod } m_2)$ & $(m_1, m_2) = 1$, then $a \equiv b \text{ (mod } m_1 m_2)$.

Proof :

If $(m_1, m_2) = 1$, then $[m_1, m_2] = m_1.m_2$.

so $a \equiv b \text{ (mod } [m_1, m_2])$

$\Rightarrow a \equiv b \text{ (mod } m_1 m_2)$.

Example(10):

Use the theory of congruence

(i) to find the remainder when 2^{50} is divided by 7.

(ii) Verify that $89 \mid 2^{44} - 1$.

Solution *:*

(i) $2^3 \equiv 1 \text{ (mod } 7)$

$\therefore (2^3)^{16} \equiv (1)^{16} \text{ (mod } 7)$

$2^{48} \equiv 1 \text{ (mod } 7)$

Also $2^2 \equiv 1 \text{ (mod } 7)$

$\therefore 2^{50} \equiv 4 \text{ (mod } 7)$

$\therefore$ remainder is 4.

(ii) we have

$2^{11} - 1 = 2047 = 23 \times 89 \Rightarrow 89 \mid 2^{11} - 1$,

$2^{11} - 1 \equiv 0 \text{ (mod } 89)$

$2^{11} \equiv 1 \text{ (mod } 89)$

$\therefore (2^{11})^4 \equiv 1^4 \text{ (mod } 89)$

$2^{44} \equiv 1 \text{ (mod } 89)$

$\Rightarrow 89 \mid 244 - 1$.

3.3 Different Bases and Special Divisibility Tests

Consider the integer 935. we know that 935 is

$$9 \times 102 + 3 \times 101 + 5,$$

i.e., it is the value of the polynomial $9x2 + 3x + 5$. for $x = 10$.

In general we can write any integer in the form of a polynomial,

$r_m\, 10^m + r_{m-1}\, 10^{m-1} + r_{m-2}\, 10^{m-2} + \ldots\ldots + r_1\, 10 + r_0,$

where $0 < r_m < 10$ & $0 \le r_i < 10$, for i= 0 ,1 ,2 ,..,m - 1.

Such an expression for a positiveve integer N is called its representation in the scale of 10

and 10 is called the base or radix.

For the sake of convenience we usually take the base as the integer 10.

However, any fixed integer greater than 1 can serve as a base and is clear from the following theorem.

Theorem ***3.3.1:***

Let b be an integer > 1, then every positive integer N can be written uniquely in terms of powers of b as

$$N = a_m\, b^m + a_{m-1}\, b^{m-1} + \ldots\ldots + a_2\, b^2 + a_1\, b + a_0 ,$$

where $0 < a_m < b$, $0 \le a_i < b$ for $i = 1, 2, 3, \ldots, m - 1$.

Proof :

By Theorem (1.1.4)(Division Algorithm) we can find unique integers q_1 and a_0 satisfying

$$N = q_1\, b + a_0, \qquad 0 \le a_0 < b.$$

If $q_1 \ge b$ we can divide once more , obtaining

$$q_1 = q_2\, b + a_1, \qquad 0 \le a_1 < b,$$

substituting for q_1 in the above equation we get

$$N = (q_2\, b + a_1)b + a_0,$$
$$= q_2 b_2 + a_1 b + a_0.$$

If $q_2 \ge b$, we divide once again obtaining

$$q_2 = q_3\, b + a_2 , \; 0 \le a_2 < b.$$

Thus

$$N = (q_3 b + a_2)b_2 + a_1 b + a_0$$
$$= q_3 b_3 + a_3 b_2 + a_1 b + a_0.$$

Since $N > q_1 > q_2 > \ldots\ldots\ldots \ge 0$ is a strictly decreasing sequence of integers, this process must eventually terminate say at $(m - 1)^{th}$ stage where,

$$q_{m-1} = q_m\, b + a_{m-1} , \qquad 0 \le a_{m-1} < b \;\&\; 0 < q_m < b .$$

Setting $a_m = q_m$, we reach the representation,

$$N = a_m b_m + a_{m-1}\, b_{m-1} + \ldots\ldots + a_2\, b_2 + a_1 b + a_0 \quad \ldots\ldots\ldots\ldots (1)$$

The uniqueness of the expression follows from the uniqueness of the integers $a_0, a_1, a_2, \ldots\ldots\ldots, a_m$ which completes the proof.

The representation of N in (1) is called the representation of N in the scale b and b is called the base

or radix.The important point in all this is that N is completely determined by the ordered array

$a_m, a_{m-1}, \ldots, a_1, a_0$ of co-efficients with the powers of b and the plus sign between them.

Thus (1) may be written in the abbreviated from as

$$N = (a_m, a_{m-1}, \ldots\ldots\ldots\ldots, a_1, a_0)_b$$

The base is specified at the right end . If no base is specified, it means that the integer is written in the scale of 10. The system of writing integers in the base 10 is called

Decimal system (from the Latin decem, 10).

After 10, the most commonly used base is 2 and in this case the system of writing integers is

called the Binary system (from the Latin binarius, 2). In this system a_i is either 0 or 1 and

we write an integer as sums of powers of 2. This system is frequently used in high speed computers.

Although the expression for an integer in this case is lengthy, yet it only involves two digits 0 &

1 which simplifies the mechanism of the computer. We are using the Decimal system without

writing the base 10, through in fact.

Example(11):

$1561 = 1.10^3 + 5.10^2 + 6.10^1 + 1 = (1651)_{10}$ or (1561)

10 | 1561
10 | 156 - 1
↑
10 | 15 – 6
| ↑
| 1→ 5

Example(**12**):

(i) If N= 243 and b=7, then

7 | 243
7 | 34 - 5
| ↑
| 4 → 6

$243 = (465)_7 = 4.7^2 + 6.7 + 5.$

(ii) N= 345 , b = 4,then

4 | 345
4 | 86 – 1
| ↑
4 | 21 – 2
| ↑
4 | 5 – 1
| ↑
| 1→ 1

$345 = 1.4^4 + 1.4^3 + 1.4^2 + 2.4 + 1 \Rightarrow 345 = (11121)_4.$

(iii) N= 89, b = 2

2 | 89
2 | 44 – 1
2 | 22 – 0
2 | 11 – 0
2 | 5 – 1
2 | 2 – 1

| 1 – 0

$89 = 1.2^6 + 0.2^5 + 1.2^4 + 1.2^3 + 0.2^2 + 0.2 + 1$

$= 1.2^6 + 1.2^4 + 1.2^3 + 1 \Rightarrow 89 = (1011001)_2$.

We are about ready to derive criteria for determining whether an integer is divisible by 9 or

11 without performing the actual division, for this we have.

Theorem ***3.3.2:***

Let $p(x) = \sum_{k=0}^{m} C_k x_k$ be a polynomial function of x with integral coefficients C_k .If $a \equiv b \pmod m$,

then $p(a) \equiv p(b) \pmod m$.

Proof :

Given that $a \equiv b \pmod m$, therefore $a^k \equiv b^k \pmod m$, for k=0, 1, 2,.... ,m by Theorem 3.2.3.

$\therefore C_k a_k \equiv C_k b_k \pmod m$, k = 0, 1, 2,... ,m.

Adding the m+1 congruence, we get

$$\sum_{k=0}^{m} C_k a_k \equiv \sum_{k=0}^{m} C_k b_k \pmod m,$$

or $p(a) \equiv p(b) \pmod m$).

Note:

If p(x) is a polynomial with integral coefficients, one says that a is a solution of the congruence $p(x) \equiv 0 \pmod m$ if $p(a) \equiv 0 \pmod m$.

Corollary ***3.3.3:***

If a is solution of $p(x) \equiv 0 \pmod m$, and $a \equiv b \pmod m$,

then b is also a solution.

Proof :

By the Theorem 3.3.2 , if $a \equiv b \pmod m$, then $p(a) \equiv p(b) \pmod m$.

If a is a solution of $p(x) \equiv 0 \pmod m$, then $p(b) \equiv p(a) \equiv 0 \pmod m$, making b a solution.

Theorem ***3.3.4:***

Let $N = a_m 10_m + a_{m-1} 10^{m-1} + ... + a_1 10 + a_0$,

be the decimal expansion of the positive integer N and let

$S = a_0 + a_1 + ... + a_m$. Then $9 \mid N$ iff $9 \mid S$.

Proof :

Consider $p(x) = \sum_{k=0}^{m} a_k x_k$, a polynomial with integral coefficients. The key observation is that

$10 \equiv 1 \pmod 9$, which implies that $p(10) \equiv p(1) \pmod 9$ but

$p(10) = N$ & $p(1) = a_0 + a_1 + ... + a_m = S$, so that $N \equiv S \pmod 9$,

$\Rightarrow N \equiv 0 \pmod 9$ iff $S \equiv 0 \pmod 9$,

which is what we wanted to prove.

Theorem ***3.3.5:***

Let $N = a_m 10^m + a_{m-1} 10^{m-1} + ... + a_1 10 + a_0$,

be the decimal representation of the positive integer N, and let

$T= a_0 - a_1 + a_2 - a_3 +.....+(-1)^m a_m$.

Then $11 \mid N$ iff $11 \mid T$.

Proof :

Let $p(x) = \sum_{k=0}^{m} a_k x_k$ be a polynomial with integral coefficient. The key observation is that

$10 \equiv -1 \pmod{11}$.

Therefore, $p(10) \equiv p(-1) \pmod{11}$.

But $p(10) = N$ and $p(-1) = a_0 - a_1 + a_2 - a_3 +....+(-1)^m a_m = T$,

So that $N \equiv T \pmod{11}$.

This implies that both N & T are divisible by 11 or neither is divisible by 11.

Example (12):

Without performing the divisions, determine whether N=1571724 is divisible by 9 or 11.

Solution *:*

(i) The digital sum is $S=1 +5 +7+ 1+ 2 +4 =27$ and $9 \mid 27 \Rightarrow 9 \mid N$.

(ii) The alternating sum is $T=4 - 2 + 7 -1 + 7 - 5 + 1 = 11$ 11 is divisible by 11 and so N is divisible by 11.

3.4 linear Congruences

A congruence of the form $ax \equiv b \pmod m$, where x is an unknown integer is called a linear

congruence in one variable.

We first note that if $x = x_0$ is a solution of the congruence $ax \equiv b \pmod m$, and if $x_1 \equiv x_0 \pmod m$,

then $ax_1 \equiv ax_0 \equiv b \pmod m$, so that x_1 is also a solution. Hence if one members of a congruence

class modulo m is a solution , then all member of this class are solutions. How many of the m congruence classes modulo m give solutionsthis is exactly the same as asking how many incongruent solutions there are modulo m.

Theorem ***3.4.1:***

The linear congruence $ax \equiv b \pmod m$ .....(1)

where $a \equiv 0 \pmod m$, $(a,m) = d$, has solutions if and only if $d \mid b$.

Furthermore, if the solutions of (1) exsist, they are exactly d in number.

Proof :

The congruence (1) is equivalent to the linear diophantine equation

$ax - my = b$ .....(2),

where $y \in Z$, by Theorem1.5.2 the equation (2) has solution iff $d \mid b$ and hene the congruence (1) is solvable iff $d \mid b$.This prove the first part of the theorem.

Suppose that $d \mid b$ by Theorem1.5.2 eq.(2) has solution given by

$$x = x_0 + \frac{m}{d}\, t \ , \ y = y_0 + \frac{a}{d}\, t \ ,$$

where $t \in Z$ and (x_0 , y_0) is a solution of (2). By taking

$t = 0, 1 , 2,... , (d - 1), d , (d + 1), (d + 2),.....,$

we get respectively

$$x = x_0 \ , \ x + \frac{1}{d}\, m \ , \ x_0 + \frac{2}{d}\, m \ , \ x_0 + \frac{3}{d}\, m \ ,..... , \ x_0 + \frac{d-1}{d}\, m,$$

$$x_0 + m \ , \ x_o + m + \frac{1}{d}\, m \ , \ x_0 + m + \frac{2}{d}\, m,.....$$

It is clear that the first d solutions are distinct but the $(d + 1)^{th}$ solution is the same as the

first solution because

$x_0 + m \equiv x_0 \pmod m$.

Similarly, the $(d+2)^{th}$ solution is the same as the second solution as

$x_0 + \frac{1}{d}\, m \equiv x_0 + m + \frac{1}{d}\, m \pmod m$ and so on , hence the congruence (1) has just

d incongruent solutions given by

$x \equiv x_0 + (\frac{m}{d}\,)\, t \pmod m$, $t = 0 , 1 , 2,.....,d- 1.$

Corollary ***3.4.2:***

If $(a,m) = 1$, then the linear congruence $ax \equiv b \pmod m$

has a unique (just one) solution.

Example (13):

Solve if possible the congruence

(i) $18x \equiv 30 \pmod{42}$.

(ii) $2x \equiv 3 \pmod 7$.

(iii) $3x \equiv 5 \pmod 6$.

(iv) $9x \equiv 12 \pmod{15}$.

(v) $7x \equiv 1 \pmod{31}$.

Solution *:*

(i) (18,42) = 6 and $6 \mid 30$, hence the given congruence has d =6 solutions.

By inspection or by trails one solution is found to be

$x \equiv x_0 \pmod{42}$

$x \equiv 4 \pmod{42}$

Therefore the six solutions are as follows

$x \equiv 4 + (\frac{42}{6})\, t \pmod{42}$, $t = 0, 1, 2, 3, 4, 5$.

i.e., $x \equiv 4 + 7t \pmod{42}$

$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}$.

(ii) since (2,7) =1 , therefore the given congruence has a unique solution by trail we found

$x \equiv 5 \pmod 7$

$x = 5 + 7t \pmod 7$, $t=0$,

$x \equiv 5 \pmod 7$.

(iii) since (3,6) = 3 and $3 \nmid 5$ and so the given congruence has no solution.

(iv) since (9,15) = 3, $3 \mid 12$,we have 3 solutions.

$x \equiv 3 \pmod{15}$

$x \equiv 3 + \frac{15}{3}\, t \pmod{15}$, $t = 0, 1, 2$

$x \equiv 3 + 5t \pmod{15}$

$x \equiv 3, 8, 13 \pmod{15}$

(v) since (7,31) =1, we have a unique solution.

$x \equiv 9 \pmod{31}$.

Definition ***3.4.3:***

Given an integer a with (a,m) =1, a solution of $ax \equiv 1 \pmod m$ is called an inverse of a modulo m.

Example (**14**):

Since the solution of $7x \equiv 1 \pmod{31}$ satisfy $x \equiv 9 \pmod{31}$ [Example 13(v)].

So 9 and all integers congruent to 9 modulo 31 are inverse of 7 modulo 31.Since $9.7 \equiv 1 \pmod{31}$,

7 is an inverse of 9 modulo 31.

When we have an inverse of a modulo m, we can use it to solve any congruence of the form $ax \equiv b \pmod m$,

let $\bar{a}$ be the inverse of a modulo m, so that $a\bar{a} \equiv 1 \pmod m$, then if $ax \equiv b \pmod m$, we can

multiply both sides of this congruence by $\bar{a}$ to find $\bar{a}(a\,x) \equiv b \pmod m$, so that

$x \equiv b \pmod m$.

Example (**15**):

To find the solution of $7x \equiv 22 \pmod{31}$ we multiply both sides of this congruence by 9 an

inverse of 7 modulo 31 to obtain $9.7x \equiv 9.22 \pmod{31}$.

Hence $x \equiv 198 \equiv 12 \pmod{31}$.

Theorem ***3.4.4:***

Let p be prime. The positive integer a is its own inverse modulo p iff

$a \equiv 1 \pmod p$ or $a \equiv -1 \pmod p$.

Proof :

If $a \equiv 1 \pmod p$ or $a \equiv -1 \pmod p$, then

$a^2 \equiv 1 \pmod p$ so that a is its own inverse modulo p.

Conversly:

If a is its own inverse modulo p , then

$a^2 = a.a \equiv 1 \pmod{p}$, hence $p \mid (a^2 - 1)$.
Since $a^2 - 1 = (a - 1)(a + 1)$, either $p \mid a - 1$ or $p \mid a + 1$,
therefore either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

3.5 The Chinese remainder Theorem

We consider systems of congruences that involve only one variable, but different moduli.

Such systems arose in ancient Chinese puzzles such as the following : find a number that

leaves a remainder of 1 when divided by 3 , a remainder 2 when divided by 5 and a remainder

of 3 when divided by 7.

This puzzle leads to the following system of congrunces:

$x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$.

We now give a method of finding all solutions of systems of simultaneous congruences such as above.

Theorem ***3.5.1***

The Chinese remainder theorem.

Let $m_1, m_2, \ldots, m_r$ be pair wise relatively prime positive integers,

i.e. , gcd $(m_i , m_j) = 1$ for $i \neq j$,then the system of congruences

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

.

.

.

$x \equiv a_r \pmod{m_r}$,

has a unique solution modulo $M = m_1 m_2 \ldots m_r$.

Proof :

First we construct a simultaneous solution to the system of congruences , let

$M_k = M/m_k = m_1 m_2 \ldots m_{k-1} m_{k+1} \ldots m_r$.

$(M_k , m_k) = 1$, since $(m_j , m_k) = 1$, $j \neq k$. By Theorem3.4.3 we can find an inverse y_k of M_k

modulo m_k, so $M_k y_k \equiv 1 \pmod{m_k}$.

We now form the sum, $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_r M_r y_r$.

This integer x is a simultaneous solution of the r congruences.

We must show that $x \equiv a_k \pmod{m_k}$, k=1,2,.....,r.

Since $m_k \mid M_j$, $j \neq k$, we have $M_j \equiv 0 \pmod{m_k}$.

Therefore in the sum for x all the terms expect the k^{th} term are congruent to 0 (mod m_k)

hence $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, since $M_k y_k \equiv 1 \pmod{m_k}$.

We now show that any two solutions are congruent modulo M.

Let x_0 and x_1 be simultaneous solutions to the system of r congruences. Then for each k

$x_0 \equiv x_1 \equiv a_k \pmod{m_k}$, so $m_k \mid (x_0 - x_1)$.

Using Theorem (3.2.8). we see that $M \mid (x_0 - x)$.

So $x_0 \equiv x_1 \pmod M$.

This shows that solution of the system of r congruences is unique modulo M.

Example (**16**):

To solve the system

$x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 5$

$x \equiv 3 \pmod 7$

Solution *:*

we have

$M=3.5.7=105$

$M_1 = 105/3 = 35$

$M_2 = 105/5 = 21$

$M_3 = 105/7 = 15.$

To determine y_1, we solve $35\ y_1 \equiv 1 \pmod 3$,

$\therefore y_1 \equiv 2 \pmod 3$.

To find y_2, we solve $21\ y_2 \equiv 1 \pmod 5$,

$\therefore y_2 \equiv 1 \pmod 5$.

To find y_3 we solve $15\ y_3 \equiv 1 \pmod 7$,

$\therefore y_3 \equiv 1 \pmod 7$.

Hence $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{105}$

$\equiv 1.35.2 + 2.21.1 + 3.15.1 \mod (105)$

$\equiv 157 \pmod{105}$

$\equiv 52 \pmod{105}$

Example (17):

Solve the system

$x_1 \equiv 1 \pmod 5$

$x_2 \equiv 2 \pmod 6$

$x_3 \equiv 3 \pmod 7$

Solution *:*

we have $M=5.6.7=210$.

$M_1 = 210/5 = 42,$

$M_2 = 210/6 = 35,$

$M_3 = 210/7 = 30.$

Find y_1, y_2, y_3.

$42\ y_1 \equiv 1 \pmod 5 \Rightarrow y_1 \equiv 3 \pmod 5,$

$35\ y_2 \equiv 1 \pmod 6 \Rightarrow y_2 \equiv 5 \pmod 6,$

$30\ y_3 \equiv 1 \pmod 7 \Rightarrow y_3 \equiv 4 \pmod 7.$

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{210},$

$\equiv 1.42.3 + 2.35.5 + 3.30.4 \pmod{210}$

$\equiv 126 + 350 + 360 \pmod{210}$

$\equiv 836 \pmod{210}$

$\equiv 206 \pmod{210}$

3.6 : Applications of Congruences

Using congruences we can develop divisibility tests for integers based on their expansions

with respect to different bases. We begin with tests that use decimal notation let

$n = (a_k a_{k-1} .... a_1 a_0)_{10}$, then

$n = a_k 10^k + a_{k-1} 10^{k-1} + ...+ a_1 10 + a_0$, $0 \le a_i \le 9$ for $i = 0, 1, 2, ... , k$.

First , we develop tests for divisibility by powers of 2.

Since $10 \equiv 0 \pmod 2$ $\Rightarrow$ $10^i \equiv 0 \pmod{2^i}$ for all positive integers i.

Hence,

$n \equiv (a_0)_{10} \pmod 2$

$n \equiv (a_1 a_0)_{10} \pmod{2^2}$

$n \equiv (a_2 a_1 a_0)_{10} \pmod{2^3}$

.

.

.

.

$n \equiv (a_{k-1} a_{k-2} ..... a_2 a_1 a_0)_{10} \pmod{2^k}$.

These congruence tells us that to determine whether an integer n is divisible by 2 , we only

need to examine the last digits for divisibility by 2 . similarly to determine whether n is divisible by 4. we only need to check the integer made up of the last two digits of n for divisibility by 4.

In general to test n for divisibility by 2^i , we only need to check the integers made up of the

last i digits of n for divisibility by 2^i.

Example(17):

Let n=32688048 . we see that $2 \mid n$ since $2 \mid 8$, $4 \mid n$, since $4 \mid 48$, $8 \mid n$, since $8 \mid 048$ i.e., $8 \mid 48$,

$16 \mid n$, since $16 \mid 8048$, but $32 \nmid n$, since $32 \nmid 88048$.

Next , we develop tests for divisibility for powers of 5.

Since $10 \equiv 0 \pmod 5$,we have $10^i \equiv 0 \pmod{5^I}$.

Hence divisibility test for powers of 5 are analogous to those of powers of 2. we only need to

check the integers madeup of the last i digits of n to determine whether n is divisible by 5^i .

Example (18):

Let n=15535375 . $5 \mid n$, since $5 \mid 5$. $25 \mid n$, since $25 \mid 75$.

$125 \mid n$, since $125 \mid 375$, but $625 \nmid n$, since $625 \nmid 5375$.

Next, we develop tests for divisibility by 3 and by 9.

Note that both the congruences $10 \equiv 1 \pmod 3$ and $10 \equiv 1 \pmod 9$ hold .

Hence

$10^k \equiv 1 \pmod 3$ and $10^k \equiv 1 \pmod 9$, so

$(a_k a_{k-1} ... a_2 a_1 a_0) = a_k 10^k + a_{k-1} 10^{k-1} + ... a_1 10 + a_0$,

$\equiv a_k + a_{k-1} + ... a_1 + a_0 \pmod 3$ and $\pmod 9$.

Hence we only need to check whether the sum of digits of n is divisible by 3 or by 9 , to see whether n is divisible by 3 or by 9.

Example (19):

Let n = 4127835, then the sum of digits of n is S =4+1+2+7+8+3+5 = 30.

Since $3 \mid 30$ but $9 \nmid 30$, so $3 \mid n$, but $9 \nmid n$.

A rather simple test can be found for divisibility by 11.

Since $10 \equiv -1 \pmod{11}$, we have

$$(a_k a_{k-1} \ldots a_1 a_0)_{10} \equiv a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0,$$
$$\equiv a_k (-1)^k + a_{k-1} (-1)^{k-1} + \ldots - a_1 + a_0 \pmod{11}.$$

This shows that $(a_k a_{k-1} \ldots a_1 a_0)_{10}$ is divisible by 11 iff $a_0 - a_1 + \ldots (-1)^k a_k$, the integer formed by alternately adding and subtracting the digits is divisible by 11.

Example (20):

We see that 723160823 is divisible by 11, since alternately adding and subtracting its digits yields to

$T = 3 - 2 + 8 - 0 + 6 - 1 + 3 - 2 + 7 = 22$, which is divisible by 11.

On the other hand 33678924 is not divisible by 11,

since $T = 4 - 2 + 9 - 8 + 7 - 6 + 3 - 3 = 4$, $11 \nmid 4$.

Next we develop a test simultaneously test for divisibility by the primes 7, 11, 13.

Note that $7.11.13 = 1001$ and $10^3 = 1000 \equiv -1 \pmod{1001}$.

Hence

$$(a_k a_{k-1} \ldots a_1 a_0)_{10} = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0,$$
$$\equiv (a_0 + 10 a_1 + 100 a_2) + 1000 (a_3 + 10 a_4 + 100 a_5)$$
$$+ (1000)^2 (a_6 + 10 a_7 + 100 a_8) + \ldots\ldots \pmod{1001}$$
$$\equiv (100 a_2 + 10 a_1 + a_0) - (100 a_5 + 10 a_4 + a_3)$$
$$+ (100 a_8 + 10 a_7 + a_6) - \ldots\ldots \pmod{1001}$$
$$\equiv (a_2 a_1 a_0)_{10} - (a_5 a_4 a_3)_{10} + (a_8 a_7 a_6)_{10} \ldots\ldots \pmod{1001}.$$

This congruence tells us that an integer is congruent modulo 1001 to the integer formed by adding and subtracting the three digits integers with decimal expansions formed from successively blocks of three decimal digits of the original number,where digits are grouped starting with the right most digit. As a consequence since 7,11 and 13 are divisors of 1001, we need to check whether this alternating sum and difference of blocks of three digits is divisible by 7 , 11 or 13.

Example (21):

Let $n = 59358208$. Since the alternating sum and difference of the integers formed from blocks of three digits $208 - 358 + 59 = -91$ which is divisible by 7 & 13 but not by 11, so n is divisible by 7 and 13 but not by 11.

Chapter 4

Theorems of Wilson , Fermat & Eluer

4.1 Wilson's Theorem & Fermat's Little Theorem

Theorem ***4.1.1:***

Wilson's Theorem

If p is prime , then $(p-1)! \equiv -1 (\mathrm{mod}\, p)$

Proof :

When p = 2 then,

(p-1)! ≡ 1 ≡ -1(mod2)

So the Theorem is true for p=2.

Let p > 2 by Theorem 3.4.1, for each integer a with $1 \le a \le p-1$, there is an inverse $\bar{a}$,

$1 \le \bar{a} \le p-1$,with $a\bar{a} \equiv 1 (\mathrm{mod}\, p)$.

By Theorem 3.4.4, the only positive integers less than p that are their own inverse are 1 & $p-1$.

So we group the integers from 2 to $p-2$ into $p-3/2$ pairs of integers, with the product of each pair congruent to 1 modulo p.

Hence we have

$2.3.....(p-3)(p-2) \equiv 1 (\mathrm{mod}\, p)$.

We multiply both sides of this congruence by 1 and $p-1$ t0 obtain

$(p-1)! \equiv 1.2.3.....(p-3)(p-2)(p-1) \equiv 1.(p-1) \equiv -1 (\mathrm{mod}\, p)$.

Example (**1**):

Let p = 7 we have (7-1)! = 6! = 1.2.3.4.5.6

We rearrange the factors in the product grouping together pairs of inverses modulo 7. We note that

$2.4 \equiv 1 (\mathrm{mod}\, 7), 3.5 \equiv 1 (\mathrm{mod}\, 7)$, so $6! \equiv 1.(2.4)(3.5).6 \equiv 1.6 \equiv -1 (\mathrm{mod}\, 7)$

The proof of wilson'sTheorem, has given by Joseph lagrange in 1770.

Now we see the converse of Wilson's Theorem.

Theorem ***4.1.2:***

If n is a positive integer such that

(n-1)! ≡ $-1 (\mathrm{mod}\, n)$ then n is a prime

Proof :

Assume that n is a composite integer and that

(n-1)! ≡ $-1 (\mathrm{mod}\, n)$.

Since n is composite, so $n = ab$, where $1 < a < n$, $1 < b < n$.

Since $a <$ n , then $a \mid$ (n-1)! because a is one of the n-1 numbers multiplied together to form(n-1)!.

Since

(n-1)! $\equiv -1(\mathrm{mod}\, n) \Rightarrow n \mid (n-1)! + 1.$

By Theorem 1.1.2 a also divides (n-1)! + 1.

By Theorem 1.1.3, since $a \mid (n-1)!$ and $a \mid ((n-1)! + 1)$ we conclude that $a \mid ((n-1)! + 1) - (n-1)! = 1,$

which is a contradiction since $a > 1$.

Example (2):

Since (6-1)! $\equiv$ 5! $\equiv$ 120 $\equiv 0(\mathrm{mod}\, 6)$ by Theorem 4.1.2, it is obvious that 6 is not a prime.

Theorem *4.1.3:*

If p is a prime of the form 4k+1 then the congruence $x^2 + 1 \equiv 0(\mathrm{mod}\, p)$ is solvable.

Proof :

Since $p = 4k+1$ then consider the following congreunce :

$4k \equiv -1(\mathrm{mod}\, p)$

$4k - 1 \equiv -2(\mathrm{mod}\, p)$

$4k - 2 \equiv -3(\mathrm{mod}\, p)$

.

.

$2k + 1 \equiv -2k(\mathrm{mod}\, p)$

$(2k)! \equiv (2k)!(\mathrm{mod}\, p)$

Multiplying the above congrunces we get

$4k! \equiv ((2k)!)^2(\mathrm{mod}\, p)$

or $(p-1)! \equiv ((2k)!)^2(\mathrm{mod}\, p)$

or $((2k)!)^2 \equiv (p-1)!(\mathrm{mod}\, p)$

i.e., $((2k)!)^2 \equiv -1(\mathrm{mod}\, p)$

or $((2k)!)^2 + 1 \equiv 0(\mathrm{mod}\, p)$

Hence $x \equiv (2k)!(\mathrm{mod}\, p)$ is the solution of the congrunce, $x^2 + 1 \equiv 0(\mathrm{mod}\, p)$.

Example (3):

Verify the above theorem if p =13.

Solution *:*

p = 13 = 4.3+1, so k=3

we want to know the solution of the congrunce

$x^2 + 1 \equiv 0(\mathrm{mod}\, 13)$

is $x \equiv (2.3)!(\mathrm{mod}\, 13)$

$x \equiv 6!(\mathrm{mod}\, 13)$

$x \equiv 6.5.4.3.2.1(\mathrm{mod}\, 13)$

$x \equiv 30.24(\mathrm{mod}\, 13)$

$x \equiv 4(-2)(\mathrm{mod}\, 13)$

$x \equiv -8(\mathrm{mod}\, 13)$

$x \equiv 5(\mathrm{mod}\, 13)$

So $5^2 + 1 \equiv 0(\mathrm{mod}\, 13)$

i.e., $26 \equiv 0(\mathrm{mod}\, 13)$

Example (4):

Show that 18!$\equiv -1(\mathrm{mod}\, 437)$

Solution *:*

$437 \equiv 19 \times 23.$

By Wilson's Theorem $18! \equiv -1 (\mathrm{mod}\, 19) \rightarrow$ [1]

Also by Wilson's Theorem we have $22! \equiv -1 (\mathrm{mod}\, 23)$

i.e., $22.21.20.19.(18)! \equiv -1 (\mathrm{mod}\, 23)$

$(-1).(-2).(-3).(-4)(18)! \equiv -1 (\mathrm{mod}\, 23)$

$24(18)! \equiv -1 (\mathrm{mod}\, 23)$

$1(18)! \equiv -1 (\mathrm{mod}\, 23)$

$(18)! \equiv -1 (\mathrm{mod}\, 23) \rightarrow$ [2]

Since (19,23)= 1 , therefore from [1] and [2] ,

$(18)! \equiv -1 (\mathrm{mod}\, 19 \times 23) \Rightarrow (18)! \equiv -1 (\mathrm{mod}\, 437).$

Theorem ***4.2.1:***

Fermat's Little Theorem

If p is a prime and a is a positive integer with p$\not|$ a then $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$

Proof :

Let {0 , 1 , 2 , ... , p-1} be a C.R.S.(mod p)$\rightarrow$ [1]

$\because$ p$\not|$ a $\therefore$ (a,p)=1,then Theorem 3.2.6 implies that

{0, a , 2a , ... , a(p-1)} is also a C.R.S.(mod p)$\rightarrow$ [2]

Thus each element in [1] congruent (mod p) to some element of [2] though not necessarily in the same order.

Since $0 \equiv 0 (\mathrm{mod}\, p)$, then

$a.2a.3a. \ldots (p\text{-}1)a \equiv 1.2.3 \ldots (p-1) (\mathrm{mod}\, p)$

i.e. , $a^{p-1}(p-1)! \equiv (p-1)! (\mathrm{mod}\, p)$

Dividing both sidesby (p-1)! which is the coprime to p , we get

$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$

Example (**5**):

Let p = 7 and a = 3, then

$1.3 \equiv 3 (\mathrm{mod}\, 7), \quad 2.3 \equiv 6 (\mathrm{mod}\, 7), \quad 3.3 \equiv 2 (\mathrm{mod}\, 7)$

$4.3 \equiv 5 (\mathrm{mod}\, 7), \quad 5.3 \equiv 1 (\mathrm{mod}\, 7), \quad 6.3 \equiv 4 (\mathrm{mod}\, 7)$

consequently,

$(1.3)(2.3)(3.3)(4.3)(5.3)(6.3) \equiv 3.6.2.5.1.4 (\mathrm{mod}\, 7)$

So that

$3^6 6! \equiv 6! (\mathrm{mod}\, 7) \quad (\div 6! \text{ since } (6!, 7) = 1)$

$3^6 \equiv 1 (\mathrm{mod}\, 7).$

Example (**6**):

Find the least positive residue of 3^{201} modulo 11 with the help of F.L.T.

$\because (3, 11) = 1$ by F.L.T. $3^{11-1} \equiv 1 (\mathrm{mod}\, 11)$

$\Rightarrow 3^{10} \equiv 1 (\mathrm{mod}\, 11)$

hence $(3^{10})^{20} \equiv (1)^{20} (\mathrm{mod}\, 11).$

Thus

$3^{201} = (3^{10})^{20}.3 \equiv 3 (\mathrm{mod}\, 11)$

$\therefore 3^{201} = 3 (\mathrm{mod}\, 11).$

Corollary ***4.2.2***

If p is a prime and a is a positive integer then $a^p \equiv a (\mathrm{mod}\, p)$.

Proof :

If $p \mid a$, then $a \equiv 0(\mathrm{mod}\, p) \Rightarrow a^p \equiv 0(\mathrm{mod}\, p) \Rightarrow a^p \equiv 0 \equiv a(\mathrm{mod}\, p)$,

hence $a^p \equiv a(\mathrm{mod}\, p)$.

If $p \nmid a$, then by **Fermat's Little Theorem** $a^p \equiv a(\mathrm{mod}\, p)$.

Example (**7**):

If p is a prime prove that $(p-1)!\, a^p + a \equiv 0(\mathrm{mod}\, p)$

Solution *:*

$(p-1)! \equiv -1(\mathrm{mod}\, p)$

$a^p \equiv a\ (\mathrm{mod}\, p)$

$(p-1)!\, a^p \equiv -a\ (\mathrm{mod}\, p)$

$(p-1)!\, a^p + a \equiv 0\ (\mathrm{mod}\, p)$

Theorem ***4.2.3:***

If p is a prime and a is an integer with $p \nmid a$, then a^{p-2} is an inverse of a moduls p.

Proof :

If $p \nmid a$ by F.L.T we have $a.a^{p-2} = a^{p-1} \equiv 1(\mathrm{mod}\, p)$,

hence a^{p-2} is an inverse of modulo p.

Example (**8**):

Since $(2, 11) = 1$, by F.L.T. $2^{10} \equiv 1(\mathrm{mod}\, 11)$

hence $2.2^9 = 2^{10} \equiv 1(\mathrm{mod}\, 11)$ $\therefore 2^9$ is an inverse of 2 modulo 11.

Corollary ***4.2.4:***

If a and b are positive integers and p is a prime with $p \nmid a$,then the solution of the linear

congruence $ax \equiv b(\mathrm{mod}\, p)$ are the integers x such that $x \equiv a^{p-2} b(\mathrm{mod}\, p)$.

Proof :

Suppose that $ax \equiv b(\mathrm{mod}\, p)$ .Since $p \nmid a$ from theorem above a^{p-2} is an inverse of a (mod p).

Multiplying both sides of the original congruence by a^{p-2} , we have

$a^{p-2} ax \equiv a^{p-2} b(\mathrm{mod}\, p)$,

hence ,

$x \equiv a^{p-2} b(\mathrm{mod}\, p)$.

Theorem ***4.2.5:***

If p and q are different primes such that $a^p \equiv a(\mathrm{mod}\, q)$ and $a^q \equiv a(\mathrm{mod}\, p)$, then $a^{pq} \equiv a(\mathrm{mod}\, pq)$.

Proof :

Given that $a^p \equiv a(\mathrm{mod}\, q)$

$\therefore (a^p)^q \equiv a^q(\mathrm{mod}\, q) \Rightarrow a^{pq} \equiv a^q(\mathrm{mod}\, q)$.

By corollary 4.2.2 $a^q \equiv a(\mathrm{mod}\, q)$,

hence

$a^{pq} \equiv a(\mathrm{mod}\, q) \rightarrow \boxed{1}$.

Similary

$a^{pq} \equiv a(\mathrm{mod}\, p) \rightarrow \boxed{2}$.

$\because (p, q) = 1$, therefore by corollary 3.2.9

$a^{pq} \equiv a(\mathrm{mod}\, pq)$.

Theorem ***4.2.6:***

For any prime p and $a, b \in Z^+$,then

$(a+b)^p \equiv a^p + b^p (\text{mod}\, p)$.

Proof :

We have

$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \ldots\ldots + \binom{p}{p-1} ab^{p-1} + b^p$.

$\because\ p \mid \binom{p}{i}$, i = 1,2,.....,p-1 (Example 7 chapter 2)

$\therefore\ \binom{p}{i} \equiv 0 (\text{mod}\, p)$

Hence

$$(a+b)^p \equiv a^p + b^p (\text{mod}\, p).$$

Example (9)

(i) If $(a, 35) = 1$, show that $a^{12} \equiv 1 (\text{mod}\, 35)$

(ii) If $(a, 42) = 1$, show that $168 \mid a^6 - 1$.

(i) $(a, 35) = 1 \Rightarrow (a, 5) = 1$, $(a, 7) = 1$.

Now since $(a, 5) = 1$,

$\therefore\ a^4 \equiv 1 (\text{mod}\, 35)$

$\therefore\ (a^4)^3 \equiv 1 (\text{mod}\, 5)$

i.e , $a^{12} \equiv 1 (\text{mod}\, 5) \rightarrow \boxed{1}$

Also since $(a, 7) = 1$

$\therefore\ a^6 \equiv 1 (\text{mod}\, 7)$

$\therefore\ (a^6)^2 \equiv 1^2 (\text{mod}\, 7)$

$\therefore\ a^{12} \equiv 1 (\text{mod}\, 7) \rightarrow \boxed{2}$

Since (5 , 7) = 1, from $\boxed{1}$ and $\boxed{2}$,

$a^{12} \equiv 1 (\text{mod}\, 35)$.

(ii) $(a, 42) = 1 \Rightarrow (a, 2) = 1$, $(a, 3) = 1$, $(a, 7) = 1$

Now by F.L.T. $(a, 3) = 1, \Rightarrow a^2 \equiv 1 (\text{mod}\, 3)$,

$$\Rightarrow a^6 \equiv 1 (\text{mod}\, 3) \rightarrow \boxed{1},$$

and $(a, 7) = 1 \Rightarrow a^6 \equiv 1 (\text{mod}\, 7) \rightarrow \boxed{2}$

$\because\ (a, 2) = 1 \Rightarrow a$ is odd and so $8 \mid a^2 - 1$ (Example 8 chapter 1).

i.e., $a^2 - 1 \equiv 0 (\text{mod}\, 8)$

or $a^2 \equiv 1 (\text{mod}\, 8)$

$(a^2)^3 \equiv 1^3 (\text{mod}\, 8)$

i.e., $a^6 \equiv 1 (\text{mod}\, 8) \rightarrow \boxed{3}$

Since 8,3 and 7 are relatively prime in pairs

$\therefore\ a^6 \equiv 1 (\text{mod}\, 8.3.7)$

i.e., $a^6 \equiv 1 (\text{mod}\, 168)$

$\Rightarrow$ $168 \mid a^6 - 1$.

Example (10)

Prove that $a^{21} \equiv a (\text{mod}\, 15)\ \forall a \in Z$.

We have $a^3 \equiv a (\text{mod}\, 3)\quad \forall a \in Z$,

$(a^3)^7 \equiv a^7 (\text{mod}\, 3)$

or $a^{21} \equiv a^3 a^3 a (\text{mod}\, 3)$

$a^{21} \equiv a.a.a (\text{mod}\, 3)$

$a^{21} \equiv a^3 (\text{mod}\, 3)$

$$a^{21} \equiv a(\text{mod}\,3) \rightarrow \boxed{1}$$

Also $a^5 \equiv a(\text{mod}\,5) \quad \forall a \in Z$

$$a^{20} \equiv a^4(\text{mod}\,5)$$

$$a^{21} \equiv a^5(\text{mod}\,5)$$

or $a^{21} \equiv a(\text{mod}\,5) \Rightarrow \boxed{2}$

from $\boxed{1}$ and $\boxed{2}$ since (3,5)=1 , therefore

$$a^{21} \equiv a(\text{mod}\,15).$$

Example (11)

Employ Fermats theorem to prove that if p is an odd prime , then

(i) $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots\ldots + (p-1)^{p-1} \equiv -1(\text{mod}\,p)$

(ii) $1^p + 2^p + 3^p + \ldots\ldots\ldots + (p-1)^p \equiv 0(\text{mod}\,p)$.

Solution *:*

(i) Since (1,p)=1 $\quad \therefore\ 1^{p-1} \equiv 1(\text{mod}\,p)$

(2,p)=1 $\quad \therefore\ 2^{p-1} \equiv 1(\text{mod}\,p)$

(3,p)=1 $\quad \therefore\ 3^{p-1} \equiv 1(\text{mod}\,p)$

.

.

.

(p-1,p)=1 $\quad \therefore\ (p-1)^{p-1} \equiv 1(\text{mod}\,p)$

Adding this congrunces , we get

$1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots\ldots + (p-1)^{p-1}$

$\equiv 1 + 1 + 1 + \ldots\ldots + 1(\text{mod}\,p)(p-1 \text{ times })$

$\equiv p - 1(\text{mod}\,p) \rightarrow \boxed{1}$

$p \equiv 0(\text{mod}\,p) \Rightarrow p - 1 \equiv -1(\text{mod}\,p) \rightarrow \boxed{2}$,

from $\boxed{1}$ and $\boxed{2}$ we get

$1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots\ldots + (p-1)^{p-1} \equiv -1(\text{mod}\,p)$

(ii) By corollary 4.2.2, we get

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

$\therefore\ 1^p + 2^p + 3^p + \ldots\ldots\ldots + (p-1)^p \equiv 1 + 2 + 3 + \ldots\ldots\ldots (p-1)(\text{mod}\,p)$

$$\equiv \frac{p(p-1)}{2}(\text{mod}\,p)$$

$$\equiv 0(\text{mod}\,p)$$

($\because$ p is odd , $\therefore\ p-1$ is even & so $\frac{p(p-1)}{2}$ is a multiple of p)

Example (12)

Assume that p & q are distinct odd primes such that p-1 | q-1 , if (a,pq)=1 , show that $a^{q-1} \equiv 1(\text{mod}\,pq)$.

Solution *:*

p-1 | q-1 $\Rightarrow q - 1 = k(p-1), \quad k \in Z.$

Now since (a,q)=1

$$\therefore\ a^{q-1} \equiv 1(\text{mod}\,q) \rightarrow \boxed{1}$$

Also (a,p)=1 $\quad \therefore\ a^{p-1} \equiv 1(\text{mod}\,p)$

now $\quad (a^{p-1})^k \equiv 1^k(\text{mod}\,p)$

or $\quad a^{k(p-1)} \equiv 1(\text{mod}\,p)$

i.e., $\quad a^{q-1} \equiv 1(\text{mod}\,p) \rightarrow \boxed{2}$

Since (p,q)=1 , therefore from $\boxed{1}$ and $\boxed{2}$ we have

$$a^{q-1} \equiv 1(\mathrm{mod}\, pq).$$

Example (13)

If p & q are distinct primes , prove that $p^{q-1} + q^{p-1} \equiv 1(\mathrm{mod}\, pq)$.

Solution *:*

$\because\ (p,q) = 1$, by F.L.T. ,we have

$p^{q-1} \equiv 1(\mathrm{mod}\, q)$.Since $q \mid q^{p-1}$ $\quad \therefore\ q^{p-1} \equiv 0(\mathrm{mod}\, q)$

$$\Rightarrow p^{q-1} + q^{p-1} \equiv 1(\mathrm{mod}\, q) \rightarrow \boxed{1}$$

Similarlly $q^{p-1} \equiv 1(\mathrm{mod}\, p)$, $p^{q-1} \equiv 0(\mathrm{mod}\, p)$

$$\therefore\ p^{q-1} + q^{p-1} \equiv 1(\mathrm{mod}\, p) \rightarrow \boxed{2}$$

$\because\ (p,q) = 1$, therefore $\boxed{1}$ and $\boxed{2}$ imply that

$$p^{q-1} + q^{p-1} \equiv 1(\mathrm{mod}\, pq).$$

4.3 Euler's Theorem

Definition ***4.3.1*** *:*

let n be a positive integer.The Eulers phi-function $\phi(n)$ is defined to be the number of positive integers not exceeding n that are relatively prime to n.

This function is named after the great Swiss Mathematication Leonhard Euler .

$\phi(n)$ for $1 \le n \le 12$,

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Definition ***4.3.2*** *:*

A reduced residue system (R.R.S.) modulo n is a set of $\phi(n)$ integers such that each element of the set is relatively prime to n and no two differents element of the set are congurent modulo n.

Example (14)

The set 1,3,5,7 is a reduced residue system modulo 8.

The set -3,-1,1,3 is also such a set.

Theorem ***4.3.3*** *:*

If $\{a_1, a_2, \ldots\ldots\ldots a_{\phi(m)}\}$ is a reduced residue system (R.R.S) (mod m) and $(a,\mathrm{m}) = 1$ then

$\{ aa_1, aa_2, \ldots\ldots\ldots, aa_{\phi(m)}\}$ is also a R.R.S (mod m).

Proof :

Let A= $\{aa_1, aa_2, \ldots\ldots\ldots, aa_{\phi(m)}\}$

1-A has $\varphi(m)$ element.

2-No two element of A are congurent modulo m ,for if $aa_i \equiv aa_j(\mathrm{mod}\, m)$ for i ≠ j , then since $(a,m) = 1$ this imlies that $a_i \equiv a_j(\mathrm{mod}\, m)$, which is a contradiction because the integers $a_1, a_2, \ldots\ldots\ldots a_{\phi(m)}$,

are incongurent (mod m) as $\{a_1, a_2, \ldots\ldots\ldots a_{\phi(m)}\}$ is a R.R.S.(mod m).

Hence all the integes of A are incongurent (mod m) and is therefore a R.R.S.(mod

m).

Example (15):

The set $1,3,5,7$ is a R.R.S.(mod 8).Since $(3,8) = 1$, then $3.1=3$, $3.3=9$, $3.5=15$, $3.7=21$ is also a R.R.S.(mod 8).

Theorem *4.3.4*

If m is a positive integer and a is a an integer with $(a,m) = 1$, then $a^{\varphi(m)} \equiv 1(\text{mod}\, m)$.

Let A = $\{a_1, a_2, \ldots\ldots\ldots a_{\phi(m)}\}$ be a R.R.S.(mod m) .Therefore by Theorem 4.3.3 ,

B = $\{aa_1, aa_2, \ldots\ldots\ldots, aa_{\phi(m)}\}$ is also a R.R.S.(mod m).This implies that the integers in the set

B are congurent modulo m to the integers in the set A ,though not necessarly in the same

order. Multiplying out we get

$$aa_1 \cdot aa_2 \cdot \ldots\ldots\ldots \cdot aa_{\phi(m)} \equiv a_1 \cdot a_2 \cdot \ldots\ldots\ldots \cdot a_{\phi(m)} (\text{mod}\, m)$$

or

$$a^{\phi(m)}(a_1 \cdot a_2 \cdot \ldots\ldots\ldots \cdot a_{\phi(m)}) \equiv a_1 \cdot a_2 \cdot \ldots\ldots\ldots \cdot a_{\phi(m)} (\text{mod}\, m)$$

Since $(a_1 \cdot a_2 \cdot \ldots\ldots\ldots \cdot a_{\phi(m)}, m) = 1$, from corollary 3.2.5, we conclude that

$$a^{\varphi(m)} \equiv 1(\text{mod}\, m).$$

Example (16):

We know that both the set $\{1,3,5,7\}$ and $\{3.1, 3.3, 3.5, 3.7\}$ are R.R.S.(mod 8), hence we have the same least positive residues (mod 8).

Therefore

$$3.1, 3.3, 3.5, 3.7 \equiv 1.3.5.7(\text{mod}\, 8)$$
$$3^4 1.3.5.7 \equiv 1.3.5.7(\text{mod}\, 8).$$

Since $(1.3.5.7, 8) = 1$,

so that

$$3^{\varphi(n)} \equiv 3^4 \equiv 1(\text{mod}\, 8).$$

Example (17)

We know that $2^{\varphi(9)-1} = 2^{6-1} = 2^5 = 32 \equiv 5(\text{mod}\, 9)$ is an inverse of 2 (mod 9),since

$$2.2^{\varphi(9)-1} \equiv 1(\text{mod}\, 9),$$
$$64 \equiv 1(\text{mod}\, 9).$$

So we can solve linear congrunce $ax \equiv b(\text{mod}\, m)$ where $(a,m) = 1$, by multiplying both

sides of the congrunce by $a^{\varphi(m)-1}$ to obtain

$$a^{\varphi(m)-1} ax \equiv a^{\varphi(m)-1} b(\text{mod}\, m),$$

therefore the solutions are those integers x such that

$$x \equiv a^{\varphi(m)-1} b(\text{mod}\, m).$$

Example (18)

The solutions of $3x \equiv 7(\text{mod}\, 10)$ are given by

$$x \equiv 3^{\varphi(10)-1}.7 \equiv 3^3.7 \equiv 9(\text{mod}\, 10), \quad (\text{since } \varphi(10) = 4)$$

Definition *4.3.5*

An arithmatic function is a function that is defined for all positive integers.

Definition *4.3.6*

An arithmatic function f is called multiplicative if $f(mn) = f(m)f(n)$, whenever m and n are relatively prime positive integers.It is called completely multiplicative if $f(mn) = f(m)f(n)$, for all positive integers m and n.

Theorem ***4.3.7***

If f multiplicative function and if $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots\ldots p_s^{\alpha_s}$ is the prime factorization of the positive integer n, then

$$f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \ldots\ldots\ldots\ldots f(p_s^{\alpha_s}).$$

(The proof of this theorem is given by induction try ?)

Theorem ***4.3.8***

If p is prime then $\varphi(p) = p - 1$. Conversely if p is a positive integer with $\varphi(p) = p - 1$, then p is prime.

Proof :

If p is a prime then every positive integr less than p is relatively prime to p. Since there are $p - 1$ such integers we have $\varphi(p) = p - 1$.

Conversely suppose $\varphi(p) = p - 1$, if p is compositive,then p has a divisor d with $1 < d < p$ and p and d are not relatively prime .

Since we know that at least one of the $p - 1$ integers $1, 2, \ldots\ldots\ldots, p - 1$ namely d is not relatively prime to p , $\varphi(p) \leq p - 2$. Hence if $\varphi(p) = p - 1$ then p must be prime.

Theorem ***4.3.9***

Let p be a prime and a positive integer.Then $\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$.

Proof :

The positive integer less than p^{α} that are not relatively prime to p are those integers not exceeding p^{α} that are divisible by p,i.e.,are the multiples of p In the set $\{1, 2, 3, \ldots, p^{\alpha}\}$ every p^{th} number is a multiple of p .Thus there are $\frac{p^{\alpha}}{p} = p^{\alpha-1}$ multiples of p in the above set. Hence the number of integers $\leq p^{\alpha}$ that are relatively prime to p^{α} are $p^{\alpha} - p^{\alpha-1}$,i.e.,

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha}(1 - \frac{1}{p}).$$

Example (19)

Using the above we find that

$\varphi(5^3) = 5^3 - 5^2 = 100$

$\varphi(2^{10}) = 2^{10} - 2^9 = 512$

$\varphi(11^2) = 11^2 - 11 = 110.$

Theorem ***4.3.10***

The function φ is multiplicative i.e., if $(m, n) = 1$, then

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Corollary ***4.3.11***

If $m_1, m_2, \ldots\ldots\ldots, m_k$ are natural numbers that are relatively prime in pairs then

$$\varphi(m_1 m_2 \ldots\ldots\ldots m_k) = \varphi(m_1) \cdot \varphi(m_2) \cdot \ldots\ldots\ldots\ldots \cdot \varphi(m_k)$$

Example (20):

Prove that if n is an odd integer then $\varphi(2n) = \varphi(n)$.

Solution *:*

If n is an odd then $(2, n) = 1$ and so

$$\varphi(2n) = \varphi(2)\varphi(n)$$
$$\varphi(2n) = 1.\varphi(n)$$
$$\varphi(n) = \varphi(n).$$

Theorem ***4.3.12***

Let $m = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_r^{\alpha_r}$, where p_i are distinct primes and $\alpha_i \in \mathbf{Z}^+$, then

$$\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}).....(1 - \frac{1}{p_r}).$$

Proof :

Since the p_i are distinct primes ,therefore, the numbers $p_1^{\alpha_1}, p_2^{\alpha_2}, ..., p_r^{\alpha_r}$ are relatively primein pairs.

Therefore by Corollary 4.3.11,we have

$$\varphi(p_1^{\alpha_1}.p_2^{\alpha_2}.....p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1}).\varphi(p_2^{\alpha_2}).....\varphi(p_r^{\alpha_r})$$

$$= (p_1^{\alpha_1})(1 - \frac{1}{p_1}).(p_2^{\alpha_2})(1 - \frac{1}{p_2}).....(p_r^{\alpha_r})(1 - \frac{1}{p_r})$$

$$= p_1^{\alpha_1}.p_2^{\alpha_2}.p_r^{\alpha_r}(1 - \frac{1}{p_1}).(1 - \frac{1}{p_2}).....(1 - \frac{1}{p_r})$$

$$= m(1 - \frac{1}{p_1}).(1 - \frac{1}{p_2}).....(1 - \frac{1}{p_r}).$$

Example (21)

$$\varphi(100) = \varphi(2^2.5^2) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40.$$
$$\varphi(720) = \varphi(2^4.3^2.5) = 720(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 192$$
$$\varphi(450) = \varphi(2.3^2.5^2) = 450(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 120$$

Example (22)

If f is an arithmatic function ,then

$$\sum_{d/12} f(d) = f(1)f(2)f(3)f(4)f(6)f(12)$$

for example

$$\sum_{d/12} d^2 = 1^2 + 2^2 + 3^2 + 4^2 + 6^2 + 12^2$$
$$= 1 + 4 + 9 + 16 + 36 + 144 = 210.$$

The following result which states that n is the sum of values of the phi-function at all the

positive divisors of n will be useful.

Theorem ***4.3.13***

Let n be positive integer,then $\sum_{d/n} \varphi(d)$.

Let $n = p^\alpha$, then the divisor of p^α are $,1, p, p^2, ..., p^\alpha$. Therefore

$$\sum_{d/n} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + ...+\varphi(p^\alpha)$$

$= 1 + p - 1 + p^2 - p + \ldots\ldots\ldots + p^{\alpha} - p^{\alpha-1}$

$= p^{\alpha} = n.$

Hence the result is true for $n = p^{\alpha}$.

Now let $n = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots\ldots\ldots p_r^{\alpha_r}$. Consider the product

$[\varphi(1) + \varphi(p_1) + \varphi(p_1^2) + \ldots + \varphi(p_1^{\alpha_r})] \times [\varphi(1) + \varphi(p_2) + \varphi(p_2^2) + \ldots + \varphi(p_2^{\alpha_r})] \times \ldots\ldots$

$\times[\varphi(1) + \varphi(p_r) + \varphi(p_r^2) + \ldots + \varphi(p_r^{\alpha_r})]$

$= \sum \varphi(p_1)^{\delta_1}.\varphi(p_2)^{\delta_2}\ldots\ldots\varphi(p_r)^{\delta_r}$

$= \sum \varphi(p_1^{\delta_1}.p_2{}^{\delta_2}\ldots\ldots p_r{}^{\delta_r}) \qquad 0 \le \delta_i \le \alpha_i, \quad i = 1, 2, 3, \ldots\ldots, r$

As δ_i varies between 0 and α_i, the product of $p_1^{\delta_1}.p_2{}^{\delta_2}\ldots\ldots p_r{}^{\delta_r}$ varies over all the divisors of n.

This implies that the R.H.S. is equal to $\sum_{d/n} \varphi(d)$. The L.H.S. by the result proved for $n = p^{\alpha}$ is equal to $p_1^{\alpha_1}.p_2^{\alpha_2}\ldots\ldots\ldots p_r^{\alpha_r} = n$. Hence $\sum_{d/n} \varphi(d) = n.$

Example (23)

Prove that $\varphi(m^2) = m\varphi(m) \qquad \forall m \in \mathbf{Z}^+.$

Solution *:*

Let $m = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots\ldots\ldots p_r^{\alpha_r} \quad \therefore \; m = p_1^{2\alpha_1}.p_2^{2\alpha_2}\ldots\ldots\ldots p_r^{2\alpha_r}.$

$\varphi(m^2) = \varphi(p_1^{2\alpha_1}.p_2^{2\alpha_2}\ldots\ldots\ldots p_r^{2\alpha_r})$

$\varphi(m^2) = p_1^{2\alpha_1}.p_2^{2\alpha_2}\ldots\ldots\ldots p_r^{2\alpha_r}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots\ldots\ldots(1 - \frac{1}{p_r})$

$\varphi(m^2) = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots\ldots\ldots p_r^{\alpha_r} \cdot p_1^{\alpha_1}.p_2^{\alpha_2}\ldots\ldots\ldots p_r^{\alpha_r}.(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots\ldots\ldots(1 - \frac{1}{p_r})$

$\varphi(m^2) = m\varphi(m).$

Example (24):

If $(a, n) = 1$ and $(a - 1, n) = 1$. Prove that

$1 + a + a^2 + \ldots\ldots\ldots + a^{\varphi(n)-1} \equiv 0 (\mathrm{mod}\, n).$

Solution:

We have

$a^{\varphi(n)} - 1 = (a - 1)(a^{\varphi(n)-1} + a^{\varphi(n)-2} + \ldots\ldots\ldots + a^2 + a + 1)$

By Theorem 4.3.4 $a^{\varphi(n)} - 1 \equiv 0 (\mathrm{mod}\, n)$

$\Rightarrow (a - 1)(a^{\varphi(n)-1} + a^{\varphi(n)-2} + \ldots\ldots\ldots + a^2 + a + 1) \equiv 0 (\mathrm{mod}\, n)$

and since $(a - 1, n) = 1,$

$\therefore \; a^{\varphi(n)-1} + a^{\varphi(n)-2} + \ldots\ldots\ldots + a^2 + a + 1 \equiv 0 (\mathrm{mod}\, n),$

or $1 + a + a^2 + \ldots\ldots\ldots + a^{\varphi(n)-1} \equiv 0 (\mathrm{mod}\, n).$

Example (25):

Find the unit digits of 7^{400} by use Euler's Theorem.

Solution *:*

Since $(7, 10) = 1,$ therefore by use Euler's Theorem,

$7^{\varphi(10)} \equiv 1 (\mathrm{mod}\, 10)$

$7^4 \equiv 1 (\mathrm{mod}\, 10) \quad \Rightarrow \quad (7^4)^{100} \equiv (1)^{100} (\mathrm{mod}\, 10)$

$\therefore \; 7^{400} \equiv 1 (\mathrm{mod}\, 10) \Rightarrow$ the unit digit of 7^{400} is 1.

Example (26):

Find the solution of the congruence $4x \equiv 7 (\mathrm{mod}\, 9).$

Solution *:*

$x \equiv 4^{\varphi(9)-1}.7(\mathrm{mod}\,9)$
$x \equiv 4^{5}.7(\mathrm{mod}\,9)$
$x \equiv 64.16.7(\mathrm{mod}\,9)$
$x \equiv 1.7.7(\mathrm{mod}\,9)$
$x \equiv 49(\mathrm{mod}\,9)$
$x \equiv 4(\mathrm{mod}\,9)$
$\therefore\ x \equiv 4(\mathrm{mod}\,9)$ is the soletion of the given congurence.

Chapter 5
Number-Theoretic Functions

Definition 5.1:

The Sum of divisors function, denoted by σ , is defined by setting $\sigma(n)$ equal to the sum of all the positive divisors of n.

Definition 5.2:

The number of divisors finction, denoted by τ , is defined by setting $\tau(n)$ equal to the number of positive divisors of n.

Example (1) :

The positive divisors of 20 are

1 , 2 , 4 , 5 , 10 , 20.

$\sigma(20) = 1 + 2 + 4 + 5 + 10 + 20 = 42$, and $\tau(20) = 6$.

Note:

(1) If n is a prime number then its only positive divisors are 1, & n itself and so,

$\tau(n) = 2, \qquad \sigma(n) = 1 + n$.

for axample :

$\tau(2) = \tau(3) = \tau(5) = \tau(7) = \ldots\ldots = \tau(101) = 2$.

(2) $\sum_{d/n} f(d)$ means " Sum the values $f(d)$ as d runs over all the positive divisors of the positive integer ".

for example :

$\sum_{d/20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20)$.

(3)With this understanding and may be expressed in the form :

(i) $\tau(n) = \sum_{d/n} 1$,

(ii) $\sigma(n) = \sum_{d/n} d$ and also $\sigma(n) = \sum_{d/n} \frac{n}{d}$,

$\Rightarrow \sigma(n) = \sum_{d/n} d = \sum_{d/n} \frac{n}{d}$, since if d is a divisor of n so is $\frac{n}{d}$.

Example (2) :

If $n = 10$, then the four positive divisors of n are 1,2,5,10.

$\therefore \tau(10) = \sum_{d/10} 1 = 1 + 1 + 1 + 1 = 4$,

$$\sigma(10) = \sum_{d/10} d = 1 + 2 + 5 + 10 = 18,$$

$$= \sum_{d/10} \frac{10}{d} = \frac{10}{1} + \frac{10}{2} + \frac{10}{5} + \frac{10}{10} = 10 + 5 + 2 + 1 = 18.$$

Theorem *5.3:*

The function τ is multiplicative i.e., if $(m, n)=1$, then $\tau(m.n) = \tau(m).\tau(n)$.

Proof :

Let $\tau(m) = r$ and $\tau(n) = s$ .Then $\tau(m)\tau(n) = rs$.

Let the r divisors of m be $\alpha_1, \alpha_2, \ldots, \alpha_r$,and the s divisors of n be $\beta_1, \beta_2, \ldots, \beta_s$.

Clearly the rs numbers $\alpha_i\beta_j (i = 1, 2, \ldots, r, j = 1, 2, \ldots, s)$ are all divisors of mn.

Thus $\tau(mn) \geq rs$. We prove that the equality holds.

If $\tau(m.n) > rs$, then there is a divisor d of mn which is different from the rs divisors $\alpha_i\beta_j$ of mn.

Either $d \mid m$ or $d \mid m$ which means that either d is one of the α_i or d is one of the β_j and

consequently d is one of the $\alpha_i\beta_j$ which is a contradiction, or d can be resolved into 2

factors d' and d'' prime to each other such that one of them divides m and the other divide n. Thus d' is one of the $\alpha_1, \alpha_2, \ldots, \alpha_r$ and d'' is one of the $\beta_1, \beta_2, \ldots, \beta_s$ and so $d'd''$ is one of the $\alpha_i\beta_j$ which is a contradiction.

Thus $\tau(mn) \not> rs$ and so $\tau(mn) = rs$,

hence $\tau(mn) = \tau(m)\tau(n)$.

Example (3):

Let m = 4 & n = 7 so (4,7) = 1

The divisors of 4 are 1,2,4,

$\Rightarrow \tau(4) = 3$ and $\tau(7) = 2$ (since 7 is prime), $\therefore \tau(4)\tau(7) = 6$.

The divisors of 28 are 1,2,4,7,14,28 $\Rightarrow \tau(28) = 6$.

Thus $\tau(28) = \tau(4)\tau(7)$.

Theorem *5.4:* *:*

The function σ is multiplicative i.e., if $(m, n) = 1$, then $\sigma(mn) = \sigma(m)\sigma(n)$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be the divisors of m and $\beta_1, \beta_2, \ldots, \beta_s$ be the divisors of n.So

$\sigma(m)\sigma(n) = (\alpha_1 + \alpha_2 + \ldots + \alpha_r)(\beta_1 + \beta_2 + \ldots + \beta_s)$.

$$= \sum_{i=1}^{r}\sum_{j=1}^{s} \alpha_i\beta_j.$$

Clearly all terms of $\alpha_i\beta_j, (i = 1, 2, \ldots, r, j = 1, 2, \ldots, s)$ are divisors of mn and as we have proved in

Theorem 5.3, these terms are the only divisors of mn .

Hence $\sum_{i=1}^{r}\sum_{j=1}^{s} \alpha_i\beta_j = \sigma(mn)$, thus $\sigma(mn) = \sigma(m)\sigma(n)$.

Example (4):

Take m=9 and n=4 $\Rightarrow$ (9,4)=1.

$\sigma(9) = 1 + 3 + 9 = 13$

$\sigma(4) = 1 + 2 + 4 = 7$

$\sigma(9)\sigma(4) = 13.7 = 91$

$\sigma(9 \times 4) = \sigma(36) = 1 + 2 + 3 + 4 + 6 + 9 + 12 + 18 + 36 = 91$,

hence $\sigma(36) = \sigma(9)\sigma(4)$.

Note:

If (m,n) > 1 , then $\sigma(mn) \neq \sigma(m)\sigma(n)$ as well as $\tau(mn) \neq \tau(m)\tau(n)$.

Verify this by taking m=6 & n=4.

Theorem *5.5:*

If $n = p_1^{k_1}p_2^{k_2}\ldots\ldots p_r^{k_r}$ is the prime factorization of n > 1,then

a) $\tau(n) = (k_1 + 1)(k_2 + 1)\ldots\ldots(k_r + 1)$, and

b) $\sigma(n) = \dfrac{p_1^{k_1+1} - 1}{p_1 - 1} + \dfrac{p_2^{k_2+1} - 1}{p_2 - 1} + \ldots + \dfrac{p_r^{k_r+1} - 1}{p_r - 1} = \prod_{i=1}^{r} \dfrac{p_i^{k_i+1} - 1}{p_i - 1}$

Proof :

Since p_i is prime, therefore, the only divisors of $p_i^{k_i}$ are $1, p_i, p_i^2, \ldots\ldots, p_i^{k_i}$ and therefore

a) $\tau(p_i^{k_i}) = k_i + 1$.

Since τ is multiplicative function and the p_i are distinct primes therefore,

$\tau(p_1^{k_1}p_2^{k_2}\ldots\ldots p_r^{k_r}) = \tau(p_1^{k_1}).\tau(p_2^{k_2})\ldots\ldots\tau(p_r^{k_r})$,

$$= (k_1 + 1)(k_2 + 1).....(k_r + 1),$$
$$= \prod_{i=1} (k_i + 1).$$

b) $\sigma(p_i^{k_i}) = 1 + p_i + p_i^2 + ... + p_i^k = \frac{p_i^{k_i+1} - 1}{p_i - 1}.$

Since σ is multiplicative function, therefore

$\sigma(n) = \sigma(p_1^{k_1} p_2^{k_2} ..... p_r^{k_r}) = \sigma(p_1^{k_1}).\sigma(p_2^{k_2}).....\sigma(p_r^{k_r})$

$$= \frac{p_1^{k_1+1} - 1}{p_1 - 1} + \frac{p_2^{k_2+1} - 1}{p_2 - 1} + ... + \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

$$= \prod_{i=1}^{r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

Example (5):

(i) If n = 72 =$2^3 3^2$,then

$\tau(n) = \tau(72) = \tau(2^3 3^2)$
$= \tau(2^3)\tau(3^2)$
$= (3 + 1)(2 + 1)$
$= 4.3 = 12$

$\sigma(n) = \sigma(72) = \sigma(2^3 3^2)$
$= \sigma(2^3)\sigma(3^2)$
$= \frac{2^4 - 1}{2 - 1}.\frac{3^2 - 1}{3 - 1}$
$= 15.13 = 195.$

(ii) If n = 180 = $2^2 3^2.5^1$,then

$\tau(n) = \tau(180) = \tau(2^2 3^2 5^1)$
$= \tau(2^2)\tau(3^2)\tau(5^1)$
$= (2 + 1)(2 + 1)(1 + 1)$
$= 3.3.2 = 18.$

$\sigma(n) = \sigma(180) = \sigma(2^2 3^2 5^1)$
$= \sigma(2^2)\sigma(3^2)\sigma(5^1)$
$= \frac{2^3 - 1}{2 - 1}.\frac{3^2 - 1}{3 - 1}.\frac{5^2 - 1}{5 - 1}$
$= 7.13.6 = 546.$

Example (6):

Prove that $\tau(n)$ is odd if n is a square.

Solution *:*

Let n = $m^2 = (p_1^{\alpha_1} p_2^{\alpha_2} ..... p_r^{\alpha_r}) = p_1^{2\alpha_1} p_2^{2\alpha_2} ..... p_r^{2\alpha_r}$.

$\therefore \tau(n) = (2\alpha_1 + 1)(2\alpha_2 + 1).....(2\alpha_r + 1),$

whatever positive integral value may be of α_i, $2\alpha_i + 1$ is always odd and so the product

$(2\alpha_1 + 1)(2\alpha_2 + 1).....(2\alpha_r + 1)$ is odd .So $\tau(n)$ is odd.

Theorem *5.6:*

$$\prod_{d/n} d = n^{1/2\tau(n)}.$$

Proof :

Let d denote an arbitrary positive divisor of n,so that n =dd' for some d' . As d

ranges

over all $\tau(n)$ positive divisors of n , $\tau(n)$ such equation occurs.

Multiplying these together we get

$$n^{\tau(n)} = \prod_{d/n} d \prod_{d'/n} d'$$

but as d runs through the divisors of n, so does d',

hence

$$\prod_{d/n} d = \prod_{d'/n} d'.$$

Thus $$n^{\tau(n)} = (\prod_{d/n} d)^2.$$

Or equivalently

$$\sqrt{n^{\tau(n)}} = \prod_{d/n} d.$$

i.e., $$n^{1/2\tau(n)} = \prod_{d/n} d.$$

Example (**7**):

Take n = 20.

Divisors of 20 are:1,2,4,5,10,20

$$\therefore \tau(20) = 6$$

$$\prod_{d/n} d = (1)(2)(4)(5)(10)(20) = 8000$$

Also

$$20^{1/2\tau(20)} = 20^{1/2(6)}$$

$$= (20)^3 = 8000$$

Thus $$\prod_{d/n} d = 20^{1/2\tau(20)}.$$

Definition *5.7:*

The Möbius function μ named after August Ferdnand Möbius is the arithmetical function

defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^s & \text{if } n \text{ is square free with prime factorization } n = p_1 p_2 \ldots\ldots p_s \\ 0 & \text{if } n \text{ has square factor larger than 1, i.e. if } n > 1, p^2 \mid n \text{ for some prime } p \end{cases}$$

Example (**8**):

$$\mu(1) = 1,\ \ \mu(2) = 1,\ \ \mu(3) = -1,\ \ \mu(4) = 0,\ \ \mu(5) = -1,$$
$$\mu(6) = 1,\ \ \mu(7) = -1,\ \ \mu(8) = 0,\ \ \mu(9) = 0,\ \ \mu(10) = 1$$
$$\mu(30) = (-1)^3 = -1,\ \ \mu(525) = 0.$$

Theorem *5.8:*

The function μ is multiplicative, i.e., if (m,n) = 1,

then $\mu(mn) = \mu(m).\mu(n)$.

Proof :

If one of the two numbers is equal to, then the Theorem is true.

If one of the numbers m, n is divisible by the square of a prime , then the theorem is true.

If $m = p_1 p_2 \ldots\ldots p_r, \qquad n = q_1 q_2 \ldots\ldots\ldots q_s.$

and p_i, q_i are distinct primes, then $\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m).\mu(n).$

Theorem ***5.9:***

For each position integer $n \geq 1$

$$\sum_{d/n} \mu(d) = \begin{cases} 1 & if \quad n = 1 \\ 0 & if \quad n > 1 \end{cases}$$

Where d runs through the divisors of n.

Example (9):

Consider n = 10 , the divisors of 10 are : 1, 2 , 5 ,10.

$$\sum_{d/10} \mu(d) = \mu(1) + \mu(2) + \mu(5) + \mu(10),$$

$$= 1 + (-1) + (-1) + 1 = 0.$$

Theorem ***5.10:***

If f is a multiplicative arithmetic function defined by the relation $F(n) = \sum_{d/n} f(d)$. Then F is also multiplicative.

Proof :

Suppose that (m,n)=1 , if $d_1 \mid m$ and $d_2 \mid n$, then $(d_1,d_2)=1$,

and as d_1 and d_2 run through all the positive divisors of m and n respectively $d= d_1d_2$ runs

through all positive divisors of mn.

Hence

$$F(mn) = \sum_{d/mn} f(d)$$

$$= \sum_{\substack{d_1/m \\ d_2/n}} f(d_1) f(d_2)$$

$$= \sum_{d_1/m} f(d_1) \sum_{d_2/n} f(d_2),$$

$$= F(m).F(n).$$

Example (10):

Show that F(60)=F(4)F(15).

Each of the divisors of 60 may be written as the product of a divisor of 4 and a divisor of 15

in the following way:

Divisors of 60 are :

1 ,2 ,3 ,4 ,5 ,6 ,10 ,12 ,15 ,20 ,30 ,60,

1=1.1 , 2=2.1 , 3=1.3 ,4=4.1 ,5=1.5 , 6=2.3 ,10=2.5 , 12 =4.3 , 15 =1.15 , 20 =4.5 , 30=

2.15 ,60 =4.15

(In each product, the first factor is a divisor of 4 and the second is a divisor of 15).

Hence

F(60)=f(1)+f(2)+f(3)+f(4)+f(5)+ f(6)+f(10)+f(12)+f(15)+f(20)+ f(30)+f(60)

= f(1.1)+f(2.1)+f(1.3)+f(4.1)+f(1.5)+ f(2.3)+f(2.5)+f(4.3)+f(1.15)+f(4.5)+ f(2.15)+f(4.15)

=f(1)f(1)+f(2)f(1)+f(1)f(3)+f(4)f(1)+f(1)f(5)+ f(2)f(3)+f(2)f(5)+f(4)f(3)+f(1)f(15)+f(4)f(5)+ f(2)f(15)+f(4)f(15)

=(f(1) + f(2) + f(4)) (f(1)+f(3)+f(5)+f(15))

=F(4) F(15).

The Bracket Function (The greatest integer Function)

Definition ***5.11:***

For an arbitrary real number x we denote by [x] the largest integer less than or equal to x , that is [x] is the unique integer satisfying x-1 < [x] ≤ x.

Example (11):

$$\left[\frac{5}{2}\right] = 2\ ,\ \left[\frac{13}{3}\right] = 4\ ,\ [4] = 4\ ,\ [-3] = -3\ ,$$
$$\left[\frac{-7}{2}\right] = -4, [\pi] = 3, [-\pi] = -4, \left[\frac{2}{7}\right] = 0.$$

It is clear that any real number x can be written in the from,

$x=[x]+\phi, \quad 0 \le \phi < 1.$

An interesting question is to ask , how many times a particular prime p appears in n!.

Example (12):

If p =3 , n = 9 then

9!=1.2.3.4.5.6.7.8.9

=1.2 .3.2.2.5.2.3.7.2.2.2.3.3

$=2^7.3^4.5^1.7^1.$

So that the exact power of 3 which divides 9! is 4.

It is better to have a formula that gives this without writing n! in the standard from.

This is by the next theorem.

Theorem ***5.12:***

If n is a positive integer and p a prime, then the highest power of p which divides n! is

$$\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots\ldots\ldots$$

Corollary ***5.13:***

If $p_1, p_2, \ldots\ldots\ldots, p_r$ are the primes occurring in the standard from of n! ,then

$$n! = \prod_{i=1}^{r} p_i^{\sum_{k=1}^{\infty}\left[\frac{n}{p_i^k}\right]}.$$

Example (12):

Let n = 20 , p=3

20! =1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16.17.18.19.20.

We see that

3,6,9,12,15,18 are multiples of 3 and they are 6 = [20/3] in numbers.

9, 18 are multiples of 3^2 so $2 = \left[\frac{20}{3^2} \right]$ in numbers.

Since $3^3 > 20 \Rightarrow 0 = \left[\frac{20}{3^3} \right]$ and so it stops.

Thus the highest power of 3 that divides 20! equals,

$\left[\frac{20}{3} \right] + \left[\frac{20}{3} \right] = 6+2 = 8,$

i .e., $3^8 \mid 20!$.

Example (13) :

Find the number of Zeros with which the decimal representation of 50! terminates.

Solution *:*

This is equivalent to determine the number of times 10 enters into the product 50! .

We find the exponents of 2 & 5 (2×5=10) in the prime factorization of 50! , and then to

select the smaller figure.

By direct calculations we see that

$$\left[\frac{50}{2} \right] + \left[\frac{50}{2^2} \right] + \left[\frac{50}{2^3} \right] + \left[\frac{50}{2^4} \right] + \left[\frac{50}{2^5} \right] + \ldots\ldots = 25+12+6+3+1+0+0+...=47.$$

Thus the highest power of 2 dividing 50! is 47.

Similarly

$$\left[\frac{50}{5} \right] + \left[\frac{50}{5^2} \right] = 10 + 2 = 12,$$

so the highest power of 5 dividing 50! is 12.

This means that the decimal representation of 50! will have

min(12,47) = 12 zeros.

Theorem ***5.14:***

If a & b are arbitrary real numbers , then $[a+b] \geq [a]+[b]$.

Example (14):

i) let $a = \frac{20}{3} = 6\frac{2}{3}$, $b = \frac{11}{4} = 2\frac{3}{4}$.

Then $a+b = 6\frac{2}{3} + 2\frac{3}{4} = 9\frac{5}{12}$

$\therefore [a+b] = 9.$

$[a] = 6, \quad [b] = 2 , \quad [a]+[b] = 6+2=8$

$\therefore [a+b] > [a]+[b].$

ii) Let $a = 2\frac{1}{4}$, $b = 3\frac{1}{2}$, $\therefore a+b = 5\frac{3}{4}$

So $[a] = 2$, $[b] = 3$, $[a+b] = 5.$

Hence $[a+b] = [a]+[b]$.

Theorem ***5.15:***

If n and r are positive integers with $1 \leq r < n$, then the binomial coefficient

$\binom{n}{r} = \frac{n!}{r!(n-r)!}$, is also an integer.

Corollary ***5.16:***

For a positive integer r , the product of any r consecutive positive integers is divisible

by r ! .

Proof :

The product of r consecutive positive integers, the largest of which is n is:
n(n-1)(n-2).....(n-r+1).

Now

$$n(n-1)(n-2).....(n-r+1) = \left(\frac{n!}{r!(n-r)!}\right) r!.$$

Since $\frac{n!}{r!(n-r)!} = A \in Z^+$, therefore

n(n-1)(n-2).....(n-r+1)=A r!.

So r! | n(n-1)(n-2).(n-r+1)

.

Example (3):

Take n = 10, r = 3, so n-r = 7.

$$\binom{n}{r} = \left(\frac{n!}{r!(n-r)!}\right) = \binom{10}{3} = \left(\frac{10!}{(3)!(7)!}\right)$$

$$= \frac{2^8.3^4.5^2.7^1}{2^5.3^3.5^1.7^1} = 2^3.3.5.7 \in Z^+.$$

Chapter 6
Quadratic Residues

Definition ***6.1 :***

If p is an odd prime, we say that the integer a is a quadratic residue of p if (a ,p)=1 and the congruence

$x^2 \equiv$ a (mod p) has a solution .If the congruence $x^2 \equiv$ a (mod p) has no solution, we say that a is quadratic nonresidne of p.

Example (**1**):

Consider the case of the prime p =13. To find out how many of the integer 1, 2, 3,, 12 are quadratic

residues of 13 ,we must know which of the congruences,

$$x^2 \equiv a \pmod{13},$$

are solvable when a runs through the set {1 , 2,....,12 }.

Modulo 13, the squares of the integers 1,2,3,....,12 are

$1^2 \equiv 12^2 \equiv 1 \pmod{13}$
$2^2 \equiv 11^2 \equiv 4 \pmod{13}$
$3^2 \equiv 10^2 \equiv 9 \pmod{13}$
$4^2 \equiv 9^2 \equiv 3 \pmod{13}$
$5^2 \equiv 8^2 \equiv 12 \pmod{13}$
$6^2 \equiv 7^2 \equiv 10 \pmod{13}$

1 , 3 , 4 , 9 , 10 , 12 are the quadratic residues of 13 while the nonresidues are 2 , 5 , 6, 7, 8 ,11.

Observe that integers between 1 and 12 are divided equally among the quadratic residues and nonresidues.

Lemma ***6.2:***

Let p be an odd prime and a an integer not divisible by p.Then the congruence $x^2 \equiv$ a (mod p),

has either no solution or exactly two incongruent solutions modulo p.

Theorem ***6.3:***

If p is an odd prime, then there are exactly (p-1)/2 quadratic residues of p and (p-1)/2 quadratic

nonresidues of p among the integers 1 , 2 ,...., p-1.

Proof :

To find all the quadratic residues of p among the integers 1, 2,....., p-1 ,we compute the least positive residues modulo p, of the squares of the integers 1, 2,...,p-1.

Since there are p -1 squares to consider and since each congruence $x^2 \equiv$ a (mod p) has either

zero or two solutions, there must be exactly (p-1)/2 quadratic residues of p among the integers 1, 2,....,p-1.The remaining

(p-1)-(p-1)/2 = (p-1)/2 positive integers less than p-1 are quadratic nonresidues of p.

Definition ***6.4:***

Let p be an odd prime and a an integer not divisible by p. The Legendre symbol $\left[\frac{a}{p}\right]$ is defined by

$$\left[\frac{a}{p}\right] = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue of } p \end{cases}$$

This symbol is named after the French mathematician Adrien - Marie Legendre.

Example (**2**):

The previous example shows that the legendre symbol $\left[\frac{a}{p}\right]$, a = 1 ,2 ,...,12 have the following values:

$$\left[\frac{1}{13}\right] = \left[\frac{3}{13}\right] = \left[\frac{4}{13}\right] = \left[\frac{9}{13}\right] = \left[\frac{10}{13}\right] = \left[\frac{12}{13}\right] = 1,$$

$$\left[\frac{2}{13}\right] = \left[\frac{5}{13}\right] = \left[\frac{6}{13}\right] = \left[\frac{7}{13}\right] = \left[\frac{8}{13}\right] = \left[\frac{11}{13}\right] = -1.$$

Theorem ***6.5*** *:*

Euler's criterion

Let p be an odd prime and let a be a positive integer not divisible by p.

Then $\left[\frac{a}{p}\right] \equiv a^{(p-1)/2} \pmod p$.

Proof :

First assume that $\left[\frac{a}{p}\right] = 1$, then the congruence $x^2 \equiv a \pmod p$ has a solution say $x=x_0$.

Using F.L.T ,we see that,

$a^{(p-1)/2} \equiv (x_0^2)^{p-1/2} \equiv 1 \pmod p$.

Hence, if $\left[\frac{a}{p}\right] = 1$, we know that $\left[\frac{a}{p}\right] \equiv a^{(p-1)/2} \pmod p$.

Now consider the case where $\left[\frac{a}{p}\right] = -1$, then the congruence $x^2 \equiv a \pmod p$ has no solutions.

By Theorem 3.4. for each integer i such that $1 \le i \le p-1$, there is a unique integer j with $1 \le j \le p-1$, such that $ij \equiv a \pmod p$.

Furthermore since the congruence $x^2 \equiv a \pmod p$,

has no solution , we know that $i \neq j$. Thus we can group the integers 1, 2,....,p-1 into (p-1)/2

pairs each with product congruent to a. Multiplying these pairs together we find that $(p-1)! \equiv a^{(p-1)/2} \pmod p$.

Since Wilsons Theorem tells us that $(p-1)! \equiv -1 \pmod p$. So

$-1 \equiv a^{(p-1)/2} \pmod p$.

So we have $\left[\frac{a}{p}\right] \equiv a^{(p-1)/2} \pmod p$.

Example (**3**):

Let p = 23 and a = 5 .Since $5^{11} \equiv -1 \pmod{23}$,

Euler's criterion tells us that $\left[\frac{5}{23}\right] = -1$, so 5 is a quadratic nonresidues of 23.

Corollary ***6.6*** *:*

Let p be an odd prime and (a,p) = 1, then a is a quadrate residues or nonresidues of p according as

$$a^{(p-1)/2} \equiv 1 \pmod p \quad \text{or} \quad a^{(p-1)/2} \equiv -1 \pmod p.$$

Example (4):

In the case p = 13, we find that

$2^{(13-1)/2} = 2^6 = 64 \equiv 12 \equiv -1 \pmod{13}$.

So 2 is a quadratic nonresidue of 13.

Since

$3^{(13-1)/2} = 3^6 = (27)^2 \equiv 1^2 \equiv 1 \pmod{13}$,

so 3 is a quadratic residue of 13 , and so the congruence $x^2 \equiv 3 \pmod{13}$ is solvable, in fact its two incongruent solution are $x \equiv 4$ and 9 (mod 13).

Theorem ***6.7:***

Let p be an odd prime and a and b are integers not divisible by p , then

(i) If $a \equiv b \pmod{p}$ then $\left[\frac{a}{p}\right] = \left[\frac{b}{p}\right]$.

(ii) $\left[\frac{a}{p}\right]\left[\frac{b}{p}\right] = \left[\frac{ab}{p}\right]$.

(iii) $\left[\frac{a^2}{p}\right] = 1$.

Proof :

(i) If $a \equiv b \pmod{p}$, then $x^2 \equiv a \pmod{p}$ has a solution iff $x^2 \equiv b \pmod{p}$ has a solution ,

hence $\left[\frac{a}{p}\right] = \left[\frac{b}{p}\right]$.

(ii) By Euler's criterion we know that

$\left[\frac{a}{p}\right] \equiv a^{(p-1)/2} \pmod{p}$, $\left[\frac{b}{p}\right] = b^{(p-1)/2} \pmod{p}$.

$\left[\frac{ab}{p}\right] \equiv (ab)^{(p-1)/2} \pmod{p}$.

Hence $\left[\frac{a}{p}\right]\left[\frac{b}{p}\right] \equiv a^{(p-1)/2} . b^{(p-1)/2}$

$\equiv (ab)^{(p-1)/2} \equiv \left[\frac{ab}{p}\right] \pmod{p}$.

Since the only possible values of a legendre symbol are ± 1 , we conclude that $\left[\frac{a}{p}\right]\left[\frac{b}{p}\right] = \left[\frac{ab}{p}\right]$.

(iii) Since $\left[\frac{a}{p}\right] = \pm 1$ from befor (ii) it follows that $\left[\frac{a^2}{p}\right] = \left[\frac{a}{p}\right]\left[\frac{a}{p}\right] = 1$.

Corollary ***6.8:***

If p is an odd prime , then

$$\left[\frac{-1}{p}\right] = \begin{cases} 1 & if \quad p \equiv 1 \pmod{4} \\ -1 & if \quad p \equiv -1 \pmod{4} \end{cases}$$

Proof :

By Euler's criterion we know that

$\left[\frac{-1}{p}\right] \equiv (-1)^{(p-1)/2} \pmod{p}$,

if $p \equiv 1 \pmod{4}$, then $p = 4k+1$ for some integer k , thus

$(-1)^{(p-1)/2} = (-1)^{4k+1-1/2} = (-1)^{2k} = 1$, so that,so that $\left[\frac{-1}{p}\right] = 1$.

if $p \equiv 1 \pmod{4}$, then $p = 4k+3$ for some integer k ,

thus

$(-1)^{(p-1)/2} = (-1)^{4k+3-1/2} = (-1)^{2k+1/2} = -1$,

so that $\left[\frac{-1}{p}\right] = -1$.

Example (5):

Show that the congruence $x^2 \equiv -38 \pmod{13}$ is solvable.

Solution *:*

This can be done by evaluating the symbol $\left[\frac{-38}{13}\right]$

$$\left[\frac{-38}{13}\right] = \left[\frac{-1}{13}\right].\left[\frac{38}{13}\right] = 1\left[\frac{38}{13}\right] = \left[\frac{38}{13}\right]$$

since $38 \equiv 12 \pmod{13} \Rightarrow$

$$\left[\frac{38}{13}\right] = \left[\frac{12}{13}\right] = \left[\frac{3.2^2}{13}\right] = \left[\frac{3}{13}\right]\left[\frac{2^2}{13}\right] = \left[\frac{3}{13}\right]$$

$$\left[\frac{3}{13}\right] \equiv 3^{(13-1)/2} \equiv 3^6 \equiv (27)^2 \equiv 1^2 \equiv 1 \pmod{13},$$

hence $\left[\frac{3}{13}\right] = 1$ i.e., $\left[\frac{-38}{13}\right] = 1$, so $x^2 \equiv -38 \pmod{13}$, admit solution.

Lemma ***6.9:***

Gauss Lemma.

Let p be an odd prime and a an integer with (a, p)=1.

If s is the number of least positive residues of the integers a,2a,3a,..., ,$(\frac{p-1}{2})$ a, that are

greater than p/2, then $\left[\frac{a}{p}\right] = (-1)^s$.

Example (6):

Let a = 5 and p = 11 , find $\left[\frac{5}{11}\right]$ by Gauss lemma .

Solution *:*

We compute the L.P.Residues of 1.5 , 2.5, 3.5, 4.5 and 5.5 . These are 5 , 10 , 4 , 9

and 3 respectively.

Since exactly two of these are greater than 11/2 they are 9 , 10 so by Gauss lemma

$$\left[\frac{5}{11}\right] = (-1)^2 = 1.$$

Theorem ***6.10*** *:*

If p is an odd prime , then $\left[\frac{2}{p}\right] = (-1)^{(p^2-1)/8}$.

Hence 2 is a quadratic residue of all primes $p \equiv \pm 1 \pmod{8}$ and a quadratic nonresidue of all

primes $p \equiv \pm 3 \pmod{8}$.

Or in another way we say that if p is an odd prime , then

$$\left[\frac{2}{p}\right] = \begin{cases} 1 & if \ p \equiv 1 \pmod{8} \ or \ p \equiv 7 \pmod{8} \\ -1 & if \ p \equiv 3 \pmod{8} \ or \ p \equiv 5 \pmod{8} \end{cases}.$$

Example (7):

By theorem above we see that

$$\left[\frac{2}{7}\right] = \left[\frac{2}{17}\right] = \left[\frac{2}{23}\right] = \left[\frac{2}{31}\right] = 1,$$

while

$$\left[\frac{2}{3}\right] = \left[\frac{2}{5}\right] = \left[\frac{2}{11}\right] = \left[\frac{2}{13}\right] = \left[\frac{2}{19}\right] = \left[\frac{2}{29}\right] = -1.$$

Example (8):

Evaluate $\left[\frac{317}{11}\right]$.

Solution *:*

Since $317 \equiv 9 (\mathrm{mod}\, 11)$ by part (i) in Theorem 6.7

$\left[\frac{317}{11}\right] = \left[\frac{9}{11}\right] = \left[\frac{3^2}{11}\right] = 1,$ (by part (iii) of Theorem 6.7).

Example (9):

Evaluate $\left[\frac{89}{13}\right]$.

$89 \equiv -2 (\mathrm{mod}\, 13) \Rightarrow \left[\frac{89}{13}\right] = \left[\frac{-2}{13}\right] = \left[\frac{-1}{13}\right]\left[\frac{2}{13}\right].$

Since $13 \equiv 1$ (mod 4) by corollary 6.8 $\left[\frac{-1}{13}\right] = 1.$

Since $13 \equiv$ -5 (mod 8) by Theorem 6.10 $\left[\frac{2}{13}\right] = -1.$

Consequently $\left[\frac{89}{13}\right] = -1.$

The Law of Quadrate Reciprocity

Theorem ***6.11***

Let p and q be odd primes , then $\left[\frac{p}{q}\right]\left[\frac{q}{p}\right] = (-1)^{\left(\frac{p-1}{2}\,\frac{p-1}{2}\right)}$.

Corollary ***6.12:***

If p and q are distinct odd primes , then

$$\left[\frac{p}{q}\right]\left[\frac{q}{p}\right] = \begin{cases} 1 & \text{if } p \equiv 1 (\mathrm{mod}\, 4) \text{ or } q \equiv 1 (\mathrm{mod}\, 4) \text{ or both} \\ -1 & \text{if } p \equiv q \equiv 3 (\mathrm{mod}\, 4) \end{cases}$$

since the only possible values of $\left[\frac{p}{q}\right]$ or $\left[\frac{q}{p}\right]$ are ± 1 , we see that

$$\left[\frac{p}{q}\right] = \begin{cases} \left[\frac{p}{q}\right] & \text{if } p \equiv 1 (\mathrm{mod}\, 4) \text{ or } q \equiv 1 (\mathrm{mod}\, 4) \text{ (or both)} \\ \left[\frac{q}{p}\right] & \text{if } p \equiv q \equiv 3 \ (\mathrm{mod}\, 4) \end{cases}$$

This means that if p and q are odd primes, then $\left[\frac{p}{q}\right] = \left[\frac{q}{p}\right]$ unless both p and q are

congruent to 3 modulo 4,

and in that case $\left[\frac{p}{q}\right] = \left[-\frac{q}{p}\right].$

Example (10):

Show that $x^2 \equiv 13(\mathrm{mod}\,17)$ is solvable.

Solution *:*

Let p = 7 and q = 17, since $p \equiv q \equiv 1$ (mod 4) then the law of the quadratic reciprocity shows that

$\left[\frac{13}{17}\right] = \left[\frac{17}{13}\right]$,

since $17 \equiv 4(\mathrm{mod}\,13)$ by Theorem 6.7 $\left[\frac{17}{13}\right] = \left[\frac{4}{13}\right] = \left[\frac{2^2}{13}\right] = 1.$

Thus $\left[\frac{13}{17}\right] = 1 \Rightarrow x^2 \equiv 13(\mathrm{mod}\,17)$ is solvable.

Example (**11**):

Let p = 7 and q = 19, since $p \equiv q \equiv 3$ (mod 4),then the law of the quadratic eciprocity show that

$\left[\frac{7}{19}\right] = -\left[\frac{19}{7}\right]$

$-\left[\frac{19}{7}\right] = -\left[\frac{5}{7}\right]$ since $19 \equiv 5(\mathrm{mod}\,7)$.

since $5 \equiv 1(\mathrm{mod}\,4)$, by law of the quadratic eciprocity we have $\left[\frac{5}{7}\right] = \left[\frac{7}{5}\right]$.

Thus

$\left[\frac{7}{19}\right] = -\left[\frac{19}{7}\right] = -\left[\frac{5}{7}\right] = -\left[\frac{7}{5}\right] = -\left[\frac{2}{5}\right]$ (since $7 \equiv 2(\mathrm{mod}\,5)$)

$= -(-1) = 1$ (since $5 \equiv 5(\mathrm{mod}\,8)$) .

Example (**12**) :

Calculate $\left[\frac{713}{1009}\right]$ (1009 is a prime)

Solution *:*

Factor $713 = 23 \cdot 31$

$\left[\frac{713}{1009}\right] = \left[\frac{23.31}{1009}\right] = \left[\frac{23}{1009}\right]\left[\frac{31}{1009}\right]$

using the law of reciprocity we have 1009 ≡ 1 (mod 4).

$\left[\frac{23}{1009}\right] = \left[\frac{1009}{23}\right]$

$\left[\frac{1009}{23}\right] = \left[\frac{20}{23}\right]$

$\left[\frac{20}{23}\right] = \left[\frac{2^2.5}{23}\right] = \left[\frac{5}{23}\right]$

by the law of quadratic reciprocity $5 \equiv 1$ (mod 4)

$\left[\frac{31}{1009}\right] = \left[\frac{1009}{31}\right]$

$\left[\frac{1009}{31}\right] = \left[\frac{17}{31}\right]$

$\left[\frac{5}{23}\right] = \left[\frac{23}{5}\right] = \left[\frac{3}{5}\right] = \left[\frac{5}{3}\right] = \left[\frac{2}{3}\right] = -1,$ thus $\left[\frac{23}{1009}\right] = -1,$
similarly

$$\left[\frac{17}{31}\right] = \left[\frac{31}{17}\right] = \left[\frac{14}{17}\right] = \left[\frac{2}{17}\right]\left[\frac{7}{17}\right]$$
$$= \left[\frac{7}{17}\right] = \left[\frac{17}{7}\right] = \left[\frac{3}{7}\right] = -\left[\frac{7}{3}\right] = -\left[\frac{4}{3}\right] = -\left[\frac{2^2}{3}\right] = -1$$

consequently $\left[\frac{31}{1009}\right] = -1.$

therefore $\left[\frac{713}{1009}\right] = (-1)(-1) = 1.$