SHIVAJI UNIVERSITY, KOLHAPUR

CENTRE FOR DISTANCE EDUCATION

Number Theory

(Mathematics)

For

M. Sc. Part-II : Semester-III

Paper (MT 303)

(Academic Year 2021-22 onwards)

Unit-1

DIVISIBILITY

1.1 This chapter requires very basic ideas in mathematics. In fact high school mathematics is enough. We now proceed to prove a theorem which is a foundation stone for development in number theory.

Principle of well – ordering

Every non-empty set S of non-negative integers has a least element. That is, there is $a \in S$ such that $a \le b$, for all $b \in S$.

Theorem. (Division Algorithm)

Given integers a and b with $b > 0$, there exist unique integers q and r satisfying

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

The integers q and r are called respectively quotient and remainder in the division of a by b.

Proof. Let us consider the set

$$S = \{a - xb : x \text{ is integer}, a - xb \ge 0\}.$$

Claim : S is non-empty.

Consider $x = -|a|$, then $a - xb = a - \left(-|a|\right)b = a + |a|b \ge a + |a| \ge 0.$

Thus S is non empty. Thus by well – ordering principle S has a least element say r. Clearly, $0 \le r$.

Further, there is an integer q such that $r = a - q\,b$ that is $a = bq + r$.

Claim: $r < b$.

Suppose on the contrary that $r \ge b$.

Consider $a-(q+1)b=(a-qb)-b=r-b\ge 0$. Therefore, $a-(q+1)b \in S$. Thus

$$a-(q+1)=r-b<r\in S,$$

which contradicts minimality of r. Hence, $r < b$.

Thus, $0 \le r < b$.

Uniqueness: Let if possible there be integers q', r' such that $a = bq' + r', 0 \le r' < b$. Thus

$$bq+r=bq'+r' \Rightarrow r-r'=b(q'-q) \Rightarrow |r-r'|=b|q'-q|.$$

Now, $0 \le r' < b \Rightarrow -b < -r' \le 0$. This together with $0 \le r < b$, we obtain $-b < r - r' < b$. Thus, $|r-r'| < b$. Therefore, $b|q'-q| = |r-r'| < b \Rightarrow |q'-q| < 1 \Rightarrow q = q'$. Hence $r = r'$. This proves uniqueness.

Corollary : If a and b are integers with $b \neq 0$, then there exist integers q and r such that $a = bq + r, \quad 0 \leq r < |b|$.

Proof. If $b > 0$ there is nothing to prove. Suppose $b < 0$, then $-b > 0$. Therefore, there exist unique integers q and r such that $a = (-b)q + r,\ 0 \leq r < -b$. Thus, $a = b(-q) + r,\ 0 \leq r < -b$. Hence, in any case $a = bq + r, \quad 0 \leq r < |b|$.

Ex. 1. Square of an integer is of the form 4k or 4k + 1.

Solution. : We know that any integer is of the form 2k or 2k + 1. Therefore, square of an integer is of the from $(2k)^2 = 4k^2$ or $(2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$, which is precisely of the form $4k$ or $4k + 1$.

Notes : 1. Observe that what the above theorem says is that no integer of the form 4k + 2 or 4k + 3 can ever be perfect square.

2. Square of any odd integer is of the form 8k + 1.

Ex. 2. Show that the expression $\frac{a(a^2+2)}{3}$ is an integer for all $a \geq 1$.

Solution. Any integer $a \geq 1$ has one of the form 3k, 3k + 1 and 3k + 2.

a is the form of $3k$: Consider

$\frac{a(a^2+2)}{3} = \frac{3k(9k^2+2)}{3} = k(9k^2+2)$, which is an integer.

a is of the form $3k+1$: Consider

$\frac{a(a^2+2)}{3} = \frac{(3k+1)(9k^2+6k+3)}{3} = (3k+1)(3k^2+2k+1)$, an integer.

a is of the form $3k+2$: Consider

$\frac{a(a^2+2)}{3} = \frac{(3k+2)(9k^2+12k+6)}{3} = (3k+2)(3k^2+4k+2)$, an integer.

Thus is any case $\frac{a(a^2+2)}{3}$ is an integer.

Ex.3. Prove that any integer of the form of 6k + 5 is also of the form 3j + 2 but not conversely.

Solution. Any integer of the form 6k + 5 is can be written as

$$6k + 5 = 6k + 3 + 2 = 3(2k+1) + 2 = 3j + 2$$

The integer 8 is of the form 3j + 2 but not the form 6k + 5.

Ex.4. The square of any integer is of the form 3k or 3k + 1.

Solution. Any integer a has one of the three form 3k, 3k + 1 or 3k + 2.

Form 3k : $(3k)^2 = 9k^2 = 3(3k^2)$

That is, of the form of 3k.

Form 3k + 1: $(3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$.

That is the form of 3k + 1.

Form 3k + 2 : $(3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$

This is the form of 3k + 1

Ex. 5. Prove that $3a^2 - 1$ is never a perfect square .

Solution. We know that square of an integer is of the form 3k or 3k + 1 i.e. no number of the form 3k + 2 can ever be a perfect square. Observe that,

$3a^2 - 1 = 3(a^2 - 1) + 2$ is of the form 3k + 2 and hence it can never be a perfect square.

Ex.6. Prove that cube of an integer has one of the form 9k, 9k + 1, 9k + 8.

Solution. Any integer has one of the forms 3k, 3k + 1 or 3k + 2.

Form 3k : $(3k)^3 = 27k^3 = 9(3k^3)$.

This is the form of 9k.

Form 3k + 1 : $(3k+1)^3 = 27k^3 + 27k^2 + 9k + 1 = 9(3k^3 + 3k^2 + k) + 1$.

This is the form of 9k + 1.

Form 3k + 2 : $(3k+2)^3 = 27k^3 + 54k^2 + 36k + 8 = 9(3k^3 + 6k^2 + 4k) + 8$.

This is of the form 9k + 8.

Ex.7. Prove that for any integer a one of the integers $a, a+2, a+4$ is divisible by 3.

Solution. Any integer is of the form $3k, 3k+1,$ or $3k+2$. Let a be of the form $3k$ then a is divisible by 3, now if a is of the form $3k+1$, then $a+2$ is divisible by 3 and finally if a is of the form $3k+2$, then $a+4$ is divisible by 3.

Ex.8. Prove that sum of squares of two odd integers cannot be a perfect square.

Solution,. We know that, square of an odd integers is of the form 8k + 1. There are two odd integers so that sum of squares of two odd integers is of the form (8m + 1) + (8n + 1) = 8(m+n) + 2. That is, sum of squares of an odd integers is of the form 8k + 2 which can never be a perfect square.

Ex.9. Prove that the product of four consecutive integer is 1 less than a perfect square.

Solution. It is enough to prove that

$a(a+1)(a+2)(a+3)+1$ is a perfect square.

Consider

$a(a+1)(a+2)(a+3)+1 = a(a^3+6a^2+11a+6)+1$.

Also consider

$$\left[(a+1)(a+2)-1\right]^2 = (a+1)^2(a+2)^2 - 2(a+1)(a+2)+1$$

$$= (a^2+2a+1)(a^2+4a+4) - 2(a^2+3a+2)+1$$

$$= a^4+4a^3+4a^2+2a^3+8a^2+8a+a^2+4a+4-2a^2-6a-4+1$$

$$= a^4+6a^3+11a^2+6a+1$$

$$= a(a^3+6a^2+11a+6)+1.$$

Thus $a(a^3+6a^2+11a+6)+1 = \left[(a+1)(a+2)-1\right]^2$.

(Also

$$\left[a(a+3)+1\right]^2 = a^2(a+3)^2 + 2a(a+3)+1$$

$$= a^2(a^2+6a+9) + 2a^2+6a+1$$

$$= a^4+6a^3+9a^2+2a^2+6a+1$$

$$= a^4+6a^3+11a^2+6a+1$$

$$= a(a^3+6a^2+11a+6)+1$$

Thus,

$$a(a^3+6a^2+11a+6)+1 = \left[(a+1)(a+2)-1\right]^2 = \left[a(a+3)+1\right]^2)$$

Thus, $a(a+1)(a+2)(a+3)+1$ is a perfect square.

Ex.10. Establish that the difference of two consecutive cubes is never divisible by 2.

Solution. Let the consecutive numbers be a and $a+1$.

Consider, $(a+1)^3 - a^3 = 3a^2+3a+1 = 3a(a+1)+1$.

Since $a(a+1)$ is always of the form 2k, that is divisible by 2. Therefore difference of two consecutive cubes is of the form 2k + 1 which is never divisible by 2.

EXERCISES 1.1.

1. The 4^{th} power of any integer is either of the form 5k or 5k + 1.
2. For $n \geq 1$, prove that $\dfrac{n(n+1)(2n+1)}{6}$ is an integer.
3. For $n \geq 1$, prove that $\dfrac{n(n+1)(n+2)}{6}$ is an integer.

1.2 Divisibility

Definition: Let $a(a \neq 0)$ and b be integers then we say that a divides b if there is an integer c such that $ac = b$ in this case we write $a \mid b$.

Theorem : For integers *a, b, c* the following hold

a) $a \mid 0, 1 \mid a, a \mid a$

b) $a \mid 1$ iff $a = \pm 1$

c) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

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

e) $a \mid b$ and $b \mid a$, iff $a = \pm b$.

f) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

g) If $a \mid b$ and $a \mid c$, then $a \mid bx + cy$ for arbitrary integers x and y.

Proof. a) $a \cdot 0 = 0 \Rightarrow a \mid 0;\ 1 \cdot a = a \Rightarrow 1 \mid a;\ a \cdot 1 = a \Rightarrow a \mid a.$

b) $a \mid 1 \Leftrightarrow ab = 1$ for some integer b $\Leftrightarrow a = \pm 1$.

c) $a \mid b$ and $c \mid d \Rightarrow aa_1 = b$ and $cc_1 = d \Rightarrow aa_1 \cdot cc_1 = bd \Rightarrow ac(a_1c_2) = bd \Rightarrow ac \mid bd$.

d) $a \mid b$ and $b \mid c \Rightarrow aa' = b$ and $bb' = c \Rightarrow aa' \cdot b' = c \Rightarrow a \mid c$.

e) $a \mid b$ and $b \mid a \Rightarrow aa' = b$ and $bb' = a \Rightarrow aa'b' = a \Rightarrow a'b' = 1$
$\Rightarrow a' = \pm 1$ and $b' = \pm 1$.

Thus $a = \pm b$.

f) $a \mid b$ and $b \neq 0 \Rightarrow aa' = b$ with $a' \neq 0 \Rightarrow |a||a'| = |b| \Rightarrow |a| \leq |b|$ (because $|a'| \geq 1$).

g) $a \mid b$ and $a \mid c \Rightarrow aa' = b$ and $aa'' = c \Rightarrow bx + cy = aa'x + aa''y = a(a'x + a''y)$.

Thus $a \mid bx+cy$.

Definition (Common Divisor): Let a and b be two integers at least one of which is non zero, an integer c is common divisor of a and b, if $c \mid a$ and $c \mid b$.

Definition (Greatest Common Divisor): Let a and b be two integers at least one of which is non zero. Then a positive integer d is a greatest common divisor of a and b if

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

b) whenever c is a positive integer such that $c \mid a$ and $c \mid b$ then $c \leq d$.

Theorem. Given integers a and b not both of which are zero, there exist integers x and y such that $\gcd(a, b) = ax + by$.

Proof. Let us define

$S = \{au + bv : au + bv > 0, u, v \text{ are integers}\}$.

Note that $|a| = au + b.0$ where $u = 1$ and $u = -1$ according as $a > 0$ and $a < 0$. Therefore, S is non-empty set of positive integers. Hence, we can invoke principle of well-ordering which assures of a least positive integer $d \in S$. Therefore, there exist integers x and y such that $d = ax + by$.

By division algorithm there exists integers q and r such that,

$$a = dq + r, \quad 0 \le r \le d.$$

Then $r = a - dq = a - (ax + by)q = a(1 - xq) + b(-yq)$.

Hence, $r \in S$. But it contradicts minimality of d unless $r = 0$. Thus $r = 0$. Therefore $a = dq$ and so $d \mid a$ and similarly $d \mid b$.

Let c be a positive common divisor of a and b , then $c \mid a$ and $c \mid b$ hence $c \mid ax + by = d$. Thus $c \mid d$. Therefore, $c = |c| \le |d| = d$. Thus d is gcd of a and b .

Corollary – If a and b are given integers not both zero. Then the set $S = \{ax + by : x, y \text{ integers}\}$ is precisely the set of all multiples of $d = \gcd(a,b)$.

Proof. Suppose $d = \gcd(a,b)$ so that $d \mid a$ and $d \mid b$. Hence, $d \mid ax + by$, that is, $ax + by$ is multiple of d. On the other hand $d = \gcd(a,b)$, then there exist integers u, v such that $d = au + bv$. Therefore, $cd = a(cu) + b(cv)$ is of the form $ax + by$.

Definition (Relativity Prime integers)

Two integers a and b, not both of which are zero, are relativity prime if $\gcd(a,b) = 1$.

Theorem – Let a and b be integers, not both zero then a and b are relativity prime if and only if there exist integers x and y such that $1 = ax + by$

Proof. Suppose a and b are relativity prime then $\gcd(a,b) = 1$ and there exist integers x and y such that $ax + by = 1$. Conversely, suppose $ax + by = 1$. Let $d = \gcd(a,b)$, then $d \mid a$ and $d \mid b$. Therefore, $d \mid ax + by = 1$. Since $d > 0$ and $d \mid 1$, we must have $d = 1$. Hence, a and b are relatively prime.

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

Proof. Suppose $d = \gcd(a,b)$, then $d \mid a$ and $d \mid b$, so that $\frac{a}{d}$ and $\frac{b}{d}$ are integers. Since $d = \gcd(a,b)$ there exist two integers x and y such that $d = ax + by$ so that $1 = \frac{a}{d}x + \frac{b}{d}y$.

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

Corollary 2. Let $a \mid c$ and $b \mid c$ with $\gcd(a,b) = 1$, then $ab \mid c$.

Proof. Since $\gcd(a,b)=1$ and there exist integers x and y such that $ax+by=1$, so that $c=c\cdot 1=c\cdot(ax+by)=(ca)x+(cb)y$. Since $a\mid c$ and $b\mid c$ there exist integers u and v such that $au=c$ and $bv=c$. Thus $c=(ca)x+(cb)y=(ab)vx+(ab)uy=(ab)(vx+uy)$. Therefore, $ab\mid c$.

Note : Let $a=6, b=4$ and $c=12$. Here $\gcd(6,4)=2\neq 1$ and $6\mid 12$ also $4\mid 12$ but $24\nmid 12$.

On the other hand, let a = 6, b = 4 and c = 24. Here gcd(6, 4) = 2 ≠ 1 and 6 | 24 also 4 | 24 and 24 | 24. Therefore, gcd(a, b) = 1 is sufficient but not necessary for $ab \mid c$.

Theorem – (Euclid's Lemma) If $a\mid bc$ with $\gcd(a,b)=1$, then $a\mid c$.

Proof. Suppose $\gcd(a,b)=1$, then there exist two integers x and y such that $ax+by=1$. Thus $c(ax+by)=c.1=c\Rightarrow acx+bcy=c.$ Since $a\mid bc$, $a\mid acx+bcy=c.$

Note. Consider the example, $12\mid 6\times 8$ with $\gcd(12,6)=6\neq 1$, here $12\nmid 8$.

Ex. Give integers a, b, c such that $a \mid bc$, gcd(a, b) ≠ 1 but still $a \mid c$. In other words gcd(a, b) = 1 is sufficient but not necessary in the above result.

Theorem. Let a and b be integers not both zero. For a positive integer $d, d=\gcd(a,b)$ if and only if

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

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

Proof. Suppose $d=\gcd(a,b)$, then by definition (i) is obvious. Since $d=\gcd(a,b)$, there exist integers x and y such that $d=ax+by$. Now $c\mid a$ and $c\mid b$ implies $c\mid ax+by=d$. Hence, $c\mid d$.

Conversely, suppose that the conditions hold. To prove that $d=\gcd(a,b)$, the first condition of gcd is already satisfied, so it remains to prove that the given conditions imply the second condition of gcd. Suppose that c is a positive integer such that $c\mid a$ and $c\mid b$, then by hypothesis (ii), $c\mid d$ this implies $c=|c|\leq|d|=d$.

Least common multiple(lcm). The *least common multiple* of two nonzero integers a and b, denoted by $lcm(a,b)$, is the positive integer m satisfying the following conditions

i) $a\mid m$ and $b\mid m$

ii) If $a\mid c$ and $b\mid c$, with $c>0$, then $m\leq c$.

Note: Given non zero integers a and b, $lcm(a,b)$ always exists and that $lcm(a,b)\leq|ab|$.

We shall now prove relation between gcd and lcm.

Theorem: Let a and b be positive integers then, $lcm(a,b)\gcd(a,b)=ab$.

Proof.Let $d=\gcd(a,b)$, then $d\mid a$ and $d\mid b$, so that there exist integers r and s such that $a=dr$ and $b=ds$. Let $m=\frac{ab}{d}$, then $m=rb$ and $m=as$ so that $a\mid m$ and $b\mid m$, that is m is common multiple of a and b.

We shall prove that m is lcm of a and b. Let c be a positive common multiple of a and b. Then $c = au = bv$ for some integers u and v. Since $d = \gcd(a,b)$, there exist integers x and y such that $d = ax + by$. Consider

$$\frac{c}{m} = \frac{cd}{md} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \frac{c}{b}x + \frac{c}{a}y = vx + uy \left(\text{Since md = ab}\right)$$

which is an integer. Thus $\frac{c}{m} \geq 1 \Rightarrow c \geq m$. Therefore, $m = lcm(a,b)$. Thus $lcm(a,b) = \frac{ab}{d}$, that is $lcm(a,b)\gcd(a,b) = ab$.

We shall now go through some illustrative examples

Ex.1. Prove that, for a positive integer n and any integer $a, \gcd\left(a, a+n\right)$ divides n, hence $\gcd\left(a, a+1\right) = 1$.

Solution. Let $d = \gcd(a, a+n)$, then $d \mid a$ and $d \mid a+n$ implies $d \mid a+n-a = n$.

Thus if $d = \gcd\left(a, a+1\right)$ then $d \mid 1 \Rightarrow d = 1$.

Ex.2. Assuming that $\gcd\left(a,b\right) = 1$ prove that $\gcd\left(a+b, a-b\right) = 1$ or 2.

Solution. Let $d = \gcd(a+b, a-b)$, then $d \mid a+b$ and $d \mid a-b$.

Thus $d \mid (a+b)+(a-b) = 2a$ and $d \mid (a+b)-(a-b) = 2b$.

Since $\gcd(a,b) = 1$, there exist integers x and y such that $ax + by = 1$. Therefore,

$d \mid 2(ax+by) = 2(1) = 2$. Thus $d = 1$ or $d = 2$.

Ex.3. Prove that, if a and b are both odd integers then $16 \mid a^4 + b^4 - 2$.

Solution. We know that the square of an odd integer is of the form 8k + 1. Hence

$$a^4 + b^4 - 2 = \left(8m+1\right)^2 + \left(8n+1\right)^2 - 2. \quad = (64\ (m^2+n^2) + 16\ (m+n)$$

$$= 16\ [4(m^2+n^2) + (m+n)$$

Thus $16 \left| a^4 + b^4 - 2 \right.$

Lemma. If $a = bq + r$, then $\gcd\left(a,b\right) = \gcd\left(b,r\right)$.

Proof. Let d = gcd (a, b) then $d \mid a$ and $d \mid b$. Let d' = gcd (b, r). Now $d \mid a$ and $d \mid b \Rightarrow d \mid a - bq = r$ and $d \mid b \Rightarrow d \mid b$ and $d \mid r \Rightarrow d \leq d'$. On the other hand d' = gcd (b, r) $\Rightarrow d' \mid b$ and $d' \mid r \Rightarrow d' \mid bq + r$ and $d' \mid b \Rightarrow d' \mid a$ and $d' \mid b \Rightarrow d' \geq d$. Thus $d = d'$, that is, gcd (a, b) = gcd (b, r)

Using this lemma we can find gcd of given two numbers as follows.

Ex.1 Find $\gcd\left(12378, 3054\right)$ and express $\gcd\left(12378, 3054\right)$ as $12378x + 3054y$.

Solution. Consider

12378 = 3054 x 4 + 162

3054 = 162 x 18 + 138

162 = 138 x 1 + 24

138 = 24 x 5 + 18

24 = 18 x 1 + 6

18 = 6 x 3 + 0

Thus $\gcd(12378,3054)=6$.

(Note. We can find gcd in fewer steps as follows.

12378=3054x4 + 162

3054=162x19 – 24

162=24x7 – 6

24=6x4 + 0 .

What we have done here is that of the two possible remainders162(12378=3054x4 + 162) and 162 – 3054 = - 2892 (12378=3054x5 – 2892) we choose numerically smaller value 162, further, we choose 24 from the two possible values 138 and 138 – 162 = - 24. This technique reduces number of steps.)

Here, gcd(12378,3054)=gcd(3054,162)=gcd(162,138)=gcd(138,24)=gcd(2,18)=6.

Now, we shall express gcd as $12378x+3054y$.

6 = 24 – 18 x 1

= 24 – (138 – 24 x 5)

= - 138 + 24 x 6

= - 138 + (162 – 138 x 1) 6

= 162 x 6 – 138 x 7

= 162 x 6 – (3054 – 162 x 18) x 7

= 162 x 132 – 3054 x 7

= (12378 – 3054 x 4) x 132 – 3054 x 7

= 12378 x 132 + 3054 (- 535)

Thus 6 = 12378 x 132 + 3054 (- 535) .

Theorem. If $k>0,$ then $\gcd(ka,kb)=k\cdot\gcd(a,b)$.

Proof. Let $d=\gcd(a,b)$ then $d\mid a$ and $d\mid b$. Therefore for any $k>0, kd>0$ and $kd\mid ka$ also $kd\mid kb$. Let c be a positive integer such that $c\mid ka$ and $c\mid kb$. Since $d=\gcd(a,b)$, there exist integers x and y such that $d=ax+by$. Thus $c\mid ka$ and $c\mid kb\Rightarrow c\mid k(ax+by)=kd$. Hence, $kd=\gcd(ka,kb)$. Thus, $\gcd(ka,kb)=k\cdot\gcd(a,b)$.

Corollary. For any integer $k\neq 0$, $\gcd(ka,kb)=|k|\gcd(a,b)$.

Proof. If $k>0$ there is nothing to prove. Let $k<0$, then there is $m>0$ such that $k=-m$.

Therefore, $\gcd(ma,mb)=m\cdot\gcd(a;b)\Rightarrow\gcd(-ka,-kb)=-k\cdot\gcd(a,b)$. Hence, $\gcd(ka,kb)=|k|\cdot\gcd(a,b)$.

Exercises 1.2.

1. If $a\mid b$, show that $(-a)\mid b, a\mid(-b), (-a)\mid(-b)$.
2. If $a\mid b$, then prove that $a\mid bc$.
3. If $a\mid b$, then prove that $ac\mid bc$. Is the converse true.
4. Prove or disprove. If $a\mid b+c$ then $a\mid b$ or $a\mid c$.
5. Assuming that $\gcd(a,b)=1$, prove that $\gcd(2a+b,a+2b)=1$ or 3.
6. If $\gcd(a,b)=1$, then for any nonzero integer c, $\gcd(ac,b)=\gcd(c,b)$.
7. Use Euclid's algorithm to find integer x and y such that , $\gcd(56,72)=56x+72y$.
8. Use Euclid's algorithm to find integer x and y such that ,

$\gcd(143,227)=143x+227y$.

1.3. Diophantine Equations

In general any equation in one or more unknowns which is to be solved in integers is Diophantine equation.

The name honours the Greek mathematician Diophantus. There is an interesting problems saying something about how long did Diophantus lived?

Ex.1. His boyhood lasted 1/6th of his life; his beard grew after 1/12th more, after 1/7th more he married, and his son was born 5 years later. The son lived to 1/2th his father age and the father died after four years after his son

Solution. Let x be the age of Diophantus when he died. From the given information we have

$$\frac{1}{6}x+\frac{1}{12}x+\frac{1}{7}x+5+\frac{1}{2}x+4=x$$

$$\Rightarrow\frac{1}{6}x+\frac{1}{12}x+\frac{1}{7}x++\frac{1}{2}x+9=x$$

$$\Rightarrow\frac{2}{12}x+\frac{1}{12}x+\frac{1}{7}x+\frac{1}{2}x+9=x$$

$$\Rightarrow\frac{2x+x+6x}{12}+\frac{1}{7}x+9=x$$

$$\Rightarrow\frac{9x}{12}+\frac{1}{7}x-x+9=0$$

$$\Rightarrow \frac{7\times 9x+12x-84x}{84}+9=0$$

$$\Rightarrow \frac{63x+12x-84x}{84}+9=0$$

$$\Rightarrow \frac{-3x}{28}+9=0 \Rightarrow 9=\frac{3x}{28} \Rightarrow 3x=252$$

$$\Rightarrow x=84.$$

Note. Diophantine equations may be of any degree and in any number of (variable) unknowns. However in this course, we are interested in linear Diophantine questions of the form $ax+by=c$. A Diophantine equation may have number of solutions.

e.g. $3.4 + 6.1 = 18$,

$3.2 + 6.2 = 18$.

$3(-2) + 6.4 = 18$.

That is (4, 1), (2, 2), (- 2, 4) are all solutions of $3x+6y=18$.

Theorem. The linear Diophantine equation $ax + by = c$ has a solution if and only if $d|c$ where $d=\gcd(a,b)$. If x_0, y_0 is any particular solution of this equation then all other solutions are given by $x=x_0+\left(\frac{b}{d}\right)t, y=y_0-\left(\frac{a}{d}\right)t$ where 't' is any arbitrary integer.

Proof – Let $d=\gcd(a,b)$ then $d|a$ and $d|b$. Suppose $ax + by = c$ has a solution, that is, there exist integers x and y such that $ax + by = c$. Since $d|a$ and $d|b$, we have $d \mid ax + by = c$. Thus $d|c$.

Conversely, suppose that $d|c$. Since $d=\gcd(a,b)$, there exist integers x_0 and y_0 such that $d=ax_0+by_0$. Since $d|c$ there is an integer *r* such that $dr = c$ .Thus ,

$$c=dr=(ax_0+by_0)r=a(x_0r)+b(y_0r)$$

Hence $x=x_0r, y=y_0r$ is a solution of $ax + by = c$.

This proves the first part of the theorem.

Suppose that, $ax + by = c$ has a solution (x_0,y_0) then $ax_0+by_0=c$.

Let (x,y) be any solution of $ax + by = c$, then

$$ax+by=ax_0+by_0 \Rightarrow a(x-x_0)=b(y-y_0) \qquad \text{---------- (1)}$$

Since $d=\gcd(a,b)$, there exist relatively prime integers r and s such that , $dr = a$ and $ds = b$. Thus (1) becomes

$$dr(x-x_0)=ds(y_0-y)$$

$\Rightarrow r(x-x_0)=s(y_0-y)$

Since $r \mid r(x-x_0)=s(y_0-y)$ and $\gcd(r,s)=1$ by invoking Euclid's lemma ,we obtain $r \mid y_0-y$.

Therefore, there is an integer 't' such that

$y_0-y=rt$

$\Rightarrow y=y_0-rt$

$\Rightarrow y=y_0-\left(\frac{a}{d}\right)t$

Further, $x-x_0=st$

$\Rightarrow x=x_0+st$

$\Rightarrow x=x_0+\left(\frac{b}{d}\right)t$

Let $x^1=x_0+\frac{b}{d}t$ and $y^1=y_0-\frac{a}{d}t$, then

$ax^1+by^1=a\left(x_0+\frac{b}{d}t\right)+b\left(y_0-\frac{a}{d}t\right)=ax_0+by_0=c$.

Thus every other solution of $ax+by=c$ is of the form $x=x_0+\frac{b}{d}t$ and $y=y_0-\frac{a}{d}t$ where 't' is an arbitrary integer.

Note. Thus there are infinitely many solutions of the given equation, one for each value of 't'.

Ex.1. Solve $172x+20y=1000$.

Solution. Here $\gcd(172,20)=4$ and $4 \mid 1000$. Therefore given Diophantine equation has a solution.

Consider,

$172=20\times 8+12$

$20=12\times 1+8$

$12=8\times 1+4$

$8=4\times 2+0$.

Thus $\gcd(172,20)=4$. Now

$4=12-8\times 1$

$=12-(20-12\times 1)1$

$$= 12 \times 2 - 20$$

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

$$= 172 \times 2 - 20 \times 17$$

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

Thus

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

Multiplying both sides by 250, we obtain

$$1000 = 172(500) + 20(-4250)$$

Thus, $(500, -4250)$ is a solution of given Diophantine equation.

General solution of given Diophantine equation is

$$x = x_0 + \frac{b}{d}t = 500 + \frac{20}{4}t = 500 + 5t$$

and

$$y = y_0 - \frac{a}{d}t = -4250 - \frac{172}{4}t = -4250 - 43t\ .$$

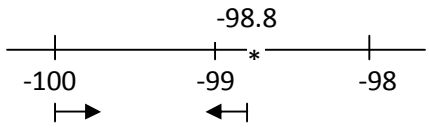
Thus, $(500 + 5t, -4250 - 43t)$ is general solution where 't' is an arbitrary integer.

We can proceed further to test whether the given equation has positive solution.

Consider,

$500 + 5t > 0$ and $-4250 + 43t > 0$

$\Rightarrow t > -100$ and $t \le \frac{-4250}{43} = -98.8$



$\Rightarrow t = -99$

$\Rightarrow x = 5$ and $y = 7$

Thus (5, 7) is the positive solution and that it is only positive solution.

Corollary. If $\gcd(a,b) = 1$ and it x_0, y_0 is particular solution of linear Diophantine equation $ax + by = c$ then all the solution are given by, $x = x_0 + bt, y = y_0 - at$.

Note : Certain Diophantive equations need not have positive solution at all.

Note. Each of the following Diophantine equations do not have solution.

a) $6x + 51y = 22$

b) $33x + 14y = 115$

c) $14x + 35y = 93$.

Ex.2. Determine all solution in the integers of the following Diophantine equation

a) $56x + 72y = 40$,

b) $24x + 138y = 18$,

c) $221x + 35y = 11$.

Solution. a) First of all we shall find the gcd of 56 and 72. Consider

$$72 = 56 \times 1 + 16$$

$$56 = 16 \times 3 + 8$$

$$16 = 8 \times 2 + 0.$$

Thus $\gcd(56, 72) = 8$ and that $8 \mid 16$, therefore solution exists.

Now $8 = 56 - 16 \times 3$

$$= 56 - 3 \times (72 - 56)$$

$$= 56 \times 4 + 72 \times (-3).$$

Thus, $8 = 56 \times 4 + 72 \times (-3)$.

Multiplying both sides by 5, we get,

$$40 = 56 \times 20 + 72 \times (-15).$$

Thus, (20, - 15) is solution of given Diophantine equation.

General solution of given Diophantine equation is

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

$$x = 20 + \frac{72}{8}t \quad y = -15 - \frac{56}{8}t$$

$$x = 20 + 9t \quad y = -15 - 7t.$$

Thus, $(20 - 9t, -15 - 7t)$ is general solution,where 't' is arbitrary integer.

We can proceed further to test whether the given equation has positive solution.

Consider,

$$20 + 9t > 0 \quad -15 - 7t > 0$$

$$t > \frac{-20}{9} \quad t < \frac{-15}{7}$$

$$t > -2.22 \quad t < -2.14.$$

Observe that there is no integer t satisfying the given conditions. Hence, there is no positive solution.

b) $24x + 138y = 18$

Here $\gcd(24,138)=6$ and that 6|18.

Therefore, the given Diophantine equation has a solution.

Consider,

$$138=24\times5+18$$

$$24=18\times1+6$$

$$18=6\times3+0$$

Thus, $\gcd(24,138)=6$. Now

$$6=24-18\times1$$

$$=24-(138-24\times5)$$

$$=24\times6+138(-1).$$

Thus

$$6=24\times6+138(-1).$$

Multiplying both the sides by 3.

$$18=24\times18+138\times(-3)$$

Thus (18, - 3) is solution of given equation. The general solution of the given equation is

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

$$x=18+\frac{138}{6}t \quad y=(-3)-\frac{24}{6}t$$

$$x=18+23t \quad y=-3-4t.$$

Thus, $(18+23t,-3-4t)$ is general solution, where 't' is arbitrary integer.

We can proceed further to test whether the given equation has positive solution.

Consider,

$$18+23t>0 \quad -3-4t>0$$

$$23t>-18 \quad -4t<3$$

$$t>\frac{-18}{23} \quad t<\frac{-3}{4}.$$

$$\Rightarrow t>-0.7826 \quad t<-0.75.$$

Observe that there is no integer t satisfying the given conditions. Hence, there is no positive solution.

c) $221x+35y=11.$

Here gcd (221, 35) = 1 and 1|11

Therefore the given Diophantine equation has a solution.

Consider,

$221 = 35 \times 6 + 11$

$35 = 11 \times 3 + 2$

$11 = 2 \times 5 + 1$

$2 = 2 \times 1 + 0$.

Therefore, $\gcd(221, 35) = 1$.

Now $1 = 11 - 2 \times 5$

$= 11 - 5 \times (35 - 11 \times 3)$

$= 35 \times (-5) + 11 \times 16$

$= 35 \times (-5) + 16 \times (221 - 35 \times 6)$.

Thus $1 = 221 \times 16 + 35 \times (-101)$.

Multiplying on both sides by 11, we get

$11 = 221 \times 16 + 35 \times (-1111)$.

Thus $(176, -1111)$ is solution of given Diophantine equation.

General solution of given Diophantine equation

$x = x_0 + \frac{b}{d}t \;\; y = y_0 - \frac{a}{d}t$

$x = 176 + \frac{35}{1}t \;\; y = (-1111) - \frac{221}{1}t$

$x = 176 + 35t \;\; y = -1111 - 221t$

Thus, $(176 + 35t, -1111 - 221t)$ is general solution.Where 't' is arbitrary integer.

We can proceed further to test whether the given equation has positive solution.

Consider,

$176 + 35t > 0 \Rightarrow t > \frac{-176}{35} \Rightarrow t > -5.028$

and

$-1111 - 221t < 0 \text{ implies } t < \frac{-1111}{221} \Rightarrow t < -5.0271$.

Observe that there is no integer t satisfying the given conditions. Hence, there is no positive solution.

Ex.3. A customer brought a dozen pieces of fruit apples and oranges, for $1.32. If an apple costs 3 – cents more than an orange and more apples than oranges were purchased. How many pieces of each kind were brought?

Solution – Let x be the number of apples and y be the number of oranges. Let z be the cost of oranges .

Then, $x + y = 12$ (1)

And $(z+3)x+zy=132$ (2)

From (2) we have

$$z(x+y)+3x=132$$

$$\Rightarrow 12z+3x=132$$

$$\Rightarrow 4z+x=44 \quad (3)$$

Here $\gcd(1,4)=1$ and $1|44$ Hence, Equation (3) has a solution. Now

$$1=4\times 1+1(-3)$$

$$\Rightarrow 44=4(44)+1(-132)$$

Thus (44, - 132) is a particular solution .

General Solution is,

$$z=44+t\ ,\ x=-132-4t \quad (4)$$

where t is any integer.

For positive solution we must have

$44+t>0$ and $-132-4t>0$

$\Rightarrow t>-44$ and $t<-33 \Rightarrow -44<t<-33$.

We shall now prepare the table of permissible values of x,y and z. In view of Equation(1) and Equation (4), we have

t	z	x	y	(z + 3) x + zy
- 35	9	8	4	132
- 34	10	4	8	132

Thus $x=8, y=4$ or $x=8, y=4$ are two possible solutions.

We have not listed other values of t because the values of x or y is zero or negative in those cases.

Since number of apples is more than oranges x = 8, y = 4 is the solution.

Ex. 4. If a cock is worth 5 coins a hen 3 coins and three chicks together 1 coin how many cocks, hens and chicks totaling 100 can be brought for 100 coins.

Solution. Let x be the number of cocks y be the number of hens and 'z' be the number of chicks.

Then $5x+3y+\frac{z}{3}=100$

And $x+y+z=100$

Thus $15x+9y+z=300$, (1)

$x+y+z=100$. (2)

From (1) and (2) we obtain

$4x+8y=200$.

That is $7x+4y=100$. (3)

Here $\gcd(7,4)=1|100$. Hence equation (3) has a solution .

Now $1=7(-1)+4(2)\Rightarrow 100=7\times(-100)+4(200)$.

Thus, (- 100, 200) is a particular solution of given Diophantine equation.

General solution is

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

$=-100+\frac{4}{1}t \quad y=200-\frac{7}{1}t$

$x=-100+4t \quad y=200-7t$.

where t is any integer.

For positive solution we must have

$-100+4t>0$ and $200-7t>0$

$-25+t>0,\ t<\frac{200}{7}<29$

Thus, $25<t<29$

We can now prepare table of possible solutions.

t	x	y	z	15x + 9y + z
26	4	18	78	300
27	8	11	81	300
28	12	4	84	300.

Exercises 1.3

1. Determine all the solutions in the positive integers of the following Diophantine equations

   a) 18x+5y=48

b) $54x+21y=906$

c) $158x - 57y = 7$

(Ans. a) (1,6) b) (2,38), (9,20), (16,2) c) (17 - 57t , 47-158t) where $t \leq 0$)

2. A certain number of sixes and nines is added to give a sum of 126;if the number of sixes and nines is interchanged, the new sum is 114.How many of each were there originally?

(Ans.six 6's and ten 9's)

3. When Mr. Smith cashed a cheque at his bank, the teller mistook the number of cents to the number of dollars and vice versa. Unaware of this , Mr. Smith spent 68 cents and then noticed to his surprise that he had twice the amount of the original cheque. Determine the smallest value for which the cheque could have been written.

(Ans. $10.21)

❑❑❑

Unit-2

PRIMES AND THEIR DISTRIBUTION

2.1 Fundamental Theorem of Arithmetic

Definition. An integer $p > 1$ is a **prime integer** or simply a **prime** if it's only divisors are 1 and p . An integer greater than 1 that is not prime is called **composite** integer.

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

Proof. If $p \mid a$ then there is nothing to prove.

Suppose $p \nmid a$ then p being prime its only divisors are 1 and p, therefore $\gcd(p,a) = 1$ or p . If $\gcd(p,a) = p$ then $p \mid a$, which is absurd.

Hence $\gcd(p,a) = 1$. Then by Euclid's lemma $p \mid ab$ and $\gcd(p,a) = 1$ together give us $p \mid b$.

Corollary. If p is prime and $p \mid a_1 a_2 ... a_n$ then $p \mid a_k$ for some $1 \le k \le n$.

Proof. We shall prove this by induction on n .

Suppose n = 2, then $p \mid a_1 a_2 \Rightarrow p \mid a_1$ or $p \mid a_2$ by known result. Hence the result holds for $n = 2$.

Suppose the result holds for n = m and

Consider.

$p \mid a_1 a_2 ... a_m a_{m+1}$

$\Rightarrow p \mid (a_1 a_2 ... a_m) a_{m+1}$

$\Rightarrow p \mid a_1 a_2 ... a_m$ or $p \mid a_{m+1}$

$\Rightarrow p \mid a_k$ for some $1 \le k \le m$ or $p \mid a_{m+1}$

$\Rightarrow p \mid a_k$ for some $1 \le k \le m+1$

Hence , the result holds for $n = m+1$ whenever it holds for $n=m$.

Therefore, by principle of mathematical induction the result holds for any n.

Theorem. If $p, q_1, q_2, ... q_n$ are all primes and $p \mid q_1 q_2 ... q_n$ then $p = q_k$ for some k, $1 \le k \le n$.

Proof. In view of the above corollary, $p \mid q_1 q_2 ... q_n$ implies $p \mid q_k$ for some $1 \le k \le n$ Since both p and q_k are primes and that $q_k > 1, p > 1$ we have $p = q_k$.

Theorem. (Fundamental Theorem of Arithmetic)

Every positive integer n >1, can be expressed as product of primes, this representation is unique apart from the order in which the factors occur .

Proof. If n is prime there is nothing to prove. Suppose 'n' is composite, then there exist an integer d >1 such that d|n with 1 < d < n. Thus there is a set of divisors of n such that 1 < d < n. Therefore, there is a smallest integer p_1 such that $1 < p_1 < n$ and $p_1 \mid n$.

Claim : p_1 is prime.

Suppose on the contrary that p_1 is composite integer, then there is a divisor $q(1 < q < p_1)$ of p_1 which is ultimately a divisor of n, which contradicts minimality of p_1.Hence p_1 is prime. Thus we have $n = p_1 n_1$, where p_1 is prime and $n > n_1$. If n_1 is prime, we are done, otherwise there is prime p_2 dividing n_1.Let $n_1 = p_2 n_2$ with $n > n_1 > n_2$. If n_2 is prime we stop here. Otherwise there is a prime p_3 and $n_2 = p_3 n_3$ with $n > n_1 > n_2 > n_3$. Since n is finite the above process can not be continued indefinitely, that is to say, there is a positive integer r such that $n_{r-1} = p_r q_r$ where p_r and q_r are primes.

Thus $n = p_1 p_2 ... p_r q_r$ is prime factorization of $n > 1$.

Uniqueness : Let $q_1, q_2, ..., q_s$ be primes such that, $n = p_1 p_2 ... p_r = q_1 q_2 ... q_s$ where $p_a, ... p_r$ and $q_a, ... q_s$ are primes written in increasing order, that is $p_1 \le p_2 \le p_3 \le ... \le p_r$ and $q_1 \le q_2 \le ... \le q_s$.

Now, $p_1 \mid p_1 p_2 ... p_r = q_1 q_2 ... q_s \Rightarrow p_1 = q_k$ for some $1 \le k \le s$.

By hypothesis $p_1 = q_k \ge q_1$. Thus $p_1 \ge q_1$.Now, starting with q_1 instead of p_1 we obtain $p_1 \le q_1$.Thus $p_1 = q_1$. Therefore, we have $p_2 p_3 ... p_r = q_2 q_3 ... q_s$ Repeating the above process we obtain $1 = q_{r+1} ... q_s$ .This is possible only if $r = s$ and $p_k = q_k$ for all k .

Hence the uniqueness.

Corollary. Any positive integer n > 1, can be written uniquely in the canonical form n = $p_1^{k1} p_2^{k2} ... p_r^{kr}$ where for i = 1, 2, ... r each k_r is a positive integer and each p_i is a prime with $p_1 < p_2 < ... < p_r$.

Proof. Proof is immediate from the above theorem.

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

Proof. Suppose on the contrary that $\sqrt{2}$ is rational, then there exist integers $a, b \neq 0$ such that $\sqrt{2} = \frac{a}{b}$, where $\gcd(a,b) = 1$.Squaring both sides, we obtain $2b^2 = a^2$.

If $b > 1$, then by Fundamental theorem of arithmetic, there is a prime p such that $p \mid b$. Hence, $p \mid a^2$, but then $p \mid a$,so that $\gcd(a,b) \geq p$, which is impossible. Thus we have $b = 1$ so that $a^2 = 2$ and there is no integer a whose square is 2. Hence, we arrive at contradiction. Therefore $\sqrt{2}$ is irrational.

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

Solution. For $3n+1$ is to be odd we must have 3n to be even and hence n must be even.

Ex.2 Every integer of the form $n^4 + 4$ is composite for $n > 1$.

Solution. Observe that

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

$$= \left(n^2 + 2\right)^2 - \left(2n\right)^2$$

$$= \left(n^2 + 2 + 2n\right)\left(n^2 + 2 - 2n\right),$$

which is composite for n>1.

Ex.3 The only prime of the form $n^2 - 4$ is 5

Solution. For $n = 3, n^2 - 4 = 5$ and for $n \geq 4$, we have $n^2 - 4 = (n + 2)(n - 2)$, which is composite.

Ex.4 . Prove that every number of the form 3n + 2 has a prime factor of the same form.

Proof. We know that product of any number of integers of the form 3n+1 is also a number of the form 3n+1 and that product of any number of integers of the form 3n is also a number of the form 3n. Therefore, the prime factorization of any number of the form 3n+2 must contain a prime of the form 3n+2.

Theorem(Euclid's Theorem). There is an infinite number of primes.

Proof. Let $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots$ be primes in natural order. If possible there be last prime p_n. That is $p_1, p_2, \ldots, p_n$ are the only primes.

Consider

$$P = p_1 p_2 \ldots p_n + 1$$

Clearly, $P > 1$ therefore, by Fundamental theorem of Arithmetic P has a prime factor p. which is one of $p_1, p_2, \ldots, p_n$. Therefore $p \mid p_1 p_2 \ldots\ldots p_n$. Further $p \mid P$

Thus $p \mid P - p_1 p_2 \ldots\ldots p_n = 1$. Therefore, $p \mid 1$ which is absurd.

Hence, the infinitude of primes.

Note. Let $p^{\#}$ denote the product of primes less than or equal to p, where p is prime.

Consider $p^{\#} + 1$

This number is called 'Euclid's number' or 'Euclidean number'

Consider,

$3 = 2^{\#} + 1 = 2 + 1$

$7 = 3^{\#} + 1 = 2.3 + 1$

$31 = 5^{\#} + 1 = 2.3.5. + 1$

$211 = 7^{\#} + 1 = 2.3.5.7 + 1$

$2311 = 11^{\#} + 1 = 2.3.5.7.11 + 1$

All numbers of the form $p^{\#}+1$ need not be prime.

Let $n_1 = 2$

$n_2 = n_1 + 1$

$n_3 = n_2 \cdot n_1 + 1$

$n_4 = n_3 \cdot n_2 \cdot n_1 + 1$

.

.

.

$n_k = n_{k-1} n_{k-2} \ldots n_1 + 1$

.

.

.

Since each $n_k > 1$, each n_k has a prime divisor. Interestingly no two n_k 's have same prime divisor.

Let,

$d = \gcd(n_i, n_k)$ where $i < k$.

Suppose $d \mid n_i$ then as $i < k, d \mid n_1 n_2 n_3 \ldots n_{k-1}$

Further $d \mid n_k \Rightarrow d \mid n_k - n_1 \cdot n_2 \ldots . n_{k-1} = 1$

Thus $d = 1$

Hence $\gcd(n_i, n_k) = 1$.

Thus, there are atleast as many different prime as different n_k's. Therefore primes are infinite in number.

Now, let us come back to primes $p_1, p_2, \ldots, p_n \ldots$ in natural order. Consider $P = p_1 p_2 \ldots p_{n-1} + 1$.

Then prime divisor p of P is none of $p_1, p_2, \ldots, p_{n-1}$ .Therefore $p_n \leq$ p .

In other words, if there are several such primes p dividing P then p_n can not exceed the smallest of these. That is $p_n \leq p_1 p_2 \ldots p_{n-1} + 1 \ (n \geq 2)$

With slight modification, we can write

$p_n \leq p_1 p_2 \ldots p_{n-1} - 1 \ (n \geq 3)$.

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

Proof. We shall prove this theorem by induction on n. For $n = 1, p_1 = 2$ and $2^{2^{n-1}} = 2$. Thus the results holds. Let the result hold true for all integers < n.

We know, $p_n \leq p_1 p_2 \ldots p_{n-1} + 1$

$\leq 2 \cdot 2^2 \cdot 2^{2^2} \cdot \ldots \cdot 2^{2^{n-2}} + 1$

$= 2^{1+2+2^2+\ldots+2^{n-2}} + 1$

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

$\leq 2^{2^{n-1}-1} + 2^{2^{n-1}-1}$

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

Thus $p_n \leq 2^{2^{n-1}}$.

Hence, the result holds true for n. Therefore, by principle of induction the result holds for any n.

From this theorem following result follows immediately.

Corollary .There are at least n + 1 primes less than 2^{2^n} .

Proof. From the above theorem $p_1, p_2, \ldots, p_n$ are primes less than 2^{2^n} .

Exercises 2.1

1. Exhibit five primes of the form $n^2 - 2$.
2. Prove that the only prime of the form $n^3 - 1$ is 7.
3. Find four primes of the form $2^n - 1$.
4. Find prime factorizations of the integers 1234 and 10140.
5. If $n > 1$ is an integer not of the form $6k + 1$, prove that either 2 or 3 divides $n^2 + 2^n$.
6. Prove that any integer of the form $8^k + 1$, where $n \geq 1$, is composite.
7. Find all primes that divide $50!$.
8. If $p \geq 5$ is a prime number, show that $p^2 + 2$ is composite.

2.2 SIEVE OF ERATOSTHENES

Let $a > 1$ be a composite number then there exist integers $b, c(1 < b < a; 1 < c < a)$ such that $a = bc$. Assuming $b \leq c$, we have $b^2 \leq bc = a$ and hence $b < \sqrt{a}$. Since $b > 1$, b has a prime factor p . If p is prime divisor of $b > 1$, then $p \mid b \Rightarrow p \mid a$ and that $p \leq b < \sqrt{a}$. Thus a composite number a always posseses a prime divisor $p \leq \sqrt{a}$.

Therefore to find a prime factors of any integer $a > 1$. It is enough to test the primes less than $\sqrt{a}$. More precisely the number 100 has a prime factor which is one amongst 2, 3, 5, 7. Infact $100 = 2^2.5^2$.

Let us consider the number a = 2093. Here the smallest prime dividing a is 7 and so 2093 = 7 x 299. Further smallest divisor of 299 is 13, thus 299=13x23. Thus $a = 7 \times 13 \times 23$.

Let us consider the application of sieve of Eratothenes to obtain all the primes less than 100.

1	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~~

Begin with 2 and score off all the multiples of 2 higher than 2 higher than 2. Then take 3 and score off all multiples of 3 other than 3. Repeated it for 5, 7 and the integers that survise scoring off are the primes less than 100.

Primes less than 100 are,

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

Exercises 2.2

1. Determine whether the integer 501 is prime by testing all primes $p \le \sqrt{501}$ as possible divisors.
2. Apply sieve of Eratosthenes to obtain all primes between 200 and 300.
3. Show that any composite three digit number must have a prime factor less than or equal to 31. What can be said about four digit number?

2.4 Goldbach Conjecture

The difference between consecutive primes could be small as with the pairs 11, 13 and 17, 19 and for that matter 1,000,000,000,061 and 1,000,000,000,063. We call such pairs as twin primes i. e. pair of primes of the form p and p + 2. The electronic computers have discovered 152892 twin primes < 3, 000,000,0 and 20 pairs between 10^{12} and $10^{12}+10000$.

The largest twin prime pair known is $3756801695685 \cdot 2^{666669} \pm 1$(as of January 2016)

Proposition. Given any positive integer n, there exist n consecutive integers, all of which are composite.

Proof. Given an integer n, n – consecutive composite integers are

$(n+1)!+2,(n+1)!+3,...,(n+1)!+(n+1)$.

e.g. 5! + 2 = 2 x 61

5! + 3 = 3 x 41

5! + 4 = 4 x 31

5! + 5 = 5 x 25.

Goldbach Conjecture: Every even integer greater than 4 can be written as sum of two odd primes.

e.g. 6=3+3

8=5+3

10=5+5=3+7

12=5+7

14=11+3=7+7

16=3+13=5+11

18=7+11=5+13

20=7+13=3+17 …

Though this appears to be simple no proof has been found till todate. It is still an open problem.

It has been verified by computation for all even integers less than 4×10^{11} , G.H. Hardy in his address to the mathematical society of Copenhagen in 1921 stated that the Goldbach conjecture appeared. "…Probably as difficult as any of the unsolved problems in mathematics". It is currently known that every even integer is the sum of 6 or fewer primes.

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

Proof. Let $4m+1$ and $4n+1$ be two integers then

$(4m+1)(4n+1)=16mn+4(m+n)+1=4(4mn+m+n)+1$.

which is of the form $4n+1$.

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

Proof. Suppose that there are only a finite number of primes of the form $4n+3$, namely $p_1, p_2, ..., p_r$.

Consider, $N=4p_1p_2...p_r-1=4(p_1p_2.....p_r-1)+3$.

Clearly, N > 1 and is of the form $4n+3$

Since N > 1, it has prime factorization $N=q_1q_2.....q_s$. Further N being odd number $q_k\neq2(1\le k\le s)$. If some q_k divides $4p_1p_2.....p_r$ then as $q_k\mid N$

$q_k\mid 4p_1p_2....p_r-N=1\Rightarrow q_k\mid1\Rightarrow q_k=1$ which is absurd. Thus q_k is other than $p_1, ..., p_r$ for $\le k\le s$

Further, each $q_k(1\le k\le s)$, being odd it is of the form $4n+1$ or $4n+3$. Since N is of the form $4n+3$, all q_k's can not be of the form $4n+1$ because product of finite number of integers of the term $4n+1$ is of the same form. Therefore, there is atleast one q_k of the form

$4n+3$. Thus q_k is a prime of the form $4n+3$ other than $p_1, p_2, ..., p_r$. Thus we arrive at contradiction .

Therefore there are infinitely many primes of the form $4n+3$.

Theorem. If all the $n > 2$ terms of the arithmetic progression p, p + 2d, ..., p+ (n – 1)d are prime numbers then the common difference d is divisible by every prime q < n.

Proof. Let q be a prime less than n. Let if possible $q \nmid d$.

Claim. The first q terms of the progression namely, $p, p+d, ..., p+(q-1)d$ will leave different remainders upon division by q.

Suppose on the contrary that $p+rd$ and $p+sd\,(0 \le r < s < q)$ leave the same remainder upon division by q. Then $p+rd = q_1 q + r$ and $p+sd = q_2 q + r$, where q_1 and q_2 are quotients. Therefore, $(s-r)d = (q_2 - q_1)q$. Thus $q \mid (s-r)d$ .Since 'q' is prime and $q \nmid d, \gcd(q,d) = 1$ .Hence by Euclid's lemma, $q \mid (s-r)$ which is absurd as $0 \le r \le s \le q$.

Hence, the claim.

Since the q integers $p, p+d, p+2d, ...p+(q-1)d$ leave different remainders upon division by q, one of the above q numbers will leave remainder 0. Note that the q remainders upon division by q are 0, 1, 2, …,q – 1 . Let $0 \le t < q$ be such that $q \mid p+td$ .Note that if p < n, then one of the members of the progression p, p + d, … ,p + (n – 1) d is of the form p + pd = p(1 + d), contradicting the fact that all members of the progression are primes. Therefore, we have $q < n \le p \le p+td$.

Thus, we arrive at the conclusion that $p+td$ is composite, which is absurd. Therefore, $q \mid d$.

(e.g. p = 5, n = 7, d = 4, one of 1, 2, …., (7 - 1) is p = 5 and one of p, $p+d$, $p+2d, ...p+(n-1)d$ namely 5, 5 + 4, 5 + 2 × 4, 5 + 3 × 4, 5 + 4 × 4, 5 + 5 × 4, 5 + 6 × 4 is 5 + 5 × 4 that is $p+pd$ form. And also n = 3, p = 3, d = 4, q = 2 < 3 = n, consider 3, 3 + 4 = 7, 3 + 2 × 4 = 11 are all primes. Here q = 2 divides d = 4.)

❑❑❑

Unit – III

CONGRUENCES

3.1 Properties of Congruences:

Definition. Let n be a positive integer, then two integers a and b are said to be congruent modulo n written as $a \equiv b \pmod{n}$ if and only if $n \mid a-b$, that is , $a-b=kn$, for some integer k .

Let us take $n=9$, then

$25 \equiv 7 \pmod{9}, \quad -23 \equiv 4 \pmod{9}, \quad 39 \equiv -6 \pmod{9}, \quad -41 \equiv -5 \pmod{9}$,

because $25-7=2(9), 23-(-4)=3(9), 36-(-9)=5(9), -41-(-5)=-4(9)$.

Note. Congruence relation is an equivalence relation.

Let a and n be a given integers, then there exist integers q and r , such that $a=qn+r, 0 \le r < n$. Observe that in this case $a \equiv r \pmod{n}$. Thus every integer is congruent modulo n to one of the integers $0,1,2,\ldots,n-1$. In particular, $a \equiv 0 \pmod{n}$ if and only if $n \mid a$. The set of integers $0,1,2,\ldots,n-1$ is called the *set of least nonnegative residues modulo* n . Moreover, the set of integers $a_1, a_2, \ldots, a_n$ is said to be complete set(system) of residues modulo n , if every integer is congruent modulo n to one and only one of a_k . In other words, $a_1, a_2, \ldots, a_n$ is congruent modulo n to $0,1,2,\ldots,n-1$, taken in some order. For example, $-14,-16,15,23,31,41,45$ is complete set(system) of residues modulo 7; Here, we have

$$-14 \equiv 0, -16 \equiv 5, 15 \equiv 1, 23 \equiv 2, 31 \equiv 3, 41 \equiv 6, 46 \equiv 4 .$$

Theorem. For arbitrary integers a and b, $a \equiv b \pmod{n}$ if and if only a and b leave the same remainder upon division by n.

Proof. Suppose $a \equiv b \pmod{n}$, then $a=b+qn$ for some integer q. By division algorithm there exist integers q_1 and r such that $a=nq_1+r, 0 \le r < n$, then $a=b+qn$ gives us

$nq_1+r=b+qn$

$\Rightarrow b=(q_1-q)n+r$.

Thus a and b leave the same remainder upon division by n .

Conversely, suppose that a and b leave the same remainder on division by n, then $a=q_1n+r$ and $b=q_2n+r$ where q_1, q_2 are quotients and r is remainder on division by n .

Thus, $a-b=(q_1-q_2)n \Rightarrow a \equiv b \pmod{n}$.

Theorem. Let $n>0$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold

a) $a \equiv a \pmod{n}$.

b) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.

c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a+c \equiv b+d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

e) If $a \equiv b \pmod{n}$, then $a+c \equiv b+c \pmod{n}$ and $ac \equiv bc \pmod{n}$.

f) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k.

Proof. a) $a \equiv a \pmod{n}$

Since $(a-a)=0=0.n$ for any integer a

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

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

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

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

$\Rightarrow a-b=k.n$ for some k

$\Rightarrow b-a=(-k)n$

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

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

c) Let $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$

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

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

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

$\Rightarrow a = c \pmod{n}$.

Thus if $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$

d) Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$

$\Rightarrow n \mid (a-b)$ and $n \mid (c-d)$

$\Rightarrow a - b = nr$ and $c - d = ns$ for some integers r, s

Now,

$(a+c)-(b+d) = (a-b)+(c-d)$

$= nr + ns$

$= n(r+s)$.

Therefore, $n \mid (a+c)-(b+d)$

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

$a + c \equiv b + d \pmod{n}$.

Now, $ac - bd = ac - bc + bc - bd = (a-b)c + (c-d)b = nrc + bns$

$\Rightarrow ac - bd = n(rc + bs)$

$\Rightarrow n \mid ac - bd \Rightarrow ac \equiv bd \pmod{n}$

e) Suppose $a \equiv b \pmod{n}$ but $c \equiv c \pmod{n}$ always holds. Thus

$a + c \equiv b + c \pmod{n}$.and also ac $\equiv$ bc(modn)

Also, $a \equiv b \pmod{n}$ but $c \equiv c \pmod{n}$ always holds.

Then by (iv) we have

$ac \equiv bc \pmod{n}$.

f) Suppose $a \equiv b \pmod{n} \Rightarrow n \mid (a-b)$.

We know that if k is positive integer then

$a^k - b^k = (a-b)\left(a^{k-1} + a^{k-2}b + ... + b^{k-1}\right)$

Since, $n \mid a - b$, we have

$n \mid (a-b)\left(a^{k-1}+a^{k-2}b+....+b^{k-1}\right)=a^k-b^k$

Therefore, $n \mid a^k-b^k \Rightarrow a^k \equiv b^k \pmod{n}$.

Ex. 1 Show that $41 \mid 2^{20}-1$.

Solution. To prove this, it is enough to show that $2^{20} \equiv 1 \pmod{41}$.

We know that $2^7 \equiv 5 \pmod{41} \Rightarrow 2^{14} \equiv 25 \pmod{41}$.

And $2^6 \equiv 23 \pmod{41}$.

Thus,

$2^{20}=2^{14}2^6 \equiv 25.23 \pmod{41} \Rightarrow 2^{20} \equiv 1 \pmod{41}$.

Ex.2. Find last two digits of the number 9^{9^9}.

Solution. We know $9 \equiv -1 \pmod{10}$, therefore $9^9 \equiv (-1)^9 \equiv -1 \equiv 9 \pmod{10}$.

Next, $9^2=81 \equiv -19 \pmod{100} \Rightarrow 9^4 \equiv 361 \equiv -39 \pmod{100} \Rightarrow 9^8 \equiv 21 \pmod{100}$.

Further, $9^9 \equiv 89 \pmod{100}$ and $9^{10} \equiv 1 \pmod{100}$.

Thus $9^{9^9}=9^{9+10k}=9^9 \cdot 9^{10k} \equiv 89 \cdot 1 \pmod{100}$.

Therefore, 89 are the last two digits.

Ex.3 Find the remainder obtained upon dividing, 1 ! + 2! + 3! + ... + 100! by 12.

Solution. Since each of $4!,5!,\ldots,100!$ contain $4!=1 \cdot 2 \cdot 3 \cdot 4=24$, 4! + …+ 100! is divisible by 12 the remainder is 1! + 2! + 3! = 1 + 2 + 6 = 9.

Theorem. If $ca \equiv cb \pmod{n}$ then $a \equiv b \left(\bmod \frac{n}{d}\right)$ where $d=\gcd(c,n)$

Proof. Given $d=\gcd(c,n)$ then d|c and d|n, therefore $\frac{n}{d}$ is an integer.

Consider, $ca \equiv cb \pmod{n}$, then $c(a-b)=nk$ for some integer k.

Now as d|c and d|n, there exist integer r and s such that $\gcd(r,s)=1$ and $dr=c$ and $ds=n$

Thus $dr(a-b)=dsk \Rightarrow r(a-b)=sk$.

Since, r and s are relatively prime

$r(a-b)=sk \Rightarrow s \mid (a-b)$

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

$\Rightarrow a \equiv b\left(\bmod \frac{n}{d}\right)$.

Hence the result.

Corollary. If $ca \equiv cb(\bmod n)$ and $\gcd(c,n)=1$ then $a \equiv b(\bmod n)$

Corollary. If $ca \equiv cb(\bmod p)$ and $p \nmid c$, where p is a prime number, then $a \equiv b(\bmod p)$.

Proof. Since p is a prime $\gcd(c,p)=p$ or 1. However as $p \nmid c, \gcd(c,p)=1$ and the result follows.

Ex.4 Prove each of the following

a) If $a \equiv b(\bmod n)$ and $m \mid n$ then $a \equiv b(\bmod m)$

b) If $a \equiv b(\bmod n)$ and $c>0$ then $ca \equiv cb(\bmod cn)$

c) If $a \equiv b(\bmod n)$ and the integers a,b,n are divisible by $d>0$ then $\frac{a}{d} \equiv \frac{b}{d}\left(\bmod \frac{n}{d}\right)$.

Solution. a) Suppose $a \equiv b(\bmod n)$, then there is an integer k such that $a=b+kn$, since $m \mid n$ there is an integer t such that $n=mt$. Thus $a=b+ktm=b+(kt)m$ and hence, $a \equiv b(\bmod m)$.

b) Suppose $a \equiv b(\bmod n)$, then there is an integer k such that $a=b+kn$. Thus we have for $c>0$ $ca=cb+ckn=cb+k(cn)$. Therefore, $ca \equiv cb(\bmod cn)$.

c) Suppose $a \equiv b(\bmod n)$, then there is an integer k such that $a=b+kn$ so that $\frac{a}{d}=\frac{b}{d}+k\frac{n}{d}$, for any $d>0$. Since each of the integers a,b,n are divisible by $d>0$, each of the numbers $\frac{a}{d},\frac{b}{d},\frac{n}{d}$ are integers so $\frac{a}{d} \equiv \frac{b}{d}\left(\bmod \frac{n}{d}\right)$.

Ex. 4. Give an example to show that $a^2 \equiv b^2(\bmod n)$ need not imply $a \equiv b(\bmod n)$

Solution. $5^2 \equiv 4^2(\bmod 9)$ but $4 \not\equiv 5(\bmod 9)$

Ex.5. If $a \equiv b(\bmod n)$ prove that $\gcd(a,n) \equiv \gcd(b,n)$.

Solution. Suppose $a \equiv b(\bmod n)$, then there exist positive integer k such that $a=b+kn$. Let $d=\gcd(a,n), d'=\gcd(b,n)$. Since $d=\gcd(a,n)$, we have $d \mid a$ and $d \mid n$, so that $d \mid a, d \mid kn \Rightarrow d \mid a-kn=b$. Thus $d \mid b$ and $d \mid n$. Therefore, $d \le d'$. Further, $d'=\gcd(b,n)$,

we have $d'|b$ and $d'|n$, so that $d'|b, d'|kn \Rightarrow d'|b+kn=a$. Thus $d'|a$ and $d'|n$. Therefore, $d' \le d$ .Thus $d = d'$.

Ex.6. Find the remainder when 2^{50} is divided by 7.

Solution. We know,

$2^3 \equiv 1 \pmod 7$

$\Rightarrow 2^{48} = \left(2^3\right)^{16} \equiv 1^{16} \pmod 7$

$\Rightarrow 2^{48} \equiv 1 \pmod 7$

$\Rightarrow 2^{50} = 2^{48+2} = 2^{48}2^2 \equiv 1 \cdot 4 \equiv 4 \pmod 7$.

Thus $2^{50} \equiv 4 \pmod 7$, that is, remainder when 2^{50} is divided by 7is 4.

Ex.7 Find the remainder when 4444^{4444} is divided by 9.

Solution. Note that $1111 = 123 \times 9 + 4$, so that $1111 \equiv 4 (\text{mod}\, 9)$.

Then $4444 \equiv 16 (\text{mod}\, 9) \Rightarrow 4444 \equiv -2 (\text{mod}\, 9)$. Therefore $4444^{4444} \equiv (-2)^{4444} (\text{mod}\, 9)$ or $4444^{4444} \equiv 2^{4444} (\text{mod}\, 9)$. Now $2^3 \equiv -1 (\text{mod}\, 9)$ implies $2^9 \equiv -1 (\text{mod}\, 9)$.

Thus $2^{1111} = 2^{123 \times 9 + 4} = \left(2^9\right)^{123} \times 2^4 \equiv (-1)^{123} \times 16 \equiv (-1) \times 7 \equiv -7 \equiv 2 (\text{mod}\, 9)$.

Hence, $2^{4444} = \left(2^{1111}\right)^4 \equiv 2^4 \equiv 7 (\text{mod}\, 9)$.

Thus $4444^{4444} \equiv 2^{4444} \equiv 7 (\text{mod}\, 9)$. Therefore, the remainder is 7.

Ex.8. What is the remainder when the following sum is divided by 4?

$1^5 + 2^5 + 3^5 + \cdots + 100^5$.

Solution.Observe that each of $2^5, 4^5, 6^5, \ldots, 100^5$ is divisible by 4. Now what remains to be examined is the sum $1^5 + 3^5 + 5^5 + \cdots + 99^5$ which contains 50 terms. This can be rearranged in 25 pairs as follows.

$(1^5 + 3^5) + (5^5 + 7^5) + \cdots + (97^5 + 99^5)$.

Here each pair is of the form,

$(2n-1)^5 + (2n+1)^5 = (2n-1+2n+1)\left[(2n-1)^4 + (2n-1)^3(2n+1) + \cdots + (2n-1)(2n+1)^3 + (2n+1)^4\right]$

$= (4n)\left[(2n-1)^4 + (2n-1)^3(2n+1) + \cdots + (2n-1)(2n+1)^3 + (2n+1)^4\right]$

Thus whole sum is divisible 4 and hence the remainder is zero.

3.2 SPECIAL DIVISIBILITY TESTS

In this section we will see a mathematical formulation of divisibility tests.

Theorem. Given an integer $b > 1$, any positive integer N can be written uniquely in terms of powers of b as $N = a_m b^m + a_{m-1} b^{m-1} + a_{m-2} b^{m-2} + \cdots + a_1 b + a_0$ where the coefficients a_k can take on b different values $0, 1, 2, \ldots, b-1$.

Proof. By division algorithm there exist integers q_1 and a_0 such that

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

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

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

Substituting for q_1 , we obtain

$$N = (q_2 b + a_1) b + a_0 = q_2 b^2 + a_1 b + a_0, 0 \le a_1, a_0 < b .$$

Further,if $q_2 \ge b$, we can proceed to get

$$N = q_3 b^3 + a_2 b^2 + a_1 b + a_0, 0 \le a_2, a_1, a_0 < b .$$

Since, $N > q_1 > q_2 > \cdots \ge 0$ is strictly decreasing sequences, this process should terminate in finite number of steps to give us

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

where the coefficients a_k can take on b different values $0, 1, 2, \ldots, b-1$.

Uniqueness:

Suppose that, N has two distinct representations as follows

$$N = a_m b^m + a_{m-1} b^{m-1} + a_{m-2} b^{m-2} + \cdots + a_1 b + a_0 = c_m b^m + c_{m-1} b^{m-1} + c_{m-2} b^{m-2} + \cdots + c_1 b + c_0$$

where, $0 \le a_i < b$ for each i and $0 \le c_j < b$ for each j . This can be written as

$$0 = d_m b^m + d_{m-1} b^{m-1} + \cdots + d_1 b + d_0$$

where $d_k = a_k - c_k$. Since the two representations are different there exist $d_i \ne 0$ for some i . Let k be the smallest subscript for which $d_k \ne 0$. Then

$$0 = d_m b^m + d_{m-1} b^{m-1} + \cdots + d_{k+1} b^{k+1} + d_k b^k .$$

This gives us

$$d_k = -b(d_m b^{m-k-1} + \cdots + d_{k-1}) .$$

Thus we have $b \mid d_k$. The inequalities $0 \le a_k < b$ and $0 \le c_k < b$ give us $-b \le a_k - c_k < b$ or $| d_k | < b$. Therefore, b cannot divide d_k . Hence, we must have $d_k = 0$, for all k. Thus $a_k = c_k$ for all k . Therefore, the representation is unique.

Theorem. Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k . If $a \equiv b (\mathrm{mod}\, n)$, then $P(a) \equiv P(b) (\mathrm{mod}\, n)$.

Proof. Observe that $a \equiv b (\mathrm{mod}\, n)$ implies $a^k \equiv b^k (\mathrm{mod}\, n)$ for $k = 1, 2, \ldots, m$. Hence, $c_k a^k \equiv c_k b^k (\mathrm{mod}\, n)$ for $k = 1, 2, \ldots, m$. Therefore, we have

$$\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k (\mathrm{mod}\, n) \ .$$

That is $P(a) \equiv P(b) (\mathrm{mod}\, n)$.

Corollary. If a is a solution of $P(x) \equiv 0 (\mathrm{mod}\, n)$ and $a \equiv b (\mathrm{mod}\, n)$, then b is also a solution.

Proof.Since $a \equiv b (\mathrm{mod}\, n)$, we have $P(a) \equiv P(b) (\mathrm{mod}\, n)$. Further, a is a solution of $P(x) \equiv 0 (\mathrm{mod}\, n)$, we have $P(a) \equiv 0 (\mathrm{mod}\, n)$, therefore, $P(b) \equiv 0 (\mathrm{mod}\, n)$. Thus b is also a solution of $P(x) \equiv 0 (\mathrm{mod}\, n)$.

This result can be used to develop tests of divisibility. Let us begin with test of divisibility by 9, in decimal system.

Theorem. Let $N = a_m 10^m + a_{m-1} 10^{m-1} + a_{m-2} 10^{m-2} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N , $0 \le a_k < 10$, and let $S = a_0 + a_1 + \cdots + a_m$. Then $9 \mid N$ if and only if $9 \mid S$.

Proof. We know that $10 \equiv 1 (\mathrm{mod}\, 9)$. Let $P(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$. Then in view of above theorem $P(10) \equiv P(1) (\mathrm{mod}\, 9)$. Clearly,

$$P(10) = a_m 10^m + a_{m-1} 10^{m-1} + a_{m-2} 10^{m-2} + \cdots + a_1 10 + a_0 = N$$

and

$$P(1) = a_0 + a_1 + \cdots + a_m = S \ .$$

Thus $N \equiv S (\mathrm{mod}\, 9)$. Therefore, $9 \mid N$ if and only if $9 \mid S$.

In view of this result, we have an integer N is divisible by 9 if and only if sum of digits in N is divisible by 9.

Let us now proceed to divisibility by 11.

Theorem.Let $N = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N , $0 \le a_k < 10$, and let $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Then $11 | N$ if and only if $11 | T$.

Proof. We know that $10 \equiv -1 (\mathrm{mod} 11)$. Let $P(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$. Then in view of above theorem $P(10) \equiv P(-1)(\mathrm{mod} 11)$. Clearly,

$$P(10) = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0 = N$$

and

$$P(-1) = a_0 - a_1 + \cdots + (-1)^m a_m = T .$$

Thus $N \equiv T (\mathrm{mod} 11)$. Therefore, $11 | N$ if and only if $11 | T$.

In view of this result, we have an integer $N = a_m 10^m + a_{m-1}10^{m-1} + a_{m-2}10^{m-2} + \cdots + a_1 10 + a_0$ is divisible by 11 if and only if $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$ is divisible by 11.

Ex.9 Without performing the divisions, determine whether the integers 176,521,221 and 149,235,678 are divisible by 9 or 11?

Solution. a) Consider the integer 176,521,221. Observe that

i) 1+7+6+5+2+1+2+2+1=27, which is divisible by 9. Therefore, 176,521,221 is divisible by 9.

ii) 1-7+6-5+2-1+2-2+1= - 3 , which is not divisible by 11. Therefore, 176,521,221 is not divisible by 11.

b) Consider the integer 149,235,678. Observe that

i) 1+4+9+2+3+5+6+7+8=45 , which is divisible by 9. Therefore, 149,235,678 is divisible by 9.

ii) 1-4+9-2+3-5+6-7+8= 11 , which is divisible by 11. Therefore, 149,235,678 is divisible by 11.

Looking at the above results regarding divisibility, students are advised to develop divisibility tests for other integers in decimal as well as other systems also. For example, $10 \equiv 1 (\mathrm{mod} 3)$ gives us divisibility test for divisibility by 3 in decimal system where as $9 \equiv 0 (\mathrm{mod} 3)$ gives us divisibility test for divisibility by 3 in the system to the base 9 and $9 \equiv 1 (\mathrm{mod} 8)$ gives us divisibility test for divisibility by 8 in the system to the base 9. Let $P(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$. Let $N = a_m 9^m + a_{m-1}9^{m-1} + a_{m-2}9^{m-2} + \cdots + a_1 9 + a_0$ where $0 \le a_k < 9$ be a number to the base 9. Then $9 \equiv 0 (\mathrm{mod} 3)$ implies $P(9) \equiv P(0)(\mathrm{mod} 3) \Rightarrow N \equiv a_0 (\mathrm{mod} 3)$. Therefore, $3 | N$ if and only if $3 | a_0$. Similarly, we can prove that $8 | N$ if and only if $8 | a_0 + a_1 + \cdots + a_m$.

Ex.10 Test whether the integer $(447836)_9$ is divisible by 3 and 8?

Solution. Consider $(447836)_9$. Here $a_0 = 6$ and is divisible by 3. Therefore, $(447836)_9$ is divisible by 3. Now consider $4+4+7+8+3+6=32$ which is divisible by 8. Hence, $(447836)_9$ is divisible by 8.

Exercises 3.1

1. Prove that the integer $53^{103}+103^{53}$ is divisible by 39.
2. Use theory of congruence to verify that $89 \mid 2^{44}-1$ and $97 \mid 2^{48}-1$.
3. For any integer a, prove that $a^4 \equiv 0 (\text{mod}\, 5)$ or $a^4 \equiv 1 (\text{mod}\, 5)$.
4. Working with modulo 9 or 11m find the missing digit in the calculation below
   a) $51840 \times 273581 = 1418243x040$
   b) $2x99561 = [3(523+x)]^2$

   (Ans. a) 9, b) 4)

3.3. Linear congruences:

Definition. An equation of the form $ax \equiv b (\text{mod}\, n)$ is called linear congruence.

An integer x_0 is a solution of $ax \equiv b (\text{mod}\, n)$ if $ax_0 \equiv b (\text{mod}\, n)$.

We begin with

Theorem. The linear congruence $ax \equiv b (\text{mod}\, n)$ has a solution if and only if $d \mid b$, where $d = \gcd(a,n)$. If $d \mid b$, then it has d mutually incongruent solutions modulo n.

Proof. Observe that $ax \equiv b (\text{mod}\, n)$ is equivalent to linear Diophantine equation $ax - ny = b$. We know that $ax - ny = b$ has a solution if and only if $d \mid b$. Moreover if it has a solution x_0, y_0 then any other solution has the form $x = x_0 + \frac{n}{d}t, y = y_0 + \frac{b}{d}t$ for some choice of integer t. Consider the following set of d solutions

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \cdots, x_0 + \frac{(d-1)n}{d}.$$

We shall prove that these d solutions are mutually incongruent modulo n.

Suppose on the contrary that

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 (\text{mod}\, n)$$

where $0 \le t_1 < t_2 \le d-1$, then

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 (\mathrm{mod}\, n).$$

Now $\gcd\left(\frac{n}{d}, n\right) = \frac{n}{d}$, and therefore, we can cancel $\frac{n}{d}$ to get

$$t_1 \equiv t_2 (\mathrm{mod}\, d).$$

which implies $d \mid t_1 - t_2$. Since $0 \le t_1 < t_2 \le d-1$, d cannot divide $t_1 - t_2$. Thus we arrive at contradiction.

Now it remains to prove that any other solution $x_0 + \frac{n}{d}t$ is congruent modulo n to one of the d integers listed above. By division algorithm, we have $t = dq + r$ where q and r are integers with $0 \le r < d$. Hence,

$$x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r) = x_0 + nq + \frac{n}{d}r \equiv x_0 + \frac{n}{d}r (\mathrm{mod}\, n).$$

This proves the result.

Corollary.If $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b (\mathrm{mod}\, n)$ has a unique solution modulo n.

This is immediate from the above theorem.

Ex.11. Solve $18x \equiv 30 (\mathrm{mod}\, 42)$.

Solution. Consider $18x \equiv 30 (\mathrm{mod}\, 42)$. Here, $\gcd(18, 42) = 6$ and that $6 \mid 30$. Therefore, there are 6 incongruent solutions modulo 42 given by $x \equiv x_0 + \frac{n}{d}t (\mathrm{mod}\, n)$ where x_0 is a particular solution of given linear congruence and $t = 0, 1, \ldots, 5$. Now
$18x \equiv 30 (\mathrm{mod}\, 42) \Rightarrow 3x \equiv 5 (\mathrm{mod}\, 7)$ multiplying both sides by 5, we obtain
$15x \equiv 25 (\mathrm{mod}\, 7) \Rightarrow x \equiv 4 (\mathrm{mod}\, 7)$. Thus $x_0 = 4$ is a particular solution.

Hence, the six solutions incongruent modulo 42. Thus the 6 solutions are
$x = 4 + \frac{42}{6}t (\mathrm{mod}\, 42) \equiv 4 + 7t (\mathrm{mod}\, 42)$, that is, $x \equiv 4, 11, 18, 25, 32, 39 (\mathrm{mod}\, 42)$.

Ex.12 Using congruence solve $4x + 51y = 9$.

Solution. Consider $4x + 51y = 9$. This can be written as linear congruence $4x \equiv 9 (\mathrm{mod}\, 51)$. We now solve this linear congruence for x. Now consider $4x \equiv 9 (\mathrm{mod}\, 51)$.

Multiplying both sides by 13, we get $52x \equiv 117 (\mathrm{mod}\, 51)$, Thus $x \equiv 52x \equiv 117 (\mathrm{mod}\, 51)$.

Therefore, $x \equiv 117 \equiv 15 (\mathrm{mod}\, 51)$. Hence, $x = 15 + 51t$ where t is any integer.

Next we can take

$51y \equiv 9(\text{mod}\,4) \Rightarrow 3y \equiv 1(\text{mod}\,4) \Rightarrow 9y \equiv 3(\text{mod}\,4) \Rightarrow y \equiv 3(\text{mod}\,4) \Rightarrow y = 3 + 4s,$

where s is any integer. Using values of x and y in $4x + 51y = 9,$

we obtain the relation between r and s given by $4(15 + 51t) + 51(3 + 4s) = 9 \Rightarrow r + t + 1 = 0.$

In general $x = 15 + 51t$ and $y = 3 + 4(-1 - t) = -1 - 4t$, where t is any integer.

Note. Value of y in terms of t can also be obtained directly on putting value of x in terms of t in the equation $4x + 51y = 9$.

Theorem. (Chinese Remainder Theorem)

Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$x \equiv a_1(\text{mod}\,n_1)$
$x \equiv a_2(\text{mod}\,n_2)$
$\vdots$
$x \equiv a_r(\text{mod}\,n_r)$

has a simultaneous solution, which is unique modulo the integer $n_1 n_2 \cdots n_r$.

Proof.Let $n = n_1 n_2 \cdots n_r$. For each $k = 1, 2, \ldots, r$, let $N_k = \dfrac{n}{n_k} = n_1 n_2 \cdots n_{k-1} n_{k+1} \cdots n_r$. Since n_i are relatively prime in pairs, $\gcd(N_k, n_k) = 1,$ for $k = 1, 2, \ldots, r$. Hence, each of the linear congruence $N_k x \equiv 1(\text{mod}\,n_k)$ has a unique solution say x_k, for $k = 1, 2, \ldots, r$. Thus $N_k\, x_k \equiv 1(\text{mod}\ n_k)$

Let $\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$.

Claim: $\bar{x}$ is simultaneous solution of the system.

Since $n_k \mid N_i$ for $i \neq k$, $N_i \equiv 0(\text{mod}\,n_k)$ for $i \neq k$.

Hence,

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r \equiv a_k N_k x_k (\text{mod}\,n_k).$$

Since $N_k x_k \equiv 1(\text{mod}\,n_k)$, we have $\bar{x} \equiv a_k \cdot 1 \equiv a_k (\text{mod}\,n_k)$,for $k = 1, 2, \ldots, r$.

This proves the existence of solution

Uniqueness:

Let x' be any other solution of the given system of linear congruences, then $x' \equiv a_k \pmod{n_k}$, for each k = 1, 2,..., r .

Hence $\bar{x} \equiv x' \pmod{n_k}$, (k = 1, 2, …, r)

$\Rightarrow n_k \mid \bar{x} - x'$ (k = 1, 2, …, r) .

Since $gcd(n_i, n_k) = 1$, for $i \neq k$, we have

$n = n_1 n_2 \ldots n_r \mid \bar{x} - x'$

$\Rightarrow \bar{x} \equiv x' \pmod{n}$.

Hence the uniqueness.

Ex.12 The problem posed by Sun – Tsn corresponds to the system of three congruences

$x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{5}$

$x \equiv 2 \pmod{7}$.

Solution – Here $n_1 = 3, n_2 = 5, n_3 = 7$.

So $n = n_1 n_2 n_3 = 3.5.7 = 105$

$$N_1 = \frac{n}{n_1} = \frac{105}{3} = 35$$

$$N_2 = \frac{n}{n_1} = \frac{105}{5} = 21$$

$$N_3 = \frac{n}{n_3} = \frac{105}{7} = 15$$

Consider,

$N_1 x \equiv 1 \pmod{3} \Rightarrow 35x \equiv 1 \pmod{3}$

By inspection $x_1 = 2$ is a solution of this linear congruence.

Next,

$$N_2 x \equiv 1(\mathrm{mod}\,5) \Rightarrow 21x \equiv 1(\mathrm{mod}\,5)$$

By inspection $x_2 = 1$ is a solution of this linear congruence.

Further,

$$N_3 x = 1(\mathrm{mod}\,7) \Rightarrow 15x \equiv 1(\mathrm{mod}\,7)$$

By inspection $x_3 = 1$ of this linear congruence.

Consider,

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3$$

$$= 2.35.2 + 3.21.1 + 2.15.1$$

$$\bar{x} = 233$$

Thus $\bar{x} = 233(\mathrm{mod}\,105)$, that is, $\bar{x} = 23(\mathrm{mod}\,105)$ is simultaneous solution given congruences.

Ex.13 Solve $17x \equiv 9(\mathrm{mod}\,276)$.

Solution. Note that $276 = 3.4.23$ and given linear congruence is equivalent to

$$17x \equiv 9(\mathrm{mod}\,3) \text{ or } x \equiv 0(\mathrm{mod}\,3), \quad (1)$$

$$17x \equiv 9(\mathrm{mod}\,4) \text{ or } x \equiv 1(\mathrm{mod}\,4), \quad (2)$$

$$17x \equiv 9(\mathrm{mod}\,23). \quad (3)$$

Now

$$x \equiv 0(\mathrm{mod}\,3) \Rightarrow x = 3k \text{, for any integer k.} \quad (4)$$

Using this in the second, we get

$$3k \equiv 1(\mathrm{mod}\,4) \text{ or}$$

$$k \equiv 9k \equiv 3(\mathrm{mod}\,4)$$

$$\Rightarrow k = 3 + 4j \text{, for any integer j.} \quad (5)$$

Thus, $x = 3k = 3(3+4j) = 9+12j$. (6)

Using this in (3), we obtain

$$17(9+12j) \equiv 9(\mathrm{mod}\,23)$$

$\Rightarrow 204j \equiv -144 \pmod{23}$

$\Rightarrow 3j \equiv 6 \pmod{23}$

$\Rightarrow j \equiv 2 \pmod{23}$

$\Rightarrow j \equiv 2 + 23t$, where 't' is arbitrary integer.

Thus, $x = 9 + 12(2 + 23t) = 33 + 276t$.

Hence, $x = 33 \pmod{276}$ is the solution.

Linear Congruence of Two Variables

Linear congruence of two variables is a congruence of the form

$ax + by \equiv c \pmod{n}$.

Theorem. The system of linear congruences $ax + by \equiv r \pmod{n}$ and $cx + dy \equiv s \pmod{n}$ has a unique solution modulo n whenever $\gcd(ad - bc, n) = 1$

Proof. Consider $ax + by \equiv r \pmod{n}$ …….. (1)

and $cx + dy \equiv s \pmod{n}$. ……(2)

$((1) \times d - (2) \times b)$ gives us

$(ad - bc)x \equiv (dr - bs) \pmod{n}$. ……..(3)

Since $\gcd(ad - bc, n) = 1$,

$(ad - bc)z \equiv 1 \pmod{n}$ …….. (4)

has a unique solution of modulo n.

Let 't' be a solution of (4) then

$(ad - bc)t \equiv 1 \pmod{n}$ …….. (5)

Multiplying both sides of (3) by 't' we obtain

$(ad - bc)xt \equiv (dr - bs)t \pmod{n}$ ……(6)

Using (5) in (6) we get,

$x \equiv (dr - bs)t \pmod{n}$.

Similarly, $(1)\times c-(2)\times a$ gives us

$(bc-ad)y\equiv(cr-as)(\mathrm{mod}\,n)$

$\Rightarrow(ad-bc)y\equiv(as-cr)(\mathrm{mod}\,n)$

$\Rightarrow y\equiv(as-cr)t(\mathrm{mod}\,n)$

Ex.14 Solve $7x+3y\equiv 10(\mathrm{mod}16)$ ….. (1)

$2x+5y\equiv 9(\mathrm{mod}16)$ ….. (2)

Solution. Observe that $\gcd(7\times5-3\times2,16)=\gcd(35-6,16)=\gcd(29,16)=1.$

Hence, solution exists.

Consider, $(ad-bc)z\equiv 1(\mathrm{mod}\,n)\Rightarrow(7\times5-3\times2)z\equiv 1(\mathrm{mod}16)$ that is, $29z\equiv 1(\mathrm{mod}16)$

By inspection $z=5$ is a solution, therefore $t=5$.

Therefore, $x\equiv(dr-bs)t(\mathrm{mod}\,n)$ gives us

$x\equiv(5\cdot10-3\cdot9)(5)(\mathrm{mod}16)\Rightarrow x\equiv23\cdot5(\mathrm{mod}16)\Rightarrow x\equiv115(\mathrm{mod}16)\Rightarrow x\equiv3(\mathrm{mod}16)$

Similarly, $y\equiv(7\cdot9-2\cdot10)(5)\equiv43\cdot5\equiv215\equiv7(\mathrm{mod}16)$

We can also solve this problem directly as follows.

$(1)\times5-2(3)$ gives us

$35x+15y\equiv50(\mathrm{mod}16)$

$6x+15y\equiv27(\mathrm{mod}16)$

$\Rightarrow29x\equiv23(\mathrm{mod}16)$

$\Rightarrow13x\equiv7(\mathrm{mod}16)$

$\Rightarrow x\equiv3(\mathrm{mod}16)$

Next, $(1)\times2-2\times7$ gives us

$14x+6y\equiv20(\mathrm{mod}16)$

$14x+35y\equiv63(\mathrm{mod}16)$

$\Rightarrow$ -29y $\equiv$-43 (mod16)

$\Rightarrow$ 29y $\equiv$ 43 (mod16)

-3y $\equiv$ -5 (mod16)

33y $\equiv$ 55 (mod 16) (multiplying by 11 an brth sides)

$\Rightarrow y \equiv 7(\text{mod}16)$

EXERCISES 3.2

1. Solve $25x \equiv 15(\text{mod}\,29)$ (Ans. $x \equiv 18(\text{mod}\,29)$)
2. Solve $140x \equiv 133(\text{mod}\,301)$ (Ans. 16 + 63t, t = 0, 1, 2, ..., 6)
3. Using congruences, solve $12x + 25y = 331$. (Ans. $x = 13 + 25t; y = 7 - 12t$)

❑❑❑

Unit-4
Fermat's Theorem

4.1 Let us begin with Fermat's theorem

Theorem. Let p be prime and a is an integer such that $p \nmid a$ then

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

Proof. Consider the numbers $a, 2a, 3a, \ldots, (p-1)a$.

Claim. These $(p-1)$ integers are incongruent modulo p.

Let if possible $ra \equiv sa \pmod{p}$

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

Since $p \nmid a$ and p is prime $\gcd(p, a) = 1$ So, $ra \equiv sa \pmod{p}$

$\Rightarrow r \equiv s \pmod{p}$

$\Rightarrow p \mid r - s.$

Since, $1 \le r < s < p$, p can not divide $r - s$.

Hence a, $2a$, ..., $(p\text{-}1)\,a$ leave different remainders when divided by p. Therefore, a, $2a$, ..., $(p\text{-}1)\,a$ leave remainders 1, 2, ..., p-1 in some order.

Therefore,

$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) (\text{mod } p)$

$\Rightarrow 1 \cdot 2 \cdot 3 \cdots (p-1) a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) (\text{mod } p)$

$\Rightarrow (p-1)! a^{p-1} \equiv (p-1)! (\text{mod } p)$

$\Rightarrow a^{p-1} = 1 \pmod{p}.$

Note that as gcd (p, (p-1)!) = 1 we can cancel $(p-1)!$ from both sides.

Corollary. If p is prime, then $a^p \equiv a \pmod{p}$ for every integer a .

Proof. If $p \mid a$ then the result is trivially true. Further if $p \nmid a$ then by Fermat's theorem

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

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

Ex. 1 Find the remainder when, 5^{38} is divided by 11.

Solution. By Fermat's Theorem $5^{10} \equiv 1(\text{mod}11)$. Clearly $5^2 \equiv 3(\text{mod}11)$ and $3^4 \equiv 4(\text{mod}11)$

Thus, $5^8 \equiv 3^4 \equiv 4(\text{mod}11)$.

Hence, $5^{38} = 5^{30}5^8 = (5^{10})^3 5^8 \equiv 1^3 \cdot 4 \equiv 4(\text{mod}11)$

Therefore, $5^{38} \equiv 4(\text{mod}11)$.

Thus remainder is 4.

Ex.2. Use Fermat's theorem to verify that $17|11^{104} + 1$.

Solution. By Fermat's theorem

$11^{16} \equiv 1(\text{mod}17)$.

Further $\left(11^{16}\right)^6 \equiv 1^6 (\text{mod}17) \Rightarrow 11^{96} = \left(11^{16}\right) \equiv 1^6 \equiv 1(\text{mod}17)$.

Now

$11^2 = 121 \equiv 2(\text{mod}17) \Rightarrow 11^8 \equiv 2^4 \equiv (-1)(\text{mod}17)$.

Thus

$11^{104} = 11^{96}.11^8 \equiv 1(-1)(\text{mod}17) \Rightarrow 11^{104} + 1 \equiv 0(\text{mod}17)$.

Note. If $a^n \equiv a(\text{mod}n)$ fails to hold good for some choice of a then n is necessarily composite.

For example, $n = 117$, then $2^{117} = 2^{16 \cdot 7+5} = (2^7)^{16} \cdot 2^5$.

Here $2^7 = 128 \equiv 11(\text{mod}117)$.

So that

$2^{117} = (2^7)^{16} \cdot 2^5 \equiv 11^{16} \cdot 2^5 (\text{mod}117)$.

Now $(11)^{16} = (121)^8 \equiv 4^8 (\text{mod}117)$.

Thus,

$2^{117} \equiv 4^8 \cdot 2^5 \equiv 2^{21} (\text{mod}117)$.

Now,

$2^{21} = \left(2^7\right)^3 \equiv 11^3 (\text{mod}117)$.

Therefore,

$$11^3 = 121 \cdot 11 \equiv 4.11 (\text{mod} 117)$$

Thus

$$2^{21} \equiv 11^3 \equiv 44 (\text{mod} 117).$$

Hence,

$$(a1 + q^{p-1} \equiv 1 (\text{mod } pq).$$

Thus,

$$2^{117} = 44 (\text{mod} 117)$$

$$2^{117} \not\equiv 2 (\text{mod} 117)$$

and that 117=13x9 is composite.

Lemma. If p and q are distinct primes with $a^p \equiv a$ (mod$q$) and $a^q \equiv a$ (mod$p$) and then

$$a^{pq} = a (\text{mod } pq).$$

Proof – By Fermat's theorem

$(a^q)^p \equiv a^q$ (mod p) and $(a^p)^q \equiv a^p$ (mod q)

These two along with

$$a^q \equiv a (\text{mod } p) \text{and } a^p \equiv a (\text{mod } q)$$

Gives us

$(a^q)^p \equiv a^q$ (mod p) $\Rightarrow$ $a^{pq} \equiv a$ (mod p)

And

$(a^p)^q \equiv a^p \equiv a$ (mod q)

$$\Rightarrow a^{pq} \equiv a (\text{mod } q)$$

Since p and q are distinct primes $\gcd(p,q) = 1$ and , hence, $a^{pq} \equiv a (\text{mod } pq)$.

Ex.3. Let p and q be distinct primes, prove that $p^{q-1} + q^{p-1} \equiv 1 (\text{mod } pq)$.

Solution. By Fermat's theorem $p^{q-1} \equiv 1 (\text{mod } q)$ and $q^{p-1} \equiv 1 (\text{mod } p)$. Also $p^{q-1} \equiv 0 (\text{mod } p)$ and $q^{p-1} \equiv 0 (\text{mod } q)$. Thus $p^{q-1} + q^{p-1} \equiv 1 (\text{mod } p)$ and $p^{q-1} + q^{p-1} \equiv 1 (\text{mod } q)$, therefore, $p^{q-1} + q^{p-1} \equiv 1 (\text{mod } pq)$.

Ex.4. Let p and q be distinct odd primes such that $p-1 \mid q-1$. If $\gcd(a, pq) = 1$, prove that $a^{q-1} \equiv 1 (\text{mod } pq)$.

Solution. Since $\gcd(a, pq) = 1$ and p, q are relatively prime $\gcd(a, p) = 1$ and $\gcd(a, q) = 1$.

By Fermat's theorem $a^{q-1} \equiv 1 (\mathrm{mod}\, q)$ and $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

Since $p-1 \mid q-1$, $(a^{p-1}-1) \mid (a^{q-1}-1)$.

Therefore, as $p \mid a^{p-1}-1$, we have $p \mid a^{q-1}-1$. Hence, $a^{q-1} \equiv 1 (\mathrm{mod}\, p)$.

Thus $a^{q-1} \equiv 1 (\mathrm{mod}\, pq)$.

Ex.5. Find the units digit of 3^{100} by use of Fermat's theorem.

Solution.Observe that by Fermat's theorem $3^4 \equiv 1 (\mathrm{mod}\, 5)$ and $3^4 \equiv 1 (\mathrm{mod}\, 2)$.

Since $\gcd(5, 2) = 1$, we get $3^4 \equiv 1 (\mathrm{mod}\, 10)$. Thus $3^8 = (3^4)^2 \equiv 1^2 \equiv 1 (\mathrm{mod}\, 10)$.

Hence, $3^9 = 3^8 3 \equiv 1 \cdot 3 \equiv 3 (\mathrm{mod}\, 10)$. Further, $3^{100} = 3 \cdot (3^9)^{11} \equiv 3 \cdot 3^{11} \equiv 3^4 \cdot 3^8 \equiv 1 \cdot 1 \equiv 1 (\mathrm{mod}\, 10)$.

Thus units digit is 1.

4.2 Pseudo Prime

By Fermat's theorem $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ happens for all prims p with the condition that $p \nmid a$

However $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$ may hold for non-prime p also.

Consider the example

$$2^{10} = 1024 = 31 \times 33 + 1 \ .$$

That is

$$2^{10} \equiv 1 (\mathrm{mod}\, 31) \Rightarrow 2^{11} \equiv 2 (\mathrm{mod}\, 31).$$

And by Fermat's theorem

$$2^{10} \equiv 1 (\mathrm{mod}\, 11).$$

So that

$$2^{31} = 2 \times 2^{30} = 2 \times (2^{10})^3 \equiv 2 \times 1 (\mathrm{mod}\, 11) \ .$$

Therefore,

$$2^{11 \cdot 31} \equiv 2 (\mathrm{mod}\, 11 \cdot 31)$$

$$\Rightarrow 2^{341} \equiv 2 (\mathrm{mod}\, 341)$$

$$\Rightarrow 2^{340} \equiv 1 (\mathrm{mod}\, 341)$$

Thus $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ holds for non-prime n. In other words, $n | a^{n-1} - 1$.

In particular $n | 2^{n-1} - 1$.

Such a composite integer 'n' is called Pseudo prime.

Note. $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ need not imply n is prime.

Definition.A composite number n is *pseudo prime* if $n | 2^n - 2$.

Note. Smallest pseudo prime is 341. Some others are 561, 645, 1105.

Theorem. If n is an odd pseudo prime then $M_n = 2^n - 1$ is a larger one .

Proof. Let 'n' be an odd pseudo prime. Since n is composite, let $n = rs,$ where $r, s > 1$ we may assume that $1 < r \le s < n$. Then

$M_n = 2^n - 1$

$= 2^{rs} - 1$

$= \left(2^r\right)^s - 1$

$= (2^r - 1)\left[(2^r)^{s-1} + (2^r)^{s-2} + ... + (2^r) + 1\right]$

Thus M_n is composite number .

Since n is pseudo prime, $n|2^n - 2$. .

That is, $2^{n-1} - 2 = kn$ for some integer k.

Now,

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

$= 2^{kn} - 1$

$= (2^n - 1)\left[(2^n)^{k-1} + (2^n)^{k-2} + \cdots + 1\right]$

$= M_n\left[(2^n)^{k-1} + (2^n)^{k-2} + \cdots + (2^n) + 1\right]$.

Thus ,

$M_n | 2^{M_n - 1} - 1 \Rightarrow M_n | 2\left(2^{M_n - 1} - 1\right) = 2^{M_n} - 2$.

Therefore, M_n is pseudo prime.

Definition. **(Pseudo Prime to base a).** A composite integer n for which $a^n \equiv a (\mathrm{mod}\, n)$ holds in called pseudo prime to the base a .

Notes . 1. Pseudo prime to the base 2 is called pseudo prime.

2. 91 is smallest pseudo prime to the base 3.

3. 217 is the smallest pseudo prime to the base 5.

4. There are infinitely many pseudo primes to any given base

5. There are 245 pseudo prime less than one million.

6. First example of even pseudo prime is 161038 = 2x73x1103 and was found in 1950.

7. There exist composite number n which are pseudo prime to every base a i.e. $a^n \equiv a(\mathrm{mod}\, n)$ for all *'a'*. The least such integer is 561. These exceptional numbers are called as absolute pseudo primes or Carmichael numbers_.

Carmichael indicated four absolute pseudo primes namely 561, 1105, 2821, 15841.

Ex.6. Prove that 561 is an absolute pseudo prime.

Solution. Note that 561 = 3x11x17.

Let $\gcd(a,561)=1$ then $\gcd(a,3)=1$, $\gcd(a,11)=1, \gcd(a,17)=1$.

Hence by Fermat's theorem

$a^2 \equiv 1(\mathrm{mod}\, 3), a^{10} \equiv 1(\mathrm{mod}\, 11)$, $a^{16} \equiv 1(\mathrm{mod}\, 17)$

$\Rightarrow a^{560} \equiv (a^2)^{280} \equiv 1^{280} \equiv 1 \pmod 3$,

$a^{560} \equiv (a^{10})^{56} \equiv 1^{56} \equiv 1 \pmod{11}$,

$a^{560} \equiv (a^{16})^{35} \equiv 1^{35} \equiv 1 \pmod{17}$,

Thus, $a^{560} \equiv 1(\mathrm{mod}\, 3\cdot 11\cdot 17)$.

That is, $a^{560} \equiv 1 \pmod{561}$ i.e., $a^{561} \equiv a \pmod{561}$.

Theorem. Let n a composite square free integer say, $n = p_1 p_2 \ldots p$ where the p_i are distinct primes. If $p_{i-1} \mid n-1$ for $i = 1,2,\ldots,r$ then n is absolute pseudo prime.

Proof. Suppose a is an integer relatively prime to n, that is $\gcd(a,n)=1$.

Then $\gcd(a, p_i)=1$ for $i = 1,2,\ldots,r$.

Hence, by Fermat's theorem, $a^{p_i-1} \equiv 1(\mathrm{mod}\, p_i)$.

Thus $p_i \mid a^{p_i-1}-1$.

Since $p_i \mid n-1$ for each $i = 1,2,\ldots,r$, we have $a^{p_i-1}-1 \mid a^{n-1}-1$.

Thus $p_i \mid a^{n-1} - 1$ for all $i = 1, 2, \ldots, r$.

Therefore, $n = p_1 p_2 \ldots p_n \mid a^{n-1} - 1$.

Thus, $a^{n-1} \equiv 1 (\text{mod} n)$, for all integers a . (relative prime ton)

Hence n is absolute pseudo prime.

e. g. 1) 561 = 3 .11. 17

2|560, 10|560, 16|560

2) 1729 = 7. 13. 19

6|1728, 12|1728, 16|1728

3) 10585 = 5. 29. 73

4|10584, 28|10584, 72|10584

Note. 1) Therefore are only 43 absolute pseudo primes less than one million.

4.3 Wilson's Theorem

Statement. For any prime $p, (p-1)! \equiv -1 (\text{mod}\, p)$.

Proof. For p = 2, 3 the result is trivial

Let p > 3

Let a be any one of the integers 1, 2, 3, …, p – 1 .

Then $\gcd(a, p) = 1$.

Consider the linear congruence $ax \equiv 1 (\text{mod}\, p)$. Since $\gcd(a, p) = 1$ the linear congruence $ax \equiv 1 (\text{mod}\, p)$ has a unique solution modulo p.

Let a' be a solution of $ax \equiv 1 (\text{mod}\, p)$, such that a' is one amongst 1, 2, …, p – 1 .

Thus a' is unique integer such that $1 \le a' \le p-1$ satisfying $aa' \equiv 1 (\text{mod}\, p)$.

Claim - : $a = a'$ if and only if either $a = 1$ or $a = p - 1$.

Consider,

$a^2 \equiv 1 (\text{mod}\, p)$

$\Rightarrow a^2 - 1 \equiv 0 (\text{mod}\, p)$

$\Rightarrow (a-1)(a+1) \equiv 0 (\text{mod}\, p)$

$\Rightarrow a - 1 \equiv 0 (\text{mod}\, p) \text{ or } \Rightarrow a + 1 \equiv 0 (\text{mod}\, p)$

Hence either $a = 1$ or $a = p - 1$.

Thus for any a other than 1 and p – 1, a' is distinct from a .

Thus we obtain $((p-3)/2)$ pairs (a, a') such that, $aa' \equiv 1 (\text{mod } p)$.

Hence,

$2 \cdot 3 \cdots (p-2) \equiv 1 (\text{mod } p)$

$\Rightarrow (p-2)! \equiv 1 (\text{mod } p)$

$\Rightarrow (p-1)(p-2)! \equiv p-1 (\text{mod } p)$

$\Rightarrow (p-1)! \equiv -1 (\text{mod } p)$

e.g. Let $p = 13$

$2.7 \equiv 1 (\text{mod} 13)$

$3.9 \equiv 1 (\text{mod} 13)$

$4.10 \equiv 1 (\text{mod} 13)$

$5.8 \equiv 1 (\text{mod} 13)$

$6.11 \equiv 1 (\text{mod} 13)$

Hence, $11! \equiv 1 (\text{mod} 13)$

i.e., $12! \equiv -1 (\text{mod} 13)$.

Converse of Wilson's theorem is also true

Theorem.If $(n-1)! \equiv -1 (\text{mod } n)$ then is prime.

Proof. Suppose n is composite then there is d such that 1< d < n and d|n. Then d |(n – 1) ! Thus $d \mid -1$, so that we arrive at contradiction. Hence n is prime.

Theorem. The quadratic congruence $x^2 + 1 \equiv 0 (\text{mod } p)$ where p is odd prime, has a solution if and only if $p \equiv 1 (\text{mod} 4)$.

Proof. Let a be any solution of $x^2 + 1 \equiv 0 (\text{mod } p)$ .Then $a^2 \equiv -1 (\text{mod } p)$.

Since $p \nmid a$, Fermat's theorem gives us

$1 \equiv a^{p-1} \equiv \left(a^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} (\mathrm{mod}\, p)$.

This holds only if $\frac{p-1}{2}$ is even.

i.e. $p-1 \equiv 0(\mathrm{mod}\, 4)$ or $p \equiv 1(\mathrm{mod}\, 4)$

(If p is of the form 4k + 3 then $\frac{p-1}{2}$ is of the form 2k + 1 and hence

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

So that, $1 \equiv -1(\mathrm{mod}\, p)$ which is impossible for odd prime)

Conversely,

Suppose that $p \equiv 1(\mathrm{mod}\, 4)$

To prove that $x^2 + 1 \equiv 0(\mathrm{mod}\, p)$ has a solution.

We know,

$p-1 \equiv -1(\mathrm{mod}\, p)$

$p-2 \equiv -2(\mathrm{mod}\, p)$

.

.

.

$\frac{p+1}{2} \equiv -\left(\frac{p-1}{2}\right)(\mathrm{mod}\, p)$.

Consider,

$(p-1)! = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) \cdots (p-1)$

$= 1 \cdot (p-1) \cdot 2 \cdot (p-2) \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)$.

Thus we obtain,

$(p-1)! \equiv 1(-1)2(-2)3(-3).....\left(\frac{p-1}{2}\right)\left(-\left(\frac{p-1}{2}\right)\right)$

$\equiv (-1)^{\left(\frac{p-1}{2}\right)}\left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$.

Since, $p \equiv 1(\mathrm{mod}\, 4)$, $\left(\frac{p-1}{2}\right)$ is even and hence, $(p-1)! \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$.

By Wilson's theorem, we have

$(p-1)! \equiv -1(\mathrm{mod}\, p)$.

Thus,

$-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$.

That is, $\left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 \equiv 0(\mathrm{mod}\, p)$.

Therefore, $x = \left(\frac{p-1}{2}\right)!$ is a solution of quadratic congruence $x^2 + 1 \equiv 0(\mathrm{mod}\, p)$.

Ex.7. Find the remainder when 15! is divided by 17 .

Solution. By Wilson's theorem, we have $16! \equiv -1(\mathrm{mod}17)$, that is, $16! \equiv 16(\mathrm{mod}17)$.

Since $\gcd(16,17) = 1$, we can cancel 16 from both sides and we get, $15! \equiv 1(\mathrm{mod}17)$.

Therefore, the remainder is 1.

Note. It may be noted that, for any prime p, $(p-2)! \equiv 1(\mathrm{mod}\, p)$ which is an intermediate step in the proof of Wilson's theorem.

Ex.8 Find the remainder when 2.26!is divided by 29.

Solution. By Wilson's theorem, $28! \equiv -1(\mathrm{mod}\, 29)$, that is , $-1 \equiv 28!(\mathrm{mod}\, 29)$. Therefore,

$-1 \equiv 26!27.28(\mathrm{mod}\, 29)$

$\Rightarrow -1 \equiv 26!(-2)(-1)(\mathrm{mod}\, 29)$

$\Rightarrow -1 \equiv 26!(2)(\mathrm{mod}\, 29)$

$\Rightarrow 2.26! \equiv 28(\mathrm{mod}\, 29)$.

4.4 Fermat's Factorization Method

In this method we try to write integer n as difference of two squares. We start with an integer a whose square is greater than n and nearest to n and proceed further by taking $a+1, a+2, ..., a+k$ till we get an integer b such that $(a+k)^2 - n = b^2$.

Ex.9 Using Fermat's factorization method factorize 119143.

Solution. Observe that, $345^2 < 119143 < 346^2$.

Consider,

$346^2 - 119143 = 119716 - 119143 = 573$

$347^2 - 119143 = 120409 - 119143 = 1266$

$348^2 - 119143 = 121104 - 119143 = 1961$

$349^2 - 119143 = 121801 - 119143 = 2658$

$350^2 - 119143 = 122501 - 119143 = 3357$

$351^2 - 119143 = 123204 - 119143 = 4058$

$352^2 - 119143 = 123902 - 119143 = 4761 = (69)^2$.

Thus,

$352^2 - 119143 = (69)^2 \Rightarrow 119143 = 352^2 - (69)^2$

$= (352+69)(352-69)$

$= 421 \times 283$.

Ex.10. Factors 23449

Solution. Observe that $153^2 < 23449 < 154^2$.

Consider

$154^2 - 23449 = 23716 - 23449 = 267$

$155^2 - 23449 = 24025 - 23449 = 576 = 24^2$.

Thus

$155^2 - 23449 = 24^2$

$23449 = 155^2 - 24^2$

$= (155+24)(155-24)$

$= 179 \times 131$.

Note. While examinating the difference for possible square many values can be excluded by inspection. We know that the square must end in one of the 6 digits 0, 1, 4, 5, 6, 9

Further by calculating the squares of the integers the last two digits are limited to 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 69, 76, 81, 84, 89, 96.

Ex.11. Factorize 2279, 10541, 340663.

Solution. 1) 2279

We observe that-

$47^2 < 2279 < 48^2$.

Consider,

$48^2 - 2279 = 25 = 5^2$.

Therefore, $2279 = 48^2 - 5^2$.

$2279 = (48+5)(48-5)$

$= 53 \times 43$

2) 10541

We observe that

$102^2 < 10541 < 103^2$.

Consider $103^2 - 10541 = 68$

$1024 - 10541 = 275$

$105^2 - 10541 = 484 = 22^2$

$105^2 - 10541 = 22^2$

$10541 = 105^2 - 22^2$

$= (105-22)(105+22)$

$= 83 \times 127$

3) 340663

We observe that

$583 < 340663 < 590$

Consider

$(584)^2 - 340663 = 393$

$(585)^2 - 340663 = 1562$,

$(586)^2 - 340663 = 2733$,

$(587)^2 - 340663 = 3906$,

$(588)^2 - 340663 = 5081$,

$(589)^2 - 340663 = 6258$,

$(590)^2 - 340663 = 7439$,

$(591)^2 - 340663 = 8618$,

$(592)^2 - 340663 = 9801 = 99^2$.

Thus $(592)^2 - 340663 = 99^2$.

Hence,

$340663 = (592)^2 - 99^2$

$= (592 - 99)(592 + 99)$

$= 493 \times 691$.

4.5 Generalization of Fermat's Factorization Method

Here we look for two integers x and y such that $x^2 - y^2$ is a multiple of n. In other words $x^2 \equiv y^2 \pmod{n}$.

Let d = gcd (x – y, n) (or d = gcd (x + y, n)

Then is d a non – trivial divisor of n?, that is, do we have $1 < d < n$?

In practice, n is usually the product of two primes p and q . Let n be a number of the form n = pq, where p and q are prime integers. With no loss of generality we can take p < q.

Note that d is one of the integer 1, p, q, pq. Suppose that $p \mid x - y$ and $q \mid x - y$ then $pq \mid x - y$. But then $n = pq \mid x - y$ that is $x \equiv y \pmod{n}$. Similarly if $p \mid x + y$ and $q \mid x + y$ then $x \equiv -y \pmod{n}$. Since $x \not\equiv \pm y \pmod{n}$. Hence, one of p and q divides $(x+y)$ and the other $(x-y)$. Thus $\gcd(x-y, n)$ and $\gcd(x+y, n)$ give us the two divisors of n.

Ex.12. Factorize 2189.

Solution – Consider n = 2189.

Let us look for squares close to multiple of n.

Observe that $47^2 - 2189 = 20$.

Now $66^2 - 2 \times 2189 = -22$,

$(81)^2 - 3 \times 2189 = -6$,

$(94)^2 - 4 \times 2189 = 80$,

$(105)^2 - 5 \times 2189 = 80$,

$(115)^2 - 6 \times 2189 = 91$,

$(124)^2 - 7 \times 2189 = 53$,

$(132)^2 - 8 \times 2189 = -88$,

$(140)^2 - 9 \times 2189 = -101$,

$(148)^2 - 10 \times 2189 = 14$,

$(155)^2 - 11 \times 2189 = -54$.

Now, $81 \times 155 = 12555 \equiv -579 \pmod{2189} \Rightarrow 81^2 \times 155^2 \equiv (579)^2 \pmod{2189}$.

Further

$81^2 \equiv -6 \pmod{2189}$ and $155^2 \equiv -54 \pmod{2189}$.

Thus $(81)^2 (155)^2 \equiv (-6)(-54) \equiv (18)^2 \pmod{2189}$.

Hence $(579)^2 \equiv (18)^2 \pmod{2189}$.

Thus $\gcd(579+18, 2189) = \gcd(597, 2189) = 199$ and
$\gcd(579-18, 2189) = \gcd(561, 2189) = 11$ are factors of 2189.

EXERCISES

1. Factor the number $2^{11} - 1$ by Fermat's factorization method.(Ans. 89x23)
2. Employ the generalized Fermat's method to factor each of the following numbers
   a) 2911 [Hint, $138^2 \equiv 67^2 \pmod{2911}$]
   b) 4573 [Hint, $177^2 \equiv 92^2 \pmod{2911}$]

❑❑❑

Unit-5
Number Theoretic Functions

5.1 A function from set of integers into set of integers is called *number theoretic function*.

We begin with

Definition. For any integer n the number of positive divisors of n is denoted by $\tau(n)$.

Definition. For any integer n the sum of all positive divisors of n is denoted by $\sigma(n)$.

e.g. 1. $\tau(1)=1,\tau(2)=2,\tau(3)=2,\tau(4)=3,\tau(5)=2,\tau(6)=4,\tau(7)=2,\tau(8)=4,\tau(9)=3,\tau(10)=4$

2. $\sigma(1)=1,\sigma(2)=3,\sigma(3)=4,\sigma(4)=7,\sigma(5)=6,\sigma(6)=12,\sigma(7)=8,\sigma(8)=15$,

$\sigma(9)=13,\sigma(10)=18$.

Notation. Let n be any integer and $d_1,d_2,\ldots,d_r$ denote divisors of n , then

$$\sum_{d|n} f(d)=f(d_1)+f(d_2)+\cdots+f(d_r).$$

With this notation we have $\tau(n)=\sum_{d|n}1;\sigma(n)=\sum_{d|n}d$.

Note: For any prime $p,\tau(p)=2,\sigma(p)=p+1$.

Theorem. If $n=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$ is the prime factorization of $n>1$, then the positive divisors of n are precisely those integers d of the form $d=p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}$ where $0\le a_i<k_i$ for $i=1,2,\ldots,r$.

Proof. Note that the divisor $d=1$ is obtained when $a_1=a_2=\cdots=a_r=0$ and n itself occurs when $a_1=k_1,a_2=k_2,\ldots,a_r=k_r$. Let d be the nontrivial divisor of n , then $n=dd'$ where $d,d'>1$. Let $d=q_1q_2\cdots q_s,d'=t_1t_2\cdots t_u$ be the prime factorizations of d and d' . Then $p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}=q_1q_2\cdots q_st_1t_2\cdots t_u$ will be two factorizations of n .

Hence, by uniqueness of factorization, we obtain $d=p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}$, where $0\le a_i\le k_i$ and the possibility that $a_i=0$ is permitted.

Conversely, let $d=p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}$, where $0\le a_i<k_i$.

Then

$$n=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}=p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}p_1^{k_1-a_1}p_2^{k_2-a_2}\ldots p_r^{k_r-a_r}=dd'$$

where $d'=p_1^{k_1-a_1}p_2^{k_2-a_2}\ldots p_r^{k_r-a_r}$ and $k_i-a_i\ge 0$ for $1\le i\le r$. Then $d'>0$ and $d\mid n$.

Theorem. If $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ is the prime factorization of $n > 1$, then

a) $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$

b) $\sigma(n) = \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{k_2+1} - 1}{p_2 - 1} \right) \cdots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1} \right)$.

Proof. We know that every divisor of n is of the form $d = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ where $0 \le a_i < k_i$. There are $k_1 + 1$ choices for the exponent a_1, there are $k_2 + 1$ choices for the exponent $a_2, \dots$ and $k_r + 1$ choices for the exponent a_r. Hence, $\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$.

Further,

$\sigma(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{k_1})(1 + p_2 + p_2^2 + \cdots + p_2^{k_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{k_r})$

Thus $\sigma(n) = \left(\frac{p_1^{k_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{k_2+1} - 1}{p_2 - 1} \right) \cdots \left(\frac{p_r^{k_r+1} - 1}{p_r - 1} \right)$.

e.g. Let $n = 180 = 2^2 \cdot 3^2 \cdot 5^1$.

Therefore,

$\tau(180) = (2+1)(2+1)(1+1) = 18$ and $\sigma(180) = \left(\frac{2^3 - 1}{2 - 1} \right) \left(\frac{3^3 - 1}{3 - 1} \right) \left(\frac{5^2 - 1}{5 - 1} \right) = 546$.

Theorem. The product of positive divisors of $n > 1$ is $n^{T(n)/2}$.

Proof. Let d and d' be a positive divisors of n then $n = dd'$, where $1 \le d \le n, 1 \le d' \le n$.

So, $n^{\tau(n)} = \prod_{d|n} d \prod_{d'|n} d'$ .Since $\prod_{d|n} d = \prod_{d'|n} d'$.

We have , $n^{\tau(n)} = \left(\prod_{d|n} d \right)^2 \Rightarrow n^{\frac{\tau(n)}{2}} = \prod_{d|n} d$.

e.g. $\prod_{d|16} d = 16^{\tau(16)/2} = 16^{5/2} = 2^{10} = 1024.$

Note that , $\tau(20) = \tau(5) \cdot \tau(4)$ but $\tau(20) \ne \tau(10) \cdot \tau(2)$ and $\sigma(20) = \sigma(5) \cdot \sigma(4)$ but $\sigma(20) \ne \sigma(10) \cdot \sigma(2)$.

5.2 Multiplicative Function

Let f be a number theoretic function, then f is multiplicative if,

$f(m.n) = f(m) \cdot f(n)$ whenever $\gcd(m, n) = 1$.

Theorem.The function τ and σ are multiplicative.

Proof : Let m, n be integers such that $\gcd(m,n)=1$. If either m = 1 or n = 1 then as $\sigma(1)=1$ and , $\tau(1)=1$,the result is trivial.

Suppose that m > 1 and n > 1.

By fundamental theorem of Arithmetic

$m=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$ and $n=q_1^{l_1}q_2^{l_2}\ldots q_s^{l_s}$.

where, $p_1,p_2,\ldots,p_r$ and $q_1,q_2,\ldots,q_s$ are primes and $k_1,k_2,\ldots,k_r;l_1,l_2,\ldots,l_s$ are positive integers.

Thus, $mn=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}q_1^{l_1}q_2^{l_2}\ldots q_s^{l_s}$.

Since m and n are relatively prime, $p_1,p_2,\ldots,p_r$ and $q_1,q_2,\ldots,q_s$ are distinct primes, we have

$$\sigma(mn)=\left(\frac{p_1^{k_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{k_2+1}-1}{p_2-1}\right)\cdots\left(\frac{p_r^{k_r+1}-1}{p_r-1}\right)\left(\frac{q_1^{l_1+1}-1}{q_1-1}\right)\left(\frac{q_2^{l_2+1}-1}{q_2-1}\right)\cdots\left(\frac{q_s^{l_s+1}-1}{q_s-1}\right)=\sigma(m)\sigma(n)$$

and

$$\tau(mn)=(k_1+1)(k_2+1)\cdots(k_r+1)(l_1+1)(l_2+1)\cdots(l_s+1)=\tau(m)\tau(n)$$

Lemma. If $\gcd(m,n)=1$ then the set of positive divisors of mn consists of all products d_1d_2 where $d_1 \mid m$ and $d_2 \mid n$ and $\gcd(d_1,d_2)=1$. Furthermore, these products are all distinct.

Proof. Suppose m > 1 and n > 1, then, by Fundamental theorem of Arithmetic both m and n have prime factorization as follows. $m=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}$ and $n=q_1^{l_1}q_2^{l_2}\ldots q_s^{l_s}$.

Then $mn=p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}q_1^{l_1}q_2^{l_2}\ldots q_s^{l_s}$ and any divisor of mn is of the form $d=p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}q_1^{b_1}q_2^{b_2}\ldots q_s^{b_s}$ where $0\le a_i<k_i$ and $0\le b_i<l_i$.

Let $d_1=p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}, d_2=q_1^{b_1}q_2^{b_2}\ldots q_s^{b_s}$. Hence, $d_1 \mid m$ and $d_2 \mid n$, $d = d_1d_2$, $\gcd=(d_1,d_2)=1$ and d_1, d_2 are infact distinct.

Theorem. If f is a multiplicative function and F is defined by $F(n)=\sum_{d\mid n}f(d)$. Then F is also multiplicative.

Proof. Let m, n be relatively prime integers.

Consider,

$$F(mn)=\sum_{d|mn} f(d)=\sum_{\substack{d_1|m\\ d_2|n}} f(d_1d_2).$$

Then $F(mn)=\sum_{\substack{d_1|m\\ d_2|n}} f(d_1)f(d_2)$.

Since $\gcd(d_1,d_2)=1$ we can write

$$F(mn)=\left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right).$$

Thus $F(mn)=F(m)F(n)$.

e.g. Let m = 8, n = 3, then

F(8.3) = f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24)

= f(1.1) + f(2.1) + f(1.3) + f(4.1) + f(2.3) + f(8.1) + f(4.3) + f(8.3)

= f(1).(1) + f(2). f(1) + f(1).f(3) + f(4) . f(1)+ f(2) . f(3) + f(8) . f(1) + f(4) . f(3) + f(8) . f(3)

= (f(1) + f(2) + f(4) + f(8)) (f(1) + f(3)) = f(8) . f(3)

Corollary. The function τ and σ are multiplicative.

Proof. We know $f(n)=1$ and $f(n)=n$ are multiplicative. Hence, $\tau(n)=\sum_{d|n}1$ and

$\sigma(n)=\sum_{d|n} d$ are multiplicative.

5.3 The Mobius inversion formula

We begin with

Definition.(Mobius μ Function).

For a positive n, define the function μ by the rules

$$\mu(n)=\left\{\begin{array}{lll} 1, & \text{if } n=1 & \\ 0, & \text{if } p^2|n & \text{for some prime p} \\ (-1)^r & \text{if } n=p_1p_2\ldots p_r & \text{where } p_i s \text{ are all distinct}\end{array}\right\}$$

e.g. $\mu(1)=1,\mu(2)=-1,\mu(3)=-1,\mu(4)=0,\mu(5)=-1,$

$\mu(6)=1,\mu(7)=-1,\mu(8)=0,\mu(9)=0,\mu(10)=1,$

$\mu(30)=\mu(2\times3\times5)=(-1)^3=-1.$

Theorem. The function μ is a multiplicative function.

Proof. Let a, b be two relatively prime positive integers.

If p is a prime such that $p^2 \mid a$ or $p^2 \mid b$, then $\mu(a)=0$ or $\mu(b)=0$ accordingly.

In this case $p^2 \mid ab$ and hence, $\mu(ab)=\mu(a).\mu(b)=0$.

Let both a and b be square free. Since a and b are relatively prime, there is no common prime divisor.

Let $a = p_1 p_2 \ldots p_r$ and $b = q_1 q_2 \ldots q_s$ where $p_1, p_2, \ldots, p_r; q_1, q_2, \ldots, q_s$ are all distinct.

Hence, ab is square free and $ab = p_1 p_2 \ldots p_r q_1 q_2 \ldots q_s$.

So, $\mu(ab) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(a).\mu(b)$.

Hence, the result.

Theorem – For each positive integer $n \geq 1$

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1 \end{cases}$$

where d runs through the positive divisors of n.

Proof – If n = 1, then $\sum_{d|1} \mu(d) = \mu(1) = 1$. Suppose $n > 1$, then let $F(n) = \sum_{d|n} \mu(d)$.

Let $n = p^k$, for some prime p and $k \geq 1$, then

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^K)$$

$$= 1 + (-1) + 0 + 0 + \ldots.. + 0$$

$$= 0 .$$

Let n > 1, then there is prime factorization of n namely $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, $1 \leq k_i, i = 1, \ldots., r$.

Since μ is multiplicative, $F(n) = \sum_{d|n} \mu(d)$ is multiplicative.

Consider,

$$F(n) = F(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r}) = 0.$$

Since $F(p^k) = \sum_{d|p^k} \mu(d) = 0$.

Thus, we have $\sum_{d|n} \mu(d) = F(n) = 0$ for n>1.

Theorem. (Mobius Inversion Formula)

Let F and f be two number theoretic functions related by the formula

$F(n)=\sum_{d|n} f(d)$. Then

$$f(n)=\sum_{d/n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d/n}\mu\left(\frac{n}{d}\right)F(d)$$

Proof. Note that, the two expressions

$$\sum_{d/n}\mu(d)F\left(\frac{n}{d}\right) \text{ and } \sum_{d/n}\mu\left(\frac{n}{d}\right)F(d)$$

are infact one and the same as one can be obtained by replacing dummy index d by $d'=\frac{n}{d}$; as d ranges over all positive divisors of n.

Consider

$$\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d|n}\left(\mu(d)\sum_{c|(n/d)}f(c)\right)$$

$$=\sum_{d|n}\left(\sum_{c|(n/d)}\mu(d)f(c)\right). \qquad \ldots\ldots (1)$$

Now, $d\mid n$ and $c\mid\frac{n}{d}\Rightarrow da=n$ and $cb=\frac{n}{d}$, for some integers a and b $\Rightarrow c\mid n$ and $d\mid\frac{n}{c}$.

Using this in Equation (1), we obtain

$$=\sum_{d|n}\left(\sum_{c|(n/d)}\mu(d)f(c)\right)=\sum_{c|n}\left(\sum_{d|(n/c)}f(c)\mu(d)\right)=\sum_{c|n}\left(f(c)\sum_{d|(n/c)}\mu(d)\right)$$

We know that

$\sum_{d|\frac{n}{c}}\mu(d)=0$, for all $\frac{n}{c}>1$

$= 1,\ n = c$

Therefore, $\sum_{d|\frac{n}{c}}\mu(d)=1$.

Hence, we obtain $\sum_{c|n}\left(f(c)\sum_{d|(n/c)}\mu(d)\right)=\sum_{c=n}f(c)\cdot 1=f(n).$

Hence, $f(n)=\sum_{d|n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d|n}\mu\left(\frac{n}{d}\right)F(d)$

Note. We know $\tau(n)=\sum_{d|n}1, \sigma(n)=\sum_{d|n}d$.

Hence, $1=\sum_{d|n}\mu\left(\frac{n}{d}\right)\tau(d)$ and $n=\sum_{d|n}\mu\left(\frac{n}{d}\right)\sigma(d)$.

Theorem. If F is a multiplicative function and $F(n)=\sum_{d|n}f(d)$. Then f is also multiplicative.

Proof. Let m, n be relatively prime positive integers.

We know that any divisor d of mn is of the form $d = d_1 d_2$, where $d_1 \mid m, d_2 \mid n$ and $\gcd(d_1,d_2)=1.$

Invoking inversion formula, we have

$$f(mn)=\sum_{d|mn}\mu(d)F\left(\frac{mn}{d}\right)$$

$$=\sum_{\substack{d_1|m,\\ d_2|n}}\mu(d_1d_2)F\left(\frac{mn}{d_1d_2}\right)$$

$$=\sum_{\substack{d_1|m,\\ d_2|n}}\mu(d_1)\mu(d_2)F\left(\frac{m}{d_1}\right)F\left(\frac{n}{d_2}\right)$$

$$=\sum_{d_1|m}\mu(d_1)F\left(\frac{m}{d_1}\right)\cdot\sum_{d_2|n}\mu(d_2)F\left(\frac{n}{d_2}\right)$$

$$=f(m)f(n)$$

Thus f is multiplicative.

Ex. For each positive integer *n*, show that $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3)=0$.

Sol. Observe that one of the four consecutive integers *n*, (*n* + 1), (*n* + 2), (*n* + 3) is always divisible by $4 = 2^2$ and hence, not square free. Thus one of $\mu(n),\mu(n+1),\mu(n+2),\mu(n+3)$ is always zero.

5.4 Greatest Integer Function

For any real number x, the greatest integer function denoted by $[x]$ is defined as the largest integer less than or equal to x, that is, $[x]$ is the unique integer satisfying $x-1<[x]\le x$.

Note that any real number x can be written as, $x=[x]+\theta$, where $0\le\theta<1$. Moreover, $[x]=x$ if and only if x is an integer.

Theorem. If n is a positive integer and p is a prime, then the exponent of the highest power of p that divides $n!$ is $\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$ where the series is finite since $\left[\frac{n}{p^k}\right]=0$ for $p^k>n$.

Proof. Among the first n integers those divisible by prime p are p, 2p, 3p, …,tp where t is the greatest integer such that $tp\le n$. In other words t is the largest integer less than or equal to $\frac{n}{p}$, so that $\left(t=\left[\frac{n}{p}\right]\right)$.

Thus there are $\left[\frac{n}{p}\right]$ multiplies of p occurring in n!, namely, $p,2p,\ldots,\left[\frac{n}{p}\right]p$.

Further, among the first n integers those divisible by p^2 are $p^2,2p^2,\ldots,tp^2$,

where, t is the largest positive integer such that $tp^2\le n$, that is, $t=\left[\frac{n}{p^2}\right]$.

Thus there are $\left[\frac{n}{p^2}\right]$ multiplies of p^2 occurring in n!, namely, $p^2,2p^2,\ldots,\left[\frac{n}{p^2}\right]p^2$.

Similarly, those integers which are divisible by p^3 are precisely $\left[\frac{n}{p^3}\right]$ in number and so on.

Observe that highest power of p that divides n is the sum of these integers namely, $\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots..=\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$.

Note. In view of this result, we can write $n!=\prod_{p\le n}p^{\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]}$.

Ex.1. Determine the number of zeros with which the decimal representation of 50! terminates.

Solution. To determine the number of zeros, it is enough to observe how may tens divide 50!.

That is, how many pairs of 5 and 2 divide50!.

For that we are to find the exponents of 2's and 5's that divide 50!.

The exponent of $2 = \sum_{k=1}^{\infty}\left[\frac{50}{2^k}\right]$

$$=\left[\frac{50}{2}\right]+\left[\frac{50}{2^2}\right]+\left[\frac{50}{2^3}\right]+\left[\frac{50}{2^4}\right]+\left[\frac{50}{2^5}\right]$$

$$=25+12+6+3+1$$

$$=47.$$

And,

Exponent of $5=\sum_{k=1}^{\infty}\left[\frac{50}{5^k}\right]$

$$=\left[\frac{50}{5}\right]+\left[\frac{50}{5^2}\right]$$

$$=10+2$$

$$=12.$$

Thus there are 12 pairs and hence 12 zeros.

Theorem. If n and r are positive integer with $1 \le r \le n$ then the binomial coefficient

$\binom{n}{r}=\frac{n!}{(n-r)!r!}$ is also an integer .

Proof. We know that for any two real numbers a and b

$$[a+b] \ge [a]+[b].$$

Using this we can write

$$\left[\frac{n}{p^k}\right] \ge \left[\frac{n-r}{p^k}\right]+\left[\frac{r}{p^k}\right]$$

where p is a prime and k is a positive integer.

Thus $\sum_{k\ge1}\left[\frac{n}{p^k}\right] \ge \sum_{k\ge1}\left[\frac{n-r}{p^k}\right]+\sum_{k\ge1}\left[\frac{r}{p^k}\right]$. …… (1)

Thus L.H.S. of Equation (1) is the exponent of highest power of p that divides n! and R.H.S. of (1) is the highest power of p that divides $(n-r)!$ plus highest power of p that divides r!.

Thus r.h.s of (1) is the highest power of p that divides the product $(n-r)!r!$.

Thus highest power of p that divides $(n-r)!r!$ is less than or equal to highest power of p that divides n!.

Hence, $\frac{n!}{(n-r)!r!}$ is always an integer.

Corollary. For a positive integer r the product of any r consecutive positive integer is divisible by r!

Proof. Let n be a positive integer such that n, n – 1, n – 2, ….., n – (r – 1) are r consecutive positive integers.

Consider,

$$n\,(n-1)\ldots(n-r+1) = \frac{n\,(n-1)\ldots(n-r+1)(n-r)\ldots 2.1}{(n-r)\ldots 2.1}$$

$$= \frac{n!}{(n-r)!}$$

$$= \frac{n!}{(n-r)!r!} \times r!$$

Since, $\frac{n!}{(n-r)!r!}$ is an integer, the product of *r* consecutive positive integer is divisible by r!.

e.g. $n(n+1)(n+2)(n+3)$ are divisible by 4!.

Theorem. Let f and F be number theoretic functions such that $F(n) = \sum_{d|n} f(d)$.

Then for any positive integer N,

$$\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N} f(k)\left[\frac{N}{k}\right].$$

Proof. We have $F(n) = \sum_{d|n} f(d)$.

Therefore, $\sum_{n=1}^{N} F(n) = \sum_{n=1}^{N}\sum_{d|n} f(d)$.

The strategy is to collect terms with equal values of f(d) in the double sum.

Let $k \le n$ be fixed, then f(k) appears in $\sum_{d|n} f(d)$ if and only if k divides n.

Since each integer divides itself, f(k) appears in the sum at least once for each k, $1 \le k \le n$. Now in order to find the number of sums $\sum_{d|n} f(d)$ in which f(k) occurs, it is enough to find the number of integers amongst the numbers 1,2,3,…,N which are divisible by k. These are exactly $\left[\frac{N}{k}\right]$ of them; $k, 2k, \ldots, \left[\frac{N}{k}\right]k$. Thus for each k such that $1 \le k \le N$, $f(k)$ is a term of the sum $\sum_{d|n} f(d)$ for $\left[\frac{N}{k}\right]$ different positive integers less than or equal to N. Thus $\sum_{n=1}^{N}\sum_{d|n} f(d) = \sum_{k=1}^{N} f(k)\left[\frac{N}{k}\right]$.

e.g., Let us consider N = 10.

$$\sum_{n=1}^{10}\sum_{d|n} f(d) = \sum_{d|1} f(d) + \sum_{d|2} f(d) + \cdots + \sum_{d|10} f(d)$$

$$\begin{aligned}
&= f(1)\\
&+\big(f(1)+f(2)\big)\\
&+\big(f(1)+f(3)\big)\\
&+(f(1)+f(2)+f(4))\\
&+(f(1)+f(5))\\
&+(f(1)+f(2)+f(3)+f(6))\\
&+(f(1)+f(7))\\
&+(f(1)+f(2)+f(4)+f(8))\\
&+(f(1)+f(3)+f(9))\\
&+\big(f(1)+f(2)+f(5)+f(10)\big)
\end{aligned}$$

$$\begin{aligned}
&= f(1)(10)+f(2)(5)+f(3)(3)+f(4)(2)+f(5)(2)\\
&+f(6)(1)+f(7)(1)+f(8)(1)+f(9)(1)+f(10)(1)
\end{aligned}$$

$$= f(1)\left[\frac{10}{1}\right]+f(2)\left[\frac{10}{2}\right]+f(3)\left[\frac{10}{3}\right]+f(4)\left[\frac{10}{4}\right]+f(5)\left[\frac{10}{5}\right]$$

$$+f(6)\left[\frac{10}{6}\right]+f(7)\left[\frac{10}{7}\right]+f(8)\left[\frac{10}{8}\right]+f(9)\left[\frac{10}{9}\right]+f(10)\left[\frac{10}{10}\right]$$

Thus $\sum_{n=1}^{N} F(n) = \sum_{k=1}^{N} f(k)\left[\frac{N}{K}\right]$.

Corollary. If N is a positive integer then $\sum_{n=1}^{N}\tau(n)=\sum_{k=1}^{N}\left[\frac{N}{k}\right]$

Proof . We know $\tau(n)=\sum_{d|n}1$. Thus by taking τ for F and f to be the constant function $f(n)=1$ for all n , we obtain

$$\sum_{n=1}^{N}\tau(n)=\sum_{k=1}^{N}1.\left[\frac{N}{k}\right]=\sum_{k=1}^{N}\left[\frac{N}{k}\right].$$

Similarly, we obtain

Corollary. If N is a positive integer then $\sum_{n=1}^{N}\sigma(n)=\sum_{k=1}^{N}k\left[\frac{N}{k}\right].$

e.g. Consider the case N = 6

$$\sum_{n=1}^{N}\tau(n)=\sum_{k=1}^{6}\left[\frac{6}{k}\right]=\left[\frac{6}{1}\right]+\left[\frac{6}{2}\right]+\left[\frac{6}{3}\right]+\left[\frac{6}{4}\right]+\left[\frac{6}{5}\right]+\left[\frac{6}{6}\right]$$

$$=6+3+2+1+1+1$$

$$=14$$

And

$$\sum_{n=1}^{6}\sigma(n)=\sum_{k=1}^{6}k.\left[\frac{6}{k}\right]$$

$$=1(6)+2(3)+3(2)+4(1)+5(1)+6(1)$$

$$=33.$$

Exercises

1. Find the highest power of 5 dividing 1000! And highest power of 7 that divides 2000!
2. Determine the number of zeros with which the decimal representation of 1000! terminates.
3. For what value of n does n! terminates in 37 zeros?

Answers: 1. 249,164 2. 249 3.150.

❑❑❑

Unit-6

Euler's Generalization of Fermat's theorem

6.1 We begin with

Definition – (Euler phi function)

For $n \geq 1$, let $\phi(n)$ denote the number of positive integers less than or equal to n and relatively prime to n.

e.g., $\phi(1)=1, \phi(2)=1, \phi(3)=2, \phi(4)=2, \phi(5)=4, \phi(6)=2, \phi(7)=6,$

$\phi(8)=4, \phi(9)=6, \phi(10)=4, \phi(30)=8.$

Note. For any prime p, $\phi(p)=p-1$.

Theorem. If p is a prime and $k>0$ then $\phi(p^k)=p^k-p^{k-1}=p^k\left(1-\frac{1}{p}\right)$.

Proof. Since $\gcd(n, p^k)=1$ if and only if $p \nmid n$. Amongst the integers 1, 2, ..., p^k those divisible by p are p, $2p$, $3p$, ..., (p^{k-1}) p. Thus the number of positive integers less than or equal to p^k that are divisible by p are p^{k-1} .

Therefore, number of positive integers less than p^k that are relatively prime to p^k is

$$\phi(p^k)=p^k-p^{k-1}=p^k\left(1-\frac{1}{p}\right).$$

Lemma. Given integers $a,b,c, \gcd(a,bc)=1$ if and only if $\gcd(a,b)=1$ and $\gcd(a,c)=1$

Proof. Suppose $\gcd(a,bc)=1$ .Let $d=\gcd(a,b)$, then $d \mid a$ and $d \mid b$, so that $d \mid a$, $d \mid bc$ and hence, $d \leq \gcd(a,bc)=1$. Therefore d = 1 .Similarly $\gcd(a,c)=1$.

Conversely, suppose that $\gcd(a,c)=1$.

Let d_1 = gcd (a,bc). Let if possible $d_1 > 1$ it must have prime factor p. Since p is prime, $d_1 \mid bc \Rightarrow p \mid bc \Rightarrow p \mid b$ or $p \mid c$. Suppose $p|b$. Further, $p \mid d_1$ and $d_1 \mid a \Rightarrow p \mid a$ consequently, $p \leq \gcd(a,b)$ which is absurd. On the other hand if we take $p|c$, then $p \leq \gcd(a,c)$ is also a contradiction.

Hence, $\gcd(a,bc)=1$.

Theorem. The function ϕ is a multiplicative function.

Proof. Let m, n are relatively prime integers. Since $\phi(1)=1$ the result holds trivially when either m = 1 or n = 1. Let m > 1 and n > 1.

Let us arrange m, n integers form 1 to mn as follows

1	2	…	r	…	m
m + 1	m +2	…	m + r	…	2m
2m + 1	2m + 2	…	2m + r	…	3m
(n – 1)m + 1	(n – 1) m + 2	…	(n – 1)m + r	…	nm.

Now, $\phi(mn)$ is equal to the number of entries in the array which are relatively prime to mn.

We know that a number is relatively prime to mn if and only if it is relatively prime to both m and n. We know that, $\gcd(qm+r,m)=\gcd(m,r)$, that is, if an element in the first row is relatively prime to m, then the whole column corresponding to that element is relatively prime to m. Therefore as many as $\phi(m)$ columns are there each integer of which is relatively prime to m.

Consider the entries in the r^{th} column

r, m + r, 2m + r, … , (n – 1)m + r.

Let r be such that $\gcd(m,r)=1$.

Since,

$km+r \equiv jm+r \pmod{n},\ (0 \le j < k < n)$

$\Rightarrow km \equiv jm \pmod{n}$

$\Rightarrow k \equiv j \pmod{n}$

$\Rightarrow n \mid k-j$.

which is absurd, no two entries in the rth column are congruent to one another modulo n. Therefore, $r, m+r, 2m+r, \ldots, (n-1)m+r$ are congruent to 0, 1, 2, … , n – 1 modulo n in some order.

Thus the rth column contains exactly as many integers relatively prime to n as the number of integers 0, 1, 2, …., n – 1 which are relatively prime to n. Thus there are exactly $\phi(n)$ integers in the r^{th} column that are relatively prime to n. Therefore, each of the $\phi(m)$ columns contain $\phi(n)$ integers which are relatively prime to n. Hence, there are $\phi(m)\phi(n)$ integers which are relatively prime to both m and n

Hence, $\phi(mn)=\phi(m)\phi(n)$ .Thus, ϕ is multiplicative function.

Theorem. If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then

$$\phi(n) = \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\ldots \left(p_r^{k_r} - p_r^{k_r-1}\right)$$

$$= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots \left(1-\frac{1}{p_r}\right).$$

Proof. We shall prove this theorem by induction on r. For $r = 1,$ we have $n = p_1^{k_1}$ and

$$\phi(n) = \phi\left(p_1^{k_1}\right) = p_1^{k_1} - p_1^{k_1-1} = p_1^{k_1}\left(1-\frac{1}{p_1}\right) = n\left(1-\frac{1}{p_1}\right).$$

Let the result hold for $r = s$.

Consider,

$$n = p_1^{k_1}\ldots\ p_s^{k_s} p_{s+1}^{k_{s+1}}.$$

Since $\gcd(p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}, p_{s+1}^{k_{s+1}}) = 1$, we can write

$$\phi(n) = \phi\left(p_1^{k_1}\ldots\ p_s^{k_s} p_{s+1}^{k_{s+1}}\right)$$

$$= \phi\left(p_1^{k_1}\ldots\ p_s^{k_s}\right)\phi\left(p_{s+1}^{k_{s+1}}\right) \qquad \text{(Since } \phi \text{ is multiplicative)}$$

$$= \left(p_1^{k_1} - p_1^{k_1-1}\right)\ldots \left(p_s^{k_s} - p_s^{k_s-1}\right)\left(p_{s+1}^{k_{s+1}} - p_{s+1}^{k_{s+1}-1}\right).$$

Hence, the result holds for $r = s+1$ whenever it holds for $r = s$. Therefore by principle of induction the result holds for any r.

e.g. Let n = 360 then $n = 2^3 3^2.5$, so that

$$\phi(360) = 360\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 96.$$

Theorem. For $n > 2, \phi(n)$ is an even integer .

Proof. Suppose n is a power of 2. Let $n = 2^k$, for some positive integer $k > 1$.

Then, $\phi(n) = \phi\left(2^k\right) = 2^k\left(1-\frac{1}{2}\right) = 2^{k-1}$ which is even.

Suppose n is not power of 2 an odd integer. Then there is an odd prime p that divides n.

Let $n = p^k.m$ where $p \nmid m$ and $k \geq 1$. Since $p \nmid m, \gcd\left(p^k, m\right) = 1$ and as ϕ is multiplicative

$$\phi(n) = \phi(p^k m) = \phi(p^k)\phi(m) = p^{k-1}(p-1)\phi(m).$$

Since p is odd prime, p – 1 is even,so $\phi(n)$ is even.

6.2 Euler's Theorem

Lemma – Let $n > 1$ and $\gcd(a,n) = 1$.If $a_1, a_2, \ldots, a_{\phi(n)}$ are positive integers less than n and relatively prime to n, then $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Proof. Claim : No two integers aa_1, aa_2, ..., $aa_{\phi(n)}$ are congruent modulo n.

Let if possible $aa_i \equiv aa_j \pmod{n}$, $1 \le i < j \le \phi(n)$, then as $\gcd(a,n) = 1$, we have

$$a_i = a_j \pmod{n} \Rightarrow n \mid a_i - a_j$$

which is absurd.

Now, $\gcd(a_i,n) = 1$and $\gcd(a,n) = 1$, $1 \le i \le \phi(n)$ implies that $\gcd(aa_i,n) = 1$ for each $i = 1,2,\ldots,\phi(n)$. Thus for any fixed $1 \le i \le \phi(n)$, aa_i is congruent modulo n to unique integer b , $1 \le b < n$. Hence, $\gcd(b,n) = \gcd(aa_i,n) = 1$. Therefore, b must be one of $a_1, a_2, \ldots, a_{\phi(n)}$.

Theorem (Euler's Theorem). Let $n \ge 1$ and $\gcd(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. Without loss of generality we can take n > 1. Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. Then as $\gcd(a,n) = 1$, $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order .

Let $a'_1, a'_2, \ldots, a'_{\phi(n)}$ be a rearrangement of $a_1, a_2, \ldots, a_{\phi(n)}$ such that

$$aa_1 \equiv a'_1 \pmod{n}$$

$$aa_2 \equiv a'_2 \pmod{n}$$

$$\vdots$$

$$aa_{\phi(n)} \equiv a'_{\phi(n)} \pmod{n}$$

Thus, $(aa_1)(aa_2)\cdots(aa_{\phi(n)}) \equiv a'_1 a'_2 \cdots a'_{\phi(n)} \pmod{n}$, that is, $(aa_1)\ldots(aa_{\phi(n)})$

$\equiv a_1 a_2 \ldots a_{\phi(n)} \pmod{n}$.

Therefore, $a^{\phi(n)} a_1 a_2 \ldots a_{\phi(n)} \equiv a_1 a_2 \ldots a_{\phi(n)} \pmod{n}$.

Since each a_i is relatively prime to n for $i = 1,2,\ldots,\phi(n)$, we can write

$a^{\phi(n)} \equiv 1(\mathrm{mod}\, n)$.

Note. Note that, Euler's theorem is Euler's generalization of Fermat's theorem.

Corollary. If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1(\mathrm{mod}\, p)$.

Ex.1 Find last two digits in the decimal representation of 3^{256}.

Solution. We have to find smallest positive integer to which 3^{256} is congruent modulo 100.

Note that $\gcd(3,100)=1$ and $\phi(100)=100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=40.$ so that by Euler's theorem

$3^{\phi(100)} \equiv 1(\mathrm{mod}100)$ that is, $3^{40} \equiv 1(\mathrm{mod}100)$.

Thus, $3^{240} = \left(3^{40}\right)^6 \equiv 1(\mathrm{mod}100)$.

Now, $3^4 \equiv 81 \equiv (-19)(\mathrm{mod}100) \Rightarrow 3^8 \equiv \left(3^4\right)^2 \equiv (-19)^2 (\mathrm{mod}100) \Rightarrow 3^8 \equiv (-39)(\mathrm{mod}100)$.

Thus $3^{16} \equiv (-39)^2 \equiv 21(\mathrm{mod}100)$.

Therefore, $3^{256} = 3^{240} \cdot 3^{16} \equiv 1 \cdot 21(\mathrm{mod}100)$.

Hence, the last two digits in the decimal representation of 3^{256} are 21.

Ex.2.Using Euler's theorem, prove that , for any integer a , $a^{37} \equiv a(\mathrm{mod}1729)$.

Solution. Observe that $1729 = 7 \cdot 13 \cdot 19$. Let a be an integer such that, $\gcd(a,1729)=1$,then

$\gcd(a,7)=1, \gcd(a,13)=1, \gcd(a,19)=1$ and so

$a^6 \equiv 1(\mathrm{mod}\,7), a^{12} \equiv 1(\mathrm{mod}13), a^{18} \equiv 1(\mathrm{mod}19)$.

Thus, $a^{lcm(6,12,18)} \equiv 1(\mathrm{mod}\,7 \cdot 13 \cdot 19) \Rightarrow a^{36} \equiv 1(\mathrm{mod}1729) \Rightarrow a^{37} \equiv a(\mathrm{mod}1729)$.

However, if $1729 \mid a$, there is nothing to prove.

Ex.3. If m and n are relatively prime positive integers, then $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$

Hence deduce, $p^{q-1} + q^{p-1} \equiv 1(\mathrm{mod}\, pq)$ where p and q are distinct primes.

Solution. Since $\gcd(m,n)=1$ we have $m^{\phi(n)} \equiv 1(\mathrm{mod}\, m)$ and $n^{\phi(m)} \equiv 1(\mathrm{mod}\, n)$ also

$m^{\phi(n)} \equiv 0(\mathrm{mod}\, m); n^{\phi(m)} \equiv 0(\mathrm{mod}\, n)$.

Thus, $m^{\phi(n)} + n^{\phi(m)} \equiv 1(\mathrm{mod}\, n)$ and $m^{\phi(n)} + n^{\phi(m)} \equiv 1(\mathrm{mod}\, m)$.

Hence, $m^{\phi(n)} + n^{\phi(m)} \equiv 1(\mathrm{mod}\, mn)$.

For distinct primes p and q we have

$p^{\phi(q)} + q^{\phi(p)} \equiv 1(\mathrm{mod}\, pq)$.

That is, $p^{q-1} + q^{p-1} \equiv 1(\mathrm{mod}\, pq)$.

Exercises

1. Use Euler's theorem to establish the following

   a) For any integer a , $a^{13} \equiv a(\mathrm{mod}\, 2730)$

   b) For any integer a , $a^{33} \equiv a(\mathrm{mod}\, 4080)$.

2. Find the unit's digit of 3^{100} using Euler's theorem.(Ans. 1)

6.3 Some properties of the Phi – function :

Theorem. (Gauss) For each positive integer $n \geq 1$, $n = \sum_{d|n} \phi(d)$

The sum being extended over all positive divisors of n.

Proof. The integers between 1 and n can be separated into classes as follows:

If d is a divisor of n we put the integer m in the class S_d provided $\gcd(m,n) = d$.

In symbols, $S_d = \{m : \gcd(m,n) = d; 1 \leq m \leq n\}$.

Since $\gcd(m,n) = d$, we have, $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

Therefore, number of positive integers in S_d is precisely $\phi\left(\frac{n}{d}\right)$.

Further, each integer between 1 and n belongs to precisely one S_d .

Therefore,

$$n = \sum_{d|n} |S_d| = \sum_{d|n} \phi\left(\frac{n}{d}\right).$$

But as 'd' runs over all the positive divisors of n, so does n/d, hence,we can write

$$n = \sum_{d|n} \phi(d).$$

e.g. Let n=10, the integers relatively prime to 10 are 1,3,7,9 and divisors of 10 are 1,2,5,10. Consider

$S_1 = \{1,3,7,9\}, S_2 = \{2,4,6,8\}, S_5 = \{5\}, S_{10} = \{10\}$ and $\phi(10) = 4, \phi(5) = 4, \phi(2) = 1, \phi(1) = 1$.

Observe that $\phi(10) = \phi(10/1) = |S_1| = 4, \phi(5) = \phi(10/2) = |S_2| = 4, \phi(2) = \phi(10/5) = |S_5| = 1,$

$\phi(1) = \phi(10/10) = |S_{10}| = 1$. Therefore,

$$\sum_{d|10} \phi(d) = \phi(1) + \phi(2) + \phi(5) + \phi(10) = 1 + 1 + 4 + 4 = 10.$$

Lemma. For integers *a, n*, gcd(*a, n*) = 1 if and only of $\gcd(n-a, n) = 1$.

Proof. Suppose $\gcd(a, n) = 1$, and $d = \gcd(n-a, n) \Rightarrow d \mid n-a, d \mid n$, hence, $d \mid n, d \mid n-(n-a) = a \Rightarrow d \le \gcd(a, n) = 1 \Rightarrow d = 1$. That is, $\gcd(n-a, n) = 1$. On the other hand, suppose $\gcd(n-a, n) = 1$ and $d = \gcd(a, n)$, then $d \mid a, d \mid n \Rightarrow d \mid n-a, d \mid n \Rightarrow d \le \gcd(n-a, n) = 1 \Rightarrow d = 1$. Thus $\gcd(a, n) = 1$.

Let us fix *n* = 15, then the integers relatively prime to 15 are 1, 2, 4, 7, 8, 11, 13, 14.

Then $15-1 = 14, 15-2 = 13, 15-4 = 11, 15-7 = 8, 15-8 = 7, 15-11 = 4, 15-13 = 2, 15-14 = 1$ are also relatively prime to 15 and is indeed a rearrangement of all integers relatively to 15. Thus we can write

$$1+2+4+7+8+11+13+14 =$$

$$(15-1)+(15-2)+(15-4)+(15-7)+(15-8)+(15-11)+(15-13)+(15-14)$$

Thus

$$1+2+4+7+8+11+13+14 = 8\times 15 - (1+2+4+7+8+11+13+14)$$

That is

$$2(1+2+4+7+8+11+13+14) = 8\times 15,$$

Or

$$1+2+4+7+8+11+13+14 = \frac{\phi(15)\times 15}{2}.$$

Thus, we have

Theorem. For $n > 1$, the sum of the positive integers less than n and relatively prime to n is $\frac{1}{2} n\phi(n)$.

Proof. Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. Since, $\gcd(a, n) = 1$ if and only if $\gcd(a-n, n) = 1$, the numbers $n-a_1, n-a_2, \ldots, n-a_{\phi(n)}$ are equal in some order to $a_1, a_2, \ldots, a_{\phi(n)}$. Thus

$$a_1 + a_2 + \cdots + a_{\phi(n)} = (n-a_1) + (n-a_2) + \cdots + (n-a_{\phi(n)})$$

$$= n\phi(n) - (a_1 + a_2 + \cdots + a_{\phi(n)}).$$

Hence, $2\left(a_1 + a + \cdots + a_{\phi(n)}\right) = n\phi(n)$ and the result follows.

Theorem. For any integer n $\phi(n) = n\sum_{d|n} \frac{\mu(d)}{d}$.

Proof. We know

$F(n) = n = \sum_{d|n} \phi(d)$.

By inversion formula, we obtain

$$\phi(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} \mu(d) \frac{n}{d}$$

$$= \sum_{d|n} n \frac{\mu(d)}{d}$$

$$= n\sum_{d|n} \frac{\mu(d)}{d}.$$

Let us illustrate this for $n = 10$,

$$10\sum_{d|n} \frac{\mu(d)}{d} = 10\left[\mu(1) + \frac{\mu(2)}{2} + \frac{\mu(5)}{5} + \frac{\mu(10)}{10}\right]$$

$$= 10\left[1 + \frac{(-1)}{2} + \frac{(-1)}{5} + \frac{(-1)^2}{10}\right]$$

$$= 10\left[1 - \frac{1}{2} - \frac{1}{5} + \frac{1}{10}\right]$$

$$= 10\frac{2}{5} = 4 = \phi(10).$$

❑❑❑

Unit-7
Primitive Roots and Indices

7.1 Let us begin with the definition of order of an integer modulo n.

Definition. Let $n > 1$ and a be an integer such that $\gcd(a,n) = 1$. Then the smallest positive integer k such that $a^k \equiv 1 (\mathrm{mod}\, n)$ is called order of a modulo n.

e.g. – 1) Let $a = 2$ and $n = 5$. Here $2^4 \equiv 1 (\mathrm{mod}\, 5)$, then order of 2 modulo 5 is 4.

2) Let $a = 3$ and $n = 5$. Here $3^4 \equiv 1 (\mathrm{mod}\, 5)$, then order of 3 modulo 5 is 4.

3) Let $a = 2$ and $n = 7$. Here $2^3 \equiv 1 (\mathrm{mod}\, 7)$, then order of 2 modulo 7 is 2.

Notes. 1. If $a \equiv b (\mathrm{mod}\, n)$ then order of a modulo n is same as order of b modulo n.

2. If $\gcd(a,n) > 1$ then $ax \equiv 1 (\mathrm{mod}\, n)$ has no solution. Then we can not talk about order a modulo n. Therefore, whenever we talk order of a modulo n it is assumed that $\gcd(a,n) = 1$.

Theorem – Let the integer a have order k modulo n, then $a^h \equiv 1 (\mathrm{mod} n)$ if and only if $k \mid h$ in particular $k \mid \phi(n)$.

Proof. Let h be any positive integer such that $a^h \equiv 1 (\mathrm{mod}\, n)$.

Since k is order of a modulo n we have $a^k \equiv 1 (\mathrm{mod}\, n)$.

By division algorithm there exist integers q and r such that $h = kq + r$ where $0 \le r < k$.

Hence, $a^h = a^{qk+r} = (a^k)^q a^r \equiv (1)^q a^r \equiv a^r (\mathrm{mod}\, n)$. Thus $a^r \equiv a^h (\mathrm{mod}\, n)$ this together with $a^h \equiv 1 (\mathrm{mod}\, n)$ gives us $a^r \equiv 1 (\mathrm{mod}\, n)$ .If $0 < r < k$, minimality of k is contradicted. Hence, $r = 0$. Thus $h = kq$ or $k \mid h$.

Conversely, if $k \mid h$ then there is an integer q such that $kq = h$ and

$a^k \equiv 1 (\mathrm{mod}\, n) \Rightarrow (a^k)^q \equiv 1^q (\mathrm{mod}\, n) \Rightarrow a^h = a^{kq} \equiv 1 (\mathrm{mod}\, n)$.

Since $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$ by Euler's theorem, we have, $k \mid \phi(n)$.

Theorem. If the integer a has order k modulo n then $a^i \equiv a^j (\mathrm{mod}\, n)$ iff $i \equiv j (\mathrm{mod}\, k)$.

Proof. With no loss of generality we can take $i > j$ Since $a^i \equiv a^j \pmod{n}$ and $\gcd(a,n)=1$ we have, $a^{i-j} \equiv 1 \pmod{n}$.

Since a has order k modulo n, $k \mid i-j$ i.e. $i \equiv j \pmod{k}$.

Conversely, if $i \equiv j \pmod{k}$ then $k \mid i-j$ therefore $i = j + kq$ for some integer q. Then,

$a^i = a^{j+qk} = a^j \left(a^k\right)^q \equiv a^j \cdot 1 \pmod{n} \Rightarrow a^i \equiv a^j \pmod{n}$.

Thus, $a^i \equiv a^j \pmod{n}$.

Corollary. If a has order k modulo n then integers $a, a^2, \ldots, a^k$ are incongruent modulo n.

Proof. Let if possible $a^i \equiv a^j \pmod{n}$ with $1 \le j < i \le k$ then $i \equiv j \pmod{k}$, that is, $k \mid i-j$ which is absurd.

Theorem. If the integer a has order k modulo n and h>0 then a^h has order $k / \gcd(h,k)$ modulo n.

Proof. Let $d = \gcd(h,k)$ then d|h and d|k . Therefore, there exist integers h_1 and k_1 such that $dh_1 = h$ and $dk_1 = k$ with $\gcd(h_1,k_1)=1$.

Consider, $\left(a^h\right)^{k_1} = a^{hk_1} = a^{(h_1 d)(k/d)} = a^{h_1 k} = \left(a^k\right)^{h_1} \equiv 1^{h_1} \equiv 1 \pmod{n}$.

Thus, if r is the order a^h modulo n, then $r \mid k_1$.

On the other hand we have,

$a^{hr} = (a^h)^r \equiv 1 \pmod{n}$

$\left(a^h\right)^r = a^{hr} \equiv 1 \pmod{n}$.

Since the integer a has order k modulo n, $a^k \equiv 1 \pmod{n}$. Therefore, we have $k \mid hr$.

Hence, $k \mid hr \Rightarrow k_1 d \mid dh_1 r \Rightarrow k_1 \mid h_1 r$ .Since $\gcd(h_1,k_1)=1$ by Euclid's lemma $k_1 \mid r$.

Thus $k_1 \mid r$ Therefore, $r = k_1 = k/d = k/\gcd(h,k)$.

Corollary. Let a have order k modulo n. Then a^h also has order k if and only if $\gcd(h,k)=1$.

Definition (Primitive Root). Let n > 1 and a be an integer such that $\gcd(a,n)=1$ Then a is primitive root of n if order of a modulo n is $\phi(n)$.

e.g. 1) 2 and 3 are primitive roots of 5

2) 3 and 5 are primitive root of 7.

Let us consider $n = 7$

Integer	1	2	3	4	5	6
Order	1	3	6	3	6	2

Now for $n = 11$

Integer	1	2	3	4	5	6	7	8	9	10
Order	1	10	5	5	5	10	10	10	5	2

Looking at the table, 3, 6 are primitive roots of 7 and 2, 6, 7, 8 are primitive roots of 11.

Ex.1 Show that if $F_n = 2^{2^n} + 1, (n > 1)$ is a prime then 2 is not a primitive root of F_n.

Solution. Consider

$$2^{2^{n+1}} - 1 = \left(2^{2^n}\right)^2 - 1$$

$$= \left(2^{2^n} + 1\right)\left(2^{2^n} - 1\right)$$

$$= F_n\left(2^{2^n} - 1\right)$$

$$\Rightarrow 2^{2^{n+1}} \equiv 1 \pmod{F_n}$$

Thus order of 2 modulo F_n can not exceed 2^{n+1}. Since F_n is prime

$$\phi(F_n) = F_n - 1 = 2^{2^n}$$

Since $2^{n+1} < 2^{2^n}, 2$ is not a primitive root of n.

Theorem. Let $\gcd(a, n) = 1$ and let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. If a is a primitive root of n, then a, a^2,..., $a^{\phi(n)}$ are congruent modulo n to a_1, a_2,..., $a_{\phi(n)}$ in some order.

Proof. Since $\gcd(a, n) = 1$, $a, a^2, \ldots, a^{\phi(n)}$ are relatively prime to n. It remains to show that $a, a^2, \ldots, a^{\phi(n)}$ are incongruent modulo n.

Let if possible, $a^i \equiv a^j \pmod{n}$, $\Rightarrow i \equiv j \pmod{\phi(n)}$

where $1 \le j < i \le \phi(n)$ then $\phi(n) \mid i - j$, which is impossible.

Now for fixed $k, 1 \le k \le \phi(n)$, there is a positive integer r, $r < n$ such that $a^k \equiv r \pmod{n}$ and

$\gcd(a^k, n) = \gcd(r, n) = 1$. So that r is positive integer less than n, relatively prime to n. Hence r must be one of $a_1, a_2, \ldots, a_{\phi(n)}$. Since $a_1, a_2, \ldots, a_{\phi(n)}$ are incongruent modulo n, $a, a^2, \ldots, a^{\phi(n)}$ are congruent to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Corollary. If n has a primitive root then it has exactly $\phi(\phi(n))$ of them.

Proof. Suppose that a is a primitive root of n. Then a must be congruent to one of $a_1, a_2, \ldots, a_{\phi(n)}$ where $a_1, a_2, \ldots, a_{\phi(n)}$ are positive integers less than n relatively prime to n.

We know that $a, a^2, \ldots, a^{\phi(n)}$ are congruent modulo n to $a_1, a_2, \ldots..a_{\phi(n)}$ in some order. Further number $a^k, 1 \le k \le \phi(n)$ has order $\phi(n)$ if $\gcd(k, \phi(n)) = 1$. Hence, there are exactly $\phi(\phi(n))$ primitive roots of n.

Ex.2. Find the order of the integers 2, 3 and 5 modulo 17.

Solution. Consider the factors $2, 4, 8, 16$ of $\phi(17) = 16$. Now $2^2 \not\equiv 1 \pmod{17}, 2^4 \not\equiv 1 \pmod{17}$ but $2^8 \equiv 1 \pmod{17}$ .Therefore, order of 2 modulo 17 is 8. Hence, 2 is not primitive root of 17.Next, $3^2 \not\equiv 1 \pmod{17}, 3^4 \not\equiv 1 \pmod{17}, 3^8 \not\equiv 1 \pmod{17}$ but $3^{16} \equiv 1 \pmod{17}$ .Therefore, order of 3 modulo 17 is $\phi(17) = 16$. Hence, 3 is a primitive root of 17. Further, $5^2 \not\equiv 1 \pmod{17}, 5^4 \not\equiv 1 \pmod{17}, 5^8 \not\equiv 1 \pmod{17}$ but $5^{16} \equiv 1 \pmod{17}$. Hence, 5 is a primitive root of 17.

Ex.3. Prove that $\phi(2^n - 1)$ is multiple of n for any n > 1.

Solution. Since, $2^n \equiv 1 \pmod{2^n - 1}$, therefore 2 has order n modulo $2^n - 1$.

Therefore, $n \mid \phi(2^n - 1)$

Ex.4. If p is a composite number such that $2^p - 1$ is prime then p is a pseudoprime.

Solution. Since $2^p \equiv 1 \pmod{2^p - 1}$ therefore 2 has order p modulo 2^{p-1} .

Therefore, $p \mid \phi(2^p - 1) = 2^p - 2$ .Hence, p is pseudoprime.

Ex.5. Assume that order of a modulo n is h and the order of b modulo n is k. Show that order of ab modulo n divides hk. In particular, if $\gcd(h, k) = 1$, then order of ab is hk.

Solution. Given that $a^h \equiv 1 \pmod{n}$ and $b^k \equiv 1 \pmod{n}$. Thus, $(ab)^{hk} \equiv 1 \pmod{n}$.

Thus, order of ab modulo n divides hk. Note that, $ab^{lcm(h,k)} \equiv 1 \pmod{n}$. Therefore, if $\gcd(h,k)=1$, then $lcm(h,k)=hk$ and hence, order of ab is hk.

Ex.6. The odd prime divisors of the integer n^2+1 are of the form $4k+1$

Solution. Let p be an odd prime divisor of n^2+1 then $n^2+1 \equiv 0 \pmod{p}$.

$\Rightarrow n^2 \equiv (-1) \pmod{p}$

$\Rightarrow n^4 \equiv 1 \pmod{p}$

$\Rightarrow 4 \mid \phi(p) = p-1$

$\Rightarrow p = 4k+1$.

Ex.7 The odd prime divisors of the integers (n^4+1) are of the form $8k+1$.

Solution. Let p be a prime divisors of n^4+1.Then

$n^4+1 \equiv 0 \pmod{P}$

$n^4 \equiv (-1) \pmod{P}$

$n^8 \equiv (-1)^2 \pmod{P}$

$n^8 \equiv 1 \pmod{P}$

$8 \mid \phi(p) = p-1$

$\Rightarrow p = 8k+1$.

Exercises

1. Find the order of the integers 2, 3 and 5
   a) modulo 19 b) modulo 23.
2. Find orders of all the positive integers less 13, which of them are primitive roots of 13.

7.2 Primitive Roots for Primes

Theorem. (Lagrange) If p is a prime and, $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ $(a_n \not\equiv 0 \pmod{p})$ is a polynomial of degree $n \geq 1$ with integral coefficients then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n incongruent solutions modulo p.

Proof. We shall prove this theorem by induction on n. Let n = 1 then $f(x) = a_1 x + a_0$.

Since $\gcd(a_1, p) = 1$ the linear congruence $a_1 x \equiv -a_0 \pmod{p}$ has a unique solution.

Hence, $a_1x + a_0 \equiv 0(\text{mod } p)$ has unique solution for n = 1.

Suppose that the result holds for n = k – 1. Let $f(x)$ be a polynomial of degree k.

If $f(x) \equiv 0(\text{mod } p)$ has no solution then there is nothing to prove.

Let $f(x) \equiv 0(\text{mod } p)$ have a solution a . By division algorithm we have
$f(x) = (x-a)g(x) + r,$ where r is constant. i.e. r is an integer and $\deg(g(x)) = k-1$.

Since a is a solution of $f(x) \equiv 0(\text{mod } p)$,we have $f(a) \equiv 0(\text{mod } p)$.

Hence , $0 \equiv f(a) = (a-a)g(a) + r \equiv r(\text{mod } p)$

Thus, $r \equiv 0(\text{mod } p)$.

Hence, $f(x) \equiv (x-a)g(x)(\text{mod } p)$.

Let b be any other solution of $f(x) \equiv 0(\text{mod } p)$ other than a .

Then, $0 \equiv f(b) \equiv (b-a)g(b)(\text{mod } p)$.

Since, $(b-a) \not\equiv 0(\text{mod } p)$, we have $g(b) \equiv 0(\text{mod } p)$.

Thus any solutions of $f(x) \equiv 0(\text{mod } p)$ other than a is a solution of $g(x) \equiv 0(\text{mod } p)$.

Since $g(x)$ is of degree $k-1, g(x) \equiv 0(\text{mod } p)$ can have at most k – 1 zeros incongruent modulo p.

Thus $f(x) \equiv 0(\text{mod } p)$ can have at most $(k-1)+1 = k$ incongruent solutions modulo p.

Hence, the result follows by principle of induction.

Corollary. If p is a prime number and $d \mid p-1$, then the congruence $x^d - 1 \equiv 0(\text{mod } p)$ has exactly d solutions.

Proof. Since $d \mid p-1$ we have $dk = p-1$ where k is an integer then

$x^{p-1} - 1 = x^{dk} - 1$

$= \left(x^d\right)^k - 1$

$= \left(x^d - 1\right)\left(\left(x^d\right)^{k-1} + ... + 1\right).$

Let $f(x) = (x^d)^{k-1} + (x^d)^{k-2} + ... + 1.$

Note that, $\deg(f(x)) = d(k-1) = p-1-d$ and that $f(x)$ has integral coefficients.

By Lagrange's theorem, $f(x) \equiv 0(\text{mod } p)$ can have most p – 1 – d solutions incongruent modulo p.

By Fermat's Theorem $x^{p-1} \equiv 1 (\text{mod } p)$ has precisely p – 1 solutions incongruent modulo p, namely the integers $1, 2, \ldots, p-1$.

Observe that $0 \equiv a^{p-1} - 1 \equiv \left(a^d - 1\right) f(a) (\text{mod } p)$ with $p \nmid f(a)$ implies that $p \mid a^d - 1$.

Hence, any solution $x \equiv a (\text{mod } p)$ of $x^{p-1} - 1 \equiv 0 (\text{mod } p)$ other than the solution of $f(x) \equiv 0 (\text{mod } p)$ must satisfy $x^d - 1 \equiv 0 (\text{mod } p)$. Thus $x^d - 1 \equiv 0 (\text{mod } p)$ must have at least $p - 1 - (p - 1 - d) = d$ solutions. Since $x^d - 1 \equiv 0 (\text{mod } p)$ can have at most d solutions, it must have exactly d solutions.

Using this corollary we can prove Wilsons theorem

Theorem. (Wilson's theorem)

If p is prime, $(p-1)! \equiv -1 (\text{mod } p)$.

Proof. Consider $f(x) = (x-1)(x-2)\ldots \left(x - (p-1)\right) - \left(x^{p-1} - 1\right)$

$= a_{p-2} x^{p-2} + a_{p-3} x^{p-3} + \ldots + a_1 x + a_0$

where , $a_0, a_1, \ldots, a_{p-2}$ are integers and that degree of $f(x)$ is p – 2 .

We know that $x^{p-1} - 1 \equiv 0 (\text{mod } p)$ has exactly (p – 1) incongruent solutions modulo p. By construction each of 1 to p – 1 is a solution of $f(x) \equiv 0 (\text{mod } p)$ and that 1, 2,…, (p – 1) are incongruent modulo p.

Since degree of $f(x)$ is p – 2 by Lagrange's theorem $f(x) \equiv 0 (\text{mod } p)$ can have at most p – 2 incongruent solutions modulo p.

This is possible only if

$a_{p-2} \equiv a_{p-3} \equiv \cdots \equiv a_1 \equiv a_0 \equiv 0 (\text{mod } p)$.

Thus $(x-1)(x-2)\ldots(x-(p-1)) - (x^{p-1} - 1) \equiv 0 (\text{mod } p)$ holds for any integer x .

Therefore, for $x = 0,$ we obtain

$(-1)(-2)\cdots(-(p-1)) \equiv -1 (\text{mod } p) \Rightarrow (-1)^{p-1} (p-1)! \equiv -1 (\text{mod } p)$.

If p is odd prime then p – 1 is even and for p=2, we have $-1 + 1 \equiv 0 (\text{mod } p)$. Hence,

$(p-1)! \equiv -1 (\text{mod } p)$.

This proves Wilson's theorem .

Theorem. If p is a prime number and $d \mid p-1$, then there are exactly $\phi(d)$ incongruent integers having order d modulo p.

Proof. Suppose $d \mid p-1$. Let $\psi(d)$ denote the number of integers k, $1 \le k \le p-1$ that have order d modulo p. Since each integer $1, 2, \ldots, p-1$ has order d, for some $d \mid (p-1)$.

Thus, $p-1 = \sum_{d \mid p-1} \psi(d)$.

By Gauss' theorem

$p-1 = \sum_{d \mid p-1} \phi(d)$.

Thus $\sum_{d \mid p-1} \psi(d) = \sum_{d \mid p-1} \phi(d)$ ------ (1)

Claim - $\psi(d) \le \phi(d)$ for each divisor d of p – 1 .

Let d be an arbitrary divisor of p – 1, then either $\psi(d) = 0$, or $\psi(d) > 0$, If $\psi(d) = 0$, then $\psi(d) < \phi(d)$ holds trivially.

Suppose $\psi(d) > 0$ then there is an integer a such that order of a modulo p is d with $\gcd(a, p) = 1$.

Further, $a, a^2, \ldots, a^d$ are incongruent modulo p and that each of them satisfies the polynomial congruence

$$x^d - 1 \equiv 0 \pmod{p} \qquad (2)$$

for $(a^k)^d = (a^d)^k \equiv 1^k \equiv 1 \pmod{p}$ for $k = 1, 2, \ldots, d$.

Therefore, by corollary to Lagrange's theorem, there can be no other solution of Equation(2).

Thus any integer having order d modulo p must be congruent to one of $a, a^2, \ldots\ldots, a^d$ modulo p. But only $\phi(d)$ integer amongst $a, a^2, \ldots\ldots, a^d$ can have order d modulo p. In other words a^k has order d modulo p if and only if $\gcd(k, d) = 1$. Thus $\psi(d) = \phi(d)$ that is, the number of integers having order d modulo p is equal to $\phi(d)$. Thus $\psi(d) \le \phi(d)$.

In view of Equation (1) we must have $\phi(d) = \psi(d)$ otherwise L.H.S. of (1) would be less than R.H.S. of (1) which is not possible. Hence, the result.

Corollary. If p is a prime, then there are exactly $\phi(p-1)$ incongruent primitive roots.

Proof. Any primitive root of p has order $\phi(p) = p-1$. Therefore, number of primitive roots of p is exactly $\phi(p-1)$.

e.g. Let p = 13 then the divisors of p – 1 = 13 – 1 = 12 are 1, 2, 3, 4, 6,12.

Order of 1 modulo 13 is 1

Order of 2, 6, 7, 11 is 12

Order of 3, 9 is 3

Order of 5, 8 is 4

Order of 4, 10 is 6

Order of 12 is 2

It is interesting to note that, the number of incongruent solutions of $x^6 \equiv 1 \pmod{13}$ is indeed the sum of integers of order 6, 3, 2 and 1. Thus the number of incongruent solutions of $x^6 \equiv 1 \pmod{13}$ is 2 + 2 + 1 + 1 = 6, namely 4, 10 of order 6; 3, 9 of order 3; 12 of order 2; 1 of order 1.

Ex.1. If p is a prime of the form 4k + 1, then the quadratic congruence $x^2 \equiv -1 \pmod{p}$,admits a solution.

Solution. Since $4 \mid p-1 = \phi(p)$ there is an element a of the order 4, that is $a^4 \equiv 1 \pmod{4}$. Thus, $(a^2+1)(a^2-1) \equiv 0 \pmod{p} \Rightarrow a^2 \equiv 1 \pmod{p}$ or $a^2 \equiv -1 \pmod{p}$.

Since order of a modulo p is 4, $a^2 \equiv 1 \pmod{p}$ is not possible. Hence $a^2 \equiv -1 \pmod{p}$ so that $x^2 \equiv -1 \pmod{p}$ has a solution.

Ex.2. If p is an odd prime, prove that the only incongruent solutions of $x^2 \equiv 1 \pmod{p}$ are 1 and p – 1

Solution. We know that $x^2 \equiv 1 \pmod{p}$ has 2 incongruent solutions modulo p.

Since 1 and 1 – p are already solutions of $x^2 \equiv 1 \pmod{p}$, they are the only two incongruent solutions of $x^2 \equiv 1 \pmod{p}$.

Ex.3. If p is an odd prime, prove that congruence $x^{p-2} + x^{p-3} + \cdots + x + 1 \equiv 0 \pmod{p}$

has exactly p – 2 incongruent solutions and they are the integers $2, 3, \ldots, p-1$.

Solution. We know $x^{p-1} - 1 \equiv 0 \pmod{p}$ has solution $2, 3, \ldots, p-1$.

Since $x^{p-1} - 1 \equiv (x-1)\left(x^{P-2} + \ldots + x + 1\right)$ and $x \equiv 1 \pmod{p}$ has solution 1.

Therefore, $x^{p-2} + x^{p-3} + \cdots + x + 1 \equiv 0 \pmod{p}$ has solutions $2, 3, \ldots, p-1$.

Not let us recall the results :

Let gcd(a, n) =1 and let $a_1, a_2, ..., a_{\phi(n)}$ be the positive integers less than n and relatively prime to n. If a is a primitive root n, then $a, a^2, ..., a^{\phi(n)}$ are congruent modulo n to $a_1, a_2, ..., a_{\phi(n)}$ in some order.

And

Let a have order k modulo n. Then a^k also has order k if and only if gcd(h, k) = 1.

The later can be rephrased as

Let a be a primitive root then a have order $\phi(n)$ modulo n. Then a^h also has order $\phi(n)$ if and only if $\gcd(h, \phi(n)) = 1$. This is equivalent to the statement.

An integer a^h is a primitive root of n if and only if $\gcd(h, \phi(n)) = 1$.

Thus if, we can begin with the smallest primitive root a of an integer n (if exists), then we can use it to find other primitive roots. Interestingly, we need not have to search too far for smallest primitive root as most primes have either 2 or 3 as their primitive root. Let us consider p = 23, by trial and error we can ensure that 5 is the smallest primitive root. Now we can begin with this primitive root and compute others. In view of above result 5^h is a primitive root if $\gcd(h, \phi(23)) = \gcd(h, 22) = 1$ that is, h = 1, 3, 5, 7, 9, 13, 15, 17, 19, 21 and so $5, 5^3, 5^5, 5^7, 5^9, 5^{13}, 5^{15}, 5^{17}, 5^{19}, 5^{21}$ are primitive roots. Consider,

$5^3 = 5 \times 25 \equiv 5 \times 2 \equiv 10 \pmod{23}, 5^5 = 5^3 \cdot 5^2 \equiv 10 \times 25 \equiv 10 \times 2 \equiv 20 \pmod{23},$

$5^7 = 5^5 \cdot 5^2 \equiv 20 \times 2 \equiv 17 \pmod{23},\ 5^9 = 5^7 \cdot 5^2 \equiv 17 \times 2 \equiv 11 \pmod{23},$

$5^{11} \equiv 11 \times 25 \equiv 11 \times 2 \equiv 22 \pmod{23},\ 5^{13} = 22 \times 25 \equiv 22 \times 2 \equiv 21 \pmod{23},$

$5^{15} \equiv 21 \times 25 \equiv 21 \times 2 \equiv 19 \pmod{23},\ 5^{17} = 19 \times 25 \equiv 19 \times 2 \equiv 15 \pmod{23},$

$5^{19} \equiv 15 \times 25 \equiv 15 \times 2 \equiv 7 \pmod{23},\ 5^{21} = 7 \times 25 \equiv 7 \times 2 \equiv 14 \pmod{23}.$

Thus the primitive roots are 5, 7, 10, 11, 14, 15, 17, 19, 20, 21. Observe that the number of primitive roots incongruent modulo 23 is $\phi(\phi(23)) = \phi(22) = \phi(11) = 10$. Here we have also calculated 5^{11} for our calculation purpose.

Note that there are 5 pairs $\{5, 5^{21}\}, \{5^3, 5^{19}\}, \{5^5, 5^{17}\}, \{5^7, 5^{15}\}, \{5^9, 5^{13}\}$ such that $rr' \equiv 1 \pmod{23}$.

This can also be used to find integers of given order from smallest primitive root. Recall the result :

Let a have order k modulo n. Then a^h also has order $\frac{k}{\gcd(h,k)}$.

Thus, if a is a primitive root, then order of a is $\phi(n)$ so that a^h has order $\frac{\phi(n)}{\gcd(h,\phi(n))}$.

We can use this result to find integers of a given order from a primitive root.

Let us consider p = 13 and it's primitive root 2. Let us find integers of order 6. Here, $\phi(13)=12$, so the integers of order 6 are those integers 2^h with

$$6=\frac{12}{\gcd(h,12)}\Rightarrow \gcd(h,12)=2\Rightarrow h=2,10.$$

Thus 2^2, 2^{10} are integers of order 6. Now, $2^2=4$, $2^{10}=1024\equiv 10(\mathrm{mod}\,13)$. Therefore, 4 and 10 are integers of order 6.

Let us discuss how to find the number of integers of a given order k modulo n.

Let n be an integer having primitive root a, then $a,a^2,...,a^{\phi(n)}$ are congruent to $a_1,a_2,...,a_{\phi(n)}$ in some order. Further, if a have order k modulo n. Then a^h also has order $\frac{k}{\gcd(h,k)}$.

Thus if, a is a primitive root, then order of a is $\phi(n)$ so that a^h has order $\frac{\phi(n)}{\gcd(h,\phi(n))}$. Thus integers of order k are those a^h for which $\frac{\phi(n)}{\gcd(h,\phi(n))}=k$ that is, we have to find h such that $\frac{\phi(n)}{k}=\gcd(h,\phi(n))$. Let us consider p = 43. Here, $\phi(43)=42$, so that there are integers of order 1, 2, 3, 6, 7, 14, 21, 42. First we shall find a primitive root of 43. Let us start with 2. We have

$2^5\equiv 32\equiv -11(\mathrm{mod}\,43), 2^6\equiv 21(\mathrm{mod}\,43), 2^7\equiv -1(\mathrm{mod}\,43)$ and

$2^{14}=(2^7)^2\equiv(-1)^2\equiv 1(\mathrm{mod}\,43)$.

Thus 2 is not a primitive root. Consider

$3^4=81\equiv -5(\mathrm{mod}\,43), 3^6=3^4\cdot 3^2\equiv(-5)(9)\equiv -2(\mathrm{mod}\,43), 3^7\equiv -6(\mathrm{mod}\,43),$

$3^{14}\equiv 36\equiv -7(\mathrm{mod}\,43)$

Thus $3^{21}=3^{14}\cdot 3^7\equiv(-7)(-6)\equiv -1(\mathrm{mod}\,43)$. Hence, 3 is primitive root of 43.

Power of 3	No. cong. mod 43	Power of 3	No. cong. mod 43	Power of 3	No. cong. mod 43
1	03	15	22	29	18
2	09	16	23	30	11
3	27	17	26	31	33
4	38	18	35	32	13
5	28	19	19	33	39
6	41	20	14	34	31
7	37	21	42	35	07
8	25	22	40	36	21
9	32	23	34	37	20
10	10	24	16	38	17
11	30	25	05	39	08
12	04	26	15	40	24
13	12	27	02	41	29
14	36	28	06	42	01

Table 1

Clearly, only element of order 1 is 1,

Now integers of order 2 are those 3^h for which $\frac{42}{2} = \gcd(h,42) \Rightarrow \gcd(h,42) = 21 \Rightarrow h = 21$.

Thus there is only one integer of order 2, namely $3^{21} \equiv -1 \equiv 42 \pmod{43}$, that is 42.

Next integers of order 3 are those 3^h for which $\frac{42}{3} = \gcd(h,42) \Rightarrow \gcd(h,42) = 14 \Rightarrow h = 14,28$.

Thus there two integer of order 3, namely 6 and 36.

Now integers of order 6 are those 3^h for which $\frac{42}{6} = \gcd(h,42) \Rightarrow \gcd(h,42) = 7 \Rightarrow h = 7,35$.

Thus there are 3 integers of order 6, namely 37, 7.

Further, integers of order 7 are those 3^h for which

$\frac{42}{7} = \gcd(h,42) \Rightarrow \gcd(h,42) = 6 \Rightarrow h = 6,12,18,24,30,36$. Thus there are 6 integers of order 7 namely 41, 4, 35, 16, 11, 21.

Further, integers of order 14 are those 3^h for which

$\frac{42}{21} = \gcd(h,42) \Rightarrow \gcd(h,42) = 2 \Rightarrow h = 2,4,8,10,16,20,22,26,32,34,38,40$. Thus there are 12 integers of order 21, namely 9, 38, 25, 10, 23, 14, 40, 15, 13, 31, 17, 24.

Finally, integers of order 42, that is, primitive roots are those 3^h for which

$\frac{42}{42} = \gcd(h,42) \Rightarrow \gcd(h,42) = 1 \Rightarrow h = 1,5,11,13,17,19,23,25,29,31,37,41$. Thus there are 12 primitive roots for 43, namely 3, 28, 30, 12, 26, 19, 34, 5, 18, 33, 20, 29.

Note that there are 6 pairs $\{2,2^{41}\},\{2^5,2^{37}\},\{2^{11},2^{30}\},\{2^{13},2^{29}\},\{2^{17},2^{28}\},\{2^{19},2^{23}\}$ such that $rr' \equiv 1 \pmod{43}$.

Let us put it in tabular form.

Sr. No.	Order	Integers	No. of integers
1	1	1	01
2	2	42	01
3	3	6, 36	02
4	6	7, 37	02
5	7	4, 11, 16, 21, 35, 41	06
6	14	2, 8, 22, 27, 32, 39	06
7	21	9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38	12
8	42	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34	12
		Total	42

Ex. Find all positive integers less than 61 having order 4 modulo 61.

Solution. Let us find smallest possible positive primitive root modulo 61. Let us begin with 2. Consider the nearest power of 2 to 61. Note that $\phi(61) = 60$ and divisors of 60 are 1, 2, 3, 4, 5, 6, 12, 15, 20, 30, 60. We have $2^8 \equiv 12 \pmod{61}, 2^{12} = 2^8 \cdot 2^4 \equiv 12 \cdot 16 \equiv 9 \pmod{61}$,

$2^{15} = 2^{12} \cdot 2^3 \equiv 9 \cdot 8 \equiv 11 \pmod{61}$ so $2^{20} = 2^{12} \cdot 2^8 \equiv 9 \cdot 3 \equiv 27 \pmod{61}$,

$2^{30} = (2^{15})^2 = (11)^2 = 121 \equiv -1 \pmod{61} \Rightarrow 2^{60} \equiv 1 \pmod{61}$.

Thus 2 is a primitive root. The positive integers less than 61 having order 4 are those 2^h for which $\frac{60}{4} = \gcd(h,60) \Rightarrow \gcd(h,60) = 15 \Rightarrow 15,45$. Thus $2^{15} \equiv 11 \pmod{61}$ and

$2^{45} = 2^{30} \cdot 2^{15} \equiv (-1)(11) \equiv 50 \pmod{61}$. Hence 11 and 50 are two integers of order 4 modulo 61.

Exercises :

1. Assuming that r is primitive root of the odd prime p, then prove that $r^{(p-1)/2} \equiv -1 \pmod{p}$.

2. Assuming that r is primitive root of the odd prime p, and r' is another primitive root of p, then prove that rr' is not a primitive root of p.

3. For a prime $p > 3$, prove that the primitive roots of p occur in incongruent pairs r, r' where $rr' \equiv 1 \pmod{p}$.

4. Let r be a primitive root of the odd prime p. Then prove the following :

   (a) If $p \equiv 1 \pmod{4}$, then $-r$ is primitive root of p.

   (b) If $p \equiv 3 \pmod{4}$, then $-r$ has order $(p-1)/2$ modulo p.

7.3 Composite Numbers having primitive root

Theorem. For $k \geq 3$ then integer 2^k has no primitive roots.

Proof. We shall prove this result by induction on k. However, we begin by showing that if a is an odd integer then, $a^{2^{k-2}} \equiv 1 \pmod{2^k}$. ..... (1)

For k = 3 this holds trivially because we know that square of an odd integer is of the form 8k + 1, i.e. if a is an odd integer $a^2 \equiv 1 \pmod{8}$.

Suppose k > 3.Let the result (1) holds true for k, that is, our induction hypothesis is $a^{2^{k-2}} \equiv 1 \pmod{2^k}$.

Therefore, $a^{2^{k-2}} = 1 + b2^k$, where b is an integer.

Consider

$$a^{2^{k-1}} = \left(a^{2^{k-2}}\right)^2 = \left(1 + b2^k\right)^2 = 1 + b2^{k+1} + b^2 2^{2k} = 1 + 2^{k+1}\left(b + b^2 2^{k-1}\right) \equiv 1 (\text{mod}\, 2^{k+1}) .$$

Thus, $a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$.

Therefore, (1) holds for k + 1 whenever it holds for k.

Hence, by principle of mathematical induction (1) holds for all $k \geq 3$.

Note that, the integers that are relatively prime to 2^k are the odd integers . This is to support the choice of a as odd integer in (1) and $\phi\left(2^k\right) = 2^k / 2 = 2^{k-1}$.

Thus $a^{2^{k-2}} = a^{\phi(2^k)/2} \equiv 1 (\mathrm{mod}\, 2^k)$

Thus 2^k has no primitive root because order of a modulo 2^k is less than or equal to $\frac{\phi(2^k)}{2}$.

Theorem. If $\gcd(m,n)=1$, where $m>2$ and $n>2$ then the integer mn has no primitive root.

Proof. Let be a an integer such that $\gcd(a,mn)=1$, that is, $\gcd(a,m)=1$ and $\gcd(a,n)=1$. Let $h = lcm(\phi(m),\phi(n))$ and $d = \gcd(\phi(m),\phi(n))$.

Since $\phi(m)$ and $\phi(n)$ are even integers, we have $d \geq 2$.

Hence, $h = \frac{\phi(m)\cdot\phi(n)}{d} \leq \frac{\phi(m)\cdot\phi(n)}{2} = \frac{\phi(mn)}{2}$.

By Euler's theorem, $a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$ so that $a^h = \left(a^{\phi(m)}\right)^{\phi(n)/d} \equiv 1^{\phi(n)/d} \equiv 1 (\mathrm{mod}\, m)$.

Similarly, $a^h \equiv 1 (\mathrm{mod}\, n)$. Since $\gcd(m,n)=1 \Rightarrow a^h \equiv 1 (\mathrm{mod}\, mn)$.

Thus, $a^{\phi(mn)/d} \equiv 1 (\mathrm{mod}\, mn)$. Thus, order of a modulo mn is less than or equal to $\frac{\phi(m)\cdot\phi(n)}{d} = \frac{\phi(mn)}{d} \leq \frac{\phi(mn)}{2} < \phi(mn)$.

Thus mn cannot have primitive roots.

Corollary. The integer n fails to have primitive root if either.

a) n is divisible by two odd primes or

b) n is of the form $n = 2^m \cdot p^k$,

where p is an odd prime and $m \geq 2$.

Proof. a) Let $n = pq$ where p and q are distinct odd primes. Hence $p>2$ and $q>2$ and above theorem applies.

b) Since p is odd prime we have $\gcd(2^m, p^k)=1$ and as $m \geq 2, 2^m \geq 2$ & $p^k > 2$. Therefore, above theorem applies.

Lemma. If p is an odd prime then there exists a primitive root r of p such that $r^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$.

Proof – Since p is an odd prime, it has a primitive root. Let r be one of the primitive roots of p. If $r^{p-1} \not\equiv 1 (\mathrm{mod}\, p^2)$ we are through.

Suppose $r^{p-1} \equiv 1 (\mathrm{mod}\, p^2)$ then let $r' = r + p$ and

consider, $(r')^{p-1} = (r+p)^{p-1} = r^{p-1} + (p-1)pr^{p-2} + \frac{(p-1)(p-2)}{2!}p^2r^{p-3} + \cdots$ to p terms.

Thus $(r')^{p-1} \equiv r^{p-1} + (p-1)pr^{p-2} \pmod{p^2}$.

Since, $r^{p-1} \equiv 1 \pmod{p^2}$, we have $(r')^{p-1} \equiv 1 - pr^{p-2} \pmod{p^2}$.

Since, r is a primitive root of $p, \gcd(r, p) = 1$, we obtain $p \nmid r^{p-2}$. Note that as r is a primitive root so does $r' = r + p$. Hence, $(r')^{p-1} \not\equiv 1 \pmod{p^2}$ proves the lemma.

Corollary. If p is an odd prime then p^2 has primitive root. In fact for a primitive root r of p either r or r + p (or both) is a primitive root of p^2.

Proof. Since p is an odd prime, p has a primitive root r. We know that either $r^{p-1} \not\equiv 1 \pmod{p^2}$ or $(r+p)^{p-1} \not\equiv 1 \pmod{p^2}$. Since, $\phi(p^2) = p(p-1)$ we must have

$r^{p-1} \equiv 1 \pmod{p^2}$ or $(r+p)^{p-1} \equiv 1 \pmod{p^2}$.

So that r or r + p is a primitive root of p^2. Note that if $r^{p-1} \not\equiv 1 \pmod{p^2}$, order of r modulo p^2 must be $\phi(p^2) = p(p-1)$ and similarly if $(r+p)^{p-1} \not\equiv 1 \pmod{p^2}$, order of r modulo p^2 must be $\phi(p^2) = p(p-1)$.

Ex. Find primitive roots of 25.

Solution. We know that 2, 3 are the primitive roots of 5. Note that there are $\phi(\phi(25)) = \phi(20) = 8$ primitive roots of 25. We know that if r is a primitive root of p then r or $r + p$ is a primitive root of p^2. Therefore, 2 or 7 and 3 or 8 are primitive rots of 25. Observe that $2^4 \not\equiv 1 \pmod{25}$ and $3^4 \not\equiv 1 \pmod{25}$. Therefore, 2 and 3 are primitive roots of 25. However, there are six more primitive roots of 25 which can be found by brute method or starting with 2 or 3. Now let us take 2. The primitive roots of 25 are those powers h or 2 such that gcd(h, 20) - 1. Thus h = 1, 3, 7, 9, 11, 13, 17, 19. Thus $2^3 = 8$, $2^7 = 128 \equiv 3 \pmod{25}$, $2^9 \equiv 12 \pmod{25}$, $2^{11} \equiv 23 \pmod{25}$, $2^{13} \equiv 17 \pmod{25}$, $2^{17} \equiv 22 \pmod{25}$, $2^{19} \equiv 13 \pmod{25}$. Thus the primitive roots are 2, 3, 8, 12, 13, 17, 22, 23.

Note. In the above example 2 and 3 are primitive root of 5 as well as 25. Further, 2 is primitive root but 2 + 5 = 7 is not where as both 3 and 3 + 5 = 8 are primitive roots. Note that $7^4 \equiv 1 \pmod{25}$. Thus $r^{p-1} \not\equiv 1 \pmod{p^2}$ guarantees that r is primitive root of p^2. Further 3, 8, 13, 23 are congruent modulo 5 and 2, 12, 17, 22 are congruent modulo 5. Also $7 \equiv -18 \pmod{25}$ implies $7^4 \equiv 18^4 \equiv 1 \pmod{25}$. The next result assures that if r is a primitive root of p with the property that $r^{p-1} \not\equiv 1 \pmod{p^2}$, then r is a primitive root of p^k for each positive integer $k \geq 2$.

Lemma. Let p be an odd prime and let r be a primitive root of p with the property that $r^{p-1} \not\equiv 1 \pmod{p^2}$. Then for each positive integer $k \geq 2$, $r^{p^{k-2}(p-1)} \not\equiv 1 (\text{mod } p^k)$

Proof. We shall prove this result by induction on k. For k = 2, the result holds trivially ,

Suppose that the result holds for k = n, i. e., $r^{p^{n-2}(p-1)} \not\equiv 1 (\text{mod } p^n)$.

Since $\gcd(r, p^{n-1}) = \gcd(r, p^n) = 1$, by Euler's theorem, we obtain

$r^{\phi\left(p^{n-1}\right)} \equiv 1 (\text{mod } p^{n-1}) \Rightarrow r^{p^{n-2}(p-1)} \equiv 1 (\text{mod } p^{n-1}) \Rightarrow 1 + ap^{n-1}$,

for some integer a such that, $p \nmid a$, otherwise, we would have, $r^{p^{n-2}(p-1)} \equiv 1 (\text{mod } p^n)$

which is absurd.

Now consider

$$r^{p^{n-1}(p-1)} = \left(r^{p^{n-2}(p-1)}\right)^p = \left(1 + ap^{k-1}\right)^p = 1 + p \cdot a \cdot p^{k-1} + \cdots .$$

Thus $r^{p^{n-1}(p-1)} \equiv 1 + ap^n (\text{mod } p^{n+1})$.

As $p \nmid a$, we have

$$r^{p^{n-1}(p-1)} \not\equiv 1 (\text{mod } p^{n+1}) .$$

Therefore the result holds true for any k by induction.

Theorem. If p is an odd prime and $k \geq 1$, then there exists a primitive root for p^k.

Proof. We know that, if p is an odd prime then there is a primitive root r modulo p such that $r^{p-1} \not\equiv 1 \pmod{p^2}$ and that for such an r, for each positive integer $k \geq 2$, $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$. Thus it is enough to find an r such that $r^{p-1} \not\equiv 1 \pmod{p^2}$ which serves as a primitive root for all powers of p.

Let n be the order of r modulo p^k, then n must divide $\phi\left(p^k\right) \mid p^{k-1}(p-1)$. Since n is the order of r modulo p^k, we have $r^n \equiv 1 \pmod{p^k}$ which implies that $r^n \equiv 1 \pmod{p}$. Therefore, $\phi(p) = p - 1 \mid n$. Thus n has the form $n = p^m(p-1)$, where $0 \leq m \leq k-1$. In case $m < k-1$, then we would have $n \mid p^{k-2}(p-1)$ and we get $r^{p^{k-2}(p-1)} \equiv 1 \pmod{p^k}$ which contradicts our assumption that $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$. Therefore, $n = p^{k-1}(p-1)$, that is, r is primitive root modulo p^k for any integer $k \geq 1$.

Finally we consider the case $2p^k$, where $k \geq 1$.

Corollary. There are primitive roots for $2p^k$ where p is an odd prime and $k \geq 1$.

Proof. We know that p^k with $k \geq 1$ has primitive root and let r be a primitive root for p^k. With no loss of generality, we may take r to be an odd integer, for if it were even then $r + p^k$ would be an odd primitive root for pk. Since r is odd, we have $\gcd\left(r, 2p^k\right) = 1$. Let n be the order of r modulo $2p^k$. Then r must divide $\phi\left(2p^k\right) = \phi(2)\phi\left(p^k\right) = \phi\left(p^k\right)$. Now $r^n \equiv 1\left(\bmod 2p^k\right) \Rightarrow r^n \equiv 1\left(\bmod p^k\right)$. Therefore, $\left(2p^k\right) | n$. On the other hand $n | \left(2p^k\right) = \phi\left(p^k\right)$. Thus $n = \phi\left(p^k\right)$ and consequently, r is primitive roots for $2p^k$.

Note that 1 primitive roots for 2, 3 is primitive root for 4 and thus we summarize.

Theorem. An integer $n > 1$ has a primitive root if and only if $n = 2, 4, p^k$ or $2p^k$.

Ex. Find four primitive roots of 26.

Solution. The integer 26 is of the form $26 = 2 \times 13$, that is of the form $2p$ and therefore, it has primitive roots. We begin by evaluating $\phi(26) = \phi(2 \cdot 13) = \phi(13) = 12$. Therefore, order of any integer relatively prime to 26 is divisor of 12. Note that the divisors of 12 are 1, 2, 3, 4, 6, 12. Further, there are exactly $\phi\left(\phi(13)\right) = \phi(12) = \phi(3)\phi(4) = 2 \cdot 2 = 4$ primitive roots. We can directly find the primitive roots or use the method of obtaining the primitive roots starting from the smallest primitive root. Let us do it directly. The integers relatively prime to 26 are 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25. Clearly, $3^3 = 27 \equiv 1(\bmod 26)$ so order of 3 is 3. Next, $5^2 \equiv 25 \equiv -1(\bmod 26) \Rightarrow 5^4 \equiv 1(\bmod 26)$ so that order of 5 is 4. Now $7^2 = 49 \equiv -3(\bmod 26)$, $7^3 = 7^2 \cdot 7 \equiv -3 \cdot 7 \equiv 5(\bmod 26)$ and

$7^6 \equiv 5^2 \equiv -1(\bmod 26) \Rightarrow 7^{12} \equiv 1(\bmod 26)$, that is, order of 7 is 12, hence 7 is primitive root. Clearly, $9^3 = \left(3^2\right)^3 = \left(3^3\right)^2 \equiv 1$, therefore, 9 is not a primitive root. Now, $11^2 = 121 \equiv 17(\bmod 26)$ and, $11^3 = 11^2 \cdot 11 \equiv 17 \cdot 11 \equiv (-9)11 \equiv 5(\bmod 6)$ thus $11^4 = \left(11^2\right)^2 \equiv (-9)(-9) \equiv 81 \equiv 3(\bmod 26)$. Next $11^6 = \left(11^3\right)^2 \equiv 5^2 \equiv -1(\bmod 26)$ therefore, order of 11 is 12, that is 11 is also a primitive root modulo 26. Consider, $15 \equiv -11(\bmod 26)$, $(15)^2 \equiv (-11)^2 \equiv (11)^2 \equiv (-9)(\bmod 26)$, further, $(15)^3 = (15)^2(15) \equiv (-9)(-11) \equiv -5(\bmod 26)$, $(15)^4 \equiv (15)^2 \equiv (-9)^2 \equiv 3(\bmod 26)$ and $(15)^6 \equiv \left(15^3\right)^2 \equiv (-5)^2 \equiv -1(\bmod 26)$, therefore, 15 is a primitive root for 26. Thus we have found 3 primitive roots and obvious guess for the fourth one is 19 as $19 \equiv -7(\bmod 26)$ and we are just required to verify that $(19)^3 \not\equiv 1(\bmod 26)$ and $(19)^3 \not\equiv -1(\bmod 26)$. For that it is enough to see that $(-7)^3 = (-7)^2(-7) = (7)^2(-7) \equiv (-3)(-7) \equiv -5(\bmod 26)$ so

$(-7)^3 \equiv (19)^3 \equiv -5 (\mathrm{mod}\, 26)$ Thus the fourth primitive root is 19. Thus once we verify that 7 and 11 are primitive roots obvious guess are 19 and 15.

Alternatively, once we obtain 7 as the smallest primitive root, the other three are 7^5, 7^7, 7^{11}. Consider $7^2 = 49 \equiv -3 (\mathrm{mod}\, 26)$, $7^3 = 7^2 \cdot 7 \equiv (-3) \cdot 7 \equiv 5 (\mathrm{mod}\, 26)$, $7^4 = (7^2)^2 \equiv (-3)^2 \equiv 9 (\mathrm{mod}\, 26)$ therefore, $7^5 = 7^2 \cdot 7^3 \equiv (-3) \cdot 5 \equiv 11 (\mathrm{mod}\, 26)$, $7^7 = 7^4 \cdot 7^3 \equiv 9 \cdot 5 \equiv 19 (\mathrm{mod}\, 26)$, and $7^{11} = (7^7)(7^4) \equiv 19 \cdot 9 \equiv (-7) 9 \equiv 15 (\mathrm{mod}\, 26)$. Thus the four primitive roots are 7, 11, 15, 19.

Let us find integers of order 6 modulo 26. Here, $\phi(26) = \phi(13) = 12$, so the integers of order 6 are those integers 7^h with $h = \dfrac{\phi(26)}{\gcd(h, \phi(26))} \Rightarrow 6 = \dfrac{12}{\gcd(h,12)} \Rightarrow \gcd(h,12) = 2 \Rightarrow h = 2,10$. Thus integers of order 6 modulo 26 are $7^2, 7^{10}$. Thus smallest positive integers of order 6 modulo 26 are, $7^2 = 49 \equiv 23 (\mathrm{mod}\, 26)$, $7^3 \equiv 5 (\mathrm{mod}\, 26) \Rightarrow 7^6 = (7^3)^2 \equiv (5)^2 \equiv 25 (\mathrm{mod}\, 26)$ and $7^{10} = 7^6 \cdot 7^2 \cdot 7^2 \equiv (-1) \cdot (-3)(-3) \equiv -9 \equiv 17 (\mathrm{mod}\, 26)$. Thus integers of order 6 modulo 26 are 17, 23. However, one is tempted to wonder if 3, 9 are also integers of order 6, but both are clearly ruled out, for $3^3 \equiv 1$ and $9^3 \equiv (3^3)^2 \equiv 1^2 \equiv 1$.

Now let us find integers of order 3 modulo 26. Here, $\phi(26) = \phi(13) = 12$, so the integers of order 3 are those integers 7^h with

$$h = \frac{\phi(26)}{\gcd(h, \phi(26))} \Rightarrow 3 = \frac{12}{\gcd(h,12)} \Rightarrow \gcd(h,12) = 4 \Rightarrow h = 4,8.$$

Thus the integers of order 3 are, $7^4 = (7^2)^2 \equiv (-3)^2 \equiv 9 (\mathrm{mod}\, 26)$ and

$7^8 = (7^4)^2 \equiv (9)^2 \equiv 3 (\mathrm{mod}\, 26)$, that is 3 and 9 are integers of order 3 modulo 26.

Now let us find integers of order 2 modulo 26. Here, $\phi(26) = \phi(13) = 12$, so the integers of order 2 are those integers 7^h with

$$h = \frac{\phi(26)}{\gcd(h, \phi(26))} \Rightarrow 2 = \frac{12}{\gcd(h,12)} \Rightarrow \gcd(h,12) = 6 \Rightarrow h = 6.$$

Thus the integer of order 2 is, $7^6 \equiv 25 (\mathrm{mod}\, 26)$. Thus 25 is integers of order 2 modulo 26.

Similarly, the integers of order 4 are those integers 7^h with

$$h = \frac{\phi(26)}{\gcd(h, \phi(26))} \Rightarrow 4 = \frac{12}{\gcd(h,12)} \Rightarrow \gcd(h,12) = 3 \Rightarrow h = 3,9$$ and hence, the integers of

order 3 are, $7^3 \equiv 5 (\mathrm{mod}\, 26)$ and $7^9 = (7^8) \cdot 7 \equiv 3 \cdot 7 \equiv 21 (\mathrm{mod}\, 26)$. Thus 5 and 21 are integers of order 4 modulo 26.

In general we can list the integers as follows :

Primitive roots are $7, 7^5, 7^7, 7^{11}$; that is 7, 11, 15, 19.

Integers of order 6 modulo 256 are, $7^2, 7^6, 7^{10}$; that is 17, 23,

integers of order 4 modulo 26 are, $7^3, 7^9$; that is5, 21,

integers of order 3 modulo 26 are, $7^4, 7^8$; that is, 3, 9,

integers of order 2 modulo 26 is, 7^6 ; that is, 25,

Integers of order 1 modulo 26 is, 1.

Ex. Find all primitive roots of 41 and 82.

Solution. Consider $2^5 \equiv -9 (\mathrm{mod}\, 41)$, $2^{10} \equiv -1 (\mathrm{mod}\, 41)$, so 2 is not a primitive root of 41. Next $3^4 \equiv -1 (\mathrm{mod}\, 41)$ implies that 3 is also not a primitive root of 41. Further, $4^5 = 2^{10} \equiv -1 (\mathrm{mod}\, 41)$ and hence 4 is also not a primitive root. Now $5^3 \equiv -2 (\mathrm{mod}\, 41)$, $5^6 \equiv 4 (\mathrm{mod}\, 41)$, $5^4 \equiv -10 (\mathrm{mod}\, 41)$, $5^{10} = 5^6 \cdot 5^4 \equiv (4)(-10) \equiv -1 (\mathrm{mod}\, 41)$ therefore, 5 is also not a primitive root. Consider, $6^2 \equiv -5 (\mathrm{mod}\, 41)$, $6^4 \equiv 25 (\mathrm{mod}\, 41)$, $6^6 = 6^4 \cdot 6^2 \equiv -2 (\mathrm{mod}\, 41)$, $6^{10} = 6^6 \cdot 6^4 \equiv -9 (\mathrm{mod}\, 41)$. Thus $6^{20} \equiv -1 (\mathrm{mod}\, 41)$ and hence 6 is primitive root of 41.

Now 6 being an even integer it cannot be a primitive root of 82 and hence, 6 + 41 = 47 is primitive root of 82.

Notes :

1. Clearly, 2 is primitive root of 3 and $2^2 = 4 \not\equiv 1 (\mathrm{mod}\, 9)$, so 2 is primitive root of all powers of 3.
2. Since $\phi(2p^n) = \phi(p^n)$, they have same number of primitive roots.
3. Any primitive root of p^2 is also a primitive root of p^n for $n \geq 2$.

Exercise :

1. Prove that 3 is a primitive root of all integers of the form 7^k and $2 \cdot 7^k$.
2. Prove that any primitive root r of p^n is also a primitive root of p.

❑❑❑

7.4 THE THEORY OF INDICES

Consider the Table 1. In this table we have we out powers of primitive root 3 and the positive integers less than 43 congruent to it modulo 43. However, if we take any other primitive root and the table would be different. Thus for a given primitive root we can always work out such a table. For example, we have $3^{35} \equiv 7 \pmod{43}$ and in this case we say that index of 7 relative to (primitive root) 3 is 35. Similarly, $3^{29} \equiv 18 \pmod{43}$ and in this case we say that index of 18 relative to (primitive root) 3 is 29.

The concept of indices was introduced by Gauss. Let n be any integer that admits a primitive r. We know that, $\phi(n)$ the integers r, r^2, ..., $r^{\phi(n)}$ are congrnent modulo n to a_1, a_2,...., $a_{\phi(n)}$, the $\phi(n)$ integers less than n and relatively prime to n. In other words each integer a such that $\gcd(a,n)=1$ can be expressed as $a \equiv r^k \pmod{n}$ for a suitable choice of k, where $1 \le k \le \phi(n)$. This idea prompts the following definition.

Definition : Let r be a primitive root of n and $\gcd(a,n)=1$. Then the smallest integer k such that $a \equiv r^k \pmod{n}$ is called index of a relative to r and is denoted by $\text{ind}_r a$.

Notes :

1. Clearly, $1 \le ind_r a \le \phi(n)$.

2. Whenever we talk about index it is assumed that $\gcd(a,n)=1$.

3. If $a \equiv b \pmod{n}$ then $ind_r a = ind_r b$ that is $r^{ind,a} \equiv r^{ind,b} \pmod{n}$.

   Clearly, $1 \le \text{ind}_r a \le \phi(n)$ and that $r^{\text{ind}_r a} \equiv a \pmod{n}$.

   e.g. Let us consider $n=5$ and primitive root $r=2$ of 5. Then

   $2^1 \equiv 2 \pmod{5}$, $2^2 \equiv 4 \pmod{5}$, $2^3 \equiv 3 \pmod{5}$ and $2^4 \equiv 1 \pmod{5}$.

   Thus $\text{ind}_2 1 = 4$, $\text{ind}_2 2 = 1$, $\text{ind}_2 3 = 3$ and $\text{ind}_2 4 = 2$.

   Note that $a \equiv b \pmod{n} \Rightarrow \text{ind } a = \text{ind } b$.

   Let $a \equiv b \pmod{n}$ and r be a primitive root of n.

   Then $r^{\text{ind } a} \equiv a \pmod{n}$ and $r^{\text{ind } b} \equiv b \pmod{n}$.

Thus $r^{\text{ind } a} \equiv r^{\text{ind } b} (\text{mod } n)$.

Therefore, $\text{ind } a \equiv \text{ind } b \left(\text{mod } \phi(n)\right)$ which is possible only if $\text{ind } a = \text{ind } b$. Thus, when setting up tables of values of ind a, it is enough to take integers less than a and relatively prime to n.

Theorem : If n has a primitive root r and ind a denotes index of a relative to r, then the following properties hold.

(a) $\text{ind } ab \equiv \text{ind } a + \text{ind } b \left(\text{mod } \phi(n)\right)$

(b) $\text{ind } a^k \equiv k \text{ ind } a \left(\text{mod } \phi(n)\right)$ for $k > 0$

(c) $\text{ind } 1 \equiv 0 \left(\text{mod } \phi(n)\right)$, $\text{ind } r \equiv 1 \left(\text{mod } \phi(n)\right)$

Proof : By definition of index

(a) $r^{\text{ind } a} \equiv a \ (\text{mod } n)$ and $r^{\text{ind } b} \equiv b \ (\text{mod } n)$

Therefore $r^{\text{ind } a + \text{ind } b} \equiv ab \ (\text{mod } n)$.

Since $r^{\text{ind } ab} \equiv ab \ (\text{mod } n)$ we have $r^{\text{ind } a + \text{ ind } b} \equiv r^{\text{ind } ab} \ (\text{mod } n)$.

Hence, $\text{ind } a \ + \ \text{ind } b \equiv \text{ind } ab \left(\text{mod } \phi(n)\right)$.

(b) Note that $r^{\text{ind } a^k} \equiv a^k (\text{mod } n)$.

And $r^{k \text{ ind } a} = \left(r^{\text{ind } a}\right)^k \equiv a^k (\text{mod } n)$.

Hence, $r^{\text{ind } a^k} \equiv r^{k \text{ ind } a} (\text{mod } n)$.

Therefore, $\text{ind } a^k \equiv k \text{ ind } a \left(\text{mod } \phi(n)\right)$.

(c) Finally, $r^{\phi(n)} \equiv 1 (\text{mod } n) \Rightarrow \text{ind } 1 \equiv 0 \left(\text{mod } \phi(n)\right)$ and $\text{ind } r \equiv 1 \left(\text{mod } \phi(n)\right)$.

The theory of indices can be used to solve certain types of congruences. Consider the binomial congruence.

$$x^k \equiv a (\text{mod } n) \qquad (k \geq 2) \qquad \ldots\ldots (1)$$

where n is a positive integer having primitive root and $\gcd(a,n)=1$. In view of above theorem (1) is equivalent to the linear congruence.

$$k \operatorname{ind} x \equiv \operatorname{ind} a \pmod{\phi(n)} \quad \text{..... (2)}$$

Let $d=\gcd(k,\phi(n))$. If $d \nmid \operatorname{ind} a$ then (2) is not solvable. However, if $d \mid \operatorname{ind} a$, then (2) has exactly d values of index modulo $\phi(n)$. Consequently, there are d solutions of (1).

Consider the case $k=1$, $n=p$ where p is odd prime. In this case (1) becomes,

$$x^2 \equiv a \pmod{p} \quad \text{..... (3)}$$

Since $\gcd(2,p-1)=2$, (3) has two solutions provided $2 \mid \operatorname{ind} a$.

Let r be a primitive root of p. Then $r, r^2, \ldots, r^{p-1}$ are congruent modulo p to $1, 2, .., p-1$ in some order. The even powers of r produce the values of a for which the congruence $x^2 \equiv a \pmod{p}$ is solvable. Note that there are precisely $(p-1)/2$ such choices for a.

Example : Solve $4x^9 \equiv 7 \pmod{13}$ ..... (1)

Solution : The above equation can be solved using theory of indices. Let us fix 2 as primitive root of 13. Note that,

$2^1 \equiv 2 \pmod{13}$, $2^2 \equiv 4 \pmod{13}$, $2^3 \equiv 8 \pmod{13}$

$2^4 \equiv 3 \pmod{13}$, $2^5 \equiv 6 \pmod{13}$, $2^6 \equiv 12 \pmod{13}$

$2^7 \equiv 11 \pmod{13}$, $2^8 \equiv 9 \pmod{13}$, $2^9 \equiv 5 \pmod{13}$

$2^{10} \equiv 10 \pmod{13}$, $2^{11} \equiv 7 \pmod{13}$, $2^{12} \equiv 1 \pmod{13}$

Thus index table can be written as,

a	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind} a$	12	1	4	2	9	5	11	3	8	10	7	6

Now (1) has a solution iff

$$\operatorname{ind}_2 4 + 9\operatorname{ind}_2 x \equiv \operatorname{ind}_2 7 \pmod{12}$$

$$\Rightarrow \quad 2+9\text{ind}_2\, x \equiv 11 (\text{mod}\, 12)$$

$$\Rightarrow \quad 9\text{ind}_2\, x \equiv 9 (\text{mod}\, 12)$$

$$\Rightarrow \quad \text{ind}_2\, x \equiv 1 (\text{mod}\, 4)$$

$$\Rightarrow \quad \text{ind}_2\, x \equiv 1, 5, 9$$

Looking at the index table, we obtain

$$x \equiv 2, 5 \text{ or } 6 (\text{mod}\, 13)$$

Note : Let us consider $p = 13$. We can obtain $\phi(\phi(13)) = 4$ primitive roots of 13. If we know one of them. Let us start with 2. Infact remaining 3 can be obtained from the powers $2^k (1 \le k \le \phi(n))$ where $\gcd(k, \phi(13)) = \gcd(k, 12) = 1$. They are

$$2^1 \equiv 2,\ 2^5 \equiv 6,\ 2^7 \equiv 11,\ 2^{11} \equiv 7 (\text{mod}\, 13).$$

Theorem : Let n be an integer possessing primitive root and let $\gcd(a, n) = 1$. Then the congruence $x^k \equiv a (\text{mod}\, n)$ has a solutions if and only if

$$a^{\phi(n)/d} \equiv 1 (\text{mod}\, n)$$

where $d = \gcd(k, \phi(n))$, if it has a solution, there are exactly d solutions modulo n.

Proof : Taking indices, the congruence $a^{\phi(n)/d} \equiv 1 (\text{mod}\, n)$ is equivalent to $\frac{\phi(n)}{d} \text{ind}\, a \equiv \text{ind}\, 1 (\text{mod}\, \phi(n))$.

Since $\text{ind}\, 1 \equiv 0 (\text{mod}\, \phi(n))$, we obtain.

$$\frac{\phi(n)}{d} \text{ind}\, a \equiv 0 (\text{mod}\, \phi(n))$$

$$\Rightarrow \text{ind}\, a \equiv 0 (\text{mod}\, d)$$

$$\Rightarrow d \mid \text{ind}\, a$$

But this is necessary and sufficient condition for congruence $x^k \equiv a \pmod{n}$ to be solvable. However, if the congruence has solution, then there are exactly d solutions modulo n.

Corollary : Let p be a prime and $\gcd(a, p) = 1$. Then the congruence $x^k \equiv a \pmod{p}$ has a solution if and only if $a^{(p-1)/d} \equiv 1 \pmod{p}$, where $d = \gcd(k, p-1)$.

Example : Consider $x^3 \equiv 4 \pmod{13}$.

Here $d = \gcd(3, \phi(13)) = \gcd(3,12) = 3$ and so $\phi(13)/d = 4$. Observe that $4^4 \not\equiv 1 \pmod{13}$. Hence, this congruence has no solution.

Example : Solve $x^3 \equiv 5 \pmod{13}$.

Solution : Here $d = \gcd(3, \phi(13)) = 4$ and $5^4 \equiv 1 \pmod{13}$.

Hence, $x^3 \equiv 5 \pmod{13}$ has a solution. Now the given congruence is equivalent to

$$3 \operatorname{ind} x \equiv \operatorname{ind} 5 \pmod{12}$$

$$3 \operatorname{ind} x \equiv 9 \pmod{12}$$

$$\operatorname{ind} x \equiv 3 \pmod{4}$$

$$\operatorname{ind} x \equiv 3, 7 \text{ or } 11$$

And hence, $x \equiv 7, 8 \text{ or } 11 \pmod{13}$.

Example : Solve $x^{12} \equiv 13 \pmod{17}$.

Solution. We have $x^{12} \equiv 13 \pmod{17}$

We know that 3 is a primitive root of 17 and therefore, this is equivalent to

$$12 ind_3 x \equiv ind_3 13 \pmod{\phi(17)} \text{ or } 12 ind_3 x \equiv 4 \pmod{16}$$

Clearly $\gcd(12,16) = 4 \mid 4$ and hence $12 ind_3 x \equiv 4 \pmod{16}$ or $3 \cdot ind_3 x \equiv 1 \pmod{4}$ has a solution $ind_3 x = 3$. Thus $x = 10$. Thus solutions modulo 17 are 2, 6, 10, 14.

If we take primitive root 5 instead of 3, we have $ind_3 x = 3$ implies $x = 6$ and in this case also solutions modulo 17 are 2, 6, 10, 14.

Note that gcd(12, 16) = 4 and hence there are 4 incongruent solutions modulo 17.

Ex. Solve $8x^5 \equiv 10 (\text{mod} 17)$.

Solution. We have $8x^5 \equiv 10 (\text{mod} 17)$

We know that 3 is a primitive toot of 17 and therefore, this is equivalent to

$$ind_3 8 + 5 \cdot ind_3 10 \left(\text{mod}\, \phi(17)\right) \text{ or } 10 + 5 \cdot ind_3 x \equiv 4 (\text{mod} 16)$$

Thus

$$5 \cdot ind_3 x \equiv 10 (\text{mod} 16) \Rightarrow ind_3 x \equiv 2 (\text{mod} 16) \Rightarrow ind_3 x = 2 \Rightarrow x = 9$$

Therefore, the solution is 9 modulo 17.

Ex. Solve $7^x \equiv 7 (\text{mod} 17)$.

Solution. We have $7^x \equiv 7 (\text{mod} 17)$

We know that 3 is a primitive root of 17 and therefore, this is equivalent to

$$x \cdot ind_3 7 \equiv ind_3 7 \left(\text{mod}\, \phi(17)\right) \text{ or } x \equiv 1 (\text{mod} 16).$$

Thus, the solution is 1 modulo 16.

Note that in above example solution is congruent to $\phi(17) = 16$ but not 17 which is the case in earlier examples.

Ex. Find the remainder when $3^{24} \cdot 5^{13}$ is dividisble by 17.

Solution. We have to solve

$$3^{24} \cdot 5^{13} \equiv x (\text{mod} 17).$$

Using theory of indices we can write

$$24 \cdot ind_3 3 + 13 \cdot ind_3 5 \equiv ind_3 x \left(\text{mod}\, \phi(17)\right).$$

Thus we have

$$24 \cdot 1 + 13 \cdot 5 \equiv ind_3 x (\text{mod} 16) \Rightarrow ind_3 x \equiv 9 (\text{mod} 16) \Rightarrow ind_3 x = 9 \Rightarrow x = 12.$$

Therefore, only solution is 12 modulo 17. Thus 12 is the remainder.

Exercise :

1. Determine whether the two congruences $x^5 \equiv 13 (\mathrm{mod}\, 23)$ and $x^{17} \equiv 15 (\mathrm{mod}\, 29)$ are solvable.

2. For which values of b is the exponential congruence $9^x \equiv b (\mathrm{mod} 13)$ solvable ?

3. Solve the congruence $7x^3 \equiv 3 (\mathrm{mod} 11)$.

4. Solve the congruence $3x^4 \equiv 5 (\mathrm{mod} 11)$.

5. Determine the integers $a (1 \le a \le 12)$ such that the congruence $ax^4 \equiv b (\mathrm{mod} 13)$ has solution for $b = 2$, 5 and 6.

Unit - 8
THE QUADRATIC RECIPROCITY LAW

8.1 QUADRATIC RESIDUE

The qudratic reciprocity law deals with solvability of quadratic congruences. Consider the congruence.

$$ax^2 + bx + c \equiv 0 \pmod{p} \qquad \text{..... (1)}$$

where p is prime and $a \not\equiv 0 \pmod{p}$.

Since p is odd prime and $p \nmid a$, we have $\gcd(4a, p) = 1$. Therefore, the quadratic congruence in Eq^n. (1) is equivalent to,

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}$$

$$\Rightarrow 4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$

$$\Rightarrow (2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$$

Now put $2ax + b = y$ and $d = b^2 - 4ac$, then we get

$$y^2 \equiv d \pmod{p} \qquad \text{..... (2)}$$

If $x \equiv x_0 \pmod{p}$ is a solution of the quadratic congruence in Eq^n. (1), then the integer $y \equiv 2ax_0 + b \pmod{p}$ is a solution of Eqn. (2). Conversely, if $y \equiv y_0 \pmod{p}$ is a solution of quadratic congruence in Eqn. (2), then $2ax \equiv y_0 - b \pmod{p}$ can be solved to obtain solution to Eq^n. (1).

Thus, the problem of finding a solution to the quadratic congruence in Eq^n. (1) is equivalent to that of finding a solution to linear congruence and a quadratic congruence of the form.

$$x^2 \equiv a \pmod{p}. \qquad \text{..... (3)}$$

If $p \mid a$, then the quadratic congruence in Eqn. (3) has $x \equiv 0 \pmod{p}$ as its only solution. To avoid trivialities, let us agree to assume hereafter that $p \nmid a$. Thus whenever $x = x_0$ is a solution of $x^2 \equiv a \pmod{p}$, there is also a second solution $x = p - x_0$. Since $x_0 \equiv p - x_0 \pmod{p}$ implies $2x_0 \equiv 0 \pmod{p}$ or equivalently $x_0 \equiv 0 \pmod{p}$ which is impossible as $p \nmid a$. x_0 and $p - x_0$ are incongruent modulo *p*. By Lagranges theorem $x^2 \equiv a \pmod{p}$ admits two solutions x_0 and $p - x_0$ exhaust the incongruent solutions of $x^2 \equiv a \pmod{p}$. Thus $x^2 \equiv a \pmod{p}$ has exactly two solutions or no solutions.

e.g. consider the quadratic congruence

$$5x^2 - 6x + 2 \equiv 0 \pmod{13}$$

This is equivalent to,

$$4 \times 5(5x^2 - 6x + 2) \equiv 0 \pmod{13}$$

$$\Rightarrow (100x^2 - 120x + 36) + 4 \equiv 0 \pmod{13}$$

$$\Rightarrow (100x - 6) \equiv 9 \pmod{13}$$

$$\Rightarrow y^2 \equiv 9 \pmod{13} \qquad \text{..... (4)}$$

where $y = 10x - 6$.

Clearly, (4) has solutions $y \equiv 3, 10 \pmod{13}$.

Next consider the linear equations

$$10x - 6 \equiv 3 \pmod{13} \text{ and } 10x - 6 \equiv 10 \pmod{13}$$

or equivalently

$$10x \equiv 9 \pmod{13} \text{ and } 10x \equiv 3 \pmod{13}$$

It can be seen that $x \equiv 10 \pmod{13}$ and $x \equiv 12 \pmod{13}$ are solutions of the above linear congruences. Hence, $x = 10, 12$ are solutions of quadratic congruence modulo 13.

Definition : Let p be an odd prime and $\gcd(a, p) = 1$. If the quadratic congruence $x^2 \equiv a \pmod{p}$ has a solution then *a* is said to be **quadratic residue of *p*** otherwise *a* is called **quadratic non-residue of *p***.

Note : If $a \equiv b \pmod{p}$, then a is quadratic residue. If and only if b is a quadratic residue of p.

Example : Consider the example with $p = 13$. We shall find out how many of the integers 1, 2, ..., 12 are quadiatic residues of 13. That is to find which of the congruences $x^2 \equiv a \pmod{13}$ are solvable when a runs through $\{1, 2, ..., 12\}$.

Consider,

$$1^2 \equiv 12^2 \equiv 1$$

$$2^2 \equiv 11^2 \equiv 4$$

$$3^2 \equiv 10^2 \equiv 9$$

$$4^2 \equiv 9^2 \equiv 3$$

$$5^2 \equiv 8^2 \equiv 12$$

$$6^2 \equiv 7^2 \equiv 10 \cdot$$

Thus 1, 3, 4, 9, 10, 12 are quadratic residues of 13 and 2, 5, 6, 7, 8, 11 are quadratic non-residues.

Further, there are two pairs of consecutive quadratic residues namely 3, 4 and 9, 10.

In general for any odd prime p there are $\frac{1}{4}\left(p - 4 - (-1)^{(p-1)/2}\right)$ consecutive pairs.

For $p = 3$, there are $\frac{1}{4}\left(13 - 4 - (-1)^{(13-1)/2}\right) = 2$ pairs.

Theorem : (Euler's Criterion)

Let p be an odd prime and $\gcd(a, p) = 1$. Then a is a quadratic residue of p if and only if $a^{(p-1)/2} = 1 \pmod{p}$.

Proof : Suppose that a is a quadratic residue of p, so that $x^2 \equiv a \pmod{p}$ admits a solution, call it x_1. Since $\gcd(a, p) = 1$, $\gcd(x_1, p) = 1$. Then $x_1^2 \equiv a \pmod{p}$, i.e. $a \equiv x_1^2 \pmod{p}$. Therefore, by Fermat's theorem.

$$a^{(p-1)/2} = \left(x_1^2\right)^{\frac{(p-1)}{2}} \equiv x_1^{p-1} \equiv 1 \pmod{p}.$$

Conversely, suppose that $a^{(p-1)/2} = 1 \pmod{p}$ holds. Let r be a primitive root of p. Then we know that $r, r^2, \ldots, r^k$ are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ a integer less than n and relatively prime to n. Since $\gcd(a, n) = 1$, there is a positive integer k, $1 \le k \le p-1$ such that $r^k \equiv a \pmod{p}$. Then $r^k \equiv a \pmod{p}$ for some integer k, with $1 \le k \le p-1$.

Thus,

$$r^{k(p-1)/2} = a^{(p-1)/2} \equiv 1 \pmod{p}. \qquad \ldots\ldots (1)$$

Hence, order of r, that is, $p-1$ must divide the exponent $k(p-1)/2$ of r in (1). Thus k has to be even. Let $k = 2j$. Then

$$\left(r^j\right)^2 = r^{2j} = r^k \equiv a \pmod{p}.$$

Thus r^j is a solution of quadratic congruence $x^2 \equiv a \pmod{p}$. Therefore, a is a quadratic residue of p.

Note : Suppose that p is an odd prime and $\gcd(a, p) = 1$, then

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

$$\Rightarrow \left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) \equiv 0 \pmod{p}$$

$$\Rightarrow a^{(p-1)/2} \equiv 1 \pmod{p} \text{ or } a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Note that if a satisfies both $a^{(p-1)/2} \equiv 1 \pmod{p}$ and $a^{(p-1)/2} \equiv -1 \pmod{p}$ then we would have $1 \equiv -1 \pmod{p}$ which is absurd. Hence, exactly, one of the two holds. Therefore, if $a^{(p-1)/2} \not\equiv 1 \pmod{p}$ then we must have $a^{(p-1)/2} \equiv -1 \pmod{p}$. Therefore, the integer a is quadratic non-residue of p iff $a^{(p-1)/2} \equiv -1 \pmod{p}$. Thus we have

Corollary : Let p be an odd prime and $\gcd(a, p) = 1$. Then a is quadratic residue or non-residue according to whether.

$$a^{(p-1)/2} = 1 \pmod{p} \text{ or } a^{(p-1)/2} = -1 \pmod{p}$$

Note : We have seen that 3 is quadratic residue and 2 is non-residue of 13. Observe that

$$2^{(13-1)/2} = 2^6 = 64 \equiv 12 \equiv -1 \pmod{13}$$

and $$3^{(13-1)/2} = 3^6 = (27)^2 \equiv (1)^2 \equiv 1 \pmod{13}$$

Example : Solve $x^2 + 7x + 10 \equiv 0 \pmod{11}$.

Solution : Consider $x^2 + 7x + 10 \equiv 0 \pmod{11}$

$$\Rightarrow 4x^2 + 28x + 40 \equiv 0 \pmod{11}$$

$$\Rightarrow (2x + 7)^2 \equiv 9 \pmod{11}.$$

Now consider the congruence,

$$y^2 \equiv 9 \pmod{11} \qquad \text{..... (1)}$$

where $y = 2x + 7$.

Observe that $y \equiv 3, 8 \pmod{11}$ are solution of Eq^n. (1).

Now, we consider $2x + 7 \equiv 3 \pmod{11}$ and $2x + 7 \equiv 8 \pmod{11}$. These are equivalent to,

$$2x \equiv -4 \pmod{11} \text{ and } 2x \equiv 1 \pmod{11}$$

Consider $2x \equiv -4 \pmod{11} \Rightarrow x \equiv -2 \pmod{11}$

$$\Rightarrow x \equiv 9 \pmod{11}$$

and $2x \equiv 1 \pmod{11} \Rightarrow 6(2x) \equiv 6(1) \pmod{11} \Rightarrow x \equiv 12x \equiv 6 \pmod{11}$

$$\Rightarrow x \equiv 6 \pmod{11}.$$

Thus $x \equiv 6, 9 \pmod{11}$ are the solutions of given quadratic congruence.

8.2 THE LEGENDRE SYMBOL AND ITS PROPERTIES :

Definition : Let p be an odd prime and let $\gcd(a, p) = 1$. The Legendre symbol (a/p) is defined by

$$(a/p) = \begin{cases} 1 & \text{If } a \text{ is quadratic residue of } p \\ -1 & \text{If } a \text{ is quadratic non-residue of } p \end{cases}.$$

Legendre symbol is also written as $\left(\frac{a}{p}\right)$ or (a/p). In the symbol (a/p), a is called numerator and p is called denominator.

e.g. Let us take $p = 13$. Then

$$(1/13) = (3/13) = (4/13) = (9/13) = (10/13) = (12/13) = 1$$

and $$(2/13) = (5/13) = (6/13) = (7/13) = (8/13) = (11/13) = -1$$

Recall that 1, 3, 4, 9, 10, 12 are quadratic residues and 2, 5, 6, 7, 8, 11 are non-residues.

Remark : For $p \mid a$, we have purposely left the symbol (a/p) undefined. Some authors define $(a/p) = 0$ in case $p \mid a$. The advantage of this is that the number of solutions of $x^2 \equiv a \pmod{p}$ is given by $1 + (a/p)$. Observe that if $\left(\frac{a}{p}\right) = 1$ then there are 2 solutions, if $\left(\frac{a}{p}\right) = -1$, number of solutions is zero. However, if $p \mid a$, then $x^2 \equiv a \pmod{p}$ becomes $x^2 \equiv 0 \pmod{p}$ and in this case there is only one solution.

Theorem : Let p be an odd prime and let a and b be integers that are relatively prime to p. Then the Legendre symbol has the following properties :

(a) If $a \equiv b \pmod{p}$, then $(a/p) = (b/p)$,

(b) $(a^2/p) = 1$,

(c) $(a/p) \equiv a^{(p-1)/2} \pmod{p}$,

(d) $(ab/p) = (a/p)(b/p)$,

(e) $(1/p) = 1$ and $(-1/p) = (-1)^{(p-1)/2}$.

Proof : (a) If $a \equiv b \pmod{p}$, then the congruences $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ have exactly the same solutions if any at all. Thus $x^2 \equiv a \pmod{p}$ and $x^2 \equiv b \pmod{p}$ are both solvable, or neither one has a solution, which is exactly $(a/p) = (b/p)$.

(b) Since a trivially satisfies $x^2 \equiv a^2 \pmod{p}$ we have $(a^2/p) = 1$.

(c) We know that $a^{(p-1)/2} \equiv 1 \pmod{p}$ or $a^{(p-1)/2} \equiv -1 \pmod{p}$ according as a is quadratic residue or non-residue of p. Hence, $(a/p) \equiv a^{(p-1)/2} \pmod{p}$.

(d) $(ab/p) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv (a/p)(b/p) \pmod{p}$. Since Legendre symbol assumes values 1 and –1 only, if $(ab/p) \neq (a/p)(b/p)$, we would have $1 \equiv -1 \pmod{p}$ which is absurd because $p > 2$. Therefore, we must have $(ab/p) = (a/p)(b/p)$.

(e) Since $(a^2/p) = 1$, for $a = 1$, we have $(1/p) = 1$.

For the other part let $a = -1$ so that

$$(-1/p) \equiv (-1)^{(p-1)/2} \pmod{p} \qquad \text{..... (1)}$$

Since the quantities $(-1/p)$ and $(-1)^{(p-1)/2}$ are either 1 or – 1, Eqn. (1) implies that $(-1/p) = (-1)^{(p-1)/2}$.

Note : $(ab^2/p) = (a/p)(b^2/p) = (a/p)$.

Corollary : If p is an odd prime, then

$$(-1/p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}.$$

Note : In view of above corollary, we obtain, the quadratic congruence $x^2 \equiv -1 (\text{mod } p)$ has a solution iff p is of the form 4k + 1.

Example : Show that $x^2 \equiv -46 (\text{mod } 17)$ has no solution.

Solution : The given problem is equivalent to evaluating $(-46/17)$. We know

$$(-46/17) = (-1/17)(46/17) = (46/17) \qquad \left((-1/17) = (-1)^{(17-1)/2} = (-1)^8 = 1\right)$$

Since $46 \equiv 12 (\text{mod } 17)$, we have

$$(46/17) = (12/17)$$

Thus $(12/17) = (3 \times 2^2/17) = (3/17)(2^2/17) = (3/17)$

But $(3/17) \equiv 3^{(17-1)/2} \equiv 3^8 \equiv (81)^2 \equiv (-4)^2 \equiv -1 (\text{mod } 17)$

Therefore, $(3/17) = -1$ and consequently, $(46/17) = -1$.

Thus $x^2 \equiv -46 (\text{mod } 17)$ has no solution.

Theorem : There are infinitely many primes of the form 4k + 1.

Proof : Suppose that there are finitely many such primes say $p_1, p_2, \ldots, p_n$ and consider,

$$N = (2p_1, p_2, \ldots, p_n)^2 + 1$$

Clearly, N is odd, so that there exists some odd prime p with $p \mid N$. To put it another way,

$$(2p_1, p_2, \ldots, p_n)^2 \equiv -1 (\text{mod } p)$$

Thus $(-1/p) = 1$. We know that $(-1/p) = 1$ only if p is of the form 4k + 1.

Hence, p must be one of $p_1, p_2, \ldots, p_n$ but then $p \mid N - (2p_1, p_2, \ldots, p_n)^2 \equiv 1$ or $p \mid 1$. Which is absurd. Hence, the result.

Theorem : If p is an odd prime, then $\sum_{a=1}^{p-1}(a/p)=0$.

Hence, there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues of p.

Proof : Let r be a primitive root of p. We know that the powers $r, r^2, ..., r^{p-1}$ are congruent modulo p to 1, 2, ..., $p-1$ in some order. That is $r, r^2, ..., r^{p-1}$ are just a permutation of the integers 1, 2, ..., $p-1$ modulo p. This for any a lying between 1 and $p-1$, inclusive there is a unique positive integer $k\,(1 \le k \le p-1)$, such that $a \equiv r^k \pmod p$.

Since r is a primitive root of p, we have

$$r^{p-1}-1 \equiv 0 \pmod p \Rightarrow \left(r^{(p-1)/2}-1\right)\left(r^{(p-1)/2}+1\right) \equiv 0 \pmod p$$

$$\Rightarrow r^{(p-1)/2} \equiv 1 \pmod p \text{ or } r^{(p-1)/2} \equiv -1 \pmod p$$

As r is primitive root of p, $r^{(p-1)/2} \not\equiv 1 \pmod p$ and hence

$$r^{(p-1)/2} \equiv -1 \pmod p.$$

Thus $(a/p) = (r^k/p) \equiv (r^k)^{(p-1)/2} = \left(r^{(p-1)/2}\right)^k \equiv (-1)^k \pmod p$.

Therefore, $(a/p) = (-1)^k = (r^k/p)$ are equal to 1 or -1.

Hence, $\sum_{a=1}^{p-1}(a/p) = \sum_{k=1}^{p-1}(-1)^k = 0$.

and the theorem is proved.

Corollary : The quadratic residues of an odd prime p are congruent modulo p to the even powers of the primitive root r of p; the quadratic non-residues are congruent to the odd powers of r.

Proof : The result follows immediately from

$$(a/p) = (r^k/p) \equiv (-1)^k \pmod p.$$

Theorem (Gauss' Lemma) :

Let p be an odd prime and let $\gcd(a, p) = 1$. If n denotes the number of integers in the set.

$$S = \left\{ a, 2a, 3a, ..., \left(\frac{p-1}{2} \right) a \right\}$$

whose remainders upon division by p exceed $p/2$, then

$$(a / p) = (-1)^n .$$

Proof : Since $\gcd(a, p) = 1$, we find that none of the $(p-1)/2$ integers in S is congruent to zero and no two are congruent to each other modulo p. Let $r_1, r_2, ..., r_m$ be those remainders upon division by p such that $0 < r_i < p/2$ and let $s_1, s_2, ..., s_n$ be those remainders such that $p/2 < s_i < p$.

Then $m + n = (p-1)/2$ and the integer.

$$r_1, r_2, ..., r_m, p - s_1, p - s_2, ..., p - s_n$$

are all positive and less than $p/2$.

To prove that these integers are all distinct it suffices to show that no $p - s_i$ is equal to any r_j. Assume on the contrary that,

$$p - s_i = r_j$$

for some choice of i and j. Then there exist integers u and v, with $1 \le u$, $v \le (p-1)/2$ satisfying $s_i \equiv ua \pmod{p}$ and $r_j \equiv va \pmod{p}$. Hence,

$$(u + v)\, a \equiv s_i + r_j = p \equiv 0 \pmod{p}$$

which says that $u + v \equiv 0 \pmod{p}$. But the latter congruence can not take place because $1 < u + v \le p - 1$.

Note that $(p-1)/2$ numbers $r_1, r_2, ..., r_m$, $p-s_1, p-s_2, ..., p-s_n$ are simply the integers 1, 2, ..., $(p-1)/2$, not necessarily in order of appearance. Thus, their product is $\left(\frac{p-1}{2}\right)!$.

Therefore, $\left(\frac{p-1}{2}\right)! = r_1...r_m(p-s_1)...(p-s_n)$

$$\equiv r_1...r_m(-s_1)...(-s_n)(\text{mod } p)$$

$$\equiv (-1)^n r_1...r_m s_1...s_n(\text{mod } p).$$

But, we know that $r_1, ...r_m, s_1, ..., s_n$ are congruent modulo p to $a, 2a, ..., \left(\frac{p-1}{2}\right)a$, in some order, so that

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^n a \cdot 2a.....\left(\frac{p-1}{2}\right)a(\text{mod } p)$$

$$\equiv (-1)^n a^{(p-1)/2}\left(\frac{p-1}{2}\right)!(\text{mod } p)$$

Since $\left(\frac{p-1}{2}\right)!$ is relatively prime to p, we obtain

$$1 \equiv (-1)^n a^{(p-1)/2}(\text{mod } p)$$

$$\Rightarrow a^{(p-1)/2} \equiv (-1)^n(\text{mod } p).$$

By Euler's criteria, we obtain,

$$(a/p) \equiv a^{(p-1)/2} \equiv (-1)^n(\text{mod } p).$$

Thus $(a/p) = (-1)^n$.

Let us consider the case $p = 13$ and $a = 5$.

Then $(p-1)/2 = 6$, so that $s = \{5,10,15,20,25,30\}$.

Modulo 13, the members of S are the same as the integers 5, 10, 2, 7, 12, 4. Three of these are greater than 13/2. Hence, $n = 3$ and consequently,

$$(5/13) = (-1)^3 = -1 \cdot$$

Theorem : If p is an odd prime, then

$$(2/p) = \begin{cases} 1 & \text{if } p \equiv 1 (\text{mod } 8) \text{ or } p \equiv 7 (\text{mod } 8) \\ -1 & \text{if } p \equiv 3 (\text{mod } 8) \text{ or } p \equiv 5 (\text{mod } 8) \end{cases}.$$

Proof : By Gauss' Lemma, $(2/p) = (-1)^n$, where n is the number of integers in the set.

$$S = \left\{1 \cdot 2, 2 \cdot 2, 3 \cdot 2, ..., \left(\frac{p-1}{2}\right) \cdot 2\right\}$$

which upon division by p leave remainder greater that $p/2$. The members of S are all less than p, so that it suffices to count the number that are greater than $p/2$.

For $1 \le k \le \left(\frac{p-1}{2}\right)$, we have $2k < p/2$ iff $k < p/4$. Therefore, there are $[p/4]$ integers in S less than $p/2$; hence $n = \frac{p-1}{2} - \left[\frac{p}{4}\right]$ is the number of integers that are greater than $p/2$.

Now, we have four possibilities, for any odd prime has one of the forms $8k + 1$, $8k + 3$, $8k + 5$ or $8k + 7$. A simple calculation shows that,

If $p = 8k+1$, then $n = 4k - \left[2k + \frac{1}{4}\right] = 4k - 2k = 2k$.

If $p = 8k+3$, then $n = (4k+1) - \left[2k + \frac{3}{4}\right] = 4k + 1 - 2k = 2k + 1$.

If $p = 8k+5$, then $n = (4k+2) - \left[2k+1+\frac{1}{4}\right] = 4k+2-(2k-1) = 2k+1$.

If $p = 8k+7$, then $n = 4k+3-\left[2k+1+\frac{3}{4}\right] = 4k+3-(2k-1) = 2k+2$.

Thus when p is of the form $8k+1$ or $8k+7$, n is even and so $(2/p)=1$ and in case p is of the form $8k+3$ or $8k+5$, n is odd and so $(2/p)=-1$.

Corollary : If p is an odd prime, then

$$(2/p) = (-1)^{(p^2-1)/8}$$

Proof : Suppose p is of the form $8k \pm 1$, then

$$\frac{p^2-1}{8} = \frac{(8k\pm1)^2-1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k$$

Which is an even integer and hence

$$(-1)^{\left(p^2-1\right)/8} = 1 = (2/p)$$

On the other hand, if p is of the form $8k \pm 3$, then

$$\frac{p^2-1}{8} = \frac{(8k\pm3)^2-1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1$$

which is odd, so that $(-1)^{\left(p^2-1\right)/8} = -1 = (2/p)$.

Theorem : If p and $2p+1$ are both odd primes, then the integer $(-1)^{(p-1)/2}.2$ is a primitive root of $2p+1$.

Proof : For the sake of convenience, let us put $q = 2p+1$.

We distinguish the cases : $p \equiv 1 (\mathrm{mod}\, 4)$ and $p \equiv 3 (\mathrm{mod}\, 4)$

Case I : Let $p \equiv 1(\text{mod}\,4)$. In this case $(-1)^{(p-1)/2} \cdot 2 = 2$. Because $\phi(q) = q-1 = 2p$, the order of 2 modulo q is one of the numbers 1, 2, p or $2p$. We know

$$(2/p) \equiv 2^{(q-1)/2} \equiv 2^p (\text{mod}\, q)$$

But in the present setting, $q \equiv 3(\text{mod}\,8)$, hence, the Legendre symbol $(2/q) = -1$. It follows that $2^p \equiv -1(\text{mod}\, q)$ and therefore 2 can not have order p modulo q. The order of 2 being neither 1, 2 $2^2 \equiv 1(\text{mod}\, p) \Rightarrow q^{13}$ which is not possible) nor p.

Therefore, order of 2 modulo q is $2p$. Thus 2 is aprimitive root of q.

Case II : Let $p \equiv 3(\text{mod}\,4)$. In this case $(-1)^{(p-1)/2} \cdot 2 = -2$ and

$$(-2)^p \equiv (-2/q) = (-1/q)(2/q)(\text{mod}\, q).$$

Since $q \equiv 7(\text{mod}\,8)$, we have $(-1/q) = -1$ and $(2/q) = 1$.

Thus $(-2)^p \equiv -1(\text{mod}\, q)$. Arguing as in the first case, we conclude that – 2 is a primitive root of q.

Note : An odd prime p such that $2p + 1$ is also prime is called Germain prime after the French number theorist Sophie Germain (1776 – 1831).

Theorem : There are infinitely many primes of the form $8k - 1$.

Proof : Suppose on the contrary that there are only a finite numbers of primes of the form $8k - 1$ namely $p_1, p_2, ..., p_n$ and consider, $N = (4p_1, p_2, ..., p_n)^2 - 2$.

There exist atleast one odd prime divisor p of N, so that

$$(4p_1, p_2, ..., p_n)^2 \equiv 2(\text{mod}\, p).$$

In other words $(2/p) = 1$. Hence, $p \equiv \pm 1(\text{mod}\,8)$.

If all the odd prime divisors of N were of the form $8k + 1$, then N would be of the form $8a + 1$, this is clearly impossible because N is of the form $16a - 2$.

Thus, N must have a prime divisor q of the form $8k - 1$. But $q \mid N$ and $q / (4p_1, p_2, ..., p_n)^2$ leads to the contradiction that $q \mid 2$.

Lemma : If p is an odd prime and a is an odd integer, with $\gcd(a, p) = 1$, then

$$(a / p) = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]}.$$

Proof : Consider the set of integers,

$$S = \left\{ a, 2a, ..., \left(\frac{p-1}{2} \right) a \right\}.$$

By division algorithm, we have

$$ka = q_k p + t_k \qquad 1 \le t_k \le p - 1.$$

Then $\frac{ka}{p} = q_k + \frac{t_k}{p} \Rightarrow \left[\frac{ka}{p} \right] = q_k$ for $1 \le k \le \left(\frac{p-1}{2} \right)$.

Thus we can write

$$ka = \left[\frac{ka}{p} \right] p + t_k . \qquad \text{..... (1)}$$

If $t_k < p/2$, then it is one of $r_1, r_2, ..., r_m$ and if $t_k > p/2$, then it is one of the integers $s_1, ..., s_n$.

Taking the sum of $(p-1)/2$ equations in (1),

$$\sum_{k=1}^{(p-1)/2} ka = \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p} \right] p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k . \qquad \text{..... (2)}$$

We know that $(p-1)/2$ numbers,

$$r_1, \ldots, r_m, p - s_1, \ldots, p - s_n$$

are just rearrangement of the integers 1, 2, ..., $(p-1)/2$.

Hence,

$$\sum_{k=1}^{(p-1)/2} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p - s_k) = pn + \sum_{k=1}^{m} r_k - \sum_{k=1}^{n} s_k \; . \qquad \ldots\ldots (3)$$

Subtracting Eqn. (3) from Eqn. (2), we obtain,

$$(a-1) \sum_{k=1}^{(p-1)/2} k = p\left(\sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p} \right] - n \right) + 2\sum_{k=1}^{n} s_k \; . \qquad \ldots\ldots (4)$$

Since both a and p are odd integers, we have,

$$p \equiv a \equiv 1 (\mathrm{mod}\, 2)$$

and therefore Eqn. (4) can be written as,

$$0 \cdot \sum_{k=1}^{(p-1)/2} k \equiv 1 \cdot \left(\sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p} \right] - n \right) (\mathrm{mod}\, 2)$$

$$\Rightarrow n \equiv \sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p} \right] (\mathrm{mod}\, 2) \; .$$

Thus by Gauss' lemma,

$$(a / p) = (-1)^n = (-1)^{\sum_{k=1}^{(p-1)/2} \left[\frac{ka}{p} \right]} \; .$$

This proves the Lemma.

Example : Let us consider $p = 13$ and $a = 5$. Here $\left(\frac{p-1}{2} \right) = 6$.

Therefore, it is necessary to consider $\left[\frac{ka}{p} \right]$ for $k = 1, 2, \ldots\ldots, 6$. Thus,

$$\left[\frac{5}{13}\right]=\left[\frac{10}{13}\right]=0,\ \left[\frac{15}{13}\right]=\left[\frac{20}{13}\right]=\left[\frac{25}{13}\right]=1,\ \left[\frac{30}{13}\right]=2.$$

Therefore,

$$(5/13)=(-1)^{0+0+1+1+1+2}=(-1)^5=-1\ .$$

QUADRATIC RECIPROCITY LAW :

If p and q are distinct odd primes, then,

$$(p/q)(q/p)=(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

Proof : Consider the rectangle in the xy co-ordinate plane whose vertices are (0, 0), (p/2, 0), (0, q/2), and (p/2, q/2).

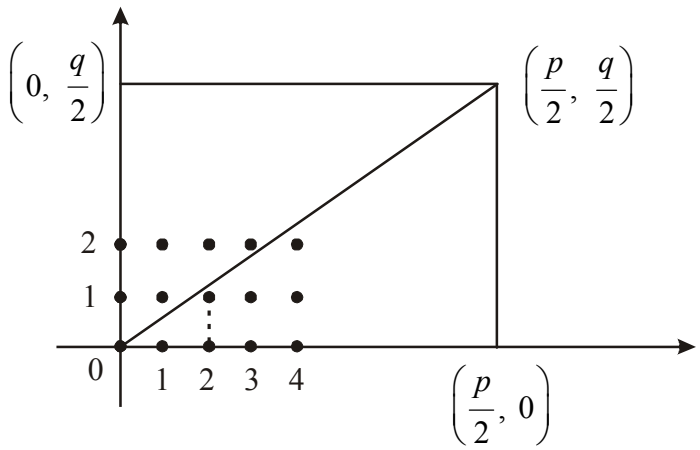
Let R denote the region within this rectangle, not including any of the bounding lines. The general plan of attack is to count the number of lattice points, that is, the points whose co-ordinates are integers, inside R in two different ways. Because p and q are both odd, the lattice points in R consist of all points (n, m), where $1\le n\le\left(\frac{p-1}{2}\right)$ and $1\le m\le\left(\frac{q-1}{2}\right)$.

Clearly, the number of such points is $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$.

Consider the diagonal D from (0, 0) to (p/2, q/2) which has the equation $y=\left(\frac{q}{p}\right)x$, or equivalently $py=qx$.

Because $\gcd(p,q)=1$, none of the lattice points inside R will lie on D, for $p/qx\Rightarrow p/x$ and $q/py\Rightarrow q/y$ and clearly there exist no such x and y such that $(x,y)\in R$. Suppose that T_1 denotes the portion of R that is below the diagonal D, and T_2 denote the portion above. By what we have just seen, it suffices to count the lattice points inside each of these triangles.

The number of integers in the interval $0 < y < \frac{kq}{p}$ is equal to $\left[\frac{kq}{p}\right]$. Thus for $1 \le k \le \left(\frac{p-1}{2}\right)$, there are precisely $\left[\frac{kq}{p}\right]$ lattice points in T_1, directly above $(k, 0)$ and below D; in other words, lying on the vertical line segment from $(k, 0)$ to $\left(k, \frac{kq}{p}\right)$. It follows that the total number of lattice points contained in T_1 is $\sum_{k=1}^{\left(\frac{p-1}{2}\right)} \left[\frac{kq}{p}\right]$.



A similar calculation, with the roles of p and q interchanged, shows that the number of lattice points within T_2 is

$$\sum_{j=1}^{\left(\frac{q-1}{2}\right)} \left[\frac{jp}{q}\right].$$

This accounts for all of the lattice points inside R, so that

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = \sum_{k=1}^{\left(\frac{p-1}{2}\right)} \left[\frac{kq}{p}\right] + \sum_{j=1}^{\left(\frac{q-1}{2}\right)} \left[\frac{jp}{q}\right].$$

Now by Gauss' Lemma, we obtain,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{j=1}^{\left(\frac{q-1}{2}\right)}\left[\frac{jp}{q}\right]} \cdot (-1)^{\sum_{k=1}^{\left(\frac{p-1}{2}\right)}\left[\frac{kq}{p}\right]}$$

$$= (-1)^{\sum_{j=1}^{\left(\frac{q-1}{2}\right)}\left[\frac{jp}{q}\right] + \sum_{k=1}^{\left(\frac{p-1}{2}\right)}\left[\frac{kq}{p}\right]}$$

$$= (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}.$$

This proves Quadratic Reciprocity Law.

Corollary 1 : If p and q are distinct odd primes then,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 (\text{mod } 4) \text{ or } q \equiv 1 (\text{mod } 4) \\ -1 & \text{if } p \equiv q \equiv 3 (\text{mod } 4). \end{cases}$$

Proof : Note that $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ is even if and only if at least one of p and q is of the form $4k+1$ and if both are of the form $4k+3$, the product $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$ is odd.

Corollary 2 : If p and q are odd primes, then,

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \equiv 1 (\text{mod } 4) \text{ or } q \equiv 1 (\text{mod } 4) \\ -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 1 (\text{mod } 4). \end{cases}$$

Proof : Note that $\left(\frac{p}{q}\right)^2 = 1 = \left(\frac{q}{p}\right)^2$ so that the result follows from above corollary.

Note : Let p be an odd prime and $a \neq \pm 1$ to be an integer not divisible by p. Suppose that a has the factorization.

Therefore, $a = \pm 2^{k_0} p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$

where p_i are distinct primes. Because the legendre symbol is multiplicative.

$$\left(\frac{a}{p}\right) = \left(\pm\frac{1}{p}\right)\left(\frac{2}{p}\right)^{k_0}\left(\frac{p_1}{p}\right)^{k_1}\ldots\left(\frac{p_r}{p}\right)^{k_r}.$$

To calculate $\left(\frac{a}{p}\right)$, we have only to calculate each of the symbols $\left(-\frac{1}{p}\right)$, $\left(\frac{2}{p}\right)$ and $\left(\frac{p_i}{p}\right)$. The values of $\left(-\frac{1}{p}\right)$ and $\left(\frac{2}{p}\right)$ were discussed earlier, so that one stumbling block is $\left(\frac{p_i}{p}\right)$, where p_i and p are distinct odd primes, this is where the Quadratic Reciprocity Law enters. Corollary 2 allows us to replace $\left(\frac{p_i}{p}\right)$ by a new Legendre symbol having a smaller denominator. Through continued inversion and division, the computation can be reduced to that of the known quantities $\left(-\frac{1}{q}\right)$, $\left(\frac{1}{q}\right)$, $\left(\frac{2}{q}\right)$.

Consider the Legendre symbol $\left(\frac{29}{53}\right)$. Here $29 \equiv 1 (\mathrm{mod}\, 4)$ and $53 \equiv 1 (\mathrm{mod}\, 4)$, we see that,

$$\left(\frac{29}{53}\right) = \left(\frac{53}{29}\right) = \left(\frac{24}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)\left(\frac{4}{29}\right)$$

$$= \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)$$

Since $29 \equiv 5 (\mathrm{mod}\, 8)$, $\left(\frac{2}{29}\right) = -1$. And

$$\left(\frac{3}{29}\right) = \left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = -1 \quad (\text{Since } 3 \equiv 3 (\mathrm{mod}\, 8))$$

Thus, $\left(\frac{29}{53}\right) = (-1)(-1) = 1.$

Theorem 1 : If $p \neq 3$ is an odd prime, then

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 (\mathrm{mod}\, 12) \\ -1 & \text{if } p \equiv \pm 5 (\mathrm{mod}\, 12). \end{cases}$$

Proof : Let $p \neq 3$ be an odd prime. Since $3 \equiv 3 (\mathrm{mod}\, 4)$ we have,

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{if } p \equiv 1 (\mathrm{mod}\, 4) \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

Now $p \equiv 1 (\mathrm{mod}\, 3)$ or $p \equiv 2 (\mathrm{mod}\, 3)$, therefore

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 (\mathrm{mod}\, 3) \\ -1 & \text{if } p \equiv 2 (\mathrm{mod}\, 3). \end{cases}$$

Thus $\left(\frac{3}{p}\right) = 1$ if and only if

$p \equiv 1 (\mathrm{mod}\, 4)$ and $p \equiv 1 (\mathrm{mod}\, 3)$ or $p \equiv 3 (\mathrm{mod}\, 4)$ and $p \equiv 2 (\mathrm{mod}\, 3)$.

Thus $p \equiv \pm 1 (\mathrm{mod}\, 12)$. Hence, the result follows.

QUADRATIC CONGRUENCES WITH COMPOSITE MODULI

In this section we shall be dealing with composite moduli. We begin with,

Theorem : If p is an odd prime and $\gcd(a, p) = 1$, then the congruence $x^2 \equiv a \pmod{p^n}$, $n \geq 1$ has a solution if and only if $\left(\frac{a}{p}\right) = 1$.

Proof : Suppose $x^2 \equiv a \pmod{p^n}$ has a solution, then so does $x^2 \equiv a \pmod{p}$, in fact the same solution, thus $\left(\frac{a}{p}\right) = 1$.

Conversely, suppose that $\left(\frac{a}{p}\right) = 1$. We shall use induction to prove the result. Since $\left(\frac{a}{p}\right) = 1$, $x^2 \equiv a \pmod{p}$ has a solution, so that result holds for $n = 1$. Let the result hold for $n = k \geq 1$, that is, $x^2 \equiv a \pmod{p^k}$ has a solution x_0. Then

$$x_0^2 \equiv a \pmod{p^k}.$$

So that $x_0^2 = a + bp^k$ for some integer b.

Since $\gcd(2x_0, p) = 1$, the congruence $2x_0 y \equiv -b \pmod{p}$ has a unique solution x_0 modulo p. Consider,

$$x_1 = x_0 + y_0 p^k$$

Then $x_1^2 = x_0^2 + 2x_0 y_0 p^k + y_0^2 p^{2k}$

$$= a + (b + 2x_0 y_0) p^k + y_0^2 p^{2k}.$$

In view of $2x_0 y \equiv -b \pmod{p}$, $p \mid 2x_0 y_0 + b$. Thus, we obtain

$$x_1^2 \equiv a \pmod{p^{k+1}}.$$

Therefore, $x^2 \equiv a \pmod{p^{k+1}}$ has a solution for $n = k + 1$.

Hence, by induction the result holds for any n.

We shall now state and prove some results for $p = 2$.

Theorem : Let a be an odd integer. Then we have the following.

a) $x^2 \equiv a \pmod 2$ always has a solution.

b) $x^2 \equiv a \pmod 4$ has a solution if and only if $a \equiv 1 \pmod 4$.

c) $x^2 \equiv a \pmod{2^n}$, for $n \geq 3$, has a solution if and only if $a \equiv 1 \pmod 8$.

Proof :

a) The result is trivial for any odd $x = 2k+1$ and $x = 2l+1$, $x^2 - a = 4k^2 + 4k - 4l^2 - 4l$ is always divisible by 2.

b) Suppose $x^2 \equiv a \pmod 4$, then as square of an odd integer is of the form $4k+1$, a must be of the same form, that is $a \equiv 1 \pmod 4$.

Conversely, suppose $a \equiv 1 \pmod 4$ then there are two solutions modulo 4, namely, $x = 1$ and $x = 3$.

c) We know that square of an odd integer is congruent to 1 modulo 8, a must be of the form $8k+1$. Conversely, suppose $a \equiv 1 \pmod 8$, we shall use induction on n. Let $n = 3$, then 1, 3, 5, 7 are solutions of $x^2 \equiv 1 \pmod 8$. Let the result hold for $n = k \geq 1$, then $x^2 \equiv a \pmod{2^k}$ admits a solution x_0, that is, $x_0^2 = a + b2^k$ for some integers b. Since a is odd, so does x_0. Therefore, $x_0 y \equiv -b \pmod 2$ admits a unique solution y_0.

Consider $x_1 = x_0 + y_0 2^{k-1}$ and

$$\begin{aligned} x_1^2 &= x_0^2 + 2x_0 y_0 2^{k-1} + y_0^2 2^{2k-2} \\ &= a + b \cdot 2^k + x_0 y_0 2^k + y_0^2 2^{2k-2} \\ &= a + (b + x_0 y_0) 2^k + y_0^2 \cdot 2^{2k-2}. \end{aligned}$$

Since $2 / x_0 y_0 + b$ we have

$$x_1^2 \equiv a \pmod{2^{k+1}}.$$

Note that $2k - 2 = k + 1 + k - 3 \geq k + 1$.

Thus the result holds for $n = k+1$. Therefore, by principle of induction, the result holds for any n.

Theorem : Let $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \ldots . p_r^{k_r}$ be the prime factorization of $n > 1$ and let $\gcd(a, n) = 1$. Then $x^2 \equiv a \pmod{n}$ is solvable if and only if

a) $\left(\frac{a}{p_i}\right) = 1$ for $i = 1, 2, \ldots, r$

b) $a \equiv 1 \pmod{4}$ if $4 \mid n$, but $8 \nmid n$; $a \equiv 1 \pmod{8}$ if $8 \mid n$.

Proof : Observe that the problem of solving quadratic congruence $x^2 \equiv a \pmod{n}$ is equivalent to that of solving system of congruences.

$$x^2 \equiv a \pmod{2^{k_0}}$$
$$x^2 \equiv a \pmod{p_1^{k_1}}$$
$$x^2 \equiv a \pmod{p_2^{k_2}}$$
$$\vdots$$
$$x^2 \equiv a \pmod{p_r^{k_r}}$$

In view of last two results, the result follows.

Example : Show that 7 and 18 are the only incongruent solution of $x^2 \equiv -1 \pmod{5^2}$.

Solution : Consider $x^2 \equiv -1 \pmod{5}$. Clearly, $x_0 = 2$ is a solution of this quadratic congruence. Observe that $x_0^2 = 4 = -1 + (1)5$ so that $b = 1$ and consider the congruence $2x_0 y \equiv -b \pmod{5}$, that is,

$$2(2)\, y \equiv -1 \pmod{5} \Rightarrow 4y \equiv -1 \pmod{5}$$

Clearly, unique solution of this congruence is $y_0 = 1$.

Thus, $x_1 = x_0 + y_0 p = 2 + (1) \cdot 5 = 7$ is a solution of $x^2 \equiv -1 \pmod{5^2}$.

Moreover, $-7 \equiv 18 \pmod{5^2}$ is the only other solution.

Example 2 : Using above example solve $x^2 \equiv -1 \pmod{5^3}$.

Solution : We know from above example that $x_0 = 7$ is a solution of $x^2 \equiv -1 \pmod{5^2}$. With this we proceed to next step $x_0^2 = a + b \cdot 5^2 \Rightarrow 49 = (-1) + 2 \times 5^2$ so that $b = 2$. Now

consider $2x_0 y \equiv -b \pmod{5^2}$, that is, $14y \equiv -2 \pmod{5^2}$. Here $y_0 = 7$ is a solution of $14y \equiv -2 \pmod{5^2}$. Thus $x_1 = x_0 + y_0 p^k = 7 + 7 \cdot 5^2 = 182$.

Thus $57 \equiv 182 \pmod{125}$ and $-68 \equiv 182 \pmod{125}$ are solutions of $x^2 \equiv -1 \pmod{125}$.

In fact 57 and 68 are the only incongruent solutions of $x^2 \equiv -1 \pmod{125}$.

EXERCISE :

1. Solve $x^2 \equiv 7 \pmod{3^3}$
2. Solve $x^2 \equiv 31 \pmod{11^4}$
3. Solve $x^2 \equiv 1 \pmod{2^5}$
4. Solve $x^2 + 5x + 6 \equiv 0 \pmod{5^3}$

Answer :

1. $x \equiv 13, 14 \pmod{3^3}$
2. $x \equiv 5008, 9633 \pmod{11^4}$
3. $1,\ -1,\ 1+2^4,\ -1+2^4$
4. $x \equiv 122, 123 \pmod{5^3}$

REFERENCES:

1. David M. Burton, Elementary Number Theory, Tata McGraw Hill Education Private Limites, New Delhi, Sixth Edition(2011).
2. Ajay Kr Chaudhary, Introduction to Number Theory, New Central Book Agency (P) Ltd. Delhi, Kolkata, Pune, Ernakulam.