**Unit-1**

**Mathematical induction**

**Mathematical induction**

Induction means the inference of general law from particular instances.

OR

Mathematical induction means of proving a theorem by showing that it is true of any particular case, it is true of the next cases in a series and then showing that it is indeed true in one particular case.

**Working procedure of mathematical induction**

Let p (n) be a statement of a theorem for all n ϵ N. Then,

1. Verify the result is true for n = 1.
2. Suppose that the result is true for n = k.
3. Show that the result is true for n = k + 1.

Thus, p (n) is true for all n ϵ N

1. **Prove the statement by using mathematical induction : 2 + 4 + 6 + ……. + 2n = +n, Ɐ n ϵ N**

Proof :- Let p (n) = 2 + 4 + 6 + …….. + 2n = + n.

If n = 1, then, p (1) = 2 = + 1

Since the statement is true for n = 1. Let us assume that the given statement is true for n = k

I.e. p (k) = 2 + 4 + 6 + ……..+ 2k = + k.

Now we have to prove that it is true for n = k + 1.

I.e. p (k +1) is true.

Now, P (k + 1) = 2 + 4 + 6 +……… + 2k + 2 (k +1)

= +k + 2k +2

=( + 2k + 1) + (k + 1)

= + (k + 1), which is true for n = k + 1.

So, the theorem is true for n = 1. It is also true for n = k. Then, it is concluded true for n = k +1. Hence it is true for all n.

Proved

1. **Prove the statement by mathematical induction for every natural number n the proposition p (n) = + + + ………… + = .**

Proof:- Here the given proposition is p (n) = + + + ………… + = .

If n = 1, then, p (1) = = 1 = .

The proposition is true for n = 1. Let us assume that the proposition is true for n = k

I.e. p (k) = + + + ………… + =.

Now we have to show that the proposition is true for n = k + 1.

I.e. p (k +1) is true.

Now, p (k +1) = + + + ………… + +

= +

= (k + 1) [ + (k + 1)]

= [2 + k +6k +6]

=

=

=

=

= , which is true for n = k + 1.

So, the proposition is true for n = 1. It is also true for n = k. It is concluded true for n = k +1. Hence it is true for all n.

Proved

1. **By using mathematical induction to show that - 1 isdivisible by 24.**

Proof : Let p (n) = - 1

If n = 1, then, p (1) = - 1

= -1

= 25 – 1

= 24

So, 24is divisible by 24. Which implies that the statement is true for n = 1.

Let us assume that the statement is true for n = k

I.e. p (k) = -1 is divisible by 24.

Then, – 1 = 24m for some m

i.e. = 24m +1

Now, we have to show that the statement is true for n = k + 1

i.e. p (k + 1) is divisible by 24.

Now, p (k + 1) = – 1

= . - 1

= ( 24m + 1) . - 1

= 24m . + - 1

= 600m + 24

= 24 (25m + 1) which is divisible by 24.

So, the statement is true for n = 1. It is also true for n = k. It is concluded true for n = k + 1. Hence, the statement is true for all n.

Proved

1. **Let S(n) = (1- )(1 - )…….(1 - ). Prove the statement p(n) : S(n) = by mathematical induction.**

Proof : Let p(n) : S(n) = (1 - )(1 - ) …….(1 - ) =

If n = 1, then, p(1): S(1) = 1 - = =

So, the statement is true for n = 1.

Let us assumethat the statement is true for n = k

I.e. p(k): S(k) = (1 - )(1 - ) …….(1 - ) =

Now we have toshow that the statement is true for n = k +1

I.e. p(k +1) : S(k +1) is true.

Now, p(k +1): S(k +1) = (1 - )(1 - ) …….(1 - )

= (1 - )

= x

= x

=

= which is true for n = k + 1.

So, the statement is true for n = 1. It is also true for n = k. then, it is concluded true for n = k + 1. Hence, the theorem is true for all n.

Proved

**Binomial Expression**

Binomial expression is an expression consisting of two terms.

Eg. X +1, x + a, x + y are all binomial expression.

**Factorial notation**

1. n! = n (n – 1) (n – 2)…….3.2.1
2. 5! = 5.4.3.2.1 = 120

**Permutation**

The arrangement or selection of objects with some order is called permutation.

Eg. Arrangement of three letters A, B, and C are as follows:

1. ABC
2. BCA
3. CAB
4. ACB
5. BAC
6. CAB

So, three letters A, B, C are arranged by 6 ways.

**Formula of permutation**

1. P (n, r) =
2. P (n, r) = (repeated permutation)
3. P (n, r) =(n -1)! (circular permutation)

**Combination**

The selection of objects without order is called combination.

From above example of permutation, three letters A, B, C arranged in 6 ways, but there are same selections of letter A, B, C. So selection of three letters is one ways. Hence, combination of three latter taken from three letters is one ways.

**Formula of combination**

1. C (n, r) =

**Prove that C (n, r) + C (n, r-1) = C (n+1, r), 1≤k≤n**

Proof: we know that C (n, r) = ……… (1)

C (n, r-1) = ........................ (2)

Adding (1) and (2), we get

C (n, r) + C (n, r-1) = +

= +

= [ + ]

= [ ]

= [ ]

=

=

= C (n+1, r)

Hence, C (n, r) + C (n, r-1) = C (n+1, r), 1≤k≤ n

Proved //

Binomial Expansion

* = 1
* = a + b = c ( 1, 0)a + c (1, 1)b
* =+ 2ab + = c (2, 0) + c (2, 1)ab + c(2, 2)
* = + 3b + 3a+

= c(3, 0) + c(3, 1)b + c(3, 2)a + c(3, 3)

……………………………………………………………..

……………………………………………………………..

……………………………………………………………..

* = c(n, 0) + c( n, 1) b + c(n, 2) + …………+ c(n, r) + ………..+ c(n, n)…….(i)

**Expansion of**

Put b = x in equation (i),

= c(n, 0) + c( n, 1) + c(n, 2) + …………+ c(n, r) + ………..+ c(n, n) …….(ii)

**Expansion of and**

Put a = 1 in (ii), we get,

1. = c(n, 0) + c( n, 1) + c(n, 2) + …………+ c(n, r) + ………..+ c(n, n)

= c(n, 0) + c( n, 1) + c(n, 2) + …………+ c(n, r) + ………..+ c(n, n) ……..(iii)

= 1 + n + + …………+ + ………..+ …….. (iv)

Replacing x by –x in (iii), we get,

1. = 1 - n + + ……+ …….. (v)

**Binomials coefficients**

We have,

= c(n, 0) + c( n, 1) + c(n, 2) + ………+ c(n, r) + ………..+ c(n, n)……. (vi)

Put x = 1 I n (vi), we get,

= c(n, 0) + c( n, 1) + c(n, 2) + ………+ c(n, r) + ………..+c(n, n)

**= + + + ………+ = sum of binomial coefficients**

Again put x = -1 in (vi)

= c(n, 0) + c( n, 1)(-1) + c(n, 2) + ………………+ c(n, r) + ………..+ c(n, n)

0 = - + - + ………+

**i.e. + + + ……… = + + + ………**

**Note:**

1. = + + + ………+

+ + ………+ = -

+ + ………+ = – 1

1. + + + ……… = + + + ……… =

**General term of**

1. First term = = c(n, 0)
2. Second term = = c(n, 1)x
3. Third term = = c(n, 2)
4. term = = c(n, r) ( general term )

**Middle term of**

1. If n is even. Then, there is odd no. of term in the expansion. So there is only one middle term.

Middle term = = c(n, )

1. If n is odd. Then, there is even no. of term in the expansion. So there will be two middle terms.

Middle term = = c(n, )

Middle term = = c(n, )

**Pascal’s Triangle**

Pascal’s triangle is given as follows

1n = 0

1 1 n = 1

1 2 1 n = 2

1 3 3 1n = 3

1 4 6 4 1n = 4

Expansion of by using Pascal’s triangle

= +4x + 6 + 4 +

1. **Find the expansion of by using binomial theorem.**

**Solution:**

= c(5, 0) + c(5, 1).3 + c(5, 2) + c(5, 3) + c(5, 4) + c(5, 5)

# = 32 +× × + × × 9+ × × 27 + × 2x × 81 + [ c(5, 0) = 1 = c(5, 5) ]

# = + × + × +× + × +

# = +2 + + + + ans

1. **Find the term of (.**

Solution:Let term is the general term of the expansion of

= c(12, r) ……(i)

Now, for term, r + 1 = 10 r = 10 – 1 r = 9

Using r = 9 on (i), we get

= c (12, 9)

=

=

= × 8 ×

= ans

1. **Find the coefficient of in the expansion of**

Solution: Let term is the general term of the expansion of

= c (9, r) …… (i)

Now, for coefficient of,we get, 9 – r = 6 or, r = 3

So, = c (9, 3)

=

=

= 84

The coefficient of in the expansion of is 84. Ans

1. **Find the general term in the expansion of**.

Solution: Let term is the general term of the expansion of

= c (n, r)

= c (n, r)

# = c (n, r)

1. **Find the middle term in the expansion of**.

Solution: Here n = 6, which is even. So, there is only one middle term in the expansion of.

i.e., =

=

= c (6, 3)

=

= ×27

= 540 ans

1. Find the middle term in the expansion of.

Solution: Here n = 11, which is odd. So, there are two middle terms in the expansion of.

1. == = = c(11, 5)

= × = = - 462 ans

1. = = = c(11, 6)

= × = = 462 ans

1. **Find the term free (or independent) from x in the expansion of**.

Solution: Let be the term of free (or independent) of x.

Then, = c (12, r) = c (12, r)

= c (12, r) = c (12, r) ….. (i)

For the term free (or independent) of x,

12 – 3r = 0 3r = 12 r = 4

The term of free (or independent) of x is i.e. term.

Its value is = = c (12, 4)=

= = ans

1. **Prove that for n 1, C (2n, n) =**

Proof: LHS = c (2n, n)

=

=

=

=

=

= RHS

proved

**unit-II**

**Divisibility theory**

**Divisibility of integer:**

An integer b is said to be divisible by an integer a 0, if there exists an integer c such that b = ac. It is denoted by a|b. If b is not divisible by a then we can write ab.

**Properties:**

* a|o, 1|a and a|a
* a|b and b|a iff a = b
* If a|b and c|dthen ac|bd
* If a|b and a|c then a|bx + cy for some x, y
* If a|b and a|c then a|bc
* If a|b and b 0 then |a| |b|

**Theorem: For a, b, c Z, a|b and a|c then a|bx + cy Ɐ x, y ϵ Z**

Proof: since a|b then p ϵ Z such that b = pa

and**a**|c then q ϵ Z such that c = qa

Now, bx +cy = pax + qay = a(px + qy)

Since, px + qy ϵ z, so, a|bx + cy Ɐ x, y ϵZ.

Proved

**Theorem: a, b ϵ Z if a|b and b 0 then |a| |b|**

Proof: Given that a|b then for some x ϵ Z, b = ax and since b 0, we have x 0, hence |x| 1

Now, b = ax |b| = |ax| |b| = |a||x| ……….. (i)

Again, |a| ≤ |a||x| because |x| 1 …….. (ii)

From (i) and (ii), we get

|a| ≤ |b|

Proved

**Division algorithm: Given integers a and b with b 0, there exists unique q and r satisfying a = qb + r, 0 ≤ r b. The integers q and r respectively called quotient and reminder in the division of a by b.**

Proof: Let a and b are any two integers such that b 0, let us consider the set of integers are { ……. -3b, -2b, -b, 0, b, 2b, 3b, ……. }.

By Archimedean property, bq ≤ a≤ b(q +1) …….. (i)

Subtract bq on both sides of (i), we get

0 ≤ a –bq ≤ b

0 ≤ r≤ b where r = a –bq a = bq + r

Again, q, , r and are integers such that a = bq + r and a = b +

Then, a = bq + r = b + for 0 ≤ r, < b

bq -b= - r

b(q -)= -r

(q - ) =

b|()

Since r and are less than b but b|( - r). So, the number ( - r) must be zero.

- r = 0 r =

By this, bq + r = b +

bq + r = b + r

bq = b

q =

Hence, q and r are unique integers. This completes the proof of the theorem.

**Common divisor:**

If a and b be two arbitrary integers then an integer d is said to be a common divisor of integers a and b if d|a and d|b.

**Greatest common divisor (GCD)**

A positive integer d is said to be greatest common divisor of given two integers a and b if d satisfies the following:

1. d|a and d|b
2. If c|a and c|b then c ≤ d.

Examples: Find the GCD of 12 and 18.

Solution: The positive divisors of 12 are 1, 2, 3, 4, 6, 12 and the positive divisors of 18 are 1, 2, 3, 6, 9, 18.

Hence the positive common divisors of 12 and 18 are 1, 2, 3 and 6.

So, gcd(12, 18) = 6

**Theorem: given integer a and b both of which are non zero, x, y Z such that gcd(a, b) = ax + by.**

Proof: consider the non empty set of all positive linear combination of a and b such that S = { a + b: a + b> 0 where , Z}

Let us choose x and y such that ax + by will give a least positive integer d in the set s. thus ax + by = d. Now, we can write gcd(a, b) = d for this we have to show that d|a and d|b.

If possible, suppose that da. Thus by division algorithm q, r Z such that a = dq + r, 0≤ r< d.

Thus r = a – dq = a –q(ax + by) =a(1-qx) +b(-qy)

Hence r S, s0 d cannot be a least positive integer since r < d. which is contradiction so we must have d|a. By same process, we can show d|b.

Now, if c is an arbitrary common positive divisor of a and b. Then we can write, c|a and c|b. It follows that c|ax + by, i.e. c|d. where d = ax +by and we know that c ≤ d. so that d is greater than every positive common divisor of a and b.

So, gcd(a, b) = d= ax + by .

Proved

**Relatively prime integers:**

If a and b are any two integers such that at least one of which is non-zero, then a and b are said to be relatively prime if gcd(a, b) = 1.

**Theorem: let a and b be integers not both zero. Then a and b are relatively prime iff x, y Z such that ax + by = 1.**

Proof: let a and b are relatively prime, then gcd(a, b) = 1 and for the given integer a and b x, y Z such that gcd(a, b) = ax + by.

Which implies that ax + by = 1.

Conversely, if ax + by = 1, then we have to show that a and b are relatively prime. Let gcd(a, b) = d

d|a and d|b d| ax +by for x,y Z d|1 d = 1

Hence, gcd(a, b) = 1, therefore a and b are relatively prime.

**Theorem: if gcd(a, b) = d then gcd( , ) = 1.**

Proof: since gcd(a, b) = d it can expressed as the linear combination of a and b such that d = ax + by for any x, y Z.

Dividing both sides by d, we get 1 = x + y

Since and are integer with gcd(a, b) = d then for any a, b Z and a 0, b 0.

If 1 = x + y, then we can write gcd( , ) = 1.

gcd( , ) = 1

**Euclid lemma: If a|bc with gcd(a, b) = 1 then a|c.**

Proof: since a|ac and a|bc. Then we can write a| acx + bcy

a| c(ax + by) …… (i)

Since gcd(a, b) = 1 so there exists x, y Z such that ax + by = 1 …. (ii)

From (i) and (ii),

We get a|c

**Theorem: Let a, b be integers not both zero for a positive integer d, d = gcd(a, b) iff (i) d|a and d|b (ii) whenever c|a and c|b then c|d.**

Proof: since gcd(a, b) = d then d|a and d|b

If a and b are integers, a 0, b 0 then x, y Z such that gcd(a, b) = ax + by. Thus, if c|a and c|b then c|ax + by c|d

Conversely, let d|a and d|b. Let c|a and c|b then c|d implies that c ≤ d because d > 0. Hence gcd(a, b) = d

**Lemma: If a = qb + r then gcd(a, b) = gcd(b, r).**

Proof: Let gcd(a, b) = d

d|a and d|b d|a – qb d|r

So, we have d|b and d|r.

Hence d is a common divisor of both b and r.

If c is an arbitrary common divisor of b and r. then c|b and c|r

c|qb + r c|a This shows that c is common divisor of a and b. Hence c ≤ d. Then by definition it follows that d = gcd(b, r)

gcd(a, b) = gcd(b, r)

**Euclidean algorithm:**

**Given integers b and c > 0, we have a repeated application of division algorithm, we obtain a series of equations**

**b = c + , 0 ≤ <c …… (1)**

**c = + , 0 ≤ < …… (2)**

**= + , 0 ≤ < …… (3)**

**………………………………**

**…………………………………**

**= + , 0 ≤ < …… (n-1) and**

**= + 0 ……….…… (n)**

**The greatest common divisor of b and c is . The least non-zero remainder in the division process is equal to the gcd(b, c) and can be expressed as the linear combination of and i.e. gcd(b, c) = b +c.**

Proof: The chain of equation is obtained by dividing b by c, c by; by; ….. ; by **.** This process ends when the remainderbecomes zero if the division is exact.If not exact we write 0 <<c in stead of 0 ≤ <c.

If = 0 the chain stop and c becomes gcd of b and c.

We have to prove that gcd(b, c) = gcd(c, r) for c =qb + r

So, gcd(b, c) = gcd(c, ) = gcd(, ) = ……. = gcd(, 0) =

We have to show that is a linear combination of b and c.

From given equation, = -

Also from algorithm, = -

= - ( - )

# = +( - )

This represents as linear combination of and .

Continuing backward through system of equations, we eliminate remainders , , …. , until we reached to the stage = gcd(b, c) is expressed as a linear combination of b and c . so we can write

= b +c

**Theorem: If k > 0, then gcd(ka, kb) = |k| gcd(a, b).**

Proof: we know that the equation of Euclidean algorithm multiplying by k, then we get,

ak = + k , 0 ≤ k < bk …… (1)

bk = k + k , 0 ≤ k<k …… (2)

………………………………

…………………………………

k = k + k, 0 ≤ k<k …… (n-1) and

k = k+ 0 ……….…… (n)

# By Euclidean algorithm, gcd(ak, bk) = k = k = k gcd(a, b).

# Examples: find the gcd(427, 616) and express it in terms of 427x + 616y.

Solution: we have, by using division algorithm,

616 = 1. 427 + 189

427 = 2. 189 + 49

189 = 3.49 + 42

49 = 1. 42 + 7

42 = 7. 6 + 0

We have, = 7 (least / last non-zero remainder)

gcd(616, 427) = 7

Now, we can express 7 on linear combination of 616 and 427.

We have,

7 = 49 – 1. 42

= 49 –[189 – 3. 49]

= 4. 49 – 189

= 4.[427 – 2. 189] – 189

= 4. 427 -9. 189

= 4. 427 – 9. [616 – 1.427]

= 13 . 427– 9. 616

= 427x + 616y where x= 13 and y = -9

gcd(616, 427) = 7 = 427x + 616y ans

# Examples: find the gcd(24, 138) and express it in terms of 24x + 138y.

# Solution: we have, by using division algorithm,

# 138 = 5. 24 + 18

24 = 1. 18 + 6

18 = 6. 3

We have, = 6 (least / last non-zero remainder)

gcd(24, 138) = 6

Now, we can express 6 on linear combination of 24 and 138.

We have,

6 = 24 – 1. 18

=24 – 1. (138 – 5. 24)

= 6. 24 – 1.138

= 24x + 138y where x = 6 and y = -1

# gcd(24, 138) = 6 = 24x + 138y ans

# Least common multiple (LCM):

The positive integer m is said to be the LCM of integer a and b if it satisfies the following.

1. a|m and b|m
2. If a|c and b|c wuth c > 0 then m ≤ c

Examples: Find the LCM of 6 and 8.

Solution:

The multiples of 6 is = {6, 12, 18, 24, 30, 36, 42, 48, ……}

The multiples of 8 is = {8, 16, 24, 32, 40, 48, ……}

The common multiples of 6 and 8 are = = {24, 48, ….. }

The least common multiple of 6 and 8 is 24.

LCM = 24 ans

**Theorem: For positive integers a and b; gcd(a, b).LCM(a, b) = a.b**

Proof: Let gcd(a, b) = d d|a and d|b

a = dr and b = ds for some r, s Z

If m = then m = = a.s and m = = b.r a|m and b|m

Let, c be any positive integer and is common multiple of a and b

i.e. c = av and c = bu

since gcd(a, b) = d then x, y such that d = ax + by

Now, = = = = = x + y = ux + vy

i.e. = ux + vy m|c

so, we conclude that m ≤ c.

Then by definition, LCM(a, b) = m = =

LCM(a, b).gcd(a, b) = a.b

**Diophantine equation:**

The equation in which we wish to find the solutions of such equations with integral values of variables is known as Diophantine equations.

**Theorem: The linear Diophantine equation ax + by = c has a solution iff d|c where d = gcd(a, b). If and is particular solution of this equation then all other equations are given by x = + t and y = - t for t Z.**

Proof: Let the Diophantine equation ax + by = c has a solution iff d|c where d = gcd(a, b). we know r, s Z, such that a = dr and b = ds. If the solution of ax + by = c exists.

So that a + b = c for some and

Then, c = a + b = dr + ds = d(r + s)

d|c

Conversely, assume that d|c c = dt

The integers and satisfies d = a + b .

Multiplying the relation by t, then, c = dt =t(a + b) = a(t) + b(t).

Hence the Diophantine equation ax + by = c has x = t and y = t as a particular solution.

Let us suppose and is any other solution of equation other than , . Then a + b = c = a + b a - a = b - b

a( - ) = b( - ) ……… (i)

Suppose there exists relatively prime integer r and s such that a = dr and b = ds. On substitution of value of a and b in (i), we get

dr( - ) =ds( - ) r( - ) =s( - ) r| s( - ) with gcd(r, s) = 1 then r|( - ) - = r.t for some t Z

Similarly s| r( - ) s|( - ) - = s.t for some t Z.

= + s.t and = - r.t

x = + t and y = - t

These values of and satisfies the equation a + b = c

i.e. a + b = a( + t) + b( - t) = a + t + b - t = a + b = c

Hence, there is an infinite number of solutions of the linear Diophantine equation for each values of t.

**Examples: find the solutions of linear Diophantine equation 56x + 72y = 40.**

Solution: we have to find gcd of 56 and 72 by using Euclidean algorithm

72 = 1. 56 +16

56 =3. 16 +8

16 = 2. 8 + 0

We have, = 8 (least / last non-zero remainder)

gcd(56, 72) = 8

Now, we can express 8 on linear combination of 56 and 72.

We have, 8 = 56 – 3. 16

= 56 – 3.(72 – 1. 56)

= 4. 56 – 3. 72

8 = 4. 56 + (-3). 72 …….. (i)

Multiplying both sides of (i) by 5, we get

40 = 20. 56 + (-15). 72

So that, = 20 and = -15 is the particular solution to given Diophantine equation. The other solution are given by

x = + t = 20 + t = 20 + 9t

and y = - t = -15 - t = -15 – 7t, for some t Z.

**prime number and composite number**

An integer p > 1 is called a prime number if its positive divisors are only 1 and p.

A number which is greater than 1 and not a prime number is called composite number.

**Even and odd number**

An integer a is said to be even number if there exists a natural number k such that a = 2k.

An integer a is said to be odd number if there exists a natural number k such that a = 2k + 1.

An integer a is said to be square number if there exists a natural number k such that a = 3k or 3k + 1.

An integer a is said to be cubic number if there exists a natural number k such that a = 9k, 9k + 1 or 9k + 8.

An integer a is said to be fourth power number if there exists a natural number k such that a = 5k or 5k + 1.

**Theorem: if p is prime and p|ab then p|a or p|b.**

Proof: let p is prime and p|ab. If p|a then, there is nothing to prove. Let pa. since p and I are only positive divisors of p,this implies that gcd(a, p) = 1 i.e. p and a are relatively prime. We have p|ab and gcd(a, p) = 1. Hence, by Euclid lemma p|b.

**Theorem: If p is prime and p|……, then p| for some k where 1 ≤ k < n.**

Proof: we prove this theorem by mathematical induction. For n = 1the result is obviously holds. If n = 2 then we have p| p| or p|, we assume that the statement is true for n > 2 and less than n.

Now, if p|…… i.e. p|c where c = ……. Then, p| or p|c

If p|c then by induction we can write p| for some k.

**Fundamental theorem of algebra:**

**Every positive integer n > 1 can be expressed as a product of primes. This representation is unique apart from the older in which the factors occur.**

Proof: Let n may be prime or composite. If n is prime then there is nothing to prove. Let n is composite then there exists an integer d such that d|nwhere 1 < d < n. among all such integers d, let us choose is a smallest integer. Then must be prime. If not it is composite,then it would have adivisor q such that q| and |n. this implies q|n, so this contradicts that is a smallest integer. Hence must be a prime. Then we can write n = where is a prime and 1<<n. If is also prime then we get required solution. If is composite then there exists and such that = where is prime and we have n = = , 1 <<. If is prime then we get solution. If not we can write = and is prime , 1 <<n =

The decreasing sequence n >>> …… > 1 must after finite number of step is prime This leads to a factorization of n as n =

For uniqueness:

Let us assume that the integer n can be improved as a product of primes in two ways n = and n = , r ≤ s

n = = where and are all primes written in increasing magnitude so that and

Since | = for some k.

But, and similarly

= we can write

=

=

On repeating same process we get =

=

On continuing process =

1 = which is impossible since > 1 hence r = s and = for i = 1, 2, … , n. Hence the representation is unique.

**Theorem: prove that is irrational number.**

Proof: here, the given number is . Let us assume that is rational number.

Then, = where gcd(p, q) = 1

5 = 5 = = …… (1)

5| 5|p

There exists an integer r such that p = 5r and put the value of p in equation (i), we get

= = = 5 = 5| 5|q

There exists an integer t such that q = 5t

gcd(p, q) = 5 which contradicts the gcd(p, q) = 1.

So our assumption is wrong. So, is irrational number.

**Theorem: there are an infinite number of primes.**

Proof: If possible suppose that, , …… ,be the finite number of primes. Consider an integer N = ….. + 1.

Since N > 1 and N is divisible by some primes ; 1 ≤ i ≤ k. since and |….. then |[N - …..]|1, which is impossible and our assumption is wrong. Hence, there is infinite number of primes.

**Theorem: the product of two or more integers of the form 4n + 1 of the same form.**

Proof: It is sufficient to show that the product of just two integers. Let k = 4n + 1 and = 4m + 1 be two integers.

Then, k. = (4n + 1)( 4m + 1)

= 16mn + 4n + 4m + 1

= 4(4mn + n + m) + 1

=4N + 1 where N = 4mn + n + m

So, it is also of form 4n + 1.

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

**Theorem: There are an infinite number of primes of the form 4n + 3**.

Proof: If possible suppose there are only finite number of primes of the form 4n + 3. Let us say them ……. Consider a positive integer N such that, N = 4(……) – 1

= 4(……) – 4 + 3

= 4(…… - 1) + 3

Let N =…… be its prime factorization. Since N is an odd integer.

We have 2. So that, each is either of the form 4n + 1 or 4n + 3.

Also we have the product of the primes of the form 4n + 1 is again of the same form. To express N as the form 4n + 3. N must contain at least one positive factor of the form 4n + 3. But cannot be found among the above ……which is contradiction. Hence there is an infinite number of prime of the form 4n + 3.

**Theorem: If is the prime number then ≤ .**

Proof: we use induction on n.

If n = 1 then ≤ = = = 2

The theorem is true for n = 1

Let us assume that the theorem is true for n = k i.e. ≤

Then we have to show that it is true for n = k + 1

Now, ≤ …… + 1

≤ 2. . …… + 1

= + 1

= + 1

≤ +

= 2.

=

= , which is true for n = k + 1.

Hence the theorem is true for all n.

**Goldbach conjecture:**

Every even integer except 2 can be represented as the sum of two primes or 1.

Examples: 4 = 2 + 2 = 1 + 3

8 = 3 + 5 = 1 + 7

**Twin primes:**

A twin prime is a prime number that has a prime gap of two.

Examples:

1. 3 and 5 is a twin prime.
2. 41 and 43 is a twin prime.

**Unit – iii**

**Theory of congruence**

**a is congruent to b modulo n**

let nbe an integer. Two integers a and b are said to be congruent modulo n (a is congruent to b modulo n) if n|a-b and denoted by a b(modn).

If n then a is incongruent to b modulo n and denoted by ab.

Examples:

* 327(mod8) because 8|27-3 i.e. 8|24
* 219(mod9) because 919-2 i.e. 9.

**Note:**

* Since 1|a-b then a and b are congruent modulo 1.
* If any two integers are modulo 2 then either both odd or even.

**Theorem: Let n be non-zero integer then a b(modn) iff a and b have the same non negative remainder when divided by n.**

Proof: since a b(modn) n|a-b a – b = kn, k Z a = b + kn. Dividing b by n, b leaves a certain remainder r, i.e. b = qn + r, 0 r < n

Therefore, a = b + kn

= qn + r + kn

= (q + k)n + r

This shows that a leaves same remainder r when divided by n.

Conversely, if a and b have the same non negative remainder when divided by n. Then, a = n + r and b = n + r, 0 r < n.

Now, a – b = (n + r) – (n + r) = n – n = ( – )n n|a-b

a b(modn)

**Properties of congruence**

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

1. **If a a(modn**) **[reflective]**
2. **If a b(modn) then b a(modn) [symmetric]**
3. **If a b(modn) and b c(modn) then a c(modn) [ transitive]**
4. **If a b(modn) and c (modn) then a + c b + d(modn) and ac bd(modn)**
5. **If a b(modn) then a + c b + c(modn) and ac bd(modn)**
6. **If a b(modn) then (modn), for any k**

Proof:

1. For any integer a, we have, a – a = 0 = 0.n n|a- a

a (modn)

1. Since ab(modn) n|a- b a – b = kn, k

Now, b – a = -(a – b) = - (kn) = (-k)n n|b - a

Then by definition, b (modn)

1. Since, a b(modn) n|a- b a – b = n, Z

Again, b (modn) n|b - c b – c = n, Z

Now, a – c = (a – b) + (b – c) = n + n =( + )n

n|a- c, + Z a (modn)

1. Since, a b(modn) n|a- b a – b = n, Z

And c (modn) n|c - d c – d = n, Z

Now, (a – b) + (c – d) = n + n =( + )n

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

n|(a + c) – (b + d), + Z a + c (modn)

Again, ab(modn) n|a- b a – b = n, Z a = b + n

And c (modn) n|c - d c – d = n, Z c = d + n

Now, ac = (b + n)( d + n) = bd + bn + dn +

ac – bd = n(b + d + n|ac – bd ac bd(modn)

1. Since, a b(modn) n|a- b a – b = kn, k Z

Now, a – b + c – c = kn, k Z

(a + c) - (b + c) = kn

n|(a + c) – (b + c), k Z a + c (modn)

Again, ab(modn) n|a- b a – b = kn, k Z

Now, (a – b)c = kn.c, k Z

n|ac – bd ac bc(modn)

1. We use induction on k.

If k = 1, then obviously a b(modn) …… (i)

By induction hypothesis suppose (modn) ….. (ii) is for the k = k-1

Now, (modn)

(modn) which is true for all k.

**Theorem: Ifca cb(modn) then a (mod)where d = gcd(c, n).**

PROOF: IF ca cb(modn) n|ca-cb ca-cb = kn where k Z

c(a-b) = kn …… (i)

We have gcd(c, n) = d

Then there exists relatively prime integers r and s satisfying c = dr, n = ds

Now, substituting the value of c and n in equation (i) we get,

dr(a-b) = k.ds r(a-b) = ks s|r(a-b) and gcd(r, s) = 1, by Euclid Lemma s|a-b b(mods) a (mod).

**Theorem: If ca cb(modn) and gcd(c, n)= 1 then a (modn).**

Proof: IF ca cb(modn) a (mod) where d= gcd(c, n) …… (i)

But given that gcd(c, n) = 1

d = gcd(c, n) = 1

From (i),

ca cb(modn) a (mod)

Hence, ca cb(modn) a (modn)

**Theorem: If ca cb(modp) and pc where p is a prime number then a (modn).**

Proof: IF ca cb(modp) a (mod) where d= gcd(c, p) …… (i)

But given that pc gcd(c, p) = 1

d = gcd(c, p) = 1

From (i),

ca cb(modp) a (mod)

Hence, ca cb(modp) a (modp)

**Theorem: If a b(modn) and m|n then a b(modm).**

Proof: Given, a b(modn) n|a- b a – b = n, Z ….. (i)

Since m|n n = m, Z ….. (ii)

From (i) and (ii),

a – b = m a – b = km, where k =

m|a- b a b(modm)

**Theorem: If a b(modn) and c > 0 then ca b(modn).**

Proof: Given, a b(modn) n|a- b a – b = kn, k Z ….. (i)

c(a – b) = c.kn ca – cb = (cn)k cn|ca- cb

ca b(mod cn).

**Theorem: If a b(modn) and the integer a, b, n are all divisible by d >0 then(mod).**

Proof: Given, a b(modn) n|a- b a – b = kn, k Z ….. (i)

Given that d|a, d|b, d|n there exists x, y, z Z such that a = xd, b = yd and n = zd

From (i), a – b = kn dx – dy = k.dz x – y = kz z|x-y x (modz)

(mod).

**Theorem: If ab cd(modn) and b (modn) with gcd(b, n) = 1 then a c(modn).**

PROOF: IF abcd(modn) n|ab-cd ab-cd = n where Z … (i)

Also b d(modn) n|b-d b-d = n where Z … (ii)

From (i), we have,

ab-cd = n ab-bc + bc - cd = n b(a-c) + c(b – d) = n

b(a-c) + cn = n b(a-c) = n - cn b(a-c) = ( - c)n

n|b(a-c) n|b or n|a-c

But gcd(b, n) = 1 nb

By Euclid Lemma n|a-cc(modn).

**Theorem: if If a b(mod) and a (mod) then b c(modn) where the integer n = gcd(, .**

PROOF: IF a b(mod) |a-b a-b = , where Z … (i)

Also a(mod) |a-c a-c = , where Z … (ii)

Subtracting (i) from (ii), we have,

(a-c)-(a-b) = - b-c = - …. (iii)

Since, gcd(, = n n| and n|= xn, = yn, x, y Z

From (iii), we get,

b-c = - = (- n|b-c, - Z b c(modn).

**Theorem: Let n Z be an integer and n 0 then a b(modn) iff a (modn)where r is remainder when n divides b.**

Proof: Let n and a b(modn) then we have to show that a r(modn)

We have a b(modn) n|a- b a – b = n a = b + n, Z ….. (i)

By division algorithm, for b and n there exists q, r Z such that b = nq + r….. (ii)

From (i) and (ii),

a = nq + n + r a – r = (q + )n n|a- r a (modn)

conversely, suppose a (modn), where r is the remainder upon division by n then we have to show that a (modn). Since r is remainder upon division b by n then b = qn + r with quotient q. i.e. r = b – qn and a (modn) a (modn) a - b 0(modn) n|a- b a b(modn)

**Linear congruence:**

An equation of the form ax b(modn) is called linear congruence.

**Note:** ax b(modn) is solvable iff the Diophantine equation ax – ny = b is solvable.

**Theorem: The linear congruence ax b(modn) has a solution iff d|b where d = gcd(a, n). If d|b, then it has d mutually incongruent solutions modulo n.**

Proof: The given linear congruence ax b(modn) can be written in the form of Diophantine equation ax – ny = b. The congruence is solvable iff the linear Diophantine equation is solvable. The Diophantine equation is solvable iff d|b, where d = gcd(a, n). Thus ax b(modn) is solvable iff d|b.

When d|b the linear Diophantine equation has infinitely many solutions, given by

X = + and y = + , where and are particular solutions.

Hence the linear congruence has infinitely many solutions

X = + ………. (i)

Let= + and = + be two solutions of linear congruence which are congruent modulo n.

So, + + (modn)

(modn)

(, n) = so (|n

(mod d)

d| - which is impossible, hence there are exactly d incongruent classes modules d. Therefore, the linear congruence, when solvable has exactly d incongruent solutions, given by x = + , 0t < d.

* **Solve the linear congruence 25x 15(mod29).**

Solution: we find the gcd of 25 and 29 by Euclidean algorithm

29 = 1.25 + 4

25 = 6.4 + 1

4 = 4.1 + 0

Gcd(25, 29) = 1

Since,gcd(a, n) = gcd(25, 29) = 1 and 1|15. There is exactly one solution, which is incongruent modulo 29.

So, the general solution of linear congruence is given by,

x = + , where is particular solution.

x = +

x = + 29,t = 0, …… (i)

Express gcd as linear combination of 25 and 29

1 = 25 – 6.4 []

= 25 – 6(29 – 1.25)

= 7.25 – 6.29

15 = 105.25 – 90.29

15 = 25 – 29 where, = 105, = 90

From (i),

x = 105 + 29.0mod29 x = 105mod29 x = 18mod29 ans

* **Solve the linear congruence 34x 60(mod98).**

Solution: we find the gcd of 34 and 98 by Euclidean algorithm

98 = 2.34 + 30

34 = 1.30 + 4

30 = 7.4 + 2

4 = 2.2 + 0

Gcd(34, 98) = 2

Since,gcd(a, n) = gcd(34, 98) = 2 and 2|60. There is exactly two solution, which is incongruent modulo 98.

So, the general solution of linear congruence is given by,

x = + , where is particular solution.

x = +

x = + 49, t = 0, 1 …… (i)

Express gcd as linear combination of 34 and 98

2 = 30 – 7.4

= 30 – 7(34 – 1.30)

= 8.30 – 7.34

= 8.(98 – 2.34) – 7.34

= -23.34 + 8.98

60 = -690.34 + 240.98

60 = 34 – 98 where, = -690, = 240

From (i),

At t = 0

x = -690 + 49.0mod98 x = -690mod98 x = -4mod98

x = 94mod98

At t = 0

x = -690 + 49.1mod98 x = -641mod98 x = -53mod98

x = 45mod98 ans

**Fermat’s factorization method:**

* **Factorize 2,15,275 using Fermat’s factorization method.**

Solution: we have n = 2,15,275. Also we have k = 463.97 and < 2,15,275 <. We find x and y in - n = from - 2,15.275 for 464 k = 1,07,638

- 2,15,275 = 21

- 2,15,275 = 950

- 2,15,275 = 1881

- 2,15,275 = 2814

- 2,15,275 = 3749

- 2,15,275 = 4686

- 2,15,275 = 5625 =

Now, - = 2,15,275

2,15,275 = (470 + 75)(470 – 75)

2,15,275 = 445 × 395 ans

**Factorize the following by using Fermat’s factorization method.**

* 73,151
* 161463
* 119143

**Fermat’s little theorem:**

**If p is a prime and p does not divide a then 1(mod p).**

Proof: consider the set of first (p – 1) positive multiples of a.

i.e. a = {a, 2a, 3a, ……. , (p-1)a} ……. (i)

None of these integers are congruent modulo p to any other, nor is any congruent to zero.

If possible let ra sa(mod p) where 1 ≤ r < s ≤ p -1

r s(mod p) which is impossible since r and s are successive integers.

Hence (i) has (p – 1) incongruent multiplies of a. Therefore the above set integers 1a, 2a, 3a, … , (p-1)a must be congruence to one of 1, 2, 3, ….. , (p-1).

Now multiplying all these congruence we get

1a.2a.3a….(p-1)a 1.2.3….(p-1)(mod p)

(p-1)! (p-1)!(mod p)

1(mod p).

**Verification\ illustration of Fermat’s little theorem:**

Let p = 7 and a = 12. The least residuws of 1.12, 2.12, 3.12, 4.12, 5.12, 6.12 modulo 7 are a permutation of integers 1, 2, 3, 4, 5, 6.

So, 1.12.2.12.3.12.4.12.5.12.6.12 1.2.3.4.5.6(mod 7)

6!. 6!(mod 7)

(mod 7)

This verifies the Fermat’s little theorem.

**Theorem: If p is a prime then a(mod p) for any integer a.**

Proof: The Fermat’s little theorem is given by,

1(mod p) ……. (i)

Multiplying (i) by a, we get,

a. a.1(mod p)

a(mod p)

* **Use Fermat’s little theorem to find the remainder when is divided by 17.**

Solution: we have, 24 7 (mod 17)

By Fermat’s little theorem, we know that, 1(mod 17)

1(mod 17) …….. (i)

Now, (mod 17)

(mod 17)

((mod 17)

.7 (mod 17)

.7 (mod 17)

-32.7 (mod 17)

2.7 (mod 17)

14 (mod 17)

The remainder when is divided by 17 is 14.

**Theorem: Let p be a prime and a be any integer such that pa then is an inverse of a in modulo p and the solution of the linear congruence ax b(mod p) is given by x b(mod p).**

Proof: Let p be a prime and a be any integer such that pa then by Fermat’s little theorem, we have,

1(mod p) …… (i)

1(mod p).

is an inverse of a(mod p).

Again, we have the linear congruence ax b(mod p)

x b(mod p)

x b(mod p)

Hence, x b(mod p) is the solution of ax b(mod p).

* **Solve 16x 6(mod 7).**

Solution: By Fermat’s little theorem, we know that, 1(mod 7)

1(mod 7)

16. 1(mod 7) …….. (i)

We got that is an inverse of 16(mod 7).

(mod 7) 32(mod 7) 4(mod 7)

Now, 16x 6(mod 7) x 6(mod 7) x 4.6(mod 7)

x 3(mod 7) which is required solution.

**Invertible (mod n):**

If gcd(a, n) = 1 there is a unique least residue, x such that ax 1(mod n). Then a is said to be invertible and x is called an inverse of a modulo n. It is denote by . If = a then a is said to be self-invertible.

**Theorem: A positive integer a self-invertible modulo p iff a 1(mod p).**

Proof: Let the positive integer a is self-invertible modulo p.

a.1(mod p) a.a 1(mod p) 1(mod p) p| 1 p| (a1)(a+ 1) p| (a – 1) or p|(a + 1)

a 1(mod p) or a -1(mod p) a 1(mod p)

Conversely, suppose a 1(mod p) a 1(mod p) or a -1(mod p)

1(mod p) a.a1(mod p) …. (i)

We know that a.1(mod p) ….. (ii)

From (i) and (ii), we get, a = a is self-invertible modulo p.

**Wilson’s theorem:**

**If p is a prime, then (p-1)! -1(mod p).**

Proof: if p = 2 then (p-1)! = (2-1)! = 1! = 1 -1(mod p = 2)

So, we suppose p > 2, We know that the least positive restudies 1 through p-1 are invertible modulo p. But we know that 1 and p-1 are self-invertible modulo p. So we can group the remaining p-3 residues, 2 through p-2, into pairs of inverses a and b = such that a.b1(mod p).

Thus, 2.3.4…..(p-2) 1(mod p)

Now, (p-1)! = 1.2.3.4……(p-2)(p-1)

1.1(p-1)(mod p)

(p- 1)(mod p)

-1(mod p)

**Converse of Wilson’s theorem:**

**If n is positive integer such that (n-1)! -1(mod n)then n is prime.**

Proof: If possible suppose n is composite. Then n = a.b with 1<a, b<n, since a|n and n|(n-1)!+1. Since 1<a<n we must have a is one of the integers 2 through (p-1). So, a|(n-1)!

Hence a|[(n-1)! +1]-(n-1)! i.e. a|1. Which contradiction to 1<a<n. Therefore n is a prime.

**Verification\illustration of the Wilson’s theorem:**

Let p = 13 then we have integers 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. We can group such integers into 5 pairs of inverses such that

2.7 1(mod 13) 3.9 1(mod 13)

4.10 1(mod 13) 5.8 1(mod 13)

6.11 1(mod 13)

Now, (13 – 1)! = 12! = 1.2.3.4.5.6.7.8.9.10.11.12

1.1.12(mod 13)

12(mod 13)

-1(mod 13)

**Theorem: The quadratic congruence + 1 0(mod p), where p is an odd prime, has a solution iff p 1(mod 4).**

Proof: Let a be any solution of + 1 0(mod p).

So that + 1 0(mod p) -1(mod p). since p<a, by Fermat’s theorem, we have 1(mod p)

The possibility that p = 4k + 3 for some k does not arise.

For, = = = = -1

Hence, 1 -1(mod p) p|1+1 p|2, which is false.

p must be of the form 4k + 1.

We have (p-1)! = 1.2.3…….….. (P-2)(P-1)

And p-1 -1(mod p)

p-2 -2(mod p)

- (mod p)

Arranging these factors,

(p-1)! 1.(p-1).2.(p-2).3.(p-3)…….

1.-1.2.-2.3.-3…….

(mod p)

(mod p)

We assume that p is of the form 4k + 1, then

-1 (mod p)

(mod p)

Hence, satisfies the quadratic congruence + 1 0(mod p)

Hence, the quadratic congruence + 1 0(mod p), where p is an odd prime, has a solution iff p 1(mod 4).

**Unit – iv**

**Euler’s generalizations and its application**

**Euler’s phi-function:**

Let n be a positive integer then the number of positive integers which are less than n and relatively prime to the n is called Euler’s phi-function. It is denoted by (n).

Examples:

1. (1) = 1, since, gcd(2, 1)= 1
2. (2) = 1, since, gcd(2, 1)= 1, gcd(2, 2) 1
3. (6) = 2, since, gcd(6, 1)= 1, gcd(6, 2) 1, gcd(6, 3) 1, gcd(6, 4) 1, gcd(6, 5) = 1, gcd(6, 6) 1
4. (9) = 6, since, gcd(9, 1)= 1, gcd(9, 2) = 1, gcd(9, 3) 1, gcd(9, 4) = 1, gcd(9, 5) = 1, gcd(9, 6) 1, gcd(9, 7) = 1, gcd(9, 8) = 1, gcd(9, 9) 1

**Theorem: A positive integer p is prime iff (p) = p-1.**

Proof: let p be a prime. Then gcd(1, p) = 1, gcd(2, p) = 1, gcd(3, p) = 1, ……. , gcd(p-1, p) = 1 but gcd p1, p) = p 1. Hence, there are p-1 positive integers not greater than p that are relatively prime to p. So (p) = p-1.

Conversely, (p) = p-1. If possible, we let p is not a prime then d|p where 1 < d <p. There are exactly p-1 positive integers less than p and d is one of them and gcd(d, p) 1. Which implies that (p) < p-1, which is a contradiction. Hence, p must be prime.

**Euler’s theorem: Let n be a positive integer and a be any integer with gcd(a, n) = 1 then 1(modn).**

Proof: let , , ……., be the positive integers less than n, (n > 1) and are relatively prime ton. Since gcd(a, n) = 1q. It follows that a, a, a, …… , a are congruent modulo n to , , , …… , in some order then a, a, a, …… , a are congruent not necessarily in order of appearance to , , , …… ,

Then, a(mod n), a(mod n), ………….., a(mod n), where , , ……, are the integers , , ……, in some order.

On taking the product of these (n) congruence, we get,

(a)(a)………(a) (mod n)

…… (mod n)

**.**………… (mod n) ……. (i)

Since, gcd(a, n) = 1 for each i, we have gcd( …… = 1

Dividing both sides of (i) by common factor ……

We get, 1(modn).

**Corollary: Let p be a prime and a be any integer such that pa then 1(modn).**

**Proof:** since p is a prime, then = p – 1.

By Euler’s theorem, we have, 1(modn).

1(modn).

**Theorem: Let n be a positive integer and a be**

**any integer with gcd (a, n) = 1 then is an inverse of a modulo n and the solution of linear congruence ax b(modn) is given by x b(modn).**

Proof: Since gcd(a, n) = 1, by Euler’s theorem we get

1 (mod n)

1(mod n)

is an inverse of a (mod n)

Since, ax b(modn) . axb(mod n)

xb(mod n).

* **Solve the linear congruence 33x 23(mod 13).**

Solution: the solution of 33x 23(mod 13) is x.23(mod 13).

x.23(mod 13)

x. (-3)(mod 13)

x.(-3)(mod 13)

x.(-3)(mod 13)

x(mod 13)

x(mod 13)

x(mod 13)

x(mod 13) which is required solution.

**Theorem: Let p be a prime and n be any positive integer then**

**) = - = (1 - ).**

Proof: We know that ) = number of positive integers less than and relatively prime to .) = number of positive integers less than - number of positive integers less than and not relatively prime to p.

Since the integer that are multiples of p is p, 2p, 3p, …….,()p are not relatively prime to p and they are in number.

Thus, ) = - = (1 - ).

**Theorem: For given integer a, b, c; gcd(a, bc) = 1 iff gcd(a, b) = 1 and gcd(a, c) = 1.**

Proof: suppose gcd(a, bc) = 1. Let gcd(a, b) = d then d|a and d|b d|a and d|bc gcd(a, bc) d. since gcd(a, bc) = 1. So we must have d = 1 i.e. gcd(a, b) = 1 then gcd(a, c) = 1.

Conversely, let gcd(a, b) =1 = gcd(a, c). Suppose gcd(a, bc) = >1 then must have a prime divisor p. since |bc p|bc p|b and p|c.

If p|b then gcd(a, b), p, p|a which is contradiction.

p|c then gcd(a, c) p, which is contradiction. So we must have gcd(a, bc) = 1. i.e. =1.

**Theorem: is multiplicative function.**

Proof: Let m and n be two integers with gcd(m, n) = 1 then we have to show (mn) **= (m).(n).** If m = 1 and n = 1 then obviously we have (1) = 1. The theorem is trivial. Suppose m > 1 and n > 1. Then arranging the integers from 1 to mn in m number of columns and n number of rows we can write

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

Also we know that (mn) is equal to the number of entries in the above array which are relatively prime to mn. Since gcd(qm+r, n) = gcd(r, n), the number of column is relatively prime to m if r is relatively prime to m. So only (m) columns contain integers relatively prime to m and every element in column contains integers relatively prime to m. Then we have to show that there are exactly (n) integers in each of (m) columns which are relatively prime to n i.e. there are altogether (m) .(n) numbers in table which are relatively prime to both m and n.

Let gcd(r, m) = 1. And the entries in column is r, m + r, 2m + r, ……., (n-1)m + r. There are n integers in this sequence and no two are congruent modulo n.

If possible suppose km + r jm + r(mod n) with 0 k < j n.

km jm(mod n) k j(mod n), which is contradiction. So the number in the columns are congruent modulo n to 0, 1, 2, …., n-1 in some order. But if s j(mod n) then, gcd(s, t) = 1 iff gcd(t, n) = 1. This shows that column contains as many integers which are relatively prime to nas in the set {0, 1,2, …., n-1}. So the total numbers of integers in the array relatively prime to both m and n are **(m).(n).**

(mn) = (m).(n).

Hence, is multiplicative function.

**Theorem: Let n = ….. be canonical decomposition of positive integer n then ) = n(1 - ) (1 - ) (1 - )…… (1 - ).**

Proof: we have, ) = …..)

= …..)

= (1 - ) (1 - ) (1 - )…… (1 - )

=…..(1 - ) (1 - ) (1 - )…… (1 - )

= n(1 - ) (1 - ) (1 - )…… (1 - ) where n = …...

**Theorem: For n > 2; ) is an even integer.**

Proof: First suppose that n can be express as the power of 2. Let us consider n = with k 2 then we can write

) = = (1- ) = . =

Since k 2. So we must have is even. Again suppose n cannot be express as the power of 2. Then p|n for some odd prime p. which can be written as n = .m with k 1 and gcd(, m) = 1. Since is multiplicative function.

We can write = = (p -1)

Since, p is odd prime so 2|p-1. Hence (p -1) is even.

**Properties of Euler’s phi-functions:**

**Theorem (Gauss): For each positive integer n 1, n = . When the sum being extended over all positive divisor of n.**

Proof: If d is a positive divisor of n, we put integer m in the set with gcd(m, n) = d i.e. = {m: gcd(m, n) = d; 1 m n}.

We have gcd(m, n) = d iff gcd() = 1. The number of integers in the class is equal to the number of positive integer not exceeding which are relatively prime to . i.e. ) lies in exactly one class

Then n =

Since d denotes all the positive divisor of n.

Hence, n = .

**Theorem: N > 1, the sum of positive integers less than n and relatively prime to n is n**

**Symbolically, n =**

Proof: Let , , ……., be the positive integer less than n and relatively prime to n. Since gcd(a, n) = 1 iff gcd(n-a, n) = 1.

We have, + + …….+ = n- + n- + …….+ n-

+ + …….+ = n – (+ + …….+ )

2(+ + …….+ ) = n

+ + …….+ =

n = .

**Theorem: for any positive integer n; = .**

Proof: By inversion formula F(n) = n = =

= F( = .

**Primitive root of integer:**

Let a is an integer of order modulo n with gcd(a, n) = 1 then a is a primitive root of n.

If 1(mod n) for k < then n has a primitive root.

**Examples: find the primitive root of 7.**

Solution:

We have = 3 (mod 7)

= 2 (mod 7)

= 6 (mod 7)

= 4 (mod 7)

= 5 (mod 7)

= 1 (mod 7)

6 is order of 3 modulo 7.

Also, = 6, so 1(mod 7).

So, 3 is primitive root of 7.

**Theorem: Let gcd(a, n) = 1 and , , ……, be the primitive integer less than n, and relatively prime to n. If a is primitive root of n then a, , ……., are congruent to , , ……, is same order.**

Proof: Since gcd(a, n) = 1 so it holds for all power of a. Hence is congruent modulo n to some one of the a; the number in the set {a, , ……, are incongruent. Thus their power must represent the integers **, , ……,** in same order.

**Corollary: If n has a primitive root, then it has exactly of them.**

Proof: Suppose that a is a primitive root of n, then any other primitive root of n is found among the member of the set {a, , ……, . But the number of power , 1 k which of integer k for which gcd(k, ) = 1. There are such integer. Hence integers are primitive roots of n.

**Lagrange’s theorem:If p is a prime and f(x) =anxn + an-1xn-1 + …… + a00(modp)is a polynomial of degree n 1 with integral coefficient then the congruence f(x) 0(modp) has at most n incongruent solutions modulo p.**

Proof: We use induction on n, the degree of f(x).

If n = 1; then f(x) = a1x + a0. Since the gcd(a, p) = 1, then by linear congruence a1x -a0 (modp) has a unique solution modulo p.

Suppose the theorem is true for the polynomial of degree k-1. Consider the degree of f(x) is k. then either f(x) 0(modp) has no solution or the congruence has at least one solution (say a).

If f(x) is divisible by (x – a) then, f(x) = (x – a)q(x) + r, where q(x) is of degree k – 1 with integral coefficient and r Z.

If x = a we have, 0 f(a) = (a – a)q(a) + r r(modp)

So, f(x) = (x – a)q(x)(modp).

Suppose h is another one incongruent solutions of f(x) 0(modp) then , 0 f(h) = (h – a)q(h)(modp)

Since h – a 0(modp) q(h) 0(modp) i.e. any solution of f(x) 0(modp) which is different from a must satisfy q(x) 0(modp).

Hence by induction f(x) 0(modp) will have no more than k incongruent solution.

**Corollary: If p is a prime number and d|p-1, then the congruence xd – 1 0(modp) has exactly d solution.**

Proof: since, we have for some k; p – 1 = dk

xp-1 – 1 (xd – 1) f(x)

For f(x) xd(k-1) + xd(k-2) + ……. + xd + 1 has integral coefficients of degree d(k-1) = p-1-d. By Lagrange’s theorem, the congruence f(x) 0(mod p) has at most p-1-d solutions.

By Fermat’s theorem, xp-1 -1 0(mod p) has p-1 incongruent solutions 1, 2, ……, p-1.

Now, any solution x = a of xp-1 -1 0(mod p) that is not a solution of f(x) 0(mod p), must satisfy xd -1 0(mod p).

i.e. 0 ap-1 -1 (xd -1)f(a)(mod p) with p < f(a)

p| ad -1 xd -1 0(mod p) must have at least (p-1)-(p-1-d) = d solutions.

Hence, the congruence has no more solution than d.

**Theorem: If p is a prime number and p|ad -1, then there are exactly (d) incongruent integers having order d modulo p.**

**Proof:** let p|ad -1 and (d) be the number of integers k; 1 ≤ k ≤ p-1. Which has orderd modulo p. since each integer between 1 and p-1 has order d for some p|ad -1.

Then, p-1 = **= ……. (i)**

By Gauss theorem, p-1 = **= ……. (ii)**

We have to show that (d) ≤ for each p| ad -1. Given that d be arbitrary divisor of p-1, then there exists either (d) = 0 or (d) > 0.

If (d) = 0 then obviously (d) ≤ .

Suppose (d) > 0 so there exists an integer a of order d. Then the integer a, a2, ……, ad are incongruent modulo p and each of them satisfies xd -1 0(mod p) i.e. 1(mod p)

By Lagrange’s theorem there is no solution. This implies that any integer which has order d modulo p must be congruent one of a, a2, ……., ad. But of that we mentioned powered have order d, namely those ak for which the exponent k has gcd(k, d) = 1 = (d).

Hence, the number of integers having order d modulo p is equal to .

**Quadratic residues and non-residues:**

Let p be an odd prime and gcd(a, p) = 1. If the congruence x2 a(mod p) has a solution, then a is said to be a quadratic residue of p, otherwise a is called a quadratic non-residue of p.

* **Find the quadratic residues and non-residues of 7.**

Solution: we have, p = 7 then

12 1(mod 7) 22 4(mod 7)

32 2(mod 7) 42 2(mod 7)

52 4(mod 7) 62 1(mod 7)

Here, 1, 2, 4 are quadratic residues of 7 and 3, 5, 6 are quadratic non-residues of 7.

**Euler’s criterion: Let p be an odd prime and gcd(a, p) = 1. Then a is a quadratic residue of p iff 1(mod p).**

Proof: Suppose a is a quadratic residue of p. So that x2 a(mod p) admits a solution (say x1**).** Since gcd(a, p) = 1, then gcd(x1, p) = 1. Then by Fermat’s theorem 1(mod p).

Conversely, suppose 1(mod p) holds. Let r be a primitive root of p. then afor some integer k, with 1≤ k≤ p-1.

1(mod p).

Since the order of r (i.e. p-1) must divide the exponent . then we have k is an even integer say k = 2j

i.e. r2jrk a(mod p) making the integer rj a solution of congruence x2 a(mod p). i.e. a is quadratic residue of prime p.

now, if a is an odd prime and gcd(a, p) = 1,

then ( -1)( + 1) = ( 0(mod p).

so, either 1(mod p) or, -1(mod p) not both.

If both holds, then 1 -1(mod p) p|2 which is contradiction that p is an odd integer. Since a quadrqtic non residue of p does not satisfy 1(mod p). it must satisfy -1(mod p). i.e. if a is a quadratic non-residue of p iff -1(mod p).

**The Legendre symbol:**

Let p be an odd prime and gcd(a, p) = 1. The Legendre symbol is denoted by (a/p) and defined by

() or (a/p) =

**Theorem: Let p be an odd prime and a and b be integer with gcd(a, p) = 1 and gcd(b, p) = 1. Then the Legendre symbol has the following properties.**

1. **If a b(mod p) then (a/p) = (b/p)**
2. **(a2/p) = 1**
3. **(a/p) (mod p)**
4. **(ab/p) = (a/p)(b/p)**
5. **(1/p) = 1, (-1/p) =**

Proof:

1. If a b(mod p) then, the congruence x2 a(mod p) and x2 a(mod p) has some solutions. Then x2 a(mod p) and x2 b(mod p) are both solvable or neither have a solution. (a/p) = (b/p).
2. Let a is an integer trivially satisfies the congruence x2 a2(mod p) then (a2/p) 1.
3. Since, p is an odd prime an
4. d gcd(a, p) = 1 then 1(mod p) i.e. (a/p) (mod p).
5. By (3), we have, (ab/p) = = (a/p)(b/p)(mod p).

If possible suppose (ab/p) (a/p) or (ab/p) (b/p)

So, the Legendre symbol takes values 1 and -1. This implies 1 -1(mod p) 2 0(mod p) p|2 which is contradiction that p > 2.

So, (ab/p) = (a/p)(b/p).

1. In (2) if a = 1then obviously, (1/p) = 1

Let a = -1 since (-1/p) and are either 1 or -1 the congruence. (-1/p) (mod p) (-1/p) =

**Theorem: There are infinitely many primes of the form 4k + 1.**

Proof: Let p1,  p2,  p3 ……, pn be the finite number of primes and consider the integer N = (p1p2 p3 …… pn )2 + 1 is an odd prime p with p|N i.e (p1p2 p3 …… pn )2 -1(mod p).

By Legendre symbol, (-1/p) = 1 holds only if p is of the form 4k + 1. Hence p is one of the prime (say pj ) of above set. This implies that p|N-(p1p2 p3 …… pn )2 p|1, which is contradiction. So, our assumption is wrong.

Hence there are infinitely many primes of the form 4k + 1.

**Theorem: If p is an odd prime, then = 0 hence there are precisely quadratic residues and quadratic non residues of p.**

Proof: Suppose r be a primitive root of p. we know that the powers r, r2, ……, rp-1 are just a permutation of integers 1, 2, ……, p-1 for 1 ≤ a ≤ p-1 there exists a unique positive integer k, (1 ≤ k ≤ p-1) such that a rk(mod p). Then by Euler’s criterion

(a/p) = (rk/p)(mod p) (mod p) (-1)k (mod p).

Since r is primitive root of p, -1(mod p).

Also by Legendre symbol (a/p) = (-1)k are equal to 1 or -1.

i.e (a/p) = (-1)k

By adding the Legendre symbols up to p-1,

= = 0

**Theorem: Let p be an odd prime and gcd(a, p) = 1. If n is the number of integers in the set S , S = {a, 2a, 3a, ……., } whose remainders upon division of p exceeds , then (a/p) = .**

Proof: We have gcd(a, p) = 1 and n is the number of integers in the set S, S = {a, 2a, 3a, ……., } whose remainders upon division of p exceeds in S. None of integers is congruent to zero and no two are congruent to each other modulo p. Let r1, r2, ……, rmbe those remainders upon division by p such that 0 < r1< and s1, s2, ……, sn be those remainders such that p > sj>, then m + n = and the remainders r1, r2, ……, rm, p-s1, p-s2, ……, p-snare all positive and less than .

If possible, suppose p - si rj for some I and j then there exists u, v with 1 ≤ u, v ≤ such that si ua (mod p) and rj va (mod p).

Hence (u + v)a si + rj  p 0(mod p)

u + v 0(mod p) since gcd(a, p) = 1.

But, we have 1 < u + v < (p-1). So there are numbers r1, r2, ……, rm, p-s1, p-s2, ……, p-sn are simply the integers 1, 2, ……, with or without order and their product is ()!

So, ()! = r1. r2.……rm, (p-s1)) p-s2) ……(p-sn)

= r1 r2 …… rm, (-s1)(-s2)……(-sn)(mod p)

= (-1)n r1 r2……, rms1s2……sn (mod p)

But we know that r1, r2, ……, rm, s1, s2, ……, sn are congruent modulo p to a, 2a , 3a, ……, ()a in some order. So that

()! (-1)na.2a…….()a (mod p)

(-1)n ()! (mod p)

1 (-1)n (mod p)

Multiplying both side by (-1)n

(-1)n (mod p)

(a/p) = (-1)n.

**Theorem: If p is an odd prime**

**Then**

Proof: By Gauss lemma, (2/p) = (-1)n and n is the number integer in the set S = {2, 2.2, 2.3, ……, .2}

The member of S are all less than p and the remainder in S when divisible by p are greater than . Then it is sufficient to count the number that exceed for 1 n ≤ , 2k < iff k <. We have [] is the greatest integers function then [] integers in S are less than .

Hence, n = – [ integers which are greater than . Now we have the following four possibilities, for any odd prime of the form 8k + 1 or 8k + 3 or 8k + 5 or 8k + 7.

If p = 8k + 1, then

n = 4k – [2k + ] = 4k – 2k = 2k

If p = 8k + 3, then n = 4k+1 – [2k + ] = 4k+1 – 2k = 2k+1

If p = 8k + 5, then n = 4k+2 – [2k + 1+] = 4k+2 – 2k-1 = 2k +1

If p = 8k + 7, then n = 4k+3 – [2k +1+ ] = 4k+3 – 2k-1 = 2k+2

For p of the form 8k + 1 or 8k + 7, n is even. (2/p) = 1 and for p of the form 8k + 3 or 8k + 5, n is odd. (2/p) = -1

**Theorem: If p and 2p + 1 are both odd primes, then the integers .2 is a primitive root of 2p + 1.**

Proof: Suppose q = 2p + 1 then p 1(mod 4) and p 3(mod 4).

If p 1(mod 4) then .2 = 2

Since (q) = q – 1 = 2p, the order of 2 modulo q is one of the number 1, 2, p or 2p. By Legendre symbol, (2/q) (mod q)

But we have p 3(mod 8), by Legendre symbol,

(2/q) = -1 -1(mod 8)

This implies that 2 cannot have order p modulo 8. The order of 2 being neither 1, 2 nor p, then we conclude that the order of 2(mod q) is 2p. This makes that 2 is a primitive root of q.

Let p 3(mod 4), this implies that .2 = -2 and

(-2/q) (-1/q)(2/q)(mod q)

Since qc 7 (mod 8) then (-1/q) = -1 (2/q) = 1 -1(mod p)

i.e. -2 is primitive root of q.

**Theorem: There are infinitely many primes of the form 8k - 1.**

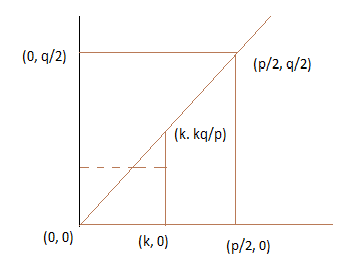
Proof: If possible suppose that there are only a finite number of such primes p1, p2….. pn and consider an integer N = – 2.

There exists at least one odd prime divisor of N, so that 2(mod p) (2/p) = 1.

We know that p 1(mod 8). If all the odd prime divisor of N are of the form 8k + 1 then N were of the form 16a + 2 which is impossible since N is of the form 16a – 2. Thus N must have prime divisor q of the form 8k – 1. But q|N and q| q|N-q|2 which is contradiction. So, we must have there are infinitely many primes of the form 8k – 1.

**Quadratic reciprocity (Gauss Quadratic reciprocity law):**

**If p and q are distinct odd primes, then (p/q)(q/p) =**

(Proof: Consider a rectangle with vertices (0, 0), (p/2, 0), (0, q/2) and (p/2, q/2). Let R be the region within this rectangle without the boundary lines. We can count the lattice points in R two different ways.

Since p and q both are odd, the lattice points in R consists of all points (n, m) with 1 ≤ n ≤ (p-1)/2 and 1 ≤ m ≤ (q-1)/2.

The total number of points are (.

The equation of diagonal (D) is y = (q/p)x or py = qx.

Since gcd(p, q) = 1 no points of r will lie on D.

Let T1 and T2 be the portion below and above the D, then we have to count the points in two triangles.

The number of integers in 0 < y < kq/p is equal to [kq/p]. So for 1 ≤ k ≤ (p-1)/2, there are precisely [kq/p] lattice points in T1 directly above (k, 0) below D.

Then the total number of lattice points on T1 =

Similarly, the total number of lattice points on T2 =

( = +

By Gauss lemma, = +

=

=

**Theorem: If p is an odd prime and gcd(a, p) = 1 then the congruence x2a(mod pn) has a solution iff (a/p) = 1 (n 1)**.

Proof: If x2 a(mod pn) has a solution, and x2 a(mod pn)

So we have (a/p) = 1

Conversely, suppose (a, p) = 1. Then we use induction on n.

If n = 1 then the result is trivial for (a/p) = 1 i.e. x2 a(mod p) is solvable. Suppose the result is true for n = k > 1 so that x2 a(mod pk) is solvable with solution x0, then = a + bpk, for some b.

We have to show that x2 a(mod pk+1)

We solve the linear congruence 2x0y -b(mod p) has a unique solution y0 modulo p.

Since gcd(2x, p) = 1 and suppose x1 = x0 + y0pk

On squaring, (x0 + y0pk)2 = x02 + 2 x0y0pk + y02 p2k

= a + (b + 2 x0y0)pk + y02 p2k [ x02 = a +bpk]

But b| b + 2 x0y0

x2 (x0 + y0pk)2 a(mod pk+1)

x2 a(mod pn) has a solution for n = k+1.

Hence by induction x2 a(mod pn) is true for all n.

**Theorem: Let a be an odd integer. Then**

1. **x2 a(mod 2) always has a solution.**
2. **x2 a(mod 4) has a solution iff a 1(mod 4)**
3. **x2 a(mod 2n) has a solution for n 3 iff a 1(mod 8).**

Proof:

1. Given a is odd integer. So, a 1(mod 2). x2 1(mod 2). Hence, x2 a(mod 2) has exactly one solution x = 1.
2. Let x2 a(mod 4) is solvable. a is odd. x2 is odd. x is odd. x2 1(mod 8) [ the square of an odd integer 1 (mod 8) x2 1(mod 4) a 1(mod 4).

Conversely, let a 1(mod 4) then 1 and 3 satisfy x2 1(mod 4). Hence x2 1(mod 4) is solvable and consequently x2 a(mod 4) is solvable.

1. Let x2 a(mod 2n) is solvable then x2 a(mod 2) is solvable.

Let a is odd. x2 is odd. x2 1(mod 8) a 1(mod 8).

Conversely, let a 1(mod 8). We will use induction on n of the given congruence x2 a(mod 2n) is solvable for n > 2. We have seen that x2 1(mod 8) is solvable and solutions are1, 3, 5 and 7. Let x2 a(mod 2k) has a solution x0 for any k > 2, then x02. Then x02 for some t Z. we generate a solution of x2 in the form x0 + b.tk-1

(x0 + b.2k-1)2 = x02 + 2.x0.b 2k-1 + b222k-2

x02 + x0.b 2k + b2 0.(mod 2k+1), k > 2

a + t.2k + bx0 2k(mod 2k+1)

a + (t+ bx0 )2k(mod 2k+1)

Choosing b such that t+ bx0 0(mod 2) and it exists because x0 is an odd. Then we have (x0 + b.2k-1)2 a(mod 2k+1). Hence x2 is solvable with x0 + b.2k-1 as a solution for n > 2.