I M.Sc MATHEMATICS

SUBJECT CODE : 7MMA1E1

SUBJECT NAME : NUMBER THEORY

HANDLED BY

Mrs. R. ANULA DEVI

I YEAR – I SEMESTER
COURSE CODE: 7MMA1E1

ELECTIVE COURSE-I (A) – NUMBER THEORY

Unit I

The fundamental Theorem of Arithmetic: Introduction – divisibility – greatest common divisor – Prime Numbers – The Fundamental theorem of arithmetic – The series of reciprocals of the primes the Euclidean Algorithm – the greatest common divisors of more than two numbers.

Unit II

Arithmetical functions and Dirichlet Multiplication: Introduction; the Mobius function $\mu(n)$ – θ and μ – product formula for $\theta(n)$ the Dirichlet product of arithmetical functions Dirichlet inverses and the mobius inversion formula the Mangoldt function Λ (n) – Multiplicative functions – Multiplicative functions; and Dirichlet multiplication – the inverse of a Completely multiplicative function – Liouville's fn λ (n) – the division functions $\sigma\alpha$ (n) – Generalized Convolutions – Formal Power Series – the Bell series of an arithmetical function Bell series and Dirichlet Multiplication – Derivatives of arithmetical functions the selberg identity.

Unit III

Averages of Arithmetical Functions: Introduction The big on notation Asymptotic equality of functions – euler's summation formula some elementary asymptotic formulas – the average order of d (n) – the average order of the division functions σ £(n) – the average order of Ψ (n) an application to the distribution of lattice points. Visible from the origin the average order μ (n) and of Λ (n) the partial sums of a Dirichlet product – Applications to $\mu(n)$ and Λ (n) Another identity for the partial sums of a Dirichlet product.

Unit IV

Congruences: Definition and Basic properties of congruences Residue classes and complete residue systems linear congruences – reduced residue systems and the Euler – Fermat theorem– Polynomial congruences modulo Lagrange's theorem – Applications of Lagrange's theorem Simultaneous linear congruences the Chinese remainder theorem – Application of the Chinese remainder theorem – polynomial congruences with prime power moduli the principle of cross classification a decomposition property of reduced residue systems.

Unit V

Quadratic residuces and the Quadratic Reciprocity Law: Lagrange's symbol and its properties– evaluation of (-1/p) and (2/P) – Gauss's Lemma – the quadratic reciprocity law applications of the reciprocity law the Jacobi symbol applications to Diophantine Equations.

Text Book

Tom M. Apostal, Introduction to Analytic Number theory, Springer Verlag.
Chapters : I, II, III, V & IX (upto Diophantine equations)

Books for Supplementary Reading and Reference:

1. Niven and H.S.Zuckerman, An Introduction to the Theory of Numbers, 3rd Edition, Wiley Eastern Ltd., New Delhi, 1989.
2. D.M.Burton, Elementary Number Theory, Universal Book Stall, New Delhi, 2001.

♣♣♣♣♣♣♣♣♣

UNIT - I

FUNDAMENTAL THEOREM of ARITHMETIC

unit - I

The fundamental theorem of Arithmetic :-

property of Integers :-

The principle of induction :-

If Q is a set of integers such that

(i) $1 \in Q$

(ii) $n \in Q$ implies $n+1 \in Q$, then

(iii) All integers ≥ 1 belong to Q.

The well ordering principle :-

If A is a non-empty set of +ve integers Then A contains a smallest ~~number~~ number.

2m Divisibility :-

Def :-

We say d divides n and we write d/n whenever $n = cd$ for some c. We also say that n is a multiple of d, that d is a divisor of n, or that d is a factor of n. If d does not divide n we write d/n

Thm 1 :

Divisibility has the following properties.

(i) $n \mid n$ (Reflexive property)

(ii) $d \mid n$ and $(n \mid m \Rightarrow d \mid m$ (Transitive property)

(iii) $d \mid n$ and $d \mid m \Rightarrow d \mid (an + bm)$ (linearity property)

(iv) $d \mid n$ is $\Rightarrow ad \mid an$ (multiplication property)

(v) $ad \mid an$ and $a \neq 0 \Rightarrow d \mid n$ (cancellation law)

(vi) $1 \mid n$ (1 divides Every integer)

(vii) $n \mid 0$ (Every integer Divides Zero).

(viii) $0 \mid n \Rightarrow n = 0$ (Zero divides only Zero)

(ix) $d \mid n$ and $n \neq 0 \Rightarrow |d| \leq |n|$ (comparison property)

(x) $d \mid n$ and $n \mid d \Rightarrow |d| = |n|$

(xi) $d \mid n$ and $d \neq 0 \Rightarrow (n/d) \mid n$

Note :

If $d \mid n$ then n/d is called the divison Conjugate to d.

Greatest common Divisor :-

If d divides two integers a and b then d is called a common divisor of a and b.

Thus 1 is a common divisor of every pair of integers a and b.

Thm : 1

Given any two integers a and b, there is a common Divisor 'd' of a and b of the form $d = ax + by$ where x and y are integers. moreover every common divisor of a and divides this d.

proof :

To prove that d is a linear combination of a and b.

we Assume that

$$a \geq 0 \text{ and } b \geq 0 \quad \text{--->} \ (1)$$

we prove this theorem by the method of induction on n,

where $n = a + b$ ---> (2)

If $n = 0$

$$a + b = 0.$$

$$a = b = 0$$

and we can take $d = 0$, with $x = y = 0$.

Assume that the theorem has been proved for $0, 1, 2 \ldots n-1$

By symmetry we can assume $a > b$.

If $b = 0$.

Take, $d = a$, $x = 1$, $y = 0$.

If $b \geq 1$.

Apply the theorem to $a - b$ and b.

Since $(a-b) + b = a$.

$= n - b \quad (\because b \geq 1)$

$\leq n - 1 \quad -b \leq -1$.

The induction assumption is applicable and there is a common divisor d, $a - b$ and b of the form $d = (a-b)x + by$

Thus d also divides $(a-b) + b = a$.

So, d is a common divisor of a and b. and we have $d = ax + (y-x)b$, a linear combination of a and b

To complete, the proof we need to show that every common divisor divides d.

But a common divisor divides a and b. and

hence, by linearity, divides d (d/n and d/m ⇒ d/an + bm)

If $a<0$ or $b<0$ (or) both

we can apply the result just prove to $|a|$ and $|b|$

Then there is a common divisor d of $|a|$ and $|b|$ of the form,

$$d = |a|x + |b|y$$

If $a<0$,

$$|a|x = -ax = ax(-x).$$

Similarly

If $b<0$,

$$|b|y = -by = bx(-y).$$

Hence d is again a linear combination of a and b.

Thm : 2.

Given integers a and b there is one and only one number d with the following properties

(i) $d>0$ (d is non-negative)

(ii) $d|a$ and $d|b$ (d is a common divisor of a and b)

(iii) $e|a$ and $e|b \Rightarrow e|d$ (every common divisor divides d)

Prf:

By thm 1, there is atleast one d satisfying conditions 2 and 3.

Also -d satisfies there conditions, bat if d' sation satisfies 2 and 3.

Then $d \mid d'$ and $d' \mid d$

So $|d| = |d'|$.

Hence, there is exactly one $d \geq 0$, satisfying ② and ③.

Note:

In thm 2, $d = 0$ iff $a = b = 0$

otherwise $d \geq 1$.

Def: (GCD)

The number d of thm ② is called the Greatest common divisor (GCD) of a and b and its denoted by (a,b) (or) by $a \circ b$.

If $(a,b) = 1$.

Then a and b are said to be relatively prime

Properties of GCD :-

Thm :-

The GCD has the following properties.

(i) $(a,b) = (b,a)$

$a \mathbin{\mathbb{D}} b = b \mathbin{\mathbb{D}} a$ (commutative law)

(ii) $(a,(b,c)) = ((a,b),c)$

$a \mathbin{\mathbb{D}} (b \mathbin{\mathbb{D}} c) = (a \mathbin{\mathbb{D}} b) \mathbin{\mathbb{D}} c$ (associative law)

(iii) $(ac, bc) = |c|(a,b)$

$(ca) \mathbin{\mathbb{D}} (cb) = |c| (a \mathbin{\mathbb{D}} b)$ (distributive law)

(iv) $(a,1) = (1,a) = 1$; $a \mathbin{\mathbb{D}} 1 = 1 \mathbin{\mathbb{D}} a = 1$.

$(a,0) = (0,a) = |a|$ $a \mathbin{\mathbb{D}} 0 = 0 \mathbin{\mathbb{D}} a = |a|$.

Proof :-

prove that $(ac, bc) = |c|(a,b)$

Let $d = (a,b) \Rightarrow d|a$, $d|b$ and

Let $e = (ac, bc) \Rightarrow e|ac$, $e|bc$.

Then prove that $e = |c|d$

we write $d = ax + by$.

$\Rightarrow cd = acx + bcy$ ---> (1)

① => $e \mid cd$ ---> ② ($\because e \mid ac$ and $e \mid bc$)

$cd \mid (ac, bc)$

=> $cd \mid e$ ---> ③

from ② and ③

$|e| = |cd|$

(or) $e = |c| d$.

2M Euclid's lemma :-

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

Prf :

Since $(a,b) = 1$.

we can write $1 = ax + by$

$c = acx + bcy$.

But $a \mid acx$ and $a \mid bcy$

so $a \mid c$.

Hence proved.

2M Prime numbers :-

Def :

An integer n is called prime, if $n > 1$ and if the only positive divisors of n are 1 and n,

if $n>1$ and if n is not prime then n is called composite.

Eg:

The prime numbers less than 100.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 39, 41, 43, 47, 53, 59, 61, 67, 69, 71, 73, 79, 81, 83, 87, 89, 97.

Note:

Prime numbers are usually denoted by p, p', p_1 and q, q', q_1.

Thm: 1

Every integer $n>1$ is either a prime or a product of prime numbers.

Pf:

We prove this theorem by using the method of induction on n.

Case (i)

The theorem is true for $n=2$.

Case (ii)

Assume that it is true for every integer $<n$.

case (iii)

Let us prove this theorem for n.

If n is not a prime, then it has a positive divisor $d \neq 1$ and $d \neq n$.

Hence $n = cd$ where $c \neq n$.

But both c and d are $< n$ and < 1.

So each c and d is a product of prime numbers

Hence $n = cd$.

U.Q 2m

Thm : 2.

If a prime p does not divide a then $(p, a) = 1$

Proof :

Let $d = (p, n)$ then $d \mid p$ and $d \mid n$.

$d \mid p \Rightarrow d = 1$ or $d = p$

But $d \mid a$ so $d \neq p$ $(p \mid a)$

Hence $d = 1$.

Hence $(p, a) = 1$.

1 QM

U.Q

fundamental theorem of Arith. Automatic :-

Every integer $n > 1$ can be represented as a product of prime factors in only one way apart from the order of the factors.

isor

proof:

I write thm 1 with the prof J

we prove this theorem by the method of induction on n.

Case (i)

If n = 2. then the theorem is true.

Case (ii)

Assume that the theorem is true for 2, 3.... (n-1)

Case (iii)

Let us prove this thm is true for n.

Suppose n has two representation

Say $n = p_1 . p_2 \dots p_s = q_1 . q_2 \dots q_t$.

where p_i's and q_j's are primes.

p_i must be equal to q_j, $s \le j \le t$.

Let $p_1 = q_1$, then $\frac{n}{p_1} = p_2 . p_3 \dots p_s = q_2 . q_3 \dots q_t$.

If $s > 1$, $t > 1$ we have $1 < \frac{n}{p_1} < n$.

By induction hypothesis $\frac{n}{p_1}$ is represented by

Product by prime factors in uniquity.

Hence $s = t$ and each p_i is equal to q_j

Thus $n > 1$ is represented as the product of prime in a unique way.

If $n > 1$ and if the prime factors p_i appears a times

then $n = p_1 \cdot p_2 \cdots p_n$

$$(i.e) \quad n = \prod_{i=1}^{n} p_i^{a_i}.$$

Thm :

If two integers a and b have the factorizations $a = \prod_{i=1}^{\infty} p_i^{a_i}$; $b = \prod_{i=1}^{\infty} p_i^{b_i}$ then there gcd gcd has the factorization $(a,b) = \prod_{i=1}^{\infty} p_i^{c_i}$ where each $c_i = \min\{a_i, b_i\}$, the smaller of a_i and b_i.

Prf :

Let $d = \prod_{i=1}^{\infty} p_i^{c_i}$

To prove $d = (a,b)$

Since $c_i = \min\{a_i, b_i\}$, $c_i \le a_i$ and $c_i \le b_i$

then $p_i^{c_i} \mid p_i^{a_i}$ and $p_i^{c_i} \mid p_i^{b_i}$ for each i

Hence $d \mid a$ and $d \mid b$.

Suppose $e = \prod_{i=1}^{\infty} p_i^{e_i}$ is a common factor of a and b.

(i, e) $e \mid a$ and $e \mid b$

then $e_i \leq a_i$ and $e_i \leq b_i$

Hence $e_i \leq \min\{a_i, b_i\} = c_i$.

$\Rightarrow e_i \leq c_i$

$\Rightarrow p_i^{e_i} \mid p_i^{c_i}$

$\Rightarrow e \mid d$.

clearly $d \geq 0$.

Hence (i) $d \geq 0$.

(ii) $d \mid a$ and $d \mid b$.

(iii) $e \mid a$ and $e \mid b$ implies $e \mid d$

$d = (a, b)$

(1.09) 10m

X. Thm :

The infinite series $\sum_{n=1}^{\infty} \frac{1}{p_n}$ diverges.

Pf :

Suppose $\sum_{n=1}^{\infty} \frac{1}{p_n}$ converges.

Then there is an integer k such that

$$\sum_{m=k+1}^{\infty} \frac{1}{p_m} < 1/2 \quad ---> (I)$$

Let $Q = p_1, p_2, \ldots p_k$ and

Consider the number $1 + nQ$ for $n = 1, 2, \ldots$

To prove that none of the primes

$p_1, p_2 \ldots p_k$ and is a factor of $1 + nQ$

Consider

Suppose one of the factor p_i divides $1 + nQ$

(i.e) $p_i \mid 1 + nQ$ ---> ①

Clearly $p_i \mid nQ$ ---> ②

Hence $p_i \mid 1 + nQ - nQ$ (from ① and ②)

$p_i \mid 1$

But this is not true

It is a contradiction to our assumption

Hence none of the primes $p_1, p_2 \ldots p_k$ is a factor of $1 + nQ$.

Hence the factors of $1 + nQ$ are from the primes $p_{k+1}, p_{k+2}, \ldots$

Hence for each $r \geq 1$

$$\sum_{n=1}^{r} \frac{1}{1+n\alpha} \leq \sum_{t=1}^{\infty} \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t \quad \text{---} > (2)$$

Hence the sum in the RHS is includes all the factors from LHS

$$(I) \Rightarrow \sum_{m=k+1}^{\infty} \frac{1}{p_m} \leq 1/2$$

$\therefore$ (3) becomes

$$\sum_{n=1}^{r} \frac{1}{1+n\alpha} \leq \sum_{k=1}^{\infty} (1/2)^t \quad \text{by } (I)$$

$$= 1/2 + 1/2^2 + 1/2^3 + \cdots$$

$$= 1 + 1/2 + 1/2^2 + \cdots - 1$$

$$= (1 - 1/2)^{-1} - 1$$

$$= \frac{1}{(1-1/2)} - 1 = 2 - 1 = 1.$$

$$\therefore \sum_{n=1}^{\infty} \frac{1}{1+n\alpha} \leq 1$$

Thus the LHS has a bounded sems and Hence converges.

But this is a contradiction.

Because the integral test or the limit comparision test show that this series diverges.

$$(i,e)\quad \int_0^\infty \frac{1}{1+na}\,dn = \lim_{m\to\infty} \int_0^m \frac{1}{1+na}\,dn$$

$$= \lim_{m\to\infty} \left[\frac{1}{a}\log(1+na)\right]_0^m$$

$$= \frac{1}{a}\left[\lim_{m\to\infty} \log(1+ma) - \log 1\right]$$

$$= \frac{1}{a} \lim_{m\to\infty} \log(1+ma).$$

which does not exists.

Hence our assumption

(i,e) $\sum_{n=1}^{\infty} \frac{1}{p_n}$ converges is wrong.

Hence the series $\sum_{n=1}^{\infty} \frac{1}{p_n}$ diverges.

5M X. ✱ ✱ 10M

(1.9) Division Algorithm :-

Given two integer a and b with $b>0$, there exists a unique pair of integer q, r. Such that $a = bq + r$, $0 \le r < b$ more over. $r = 0$ if $b|a$.

Pf:

Let S be the set of all non negative integers

Such that $y = a - bx$. where x is a integer $y \ge 0$.

$\therefore S = \{ y = a - bx \ , \ x \text{ integer } y \geq 0 \}$.

clearly S is non-empty smallest set of the all non negative integers.

By the well ordering principle S has the smallest element say $a - bq$.

Let $r = a - bq$ then $r \geq 0$.

Also $a = bq + r$

we have to prove r is less than b $(r < b)$

Suppose $r \geq b$ then $0 \leq r - b < r$.

then $r - b = a - bq - b$

$= a - b(q+1) \in S \quad [\because a - b \in S$.

Also $r - b < r$

Thus S contains an element smaller than the smallest element r

which is $\Rightarrow <=$

our assumtion is wrong.

$\therefore r < b$.

Hence $a = bq + r \quad 0 \leq r < b$.

Uniqueness part :-

Suppose there exists another pair of integers r' and q' such that $a = bq' + r' \quad 0 \leq r < b$.

Then $bq + r = bq' + r'$

(i.e) $r - r' = b(q' - q)$

$\Rightarrow b \mid r - r'$

If $r - r' = 0$ then the uniqueness so assume

$r - r' \neq 0$.

$|b| \leq |r - r'|$.

which is possible only if $r - r' = 0$.

$\Rightarrow r = r'$

Hence $q = q'$.

more over if $r = 0$.

Then $a = bq$.

Hence $b \mid a$.

Also if $b \mid a$ then $a = bq$ for some q

2M 5M (X) V.I

Euclidean Algorithm :-

Given two integers a and b with $b \nmid a$

Let $r_0 = a$ and $r_1 = b$ Applying division Algorithm repeatly we have

$r_0 = r_1 q_1 + r_2 \; ; \; 0 \leq r_2 < r_1$

$r_1 = r_2 q_2 + r_3 \; ; \; 0 \leq r_3 < r_2$

$r_a = r_3 q_3 + r_4 \; ; \; 0 \le r_4 < r_3$

$\vdots$

$r_{n-2} = r_{n-1} q_{n-1} + r_n \; ; \; 0 \le r_n < r_{n-1}$

$r_{n-1} = r_n q_n + r_{n+1} \; ; \; r_{n+1} = 0.$

Then r_n is the g.c.d of a and b.

Proof:

If we have (r_n) is a decreasing sequence of non-negative.

Hence the sequence terminate on certain stage.

Let it be r_{n+1}.

so, $r_{n+1} = 0.$

Since $r_{n-1} = r_n q_n + r_{n+1}$ with $r_{n+1} = 0.$

$\Rightarrow r_{n-1} = r_n q_n.$

so, $r_n \mid r_{n-1}$.

Since $r_{n-2} = r_{n-1} q_{n-1} + r_n$

we have $r_n \mid r_{n-2}$.

Continuing this we get $r_n \mid r_1$ and $r_n \mid r_0$

$r_n \mid b$ and $r_n \mid a$.

Suppose $d \mid a$ and $d \mid b$.

(i.e) $d \mid r_0$ and $d \mid r_1$

Since $r_0 = r_1 q_1 + r_2$.

we get $d \mid r_{n-1}$ and $d \mid r_n$

so r_n is the g.c.d of a and b.

Pblm:-

① If $(a,b) = 1$ and if $c \mid a$ and $d \mid b$ then $(c,d) = 1$

Soln:-

Suppose $(c,d) = e$.

Then $e \mid c$ and $e \mid d$.

$e \mid c \Rightarrow e \mid a$

$e \mid d \Rightarrow e \mid b$.

$\Rightarrow e \mid (a,b) = 1$.

(i.e) $e = 1$.

$\therefore (c,d) = 1$.

② If $(a,b) = (a,c) = 1$ then $d = 1$.

Soln:-

Suppose $(a,bc) = d$.

Then $d \mid a$ and $d \mid bc$.

$d \mid bc$, some prime factor say p divides b (or) c

If $p \mid b$ then $p \mid (a, b) = 1$.

So $p = 1$.

$\therefore d = 1$.

If $p \mid c$ also $p = 1$.

$\Rightarrow d = 1$.

③ If $(a, b) = 1$ then $(a^n, b^k) = 1$ for $n \geq 1, k \geq 1$.

Soln:-

we prove by induction on n and k.

Take induction on k.

If $k = 1$, $(a^n, b) = 1$.

$(a, b) = 1 \Rightarrow (a^n, b) = 1$

$\Rightarrow (a^n, b^2) = 1$.

Assume $(a^n, b^{k-1}) = 1$.

Then $(a, b), (a, b^{k-1}) = 1 \Rightarrow (a, b^k) = 1$.

now, take induction on $n = 1$.

$(a, b^k) = 1$.

$\Rightarrow (a.a, b^k) = 1$

$\Rightarrow (a^2, b^k) = 1$

Suppose $(a^{n-1}, b^k) = 1$.

then $(a, b^k) = 1$

$\Rightarrow (a^n, b^k) = 1$.

2m

(4) If $(a,b) = 1$ then $(a+b, a-b)$ is either 2 or 1

Soln:-

Suppose $(a+b, a-b) = d$.

$\Rightarrow d \mid a+b$ and $d \mid a-b$

$\Rightarrow d \mid a+b+a-b$

$\Rightarrow d \mid 2a$ ---> (1)

Also, $d \mid a+b-a+b$

$\Rightarrow d \mid 2b$ ---> (2)

Since 2 is a prime number.

(1) $\Rightarrow d = 2$ or $d \mid a$.

(2) $\Rightarrow d = 2$ or $d \mid b$.

(i.e) $d = 2$ or $d \mid (a,b) = 1$.

$\therefore d = 1$ or $d = 2$.

4.(8) If $(a,b) = 1$ then $(a+b, a^2 - ab + b^2) = 3$ or 1

Soln:-

Suppose $(a+b, a^2 - ab + b^2) = d$

then $d \mid a+b$ and $d \mid a^2 - ab + b^2$

$\Rightarrow d \mid (a+b)^2$ and $d \mid a^2 - ab + b^2$

$\Rightarrow d \mid (a+b)^2 - (a^2 - ab + b^2)$.

$\Rightarrow d \mid a^2 + b^2 + 2ab - a^2 + ab - b^2$

$\Rightarrow d \mid 3ab$

since $d = 3$ (or) $d \mid ab$ (or) $d \mid a$ (or) $d \mid b$

$\Rightarrow d = 3$ (or) $d \mid (a, b) = 1$.

$\Rightarrow d = 3$ (or) $d = 1$.

④ Prove that any integer $n \geq 12$ is the sum of two composite numbers.

Soln:

If $n = 12$.

Then $12 = 8 + 4$

$13 = 9 + 4$

$14 = 8 + 6$

$15 = 9 + 6$

To prove for $n \geq 14$.

case (i)

Suppose n is even.

Then $n-1$ is odd.

Also $n - 1 \geq 13$

Assume $n - 1 = x + y$.

where x and y composite and say x is odd.

Then $n = x + y + 1$

$= (x + 1) + y$.

Both $(x+1)$ and y are composite numbers.

case (ii)

Suppose n is odd.

Then $n-2$ is odd.

Since, $n-2 = x+y$.

$n = x+y+2$

where x and ~~$x+(y+2)$~~

$= x+(y+2)$.

where x and $(y+2)$ are composite numbers.

(2) If 2^n+1 is prime, then n is a power of 2.

Soln:-

Suppose n is not a power of 2.

(i,e) $n = 2^p \cdot q$, q is odd

$\therefore 2^n+1 = 2^{2^p \cdot q} + 1$

$= 2^{(2^p)q} + 1$

$= x^q + 1$ where $x = 2^{2^p}$

$= (x+1)(x^{q-1} - x^{q-2} \ldots - x + 1)$

$\therefore (x+1)$ is a factor of 2^n+1.

If $x+1 = 1$.

Then $2^{2^p} + 1 = 1$.

$\Rightarrow 2^{2^p} = 0$.

$\Rightarrow 2^p = 0$ which is not true

If $x+1 = 2^n + 1$.

Then $2^{2^p} + 1 = 2^n + 1$.

$\Rightarrow 2^{2^p} = 2^n$.

$\therefore n = 2^p$ which is not true.

$\therefore$ n is a power of 2.

V.I.P 10m 5m ③ If $2^n - 1$ is prime then n is prime

Soln:-

Suppose n is composite say $n = pq$, $1 < p$, $q < n$

now, $2^n - 1 = 2^{pq} - 1$

$= (2^p)^q - 1$.

$= x^q - 1$ where $x = 2^p$

$= (x-1)(x^{q-1} + x^{q-2} + \ldots + 1)$

(i,e) $(x-1)$ is a factor of $2^n - 1$.

(i,e) $(x-1) \mid 2^n - 1$.

Suppose $x-1 = 1$

$x = 2$.

$\Rightarrow 2^p = 2$.

$\Rightarrow p = 1$.

which is not possible $1 < p$.

Suppose $x-1 = 2^n - 1$

$x = 2^n$.

$2^p = 2^n$

$n = p$.

which is not possible ($n = pq$)

$\therefore 2^{n-1}$ is not a prime

which is a contradiction.

Hence n is prime.

Let $d = (826, 1890)$ compute d and write d as a Linear combination $826, 1890$.

Soln:-

$d = (826, 1890)$

$1890 = 2 \times 826 + 238$.

$826 = 3 \times 238 + 112$

$238 = 2 \times 112 + 14$

$112 = 8 \times 14$.

Since 14 is the last non-zero remainder and by Euclidean algorithm.

14 is the greatest common divisor of 826, 1890

$$14 = 238 - (2 \times 112)$$

$$= 238 - 2(826 - 3 \times 238)$$

$$= 238 - 2(826) + 6 \times 238)$$

$$= 7(238) - 2(826)$$

$$= 7(1890 - 2(826)) - 2(826)$$

$$= 7(1890) - 14(826) - 2(826)$$

$$= 7(1890) - 14(826) - 2(826).$$

$$= 7(1690) - 16(826)$$

$$\therefore 14 = 7(1890) + (-16(826)).$$

Pblm:-

$d = (414, 625)$ compute d and write d as a linear combination of 414 and 625.

Soln:-

$$625 = 1 \times 414 + 211.$$

$$414 = 1 \times 211 + 203$$

$$211 = 1 \times 203 + 8.$$

$$8 = 3 \times 2 + 2.$$

$$3 = 2 \times 1 + 1.$$

$$2 = 1 \times 2 + 0.$$

Since 1 is the g.c.d of (414, 625)

$$1 =$$

② P.T n^4+4 is composite if $n>2$.

Soln:

$$n^2+4 = (n^2)^2+4$$

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

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

We have to prove that

(n^2-2n+2) neither 1 nor n^4+4.

Case (i)

Suppose if $n^2-2n+2=1$.

Then $n^2-2n+2-1=0$.

$\Rightarrow n^2-2n+1=0$.

$\Rightarrow (n-1)^2=0$.

$\Rightarrow n-1=0$.

$n=1$.

But this is not possible because it is give that $n>1$.

$\therefore n^2-2n+2 \neq 1$

Case (ii)

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

then $n^2-2n+2-n^4-4=0$.

$\Rightarrow -n^4+n^2-2n-2=0$.

$\Rightarrow n^4 - n^2 + 2n + 2 = 0$.

$\Rightarrow n^2 [n^2 - 1] + 2(n+1) = 0$.

$\Rightarrow n^2 [(n+1)(n-1)] + 2(n+1) = 0$.

$\Rightarrow (n+1)[n^2(n-1) + 2] = 0$.

$\Rightarrow (n+1)[n^3 - n^2 + 2] = 0$.

$\Rightarrow (n+1)[n^3 - n^2 + 2] = 0$.

$\Rightarrow (n+1) = 0$, (or) $n^3 - n^2 + 2 = 0$.

But $n \neq -1$ (since $n > 1$).

$\therefore n^3 - n^2 + 2 = 0$.

But $n > 1$, $n^3 - n^2 + 2 \neq 0$.

$\therefore n^2 - 2n + 2 \neq n^4 + 4$.

$\therefore n^2 - 2n + 2$ is a composite number

$\therefore n^4 + 4$ is composite if $n > 1$.

(2) If $m \neq n$ compute the g.c.d of $(a^{2^m} + 1, a^{2^n} + 1)$ interm of a.

Soln:

Let $A_m = a^{2^m} + 1$

$A_n = a^{2^n} + 1$.

Assume $m > n$.

$A_{m-2} = a^{2^m} + 1 - 2$

$= a^{2^m} - 1 = a^{2^{m-1}+1} - 1 = a^{2^{m-1} \cdot 2} - 1$

$= (a^{2^{m-1}})^2 - 1^2$

$= (a^{2^{m-1}} + 1)(a^{2^{m-1}} - 1)$

$= (a^{2^{m-1}} + 1)(a^{2^{m-1}} + 1)(a^{2^{m-1}} - 1)$.

Continuning this process

$A_n \mid (A_m - 2)$ ---> (1)

Let $d = (A_n, A_m)$

then $d \mid A_n$ and $d \mid A_m$.

from (1) $d \mid A_{m-2}$, $d \mid A_m$ and $d \mid A_m - 2$.

$\Rightarrow d \mid A_m - A_m + 2$

$\Rightarrow d \mid 2$.

$\Rightarrow d = 1$ or $d = 2$.

case (i)

If a is odd.

then $a^{2^m} + 1$, $a^{2^n} + 1$ are even

In this case $d = 1$

$$\therefore \boxed{(Am, An) = (a^{2m}+1, a^{2n}+1) = \begin{cases} 1 & \text{if } a \text{ is even} \\ 2 & \text{if } a \text{ is odd} \end{cases}}$$

Case (ii)

If a is even

then $a^{2m}+1, a^{2n}+1$ is odd

In this case $d = 1$.

$$\therefore \boxed{(Am, An) = (a^{2m}+1, a^{2n}+1) = \begin{cases} 1 & \text{if } a \text{ is even} \\ 2 & \text{if } a \text{ is odd} \end{cases}}$$

UNIT - II

ARITHMETICAL FUNCTIONS AND DIRICHLET MULTIPLICATION.

Unit - II

Arithmatical functions and Dirichlet multiplication.

Def:

A real or complex valued function defined on the positive integers is called Arithmatical function or a number theoritic function.

Eg:

1) The mobius function $\mu(n)$

2) The Euler Totient function $\varphi(n)$

The mobius function $\mu(n)$

Def:

The mobius function μ is defined as follows:

$\mu(1) = 1$;

If $n > 1$ write $n = p_1^{a_1}, p_2^{a_2}, \ldots\ldots p_k^{a_k}$. Then

$\mu(n) = (-1)^k$ if $a_1 = a_2 = \ldots = a_k = 1$.

$\mu(n) = 0$ otherwise

Note:

$\mu(n) = 0$ iff n has a Square factor > 1

Values of $\mu(n)$;

n	:	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	:	1	-1	-1	0	-1	1	-1	0	0	1

Thm: 2.1

If $n \geq 1$ we have $\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$

Prf:

case (i)

This is clearly true if $n = 1$

case (ii)

Assume that $n > 1$

write $n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_k}$

In the sum $\sum_{d|n} \mu(d)$ the only non-zero terms ~~from~~ come from $d = 1$ and from those divisors of n which are products of distinct primes.

Thus.

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \ldots + \mu(p_k) + \mu(p_1 p_2) + \ldots + \mu(p_{k-1} p_k) + \ldots + \mu(p_1 p_2 \cdots p_k)$$

$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k$$

$$= (1-1)^k = 0.$$

Note :-

$[x]$ denote the greatest integer $\leq x$ and the above thm is one of the fundamental property of Mobius function.

The Euler Totient function $\varphi(n)$.

Def:-

If $n \geq 1$ the Euler totient $\varphi(n)$ is defined to be the number of positive integers not exceeding n which are relatively prime to n : thus,

$$\varphi(n) = \sum_{k=1}^{n}{}' 1,$$

where the $'$ indicates that the sum is extended over those k relatively prime to n.

Values of $\varphi(n)$

n :	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$:	1	1	2	2	4	2	6	4	6	4

Thm 2.2

If $n \geq 1$ we have $\sum_{d/n} \varphi(d) = n$.

Pf:

Let S denote the set $\{1, 2, \ldots, n\}$.

We distribute the integers of S into disjoint sets as follows.

for each divisor d of n,

Let $A(d) = \{k : (k, n) = d, 1 \leq k \leq n\}$.

(i.e) A(d) contains those elements of S which have the G.C.D. d with n.

Let us prove that the sets A(d) form a disjoint collection whose union is S.

(1) To prove that the set A(d)'s disjoint

(i.e) to prove $A(d_1) \cap A(d_2) = \varphi$

Suppose $A(d_1) \cap A(d_2)$

Then $(k, n) = d_1$ and $(k, n) = d_2$

$d_1 = d_2$.

$\therefore$ A(d)'s are disjoint.

(ii) To prove that $\bigcup_{d|n} A(d) = S$.

Since $A(d) \subseteq S$.

we have $\bigcup_{d|n} A(d) \subseteq S$

To prove $S \subset \bigcup_{d|n} A(d)$

Let $k \in S$.

Then $(k, n) = l$ for some l.

(i.e) $k \in A(l)$ for some l.

(i.e) $k \in \bigcup_{d|n} A(d)$

(i.e) $S \subset \bigcup_{d|n} A(d)$

$\therefore S = \bigcup_{d|n} A(d)$

If $f(d)$ denotes the number of integers in $A(d)$

we have $\sum_{d|n} f(d) = n$ ---> (1)

But $(k, n) = d$ iff $\left(\frac{k}{d}, \frac{n}{d}\right) = 1$ and

$0 < k \leq n$ iff $0 < \frac{k}{d} \leq \frac{n}{d}$.

$\therefore$ Let $q = k/d$.

There is a one-to one correspondence between the elements in $A(d)$ and those integer q satisfying

$0 < q \leq n/d$, $(q, n/d) = 1$

The number of set of is $\varphi\left(\frac{n}{d}\right)$

Hence $f(d) = \varphi\left(\frac{n}{d}\right)$ and

① becomes $\sum_{d/n} \varphi\left(n/d\right) = n$.

This is equivalent to $\sum_{d/n} \varphi(d) = n$.

because d through all divisors of n

so does n/d.

Hence the proof.

A Relation connecting φ and μ

Thm : 3

If $n \geq 1$ we have $\varphi(n) = \sum_{d/n} \mu(d) \frac{n}{d}$

Pf :

The sum * defined in $\varphi(n)$ can be re written in the form $\varphi(n) = \sum_{k=1}^{n} \left[\frac{1}{(n,k)}\right]$

where, now k runs through all integers $\leq n$.

By using thm 2.1 with n replaced by (n,k)

To obtain $\varphi(n) = \sum_{k=1}^{n} \sum_{d/(n,k)} \mu(d)$.

$$= \sum_{k=1}^{n} \sum_{\substack{d/n \\ d/k}} \mu(d)$$

for a fixed divisor d of n we must sum over all those k in the range $1 \le k \le n$ which are multiples of d.

If we write $k = qd$ then $1 \le k \le n$ iff $1 \le q \le n/d$.

Hence the last sum for $\varphi(n)$ can be written as $\varphi(n) = \sum_{d/n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d/n} \mu(d) \sum_{q=1}^{n/d} 1$

$$= \sum_{d/n} \mu(d) \frac{n}{d}.$$

Hence the proof.

A product formula for $\varphi(n)$

Thm : 2.4

For $n \ge 1$ we have $\varphi(n) = n \prod_{p/n} \left(1 - \frac{1}{p}\right)$.

Pf:

Case (i)

If $n = 1$. the product is empty.

since there are no primes which divide 1

∴ The product is to be assigned the value 1

$\therefore \varphi(1) = 1 \qquad 1 = n \prod_{p/n} (1 - 1/p)$

$L.H.S \quad \varphi = 1 \cdot \prod_{p/1} (1 - 1/p)$

$= 1 \cdot 1$

$= 1.$

Case (ii)

If $n > 1$.

Let $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, be the distinct prime divisors of n.

The product can be written as

$$\prod_{p/n} (1 - 1/p) = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \text{ ---->①}$$

$$= 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k}$$

$$+ \ldots\ldots + \frac{(-1)^r}{p_1 p_2 \ldots p_r}.$$

In a term $\sum \frac{1}{p_i p_j p_k}$ it is understood that

we consider all possible products $p_i p_j p_k$ of distinct prime factors of n taken 3 at a time

Each term on the RHS of eqn ① is of the form $\pm 1/d$, where d is a divisor of n which is either 1 or a product of distinct primes.

The numerater ± 1 is exactly $\mu(d)$ since $\mu(d) = 0$ if d is a divisible by the square of any p_i

∴ The sum in ① is exactly the same as

$$\sum_{d/n} \frac{\mu(d)}{d}$$

The prof is complete.

Thm :

Euler's totient has the following properties :

(a) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ for prime p and $\alpha \geq 1$.

(b) $\varphi(mn) = \varphi(m)\varphi(n)(d \mid \varphi(d))$, where $d = (m,n)$.

(c) $\varphi(mn) = \varphi(m)\varphi(n)$ if $(m,n) = 1$.

(d) $a \mid b$ implies $\varphi(a) \varphi(b)$.

(e) $\varphi(n)$ is even for $n \geq 3$. moreover if n has r distinct odd prime factors, then $2^r \mid \varphi(n)$.

Pf:

(i) let us prove that $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ for prime p and $\alpha \geq 1$. W.k.T by thm.

$$\varphi(n) = n \prod_{p \mid n} (1 - 1/p) \text{ for } n \geq 1.$$

Take $n = p^\alpha$.

$$\therefore \varphi(p^\alpha) = p^\alpha \cdot \prod_{p \mid p^\alpha} (1 - 1/p)$$

$$= p^\alpha \cdot p^\alpha / p$$

$$= p^\alpha - p^{\alpha-1}.$$

Let us prove that

$$\varphi(mn) = mn \prod_{p \mid m} (1 - 1/p) \prod_{p \mid n} (1 - 1/p)$$

$$\prod_{p \mid (m,n)} (1 - 1/p)$$

$$\left[\because \varphi(n) = n \prod_{p \mid n} (1 - 1/p) \right.$$

$$= m \prod_{p/m} (1-1/p) \; n \prod_{p/n} (1-1/p)$$

$$\prod_{p/(m,n)} (1-1/p)$$

$$= \frac{\varphi(m)\,\varphi(n)}{\prod_{p/d} (1-1/p)} = \frac{\varphi(m)\cdot\varphi(n)}{(\varphi(d)/d)}$$

$$= \varphi(m) \cdot \varphi(n)\, d/\varphi(d).$$

Let us prove that

$$\varphi(mn) = \varphi(m).\varphi(n).$$

If m and n are relatively prime.

$$d = 1.$$

W.K.T $\varphi(mn) = \varphi(m)\,\varphi(n).\dfrac{d}{\varphi(d)}$

$$= \varphi(m).\varphi(n).\frac{1}{\varphi(1)}$$

$$\varphi(mn) = \varphi(m).\varphi(n) \quad (\because \varphi(1) = 1).$$

If a/b then $\varphi(a) \mid \varphi(b)$.

Pf:-

If $b = 1$ then $a = 1$.

Also $\varphi(1) = 1$.

$$\varphi(a) \mid \varphi(b).$$

Assume $b > 1$.

Since $a \mid b$, $b = ca$ for some c $a \leq c \leq b$.

If $c = b$, then $a = 1$.

$\therefore \varphi(a) = \varphi(1) = 1$.

(i.e) $1 \mid \varphi(b)$

(i.e) $\varphi(a) \mid \varphi(b)$

So assume $c < b$. we prove the thm by induction on b.

$\because$ the thm is true for $b = 1$.

we can assume the thm is true for all integer $< b$.

Since $c < b$, the thm is true for c.

Also $\varphi(b) = \varphi(ca)$

$= \varphi(c) \cdot \varphi(a) \; \frac{d}{\varphi(d)}$

where $d = (a, c)$

Since $d \mid c$ and $c < b$.

(i.e) $\varphi(c)$ as an integer multiple of $\varphi(d)$.

$$\left[\varphi(a) = \varphi(a) \, d \, \frac{\varphi(c)}{\varphi(d)} \right.$$

$= \text{integer multiple of } \varphi(a)\ ]$

$\therefore \varphi(a) \mid \varphi(b)$.

Let us prove that $\varphi(n)$ is even.

If $n \geq 3$.

further if n has r distinct odd prime factors

Then $2^r \mid \varphi(n)$.

Pf:

Let $n = 2^\alpha$, $\alpha \geq 2$.

Then $\varphi(n) = \varphi(2^\alpha)$.

$= 2^\alpha - 2^{\alpha-1}$

$=$ even.

If n has atleast one odd prime

Then $\varphi(n) = n \prod_{p/n} (1 - 1/p)$

$= n \prod_{p/n} \left(\frac{p-1}{p}\right)$

$= \dfrac{n \prod_{p/n} (p-1)}{\prod_{p/n} p}$

$= \dfrac{n}{\prod_{p/n} p} \cdot \prod_{p/n} (p-1)$

where $c(n)$ is an integer

Also, $p-1$ is even each $p-1$ contains atleast one 2

then the RHS is a multiple of 2.

$\therefore \varphi(n)$ is even Each odd prime p contributes a factor 2 for the product.

So $2 \mid \varphi(n)$ if n has r distinct prime

Since there are r distinct primes,

we have $2^r \mid \varphi(n)$.

Remark:

we have $\varphi(2) = 1$.

$$\varphi(4) = 2.$$

$$\varphi(4) \neq \varphi(2) \cdot \varphi(2)$$

$$2 \neq 1 \cdot 1.$$

Def:

Let f and g be the arithmetical function then the Dirichlet product (or) convolution of f and g is written as $(f \times g)(n) = \sum_{d \mid n} f(d)\, g\left(\frac{n}{d}\right)$.

Def:

An Arithmetic function N is defined by $N(n) = n \forall n$

Remark:

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

$$= \sum_{d|n} \mu(d) \cdot N(n/d)$$

$$\varphi = \mu * N$$

Thm: 2.6

Prove that Dirichlet product is commutative

Pf:

The Dirichlet prime is.

$$(f*g)(n) = \sum_{d|n} f(d)\, g(n/d)$$

[if $d_1, d_2 \ldots d_k$ are the divisors of n. then

$$n = a_1 d_1 = a_2 d_2 = \ldots = a_k d_k$$

now, $(f*g)(n) = f(d_1)\, g(a_1) + f(d_2)\, g(a_2)$

$$+ f(d_k)\, g(a_k) \cdot]$$

$$(f*g)\, n = \sum_{ab=n} f(a)\, g(b)$$

$= (g * f)(n)$.

$(f * g)(n) = (g * f)(n)$.

Prove that Dirichlet product is associative.

Pf:-

We have to prove that

$(f * g) * k = f * (g * k)$

Let $f * g = A$.

Now, $((f * g) * k)(n) = (A * k)(n)$.

$= \sum_{d|n} A(d)\, k(n/d)$.

$= \sum_{ab=n} A(a)\, k(b)$.

$= \sum_{ab=n} (f * g)(a)\, k(b)$.

$= \sum_{ab=n} \sum_{ce=n} f(c)\, g(e)\, k(b)$

$= \sum_{c.eb=n} f(c)\, g(e)\, k(b)$ ---> (1)

Now, Let $g * k = B$.

$$(f(g*k))(n) = (f*B)(n)$$

$$= \sum_{ca=n} f(c)\ B(a)$$

$$= \sum_{ca=n} f(c)\ (g*k)(a)$$

$$= \sum_{ca=n} f(c) \sum_{eb=na} g(e)\ k(b).$$

$$= \sum_{c.eb=n} f(c)\ g(e)\ k(b) \quad \text{---> (2)}$$

from (1) and (2) we get

$$((f*g)*k)(n) = (f*(g*k))(n).$$

(i.e) $(f*g)*k = f*(g*k)$.

Identity function :-

Def:

The Arithmetic function I given by

$$I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$$ is called the identity function.

Thm:

for all f we have $I*f = f*I = f$.

Pf:

we have $(f*I)(n) = \sum_{d|n} f(d)\ I\left(\frac{n}{d}\right)$

$$= \sum_{d|n} f(d) \left[\frac{1}{(n/d)}\right]$$

$$= \sum_{d|n} f(d) \left[d/n \right]$$

$$= f(n) \quad \left[\because I\, d/n \right] = 0 \text{ if } d < n \Big]$$

$$\therefore f * I = f$$

Similarly $I * f = I$.

$$f * I = I * f = f.$$

Dirichlet inverse and the mobius inversion formula

Thm: If f is an arithmetic function with $f(1) \neq 0$ there is a unique arithmetrical function f^{-1}, called the Dirichlet inverse of f, such that $f * f^{-1} = f^{-1} * f = I$. moreover f^{-1} is given by the recursion formulas.

$$f^{-1}(1) = \frac{1}{f(1)}, \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d)$$

for $n > 1$.

Pf:

Let $n = 1$.

we have $(f * f^{-1})(n) = I(n)$.

Since $f(1) \neq 0 \Rightarrow f^{-1}(1) = 1/f(1)$.

To prove that

$(f * f^{-1})(n) = I(n)$ has a unique set

whose value is $f^{-1}(n)$.

now $(f * f^{-1})(n) = I(n)$.

$$\Rightarrow \sum_{d|n} f^{-1}(d)\, f(n/d) = I(n).$$

since $n > 1$.

$$\sum_{d|n} f^{-1}(d)\, f(n/d) = 0.$$

(i.e) $$f(1) f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f^{-1}(d)\, f(n/d) = 0.$$

Since $f(1) \neq 0$.

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{d|n} f^{-1}(d)\, f(n/d).$$

Remark:

we know $$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right]$$

$$\sum_{d|n} \mu(d) = I(n).$$

Def:

we define the unit function u to be the function

such that $u(n) = 1$. for all n.

$$\mu * u = I.$$

Thus u and μ are Dirichlet inverses of each other

$$u = \mu^{-1} \text{ and } \mu = u^{-1}.$$

Thm:

Mobius inversion formula.

The equation $f(n) = \sum_{d|n} g(d)$ ---> (1) implies $g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$ ---> (2)

Conversely (2) implies (1)

Prf:

Let $f(n) = \sum_{d|n} g(d)$.

$$= \sum_{d|n} g(d) \cdot 1$$

$$= \sum_{d|n} g(d) \cdot u(n/d)$$

$$f(n) = (g * u)(n)$$

$$\Rightarrow f \Rightarrow g * u.$$

$$\Rightarrow f * \mu = (g * u) * \mu.$$

$$g * \mu = g * (u * \mu)$$

$$f * \mu = g * I$$

$$= g.$$

$$g(n) = (f * \mu)(n).$$

$$g(n) = \sum_{d|n} f(d)\,\mu(n/d)$$

Let $g(n) = \sum_{d|n} f(d)\,\mu(n/d)$

$= (f * \mu)(n)$

$g(n) = (f * \mu)(n)$

$g = f * \mu$.

multiply by u on both side

$g * u = (f * \mu) * u$

$= f * (\mu * u) = f.$

$f(n) = (g * u)(n)$

$= \sum_{d|n} g(d)\, u(n/d)$

$= \sum_{d|n} g(d)$

Def:

The Mangoldt function $\Lambda(n)$:

for every integer $n \geq 1$ we define $\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m \text{ for some prime } p \text{ and } m \geq 1, \\ 0 & \text{otherwise.} \end{cases}$

Table values of $\Lambda(n)$:

n:	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$:	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0

Thm :

If $n \geq 1$, we have $\log n = \sum_{d|n} \Lambda(d)$.

Prf :

Step 1 : If $n = 1$.

L.H.S $\log n = \log 1 = 0$.

RHS : $\sum_{d|n} \Lambda(d) = \Lambda(1)$

$= 0$.

$\therefore \log n = \sum_{d|n} \Lambda(d)$.

Step 2 :

If $n > 1$.

Let $n = p_1^{a_1}, p_2^{a_2} \ldots p_r^{a_r}$

$= \prod_{k=1}^{r} p_k^{a_k}$.

$\log n = \log (p_1^{a_1}, p_2^{a_2}, \ldots p_r^{a_r})$

$= \log p_1^{a_1} + \log p_2^{a_2} + \ldots + \log p_r^{a_r}$

$= a_1 \log p_1 + a_2 \log p_2 + \ldots + a_r \log p_r$

$\log n = \sum_{k=1}^{r} a_k \log p_k$ --> (1)

RHS : $\sum_{d|n} \Lambda(d)$.

The only non zero terms (or) the sum come from

those divisors d of the form p_k^m for $m = 1, 2, \ldots a_k$

and $k = 1, 2, \ldots r$.

Hence $$\sum_{d|n} \Lambda(d) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k^m)$$

$$= \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log p_k$$

$$= \sum_{k=1}^{r} \log p_k = \sum_{k=1}^{r} a_k \log p_k \rightarrow (2)$$

from eqn (1) and (2) we have.

$$\log n = \sum_{d|n} \Lambda(d)$$

Hence the proof.

Thm :

If $n \geq 1$, we have $\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d$.

pf :

W.K.T $\log n = \sum_{d|n} \Lambda(d)$

By mobius inversion formula.

$$\Lambda(n) = \sum_{d|n} \log d \cdot \mu(n/d)$$

$$= (\log * \mu)(n).$$

$$= (\mu * \log)(n).$$

$$\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d) \rightarrow (1)$$

$$= \sum_{d|n} \mu(d) [\log n - \log d]$$

$$= \sum_{d|n} \mu(d) \log n - \sum_{d|n} \mu(d) \log d.$$

for $n = 1$, $\log 1 = 0$ and

for $n > 1$, $\sum_{d|n} \mu(1) = 0$ [$\because$ If $n \geq 1$ $\sum_{d|n} \mu(d) = [1/n] = \begin{cases} 1 & \text{if } n > 1 \\ 0 & \text{if } n > 1 \end{cases}$]

$$\therefore \Lambda(n) = 0 - \sum_{d|n} \mu(d) \log d, \quad n > 1$$

$$= - \sum_{d|n} \mu(d) \log d.$$

multiplicative function.

Def:

An arithmatical function f is called multiplicative if f is not identically zero and if $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$.

Def:

A multiplicative function f is called completly multiplicative. if we also have $f(m,n) = f(m)\,f(n)$ for all m, n.

Eg:

Let $f_\alpha(n) = n^\alpha$, $\alpha \in \mathbb{C}$ where α is a fixed real or complex number this function is completly multiplicative

Eg:

$f_\alpha(n) = n^\alpha$, $\alpha \to$ real or complex.

$\Rightarrow f_\alpha(mn) = (mn)^\alpha = m^\alpha n^\alpha = f_\alpha(m) \cdot f_\alpha(n)$.

$\therefore f_\alpha(n)$ is not identically zero.

Eg:

The unit function $u = f_0$ is completely multiplicative

$u(n) = 1$.

$u(mn) = 1$

$= 1.1$

$= u(m) \cdot u(n)$. and u is not identically zero.

Eg:

The identity function $I(n) = \left[\frac{1}{n}\right]$ is identity completely multiplicative.

Pf:

$I(n) = [1/n]$

$I(mn) = [1/mn]$.

If $n = m = 1$. then $mn = 1$.

$\therefore I(mn) = 1/1 = 1$.

$\therefore I(mn) = I(m) \cdot I(n)$.

If $m > 1$, $n > 1$.

Then $mn > 1$.

Also $I(m) = 0$ or $I(n) = 0$.

$I(mn) = 0 = 0.0 = I(m) \cdot I(n)$.

$\therefore I(mn) = I(m) \cdot I(n)$.

Eg :

Prove that μ and φ are multiplicative but not completely multiplicative.

Pf :

Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ and

$n = q_1^{\beta_1} q_2^{\beta_2} \ldots q_s^{\beta_s}$

$mn = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \cdot q^{\beta_1} \ldots q_s^{\beta_s}$

with $(m,n) = 1$.

$\mu(mn) = (-1)^k (-1)^s$ where $\alpha_1 = \alpha_2 = \ldots = \alpha_k$

$\beta_1 = \beta_2 = \ldots = \beta_s$

$= \mu(m) \cdot \mu(n)$.

$\therefore \mu(m*n) = \mu(m) \cdot \mu(n)$.

Illy $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ if $(m,n) = 1$.

Thm :

If f is multiplicative then $f(1) = 1$.

Pf :

Given f is multiplicative

To prove $f(1) = 1$.

$f(n) = f(n \cdot 1)$.

$f(mn) = f(m) f(n)$.

$f(1) = 1 \quad (\because f(n) \neq 0)$.

Thm :-

Given f with $f(1) = 1$.

(i) f is multiplicative iff $f(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) \dots f(p_k^{\alpha_k})$. for all primes p_i and all integers then $\alpha_i \geq 1$.

(ii) If f is multiplicative then f is completly multiplicative iff $f(p^\alpha) = f(p)^\alpha$, $\alpha \geq 1$ and prime

Soln :-

since f is multiplicative.

$f(mn) = f(m) \cdot f(n)$ whenever $(m, n) = 1$.

consider $f(p_1^{\alpha_1} \dots p_k^{\alpha_k})$ with $(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$.

$f(p_1^{\alpha_1} \dots p_k^{\alpha_k}) \Leftrightarrow f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \dots f(p_k^{\alpha_k})$

$\Leftrightarrow f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \dots f(p_3^{\alpha_3}) \dots f(p_k^{\alpha_k})$

Suppose f is multiplicative

Let $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

$n = q_1^{\beta_1} \cdots q_s^{k s}$

$f(mn) = f(p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_s^{\beta_s})$

$= f(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) f(q_1^{\beta_1} \cdots q_s^{\beta_s})$

$= f(m) f(n)$

$\therefore f$ is completely multiplicative.

Conversely,

Let us assume that f is completely multiplicative

To prove $f(p^{\alpha}) = f(p)^{\alpha}$.

LHS $f(p^{\alpha})$.

$= f(p^{\alpha-1} \cdot p^1) = f(p^{\alpha-1}) f(p)$

$= f(p^{\alpha-2} p^1) \cdot f(p) = f(p^{\alpha-2}) f(p) \cdot f(p)$

$= f(p^{\alpha-2}) \cdot f(p)^2$.

$f(p^{\alpha}) = f(p)^{\alpha}$

$f(p^{\alpha}) = f(p)^{\alpha}$.

The converse is also true.

conversely,

Let us assume that $f(p^{\alpha}) = f(p)^{\alpha}$.

To prove that f is multiplicative and f is completly multiplicative

Suppose $m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$.

$n = p_1^{\beta_1} \ldots p_s^{\beta_s}$.

$mn = p_1^{(\alpha_1+\beta_1)} \ldots p_k^{(\alpha_k+\beta_k)}$ if $(k > s)$

$f(mn) = f(p_1^{\alpha_1+\beta_1} \ldots p_k^{\alpha_k+\beta_k})$

$= f(p_1^{\alpha_1} \cdot p_1^{\beta_1}) \ldots f(p_k^{\alpha_k} \cdot p_k^{\beta_k})$

$= f(p_1^{\alpha_1}) \cdot f(p_1)^{\beta_1} \ldots f(p_k)^{\alpha_k} \cdot f(p_k)^{\beta_k}$

$\therefore$ f is multiplicative

$= f(p_1^{\alpha_1}) f(p_2)^{\alpha_2} \ldots r(p_k^{\alpha_k}) \cdot f(p_1^{\beta_1})$

$\cdot f(p_2^{\beta_2}) \ldots f(p_k^{\beta_k})$.

$F(m,n) = f(m) F(n)$.

Hence f is completely multiplicative.

multiplicative functions and Dirichlet multiplication

Thm:

If f and g are multiplicative so is their dirichlet product $f * g$.

Pf:

Given f and g are multiplicative.

$$f(mn) = f(m)\,f(n) \quad \text{for } (m,n) = 1.$$

$$g(mn) = g(m)\,g(n) \quad \text{for } (m,n) = 1.$$

To prove

$f * g$ multiplicative.

W.K.T

$$(f * g)(n) = \sum_{d|n} f(d)\, g(n/d).$$

Let $h = f * g$ and choose relatively prime integers m and n.

$$\text{Then } h(mn) = \sum_{d|mn} f(d)\, g\left(\frac{mn}{d}\right)$$

Every divisor d of mn can be expressed in the from $d = ab$ where $a|m$ and $b|n$.

moreover $(a,b) = 1$, $\left(\frac{m}{a}, \frac{n}{b}\right) = 1$ and

there is a one to one correspondence between the set of product ab and the divisors d of mn.

Hence $h(mn) = \sum_{d=ab \mid mn} f(ab)\, g\left(\frac{mn}{ab}\right)$

$$= \sum_{\substack{a \mid m \\ b \mid n}} f(a) f(b)\, g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right)$$

for $(a,b) = 1$.

$$= \sum_{a \mid m} f(a) \cdot g\left(\frac{m}{a}\right) \cdot \sum_{b \mid n} f(b)\, g\left(\frac{n}{b}\right)$$

$$= (f * g)\, m \cdot (f * g)\, n$$

$$h(m,n) = h(m) \cdot h(n).$$

Hence $f * g\,(m/n) = f * g\,(m) \cdot f * g\,(n)$.

$\therefore f * g$ is a multiplicative.

Thm:

If both g and $f * g$ are multiplicative then f is also multiplication.

Pf:

Given g and $f * g$ are multiplicative.

$g(mn) = g(m) \cdot g(n)$ for $(m,n) = 1$.

$f * g\,(mn) = f * g\,(m) \cdot f * g\,(n)$.

Let $f * g = h$.

$h(mn) = h(m) \cdot h(n)$.

To prove f is multiplicative.

(i.e) To prove $f(mn) = f(m) f(n)$ for $(m,n) = 1$.

Suppose, f is not multiplicative.

Deduce that h is also not multiplicative.

Since f is not multiplicative there exists a positive integer m and n with $(m,n) = 1$

Such that $f(mn) \neq f(m) f(n)$.

We choose such a pair m and n for which the product mn is as small as possible.

Case (i)

If $mn = 1$.

Then $f(1) \neq f(1) \cdot f(1)$.

So $f(1) \neq 1$.

Since $h(1) = f(1) \cdot g(1)$.

$h(1) = f(1) \cdot 1$ ($\because g$ is multiplicative)

$h(1) \neq 1$.

h is not multiplicative

which is $\Rightarrow \leq$

$\therefore$ f is a multiplicative.

Case (ii)

If $(mn) > 1$.

There we take $f(ab) = f(a)f(b)$ $\forall$ positive integers a and b with $(a,b) = 1$ and $ab < mn$.

$$h(mn) = \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(ab) \cdot g\left(\frac{mn}{ab}\right) + f(m) \cdot g(n).$$

$$= \sum_{\substack{d|m \\ b|n \\ ab|mn}} f(a) \cdot f(b) \cdot g\left(\frac{m}{a}\right) \cdot g\left(\frac{n}{b}\right) + f(mn) \cdot 1$$

<---- by (*)

and g is multiplicative

$g(1) = 1$]

$$= \sum_{a|m} f(a) \cdot g\left(\frac{m}{a}\right) \sum_{b|n} f(b)$$

$$g(n/b) - f(m) f(n) + f(mn).$$

$$= h(m) h(n) - f(m) f(n) + f(mn).$$

$$h(mn) = h(m) h(n) - f(m) f(n) + f(mn) \quad \text{--->} (1)$$

$$\therefore f(mn) \neq f(m) \cdot f(n).$$

(1) $\Rightarrow$ $h(mn) \neq h(m) \cdot h(n)$.

so this not multiplicative. But this is a

$\Rightarrow \angle =$

$\therefore$ f is multiplicative.

Thm :-

If g is multiplicative so is g^{-1} its also multiplicative

pf :-

Let $g * g^{-1} = I$.

w.k.T I is multiplicative. $g * g^{-1}$ is multiplicative

By thm g is multiplicative the f is also multiplicative

$\therefore$ g is multiplicative.

and $g * g^{-1}$ is multiplicative.

$\therefore g^{-1}$ is multiplicative.

The Inverse of a completely multiplicative function.

State :-

Let f be multiplicative then f is completly

$f^{-1}(n) = \mu(n) \cdot f(n) \quad \forall \; n \geq 1.$

Prf:-

Let $g(n) = \mu(n) \cdot f(n)$ ---> ①.

If f is completely multiplicative.

we have $(g * f)(n) = \sum_{d/n} g(d) f(n/d)$

$= \sum_{d/n} \mu(d) f(d) f(n/d)$ (from ①)

$= \sum_{d/n} \mu(d) f(n)$ ($\because f(m) \cdot f(n) = f(mn)$).

$= I(n) \cdot f(n)$

$= I(n) f(1)$ $\quad I(n) = [1/n]$

$= I(n)$. $= \begin{cases} 1 & \text{if } n=1 \\ 0 & n>0 \end{cases}$

$g * f = I$.

g is inverse of f.

$f^{-1}(n) = g(n)$.

$f^{-1}(n) = \mu(n) f(n)$

Hence the proof.

Conversely,

Suppose $f^{-1}(n) = \mu(n) f(n) \; \forall n \geq 1$.

To prove f is completly multiplicative and f is

multiplicative.

w.k.T If f is multiplicative then f is completly iff $f(p^\alpha) = f(p)^\alpha$ primes p & and all integer $\alpha \geq 1$.

$\therefore$ It is enough to prove that $f(p^\alpha) = f(p)^\alpha$ for some α. for $n > 1$.

$$g * f(n) = I(n) = 0 \quad [\because \text{if } n > 1,\ I(n) = 0 \text{ def } I(n)]$$

$$\Rightarrow \sum_{d/n} g(d)\, f(n/d) = 0.$$

$$\Rightarrow \sum_{d/n} \mu(d)\, f(d)\, f(n/d) = 0 \quad \text{where } g(n) = f^{-1}(n).$$

Take $n = p^\alpha$.

$$\Rightarrow \sum_{d/p^\alpha} \mu(d)\, f(d)\, f\left(p^\alpha/d\right) = 0.$$

$$\Rightarrow \mu(1) f(1) f(p^\alpha) + \mu(p) f(p) f(p^{\alpha-1}) = 0.$$

($\because 1, p, p^2, \ldots p^\alpha$ are the divisor of n and $\mu(p^\alpha) = 0$ for $\alpha \geq 2$).

$$\Rightarrow 1.1\, f(p^\alpha) + (-1)^k f(p)\, f(p^{\alpha-1}).$$

$$\therefore f(p^\alpha) = f(p)\, f(p^{\alpha-1})$$

$$= f(p)\, f(p^{\alpha-2} p)$$

$$= f(p)\, f(p)\, f(p^{\alpha-2}).$$

$= f(p)\, f(p)\, f(p)\, f(p^{\alpha-2})$

$= f(p)\, f(p) \cdots f(p^{\alpha})$.

$f(p^{\alpha}) = f(p)^{\alpha}$.

Hence f is completely multiplicative.

Eg:

(iv) find the inverse euler's φ function.

Soln:

W.K.T $\varphi(n) = \sum_{d/n} \mu(d)\left(n/d\right)$ and $N(n) = n$ ---> (2)

using (2) (1) $\Rightarrow \varphi(n) = \sum_{d/n} \mu(d)\, N(n/d)$

$= (\mu * N)(n)$ (∵ By the Def Dirchlet product).

(1,e) $\varphi = \mu \times N$.

$\varphi^{-1} = \mu^{-1} * N^{-1}$

$= u * N^{-1}$ (∵ $\mu^{-1} = u$)

$= u * (\mu N)$ (∵ N i completely multiple $N^{-1}(n) = \mu(n)$.

$= (\mu N) * u$ (∵ Dirchelet product is commulative)

$\varphi^{-1}(n) = (\mu N * u)(n)$.

$= \sum_{d/n} \mu N(d)\, u(n/d)$.

$$= \sum_{d|n} \mu N(d) = 1.$$

$$= \sum_{d|n} \mu(d) N(d)$$

Thm :

If f is multiplicative we have $\sum_{d|n} \mu(d) f(d)$

$$= \prod_{p|n} (1 - f(p)).$$

Prof :

Let $g(n) = \sum_{d|n} \mu(d) f(d)$.

To prove $g(n) = \prod_{p|n} (1 - f(p))$.

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

$$= \prod_{p=1}^{ik} p_i^{\alpha_i}$$

$$= \prod p^{\alpha}.$$

$$g(n) = g\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right)$$

$$g(n) = \prod_{d|p^{\alpha}} g(p^{\alpha}).$$

$$g(p^{\alpha}) = \sum_{d|p_i^{\alpha}} \mu(d) f(d).$$

$d|p^{\alpha} \Rightarrow d = 1$ or $d = p^{\alpha}$.

$$g(p^{\alpha}) = \mu(1) f(1) + \mu(p^1) f(p^1) + \mu(p^2) f(p^2)$$

$= 1.1 + (-1) f(p) + 0 + 0 \cdots$

$= 1 - f(p)$.

$$g(n) = \prod_{d \mid p^\alpha} (1 - f(p)).$$

$$g(n) = \prod_{d \mid n} (1 - f(p)).$$

Def:

we define $\lambda = (1) = 1$. and if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

we define $\lambda(n) = (-1)^{\alpha_1 + \alpha_2 + \cdots + \alpha_k}$.

Note: λ is completely multiplicative.

Thm:

for every $n \geq 1$, we have $\sum_{d \mid n} \lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a square} \\ 0 & \text{otherwise} \end{cases}$

Also $\lambda^{-1}(n) = |\mu(n)|$ for all n.

Pf:

Let $g(n) = \sum_{d \mid n} \lambda(d)$.

Then g is multiplicative.

we compute $g(p^\alpha)$ for prime powers

$$g(p^\alpha) = \sum_{d \mid p^\alpha} \lambda(d).$$

$$= \lambda(1) + \lambda(p^1) + \lambda(p^2) + \cdots + \lambda(p^\alpha).$$

$$= 1 + (-1)^1 + (-1)^2 + \cdots + (-1)^\alpha$$

$$g(p^{\alpha}) = \begin{cases} 1 & \text{if } \alpha \text{ is even} \\ 0 & \text{if } \alpha \text{ is odd} \end{cases}$$

Hence if $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

we have $g(n) = \prod_{i=1}^{k} g(p_i^{\alpha_i})$

if any exponent α_i is odd then $g(p_i^{\alpha_i}) = 0$.

$\therefore g(n) = 0$.

If all the components α_i are even.

Then $g(p_i^{\alpha_i}) = 1$ for all i.

$g(n) = 1$.

This implies $g(n) = \begin{cases} 1 & \text{if } n \text{ is a Square} \\ 0 & \text{otherwise.} \end{cases}$

Also $\lambda^{-1}(n) = \mu(n) \cdot \lambda(n)$.

Since λ is multiplicative.

from the $\lambda^{-1}(n) = \mu(n)\,\mu(n)$

$= \mu^2(n)$

$= |\mu(n)|$

Hence the proof.

The divisor function $\sigma_\alpha(n)$.

Def:

For real or complex α and any integer $n \geq 1$ we define $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$, the sum of the α th powers of the divisor of n.

The function σ_α are called divisor functions.

8^0 Divisors functions are multiplicative Because $\sigma_\alpha = u * N$. The Dirichelt product of two multiplicati -ve functions

(i) when $\alpha = 0$, $\sigma_0(n)$ is the number of divisors of n this is denoted by $d(n)$.

(ii) when $\alpha = 1$ $\sigma_1(n)$ is the sum of the divisors of n and its denoted by $\sigma(n)$.

$\therefore \sigma_\alpha$ is multiplicative.

we have $\sigma_\alpha(p_1^{\alpha_1}, p_2^{\alpha_2} \ldots p_k^{\alpha_k}) = \sigma_\alpha(p_1^{\alpha_1}) \sigma_\alpha(p_2^{\alpha_2}) \ldots \sigma_\alpha(p_k^{\alpha_k})$

Compute $\sigma_\alpha(p^\alpha)$.

The divisors of a prime power p^α are $1, p_1, p^2 \ldots p^\alpha$.

The Dirichelet inverse of σ_α can be expressed as the Linear combination of the α th powers of the divisors of n.

Thm:- for $n \geq 1$ we have

$$\sigma_\alpha^{-1}(n) = \sum_{d|n} d^\alpha \mu(d) \cdot \mu(n/d)$$

prf:-

from the def of the divisors function.

$$\text{W.K.T} \quad \sigma_\alpha(n) = \sum_{d|n} d^\alpha$$

$$= \sum_{d|n} N^\alpha(d)$$

$$= \sum_{d|n} N^\alpha(d) \cdot \mu(n/d)$$

$$= (N^\alpha * \mu)(n).$$

N^α is Completly multiplicative.

$$\sigma_\alpha^{-1} = (\mu N^\alpha) * u^{-1} \quad (\because N^{\alpha-1} = \mu N^\alpha).$$

$$= \mu N^\alpha * \mu \quad (\mu * u = I)$$

$$= \sum_{d|n} (\mu N^\alpha)(d) \cdot \mu(n/d)$$

$$= \sum_{d|n} \mu(d) N^\alpha(d) \cdot \mu(n/d)$$

$$= \sum_{d|n} \mu(d)\, d\, \mu(n/d)$$

$$= \text{RHS}.$$

Generalized convolutions

Define a function G on $(0, +\infty)$ which also generator for $0 < \alpha < 1$ we denote the function G by $\alpha \circ f$. Thus $(\alpha \circ f)(x) = \sum_{n \le x} \alpha(n) f\left(\frac{x}{n}\right)$.

Note:

If $f(x) = 0$ $\forall$ non integral x the restriction of f to the integer is an arithmatical function and we find that $(\alpha \circ f)(x) = (\alpha \circ f)(m)$ for all integer $m \ge 1$.

So the operation can be regarded as a generali-zation the Dirichlet convolution.

The operation $\circ$ is sig. in general neighther commutative nor associative.

Associative property relating $\circ$ and $*$ for every arithmatical function α and β we have $\alpha \circ (\beta \circ f)$

$= (\alpha * \beta) \circ f$.

Pf:

To prove $\alpha o (\beta o f) = (\alpha * \beta) o f$.

W.K.T $(f * g)(n) = \sum_{d|n} f(d) g(n/d)$

$$(\alpha o f)(x) = \sum_{n \le x} \alpha(n) f\left(\frac{x}{n}\right)$$

LHS.

for $x > 0$ we have

$$\{\alpha o (\beta o f)\}(x) = \sum_{n \le x} \alpha(n) (\beta o f)\left(\frac{x}{n}\right)$$

$$= \sum_{n \le x} \alpha(n) \sum_{m \le x/n} \beta(m) f\left(\frac{x}{mn}\right)$$

$$= \sum_{mn \le x} \alpha(n) \beta(m) f\left(\frac{x}{mn}\right)$$

$$= \sum_{k \le x} \left(\sum_{n|k} \alpha(n) \beta\left(\frac{k}{n}\right) \right) f\left(\frac{x}{k}\right)$$

$$= \sum_{k \le x} (\alpha * \beta)(k) f\left(\frac{x}{k}\right)$$

$$= \{(\alpha * \beta) o f\}(x).$$

Note:

The indentity function $I(n) = (1/n)$ for Dirichlet Convellution is also a left identity for the operatio

(i.e) we have $(I o f)(n) = \sum_{n \le x} I(n) f\left(\frac{x}{n}\right)$

$$= \sum_{n \le x} \left[\frac{1}{n}\right] f(x/n) = f(x).$$

Thm :-

Generalized inversion formula :-

Statements :

If α has a dirichelt inverse then the eqn

$G(x) = \sum_{n \le x} \alpha(n) f(x/n)$ ---> ① implies

$f(x) = \sum_{n \le x} \alpha^{-1}(n) G(x/n)$ ---> ② conversely ② implies ①.

pf :-

We know that $(\alpha \circ f)(n) = \sum_{n \le x} \alpha(n) f\left(\frac{x}{n}\right)$

If α has a Dirichelet inverse α^{-1}.

Then $\alpha * \alpha^{-1} = I$.

If $G = \alpha \circ f$.

Then $\alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ f)$

$= (\alpha^{-1} * \alpha) \circ f$

$= I \circ f = f$.

$\alpha^{-1} \circ G = f$.

(ii) $f(x) = (\alpha^{-1} \circ G)(x)$

$= \sum_{n \le x} \alpha^{-1}(n) g(x/n)$.

Hence (i) => (ii)

formal power series.

(i) Power Series :

An infinite series of the form $\sum_{n=0}^{\infty} a(n)\, x^n$

$= a(0) + a(1)x + a(2)x^2 + \ldots + a(n)x^n$. is called a power series in x. Both x and the coefficients $a(n)$ are real or complex numbers. To each power series there corresponds a radius of convergence $r \geq 0$. such that the series converges absolutely if $|x| < r$ and diverges if $|x| > r$ (r can be ∞).

(ii) The symbol x^n is simply a device for locating the position of the nth coefficient $a(n)$. the coefficient $a(0)$ is called the <u>constant coefficient</u> of the series.

(iii) If $A(x)$ and $B(x)$ are two formal series say $A(x) = \sum_{n=0}^{\infty} a(n)\, x^n$ and $B(x) = \sum_{n=0}^{\infty} b(n)\, x^n$

we define equality : $A(x) = B(x)$ means that $a(x) = b(x)$ for all $n \geq 0$. sum : $A(x) + B(x) = \sum_{n=0}^{\infty} (a(n) + b(n))\, x^n$.

product : $A(x)B(x) = \sum_{n=0}^{\infty} c(n)\, x^n$, where

$$c(n) = \sum_{k=0}^{n} a(k)\, b(n-k). \quad \text{--->} (1)$$

The sequence $\{c(n)\}$ determined by eqn (1) is called the cauchy product of the sequences $\{a(n)\}$ and $\{b(n)\}$.

formal power series from a ring. The ring has a zero element for addition which we denote by 0.

$$0 = \sum_{n=0}^{\infty} a(n)\, x^n, \text{ where } a(n) = 0 \ \forall\ n \geq 0.$$

and an identity element for multiplication which we denote by 1.

$$1 = \sum_{n=0}^{\infty} a(n)\, x^n, \text{ where } a(0) = 1 \ \forall\ n \geq 1.$$

Def:

A formal power series is called a formal polynomial all its coefficients are zero from some point on.

Inverse:

for each formal power series $A(x) = \sum_{n=0}^{\infty} a(n)\, x^n$. with constant coefficient $a(0) \neq 0$.

there is uniquly determined normal power series

$B(x) = \sum_{n=0}^{\infty} b(n)\, x^n$ such that $A(x) \cdot B(x) = 1$

It's coefficient can be determined by solving the finite system of equations.

$$a(0)\,b(0) = 1.$$

$$a(0)\,b(1) + a(1)\,b(0) = 0.$$

$$a(0)\,b(0) + a(1)\,b(1) + a(2)\,b(0) = 0.$$

$$\vdots$$

in succession for $b(0), b(1), b(2) \ldots$

the series $B(x)$ is called the inverse of $A(x)$ and its denoted by $B(x) = A(x)^{-1}$ (or)

$$\boxed{B(x) = \frac{1}{A(x)}}$$

Defn:

The series $A(x) = 1 + \sum_{n=1}^{\infty} a^n x^n$ is called a Geomentric series. It's inverse k the formal polynomial $B(x) = 1 - ax$. In otherwords

$$\boxed{\frac{1}{B(x)} = \frac{1}{1-a(x)} = A(x) = 1 + \sum_{n=1}^{\infty} a^n x^n.}$$

The Bell series of an arithmetical function

Def: Bell series :-

Given an arithmetical function f and a prime p we denote by $f_p(n)$ the formal power

Series $f_p(x) = \sum_{n=0}^{\infty} f(p^n) x^n$ and call this the Bell Series of f modulo p.

Uniqueness theorem :-

Let f and g be multiplicative functions then $f = g$ iff $f_p(x) = g_p(x)$ for all primes p.

Pf :-

Let us assume that $f = g$.

Then $f(p^n) = g(p^n)$ for all p and all $n \geq 0$.

$$f(p^n) x^n = g(p^n) x^n.$$

$$\sum_{n=0}^{\infty} f(p^n) x^n = \sum_{n=0}^{\infty} g(p^n) x^n.$$

$$f_p(x) = g_p(x).$$

Conversely

If $f_p(n) = g_p(n)$

Then $f(p^n) = g(p^n)$ for all $n \geq 0$.

$\therefore$ f and g are multiplicative functions.

$$f = g.$$

Hence the proof.

Eg : 1

Mobius function μ.

$\mu(p) = (-1)^1$ and $\mu(p^n) = 0$ for $n \geq 2$.

find $\mu_p(x)$.

Soln :-

$$f_p(x) = \sum_{n=0}^{\infty} f(p^n) x^n$$

$$\mu_p(x) = \sum_{n=0}^{\infty} \mu(p^n) x^n$$

$$= 1 - x.$$

Eg :- Euler totient function φ.

Let $\varphi(p^n) = p^n - p^{n-1}$ for $n \geq 1$, find $\varphi_p(x)$.

Soln :-

$$f_p(x) = \sum_{n=0}^{\infty} f(p^n) x^n.$$

$$\varphi_p(x) = \sum_{n=0}^{\infty} \varphi(p^n) x^n.$$

$$= 1 + \sum_{n=1}^{\infty} \varphi(p^n) x^n.$$

$$= 1 + \sum_{n=1}^{\infty} [p^n - p^{n-1}] x^n.$$

$$= 1 + \sum_{n=1}^{\infty} p^n x^n - x \sum_{n=1}^{\infty} p^{n-1} x^{n-1}$$

$$= \sum_{n=0}^{\infty} p^n x^n - x \sum_{n=0}^{\infty} p^0 x^0.$$

$$= (1-x) \sum_{n=0}^{\infty} p^n x^n$$

$$= (1-x)\left(1 + px + (px)^2 + \cdots\right)$$

$$= (1-x)(1-px)^{-1}.$$

$$= \frac{1+x}{1-px}.$$

Completely multiplicative functions if f is completly multiplicative find $fp(x)$.

Soln:

$$fp(x) = \sum_{n=0}^{\infty} f(pn)x^n.$$

If f is completely multiplicative $f(pn) = f(p)^n$

$$fp(x) = \sum_{n=0}^{\infty} [f(p)]^n x^n.$$

$$= 1 + f(p)x + (f(p)x)^2 + \cdots$$

$$= (1 - fp(x)]^{-1} = \frac{1}{1 - fp(x)}$$

find $up(x)$

Soln:

$$up(x) = \sum_{n=0}^{\infty} u(pn)x^n.$$

W.K.T $u(pn) = 1.$

$$up(x) = \sum_{n=0}^{\infty} 1 \cdot x^n.$$

$$= 1 + x + x^2 + \cdots$$

$$= (1-x)^{-1} = \frac{1}{(1-x)}$$

(5) find λp $fp(x)$

$$fp(x) = \sum_{n=0}^{\infty} f(p^n)\, x^n.$$

W.K.T $\lambda(p^n) = (-1)^n$

$$\therefore \lambda p(n) = \sum_{n=0}^{\infty} \lambda(p^n) x^n.$$

$$= \sum_{n=0}^{\infty} (-1)^n x^n.$$

$$= (-1)^0 x^0 + (-1)^1 x^1 + (-1)^2 x^2 + \ldots$$

$$= 1 - x + x^2 - \ldots$$

$$= (1+x)^{-1} = 1/1+x.$$

(6) find $\nu p^\alpha(x)$.

$$fp(x) = \sum_{n=0}^{\infty} f(p^n) x^n.$$

$$\nu p^\alpha(x) = \sum_{n=0}^{\infty} \nu(p^{\alpha n})\, x^n.$$

$$= \sum_{n=0}^{\infty} (p)^{n\alpha}\, x^n$$

$$= 1 + p^\alpha x + p^{2\alpha} x^2 + \ldots$$

$$= (1 - x p^\alpha)^{-1} = \frac{1}{1 - x p^\alpha}.$$

(7) find $I_p(x)$.

$$I_p(x) = \sum_{n=0}^{\infty} I(p^x) \cdot x^n$$

$$= \sum_{n=0}^{\infty} \left[\frac{1}{p^n}\right] x^n$$

$$= 1 + 0 + 0$$

$$= 1$$

Bell Series and Dirichlet multiplication.

Thm :-

for any two arithmetical function f and g. Let $h = f * g$ Then for every prime p we have $h_p(x) = f_p(x)$

pf :- w.k.T If f and g are two arithmatical function then their dirichelet product or cdirichilet Convelution to be the arthmetikal function h defined by the eqn $h(n) = (f * g)(n) = \sum_{d|n} f(d)\, g(n/d)$.

used by the bell series.

$$h_p(x) = \sum_{n=0}^{\infty} h(p^n) \cdot x^n.$$

$\because$ the divisors of prime p^n are $1, p, p^2 \ldots p^n$

$$\therefore h(p^n) = \sum_{d|p^n} f(d)\, g(p^n/d)$$

$$= \sum_{k=0}^{n} f(p^k) \cdot g(p^{n-k})$$

The Last Sum is the Cauchy product of the sequence $\{f(p^n)\}$ and $\{g(p^n)\}$.

Ex:1 find $\mu^2 p(x)$.

Soln :-

w.k.T $\lambda^{-1}(n) = \lambda(n)\,\mu(n)$

$= \mu^2(n)$.

$$\therefore \mu^2 p(x) = 1/\lambda p(x) = \frac{1}{(1/1+x)} = 1+x$$

Ex: 2 find $(\sigma_\alpha) p(x)$

w.k.T $\sigma_\alpha = N^\alpha \mu$.

$$(\sigma_\alpha) p(x) = N_p^\alpha(x) \cdot up(x).$$

$$= \frac{1}{1-p^\alpha x} \cdot \frac{1}{1-x}.$$

$$= \frac{1}{1 - x(1+p^\alpha) + p^\alpha x^2}$$

$$= \frac{1}{1 - x\sigma_\alpha(p) + p^\alpha x^2} \quad \left[\because \sigma_\alpha(n) = \sum_{d/n} d^\alpha\right]$$

Let $f(n) = 2^{v(n)}$ where $v(1) = 0$ and $v(n) = k$ if $p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$ then find $fp(x)$.

w.k.T $fp(x) = \sum_{n=0}^{\infty} f(p^n) \cdot x^n$

$$fp(x) = \sum_{n=0}^{\infty} 2^{v(p^n)} \cdot x^n.$$

$$= 2^{v(p^n)} \cdot x^n + \sum_{n=1}^{\infty} 2^{v(p^n)} \cdot x^n$$

$$v(p) = 2^{v(1)} + \sum_{n=1}^{\infty} 2^{v(p^n)} \cdot x^n$$

$$= 1 + \sum_{n=1}^{\infty} 2^1 \cdot x^n = 1 + 2\sum_{n=1}^{\infty} x^n.$$

$$= 1 + 2\left[x + x^2 + \ldots\right]$$

$$= 1 + 2x\left[1 + x + x^2 + \ldots\right]$$

$$= 1 + 2x\left[1 - x\right]^{-1} = 1 + \frac{2x}{1-x}.$$

$$= \frac{1-x+2x}{1-x} = \frac{1+x}{1-x} = \mu p^2(x) \cdot up(x)$$

$$\Rightarrow f = \mu^2 * u.$$

$$\Rightarrow 2^{v(n)} = \sum_{d|n} \mu^2(d).$$

Derivatives of Arithmatical functions.

Def:-

for any arithmatical function f we define is derivative f' to be the arithmatical function given by the eqn. $\boxed{f'(n) = f(n) \log n \quad \text{for } n \geq 1.}$

Ex:- find $I n \log n = ?$

Soln:-

$$I'(n) = I(n) \log n$$

$$= [1/n] \log n.$$

$$= \begin{cases} 1 \cdot \log 1 & ; n = 1 \\ 0 \cdot \log n & ; n > 1 \end{cases}$$

$$= 0.$$

$$u'(n) = u(n) \log n = 1 \times \log n = \log n.$$

Note:-

W.K.T $\log n = \sum_{d|n} n(d)$

$$\Rightarrow u'(n) = (n * u)(n).$$

$$\Rightarrow \boxed{u' = n * u.}$$

If f and g are arithmatical functions we have

a) $(f * g)' = f' + g'$.

b) $(f * g)' = f' * g + f * g'$.

c) $(f^{-1})' = -f' * (f * f)^{-1}$. provided that $f(n) \neq 0$.

Pf:-

a) $(f+g)(n) = f(n) + g(n)$.

$\Rightarrow (f+g)'(n) = f'(n) + g'(n)$.

(i.e) $(f+g)' = f' + g'$.

b) $\log n = \log(d \times n/d)$.

$\log n = \log d + \log(n/d)$.

$(f * g)'(n) = (f * g)\, n \log n$

$= \sum_{d|n} f(d) \cdot g(n/d) \log n$.

$= \sum_{d|n} f(d)\, g(n/d) \log d - \sum_{d|n} f(d)\, g(n/d) \log(n/d)$

$= \sum_{d|n} f'(d)\, g(n/d) + \sum_{d|n} f(d) \cdot g'(n/d)$

$= (f' * g)(n) + (f * g')(n)$

$\therefore (f * g)' = f' * g + g' * f$.

W.K.T $I' = 0 \Rightarrow (f * f^{\circ})' = 0$.

from (b)

$$\Rightarrow f' * f^{-1} + f * f^{-1} = 0.$$

$$\Rightarrow f * f^{-1} = -f' * f^{-1}$$

multiply by f^{-1} on both sides.

we get $f^{-1} * (f * g) = f^{-1} * (-f' * f^{-1})$.

$$f^{-1} = -f' * [f^{-1} * f^{-1}]$$

$$= -f' * [f * f]^{-1}$$

$$(f^{-1})' = -f' * (f * f)^{-1}$$

Hence the proof.

The Selberg identity:

Thm:- for $n \geq 1$, we have.

$$\Lambda(n) \log n + \sum_{d/n} \Lambda(d) \Lambda(n/d) = \sum_{d/n} \mu(d) \log^2 \frac{n}{d}.$$

W.K.T.

$$\Lambda * u = u'. \quad \text{---} \rightarrow (1)$$

Diff (1)

$$\Lambda' * u + \Lambda * u' = u'' \quad \text{---} \rightarrow (2)$$

Sub (3) in (2)

$$\Rightarrow \Lambda' * u + \Lambda * (\Lambda * u) = u''.$$

multiply by $\mu = u^{-1}$

$$[\Lambda' * u] * u^{-1} + [\Lambda * (\Lambda * u)] * u^{-1} = u'' * \mu$$

$$\Lambda' + \Lambda * \Lambda = u'' * \mu.$$

$$\Rightarrow \Lambda(n) \log n + \sum_{d/n} \Lambda(d)\, \Lambda(n/d) = (\log^2 * \mu)(n)$$

$$= \sum_{d/n} \mu(d) \log^2(n/d).$$

Hence the proof.

Unit - III

Averages of Arithmetic functions:

The Arithmetic mean

$$\overline{f}(n) = \frac{1}{n} \sum_{k=1}^{n} f(k)$$

Results:

$$\sum_{k \le x} d(k) = x \log x + (2C-1)x + O(\sqrt{x}) \text{ for all } x \ge 1$$

Here C is euler's Constant defined by

$$C = \lim_{n \to \infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right)$$

→ The Symbol $O\sqrt{x}$ represents an unspecified function of x which grows no faster than some Constant times $\sqrt{x}$.

This is an Example of the "big oh" Notation.

The "Big oh" Notation:

Asymptotic Equality of functions

Definition: Boundedness of function

If $g(x) > 0$ for all $x \geq a$, a constant A

we write

$f(x) = O(g(x))$ to mean that the quotient $\frac{f(x)}{g(x)}$ is bound for $x \geq a$.

That is There exists a Constants $M > 0$ such that $|f(x)| \leq M \cdot g(x)$ for all $x \geq a$.

Definition: (Asymptotic)

If $\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1$

we say that $f(x)$ is Asymptotic to $g(x)$ as $n \to \infty$ and we write

$$f(x) \sim g(x) \quad \text{as} \quad x \to \infty$$

Euler Summation formula

If f has a continuous derivative f' on the interval $[y, x]$ where $0 < y < x$, then

$$\sum_{y \leq n \leq x} f(n) = \int_y^x f(t)\,dt + \int_y^x (t - [t])f'(t)\,dt + f(x)([x] - x) - f(y)([y] - y)$$

proof: Let $m = [y]$; $k = [x]$

For integers n and $n-1$ in $[y, x]$

we have

$$\int_{n-1}^{n} [t] f'(t)\, dt = \int_{n-1}^{n} (n-1) f'(t)\, dt$$

$$= (n-1) \Big[f(t) \Big]_{n-1}^{n}$$

$$= (n-1) \{ f(n) - f(n-1) \}$$

$$= (n-1) f(n) - (n-1) f(n-1)$$

$$= n f(n) - f(n) - (n-1) f(n-1)$$

$$= \{ n f(n) - (n-1) f(n-1) \} - f(n)$$

Swimming from $n = m+1$ to $n = k$

we find $\int_{m}^{k} [t] f'(t)\, dt = \sum_{n=m+1}^{k} \{ n f(n) - (n-1) f(n-1) \}$

$$= \sum_{y < n \le x} f(n)$$

$$\Rightarrow \sum_{y < n \le x} f(n) = -\int_{m}^{k} [t] f'(t)\, dt + k f(k) - m f(x)$$

$$= -\int_{y}^{x} [t] f'(t)\, dt + k f(x) - m f(y)$$

(1)

Consider

$$\int_y^x f(t)\,dt = \Big[t f(t)\Big]_y^x - \int_y^x t f'(t)\,dt$$

$\int u\,dv = uv - \int v\,du$

$u = f(t);\ dv = dt$

$du = f'(t);\ \int dv = \int dt = t$

$v = t$

$$= \Big[x f(x) - y f(y)\Big] - \int_y^x t f'(t)\,dt$$

$$\Rightarrow \int_y^x f(t)\,dt + \int_y^x t f'(t)\,dt - \Big[x f(x) - y f(y)\Big] = 0 \quad \text{— (2)}$$

(1) + (2)

$$\Rightarrow \sum_{y<n\le x} f(n) + 0 = -m f(y) + k f(x) - \int_y^x [t] f'(t)\,dt$$

$$+ \int_y^x f(t)\,dt + \int_y^x t f'(t)\,dt - \Big[x f(x) - y f(y)\Big]$$

$$= \int_y^x f(t)\,dt + \int_y^x \big[t - [t]\big] f'(t)\,dt - m f(y) + k f(x) - x f(x) + y f(y)$$

$$= \int_y^x f(t)\,dt + \int_y^x \big[t - [t]\big] f'(t)\,dt - [y] f(y) + [x] f(x) - x f(x) + y f(y)$$

$$= \int_y^x f(t)\,dt + \int_y^x \big[t - [t]\big] f'(t)\,dt + \big[[x] - x\big] f(x) - \big([y] - y\big) f(y)$$

Hence the proof.

Theorem:

Take $f(t) = \frac{1}{t}$ in Eulers Summation formula and prove that $\sum_{n \le x} \frac{1}{n} = \log x + c + O(1/x)$

proof:

We Know That

$$\sum_{y \le n \le x} f(n) = \int_y^x f(t)\,dt + \int_y^x t - [t] f'(t)\,dt + ([x] - x) f(x) - ([y] - y) f(y).$$

$$\sum_{1 \le n \le x} \frac{1}{n} = 1 + \sum_{1 < n \le x} \frac{1}{n}$$

$$= 1 + \int_1^x \frac{1}{t}\,dt + \int_1^x t - [t] \left(\frac{-1}{t^2}\right) dt + \left([x] - x\right) \frac{1}{x} + C.$$

$$= 1 + [\log t]_1^x - \int_1^x \frac{t - [t]}{t^2}\,dt + \frac{[x] - x}{x} \qquad [\because y - [y] = 1 - 1 = 0]$$

$$= 1 + \log x - \int_1^x \frac{t - [t]}{t^2}\,dt + O(1/x)$$

$$= 1 + \log x - \int_1^\infty \frac{t - [t]}{t^2}\,dt + \int_x^\infty \frac{t - [t]}{t^2}\,dt + O\left(\frac{1}{x}\right)$$

Consider

$$\int_1^\infty \frac{t - [t]}{t^2}\,dt < \int_1^\infty \frac{1}{t^2}\,dt$$

$$= \left[-\frac{1}{t} \right]_1^{\infty}$$

$$= 0 + 1$$

$$= 1 < \infty$$

III^{ly}

$$\int_x^{\infty} \frac{t - [t]}{t^2}\, dt < \left[\frac{-1}{t} \right]_x^{\infty}$$

$$= 0 + \frac{1}{x}$$

$$= \frac{1}{x}$$

$$\therefore \sum_{n \le x} \frac{1}{n} = \log x + 1 - \int_1^{\infty} \frac{t - [t]}{t^2}\, dt + O\left(\frac{1}{x}\right) + O\left(\frac{1}{x}\right)$$

$$= \log x + C + O\left(\frac{1}{x}\right)$$

where $C = 1 - \int_1^{\infty} \frac{t - [t]}{t^2}\, dt + O\left(\frac{1}{x}\right)$ as $x \to \infty$

$$\sum_{n \le x} \frac{1}{n} - \log x = C \text{ and } \frac{1}{x} \to 0$$

$$\sum_{n \le x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$$

Definition:

The Zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{if } s>1 \text{ and}$$

$$\zeta(s) = \lim_{x\to\infty} \left[\sum_{n\le x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \right] \text{ if } 0<s<1$$

Theorem 2:

prove that $\sum_{n\le x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s})$, $s>0$, $s\neq 1$

proof:

We know That

$$\sum_{y<n\le x} f(n) = \int_y^x f(t)\,dt + \int_y^x (t-[t]) f'(t)\,dt$$

$$+ ([x]-x) f(x) - ([y]-y) f(y) \quad \text{---(1)}$$

Take, $f(t) = \frac{1}{t^s}$

$$\sum_{n\le x} \frac{1}{n^s} = 1 + \sum_{1\le n\le x} \frac{1}{n^s}$$

$$= 1 + \int_1^x \frac{1}{t^s}\,dt + \int_1^x t-[t] \left(\frac{-s}{t^{s+1}}\right) dt$$

$$+ ([x]-x)\, x^{-s} + 0$$

$$= 1 + \left[\frac{t^{-s+1}}{-s+1}\right]_1^x - s\int_1^x \frac{t-[t]}{t^{s+1}}\,dt + ([x]-x)\, x^{-s}$$

$$= 1 + \frac{x^{1-s}}{1-s} - s\int_1^x \frac{t - [t]}{t^{s+1}}\,dt + \left([x] - x\right)x^{-s}$$

$$= 1 + \frac{x^{1-s}}{1-s} - \frac{1}{1-s} - s\int_1^x \frac{t-[t]}{t^{s+1}}\,dt + O(x^{-s})$$

$$\left[\because \left|([x]-x)\,x^{-s}\right| \leq \right.$$

Now,

$$\int_1^\infty \frac{(t-[t])}{t^{s+1}}\,dt \leq \int_1^\infty \frac{1}{t^{s+1}}\,dt$$

$$= \left[\frac{t^{-s}}{-s}\right]_1^\infty$$

and $s\int_1^\infty \frac{t-[t]}{t^{s+1}}\,dt \leq s \cdot \frac{1}{s} = 1$

Also,

$$s\int_x^\infty \frac{t-[t]}{t^{s+1}}\,dt = O(x^{-s})$$

$$\therefore \sum_{n \leq x} \frac{1}{n^s} = \frac{-1}{1-s} + \frac{x^{1-s}}{1-s} + 1 - s\int_1^\infty \frac{(t-[t])}{t^{s+1}}\,dt + O(x^{-s})$$

$$= \frac{x^{1-s}}{1-s} + C(s) + O(x^{-s})$$

where

$$C(s) = 1 - s\int_1^{\infty} \frac{t - [t]}{t^{s+1}}\,dt - \frac{1}{1-s} \quad \text{AS } s \to 1 \text{ as } x \to$$

$$\sum_{n \le x} \frac{1}{n^s} = C(s)$$

$$\left[\because x^{1-s} \to 0 \text{ as } x \to \infty\right]$$

i.e) $f(s) = C(s)$

If $0 < s < 1$, Then,

$$\sum_{n \le x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} = C(s) + O(x^{-s})$$

$$\lim_{x \to \infty} \left(\sum_{n \le x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \right) = C(s)$$

i.e) $f(s) =$

Hence

$$\sum_{n \le x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + f(s) + O(x^{-s})$$

if $s > 0, s \neq 1$

Theorem 3 :

For $x \ge 1$, we have $\sum_{n > x} \frac{1}{n^s} = O(x^{1-s})$

if $s > 1$

proof:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n \le x} \frac{1}{n^s} + \sum_{n > x} \frac{1}{n^s}$$

$$= \frac{x^{1-s}}{1-s} + f(s) + O(x^{-s}) + \sum_{n>x} \frac{1}{n^s}$$

(by previous theorem)

$$\sum_{n>x} \frac{1}{n^s} = -\frac{x^{1-s}}{1-s} - f(s) + O(x^{-s}) + \sum_{n=1}^{\infty} \frac{1}{n^s}$$

But $f(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ if $s > 1$

$$\therefore \sum_{n>x} \frac{1}{n^s} = \frac{x^{1-s}}{s-1} - f(s) + O(x^{-s}) + f(s)$$

$$= \frac{x^{1-s}}{s-1} + O(x^{-s})$$

$$\sum_{n>x} \frac{1}{n^s} = O(x^{1-s}) \quad \left(\because x^{-s} \le x^{1-s}\right)$$

Hence the Theorem.

Theorem A:

For $x \geq 1$, we have $\sum_{n \leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha})$

proof:

Take $f(t) = t$ in the euler Summation formula

Then $\sum_{n \leq x} n^{\alpha} = 1 + \sum_{1 < n \leq x} n^{\alpha}$

$$= 1 + \int_1^x t^{\alpha} dt + \int_1^x (t - [t]) \alpha t^{\alpha-1} dt + ([x] - x) x^{\alpha}$$

$$= 1 + \left[\frac{t^{\alpha+1}}{\alpha+1}\right]_1^x + \alpha \int_1^x (t - [t]) t^{\alpha-1} dt + O(x^{\alpha})$$

$$= 1 + \left[\frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1}\right] + \alpha \int_1^{\infty} (t - [t]) t^{\alpha-1} dt$$

$$- \alpha \int_x^{\infty} (t - [t]) t^{\alpha-1} dt + O(x^{\alpha})$$

Now, $\alpha \int_1^{\infty} (t - [t]) t^{\alpha-1} dt \leq \alpha \int_1^{\infty} t^{\alpha-1} dt$

$$= \alpha \left[\frac{t^{\alpha}}{\alpha}\right]_1^{\infty}$$

$$= \alpha \cdot \frac{1}{\alpha} = 1$$

$$\alpha \int_x^{\infty} t - [t] \, t^{\alpha-1} dt \leq \alpha \left[\frac{t^{\alpha}}{\alpha}\right]_x^{\infty}$$

$$= \alpha \cdot \frac{x^\alpha}{\alpha} \qquad (\because O(1) = O(x^0))$$

$$= x^\alpha$$

$$\sum_{n \le x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha)\, n$$

Theoram :

For all $x \ge 1$, $\sum_{n \le x} d(n) = x \log x + (2C-1)\, x + O(\sqrt{x})$ where C is Euler's Constant

proof :

Since $d(n) = \sum_{d(n)} 1$

We have, $\sum_{n \le \alpha} d(n) = \sum_{n \le \alpha} \sum_{d/n} 1$

This is a double Sum extended over n and d.

Since $\frac{d}{n}$ we can write

$n = qd$ and extend the Sum overall pairs of positive integers q, d with $qd \le \alpha$.

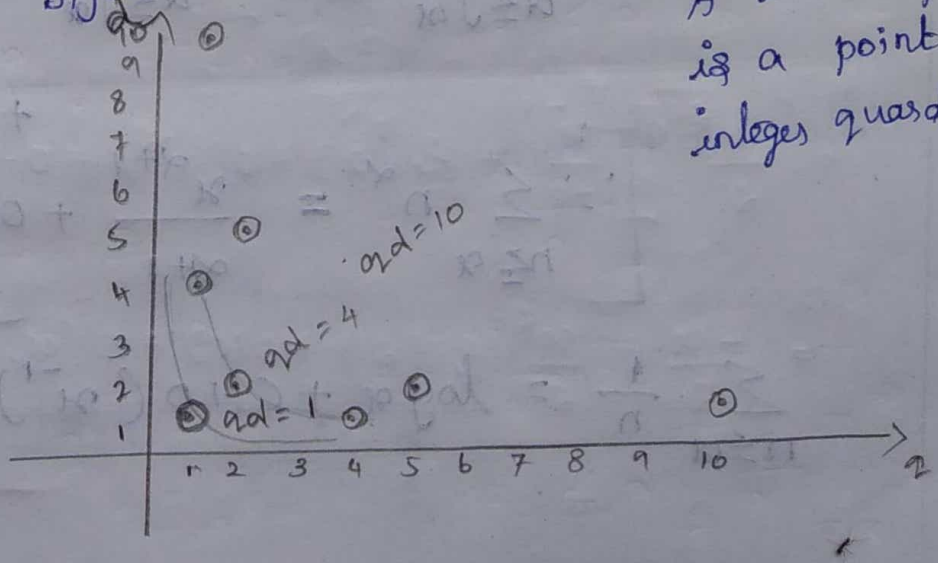
Thus $\sum_{n \le x} d(n) = \sum_{\substack{q,d \\ qd \le x}} 1$ — (1)

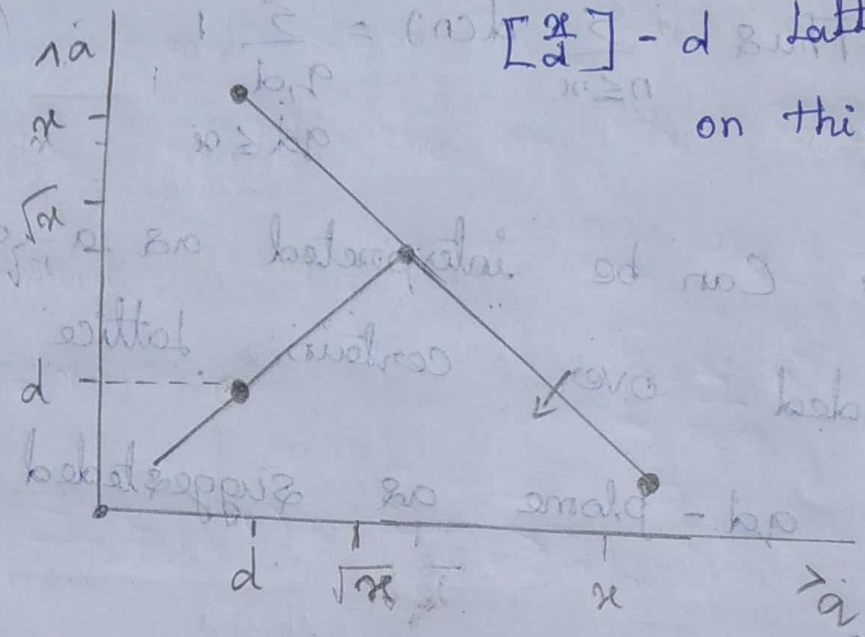
This can be interpreted as a sum extended over certain lattice points in qd-plane as suggested by the figure.

The lattice points with $qd = n$ lie on a hyperbola. So the sum in (1) counts the numbers of lattice points which lie on the hyperbola corresponding to $n = 1, 2 \ldots [x]$

By symmetry of the hyperbola region about the line $q = d$ and the number of lattice points twice below the line $q = d$ and the no of lattice points on the bijection Line segment

A lattice point is a point with integer quardinate





$[\frac{x}{d}] - d$ lattice points on this segment

$$\sum_{n \le x} d(n) = 2 \sum_{d \le \sqrt{x}} \left\{ \left[\frac{x}{d} \right] - d \right\} + [\sqrt{x}]$$

Since $|[y] - y| \le 1$

$$[y] - y = O(1)$$

we have $[y] = y + O(1)$

$$\sum_{n \le x} d(n) = 2 \sum_{d \le \sqrt{x}} \left\{ \frac{x}{d} + O(1) - d \right\} + O\sqrt{x}$$

$$= 2x \sum_{d \le \sqrt{x}} \frac{1}{d} - 2 \sum_{d \le \sqrt{x}} d + 2 \sum_{d \le 1} O(1) + O(\sqrt{x})$$

$$\left[\because \sum_{n \le x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha}) \right.$$

$$\left. \sum_{n \le x} \frac{1}{n} = \log x + C + O(x^{-1}) \right]$$

$$\sum_{n\le x} d(n) = 2x\left\{\log\sqrt{x} + c + O\left(\frac{1}{\sqrt{x}}\right)\right\} - 2\left\{\frac{(\sqrt{x})^2}{2} + O(\sqrt{x})\right\} + O(\sqrt{x})$$

$$= x\log(\sqrt{x})^2 + 2cx + 2\sqrt{x}\cdot\sqrt{x}\cdot O\left(\frac{1}{\sqrt{x}}\right) - (\sqrt{x})^2 - 2\cdot O\sqrt{x} + O\sqrt{x}$$

$$= x\log x + (2c-1)x + (O\sqrt{x})$$

---

1) For $x \ge 1$, we have

$$\sum_{n\le x} \sigma_1(n) = \frac{1}{2}\zeta(2)x^2 + O(x\log x)$$

Soln:

$$\sigma_1(n) = \sum_{d/n} d = \sum_{q/n} q$$

$$\sum_{n\le x} \sigma_1(n) = \sum_{n\le x}\sum_{d/n} d$$

$$= \sum_{qd} q, \text{ where } qd = n$$

$$qd \le x$$

∴ we take the sum over this lattice poi

Since $qd \le x$

we have $1 \le q \le \frac{x}{d}$

For fixed $d \leq x$, we count the no of lattice points lie on the horizontal line segment $1 \leq q \leq x/d$ and the sum over $d \leq x$

$$\left[\because \sum_{n \leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha})\right]$$

$$\sum_{n \leq x} \sigma_1(x) = \sum_{d \leq x} \sum_{q \leq x/d} q$$

$$\sum_{n \leq x} \sigma_1(n) = \sum_{d \leq x} \left\{ \frac{(x/d)^{1+1}}{1+1} + O\left(\frac{x}{d}\right) \right\}$$

$$= \frac{x^2}{2} \sum_{d \leq x} \frac{1}{d^2} + O\left(\sum_{d \leq x} (x/d)\right)$$

$$\left[\because \sum_{n \leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s})\right.$$

$$\left.\sum_{n \leq x} \frac{1}{n} = \log x + c + O(1/x)\right]$$

$$\therefore \sum_{n \leq x} \sigma_1(n) = \frac{x^2}{2}\left[\frac{x^{1-2}}{1-2} + \zeta(2) + O(x^{-2})\right] + O\left[x \log x + c + O\left(\frac{1}{x}\right)\right]$$

$$= \frac{x^2}{2}\left[\frac{x^{-1}}{-1} + \zeta(2) + O(x^{-2}) + O\left\{x \log x + c + O(1/x)\right\}\right.$$

$$= \frac{-x}{2} + \frac{x^2}{2}\zeta(2) + O(1) + O(x \log x) + O(x) + O(1)$$

$$= \frac{x^2}{2} \zeta(2) + O(x) + O(1) + O\left[x \log x + O(x) + O(1)\right]$$

$$= \frac{x^2}{2} \zeta(2) + O(x \log x)$$

Hence $\sum_{n \le x} \sigma_1(n) = \frac{x^2}{2} \zeta(2) + O(x \log x)$

For $x > 1$, $\sum_{n \le x} \varphi(n) = \frac{3}{\pi^2} x^2 + O(x \log x)$

(or) prove that the average order of $\varphi(n)$ is $\frac{3n}{\pi^2}$

proof:

we have $\varphi(n) = \sum_{d|n} \mu(d) \cdot n/d$

$$\sum_{n \le x} \varphi(n) = \sum_{n \le x} \sum_{d|n} \mu(d) \cdot n/d$$

$$= \sum_{\substack{q,d \\ qd \le x}} \mu(d) \cdot q \cdot$$

$$\left(\sum_{n \le x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha) \right)$$

$$= \sum_{d \le x} \mu(d) \sum_{q \le x/d} q$$

$$= \sum_{d \le x} \mu(d) \left\{ \left(\frac{x}{d}\right)^2 \frac{1}{2} + O(x/d) \right\}$$

$$= \sum_{d \le x} \mu(d) \frac{x^2}{2} \cdot \frac{1}{d^2} + O\left(\sum_{d \le x} \mu(d) \, x/d \right)$$

$$= \frac{x^2}{2} \sum_{d \le x} \frac{\mu(d)}{d^2} + O\left[x \cdot \sum_{d \le x} \frac{\mu(d)}{d} \right]$$

$$\left(\because \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} = \frac{1}{\zeta(2)} \right)$$

i.e) $$\sum_{n \le x} \frac{\mu(n)}{\pi^2} + \sum_{n > x} \frac{\mu(n)}{\pi^2} = \frac{6}{\pi^2}$$

$$\therefore \sum_{n \le x} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} - \sum_{n > x} \frac{\mu(n)}{n^2}$$

$$= \frac{6}{\pi^2} + O\left(\sum_{n > x} \frac{1}{n^2} \right)$$

$$= \frac{6}{\pi^2} + O(x^{-1})$$

$$\therefore \sum_{n \le x} \varphi(n) = \frac{1}{2} x^2 \left[\left\{ \frac{6}{\pi^2} + O\left(\frac{1}{x}\right) \right\} + O\left(x \sum_{d \le x} \frac{1}{d} \right) \right]$$

$$= \frac{3x^2}{\pi^2} + O(x) + O\left[x \left\{ \log x + C + O\left(\frac{1}{x}\right) \right\} \right]$$

$$\therefore \sum_{n \le x} \varphi(n) = \frac{3x^2}{\pi^2} + O(x \log x)$$

An application to the distribution of Lattice points visible from the origin.

Definition : Mutually visible

Two lattice point ~~pornd~~ p and Q are said to be Mutually visible if the line segment which joints them contains no lattice points other than the end point p and Q.

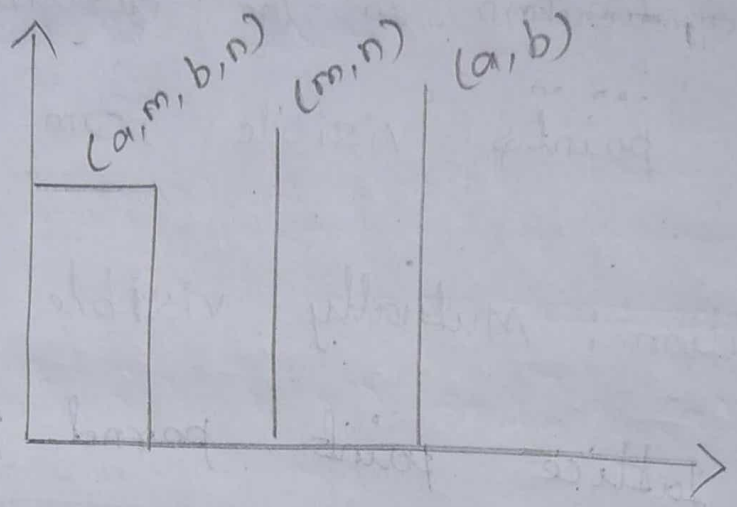
Theorem :

Two lattice points (a, b) and (m, n) are mutually visible iff (a-m) and (b-n) are relatively prime.

proof

Given (a, b) and (m, n) are mutually visible.

$\Rightarrow$ (a-m), (b-n) are visible from the origin.



$(m,n) = (0,0)$

a, b is visible from the origin

$\therefore (a-0, b-0) = 1$

i.e) $(a,b) = 1$

So we assume $(m,n) = (0,0)$

Let (a,b) is visible from the origin

Let $(a,b) = d$

We have to prove That $d = 1$

Suppose $d > 1$, Then

$a = da'$ and $b = db'$

So the Lattice points (a', b') lies on the line segment joining $(0,0)$ and (a,b)

which is a Contradiction

$\therefore \boxed{d = 1}$

Hence $(a, b) = 1$

i.e) $(a-0, b-0) = 1$

$\Rightarrow (a-m, b-n) = 1$

Conversely,

Suppose $(a, b) = 1$

Suppose (a, b) is not visible from the origin.

Suppose (a, b) be a point lies in the line segment joining $(0, 0)$ and (a, b)

$\therefore a' = ta \; ; \; b' = tb$ where $0 < t < 1$

Since t is rational

Let $t = s/r \; ; (s, r) = 1$

Then $a' = s/r \cdot a \; ; \; b' = s/r \cdot b$

i.e) $sa = a'r$ and $sb = b'r$

But $(s, r) = 1$

So, r/a and r/b

i.e) $(a, b) = r$

which is $\Rightarrow\Leftarrow$ $(\because (a,b)=1)$

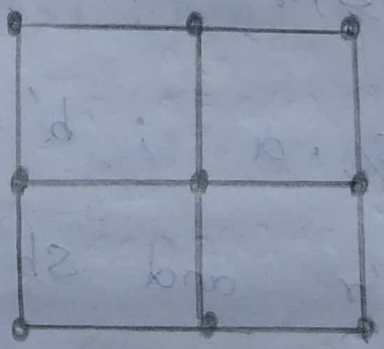
$\therefore$ (a,b) is visible from the origin

Definition : $N(r)$ and $N'(r)$

Consider the largest square region in the xy plane.

Defined by the inequalities $|x| \leq r$ and $|y| \leq r$

Let $N(r)$ denote the no. of lattice points lies in the square and $N'(r)$ denote the no of lattice points are visible from the origin.



Theorem:

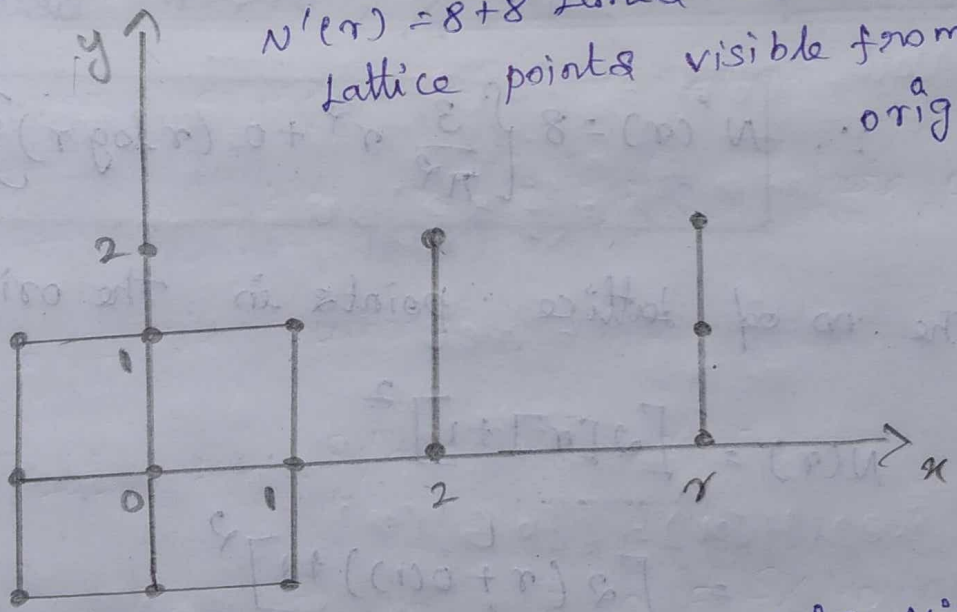
The set of all lattice points visible from the origin has density $\frac{6}{\pi^2}$

proof: We have to prove that

$$\lim_{r\to\infty} \frac{N'(r)}{N(r)} = \frac{6}{\pi^2}$$

The set of 8 lattice points are visible from the origin.

$N'(r) = 8+8$ times the Number of lattice points visible from the origin.



The Number of lattice points visible from the region is

$$\{(x,y) : 2 \le x \le r \; ; \; 1 \le y \le x\}$$

$$N'(r) = 8+8 \sum_{2\le x\le r} \sum_{1\le y\le x} 1$$

$$= 8 + 8 \sum_{2 \le n \le r} \sum_{1 \le m \le n} 1 \qquad (\because (m,n) = 1)$$

$$= 8 + 8 \sum_{2 \le n \le r} \varphi(n)$$

$$= 8 \left\{ 1 + \sum_{2 \le n \le r} \varphi(n) \right\}$$

$$= 8 \left\{ \varphi(1) + \sum_{2 \le n \le r} \varphi(n) \right\}$$

$$= 8 \sum_{1 \le n \le r} \varphi(n) \quad \text{---} \quad (1)$$

But $\sum_{n \le r} \varphi(n) = \frac{3}{\pi^2} r^2 + O(r \log r)$

$$\therefore \boxed{N'(r) = 8 \left\{ \frac{3}{\pi^2} r^2 + O(r \log r) \right\} \text{ by } (1)}$$

The no of lattice points in the origin is

$$N(r) = [2[r] + 1]^2$$

$$= [2(r + O(1)) + 1]^2$$

$$= (2r + O(1) + 1)^2$$

$$= (2r + (O(1))^2$$

$$= 4r^2 + 4r\, O(1) + O(1)^2$$

$$\boxed{N(r) = 4r^2 + O(r)} \quad \text{---} \quad (2)$$

Now $\frac{N'(x)}{N(x)} = \frac{2A\pi^x/\pi^2 + O(x\log x)}{Ax^2 + O(x)}$

$$= \frac{A\left(\frac{6x}{\pi^2}\right) + O\left(\frac{\log x}{x}\right)}{Ax^2 + O(1/x)}$$

Divide both x^2

$$= O(x\log x) = O\left(\frac{x^2\log x}{x}\right)$$

$$= \frac{6/\pi^2 + O(\log x/x)}{1 + O(1/x)}$$

Also $x \to \infty$, $1/x \to 0$ and $\frac{\log x}{x} \to 0$

$$\therefore \lim_{x\to\infty} \frac{N'(x)}{N(x)} = \frac{6}{\pi^2}$$

Theorem :

Let $F(x) = \sum_{n\le x} f(n)$, $G(x) = \sum_{n\le x} g(n)$

and Let $h = f \times g$ and $H(x) = \sum_{n\le x} h(x)$

Then $H(x) = \sum_{n\le x} f(n)$, $G(x/n) = \sum_{n\le x} g(n)F\left(\frac{x}{n}\right)$

Proof :

Let $U(x) = \begin{cases} 0 & \text{if } 0 < x < 1 \\ 1 & \text{if } x \geq 1 \end{cases}$

Now, $(f * U)(x) = \sum_{n \leq x} f(n) \cdot U(x/n)$

$\left[\because n \leq x, \frac{x}{n} > 1, U(x/n) = 1\right]$

$(fU)(x) = \sum_{n \leq x} f(n) = F(x)$

i.e) $F = fU$

III'y $G = gU$

Now, $fG = f(gU)$

$= (f * g)U$

$= hU$

$= H$

i.e) $H(x) = (fG)(x)$

$= \sum_{n \leq x} f(n) \cdot G\left(\frac{x}{n}\right)$

III'y $gF = H$

$H(x) = (gF)(x)$

$H(x) = \sum_{n \leq x} g(n) \cdot F\left(\frac{x}{n}\right)$

Theorem :

If $F(x) = \sum_{n \le x} f(n)$ we have,

$$\sum_{n \le x} \sum_{d/n} f(d) = \sum_{n \le x} f(n) \left[\frac{x}{n}\right] = \sum_{n \le x} F\left(\frac{x}{n}\right)$$

proof :

If $g(n) = 1$. Then $G(x) = \sum_{n \le x} g(n)$

$$= \sum_{n \le x} \log n = \log 1 + \log 2 + \cdots + \log [x]$$

$$= \log (1, 2, \ldots [x])$$

$$= \log [x]!$$

$$\sum_{n \le x} \nu(n) \left[\frac{x}{n}\right] = \log [x]!$$

Theorem :

For all $x \ge 1$, $\left| \sum_{n \le x} \frac{\mu(n)}{n} \right| \le 1$ with equality holds only if $x < 2$.

proof

Given, If $x \le 2$ then takes the value and so, $\mu(1) = 1$

Hence the equality holds.

Assume $x \geq 2$

Let $\{y\} = y - [y]$

$$1 = \sum_{n \leq x} \mu(n) \left[\frac{x}{n}\right]$$

$$1 = \sum_{n \leq x} \mu(n) \left[\frac{x}{n} - \left[\frac{x}{n}\right]\right]$$

$$1 = x \sum_{n \leq x} \frac{\mu(n)}{n} - \sum_{n \leq x} \mu(n) \left\{\frac{x}{n}\right\} \quad \text{—} (1)$$

But $0 < \{y\} < 1$

$$(1) \Rightarrow \left| x \sum_{n \leq x} \frac{\mu(n)}{n} \right| = \left| 1 + \sum_{1 \leq x} \mu(n) \left\{\frac{x}{n}\right\} \right|$$

$$= 1 + \sum_{n \leq x} \left\{\frac{x}{n}\right\} \quad (\text{since } |\mu(n)| \leq 1)$$

$$= \sum_{n \leq x} 1$$

$$= [x]$$

Now $$\sum_{n \leq x} F\left[\frac{x}{n}\right] = \sum_{n \leq x} g(n) f\left[\frac{x}{n}\right]$$

$$H(x) = \sum_{n \leq x} F\left[\frac{x}{n}\right] \quad \text{—} (i)$$

But $h = f * g$

Then $H(x) = \sum_{n \le x} h(n)$

$= \sum_{n \le x} (f * g)(n)$

$= \sum_{n \le x} \sum_{d/n} f(d)\, g(n/d)$

$\left[\because g(n) \Rightarrow g(n/d) = 1 \right]$

$H(x) = \sum_{n \le x} \sum_{d/n} f(d)$ —— (ii)

From (1) and (2) we get

$\sum_{n \le x} \sum_{d/n} f(d) = \sum_{n \le x} F\left[\frac{x}{n}\right]$

Theorem 3.11:

If $F(x) = \sum_{n \le x} f(n)$ we have

$\sum_{n \le x} \sum_{d/n} f(d) = \sum_{n \le x} f(n) \left[\frac{x}{n}\right] = \sum_{n \le x} F\left(\frac{x}{n}\right)$

proof:

By thm

If $h = f * g$

Let $H(x) = \sum_{n \le x} h(n)$, $F(x) = \sum_{n \le x} f(n)$

and $G(x) = \sum_{n \le x} g(n)$

Then we have

$$H(x) = \sum_{n \le x} f(n)\, G\left(\frac{x}{n}\right) \quad \text{---} (1)$$

$$= \sum_{n \le x} g(n)\, F\left(\frac{x}{n}\right) \quad \text{---} (2)$$

If $g(n) = 1$ for all n then $G(x) = [x]$

Then we have

$$H(x) = \sum_{n \le x} g(n)\, F\left(\frac{x}{n}\right)$$

$$= \sum_{n \le x} F\left(\frac{x}{n}\right)$$

$$H(x) = \sum_{n \le x} f(n)\, G\left(\frac{x}{n}\right)$$

$$= \sum_{n \le x} f(n) \left[\frac{x}{n}\right]$$

$$H(x) = \sum_{n \le x} h(n)$$

$$= \sum_{n \le x} (f * g)(n)$$

$$= \sum_{n \le x} \sum_{d/n} f(d)\, g(n/d)$$

(By dirichelt product)

$$= \sum_{n \le x} \sum_{d/n} f(d)$$

$$\therefore \sum_{n \le x} \sum_{d/n} f(d) = \sum_{n \le x} f(n) \left[\frac{x}{n}\right] = \sum_{n \le x} F\left(\frac{x}{n}\right)$$

Hence proved.

Theorem : 3.12

For $x \ge 1$, we have

$$\sum_{n \le x} \mu(n) \left[\frac{x}{n}\right] = 1 \text{ and } \sum_{n \le x} \Lambda(n) \left[\frac{x}{n}\right] = \log [x]!$$

proof : By Thm

If $F(x) = \sum_{n \le x} f(n)$ we have

$$\sum_{n \le x} \sum_{d/n} f(d) = \sum_{n \le x} f(n) \left[\frac{x}{n}\right] = \sum_{n \le x} F\left(\frac{x}{n}\right)$$

$$\sum_{n \le x} f(n) \left[\frac{x}{n}\right] = \sum_{n \le x} \sum_{d/n} f(d)$$

$$\sum_{n \le x} \mu(n) \left[\frac{x}{n}\right] = \sum_{n \le x} \sum_{d/n} \mu(d)$$

$$= \sum_{n \le x} \left[\frac{1}{n}\right]$$

$$= 1$$

and also

$$\sum_{n \le x} f(n) \left[\frac{x}{n}\right] = \sum_{n \le x} \sum_{d/n} f(d)$$

$$\sum_{n \le x} \wedge(n) \left[\frac{x}{n}\right] = \sum_{n \le x} \sum_{d/n} \wedge(d)$$

$$= \sum_{n \le x} \log n$$

$$= \log [x]!$$

Theorem :

For all $x \ge 1$

$$\left| \sum_{n \le x} \frac{\mu(n)}{n} \right| \le 1$$ with Equality holding only if $x < 2$

proof :

Case (i)

If $x < 2$,

There is only one term in the Sum

$\mu(1) = 1$.

Case (ii)

Now, Assume that $x \geq 2$,

For each real y

Let $\{y\} = y - [y]$

Then By Thm 3.12

$$\sum_{n \leq x} \mu(n) \left[\frac{x}{n}\right] = 1$$

$$\Rightarrow 1 = \sum_{n \leq x} \mu(n) \left[\frac{x}{n}\right]$$

$$= \sum_{n \leq x} \mu(n) \left(\frac{x}{n} - \left\{\frac{x}{n}\right\}\right)$$

$$1 = x \sum_{n \leq x} \frac{\mu(n)}{n} - \sum_{n \leq x} \mu(n) \left\{\frac{x}{n}\right\}$$

Since $0 \leq \{y\} < 1$

This implies $\Rightarrow x \sum_{n \leq x} \frac{\mu(n)}{n} = 1 + \sum_{n \leq x} \mu(n) \left\{\frac{x}{n}\right\}$

$$x \left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| = \left| 1 + \sum_{n \leq x} \mu(n) \left\{\frac{x}{n}\right\} \right|$$

$$\leq 1 + \sum_{n \leq x} \left\{ \frac{x}{n} \right\}$$

$$\leq 1 + \{x\} + \sum_{2 \leq n \leq x} \left\{ \frac{x}{n} \right\} < 1 + \{x\} + \sum_{2 \leq n \leq x} 1$$

$$\because \left\{ \frac{x}{n} \right\} < 1$$

$$= 1 + \{x\} + \sum_{2 \leq n \leq x} \left(\frac{x}{n} - \left[\frac{x}{n} \right] \right)$$

$$= 1 + \{x\} + \sum_{2 \leq n \leq x} \frac{x}{n} - \sum_{2 \leq n \leq x} \left[\frac{x}{n} \right]$$

$$= 1 + \{x\} + [x] - 1 \qquad \{x\} = x - [x]$$

$$x = \{x\} + [x]$$

$$< x$$

Divide by x

$$x \left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq x$$

$$\therefore \left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1$$

Hence proved.

Theorem 3.14 :

Legendre's indentity

Statement :

For every $x \geq 1$, we have

$[x]! = \prod_{p \le x} p^{\alpha(p)}$ where the product

is extended overall primes $\le x$ and

$$\alpha(p) = \sum_{m=1}^{\infty} \left[\frac{x}{p^m} \right]$$

proof:

Since $\Lambda(n) = 0$,

unless n is a prime power and

$$\Lambda(p^m) = \log p$$

By thm 3.12

we have $\sum_{n \le x} \Lambda(n) \left[\frac{x}{n} \right] = \log [x]!$

$$\Rightarrow \log [x]! = \sum_{n \le x} \Lambda(n) \left[\frac{x}{n} \right] \qquad n = p^m$$

$$= \sum_{p^m \le x} \Lambda(p^m) \left[\frac{x}{p^m} \right]$$

$$= \sum_{p \le x} \sum_{m=1}^{\infty} \left[\frac{x}{p^m} \right] \log p$$

$$= \sum_{p \le x} \alpha(p) \log p$$

$$= \sum_{p \le x} \log p^{\alpha(p)}$$

$$\log [x]! = \log \prod_{p \le x} p^{\alpha(p)}$$

$$[x]! = \prod_{p \le x} p^{\alpha(p)}$$

Theorem 3.15 :

If $x \ge 2$, we have

$$\log [x]! = x \log x - x + O(\log x) \text{ and}$$

hence $$\sum_{n \le x} \Lambda(n) \left[\frac{x}{n}\right] = x \log x - x + O(\log x)$$

Proof :

W.K.T the Euler Summation formula

we have

$$\sum_{y < n \le x} f(n) = \int_y^x f(t)\,dt + \int_y^x (t - [t])\, f'(t)\,dt$$

$$+ f(x)([x] - x) - f(y)([y] - y)$$

$$u = \log t$$

$$du = \frac{1}{t} dt$$

$$dt = dv$$

$$\sum_{1 < n \le x} \log n = \int_1^x \log t\,dt + \int_1^x t - [t] \cdot \frac{1}{t}\,dt - (x - [x]) \log x$$

$$= [t \log t]_1^x - \int_1^x t \cdot \frac{1}{t}\, dt + \int_1^x \frac{t - [t]}{t}\, dt$$

$$- (x - [x]) \log x$$

$$= x \log x - [t]_1^x + \int_1^x \frac{t - [t]}{t}\, dt + O(\log x)$$

$$= x \log x - x + 1 + \int_1^x \frac{t - [t]}{t}\, dt + O(\log x)$$

Now $[t] = t + O(1)$

$$\int_1^x \frac{t - [t]}{t}\, dt = \int_1^x \left[\frac{t = t - O(1)}{t}\, dt\right]$$

$$= O\left(\int_1^x \frac{1}{t}\, dt\right)$$

$$= O(\log x)$$

$$\log [x]! = x \log x - x + 1 + O(\log x)$$

By $\sum_{n \le x} \Lambda(n) \left[\frac{x}{n}\right] = \log [x]!$

$$\sum_{n \le x} \Lambda(n) \left[\frac{x}{n}\right] = x \log x - x + O(\log x)$$

Theorem 3.16 :

For $x \geq 2$ we have

$$\sum_{p \leq x} \left[\frac{x}{p}\right] \log p = x \log x + O(x)$$

where the sum is Extended over all primes $\leq x$.

Proof :

Since $\Lambda(n) = 0$

unless n is a prime power

we have

$$\sum_{n \leq x} \left[\frac{x}{n}\right] \Lambda(n) = \sum_{p} \sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \left[\frac{x}{p^m}\right] \Lambda(p^m)$$

Now $p^m \leq x$ implies $p \leq x$.

Also, $[x/p^m] = 0$ if $p > x$.

So, we can write the last sum as

$$\sum_{p \leq x} \sum_{m=1}^{\infty} \log \left[\frac{x}{p^m}\right] \leq \sum_{p \leq x} \left[\frac{x}{p}\right] \log p + \sum_{p \leq x} \sum_{m=2}^{\infty} \left[\frac{x}{p^m}\right] \log p \quad -(1)$$

Next we prove that the last sum is $o(x)$

we have

by (1)

$$\sum_{p \le x} \log p \sum_{m=2}^{\infty} \left[\frac{x}{p^m}\right] \le \sum_{p \le x} \log p \sum_{m=2}^{\infty} \frac{x}{p^m}$$

$$= x \sum_{p \le x} \log p \sum_{m=2}^{\infty} \left(\frac{1}{p}\right)^m$$

$$= x \sum_{p \le x} \log p \left[\frac{1}{p^2} + \frac{1}{p^3} + \cdots\right]$$

$$= x \sum_{p \le x} \log p \cdot \frac{1}{p^2} \left[1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right]$$

$$= x \sum_{p \le x} \log p \cdot \frac{1}{p^2} \left[1 - \frac{1}{p}\right]^{-1}$$

$$= x \sum_{p \le x} \log p \cdot \frac{1}{p^2} \left[\frac{1}{1 - \frac{1}{p}}\right]$$

$$= x \sum_{p \le x} \log p \cdot \frac{1}{p^2} \left[\frac{1}{\frac{p-1}{p}}\right]$$

$$= x \sum_{p \le x} \frac{\log p}{p(p-1)}$$

$$\leq x \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} = O(x) \quad \text{---} (2)$$

Sub (2) in (1) and

$$\sum_{n \leq x} \left[\frac{x}{n}\right] \Lambda(n) = \sum_{p \leq x} \left[\frac{x}{p}\right] \log p + O(x)$$

By Thm 3.15 we have

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] = x \log x - x + O[\log x]$$

$$\therefore \sum_{p \leq x} \left[\frac{x}{p}\right] \log p = x \log x + O(x)$$

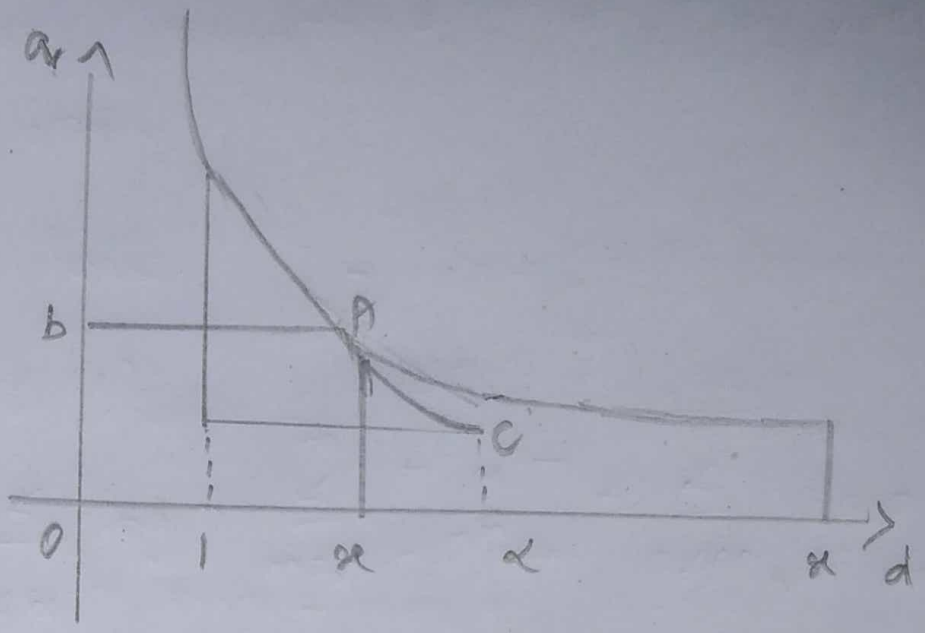
Neither identity for the partial sums of a Dirichlet product.

Theorem 3.17:

If a and b are positive real number such that $ab = x$ then

$$\sum_{\substack{q,d \\ qd \leq x}} f(d) g(q) = \sum_{n \leq a} f(n) G\left(\frac{x}{n}\right) + \sum_{n \leq b} g(n) F\left(\frac{x}{n}\right) - F(a) G(b)$$

Proof:



$$F(x) = \sum_{n \le x} f(n) \qquad G(x) = \sum_{n \le x} g(n)$$

$$H(x) = \sum_{n \le x} (f * g)(n)$$

so that $$H(x) = \sum_{n \le x} \sum_{d/n} f(d)\, g(n/d)$$

$$= \sum_{q \cdot d \le x} f(d)\, g(d)$$

$$qd \le x$$

Unit-4

Congruences :

Def:

Given integers a, b, m with $m > 0$. We say that a is Congruent to b modulo m and we write $a \equiv b \pmod{m}$ — (1)

$$a \equiv b \pmod{m} \quad \text{— (1)}$$

m divides the difference $a-b$. The Number m is called the modulus the congruence.

The congruence (1) is equivalent to the divisibility relation $m \mid (a-b)$

Note :

1) $a \equiv 0 \pmod{m}$ iff $m \mid a$
2) $a \equiv b \pmod{m}$ iff $a-b \equiv 0 \pmod{m}$
3) If $m \times (a-b)$ then $a \not\equiv b \pmod{m}$ and say that a and b are incongruent Mod m.

Eg: $10 = 2 \pmod{4}$

$16 = -4 \pmod{5}$

$2 = -1 \pmod{3}$

$50 = 5 \pmod{9}$

Ex:

1) n is even if $n \equiv 0 \pmod{2}$
2) n is odd if $n \equiv 1 \pmod{2}$

3) $a \equiv b \pmod{1}$ for every a and b

4) If $a \equiv b \pmod{m}$ then,

$a \equiv b \pmod{d}$ when $d|m$, $d > 0$

V.R: 5m

Thm:

Congruence is an equivalence:

(i) we have $a \equiv a \pmod{m}$ (Reflexive)

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ (Symmetry)

(iii) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ imply $a \equiv c \pmod{m}$ (Transitivity)

Proof:

The Proof follows from the properties of Divisibility.

(i) W.K.T Every integer divides zero

$\therefore m|0$ $\quad m|a-a$

ie) $a \equiv a \pmod{m}$

(ii) $a \equiv b \pmod{m} \Rightarrow m|a-b$

if $m|a-b$ Then $m|b-a$

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

(iii) $a \equiv b \pmod{m} \Rightarrow m|(a-b)$

$b \equiv c \pmod{m} \Rightarrow m|b-c$

$\Rightarrow m|a-b+b-c$

$\Rightarrow m|a-c$

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

V.R.

Thm 2:

(i) If $a \equiv b \pmod{m}$ and $\alpha \equiv \beta \pmod{m}$

Then we have,

(ii) $ax + \alpha y \equiv bx + \beta y \pmod m$ for all integer x and y

(iii) $a\alpha \equiv b\beta \pmod m$

(iv) $f(a) \equiv f(b) \pmod m$ $\forall$ polynomial f with integer co-efficient

(i) Given,

$$a \equiv b \pmod m$$

$$\Rightarrow m \mid a-b$$

$$\Rightarrow m \mid x(a-b) \quad \text{—— (1)}$$

III^{ly} $\alpha = \beta \pmod m$

$$\Rightarrow m \mid \alpha - \beta$$

$$\Rightarrow m \mid y(\alpha - \beta) \quad \text{—— (2)}$$

from (1) and (2),

$$\Rightarrow m \mid ax - bx + \alpha y - \beta y$$

$$\Rightarrow m \mid (ax + \alpha y) - (bx + \beta y)$$

$$\Rightarrow ax + \alpha y = (bx + \beta y) \pmod m$$

(iii) Given,

$$\Rightarrow m \mid (a-b) \Rightarrow m \mid \beta(a-b)$$

$$\Rightarrow m \mid \alpha - \beta \Rightarrow m \mid a(\alpha - \beta)$$

$$\Rightarrow m \mid \beta a - \beta b + a\alpha - a\beta$$

$$\Rightarrow m \mid a(\alpha - \beta) + \beta(a-b)$$

$$\Rightarrow m \mid a\alpha - b\beta$$

$$\Rightarrow m \mid a\alpha - b\beta$$

$a\alpha - b\beta = a\alpha - a\beta + a\beta -$

$= a(\alpha - \beta) + \beta(a -$

(iii) Let us prove this by function.

case (i) : If $n = 1$.

$a \equiv b \pmod m$. It is obvious.

case (ii)

Let us assume that (iii) is true for $n-1$

$a \equiv b \pmod m$

$a^{n-1} = b^{n-1} \pmod m$

$a \cdot a^{n-1} = b \cdot b^{n-1} \pmod m$

$a^n = b^n \pmod m$

(iv)

To prove $f(a) \equiv f(b) \pmod m$

Suppose $f(x) = c_0 + c_1 x + \ldots + c_n x^n$

Then $f(a) = c_0 + c_1 a + \ldots + c_n a^n$

and $f(b) = c_0 + c_1 b + \ldots + c_n b^n$

$m|0 \Rightarrow m \mid 0$

Since $c_0 = c_0 \pmod m$ and $a \equiv b \pmod m$

$c_1 a \equiv c_1 b \pmod m$

$c_2 a^2 = c_2 b^2 \pmod m$

$\vdots$

$c_n a^n = c_n b^n \pmod m$

$\Rightarrow c_0 + c_1 a + \ldots + c_n a^n \equiv c_0 + c_1 b + c_2 b^2 + \ldots + c_n b^n \pmod m$

i.e) $f(a) \equiv f(b) \pmod m$

Ex:

Test for divisibility by 9.

An integer $n > 0$, is divisible by 9 iff the sum of digits in its decimal expansion is divisible by 9.

Proof:

Let us prove this Property using Congruences.

Let $a_0, a_1, \ldots a_k$ be the Decimal notation of n

149 = 100+40+9 = 9 ×4×10

i.e) $n = a_0 + 10a_1 + 10^2 a_2 + \ldots 10^k a_k$

$a_0 \equiv a_0 \pmod 9$

$10 \equiv 1 \pmod 9 \Rightarrow 10a_1 \equiv a_1 \pmod 9$

$10^2 \equiv 1 \pmod 9 \Rightarrow 10^2 a_2 \equiv a_2 \pmod 9$

$\vdots$

$10^k \equiv 1 \pmod 9 \Rightarrow 10^k a_k \equiv a_k \pmod 9$

$n \equiv a_0 + a_1 + \ldots + a_k \pmod 9$

Hence the Proof.

III[4] A number is divisible by 3 iff the sum of its digits is divisible by 3.

Ex 2:

Prove that Fermat no. $Fn = 2^{2^n} + 1$ is composite for $n = 5$. (or) Fn is divisible by 641.

Proof:

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

$F_1 = 2^{2^2} + 1 = 4 + 1 = 5$ is a Prime

$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17$

$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 65$

$F_4 = 2^{16} + 1 = 65536 + 1 = 65537$ is a Prime

$f_5 = 2^{2^5} + 1 = 2^{32} + 1$

$2^{32} = (2^{16})^2$

$2^{16} = (2^8)^2 = 65536$

$2^{16} \equiv 154 \pmod{641}$

$\Rightarrow (2^{16})^2 \equiv (154)^2 \pmod{641}$

$\Rightarrow 2^{32} \equiv 23716 \pmod{641}$

$F_5 = 2^{32} + 1 \equiv 0 \pmod{641}$

$F_5 \equiv 0 \pmod{641}$

$\therefore F_5$ is a composite Number.

Note:

$48 \equiv 8 \pmod{10}$ are divisible by 6

But $8 \not\equiv 3 \pmod{10}$

Thm 3:

If $c > 0$, then $a \equiv b \pmod{m}$ iff $ac \equiv bc \pmod{mc}$

Proof:

$a \equiv b \pmod{m}$

$\Rightarrow m \mid b-a$

$\Leftrightarrow cm \mid c(b-a)$

$\rightarrow cm \mid bc-ac$

$\Rightarrow ac \equiv bc \pmod{mc}$

Hence the proof.

Thm 4:

CANCELLATION LAW

If $ac \equiv bc \pmod{m}$ and if $d = (m, c)$, then

$$a \equiv b \pmod{\frac{m}{d}}$$

In otherwords a common factor c can be Cancelled provided the Modulus is divide by $d = (m, c)$

In Particular a common factor which is relatively Prime to the modulus can always be cancelled.

Proof:

$$ac = bc \pmod m$$

$$\Rightarrow m \mid c(a-b)$$

$$\Rightarrow \frac{m}{d} \mid \frac{c}{d}(a-b) \quad \text{——— } ①$$

But,

$$(m,c) = d \Rightarrow \left(\frac{m}{d}, \frac{c}{d}\right) = 1$$

$$\Rightarrow \frac{m}{d} \mid \frac{c}{d}$$

$$① \Rightarrow \frac{m}{d} \mid (a-b)$$

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

Hence the Proof.

Thm: 5

Assume $a \equiv b \pmod m$, If $d|m$ and $d|a$ then $d|b$

Proof:

Let $d>0$,

If $d|m$ then $a \equiv b \pmod m$

$$\Rightarrow a \equiv b \pmod d \quad — ①$$

If $d|a$ then $a \equiv 0 \pmod d$ — ②

Comparing ① and ②,

$$b = 0 \pmod d$$

$$\Rightarrow d|b$$

Hence the Proof.

$a \equiv b \pmod m$
$\Rightarrow m \mid a-b$
$d|m$, $d|a$
$d|m \Rightarrow d \mid a-b$
$\frac{d}{a}$ & $\frac{d}{b} \Rightarrow$
$\Rightarrow d|b$

Bm
U.D:

Thm 6:

If $a \equiv b \pmod m$ then $(a|m) = (b|m)$

In otherwords the Numbers which are congruent mod m have the same gcd with m.

Proof: Let $d = (a, m)$ and $e = (b, m)$

To Prove $d = e$.

$d = (a, m) \Rightarrow d \mid m$ and $d \mid a$

$a \equiv b \pmod m \Rightarrow m \mid a-b$

$d \mid m \Rightarrow d \mid a-b$

$d \mid a$, $d \mid m$ and $m \mid a-b$, so $d \mid b$

$\therefore d \mid e$ — ①

Uly $e = (b, m)$

$\Rightarrow e \mid b$ and $e \mid m$

$\Rightarrow$ so $e \mid a$ and $e \mid m$

$e \mid m \Rightarrow e \mid a-b$

$e \mid a-b$ & $e \mid b \Rightarrow e \mid a$

$e \mid a$ & $e \mid m \Rightarrow e \mid (a, m)$

ie) $e \mid d$ — ②

from ① and ②

$d = e$

Hence the $(a, m) = (b, m)$

Thm 7:

If $a \equiv b \pmod m$ and if $0 \leq |b-a| < m$ then $a = b$.

$10 \equiv 2 \pmod 4$

$4 \mid |10-2| - 8$

$8 < m < 4$

Proof: $a \equiv b \pmod m$

$\Rightarrow m \mid a-b$

and $|b-a| < m$

$m \mid (a-b)$ and $(a-b) < m$

$\Leftrightarrow a-b=0$

$\Rightarrow a=b$

Hence Proved. ✓

Thm 8:

We have $a \equiv b \pmod m$ iff a and b given the same remainder when divided by m.

Proof:

Let $a = mq + r$; $b = mQ + R$

Where $0 \le r < m$ and $0 \le R < m$.

Then $a-b = mq + r - mQ - R$

$a-b = m(q-Q) + r - R$

$\Rightarrow (a-b) - (r-R) = m(q-Q)$

$\therefore m \mid (a-b) - (r-R)$

Conversely,
Assume a & b have the same remainder when divided by m.

$a = mq + r$

$b = mq - mQ$

$(a-b) = m(q-Q)$

$\Rightarrow m \mid a-b$

$a \equiv b \pmod m$

By thm ④,

$r = R$

Hence the Proof.

Thm 9:

If $a \equiv b \pmod m$ and $a \equiv b \pmod n$ where $(m,n) = 1$ then $a \equiv b \pmod{mn}$

3 | 45
9 | 45

Proof:

$a \equiv b \pmod m$

$\Rightarrow m \mid (a-b)$ — ①

$a \equiv b \pmod n$

$\Rightarrow n \mid (a-b)$ — ②

Since $(m,n) = 1$

from ① and ② $mn \mid a-b$

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

Hence the Proof.

v.k:

Def:

Let $m > 0$ be an integer & $\hat{a}$ be the set of all integers x such that $x \equiv a \pmod m$ then $\hat{a}$ is called the "residue class a modulo m".

ie) $\hat{a} = \{x : x \equiv a \pmod m\}$.

Note:

The elements of $\hat{a}$ is of the form

$x = a + mq, \quad q = 0, \pm 1, \pm 2 \cdots$

Qm *.

Thm 10:

(i) $\hat{a} = \hat{b} \iff a \equiv b \pmod m$

Proof: $\hat{a} = \hat{b} \Rightarrow a + mq = b + mq_1$

$\Rightarrow a - b = m(q_1 - q)$

$\Rightarrow m \mid a - b$

$\Rightarrow a \equiv b \pmod m$

Conversely,

$a \equiv b \pmod m$

$a + mq \equiv (b + mq) \bmod m$

$\hat{a} = \hat{b}$

Hence the proof ✓

v.k

Qm ≠ 5m

(ii) x and y belongs to same residue class of modulo m iff $x \equiv y \pmod m$

Proof: Suppose, $x, y \in \hat{a}$

$x = a + mq, \quad y = a + mq_1$

$x - y = a - a + m(q - q_1)$

$= m(q - q_1)$

$\Rightarrow m \mid x - y$

$\Rightarrow x \equiv y \pmod m$

Conversely, if $x \equiv y \pmod m$ [∵ By (i)]

by $\hat{x} = \hat{y} \Rightarrow x$ and y belongs to same residue class modulo m.

(iii) The residue class $\hat{1}, \hat{2}, \ldots \hat{m}$ are disjoint and the union is the set of an integers.

Proof:

Consider, the integers $0, 1, 2, \ldots m-1$

Since $m \equiv 0 \pmod m$ $(m \mid m-0)$

$m, 0$ are two integers of same residue class modulo m [By Previous thm 10(ii)]

Any two integers $0, 1, 2 \ldots m-1$ are incongruent modulo m.

[∵ Difference between any two elements $< m$] by thm 7.

So that m does not divides the difference by (iii)

$\hat{0}, \hat{1}, \ldots \hat{m-1}$ are all disjoint

But every integer must be in exactly one of these class. Because $x = q \cdot m + r$

$0 \leq r < m$

$x \equiv r \pmod m$

$x \in \hat{r}$

then $x = mq + r$ where $0 \leq r < m$

$x \equiv r \pmod m$

then $x \in \hat{r}$

Since $m \equiv 0 \pmod m$, $\hat{m} = \hat{0}$

$\therefore \hat{1}, \hat{2}, \hat{3} \ldots \hat{m}$ covers all integers

(C.R.S) No two elements in the set $\{1, 2, \ldots m\}$ are congruent to modulo m.

Def:

Complete residue system modulo m.

The set of m representive one from each of the residue classes $\hat{1}, \hat{2}, \ldots \hat{m}$ is called a "complete residue system modulo m".

Note: [No two elements in the set $a_1, a_2 \ldots a_m$ are congruent modulo m.] complete residue system Incongruent.

Ex: $\{1, \ldots : m\}$

Thm 11:

Let $(k, m) = 1$. If $\{a_1, a_2, \ldots . a_m\}$ is complete residue system modulo m. Then so $\{ka_1, ka_2 \ldots ka_m\}$

Proof:

first to prove

$$k a_i \not\equiv k a_j \pmod m \quad \text{for all } i \neq j$$

Suppose $ka_i \equiv ka_j \pmod m$

$$ka_i - ka_j \equiv 0 \pmod m$$

$$\Rightarrow m \mid ka_i - ka_j$$

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

But $m \mid a_i - a_j$

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

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

$$\Rightarrow \hat{a_i} = \hat{a_j}$$

Which is $\Rightarrow \Leftarrow$

Since $\{a_1, a_2 \ldots a_m\}$ is a complete residue modulo m.

Also, There are element

(ie) $\{ka_1, ka_2 \ldots ka_m\}$ is a set of m

v.q, 2m
2m.

Defn:

Let $f(x)$ be a polynomial with integer co-efficient of all integer a satisfies the congruent $f(a) \equiv 0 \pmod m$ Then a is called the solution of the congruent."

$2x \equiv 1 \pmod 4$
$4 \mid 2x-1$

Ex: 1

The linear congruent $2x \equiv 1 \pmod 4$ has no solution

$2x-1$ for every x
$2x-1$ is not divisible by 4

v.q
2m,

Ex: 2

The Quadratic congruent $x^2 \equiv 1 \pmod 8$ has exactly 4 solutions.

$x^2 \equiv 1 \pmod 8$
$\Rightarrow 8 \mid x^2-1$

Given by $x \equiv 1, 3, 5, 7 \pmod 8$

Thm 12:

Let $(a, m) = 1$, then the linear congruent $ax \equiv b \pmod m$ has a unique solution

Proof:

Consider the set of Integers $\{1, 2, \ldots m\}$ they form a complete residue system modulo m.

Hence one of element in $\{a, 2a \ldots ma\}$ is congruent to b modulo m.

Hence one of the $1, 2 \ldots m$ is a solution of $ax \equiv b \pmod m$

Thm 13:

Let $(a, m) = d$, then the linear congruence $ax \equiv b \pmod m$ has a solution $\Leftrightarrow d \mid b$

Proof:

Suppose $ax \equiv b \pmod{m}$ has a Solution

Then $m \mid ax - b$

Since $(a, m) = d$

$\Rightarrow d \mid a$ and $d \mid m$

$\Rightarrow d \mid a$ and $d \mid ax - b$

Since $d \mid a \Rightarrow d \mid ax$

$\Rightarrow d \mid ax - (ax - b)$

$\Rightarrow d \mid b$

Conversely,

Suppose $d \mid b$

$(a, m) = d \Rightarrow \left(\frac{a}{d}, \frac{m}{d}\right) = 1$

Also $ax \equiv b \pmod{m}$

$\Rightarrow \frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

Since $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$

$\Rightarrow \frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ has a Solution

This solution is a solution of

$ax \equiv b \pmod{m}$

$ax \equiv b \pmod{n}$ has a Solution.

Hence the Proof.

Thm 14:

Let $(a, m) = d$ and $d \mid b$, then the congruence $ax \equiv b \pmod{m}$ has exactly d Solutions modulo m. These solutions are given by $1 + t + \frac{m}{d}, t + \frac{2m}{d}, \ldots$

$t + (d-1)\frac{m}{d}$, where t is the solution, unique modulo $\frac{m}{d}$, of the linear congruence $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

Proof:

$$ax \equiv b \pmod{m} \quad -①$$

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \quad -②$$

Now, $(a,m) = d \Leftrightarrow \left(\frac{a}{d}, \frac{m}{d}\right) = 1$

since $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$

$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$ has a solution by thm 13.

Consequently any solution of ② is a solution of ①

Conversely, Every solution of eqn ① satisfy eqn ②

we have Prove that the 'd/a' numbers

$t, t + \frac{m}{d}, t + \frac{2m}{d} \ldots t + (d-1)\frac{m}{d}$ are any solution of ②

and hence of ①

clearly any two of the 'd' numbers are in congruent modulo m.

Suppose $t + r\frac{m}{d} \equiv t + s\frac{m}{d} \pmod{m}$, $0 \le r, s < d$

Then $\frac{rm}{d} \equiv s\frac{m}{d} \pmod{m}$

$r\frac{m}{d} \cdot \frac{d}{m} = s\frac{m}{d} \cdot \frac{d}{m}$

$(m = dm = \frac{d}{m})$

i.e) $r \equiv s \pmod{d}$ by thm 7.

$r = s$.

Now, To Prove d numbers are the only solution of ①

Suppose, y is a solution of ①

Then,

$ay \equiv at \pmod m$

Since, $(a, m) = d$; $y \equiv t \pmod{m/d}$

$y \equiv t + k\frac{m}{d}$ for some

But $k = r \pmod d$ for $0 \le r < d$

$\therefore k\frac{m}{d} \equiv r \cdot \frac{m}{d} \pmod{d \cdot \frac{m}{d}}$

i.e) $k\frac{m}{d} = r = r \cdot \frac{m}{d} \pmod m$ — (4)

Sub (4) in (3),

$\therefore y \equiv t + r \cdot \frac{m}{d} \pmod m$

i.e) y is congruent to one of the d numbers

Thus the d numbers are the Solution.

Thm: 5.15

If $(a, b) = d$, there exist an integer x and y such that $ax + by = d$.

Proof:

Since $(a, b) = d$ the linear congruence

$ax \equiv d \pmod b$ has a

Since $ax \equiv d \pmod b$

$\Rightarrow b \mid ax - d$ or $b \mid d - ax$

If there exists any y such that

$d - ax = by$

$\Rightarrow ax + by = d$

Reduced Residue System modulo m

Defn:

By a Reduced Residue System modulo m we mean any set of $\phi(m)$ integer incongruent modulo m. each of these which is relatively to m. is called "Reduced Residue System" modulo m.

Thm 15.16

If $\{a_1, a_2 \ldots a_{\phi(m)}\}$ is a Reduced Residue System modulo m $(k, m) = 1$, the $\{ka_1, \ldots ka_{\phi(m)}\}$ is also a RRSM.

Proof:

No two integer in the set $\{ka_1, ka_2, \ldots ka_{\phi(m)}\}$ are congruent modulo m.

To Prove $ka_i \not\equiv ka_j \pmod m \quad \forall\ i \neq j$

$$m \mid k(a_i - a_j)$$

$$m \mid a_i - a_j$$

$$a_i \equiv a_j \pmod m$$

For if $ka_i \equiv ka_j \pmod m$

we have $a_i \equiv a_j \pmod m \quad [\because (k, m) = 1]$

which is $\Rightarrow \Leftarrow$

Since $[a_1, a_2 \ldots a_{\phi(m)}]$ are congruent modulo m.

Also there are $\phi(m)$ integers. $(a_i, m) = 1$

we have $(k, m) = 1$

$\Rightarrow (ka_i, m) = 1$

Hence,

$(ka_1, ka_2, \ldots ka_{\phi(m)})$ is a Reduced Residue System modulo m.

V.Q.

EULER FERMAT THEOREM - 17

If $(a,m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$

Proof:

Let $\{b_1, b_2 \ldots b_{\phi(m)}\}$ be a RRS of 'm'

Since $(a,m) = 1$

$\{ab_1, ab_2, \ldots ab_{\phi(m)}\}$ is called RRSM 'm' (by above theorem)

Hence $ab_1, ab_2, \ldots ab_{\phi(m)} \equiv b_1, b_2 \ldots b_{\phi(m)} \pmod{m}$

$\Rightarrow a^{\phi(m)} b_1, \ldots b_{\phi(m)} \equiv b_1, b_2 \ldots b_{\phi(m)} \pmod{m}$

Since each b_i is relatively Prime to m

$\therefore a^{\phi(m)} = 1 \pmod{m}$

V.Q 2M: Jun **

Thm - 18

If a Prime p does not divide a then $a^{P-1} \equiv 1 \pmod{p}$

Proof:

Given $p \nmid a \Rightarrow (a,P) = 1$

By Euler Fermat's thm,

$a^{\phi(P)} \equiv 1 \pmod{P}$

But $\phi(P) = P - 1$

$\therefore a^{P-1} \equiv 1 \pmod{P}$

Hence Proved

Little Foomat thm

Statement :19

For any integer 'a' and any Prime P then $a^P \equiv a \pmod P$ Write thm 18, 17

Proof:

Let $P \nmid a$ then $a^{P-1} \equiv 1 \pmod P$

$\Rightarrow a^P \equiv a \pmod P$

To Prove.

If $P \mid a$

$a^P \equiv a \pmod P$

Let $P \mid a$ then $P \mid a^P$

$\Rightarrow a^P - a \equiv 0 \pmod P$

$\Rightarrow a^P \equiv a \pmod P$

Hence proved

$2 \mid 4 \Rightarrow 2 \mid 4^3$

$P \mid a^P - a$

$a^P - a \equiv 0 \pmod P$

Thm 20:

If $(a, m) = 1$, then the solution of the congruent $ax \equiv b \pmod m$ is given by $x \equiv ba^{\phi(m)-1} \pmod m$

Proof:

Since $(a, m) = 1$ [By EFT]

$\Rightarrow a^{\phi(m)} \equiv 1 \pmod m$

$\Rightarrow ba^{\phi(m)} \equiv b \pmod m$ —①

Given $ax \equiv b \pmod m$ —②

From ① & ②

$\Rightarrow ax \equiv ba^{\phi(m)} \bmod (m)$

$\Rightarrow x \equiv ba^{\phi(m)} a^{-1} \pmod m$

Since, $(a, m) = 1$

$\Rightarrow x \equiv b a^{\phi(m-1)} \pmod{m}$

Hence Proved.

2m Q.

Pblm 1:

Solve the congruence $5x \equiv 3 \pmod{24}$

$ax \equiv b \pmod{m}$

Sol:

$5x \equiv 3 \pmod{24}$

This is of the form $ax \equiv b \pmod{m}$

Hence $(a, m) = 1$

$a = 5 ; \; b = 3 ; \; m = 24$

$(a, m) = 1$

The solution is

$x \equiv b a^{\phi(m)-1} \pmod{m}$

$x \equiv (3) \cdot 5^{\phi(24)-1} \pmod{24}$ — (1)

$B = 1, 2, 5$

$= 1, 2 \Rightarrow \phi(3) = 2$

$8 = 1, 2, 3, 4, 5, 6, 7$

$\phi(8) = 4$

$\phi(24) = \phi(3) \cdot \phi(8)$

$= 2 \cdot 4 = 8$

Now,

$24 = 3 \cdot 8$

$\phi(24) = \phi(3) \cdot \phi(8)$

$= 2 \cdot 4$

$= 8$

$\phi(24) = 8$

(1) $\Rightarrow x \equiv 3 \cdot 5^{\phi(24)-1} \pmod{24}$

$x \equiv 3 \cdot 5^{8-1} \pmod{24}$

$x \equiv 3 \cdot 5^{7} \pmod{24}$

Consider 5^7,

Now, $5^2 \equiv 1 \pmod{24}$

$5^4 \equiv 1 \pmod{24}$

$5^6 \equiv 1 \pmod{24}$

$5^7 \equiv 5 \pmod{24}$

$x \equiv 35 \pmod{24}$

$x \equiv 15 \pmod{24}$

U & X. Solve the problem ~~25~~ $x = 15$

$ax \equiv b \pmod{m}$

Soln:

$a = 25,\ b = 15,\ m = 120$

$(a, m) = d = (25, 120) = 5.$

Now, $25x \equiv 15 \pmod{120}$

$5x \equiv 3 \pmod{24}$

By above problem,

$\therefore t = 15 \pmod{24}$ is a solution (by above thm of the $5x \equiv 3 \pmod{24}$)

The solution of $25x \equiv 15 \pmod{120}$ are

$x = t,\ t + \frac{m}{d},\ t + \frac{2m}{d},\ t + \frac{3m}{d},\ t + \frac{4m}{d}$

$t = 15,\ m = 24,\ d = 1.$

i.e) $x = 15,\ 15+24,\ 15+48,\ 15+72,\ 15+96 \pmod{120}$

i.e) $x = 15, 39, 63, 89, 111 \pmod{120}$

Lagrange's thrm for polynomial congruence modulo p [Book 115]

U & X. Let p be a prime and let $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ be a polynomial with $c_0, c_1 \ldots c_n$ are integers such that $c_n \not\equiv 0 \pmod{p}$ then $f(x) \equiv 0 \pmod{p}$ has almost n solution

Proof:

we prove this thrm by introduction on n = degree $(f(x))$

If $n=1$, then $f(x) = c_0 + c_1 x \equiv 0 \pmod{p}$

Also, $p \nmid c_1$

$(p, c_1) = 1$

Hence, $c_0 + c_1 x \equiv 0 \pmod{p}$ has a unique solution

Suppose, $f(x)$ is a degree $(n-1)$ and assume that the result is true for $n-1$

we have to prove the thrm for degree $(f(x)) = n$.

Suppose $f(x) \equiv 0 \pmod{p}$ has $(n+1)$ solutions Say $x_1, x_2 \ldots x_n$ then, $f(x_k) \equiv 0 \pmod{p}$ for $k = 0, 1, \ldots n$

Now,

$$f(x) - f(x_0) = \sum_{i=0}^{n} c_i x^i - \sum_{i=0}^{n} c_i x_0^i$$

$$= \sum_{i=0}^{n} c_i (x^i - x_0^i)$$

$= (x - x_0)\, g(x)$, where $g(x)$ is a Polynomial of degree $n-1$. remaining in Back.

** Thrm

For any prime p all the co-efficients of $f(x) = (x-1)(x-2)\ldots(x-p+1) - x^{p-1} + 1$ are divisible by p.

Proof:

Let $g(x) = (x-1)(x-2)\ldots(x-p+1)$

Then $1, 2 \ldots p-1$ are the roots of $g(x)$

$g(x) \equiv 0 \pmod{p}$ has $(p-1)$ solution

Let $h(x) = x^{p-1} - 1$

Now, $f(x) = g(x) - h(x)$ is polynomial of degree $p-2$.

But $f(x) \equiv 0 \pmod p$ has $(p-1)$ sets.

Hence any co-efficients $f(x)$ is divisible by p (by Previous thm)

WILSON'S THEOREM:

For any Prime p $(p-1)! \equiv -1 \pmod p$

Proof:

The constant term in

$f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$ is $(p-1)!+1$

Since, $p \nmid (p-1)! + 1$

we have, $(p-1)! + 1 \equiv 0 \pmod p$

$(p-1)! \equiv -1 \pmod p$

Inverse of wilson's Thm:

If $(n-1)! \equiv -1 \pmod n$ then n is prime

Proof:

suppose, n is composite.

Say $n = pq$, $1 < p$, $q < n$

clearly $p \mid (n-1)!$

Since $p < n$

Also $0 \mid (n-1)! + 1$

$[\because (n-1)! \equiv -1 \pmod n]$.

Also $p \mid 0$ since $n = pq$

Hence, $p \mid (n-1)! + 1$

Hence $P \mid (n-1)! + 1 - (n-1)!$

i.e) $P \mid 1$

which is contradiction

Since $P > 1$

Hence n is a Prime ∈

WOLSTEN HOLME'S THRM:

For any prime $P \geq 5$ we have $\sum_{k=1}^{P-1} \frac{(P-1)^1}{k} \equiv 0 \pmod{P^2}$

Proof:

The Sum in the LHS is the Sum of the Product of the Numbers $1, 2 \ldots (P-1)$

taken $(P-2)$ at a time.

The Sum is also equal to the co-effient of x in the polynomial $g(x) = (x-1)(x-2)\ldots(x-P+1)$ ——①

Let $g(x) \equiv x^{P-1} - S_1 x^{P-2} + S_2 x^{P-3} + \ldots$

$+ S_{P-3} x^2 - S_{P-2} x + (P-1)!$

where S_k in the Sum of the Product of the Numbers $1, 2, \ldots (P-1)$ taken K at a time.

By an earlier therm,

$S_1, S_2 \ldots S_{P-2}$ are divisible by P.

To Prove that,

S_{P-2} is divisible by P^2.

Now $g(p) = p$;

we have to Prove,

$$S_{p-2} \equiv 0 \pmod{p^2}$$

for it is enough to Prove that

$$S_{p-2}\, p \equiv 0 \pmod{p^3}$$

$x = p$ in (1)

Also $g(p) = (p-1)(p-2)\cdots 1$

$= (p-1)!$ —— (3) by 1

From (2) and (3) we get

$$(p-1)! = p^{p-1} - s_1 p^{p-2} + \cdots s_{p-3} p^2 + s_{p-2} p + (p-1)!$$

$$s_{p-2}\, p = p p^{-1} - s_1 p^{p-2} + \cdots + s_{p-3} p^2$$

Since $p > 5$

$$p^3 \mid s_{p-2}\, p \qquad [\, p \mid s_{p-2}\,]$$

$$\Rightarrow p^2 \mid s_2$$

$$\therefore s_{p-2} \equiv 0 \pmod{p^2}$$

Hence $\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}$

Binese Remainder thm:

Let $m_1, m_2 \cdots m_r$ be the positive integer relatively Prime in pairs. Let $b_1, b_2, \cdots b_r$ be the orbitary integers. Then the System of congruen

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv b_r \pmod{m_r}$$

has exactly one solution modulo the Product $m_1, m_2 \cdots m_r$.

Proof: Let $M = m_1, m_2 \cdots m_r$

Then $(M_r, M_k) = 1 \quad \forall \quad k = 1, 2, \cdots r$.

$\therefore$ Each M_k has a unique reciprocal M_k modulo m_k where $M_k = \frac{M}{m_k}$

Let $x = b_1 M_1 M_1' + b_2 M_2 M_2' + \cdots b_r M_r M_r'$

Consider each term in this sum modulo m_k.

Claim:

x is the required solution of the System of linear congruence.

we have since $M_i \equiv 0 \pmod{m_k} \; \forall \; i \neq k$, we have

i.e) $x \equiv b_k M_k M_k' \pmod{m_k}$

$x \equiv b_k \pmod{m_k} \quad \forall \; k = 1, 2, \cdots r$

x satisfies every convergence of System

Hence x is the required sets.

Uniqueness Part:

Let x and y be two solutions of the System of congruence

$x \equiv b_k \pmod{m_k} \quad \forall \; k$

$y \equiv b_k \pmod{m_k}$

$$x \equiv y \pmod{m_k}$$

Since $(m_i, m_j) = 1 \quad \forall \quad i \neq j$

we have,

$$x \equiv y \pmod{m_1 m_2 \cdots m_r}$$

$$\Rightarrow x \equiv y \pmod{m}$$

Hence the solution is unique.

UNIT-V

Quadratic Residue

If congruence $x^2 \equiv n \pmod{p}$ → ① has a solution we say that n is a Quadratic residue mod p and we write nRp. If ① has no solution we say that n is Quadratic non residue mod p and we write $n\bar{R}p$.

Example:

To find the quadratic Residue modulo 11 solution.

We square the number $1, 2, \ldots 10$ and residue mod 11

we obtain

$4^2 \equiv 5 \pmod{11}$; $8^2 \equiv 9 \pmod{11}$

$5^2 \equiv 3 \pmod{11}$; $9^2 \equiv 4 \pmod{11}$

$6^2 \equiv 3 \pmod{11}$; $10^2 \equiv 1 \pmod{11}$

$7^2 \equiv 5 \pmod{11}$

Consequently the quadratic residue mod 11 are 1, 3, 4, 5, 9 and non residue are 2, 6, 7, 8, 10

Theorem: 5.1

Let p be an odd prime. then every reduced residue system mod p contains exactly $(p-1)/2$ quadratic residues and exactly $(p-1)/2$ quadratic non-residue mod p. the quadratic residue belong to the residue classes containing the number of $1^2, 2^2, \ldots \left(\frac{p-1}{2}\right)^2$ → ①

Proof: First note that the number of in ① are distinct mod p.

If $x^2 \equiv y^2 \pmod{p}$ with $1 \le x \le \frac{(p-1)}{2}$ and $1 \le y \le \frac{(p-1)}{2}$ then $(x-y)(x+y) \equiv 0 \pmod{p}$

But $1 < x+y < p$

So $x - y \equiv 0 \pmod{p}$

$\Rightarrow x \equiv y \pmod{p}$

Hence $x = y$

Since $(p-k)^2 \equiv k^2 \pmod{p}$

Every quadratic residue is congruent mod p to exactly one of the number in ①

Legendre's symbol and its properties

Let p be an odd Prime. If $n \not\equiv 0 \pmod p$ we define legendre's symbol (n/p) as follows

$$(n/p) = \begin{cases} +1 & \text{if } nRp \\ -1 & \text{if } n\bar{R}p \end{cases}$$

If $n \equiv 0 \pmod p$ we define $(n/p) = 0$ ②

Example: $(1/p) = 1$; $(m^2/p) = 1$

$(7/11) = -1$; $(22/11) = 0$

Theorem: 5.2

Euler's criterion.

let p be an odd prime then for all n we have

$(n/p) \equiv n^{(p-1)/2} \pmod p$

Proof: If $n \equiv 0 \pmod p$

The result is trivial

since both members are congruent

Now, suppose that $(n/p) = 1$

then there exists an integer x such that

$x^2 \equiv n \pmod p$

and hence $n^{p-1/2} \equiv x^{2\frac{(p-1)}{2}} = x^{p-1} \equiv 1 = (n/p) \pmod p$

[using Fermat's theorem]

This prove the theorem if $(n/p) = 1$

Now, suppose that $(n/p) = -1$

Consider the polynomial $f(x) = x^{p-1/2} - 1$

since $f(x)$ has degree $(p-1)/2$ the congruence $f(x) \equiv 0 \pmod p$ has atmost $(p-1)/2$ solution

But the $(p-1)/2$ quadratic residues mod p are solution. so the non residues are not

hence $n^{(p-1)/2} \not\equiv 1 \pmod p$ if $(n/p) = 1$

But $n^{(P-1)/2} \equiv \pm 1 \pmod{p}$

$\therefore n^{(P-1)/2} \equiv (n/p) \pmod{p}$ (3)

Theorem: 5.3 Gauss lemma

Assume $n \not\equiv 0 \pmod{p}$ and consider the least positive residues mod p of the following $(P-1)/2$ multiples of n. $n, 2n, 3n, \cdots$ $(P-1)/2\, n \rightarrow$ (1) if m denotes the number of these residue which exceeds $P/2$ then $(n/p) = (-1)^m$ 2m

NOV-19

Proof: The number in (1) are congruent mod p we consider their least positive residues and distributive them into 2 disjoint set A and B

According as the residues are $< P/2$ or $> P/2$

Thus $A = \{a_1, a_2, \cdots, a_k\}$

where each $a_i \equiv tn \pmod{p}$

For some $t \leq (P-1)/2$ and $0 < a_i < P/2$

and $B = \{b_1, b_2, \cdots b_m\}$

where each $b_i \equiv sn \pmod{p}$

For some $s \leq (P-1)/2$ and $P/2 < b_i < P$

Note that $m+k = (P-1)/2$

since A and B are distinct

The number m of elements in B is pertinent

Form a new set c of m elements By subtracting each b_i from P Thus $C = \{c_1, c_2, \cdots c_m\}$

where $c_i = P - b_i$

Now, $0 < c_i < P/2$

So the elements of c lies in the same interval as the elements of A

we show that the sets A and c are disjoint

Assume $c_i = a_j$ for some pair i and j

Then $P - b_i = a_j$ (or) $a_j + b_i \equiv 0 \pmod{p}$

$\therefore tn + sn \equiv 0 \pmod{p}$

$(t+s)n \equiv 0 \pmod{p}$

For some s and t with $1 \le t < p/2$, $1 \le s < p/2$

But this is impossible

Since $p \nmid n$ and $0 < s+t < p$

$\therefore$ A and c are disjoint

So their union AUC contains

$m+k = (p-1)/2$ Integer in the interval $\left[1, \frac{(p-1)}{2}\right]$

Hence $AUC = \{a_1, a_2, \ldots a_k, \ldots c_1 c_2 \ldots c_m\}$

$= \{1, 2, \ldots (p-1)/2\}$

Now, Form product of all elements in AUC to obtain

$\{a_1, a_2, \ldots a_k, c_1, \ldots c_m\} = \left(\frac{(p-1)}{2}\right)!$

Since $c_i = p - b_i$

This gives up

$\left(\frac{p-1}{2}\right)! = a_1 a_2 \cdots a_k (p-b_1)(p-b_2) \ldots (p-b_m)$

$\left(\frac{p-1}{2}\right)! \equiv (-1)^m a_1 a_2 \cdots a_k b_1 b_2 \ldots b_m \pmod{p}$

$\equiv (-1)^m n^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$

$n^{\frac{p-1}{2}} \equiv (-1)^m \pmod{p}$

By Euler's criterion

$(-1)^m \equiv n^{\frac{p-1}{2}} \pmod{p}$

Hence $(-1)^m \equiv (n/p) \pmod{p}$

Theorem : 5.4

Legendre's symbol (n/p) is a completely multiplicative of n.

Proof: If p/m and p/n

then p/mn So $\left(\frac{mn}{p}\right) = 0$ and

either $(m/p) = 0$ (or) $(n/p) = 0$

$\therefore (mn/p) = (m/p)(n/p)$ if (p/m) (or) (p/n)

then $p \nmid m$ and $p \nmid n$

NOV-19

APR-19

then $P \nmid mn$ and we have

$$\left(\frac{mn}{p}\right) \equiv (mn)^{\left(\frac{p-1}{2}\right)} \pmod p$$

$$\equiv m^{\left(\frac{p-1}{2}\right)} n^{\left(\frac{p-1}{2}\right)} \pmod p \quad (5)$$

$$\equiv \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \pmod p$$

But each of $\left(\frac{mn}{p}\right)$, $\left(\frac{m}{p}\right)$ and $\left(\frac{n}{p}\right)$ is 1 (or) -1

So the difference,

$\left(\frac{mn}{p}\right) - \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \equiv 0 \pmod p$ is either 2 (or) -2 since the difference is divisible by p it must be 0

Theorem: 5.5 Evaluation of $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$

For every odd prime p we have

$$\left(\frac{-1}{p}\right) - (-1)^{\left(\frac{p-1}{2}\right)} = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4 \\ -1 \text{ if } p \equiv -1 \pmod 4 \end{cases}$$

Proof: By Euler's Criterion

we have $\left(\frac{-1}{p}\right) \equiv (-1)^{\left(\frac{p-1}{2}\right)} \pmod p$

since each member of this congruence is 1 or -1

The two members are equal

Theorem: 5.6

For every odd prime p we have

$$\left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8}\right)} = \begin{cases} 1 \text{ if } p = \pm 1 \pmod 8 \\ -1 \text{ if } p = \pm 3 \pmod 8 \end{cases}$$

Proof: Consider the following $\left(\frac{p-1}{2}\right)$ congruence

$$p-1 \equiv 1(-1)^1 \pmod p$$

$$2 \equiv 2(-1)^2 \pmod p$$

$$p-3 \equiv 3(-1)^3 \pmod p$$

$$4 \equiv 4(-1)^4 \pmod p$$

$$\vdots \qquad \vdots$$

$$r \equiv \left(\frac{p-1}{2}\right)(-1)^{\left(\frac{p-1}{2}\right)} \pmod p$$

Whenever r is either $p - \left(\frac{p-1}{2}\right)$ or $\frac{p-1}{2}$ multiply these together and note that each integer on the left is even

we obtain

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv \left(\frac{p-1}{2}\right)! (-1)^{1+2+\cdots+\left(\frac{p-1}{2}\right)} \pmod p$$

This given us

$$2^{\left(\frac{p-1}{2}\right)} \cdot \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! (-1)^{\left(\frac{p^2-1}{8}\right)} \pmod p$$

since $(p-1/2) \not\equiv 0 \pmod p$

$$\Rightarrow 2^{(p-1/2)} \equiv (-1)^{\left(\frac{p^2-1}{8}\right)} \pmod p$$

(6)

By Euler's criterion we have

$$2^{(p-1)/2} \equiv (2/p) \pmod p$$

and since each member is 1 or -1

The two members are equal

Theorem : 5.7

Let μ be the number defined is Gauss lemma then

$$m \equiv \sum_{t=+1}^{(p-1)/2} \left[\frac{tn}{p}\right] + (n-1)\frac{p^2-1}{8} \pmod 2$$ In particular if n is odd we have $M \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] \pmod 2$

Proof:

Let m is the number of least positive residues of the number $n, 2n, 3n, \ldots \left(\frac{p-1}{2}\right)n$ with exceed $p/2$

Take a typical number say tn divide it by p and examine the size of the remainder. we have

$$\frac{tn}{p} = \left[\frac{tn}{p}\right] + \left\{tn/p\right\} \text{ where } 0 < \left\{\frac{tn}{p}\right\} < 1$$

So $tn = p\left[\frac{tn}{p}\right] + r_t \rightarrow (1)$ where $0 < r_t < p$

The number $r_t = tn - p\left[tn/p\right]$ is the least positive residue of tn modulo p

Referring to the set A and B used in the points of the Gauss lemma

we have $\{r_1, r_2, \ldots r_{p-1/2}\} = \{a_1, a_2, \ldots a_k, b_1, b_2, \ldots b_m\}$

By Gauss Lemma

$$\{1, 2, \ldots \left(\frac{p-1}{2}\right)\} = \{a_1, a_2 \ldots a_k\, c_1 c_2 \ldots c_m\}$$

where each $c_i = p - b_i$

Now, we compute the sums of the element in these sets to obtain the two equation

$$\sum_{t=1}^{(p-1)/2} r_t = \sum_{i=1}^{k} a_i + \sum_{j=1}^{m} b_j \text{ and } \rightarrow (2)$$

$$\sum_{t=1}^{(p-1)/2} t = \sum_{i=1}^{k} a_i + \sum_{i=1}^{m} c_i \quad (7)$$

$$\sum_{t=1}^{(p-1)/2} t = \sum_{i=1}^{k} a_i + mp - \sum_{j=1}^{m} b_j \rightarrow (3)$$

In the equation (2) we replace r_t by its definition we obtain

$$\sum_{i=1}^{k} a_i + \sum_{j=1}^{n} b_j = n \sum_{t=1}^{(p-1)/2} t - p \sum_{t=1}^{(p-1)/2} [tn/p] \rightarrow (4)$$

The equation (3)

$$mp + \sum_{i=1}^{k} a_i - \sum_{j=1}^{m} b_j = \sum_{t=1}^{(p-1)/2} t \rightarrow (5)$$

Adding (3) and (4) we get

$$mp + 2\sum_{i=1}^{k} a_i = (n+1)\sum_{t=1}^{(p-1)/2} t - p \sum_{t=1}^{(p-1)/2} [tn/p]$$

$$= (n+1)\frac{p^2-1}{8} - p \sum_{t=1}^{(p-1)/2} [tn/p]$$

Now, we reduce this modulo 2

$n+1 \equiv (n-1) \pmod 2$ and

$p \equiv 1 \pmod 2$ $(p-1)/2$

$$m \equiv (n - n\left(\frac{p^2-1}{8}\right) + \sum_{t=1}^{(p-1)/2} [tn/p] \pmod 2$$

Theorem 5.8 Quadratic Reciprocity Law

If p and q are distinct odd primes then $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$

Proof: By Gauss Lemma

We have $(q/p) = (-1)^m$

We have $m = \sum_{t=1}^{(p-1)/2} \left(\frac{tq}{p}\right) \pmod 2$ (By thm 5.7)

If m is odd we have

$$m = \sum_{t=1}^{(p-1)/2} \left[\frac{tq}{p}\right] \pmod 2$$

Similarly

$$(P/q) = (-1)^n$$

where $n \equiv \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q}\right] \pmod 2$

hence $(P/q)(q/P) = (-1)^{m+n}$ and $(P/q)(q/P) = (-1)^{\frac{(P-1)(q-1)}{4}}$

at once from the identity

$$\sum_{t=1}^{(P-1)/2} \left[\frac{tq}{p}\right] + \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q}\right] = \frac{P-1}{2} \cdot \frac{q-1}{2} \rightarrow (1)$$

TO prove:-

$$\sum_{t=1}^{(P-1)/2} \left[\frac{tq}{P}\right] + \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q}\right] = \frac{P-1}{2} \cdot \frac{q-1}{2}$$

Consider the function

$$f(x,y) = qx - Py$$

If x and y are non-zero integers then $f(x,y)$ is a non-zero integers

Moreover as x takes the values $1, 2, \ldots \frac{(P-1)}{2}$ and also takes the values $1, 2, \ldots (q-1)/2$ then $f(x,y)$ takes $\left(\frac{P-1}{2}\right)\left(\frac{q-1}{2}\right)$ values no two of which are equal

since $f(x,y) - f(x',y') = f[(x-x'), (y-y')] \neq 0$

Now, we count the number of values of $f(x,y)$ which are positive and the number which are negative for each fixed x we have, $f(x,y) > 0$ iff $y < \frac{qx}{P}$ (or) $y \leq \left[\frac{qx}{P}\right]$ Hence the total number x positive value is

$$\sum_{x=1}^{(P-1)/2} \left[qx/P\right]$$

Similarly the number of negative value is $\sum_{y=1}^{\frac{(P-1)}{2}} \left[Py/q\right]$

Since the number of positive and negative values is $\frac{P-1}{2} \cdot \frac{q-1}{2}$ Hence $\sum_{t=1}^{(P-1)/2} \left[\frac{tq}{P}\right] + \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q}\right] = \frac{P-1}{2} \cdot \frac{q-1}{2}$

$$(p/q)(q/p) = (-1)^{m+n}$$

$$\sum_{t=1}^{(p-1)/2} \left[\frac{tq}{p}\right] + \sum_{s=1}^{(q-1)/2} \left[\frac{sp}{q}\right]$$

$$= (-1) \quad (9)$$

$$= (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

$$= (-1)^{(p-1)(q-1)/4}$$

Jacobi symbol

If p is a positive odd integer and with prime factorization $p = \prod_{i=1}^{r} p_i^{a_i}$ the Jacobi symbol (n/p) is defined for all integers n by the equation $(n/p) = \prod_{i=1}^{r} (n/p_i)^{a_i}$

where (n/p_i) is the Legendre symbols. we also defined

$(n/1) = 1$

Note:- If p and q are odd positive integers we have

a) $(m/p)(n/p) = (mn/p)$

b) $(n/p)(n/q) = (n/pq)$

c) $(m/p) = (n/p)$ whenever $m \equiv n \pmod{p}$

d) $(a^{2n}/p) = (n/p)$ whenever $(a, p) = 1$

Theorem :5.9

If p is an odd positive integer we have $(-1/p) = (-1)^{(p-1/2)}$

and $(2/p) = (-1)^{p^2-1/8}$

Proof: write $p = p_1 p_2 \cdots p_m$ where the prime factor p_i are not necessarily distinct

This can be also written as

$$p = \prod_{i=1}^{m} (1 + p_i - 1)$$

$$= 1 + \prod_{i=1}^{m} (p_i - 1)$$

$$= 1 + (p_1 - 1)(p_2 - 1) \cdots (p_m - 1)$$

$$= 1 + \sum_{i=1}^{m} (p_i - 1) + \sum_{j \neq i} (p_i - 1)(p_j - 1) + \cdots$$

But each factor $p_i - 1$ is even so each sum after the

first divisible by 4

Hence $p = 1 + \sum_{i=1}^{m} (p_i - 1) \pmod 4$

$\frac{1}{2}(p-1) \equiv \sum_{i=1}^{m} \frac{1}{2}(p_i - 1) \pmod 2$

$\therefore \left(\frac{-1}{p}\right) = \prod_{i=1}^{m} \left(\frac{-1}{p_i}\right)$

$= \prod_{i=1}^{m} (-1)^{\left(\frac{p_i-1}{2}\right)}$

$= (-1)^{p-1/2}$

$\left(\frac{-1}{p}\right) = (-1)^{p-1/2}$

$p^2 = \prod_{i=1}^{m} (1 + p_i^2 - 1)$

$\sum_{i=1}^{m} (p_i^2 - 1) + \sum_{i=1}^{m} (p_i^2 - 1)(p_j^2 - 1) + \cdots$

Since p_i is odd

we have $p_i^2 \equiv 1 \pmod 8$

$p_i^2 - 1 \equiv 0 \pmod 8$

$p^2 = 1 + \sum_{i=1}^{m} (p_i^2 - 1) \pmod{64}$ (or)

$\frac{1}{8}(p^2 - 1) = \sum_{i=1}^{m} \frac{1}{8}(p_i^2 - 1) \pmod 8$

hence $\left(\frac{2}{p}\right) = \prod_{i=1}^{m} \left(\frac{2}{p_i}\right) = \prod_{i=1}^{m} (-1)^{p^2-1/8}$

$\left(\because \left(\frac{2}{p}\right) = (-1)^{p^2-1/8}\right)$

$\left(\frac{2}{p}\right) = (-1)^{\left(\frac{p^2-1}{8}\right)}$

Theorem : 5.10

Reciprocity law for Jacobi symbol

If p and q are positive odd integers with $(p, q) = 1$ then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$

Proof : write $p = p_1 p_2 \cdots p_n$

$q = q_1 q_2 \cdots q_m$

where p_i and q_j are primes

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \prod_{i=1}^{m} \prod_{i=1}^{n} \left(\frac{p_i}{q_i}\right)\left(\frac{q_i}{p_i}\right)$

$= (-1)^r$ where $r = m+n$

Apply theorem 5.8

Nov-19

To each factor, we find that

$$r = \sum_{i=1}^{m} \sum_{j=1}^{n} \tfrac{1}{2}(p_i - 1)\tfrac{1}{2}(q_j - 1) \quad (11)$$

$$= \sum_{i=1}^{m} \tfrac{1}{2}(p_i - 1) \sum_{j=1}^{n} \tfrac{1}{2}(q_j - 1)$$

we know that

$$\sum_{i=1}^{m} \tfrac{1}{2}(p_i - 1) \equiv \tfrac{1}{2}(P-1) \pmod 2 \quad \text{By thm 5.9}$$

similarly, $\sum_{j=1}^{n} \tfrac{1}{2}(q_j - 1) \equiv \tfrac{1}{2}(Q-1) \pmod 2$

$$\therefore r = \left(\frac{P-1}{2}\right)\left(\frac{Q-1}{2}\right) \pmod 2$$

Hence $(P/Q)(Q/P) = (-1)^{\frac{(P-1)(Q-1)}{4}}$

Theorem: 5.11 Diophantine equation $y^2 = x^3 + k \rightarrow (1)$ has no solution if k has the term $k = (4n-1)^3 - 4m^2 \rightarrow (2)$ where m and n are integers such that no solution prime $p \equiv (-1) \pmod 4$ divides m.

Proof: Assume a solution x, y exists and obtain a contradiction by considering the equation modulo 4

Since $k \equiv (-1) \pmod 4$ we have

$$y^2 \equiv x^3 - 1 \pmod 4 \rightarrow (3)$$

Now, $y^2 \equiv 0$ (or) $1 \pmod 4$ for every y

so equation (3) cannot be satisfies

If x is even (or) if $x \equiv -1 \pmod 4$

we must have $x \equiv 1 \pmod 4$

Now, Let $a = 4n-1$

so that $k = a^3 - 4m^2$

Now equation (1) in the form

$$y^2 + 4m^2 = x^3 + a^3 \rightarrow (4)$$

$$= (x+a)(x^2 - ax + a^2)$$

Since $x \equiv 1 \pmod 4$ and $a \equiv (-1) \pmod 4$ we have from (4)

$$x^2 - ax + a^2 \equiv 1 - a + a^2 \equiv (-1) \pmod 4 \rightarrow (5)$$

Hence $x^2 - ax + a^2$ is odd

equation (5) Show that all its prime factors cannot be $p \equiv 1 \pmod 4$

Some prime $p \equiv (-1) \pmod 4$ divides $x^2 - ax + a^2$ and equation (4) shows that this also divides $y^2 + 4m^2$

In other words $y^2 \equiv -4m^2 \pmod p$ (12)

For some $p \equiv (-1) \pmod 4$

But $p \nmid m$ by hypothesis

So, $\left(\frac{-4m^2}{p}\right) = \left(\frac{-1}{p}\right) = -1$

Which is contradiction

The Diaphantine equation has no solutions

Nov-19

Define Jacobi symbols $\left(\frac{n}{p}\right)$

Find the values of $\left(\frac{-1}{11}\right)$ & $\left(\frac{-1}{17}\right)$