ALAGAPPA UNIVERSITY

(Accredited with 'A+' Grade by NAAC (with CGPA: 3.64) in the Third Cycle and Graded as category - I University by MHRD-UGC)
(A State University Established by the Government of Tamilnadu)

KARAIKUDI – 630 003

DIRECTORATE OF DISTANCE EDUCATION

M.Sc. (MATHEMATICS)

III- SEMESTER

311 33

ANALYTIC NUMBER THEORY

Author:
Dr. B. Sundaravadivoo
Assistant Professor
Department of Mathematics,
Alagappa University
Karaikudi.

ANALYTIC NUMBER THEORY

CONTENT

PAGE NO

Notes

BLOCK I – FUNDAMENTAL, PRIME NUMBERS AND ARITHMETIC FUNCTIONS

UNIT: I DIVISIBILITY

Structure

1.1 Introduction:

This unit introduces the basic concepts of elementary number theory such as divisibility, greatest common divisor, prime and composite numbers. We will start by discussing the notion of divisibility for the set of integers. We will be frequently using the fact that both addition and multiplication in the set of integers are associative, commutative and we also have distributive property a(b+c)= ab+ac for any integers a, b, c. These operations give the structure of a commutative ring to the set of integers. Divisibility can be studied more generally in any commutative ring, for example, the ring of polynomials with rational coefficients.

1.2 Objectives:

Students will be able to

- Identify and list all factors of a given whole number.
- Determine the greatest common factor of two or more whole numbers.
- Describe the procedure for finding the greatest common factor of two or more whole numbers.
- Recognize the difference between a common factor and the greatest common factor of two or more whole numbers.

Definition 1.1.1: (The principle of induction) If Q is a set of integers such that

(a) $1 \in Q$,
(b) $n \in Q$ implies $n+1 \in Q$, then
(c) all integers ≥ 1 belong to Q.

Definition 1.1.2: (The well-ordering principle): If A is a nonempty set of positive integers, then A contains a smallest member.

Notes

1.3Divisibility:

$d|n \Longrightarrow n = cd$ where $c \epsilon Z.$

Which satisfies the following properties.

(i) $d|d \Longrightarrow d = d.1$ where $1 \in Z(Reflexive\ )$
(ii) If $a|b$ and $b|c$ then $a|c(Transitive)$

For, $a|b \Longrightarrow b = ka$ where k ∈ Z

$b|c \Rightarrow c = ma$ where m∈ Z

$c = mka$, m∈ Z, k ∈ Z

$c = pa\ ,\quad mk = p$

$\Longrightarrow a|c$

(iii) If $d|a$ and $d|b$ then $d|(ax \pm by)(Linearity)$
$d|a \Longrightarrow a = kd$ where k ∈ Z
$d|b \Longrightarrow b = ma\ where\ m\ \epsilon\ Z$
$(ax \pm by) = kxd\ \ \pm myd$

$= (kx \pm my)d$

$= td\ where\ t = kx \pm my\ \ \in Z$

$\therefore d|(ax \pm by)$

(iv) $d|n$ and $n|d \Longrightarrow |d| = |n|(Comparison)$
(v) If $d|a\ and\ d|b$
The d is divisor of both a and b. $(common\ divisor)$
(vi) $d|a \Longrightarrow dx|ax$ is called a **multiplication property.**
(vii) If $x \neq 0, d|a$ is called **cancellation property.**

Definition 1.1.3:

If $d|a\ and\ d|b$ then d is said to be a **common divisor** of **a** and **b.**

Theorem:1.1

Given any two integers a and b there is a common divisor d of a and b is of the form $d = ax \pm by$ where x and y are integers more over the common divisors of a and b divides this d.

Proof: Case(i): Let a ≥ 0, b ≥ 0

and Let n = $a + b$

The proof is given by induction on n.

If n = 0 $\Longrightarrow a + b = 0$

$\Longrightarrow a = 0\ and\ b = 0$

$\therefore d = 0$, $x = 0$ and $y = 0$

∴ The result is true for n = 0

By induction principle we assume that the result is true for n = 0, 1, 2, …,(n-1).

Suppose $a \geq b$.

If b=0, Let us take d = a, x = 1, y = 0

If $b \geq 1$, then we consider (a-b) and b

Now (a-b) + b = a

$$= n - b$$

$$\leq n - 1$$

By our assumption the result is true for (a-b) and b.

$$\therefore d = (a - b)\, x + by$$

$$\Longrightarrow d|(a - b)x \text{ and } d|b$$

By Linearity, $d|(a - b) + b$

$$\Longrightarrow d|a$$

Thus $d|a$ *and* $d|b$

Hence, d is a common divisor of a and b

And $d = ax + (y - x)b$

or $d = aX + bY$ where $x = X$, $y - x = Y$ are integers.

If $e|a$ *and* $e|b$

Then by Linearity $e|ax + by$

$$\Rightarrow e|d$$

Case(ii) Let $a < 0$ (or) $b < 0$ (or) both.

If $a < 0$ *then* $|a| \geq 0$ and $b < o$ *then* $|b| \geq 0$

By case (i), d is a common divisor of $|a|$ *and* $|b|$.

By case (i) $d = |a|x + |b|y$ *where* $x, y \in Z$

Since $a < 0 \Longrightarrow |a| = -a$

Since $b < 0 \Longrightarrow |b| = -b$

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

$\quad = -a(x) + (-by)$

Notes

$= a(-x) + b(-y)$

$d = aX + bY$, $where\ X = -x, Y = -y$ are some integers.

Theorem 1.2:

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

(i) $d \geq 0$
(ii) $d|a\ and\ d|b$
(iii) $e|a\ and\ e|d \Longrightarrow e|d$

Proof: Given $d \geq 0$, by theorem 1.1 case (i) d satisfies conditions (ii) and (iii) and (-d) also satisfies the condition (ii) and (iii).

If $d'$is a another common divisor which satisfies condition (ii) and (iii).

Then, $d'|d\ and\ d|d'$

$\therefore |d| = |d'|$

$$i.e)\ d = d'$$

Hence, there is exactly one d≥ 0 which satisfies the (ii) and (iii).

1.4 Greatest Common Divisor

Definition 1.1.4:

An integer $d \geq 0$ is said to be the **greatest common divisor** of two integers **a** and **b**. If **,**

(i) $d|a\ and\ d|b$
(ii) $e|a\ and\ e|b \Longrightarrow e|d$

Note:

(i) $(a, b) = d$
(ii) $(a, b) = 1$ $t$hen a and b are relatively prime.

Theorem 1.3: Euclid's Lemma

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

Proof: Given $(a, b) = 1$

$1 = ax + by,$ where $x, y \in Z$

$c = acx + bcy$

$since\ \ a|acx\ \ and\ \ a|$bcy

$\Longrightarrow a|acx + bcy$ $\qquad (Linearity)$

$\Longrightarrow a|c.$

1.5 Exercises:

Notes

1. If $(a, b) = 1$ and if c/a and d/b, then $(c, d) = 1$.

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

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

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

5. If $(a, b) = 1$ and if $d/(a + b)$, then $(a, d) = (b, d) = 1$.

UNIT: II FUNDAMENTAL THEOREM OF ARITHMETIC

Structure

2.1 Introduction:

This unit explores the special significance of the case in which the remainder in the Division Algorithm turns out to be zero. We elaborately discuss Euclid's algorithm for finding the greatest common divisor of two non-zero integers. The algorithm not only determines the gcd, but it also allows us to express the gcd as an integral linear combination of the given integers.

2.2 Objectives:

Students will be able to

- to compute Greatest Common Divisor
- to compute multiplicative inverse
- Recognize the difference between a common factor and the greatest common factor of two or more whole numbers.

2.3 Prime Numbers:

Definition 2.1.1: 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.

Theorem 2.1:

Every integer $n > 1$ is either a prime (or) a product of primes.

Proof:

We use induction on n

When $n = 2$ which is a prime.

$\therefore$ The result is true.

We assume that the result is true for all integers >1 but less than n.

If n is a prime, there is nothing to prove.

If not, then n is composite.

Let n=cd, where 1<c<n,1<d<n

Since c<n and d<n

Then by assumption c and d prime or product of prime.

$\therefore$ n = cd is a product of prime .

Theorem 2.2: (Euclid) There are infinitely many primes.

Proof: Suppose that there are finite number of primes (say) $p_1, p_2, \dots, p_n$.

Let $N = 1 + p_1 p_2 \dots p_n$

Now N>1 so either N is prime or N is a product of primes.

Since N exceeds each p_i , and so N is not a prime.

If $p_i | N$ and $p_i | p_1 p_2 \dots p_i \dots p_n$

$\Rightarrow p_i | N - p_1 p_2 \dots p_i \dots p_n$

$\Rightarrow p_i | 1$

This is not true.

$\therefore$ No prime divides N.

$\therefore$ N is not a product of prime.

This contradicts to the above theorem.

$\therefore$ There are infinitely many primes.

Theorem 2.3: If a prime p does not divide a then (p,a)=1.

Proof: Let (p,a)=d

We have d$|p$ and d$|a$

Since d$|p \Rightarrow d = 1 \; or \; d = p$

Since d$|a$ and d$|p$ $\Rightarrow$d$|a$

$\Rightarrow\Leftarrow$ to p does not divide a

$\therefore$ d = 1

Hence (p,a)=1.

Theorem 2.4: If a prime p divides ab, then p$|a$ or p$|b$. More generally if p$|a_1 a_2 \dots a_i \dots a_n \Rightarrow$ p must divide at least one of $a_1 a_2 \dots a_i \dots a_n$.

Proof: Assume p$|ab$ and p does not divide a.

To prove that p$|b$.

Since p does not divide a, by theorem 1.6, (p,a)=1

By Euclids lemma, p$|b$.

The general case is proved by induction on n.

The proof is left to the reader.

Theorem 2.5: (Fundamental Theorem of Arithmetic)

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

Proof:

We use induction on n

When $n = 2$ which is a prime.

There is nothing to prove

Assume that the result is true for all integers $< n$.

When n is prime, the theorem is true.

If not, n is a composite.

Suppose n has 2 factorization (say)

$n = p_1p_2 \ldots\ldots. p_s = q_1q_2 \ldots\ldots. q_t$ (1)

Where p_i's and q_j's are primes.

Claim: $s = t$ *and* p_i= some q_j's

Since $p_1|p_1p_2 \ldots. p_s = q_1q_2 \ldots\ldots. q_t$

$\Longrightarrow$ $p_1|q_1q_2 \ldots\ldots\ldots q_t$

$\Longrightarrow$ $p_1|p_1$ divides atleast one of the factors.

Without loss of generality, We have $p_1|q_1$ and p_1, q_1 are primes.

$\therefore$ $p_1 = q_1$

From (1) $n = p_1p_2 \ldots\ldots\ldots\ldots p_s = q_1q_2 \ldots\ldots\ldots\ldots q_t$

$\frac{n}{p_1} = p_2p_3 \ldots\ldots\ldots\ldots p_s = q_2q_3 \ldots\ldots\ldots\ldots q_t$

Since $1 < \frac{n}{p_1} < n$

$\therefore$ By our assumption, the result is true for $\frac{n}{p_1}$

We have $s-1 = t-1$ and $p_i = q_j, \quad i \neq j$

$\therefore s = t$, For all $i \neq j, 1 < i < s-1, 1 < j < t-1$

$\therefore p_1 = q_1, p_i$ equals to some q_j, i=1,2,...,s-1, j-1,2,...t-1.

$\therefore$ s $\leq t$ and $p_i = q_j$, for all $i \neq j$

Hence every integer $n > 1$ is uniquely written as the product of prime factors.

Theorem 2.6:

If n=$\prod_{i=1}^{r} p_i^{\alpha_i}$, the set of positive divisors of n is the set of numbers of the form $\prod_{i=1}^{r} p_i^{c_i}$ where 0$\leq c_i \leq a_i$ for i =1,2,……..r.

Proof: Exercise

Note. If we label the primes in increasing order, thus

$p_1 = 2, \; p_2 = 3, \; p_3 = 5 \dots \dots \dots, p_n$ =the nth prime,

Every positive integer n (including 1) can be expressed in the form

n=$\prod_{i=1}^{\infty} p_i^{a_i}$

where now each exponent $a_i \geq 0$. The positive divisors of n are all numbers of the form

$\prod_{i=1}^{\infty} p_i^{c_i}$ where 0$\leq c_i \leq a_i$. The products are of course, finite.

Theorem 2.7:

If two positive integers a and b have the factorizations a= $\prod_{i=1}^{\infty} p_i^{\alpha_i}$, b=$\prod_{i=1}^{\infty} p_i^{\alpha_i}$ then g. c .d has the factorizations (a ,b)= $\prod_{i=1}^{\infty} p_i^{c_i}$ where each $c_i = \min\{a_i, b_i\}$ the smaller a_i *and* b_i.

Proof:

Let d= $\prod_{i=1}^{\infty} p_i^{c_i}$. Since $c_i \leq a_i$ and $c_i \leq b_i$ we have d | a and d | b so d is a common divisor of a and b . Let e be any common divisor of a and b , and write e= $\prod_{i=1}^{\infty} p_i^{e_i}$. Then $e_i \leq b_i$ *and* $e \leq c_i$. Hence e | d, so d is a g. c .d of a and b.

2.4 The series of reciprocals of the primes:-

Theorem 2.8:-

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

Proof:

The following short proof of this theorem is due to Clarkson. We assume the series converges and obtain a contradiction. If the series converges there is an integer k such that

Notes

$$\sum_{m=k+1}^{\infty} \frac{1}{p_m} < \frac{1}{2}.$$

Let $Q = p_1, p_2, \dots, p_k$, and consider the numbers 1+nQ for n=1,2,… None of these is divisible by any of the primes $p_1, p_2, \dots, p_k$. Therefore, all the prime factors of 1+nQ occur among the primes $p_{k+1}, p_{k+2}, \dots$ Therefore for each $r \geq 1$ we have

$$\sum_{n=1}^{r} \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right).$$

Since the sum on the right includes among its terms all the terms on the left. But the right-hand side of this inequality is dominated by the convergent geometric series

$$\sum_{t=1}^{\infty} \left(\frac{1}{2}\right)^t.$$

Therefore the series $\sum_{n=1}^{\infty} 1/(1+nQ)$ has bounded partial sums and hence converges. But this is a contradiction because the integral test or the limit comparison test shows that this series diverges.

Theorem 2.9: Division Algorithm

Given integers a and b with $b > 0$ there exits unique integers q and r such that $a = bq + r$ where $0 \leq r < b$. More over $r = 0 \Leftrightarrow b|a$.

Proof:

Let $\mathrm{S} = \{\mathrm{y/y = a - bx,\ \ x\ is\ an\ integer,\ \ y > 0}\}$ be the set of positive integers.

$\therefore$ S is non-empty.

By well-ordering principle, S contains a smallest member (say) $a - bq$

Let $r = a - bq$ and so $r \geq 0$

$\Longrightarrow a = bq + r$ with $r \geq 0$.

Claim: $r < b$

Suppose that $r \geq b$

$\Rightarrow r - b \geq 0$

$r - b = a + bq - b$

$\qquad = \mathrm{a - b(q + 1) \in S}$

$\therefore 0 \leq r - b < r$

$r - b \in S$ *and* $r - b$ is the smallest element in S.

$\Rightarrow\Leftarrow$ *to* r is the smallest element in S.

$\therefore r < b$

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

To prove that:

The integers q and r are unique suppose that, the another pair of integers q' and r'.

Such that, $a = bq + r, \quad 0 \leq r < b$

$$a = bq' + r', \quad 0 \leq r' < b$$

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

$\Rightarrow b(q - q') = r' - r$

$\Rightarrow b | r' - r$

If $r' - r \neq 0$

$\Rightarrow |r' - r| \geq b \qquad (Comparision\ property)$

$\Rightarrow\Leftarrow \quad 0 \leq r < b, \ 0 \leq r' < b$

$\therefore \ r' - r = 0$

$\Rightarrow r = r'$

Also $q = q' \begin{pmatrix} \therefore b(q - q') = 0 \\ \Rightarrow q - q' = 0 \ , \quad b > 0 \end{pmatrix}$

Hence there is a unique integer q and r such that , $a = bq + r, 0 \leq r < b$.

If $r = 0$, then $a = bq \Leftrightarrow b | a$.

2.5 Euclidean Algorithm

Theorem 2.10: Euclidean Algorithm

Given positive integers a and b where $b \nmid a$. Let r_0= a and r_1= b, and apply the division algorithm repeatedly to obtain the set of remainders $r_2, r_3, \ldots\ldots r_n, r_{n+1}$ *defined succesively by the* relations

$r_0 = r_1 q_1 + r_2, \quad 0 \leq r_2 < r_1$

$r_1 = r_2 q_2 + r_{3,} 0 \leq r_3 < r_2$

$$\vdots$$

$r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1}$

$r_{n-1} = r_n q_n + r_{n+1,} 0 \leq r_n < r_{n-1}$

Then r_n , last nonzero remainder in this process is (a,b), the greatest common divisor of a and b.

Proof:

Given r_n is decreasing and positive.

Now, $r_{n-1} = r_n q_n + r_{n+1}$

$\Longrightarrow r_{n-1} = r_n q_n (\because \; r_{n+1} = 0)$

$\Longrightarrow r_n | r_{n-1}$

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

$= \; r_n \, q_n q_{n-1} + r_n$

$= r_n (q_n q_{n-1} + 1)$

$\Longrightarrow r_n | r_{n-2}$

Continuing like this, we get

$r_n | r_1 = \text{b}, \quad r_n | r_0 = \text{a}$

$\Longrightarrow r_n$ is a common divisor of a and b.

If $d|a = r_0$ and $d|b = r_1$

$\therefore \; d|r_0 = r_1 q_1 (By\ linearity)$

$\Longrightarrow d|r_2$

Similarly, $d|r_3$, $d|r_4$ ………., $d|r_{n-1}$, $d|r_n$

$\therefore$ r_n is the Greatest common divisor of a and b.

2.6 Exercises:

(1) Prove that $\mathrm{n}^4 + 4$ is composite if $\mathrm{n} > 1$.

(2) Prove that every $\mathrm{n} \geq 12$ is the sum of two composite numbers.

(3) Prove that if $2^{\mathrm{n}} - 1$ is prime, then n is prime.

(4) Prove that if $2^{\mathrm{n}} + 1$ is prime, then n is a power of 2.

(5) Let $\mathrm{d} = (826{,}1890)$. Use the Euclidean algorithm to compute d, then express d as a linear combination of 826 and 1890.

UNIT: III ARITHMETICAL FUNCTIONS AND DIRICHLET MULTIPLICATION

Structure

3.1 Introduction:

Number theory, like many branch of mathematics, is often concerned with sequences of real or complex numbers. In number theory such sequence are called arithmetical functions. This unit introduces several arithmetical functions which play an important role in study of divisibility properties of integers and the distribution of primes.

3.2 Objectives:

The students will be able to

- Describe the properties of Mobius function
- Determine the product formula for Eulers totient function
- Identify the relation between $\phi(n)$ *and* μ(n)

Definition 3.1.1: A real or complex-valued function defined on the positive integers is called an arithmetical function or a number-theoretic function.

3.3The Möbius function μ$(\boldsymbol{n})$

Definition 3.1.2: The Möbius function (μ) is an arithmetic function defined by,

If $n = 1$, $\mu(1) = 1$

If $n > 1, then\ n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots\ldots p_k^{\alpha_k}$ where P_i's are distinct primes.

$$\mu(n) = \begin{cases} (-1)^k & if\ \ \alpha_1 = \alpha_2 = \cdots\cdots = \alpha_k \\ 0 & otherwise \end{cases}$$

Note:

(i) **n:** 1 2 3 4 5 6 7 8 9 10

$\boldsymbol{\mu(n)}$: 1 -1 -1 0 -1 1 -1 0 0 1

(ii) $\mu(n) = 0$, If n is square free.

Theorem 3.1:

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

Proof:

If $n = 1$, then

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

If $n > 1$, then $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}$ where P_i's are distinct primes and $\alpha_1, \alpha_2, \ldots\ldots\ldots, \alpha_k \geq 1$.

Consider, $\sum_{d|n} \mu(n) = \sum_{d|p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_k^{\alpha_k}} \mu(n)$

The sum $\sum_{d|n} \mu(n)$ has a non-zero terms only When

$d = 1, (p_1, p_2, p_3, \ldots, p_k), (p_1\ p_2, \ldots, p_{k-1}p_k),$

$(p_1 p_2 p_3, \ldots\ldots, p_{k-2} p_{k-1} p_k), \ldots\ldots\ldots, (p_1 p_2 \ldots\ldots\ldots p_k).$

$\sum_{d|n} \mu(n) = \mu(1) + [\mu(p_1) + \cdots\cdots + \mu(p_k)] + [\mu(p_1 p_2) + \cdots\cdots +$ $\mu(pk{-}1pk)$

$+[\mu(p_1 p_2 \cdots\cdots\cdots p_k)]$

$= 1 + kc_1\ (-1) + kc_2(-1)^2 + \cdots\cdots\cdots\cdots + kc_k(-1)^k$

$= 0$

3.4 Euler's totient function

Definition 3.1.3: (Euler's totient function) $\boldsymbol{\phi(n)}$

If $n \geq 1$, the Euler's totient function $\phi(n)$ is an arithmetic function defined to be the set of positive integers not exceeding n which are relatively prime to n.

$Thus\ \phi(n) = \sum_{k=1}^{n}{}' \, 1$, where dash denotes the sum is taken over those k which are relatively prime to n.

Theorem 3.1:-

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

Proof:-

Let S = {1,2,…,n}.

For each divisor d of n, let $A(d) = \{k: (k, n) = d, 1 \leq k \leq n\}$.

That is, A(d) contains those elements of S which have the gcd d with n.

Claim: The subsets A(d) of S form a disjoint collection whose union is S.

If $d_1 \neq d_2$ are two divisors of n.

Let $x \in A(d_1) \cap A(d_2)$

$\Longrightarrow x \in A(d_1)$ and $x \in A(d_2)$

$\Longrightarrow$ (x,n)= d_1 and (x,n)= d_2

$\Longrightarrow d_1 = d_2$

This is a contradiction.

The subsets A(d) form a disjoint collection whose union is S. Therefore if f(d) denotes the number of integers in A(d) we have

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

But (k,n)=d if and only if $(k/d\,, n/d) = 1$, and $o < k \leq n$ if and only if $0 < k/d \leq n/d$. Therefore , if we let q=k/d there is 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 such q is $\varphi\left(\frac{n}{d}\right)$.

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

$$\sum_{d|n} \varphi(n/d) = n.$$

But this is equivalent to the statement $\sum_{d|n} \varphi(d) = n$ because when d runs through all divisors of n so does n/d. This completes the proof.

Theorem:3.2

If $n > 1$, we have $\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$

Proof: By the definition of ϕ, we have

$\phi(n) = \sum_{k=1}^{n}{}' \, 1$, where dash denotes the sum is taken over those k which are relatively prime to n.

$= \sum_{k=1}^{n} \left[\frac{1}{(n,k)}\right]$ relatively prime to n.

$= \sum_{k=1}^{n} \sum_{d|(n.k)} \mu(d)$ (by theorem 3.1)

$$= \sum_{k=1}^{n} \sum_{d|n \,\&\, d|k} \mu(d)$$

For a fixed d, the first sum is taken over all k which are multiples of d.

Notes

$1 \leq k \leq n \Leftrightarrow 0 < k \leq n$

$\Leftrightarrow 0 < \frac{\mathrm{k}}{\mathrm{d}} \leq \frac{\mathrm{n}}{\mathrm{d}}$

$\Leftrightarrow 0 < q \leq \frac{n}{d}$, where $\mathrm{q} = \frac{\mathrm{k}}{\mathrm{d}}$

$\Leftrightarrow 1 \leq \mathrm{q} \leq \frac{\mathrm{n}}{\mathrm{d}}$

$$\phi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d)$$

$$= \sum_{d|n} \mu(d) \sum_{q=1}^{\frac{n}{d}} 1$$

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

3.5 A Relation Connecting $\boldsymbol{\phi}$ *and* $\boldsymbol{\mu}$

Theorem: 3.3 Product formula for Euler's Totient function

If $n \geq 1$, where $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ where p is prime divisor of n.

Proof:

When $n = 1$, L.H.S:$\phi(n) = 1$

R.H.S $= \prod_{p|1}(1 - \frac{1}{p})$ where P is prime.

No prime divides one , so the product is empty.

So assume that R.H.S =1

If $n > 1$, then $n = {p_1}^{\alpha_1} \dots \dots \dots {p_r}^{\alpha_r}$ where p_i's are distinct primes.$\alpha_1, \dots, \alpha_k \geq 1$

Consider,

$$\prod_{p|n} \left(1 - \frac{1}{n}\right) = \prod_{i=1}^{r} \left(1 - \frac{1}{n}\right)$$

$$= \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \dots \dots \dots . \left(1 - \frac{1}{p_r}\right)$$

$$= 1 - \left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_r}\right) + \left(\frac{1}{p_1p_2} + \frac{1}{p_1p_3} + \cdots + \frac{1}{p_{r-2}p_{r-1}p_r}\right) + \cdots\cdots \frac{(-1)^r}{p_1p_2 \ldots \ldots . p_r}$$

$$= 1 + \sum_{i=1}^{r} \frac{(-1)}{p_i} + \sum_{\substack{i,j=1 \\ i\neq j}}^{r} \frac{(-1)^2}{p_ip_j} + \sum_{\substack{i,j,k=1 \\ i\neq j\neq k}}^{r} \frac{(-1)^3}{p_1p_2p_3} + \cdots\cdots + \frac{(-1)^r}{p_1 \ldots \ldots p_r}$$

$$= 1 + \sum_{i=1}^{r} \frac{(-1)}{p_i} + \sum_{\substack{i,j=1 \\ i\neq j}}^{r} \frac{\mu(p_ip_j)}{p_ip_j} + \sum_{\substack{i,j,k=1 \\ i\neq j\neq k}}^{r} \frac{\mu(p_ip_jp_k)}{p_ip_jp_k} + \cdots\cdots + \frac{\mu(p_1p_2 \ldots \ldots p_r)}{p_1p_2 \ldots \ldots p_r}$$

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

R.H.S $\quad = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$

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

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

$= \phi(n)$ (by theorem 3.2)

$= \mathbf{L.H.S}$

Theorem: 3.4 Properties of Euler's Totient Function

(i) $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$, where p is a prime and $\alpha \geq 1$

(ii) $\phi(mn) = \phi(m)\phi(n)\frac{d}{\phi(d)},\ where\ d = (m,n)$

(iii) $\phi(mn) = \phi(m)\phi(n)\ if\ (m,n) = 1$

(iv) a|b $\Rightarrow \phi(a)|\phi(b)$

(v) $\phi(n)\ is\ even\ for\ n \geq 3.$

Moreover if n has r distinct odd prime factors then $2^r|\phi(n)$

Proof:

(i) By the product formula,

$\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$ where p is prime divisor of n

Put $n = p^\alpha$, we get

$$\phi(p^\alpha) = p^\alpha \prod_{p|p^\alpha}(1 - \frac{1}{p})$$

Since the prime divisor of p^α is p only.

$$\therefore\ \phi(p^\alpha) = p^\alpha\left(1-\frac{1}{p}\right)$$

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

(ii) By the product formula,

$\phi(n) = n\prod_{p|n}(1-\frac{1}{p})$ where p is a prime divisor of n

$$\frac{\phi(n)}{n} = \prod_{p|n}(1-\frac{1}{p})$$

Put n = mn, we have

$$\frac{\phi(mn)}{mn} = \prod_{p|mn}(1-\frac{1}{p})$$

Since each prime divisors of mn is either a prime divisor of m or of n and those primeswhich divide both m and n it also divide (m,n)

$$\therefore\quad \frac{\phi(\mathrm{mn})}{\mathrm{mn}} = \frac{\prod_{\mathrm{p|m}}(1-\frac{1}{\mathrm{p}})\prod_{\mathrm{p|n}}(1-\frac{1}{\mathrm{p}})}{\prod_{\mathrm{p|(m,n)}}(1-\frac{1}{\mathrm{p}})}$$

$$\Rightarrow \phi(mn) = \frac{m\prod_{p|m}\left(1-\frac{1}{p}\right)n\prod_{p|n}(1-\frac{1}{p})}{\prod_{p|d}(1-\frac{1}{p})}$$

$$= \frac{\phi(m)\phi(n)}{\frac{\phi(d)}{d}}$$

$$\therefore \phi(mn) = \phi(m)\phi(n)\frac{d}{\phi(d)},\quad 1.d = (m,n)$$

(iii) By property(ii)

$$\phi(mn) = \phi(m)\phi(n)\frac{d}{\phi(d)},\quad d = (m,n)$$

Put d=1 then $\phi(\mathrm{d}) = \phi(1) = 1$

$$\therefore\ \frac{d}{\phi(d)} = 1$$

$$\phi(mn) = \phi(m)\phi(n), (m,n) = 1$$

(iv) Given a|b$\Rightarrow b = ac\ where\ \ 1 \le c \le b$

When $c = b\ \Rightarrow a = 1$

$$\Rightarrow \phi(a) = \phi(1)$$

$$\Rightarrow \phi(a) = 1$$

Notes

WKT, 1 divides every integer

$\Rightarrow 1|\phi(b) \Rightarrow \phi(a)|\phi(b)$

When $c < b$,

$Now\ b = ac$

$\Rightarrow \phi(b) = \phi(c)$

$\Rightarrow \phi(b) = \phi(a)\phi(c)\dfrac{d}{\phi(d)}, \quad where \quad d = (a,c)$

$$\phi(b) = d\ \phi(a)\frac{\phi(c)}{\phi(d)} \longrightarrow (*)$$

The proof is given by induction on b.

If b = 1, $\Rightarrow \phi(b) = \phi(1) = 1$

(*) becomes, $1 = d\ \phi(a)\frac{\phi(c)}{\phi(d)}$

$\Rightarrow \phi(a)|1 \Rightarrow \phi(a)|\phi(b)$

∴The result is true for b = 1

By induction we assume that the result is true for all integers $< b$.

Since $c < b$, The result is true for c.

$\therefore d = (a,c) \Rightarrow d|a\ and\ d|c$

$d|c \Rightarrow \phi(d)|\phi(c)$

$\Rightarrow \phi(c) = k\phi(d), \quad k\epsilon Z$

$\Rightarrow \frac{\phi(c)}{\phi(d)}$=k

Equation (*) becomes,

$\phi(b) = d\ \phi(a)k$

$\Rightarrow \phi(a)|\phi(b)$

(v) put $n = 2^\alpha$, $\quad \alpha \geq 2$

By property (1)

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

$\phi(2^\alpha) = 2^\alpha - 2^{\alpha-1}$

$= 2^\alpha\left(1 - \dfrac{1}{2}\right)$

$\therefore \phi(n)$ is even for $n \geq 3$

Notes

If n has atleast one odd prime factor, by product formula,

$\phi(n) = n\prod_{p|n}(1-\frac{1}{p}) = n\prod_{p|n}(1-\frac{1}{p})$

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

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

$\phi(n) = nc\prod_{p|n}(p-1)$ where c = $\frac{1}{\prod_{p|n} p}$

Where nc is an integer for at least one odd prime factor, we will get (p-1) is even.

$\therefore \phi(n)$is even

If n has r distinct odd prime factors

$\therefore$ Each term of the product $\prod_{p|n}(p-1)$contributes a factor 2 to this product.

$\therefore\ 2^r|\prod_{p|n}(p-1)$

$\Rightarrow 2^r|\phi(n)$

Hence proved

3.6 Exercise:

1. Find all integer n such that

(a) $\varphi(n) = n/2$, (b) $\varphi(n) = \varphi(2n)$, (c) $\varphi(n) = 12$

2. For each of the following statement either give a proof or exhibit a counter example.

(a) If (m,n)=1 then $(\varphi(m), \varphi(n))$ = 1
(b) If n is composite then $(n, \varphi(n))$>1
(c) If the same primes divide m and n then $n\varphi(m) = m\varphi(n)$

3. Prove that

$$\frac{n}{\varphi(n)} = \sum_{d|n}\frac{\mu^2(d)}{\varphi(d)}.$$

Prove that $\varphi(n) > n/6$for all n with at most 8 distinct prime factors.

UNIT:IV DIRICHLET PRODUCT OF ARITHMETICAL FUNCTIONS

Structure

4.1 Introduction:

The two obvious operations on the set of arithmetic functions are point wise addition and multiplication. The constant functions f= 0 and f= 1are neutral elements with respect to these operations, and the additive and multiplicative inverses of a function f are given by−f and 1/f, respectively. While these operations are sometimes useful, by far the most important operation among arithmetic function is called Dirichlet product, an operation that, at first glance, appears mysterious and unmotivated, but which has proved to be an extremely useful tool in the theory of arithmetic functions.

4.2 Objectives:

The students will be able to

- Derive Mobius inversion formula
- Describe the properties of Mangolt function
- Recognise the Dirichlet inverse of arithmetical functions

Definition 4.1.1:

Let f and g be arithmetic functions. Then, the Dirichlet multiplication of f and g is denoted by h and is defined as

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

$$= \sum_{d|n} f(d)\ g\left(\frac{n}{d}\right)$$

Definition 4.1.2:

The power function n^{α} is an arithmetic function is defined by $N^{\alpha}(n) = n^{\alpha}\ \forall\ \alpha$

Definition 4.1.3:

The unit function u is an arithmetic function is defined by $u(n) = 1\ \forall\ n$.

Definition 4.1.4:

The identity function I is an arithmetic function is defined by

$$I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 \; if \; n = 1 \\ o \; if \; n > 0 \end{cases}$$

Result:

Express $\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right]$ as a dirichlet multiplication

Proof:

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

$$\sum_{d|n} \mu(d) u\left(\frac{n}{d}\right) = I(n)$$

$$(\mu * u)(n) = I(n)$$

$$\mu * u = I$$

Result:

Express $\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$ in dirichlet multiplication.

Proof: $\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$

$$= \sum_{d|n} \mu(d) \, N\left(\frac{n}{d}\right)$$

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

$$\mu * N = \phi$$

Note:

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

$$= \sum_{cd=n} f(d) g(c)$$

Theorem: 4.1

Dirichlet multiplication is commutative and associative

Proof:

Let f and g be two arithmetic functions

To prove: $\boldsymbol{f * g = g * f}$

$$(f * g)(n) = \sum_{cd=n} g(d)f(c)$$

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

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

Hence dirichlet multiplication is commutative.

Let $f, g \text{ and } h$ be an arithmetic function.

To prove: $\boldsymbol{f * (g * h) = (f * g) * h}$

L.H.S $= f * (g * h)$

$$= f * A \quad where\ A = g * h.$$

$$(f * A)(n) = \textstyle\sum_{ad=n} f(a)A(d)$$

$$= \sum_{ad=n} f(a) \sum_{bc=d} g(b)h(c) \left(\begin{aligned} \therefore A(d) &= (g * h)(d) \\ &= \sum_{bc=d} g(b)h(c) \end{aligned} \right.$$

R.H.S$= (f * g) * h$

$$= B * h \quad \text{where } B = f * g$$

$$(B * h)(n) = \sum_{dc=n} B(d)h(c)$$

$$= \sum_{dc=n} \sum_{ab=d} f(a)g(b)h(c)$$

$$= \sum_{abc=n} f(a)g(b)h(c)$$

Hence dirichlet multiplication is Associative.

Theorem: 4.2

For any arithmetic function f we have $f * I = I * f = f$ where I is identity function.

Proof:

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

$$= \sum_{1|n} I(1) f\left(\frac{n}{1}\right) + \sum_{\substack{d|n \\ d>1}} I(d) f\left(\frac{n}{d}\right)$$

Notes

$$= f(n) + 0$$

$$= f(n)$$

$\therefore (I * f) = f$

Since Dirichlet multiplication is commutative.

$(\mathrm{f} * \mathrm{I}) = \mathrm{f}$

$f * I = (I * f) = f$

Hence proved.

4.3 Dirichlet Inverses and Mobius Inversion Formula

Theorem: 4.3

If f is an arithmetic function with $f(1) \neq 0$ there is a unique inverse $f^{-1}$is called the dirichlet inverse such that $(f * f^{-1}) = f^{-1} * f = I$. Then,

(i) $f^{-1} = \frac{1}{f(1)}\ for\ n = 1.$

(ii) $f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d)\ for\ n > 1.$

Proof:

(i)If $n = 1$

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

$$(\mathrm{f} * \mathrm{f}^{-1})\ 1 = \mathrm{I}(1)$$

$$\sum_{\mathrm{d}|1} \mathrm{f(d)} \mathrm{f}^{-1}\left(\frac{1}{\mathrm{d}}\right) = 1$$

$\Rightarrow f^{-1}(1) = \frac{1}{f(1)}\ for\ n = 1$

Since $f(1) \neq 0$ so f^{-1} exists and is uniquely determined.

(ii) For $n > 1$, we have

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

$$\Rightarrow (f^{-1} * f)(n) = 0$$

$$\Rightarrow \sum_{d|n} f^{-1}(d) f\left(\frac{n}{d}\right) = 0$$

$$f^{-1}(n) f(1) + \sum_{\substack{d|n \\ d<n}} f^{-1}(d) f\left(\frac{n}{d}\right) = 0$$

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

$$\Rightarrow f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \qquad for\ n > 1.$$

Theorem 4.4: Mobius inversion formula

The equation $f(n) = \sum_{d|n} g(d)\ if\ and\ only\ if\ g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$

Proof:

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

$$= \sum_{d|n} g(d)u\left(\frac{n}{d}\right)$$

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

$$f = g * u$$

Multiply μ on both sides to the above equation, we get

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

$$= g * (u * \mu) \qquad (\therefore Dirichlet\ product\ is\ associative)$$

$$= g * (\mu * u) \qquad (\therefore Dirichlet\ product\ is\ commutative)$$

$$= g * I$$

$$= g$$

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

$$= \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$$

Conversely assume that, $g(n) = \sum_{d|n} f(d)\left(\frac{n}{d}\right)$

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

$$g = f * \mu$$

Multiply u on both sides of the above equation, we get

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

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

$$= f * I$$

$$= f$$

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

Notes

$$= \sum_{d|n} g(d)u\left(\frac{n}{d}\right)$$

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

4.4 Mongoldt function

Definition 4.1.5: Mongoldt function ($\boldsymbol{\Lambda}(\mathbf{n})$)

For every integer $n \geq 1$ the Mongoldt's function Λ is defined by

$$\Lambda(n) = \begin{cases} \log p & if\ n = p^m\ for\ some\ prime\ P\ and\ s\ m \geq 1, \\ 0 & otherwise \end{cases}$$

Assume that $\Lambda(1) = 0, when\ n = 1.$

Note:

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

Theorem 4.5:

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

Proof:

If $\quad n = 1$

L.H.S = $\sum_{d|1} \Lambda(d)$

$= \Lambda(1) = 0$

R.H.S = $\log 1 = 0$

$\therefore$ R.H.S = L.H.S

For $n > 1,$

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots \dots p_k^{\alpha_k}\ where\ P_i's\ are\ distinct\ primes\ and\ \alpha_i > 1.$

R.H.S =$\log(p_1^{\alpha_1} p_2^{\alpha_2} \dots \dots p_k^{\alpha_k})$

$= \log p_1^{\alpha_1} + \log p_2^{\alpha_2} + \cdots \cdots + \log p_k^{\alpha_k}$

$= \alpha_1 \log p_1 + \alpha_2 \log p_2 + \cdots \cdots + \alpha_k \log p_k$

$$= \sum_{i=1}^{k} \alpha_i \log p_i$$

L.H.S $= \sum_{d|p_1^{\alpha_1} p_2^{\alpha_2} \dots\dots p_k^{\alpha_k}} \Lambda(d)$

The non-zero items of $\sum_{d|n} \Lambda(d)$ occurs only when
$d = (p_1, p_1^2 \dots \dots p_1^{\alpha_1}), (p_2, p_2^2 \dots \dots p_2^{\alpha_2}), \dots, (p_k, p_k^2, \dots \dots p_k^{\alpha_k})$

L.H.S:

$$\sum_{d|n} \Lambda(d) = \Lambda(p_1) + \Lambda({p_1}^2) + \Lambda({p_1}^{\alpha_1}) + \Lambda(p_2) + \Lambda({p_2}^2) + \Lambda({p_2}^{\alpha_2})$$

$$+ \cdots\cdots + \Lambda\,(p_k) + \Lambda(p_k)^2 + \Lambda({p_k}^{\alpha_k})$$

$$= \log p_1 + \log p_1 + \log p_1 + \log p_2 + \log p_2 + \cdots\cdots \log p_2 + \log pk + \log pk + \cdots\cdots + \log pk$$

$$= \alpha_1 \log p_1 + \alpha_2 \log p_2 + \cdots\cdots\cdots + \alpha_k \log p_k$$

$$= \sum_{i=1}^{k} \alpha_i \log p_i$$

= R.H.S

Theorem 4.6:

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

Proof:

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

By Mobius Inversion formula

i.e) $f(n) = \sum_{d|n} g(d) \quad iff \; g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$

Take f =log, g=Λ in Mobius inversion formula

Then we have

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

$$\Leftrightarrow \Lambda(n) = \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right)$$

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

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

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

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

Notes

4.5 Exercise:

1. Prove that $\sum_{d|n} \mu(d) log^m$(d)=0 if m$\geq$ 1 and n has m distict prime factors.

Notes

BLOCK II: MULTIPLICATIVE FUNCTIONS AND FORMAL POWER SERIES

UNIT-V: MULTIPLICATIVE FUNCTIONS

Structure

5.1 Introduction:

This unit introduces the Dirichlet product of two arithmetic functions. It will give the set of all arithmetic functions the structure of a monoid. Further,we will see how the Dirichlet product gives the structure of an abelian group to the set of all arithmetic functions which do not vanish at 1. The Mobius Inversion Formula also follows easily from Dirichlet product.

5.2 Objectives:

The students will be able to

- Identify the properties of Liouvilles function
- Describe the difference between multiplicative and completely multiplicative functions
- Determine the properties of divisor functions

5.3 Multiplicative function

Definition 5.1.1: Multiplicative function:

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

Definition 5.1.2: Completely multiplicative function:

Notes

A multiplicative function f is said to be completely multiplicative

if $f(m,n) = f(m)f(n) \quad for\ all\ m,n.$

Example:

1. Euler's totient function is multiplicative but not completely multiplicative.

By the proof of Euler's totient function
$\varphi(mn) = \varphi(m)\varphi(n) \quad whenever\ (m,n) = 1$
$\therefore$ φ is multiplicative.

Euler totient function is multiplicative but not completely multiplicative.

$$\varphi(8) = 4, \qquad \varphi(2) = 1, \qquad \varphi(4) = 2$$

$$\therefore\ \varphi(8) \neq \varphi(2)\varphi(4)$$

$$4 \neq 2$$

2.The power series is completely multiplicative.

$$N^{\alpha}(mn) = m^{\alpha}n^{\alpha}$$

$$= N^{\alpha}(m)N^{\alpha}(n) \qquad \forall\, m,n$$

3.The unit function is completely multiplicative.

$$u(mn) = u(m)u(n) \qquad \forall\, m,n$$

4. The identity function is completely multiplicative.

If $m = 1,\ n = 1$

Then $mn = 1$

$$I(m) = 1, \qquad I(n) = 1$$

$I(mn) = 1$

$$I(mn) = I(m)I(n)$$

$If\ m = 1\ (or)\ n > 1\ then\ \ mn > 1$

$$I(m) = 1, \qquad I(n) = 0, \qquad I(mn) = 0$$

$I\ \ (mn) = I(m)I(n)$

Similarly, $m > 1\ (or)\ n = 1, m > 1,\ n > 1\ then\ mn > 1$

$\therefore I(mn) = I(m)I(n) \quad \forall\, m,n$

5.Mongoldt function is not completely multiplicative.

If $(2,7) = 1$

$\Lambda(2) = \log 2 \quad m = 2$

$\Lambda(7) = \log 7 \quad n = 7$

$\Lambda(4) = 0 \quad mn = 14$

$\Lambda(14) \neq \Lambda(2)\Lambda(7)$

$\therefore$ Mongoldt function is not multiplicative

Hence Mongoldt function is not completely multiplicative.

Notes

6.Mobius function is multiplicative but not completely multiplicative.

Let $(m, n) = 1$

To prove: $\mu(m, n) = \mu(m)\mu(n)$

Suppose that either m is square free or n is both m and n are square free.

$$\therefore \mu(m) = 0, \ \mu(n) = 0$$

$\mu(mn) = 0$

$\mu(mn) = \mu(m)\mu(n), \quad (m, n) = 1$

Let $m = p_1 p_2 \dots \dots \dots p_k$ where $p_i's$ are distinct primes $i = 1.2 \dots \dots k$

And $n = q_1 q_2 \dots \dots \dots q_k$ where $q_j's$ are distinct primes $j = 1.2 \dots \dots s$

$$mn = p_1 p_2 \dots \dots p_k q_1 q_2 \dots \dots q_s$$

$\mu(m) = (-1)^k, \ \mu(n) = (-1)^s$

$\mu(mn) = (-1)^{k+s}$

$= (-1)^k(-1)^s$

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

$\therefore$ Mobius function is multiplicative

Now, $\mu(4) = 0$

$\mu(2) = -1$

$\mu(4) \neq \mu(2)\mu(2)$

$0 \neq (-1)(-1)$

Hence Mobius function is not completely multiplicative.

Theorem: 5.1

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

Proof:

Given f is multilplicative.

$f(mn) = f(m)f(n), \quad f(m, n) = 1$

Notes

$\mathrm{n} = \mathrm{n}.1$

$\mathrm{f(n)} = \mathrm{f(n\,.1)}$

$= \mathrm{f(n)\, f(1)}$

$\mathrm{f(1)} = 1$

Theorem: 5.2

Let f *be* an arithmetic function with f(1)=1. Then

(a) f is multiplicative if and only if

$f(p_1^{\alpha_1} p_2^{\alpha_2} \dots \dots \dots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \dots \dots \dots f(p_k^{\alpha_k})$ for all primes p_i and all integers $\alpha_i \geq 1$.

(b) If f is multiplicative then f is completely multiplicative if and only if

$f(p^\alpha) = [f(p)]^\alpha \quad$ *for all primes p and all integers* $\alpha \geq 1$

Proof:

Suppose f is multiplicative

Then $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$

The result will prove by induction on "k"

When $k = 1$

$f(p_1^{\alpha_1}) = f(p_1^{\alpha_1})$

The result is true for $k = 1$

We assume that the result is true for all integers $< k$

(i.e) $f(p_1^{\alpha_1} p_2^{\alpha_2} \dots \dots p_k^{\alpha_{k-1}}) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \dots \dots f(p_k^{\alpha_{k-1}})$

Since $p_{1,} p_{2,\dots\dots} p_k$ are distinct primes.

$$\therefore (p_1^{\alpha_1}, p_2^{\alpha_2}, \dots \dots, p_k^{\alpha_k}) = 1$$

Now, $f(p_1^{\alpha_1} p_2^{\alpha_2} \dots \dots p_k^{\alpha_{k-1}} p_k^{\alpha_k}) = f(p_1^{\alpha_1} p_2^{\alpha_2} \dots \dots p_k^{\alpha_{k-1}}) f(p_k^{\alpha_k})$

$= f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \dots \dots f(p_k^{\alpha_{k-1}}) f(p_k^{\alpha_k})$ (by assumption)

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

Conversely, assume that $f(p_1^{\alpha_1} p_2^{\alpha_2} \dots \dots \dots p_k^{\alpha_k}) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \dots \dots \dots (p_k^{\alpha_k})$

Claim: f is multiplicative

Let $(m, n) = 1$

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

$n = {q_1}^{\beta_1}{q_2}^{\beta_2} \dots \dots \dots {q_s}^{\alpha_s}$ where $p_i{}'s$ and $q_j{}'s$ are distinct primes.

Then $mn = ({p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots \dots {p_k}^{\alpha_k})({q_1}^{\beta_1}{q_2}^{\beta_2} \dots \dots {q_s}^{\beta_s})$

$$\mathrm{f(mn)} = \mathrm{f}({p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots \dots {p_k}^{\alpha_k}{q_1}^{\beta_1}{q_2}^{\beta_2} \dots \dots {q_s}^{\beta_s})$$

$$= \mathrm{f}({p_1}^{\alpha_1})\mathrm{f}({p_2}^{\alpha_2}) \dots \dots \dots \mathrm{f}({p_k}^{\alpha_k})\mathrm{f}\left({\beta_1}^{\alpha_1}\right)\mathrm{f}\left({\beta_2}^{\alpha_2}\right) \dots \dots \mathrm{f}({\beta_k}^{\alpha_k})$$

$$= \mathrm{f}({p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots \dots {p_k}^{\alpha_k})\mathrm{f}({\beta_1}^{\alpha_1}{\beta_2}^{\alpha_2} \dots \dots {\beta_k}^{\alpha_k})$$

$$= \mathrm{f(m)f(n)}$$

$\therefore f$ is multiplicative.

Proof of (b):

Suppose f is completely multiplicative.

Then $f(mn) = f(m)f(n) \qquad \forall\, m, n$

Claim: $f(p^\alpha) = [f(p)]^\alpha \qquad \forall\, \alpha$

This will prove by induction on α.

When $\alpha = 1$

$f(p') = [f(p)]'$

$\therefore$ The result is true for $\alpha = 1$

We assume that the result is true for all integers $< \alpha$

i.e) $f(p^{\alpha-1}) = [f(p)]^{\alpha-1}$

Now, $f(p^\alpha) = [f(p^{\alpha-1})(p)]$

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

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

$$= [f(p)]^\alpha$$

Hence, $f(p) = [f(p)]^\alpha \qquad \forall\, \alpha$

Conversely, assume that $f(p^\alpha) = [f(p)]^\alpha \qquad \forall\, \alpha$

Claim: f is completely multiplicative

Let $m = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots \dots {p_k}^{\alpha_k}{p_{k+1}}^{\alpha_{k+1}} \dots \dots {p_r}^{\alpha_r}$ and

$$\mathrm{n} = {p_{k+1}}^{\beta_{k+1}} \dots \dots {p_r}^{\beta_r}{p_{r+1}}^{\beta_{r+1}} \dots \dots {p_s}^{\beta_s}$$

Then

$f(mn) =$

$f({p_1}^{\alpha_1}{p_2}^{\alpha_2} \dots \dots {p_k}^{\alpha_k}{p_{k+1}}^{\alpha_{k+1}+\beta_{k+1}} \dots \dots {p_r}^{\alpha_r+\beta_r}{p_{r+1}}^{\beta_{r+1}} \dots \dots {p_s}^{\beta_s})$

Notes

$= f(p_1^{\alpha_1})f(p_2^{\alpha_2}) \dots \dots f(p_k^{\alpha_k})f\left(p_{k+1}^{\alpha_{k+1}+\beta_{k+1}}\right) \dots \dots f(p_r^{\alpha_r+\beta_r})f\left(p_{r+1}^{\beta_{r+1}}\right) \dots \dots f(p_s^{\beta_s})$

$= f(p_1)^{\alpha_1}f(p_2)^{\alpha_2} \dots \dots f(p_k)^{\alpha_k}f(p_{k+1})^{\alpha_{k+1}}f(p_{k+1})^{\beta_{k+1}} \dots \dots f(p_r)^{\alpha_r}f(p_r)^{\beta_r}f(p_{r+1})^{\beta_{r+1}}$

$= f(p_1^{\alpha_1}p_2^{\alpha_2} \dots \dots p_k^{\alpha_k}p_{k+1}^{\alpha_{k+1}} \dots \dots p_r^{\alpha_r})f(p_{k+1}^{\beta_{k+1}} \dots . p_r^{\beta_r} .. p_r^{\beta_{r+1}} \dots \dots p_s^{\beta_s})$

$= f(m)f(n)$

$\therefore f$ is completely multiplicative.

5.4. Multiplicative functions and dirichlet multiplication:

Theorem 5.3:

$If\ \ f$ and g are multiplicative. Then $(f * g)$ is multiplicative.

Proof:

Let $(m, n) = 1$

To prove that: $f * g$ is multiplicative

i.e) prove that:

$(f * g)(mn) = (f * g)(m)(f * g)(n)$

Now, $(f * g)(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right)$

The divisor of d f mn can put $d = ab$.

$$(f * g)(mn) = \sum_{ab|mn} f(ab)g\left(\frac{mn}{ab}\right)$$

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

$$\left(\begin{array}{l}\therefore\ \ f \textit{ is multiplicative and } (a, b) = 1 \\ g \textit{ is multiplicative and } \left(\frac{m}{a}, \frac{n}{b}\right) = 1\end{array}\right.$$

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

$$= (\mathrm{f} * \mathrm{g})(\mathrm{m})(\mathrm{f} * \mathrm{g})(\mathrm{n})$$

$\therefore f * g$is multiplicative.

Result:

If f is completely multiplicative and g is completely multiplicative. Then $f * g$ **need not be** completely multiplicative.

Notes

W.K.T The unit function u and the power function N are completely multiplicative.

To prove that $(u * N)$ $is\ not\ completely\ multiplicative.$

i.e) to prove that $(u * N)(p^{\alpha}) \neq [(u * N)(p)]^{\alpha}$

Consider $(u * N)(p) = \sum_{d|1} u(d)N\left(\frac{p}{d}\right)$

$$= \mathrm{u(1)N(p) + u(p)N(1)}(\because \mathrm{d = 1, p})$$

$$= \mathrm{p} + 1$$

$[(u * N)(p)]^{\alpha} = (1 + p)^{\alpha}$

$$(u * N)(p^{\alpha}) = \sum_{d|p^{\alpha}} u(d)N\left(\frac{p^{\alpha}}{d}\right)$$

$$= u(1)N(p^{\alpha}) + u(p)N(p^{\alpha-1}) + u(p^2)N(p^{\alpha-2}) + \cdots + u(p^{\alpha})N(1)$$

$$= \mathrm{p}^{\alpha} + \mathrm{p}^{\alpha-1} + \cdots\cdots\cdots + 1$$

$$\neq (1 + \mathrm{p}^{\alpha})$$

$(\mathrm{u} * \mathrm{N})(\mathrm{p}) \neq [(\mathrm{u} * \mathrm{N})(\mathrm{p})]^{\alpha}$

Theorem 5.4:

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

Proof:

The proof is given by contradiction

Assume that, f is not multiplicative

i.e) $f(mn) \neq f(m)f(n)$ whenever $(m, n) = 1$

If we choose such a $m\ and\ n$ for which the product $mn\ is\ as\ small\ as\ possible.$

i.e) $ab < mn, \qquad (a, b) = 1$

$\therefore f(ab) = f(a)f(b)$

Case(i):

If $mn = 1$

i.e) $m = 1, n = 1$

$f(mn) \neq f(m)f(n)$

$\therefore f(1) \neq 1$

$\therefore f\ is\ not\ multiplicative$

Notes

Now, $(f * g)(1) = \sum_{d|1} f(d)g\left(\frac{1}{d}\right)$

$= f(1)g(1)$

$\neq 1$

$Since\ g\ is\ multiplicative \Rightarrow g(1) = 1$ and $f(1) \neq 1$

$\Rightarrow f * g\ is\ not\ multiplicative$

$\Rightarrow\Leftarrow to\ f * g\ is\ multiplicative$

$\therefore f$ is multiplicative.

Case(ii): If $mn > 1$ and mn is the least product for which

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

If $ab < mn$, $\quad (a, b) = 1$

$f(ab) = f(a)f(b)$ here $\left(\frac{m}{a}, \frac{n}{b}\right) = 1$

Consider $(f * g)(mn) = \sum_{d|mn} f(ab)g\left(\frac{mn}{d}\right)$

$$= \sum_{ab|mn} \mathrm{f(ab)g}\left(\frac{\mathrm{mn}}{\mathrm{ab}}\right)$$

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

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

(Since $g\ is\ multiplicative\ \ and\ g(1) = 1$)

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

$= (f * g)(m)(f * g)(n) - f(m)f(n) + f(mn)$

$\therefore (f * g)(mn) \neq (f * g)(m)(f * g)(n)$

$(\because f(mn) - f(m)f(n) \neq 0)$

$\therefore f * g$ is not multiplicative.

We get a contradiction.

In both the cases we get a contradiction.

Hence f is multiplicative.

Theorem 5.5:

If g is multiplicative then its dirichlet inverse g^{-1} is also multiplicative.

Proof:

W.K.T, $g * g^{-1} = I$ where I is an identity function

The identity function is completely multiplicative.

So, I is multiplicative

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

Given: g is multiplicative.

By theorem 5.4, $g^{-1}$is multiplicative.

5.5 The inverse of a completely multiplicative function:

The dirichlet inverse of a completely multiplicative function is especially easy to determine.

Theorem 5.6:

Let f be multiplicative. Then f is completely multiplicative if and only if

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

Proof:

Assume that f is completely multiplicative

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

To prove that: $f^{-1}(n) = g(n)$

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

$$= \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right)$$

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

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

$$= f(n)\left[\frac{1}{n}\right]$$

$$= f(n)I(n)$$

$= I(n)$ $\qquad$ $(\therefore f(n)I(n) = f(1)I(1) + 0$

Notes

$g * f = I$

$\therefore g = f^{-1}$

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

Conversely, assume that f be multiplicative and

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

To prove that: f is completely multiplicative

i.e) to prove that $f(p)^{\alpha} = (f(p))^{\alpha}$ for all prime p and $\alpha \geq 1$

W.K.T $\quad f * f^{-1} = 1$

$(\mathrm{f}^{-1} * \mathrm{f})(\mathrm{n}) = \mathrm{I}(\mathrm{n})$

$$\sum_{d|n} f^{-1}(d)f\left(\frac{n}{d}\right) = I(n)$$

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

Put $n = p^{\alpha}$

$\sum_{d|p^{\alpha}} \mu(d)f(d)f\left(\frac{p^{\alpha}}{d}\right) = 0$ if n>1

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

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

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

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

$$\vdots$$

$$\vdots$$

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

Hence f is completely multiplicative.

Result: What is the inverse Euler's totient function ?

W.K.T $\quad \phi = \mu * N$

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

W.K.T, the power function is completely multiplicative

By previous theorem,

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

$= (N\mu)(n)$

Notes

$$\therefore\ \phi^{-1} = \mu^{-1} * N^{-1}$$

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

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

$$= \sum_{d|n} (\mu N)(d) u\left(\frac{n}{d}\right)$$

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

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

Theorem 5.7:

Let f be multiplicative. Then $\sum_{d|n} f(d)\mu(d) = \prod_{p|n}(1 - f(p))$ and hence $\phi^{-1}(n) = \prod_{p|n}(1 - p)$.

Proof:

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

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

$$= \sum_{d|n} (f\mu)(d) u\left(\frac{n}{d}\right)$$

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

$$g = f\mu * u$$

Since $f\ and\ \mu$ is multiplicative

$\therefore f\mu$ is multiplicative.

W.K.T, u is multiplicative.

$f\mu * u$ is multiplicative.

$\therefore g$ is multiplicative.

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

$$= f(1)\mu(1) + f(p)\mu(p) + f(p^2)\mu(p^2) + \cdots\cdots + f(p^\alpha)\mu(p^\alpha)$$

$$(\ since d = 1, p, \ldots\ldots\ldots p^\alpha)$$

$= 1 - f(p) \quad (\therefore f\ is\ multiplicative, f(1) = 1, \mu(p^2) = \mu(p^\alpha) = 0..)$

Notes

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots \dots p_k^{\alpha_k}$ where $p_i's$ are distinct primes and $\alpha_i \geq 1$

$$g(n) = g(p_1^{\alpha_1} p_2^{\alpha_2} \dots \dots . p_k^{\alpha_k})$$

$$= g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) \dots \dots g(p_k^{\alpha_k}) \quad (\therefore g \textit{ is multiplicative}$$

$$= \big(1 - f(p_1)\big)\big(1 - f(p_2)\big) \dots \dots (1 - f(p_k))$$

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

$$\therefore \sum_{d|n} \mu(d) f(d) = \prod_{p|n} \big(1 - f(p)\big) \qquad \rightarrow (*)$$

W.K.T, $\phi^{-1}(n) = \sum_{d|n} d\, \mu(d)$

Comparing to $(*)$ we get

$$\phi^{-1}(n) = \prod_{p|n} (1 - p)$$

Definition 5.6: Liouville's function $\lambda(n)$

Definition 5.1.3: Liouville's function λ is an arithmetic function is defined by

$\lambda(1) = 1$ and i$f\ n = p_1^{\alpha_1} \dots \dots \dots p_k^{\alpha_k}$ we define

$\lambda(n) = (-1)^{\alpha_1 + \alpha_2 + \dots + \alpha_k}$

Note:

1) $\lambda(p^\alpha) = (-1)^\alpha$
$=[(-1)]^\alpha$

$\therefore$ Hence liouville's function is completely multiplicative.

Theorem 5.6:

For $every\ n \geq 1,$ we have

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & if\ n\ is\ a\ square \\ 0 & otherwise \end{cases}$$

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

Proof:

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

$$= \sum_{d|n} \lambda(d) u\left(\frac{n}{d}\right)$$

$$g(n) = (\lambda * u) n$$

Since λ *and* μ are multiplicative

Notes

$\lambda * u$ is multiplicative

Put $n = p^\alpha$

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

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

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

$$= \begin{cases} 1 \quad if \;\; \alpha \; is \; even \\ 0 \; if \; \alpha \; is \; odd \end{cases}$$

$n = {p_1}^{\alpha_1} \dots \dots \dots {p_k}^{\alpha_k}$ where $p_i' sare\ distnct\ primes\ and\ \alpha_i \geq 0$

$$g(n) = g({p_1}^{\alpha_1}) \dots \dots . g({p_k}^{\alpha_k})$$

$$= \begin{cases} 1 \quad if\ each\ \alpha_i\ is\ even \\ 0\ if\ atleast\ \alpha_i\ is\ odd \end{cases}$$

$$\alpha_i = 2\beta_j$$

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

$$n = {p_1}^{2\beta_1} \dots \dots \dots . {p_k}^{2\beta_k}$$

$$= \left({p_1}^{\beta_1}\right)^2 \dots \dots \dots . \left({p_k}^{\beta_k}\right)^2$$

$$g(n) = \begin{cases} 1\ if\ n\ is\ square \\ 0 \quad otherwise \end{cases}$$

$$\sum_{d|n} \lambda(d) = \begin{cases} 1\ if\ n\ is\ square \\ o \qquad otherwise \end{cases}$$

W.K.T λ is completely multiplicative

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

$$= \mu(n)\mu(n)$$

$$= \mu^2(n)$$

$$= |\mu(n)|$$

Definition 5.1.4: For any real or complex $\alpha\ and\ \ any\ integer\ n \geq 1$ the divisor function is defined by $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$

i.e) $\sigma_\alpha(n)$ is the sum of the α^{th} power of divisors of n.

Note: 1

$\sigma_\alpha$is multiplicative

Notes

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

$$= \sum_{d|n} N^\alpha(d)u\left(\frac{n}{d}\right)$$

$$= (N^\alpha * u)(n)$$

Note: 2

If $\alpha = 0$

$$\sigma_0(n) = \sum_{d|n} d^0 = \sum_{d|n} 1$$

The number of divisors of n it is denoted by $d(n)$.

i.e) $\sigma_0(n) = d(n)$

Note: 3

If $\alpha = 1$

$\sigma_1(n) = \sum_{d|n} d$ = sum of the divisors of n

It is denoted by $\sigma(n)$

$\therefore \sigma_1(n) = \sigma(n)$

Theorem 5.7

For $n \geq 1$, we have

$$\sigma_\alpha{}^{-1}(n) = \sum_{d|n} d^\alpha \mu(d)\mu\left(\frac{n}{d}\right)$$

Proof:

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

$$= \sum_{d|n} N^\alpha(d)u\left(\frac{n}{d}\right)$$

$$= (N^\alpha * u)(n)$$

$$\therefore \sigma_\alpha = N^\alpha * u$$

$$\sigma_\alpha{}^{-1} = (N^\alpha)^{-1} * u^{-1}$$

Since N^α is completely multiplicative

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

Notes

$$= (N^{\alpha}\mu)(n)$$

$$\therefore \sigma_{\alpha}{}^{-1}(n) = ((N^{\alpha}\mu) * \mu)(n)$$

$$= \sum_{d|n} (N^{\alpha}\mu)(d)\mu\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} (N^{\alpha})(d)\mu(d)\mu\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} d^{\alpha}\mu(d)\mu\left(\frac{n}{d}\right)$$

5.7 Exercise:

1.Assume f is multiplicative. Prove that:

(a) $f^{-1}(n) = \mu(n)f(n)$ for every square free n.
(b) $f^{-1}(p^2) = f(p)^2 - f(p^2)$ for every prime p.

2.Assume f is multiplicative. Prove that f is completely multiplicative if and only if

$f^{-1}(p^n) = 0$ for all primes p and all integers a≥ 2.

3.If f is completely multiplicative, prove that $f.(g * h) = (f.g) * (f.h)$ for all arithmetical functions g and h, where f.g denotes ordinary product (f.g)(n)=f(n)g(n).

4.If f is multiplicative and relations in (a) holds for $g = \mu$ and $h = \mu^{-1}$, prove that f is completely multiplicative.

5. If f is completely multiplicative, prove that$(f.g)^{-1} = f.g^{-1}$ for every arithmetical functions g(1)$\neq 0$.

6. If f is multiplicative and relations in (a) holds for $g = \mu^{-1}$, prove that f is completely multiplicative.

Notes

UNIT-VI: FORMAL POWER SERIES

Structure:

6.1 Introduction:

This unit gives the idea of convolutions and gives the relation between associative property of dirichlet multiplication and convolution of any three arithmetical functions. It derives the Gereralized Mobius inversion formula by using convolutions.

6.2 Objectives:

The students will be able to

- Analyse the convolution of arithmetical functions
- Describe the properties of convolutions
- Recognise the relation between power series of arithmetical functions

6.3 Generalized Convolutions

Definition 6.1.1:

Let F be a real or complex valued function defined on the positive real axis such that $F(x) = 0,\ 0 < x < 1$.

Let α be an arithmetical function then the sum of $G(x) = \sum_{n\le x} \alpha(n) F(\frac{x}{n})$ is called the generalized convolutions of G and is denoted by $G = (\alpha \circ F)$.

(i.e) $(\alpha \circ F)(x) = \sum_{n\le x} \alpha(n) F(\frac{x}{n})$.

Theorem 6.1 Associative property for relating with $\circ$ *and* $*$

For any arithmetical function α *and* β , we have $\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F$.

Proof:

$[\alpha \circ (\beta \circ F)](x) = \sum_{n\le x} \alpha(n) (\beta \circ F)(\frac{x}{n})$

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

Notes

$= \sum_{mn\le x} \alpha(n)\beta\left(\frac{k}{n}\right) F(\frac{x}{k})$, mn=k

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

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

$$= [(\alpha * \beta) \circ \mathrm{F}](x)$$

Therefore $[\alpha \circ (\beta \circ \mathrm{F})] = (\alpha * \beta) \circ \mathrm{F}$

Theorem 6.2 Generalized inversion formula

If α has a Dirichlet inverse α^{-1} then the equation $G(x) = \sum_{n\le x} \alpha(n) F(\frac{x}{n})$ if and only if $F(x) = \sum_{n\le x} \alpha^{-1}(n) G(\frac{x}{n})$

Proof:

Let $G = \alpha \circ F$

Then multiply α^{-1} on both sides

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

$$\alpha^{-1} \circ G = (\alpha^{-1} * \alpha) \circ F = I \circ F = F$$

$$\therefore F(x) = (\alpha^{-1} \circ G)(x) = \sum_{n\le x} \alpha^{-1}(n) G\left(\frac{x}{n}\right)$$

Conversely, assume that $F(x) = \sum_{n\le x} \alpha^{-1}(n)\, G\left(\frac{x}{n}\right)$

$$\therefore F(x) = (\alpha^{-1} \circ G)(x)$$

$\Rightarrow F = \alpha^{-1} \circ G$ (multiply α on both side)

$$\Rightarrow \alpha \circ F = \alpha \circ (\alpha^{-1} \circ G) = (\alpha * \alpha^{-1}) \circ G = I \circ G = G$$

$$\therefore G(x) = (\alpha \circ F)(x)$$

$$G(x) = \sum_{n\le x} \alpha(n) F\left(\frac{x}{n}\right)$$

Theorem 6.3: Generalized Möbius inversion formula

If α is completely multiplicative, then the equation $G(x) = \sum_{n\le x} \alpha(n) F\left(\frac{x}{n}\right)$ if and only if $F(x) = \sum_{n\le x} \alpha(n)\mu(n) G\left(\frac{x}{n}\right)$

Notes

Proof:

Assume that $G(x) = \sum_{n \le x} \alpha(n) F\left(\frac{x}{n}\right)$

$$G(x) = (\alpha \circ F)(x)$$

$\therefore G = \alpha \circ F$ (multiply α^{-1} on both side)

$$\alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ F) = (\alpha^{-1} * \alpha) \circ F = I \circ F = F$$

$$\therefore F(x) = (\alpha^{-1} \circ G)(x)$$

$$F(x) = \sum_{n \le x} \alpha^{-1}(n) G\left(\frac{x}{n}\right)$$

$$F(x) = \sum_{n \le x} \alpha(n)\mu(n) G\left(\frac{x}{n}\right)$$

(since α is completely multiplicative)

Conversely assume that, $F(x) = \sum_{n \le x} \alpha(n)\mu(n) G\left(\frac{x}{n}\right)$

$$F(x) = \sum_{n \le x} \alpha^{-1}(n) G\left(\frac{x}{n}\right)$$

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

$\therefore F = \alpha^{-1} \circ G$ (multiply α on both sides, we get)

$$\alpha \circ F = \alpha \circ (\alpha^{-1} \circ G) = (\alpha * \alpha^{-1}) \circ G = I \circ G = G$$

$$\therefore G(x) = (\alpha \circ F)(x) = \sum_{n \le x} \alpha(n) F\left(\frac{x}{n}\right)$$

Hence the proof

6.4 Formal power series:

In calculus an infinite series of the form

$$\sum_{n=0}^{\infty} a(n)x^n = a(0) + a(1)x + a(2)x^2 + \cdots + a(n)x^n + \ldots$$

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 $r \ge 0$ such that the series converges absolutely if $|x| < r$ and diverges if $|x| > r$.(The radius r can be $+\infty$).

In this section we consider power series from a different point of view.We call them formal power series to distinguish them from the ordinary power series of calculus. In the theory of formal power series x assigned a numerical value, and questions of convergence or divergence are not of interest.

The object of interest is the sequence of coefficients

$$(a(0), a(1), \ldots \ldots a(n), \ldots \ldots)$$

All what we do with formal power series could also be done by treating the sequence of coefficients as though it were an infinite dimensional vector with components a(0),a(1),…a(n) but for our purpose it is more convenient to display the terms as coefficients of a power series as in (12) rather than as components of a vector as in (13). 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 constant coefficients of the series.

Notes

We operate on formal power series algebraically as though they were convergent power series. If A(x) and B(x) are two formal power series, say

$$A(x) = \sum_{n=0}^{\infty} a(n)x^n \qquad and \qquad B(x) = \sum_{n=0}^{\infty} b(n)x^n$$

We define:

Equality: A(x) = B(x) means that a(n)=b(n) 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) = $\sum_{n=0}^{\infty} c(n)x^n$

$$c(n) = \sum_{k=0}^{n} a(k)b(n-k) \ldots \ldots \ldots \ldots \ldots (14)$$

The sequence $\{c(n)\}$ determined by (14) is called the Cauchy product of the sequences {a(n)} and {b(n)}.

The reader can easily verify that these two operations satisfy the commutative and associative laws, and that multiplication is distributive with respective to addition. In the language of modern algebra, formal power series form a ring. The ring has a zero element for addition which we denote by 0.

$0 = \sum_{n=0}^{\infty} a(n)x^n$,where a(n) = 0 for all $n \geq 0$,

And an identity element for multiplication which we denote by 1,

$$1 = \sum_{n=0}^{\infty} a(n)x^n \,, where\ a(0) = 1\ and\ a(n) = 0\ for\ n \geq 1,$$

A formal power series is called a formal polynomial if all its coefficients are 0from some point on.

For each formal power series $A(x) = \sum_{n=0}^{\infty} a(n)x^n$ with constant coefficients $a(0) \neq 0$, there is a uniquely determined formal power series

$B(x) = \sum_{n=0}^{\infty} b(n)x^n$such that A(x)B(x)=1. Its coefficients can be determined by solving the infinite system of equations

$$a(0)b(0) = 1$$

$$a(0)b(1) + a(1)b(0) = 0$$

Notes

In succession for b(0), b(1),b(2),… The series B(x) is called the inverse of A(x)

$$\text{The special series, } A(x) = 1 + \sum_{n=0}^{\infty} a(n)x^n$$

Is called a geometric series. Here a is an arbitrary real or complex number. Its inverse is the formal power series

$$B(x) = 1 - ax$$

In otherwords, we have

$$\frac{1}{1-ax} = 1 + \sum_{n=0}^{\infty} a(n)x^n.$$

Exercise:

1.Let f be a multiplicative and let g be any arithmetical function. Assume that

(a) $f(p^{n+1}) = f(p)f(p^n) - g(p)f(p^{n-1})$ for all primes p and all $n \geq 1$.

Prove that for each prime p the Bell series for f has the form

(b) $f_{p(x)=} \frac{1}{1-f(p)x+g(p)x^2}$.

Conversely, prove that (b) implies (a).

2. If g is completely multiplicative prove that statement (a) of above exercise 1 implies

$f(m)f(n) = \sum_{d|(m,n)} g(d)f(\frac{mn}{d^2})$,

Where the sum is extended over the positive divisors of the gcd(m,n). [Hint: Consider first the case $m = p^a, n = p^b$.]

UNIT: VII BELL SERIES

Structure

7.1 Introduction:

This unit explores the properties of multiplicative arithmetical functions using formal power series. It explains the relation between multiplication of Bell series to Dirichlet multiplication. It states that the usual rules for differentiating sums and products also hold if the products are dirichlet products.

7.2 Objectives:

The students will be able to

- Describe the Bell series of arithmetical functions
- Determine the derivatives of inverse functions
- Derive Selberg identity

7.3 The Bell series of an arithmetical function:

Given an arithmetical function f and a prime p, we denote by $f_p(x)$ 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.

Bell series are especially useful when f is multiplicative.

Theorem:7.1 (Uniqueness theorem)

Let f and g be multiplicative functions then f = g if and only if,

$f_p(x) = g_p(x)$ for all primes p.

Proof:

If f = g then $f(p^n) = g(p^n)$ for all p and all $n \geq 0$, so $f_p(x) = g_p(x)$. Conversely, if $f_p(x) = g_p(x)$ for all p then $f(p^n) = g(p^n)$ for all $n \geq 0$. Since f and g are multiplicative and agree at all prime powers they agree at all the positive integers, so f = g.

Notes

Example: 1

Mobius function μ. Since $\mu(p) = -1$ and $\mu(p^n) = 0$ for n ≥ 2 we have

$$\mu_p(x) = 1 - x.$$

7.4 Bell series and Dirichlet multiplication:

Theorem:7.2

For any two arithmetical functions f and g let $h = f * g$. Then for every prime p we have $\mu_p(x) = f_p(x) g_p(x)$

Proof:

Since the divisors of p^n are 1, p, p^2 ... p^n we have

$$h(p^n) = \sum_{d|p^n} f(d) g\left(\frac{p^n}{d}\right) = \sum_{n=0}^{\infty} f(p^k) g(p^{n-k}).$$

This completes the proof because the last sum is the Cauchy product of the sequences {f(p^n)} and {g(p^n)}.

7.5 Derivative of arithmetical functions:

Definition 7.1.1: For any arithmetical function f we define its derivative $f'$to be the arithmetical function given by the equation $f'(n)$ =f(n)log n for n≥ 1.

Example: since I(n)log n =0 for all n we have I'=0. Since u(n)=1 for all n we have $u'(n)$=log n. Hence, the formula $\sum_{d|n} \wedge(d)$=log n can be written as

$$\wedge * u = u' \ldots\ldots\ldots\ldots\ldots(1)$$

Theorem 7.3: If f and g are arithmetical functions we have:

a) $(f + g)' = f' + g'$.
b) $(f * g)' = f' * g + f * g'$.
c) $(f^{-1})' = -f' * (f * f)^{-1}$, provide that f(1)≠0.

Proof:

The proof of (a) is immediate . of course , it is understood that f+g is the function for which (f+g)(n)=f(n)+g(n) for all n.

To prove (b) we use the identity log n=log d+log(n/d) to write

$$(f * g)'(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \log n$$

$$= \sum_{d|n} f(d) \log d \, g\left(\frac{n}{d}\right) + \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \log \frac{n}{d}$$

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

To prove(c) we apply part (b) to the formula I'=0, remembering that I=f*f^{-1}. This gives us

$$0=(f * f^{-1})'= f' * f^{-1} + f * (f^{-1})'$$

So f * $(f^{-1})' = -(f' * f^{-1}) * f^{-1} = f' * (f^{-1} * f^{-1})$.

But $(f^{-1} * f^{-1}) = (f * f)^{-1}$ so (c) is proved.

7.6 THE SELBERG IDENTITY

Using the concept of derivative we can quickly derive a formula of selberg which is sometimes used as the starting point of an elementary proof of the prime number theorem.

Theorem 7.4: (**The selberg identity)**

For n ≥1 we have, $\wedge(n) \log n + \sum_{d|n} \wedge(d)\wedge(\frac{n}{d}) = \sum_{d|n} \mu(d) log^2(\frac{n}{d})$.

Proof:

WKT $\wedge * u = u'$. Differentiation of this equation gives us

$\wedge' * u + \wedge * u' = u''$

Or since $\wedge * u = u'$,

$\wedge' * u + \wedge * (\wedge * u) = u''$

Now we multiply both sides by $\mu = u^{-1}$ to obtain

$\wedge' + \wedge * \wedge = u'' * \mu$.

This the required identity.

7.7 Exercise:

1.Prove that $\sigma_\alpha(m)\sigma_\alpha(n) = \sum_{d|(m,n)} d^\alpha \sigma_\alpha\left(\frac{mn}{d^2}\right)$.

2.Prove that Liouville's function is given by the formula $\lambda(n) = \sum_{d^2|n} \mu\left(\frac{n}{d^2}\right)$.

3.Assume that g is multiplicative and let f=g^{-1}

a) prove that if p is prime and k≥ 1 we have

f(p^k)= -$\sum_{t=1}^{k} g(p^t) f(p^{k-t})$.

b) Let h be the uniquely determined multiplicative function which agrees with f at the prime powers. Show that h*g agrees with the identity function I at the prime powers and

c) deduce that h*g=I. This shows that f=h so f is multiplicative.

4.If f and g are multiplicative and if a and b are positive integers with a≥ b, prove that the function h is given by

Notes

$h(n) = \sum_{d^a|n} f\left(\frac{n}{d^a}\right) g\left(\frac{n}{d^b}\right)$ is also multiplicative. The sum is extended over those divisors d of n for which d^a divides n.

UNIT – VIII : AVERAGES OF ARITHMETICAL FUNCTIONS

Structure

8.1 Introduction:

Big O notation is a mathematical notation that describes the limiting behavior of a function when the argument tends towards a particular value or infinity. It is a member of a family of notations invented by Paul Bachmann, Edmund Landau is called Bachmann–Landau notation or asymptotic notation. This unit explores Big oh function and its importance.

8.2 Objectives:

The students will be able to

- Determine Big oh function and its relations
- Recognise the equality of functions
- Describe the properties of Big Oh functions

General Introduction:

The last chapter discussed various identities satisfied by arithmetical functions such as $\mu(n), \varphi(n), \Lambda(n)$ and the divisor functions $\sigma(n)$.we enquire about the behaviour of these and other arithmetical functions f(n) for large values of n.

For example, consider d(n), the number of divisors of n. This function takes on the value 2 infinitely often(when n is prime) and it also takes on arbitrarily large values when n has large number of divisors. Thus the value of d(n) fluctuate considerably as n increases.

Many arithmetical functions fluctuates in this manner and it is often difficult to determine their behaviour for large n. sometimes it is more fruitful to study the arithmetical mean.

$$\check{f}(n) = \frac{1}{n}\sum_{k=1}^{n} f(k)$$

Averages smooth out fluctuations so it is reasonable to expect that the mean value $\check{f}(n)$ might behave more regularly than f(n). This is indeed the case for the divisor function d(n).we will prove later that the average grows like log n. more precisely,

$$\log_{n\to\infty} \frac{\widetilde{d\ (n)}}{\log n} = 1 \ldots\ldots(1)$$

To study the average of an arbitrary function f need a knowledge of its partial sum .sometimes it is convenient to replace the upper index n by an arbitrary positive real number x and to consider instead sums of the form

$$\sum_{k\le x} f(k)$$

Here it is understood that the index k varies from 1 to $[x]$, the greatest integer $\le x$. If $0 < x < 1$ the sum is empty and we assign it the value 0. Our goal is to determine the behaviour of this sum as a function of x, especially for large x.

For the divisor function we will prove a result obtained by dirichlet in 1849, which is stronger than (1), namely

$\sum_{k\le x} d(k) = xlogx + (2c - 1)x + O(\sqrt{x})$…….(2)

For all $x \ge 1$. Here C is Euler's constant, defined by the equation

$C = \lim_{n\to\infty}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - logn\right)$………..(3)

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 "big oh" notation which is defined as follows.

8.3 The big oh notation. Asymptotic equality of functions:

Definition: If g(x)> 0, for all $x \ge a$, we write $f(x) = O(g(x))$ to mean that the quotient $\frac{f(x)}{g(x)}$ is bounded for $x \ge a$; (i.e.,) there exist a constant M> $0, such\ that$

$$|f(x)| \le Mg(x) \qquad for\ all\ x \ge a$$

An equation of the form

$$f(x) = h(x) + O\big(g(x)\big)$$

Means that $f(x) - h(x) = O\big(g(x)\big)$. we note that $f(t) = O(g(t))$ for $t \ge a$, implies

$\int_a^x f(t)dt = O\left(\int_a^x g(t)dt\right)$ for $x \ge a$

Definition: If

$$\lim_{n\to\infty} \frac{f(x)}{g(x)} = 1$$

We say that f(x) is asymptotic to g(x) as $x \to \infty$, and we write

$$f(x) \sim g(x) \quad as\ x \to \infty$$

For example, eq (2) implies that

$$\sum_{k \le x} d(k) \sim x log x \quad as\ x \to \infty.$$

In equation (2), the term x logx is called the asymptotic value of the sum; the other two terms represent the error made by approximating the sum by its asymptotic value. If we denote this error by E(x), then (2) states that

$$E(x) = (2C-1)x + O(\sqrt{x}) \ldots\ldots\ldots(4)$$

This could also be written E(x) = O(x), an equation which is correct but which does not convey the more precise information in eq (4). eq (4) tells us that the asymptotic value of E(x) is $(2C-1)x$.

Notes

8.4 Exercises:

(1) *Use Euler's summation formula to deduce the following for* $x \ge 2$,

$$\sum_{n \le x} \frac{\log n}{n} = \frac{1}{2} log^2 x + A + O\left(\frac{\log x}{x}\right), where\ A\ is\ a\ constant.$$

(2) *Use Euler's summation formula to deduce the following for* $x \ge 2$,

$$\sum_{2 \le n \le x} \frac{1}{n \log n} = \log(\log x) + B + O\left(\frac{1}{x \log x}\right), where\ B\ is\ a\ constant.$$

(3) *If* $x \ge 2$ *Prove that*

$$\sum_{n \le x} \frac{d(n)}{n} = \frac{1}{2} log^2 x + 2C \log x + O(1), where\ C\ is\ Euler's\ constant.$$

(4) *If* $x \ge 2$ *and* $\alpha > 0, \alpha \ne 1$ *Prove that*

$$\sum_{n \le x} \frac{d(n)}{n^\alpha} = \frac{x^{1-\alpha} \log x}{1-\alpha} + \zeta(\alpha)^2 + O(x^{1-\alpha}).$$

(5) *If* $x \ge 2$ *Prove that*: $\sum_{n \le x} \mu(n) \left[\frac{x}{n}\right]^2 = \frac{x^2}{\zeta(2)} + O(x log\ x).$

Notes

BLOCK III: DIRICHLET PRODUCT AND CONGRUENCES

UNIT-IX: ASYMPTOTIC FORMULAS

Structure:

9.1 Introduction:

Sometimes the asymptotic value of a partial sum can be obtained by comparing it with an integral. Eulers summation formula gives an exact expression for the error made in such approximation. This unit derives the Dirichlet asymptotic formula for the partial sums of the divisor function d(n), σ_α(n) .

9.2 Objectives:

The students will be able to

- Determine the Eulers summation formula
- Describe the asymptotic formulas
- Recognise the average order of d(n)

9.3 Euler's summation formula:

Theorem 9.1:

If f has a continuous derivative f' on the interval [y, x], where 0 < y <x, then

$$\sum_{y<n\leq x} f(n) = \int_y^x f(t)dt + \int_y^x (t-[t])\, f'(t)dt + f(x)([x]-x) - f(y)([y]-y).$$

Proof:

Notes

Let m=[y], k=[x]. For any interval (n-1, n) in [y, x], then

$$\int_{n-1}^{n} [t]f'(t)dt = \int_{n-1}^{n} (n-1)f'(t)dt$$

$$= (n-1) \int_{n-1}^{n} f'(t)dt$$

$$= (n-1)[f(n) - f(n-1)]$$

$$= \{nf(n) - (n-1)f(n-1)\} - f(n) \quad \rightarrow (1)$$

Summing up for n=m+1,m+2,...,k, we have

$$\int_{n-1}^{n} [t]f'(t)dt = \int_{m}^{m+1} [t]f'(t)dt + \int_{m+1}^{m+2} [t]f'(t)dt + \cdots \cdots \cdots$$
$$+ \int_{k-1}^{k} [t]f'(t)dt$$

$= (m+1)f(m+1) - mf(m) - f(m+1) + (m+2)f(m+2) -$
$(m+1)f(m+1) - f(m+2) + (m+3)f(m+3) - (m+2)f(m+$
$2 - fm+3+ \cdots \cdots \cdots + kfk - k-1fk-1 - f(k)$
(by using(1))

$$= kf(k) - mf(m) - f(m+1) - f(m+2) - f(m+3) - \cdots \cdots \cdots$$
$$- f(k)$$

$$\therefore \int_{m}^{k} [t]f'(t)dt = kf(k) - mf(m) - \sum_{y<n\leq x} f(n)$$

$$\sum_{y<n\leq x} f(n) = kf(k) - mf(m) - \int_{m}^{k} [t]\, f\,'(t)dt \rightarrow (2)$$

Now, $\int_m^y [t] f\,'(t)dt = \int_m^y mf\,'(t)dt = mf(y) - mf(m)$

$$\int_{m}^{y} [t]\, f'(t)dt - mf(y) = -mf(m) \rightarrow (3)$$

$$\int_{k}^{x} [t]f'(t)dt = k\int_{k}^{x} f'(t)dt = kf(x) - kf(k)$$

$$kf(k) = kf(x) - \int_{k}^{x} [t]f'(t)dt \ \rightarrow (4)$$

Using (3) and (4), (2) becomes,

Notes

$$\sum_{y<n\leq x} f(n) = kf(x) - mf(y) - \int_k^x [t]\, f'(t)dt + \int_m^y [t]\, f'(t)dt - \int_m^k [t]\, f'(t)dt$$

$$\sum_{y<n\leq x} f(n) = kf(x) - mf(y) - \int_k^x [t]\, f'(t)dt - \int_m^k [t]\, f'(t)dt - \int_y^m [t]\, f'(t)dt$$

$$= kf(x) - mf(y) - \int_y^x [t]\, f'(t)dt \qquad \rightarrow (5)$$

$$\int_y^x tf'(t)dt = xf(x) - yf(y) - \int_y^x f(t)dt$$

$$\int_y^x tf'(t)dt - xf(x) + yf(y) + \int_y^x f(t)dt = 0 \qquad \rightarrow (6)$$

Using (6) , (5) becomes

$$\sum_{y<n\leq x} f(n) = [x]f(x) - [y]f(y) - \int_y^x [t]f'(t)dt + 0$$

$$\sum_{y<n\leq x} f(n) = [x]f(x) - [y]f(y) - \int_y^x [t]f'(t)dt + \int_y^x tf'(t)dt - xf(x) + yf(y) + \int_y^x f(t)dt$$

$$\therefore \sum_{y<n\leq x} f(n) = \int_y^x f(t)dt + \int_y^x (t-[t])f'(t)dt + f(x)\{[x]-x\} - f(y)\{[y]-y\}$$

9.4 Some elementary asymptotic formulas:

Definition 9.1.1: "Euler's constant"

The Euler's constant C is defined by C$= \lim_{n\to\infty}\{\sum_{k=1}^{n}\frac{1}{k} - logn\}$

Definition 9.1.2:

Let a be a real number and let f(x) be a function and g(x) >0 , then there is a constant m>0 , such that $|f(x)| \leq mg(x)$, for all $x \geq a$. Then f(x) is said to be "big oh" of g(x)

$we\ write\ f(x)$ =O(g(x))

Result:

1. **O(f(x)) + O(f(x))= O(f(x))**

Let g(x) $= O(f(x))$, then there exists $m_1 > 0$ such that |g(x)| $\leq m_1 f(x)$, for all $x \geq a$
Let $h(x) = O(f(x))$, then there exists $m_2 > 0$ such that $|h(x)| \leq m_2 f(x)$, for all $x \geq a$

$$\begin{aligned} |g(x) + h(x)| &\leq |g(x)| + |h(x)| \\ &\leq m_1 f(x) + m_2 f(x) \\ &= (m_1 + m_2) f(x) \\ &= mf(x) \end{aligned}$$

where $m_1 + m_2 = m$

$$g(x) + h(x) = O(f(x))$$

∴O(f(x)) + O(f(x)) = O(f(x))

2. $\boldsymbol{\int_a^x O(f(x))dx = O(\int_a^x f(x)dx)}$

Let g(x) $= O(f(x))$, then there exists $m > 0$ such that $|g(x)| \leq mf(x)$, for all $x \geq a$

$$\left|\int_a^x g(x)\,dx\right| \leq \int_a^x |g(x)|dx \leq \int_a^x mf(x)dx$$

$$\int_a^x g(x)\,dx = O(\int_a^x f(x)dx)$$

$$\therefore \int_a^x O(f(x))dx = O(\int_a^x f(x)dx)$$

Definition 9.1.3: "Riemann Zeta function"
The Riemann Zeta function is defined by

$$\zeta(s) = \begin{cases} \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^s} & ,if\ s > 1 \\ \displaystyle\lim_{x\to\infty} (\sum_{n \leq x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s}) & ,if\ 0 < s < 1 \end{cases}$$

Notes

Theorem 9.2:

If $x \geq 1$ we have:

$(a)\ \sum_{n\leq x}\frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$, where C is Euler's constant.

$(b)\ \sum_{n\leq x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s})$, if $s > 0, s \neq 1$.

$(c)\ \sum_{n>x}\frac{1}{n^s} = O(x^{1-s})$, if $s > 1$.

$(d)\ \sum_{n\leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha})$, if $\alpha \geq 0$.

Proof:

For part (a):

By Euler's summation formula,

$$\sum_{y<n\leq x} f(n) = \int_y^x f(t)dt + \int_y^x (t-[t])f'(t)dt + f(x)\{[x]-x\} - f(y)\{[y]-y\}$$

$$we\ take\ f(t) = \frac{1}{t}\ with\ y = 1\ and$$

$$f'(t) = -\frac{1}{t^2}\ in\ the\ above\ formula,$$

$$\sum_{1<n\leq x}\frac{1}{n} = \int_1^x \frac{1}{t}dt + \int_1^x \{t-[t]\}\left(-\frac{1}{t^2}\right)dt + \frac{1}{x}\{[x]-x\} - f(1)(1-1)$$

$$\sum_{1<n\leq x}\frac{1}{n} = \int_1^x \frac{1}{t}dt - \int_1^\infty \{t-[t]\}\frac{1}{t^2}dt + \int_x^\infty \{t-[t]\}\frac{1}{t^2}dt + O\left(\frac{1}{x}\right)$$

$$(Adding\ 1\ on\ both\ sides\ we\ have)$$

$$\sum_{n\leq x}\frac{1}{n} = \log x + 1 - \int_1^\infty \{t-[t]\}\frac{1}{t^2}dt + \int_x^\infty \{t-[t]\}\frac{1}{t^2}dt + O\left(\frac{1}{x}\right)$$

$$= \log x + A + \int_x^\infty \{t-[t]\}\frac{1}{t^2}dt + O\left(\frac{1}{x}\right) \qquad \rightarrow (1)$$

$$where\ A = 1 + \int_1^\infty \{t-[t]\}\frac{1}{t^2}dt$$

$$consider\ \int_x^\infty \{t-[t]\}\frac{1}{t^2}dt = \int_x^\infty O\left(\frac{1}{t^2}\right)dt = O\left(\frac{1}{x}\right)$$

$$equation\ (1), becomes$$

Notes

$$\sum_{n\le x}\frac{1}{n}=\log x+A+O\left(\frac{1}{x}\right)+O\left(\frac{1}{x}\right)$$

$$\sum_{n\le x}\frac{1}{n}-\log x=A+O\left(\frac{1}{x}\right)$$

$$\lim_{n\to\infty}\left\{\sum_{n\le x}\frac{1}{n}-\log x\right\}=\lim_{n\to\infty}\left\{A+O\left(\frac{1}{x}\right)\right\}$$

$$C=A+0$$

$$\therefore\sum_{n\le x}\frac{1}{n}=\log x+C+O\left(\frac{1}{x}\right)$$

Where C is Euler's constant.

To prove part (b)

By Euler's summation formula,

$$\sum_{y<n\le x}f(n)=\int_y^x f(t)dt+\int_y^x(t-[t])f'(t)dt+f(x)\{[x]-x\}-f(y)\{[y]-y\}$$

We take $f(t)=\frac{1}{t^s}$ with $y=1$ and $f'(t)=\frac{-s}{t^{s+1}}$ in Euler's summation formula,

$$\sum_{1<n\le x}\frac{1}{n^s}=\int_1^x\frac{1}{t^s}dt+\int_1^x\{t-[t]\}\left(\frac{-s}{t^{s+1}}\right)dt+\{[x]-x\}\frac{1}{x^s}-f(1)(1-1)$$

$$\sum_{1<n\le x}\frac{1}{n^s}=\int_1^x\frac{1}{t^s}dt-\int_1^\infty\{t-[t]\}\left(\frac{-s}{t^{s+1}}\right)dt+\int_x^\infty\{t-[t]\}\left(\frac{-s}{t^{s+1}}\right)dt+O\left(\frac{1}{x^s}\right)$$

$(Adding\ 1\ on\ both\ sides\ we\ have)$

$$\sum_{n\le x}\frac{1}{n^s}=\frac{x^{1-s}}{1-s}+A(s)+\int_x^\infty\{t-[t]\}\left(\frac{s}{t^{s+1}}\right)dt+O(x^{-s})\quad\to(2)$$

$$where\ A(s)=1-\frac{1}{1-s}-\int_1^\infty\{t-[t]\}\left(\frac{s}{t^{s+1}}\right)dt$$

Notes

$$consider \int_x^\infty \{t-[t]\}\left(\frac{s}{t^{s+1}}\right)dt = O(x^{-s})$$

(2) *becomes,*

$$\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + A(s) + O(x^{-s})$$

Case (i): If s > 1,

$$\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + A(s) + O(x^{-s})$$

$$\lim_{x\to\infty}\sum_{n\le x}\frac{1}{n^s} = \lim_{x\to\infty}\left\{\frac{x^{1-s}}{1-s} + A(s) + O(x^{-s})\right\}$$

$$\sum_{n=1}^{\infty}\frac{1}{n^s} = A(s)$$

$$\zeta(s) = A(s)$$

Case (ii): If 0 < s < 1,

$$\sum_{n\le x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s} = A(s) + O(x^{-s})$$

$$\lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right) = \lim_{x\to\infty}(A(s) + O(x^{-s}))$$

$$\zeta(s) = A(s)$$

$$\therefore \sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s}) \quad if\ s > 0\,, s\ \neq 1.$$

To prove (c):

We use (b) with s > 1 to obtain

$$\sum_{n>x}\frac{1}{n^s} = \zeta(s) - \sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{s-1} + O(x^{-s}) = O(x^{1-s})$$

Since $x^{-s} \le x^{1-s}$.

To prove (d):

We take $f(t) = t^{\alpha}$ in Euler's summation formula with $y = 1$ and $f'(t) = \alpha t^{\alpha-1}$

Notes

$$\sum_{1<n\leq x} n^{\alpha}$$

$$= \int_1^x t^{\alpha} dt + \int_1^x \{t-[t]\}(\alpha t^{\alpha-1})dt + x^{\alpha}\{[x]-x\} - f(1)(1 - 1)$$

$$\sum_{1<n\leq x} n^{\alpha} = \left(\frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1}\right) + \alpha\int_1^x \{t-[t]\}t^{\alpha-1}dt + O(x^{\alpha})$$

$$consider \int_1^x \{t-[t]\}\alpha t^{\alpha-1}dt = O(x^{\alpha})$$

$$(Adding\ 1\ on\ both\ sides\ we\ get)$$

$$\sum_{n\leq x} n^{\alpha} = \frac{x^{\alpha+1}}{\alpha+1} + 1 - \frac{1}{\alpha+1} + O(x^{\alpha}) + O(x^{\alpha})$$

$$= \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha}) + O(x^{\alpha}) + O(x^{\alpha})$$

$$= \frac{x^{\alpha+1}}{\alpha+1} + O(x^{\alpha})$$

9.5 The average order of d(n):

Definition 9.1.4:

If $\lim_{x\to\infty}\frac{f(x)}{g(x)} = 1$, then $f(x)$ is said to be asymptotic to $g(x)\ as\ x \to \infty$. It is written by $f(x) \sim g(x)\ as\ \ x \to \infty$.

Definition 9.1.5:

A Lattice point is a point with integer coefficients.

Theorem 9.3: For all $x \geq 1$ we have

(i) $\sum_{n\leq x} d(n) = x\log x + O(x)$

(ii) $\sum_{n\leq x} d(n) = x\log x + (2\zeta - 1)x + O(\sqrt{x})$,

Where ζ is Euler's constant and hence the average order of d(n) is $\log n$

Proof:

$$(i)\sigma_0(n) = number\ of\ divisors\ of\ n = \sum_{d/n} 1 = d(n)$$

Notes

$$\sum_{n\leq x} d(n) = \sum_{n\leq x}\sum_{d/n} 1 = \sum_{\substack{q,d\\ qd\leq x}} 1 \quad \rightarrow (1)$$

$(since\ \frac{d}{n} \Rightarrow n = qd\ where\ q \in Z)$

$qd = n$ represents the rectangular hyperbola in the (q, d) plane .

The sum in (1) is actually the number of lattice points on the rectangular hyperpola $qd \leq x, 1 \leq q \leq \frac{x}{d}$.

For a fixed d, the sum is same as the number of lattice points in the rectangular hyperbola, then sum over all d $\leq x, we\ have,$

$$\therefore \sum_{n\leq x} d(n) = \sum_{d\leq x}\sum_{q\leq\frac{x}{d}} 1 = \sum_{d\leq x}\left(\frac{x}{d} + O(1)\right)$$

(by using theorem 9.2 with α=0)

$$= x\left(\log x + \zeta + O\left(\frac{1}{x}\right)\right) + O\big(x + O(1)\big)$$

$$= xlog\ x + \zeta x + O(1) + O(x) + O(1)$$

$$= xlog\ x + \ O(x) + O(x) + O(1)$$

$$= xlog\ x + \ O(x)$$

Taking limit and divided $xlog\ x$ on both side we get,

$$\lim_{x\to\infty}\left(\frac{\sum_{n\leq x}\frac{d(n)}{x}}{\log x}\right) = \lim_{x\to\infty}\left(1 + O\left(\frac{1}{\log x}\right)\right) = 1$$

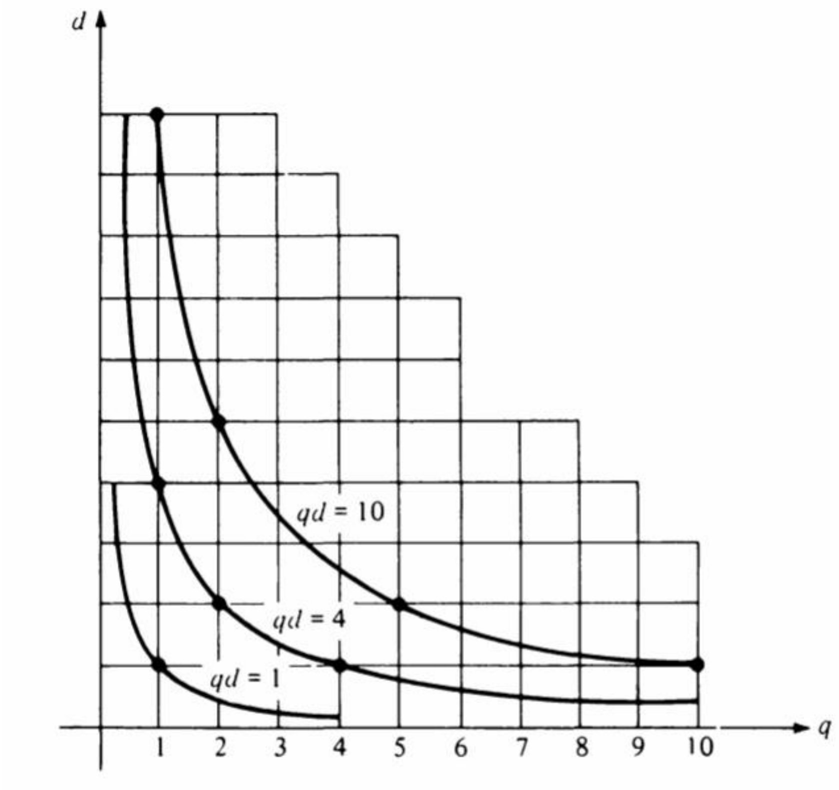
$$\therefore \sum_{n\leq x}\frac{d(n)}{x} \sim \log x$$

$$\sum_{k\leq x}\frac{d(k)}{x} \sim \log x$$

Hence the average order of $d(n)$ is $\log n$

$$(ii) \sum_{n\leq x} d(n) = \sum_{n\leq x}\sum_{d/n} 1 = \sum_{\substack{q,d\\ qd\leq x}} 1 \qquad\qquad \rightarrow (2)$$

Notes



The sum (2) is equivalent to the number of lattice points in the region bounded by $qd = x$, $q = 1$ and $d = 1$.

The total number of lattice points in the region is equal to the number below the line $q = d$ plus the number on the bisecting line segment.

$$\therefore \sum_{n \le x} d(n) = \sum_{d \le \sqrt{x}} 2\left(\left(\frac{x}{d}\right) - d\right) + \left(\sqrt{x}\right)$$

$$= \sum_{d \le \sqrt{x}} 2\left\{\left(\frac{x}{d}\right) - O(1) - d\right\} + \left(\sqrt{x}\right)$$

$$= \left\{2x \sum_{d \le \sqrt{x}} \frac{1}{d} - 2O(1) - 2\sum_{d \le \sqrt{x}} d\right\} + \left(\sqrt{x}\right)$$

$$= 2x\left\{\log\sqrt{x} + c + O\left(\frac{1}{\sqrt{x}}\right) + O(1) - 2\left(\frac{\left(\sqrt{x}\right)^2}{2} + O(\sqrt{x})\right)\right\} + (\sqrt{x})$$

$$= x\log x + 2cx + O\left(\sqrt{x}\right) + O(1) - x + O(1) + \left(\sqrt{x}\right)$$

$$= x\log x + (2c - 1)x + O(\sqrt{x}\,)$$

$$\therefore \sum_{n \le x} d(n) = x\log x + (2c - 1)x + O(\sqrt{x})$$

Notes

$$further, \qquad \frac{\sum_{n\le x} d(n)}{x\log x} = 1 + \frac{(2c-1)x}{x\log x} + O\left(\frac{\sqrt{x}}{x\log x}\right)$$

$$= 1 + \frac{(2c-1)}{\log x} + O\left(\frac{1}{\sqrt{x}\log x}\right)$$

$$\frac{\sum_{n\le x} d(n)}{x} \cong \log x \qquad as\ x \to \infty$$

$$\sum_{k\le n} \frac{d(k)}{n} \cong \log n \qquad as\ n \to \infty$$

∴ Average order of $d(n)$is $\cong \log n$.

9.6 The average order of the divisor functions $\sigma_\alpha(n)$:

Theorem 9.4:

For all $x \ge 1$ then we have $\sum_{n\le x} \sigma_1(n) = \frac{1}{2}\zeta(2)x^2 + O(xlog\ x)$ and hence the average order of $\sigma_1(n)$ is $\left(\frac{\pi^2 n}{12}\right)$

Proof:

$$\sigma_1(n) = The\ sum\ of\ dividors\ of\ n = \sum_{d/n} d$$

$$\sum_{n\le x} \sigma_1(n) = \sum_{n\le x}\sum_{d/n} d$$

$$= \sum_{n\le x}\sum_{q/n} q = \sum_{\substack{q,d \\ qd\le x}} q$$

$$\left(since\ {}^{q}/_{n} \Rightarrow n = qd\right)$$

$$= \sum_{d\le x}\left(\sum_{q\le \frac{x}{d}} q\right)$$

$$= \sum_{d\le x}\left\{\frac{\left(\frac{x}{d}\right)^2}{2} + O\left(\frac{x}{d}\right)\right\}$$

$$= \frac{x^2}{2}\sum_{d\le x}\frac{1}{d^2} + O\left\{x\sum_{d\le x}\frac{1}{d}\right\}$$

$$= \frac{x^2}{2}\left\{\frac{x^{1-2}}{1-2} + \zeta(2) + O(x^{-2})\right\} + O\left\{x\left(\log x + \zeta + O\left(\frac{1}{x}\right)\right)\right\}$$

$$= \frac{\zeta(2)x^2}{2} - \frac{x}{2} + O\left(\frac{1}{2}\right) + O(xlog\ x) + O(cx) + O(1)$$

$$= \frac{\zeta(2)x^2}{2} + O(xlog\ x) + O(xlog\ x) + O(xlog\ x) + O(xlog\ x)$$

$$= \frac{\zeta(2)x^2}{2} + O(xlog\ x)$$

We know that $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ $, if\ s > 1$

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{1}{1^2} + \frac{1}{2^2} + \cdots = \frac{\pi^2}{6}$$

(by Fourier series)

$$\sum_{n \le x} \sigma_1(n) = \frac{\pi^2 x^2}{12} + O(xlog\ x)$$

$$\lim_{n \to \infty} \left(\frac{\sum_{n \le x} \frac{\sigma_{1(n)}}{x}}{\frac{\pi^2 x}{12}} \right) = 1 + 0$$

$$\lim_{n \to \infty} \sum_{n \le x} \frac{\sigma_1(n)}{x} \cong \frac{\pi^2 x}{12}$$

$$\sum_{k \le n} \frac{\sigma_1(k)}{n} \cong \frac{\pi^2 x}{12} \quad as\ n \to \infty$$

$\therefore$ Average order of $\sigma_1(n)$ is $\frac{\pi^2 n}{12}$ as $n \to \infty$

Theorem 9.5:

If $\alpha > 0, \alpha \ne 1$ and $x \ge 1$ then we have $\sum_{n \le x} \sigma_\alpha(n) = \frac{\zeta(\alpha+1)}{\alpha+1} x^{\alpha+1} + O(x^\beta)$

Where $\beta = \max\{1, \alpha\}$

Proof:

$$\sigma_\alpha(n) = \sum_{d/n} d^\alpha = \sum_{q/n} q^\alpha$$

$$\sum_{n \le x} \sigma_\alpha(n) = \sum_{n \le x} \sum_{q/n} q^\alpha = \sum_{\substack{q,d \\ qd \le x}} q^\alpha$$

Notes

$$= \sum_{d \le x} \left(\sum_{q \le \frac{x}{d}} q^{\alpha} \right)$$

$$= \sum_{d \le x} \left[\left(\frac{\left(\frac{x}{d}\right)^{\alpha+1}}{\alpha+1} \right) + O\left(\left(\frac{x}{d}\right)^{\alpha} \right) \right]$$

$$= \frac{x^{\alpha+1}}{\alpha+1} \sum_{d \le x} \frac{1}{d^{\alpha+1}} + O\left(x^{\alpha} \sum_{d \le x} \frac{1}{d^{\alpha}} \right)$$

$$= \frac{x^{\alpha+1}}{\alpha+1} \left[\frac{x^{1-(\alpha+1)}}{-\alpha} + \zeta(\alpha+1) + O(x^{-\alpha-1}) \right]$$

$$+ O\left[\left(x^{\alpha} \left(\frac{x^{1-\alpha}}{\alpha} + \zeta(\alpha) + O(x^{-\alpha}) \right) \right) \right]$$

$$= \frac{\zeta(\alpha+1)x^{\alpha+1}}{\alpha+1} - \left(\frac{x}{\alpha(\alpha+1)} \right) + O\left(\frac{1}{\alpha+1} \right) + O\left(\frac{x}{1-\alpha} \right) + O(x^{\alpha}\zeta(\alpha))$$
$$+ O(1)$$

$$= \frac{x^{\alpha+1}\zeta(\alpha+1)}{\alpha+1} + O(x) + O(x) + O(x) + O(x^{\alpha})$$

$$\sum_{n \le x} \sigma_{\alpha}(n) = \frac{x^{\alpha+1}\zeta\,(\alpha+1)}{\alpha+1} + O(x) + O(x^{\alpha})$$

If $\quad 0 < \alpha < 1,\; x^{\alpha} \le x$

If $\quad x \ge 1,\; \alpha > 1,\; x \le x^{\alpha}$

$$\therefore \sum_{n \le x} \sigma_{\alpha}(n) = \frac{x^{\alpha+1}\zeta(\alpha+1)}{\alpha+1} + O(x^{\beta})$$

$$where\ \beta = \max\{1, \alpha\}.$$

Theorem 9.6:

$$If\ \beta > 0\ let\ \delta = \max\{0, 1-\beta\}.\ Then\ if\ x > 1\ we\ have$$

$$\sum_{n \le x} \sigma_{-\beta}(n) = \zeta(\beta+1)x + O\left(x^{\delta}\right) \qquad if\ \beta \ne 1,$$

$$= \zeta(2)x + O(\log x) \qquad if \beta = 1.$$

Proof:

We have

Notes

$$\sum_{n\le x}\sigma_{-\beta}(n)=\sum_{n\le x}\sum_{d/n}\frac{1}{d^{\beta}}=\sum_{d\le x}\frac{1}{d^{\beta}}\sum_{q\le x/d}1$$

$$=\sum_{d\le x}\frac{1}{d^{\beta}}\left\{\frac{x}{d}+O(1)\right\}=x\sum_{d\le x}\frac{1}{d^{\beta+1}}+O\left(\sum_{d\le x}\frac{1}{d^{\beta}}\right).$$

The last term is $O(\log x)$if $\beta=1$ and $O(x^{\delta})$if $\beta\neq 1$. Since

$$x\sum_{d\le x}\frac{1}{d^{\beta+1}}=\frac{x^{1-\beta}}{-\beta}+\zeta(\beta+1)x+O\left(x^{-\beta}\right)=\zeta(\beta+1)x+O\left(x^{1-\beta}\right)$$

This completes the proof.

9.7 Exercises:

(1) $If\ x\ge 1\ prove\ that$:

(a) $\sum_{n\le x}\varphi(n)=\frac{1}{2}\sum_{n\le x}\mu(n)\left[\frac{x}{n}\right]^{2}+\frac{1}{2}$

(b) $\sum_{n\le x}\frac{\varphi(n)}{n}=\sum_{n\le x}\frac{\mu(n)}{n}\left[\frac{x}{n}\right]$

(2) If $\sum_{n=1}^{\infty}\mu(n)n^{-\alpha}={}^{1}/_{\zeta(\alpha)}$ if $\alpha>1$, $Assuming\ this, prove\ that\ for\ x \ge 2\ and\ \alpha>1,$

$$\alpha\neq 2, we\ have\ \sum_{n\le x}\frac{\varphi(n)}{n^{\alpha}}=\frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)}+\frac{\zeta(\alpha-1)}{\zeta(\alpha)}+O(x^{1-\alpha}\log x)$$

(3) If $\alpha\le 1$ and $x\ge 2$ prove that $\sum_{n\le x}\frac{\varphi(n)}{n^{\alpha}}=\frac{x^{2-\alpha}}{2-\alpha}\frac{1}{\zeta(2)}+O(x^{1-\alpha}\log x)$

UNIT – X: LATTICE POINTS

Notes

Struture

10.1 Introduction:

This unit initiates the concepts of average order of Euler totient function and it introduces the notion of lattice points and its application towards the distribution of lattice points visible from the origin , further it describes the partial sums of a Dirichlet product and it provides brief demonstration on Legendre's identity and Mangoldt function.

10.2 Objectives:

The students will be able to

- Identify the average order of Eulers totient function
- Describes the partial sums of a Dirichlet product
- Determine the identity of Mangoldt function

10.3 The Average order of $\boldsymbol{\varphi(n)}$:

Theorem:10.1 For x >1, we have $\sum_{n\leq x}\varphi(n)=\frac{3}{\pi^2}x^2+O(x\log x)$, so the average order of $\varphi(n)$is $\frac{3n}{\pi^2}$.

Proof: The method is similar to that used for the divisor functions.

To prove this theorem we need the following lemma.

Lemma: Let f and g be the arithmetical functions and $F(s)=\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$ and $G(s)=\sum_{n=1}^{\infty}\frac{g(n)}{n^s}$ then $F(s)G(s)=\sum_{n=1}^{\infty}\frac{h(n)}{n^s}$ where $h=f*g$

Proof: $F(s)G(s)=\left(\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\right)\left(\sum_{n=1}^{\infty}\frac{g(n)}{n^s}\right)$

$$=\left(\frac{f(1)}{1^s}+\frac{f(2)}{2^s}+\cdots\right)\left(\frac{g(1)}{1^s}+\frac{g(2)}{2^s}+\cdots\right)$$

Notes

$$= \frac{1}{1^s}(f(1)g(1)) + \frac{1}{2^s}\big(f(2)g(1)\ f(1)g(2)\big) + \cdots$$

$$= \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d/n} f(d)g(\frac{n}{d})$$

$$= \sum_{n=1}^{\infty} \frac{1}{n^s}(f * g)(n)$$

$$= \sum_{n=1}^{\infty} \frac{1}{n^s} h(n)$$

Hence the Lemma.

Take $f(n) = \mu(n)\ and\ g(n) = u(n)$ in the above lemma Therefore

$$F(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\ and\ G(s) = \sum_{n=1}^{\infty} \frac{u(n)}{n^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} = C(s)\ \ if\ s > 1$$

$$h(n) = (\mu * u)n)) = I(n) = \begin{cases} 1\ if\ n = 1 \\ 0\ if\ n > 1 \end{cases}$$

we know that, $F(s)G(s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}$

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \zeta(s) = \sum_{n=1}^{\infty} \frac{I(n)}{n^s} = 1$$

If s=2 ,$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} \zeta(2) = 1$

$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)}$where ζ (2)=$\frac{\pi^2}{6}$

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}$$

$$\sum_{n \le x} \frac{\mu(n)}{n^2} + \sum_{n > x} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}$$

$$\sum_{n \le x} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} - \sum_{n > x} \frac{\mu(n)}{n^2}$$

$$= \frac{6}{\pi^2} - 0\left(\sum_{n > x} \frac{\mu(n)}{n^2}\right)$$

$$= \frac{6}{\pi^2} - 0\left(0\left(\frac{1}{x}\right)\right)$$

$$= \frac{6}{\pi^2} - O(\frac{1}{x}) \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

We know that $\varphi(n) = \sum_{d/n} \mu(d)\frac{n}{d}$

Notes

$$\sum_{n\le x}\varphi(n)=\sum_{n\le x}\left(\sum_{d/n}\mu(d)\frac{n}{d}\right)$$

$$\sum_{n\le x}\varphi(n)=\sum_{q\le\frac{x}{d}}\left(\sum_{d/n}\mu(d)q\right)$$

$$=\sum_{d\le x}\mu(d)\left(\sum_{q\le\frac{x}{d}}q\right)$$

$$=\sum_{d\le x}\mu(d)\left(\frac{\left(\frac{x}{d}\right)^2}{2}+O\left(\frac{x}{d}\right)\right)$$

$$=\frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2}+O\left(x\sum_{d\le x}\frac{\mu(d)}{d}\right)$$

$$=\frac{x^2}{2}\left(\frac{6}{\pi^2}-O(\frac{1}{x})\right)+O\left(x\sum_{d\le x}\frac{1}{d}\right)$$

$$=\frac{3x^2}{\pi^2}-O\left(\frac{x}{2}\right)+O\left(x\left(\log x+\ C+O\left(\frac{1}{x}\right)\right)\right)$$

$$=\frac{3x^2}{\pi^2}+O(x\ logx)+O(x\ logx)+O(xlogx)$$

$$\sum_{n\le x}\varphi(n)=\frac{3x^2}{\pi^2}+O(x\ logx)$$

$$\lim_{n\to\infty}\left(\frac{\sum_{n\le x}\frac{\varphi(n)}{x}}{\frac{3x}{\pi^2}}\right)=\lim_{n\to\infty}\left(1+O\left(\frac{\pi^2\log x}{3x}\right)\right)$$

$$\sum_{n\le x}\frac{\varphi(n)}{x}\sim\frac{3x}{\pi^2}$$

Hence the average of $\varphi(n)=\frac{3n}{\pi^2}$

10.4 An application to the distribution of lattice points visible from the origin:

The asymptotic formula for the partial sums of $\varphi(n)$ has an interesting application to a theorem concerning the distribution of lattice points in the plane which are visible from the origin.

Definition 10.1.1 : Two lattice points P and Q are said to be mutually visible if the line segment which joins them contains no lattice points other than the end points P and Q.

Theorem 10.3 : Two lattice points (a,b) and (m,n) are mutually visible if, and only if, a-m and b-n are relatively prime.

Proof: It is clear that (a, b) and (m, n) are mutually visible iff (a-m, b-n) are mutually visible from the origin. Hence it sufficies to prove the theorem when (m. n)=(0, 0).

Assume that (a, b) is visible from the origin, and let d=(a, b). we wish to prove that d=1. If d$>$ 1 then a=da^I, b=db^I and the lattice points (a^I, b^I) is on the line segment joining (0, 0) to (a, b).This contradicts the proof that d=1.

Conversely, assume that (a,b)=1. If a lattice point (a^I, b^I) is on the line segment joining (0, 0) to (a, b) we have

$$a^I = ta, \qquad b^I = tb, \quad where\ 0 < t < 1.$$

Hence t is rational, so $t = \frac{r}{s}$ where r, s are positive integers with (r, s)=1. Thus $\qquad sa^I = ar \qquad and \qquad sb^I = br,$

So $s/ar, s/br$. But (s, r)=1 so, s/a and s/b. Hence s=1 since (a,b) =1. This contradicts the inequality $0 < t < 1$. Therefore the lattice point (a, b) is visible from the origin.

There are infinitely many lattice points visible from the origin and it is natural to ask how they are distributed in the plane.

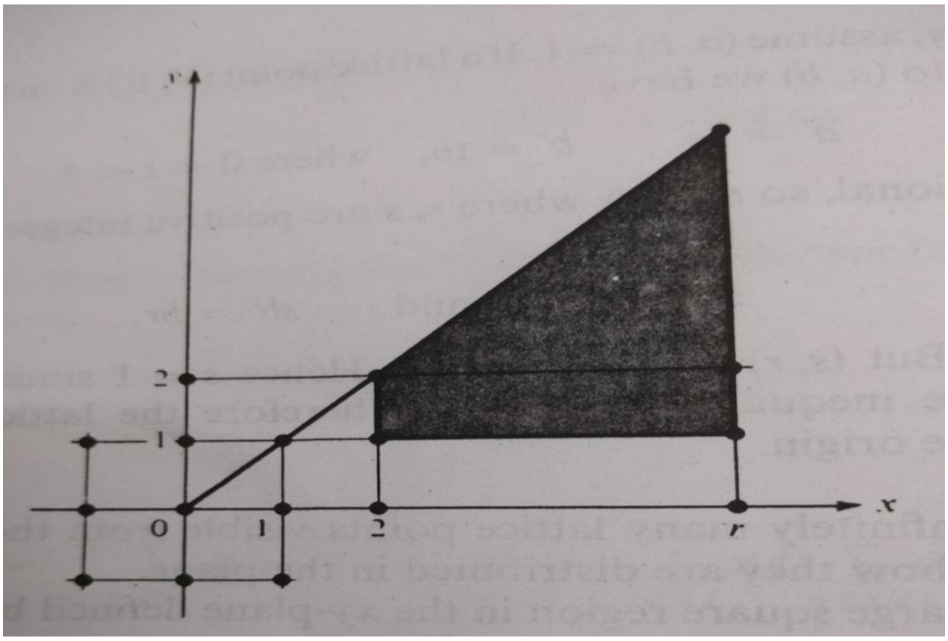
Consider a large square region in the xy-plane defined by the inequalities

$|x| \leq r, \quad |y| \leq r$. Let N(r) denote the number of lattice points in this square, and let N(r) denote the number of lattice points in this square, and let $N^I(r)$ denote the number which are visible from the origin. The quotient $N^I(r)/$N(r) measures the fraction of those lattice points in the square which are visible from the origin.

Theorem:10.4 The set of lattice points visible from the origin has density ${}^{6}/_{\pi^2}$

Proof : consider the large square region $|x| \leq r\ and\ |y| \leq r$ bounded by the lines $y = \pm r$ is dividing the axes in to 8 symmetrical regions.

Notes



The 8 lattice points are visible from the origin they are (1, 0), (1, 1), (0, 1), (-1, 1), (-1, -1), (0, -1), (-1, 0) and (1, -1). X is bounded by the lines $1 \leq x \leq r$ and y is bounded by $2 \leq y \leq x$.

Let $N'(r)$ denotes the number of lattice points visible from the origin .

$$N'(r) = 8 + 8\left(\sum_{1 \leq x \leq r} \sum_{2 \leq y \leq x} 1\right)$$

$$= 8\left(1 + \sum_{1 \leq x \leq r} \sum_{2 \leq y \leq x} 1\right)$$

$$= 8\left(1 + \sum_{1 \leq n \leq r} \sum_{1 \leq m \leq n} 1\right)$$

$$= 8\left(1 + \sum_{2 \leq n \leq r} \varphi(n)\right)$$

We know that $\sum_{n \leq x} \varphi(n) = \frac{3x^2}{\pi^2} + O(x \, logx)$

$$= 8\left(\frac{3r^2}{\pi^2} + O(r \, logr)\right)$$

$$= \frac{24r^2}{\pi^2} + O(r \, logr)$$

The total number of lattice points in the square region is,

$N(r) = (2[r] + 1)^2$and$[r] = r - \{x\} < r - 1$

$$\therefore N(r) = 4r^2 + O(1)$$

$$\frac{N'(r)}{N(r)} = \frac{\frac{24r^2}{\pi^2} + O(r\, log r)}{4r^2 + O(1)}$$

$$= \frac{6}{\pi^2} + O\left(\frac{\log r}{r}\right)$$

$$\lim_{r\to\infty} \frac{N'(r)}{N(r)} = \lim_{r\to\infty}\left(\frac{6}{\pi^2} + O\left(\frac{\log r}{r}\right)\right)$$

$$= \frac{6}{\pi^2}$$

10.5 The partial sums of a Dirichlet product :

Theorem:10.5 Let f and g be arithmetical functions and let $h = f * g$ and let $F(x) = \sum_{n\le x} f(n)$, $G(x) = \sum_{n\le x} g(n)$ and $H(x) = \sum_{n\le x} h(n)$ then $H(x) = \sum_{n\le x} f(n) G\left(\frac{x}{n}\right)$ also $H(x) = \sum_{n\le x} F\left(\frac{x}{n}\right) g(n)$.

Proof: Define $u(x) = \begin{cases} 1\ if\ x \ge 1 \\ 0\ if\ 0 < x < 1 \end{cases}$

Given $F(x) = \sum_{n\le x} f(n)$

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

$$= (f \circ u)(x)$$

Let $F = f \circ u$ $similarly\ G = g \circ u\ and\ H = h \circ u$

$$f \circ G = f \circ (g \circ u)$$

$$= (f * g) \circ u\ (Associative\ property)$$

$$= h \circ u\ (h = f * g) = H$$

$$H(x) = (f \circ G)(x)$$

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

$$g \circ F = g \circ (f \circ u)$$

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

$$= (f * g) \circ u\ (* \ is\ commutative)$$

$$= h \circ u = H$$

$$H(x) = (g \circ F)(x) = \sum_{n\le x} g(n) f\left(\frac{x}{n}\right)$$

Notes

Hence the theorem proved.

Theorem:10.6 For $x \geq 1$, we have

$$\sum_{n\leq x}\sum_{d/n} f(d) = \sum_{n\leq x} f(n)\left[\frac{x}{n}\right] = \sum_{n\leq x} F\left(\frac{x}{n}\right)$$

Proof: Put g(n)=1 in theorem 10.5,

$$G(x) = \sum_{n\leq x} 1 = [x]$$

$$g(n) = 1 = u(n)(unit\ function)$$

But $h = f * u,\ h(n) = (f * u)(n) = \sum_{d/n} f(d)u\left(\frac{n}{d}\right)$

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

$$\sum_{n\leq x}\sum_{d/n} f(d) = \sum_{n\leq x} h(n) = H(x)$$

$$H(x) = \sum_{n\leq x} f(n)G\left(\frac{x}{n}\right)$$

$$\therefore \sum_{n\leq x}\sum_{d/n} f(d) = \sum_{n\leq x} f(n)G\left(\frac{x}{n}\right)$$

10.6 Applications to $\boldsymbol{\mu(n)}$ *and* $\boldsymbol{\lambda(n)}$:

Theorem: 10.7

For $x \geq 1$,we have (i) $\sum_{n\leq x} \mu(n)\left[\frac{x}{n}\right] = 1$

(ii) $\sum_{n\leq x} \Lambda(n)\left[\frac{x}{n}\right] = \log[x]\,!$

Proof: (i) put $f(n) = \mu(n)$ in theorem 10.6, we have

$$\sum_{n\leq x} \mu(n)\left[\frac{x}{n}\right] = \sum_{n\leq x}\sum_{d/n} \mu(d)$$

$$= \sum_{n\leq x}\left[\frac{1}{n}\right]$$

$$= \sum_{n\leq x} I(n) = 1$$

(ii) Put f(n) = Λ (n) in theorem 10.6, we have

$$\sum_{n\leq x} \Lambda(n)\left[\frac{x}{n}\right] = \sum_{n\leq x}\sum_{d/n} \Lambda(d)$$

$$= \sum_{n \le x} \log n$$

$$= log1 + log2 + \cdots logx$$

$$= \log(1.2 \ldots \ldots x)$$

$$= \log([x]!)$$

Note: The sums in this theorem can be regarded as the weighted average of the functions $\mu(n)$ and $\Lambda(n)$

Theorem: 10.8 For all $x \ge 1$, we have $\left|\sum_{n \le x} \frac{\mu(n)}{n}\right| \le 1$, with equality holding only if $x < 2$.

Proof: If $x < 2$ By previous theorem,

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

$$1 = \sum_{n \le x} \mu(n) \left(\frac{x}{n} - \left\{\frac{x}{n}\right\}\right)$$

$$= x \sum_{n \le x} \frac{\mu(n)}{n} - \sum_{n \le x} \mu(n) \left\{\frac{x}{n}\right\}$$

$$x \sum_{n \le x} \frac{\mu(n)}{n} = 1 + \sum_{n \le x} \mu(n) \left\{\frac{x}{n}\right\}$$

$$\left|x \sum_{n \le x} \frac{\mu(n)}{n}\right| = \left|1 + \sum_{n \le x} \mu(n) \left\{\frac{x}{n}\right\}\right|$$

$$\le 1 + \left|\sum_{n \le x} \mu(n) \left\{\frac{x}{n}\right\}\right|$$

$$\le 1 + \sum_{n \le x} \left\{\frac{x}{n}\right\}$$

$$= 1 + \{x\} + \sum_{2 \le n \le x} \left\{\frac{x}{n}\right\}$$

$$\le 1 + \{x\} + \sum_{2 \le n \le x} 1$$

$$= 1 + \{x\} + [x] - 1$$

$$= x$$

$$\therefore \left|\sum_{n \le x} \frac{\mu(n)}{n}\right| \le 1$$

Notes

Theorem: 10.9 Legendre's identity

For $x \geq 1, we\ have\ [x]! = \prod_{p \leq x} p^{\alpha(p)}$ where the product is extended over all primes $\leq x$, and $\alpha(p) = \sum_{m=1}^{\infty} \left[\frac{x}{p^m}\right]$

Proof: We know that $\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] = \log[x]\,!$

$$\text{Put } n = p^m \log([x]!) = \sum_{p^m \leq x} \Lambda(p^m) \left[\frac{x}{p^m}\right]$$

$$= \sum_{p \leq x} \log p \sum_{n=1}^{\infty} \left[\frac{x}{p^m}\right]$$

$$= \sum_{p \leq x} \log p\ \alpha(p)$$

$$\text{Where, } \alpha(p) = \sum_{m=1}^{\infty} \left[\frac{x}{p^m}\right]$$

$$= \sum_{p \leq x} \log p^{\alpha(p)}$$

$$log[x]! = \log(\prod_{p \leq x} p^{\alpha(p)})$$

$$[x]! = \prod_{p \leq x} p^{\alpha(p)}$$

Hence the theorem proved.

Theorem: 10.10

For $x \geq 2, we\ have\ log[x]! = xlogx - x + O(logx)\ \ we\ have,$

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] = xlogx - x + O(logx)$$

Proof: Put f(t)=log(t) in Euler summation formula with y=1

$$\sum_{1<n \leq x} f(n) = \int_1^x \log t\ dt + \int_1^x (t - [t]) \frac{1}{t} dt + logx([x] - x) - 0$$

$$= xlogx - x + 1 + O\left(\int_1^x \frac{1}{t} dt\right) + O(\log x)$$

Adding 1 on both sides we get,

$$\sum_{n \leq x} \log n = xlogx - x + 2 + O(\log x) + O(\log x)$$

.

$$= xlog\ x - x + O(\log x) \ldots\ldots\ldots\ldots\ldots(1)$$

$$since, \sum_{n\leq x} \log n = \log[x]!$$

(1)becomes, $\log([x]!) = xlog\ x - x + O(\log x)$

$$wkt, \quad \sum_{n\leq x} \Lambda(n)\left[\frac{x}{n}\right] = \log[x]\,!$$

$$Therefore, \quad \sum_{n\leq x} \Lambda(n)\left[\frac{x}{n}\right] = xlogx - x + O(logx)$$

Hence the theorem proved.

Theorem:10.11 For $x \geq 2$, we have $\sum_{n\leq x} \Lambda(p)\left[\frac{x}{p}\right] = xlogx + O(x)$

Proof: WKT, $\sum_{n\leq x} \Lambda(n)\left[\frac{x}{n}\right] = \log[x]\,!$

$$\log[x]\,! = \sum_{p^m\leq x} \Lambda(p^m)\left[\frac{x}{p^m}\right]$$

$$= \sum_{p^m\leq x} \sum_{m=1}^{\infty} \Lambda(p^m)\left[\frac{x}{p^m}\right]$$

$$= \sum_{p\leq x} \Lambda(p)\left[\frac{x}{p}\right] + \sum_{p\leq x} \sum_{m=2}^{\infty} log(p)\left[\frac{x}{p^m}\right]$$

$$\sum_{p\leq x} \Lambda(p)\left[\frac{x}{p}\right] = \log[x]\,! - \sum_{p\leq x} \sum_{m=2}^{\infty} log(p)\left[\frac{x}{p^m}\right]$$

$$\leq log[x]! - \sum_{p\leq x} logp \sum_{m=2}^{\infty} \left[\frac{x}{p^m}\right]$$

$$= log[x]! - x\sum_{p\leq x} logp \sum_{m=2}^{\infty} \left[\frac{1}{p^m}\right]$$

$$= log[x]! - x\sum_{p\leq x} logp \left[\frac{1}{p^2} + \frac{1}{p^3} \ldots\right]$$

$$= log[x]! - x\sum_{p\leq x} \log p\ \frac{1}{p^2}\left[1 + \frac{1}{p} + \cdots\right]$$

$$= log[x]! - x\sum_{p\leq x} \log p\ \frac{1}{p^2}\left[\frac{1}{1-\frac{1}{p}}\right]$$

$$= log[x]! - x\sum_{p\leq x} \log p\ \frac{1}{p^2}\left[\frac{p^2}{p-1}\right]$$

Notes

$$= log[x]! - x\sum_{p\le x}\log p\ \frac{1}{p^2}\left[\frac{1}{p-1}\right]$$

$$= log[x]! - O(x)$$

We know that, $\log[x]! = xlog\ x - x + O(\log x)$

$$= xlog\ x - x + O(\log x) - O(x) = xlog\ x + O(x)$$

$$\therefore \sum_{n\le x}\Lambda(p)\left[\frac{x}{p}\right] = xlogx + O(x)$$

Hence the theorem proved.

Theorem:10.12 If a and b are the real numbers such that $ab = x$ then

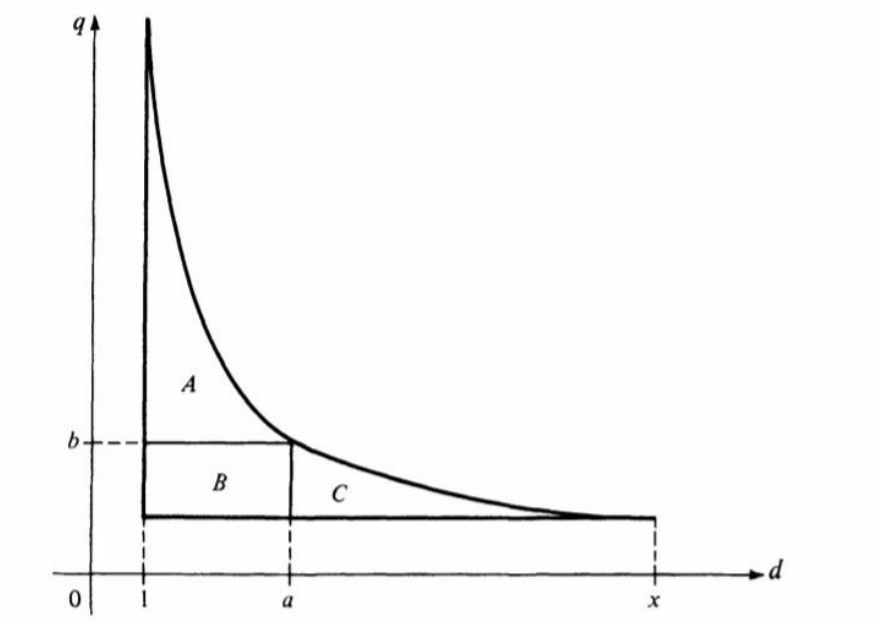
$$\sum_{\substack{q,d\\ qd\le x}} f(d)g(q) = \sum_{n\le a} f(n)G\left(\frac{x}{n}\right) + \sum_{n\le b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b)$$

Proof: Let $F(x) = \sum_{n\le x} f(n),\ G(x) = \sum_{n\le x} g(n)$ and

$H(x) = \sum_{n\le x} h(x)$where$h = f * g$ and f, g are arithmetic functions.

$$H(x) = \sum_{n\le x}(f * g)(n)$$

$$= \sum_{n\le x}\sum_{d/n} f(d)g\left(\frac{n}{d}\right)$$



$$= \sum_{\substack{q,d \\ qd \leq x}} f(d)g(q) \ldots\ldots\ldots..(1)$$

Since a and b are positive real numbers such that ab=x then (a, b) is a point on the rectangular hyperbola qd=x

Notes

The sum H(x) in (1) is extended over lattice points in the first quadrant of (q, d) plane, below the rectangular hyperbola between the two lines d=1, q=1.

Since the point (a, b) splits the region in to three parts A, B and C.

Now the sum in the region $A \cup B$ is,

$$\sum_{\substack{q,d \\ qd \leq x}} f(d)g(q) = \sum_{d \leq a} \sum_{q \leq \frac{x}{d}} f(d)g\left(\frac{x}{d}\right)$$

$$= \sum_{d \leq a} f(d) \sum_{q \leq \frac{x}{d}} g\left(\frac{x}{d}\right)$$

$$= \sum_{d \leq a} f(d)G\left(\frac{x}{d}\right)$$

$$= \sum_{n \leq a} f(n)G\left(\frac{x}{n}\right)$$

The sum in the region $B \cup C$ is,

$$\sum_{\substack{q,d \\ qd \leq x}} f(d)g(q) = \sum_{q \leq b} \sum_{d \leq \frac{x}{q}} g(q)f\left(\frac{x}{q}\right)$$

$$= \sum_{q \leq b} g(q)F\left(\frac{x}{q}\right)$$

$$= \sum_{n \leq b} F\left(\frac{x}{n}\right)g(n)$$

The sum in the region B is,

$$\sum_{qd \leq x} f(d)g(q) = \sum_{d \leq a} \sum_{q \leq b} f(d)g(q)$$

$$= \sum_{d \leq a} f(d) \sum_{q \leq b} g(q)$$

$$= F(a)G(b)$$

Thus, $H(x) = \sum_{\substack{q,d \\ qd \leq x}} f(d)g(q)$

= The sum in the region $(A \cup B)$ + The region $(B \cup C)$ – The region B

Notes

$$\sum_{\substack{q,d \\ qd \le x}} f(d)g(q) = \sum_{n \le a} f(n)G\left(\frac{x}{n}\right) + \sum_{n \le b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b)$$

Hence the theorem proved.

10.7 Excercise:

1. Let $\varphi_1(n) = n \sum_{d/n} |\mu(d)|/d$ Prove that φ_1 is multiplicative and that $\varphi_1(n) = n \prod_{p/n}(1 + p^{-1})$
2. Prove that $\varphi_1(n) = \sum_{d^2/n} \mu(d)\sigma\left(\frac{n}{d^2}\right)$ where the sum is over those divisors of n for which d^2/n
3. Prove that $\sum_{n \le x} \varphi_1(n) = \sum_{n \le x} \mu(d)s\left(\frac{x}{d^2}\right)$, where
   $$s(x) = \sum_{k \le x} \sigma(k)$$

UNIT XI: CONGRUENCES

Notes

Structure

11.1 Introduction:

A congruence is nothing more than a statement about divisibility. The theory of congruences was introduced by Carl Friedreich Gauss. Gauss contributed to the basic ideas of congruences and proved several theorems related to this theory. We start by introducing congruences and their properties. We proceed to prove theorems about the residue system in connection with the Euler ϕ-function.

11.2 Objectives:

The students will be able to

- Describe the properties of Congruences
- Determine Euler Fermat theorem
- Identify the reduced residue system

11.3 Definition and basic properties of Congruence:

Definition 11.1.1:

Given integers a, b, m with $m > 0$, we say that a is congruent to b modulo m, we write

$$a \equiv b(mod\ m) \quad ie)\ m/a - b$$

m is called the modulus of the congruence.

Note:

(i)$\mathrm{a} \equiv \mathrm{o}(\mathrm{mod\ m}) \quad \mathrm{iff\ \ m/a}$

(ii)$\mathrm{a} \equiv \mathrm{b}(\mathrm{mod\ m})$ iff $\mathrm{a} - \mathrm{b} \equiv 0(\mathrm{mod\ m})$

(iii)m does not divide $\mathrm{a} - \mathrm{b} \Rightarrow \mathrm{a} \not\equiv \mathrm{b}(\mathrm{mod\ m})$. It is called incongurent

Notes

Examples:

(i)$19 \equiv 7 (\text{mod } 12) \Rightarrow {}^{12}/_{19-7} \Rightarrow {}^{12}/_{12}$

(ii)$3^2 \equiv -1 (\text{mod } 5) \Rightarrow {}^{5}/_{9+1} \Rightarrow {}^{5}/_{10}$

Theorem 11.1:

Congruence is an equivalence relation , That is

(i)$\mathrm{a} \equiv \mathrm{a}(\text{mod m})$ (reflexive)

(ii)$\mathrm{a} \equiv \mathrm{b}(\text{mod m})$ then $\mathrm{b} \equiv \mathrm{a}(\text{mod m})$ (symmetry)

(iii)$\mathrm{a} \equiv \mathrm{b}(\text{mod m})$ and $\mathrm{b} \equiv \mathrm{c}(\text{mod m}) \Rightarrow \mathrm{a} \equiv \mathrm{c}(\text{mod m})$ (transitivity)

Proof:

(i)If $\mathrm{a} \equiv \mathrm{a}(\text{mod m})$

$\mathrm{m}/\mathrm{a} - \mathrm{a} \Rightarrow \mathrm{m}/0$

(ii)If $\mathrm{a} \equiv \mathrm{b}(\text{mod m})$ and $\mathrm{b} \equiv \mathrm{a}(\text{mod m})$

$\mathrm{m}/\mathrm{a} - \mathrm{b}$ then $\mathrm{m}/\mathrm{b} - \mathrm{a}$

(iii)If $\mathrm{a} \equiv \mathrm{b}(\text{mod m}); \mathrm{b} \equiv \mathrm{c}(\text{mod m}) \Rightarrow \mathrm{a} \equiv \mathrm{c}(\text{mod m})$

if $\mathrm{m}/\mathrm{a} - \mathrm{b}$ and $\mathrm{m}/\mathrm{b} - \mathrm{c} \Rightarrow \mathrm{m}/\mathrm{a} - \mathrm{c}$

Theorem 11.2:

If $a \equiv b(mod\ m)$ and $\alpha \equiv \beta(mod\ m)$ then we have

(i)$\mathrm{ax} + \alpha\mathrm{y} \equiv \mathrm{bx} + \beta\mathrm{y}(\text{mod m})$ for all integers x and y

(ii)$\mathrm{a}\alpha \equiv \mathrm{b}\beta(\text{mod m})$

(iii)$\mathrm{a}^{\mathrm{n}} \equiv \mathrm{b}^{\mathrm{n}}(\text{mod m})$for every positive integer n

(iv)$\mathrm{f(a)} \equiv \mathrm{f(b)}(\text{mod m})$

for every polynomial f with integer coefficient.

Proof:

(i) Given $a \equiv b(mod\ m)$ and $\alpha \equiv \beta(mod\ m)$

${}^{m}/_{a-b}$ and ${}^{m}/_{\alpha-\beta}$we have

$\Rightarrow\ m/x(a-b) + y(\alpha-\beta)$

(using linear property)

$\Rightarrow m/(ax+\alpha y) - (bx + \beta y)$

Notes

$\Rightarrow (ax+\alpha y)-(bx+\beta y)\equiv 0(mod\ m)$

$$\therefore\ \ ax+\alpha y\equiv bx+\beta y(mod\ m)$$

$$(ii) a\alpha\equiv b\beta(mod\ m)$$

$\Rightarrow a\alpha-b\beta\equiv 0(mod\ m)\Rightarrow m/a\alpha-b\beta$

Consider $a\alpha-b\beta=a\alpha-\alpha b+\alpha b-\beta b\Rightarrow\ \alpha(a-b)+b(\alpha-\beta)$

$$\Rightarrow\ m/\alpha(a-b)+b(\alpha-\beta)\ \Rightarrow m/a\alpha-b\beta$$

Hence $a\alpha\equiv b\beta(mod\ m)$

$(iii) To\ prove: a^n\equiv b^n(mod\ m)\ ,\ ie)\ to\ prove\ that\ {}^{m}/_{a^n}-b^n$

Given $a\equiv b(mod\ m)\ \Rightarrow m/a-b$

$$a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\cdots+b^{n-1})$$

$$m/(a-b)(a^{n-1}+a^{n-2}b+\cdots+b^{n-1})$$

$$m/a^n-b^n$$

(iv)To prove: f(a) ≡ f(b)(mod m)

Where f is a polynomial

$$f(x)=c_0+c_1x+c_2x^2+\cdots+c_nx^n$$

$$f(a)=c_0+c_1a+c_2a^2+\cdots+c_na^n$$

$$f(b)=c_0+c_1b+c_2b^2+\cdots+c_nb^n$$

$$f(a)-f(b)=c_1(a-b)+c_2(a^2-b^2)+\cdots+c_n(a^n-b^n)$$

$=c_1(a-b)+c_2(a^2-b^2)+\cdots+c_n[(a-b)(a^{n-1}+\cdots+b^{n-1}]\quad\rightarrow(1)$

(by (iii))

$$(1)\Rightarrow\ \ f(a)-f(b)\equiv 0(mod\ m)$$

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

Theorem 11.3:

If $c>0$, then $a\equiv b(mod\ m)\ if\ and\ only\ if\ \ ac\equiv bc(mod\ mc)$

Proof:

Assume that $a\equiv b(mod\ m)\Rightarrow m/a-b$

Now we take $a\equiv b(mod\ m)\,, c>0\ \ ac\equiv bc(mod\ mc)$

Conversely, Assume that $ac\equiv bc(mod\ mc)$

To prove that: $a\equiv b(mod\ m)$

$mc/ac-bc$

$\Rightarrow mc/(a-b)c \;\Rightarrow\; m/a-b$

(by cancellation law of divisibility)

$\therefore$ a ≡ b(mod m)

Notes

Theorem 11.4: ‘Cancellation Law’

If $ac \equiv bc(mod\ m)$ and if $d = (m,c)$ then $a \equiv b\left(mod\ \frac{m}{d}\right)$

Proof:

Assume that $ac \equiv bc(mod\ m)$ and if $d = (m,c)$

To prove: $a \equiv b\left(mod\ \frac{m}{d}\right)$

Given $ac \equiv bc(mod\ m) \Rightarrow m/ac - bc$

$\Rightarrow m/c(a-b)$

Given $d = (m,c) \Rightarrow 1 = \left(\frac{m}{d}, \frac{c}{d}\right)$

By Euclid’s Lemma {If ${}^{a}/_{bc}$ $and\ (a,b) = 1\ then\ {}^{a}/_{c}$}

$\Rightarrow \frac{m}{d}/\frac{c}{d}(a-b) \Rightarrow \frac{m}{d}/(a-b)$

Hence $a \equiv b\left(mod\ \frac{m}{d}\right)$

Theorem 11.5:

Assume $a \equiv b(mod\ m)$ if d/m and d/a then d/b

Proof:

Let $a \equiv b(mod\ m) \Rightarrow m/a-b$

Given $d/m$and $m/(a-b)$

(by transitive property)

$d/a-b$;

$a \equiv b(mod\ d), b \equiv a(mod\ d)$

Let d/a ; $a \equiv 0(mod\ d) \Rightarrow b \equiv 0(mod\ d)$

$$\therefore d/b$$

Theorem 11.6:

If $a \equiv b(mod\ m)$then $(a,m) = (b,m)$. In other words numbers which are congruent mod m have the same gcd with n

Proof:

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

Let $d = (a, m)\ and\ e = (b, m)\ Now\ d = (a, m)$

$\Rightarrow d/a$, d/m then d/b(by theorem 11.5)

$\Rightarrow d/(m, b) = d/e \qquad \rightarrow (1)$

Now $e = (b, m) \Rightarrow\ e/b\ , e/m.$

Then e/a (by theorem 11.5)

$\Rightarrow e/(m, a) = e/d \qquad \rightarrow (2)$

From (1) and (2) we get

$\mathrm{d/e}\ \text{ and }\ \mathrm{e/d} \Rightarrow \mathrm{d = e}\ \Rightarrow\ \mathrm{(a, m) = (b, m)}$

Notes

Theorem 11.7:

If $a \equiv b(mod\ m)$ and if $0 \leq (b - a) < m$ then $a = b$

Proof:

To prove that $a = b$

Using congruent definition $m/|a - b|$

$m \leq |a - b|$ more over $|a - b| \neq 0$

$m \leq |b - a|$ more over $|b - a| \neq 0$

$\mathrm{|b - a| = 0 \Rightarrow b - a = 0 \Rightarrow b = a}$

$\therefore \mathrm{a = b}$

Theorem 11.8:

We have $a \equiv b(mod\ m) if and\ only\ if\ a\ and\ b$ give a same remainder when divided by m.

Proof:

By division algorithm

Then there exists a positive integer $q,\ Q\ and\ r,\ R\ such\ that\ a = mq + r,\ \ where\ \ 0 \leq r < m$ and $b = MQ + R\ where\ 0 \leq R < M$

Now, $a \equiv b(mod\ m) \Leftrightarrow m/a - b$

$$\Leftrightarrow m/(mq + r) - (MQ + R) \Leftrightarrow M(q - Q) + r - R = mt$$

(where t is an integer)

$$\Leftrightarrow Mq - MQ + r - R = mt$$

$$\Leftrightarrow r - R = mt - Mq + MQ$$

Notes

$\Leftrightarrow r - R = M(t - q + Q)$ (where $k = (t - q + Q)$)

$\Leftrightarrow r - R = Mk$ (where k is a integer)

$$\Leftrightarrow m/r - R \Leftrightarrow r \equiv R(mod\ m)$$

$$\Leftrightarrow r = R \quad (by\ theorem\ 11.7)$$

Theorem 11.9:

If $a \equiv b(mod\ m)$ and $a \equiv b(mod\ n)$where $(m, n) = 1$, then $a \equiv b(mod\ mn)$

Proof:

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

$a \equiv b(\text{mod n})$

By definition of congruence $a \equiv b(mod\ m)$

$\Rightarrow m/a - b; a \equiv b(mod\ n) \Rightarrow n/a - b$

By the divisibility property $mn/a - b$

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

11.4 Residue classes and complete residue systems:

Definition 11.1.2:

"Residue class"

Consider the fixed modulo $m > 0$, the residue class is denoted by â . The set of all integers x such that $x \equiv a(mod\ m)$.

$$â = \{x/x \equiv a(mod\ m)\} \Rightarrow \{x/m/x - a\}$$

$$â = \{x/x - a = mq, q = 0, \pm 1, \pm 2, \dots \dots\}$$

$$â = \{x/x = mq + a, q = 0, \pm 1, \pm 2, \dots \dots\}$$

Example:

(i)$x \equiv 3(\text{mod } 5)$

$\Rightarrow 5/x - 3 \Rightarrow x - 3 = 5q, q = 0, \pm 1, \pm 2, \dots \dots$

$\Rightarrow x = \{\dots \dots - 7, -2, 3, 8, 13, \dots \dots\}$

Theorem 11.10:

For a fixed modulo $m > 0$, we have

(i)$â = \widehat{b}$ iff $a \equiv b(\text{mod m})$

(ii)Two integers x and y are in the same residue class iff $x \equiv y(\text{mod m})$

(iii)The m residue class $\hat{1},\dots\dots,\hat{m}$ are distinct and their union is the set of all integers.

Proof:

(i) Assume $\hat{a}=\hat{b}$

$$\hat{a}=\{x/x=a+mq,\ \ q=0,\pm 1,\pm 2,\dots\dots\}$$

$$\hat{b}=\{x/x=b+mr,\ \ r=0,\pm 1,\pm 2,\dots\dots\}$$

$\Leftrightarrow a+mq=b+mr$

$\Leftrightarrow a-b=mr-mq \Leftrightarrow a-b=m(r-q)$

$$(since\ r,q\ is\ an\ integer)$$

$\Leftrightarrow m/a-b \Leftrightarrow a\equiv b(mod\ m)$

(ii)Assume that x and y are in same residue class

$$x\equiv a(mod\ m) \qquad \rightarrow (1)$$

$$y\equiv a(mod\ m)\Rightarrow a\equiv y(mod\ m) \qquad \rightarrow (2)$$

(By symmetric property)

From (1) and (2)

$x\equiv y(mod\ m)$ (since transitive property)

Conversely, Assume that $x\equiv y(mod\ m)$

$y\equiv x(mod\ m)$ $\rightarrow (3)$ (By symmetric property)

We claim that, two integers x and y are in same residue class.

Suppose $x\in\hat{a}, y\in\hat{b}$

$$x\equiv a(mod\ m) \qquad \rightarrow (4)$$

$$y\equiv b(mod\ m) \qquad \rightarrow (5)$$

From (3) and (4)

$$y\equiv a(mod\ m) \qquad \rightarrow (6)$$

(6) $\Rightarrow y\in\hat{a}$.

Which is a $\Rightarrow\Leftarrow$

Hence two integers x and y are in same residue class.

$(iii) let\ \hat{\imath}\ ,\hat{\jmath}$are two residue class. $1\le i\le m, 1\le j\le m$

To prove that: the residue class$\hat{\imath}\ and\ \hat{\jmath}$ are disjoint

$$ie)\ \hat{\imath}\ \cap\ \hat{\jmath}\ =\emptyset$$

Suppose that $\hat{\imath}\ \cap\ \hat{\jmath}\ \neq\emptyset$

Notes

Let $x = \hat{\imath} \cap \hat{\jmath}$; $x \in \hat{\imath}$ *and* $x \in \hat{\jmath}$

By the definition of residue class

$x \equiv i(mod\ m) \Rightarrow i \equiv x(mod\ m)$ → (1) (by symmetry)

$$x \equiv j(mod\ m) \quad \rightarrow (2)$$

From (1) and (2)

$i \equiv j(mod\ m) \quad \Rightarrow \hat{\imath} = \hat{\jmath}$ (by (iii))

Which is a ⇒⇐

Let k be any integer

By division algorithm there exists q *and* r such that $k = mq + r, 0 \leq r < m \Rightarrow mq = k - r$

$$\Rightarrow m/k - r\ (q\ is\ the\ set\ of\ integers)$$

$$\Rightarrow k \equiv r(mod\ m)$$

Hence the union of all m residue class.

Definition 11.1.3: "Complete Residue System"

A set of m representatives, one from each of the residue classes 1, 2,…,m is called a complete residue system modulo m.

Example:

Any set consisting of m integers, incongruent mod m is a complete residue system mod m.

For example (1, 2,…, m); (0, 1, 2, …., (m-1)); {1, m+2, 2m+3, 3m+4, ……, m^2}

Theorem 11.11:

Assume that $(k, m) = 1$, if $\{a_1, a_2, \dots \dots, a_m\}$ is a complete residue system mod m so is $\{ka_1, ka_2, \dots \dots, ka_m\}$

Proof:

Given $(k, m) = 1\{a_1, a_2, \dots \dots, a_m\}$ is a complete residue system mod m

By definition of $a_i \not\equiv a_j(mod\ m)$

To prove:$\{ka_1, ka_2, \dots \dots, ka_m\}$ is a complete residue system

That is to prove $ka_i \not\equiv ka_j(mod\ m)$

Suppose $ka_i \equiv ka_j(mod\ m)$

Since $(k, m) = 1$

$a_i \equiv a_j (\text{mod } m)$

Which is a $\Rightarrow\Leftarrow$

$\therefore ka_i \not\equiv ka_j (mod\ m)$

Notes

11.5 Linear congruences:

Definition 11.1.4: "Linear congruence"

Given integers $a, b, m\ with\ m > 0$ and x is an unknown integer then the linear congruence is of the form $ax \equiv b(mod\ m)$ is said to a linear congruence

Example:

$7x \equiv 3(\text{mod } 4)$

for $x = 1, 7 \equiv 3(\text{mod } 4)$

Theorem 11.12:

Assume that $(a, m) = 1$ the linear congruence $ax \equiv b(mod\ m)$ has exactly one solution.

Proof:

Given $(a, m) = 1$

To prove: $ax \equiv b(mod\ m)$ has exactly one solution

Now, Assume that $ax \equiv b(mod\ m)$ has an solution

Since $(a, m) = 1$, by using theorem 11.11

$\Rightarrow \{1, 2, \dots \dots, m\}$is an complete residue system

$\Rightarrow \{a, 2a, \dots \dots, ma\}$is the product of a

Since $(a, m) = 1$,

$\Rightarrow \{a_1, \dots \dots, a_n\}$is an complete residue system

The linear congruence $ax \equiv b(mod\ m)$ has exactly one solution.

Theorem 11.13:

Assume $(a, m) = d$ then the linear congruence $ax \equiv b(mod\ m)$ has a solution $iff\ {}^{d}/_{b}$

Proof:

If a some exists then ${}^{d}/_{b}$

Since ${}^{d}/_{m}$ and ${}^{d}/_{a}$

Notes

Conversely, if d/b is congruence

$\frac{a}{d}x \equiv b(mod\ m)$has a solution $\left(\frac{a}{d},\frac{m}{d}\right) = 1$and this solution is also a solution of linear congruence.

Theorem 11.14:

Assume $(a, m) = d$ and suppose that d/b then the linear congruence $ax \equiv b(mod\ m)$ has exactly d solutions mod m, there are given $t, t + \frac{m}{d}, t + \frac{2m}{d}, \ldots \ldots, t + (d-1)\frac{m}{d}$ where t is the solution, unique modulo $\frac{m}{d}$ of the linear congruence $\frac{a}{d}x \equiv \frac{b}{d}(mod\ \frac{m}{d})$

Proof:

(i) The solution of $ax \equiv b(mod\ m)$ is equivalent to the solution of $\frac{a}{d}x \equiv \frac{b}{d}(mod\ m)$

Let t be the solution of $\frac{a}{d}x \equiv \frac{b}{d}(mod\ m)$

$$\frac{a}{d}t \equiv \frac{b}{d}(mod\ m) \Rightarrow \frac{m}{d}/\frac{at}{d} - \frac{b}{d}$$

$$\Rightarrow \frac{at}{d} - \frac{b}{d} = \frac{m}{d}k, \quad where\ k \in Z$$

$\frac{at-b}{d} = \frac{mk}{d} \Rightarrow m/at - b \Rightarrow at \equiv b(mod\ m)$

$t$be the solution of $ax \equiv b(mod\ m)$ is equivalent to the solution of

$$\frac{a}{d}x \equiv \frac{b}{d}(mod\ m)$$

(ii) To prove $t, t + \frac{m}{d}, t + \frac{2m}{d}, \ldots \ldots, t + (d-1)\frac{m}{d}$ has exactly d solution of modulo m.

Suppose that $t + \frac{rm}{d}, t + \frac{sm}{d}$ are the disjoint solution of $ax \equiv b(mod\ m)$

$a\left(t + \frac{rm}{d}\right) \equiv b(mod\ m) \quad 0 \leq r <\rightarrow$ (1)and

$$a\left(t + \frac{sm}{d}\right) \equiv b(mod\ m) \quad 0 \leq s < d$$

$b \equiv a\left(t + \frac{sm}{d}\right)(mod\ m) \qquad \rightarrow$ (2) (by commutative)

From (1) and (2)

$$a\left(t + \frac{rm}{d}\right) \equiv a\left(t + \frac{sm}{d}\right)(mod\ m)$$

$$t + \frac{rm}{d} \equiv t + \frac{sm}{d}(mod\ m)$$

$$\Rightarrow m/t+\frac{rm}{d}-\left(t+\frac{sm}{d}\right)$$

$$\Rightarrow m/\frac{rm}{d}-\frac{sm}{d}$$

$$\Rightarrow \frac{rm}{d}-\frac{sm}{d}=mk\Rightarrow \frac{r-s}{d}=k$$

$$\Rightarrow r-s=dk\Rightarrow d/r-s$$

$$\Rightarrow r\equiv s(mod\ m)\qquad 0\leq |r-s|<d$$

(By theorem 11.7)

$$r=s$$

Which is a ⇒⇐ to $t+\frac{rm}{d},t+\frac{sm}{d}$are the disjoint solution of $ax\equiv b(mod\ m)$

∴ $t,t+\frac{m}{d},t+\frac{2m}{d},\dots\dots,t+(d-1)\frac{m}{d}$has exactly d solution of modulo m.

(iii) To prove there is no solution except $t,t+\frac{m}{d},t+\frac{2m}{d},\dots\dots,t+(d-1)\frac{m}{d}$

Let y be the solution of $a\equiv b(mod\ m)$

$$ay\equiv b(mod\ m)\qquad\rightarrow(3)$$

Since t be the solution of $a\equiv b(mod\ m)$

$$at\equiv b(mod\ m)\Rightarrow\quad b\equiv at(mod\ m)\qquad\rightarrow(4)$$

From (3) and (4)

$$ay\equiv at(mod\ m)\Rightarrow m/ay-at\Rightarrow m/a(y-t)$$

$$\Rightarrow \frac{m}{d}/\frac{a}{d}(y-t)$$

By Euclid’s lemma: $\frac{m}{d}/(y-t)\left(since\ \left(\frac{m}{d},\frac{a}{d}\right)=1\right)$

$$\Rightarrow y-t\equiv\frac{m}{d}k\qquad\rightarrow(5)$$

By Division algorithm, there exists an integers$q\ and\ r$ such that $k=dq+r\quad 0\leq r<d$.

$$dq=k-r\ \Rightarrow q=k-r\left(\frac{1}{d}\right)$$

Multiply m on both sides $mq=k-r\left(\frac{m}{d}\right)\ \Rightarrow m/k-r\left(\frac{m}{d}\right)$

$\Rightarrow m/\frac{mk}{d}-\frac{mr}{d}\Rightarrow y-t\equiv\frac{mr}{d}(mod\ m)$

$$\Rightarrow y \equiv t + \frac{mr}{d}(mod\ m)$$

Hence there is no solution except $t, t + \frac{m}{d}, t + \frac{2m}{d}, \ldots \ldots, t + (d-1)\frac{m}{d}$.

Notes

Theorem 11.15:

If $(a, b) = d$ there exists integers $x\ and\ y$ such that $ax + by = d$

Proof:

The linear congruence $ax \equiv d(mod\ b)$ has a solution

Hence there is an integer y such that $d - ax = by$

This gives us $ax + by = d$ as required.

Note: Geometrically the pairs (x, y)satisfying $ax + by = d$ we are lattice points lying on a straight line the x coordinate of each of there points is a solution of the congruence $ax \equiv d(mod\ b)$; $(a, b) = d$

$$\Rightarrow d \equiv ax(mod\ b) \Rightarrow b/d - ax \Rightarrow d - ax$$

11.6 Reduced residue systems and the Euler-Fermat theorem:

Definition 11.1.5: "Reduced Residue System"

A reduced residue system modulo m we mean any set of $\phi(m)$ integers incongruent modulo m each of which is relatively prime to m.

Example: If m $= 10$

Reduced residue system $= (1, 3, 7, 9)$

Note: $\phi(m)$is a Euler totient function.

Theorem 11.16:

If $\{a_1,\ a_{2,} \ldots \ldots, a_{\phi(m)}\}$ is a reduced residue system modulo m and if $(k, m) = 1$ then $\{ka_1, ka_{2,} \ldots \ldots, ka_{\phi(m)}\}$ is also a reduced residue system modulo m.

Proof:

Given $\{a_1,\ a_{2,}\ \ldots \ldots, a_{\phi(m)}\}$are reduced residue system modulo m.

Assume$(k, m) = 1$,

In $\{ka_1, ka_{2,} \ldots \ldots, ka_{\phi(m)}\}$ no two of the numbers ka_i are congruent modulo m.

By definition, $(a_i, m) = 1$

$$[we\ know\ that\ (a, b) = 1, (a, c) = 1\ \ then\ (a, bc) = 1]$$

Since $(k, m) = 1, \quad (ka_i, m) = 1$

$\therefore ka_{1,}\, ka_2, \dots \dots, ka_{\phi(m)}$are reduced residue system modulo m.

Theorem 11.17: "Euler- Fermat Theorem"

Assume that $(a, m) = 1$ then we have $a^{\phi(m)} \equiv 1(mod\ m)$

Proof:

If $\{b_1, b_2, \dots \dots, b_{\phi(m)}\}$is reduced residue system modulo m (by definition)

ie) $(\mathrm{b_i}, \mathrm{m}) = 1$

since $(a, m) = 1$, then $\{ab_1, ab_2, \dots \dots, ab_{\phi(m)}\}$ is also reduced residue modulo m.

(By theorem 11.16)

The product of set of integers in the first set is congruent to product of those in the second set.

$$ie)\{b_1, b_2, \dots \dots, b_{\phi(m)}\} \equiv \{ab_1, a\, b_2, \dots \dots, ab_{\phi(m)}\}\ (mod\ m)$$

$$b_1, b_2, \dots \dots, b_{\phi(m)} \equiv a^{\phi(m)}\left(b_1, b_2, \dots \dots, b_{\phi(m)}\right)(mod\ m)$$

$$1 \equiv a^{\phi(m)}(mod\ m)$$

$a^{\phi(m)} \equiv 1(mod\ m)$ (By cancellation law)

Hence the proof.

Theorem 11.18:

If a prime p does not divide a then $a^{p-1} \equiv 1(mod\ p)$

Proof:

Given p does not divide a and we know that (a, p) =1 By usingEuler'sfermat's theorem,

$a^{\varphi(p)} \equiv 1(mod\ p)$ …………….(5)

$\varphi(p) = p - 1$ whenever p is prime

$\mathrm{a^{p-1}} \equiv 1(\mathrm{mod\ p})$

Hence proved.

Theorem 11.19:

For any integer a and any prime p, we have $a^p \equiv a(mod\ p)$

Proof:

Case 1: If p|a⇒ a$\equiv 0(mod\ p)$…….(6)

Notes

$\Rightarrow \quad a^p \equiv 0(mod\ p)$

$\Rightarrow 0 \equiv a^p(mod\ p)$………(7)

From (6) and (7) we have

$a \equiv a^p(mod\ p)$ (by transitive)

$a^p \equiv a(mod\ p)$ (by symmetric)

Case 2: If p∤a then $a^{p-1} \equiv 1(mod\ p)$...........(8)

$a^p/a \equiv 1(mod\ p)$ ....(9)

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

Hence proved.

Theorem 11.20:

If (a, m) =1 the solution (unique mod m) of the linear congruence $ax \equiv b(modm)$ is given by $x \equiv ba^{\varphi(m)-1}(modm)$.

Proof:

Given $x \equiv ba^{\varphi(m)-1}(mod\ m)$ is the solution of the linearcongruence $ax \equiv b(mod\ m)$.

$a\ (ba^{\varphi(m)-1}) \equiv b(mod\ m)$

$aba^{\varphi(m)}a^{-1} \equiv b(mod\ m)$

$ba^{\varphi(m)} \equiv b(mod\ m)$

$a^{\varphi(m)} \equiv 1(mod\ m)$.

By using Euler's Fermat theorem, The solution is unique modulo m.

11.7 Exercises:

(1)prove that $5n^3 + 7n^5 \equiv 0(mod\ 12)$ for all integers n.

(2) Find all positive integers n for which $n^{13} \equiv n(mod\ 1365)$.

(3) Find all positive integers n for which $n^{17} \equiv n(mod\ 4080)$.

(4) Prove that $\varphi(n) \equiv 2(mod\ 4)$when $n = 4$ and when $n = p^a$, p is a prime,

$p \equiv 3(mod\ 4)$.

(5) Find all n for which $\varphi(n) \equiv 2(mod\ 4)$.

BLOCK IV: POLINOMIAL CONGRUENCES AND QUADRATIC RESIDUES

Notes

UNIT-XII: APPLICATIONS OF CONGRUENCES

Structure

12.1 Introduction:

In this unit, we will discuss more than one linear congruences. Under certain conditions, we will show that such simultaneous congruences have a solution. We will also discuss the uniqueness of such a solution. For solving such congruences, thereis a well-known method known as the Chinese Remainder Theorem.

12.2 Objectives:

The students will be able to

- Solve linear congruences
- Describe the Lagranges theorem
- Determine the Chinese remainder theorem

12.3: POLYNOMIAL CONGRUENCES MODULO P:

The fundamental theorem of algebra states that every polynomial f of degree n≥1 the equation f(x)=0 has r solutions among the complex numbers. There is no direct analog of this theorem for polynomial congruences. For example,we have seen that the some linear congruences have no solutions some have exactly one solution and some have more than one. Thus, even in this special case there appears to be no simple relation between the number of solution and the degree of the polynomial. However, for congruences modulo a prime we have following theorem of Lagrange.

Notes

Theorem 12.1(Lagrange)

Given a prime p, f(x)=$c_0 + c_1x + \cdots c_nx^n$be a polynomial of degree n with integer coefficient such that $c_n$is not congruent to 0(mod p). Then the polynomial congruence f(x)≡0 (mod p) ……………(1) has at most r solutions.

Proof:

Let us given f(x)≡0(mod p). Then we have to prove by induction on n, when n=1, The congruence is linear. $c_1x+c_\circ\equiv$ (mod p) since c_1 is not congruent to 0(mod p) we have (c, p) =1 and there is exactly one solution.

Assume that the theorem is true for polynomial of degree n-1.

Assume also that the congruence (1) has n+1 incongruence solution mod p (say) x_0,x_1…………,x_n . Where f (x_i)≡0(mod p) for every i=0,1, 2,…..n. we shall obtain a contradiction we have algebraic identity.

f(x)= $c_0 + c_1x + \cdots c_nx^n$ ……………….(2)

f (x_0)= $c_0 + c_1x + \cdots c_nx^n$……………….(3)

f(x)-f(x_0) = $c_1(x - x_0) + c_2(x^2 - {x_0}^2) + \cdots c_n(x^n - {x_0}^n)$……………(4)

$= \sum_{r=1}^{n} c_r(x^r - {x_0}^r)$

$=\sum_{r=1}^{n} c_r(x - x_0)(x^{r-1} + \cdots {x_0}^{r-1})$

$= (x-x_0)\sum_{r=1}^{n} c_r(x^{r-1} + \cdots {x_0}^{r-1})$

f(x)-f (x_0)= (x-x_0) g(x), where g(x) is a polynomial of deg n-1 with integer coefficient and with leading coefficient c_n.

Thus, we have

f (x_k)-f (x_0)= $(x_k$-$x_0)$ g (x_k) ≡0(mod p)

since,f (x_k)-f (x_0)≡0(mod p) But is$(x_k$-$x_0)$ $\not\equiv$ 0 (mod p) if k≠0

So must have g (x_k)≡0(mod p) for every k≠0 By this n incongruent solution of modulo p.Which is contradiction to our hypothesis.

12.4 Applications of Lagrange's theorem

Theorem 12.2

If f(x)=c_0+c_1x +……+c_nx^n is the polynomial of degree n with integer coefficient and if the congruence f(x)≡ $0(modp)$ has more than n solution when p is a prime . Then every coefficient of f is divisibly by p.

Notes

Proof:

If some coefficient of f is not divisible by p. then k$\leq n$ and the congruence

f(x)$\equiv 0(mod\ p)$. we take

$$f(x)=c_0+c_1\,x+\ldots\ldots+c_k\,x^k+c_{k+1}x^{k+1}+\ldots.+c_n\,x^n$$

Therefore $c_0+c_1\,x+\ldots\ldots+c_k\,x^k\ \equiv 0(mod\ p)$ has more than k solution. By Lagrange's theoremP divides c_k

Which is a contradiction to our assumption.

Therefore, every coefficient of f is divisible by p.

Theorem 12.3

For any prime p all the coefficient of the polynomial f(x)=(x-1) (x-2) ……..(x-(p+1)) is divisible by p.

Proof:

Given f(x)=(x-1) (x-2) ……..(x-(p+1))-$x^{p-1}+1$

f(x)=g(x)-h(x)

g(x)=(x-1) (x-2)..........(x-(p+1))

h(x)=x^{p-1}-1

The roots of g are 1, 2,...p-1.

Hence satisfy the congruence equation

g(x)$\equiv 0(mod\ p)$

Let h(x) =x^{p-1}-1 suppose (a, m) =1, $a^{\varphi(m)}\equiv 1(mod\ m)$ (By Euler'sformatstheorem)

Assume (x, p) =1, we have $x^{\varphi(p)}\equiv 1(mod\ p)$.

By Euler's Fermat's theorem,

$\varphi(p)=(p-1)$ whenever p is a prime

$$x^{p-1}\equiv 1(mod\ p)$$

$$x^{p-1}-1\equiv 0(mod\ p)$$

h(x)$\equiv 0(mod\ p)$

f(x)=g(x)-h(x)$\equiv 0(mod\ p)$

$\Rightarrow$ f(x)$\equiv 0(mod\ p)$.

If f(x) has degree (p-2) then also f(x)$\equiv 0(mod\ p)$

Notes

∴ All the coefficient f(x) is divisible by p.

Theorem 12.4: (Wilson's Theorem)

For any prime p we have (p-1)! $\equiv -1(mod\ p)$ and prove its converse.

Proof:

Consider the polynomial are

$$(x-1)\ (x-2)\ ....(x-(p-1))-(x^{p-1}+1)$$

The constants terms of the polynomial are

$$-1, -2, -3.......(-(p-1)) +1= (-1)\ (1), (-1)\ (2), ...(-1)\ (p-1) +1$$

$$=(-1)^{p-1}(p-1)! +1$$

Since all the coefficient must be divisible by p

$$P \mid (-1)^{p-1}(p-1)! +1$$

$P \mid (p-1)! +1$ [since, where p is prime (p-1) is even]

$$(p-1)! +1 \equiv 0(mod\ p\ )$$

$$(p-1)! \equiv -1(mod\ p)$$

Conversely, For n$>$ 1

$(n-1)! \equiv\ -1(mod\ n)$

$(n-1)! +1 \equiv 0(mod\ n)$

$n \mid (n-1)! +1$

To prove n is prime

Suppose n is composite

$$n=cd$$

$$d \mid n\ ....(10)$$

since n is the divisor such that 1<d<n

$$d=1,2,\ ....(n-1) \text{then } d \mid (n-1)!..............(11)$$

From (10) and (11)

$$n \mid (n-1)!$$

$$n \nmid (n-1)! + 1$$

Which is a contradiction

∴ n is prime.

Theorem 12.5 (Wolstenholme's)

For any prime p≥ 5 we have $\sum_{k=1}^{p-1}(p-1)!/k$

Proof:

Notes

The sum$\sum_{k=1}^{p-1}(p-1)!/k$ is the sum of the product of the number 1,2, ...(p-1) taken (p-2) at a time. This sum is also equal to the coefficient of x in the polynomial.

g(x)=(x-1) (x-2) ....(x-(p+1)).

g(x) can be written in the form of

g(x)=$x^{p-1}-s_1x^{p-2}+s_2x^{p-3}+\cdots.s_{p-3}\ x^2-s_{p-2}x+(p-1!)$

where the coefficient of s_k is the k^{th} elementary symmetric function of the roots that is the sum of the product of the numbers 1,2.... (p-1) taken k at a time. (By theorem 12.7) each of the number $s_1,s_2,s_{3,\dots\dots,}s_{p-2}$ is divisible by p

we have to show that $s_{p-2}$is divisible by p^2.

The product of g(x) shows that g(p)=(p-1)!

(p-1)! =$p^{p-1}-s_1p^{p-2}-\cdots-s_2p^{p-3}s_{p-2}p^{p+(p-1)!}$

Cancelling (p-1)! And reducing the equation modulop^3 , we get

Since p>5, p$s_{p-2}\equiv 0(\text{mod } p^3)$

And hence $s_{p-2}\equiv 0(mod\ p^2)$as required.

12.5 SIMULTANEOUS LINEAR CONGRUENCES.

Theorem 12.6:(The Chinese remainder theorem)

Assume $m_1,m_{2,}\dots.m_r$ are positive integers relatively prime pairs (m_i , m_k)=1, i≠k. Let $b_1,b_2,\dots b_n$ are arbitrary integers. Then the system of congruences,

x≡ $b_1\ (mod\ m_1)$

x≡ $b_2(mod\ m_2)$

⋮

x≡ $b_r(mod\ m_r)$.

Has exactly only one solution modulus $m_1,m_{2,}\dots.m_r$.

Proof:

Let M=$m_1,m_{2,}\dots.m_r$ and $m_k\ =\ M/m_k$

Notes

By Euclid's extended algorithm

Let M'_k be a reciprocal of m_k

$M_k M'_k \equiv 1(mod\ m_k\ )$......................(12)

Let x=$b_k M_k M'_k(mod\ \ m_k\ )$ (k=1,2,....r)

X=$b_k(1)(mod\ \ m_k\ )$

Hence x satisfies every system of congruences modulo m_k

<u>UNIQUENESS:</u>

Let x and y be the two solutions of system congruences

x≡ $b_k\ (modm_k\ )$.............(13)

y≡ $b_k\ (modm_k\ )$

$b_k\ \equiv y(modm_k\ )$...............(14) (by symmetric)

From (13) and (14)

x≡ $y(mod\ m_k)$ (by transitive)

since m_k are relatively prime in pairs.

x≡ $y(mod\ m_{1,}m_{2,\dots\dots,}m_r)$

x≡ $y(mod\ m_k)$

since congruence is an equivalence relation

x=y.

Theorem 12.7:

Assume $m_{1,}m_{2\dots\dots}m_r$ are relatively prime in pairs. Let $b_{1,}b_2, \dots \dots b_r$ be arbitrary integers and let $a_{1,}a_{2,\dots}a_r$ satisfy $(a_{k,}m_k)$=1 for k=1,2,...r. then the linear system of congruence

a_1x≡ $b_1\ (mod\ m_1)$

a_2x≡ $b_2(mod\ m_2)$

$\vdots$

a_r x≡ $b_r(mod\ m_r)$. Has exactly solution modulo $m_{1,}m_{2\dots\dots}m_r$.

Proof:

Let $a_k$denote the reciprocal of $a_k$modulo m_k. This exists since $(a_{k,}m_k)$=1. Then the congruencea_kx≡ $b_k\ (modm_k\ )$ is equivalent to the congruence x≡ $b_k a'_k(mod\ m_k)$.Now apply theorem 12.10.

12.6: APPLICATIONS OF THE CHINESE REMAINDER THEOREM:

Notes

Theorem 12.12:

Let f be a polynomial with integer coefficients, let $m_{1,}m_{2\ldots\ldots}m_r$ be positive integers relatively prime in pairs and let m=$m_{1,}m_{2\ldots\ldots}m_r$. Then the congruence

f(x)≡ $0(mod\ m)$....................(15)

has a solution if and only if each of the congruences

f(x)≡ $0(mod\ m_i)$ (i= 1,2......r) ....(16) has a solution. Moreover, if v(m) and v (m_i) denote the number of solutions of (1) and (2), respectively, then

v(m)=v (m_1), v(m_2),v(m_r) ....(17)

Proof:

If f(a)≡ 0 $(mod\ m)$ then f(a)≡ 0 $(mod\ m_i)$ for each i. Hence every solution of (15) is also a solution of (16).

Conversely, let a_i be a solution of (16). Then by Chinese remainder theorem there exists an integer a such that

$a \equiv a_i\ (mod\ m_i)$ for i=1,2,...,r. ....(18)

so

$f(a) \equiv f(a_i) \equiv 0\ (mod\ m_i)$.

Since the moduli are relatively prime in pairs, we also have f(a)≡ 0 $(mod\ m)$. Therefore, if each of the congruences in (16) has a solution, so does (15).

We also know, by theorem 12.10, that each r-tuple of solutions $(a_1, a_2, \ldots, a_r)$ of the congruences in (16) gives rise to a unique integer a mod m satisfying (18). As each a_i runs through the v(m_i) solutions of (16) the number of integers a which satisfy (18) and hence (16) is v(m_1),v(m_2),...,v(m_r). This proves (17).

Theorem 12.13:

The set of lattice points in the plane visible from the origin contains arbitrarily large square gaps. That is, given any integer k>0 there exists a lattice point (a, b) such that none of the lattice points (a+r, b+s), $0 < r \leq k, 0 < s \leq k$, is visible from the origin.

Proof:

Let $p_1, p_2, \ldots.$, be the sequence of primes. Given k>0 consider the $k \times k$ matrix whose entries in the first row consists of the first k primes, those in

Notes

the second row consists of the next k primes, and so on. Let m_i be the product of the primes in the i^{th} row and let M_i be the product of the primes in the i^{th} column. Then the numbers m_i are relatively prime in pairs as are the M_i.

Next consider the set of congruences

x$\equiv -1(mod\ m_1)$

x$\equiv -2(mod\ m_2)$

$\vdots$

x$\equiv -k(mod\ m_k)$.

This system has a solution a which is unique mod $m_{1,}m_{2\ldots\ldots}m_k$. Similarly, the system

y $\equiv -1(mod\ M_1)$

y$\equiv -2(mod\ M_2)$

$\vdots$

y$\equiv -k(mod\ M_k)$.

has a solution b which is unique mod $M_1, M_2, \ldots, M_k = \boldsymbol{m_{1,}m_{2\ldots\ldots}m_k}$.

Now consider the square with opposite vertices at (a,b) and (a+k,b+k). Any lattice point inside this square has the form

(a+r, b+s), where 0<r<k, 0<s<k,

And those r=k or s=k lie on the boundary of the square. We now show that no such point is visible from the origin. In fact,

$a \equiv\ -r\ (mod\ m_r)$, and$b \equiv -s\ (mod\ M_s)$

so, the prime in the intersection of row r and column s divides both a+rand b+s. Hence a+r and b+s are not relatively prime, and therefore the lattice point (a+r , b+s) is not visible from the origin.

12.7 EXERCISES:

1.Prove the converse of Wilson's theorem: If (n-1)! +1$\equiv$ 0(mod n), then n is prime if n>1.

2. Find all positive integers n for which (n-1)! +1 is a power of n.

3. If p is an odd prime, let q=(p-1)/2. Prove that $(q!)^2 + (-1)^q \equiv 0$(mod p). This gives q! As an explicit solution to the congruence $x^2 + 1 \equiv 0(mod\ p)$ when p$\equiv 1(mod\ 4)$, and it shows that q! =± 1(mod p) if p$\equiv 3(mod\ 4)$. No simple general rule is known for determining the sign.

Notes

4.If p is odd p>1,prove that $1^2 3^2 5^2 \ldots (p-2)^2 \equiv (-1)^{(p-1)/2}$(mod p) and $2^2 4^2 6^2 \ldots (p-1)^2 \equiv (-1)^{(p+1)/2}$(mod p)

UNIT-XIII DECOMPOSITION PROPERTY

Notes

Structure

13.1 Introduction:

Generally, Solving linear congruences is fundamental in many parts of number theory. The generalization, solving polynomial congruences, is perhaps not as basic but is still an important topic. For the polynomials students have worked with in the past, namely polynomials with rational, real, or complex coefficients, the number of solutions in complex numbers is at most the degree of the polynomial. How to solve polynomial congruences mod primes and mod prime powers, the Chinese Remainder Theorem allows solving polynomial congruences for composite moduli.

13.2 Objectives:

The students will be able to

- Analyse polynomial congruence
- Describe the principle of cross classification
- Determine the decomposition property of reduced residue system

13.3 POLYNOMIAL CONGRUENCES WITH PRIME POWER MODULI:

Theorem 12.12 shows that the problem of solving a polynomial congruence f(x)$\equiv 0(mod\ m)$ can be reduced to that of solving a system of congruences

$$f(x)\equiv 0(mod\ p_i^{\alpha_i})\ (i=1,2,.....r)$$

where m=$p_1^{\alpha_1}.........p_r^{\alpha_r}$. In this section we show that the problem can be further reduced to congruences with prime moduli plus a set of linear congruences. Let f be a polynomial with integer coefficients and suppose that for some prime p and $\alpha \geq 2$ the congruence

f(x)≡ $0(mod\ p^{\alpha})$......................(1)

has a solution, say x=a, where a is chosen so that it lies in the interval 0≤ $a < p^{\alpha}$.

Notes

This solution is also satisfying each of the congruences

f(x)≡ $0(mod\ p^{\beta})$ for each $\beta < \alpha$ in particular, a satisfies the congruence

f(x)≡ $0(mod\ p^{\alpha-1})$......................(2).

Now divide a by $r^{\alpha-1}$ and write a=q$p^{\alpha-1}$+r ....(3) where 0≤ $r < p^{\alpha-1}$.

The remainder r determined by (3) is said to be generated by a. Since

r ≡ $a(mod\ p^{\alpha-1})$ the number r is also solution of (2). In other words, every solution a of congruence (1) in the interval0≤ $a < p^{\alpha}$ generates a solution r of congruence (2) in the interval

0≤ $a < p^{\alpha-1}$.

Now suppose we start with a solution r of (2) in the interval 0≤ $r < p^{\alpha-1}$ and ask whether there is a solution a of (1) in the interval 0≤ $a < p^{\alpha}$ which generates r. If so, we say that r can be lifted from $p^{\alpha-1}$to p^{α}. The next theorem shows that the possibility of r being lifted depends on f(r) mod p^{α} and on the derivative f '(r) mod p.

Theorem 13.1:

Assume $\alpha \geq 2$ and let r be a solution of the congruence f(x)≡ $o(mod)p^{\alpha-1}$............(4) lying in the interval 0≤ $r < p^{\alpha-1}$.

a)Assume f(r) ≢ (mod p). Then r can be lifted in a unique way from $p^{\alpha-1}$to p^{α}. That is, there is a unique a in the interval 0≤ $a < p^{\alpha}$ which generates r and which satisfies the congruence

f(x)≡ $o(mod)p^{\alpha}$ ....(5)

b)Assume f '(r) ≡ 0(mod p). Then we have two possibilities:

b1) If f(x)≡ $0(mod\ p^{\alpha})$, r can be lifted from $p^{\alpha-1}$to p^{α}in p distinct ways.

b2) If f(r)≢ $0(mod\ p^{\alpha})$, r cannot be lifted from$p^{\alpha-1}$to p^{α}.

Proof:

If n is the degree of f, we have the identity (Taylor's formula)

f(x+h) =f(x)+ f' (x)h +$\frac{f''(x)}{2!}h^2$+........+$\frac{f^n(x)}{n!}h^n$.......(6)

Notes

for every x and h. We note that each polynomial $f^k(x)/k!$ has integer coefficients. Now we take x=r in (6), where r is a solution of (4) in the interval 0≤ $r < p^{\alpha-1}$, and let h=q$p^{\alpha-1}$ where q is an integer to be specified presently. Since $\alpha \geq 2$ the terms in (6) involving h^2 and higher powers of h are integer multiples of p^{α}. Therefore (6) gives the congruence

$$f(r+qp^{\alpha-1}) \equiv f(r)+f'(r)qp^{\alpha-1}(mod p^{\alpha})$$

since r satisfies (4) we can write f(r)≡ $kp^{\alpha-1}$ for some integer k and the last congruence becomes

$$f(r+qp^{\alpha-1}) \equiv \{qf'(r)+k\}p^{\alpha-1}(mod\ p^{\alpha})$$

Now let

$$a=r+qp^{\alpha-1}..............(7).$$

Thensatisfies the congruence (23) if and only if q satisfies the linear congruence

$$qf'(r)+k \equiv 0(\text{mod } p)............(8)$$

If $f'(r) \not\equiv 0(mod\ p)$ this congruence has a unique solution q mod p and if we choose q in the interval 0≤ $q < p$ then the numbers a is given by(7) will satisfy (5) and will lie in the interval 0≤ $a < p^{\alpha}$.

On the other hand, if $f'(r) \equiv 0(mod\ p)$ then (8) has a solution q, if and only if,p|k that it is iff f(r)≡ $0(modp^{\alpha})$. If p∤k there is no choice of q to make a satisfy (5). But p|k then the p values q=0,1,.........,p-1 give p solution a of (5) which generate r and lie in the interval 0≤ $a < p^{\alpha}$. This completes the proof.

13.4 THE PRINICIPLE OF CROSS-CLASSIFICATION:

Some problems in number theory can be dealt with by applying a general combinatorial theorem about sets called the principle of cross-classification. This is a formula which counts the number of elements of a finite set which do not belong to certain prescribed subsets $s_1, s_2, \dots \dots . s_n$.

NOTATION: If T is a subset of S, we write N(T) for number of elements of T. We denote S-T the set of those elements of S which are not in T. Thus

$$S - \cup_{i=1}^{n} s_i$$

Consists of those elements of S which are not in any subsets of $s_1, s_2, \dots \dots . s_n$. For brevity we write $s_i s_j$, $s_i s_j s_k$......for the intersections $s_i \cap s_j$, $s_i \cap s_j \cap s_k$...... respectively.

Theorem 13.2:

Notes

If $s_1, s_2, \ldots \ldots . s_n$ are given subsets of a finite sets, the N(S$-\bigcup_{i=1}^{n} s_i$)=N(s)-$\sum_{1\le i\le n} N(s_i)$+$\sum_{1\le i\le j\le n} N(s_i s_j)$-$\sum_{1\le i\le j\le k\le n} N(s_i s_j s_k)$+........$(-1)^n$N($s_1, s_2, \ldots \ldots . s_n$).

Proof:

If T⊆S , Let $N_r(T)$ denotes the number of elements in T which is not in any of subsets $s_1, s_2, \ldots \ldots . s_n$ with $N_0(T)$ being simply N(T). The elements are enumerated by $N_{r-1}(T)$ falls into two disjoint sets. These which are not in S which are in S_r. Then we have, $N_{r-1}(T) = N_r(T) + N_{r-1}(TS_r)$.

Hence, $N_r(T) = N_{r-1}(T) + N_{r-1}(TS_r)$........(9)

We take T-S

$N_r(S) = N_{r-1}(S) + N_{r-1}(SS_r)$...............(10)

In equation (28) to express on each term on right interms of N_{r-2}(s)

$N_{r-1}(S) = N_{r-2}(S) + N_{r-2}(SS_r)$

$N_{r-1}(S_r) = N_{r-2}(S_r) + N_{r-2}(SS_r)$

$N_r(S) = N_{r-2}(S) + N_{r-2}(S_{r-1})$

$= N_{r-2}(S) - N_{r-2}(SS_{r-1}) - N_{r-2}(S_r) + N_{r-2}(SS_{r-1})$

Proceeding like this we obtain,

N(S$-\bigcup_{i=1}^{r} s_i$)=N_0(s)- $\sum_{1\le i\le r} N_0(s_i)$+$\sum_{1\le i\le j\le r} N_0(s_i s_j)$-$\sum_{1\le i\le j\le k\le r} N_0(s_i s_j s_k)$+........$(-1)^r N_0(s_1, s_2, \ldots \ldots . s_r)$............(11)

Applying r = n and N_0=N in (11) This gives the required formula.

EXAMPLE:

The product formula for Euler's totient can be derived from the cross-classification principle. Let $p_1, p_{2}, \ldots p_r$ denote the distinct prime divisors of n. Let s={1,2,3,.....n} and s_k be the subset of S consisting of those integers divisible by p_k. The numbers in S relatively prime to n are those in none of the sets $S_1, S_2, \ldots S_r$, So

$$\varphi(n) = \mathrm{N}(\mathrm{S} - \bigcup_{k=1}^{r} s_k)$$

If d|n there are n/d multiples of d in the set S. Hence

N(S_i)=$\frac{n}{p_i}$, N($S_i S_j$)=$\frac{n}{p_i p_j}$,..................N($S_1, S_2, \ldots S_r$)=$\frac{n}{p_1, p_2, \ldots p_r}$, so the cross classification principle gives us

$\varphi(n) = n - \sum_{i=1}^{n} \frac{n}{p_i} + \sum_{1\le i\le j\le r} \frac{n}{p_i p_j} -$ ....$+(-1)^r \frac{n}{p_1, p_2 \ldots p_r}$

Notes

$= n\sum_{d|n} \frac{\mu(d)}{d} = n\prod_{p|n}(1 - \frac{1}{p})$.

The next application of the cross-classification principle counts the number of elements in a reduced residue system mod k which belong to a given residue class r mod d, where d|k and (r, d) =1.

Theorem 13.3:

Given integers r, d and k such that d|k, d>0, k$\geq$ 1 and (r, d) =1. Then the number of elements in the set

$$S=\{r+td:t=1,2,......k/d\}$$

Which are relatively prime to k is $\frac{\varphi(k)}{\varphi(d)}$.

Proof:

If a prime p divides k and r+td then p∤d, otherwisep|r, contradicting the hypothesis (r, d) =1. Therefore, the primes which divide k and elements of S are those which divide k but do not divide d. Call them $p_1, p_2, ... p_m$ and let

$k'=p_1, p_2, ... p_m$

Then the elements of S are relatively prime to k are those not divisible by any of these primes. Let

$S_i=\{x:x\in S \text{ and } p_i|x\}$ (i=1,2,3......,m).

If x∈ S_i and x=r+td then r+td$\equiv 0(mod\ p_i)$. since $p_i \nmid d$ there is a unique mod $p_i$with this property, therefore exactly one t in each of the intervals $[1,p_i],[p_i+1, 2p_i],.......[(q-1)p_i+1,qp_i]$ where qp_i=k/d. Therefore $N(S_i)=\frac{k/d}{p_i}$.

Similarly,

$$N(S_iS_j)=\frac{\frac{k}{d}}{p_ip_j},..................N(S_1, S_2, ... S_m)=\frac{\frac{k}{d}}{p_1, p_2, ... p_m}$$

Hence by the cross-classification principle the number of integers in S which are relatively prime to k is

$$= \frac{k}{d}\sum_{\delta|k'} \frac{\mu(\delta)}{\delta} = \frac{k}{d}\prod_{p|k'}(1 - \frac{1}{p})=\frac{k\prod_{p|k}(1-\frac{1}{p})}{d\prod_{p|d}(1-\frac{1}{p})} =\frac{\varphi(k)}{\varphi(d)}.$$

13.5 A DECOMPOSITION PROPERTY OF REDUCED RESIDUE SYSTEMS:

As an application of foregoing theorems, we discuss a property of reduced residue system which will be used in a later chapter we begin with a numerical example.

Let S be a reduced residue system mod 15, say

S= {1,2,4,7,8,11}.

We display the 6 elements of S in a 3× 2 matrix as follows:

Notes

$$\begin{matrix} 1 & 2 \\ 4 & 8 \\ 7 & 11 \end{matrix}$$

Note that each row contains a reduced residue system mod 3 and the numbers in each column are congruent to each other mod 3. This example illustrates a general property of reduced residue described in following theorem.

Theorem 13.4:

Let S be a reduced residue system mod k and let d>0 be a divisor of k. Then we have the following decomposition of S:

a) S is the union of $\frac{\varphi(k)}{\varphi(d)}$ disjoint sets, each of which is reduced residue system mod d.

b) S is the union of $\varphi(d)$ disjoint sets, each of which consists of $\frac{\varphi(k)}{\varphi(d)}$ numbers congruent to each other mod d.

<u>Note:</u> In the foregoing examples, k=15 and d=3. the row matrix represents the disjoint set of part(a), and the column represents the disjoint set of part(b). If we apply them to the divisor d=5 we obtain the decomposition given by a matrix

$$\begin{matrix} 1 & 2 & 4 \\ 11 & 7 & 14 \end{matrix}$$

Each row is reduced residue system mod 5 and each column consists of numbers congruent to each other mod 5.

Proof:

First, we prove that the properties (a) and (b) are equivalent. If (b) holds we can display the $\varphi(k)$ element of s as a matrix using the $\varphi(d)$disjoint sets of (b) as columns. The matrix has $\frac{\varphi(k)}{\varphi(d)}$ rows. Each row contains a reduced system mod d, and these are the disjoint sets required for part (a). Similarly, it is easy to verify that (a) implies (b). Now we prove (b). Let S_d be a given reduced residue system mod d and suppose r∈ S_d. We will prove that there are at least $\frac{\varphi(k)}{\varphi(d)}$integers n in S distinct mod k, such that n≡ $r(mod\ d)$. Since there are $\varphi(d)$ values of r in S_d and $\varphi(k)$integers in S, there can't be more than $\frac{\varphi(k)}{\varphi(d)}$ such numbers in n, so this will prove part(b).

The required numbers n will be selected from the residue classes mod k represented by the following k/d integers:

Notes

$$r,\ r+d,\ r+2d, \ldots\ldots,\ r+\frac{k}{d}d.$$

These numbers are congruent to each other mod d and they are incongruent mod k. Since (r, d) =1, theorem 12.16 shows that $\frac{\varphi(k)}{\varphi(d)}$ of them are relatively prime to k, so this completes the proof.

13.6 EXERCISES:

1. Let n be a positive integer which is not a square. Prove that for every integer a is relatively prime to n there exists integers x and y satisfying

$ax \equiv y \pmod n$ with $0<x<\sqrt{n}$ and $0<|y|<\sqrt{n}$

2. Let p be a prime $p \equiv 1(mod\ 4)$ let q=(p-1)/2 and let a=q! Then prove that there exist positive integer x and y satisfying $0<x<\sqrt{p}$ and $0<y<\sqrt{p}$ such that $a^2x^2 - y^2 \equiv 0 \pmod p$.

3.For the x and y in (2) prove that $p=x^2+y^2$. This shows that every prime $p \equiv 1 \pmod 4$ is the sum of two squares.

4. prove that no prime $p \equiv 3 \pmod 4$ is the sum of two squares.

UNIT-XIV: QUADRATIC RESIDUES AND QUADRATIC RESIPROCITY LAW

Structure

14.1 Introduction:

Here we will introduce quadratic residues modulo an integer n.The quadratic residues of n are the integers which are squares modulo n. We will particularly study quadratic residues modulo an odd prime p. We will discuss Euler's criterion, which specifies when an integer is a quadratic residue modulo p. Whether an integer is a quadratic residue modulo p is indicated by a symbol called Legendre's symbol. We will also discuss properties of Legendre symbol.

14.2 Objectives

: The students will be able to

- Identify the Legendres symbol
- Determine the application of reciprocity Law
- Describe the applications of Diophantine equations

Definition14.1.1: Quadratic Residues:

Let p be an odd prime and $n \not\equiv 0 \pmod p$ consider the quadratic congruence $x^2 \equiv n \pmod p$. The value of n for which the congruence has a solution is called residues mod p(nRp) and those n for which the congruence has no solution is called quadratic non-residues mod p (n$\bar{R}$p).

Example:

1. To find the quadratic residues modulo 11.

Case 1:

Here p = 3, n = 1,2
$x^2 \equiv 1 \pmod 3$
$1^2 \equiv 1 \pmod 3$ has a solution 1R3
$x^2 \equiv 2 \pmod 3$ has no solution $2\bar{R}3$
Case 2:
Here p = 7, n = 1,2,3,4,5,6.
$x^2 \equiv 1 \pmod 7$ has a solution 1R7
$x^2 \equiv 2 \pmod 7$ has a solution 2R7
$x^2 \equiv 3 \pmod 7$ has no solution $3\bar{R}7$
$x^2 \equiv 4 \pmod 7$ has a solution 4R7
$x^2 \equiv 5 \pmod 7$ has no solution $5\bar{R}7$
$x^2 \equiv 6 \pmod 7$ has no solution $6\bar{R}7$.

P	3	5	7	11	13
nRp	1	1, 4	1, 2, 4	1, 3, 4, 5, 9	1,3,4,9,10,12
n$\bar{R}$p	2	2, 3	3, 5, 6	2, 6, 7, 8, 10	2, 5, 6,7, 8,11

Theorem: 14.1

Let p be an odd prime. Then every reduced residue system mod p contains exactly $\left(\frac{p-1}{2}\right)$ quadratic residues and exactly $\left(\frac{p-1}{2}\right)$ quadratic non-residue classes containing the numbers $1^2, 2^2, \ldots, \left(\frac{P-1}{2}\right)^2$.

Proof:

The reduced residue system mod p is $\{1, 2, .., \left(\frac{p-1}{2}\right), \ldots, p-1\}$

Claim:

The numbers $1^2, 2^2, \ldots, \left(\frac{P-1}{2}\right)^2$ are distinct (incongruent) mod p.

To prove that if $1 \le x, y \le \frac{p-1}{2}$ then $x^2 \not\equiv y^2 \pmod p$ for some $x \neq y$

Suppose $x^2 \equiv y^2 \pmod p$

$\Rightarrow x^2 - y^2 \equiv 0 \pmod p$

$\Rightarrow p \mid x^2 - y^2 \Rightarrow p \mid (x+y)(x-y)$

$\Rightarrow p \mid (x+y)$ or $p \mid (x-y)$

Since $1 \le x \le \frac{p-1}{2}$ and $1 \le y \le \frac{p-1}{2}$

$\therefore\ 2 \le x+y \le p-1 < p \Rightarrow x+y < p$

$\Rightarrow p \mid (x+y)$

Since $p \mid (x-y)$ and $0 \le |x-y| \le p-1 < p$

$\Rightarrow$ $x \equiv y \pmod p$

$\Rightarrow$ $x = y$

Which is contradiction to $x \neq y$

$\therefore x^2 \not\equiv y^2 \pmod p$

Thus, the numbers $1^2, 2^2, \ldots, \left(\frac{P-1}{2}\right)^2$ are congruent to mod p.

Hence the claim.

If k is a quadratic residue then

$(p-k)^2 = p^2 + k^2 + -2pk \equiv k^2 \pmod p$

$\therefore$ There are exactly $\left(\frac{p-1}{2}\right)$ quadratic residues and exactly $\left(\frac{p-1}{2}\right)$ quadratic non-residues mod p.

Hence the theorem.

14.3 Legendre's symbol and its property

Definition 14.1.2: Legendre's symbol

Let p be an odd prime. If $n \not\equiv 0 \pmod p$ we define the Legendre's symbol $(n \mid p)$ as follows

$$(n \mid p) = \begin{cases} 1 & if \ \ nRp \\ -1 & if \ \ n\bar{R}p \end{cases}$$

If $n \equiv 0 \pmod p$ then $(n \mid p) = 0$

Example:

Here $(1 \mid p) = 1$ if $x^2 \equiv 1 \pmod p$ (i.e.) $1Rp$

$(m^2 \mid p) = 1$ if $x^2 \equiv m^2 \pmod p$ (i.e.) mRp

$(2 \mid 5) = -1$ if $x^2 \equiv 2 \pmod 5$ (i.e.) $2\bar{R}5$

$(2 \mid 11) = -1$ if $x^2 \equiv 2 \pmod{11}$ (i.e.) $2\bar{R}11$

$(66 \mid 11) = 0$ if $x^2 \equiv 66 \pmod{11}$

Note:

Legendre's symbol is periodic function

$(m \mid p) = (n \mid p)$ whenever $m \equiv n \pmod p$ (i.e.) the Legendre's symbol is periodic with period p

Case 1: suppose $(m \mid p) = 1$

Consider quadratic congruence

$$x^2 \equiv m \pmod p \text{ has a solution}$$

since $x^2 \equiv m \pmod p$ and $m \equiv n \pmod p$

$\therefore x^2 \equiv n \pmod p$ (by transitive)

$(n \mid p) = 1$ has solution

Thus $(m \mid p) = (n \mid p)$

Case 2: $(m \mid p) = -1$

Consider quadratic congruence

$x^2 \equiv m \pmod p$ has no solution

since $x^2 \equiv m \pmod p$ and $m \equiv n \pmod p$

$\therefore x^2 \equiv n \pmod p$ (by transitive) has no solution

$\therefore$ $(n \mid p) = n\bar{R}p = -1$

Thus $(m \mid p) = (n \mid p)$

Thus, the Legendre's symbol is periodic with period p

Theorem: 14.2 Euler's Criterion

Let p be an odd prime then for all n we have $(n \mid p) \equiv n^{\frac{p-1}{2}} \ (mod\ p)$

Proof:

Case 1: If $(n \mid p) = 0 \Rightarrow n \equiv 0 \pmod p$

$\Rightarrow n^{\frac{p-1}{2}} \equiv 0 \pmod p$

$\Rightarrow n^{\frac{p-1}{2}} \equiv 0 \pmod p$

By symmetry $(n|p) \equiv n^{\frac{p-1}{2}} \pmod p$

Case 2: If $(n|p) = 1$ and $n \not\equiv 0 \pmod p$

The congruence $x^2 \equiv n \pmod p$ has solution (say "x_1")

$$x_1^2 \equiv n \pmod p$$

$n \equiv x_1^2 \pmod p$

$n^{\frac{p-1}{2}} \equiv (x_1^2)^{\frac{p-1}{2}} \pmod p$

$n^{\frac{p-1}{2}} \equiv (x_1)^{p-1} \pmod p$ (By Little Fermat theorem $a^p \equiv a \pmod p$)

$n^{\frac{p-1}{2}} \equiv 1$ (mod p)

$n^{\frac{p-1}{2}} \equiv (\, n \mid p)$ (mod p) (since (n | p) = 1)

By symmetry,

$(\, n \mid p) \equiv n^{\frac{p-1}{2}}$ (mod p)

Case 3: If (n|p) = -1 & n$\not\equiv$ 0 (mod p)

Consider the polynomial f(x) = $x^{\frac{p-1}{2}}$ -1 the deg (f(x)) = $\frac{P-1}{2}$

By Lagrange's theorem, the congruence f(x) ≡ 0 (mod p) has at most $\frac{P-1}{2}$ solutions.

It has $\frac{P-1}{2}$ quadratic residues mod p are solutions and $\frac{P-1}{2}$ quadratic non residues mod p is not solution.

$\therefore n^{\frac{p-1}{2}} \not\equiv 1$ (mod p) if (n|p) = -1

By Euler format theorem,

$n^{p-1} \equiv 1$ (mod p)

$n^{p-1} - 1 \equiv 0$ (mod p)

$(\, n^{\frac{p-1}{2}}-1)\,(\, n^{\frac{p-1}{2}}+1) \equiv 0$ (mod p)

Since $(\, n^{\frac{p-1}{2}}-1) \not\equiv 0$ (mod p)

$(\, n^{\frac{p-1}{2}}+1) \equiv 0$ (mod p)

$n^{\frac{p-1}{2}} \equiv (-1)$(mod p)

$n^{\frac{p-1}{2}} \equiv (n \mid p)$(mod p)

By symmetry, $(n \mid p) \equiv n^{\frac{p-1}{2}}$ (mod p)

Theorem: 14.3

Legendre symbol is completely multiplicative (i.e.) for all m, n, (mn|p) = (m|p)(n|p)

Proof:

Case 1: If m ≡ 0 (mod p), n ≡ 0 (mod p) then mn≡ 0 (mod p)

(i.e.) (m|p) = 0, (n|p) = 0 & (mn|p) = 0

∴ (mn|p) = (m|p) (n|p)

Case 2: If m $\not\equiv$ 0 (mod p), n $\not\equiv$ 0 (mod p) then mn $\not\equiv$ 0 (mod p)

Notes

By Euler criterion theorem,

(mn|p) ≡ $(mn)^{\frac{p-1}{2}}$ (mod p)

≡ $m^{\frac{p-1}{2}} n^{\frac{p-1}{2}}$ (mod p)

≡ $(m|p)(n|p)$ (mod p)

(mn|p)-$(m|p)(n|p)$ ≡ 0 (mod p)
(*)

Since the value of (m|p), (n|p) and (mn|p) are either 1 or -1

The value of (mn |p)-$(m|p)(n|p)$ are either 0 (or) 2 (or) -2

If (mn|p)-$(m|p)(n|p)$ = 2 (or) -2

Then 2 (or) -2 ≡ 0 (mod p) (from eqn *)

This is not true

∴(mn|p)-$(m|p)(n|p)$ = 0

⇒(mn|p) = $(m|p)(n|p)$

Note:

The Legendre symbol is also called the quadratic character (mod p) and it is denoted by $\chi(n)$ (i.e.) $\chi(n)$ = (n|p)

14.4 Evaluation of (-1|p) and (2|p)

Theorem: 14.4 Evaluation of (-1|p) and (2|p)

For every odd prime p, we have

$$(-1|p) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \ \ if \ \ p \equiv 1 \pmod 4 \\ -1 \ \ if \ \ p \equiv 3 \pmod 4 \end{cases}$$

Proof:

By Euler criterion,

$$(n|p) \equiv n^{\frac{p-1}{2}} \text{ (mod p)}$$

$$(-1|p) \equiv (-1)^{\frac{p-1}{2}} \text{ (mod p)}$$

$$(-1|p) - (-1)^{\frac{p-1}{2}} \equiv 0 \text{ (mod p)}$$

The value of $(-1|p)$&$(-1)^{\frac{p-1}{2}}$ are 1 (or) -1

The value of $(-1|p) - (-1)^{\frac{p-1}{2}}$ are 2 (or) -2 (or) 0

If $(-1|p) - (-1)^{\frac{p-1}{2}} = 2\ (or) - 2$

$$2\ (or) - 2 \equiv 0 \text{ (mod p)}$$

This is not true.

$$\therefore (-1|\text{p}) - (-1)^{\frac{p-1}{2}} = 0$$

$$(-1|\text{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \ if \ \ \text{p} \equiv \ 1 \text{ (mod 4)} \\ -1 \ if \ \ \text{p} \ \equiv \ 3 \text{ (mod 4)} \end{cases}$$

Theorem: 14.5

For every odd prime p, we have

$$(2|\text{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \ if \ \ \text{p} \equiv \pm 1 \text{ (mod 8)} \\ -1 \ if \ \ \text{p} \ \equiv \pm \ 3 \text{ (mod 8)} \end{cases}$$

Proof:

$$\text{p-1} \equiv -1 \text{ (mod p)} \equiv (-1).1 \text{ (mod p)}$$

$$2 \equiv 2 \text{ (mod p)} \equiv (-1)^2.2 \text{ (mod p)}$$

$$\text{p-3} \ \equiv -3 \text{ (mod p)} \equiv (-1)^3.3 \text{(mod p)}$$

$$4 \equiv 4 \text{ (mod p)} \equiv (-1)^4.4 \text{(mod p)}$$

$$\text{r} \equiv \frac{P-1}{2} \text{(mod p)} \equiv (-1)^{\frac{p-1}{2}}.\frac{P-1}{2} \text{(mod p)}$$

where r is either $\frac{P-1}{2}$ or p - $\frac{P-1}{2}$ $=$ $\frac{P+1}{2}$multiplying vertically we get

$$2.4.6\ldots(\text{p-3})\ (\text{p-1}) \equiv (-1)^{1+2+\cdots+\frac{P-1}{2}}.[1.2.3 \ldots \frac{P-1}{2}] \text{ (mod p)}$$

$$2^{\frac{P-1}{2}}[1.2.3 \ldots \frac{p-1}{2}] \equiv \ (-1)^{\frac{(p-1)(p+1)}{8}} \left(\frac{p-1}{2}\right)! \text{ (mod p)}$$

$$2^{\frac{P-1}{2}}[1.2.3 \ldots \frac{p-1}{2}] \equiv \ (-1)^{\frac{(p-1)(p+1)}{8}} \left(\frac{p-1}{2}\right)! \text{ (mod p)}$$

$$2^{\frac{P-1}{2}}.(\frac{p-1}{2})! \equiv \ (-1)^{\frac{p^2-1}{8}}.\left(\frac{p-1}{2}\right)! \text{ (mod p)}$$

Cancel $\left(\frac{P-1}{2}\right)!$ on both sides we get

$$2^{\frac{p-1}{2}} \equiv \ (-1)^{\frac{p^2-1}{8}} \text{(mod p)} \longrightarrow (1)$$

By Euler Criterion theorem,

$$(\text{n}\ |\text{p}) \equiv \ n^{\frac{p-1}{2}} \text{(mod p)}$$

$$\Rightarrow (2|\text{p}) \equiv \ 2^{\frac{p-1}{2}} \text{(mod p)} \longrightarrow (2)$$

Notes

From equation (1) & (2) we get

$$(2|p) \equiv (-1)^{\frac{p^2-1}{8}} (\text{mod } p)$$

$$(2|p) - (-1)^{\frac{p^2-1}{8}} \equiv 0 (\text{mod } p)$$

The values of (2|p) and $(-1)^{\frac{p^2-1}{8}}$ are either -1 (or) 1 and they simultaneously take same values,

Otherwise p|2

$\therefore$ $(2|p) = (-1)^{\frac{p^2-1}{8}}$

Case 1: Now $(-1)^{\frac{p^2-1}{8}} = 1$ if $\frac{p^2-1}{8}$ is an even say 2k

$\Rightarrow$ $p^2 - 1 = 16k$

$\Rightarrow$ $(p-1)(p+1) = 16k$

Since p is an odd prime $\Rightarrow$ either (p-1) or (p+1) is a multiple of 4 and the other is even.

(i.e.) $(p-1)(p+1) \equiv 0 \ (\text{mod } 8)$

$$(ie) \qquad p \equiv \pm 1 \ (\text{mod } 8)$$

Case 2: $(-1)^{\frac{p^2-1}{8}} = -1$ if $\frac{p^2-1}{8}$ is an odd say 2k+1

$\Rightarrow$ $p^2 - 1 = 16k + 8$

$\Rightarrow$ $p^2 - 9 = 16k$

$\Rightarrow$ $(p+3)(p-3) = 16k$

Since p is an odd prime $\Rightarrow$ either (p-3) or (p+3) is a multiple of 4 and the other is even

(i.e.) $(p+3)(p-3) \equiv 0 \ (\text{mod } 8)$

$$(ie) p \equiv \pm 3 \ (\text{mod } 8)$$

$$(2|p) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \ \ if \ \ p \equiv \pm 1 \ (\text{mod } 8) \\ -1 \ \ if \ \ p \equiv \pm 3 \ (\text{mod } 8) \end{cases}$$

14.5 Gauss Lemma

Theorem:14.6 (Gauss Lemma)

Assume $n \not\equiv 0$ (mod p) and consider the least positive residues mod p of the following $(\frac{p-1}{2})$ multiplies of n: n, 2n, 3n,…, $(\frac{p-1}{2})n$. If m denotes the number of these residues which exceeds p|2, then $(n|p) = (-1)^m$

Proof:

Claim 1: The numbers n, 2n, 3n, …, $(\frac{p-1}{2})n$ are incongruence to mod p

Suppose in ≡ jn (mod p), for i≠ j, 1≤ i, j ≤ $\frac{p-1}{2}$

$$\Rightarrow \text{in} - jn \equiv 0 \pmod p$$

$$\Rightarrow (\text{i} - j)n \equiv 0 \pmod p$$

$\Rightarrow (\text{i} - j) \equiv 0 \pmod p$ ($\because$ n $\not\equiv$ 0 (mod p))

$\Rightarrow \; i = j$ ($\because 0 < |\text{i-j}| \leq \frac{p-1}{2}$)

Which is a contradiction to i≠ j

∴ The numbers n, 2n, 3n, …, $(\frac{p-1}{2})n$ are incongruence to mod p

Let A = $\{a_1, a_2, a_3, \ldots, a_k\}$, where each $a_i \equiv tn \pmod p$ for $1 \leq t \leq \frac{p-1}{2}$ & $0 < a_i < \frac{p}{2}$

& B = $\{b_1, b_2, b_3, \ldots, b_m\}$, where each $b_j \equiv sn \pmod p$ for $1 \leq s \leq \frac{p-1}{2}$ & $\frac{p}{2} < b_j < p$

∴$m+k = \frac{p-1}{2}$ (since A and B are disjoint)

Let C = $\{c_1, c_2, c_3, \ldots, c_m\}$ `where $c_j = p - b_j$

Now, $\frac{p}{2} < b_j < p$

$\Rightarrow -\frac{p}{2} > -b_j > -p$

$\Rightarrow p - \frac{p}{2} > p - b_j > p - p$

$\Rightarrow \frac{p}{2} > c_j > 0$

$\Rightarrow 0 < c_j < -\frac{p}{2}$

Claim (2): $A \cap C = \emptyset$

Let $c_j = a_j$ some pair i& j

$\Rightarrow p - b_j = a_j$

$\Rightarrow a_i + b_j = p$

$\Rightarrow tn + sn = p$

$\Rightarrow (t + s)n = p$

Since p≡ 0(mod p)

$\Rightarrow (t + s)n \equiv 0 (\text{mod p})$

We get a contradiction ($\because (t + s) \not\equiv 0 (\text{mod p})$)

Notes

$\therefore A \cap C = \emptyset$

(i.e.) $A \cup C$ has m+k elements in the interval $[1, \frac{p-1}{2}]$

$$\therefore A \cup C = \{1, 2, \ldots, \frac{p-1}{2}\}$$

But $A \cup C = \{a_1, a_2, a_3, \ldots, a_k, c_1, c_2, c_3, \ldots, c_m\}$`

Taking product on both sides,

$1.2.3 \ldots \frac{p-1}{2} = a_1 . a_2 . a_3 \ldots, a_k . c_1 . c_2 . c_3 \ldots . c_m$

$(\frac{p-1}{2})! = a_1 . a_2 . a_3 \ldots, a_k . (p - b_1) . (p - b_2) \ldots (p - b_m).$

$(\frac{p-1}{2})! \equiv a_1 . a_2 . a_3 \ldots, a_k (-1)^m . b_1 . b_2 \ldots b_m . (\text{mod p})$

$\equiv (-1)^m a_1 . a_2 . a_3 \ldots, a_k . b_1 . b_2 \ldots b_m . (\text{mod p})$

$\equiv (-1)^m n, 2n, 3n, \ldots, (\frac{p-1}{2})n (\text{mod p})$

$\equiv (-1)^m n^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! (\text{mod p})$

Since p does not divides $\left(\frac{p-1}{2}\right)!$

By cancellation law, we get,

$$1 \equiv (-1)^m n^{\frac{p-1}{2}} (\text{mod p})$$

x $(-1)^m \Rightarrow (-1)^m \equiv (-1)^{2m} n^{\frac{p-1}{2}} (\text{mod p})$

$\Rightarrow (-1)^m \equiv n^{\frac{p-1}{2}} (\text{mod p})$

By Euler criterion theorem, we get,

$n^{\frac{p-1}{2}} \equiv (n|p) (\text{mod p})$

By equivalence relation,

$\Rightarrow (n|p) \equiv (-1)^m (\text{mod p})$

Since the values of $(-1)^m$ & $(n|p)$ are takes 1 or -1 and they simultaneously take same value otherwise $\frac{p}{2}$

$\therefore \quad (n|p) = (-1)^m$

Theorem: 14.7

Let m be the number defined in Gauss lemma then

$$m \equiv \sum_{t=1}^{\frac{P-1}{2}} [\frac{tn}{p}] + (n-1)\ \frac{p^2-1}{8} \pmod 2$$

In particular if n is odd, then

$$m \equiv \sum_{t=1}^{\frac{P-1}{2}} [\frac{tn}{p}] \pmod 2$$

Proof:

Let m be the number of least positive residue of the numbers which exceed $\frac{p}{2}$

Consider the multiple of n (say) (t.n) where $1 \leq t \leq \frac{p-1}{2}$

Now,

$$\frac{tn}{p} = \left[\frac{tn}{p}\right] + \{\frac{tn}{p}\},\ 0 < \{\frac{tn}{p}\} < 1$$

$$\Rightarrow \quad tn = p\left[\frac{tn}{p}\right] + p\{\frac{tn}{p}\}$$

$$\Rightarrow \quad tn = p\left[\frac{tn}{p}\right] + r_t,\ 0 < r_t < p$$

$$\Rightarrow \quad r_t = tn - p\left[\frac{tn}{p}\right] \longrightarrow (1)$$

By Gauss lemma,

$A \cup B = \{a_1, a_2, a_3, \ldots, a_k, b_1, b_2, b_3, \ldots, b_m\}$

$= \{r_1, r_2, \ldots, r_{\frac{p-1}{2}}\}$

$A \cup C = \{a_1, a_2, a_3, \ldots, a_k, c_1, c_2, c_3, \ldots, c_m\}$

$= \{1, 2, \ldots, \frac{p-1}{2}\}$ where $c_j = p - b_j$

Adding $A \cup B$ we get

$$\sum_{t=1}^{\frac{P-1}{2}} r_t = \sum_{t=1}^{k} a_i + \sum_{t=1}^{m} b_j$$

$$\Rightarrow \sum_{t=1}^{\frac{P-1}{2}} \left(tn - p\left[\frac{tn}{p}\right]\right) = \sum_{t=1}^{k} a_i + \sum_{t=1}^{m} b_j$$

$$\Rightarrow n\sum_{t=1}^{\frac{P-1}{2}} t - p\sum_{t=1}^{\frac{P-1}{2}} \left[\frac{tn}{p}\right] = \sum_{t=1}^{k} a_i + \sum_{t=1}^{m} b_j$$

$$\Rightarrow n[1 + 2 + \cdots + \frac{p-1}{2}] - p\sum_{t=1}^{\frac{P-1}{2}} \left[\frac{tn}{p}\right] = \sum_{t=1}^{k} a_i + \sum_{t=1}^{m} b_j$$

$$\Rightarrow n\left(\frac{p^2-1}{8}\right) - p\sum_{t=1}^{\frac{P-1}{2}} \left[\frac{tn}{p}\right] = \sum_{t=1}^{k} a_i + \sum_{t=1}^{m} b_j \longrightarrow (2)$$

Notes

Adding $A \cup C$, we get

$$1 + 2 + \cdots + \frac{p-1}{2} = \sum_{t=1}^{k} a_i + \sum_{t=1}^{m} c_j$$

$$\frac{p^2-1}{8} = \sum_{t=1}^{k} a_i + \sum_{t=1}^{m} (p - b_j)$$

$$= \sum_{t=1}^{k} a_i + \sum_{t=1}^{m} p - \sum_{t=1}^{m} b_j \longrightarrow (3)$$

(2) + (3)

$$(n+1)\left(\frac{p^2-1}{8}\right) - p\sum_{t=1}^{\frac{P-1}{2}} \left[\frac{tn}{p}\right] = 2\sum_{t=1}^{k} a_i + mp$$

$$mp = (n+1)\left(\frac{p^2-1}{8}\right) - p\sum_{t=1}^{\frac{P-1}{2}} \left[\frac{tn}{p}\right] - 2\sum_{t=1}^{k} a_i \longrightarrow (4)$$

we know that

$(n+1) \equiv (n-1) \pmod 2$ and $p \equiv \pm 1 \pmod 2$

Taking (mod 2) to equation (4)

$$m \equiv (n-1)\left(\frac{p^2-1}{8}\right) + \sum_{t=1}^{\frac{P-1}{2}} \left[\frac{tn}{p}\right] \pmod 2$$

In particular, if n is odd, (n-1) is even

$$m \equiv \sum_{t=1}^{\frac{P-1}{2}} \left[\frac{tn}{p}\right] \pmod 2$$

Hence the theorem.

Theorem: 14.8 **<u>Quadratic reciprocity law:</u>**

If p and q are distinct odd primes then $(p|q)\,(q|p) = (-1)^{\frac{(p-1)(q-1)}{4}}$

Proof:

By Gauss lemma and the previous theorem, we have

$$(q|p) = (-1)^m \quad \text{where} \quad m \equiv \sum_{t=1}^{\frac{P-1}{2}} \left[\frac{tq}{p}\right] \pmod 2$$

Similarly $(p|q) = (-1)^n$ where $n \equiv \sum_{s=1}^{\frac{q-1}{2}} \left[\frac{sp}{q}\right] \pmod 2$

Thus $(p|q)\,(q|p) = (-1)^{m+n}$

Claim: $m+n = \frac{(p-1)(q-1)}{4}$

(ie) to $\sum_{t=1}^{\frac{P-1}{2}}[\frac{tq}{p}] + \sum_{s=1}^{\frac{q-1}{2}}[\frac{sp}{q}] = \frac{(p-1)(q-1)}{4}$

Consider f (x, y) = qx-py

If x and y are non-zero integers then f(x,y) is a non-zero integers

As x takes the values 1, 2,…,$\frac{P-1}{2}$& y takes the values 1, 2,…,$\frac{q-1}{2}$ for a fixed x we have,

f (x, y) > 0 ⇔ qx-py > 0 ⇔ y <$\frac{q}{p}x$ (or) y ≤ $[\frac{q}{p}x]$

∴ The total number of positive values of

$$f (x, y) = \sum_{x=1}^{\frac{P-1}{2}}[\frac{qx}{p}]$$

for a fixed-point y,

f (x, y) < 0 ⇔ qx-py < 0

⇔ qx < py

⇔ x ≤ $[\frac{py}{q}]$

∴ The total number of negative values of

$$f (x, y) = \sum_{y=1}^{\frac{q-1}{2}}[\frac{py}{q}]$$

Thus, total number of positive and negative values of

$$f (x, y) = \sum_{x=1}^{\frac{P-1}{2}}[\frac{qx}{p}] + \sum_{y=1}^{\frac{q-1}{2}}[\frac{py}{q}]$$

But, the total number of positive and negative values of f (x, y) is $(\frac{p-1}{2})(\frac{q-1}{2}) = \frac{(p-1)(q-1)}{4}$

Thus,

$$\frac{(p-1)(q-1)}{4} = \sum_{x=1}^{\frac{P-1}{2}}[\frac{qx}{p}] + \sum_{y=1}^{\frac{q-1}{2}}[\frac{py}{q}]$$

$$\frac{(p-1)(q-1)}{4} = m+n$$

$$(-1)^{\frac{(p-1)(q-1)}{4}} = (-1)^{m+n}$$

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

$$= (p|q)\ (q|p)$$

$\therefore$ (p|q) (q|p) = $(-1)^{\frac{(p-1)(q-1)}{4}}$

Note:

Quadratic reciprocity law can also be written as

$$(q|p) = (p|q)\ (-1)^{\frac{(p-1)(q-1)}{4}}$$

14.7 Applications of Quadratic Reciprocity Law

Example:1

Determine whether 219 is quadratic residue or not residue (383)

Solution:

219 = (3× 73| 383) = (3|383)(73|383) (∵Legendre symbol is completely multiplicative)

(3|383) = (383|3) $(-1)^{\frac{(3-1)(383-1)}{4}}$ (By quadratic reciprocity law)

= (383|3) $(-1)^{\frac{(2)(382)}{4}}$

= (383|3) $(-1)^{191}$

= (383|3) (-1)

= -(383|3) (Legendre symbol is periodic with p)

= -(2|3) (∵ 383 ≡ 2 (mod 3))

= - $(-1)^{\frac{9-1}{8}}$ (using theorem 14.5 (2|p) = $(-1)^{\frac{p^2-1}{8}}$)

= 1

Now,

(73|383) = (383|73) $(-1)^{\frac{(73-1)(383-1)}{4}}$ (By quadratic reciprocity law)

= (383|3) $(-1)^{\frac{(72)(382)}{4}}$

= (383|3) $(-1)^{6876}$

= (383|73)

= (18|73) (Legendre symbol is periodic with p)

= (18|73) (∵ 383 ≡ 18 (mod 73))

= (2 ×9|73)

= (2 |73) (9|73)

= (2 |73) (1)

$= \ (-1)^{\frac{5329-1}{8}}$ (using theorem 14.5 (2|p) = $(-1)^{\frac{p^2-1}{8}}$)

= 1

∴ (219|383) = (3|383) (73|383)

= 1 ×1

= 1

∴ 219 is a quadratic residue (mod 383)

Example:2

Determine those odd prime p for which 3 is a quadratic residue or non-residue**.**

Solution:

By Quadratic reciprocity law,

$$(q|p) = (p|q)\ (-1)^{\frac{(p-1)(q-1)}{4}}$$

$$(3|p) = (p|3)\ (-1)^{\frac{(p-1)(2)}{4}}$$

$$(3|p) = (p|3)\ (-1)^{\frac{p-1}{2}} \quad (1) \longrightarrow$$

To determine (p|3),

We need to know the value of p (mod 3), and to determine $(-1)^{\frac{p-1}{2}}$, we need to know the value of

$(\frac{p-1}{2})$ mod 2 or the value of p mod 4,

Hence, we consider p (mod 12)

∴ p ≡ 1,5,7 and 11 (mod 12) (∵ p is odd)

Case 1: let p ≡ 1(mod 12)

In this case p ≡ 1 (mod 3), p ≡ 1(mod 4)

So (p|3) = (1/3) = 1 $\longrightarrow$ (2)

Also, p ≡ 1 (mod 4)

So $(\frac{p-1}{2})$ is even, $(-1)^{\frac{p-1}{2}} = 1$ $\longrightarrow$ (3)

Hence p ≡ 1 (mod 3)

Substitute (2) and (3) in (1)

⇒ (3|p) = 1

∴ 3 is quadratic residue mod 1

Case 2 : let p ≡ 5 (mod 12)

p ≡ 5 (mod 3) p ≡ 5 (mod 4)

In this case

p ≡ 2 (mod 3) p ≡ 1 (mod 4)

so (p|3) = (2|3) = $(-1)^{\frac{3^2-1}{8}}$

= -1

Also, p ≡ 5 (mod 4) ⇒ p ≡ 1 (mod 4)

From (3), $(-1)^{\frac{p-1}{2}}$ = 1

From (1), (3|p) = (1) (-1) = -1

3 is non-residues mod 5

Case 3: let p ≡ 7 (mod 12)

p ≡ 7 (mod 3) & p ≡ 7 (mod 4)

In this case

p ≡ 1 (mod 3) p ≡ 3 (mod 4)

so (p|3) = (1|3) = 1

Also, p ≡ 7 (mod 4) ⇒ p ≡ 3 (mod 4)

⇒ p-1 ≡ 2 (mod 4)

⇒ $\frac{p-1}{2}$ ≡ 1 (mod 2)

⇒ $\frac{p-1}{2}$ - 1 ≡ 0 (mod 2)

⇒ $\frac{p-1}{2}$ – 1 = 2k

⇒ $\frac{p-1}{2}$ = 2k + 1

∴ ($\frac{p-1}{2}$) is odd

Hence $(-1)^{\frac{p-1}{2}}$ = -1

From (1), (3|p) = 1. (-1) = -1

∴ 3 is non-residue mod 7

Case 4: let p ≡ 11 (mod 12)

p ≡ 11 (mod 3) & p ≡ 11 (mod 4)

In this case

p ≡ 2 (mod 3) p ≡ 3 (mod 4)

so (p|3) = (2|3) = -1

Also, p ≡ 11 (mod 4) ⇒ p ≡ 3 (mod 4)

As the case above ($\frac{p-1}{2}$) is odd ⇒ $(-1)^{\frac{p-1}{2}}$ = -1

From (1), (3|p) = (-1). (-1) = 1

∴ 3 is quadratic residue mod 11

Summarizing the result of the four cases we find

$$3Rp \ \ if \ \ \text{p} \equiv \pm 1 \text{ (mod 12)}$$

$$3\bar{R}p \ \ if \ \ \text{p} \equiv \pm\ 5 \text{ (mod 12)}$$

14.8 Jacobi symbol:

If p is a positive odd integer with prime factorization

P = $\prod_{i=1}^{r} p_i{}^{a_i}$ we have to define the Jacobi symbol for any integer ‘n’,

$$(\text{n}|\text{P}) = \prod_{i=1}^{r}(n|p_i)^{a_i} \longrightarrow (*)$$

where $(n|p_i)$ is Legendre symbol

Note:

Define (n|1) = 1 and (n|p) is called a Jacobi symbol.

Remark:

The values of (n|p) are either 1, -1 (or) 0. (n|p) = 0 with (n, p) > 1.

If the congruence x^2 ≡ n (mod p) has a solution then (($n|p_i$) = 1 for each prime p_i, in (*) and hence (n|p) = 1

However, converse is not true.

Since (n|p) = 1 if an even number of factors -1 appears in (*).

Theorem: 14.9

If P and Q are positive odd integers, we have

(a) (m|P) (n|P) = (mn|P)
(b) (m|P) (m|Q) = (mn|PQ)
(c) (m|P) = (n|P) whenever m ≡ n (mod p).
(d) $(a^2n|P)$ = (n|P) whenever (a, P) = 1

Proof:

Let P = $\prod_{i=1}^{r} p_i{}^{a_i}$ where $p_i's$ are odd prime

Now,

(a) $(m|P)\ (n|P) = \{\prod_{i=1}^{r}(m|p_i)^{a_i}\}\{\prod_{1=1}^{r}(n|p_i)^{a_i}\}$

$= \prod_{i=1}^{r}[(m|p_i)^{a_i}\,(n|p_i)^{a_i}]$

$= \prod_{i=1}^{r}[(m|p_i)(n|p_i)]^{a_i}$

$= \prod_{i=1}^{r}[(mn|p_i)]^{a_i}$

$= (mn|P)$

(ie) $(m|P)\ (n|P) = (mn|P)$

$\therefore$ Jacobi symbol is completely multiplicative.

(b) let $P = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_t^{\alpha_t}p_{t+1}^{\alpha_{t+1}}\dots p_r^{\alpha_r}$

$Q = p_t^{\beta_t}p_{t+1}^{\beta_{t+1}}\dots p_r^{\beta_r}\dots p_s^{\beta_s}$

Where $p_i's$ are odd prime and not necessarily distinct

Now, $(m|P) = (m|p_1^{\alpha_1})\ (m|p_2^{\alpha_2})\dots(m|p_t^{\alpha_t})\ (m|p_{t+1}^{\alpha_{t+1}})\dots(m|p_r^{\alpha_r})$

$(m|Q) = (m|\,p_t^{\beta_t})\ (m|p_{t+1}^{\beta_{t+1}})\dots(m|p_r^{\beta_r})\dots(m|p_s^{\beta_s})$

Then,

$(m|P)\ (m|Q) =$
m|
$p_1^{\alpha_1})\ (m|p_2^{\alpha_2})\dots(m|p_t^{\alpha_t})\ (m|p_{t+1}^{\alpha_{t+1}})\dots(m|p_r^{\alpha_r})(m|\,p_t^{\beta_t}).$

$(m|p_{t+1}^{\beta_{t+1}})\dots(m|p_r^{\beta_r})\dots(m|p_s^{\beta_s})$

$= (m|\,p_1^{\alpha_1}p_2^{\alpha_2}\dots p_t^{\alpha_t+\beta_t}p_{t+1}^{\alpha_{t+1}+\beta_{t+1}}\dots p_r^{\alpha_r+\beta_r}\dots\ p_s^{\beta_s})$

$= (m|PQ)$

$(m|P)\ (m|Q) = (m|PQ)$

(c) $P = \prod_{i=1}^{r} p_i^{a_i}$

Given that $m \equiv n \pmod P$

$$\Rightarrow P|\ m-n$$

$$\Rightarrow p_1^{a_1}p_2^{a_2}\dots p_t^{a_t}|\ m-n$$

$$\Rightarrow p_i^{a_i}|\ m-n\forall\ i$$

$$\Rightarrow p_i|\ m-n\forall\ i$$

$\therefore m \equiv n \pmod{p_i}\forall\ i$ (using Legendre symbol is periodic)

$$\Rightarrow (m|p_i) = (n|p_i)$$

$(m|P) = \prod_{i=1}^{r}(m|p_i)^{a_i}$

Notes

$= \prod_{i=1}^{r}(n|p_i)^{a_i}$

= (n|P)

∴ (m|P) = (n|P) whenever $m \equiv$ n (mod P)

(d) $(a^2n|P) = (a^2|P)$ (n|P) $\longrightarrow$ (1) (By (a))

P = $\prod_{i=1}^{r} p_i{}^{a_i}$ where $p_i's$ are odd prime not necessarily distinct prime

Now, we have to prove that $(a^2|P)$ = 1

Since (a, P) = 1 ⇒ P *does not divides* a

⇒ a ≢ 0 (mod P)

$\therefore x^2 \equiv a^2$ (mod P) has a solution

$\therefore a^2\ Rp \ \Rightarrow (a^2, P) = 1$

Theorem:14.10

If P is an odd positive integer, we have

(a) (-1|P) = $(-1)^{\frac{p-1}{2}}$

(b) (2|P) = $(-1)^{\frac{p^2-1}{8}}$

Proof:

(a) letP = $\prod_{i=1}^{m} p_i$ where $p_i's$ are odd prime not necessarily distinct prime

$= \prod_{i=1}^{m}(1 + p_i - 1)$

$= (1 + p_1 - 1)(1 + p_2 - 1) \ldots (1 + p_m - 1)$

P = 1+ $\sum_{i=1}^{m}(p_i - 1) + \sum_{i \neq j}(p_i - 1)(p_j - 1) + \cdots$

Since each $p_i's$ are odd ⇒ $p_i - 1$ is an even taking mod 4, we get

P ≡1+ $\sum_{i=1}^{m}(p_i - 1)$ (mod 4)

P -1≡ $\sum_{i=1}^{m}(p_i - 1)$ (mod 4)

$\frac{P-1}{2} \equiv \sum_{i=1}^{m} \frac{(p_i-1)}{2}$ (mod 4)

$\sum_{i=1}^{m} \frac{(p_i-1)}{2} = \frac{P-1}{2} + 2k$ for some integer k.

Now, (-1|P) = $\prod_{i=1}^{m}(-1|p_i)$

$= \prod_{i=1}^{m} (-1)^{\frac{p_i-1}{2}}$

Notes

$$= (-1)^{\sum_{i=1}^{m} \frac{(p_i-1)}{2}}$$

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

$$= (-1)^{\frac{P-1}{2}}.(-1)^{2k}$$

$$= (-1)^{\frac{P-1}{2}}$$

$\therefore$ (-1|P) = $(-1)^{\frac{P-1}{2}}$

(b) let $P^2 = \prod_{i=1}^{m} {p_i}^2$

$= \prod_{i=1}^{m} (1 + {p_i}^2 - 1)$

$= (1 + {p_1}^2 - 1)(1 + {p_2}^2 - 1) \ldots (1 + {p_m}^2 - 1)$

P = 1+ $\sum_{i=1}^{m}({p_i}^2 - 1) + \sum_{i \neq j}({p_i}^2 - 1)({p_j}^2 - 1) + \cdots$

Since each $p_i' s$ are odd $\Rightarrow$ ${p_i}^2 - 1$ is an even

We have ${p_i}^2 - 1 \equiv 0 \ (mod\ s)$

Taking mod 64, we get

$P^2 \equiv 1 + \sum_{i=1}^{m}({p_i}^2 - 1)$ (mod 64)

$P^2 - 1 \equiv \sum_{i=1}^{m}({p_i}^2 - 1)$ (mod 64)

$P^2 - 1 \equiv \sum_{i=1}^{m}({p_i}^2 - 1)$ (mod 64)

$\frac{P^2-1}{8} \equiv \sum_{i=1}^{m}(\frac{{p_i}^2-1}{8})$ (mod 8)

$\sum_{i=1}^{m}(\frac{{p_i}^2-1}{8}) = \frac{P^2-1}{8}$ + 8k for some integer k

Now,

(2|P) = $\prod_{i=1}^{m}(2|p_i)$

$$= \prod_{i=1}^{m} (-1)^{\frac{{p_i}^2-1}{8}}$$

$$= (-1)^{\sum_{i=1}^{m} \frac{{p_i}^2-1}{8}}$$

$$= (-1)^{\frac{{p_i}^2-1}{8}+8k}$$

$$= (-1)^{\frac{{p_i}^2-1}{8}}.(-1)^{8k}$$

$$= (-1)^{\frac{{p_i}^2-1}{8}}$$

$\therefore$ (2|P) = $(-1)^{\frac{{p_i}^2-1}{8}}$

Hence the theorem.

Theorem: 14.11

Reciprocity law for Jacobi symbol. If P and Q are positive odd integers with (P, Q) = 1 then

$$(P|Q)\,(Q|P) = (-1)^{\frac{(P-1)(Q-1)}{4}}$$

Proof:

Since (P, Q) = 1

Let P = $p_1, p_2, \ldots p_m$ where $p_i's$ and $q_j's$ are distinct primes

Q = $q_1, q_2, \ldots q_n$

Then (P|Q) = $\prod_{i=1}^{m} \prod_{j=1}^{n} (p_i|q_j)$

(Q|P) = $\prod_{j=1}^{n} \prod_{i=1}^{m} (q_j|p_i)$

(P|Q)(Q|P) = $\prod_{i=1}^{m} \prod_{j=1}^{n} (p_i|q_j)\,(q_j|p_i)$

$$= \prod_{i=1}^{m} \prod_{j=1}^{n} (-1)^{\frac{(p_i-1)(q_j-1)}{4}}$$

$$= (-1)^{\sum_{i=1}^{m} \frac{(p_i-1)}{2} \sum_{j=1}^{n} \frac{(q_i-1)}{2}}$$

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

$$= (-1)^{\frac{(P-1)(Q-1)}{4}} . (-1)^{4k}$$

$$= (-1)^{\frac{{p_i}^2-1}{8}}$$

$\therefore$ (P|Q) (Q|P) = $(-1)^{\frac{(P-1)(Q-1)}{4}}$

Hence the theorem.

Example:1

Determine whether -104 is a quadratic residue or non-residue of the prime 997.

Solution:

Since 104 = 2.4.13

(-104|997) = (-1|997) (2|997) (4|997) (13|997)

= - (13|997)

= - (997|13)

= - (9|13)

= - (1)

Thus -104 is a quadratic non-residue mod 997.

14.9 Applications to Diophantine equation:

Equations to be solve in integers are called Diophantine equation.

The equation $y^2 = x^3 + k$ where k is the given integer is the example of Diophantine equation.

Now, we have to find for a given k whether or not equation has integer solution x, y and if so we exhibit them.

Theorem:14.12

The Diophantine equation $Y^2 = x^3 + k$ has no solution if k has the form

k = $(4n - 1)^3 - 4\, m^2$ Where m and n are integer such that no prime

P ≡ (-1) (mod 4) divides m.

Proof:

Assume that the Diophantine equation has solution.

k = $(4n - 1)^3 - 4\, m^2$

Taking mod 4 we get,

k ≡ (-1) (mod 4)

the Diophantine equation becomes,

$Y^2 \equiv x^3 - 1 \pmod 4 \longrightarrow (1)$

For any 'y', $y^2 \equiv 0\ (or)\ 1 \pmod 4$

If x is even, then $x^3 \equiv 0 \pmod 4$

If $x \equiv -1 \pmod 4$ then $x^3 \equiv -1 \pmod 4$

The equation (1) is not satisfied

Notes

If $x \equiv 1 \pmod 4$ then $x^3 \equiv 1 \pmod 4$

So that $Y^2 \equiv x^3 - 1 \pmod 4$ satisfied

$\therefore x \equiv 1 \pmod 4$

Let a = 4n-1 then $a \equiv -1 \pmod 4$

Now, k = $(4n-1)^3 - 4\,m^2$

$= a^3 - 4\,m^2$

The equation $y^2 = x^3 + k$ becomes

$$y^2 = x^3 + a^3 - 4\,m^2$$

$$y^2 + 4\,m^2 = x^3 + a^3$$

$y^2 + 4\,m^2 = (x+a)\,(a^2 - ax + x^2)$

Consider, $(a^2 - ax + x^2) \equiv x^2 + x + 1 \pmod 4$

$\equiv 1 + 1 + 1 \pmod 4$

$\equiv -1 \pmod 4$

$(a^2 - ax + x^2) \equiv -1 \pmod 4$

$\therefore$ $a^2 - ax + x^2$ is an odd and there exists one prime divisor $\equiv -1 \pmod 4$

(i.e.) all prime divisors cannot be $\equiv 1 \pmod 4$

Let p be a prime such that p $\equiv -1 \pmod 4$ that divides $a^2 - ax + x^2$

(i.e.) p| $y^2 + 4\,m^2$

$\Rightarrow$ $y^2 + 4\,m^2 \equiv 0 \pmod 4$

$\Rightarrow$ $y^2 \equiv -4\,m^2 \pmod 4$

But p does not divides m

Since, $(-4\,m^2|\mathrm{p})$ = (-1|p) (4|p) (m^2|p)

= (-1|p)

$\therefore$ $(-4\,m^2|\mathrm{p}) = -1$ which is contradiction

The equation $y^2 = x^3 + k$ has no solution if k = $(4n-1)^3 - 4\,m^2$

14.10 Exercise:

1. Determine whether 888 is quadratic residue or non-residue of the prime 1999.

2. Determine whether 97 is a quadratic residue or non-residue mod 383.

Notes

3. Determine those odd primes p for which (-3|p) = 1 and those for which (-3|p) = -1

4. Prove that 5 is a quadratic residue of an odd prime p if p ≡ ±1 (mod 10), and that 5 is a non residue if p ≡ ± 3 (mod 10)

5. Let p be an odd prime. Assume that the set {1, 2…, p-1} can be expressed as the union of two nonempty subsets S and T, S ≠ T, such that the product (mod p) of any two elements in the same subset lies in S, whereas the product (mod p) of any elements in S with any elements in T lies in T.

Prove that S consists of the quadratic residues and T of the non residue's mod p.

6. Prove that $n^4 + 4$ composite for n > 1..