M.S c Mathematics –SEM 2 CC -10

E-content 2–**By Dr Abhik Singh**, Guest faculty, PG Department of Mathematics, Patna University, Patna

Content-Mobius Function ,Congruence of higher degree

Arithmetical Function

Definition: A function f(n) which is defined for all n>0 ,so that it represents some arithmetical property of n , is called an arithmetical function or a number-theoreti c function. Thus the function $\emptyset(n)$, t(n), $\sigma(n)$,T(n), S(n) are all examples of arithmetical function.

Mobius Function (or the Mobius Inversion Formula)

For Positive integers n we can define

$\mu(n)$ = $(-1)^{w(n)}$,if n is square free

0 , otherwise

The , $\mu(n)$ is the Mobius (μ) function.Here w(n) is the number of distinct primes dividing n.

Example

(i) $\mu(2)=(-1)^1=-1$

(ii) $\mu(3)=(-1)^1=-1$

(iii) $\mu(4)=(2^2)=0$

(iv) $\mu(6)=\mu(2.3)=(-1)^2=1$ or $\mu(6)=(-1)^{w(6)}=(-1)^2=1$

(v) $\mu(30)=\mu(2.3.5)=(-1)^3=-1$

(vi) $\mu(405)=\mu(5.9^2)=0$

Theorem1. $\boldsymbol{\mu(n)}$ **is multiplicative i.e** $\mu(ab)=\mu(a)\,\mu(b)$,a and b are relatively prime.

Proof : If a= 1 , then $\mu(ab)=\mu(b)=1.\,\mu(b)=\mu(a)\,\mu(b)$.

If a>1 and b>1 and if (a ,b)=1 .Then we with the p's distinct from q's can say that

ab $=P_1^{a1}.....P_k^{aK}.q_1^{B1}..... q^{BS}{}_S$ with the p's distinct from q's.

If $\mu(ab)=0$,either some $a_i > 1$ or some $b_i>1$.

In the first case ,say $\mu(a)=0$, therefore $\mu(a)\ \mu(b)=0=\mu(ab)$.

If $\mu(b)=0$ .Then $\mu(a)\ \mu(b)=0=\mu(a)=\mu(ab)$

If $\mu(ab)\neq 0$,then every $a_i=1$ and every $b_i=1$.Thus

$\mu(a)=(-1)^k$ and $\mu(b)=(-1)^s$

Therefore

$\mu(a)\ \mu(b)=(-1)^k\ (-1)^s=(-1^{\ k+s}=\mu(ab)$

Since (a,b)=1 implies the p's are distinct from the q's.

So in every case it is shown that $\mu(ab)=\mu(a)\ \mu(b)$

Hence $\mu(n)$ s multiplicative function.

Theorem-2 If F(n) is a multiplicative function and $F(n)=\sum_{d/n} f(d)$; then f is also multiplicative.

Proof: Let us consider two relatively prime integers m and n .Then, we have divisor d of mn ,which can be written uniquely as $d=d_1d_2$ where d_1/m and d_2/n such that $(d_1,d_2)=1$

We know that $f(mn)=\sum_{d/mn} \mu(d)F(mn/d)$

$$=\sum_{d1d2/mm} \mu(d_1d_2)F(mn/d_1d_2)$$

$$=\sum_{d1d2/mm} \mu(d_1)\mu(d_2)\ F(m/d_1)F(n/d_2)$$

[Here μ and F both are multiplicative functions]

$$=\sum_{d1/m} \mu(d_1)F(m/d_1)\sum_{d2/n} \mu(d_2)F(n/d_2)$$

$$=f(m)f(n)$$

Hence f is a multiplicative function. (Proved)

2. Congruence of Higher degree

Let us consider the general form of congruence with prime p modulo as

$f(x) = a_o x^n + \ldots\ldots\ldots + a_n \equiv 0 (\text{mod} p)$, $p \nmid a_o$.....(i)

To find the solution we proceed as follows. If some coefficient of f(x) in (1) is greater than p, we reduce them to less than p.

Also if the degree of f(x) is not less than p, we get remainder r(x) such that $f(x)=(x^p-x)q(x)+r(x)$

where ,the degree of r(x) is less than p, by using x^p-x to divide f(x), i.e we reduce f(x) to r(x) whose degree is less than p such that

$f(x) \equiv r(x) (\text{mod} p)$

by using $x^p \equiv x (\text{mod} p)$,the problem of solving (1) becomes $r(x) \equiv 0 (\text{mod} p)$.

Since the degree of r(x) is less than that of f(x),then the calculation is easy.

If $f(x)=f_1(x).f_2(x) (\text{mod} p)$ i.e $f_i(x)$ is a factor of f(x) modulo p , then to solve (1) ,is to solve

$f_1(x) \equiv 0 (\text{mod} p)$ and $f_2(x) \equiv 0 (\text{mod} p)$

Again,if $x \equiv a \pmod{p}$ is a solution of (1) ,then from

$f(x) \equiv (x-a)g(x)+r$

We have $r \equiv 0 \pmod{p}$

Therefore $(x-a)g(x) \pmod{p}$

i.e x-a is a factor of f(x) modulo p.

Hence the problem of solving (1) becomes that of solving $g(x) \equiv 0 \pmod{p}$.

Example: Let $f(x) = 6x^8+7x^7+x^6+x^5-6x^4-2x^3+8x+4$ find the solution of $f(x) \equiv 0 \pmod{p}$.....(i)

Solution: Here f(x) is of degree 8>5.

Hence we divide it by $x^5-x \pmod{5}$

And obtain $f(x) \equiv (x^5-x)(x^3+2x^2+x+1)+x^2+4x+4 \pmod{5}$

So equation (1) reduced to $x^2+4x+4 \equiv 0 \pmod{5}$

This congruence has only one solution $x \equiv 3 \pmod{5}$

Therefore (1) has only one solution $x \equiv 3 \pmod{5}$

Note: The general form of a congruence of degree n is

$F(x) \equiv 0 \pmod{m}$

Where f(x) is a polynomial of degree n such that a_n is not divisible by m.Any value of x say $x=x_o$ which satisfies (1) is

called a solution (or root) of the congruence and is written as $x \equiv x_0 (\mathrm{mod} m)$.

Assignment

1. Solve $f(x) = x^7 - 2x^6 - 7x^5 + x + 2 \equiv 0 (\mathrm{mod} 5)$