(6.2) The Mobius Inversion formula.

Möbius μ-function

Def^n(6.3) For any positive integer n, define μ by the rules

$$\mu(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ where } p_i \text{ are distinct primes.} \end{cases}$$

(e.g) $\mu(30) = \mu(2 \cdot 3 \cdot 5)$ $\quad 30 = 2 \times 3 \times 5$

$= (-1)^3$

$= -1$

$\mu(1) = 1$

$\mu(2) = -1 \quad 2 = 2 \quad n = p_1 p_2$

$\mu(3) = -1 \quad 3 = 3$

$\mu(4) = 0 \quad$ as $\quad 2^2 \mid 4$

$\mu(5) = -1$

$\mu(6) = \mu(2 \times 3) = (-1)^2 = 1$

use of μ function in ch-8 finding primitive roots of integer n, uses $\phi(n)$ Euler's

it depends on prime factoring-finding $x^4 - 1 = 0 (\bmod p)$ fun^{ns}

(2) i.e $\mu(n) = 0$ if n is not a square free integer

$\mu(n) = (-1)^r$ if n is square-free with r prime factors

[Square-free integer
(A number is said to be square free
if no prime factor divides it more than once
(i.e largest power of a prime factor that divides n is one)]

e.g. 1, 2, 3, 5, 6 ...

Remark If p is prime number then $\mu(p) = -1$ ①

and $\mu(p^k) = 0$ for $k \geq 2$

Theorem (6.5) The function μ is multiplicative function

[f is multiplicative if $f(mn) = f(m) f(n)$ whenever $\gcd(m,n) = 1$]

(pf) to show: $\mu(mn) = \mu(m)\mu(n)$ whenever $\gcd(m,n) = 1$

case ① If either $p^2 \mid m$ or $p^2 \mid n$ then $p^2 \mid mn$ (i.e m & n are no square free integers) then by def^n of μ we set $\mu(mn) = 0$

($p^2 \mid m \Rightarrow m = k_1 p^2$; means m & n are no square free integers)

and $p^2 \mid m$ or $p^2 \mid n$

$\Rightarrow \mu(m) = 0$ or $\mu(n) = 0$

$\therefore \mu(mn) = 0 = \mu(m)\mu(n)$ (by def^n of μ (cases) m & n are 1 or m, n are primes, or m & n are product of primes)

case ② If both m & n are square-free integers

say $m = p_1 p_2 \cdots p_r$, $n = q_1 q_2 \cdots q_s$, with all the primes p_i & q_j being distinct

then $\mu(mn) = \mu(p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s)$

$= (-1)^{r+s}$ (by def^n of μ)

$= (-1)^r (-1)^s$ (both m & n are square free)

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

(Hence Proved)

Remark ① if $n = 1$ then $\sum_{d \mid 1} \mu(d) = \mu(1) = 1$

(sum of all positive divisors of 1) (1 divides 1)

② If $n > 1$ then $\sum_{d \mid n} \mu(d) = F(n)$ [defined function in Sec^n 6.1]

(here f is μ)

let $n = p^k$ (*)

$F(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \dots + \mu(p^k)$

$= \mu(1) + \mu(p) + 0 + \dots + 0$ (by def^n of μ)

$= 1 + (-1)$

$= 0$

(e.g. $n = 3^2$, then $1, 3, 3^2$ divide 3^2; $n = 5^2$, then $1, 5, 5^2$ divide 5^2)

two case (*): n is prime or product of primes

let $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ (AS $n > 1$)

then

$F(n) = F(p_1^{k_1} p_2^{k_2} \dots p_r^{k_r})$

$= F(p_1^{k_1}) F(p_2^{k_2}) \dots F(p_r^{k_r})$

$= 0$ (by above)

By thm 6.4 (if f is multiplicative fn & $F(n) = \sum_{d|n} f(d)$ then F is also multiplicative)

Theorem (6.6) For each positive integer $n \geq 1$

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

(by remarks (stated above) in thm 6.6 in textbook)

where d runs through positive divisors of n.

(e.g.) $n = 10$

then $\sum_{d|10} \mu(10) = 0$ (as $n = 10 > 1$)

Now (check) $\sum_{d|10} \mu(10) = \mu(1) + \mu(2) + \mu(5) + \mu(10)$

(positive divisors of 10: 1, 2, 5, 10)

$= 1 + (-1) + (-1) + (-1)^2$ (by def^n 2 is prime)

$= 1 - 1 - 1 + 1$

$= 0$

Theorem (6.8) If F is multiplicative function

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

then f is also multiplicative.

(pf) let m & n be relatively prime positive integers.

let d be any divisor of mn

then $d = d_1 d_2$ where $d_1 | m$ & $d_2 | n$

(Basic number theory) $\gcd(d_1, d_2) = 1$

(e.g. $15 = 3 \times 5$, $3|15$, $5|15$, $\gcd(3,5)=1$)

thus, by thm 6.7 (Inversion formula)

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

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1 d_2) F\left(\frac{mn}{d_1 d_2}\right)$$

$$= \sum_{\substack{d_1|m \\ d_2|n}} \mu(d_1)\mu(d_2) F\left(\frac{m}{d_1}\right) F\left(\frac{n}{d_2}\right) \quad (\because \mu \text{ \& } F \text{ both are multiplicative})$$

$$= \sum_{d_1|m} \mu(d_1) F\left(\frac{m}{d_1}\right) \sum_{d_2|n} \mu(d_2) F\left(\frac{n}{d_2}\right)$$

$$= f(m) f(n) \quad (\text{by thm. } 6.7)$$

Exercise (6.2) 1, 3, 4, 6

(2.1) (a) For each positive integer n, show that

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$$

(b) For any integer $n \geq 1$, show that

$$\sum_{k=1}^{n} \mu(k!) = 1$$

(Sol.) (a) let n be positive integer

Now, out of consecutive integers $n, (n+1), (n+2), (n+3)$, two of them must be even

the 4 consecutive integers $n, n+1, n+2, n+3$, one must be divisible by 4. Since $4 = 2^2$, that number is not square free

and μ is multiplicative also $\gcd(n, n+1, n+2, n+3) = 1$

$\therefore \mu(n)\mu(n+1)\mu(n+2)\mu(n+3)$

$= \mu((n)(n+1)(n+2)(n+3))$

$= 0$ (since one of the must be not square free)

ie $\gcd(2,3,4,5) = 1$

$\mu(n) = 0$ if (n is not square free)

(b) For integer $n \geq 1$

consider $\sum_{k=1}^{n} \mu(k!) = \mu(1) + \mu(2) + \mu(3!) + \mu(4!) + \cdots + \mu(n!)$

$\mu(1) = 1$

$\mu(2) = \mu(2 \cdot 1) = (-1)$ since 2 is prime

$\mu(3!) = \mu(3 \cdot 2) = \mu(3)\mu(2) = (-1)(-1) = 1$

$\mu(4!) = 0$: as $4! = 2^2$ i.e $2^2 \mid 4!$

$\mu(5!) = 0$ as $5! = 5 \cdot 4 \cdot 3 \cdot 2 = 5 \cdot 2^2 \cdot 3 \cdot 2 = 5 \cdot 2^3 \cdot 3$

$5!$ is (not square free)

$\mu(k!) = 0$ for all $k \geq 4$

thus $\sum_{k=1}^{n} \mu(k!) = \mu(1) + \mu(2) + \mu(6)$

$= 1 + (-1) + 1$

$= 1$

(Q-6) Find formulas for $\sum_{d|n} \mu^2(d)/\tau(d)$ and $\sum_{d|n} \frac{\mu^2(d)}{\sigma(d)}$. that in terms of prime factorization of n. $d|n$

(Sol^n) Consider two functions

$$F(n) = \sum_{d|n} \frac{\mu^2(d)}{\tau(d)} \quad \text{and} \quad G(n) = \sum_{d|n} \frac{\mu^2(d)}{\sigma(d)}$$

let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where p_i are distinct prime

then $F(n) = F(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})$

Since $\frac{\mu^2(d)}{\tau(d)}$ & $\frac{\mu^2(d)}{\sigma(d)}$ are both multiplicative ($\tau(1)=1$, $\sigma(1)=1$) so, $\tau \neq 0$, $\sigma \neq 0$

$\therefore F(n) = F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_r^{k_r})$

Now $F(p_1^{k_1}) = F(n_1)$ (say $n_1 = p_1^{k_1}$)

$$F(n_1) = \sum_{d|n_1} \frac{\mu^2(d)}{\tau(d)}$$

$$= \frac{\mu^2(1)}{\tau(1)} + \frac{\mu^2(p_1)}{\tau(p_1)} + \frac{\mu^2(p_1^2)}{\tau(p_1^2)} + \cdots + \frac{\mu^2(p_1^{k_1})}{\tau(p_1^{k_1})}$$

($n_1 = p_1^{k_1}$)
divisors of $p_1^{k_1}$ are $1, p_1, p_1^2, p_1^3, \cdots, p_1^{k_1}$

$$= \frac{\mu(1)\mu(1)}{\tau(1)} + \frac{\mu(p_1)\cdot\mu(p_1)}{\tau(p_1)} + 0 + \cdots + 0$$

($\because p_1^2$ not square free, $\mu(p_1^2)=0$)

$$= \frac{(1)(1)}{(1)} + \frac{(-1)(-1)}{2} + 0$$

($\tau(n)=2$ if n is prime; $p_1 = 1 \times p_1$ prime)

$$= 1 + \frac{1}{2} = \frac{3}{2}$$

$\therefore F(n) = \underbrace{\frac{3}{2} \times \frac{3}{2} \times \cdots \frac{3}{2}}_{r \text{ times}}$

$$= \left(\frac{3}{2}\right)^r$$

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

$$\sigma(n) = \sigma(p_1^{k_1})\,\sigma(p_2^{k_2}) \cdots \sigma(p_r^{k_r})$$

$$\sigma(p_1^{k_1}) = \sum_{d|p_1^{k_1}} \frac{\mu^2(d)}{\sigma(d)}$$

(only consider p_1 & divisors of $p_1^{k_1}$)

$$= \frac{\mu(1)\,\mu(1)}{\sigma(1)} + \frac{\mu^2(p_1)}{\sigma(p_1)} + 0$$

$$= \frac{(1)(1)}{(1)} + \frac{(-1)(1)}{p_1+1} \qquad (\because \sigma(n) = n+1 \text{ if } n \text{ is prime})$$

$$= 1 + \frac{1}{p_1+1}$$

$$= \frac{p_1+2}{p_1+1}$$

$$\therefore \sigma(n) = \left(\frac{p_1+2}{p_1+1}\right)\cdot\left(\frac{p_2+2}{p_2+1}\right)\cdots\left(\frac{p_r+2}{p_r+1}\right)$$

(1.3) The Greatest Integer function

Defn (6.4) For any arbitrary real number x, we denoted by $[x]$ the largest integer less than or equal to x, i.e $[x]$ is the unique integer satisfying $x-1 < [x] \le x$

(e.g) $[-\frac{3}{2}] = -2$, $[\frac{1}{3}] = 0$

$[\sqrt{2}] = 1$, $[\pi] = [3.14] = [\frac{22}{7}] = 3$

$[-\pi] = -4$

How many times a particular prime p appears in $n!$

Let $p=3$ and $n=9$

$9! = 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9$

$= 2^7 3^4 5\cdot 7$

We get exact power of 3 that divides $9!$ is 4

Now, we find formula to find which power of $1.n/(a.$ divides $n!$

Theorem(6.9) If n is positive integer and p is prime then exponent of the highest power of p that divides $n!$ is $\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$

where series is finite, since $\left[\frac{n}{p^k}\right] = 0$ for $p^k > n$

(pf) Among the first n positive integers, those divisible by p are $p, 2p, 3p, \ldots, tp$ where t is the largest integer s.t $tp \le n$

i.e t is largest integer less than or equal to $\frac{n}{p}$

$$\text{i.e } t = \left[\frac{n}{p}\right]$$

Thus, there are exactly $\left[\frac{n}{p}\right]$ multiples of p occurring in the product that defines $n!$ namely

$$p, 2p, \ldots, \left[\frac{n}{p}\right]p$$

Now, the integers b/w 1 and n that are divisible by p^2 are

$$p^2, 2p^2 \ldots \left[\frac{n}{p^2}\right]p^2$$ (the exponent of p in the prime factorization of $n!$)

which are $\left[\frac{n}{p^2}\right]$ in number.

Similarly we get $p^3, 2p^3 \ldots \left[\frac{n}{p^3}\right]p^3$

After finite number of repetitions of this process we get that the total number of p divides $n!$

is $\sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$ (how much power of p divides $n!$)

(Hence Proved)