Möbius Inversion

Let f be an arithmetic function. Recall that the function F defined by

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

is called the summatory function of f.

Can we express f in terms of F?
Yes! There is a way to do this.

We look for an expression for $f(n)$ in the form

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

where μ is an arithmetic function.

Definition: The Möbius function $\mu(n)$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r \text{ where } p_i \text{ are distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

It follows that, if n is divisible by a square of a prime, then $\mu(n) = 0$.

Ex: $\mu(1) = 1$, $\mu(2) = (-1)^1 = -1$, $\mu(3) = (-1)^1 = -1$
$\mu(4) = 0$, $\mu(5) = -1$, $\mu(6) = (-1)^2 = 1$
$\mu(7) = -1$, $\mu(8) = 0$

Ex: $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$
$\mu(400) = 0$, $\mu(66) = \mu(2 \cdot 3 \cdot 11) = (-1)^3 = -1$

Theorem 7.14: The Möbius function $\mu(n)$ is a multiplicative function.

Proof: Let $m, n \in \mathbb{Z}^+$ be such that $\gcd(m,n) = 1$.
We show that $\mu(mn) = \mu(m)\mu(n)$.

Case 1: $m = 1$ or $n = 1$.

If $m = 1$, then
$$\mu(mn) = \mu(n) = \mu(1)\mu(n) = \mu(m)\mu(n).$$

Similarly, if $n = 1$, we get
$$\mu(mn) = \mu(m)\mu(n)$$

Case 2: Suppose, at least one of m and n is divisible by a square of a prime. Then, mn is also divisible by the square of this prime.

Then, $\mu(mn) = 0$

and $\mu(m)\mu(n) = 0$

$\therefore \mu(mn) = \mu(m)\mu(n)$.

Case 3: Suppose m and n are square-free.

Let $m = p_1 p_2 \cdots p_s$

and $n = q_1 q_2 \cdots q_t$.

Then, since $\gcd(m,n) = 1$, all p_i's and q_i's are distinct.

$$\therefore \mu(mn) = (-1)^{s+t}$$
$$= (-1)^s \cdot (-1)^t$$
$$= \mu(m)\,\mu(n)$$

Hence the theorem.

<u>Theorem 7.15:</u> The summatory function of the Möbius function at n,

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

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

Proof: When $n=1$,

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

Suppose $n > 1$. We know that μ is a multiplicative function (Theorem 7.14). Hence, by Theorem 7.8, $F(n)$ is also multiplicative.

We first prove that $F(p^k) = 0$ for any prime p and any $k \in \mathbb{Z}^+$.

We've

$$\begin{aligned} F(p^k) &= \sum_{d|p^k} \mu(d) \\ &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\ &= 1 + (-1) + 0 + \cdots + 0 \\ &= 0 \end{aligned}$$

Finally, let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ be the prime-power factorization of n.

Then,
$$\begin{aligned} F(n) &= F(p_1^{\alpha_1}) F(p_2^{\alpha_2}) \cdots F(p_t^{\alpha_t}) \\ &= 0 \cdot 0 \cdot \cdots 0 \\ &= 0 \end{aligned}$$

Hence the theorem.

Theorem 7.16: The Möbius Inversion Formula

Suppose f is an arithmetic function and F is the summatory function of f, so that

$$F(n) = \sum_{d \mid n} f(d), \quad n \in \mathbb{Z}^+$$

Then,

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

Proof:

$$\sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d \mid n} \left(\mu(d) \left(\sum_{e \mid \frac{n}{d}} f(e) \right) \right)$$

$$= \sum_{d \mid n} \sum_{e \mid \frac{n}{d}} \mu(d) f(e)$$

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

(This is because the set of pairs (d, e) with $d \mid n$ and $e \mid \frac{n}{d}$ is the same as the set of pairs (e, d) with $e \mid n$ and $d \mid \frac{n}{e}$.)

Now, by Theorem 7.15,

$$\sum_{d \mid \frac{n}{e}} \mu(d) = 0 \text{ unless } \frac{n}{e} = 1 \text{ (i.e., } e = n).$$

When $e = n$, we've $\displaystyle\sum_{d \mid \frac{n}{e}} \mu(d) = \mu(1) = 1.$

$$\therefore \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{n|n} \left(f(n) \cdot 1\right)$$

$$= f(n)$$

This completes the proof.

ex: Recall that

$\sigma(n)$ = summatory function of $f(n) = n$.

and $\tau(n)$ = " " " $f(n) = 1$.

Thus,

$$\sigma(n) = \sum_{d|n} d \quad \text{and}$$

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

Then, by the Möbius inversion formula,

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

and

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

Let us verify the Möbius inversion formula for $\sigma(n)$ and $\tau(n)$ for $n=12$.

Divisors of 12 are 1, 2, 3, 4, 6 and 12.

We find,

$$\sigma(1)=1,\ \sigma(2)=3,\ \sigma(3)=4,$$
$$\sigma(4)=7,\ \sigma(6)=12 \text{ and } \sigma(12)=28$$

Also, $\mu(1)=1,\ \mu(2)=-1,\ \mu(3)=-1$
$\mu(4)=0,\ \mu(6)=1,\ \mu(12)=0.$

Hence,

$$\sum_{d\mid 12}\mu(d)\sigma\left(\frac{12}{d}\right)=\mu(1)\sigma(12)+\mu(2)\sigma(6)+\mu(3)\sigma(4)+\mu(4)\sigma(3)+\mu(6)\sigma(2)+\mu(12)\sigma(1)$$
$$=(1)(28)+(-1)(12)+(-1)(7)+(0)(4)+(1)(3)+(0)(1)$$
$$=28-12-7+3$$
$$=12$$

Also,

$$\tau(1)=1,\ \tau(2)=2,\ \tau(3)=2$$
$$\tau(4)=3,\ \tau(6)=4,\ \tau(12)=6$$

$\therefore$

$$\sum_{d\mid 12}\mu(d)\tau\left(\frac{12}{d}\right)=(1)(6)+(-1)(4)+(-1)(3)+(0)(2)+(1)(2)+(0)(1)$$
$$=6-4-3+2=1$$

Theorem 7.17: Let f be an arithmetic function with summatory function
$$F(n) = \sum_{d|n} f(d).$$
Then, if F is multiplicative, then f is also multiplicative.

Proof: Exercise