April 1–Möbius inversion formula

We revisit some arithmetic functions, introduce the Möbius function, and prove the Möbius inversion formula.

Definition 1. A function f is *arithmetic* if it is defined on all positive integers.

We have seen many arithmetic functions: the Euler ϕ-function, $d(n)$ is the number of positive divisors of n, $\sigma(n)$ is the sum of positive divisors of n, $\omega(n)$ is the number of distinct prime divisors of n, $\Omega(n)$ is the number of primes dividing n counting multiplicity.

Definition 2. An arithmetic function f is *multiplicative* if for any relatively prime $m, n \in \mathbb{Z}$, $f(mn) = f(m)f(n)$. The function is *completely multiplicative* if $f(mn) = f(m)f(n)$ for all positive integers m and n.

Question 1 *The Euler ϕ-function is:*

Multiple Choice:

(a) *not multiplicative*

(b) *multiplicative* ✓

(c) *completely multiplicative*

The function $f(n) = n^2$ is:

Multiple Choice:

(a) *not multiplicative*

(b) *multiplicative*

(c) *completely multiplicative* ✓

Multiplicative functions are completely defined by their value on powers of primes. If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then for any multiplicative function f, $f(n) = f(p_1^{a_1}) f(p_2^{a_2} \cdots f(p_r^{a_r})$ by repeatedly applying the definition of a multiplicative function.

Learning outcomes:
Author(s):

Theorem 1. Let f be an arithmetic function and for $n \in \mathbb{Z}$ with $n > 0$, let

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

If f is multiplicative, then so is $F(n)$.

Proof Let m and n be relatively prime positive integers. To prove that $F(n)$ is multiplicative, we need to show that $F(mn) = F(m)F(n)$. We have that $F(mn) = \sum_{d|mn} f(d)$. Since $(m, n) = 1$, each divisor $d > 0$ of mn can be written as $d_1 d_2$ where $d_1 \mid m, d_2 \mid n$, and $(d_1, d_2) = 1$ and each such product corresponds to a divisor d of mn (see homework 10). We have

$$\begin{aligned} F(mn) &= \sum_{d_1|m, d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m, d_2|n} f(d_1) f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= F(m)F(n) \end{aligned}$$

■

Example 1. To clarify the previous proof, we look at an example: Let $m = 3$ and $n = 4$. We need to show that $F(3 \cdot 4) = F(3)F(4)$. We have

$$\begin{aligned} F(12) &= \sum_{d|12} f(d) \\ &= f(1) + f(2) + f(3) + f(4) + f(6) + f(12) \end{aligned}$$

Regroup so that the first 3 terms are factors of 4 and the last 3 terms are factors of 3.

$$= f(1) + f(2) + f(4) + f(3) + f(6) + f(12)$$

The factor each term

$$\begin{aligned} &= f(1 \cdot 1) + f(1 \cdot 2) + f(1 \cdot 4) + f(3 \cdot 1) + f(3 \cdot 2) + f(3 \cdot 4) \\ &= f(1f(1) + f(1f(2) + f(1f(4) + f(3f(1) + f(3f(2) + f(3f(4) \\ &= [f(1) + f(3][f(1) + f(2) + f(4)] \\ &= \sum_{d_1|3} f(d_1) \sum_{d_2|4} f(d_2) \\ &= F(3)F(4) \end{aligned}$$

Definition 3. An integer n is *square-free* if it is not divisible by p^2 for any prime p.

Definition 4. Let $n \in \mathbb{Z}$ with $n > 0$. The *Möbius μ-function*, denoted $\mu(n)$, is

$$\mu(n) = \begin{cases} 1 & if\ n = 1 \\ 0 & if\ p^2 \mid n,\ p \text{ prime} \\ (-1)^r & if\ n = p_1 p_2 \cdots p_r,\ p_i \text{ prime} \end{cases} = \begin{cases} 1 & if\ n = 1 \text{ or} \\ & n \text{ square-free, even number of prime factors} \\ 0 & if\ n \text{ not square-free} \\ -1 & if\ n \text{ square-free, odd number of prime factors.} \end{cases}$$

Question 2 *Since* $504 = 2^3 3^2 7, \mu(504)$ *is*

Multiple Choice:

(a) *1*

(b) *0* ✓

(c) *-1*

Since $30 = 2 \cdot 3 \cdot 5, \mu(30)$ *is*

Multiple Choice:

(a) *1*

(b) *0*

(c) *-1* ✓

Theorem 2. The Möbius μ function is multiplicative.

Proof Let m and n be relatively prime positive integers. We must show that $\mu(mn) = \mu(m)\mu(n)$. If $m = 1$ or $n = 1$, then we are done (see participation assignment).

Either m or n is divisible by p^2 for some prime p if and only if mn is divisible by p^2. Then $\mu(mn) = 0$ and either $\mu(m) = 0$ or $\mu(n) = 0$, so $\mu(m)\mu(n) = 0$.

If m and n are both square-free, then $m = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$ with $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ distinct primes. Then

$$\begin{aligned} \mu(mn) &= \mu(p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s) = (-1)^{r+s} \\ &= (-1)^r (-1)^s \\ &= \mu(m)\mu(n) \end{aligned}$$

■

Theorem 3. Let $n \in \mathbb{Z}$ with $n > 0$. Then

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

Proof Since $\mu(n)$ is multiplicative, the first theorem from this section says that $\sum_{d|n} \mu(d)$ is also multiplicative. Thus, the value of this function is determined by it's value on power of primes. Now, $F(1) = 1$. If p is prime, then

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

■

Theorem 4 (Möbius Inversion Formula)**.** Let f and g be arithmetic functions. Then

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

if and only if

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

Proof Note that $\sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$ since $\frac{n}{d}$ and d are both on the list of all divisors of d.

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

$$\begin{aligned} \sum_{d|m} \mu(d) f(\frac{n}{d}) &= \sum_{d|n} \left(\mu(d) \sum_{c|\frac{n}{d}} g(c) \right) \\ &= \sum_{c|n} \left(g(c) \sum_{d|\frac{n}{d}} \mu(d) \right) \text{ why?} \end{aligned}$$

By the previous theorem, $\sum_{d|n} \mu(d) = 0$ unless $\frac{n}{c} = 1$, ie $c = n$. Thus, the only term in the summation is $g(c)$.

($\Leftarrow$) Assume that $g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$. Then

$$\begin{aligned}\sum_{d|n} g(d) &= \sum_{d|n} \left(\sum_{c|d} \mu(\frac{d}{c}) f(c) \right) \\ &= \sum_{d|n} \left(f(c) \sum_{d=cm|n} \mu(\frac{d}{c}) \right) \text{ why?} \\ &= \sum_{c|n} \left(f(c) \sum_{m|\frac{n}{c}} \mu(m) \right) \text{ why?}\end{aligned}$$

Again, $\sum_{m|\frac{n}{c}} \mu(d) = 0$ unless $\frac{n}{c} = 1$, ie $c = n$. Thus, the only term left is $f(n)$. ■

Example 2. Let $n \in \mathbb{Z}$ with $n > 0$, and $g(n) = n$. We have

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

By the Möbius inversion formula

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

Equivalently,

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

Example 3. Let $n \in \mathbb{Z}$ with $n > 0$. We have

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

where $g(n) = 1$ for all $n > 0$. By the Möbius inversion formula

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