14. Möbius inversion formula

14.1 Möbius inversion formula

The pair of relations (13.4) and (13.5), and the pair of relations (13.6) and (13.8) are indeed special cases of a general phenomenon, known as the *Möbius inversion formula.*

Theorem 14.1 (Möbius Inversion Formula). Let $f(n)$ and $g(n)$ be arithmetic functions. If

$$g(n) = \sum_{d|n} f(d) \tag{14.1}$$

then

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right), \tag{14.2}$$

and vice versa.

R In (13.4) and (13.5), we have $f = \phi$ and $g = \mathrm{id}$; in (13.6) and (13.8), we have $f = \Lambda$ and $g = \log$.

Proof. We first prove (14.2) by (14.1). Note that

$$\begin{aligned}\sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d'|\frac{n}{d}} f(d') = \sum_{\substack{d,d' \\ dd'|n}} \mu(d) f(d') \\ &= \sum_{d'|n} f(d') \sum_{d|\frac{n}{d'}} \mu(d) = \sum_{d'|n} f(d') \varepsilon\left(\frac{n}{d'}\right) = f(n),\end{aligned}$$

where we make use of (13.3). Conversely, to show (14.1) from (14.2), we first require the trivial fact that for any arithmetic function $a(n)$,

$$\sum_{d|n} a(d) = \sum_{d|n} a\left(\frac{n}{d}\right).$$

Rewriting (14.2) as

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

it follows that

$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right) = \sum_{d|n}\sum_{d'|\frac{n}{d}} \mu\left(\frac{n/d}{d'}\right) g(d') = \sum_{\substack{d,d' \\ dd'|n}} \mu\left(\frac{n}{dd'}\right) g(d')$$

$$= \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu\left(\frac{n/d'}{d}\right) = \sum_{d'|n} g(d') \sum_{d|\frac{n}{d'}} \mu(d) = \sum_{d'|n} g(d')\varepsilon\left(\frac{n}{d'}\right) = g(n),$$

where (13.3) is also applied. ∎

There is a slightly different type of Möbius inversion formula working for functions defined on real $x > 0$. Below, in the summation $\sum_{n\leq x}$, the index n runs over all positive integers no larger than x.

Theorem 14.2 Let $F(x)$ and $G(x)$ be functions defined on real $x > 0$. If

$$G(x) = \sum_{n\leq x} F\left(\frac{x}{n}\right) \tag{14.3}$$

then

$$F(x) = \sum_{n\leq x} \mu(n) G\left(\frac{x}{n}\right), \tag{14.4}$$

and vice versa.

Proof. We first prove (14.4) by (14.3). Note that

$$\sum_{n\leq x} \mu(n)G\left(\frac{x}{n}\right) = \sum_{n\leq x}\mu(n)\sum_{m\leq\frac{x}{n}} F\left(\frac{x/n}{m}\right) = \sum_{\substack{m,n \\ mn\leq x}} \mu(n)F\left(\frac{x}{mn}\right)$$

$$(\text{with } N = mn) = \sum_{N\leq x} F\left(\frac{x}{N}\right)\sum_{n|N}\mu(n) = \sum_{N\leq x} F\left(\frac{x}{N}\right)\varepsilon(N) = F(x).$$

Conversely, to show (14.3) from (14.4), we have

$$\sum_{n\leq x} F\left(\frac{x}{n}\right) = \sum_{n\leq x}\sum_{m\leq\frac{x}{n}} \mu(m)G\left(\frac{x/n}{m}\right) = \sum_{\substack{m,n \\ mn\leq x}} \mu(m)G\left(\frac{x}{mn}\right)$$

$$(\text{with } N = mn) = \sum_{N\leq x} G\left(\frac{x}{N}\right)\sum_{m|N}\mu(m) = \sum_{N\leq x} G\left(\frac{x}{N}\right)\varepsilon(N) = G(x),$$

as required. ∎

14.2 Multiplicative Möbius inversion formula

Another important variant of Möbius inversion formula is in the multiplicative notation.

Theorem 14.3 Let $f(n)$ and $g(n)$ be arithmetic functions such that $f(n) \neq 0$ and $g(n) \neq 0$ for all n. If

$$g(n) = \prod_{d|n} f(d) \tag{14.5}$$

then

$$f(n)=\prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)}, \tag{14.6}$$

and vice versa.

Proof. We first prove (14.6) by (14.5). Note that

$$\begin{aligned}\prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)} &= \prod_{d|n}\left(\prod_{d'|\frac{n}{d}} f(d')\right)^{\mu(d)} = \prod_{d|n}\prod_{d'|\frac{n}{d}} f(d')^{\mu(d)} = \prod_{d'|n}\prod_{d|\frac{n}{d'}} f(d')^{\mu(d)}\\ &= \prod_{d'|n} f(d')^{\sum_{d|\frac{n}{d'}}\mu(d)} = \prod_{d'|n} f(d')^{\varepsilon(n/d')} = f(n).\end{aligned}$$

Conversely, to show (14.5) from (14.6), we have

$$\begin{aligned}\prod_{d|n} f(d) = \prod_{d|n} f\left(\frac{n}{d}\right) &= \prod_{d|n}\prod_{d'|\frac{n}{d}} g(d')^{\mu\left(\frac{n/d}{d'}\right)} = \prod_{d'|n}\prod_{d|\frac{n}{d'}} g(d')^{\mu\left(\frac{n}{dd'}\right)}\\ &= \prod_{d'|n} g(d')^{\sum_{d|\frac{n}{d'}}\mu\left(\frac{n/d'}{d}\right)} = \prod_{d'|n} g(d')^{\sum_{d|\frac{n}{d'}}\mu(d)} = \prod_{d'|n} g(d')^{\varepsilon(n/d')} = g(n),\end{aligned}$$

as required. ■

R Intuitively, for positive-valued f and g, we may define $\tilde{f}(n)=\log f(n)$ and $\tilde{g}(n)=\log g(n)$. By taking logarithm in (14.5) and (14.6), their equivalence becomes

$$\tilde{g}(n)=\sum_{d|n}\tilde{f}(d) \qquad \Longleftrightarrow \qquad \tilde{f}(n)=\sum_{d|n}\mu(d)\tilde{g}\left(\frac{n}{d}\right),$$

which is exactly the usual Möbius inversion formula.

14.3 Dirichlet convolutions

The Möbius inversion formula can be further understood in a more abstract way, through *Dirichlet convolutions*, named after the German mathematician Peter Gustav Lejeune Dirichlet.

Definition 14.1 For arithmetic functions f and g, their *Dirichlet convolution* is defined to be an arithmetic function h with

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

where the summation runs over all positive divisors of n. We write

$$h=f*g.$$

Dirichlet convolutions satisfy the following algebraic properties.

Theorem 14.4 For any arithmetic functions u, v and w, we have

(i) $u*v=v*u$ (commutative law);
(ii) $(u*v)*w=u*(v*w)$ (associative law).

Proof. It is straightforward to verify that

$$(u*v)(n) = (v*u)(n) = \sum_{\substack{a,b\\ab=n}} u(a)v(b)$$

and

$$\big((u*v)*w\big)(n) = \big(u*(v*w)\big)(n) = \sum_{\substack{a,b,c\\abc=n}} u(a)v(b)w(c),$$

where a, b and c run over positive integers. ■

Theorem 14.5 Let ε be the unit function. For any arithmetic function f, we have $f*\varepsilon = \varepsilon * f = f$.

Proof. We have

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

as required. ■

Theorem 14.6 Let f be an arithmetic function with $f(1)\neq 0$. Then there exists a unique arithmetic function g such that $f*g = g*f = \varepsilon$. Moreover, g is given by

$$g(1) = \frac{1}{f(1)} \tag{14.7}$$

and for $n>1$,

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n\\d<n}} f\left(\frac{n}{d}\right) g(d). \tag{14.8}$$

Proof. First, we note that $(f*g)(1) = f(1)g(1) = \varepsilon(1) = 1$ gives $g(1) = 1/f(1)$. For $n>1$, we have $\varepsilon(n) = 0$, and hence,

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

Hence, we may iteratively determine the unique $g(n)$ by (14.8). ■

Definition 14.2 Given an arithmetic function f with $f(1)\neq 0$, we call the unique arithmetic function g such that $f*g = g*f = \varepsilon$ the *Dirichlet inverse* of f, denoted by $g = f^{-1}$.

Theorem 14.7 For any arithmetic functions with $f(1)\neq 0$ and $g(1)\neq 0$, we have $(f*g)^{-1} = f^{-1}*g^{-1}$.

Proof. We have $(f*g)*(f^{-1}*g^{-1}) = (f*f^{-1})*(g*g^{-1}) = \varepsilon*\varepsilon = \varepsilon$, as required. ■

R In the language of group theory, the set of arithmetic functions f with $f(1)\neq 0$ forms an Abelien group with respect to the operation "$*$" (Dirichlet convolution), and the identity element of this group is the unit function ε.

Corollary 14.8 The Möbius function μ and the constant function $\mathbf{1}$ are Dirichlet inverses of one another.

Proof. We simply rewrite the relation (13.3), $\sum_{d|n}\mu(d)=\varepsilon(n)$, in terms of Dirichlet convolution, and find that $\mu*\mathbf{1}=\varepsilon$, yielding the desired result. ∎

R We may also interpret the Möbius inversion formula in this setting by noting that it is exactly the equivalence

$$g=f*\mathbf{1} \qquad \Longleftrightarrow \qquad f=g*\mu.$$

This is trivial since if $g=f*\mathbf{1}$, then $g*\mu=(f*\mathbf{1})*\mu=f*(\mu*\mathbf{1})=f*\varepsilon=f$; and if $f=g*\mu$, then $f*\mathbf{1}=(g*\mu)*\mathbf{1}=g*(\mu*\mathbf{1})=g*\varepsilon=g$.

Now, we consider Dirichlet convolutions on multiplicative functions.

Theorem 14.9 If f and g are multiplicative functions, so is their Dirichlet convolution $f*g$.

Proof. We write $h=f*g$. Let m and n be positive integers with $(m,n)=1$. We use the fact that if $d\mid mn$, then we may uniquely write $d=ab$ with $a\mid m$ and $b\mid n$. In particular, $(a,b)=1$ and $(\frac{m}{a},\frac{n}{b})=1$. Now,

$$\begin{aligned}h(mn)&=\sum_{d|mn}f(d)g\left(\frac{mn}{d}\right)=\sum_{a|m,b|n}f(ab)g\left(\frac{mn}{ab}\right)=\sum_{a|m,b|n}f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)\\&=\sum_{a|m}f(a)g\left(\frac{m}{a}\right)\sum_{b|n}f(b)g\left(\frac{n}{b}\right)=h(m)h(n).\end{aligned}$$

Hence, $h=f*g$ is multiplicative. ∎

Theorem 14.10 If f is a multiplicative function, so is its Dirichlet inverse f^{-1}.

Proof. Noting that f is multiplicative, we have $f(1)=1$, and hence $f^{-1}(1)=\frac{1}{f(1)}=1$. Now we shall show that for every positive integer N, $f^{-1}(N)=f^{-1}(m)f^{-1}(n)$ holds true for any positive integers m and n with $(m,n)=1$ and $mn=N$. We prove by induction on N. The base case $N=1$ is confirmed by the fact that $f^{-1}(1)=1$. Assume that the claim is true for $1,\ldots,N-1$ for some $N\geq 2$, and we shall prove the case of N. Note that

$$\begin{aligned}\varepsilon(N)=(f^{-1}*f)(mn)&=\sum_{a|m,b|n}f^{-1}(ab)f\left(\frac{mn}{ab}\right)\\&=f^{-1}(mn)f(1)+\sum_{\substack{a|m,b|n\\ab<N}}f^{-1}(ab)f\left(\frac{mn}{ab}\right)\\\text{(induc. assump.)}&=f^{-1}(mn)f(1)+\sum_{\substack{a|m,b|n\\ab<N}}f^{-1}(a)f^{-1}(b)f\left(\frac{m}{a}\right)f\left(\frac{n}{b}\right)\\&=f^{-1}(mn)f(1)-f^{-1}(m)f^{-1}(n)f(1)f(1)+\sum_{a|m,b|n}f^{-1}(a)f^{-1}(b)f\left(\frac{m}{a}\right)f\left(\frac{n}{b}\right)\\&=f^{-1}(N)-f^{-1}(m)f^{-1}(n)+(f^{-1}*f)(m)(f^{-1}*f)(n)\\&=f^{-1}(N)-f^{-1}(m)f^{-1}(n)+\varepsilon(N),\end{aligned}$$

thereby implying that $f^{-1}(N)=f^{-1}(m)f^{-1}(n)$, as required. ∎

R The set of multiplicative functions is a subgroup of the group of all arithmetic functions f with $f(1) \neq 0$.

14.4 Ramanujan's sums

We first adopt a conventional nonation in analytic number theory.

Definition 14.3 For any complex τ, we define

$$e(\tau) := e^{2\pi i\tau}.$$

Now, we introduce Ramanujan's sums, which is crucial in, for instance, the proof of I. M. Vinogradov's theorem (*Recueil Math.* **2** (1937), 179–195) that *every sufficiently large odd number is the sum of three primes.*

Definition 14.4 For q and n positive integers, *Ramanujan's sums* are defined by

$$c_q(n) := \sum_{\substack{1\le a\le q\\(a,q)=1}} e\left(\frac{an}{q}\right).$$

R Ramanujan's sums were introduced by Srinivasa Ramanujan (*Trans. Cambridge Philos. Soc.* **22** (1918), no. 13, 259–276).

We introduce another sum for q and n positive integers:

$$\eta_q(n) := \sum_{1\le a\le q} e\left(\frac{an}{q}\right).$$

Lemma 14.11 For positive integers q and n,

$$\eta_q(n) = \begin{cases} q & \text{if } q \mid n, \\ 0 & \text{if } q \nmid n. \end{cases} \tag{14.9}$$

In particular, for positive integers s and t with $(s,t) = 1$, we have $\eta_s(n)\eta_t(n) = \eta_{st}(n)$.

Proof. Let $d = (q,n)$, and write $q = q'd$ and $n = n'd$. Noting that $(q',n') = 1$, we have $\{an' : 1 \le a \le q'\}$ covers a complete system modulo q'. Now,

$$\eta_q(n) = \sum_{1\le a\le q} e\left(\frac{an}{q}\right) = \eta_q(n) := \sum_{1\le a\le q'd} e\left(\frac{an'}{q'}\right) = d\sum_{1\le a\le q'} e\left(\frac{an'}{q'}\right) = d\sum_{1\le a\le q'} e\left(\frac{a}{q'}\right)$$

Note that

$$\sum_{1\le a\le q'} e\left(\frac{a}{q'}\right) = \begin{cases} 1 & \text{if } q' = 1, \\ 0 & \text{if } q' > 1. \end{cases}$$

Finally, we use the fact that $q' = 1$ if and only if $q = d = (q,n)$, or $q \mid n$, as desired. The second part is a direct consequence of (14.9). ■

Now, we establish a relation between $c_q(n)$ and $\eta_q(n)$.

Theorem 14.12 For positive integers q and n,

$$\eta_q(n) = \sum_{d|q} c_d(n). \tag{14.10}$$

Proof. We use the fact that $\{\frac{a}{q} : 1 \le a \le q\} = \cup_{d|q}\{\frac{b}{d} : 1 \le b \le d \text{ and } (b,d) = 1\}$, by simplifying each $\frac{a}{q}$ to its irreducible form. Hence,

$$\sum_{1\le a\le q} e\left(\frac{an}{q}\right) = \sum_{d|q} \sum_{\substack{1\le b\le d \\ (b,d)=1}} e\left(\frac{bn}{d}\right),$$

as required. ■

Let us treat $\eta_q(n)$ and $c_q(n)$ as functions in q with n fixed, and define $H(q) := \eta_q(n)$ and $C(q) := c_q(n)$ for clarity. Then we may paraphrase (14.10) as

$$H = C * \mathbf{1}. \tag{14.11}$$

Corollary 14.13 Let n be a positive integer. For positive integers s and t with $(s,t) = 1$,

$$c_s(n)c_t(n) = c_{st}(n). \tag{14.12}$$

Proof. We use Theorems 14.9 and 14.10 by noting that both H and $\mathbf{1}$ are multiplicative. ■

Corollary 14.14 For positive integers q and n,

$$c_q(n) = \sum_{d|q, d|n} \mu\left(\frac{q}{d}\right) d. \tag{14.13}$$

Proof. We apply Möbius inversion formula to (14.11), and find that

$$c_q(n) = \sum_{d|q} \mu\left(\frac{q}{d}\right) \eta_d(n).$$

The desired relation follows with recourse to (14.9). ■

Theorem 14.15 For positive integers q and n,

$$c_q(n) = \mu\left(\frac{q}{(q,n)}\right) \frac{\phi(q)}{\phi\left(\frac{q}{(q,n)}\right)}. \tag{14.14}$$

Proof. For convenience, we write

$$R_q(n) := \mu\left(\frac{q}{(q,n)}\right) \frac{\phi(q)}{\phi\left(\frac{q}{(q,n)}\right)}. \tag{14.15}$$

Let n be an arbitrary positive integer. Note that $c_1(n) = R_1(n)$. Also, let s and t be such that $(s,t) = 1$. Then $(st,n) = (s,n)(t,n)$ and $\left(\frac{s}{(s,n)}, \frac{t}{(t,n)}\right) = 1$. Thus,

$$R_{st}(n) = \mu\left(\frac{st}{(st,n)}\right) \frac{\phi(st)}{\phi\left(\frac{st}{(st,n)}\right)} = \mu\left(\frac{s}{(s,n)}\right) \mu\left(\frac{t}{(t,n)}\right) \frac{\phi(s)\phi(t)}{\phi\left(\frac{s}{(s,n)}\right)\phi\left(\frac{t}{(t,n)}\right)} = R_s(n)R_t(n).$$

Recalling (14.12), it suffices to prove for prime powers p^α that $c_{p^\alpha}(n) = R_{p^\alpha}(n)$. Finally, it is straightforward to calculate from (14.13) and (14.15) that

$$c_{p^\alpha}(n) = R_{p^\alpha}(n) = \begin{cases} p^{\alpha-1}(p-1) & \text{if } (p^\alpha, n) = p^\alpha, \\ -p^{\alpha-1} & \text{if } (p^\alpha, n) = p^{\alpha-1}, \\ 0 & \text{otherwise.} \end{cases}$$

The desired relation holds true. ■