Dirichlet series

February 21, 2022

Contents

1 Arithmetic function

An *arithmetic function* f is defined to be a map from $\mathbb{N}_{>0}$ to the complex numbers $\mathbb{C}$. Assuming f is not identically zero (i.e. assign 0 to every number)

1. It is *multiplicative* if $f(mn) = f(m)f(n)$ for any co-prime m, n.
2. It is *completely multiplicative* if such identity holds for any positive integers m, n.

Remark 1.1.

1. A completely multiplicative function is always multiplicative.
2. The value at 1 of an multiplicative function is 1.
3. A multiplicative function is uniquely defined by its values at prime powers. A completely multiplicative function is uniquely defined by its values at primes.

Proof. Part 1: straight from definition.
Part 2: plug in the definition the values $m = n = 1$ (which are relatively prime), we get $f(1) = f(1)^2$. If $f(1) = 0$, then $f(m) = f(1)f(m) = 0$ for all $m \geq 1$, contradicting the definition of an arithmetic function. Thus, $f(1) = 1$.
Part 3: this follows from the unique factorization of an integer as product of distinct prime powers. For completely multiplicative function f, we can reduce the value of f at the prime powers to just the values at prime, as $f(p^k) = f(p)^k$. □

Example 1.2.

1. The map $\varepsilon(n) = 1$ if $n = 1$, and $\varepsilon(n) = 0$ otherwise. This map is completely multiplicative.

   In terms of Kronecker delta δ_{ij} (where it is 0 if $i \neq j$ and 1 otherwise), we can simply write $\varepsilon(n) = \delta_{n1}$.
2. The *unit map* $1(n) = 1$ for all $n \geq 1$. This map is also completely multiplicative.
3. The identity map $\mathrm{id}(n) = n$ is completely multiplicative.

Proof.
Part 1: let m, n be integers. We consider 2 cases

1. One of m, n is 1: wlog, say $m = 1$, we then get $\varepsilon(mn) = \varepsilon(n) = \varepsilon(m)\varepsilon(n)$
2. $m, n > 1$: then $\varepsilon(mn) = 0 = \varepsilon(m)\varepsilon(n)$

Part 2, 3: straight from definition

$$1(mn) = 1 = 1(m)1(n)$$
$$\mathrm{id}(mn) = mn = \mathrm{id}(m)\,\mathrm{id}(n)$$

□

Example 1.3 (Dirichlet characters)**.** An arithmetic function $\chi : \mathbb{N}_{>0} \to \mathbb{C}$ is a *Dirichlet character modulo* n iff

- It is completely multiplicative.
- $\chi(a) = 0$ iff a, n are not relatively prime. If $n = p$ is prime, then simply $\chi(a) = 0$ if and only if a is divisible by p.
- It is periodic with period n, i.e. $\chi(a + n) = \chi(a)$ for all $a \geq 1$.
  Note: it may have smaller period, which classifies whether a character is *primitive* or not.

There are 2 distinguished examples

1. The *principal* character χ_0 modulo n, which is defined as below
$$\chi_0(a) = \begin{cases} 1 & \text{if } \gcd(a, n) = 1 \\ 0 & \text{otherwise} \end{cases}$$
2. The Legendre symbol $a \mapsto (a/p)$ for p odd prime, which is a non-trivial character modulo p. It has order 2 since the square is always 1 except when $p \mid a$.

Proof. For the principal Dirichlet character modulo n

1. χ_0 is multiplicative: let $\gcd(a, b) = 1$. Consider the 2 following cases
   (a) One of a, b is not relatively prime to n: then ab is also not relatively prime to n, and thus, $\chi_0(ab) = 0 = 0 \cdot 0 = \chi_0(a)\chi_0(b)$.
   (b) Both are relatively prime to n: then ab is also relatively prime to n, and thus, $\chi_0(ab) = 1 = 1 \cdot 1 = \chi_0(a)\chi_0(b)$.

For the multiplicativity of Legendre symbol, see the chapter about Gauss/Jacobi sum. The other 2 properties are relatively straightforward since $(0/p) = 0$ by definition, and (a/p) only depends on the congruence class of a (also by definition). □

Example 1.4 (Filtrated Euler totient function)**.** An integer sequence $A = (a_n)_{n=1}^{\infty}$ is *poly-divisible* iff $a_i - a_j$ is divisible by $i - j$ for all $i \neq j$.

Given such poly-divisible sequence A, the *Euler function associated with* A, denoted as φ_A, counts the number indices $1 \leq k \leq n$ such that $\gcd(a_k, n) = 1$

$$\varphi_A(n) = |\{1 \leq k \leq n : \gcd(a_k, n) = 1\}|$$

Prove that

1. φ_A is multiplicative.
2. $\varphi_A(p^t) = p^{t-1}\varphi_A(p)$ for all prime p and $t \geq 1$.

When $a_n = n$ for all $n \geq 1$, we simply call $\varphi := \varphi_A$ the *Euler totient function.*

Proof. *The Euler function associated with a poly-divisible sequence: the base case $\varphi_A(1) = 1$ holds since every integer is relatively prime to 1. Denote $G_n^A = \{1 \leq k \leq n : \gcd(a_k, n) = 1\}$, so that $\varphi_A(n)$ is just the cardinality of G_n^A. To show it is multiplicative, let $m, n \geq 1$ be co-prime integers, we need to show that there is a correspondence between G_{mn}^A and $G_m^A \times G_n^A$.

1. Let $k \mapsto (k \bmod m, k \bmod n)$ be the map from G_{mn}^A to $G_m^A \times G_n^A$. It is well-defined since, if we let $u = k \bmod m \in [1, m]$, then $m \mid k - u \mid a_k - a_u$, or equivalently, $a_k \equiv a_u \pmod{m}$. Yet, $\gcd(a_k, mn) = 1$ by definition, so $\gcd(a_k, m) = 1$ and hence, $\gcd(a_u, m) = 1$. By definition, $u = k \bmod m \in G_m^A$. Similarly, $k \bmod n \in G_n^A$.
2. The inverse of the previous map requires us to find a unique $k \in \mathbb{G}_{mn}^A$ associated with a given pair $(u, v) \in \mathbb{G}_m^A \times \mathbb{G}_n^A$ such that $k \equiv u \pmod{m}$ and $k \equiv v \pmod{n}$.

   Since $\gcd(m, n) = 1$, there exists a unique $1 \leq k \leq mn$ such that $k \equiv u \pmod{m}$ and $k \equiv v \pmod{n}$ (Chinese remainder theorem). On the other hand, since $m \mid k - u \mid a_k - a_u$, we know that $\gcd(a_k, m) = \gcd(a_u, m) = 1$. Similarly, $\gcd(a_k, m) = \gcd(a_v, n) = 1$. Again, since $\gcd(m, n) = 1$, we necessarily have $\gcd(a_k, mn) = 1$, so k should be in G_{mn}^A.

*For the identity $\varphi_A(p^t) = p^{t-1}\varphi_A(p)$, we will find a correspondence between $G_{p^t}^A$ and $G_{p^{t-1}} \times G_p^A$, where $G_n = \mathbb{Z}/n\mathbb{Z} = \{k : 0 \leq k \leq n-1\}$, in order to show such. To do this, we use ideas from Hensel lemma

1. Suppose $k \in G_{p^t}^A$, let $r = k \bmod p \in [1, p]$ and $q = (k - r)/p$. Since $1 \leq k \leq p^t$

$$q \geq \left\lceil \frac{1-p}{p} \right\rceil = 0$$
$$q \leq \left\lfloor \frac{p^t - 1}{p} \right\rfloor = p^{t-1} - 1$$

   Thus, $q \in G_{p^{t-1}}$. To show the map $k \mapsto (q, r)$ from $G_{p^t}^A$ to $G_{p^{t-1}} \times G_p^A$, we need $r \in G_p^A$. Indeed, since $p \mid k - r \mid a_k - a_r$, we get $\gcd(a_r, p) = \gcd(a_k, p) = 1$.
2. Given $(q, r) \in G_{p^{t-1}} \times G_p^A$, the inverse map requires us to construct a unique $k \in G_{p^t}^A$ such that $k \equiv r \pmod{p}$, and $q = (k - r)/p$. Basically,

$k = q \cdot p + r$. Since $0 \leq q < p^{t-1}, 1 \leq r \leq p$, we have

$$k \geq 0 \cdot p + 1 = 1$$
$$k \leq (p^{t-1} - 1)p + p = p^t$$

Furthermore, since $k \equiv r \pmod{p}$, we get $p \mid k - r \mid a_k - a_r$, so $\gcd(a_k, p) = \gcd(a_r, p) = 1$, which implies a_k is relatively prime to any power of p. In other words, $k \in G^A_{p^t}$.

□

Example 1.5 (More constructions)**.**

1. Pointwise product: the product of multiplicative functions is multiplicative. The product of completely multiplicative functions is completely multiplicative.

2. Inverse: suppose a function is non-zero at every natural number. Then its inverse is multiplicative if it is multiplicative, and its inverse is completely multiplicative if it is completely multiplicative.

3. Non-integer power of a function: let α be a real number, and $f : \mathbb{N}_{>0} \to \mathbb{R}_{>0}$ be an arithemtic function on positive reals.

   (a) If f is multiplicative, then f^α is multiplicative.

   (b) If f is completely multiplicative, then f^α is completely multiplicative.

   A quintessential example of this construction is the power map $\mathrm{id}^\alpha(n) = n^\alpha$, which is completely multiplicative.

4. Composition: let $f : \mathbb{N}_{>0} \to \mathbb{N}_{>0}$ and $g : \mathbb{N}_{>0} \to \mathbb{C}$ be arithmetic functions. Suppose furthermore that one of the following holds

   (a) g is completely multiplicative.

   (b) g is multiplicative, and f forms a *strong divisibility sequence*, i.e. for all positive integers m, n

   $$\gcd(f(n), f(m)) = f(\gcd(m, n))$$

   then $g \circ f$ is multiplicative whenever f is multiplicative.

   An highly non-trivial example of this construction is

   $$h(n) = \gcd(F_n, k)$$

   where F_n denotes the n-th Fibonacci number, and k is a fixed positive integer. We will not discuss on why the Fibonacci numbers forms a strong divisibility sequence.

5. Exponentiation: define a function $w : \mathbb{N}_{>0} \to \mathbb{C}$ to be *additive* if $w(mn) = w(m) + w(n)$ for relative prime m, n. w is completely additive if the equality holds for arbitrary m, n.

   Show that the function $f(n) = e^{w(n)}$ is a multiplicative function if w is additive. f is completely multiplicative if w is completely additive.

   For example, the Liouville function $\lambda(n) = (-1)^{\Omega(n)}$ is completely multiplicative, where $\Omega(n)$ counts the number of primes (with multiplicity) of n.

6. Indicator function: let A be a subset of the positive integers, and 1_A be the *indicator function* on A

$$1_A(n) = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A \end{cases}$$

   Prove that

   (a) 1_A is multiplicative iff whenever m, n are co-prime (positive) integers, we get $mn \in A$ iff $m, n \in A$.

   (b) 1_A is completely multiplicative iff given integers m, n, then $mn \in A$ iff $m, n \in A$.

   Note 1: the unit map is just the indicator function on the set of all positive integers ($1 = 1_{\mathbb{N}_{>0}}$).
   Note 2: the principal Dirichlet character modulo n is the indicator function on the set of all positive integers co-prime to n.

Proof. All of these results are relatively evident. We only clarify parts 4-6 for readers who wish to check their work.
Part 4: suppose g is completely multiplicative, then $g(f(mn)) = g(f(m)f(n)) = g(f(m))g(f(n))$, which shows that $g \circ f$ is either multiplicative or completely multiplicative depending on whether m, n are co-prime, and whether f is completely multiplicative or just multiplicative. On the other hand, suppose g, f are multiplicative such that f forms a strong divisibility sequence, then $f(mn) = f(m)f(n)$ and $\gcd(f(m), f(n)) = 1$ whenever $\gcd(m, n) = 1$. Since g is multiplicative, we get $g(f(mn)) = g(f(m)f(n)) = g(f(m))g(f(n))$.
Part 5: since $f(mn) = e^{w(mn)} = e^{w(m)+w(n)} = e^{w(m)}e^{w(n)} = f(m)f(n)$ formally, f is multiplicative (resp. completely multiplicative) if g is additive (resp. completely additive). For the Liouville function

1. Based on the factorization $n = \prod_i p_i^{\alpha_i}$ and $m = \prod_i p_i^{\beta_i}$, Ω must be completely additive

$$\Omega(m) + \Omega(n) = \sum_i \alpha_i + \sum_i \beta_i = \sum_i (\alpha_i + \beta_i) = \Omega(mn)$$

2. Since $e^{i\pi} = -1$, we know that $\lambda(n) = (-1)^{\Omega(n)} = e^{i\pi\Omega(n)}$ must be completely additive. This relies on the fact that any multiple of additive (resp. completely additive) function is also additive (resp. completely additive), which is left to the reader.

Part 6: 1_A is multiplicative iff $1_A(mn) = 1_A(m)1_A(n)$ whenever m, n are relatively prime. When both side equal to 1 (and thus every factor is equal to 1), we have $mn \in A$ iff $1_A(mn) = 1$ iff $1_A(m) = 1_A(n) = 1$ iff $m, n \in A$. Vice versa, suppose A satisfies such property. Then $1_A(mn) = 1$ iff $mn \in A$ iff $m, n \in A$ iff $1_A(m) = 1_A(n) = 1$, so $1_A(mn) = 1_A(m)1_A(n) = 1$ in this case. Negating the whole equivalence, we have $1_A(mn) = 0$ iff $mn \notin A$ iff $m \notin A$ or $n \notin A$, iff $1_A(m) = 0$ or $1_A(n) = 0$, so $1_A(mn) = 1_A(m)1_A(n) = 0$ for the remaining case. The complete multiplicativity case is similar. □

Exercise 1.6. Suppose f is multiplicative, show that

$$f(m)f(n) = f(\gcd(m,n))f(\operatorname{lcm}(m,n))$$

for *any* integers m, n.

Proof. Use factorization, and recall

$$\gcd\left(\prod_i p_i^{\alpha_i}, \prod_i p_i^{\beta_i}\right) = \prod_i p_i^{\min\{\alpha_i,\beta_i\}}$$
$$\operatorname{lcm}\left(\prod_i p_i^{\alpha_i}, \prod_i p_i^{\beta_i}\right) = \prod_i p_i^{\max\{\alpha_i,\beta_i\}}$$

□

Remark 1.7. There is a more general identity, which has analogues in multiple areas of mathematics

1. [Set Theory] Principle of inclusion-exclusion:

$$\begin{aligned}\left|\bigcup_{i=1}^n A_i\right| = \sum_{i=1}^n |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \cdots \\ + (-1)^{k+1} \sum_{1\le i_1<\cdots<i_k\le n} \left|\bigcap_{\ell=1}^k A_\ell\right| + \cdots \\ + (-1)^{n+1}|A_1 \cap \cdots \cap A_n|\end{aligned}$$

2. [Algebra] Principle of min-max:

$$\begin{aligned}\max_{1\le i\le n} x_i = \sum_{i=1}^n x_i - \sum_{1\le i<j\le n} \min\{x_i, x_j\} + \cdots \\ + (-1)^{k+1} \sum_{1\le i_1<\cdots<i_k\le n} \min\{x_{i_1}, \ldots, x_{i_k}\} + \cdots \\ + (-1)^{n+1} \min_{1\le i\le n} x_i\end{aligned}$$

3. [Number Theory] Principle of gcd-lcm:

$$\begin{aligned}\operatorname{lcm}_{1\le i\le n} a_i = \prod_{i=1}^{n} a_i \cdot \left[\prod_{1\le i<j\le n} \gcd(a_i, a_j)\right]^{-1} \cdots \\ \left[\prod_{1\le i_1<\cdots<i_k\le n} \gcd(a_{i_1}, \ldots, a_{i_k})\right]^{(-1)^{k+1}} \cdots \\ \left[\gcd_{1\le i\le n} a_i\right]^{(-1)^{n+1}}\end{aligned}$$

4. [Number Theory - Multiplicative Function ver.]

$$\begin{aligned}f\left(\operatorname{lcm}_{1\le i\le n} a_i\right) = \prod_{i=1}^{n} f(a_i) \cdot \left[\prod_{1\le i<j\le n} f\left(\gcd(a_i, a_j)\right)\right]^{-1} \cdots \\ \left[\prod_{1\le i_1<\cdots<i_k\le n} f\left(\gcd(a_{i_1}, \ldots, a_{i_k})\right)\right]^{(-1)^{k+1}} \cdots \\ \left[f\left(\gcd_{1\le i\le n} a_i\right)\right]^{(-1)^{n+1}}\end{aligned}$$

Exercise 1.8 (Cyclic property of Euler totient)**.** Show that $\sum_{d|n} \varphi(d) = n$

Proof. The idea is to lift a *reduced* congruence class modulo d (the number of which is $\varphi(d)$) to a "distinct" congruence class modulo n (the number of which is just n), so that no congruence class modulo n are left when we exhausted all reduced classes and divisiors of n.

1. For each $1 \le t \le d, d \mid n$ such that $\gcd(t, d) = 1$, then we send t to the congruence class $s = t(n/d) \le n$, which has additive order of d. Indeed, $ds = nt \equiv 0 \pmod{n}$. If $es \equiv 0 \pmod{n}$ for some $0 \le e < d$, then etn/d is divisible by n. Since $\gcd(t, d) = 1$, e has to be divisible by d, a contradiction.

   A consequence of this, is that for $1 \le t_k \le d_k$, $d_k \mid n$, and $\gcd(t_k, d_k) = 1$ $(k = 1, 2)$, the respect congruence classes modulo n of t_1 and t_2 must be difference, assuming $d_1 \ne d_2$.

2. How about, t_1, t_2 are reduced congruence classes of the same modulo d? They are also different when sent to modulo n since if $t_1(n/d) \equiv t_2(n/d) \pmod{n}$, then $(t_1 - t_2)(n/d)$ must be divisible by n. Equivalently, $t_1 - t_2$ must be divisible by d, implying that $t_1 \equiv t_2 \pmod{d}$.

Thus, the reduced congruence classes modulo d for all $d \mid n$, are sent to different congruence classes modulo n.

Is there any congruence classes modulo n that are not represented by some reduced congruence classes modulo d for some $d \mid n$? Desiringly, no. Logically, let t be a congruence class modulo n, and $d = n/\gcd(n,t)$. Then

1. $s = dt/n = t/\gcd(n,t) \in \mathbb{Z}$
2. $\gcd(s,d) = \gcd\left(\frac{n}{\gcd(n,t)}, \frac{t}{\gcd(n,t)}\right) = 1$

So s can be considered as a reduced congruence class modulo d. The map at the beginning then lifts s to $s(n/d) = t$. We conclude that $\sum_{d|n} \varphi(d) = n$ $\square$

2 Dirichlet convolution

Given 2 arithmetic functions $f, g : \mathbb{N}_{>0} \to \mathbb{C}$, define their *Dirichlet convolution*

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

Proposition 2.1. The collection of multiplicative functions forms a commutative monoid (with Dirichlet convolution serves as multiplication). Note, however, that the convolution of 2 completely multiplicative functions may not be *completely* multiplicative.

Proof.
Closed under convolution: given $\gcd(m, n) = 1$, then every divisor d of mn can be factored uniquely as a divisor u of m and a divisor v (and vice versa). Additionally, $\gcd(u, v) = 1$. Thus,

$$\begin{aligned}
(f * g)(mn) &= \sum_{d|mn} f(d)\, g\left(\frac{mn}{d}\right) = \sum_{u|m, v|n} f(uv)\, g\left(\frac{mn}{uv}\right) \\
&= \sum_{u|m, v|n} f(u)\, f(v)\, g\left(\frac{m}{u}\right) g\left(\frac{n}{v}\right) \\
&= \left[\sum_{u|m} f(u)\, g\left(\frac{m}{u}\right)\right] \left[\sum_{v|n} f(v)\, g\left(\frac{n}{v}\right)\right] \\
&= (f * g)(m)(f * g)(n)
\end{aligned}$$

Commutative: for all $n \geq 1$

$$(f * g)(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) = \sum_{de=n} f(d)\, g(e) = \sum_{ed=n} g(e)\, f(d) = (g * f)(n)$$

Associative: for all $n \geq 1$

$$\begin{aligned}
(f*(g*h))(n) &= \sum_{u|n} f(u) \sum_{v|n/u} g(v)\, h\left(\frac{n}{uv}\right) \\
&= \sum_{u|n} f(u) \left[\sum_{vw=n/u} g(v)\, h(w)\right] \\
&= \sum_{uvw=n} f(u)\, g(v)\, h(w) \\
&= \sum_{w|n} \left[\sum_{uv=n/w} f(u)\, g(v)\right] h(w) \\
&= \sum_{w|n} \left[\sum_{u|n/w} f(u)\, g\left(\frac{n}{uw}\right)\right] h(w) \\
&= \sum_{w|n} (f*g)\left(\frac{n}{w}\right) h(w) = ((f*g)*h)(n)
\end{aligned}$$

Existence of identity: the identity (with respect to the convolution) is ε.

$$(f*\varepsilon)(n) = (\varepsilon * f)(n) = \sum_{d|n} \varepsilon(d) f\left(\frac{n}{d}\right) = \varepsilon(1) f(n) + \sum_{\substack{d|n \\ d\neq 1}} \varepsilon(d) f\left(\frac{n}{d}\right) = f(n)$$

□

Corollary 2.2 (Divisorial sum)**.** If f is multiplicative, then so is $g(n) = \sum_{d|n} f(d)$

Proof. Note that the unit map is (completely) multiplicative, so $g(n) = (f * 1)(n) = \sum_{d|n} f(d)1(n/d) = \sum_{d|n} f(d)$ is also multiplicative. □

Lemma 2.3 (Dirichlet inversion formula)**.** If f is an arithmetic function with $f(1) \neq 0$, then it has inverse g with respect to convolution. Recursively, $g(1) = (f(1))^{-1}$, and for $n > 1$

$$g(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d\neq n}} f\left(\frac{n}{d}\right) g(d)$$

Furthermore, if f is multiplicative, then its inverse is also multiplicative. And so, the collection of multiplicative functions forms an abelian group.

Proof. The recursive definition is straight from the definition of convolution. As for multiplicativity, the base case $g(1) = (f(1))^{-1} = 1$. Suppose $g(mn) =$

$g(m)g(n)$ holds for relatively prime m, n such that $mn < r$. Then for relatively prime $mn = r$ we have

$$\begin{aligned}
g(m)g(n) &= \sum_{\substack{d|m \\ d\neq m}} f\left(\frac{m}{d}\right) g(d) \cdot \sum_{\substack{e|n \\ e\neq n}} f\left(\frac{n}{e}\right) g(e) \\
&= \sum_{\substack{d|m, e|n \\ de\neq mn}} \left[f\left(\frac{m}{d}\right) g(d)\right] \cdot \left[f\left(\frac{n}{e}\right) g(e)\right] \\
&\quad - \sum_{\substack{e|n \\ e\neq n}} \left[f(1) g(m)\right] \cdot \left[f\left(\frac{n}{e}\right) g(e)\right] \\
&\quad - \sum_{\substack{d|m \\ d\neq m}} \left[f\left(\frac{m}{d}\right) g(d)\right] \cdot \left[f(1) g(n)\right] \\
&= \sum_{\substack{d|m, e|n \\ de\neq mn}} f\left(\frac{mn}{de}\right) g(de) + 2g(m)g(n) \\
&= -g(mn) + 2g(m)g(n)
\end{aligned}$$

Equivalently, $g(mn) = g(m)g(n)$. □

Let μ be the inverse of the unit map 1, called *Möbius function*. It is multiplicative because 1 is multiplicative. By definition, we obtain the following identity

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

Corollary 2.4 (Möbius inversion formula)**.** If $f, g : \mathbb{N}_{>0} \to \mathbb{C}$ be arithmetic functions, then $g(n) = \sum_{d|n} f(d)$ for all $n \geq 1$ if and only if $g(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$ for all $n \geq 1$.

Theorem 2.5 (Formula of Möbius function)**.** $\mu(n) = 0$ if n has a square factor, $\mu(n) = 1$ if n is square-free with even number of prime factors, and $\mu(n) = -1$ if n is square-free with odd number of prime factors.

Proof. We first show that $\mu(n) = \pm 1$ for square-free n. By Dirichlet inversion formula, $\mu(p) = -1(p)\mu(1) = -1$. Therefore, by unique factorization theorem, a square-free number is factored into product of *distinct* primes. Since μ is multiplicative, $\mu(n) = (-1)^{\omega(n)} = (-1)^{\Omega(n)}$ for square-free n, where $\omega(n)$ is the number of *distinct* prime factors of n.

Now, to show the remaining case, we need to show that $\mu(p^k) = 0$ for all $k \geq 2$. Again by Dirichlet inversion formula, $\mu(p^2) = -\left[1(p^2)\mu(1) + 1(p)\mu(p)\right] = 0$. By induction,

$$\mu(p^k) = -\sum_{i=0}^{k-1} 1(p^{k-i})\mu(p^i) = -\sum_{i=0}^{k-1} \mu(p^i) = -\left[\mu(1) + \mu(p) + \sum_{i=2}^{k-1} \mu(p^i)\right] = 0$$

Therefore, $\mu(n) = 0$ whenever n is not square-free (i.e. having a square factors. □

Example 2.6.

1. $\varphi * 1 = \mathrm{id}$.
2. Power sum of divisors:
$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha = (\mathrm{id}^\alpha * 1)(n)$$
3. Popovici function: let μ_k denote k-fold Dirichlet convolution of μ with itself. Show that
$$\mu_k(p^t) = (-1)^t \binom{k}{t}$$
where p is prime, $t \geq 0$.
4. Jordan totient function:
$$J_k(n) = n^k \prod_{p|n} \left(1 - \frac{1}{p^k}\right)$$
$$J_k * 1 = \mathrm{id}^k$$
$$\mathrm{id}^s \, J_s$$
5. Dedekind psi function:
$$\psi_k(n) = \frac{J_{2k}(n)}{J_k(n)} = (\mathrm{id}^k * \mu^2)(n) = n^k \prod_{p|n} \left(1 + \frac{1}{p^k}\right)$$
6. If $\varepsilon_2(n)$ is the indicator function on the set of squares, then
$$\varepsilon_2 * \psi_k = \sigma_k$$

Exercise 2.7. Find formulas for

1. $\sum_{d|n} \mu(d)\varphi(d)$
2. $\sum_{d|n} \mu(d)^2\varphi(d)^2$
3. $\sum_{d|n} \mu(d)^2\varphi(d)^2$
4. $\sum_{d|n} \mu(d)^2/\varphi(d)^2$

Exercise 2.8. Prove that for all $n \geq 1$

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the product is over prime factor of n.

Exercise 2.9. Prove that

1. $\phi(n)\phi(m) = \phi(\text{gcd}(n, m))\phi(\text{lcm}(n, m))$
2. $\phi(mn)\phi(\text{gcd}(m, n)) = \text{gcd}(n, m)\phi(m)\phi(n)$

3 Dirichlet action

The group of multiplicative functions (with values in $\mathbb{C}$) has actions on the following collections

1. The collection of all complex-valued functions on $[1, \infty)$.
2. Formal infinite series

Let $F : [1, \infty) \to \mathbb{C}$ be and $\alpha : \mathbb{N}^* \to \mathbb{C}$ be functions, then we define Mellin action of α on F as below

$$(\alpha * F)(x) = \sum_{1 \leq n \leq x} \alpha(n) F\left(\frac{x}{n}\right)$$

where the sum is over positive integers that are at most x.

Theorem 3.1 (Möbius inversion for floored summation)**.** The Mellin action is a monoid action, and a group action if one restricts to just multiplicative functions.

Proof. Identity: $(\varepsilon * F)(x) = \sum_{1 \leq n \leq x} \varepsilon(n) F\left(\frac{x}{n}\right) = \varepsilon(1) F\left(\frac{x}{1}\right) = F(x)$
Associative:

$$\begin{aligned}
[\alpha * (\beta * F)](x) &= \sum_{1 \leq n \leq x} \alpha(n)(\beta * F)\left(\frac{x}{n}\right) \\
&= \sum_{1 \leq n \leq x} \alpha(n) \sum_{1 \leq m \leq x/n} \beta(m) F\left(\frac{x}{nm}\right) \\
&= \sum_{1 \leq mn \leq x} \alpha(n)\beta(m) F\left(\frac{x}{nm}\right) \\
&= \sum_{1 \leq k \leq x} \left[\sum_{mn=k} \alpha(n)\beta(m)\right] F\left(\frac{x}{k}\right) \\
&= \sum_{1 \leq k \leq x} (\alpha * \beta)(k) F\left(\frac{x}{k}\right) = [(\alpha * \beta) * F](x)
\end{aligned}$$

□

Corollary 3.2. If $F(x) = \sum_{1 \leq n \leq x} G(x/n)$ then $G(x) = \sum_{1 \leq n \leq x} \mu(n) F(x/n)$.

The Hartman-Wintner action of arithmetic functions (with values in $\mathbb{C}$) on itself is defined as (based on their 1947 paper)

$$(\alpha \triangleleft f)(n) = \sum_{k=1}^{\infty} \alpha(k) f(kn)$$

as long as the expression on right converges absolutely for all $n \geq 1$.

Theorem 3.3 (Möbius inversion for infinite series)**.** The Hartman-Wintner action is a partial monoid action, and a partial group action if restricted to multiplicative functions.
Note: it is only partial since the summation does not necessarily converges for all arithmetic functions.

Proof. Identity: $(\varepsilon \triangleleft f)(n) = \sum_{k=1}^{\infty} \varepsilon(k) f(kn) = \varepsilon(1) f(1 \cdot n) = f(n)$
Associative: since the infinite sums are assumed to absolutely converge, we can rearrange it.

$$\begin{aligned}
[\alpha \triangleleft (\beta \triangleleft f)](x) &= \sum_{k=1}^{\infty} \alpha(k)(\beta \triangleleft f)(kn) \\
&= \sum_{k=1}^{\infty} \alpha(k) \sum_{l=1}^{\infty} \beta(l) f(kln) \\
&= \sum_{k,l=1}^{\infty} \alpha(k)\beta(l) f(kln) \\
&= \sum_{h=1}^{\infty} \left[\sum_{kl=h} \alpha(k)\beta(l) \right] f(hn) \\
&= \sum_{h=1}^{\infty} (\alpha * \beta)(h) f(hn) = [(\alpha * \beta) \triangleleft f](x)
\end{aligned}$$

□

Corollary 3.4. If $f(n) = \sum_{k=1}^{\infty} g(kn)$, then $g(n) = \sum_{k=1}^{\infty} \mu(k) f(kn)$. This holds under the assumption $\sum_{n=1}^{\infty} |f(n)| d(n) < \infty$ and $\sum_{n=1}^{\infty} |g(n)| d(n) < \infty$

4 Dirichlet series

Given a sequence of complex numbers $(f(n))_{n=1}^{\infty}$, the corresponding Dirichlet series is defined as

$$\mathcal{D}_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, s \in \mathbb{C}$$

Proposition 4.1. Treating as a formal series, then $\mathcal{D}_f(s)\mathcal{D}_g(s) = \mathcal{D}_{f*g}(s)$

Proof.

$$\mathcal{D}_f(s)\mathcal{D}_g(s) = \sum_{n,m=1}^{\infty} \frac{f(n)g(m)}{(nm)^s} = \sum_{k=1}^{\infty} \frac{1}{k^s} \sum_{nm=k} f(n)g(m) = \sum_{k=1}^{\infty} \frac{(f*g)(k)}{k^s} = \mathcal{D}_{f*g}(s)$$

□

Corollary 4.2.

1. The *Riemann zeta function* $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ has its (formal) inverse as

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

   More generally,

$$\frac{1}{\mathcal{D}_f(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)f(n)}{n^s}$$

2. If $d_\alpha(n) = \sum_{d|n} n^\alpha$, then corresponding Dirichlet series is

$$\sum_{n=1}^{\infty} \frac{d_\alpha(n)}{n^s} = \zeta(s)\zeta(s-\alpha)$$

   In particular, the Dirichlet series corresponding to the divisor function $d(n) = d_0(n)$ is the square of zeta function

Lemma 4.3 (Abel summation formula)**.** Let $(a_n)_{n=0}^{\infty}$ be a sequence of complex numbers (possibly all real). Define the associated partial summation

$$A(t) = \sum_{0 \le n \le t} a_n$$

If ϕ is a (complex-valued) continuously differentiable function on a neighborhood of $[x, y]$, then

$$\sum_{x < n \le y} a_n \phi(n) = A(y)\phi(y) - A(x)\phi(x) - \int_x^y A(u)\phi'(u)du$$

Proof. Note that $A(t) = A(\lfloor t \rfloor)$, so

$$\begin{aligned}
\sum_{x<n\le y} a_n\phi(n) &= \sum_{x<n\le y} (A(n) - A(n-1))\phi(n) \\
&= \sum_{x<n\le y} A(n)\phi(n) - \sum_{x-1<n\le y-1} A(n)\phi(n+1) \\
&= \left[\sum_{x<n\le y-1} A(n)\phi(n) + \sum_{y-1<n\le y} A(n)\phi(n)\right] \\
&\quad - \left[\sum_{x-1<n\le x} A(n)\phi(n+1) + \sum_{x<n\le y-1} A(n)\phi(n+1)\right] \\
&= \left[\sum_{x<n\le y-1} A(n)\phi(n) + A(\lfloor y \rfloor)\phi(\lfloor y \rfloor)\right] \\
&\quad - \left[A(\lfloor x \rfloor)\phi(\lfloor x \rfloor) + \sum_{x<n\le y-1} A(n)\phi(n+1)\right] \\
&= A(y)\phi(\lfloor y \rfloor) - A(x)\phi(\lfloor x \rfloor + 1) - \sum_{x<n\le y-1} A(n)\left(\phi(n+1) - \phi(n)\right) \\
&= A(y)\phi(\lfloor y \rfloor) - A(x)\phi(\lfloor x \rfloor + 1) - \sum_{x<n\le y-1} A(n)\int_n^{n+1} \phi'(u)du
\end{aligned}$$

Since $A(t)$ is constant almost everywhere for t between 2 integers (except only

at the right endpoint), we can bring it into the integrals.

$$\begin{aligned}
\sum_{x<n\leq y} a_n\phi(n) &= A(y)\phi(\lfloor y\rfloor) - A(x)\phi(\lfloor x\rfloor+1) - \sum_{x<n\leq y-1}\int_n^{n+1} A(u)\phi'(u)du \\
&= A(y)\phi(\lfloor y\rfloor) - A(x)\phi(\lfloor x\rfloor+1) - \int_{\lfloor x\rfloor+1}^{\lfloor y\rfloor} A(u)\phi'(u)du \\
&= A(y)\phi(y) - A(y)\left[\phi(y)-\phi(\lfloor y\rfloor)\right] \\
&\quad - A(x)\phi(x) + A(x)\left[\phi(\lfloor x\rfloor+1)-\phi(x)\right] \\
&\quad - \int_{\lfloor x\rfloor+1}^{\lfloor y\rfloor} A(u)\phi'(u)du \\
&= A(y)\phi(y) - A(x)\phi(x) \\
&\quad - A(y)\int_{\lfloor y\rfloor}^{y}\phi'(u)du - A(x)\int_x^{\lfloor x\rfloor+1}\phi'(u)du \\
&\quad - \int_{\lfloor x\rfloor+1}^{\lfloor y\rfloor} A(u)\phi'(u)du \\
&= A(y)\phi(y) - A(x)\phi(x) \\
&\quad - \int_{\lfloor y\rfloor}^{y} A(u)\phi'(u)du - \int_x^{\lfloor x\rfloor+1} A(u)\phi'(u)du \\
&\quad - \int_{\lfloor x\rfloor+1}^{\lfloor y\rfloor} A(u)\phi'(u)du \\
&= A(y)\phi(y) - A(x)\phi(x) - \int_x^y A(u)\phi'(u)du
\end{aligned}$$

(recall that the least integer $n > x$ is $\lfloor x+1\rfloor = \lfloor x\rfloor + 1$, while the greatest integer $n \leq y$ is $\lfloor y\rfloor$)

*If one know the Riemann-Stieltjes integral then the Abel summation formula is just integration by parts.

$$\begin{aligned}
\sum_{x<n\leq y} a_n\phi(n) &= \int_x^y \phi dA = A(y)\phi(y) - A(x)\phi(x) - \int_x^y A d\phi \\
&= A(y)\phi(y) - A(x)\phi(x) - \int_x^y A(u)\phi'(u)du
\end{aligned}$$

□

Corollary 4.4. If $a_n = 1$ (for $n \geq 1$) and $\phi(x) = x^{-s}$ on $(0,\infty)$, then $A(x) = \lfloor x\rfloor$ (since the index starts at 1) and

$$\sum_{1\leq n\leq x}\frac{1}{n^s} = \frac{\lfloor x\rfloor}{x^s} + s\int_1^x \frac{\lfloor u\rfloor}{u^{s+1}}du$$

1. If $s = 1$, we get an approximation for the harmonic series as

$$\sum_{1 \le n \le x} \frac{1}{n} = \frac{\lfloor x \rfloor}{x} + \int_1^x \frac{\lfloor u \rfloor}{u^2} du$$

Expanding more, we get the following (where $\{x\} = x - \lfloor x \rfloor$ denotes the *fractional part* of x)

$$\begin{aligned}\sum_{1 \le n \le x} \frac{1}{n} &= 1 - \frac{\{x\}}{x} + \int_1^x \frac{du}{u} - \int_1^x \frac{\{u\}}{u^2} du \\ &= \ln x + \left(1 - \int_1^x \frac{\{u\}}{u^2} du\right) - \frac{\{x\}}{x}\end{aligned}$$

Since $0 \le \frac{\{x\}}{x} < \frac{1}{x}$, and $0 \le \int_1^x \frac{\{u\}}{u^2} du \le \int_1^x \frac{1}{u^2} du = 1 - \frac{1}{x}$ (with $g(x) = \int_1^x \frac{\{u\}}{u^2} du$ increasing), we get

$$\lim_{x \to \infty} \left[\sum_{1 \le n \le x} \frac{1}{n} - \ln x \right] = \gamma < \infty$$

where $\gamma = 1 - \int_1^\infty \frac{\{u\}}{u^2} du$ is the Euler-Mascheroni constant.

2. If $x \to \infty$, we get the formula for the zeta function (only valid when $\operatorname{Re} s > 1$ in order for $\lfloor x \rfloor / x^s$ to converge to 0)

$$\zeta(s) = s \int_1^\infty \frac{\lfloor u \rfloor}{u^{s+1}} du$$

Which can be used to establish the pole at $s = 1$ with residue 1 as follows:

   (a) Convergence of ζ for $\operatorname{Re} s > 1$: given $s = \sigma + it$ ($\sigma > 1$) and $u \ge 1$, we have

$$\begin{aligned}\left| \frac{\lfloor u \rfloor}{u^{s+1}} \right| &= \frac{\lfloor u \rfloor}{u^{\sigma+1} |u^{it}|} \\ &= \frac{\lfloor u \rfloor}{u^{\sigma+1} |e^{i(t \ln u)}|} = \frac{\lfloor u \rfloor}{u^{\sigma+1}} \le u^{-\sigma}\end{aligned}$$

   Thus

$$\begin{aligned}\left| \int_x^y \frac{\lfloor u \rfloor}{u^{s+1}} du \right| &\le \int_x^y \left| \frac{\lfloor u \rfloor}{u^{s+1}} \right| du \\ &\le \int_x^y u^{-\sigma} du = \frac{y^{1-\sigma} - x^{1-\sigma}}{1 - \sigma}\end{aligned}$$

For $x < y$ sufficiently large, $\frac{y^{1-\sigma}-x^{1-\sigma}}{1-\sigma}$ is sufficiently small. We conclude $\int_1^\infty \frac{\lfloor u \rfloor}{u^{s+1}} du$ (and ζ) is absolutely convergent by Cauchy completeness.

Note: we cannot simply bound the original integral and say it is convergent, since the imaginary part may behave chaotic (also it only works for real-valued functions).

(b) Residue 1 at the *simple* pole $s = 1$: still assuming $s = \sigma + it$ for $\sigma > 1$

$$\zeta(s) = s \int_1^\infty \frac{\lfloor u \rfloor}{u^{s+1}} du = s \left(\int_1^\infty u^{-s} du - \int_1^\infty \{u\} u^{-s-1} du \right)$$

(the integrals are absolutely convergent by the same previous method, so we can split them up)

$$= s \left(\frac{\lim_{u\to\infty} u^{-s+1} - 1}{-s+1} - \int_1^\infty \{u\} u^{-s-1} du \right)$$

$$= \frac{s}{s-1} - s \int_1^\infty \{u\} u^{-s-1} du$$

(since $|u^{-s+1}| = u^{1-\sigma}$)

$$= 1 + \frac{1}{s-1} - s \int_1^\infty \{u\} u^{-s-1} du$$

For the integral $\int_1^\infty \{u\} u^{-s-1} du$, we just need to check it is finite at $s = 1$. Indeed,

$$\left| \int_1^\infty \{u\} u^{-s-1} du \right| \le \int_1^\infty \left| \{u\} u^{-s-1} \right| du$$
$$\le \int_1^\infty u^{-\sigma-1} du = \frac{1}{\sigma} \le 1$$

We then conclude

$$\lim_{s\to 1^+} \left[\zeta(s) - \frac{1}{s-1} \right] = 1 - \lim_{s\to 1^+} s \int_1^\infty \frac{\{u\}}{u^{s+1}} du$$
$$= 1 - \int_1^\infty \frac{\{u\}}{u^2} du = \gamma$$

Note: if we go through the argument carefully, the formula

$$\zeta(s) = \frac{s}{s-1} - s \int_1^\infty \{u\} u^{-s-1} du$$

(not $s \int_1^\infty \frac{\lfloor u \rfloor}{u^{s+1}} du$) actually converges for $\sigma = \operatorname{Re} s > 0$ (and agree with the old one when $\operatorname{Re} s > 1$) except at $s = 1$, so this is a

continuation of the zeta function to the left half-plane. Taking a result from complex analysis, we know that this is the *unique* meromorphic function (it still has a pole at $s = 1$) that extends the zeta function.

The corollary is quite lengthy, but it gives an important method that we will use to show the convergence of the Dirichlet series in general.

Theorem 4.5 (Local uniformness of Dirichlet series)**.** Suppose the Dirichlet series $\alpha(s) = \sum_{n=0}^{\infty} a_n n^{-s}$ converges (conditionally, no need for absolutely) at the point $s = s_0 = \sigma_0 + it_0$, and $H > 0$. Then $\alpha(s)$ is uniformly convergent in the sector $\mathcal{S} = \{s : \sigma \geq \sigma_0, |t - t_0| \leq H(\sigma - \sigma_0)\}$ (it looks like a fan, but not the entire half-plane).

Proof. Rewrite

$$\alpha(s) = \sum_{n=1}^{\infty} n^{s_0 - s} \left(a_n n^{-s_0}\right)$$

Substitute $a_n := -a_n n^{-s_0}$ (with $a_1 := \alpha(s_0) - a_1$) and $\phi(n) = n^{s_0 - s}$ into Abel summation formula, we get (for $M < N$ be integers, and $u > 1$)

$$\begin{aligned} R(u) = \sum_{1 \leq n \leq u} a_n &= \sum_{n=2}^{\infty} a_n n^{-s_0} - \sum_{n=2}^{\lfloor u \rfloor} a_n n^{-s_0} \\ &= \sum_{n=\lfloor u \rfloor + 1}^{\infty} a_n n^{-s_0} = \sum_{n > u} a_n n^{-s_0} \\ \sum_{n=M+1}^{N} a_n n^{-s} &= R(N)N^{s_0 - s} - R(M)M^{s_0 - s} - \int_M^N R(u) \left(\frac{d}{du} u^{s_0 - s}\right) du \\ &= R(N)N^{s_0 - s} - R(M)M^{s_0 - s} + (s - s_0) \int_M^N R(u) u^{s_0 - s - 1} du \end{aligned}$$

Note that $R(u) \to 0$ as $u \to \infty$, so for a given $\varepsilon > 0$, we can let $M < N$ be sufficiently large enough so that $|R(u)| < \varepsilon$ for all $u \geq N$. Hence,

$$\begin{aligned} \left| \sum_{n=M+1}^{N} a_n n^{-s} \right| &\leq |R(M)M^{s_0 - s}| + |R(M)N^{s_0 - s}| + |s_0 - s| \int_M^N |R(u)| \cdot |u^{s_0 - s - 1}| du \\ &< \varepsilon \left[M^{-(\sigma - \sigma_0)} + N^{-(\sigma - \sigma_0)} + |s - s_0| \int_N^M u^{\sigma_0 - \sigma - 1} du \right] \\ &\leq \varepsilon \left[2 + \frac{|s - s_0|}{\sigma - \sigma_0} \right] \end{aligned}$$

But for all s in the sector $\mathcal{S}$, we can bound the sum further! By triangle inequality, $|s - s_0| \leq \sigma - \sigma_0 + |t - t_0| \leq (H+1)(\sigma - \sigma_0)$, so

$$\left| \sum_{n=M+1}^{N} a_n n^{-s} \right| < (H+3)\varepsilon$$

As long as H is fixed, then the Dirichlet series $\alpha(s)$ converges uniformly in $\mathcal{S}$ by Cauchy uniform completeness. □

We can then define *abscissa of convergence* σ_c of a Dirichlet series α as the infimum of all σ such that $\alpha(\sigma + it)$ converges for some t.

Remark 4.6. By definition (and previous theorem), we know that $\alpha(s)$ converges for all $\operatorname{Re} s > \sigma_c$, and diverges for all $\operatorname{Re} s < \sigma_c$. In fact, $\alpha(s)$ is *holomorphic* on $\operatorname{Re} s > \sigma_c$ (a result of complex analysis since α uniformly converges on compact subsets).