Lecture notes on Dirichlet convolution

Siddhartha Sahi
Rutgers University

October 4, 2007

1 Convolution

An **arithmetic** function is a real or complex-valued function f whose domain is the set of natural numbers $\mathbb{N}$; e.g the Euler ϕ-function. If f, g are arithmetic functions, their **convolution** is defined as follows

$$(f * g)(n) := \sum_{d|n} f(d)\, g(n/d) = \sum_{d_1 d_2 = n} f(d_1)\, g(d_2)$$

It follows immediately from the definition that $f * g = g * f$, and also that

$$((f * g) * h)(n) = \sum_{d_1 d_2 d_3 = n} f(d_1)\, g(d_2)\, h(d_3) = (f * (g * h))(n)$$

Thus the convolution operation is *commutative* and *associative.*

Also if δ is the function $\delta(n) := \begin{cases} 1 & \text{if} \quad n = 1 \\ 0 & \text{if} \quad n > 1 \end{cases}$ then

$$(f * \delta)(n) = \sum_{d|n} f(d)\, \delta(n/d) = f(n)$$

Hence δ is an *identity* for the convolution operation.

2 Multiplicative functions

An arithmetic function f is said to be **multiplicative** if

$$f(n_1 n_2) = f(n_1)\, f(n_2) \ \text{ whenever} \gcd(n_1, n_2) = 1$$

We showed earlier that the Euler ϕ-function is multiplicative and we will see more examples in a moment.

By induction, one can see that a multiplicative function satisfies

$$f(n_1 n_2 \ldots n_k) = f(n_1)\, f(n_2) \ldots f(n_k) \ \text{ if the } n_i \text{ are pairwise coprime.}$$

In particular if $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ is the prime power decomposition of n, we get

$$f(n) = f(p_1^{a_1})\, f(p_2^{a_2}) \ldots f(p_k^{a_k})$$

Therefore f is completely determined by its values on prime powers p^a.

3 Dirichlet's theorem

Let $D(n)$ denote the set of divisors of n.

Lemma 1 *$d \in D(n_1 n_2)$ if and only if $d = d_1 d_2$ for some $d_1 \in D(n_1)$, $d_2 \in D(n_2)$.*

Proof. First suppose $d = d_1 d_2$ for some $d_1 | n_1$, $d_2 | n_2$. Then $n_1 = d_1 x_1, n_2 = d_2 x_2$.for some integers x_1, x_2, and hence $n_1 n_2 = (d_1 d_2) x_1 x_2$ and so $d = d_1 d_2$ divides $n_1 n_2$.

Conversely suppose d divides $n_1 n_2$. Let $d_1 = \gcd(d, n_1)$ then $\gcd(d/d_1, n_1/d_1) = 1$ and d/d_1 divides $(n_1 n_2/d_1) = (n_1/d_1) n_2$. Therefore d/d_1 divides n_2 and we can take $d_2 = d/d_1$. ■

Lemma 2 *Suppose* $\gcd(n_1, n_2) = 1$, *then*

1. *If $d_1 \in D(n_1)$ and $d_2 \in D(n_2)$ then* $\gcd(d_1, d_2) = 1$.
2. *The multiplication map $(d_1, d_2) \mapsto d_1 d_2$ is a bijection between $D(n_1) \times D(n_2)$ and $D(n_1 n_2)$.*

Proof. 1) Since $\gcd(d_1, d_2)$ divides d_1 and d_2, it divides n_1 and n_2, and hence divides $\gcd(n_1, n_2)$. Now $\gcd(n_1, n_2) = 1$ implies $\gcd(d_1, d_2) = 1$.

2) By the previous lemma, the map is surjective and so we only have to prove that is 1-1. Suppose that we have

$$d_1 d_2 = d_1' d_2' \text{ for some } d_1, d_1' \in D(n_1), \; d_2, d_2' \in D(n_2)$$

Then $d_1$divides $d_1' d_2'$; but by 1) d_1 is coprime to d_2', hence a_1 divides d_1'. Similarly d_1' divides d_1. Thus $d_1 = d_1'$, which implies $d_2 = d_2'$. Therefore the map is 1-1. ■

We can now prove the following useful result due to Dirichlet.

Theorem 3 *If f and g are multiplicative then so is $f * g$.*

Proof. If $\gcd(n_1, n_2) = 1$, then

$$\begin{aligned}
(f * g)(n_1 n_2) &= \sum_{d | n_1 n_2} f(d)\, g(n_1 n_2/d) \\
&= \sum_{d_1 | n_1, d_2 | n_2} f(d_1 d_2)\, g\left(\frac{n_1}{d_1}\frac{n_2}{d_2}\right) \text{ by Lemma 2 2)} \\
&= \sum_{d_1 | n_1, d_2 | n_2} f(d_1) f(d_2)\, g\left(\frac{n_1}{d_1}\right) g\left(\frac{n_2}{d_2}\right) \text{by Lemma 2 1)} \\
&= \sum_{d_1 | n_1} f(d_1)\, g\left(\frac{n_1}{d_1}\right) \sum_{d_2 | n_2} f(d_2)\, g\left(\frac{n_2}{d_2}\right) \\
&= (f * g)(n_1)(f * g)(n_2)
\end{aligned}$$

■

4 Examples of multiplicative functions

As noted earlier, the Euler ϕ-function is multiplicative.

The δ-function defined above is multiplicative as well, since

$$\delta(mn) = \delta(m)\,\delta(n) = \begin{cases} 1 & \text{if } m = n = 1 \\ 0 & \text{otherwise} \end{cases}.$$

Also the *exponential* function $e_k(n) := n^k$ is multiplicative since

$$e_k(mn) = (mn)^k = m^k n^k = e_k(m)\,e_k(n).$$

The function $\sigma_k := e_k * e_0$ is the sum of the kth powers of divisors of n

$$\sigma_k(n) := \sum_{d|n} e_k(d) * e_0(n/d) = \sum_{d|n} d^k$$

In particular $\sigma(n) = \sigma_1(n)$ is the sum of divisors and $d(n) = \sigma_0(n)$ is the number of divisors. By Dirichlet's theorem these are all multiplicative functions.

Theorem 4 *We have the following explicit formula:*

$$\sigma_k\left(\prod_i p_i^{a_i}\right) = \begin{cases} \prod_i \left(1 - p_i^{k(a_i+1)}\right) / \left(1 - p_i^k\right) & \textit{if } k \neq 0 \\ \prod_i (a_i + 1) & \textit{if } k = 0 \end{cases}$$

Proof. The divisors of p^a are p^e with $e \leq a$, and we get

$$\sigma_k(p^a) = \sum\nolimits_{e=0}^{a} e_k(p^e)\,e_0\left(p^{a-e}\right) = \sum\nolimits_{e=0}^{a} p^{ke}$$

For $k = 0$ we get $a + 1$, and for $k \neq 0$ we get $\left(1 - p^{k(a+1)}\right) / \left(1 - p^k\right)$. Since σ_k is multiplicative, the general result follows ■

5 Moebius inversion formula

The Moebius μ-function is defined as follows:

$$\mu(n) := \begin{cases} (-1)^r & \text{if } n = p_1 p_2 \ldots p_r \text{ with all } p_i \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

Thus $\mu(1) = (-1)^0 = 1$, $\mu(6) = (-1)^2 = 1, \mu(7) = -1$, $\mu(12) = 0$, etc.

Lemma 5 *The Meobius function is multiplicative, and we have $\mu * e_0 = \delta$.*

Proof. Suppose $\gcd(m, n) = 1$. Then mn is a product of distinct primes if and only if each of m, n is a product of distinct primes. In this case we have $\mu(mn) = (-1)^r = \mu(m)\,\mu(n)$ where r is the total number of prime factors of m and n. Otherwise we have $\mu(mn) = 0 = \mu(m)\,\mu(n)$.

Thus μ is multiplicative and by Dirichlet's theorem so is $\mu * e_0$. Thus it is enough to prove $(\mu * e_0)(p^a) = \delta(p^a)$ for all prime powers p^a. Now the divisors of p^a are p^e with $e \leq a$, thus we have

$$(\mu * e_0)(p^a) = \sum\nolimits_{e=0}^{a} \mu(p^e) e_0(p^{a-e}) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^a).$$

For $a > 0$ we get $(\mu * e_0)(p^a) = 1 - 1 + 0 + \ldots + 0 = 0 = \delta(p^a)$, while for $a = 0$ there is only one term and we get $(\mu * e_0)(1) = 1 = \delta(1)$. ■

Corollary 6 *(Moebius inversion formula) Let f, g be arithmetic functions then*

$$g(n) = \sum_{d|n} f(d) \text{ if and only if } f(n) = \sum_{d|n} g(d) \mu(n/d).$$

Moreover in this case g is multiplicative if and only if f is multiplicative.

Proof. The two conditions are $g = f * e_0$ and $f = g * \mu$, respectively. If $g = f * e_0$ holds then

$$g * \mu = (f * e_0) * \mu = f * (e_0 * \mu) = f * \delta = f$$

and the converse is similar. The multiplicativity follows from Dirichlet's theorem. ■

Definition 7 *If f, g are related as in the corollary above, we say that (f, g) is a Moebius pair.*

By definition, (e_k, σ_k) is a Moebius pair. Another important example is the following.

Proposition 8 *(ϕ, e_1) is a Moebius pair.*

Proof. It is enough to verfy that one of the two relations $\phi * e_0 = e_1$, $e_1 * \mu = \phi$ holds for prime powers p^a. We will check both

$$\begin{aligned}(\phi * e_0)(p^a) &= \sum_{e=0}^{a} \phi(p^e) e_0(p^{a-e}) = \sum_{e=0}^{a} \phi(p^e) \\ &= (p^a - p^{a-1}) + \ldots + (p^1 - 1) + 1 \\ &= p^a = e_1(p^a)\end{aligned}$$

Also

$$\begin{aligned}(e_1 * \mu)(p^a) &= \sum_{e=0}^{a} e_1(p^e) \mu(p^{a-e}) = \sum_{e=0}^{a} p^e \mu(p^{a-e}) \\ &= p^a(1) + p^{a-1}(-1) + 0 + \ldots + 0 \\ &= p^a - p^{a-1} = \phi(p^a).\end{aligned}$$

■

Corollary 9 *The following relation holds $\phi * \sigma_k = e_1 * e_k$.*

Proof. We have $\phi * \sigma_k = (e_1 * \mu) * (e_k * e_0) = (e_1 * e_k) * \delta = e_1 * e_k$. ■