adamant's blog

Dirichlet convolution. Part 2: Dirichlet series and prime counting

By **adamant**, [history](), 19 months ago, 🇬🇧

Hi everyone!

Recently I've published a [blog]() about how one can multiply and divide sequences with Dirichlet convolution. In this blog, we will learn about a convenient framework to reason about them in a "coordinate-free" notation, similar to how generating functions are used to analyze sequences under the regular convolution.

- **Part 1: Fast prefix sum computation**
- **Part 2: Dirichlet series and prime counting**

We will learn how to deal with Dirichlet multiplication and division in the framework of Dirichlet series, and derive a number of well known number theoretic results from this perspective. While doing so, we will learn about Riemann zeta function and will have a glimpse into why it is so important in analyzing behavior of prime numbers.

We will also learn how Dirichlet series framework helps us to, given $g(1), \ldots, g(n)$, to compute $f(1), \ldots, f(n)$ in $O(n \log n)$ such that $g(n)$ is the Dirichlet product of $f(n)$ with itself, repeated k times. Besides that, we will learn how to count prime numbers below n in $O(n^{2/3})$ using logarithms on Dirichlet series.

Convolutions recap

Let $a_1, a_2, \ldots$ and $b_1, b_2, \ldots$ be two sequences. We define their **Dirichlet convolution** as

$$(a * b)_k = \sum_{ij=k} a_i b_j.$$

Before working with it, let's recall what we did with other convolutions. Assume, more generically, that we want to analyze

$$c_k = \sum_{i \circ j=k} a_i b_j.$$

What we typically do to work with such convolutions is we introduce a family of functions ρ_i such that

$$\rho_i \rho_j = \rho_{i \circ j},$$

With these objects in mind, we can rewrite the expression above as

$$\sum_k c_k \rho_k = \sum_k \sum_{i \circ j=k} a_i b_j \rho_{i \circ j} = \left(\sum_i a_i \rho_i \right) \left(\sum_j b_j \rho_j \right).$$

Note that we vaguely described ρ_i as "functions" without going into detail about their type and/or domain. This is somewhat intentional, as specific applications may imply different specifications. Consider some standard examples (essentially taken from [here]()).

Examples

Dirichlet series

Now, what should we use for $i \circ j = ij$, where ij means simple multiplication? We already noticed that multiplying two exponents with the same base yields to summation in powers as $x^i x^j = x^{i+j}$. But what happens if we multiply two exponents with the same power? We get multiplication in bases, that is $x^s y^s = (xy)^s$. Thus, we define

$$\rho_i(s) = i^{-s},$$

where s is a positive integer greater than 1. Using such functions, we define the **Dirichlet series** of a sequence $a_1, a_2, \ldots$ as

$$\boxed{A(s) = \sum_{i=1}^{\infty} \frac{a_i}{i^s}}$$

This allows us to rewrite Dirichlet convolution as

$$C(s) = \sum_k \frac{c_k}{k^s} = \sum_k \sum_{ij=k} \frac{a_i b_j}{(ij)^s} = \left(\sum_i \frac{a_i}{i^s} \right) \left(\sum_j \frac{b_j}{j^s} \right) = A(s)B(s)$$

Note: We use i^{-s} instead of $\rho_i(s) = i^s$ by convention, and so that Dirichlet series converges for integer $s > 1$.

With formal power series, it is common to write $[x^k]F(x)$ to denote the coefficient near x^k of the expansion of $F(x)$. For notational convenience, we will also write $[n^{-s}]F(s)$ to denote the coefficient near n^{-s} of the Dirichlet series.

Dirichlet power

Consider the following problem from this blog by **jqdai0815**:

102471C - Dirichlet k-th root. Given $g(1), \ldots, g(n)$ and k, find $f(1), \ldots, f(n)$ such that $\overbrace{(f * \cdots * f)}^{k}(n) = g(n)$.

Solution. When talking about quickly raising functions to arbitrary powers, we generally have two options to proceed.

First option is to represent the power as $F^k(s) = \exp[k \log F(s)]$. Another option is to take the derivative and represent $G = F^k$ as
$$G'F = kF^k F' = kGF'.$$

The later is then used to represent the coefficients of $Q(s)$ as a reasonably small recurrence. For Dirichlet series,
$$\frac{\partial}{\partial s} \frac{1}{n^s} = \frac{\partial}{\partial s} e^{-s \ln n} = -\frac{\ln n}{n^s},$$

therefore the derivative of the full Dirichlet series rewrites as
$$F'(s) = -\sum_n \frac{f(n) \ln n}{n^s}.$$

Expanding both sides of $G'F = kGF'$ into Dirichlet product, we get
$$\boxed{\sum_{ab=n} f(b)g(a) \ln a = k \sum_{ab=n} g(a)f(b) \ln b}$$

Since individual terms of Dirichlet convolution involve much less summands than regular convolution (and the number of summands amortizes to $O(n \log n)$ over all indices), we could use the identity above to find $f(n)$ from the values of $g(n)$ and smaller values of $f(n)$. Except for, we need to print exact answer modulo prime number... What do we do about it?

Instead of $\ln n$, we need to use some function that behaves reasonably similar to $\ln n$ modulo prime numbers. But what kind of function could it be? What properties of $\ln n$ do we actually rely on in this recurrence? Well, first thing to notice is that we don't really need e to be the base of the logarithm, as we may multiply both sides by a constant to substitute it with some other base.

But that still won't do it. Instead, we should substitute the derivative with some other operation $D[\cdot]$, such that
$$D[F(s)^k] = kF(s)^{k-1} D[F(s)],$$

for any positive integer number k, and $D[F(s)]$ is something with a simple form. By induction, any operation $D[\cdot]$ satisfying Leibniz rule
$$D[F(s)G(s)] = F(s)D[G(s)] + D[F(s)]G(s)$$

will do. This is, in fact, how derivatives are *defined* in abstract algebra (see also closely related arithmetic derivative).

Since standard derivative multiplied $f(n)$ with $-\ln n$, it's reasonable to assume that the function we're looking for also applies to Dirichlet series component-wise, multiplying each $f(n)$ with another function $h(n)$. Then, the product rule rewrites as
$$h(n) \sum_{ab=n} f(a)g(b) = \sum_{ab=n} [h(a) + h(b)]f(a)g(b).$$

From this it follows that $h(n)$ could be any function such that $h(ab) = h(a) + h(b)$ for any positive integer a, b. This is it, this is the most important property of $\ln n$ in our context that we were looking for! Such functions are known as totally additive functions, and one natural example of it could be the prime omega function $\Omega(n)$, which is the number of prime divisors of n, counted with multiplicities.

Multiplicative functions

In number theory, first and most natural example of where Dirichlet series pop up are multiplicative functions. Let's see why.

A **multiplicative function** is a function $f : \mathbb{Z}_+ \mapsto \mathbb{C}$ such that $f(ab) = f(a)f(b)$ for any a, b such that $\gcd(a, b) = 1$.

From fundamental theorem of arithmetic it follows that multiplicative functions are fully defined by their values in powers of primes:

$$n = p_1^{d_1} \dots p_k^{d_k} \implies f(n) = f(p_1^{d_1}) \dots f(p_k^{d_k}).$$

Therefore, when working with multiplicative functions, it is often convenient, for each prime number p to consider the sequence

$$f(1), f(p), f(p^2), \dots,$$

and sometimes even its ordinary generating function (also known as the **Bell series**):

$$F_p(x) = \sum_k f(p^k) x^k,$$

as the Dirichlet product over just powers of primes corresponds to the regular product of such generating functions:

$$(f * g)(p^k) = \sum_{p^i p^j = p^k} f(p^i)g(p^j) = \sum_{i+j=k} f(p^i)g(p^j) = [x^k]F_p(x)G_p(x)$$

This connection re-expresses itself even more when treated through Dirichlet series framework. Let's, similarly to generating functions above, define the p-**component** of the multiplicative function's Dirichlet series $F_p(s)$ as

$$\boxed{F_p(s) = \sum_k \frac{f(p^k)}{p^{ks}}}$$

Using the notation of p-components, we can then find out that

$$\boxed{F(s) = \sum_n \frac{f(n)}{n^s} = \sum_n \frac{f(p_1^{d_1}) \dots f(p_k^{d_k})}{p_1^{-d_1 s} \dots p_k^{-d_k s}} = \left(\sum_{p_1} \frac{f(p_1^{d_1})}{p_1^{-d_1 s}} \right) \left(\sum_{p_2} \frac{f(p_2^{d_2})}{p_2^{-d_2 s}} \right) \dots = \prod_{p \text{ prime}} F_p(s)}$$

In other words, the full Dirichlet series can be represented as an infinite product over all primes (so-called **Euler product**):

$$\boxed{\sum_n \frac{f(n)}{n^s} = \prod_{p \text{ prime}} F_p(s)}$$

From this, for example, immediately follows that the Dirichlet convolution of multiplicative functions is a multiplicative function, as

$$F(s)G(s) = \prod_{p \text{ prime}} F_p(s) \prod_{p \text{ prime}} G_p(s) = \prod_{p \text{ prime}} F_p(s)G_p(s).$$

This result is quite important, as it allows us to analyze Dirichlet series of multiplicative functions as infinite sums *or* infinite products of good-looking functions, depending on what properties are of higher interest to us.

Examples and their Dirichlet series

In this section, we consider some well-known examples of multiplicative functions (taken mostly from here) and how their Dirichlet series are computed. As the main purpose of this section is to get a grasp of various perspectives used to work with Dirichlet series, we will consider several possible derivations for each function.

The constant function $I(n) = 1$. Since $I(p^k) = 1$, its p-components look like

$$\zeta_p(s) = \sum_k \frac{1}{p^{ks}} = \boxed{\frac{1}{1 - p^{-s}}}$$

Therefore, its Dirichlet series can be represented as

$$\boxed{\zeta(s) = \sum_n \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}}$$

This particular Dirichlet series is also known as the **Riemann zeta function**. From the result above it follows that multiplying the Dirichlet series of a multiplicative function $f(n)$ with the Riemann zeta function, results into a multiplicative function $g(n)$ such that

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

The Möbius function. In number theory, one often wants to inverse such transform, that is, to find $f(n)$ from a known $g(n)$. As we already noticed above, $G(s) = \zeta(s)F(s)$, thus we can express $F(s)$ as $F(s) = \zeta^{-1}(s)G(s)$. If you're familiar with Möbius inversion, you already know what happens next. We need to find the function $\zeta^{-1}(s)$ explicitly, and we can do so as

$$\zeta^{-1}(s) = \prod_{p \text{ prime}} (1 - p^{-s}).$$

If we fully expand it, we get

$$\boxed{\zeta^{-1}(s) = \sum_k (-1)^k \prod_{p_1,\dots,p_k \text{ prime}} \frac{1}{p_1^s \cdots p_k^s} = \sum_n \frac{\mu(n)}{n^s}}$$

In the identity above, we introduced the function $\mu(n)$ such that

$$\mu(n) = \begin{cases} (-1)^k, & n = p_1 \dots p_k, \\ 0, & \text{otherwise.} \end{cases}$$

The function $\mu(n)$ is also known as the Möbius function. It is a multiplicative function, that can be defined in powers of primes as $\mu(p^k) = [k = 0] - [k = 1]$, where $[\cdot]$ is the Iverson bracket, which evaluates to 1 if the expression inside is true and to 0 otherwise.

From this, we also get the **Möbius inversion formula**:

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

The power function $f(n) = n^a$. Since $f(p^k) = p^{ka}$, its p-components look like

$$F_p(s) = \sum_k \frac{p^{ka}}{p^{ks}} = \boxed{\frac{1}{1 - p^{a-s}}}$$

Thus, its Dirichlet series can be represented as

$$\boxed{F(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{a-s}} = \zeta(s - a)}$$

Of course, the same result can also be obtained directly as

$$F(s) = \sum_n \frac{n^a}{n^s} = \sum_n \frac{1}{n^{s-a}} = \zeta(s - a).$$

The divisor function $\sigma_a(n) = \sum_{d|n} d^a$. Since $\sigma_a(p^k) = \sum_{i \leq k} p^{ia}$, its p-components look like

$$F_p(s) = \sum_k \frac{1}{p^{ks}} \sum_{i \leq k} p^{ia} = \sum_i p^{ia} \sum_{k \geq i} \frac{1}{p^{ks}} = \sum_i p^{ai} \frac{p^{-is}}{1-p^{-s}} = \boxed{\frac{1}{1 - p^{-s}} \frac{1}{1 - p^{a-s}}}$$

This, in turn, means that its Dirichlet series can be represented as

$$\boxed{F(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} \frac{1}{1 - p^{a-s}} = \zeta(s)\zeta(s - a)}$$

Another way to get the same result directly is as follows:

$$F(s) = \sum_d d^a \sum_k \frac{1}{d^s k^s} = \sum_{d,k} \frac{1}{d^{s-a} k^s} = \zeta(s)\zeta(s - a).$$

And yet another way to get it is to express $\sigma_a(n)$ as the Dirichlet convolution of $f(n) = 1$ and $g(n) = n^a$. The first one has Dirichlet series $\zeta(s)$, and the second one has Dirichlet series $\zeta(s - a)$.

The Euler's totient function $\varphi(n)$. Since $\varphi(p^k) = p^k - p^{k-1}$, its p-components look like

$$F_p(s) = 1 + (p - 1) \sum_{k \geq 1} \frac{p^{k-1}}{p^{ks}} = 1 + \frac{p-1}{p} \sum_{k \geq 1} \frac{1}{p^{k(s-1)}} = 1 + \frac{p-1}{p} \frac{p^{1-s}}{1-p^{1-s}} = \boxed{\frac{1 - p^{-s}}{1 - p^{1-s}}}$$

Multiplying it over all p, we get

$$\boxed{F(s) = \prod_{p \text{ prime}} \frac{1 - p^{-s}}{1 - p^{1-s}} = \frac{\zeta(s - 1)}{\zeta(s)}}$$

Another way to derive it is to express $g(n) = n$ as the Dirichlet convolution of $\varphi(n)$ and $f(n) = 1$:

$$\sum_{d|n} \varphi\left(\frac{n}{d}\right) = n,$$

as $\varphi\left(\frac{n}{d}\right)$ is the amount of numbers k from 1 to n such that $\gcd(k, n) = d$. But the Dirichlet series of $g(n)$ is known to be $\zeta(s-1)$ and for $f(n)$ it's $\zeta(s)$, so this Dirichlet convolution, indeed, rewrites in terms of Dirichlet series as $\zeta(s)F(s) = \zeta(s-1)$.

Square-free indicator. Let $f(n)$ a function equals to 1 if n is square-free and to 0 otherwise. Its p-components are

$$F_p(s) = 1 + \frac{1}{p^s} = \boxed{\frac{1 - p^{-2s}}{1 - p^{-s}}}$$

Thus, the Dirichlet series of $f(n)$ is found as

$$\boxed{F(s) = \prod_{p \text{ prime}} \frac{1 - p^{-2s}}{1 - p^{-s}} = \frac{\zeta(s)}{\zeta(2s)}}$$

General power function. If $F(s)$ is the Dirichlet series of $f(n)$, then $F(s-a)$ is the Dirichlet series of $f(n)n^a$.

Totally multiplicative functions

A **totally multiplicative function** is a function $f : \mathbb{Z}_+ \to \mathbb{C}$, such that $f(a)f(b) = f(ab)$ for any a, b.

For a totally multiplicative functions, its Dirichlet series is even more restricted, as the function is fully determined by its values in primes:

$$n = p_1^{d_1} \dots p_k^{d_k} \implies f(n) = f(p_1)^{d_1} \dots f(p_k)^{d_k},$$

and its p-components must look like

$$F_p(s) = \sum_k \frac{f(p)^k}{p^{-ks}} = \frac{1}{1 - f(p)p^{-s}},$$

thus the Dirichlet series of a totally multiplicative function can be represented as

$$\boxed{F(s) = \prod_{p \text{ prime}} \frac{1}{1 - f(p)p^{-s}}}$$

Noteworthy, expanding the inverse of such function gives us

$$\boxed{F^{-1}(s) = \sum_k (-1)^k \prod_{p_1, \dots, p_k} \frac{f(p_1) \dots f(p_k)}{p_1^s \dots p_k^s} = \sum_n \frac{\mu(n)f(n)}{n^s}}$$

In other words, the inverse $g(n)$ of a totally multiplicative function is $g(n) = \mu(n)f(n)$. In particular, for power function $f(n) = n^a$, which is totally multiplicative, it means that the Dirichlet series of its inverse is

$$\boxed{\zeta^{-1}(s-a) = \sum_n \frac{\mu(n)n^a}{n^{-s}}}$$

Another example of a totally multiplicative function, which often occurs in a competitive programming context, is the Legendre symbol:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } a \equiv 0 \pmod{p}, \end{cases}$$

which can as well be defined explicitly as

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \quad \text{and} \quad \left(\frac{a}{p}\right) \in \{-1, 0, 1\}.$$

It is totally multiplicative in its top argument, as

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

$\exp$, $\log$ and prime-counting

Library Judge — Counting Primes. Count the number of primes no more than $n \leq 10^{11}$.

This approach was originally shared by **ecnerwala** in this comment.

We can apply logarithms and exponents to Dirichlet series, as defined by their series representations:

$$\log \frac{1}{1-x} = \sum_{k=1}^{\infty} \frac{x^k}{k}, \quad \exp x = \sum_{k=0}^{\infty} \frac{x^k}{k!}.$$

Applying the logarithm series definition to $\zeta(s)$, we get

$$\boxed{\log \zeta(s) = \sum_{p \text{ prime}} \log \frac{1}{1-p^{-s}} = \sum_{p \text{ prime}} \sum_{k=1}^{\infty} \frac{p^{-ks}}{k} = \sum_{k=1}^{\infty} \frac{1}{k} \sum_{p \text{ prime}} \frac{1}{(p^k)^s}}$$

In other words,

$$[n^{-s}] \log \zeta(s) = \begin{cases} \frac{1}{k}, & n = p^k, \\ 0, & \text{otherwise.} \end{cases}$$

That being said, if we compute prefix sums of a function with Dirichlet series $\log \zeta(s)$ up to n, we can then subtract corresponding counts over $p^2, p^3, \ldots$ to get the prime-counting function $\pi(n)$. But how do we find the prefix sums of the logarithm of $\zeta(s)$?

We can use another series representation of the logarithm as

$$\log(1+x) = -\sum_{k=1}^{\infty} \frac{(-1)^k x^k}{k},$$

and plug in $\zeta(s) - 1$ instead of x. Note that when $f(1) = 0$, the values of $F(s)^k$ have a quickly vanishing prefix, as
$$[n^{-s}]F^k(s) = \sum_{\substack{a_1 \ldots a_k = n \\ a_1, \ldots, a_k \geq 2}} f(a_1) \ldots f(a_n).$$

Therefore, the prefix of $(\zeta(s) - 1)^k$ consists entirely of zeros for $n < 2^k$. Thus, we're only interested in $F^k(s)$ for $k \leq \log_2 n$. To compute these powers, we can use the approach shared by **ecnerwala** in the comment to my previous blog about Dirichlet convolutions.

We can split the space of $xyz \leq n$ into $O(n^{2/3})$ rectanges $[x_0, x_1] \times [y_0, y_1] \times [z_0, z_1]$ and use such splitting to compute prefix sums over Dirichlet series $H(s) = F(s)G(s)$ or $F(s) = H(s)/G(s)$, assuming that the prefix sums of the series on the right-hand side are known. Doing it as is would take $O(n^{2/3} \log n)$, but we can speed up the whole computation. Let $t \approx n^{1/6}$, then
$$\zeta_t(s) = \prod_{\substack{p \text{ prime} \\ p > t}} \frac{1}{1-p^{-s}}$$

has an empty prefix of length t, and we will only need first $\frac{\log n}{\log t}$ values of $(\zeta_t(s) - 1)^k$ instead of $\log n$ to compute the prefix sums of $\log \zeta_t(s)$ up to n. To find $\zeta_t(s)$ itself, we should use the fact that multiplying with $1 - p^{-s}$ can be done in $O(\sqrt{n})$, as after such multiplication $F(\lfloor n/k \rfloor)$ simply gets reduced by $F(\lfloor n/(kp) \rfloor)$.

After this, we can add the contributions of first t terms back into logarithm to recover $\log \zeta(s)$ from $\log \zeta_t(s)$.

Note 1: As **ecnerwala** mentioned, this approach could more generally be used to sum up any totally multiplicative function over all primes up to n. Indeed, the logarithm of the Dirichlet series of a totally multiplicative function is

$$\boxed{\log F(s) = \log \prod_{p \text{ prime}} \frac{1}{1-p(s)p^{-s}} = \sum_{k=1}^{\infty} \frac{1}{k} \sum_{p \text{ prime}} \frac{f(p)^k}{(p^k)^s}}$$

Thus, as we see,

$$[n^{-s}] \log F(s) = \begin{cases} \frac{f(p)^k}{k}, & n = p^k, \\ 0, & \text{otherwise.} \end{cases}$$

Note 2: The approach above can also be used to compute prefix sums of logarithms and exponents of any Dirichlet series. Generally, we can represent any Dirichlet series as an infinite product over not necessarily prime numbers as

$$\boxed{\sum_{n=1}^{\infty} \frac{g(n)}{n^s} = \prod_{n=1}^{\infty} \frac{1}{1-f(n)n^{-s}}}$$

In his comment, **ecnerwala** calls $g(n)$ the **pseudo-Euler transform** of $f(n)$, in reference to Euler transform of integer sequences. Similarly to what we did with primes, we can find $f(1), \ldots, f(t)$ for $t \approx n^{1/6}$ and divide $G(s)$ by corresponding fractions to get

$$G_t(s) = \prod_{n > t} \frac{1}{1 - f(n)n^{-s}},$$

so that we can find prefix sums of $G_t(s)$ in $O(n^{2/3})$, and then amend them with logarithms of fractions to get $\log G(s)$. To find $G_t(s)$ itself we, again, shout notice that, again, multiplying $G(s)$ with $1 - f(t)t^{-s}$ can be done in $O(\sqrt{n})$, as after such multiplication, the value $F(\lfloor n/k \rfloor)$ gets reduced by $f(t)F(\lfloor n/(kt) \rfloor)$.

Note 3: The logarithm $\log \zeta(s)$ connects the Riemann zeta function with the prime zeta function

$$P(s) = \sum_{p \text{ prime}} \frac{1}{p^s}.$$

This connection, in turn, allows to express the prime zeta function in terms of Riemann zeta function through generalized Möbius inversion:

$$\boxed{\log \zeta(s) = \sum_{k=1}^{\infty} \frac{P(ks)}{k} \iff P(s) = \sum_{k=1}^{\infty} \frac{\mu(k)}{k} \log \zeta(ks)}$$

See also

- **Counting primes in $\tilde{O}(n^{2/3})$** — also the comment by **ecnerwala** on the approach through Dirichlet series.
- **Lucy's Algorithm + Fenwick Trees** — another approach to count primes up to n in $O(n^{2/3} \log^{1/3} n)$.

◆◆ dirichlet convolution,   tutorial