MATH 361: NUMBER THEORY — THIRD LECTURE

The topic of this lecture is *arithmetic functions and Dirichlet series*. Euler's proof that the sum $\sum 1/p$ of the reciprocal primes diverges is used to introduce the function $\zeta(s)$ as a Dirichlet series that has an Euler product representation. We then proceed to formal Dirichlet series in general, noting that their multiplication encodes the convolution of the arithmetic functions that give their coefficients. Various results about arithmetic functions, in particular the famous Möbius inversion formula, now follow from observations about Dirichlet series. Arithmetic functions having a particular property called multiplicativity correspond to Dirichlet series having Euler product representations, with so-called totally multiplicative arithmetic functions matching up with particularly nice Euler products. At the end of the writeup we prove a more general version of Möbius inversion, with no reference to Dirichlet series, in order to give an important example of its use, the cyclotomic polynomial formula.

Contents

1. Introduction

By way of introduction, consider Euclid's proof that there exist infinitely many primes: *If p_1 through p_n are prime then the number*

$$q = 1 + \prod_{i=1}^{n} p_i$$

is not divisible by any p_i. According to this argument, the next prime after p_1 through p_n could be as large as q. The overestimate is astronomical. Specifically, compute that for $n \geq 3$, because

$$p_n \leq 1 + p_1 \cdots p_{n-1} \leq (7/6) p_1 \cdots p_{n-1},$$

it follows that

$$\begin{aligned} p_n &\le (7/6)p_1 \cdots p_{n-1} \\ &\le (7/6)^2 (p_1 \cdots p_{n-2})^2 \\ &\le (7/6)^4 (p_1 \cdots p_{n-3})^4 \\ &\le \cdots \\ &\le (7/6)^{2^{n-3}} (p_1 p_2)^{2^{n-3}} \\ &= 7^{2^{n-3}} \quad (\text{because } p_1 p_2 = 6) \\ &< e^{2^{n-2}}. \end{aligned}$$

So, for example, the tenth prime p_{10} satisfies $p_{10} < 1.51143 \times 10^{11}$. Because in fact $p_{10} = 29$, we see how little Euclid's argument tells us.

By contrast, Euler argued that

$$\sum_{p \in \mathcal{P}} \frac{1}{p} \quad \textit{diverges},$$

and in fact his argument shows more. The argument proceeds as follows. Define

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s > 1.$$

The basic estimate $\int_1^\infty x^{-s}\,\mathrm{d}x < \zeta(s) < 1 + \int_1^\infty x^{-s}\,\mathrm{d}x$, obtained by first placing boxes of base 1 over the $y = 1/x$ curve and then shifting them leftward by 1 so that they lie under the curve, shows that as s approaches 1 from the right, $\zeta(s)$ is asymptotic to $1/(s-1)$ and so $\log \zeta(s)$ is asymptotic to $\log(1/(s-1))$. Here the logarithm is natural, of course. Thus

$$\lim_{s \to 1^+} \zeta(s) = \infty,$$

and also

$$\lim_{s \to 1^+} \log \zeta(s) = \infty.$$

Now, summing over values of n with steadily more prime factors gives

$$\begin{aligned} \sum_{n=2^{e_2}} n^{-s} &= \sum_{e_2=0}^{\infty} (2^{-s})^{e_2} = (1-2^{-s})^{-1}, \\ \sum_{n=2^{e_2}3^{e_3}} n^{-s} &= \sum_{e_2=0}^{\infty} (2^{-s})^{e_2} \sum_{e_3=0}^{\infty} (3^{-s})^{e_3} = (1-2^{-s})^{-1}(1-3^{-s})^{-1}, \\ &\vdots \\ \sum_{n=2^{e_2}\cdots p^{e_p}} n^{-s} &= (1-2^{-s})^{-1} \cdots (1-p^{-s})^{-1}. \end{aligned}$$

And so, being very casual about convergence, it is essentially a restatement of unique factorization that the zeta function also has an infinite product expression,

$$\zeta(s) = \sum_{n \in \mathbb{Z}^+} n^{-s} = \prod_{p \in \mathcal{P}} (1-p^{-s})^{-1}.$$

From the general series

$$\log(1-X)^{-1} = \sum_{n=1}^{\infty} X^n/n, \quad |X|<1,$$

we have (again being very casual about convergence)

$$\begin{aligned}\log\zeta(s) &= \log\prod_{p\in\mathcal{P}}(1-p^{-s})^{-1} = \sum_{p\in\mathcal{P}}\log(1-p^{-s})^{-1} = \sum_{p\in\mathcal{P}}\sum_{n=1}^{\infty}\frac{p^{-ns}}{n}\\ &= \sum_{p\in\mathcal{P}} p^{-s} + \sum_{p\in\mathcal{P}}\sum_{n=2}^{\infty}\frac{p^{-ns}}{n}\,.\end{aligned}$$

From above, we know that $\lim_{s\to 1^+}\log\zeta(s)=\infty$, and the dominant term $\sum_{p\in\mathcal{P}} p^{-s}$ at the end of the previous display is what we want to understand as s tends to 1. The other term is small,

$$\sum_{\substack{p\in\mathcal{P}\\ n\ge 2}}\frac{p^{-ns}}{n} < \sum_{\substack{p\in\mathcal{P}\\ n\ge 2}} p^{-n} = \sum_{p\in\mathcal{P}}\frac{1}{p^2(1-p^{-1})} = \sum_{p\in\mathcal{P}}\frac{1}{p(p-1)} < \sum_{n=2}^{\infty}\frac{1}{n(n-1)} = 1.$$

This shows that the quantity that we want to understand is close to a quantity that we do understand,

$$\left|\sum_{p\in\mathcal{P}} p^{-s} - \log\zeta(s)\right| < 1.$$

And so

$$\lim_{s\to 1^+}\sum_{p\in\mathcal{P}} p^{-s} = \infty,$$

and more specifically,

$$\lim_{s\to 1^+}\frac{\sum_p p^{-s}}{\log\zeta(s)} = 1.$$

This strong suggests, although it doesn't show, that *the sum of prime reciprocals grows asymptotically as the logarithm of the harmonic series*. Recall that the partial sums of the harmonic series themselves grow logarithmically, so that the sum of prime reciprocals grows very slowly. Euler's result is far stronger than Euclid's, and it illustrates *analytic number theory*.

2. Dirichlet Series

The zeta function is a particular instance of a *Dirichlet series*.

Definition 2.1. *An* **arithmetic function** *is a complex-valued function of positive integers,*

$$f : \mathbb{Z}^+ \longrightarrow \mathbb{C}.$$

Its associated **Dirichlet series** *is a formal series that depends on a parameter s,*

$$F(s) = \sum_{n=1}^{\infty}\frac{f(n)}{n^s}\,.$$

Using Dirichlet series to discuss arithmetic functions is not really necessary, but I think that the Dirichlet series clarify what is going on.

Let F and G be the Dirichlet series associated to the arithmetic functions f and g. Compute that their product is

$$F(s)G(s) = \sum_d \frac{f(d)}{d^s} \sum_e \frac{g(e)}{e^s} = \sum_{d,e} \frac{f(d)g(e)}{(de)^s} = \sum_n \frac{\sum_{de=n} f(d)g(e)}{n^s}.$$

Thus, if we define the **convolution** (or **Dirichlet product**) of f and g to be

$$f * g : \mathbb{Z}^+ \longrightarrow \mathbb{C}, \quad (f*g)(n) = \sum_{de=n} f(d)g(e)$$

(also $(f*g)(n) = \sum_{d|n} f(d)g(n/d) = \sum_{d|n} f(n/d)g(d)$, and we freely use any of the three formulas for $f*g$) then the corresponding product of Dirichlet series is

$$F(s)G(s) = \sum_{n=1}^{\infty} \frac{(f*g)(n)}{n^s}\,.$$

That is, for arithmetic functions f, g, and h, and for Dirichlet series F, G, and H,

$$\boxed{h = f*g \iff H = FG.}$$

Because the multiplication of Dirichlet series is associative and commumative,

$$\big(F(s)G(s)\big)H(s) = F(s)\big(G(s)H(s)\big) \quad \text{and} \quad F(s)G(s) = G(s)F(s)$$

(for the left equality, both are $\sum_n \sum_{cde=n} f(c)g(d)h(e)/n^s$), the same properties hold for the convolution of arithmetic functions,

$$(f*g)*h = f*(g*h) \quad \text{and} \quad f*g = g*f.$$

And because Dirichlet series with nonzero leading term are invertible ($\sum a_n n^{-s}$ has inverse $\sum b_n n^{-s}$ where $b_1 = a_1^{-1}$ and $b_n = -a_1^{-1} \sum_{1<d|n} a_d b_{n/d}$ for $n > 1$), it follows from the boxed equivalence that the arithmetic functions that do not vanish at 1 form a group under convolution.

3. Examples, Möbius Inversion

With the boxed equivalence in mind, we create a small catalogue of arithmetic functions and their Dirichlet series.

- The **identity** arithmetic function is

$$\mathrm{id}(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

  The corresponding Dirichlet series is simply

$$\mathbb{I}(s) = 1.$$

  Because $\mathbb{I}(s)$ is the multiplicative identity, id is the convolution identity.
- The **unit** arithmetic function is

$$u(n) = 1 \quad \text{for all } n.$$

  (Ireland and Rosen call this function I.) The corresponding Dirichlet series is the zeta function,

$$U(s) = \zeta(s).$$

- The reciprocal of the zeta function is the Dirichlet series

$$\zeta(s)^{-1} = \prod_p (1 - p^{-s}) = 1 - \sum_p p^{-s} + \sum_{p,q} (pq)^{-s} - \sum_{p,q,r} (pqr)^{-s} + \cdots .$$

The corresponding arithmetic function is the **Möbius function**,

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 \cdots p_k \text{ (distinct primes)}, \\ 0 & \text{if } n \text{ is divisible by a nontrivial square.} \end{cases}$$

The first case in the previous formula says in particular that $\mu(1) = 1$. Because $\zeta(s)$ and $\zeta(s)^{-1}$ are Dirichlet series inverses, u and μ are convolution inverses,

$$\mu * u = \mathrm{id}.$$

That is, because u always returns the value 1,

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

The reader may enjoy verifying this directly, without reference to Dirichlet series.

More generally, for any arithmetic functions f and g, because u and μ are inverses, we have the **Möbius Inversion Principle**,

$$\boxed{g = f * u \iff f = g * \mu.}$$

Usually this equivalence is written as the **Möbius Inversion Formula**,

$$\boxed{g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} g(d)\mu(n/d).}$$

Often the idea is that f is interesting but we don't immediately have a formula for it, while $g = f * u$ is easy to compute, so that Möbius inversion gives a formula for f. For example, consider two arithmetic functions,

$$f(n) = \text{sum of the primitive } n\text{th roots of 1},$$
$$g(n) = \text{sum of all } n\text{th roots of 1}.$$

Here f is interesting while the finite geometric sum formula shows that g is simply the convolution identity function id. The relation $f * u = g = \mathrm{id}$ says that f is the convolution inverse of u, the Möbius function. That is,

$$\text{sum of the primitive } n\text{th roots of } 1 = \mu(n).$$

The reader can enjoy verifying this for $n = 1, 2, 3, \ldots$ through the first value of n where it is not easy.

4. The Euler Totient Function

The **Euler totient function** is an arithmetic function,

$$\varphi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+, \quad \varphi(n) = \#\{x \in \{0, \ldots, n-1\} : \gcd(x, n) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^\times.$$

For the least equality in the previous display, $\gcd(x, n) = 1$ if and only if there exist a and b such that $ax + bn = 1$, which holds if and only if there exists a such that $ax \equiv 1 \bmod n$, i.e., $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Thus $\varphi(1) = 1$ and $\varphi(p) = p - 1$ for p prime.

Now we set up Möbius inversion by counting that

$$n = \sum_{d|n} \varphi(d) \quad \text{for all } n \in \mathbb{Z}^+.$$

Indeed, noting that $((n/d)k, n) = (n/d)(k, d)$ for the second equality to follow,

$$\begin{aligned} \{0, \dots, n-1\} &= \bigsqcup_{d|n} \{x \in \{0, \dots, n-1\} : (x, n) = n/d\} \\ &= \bigsqcup_{d|n} \{(n/d)k : 0 \le k < d,\ (k, d) = 1\}, \end{aligned}$$

and the desired counting formula $n = \sum_{d|n} \varphi(d)$ follows immediately by definition of the totient function. (As an example, if $n = 20$ then the disjoint union is, with $d = 1, 2, 4, 5, 10, 20$,

$$\{0\} \sqcup \{10\} \sqcup \{5, 15\} \sqcup \{4, 8, 12, 16\} \sqcup \{2, 6, 14, 18\} \sqcup \{1, 3, 7, 9, 11, 13, 17, 19\},$$

and then, e.g., for $d = 10$ the set $\{2, 6, 14, 18\} = (20/10) \cdot \{1, 3, 7, 9\}$ contains $\varphi(10) = 4$ elements.) Consequently, Möbius inversion gives

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

That is,

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = n \left(1 - \sum_{p|n} \frac{1}{p} + \sum_{p,q|n} \frac{1}{pq} - \cdots \right).$$

The alternating sum-of-sums factors to give the formula for the totient function,

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

Alternatively one can obtain the formula $\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$ by inclusion–exclusion, leading to the boxed formula for $\varphi(n)$ and also giving $n = \sum_{d|n} \varphi(d)$ for all $n \in \mathbb{Z}^+$ by Möbius inversion. In functional language, introducing the arithmetic function

$$i : \mathbb{Z}^+ \longrightarrow \mathbb{Z}, \qquad i(n) = n,$$

which is neither the convolution identity function id nor the unit function u from earlier, we have shown that $i = \varphi * u$, so that $\varphi = i * \mu$, but alternatively one can proceed from $\varphi = i * \mu$ to $i = \varphi * u$.

Some consequences of the totient function formula are

$$\begin{aligned} \varphi(p^e) &= p^e - p^{e-1} \quad \text{for } e \ge 1 \text{ (this is even if } p > 2 \text{ or } e \ge 1), \\ \varphi(mn) &= \varphi(m)\varphi(n) \quad \text{if } (m, n) = 1, \\ a \mid b &\implies \varphi(a) \mid \varphi(b), \\ n \ge 3 &\implies \varphi(n) \text{ is even}, \\ n = p_1^{e_1} \cdots p_k^{e_k} &\implies 2^k \mid \varphi(n) \text{ if all } p_i > 2 \text{ or } 4 \mid n. \end{aligned}$$

5. Two More Arithmetic Functions

The **kth power function** is

$$\pi_k : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+, \qquad \pi_k(n) = n^k.$$

The function $i(n) = n$ from just above is π_1, and the function $u(n) = 1$ from earlier is π_0. The **sum of divisor kth powers function** is

$$\sigma_k : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+, \qquad \sigma_k(n) = \sum_{d|n} d^k.$$

Especially, σ_0 counts the divisors of n and σ_1 sums them.

The Dirichlet series of π_k is

$$\Pi_k(s) = \zeta(s-k),$$

whose multiplicative inverse is

$$\zeta^{-1}(s-k) = \sum_{n\geq 1} \frac{\mu(n)}{n^{s-k}} = \sum_{n\geq 1} \frac{(\pi_k\mu)(n)}{n^s},$$

and so the convolution inverse of π_k is $\pi_k\mu$. Because $\sigma_k = \pi_k * u$ is a convolution, its convolution inverse is the convolution of the individual convolution inverses, $\pi_k\mu * \mu$. Also, the Dirichlet series $\Sigma_k(s)$ of σ_k is the product of the corresponding Dirichlet series,

$$\Sigma_k(s) = \zeta(s-k)\zeta(s),$$

as can be checked directly for practice. Möbius inversion of the relation $\sigma_k = \pi_k * u$ gives $\pi_k = \sigma_k * \mu$, i.e.,

$$n^k = \sum_{d|n} \sigma_k(d)\mu(n/d), \quad n \geq 1.$$

Altogether, we now have the convolution identity function id (recall that $\mathrm{id}(n)$ is 1 for $n = 1$ and is 0 for $n > 1$); and the convolution inverse pairs $(\pi_k, \pi_k\mu)$, including (u, μ) when $k = 0$ (recall that $u(n) = 1$ for all n); and the convolution inverse pairs $(\sigma_k, \pi_k\mu * \mu)$, with $\sigma_k = \pi_k * u$ by definition and $\pi_k = \sigma_k * \mu$ in consequence; and Euler's totient function is $\varphi = \pi_1 * \mu = i * \mu$ so that $i = \varphi * u$ (recall that $i(n) = n$ for all n).

We mention the not-at-all-obvious fact that, letting $r(n, 4)$ denote the number of representations of n as a sum of 4 squares,

$$r(n, 4) = 8\,\sigma_1(n) \quad \text{if } 4 \nmid n$$

For example, one can check directly that $r(3, 4) = 32$ and also $8\sigma_1(3) = 32$, but $r(4, 4) = 24$ while $8\sigma_1(4) = 56$.

6. Multiplicative and Totally Multiplicative Functions

Definition 6.1. *Let $f : \mathbb{Z}^+ \longrightarrow \mathbb{C}$ be an arithmetic function. Then f is* **multiplicative** *if*

$$f(nm) = f(n)f(m) \quad \textit{for all } n \textit{ and } m \textit{ such that } (n, m) = 1,$$

and f is **totally multiplicative** *if*

$$f(nm) = f(n)f(m) \quad \textit{for all } n \textit{ and } m.$$

Thus:

For nonzero multiplicative functions, $f(1) = 1$ *and* $f(\prod_p p^{e_p}) = \prod_p f(p^{e_p})$.

And:

For totally multiplicative functions, furthermore $f(\prod_p p^{e_p}) = \prod_p f(p)^{e_p}$.

The corresponding Dirichlet series conditions are

$$f \text{ is multiplicative } \iff F(s) = \prod_p \sum_{e=0}^{\infty} \frac{f(p^e)}{p^{es}}$$

and

$$f \text{ is totally multiplicative } \iff F(s) = \prod_p (1 - f(p)p^{-s})^{-1}.$$

The first equivalence follows from the formal identity that for any arithmetic function f,

$$\prod_p \sum_{e=0}^{\infty} \frac{f(p^e)}{p^{es}} = \sum_{n=1}^{\infty} \frac{\prod_{p^{e_p} \| n} f(p^{e_p})}{n^s},$$

because the right side is the Dirichlet series of f exactly when f is multiplicative. Here the notation $p^{e_p} \| n$ means that p^{e_p} is the highest power of p that divides n. The second equivalence follows from the first and from the geometric series formula.

Some further facts that are straightforward to check, either directly or by using Dirichlet series, are

- If f and g are multiplicative then so is $f * g$.
- If f is multiplicative and nonzero then so is the convolution inverse of f.
- If f is totally multiplicative and nonzero then its convolution inverse is $f\mu$.

We have seen the third bullet for $f = \pi_k$.

To establish the first bullet using Dirichlet series, compute that because f and g are multiplicative, their Dirichlet series are

$$F(s) = \prod_p \sum_{e=0}^{\infty} \frac{f(p^e)}{p^{es}} \quad \text{and} \quad G(s) = \prod_p \sum_{e=0}^{\infty} \frac{g(p^e)}{p^{es}},$$

and then it follows quickly that

$$F(s)G(s) = \prod_p \sum_{e=0}^{\infty} \frac{(f * g)(p^e)}{p^{es}},$$

so that $f * g$ is again multiplicative.

The second bullet says that if f is multiplicative and nonzero then so is the convolution inverse of f. To establish this using Dirichlet series, let g be the convolution inverse of f, and consider the Dirichlet series

$$H(s) = \prod_p \sum_{e=0}^{\infty} \frac{g(p^e)}{p^{es}}.$$

As above, $F(s)H(s)$ multiplies out to $\prod_p \sum_{e=0}^{\infty} (f * g)(p^e)/p^{es}$, and because g is the convolution inverse of f, this is 1. That is, $H(s)$ inverts $F(s)$, showing that $H(s)$ is the Dirichlet series of g, and now the form of H shows that g is multiplicative.

The third bullet says that if f is totally multiplicative and nonzero then its convolution inverse is $f\mu$. To establish this using Dirichlet series, we need to show that the inverse $F(s)^{-1}$ of the Dirichlet series of f is the Dirichlet series $\sum_n (f\mu)(n)/n^s$ of $f\mu$. Compute that indeed because $F(s) = \prod_p (1 - f(p)p^{-s})^{-1}$,

$$\begin{aligned} F(s)^{-1} &= \prod_p (1 - f(p)p^{-s}) \\ &= 1 - \sum_p f(p)p^{-s} + \sum_{p,q} f(pq)(pq)^{-s} - \sum_{p,q,r} f(pqr)(pqr)^{-s} + \cdots \\ &= \sum_{n=1}^{\infty} \frac{f(n)\mu(n)}{n^s}, \end{aligned}$$

as desired. Also, we can establish the third bullet very quickly without Dirichlet series, by recalling from section 3 that $\sum_{d|n} \mu(d)$ is 1 for $n = 1$ and is 0 for $n > 1$, and computing that

$$(f * f\mu)(n) = \sum_{d|n} f(n/d)f(d)\mu(d) = f(n) \sum_{d|n} \mu(d) = \mathrm{id}(n).$$

As an example of the first bullet, the observation from earlier that $\sigma_k = \pi_k * u$ now says that σ_k is multiplicative because π_k and u are, and indeed the verification of the Dirichlet series $\Sigma_k(s) = \zeta(s-k)\zeta(s)$, earlier left as an exercise, shows that σ_k is determined completely by the values $\sigma_k(p^e)$. By the finite geometric sum formula, these are

$$\sigma_k(p^e) = \frac{p^{(e+1)k} - 1}{p^k - 1}.$$

For another example, because Euler's totient function is the convolution $\varphi = \pi_1 * \mu$, where $\pi_1(n) = n$ and μ is the Möbius function, its Dirichlet series is the corresponding product

$$\Phi(s) = \zeta(s-1)\zeta(s)^{-1} = \prod_p (1 - p^{1-s})^{-1}(1 - p^{-s}).$$

Here the Euler factor $1 - p^{-s}$ of $\zeta(s)^{-1}$ is $\sum_{e \geq 0} \mu(p^e)p^{-es}$, the general Euler factor formula for a multiplicative function specialized to μ. Because π_1 and μ are multiplicative, so is φ, and so its Dirichlet series is

$$\Phi(s) = \prod_p \sum_{e=0}^{\infty} \frac{\varphi(p^e)}{p^{es}}.$$

Match Euler factors to show that for every prime p,

$$\sum_{e=0}^{\infty} \frac{\varphi(p^e)}{p^{es}} = (1 - p^{1-s})^{-1}(1 - p^{-s}).$$

Of course this can be verified directly, noting that $\varphi(p^e)$ is 1 for $e = 0$ and is $p^e(1 - p^{-1})$ for $e \geq 1$.

7. Abelian Group Möbius Inversion and Cyclotomic Polynomials

The arithmetic functions in this writeup have been complex-valued, but more generally we may take arithmetic functions from the positive integers to any abelian group, and Möbius inversion still holds.

To see this, note that any abelian group G carries not only addition but also scalar multiplication by $\mathbb{Z}$; e.g., $3g$ means $g+g+g$ and $(-5)g$ means $-(5g)$, taking the latter inverse in G. Now, for any functions $w : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ and $f : \mathbb{Z}^+ \longrightarrow G$, define

$$w * f : \mathbb{Z}^+ \longrightarrow G$$

to be

$$(w * f)(n) = \sum_{de=n} w(d)f(e) \quad \text{(adding and scaling in } G\text{)}.$$

If also $v : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ is integer-valued on $\mathbb{Z}^+$ then for any $n \in \mathbb{Z}^+$,

$$\begin{aligned}
(v * (w * f))(n) &= \sum_{de=n} v(d)(w * f)(e) \\
&= \sum_{de=n} \sum_{bc=e} v(d)w(b)f(c) \\
&= \sum_{bcd=n} v(d)w(b)f(c) \\
&= \sum_{ac=n} \sum_{bd=a} v(d)w(b)f(c) \\
&= \sum_{ac=n} (v * w)(a)f(c) \\
&= ((v * w) * f)(n).
\end{aligned}$$

Thus associativity still holds, $v*(w*f) = (v*w)*f$, with $v*w$ the usual convolution of integer-valued functions. Especially, $u*(\mu*f) = (u*\mu)*f = f$ by associativity and because $u*\mu = \mathrm{id}$ is still the convolution identity, and similarly $\mu*(u*f) = f$. Abelian group Möbius inversion follows: For functions $f, g : \mathbb{Z}^+ \longrightarrow G$,

$$g = u * f \iff f = \mu * g.$$

The **cyclotomic polynomials** $\Phi_n(X)$ for $n \geq 1$ are defined by the condition

$$X^n - 1 = \prod_{d|n} \Phi_d(X) \quad \text{for } n \geq 1, \qquad \text{each } \Phi_d \text{ monic}.$$

For example, $\Phi_1(X) = X - 1$ and $X^p - 1 = (X-1)\Phi_p(X)$ for p prime, so that $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. We state some facts about the cyclotomic polynomials without proof.

- The cyclotomic polynomials have integer coefficients.
- The degree of Φ_n is $\varphi(n)$, and the complex roots of Φ_n are the primitive nth complex roots of unity, $e^{2\pi ik/n}$ where $0 \leq k < n$ and $\gcd(k, n) = 1$.
- The cyclotomic polynomials are irreducible as polynomials over $\mathbb{Q}$.
- Every cyclotomic polynomial $\Phi_n(X)$ for $n > 1$ has constant term 1.

Now, let our abelian group G be $\mathbb{Q}(X)^\times$, the multiplicative group of nonzero quotients of polynomials having rational coefficients. The "addition" operation of

this group is multiplication, and the "scaling" operation is exponentiation,

$$r(X) \oplus \tilde{r}(X) = r(X)\tilde{r}(X), \qquad c \odot r(X) = r(X)^c \text{ for } c \in \mathbb{Z}.$$

In this context, the condition $X^n - 1 = \prod_{d|n} \Phi_d(X)$ for $n \geq 1$ gives by Möbius inversion in G

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}, \quad n \geq 1.$$

For example,

$$\Phi_{pq}(X) = \frac{(X^{pq} - 1)(X - 1)}{(X^p - 1)(X^q - 1)}, \quad p, q \text{ distinct primes},$$

and this is a monic polynomial with integer coefficients. Similarly,

$$\Phi_{12}(X) = \frac{(X^{12} - 1)(X^2 - 1)}{(X^6 - 1)(X^4 - 1)} = \frac{X^6 + 1}{X^2 + 1} = X^4 - X^2 + 1.$$

8. A Comment on Ireland and Rosen 2.4

Define a prime-counting function,

$$\pi : \mathbb{R} \longrightarrow \mathbb{R}, \quad \pi(x) = \#\{p \in \mathcal{P} : p \leq x\}.$$

The **Prime Number Theorem** says that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Section 2.4 of Ireland and Rosen shows that easy analytic estimates give for some constants c_1 and c_2,

$$c_1 x/\log x < \pi(x) < c_2 x/\log x.$$

The Prime Number Theorem was first proved in 1899 by Hadamard and (independently) Poussin. Elementary proofs were given in the 1940s by Erdös and Selberg. For students with background in complex analysis, see the writeup for this course that gives a short proof of the Prime Number Theorem.