

MATH 361: NUMBER THEORY — THIRD LECTURE

1. INTRODUCTION

The topic of this lecture is *arithmetic functions and Dirichlet series*.

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 $n \geq 3$, since

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

it follows that

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

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

By contrast, Euler argued that

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

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

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

Note that

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

so that also

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

(The logarithm is natural, of course.)

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,

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

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)

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

But

$$\sum_{p \in \mathcal{P}} \sum_{n=2}^{\infty} p^{-ns}/n < \sum_{p \in \mathcal{P}} \sum_{n=2}^{\infty} p^{-ns} = \sum_{p \in \mathcal{P}} p^{-2s} (1 - p^{-s})^{-1} = \sum_{p \in \mathcal{P}} \frac{1}{p^s(p^s - 1)},$$

and

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

Thus

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

Thus

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

and more specifically,

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

Thus *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 much 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,

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

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

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

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

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

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 ,

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

Since formal power series with nonzero leading term are invertible, 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

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

The corresponding Dirichlet series is simply

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

Since $\mathbf{I}(s)$ is the multiplicative identity, \mathbf{i} 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**,

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

Thus we have for any arithmetic functions f and g ,

$$\begin{aligned} g = f * u &\iff G(s) = F(s)\zeta(s) \\ &\iff F(s) = G(s)\zeta(s)^{-1} \\ &\iff f = g * \mu. \end{aligned}$$

The equivalence $g = f * u \iff f = g * \mu$ is the **Möbius Inversion Formula**,

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

As a special case, let $f = \mathbf{i}$ so that $g = u$. Then we have by Möbius inversion,

$$\mathbf{i}(n) = \sum_{d|n} \mu(d)u(n),$$

which is to say,

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

4. THE EULER TOTIENT FUNCTION

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

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

Thus $\phi(1) = 1$ and $\phi(p) = p - 1$ for p prime.

Now we set up Möbius inversion by counting that

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

Indeed,

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

(For example, if $n = 20$ then the disjoint union is

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

with, for example, $\{2, 6, 14, 18\}$ being the multiples of $20/10$ by factors coprime to 10.) The desired counting formula follows immediately by definition of the totient function. Consequently, Möbius inversion gives

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

That is,

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

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

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

(Of course, one can derive the formula directly, e.g., by an inclusion-exclusion count of the elements of $\{0, \dots, n-1\}$ that are co-prime to n .)

Some consequences of the totient function formula are

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

5. ANOTHER ARITHMETIC FUNCTION

The **sum of divisor k th powers** function is

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

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

$$\sigma_k = (k\text{th power function}) * u,$$

the Dirichlet series of σ_k is

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

and Möbius inversion gives the formula

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

6. MULTIPLICATIVE AND TOTALLY MULTIPLICATIVE FUNCTIONS

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

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

and f is **totally multiplicative** if

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

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 function g of prime powers,

$$\prod_p \sum_{e_p=0}^{\infty} g(p^{e_p}) = \sum_{n=1}^{\infty} \prod_{p^{e_p} \parallel n} g(p^{e_p}),$$

specialized to $g(p^e) = f(p^e)/p^{es}$. (The notation $p^{e_p} \parallel n$ 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 $f(1) \neq 0$ then so is the convolution inverse of f .
- If f is totally multiplicative and $f(1) \neq 0$ then its convolution inverse is $f^{-1} = \mu f$.

To establish the first bullet using Dirichlet series, compute that since 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.

To establish the second bullet using Dirichlet series, we need to show that if $f(1) \neq 0$ then the inverse of the p th factor of $F(s)$ takes the same form, i.e.,

$$\left(\sum_{e=0}^{\infty} \frac{f(p^e)}{p^{es}} \right)^{-1} = \sum_{e=0}^{\infty} \frac{g(p^e)}{p^{es}} \quad \text{for some } g.$$

Expand the desired condition,

$$\left(f(1) + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots \right) \left(g(1) + \frac{g(p)}{p^s} + \frac{g(p^2)}{p^{2s}} + \dots \right) = 1,$$

so that we want

$$\begin{aligned} 1 &= f(1)g(1), \\ 0 &= f(1)g(p) + f(p)g(1), \\ 0 &= f(1)g(p^2) + f(p)g(p) + f(p^2)g(1), \\ &\text{etc.} \end{aligned}$$

The first equation determines $g(1)$, the second determines $g(p)$, the third determines $g(p^2)$, and so on.

To establish the third bullet using Dirichlet series, we need to show that if f generates the Dirichlet series $F(s)$ then $F(s)^{-1}$ is the Dirichlet series generated by μf . Compute that indeed since $F(s) = \prod_p (1 - f(p)p^{-s})^{-1}$,

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

Or, to establish the third bullet directly, recall the identity at the very end of section 3 and compute that

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

7. A COMMENT ON IRELAND AND ROSEN 2.4

Define a prime-counting function,

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

The **Prime Number Theorem** says that

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

The Prime Number Theorem was first proved in 1899 by Hadamard and (independently) Poussin. And elementary proof was given in the 1940's by Selberg, perhaps with a significant contribution from Erdős. Section 2.4 of Ireland and Rosen is showing that easy analytic estimates show that for some constants c_1 and c_2 ,

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

For students with background in complex analysis, see the 1997 *American Mathematical Monthly* article *Newman's short proof of the prime number theorem* by Zagier.