1

Dirichlet series: I

1.1 Generating functions and asymptotics

The general rationale of analytic number theory is to derive statistical information about a sequence $\{a_n\}$ from the analytic behaviour of an appropriate generating function, such as a power series $\sum a_n z^n$ or a Dirichlet series $\sum a_n n^{-s}$. The type of generating function employed depends on the problem being investigated. There are no rigid rules governing the kind of generating function that is appropriate – the success of a method justifies its use – but we usually deal with additive questions by means of power series or trigonometric sums, and with multiplicative questions by Dirichlet series. For example, if

$$f(z) = \sum_{n=1}^{\infty} z^{n^k}$$

for $|z| < 1$, then the n^{th} power series coefficient of $f(z)^s$ is the number $r_{k,s}(n)$ of representations of n as a sum of s positive k^{th} powers,

$$n = m_1^k + m_2^k + \cdots + m_s^k.$$

We can recover $r_{k,s}(n)$ from $f(z)^s$ by means of Cauchy's coefficient formula:

$$r_{k,s}(n) = \frac{1}{2\pi i} \oint \frac{f(z)^s}{z^{n+1}}\, dz.$$

By choosing an appropriate contour, and estimating the integrand, we can determine the asymptotic size of $r_{k,s}(n)$ as $n \to \infty$, provided that s is sufficiently large, say $s > s_0(k)$. This is the germ of the Hardy–Littlewood circle method, but considerable effort is required to construct the required estimates.

To appreciate why power series are useful in dealing with additive problems, note that if $A(z) = \sum a_k z^k$ and $B(z) = \sum b_m z^m$ then the power series

coefficients of $C(z) = A(z)B(z)$ are given by the formula

$$c_n = \sum_{k+m=n} a_k b_m. \tag{1.1}$$

The terms are grouped according to the sum of the indices, because $z^k z^m = z^{k+m}$.

A *Dirichlet series* is a series of the form $\alpha(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ where s is a complex variable. If $\beta(s) = \sum_{m=1}^{\infty} b_m m^{-s}$ is a second Dirichlet series and $\gamma(s) = \alpha(s)\beta(s)$, then (ignoring questions relating to the rearrangement of terms of infinite series)

$$\gamma(s) = \sum_{k=1}^{\infty} a_k k^{-s} \sum_{m=1}^{\infty} b_m m^{-s} = \sum_{k=1}^{\infty} \sum_{m=1}^{\infty} a_k b_m (km)^{-s} = \sum_{n=1}^{\infty} \Big(\sum_{km=n} a_k b_m \Big) n^{-s}. \tag{1.2}$$

That is, we expect that $\gamma(s)$ is a Dirichlet series, $\gamma(s) = \sum_{n=1}^{\infty} c_n n^{-s}$, whose coefficients are

$$c_n = \sum_{km=n} a_k b_m. \tag{1.3}$$

This corresponds to (1.1), but the terms are now grouped according to the product of the indices, since $k^{-s} m^{-s} = (km)^{-s}$.

Since we shall employ the complex variable s extensively, it is useful to have names for its real and complex parts. In this regard we follow the rather peculiar notation that has become traditional: $s = \sigma + it$.

Among the Dirichlet series we shall consider is the *Riemann zeta function*, which for $\sigma > 1$ is defined by the absolutely convergent series

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}. \tag{1.4}$$

As a first application of (1.3), we note that if $\alpha(s) = \beta(s) = \zeta(s)$ then the manipulations in (1.3) are justified by absolute convergence, and hence we see that

$$\sum_{n=1}^{\infty} d(n) n^{-s} = \zeta(s)^2 \tag{1.5}$$

for $\sigma > 1$. Here $d(n)$ is the *divisor function*, $d(n) = \sum_{d|n} 1$.

From the rate of growth or analytic behaviour of generating functions we glean information concerning the sequence of coefficients. In expressing our findings we employ a special system of notation. For example, we say, '$f(x)$ is asymptotic to $g(x)$' as x tends to some limiting value (say $x \to \infty$), and write

$f(x) \sim g(x)$ $(x \to \infty)$, if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

An instance of this arises in the formulation of the Prime Number Theorem (PNT), which concerns the asymptotic size of the number $\pi(x)$ of prime numbers not exceeding x; $\pi(x) = \sum_{p\le x} 1$. Conjectured by Legendre in 1798, and finally proved in 1896 independently by Hadamard and de la Vallée Poussin, the Prime Number Theorem asserts that

$$\pi(x) \sim \frac{x}{\log x}.$$

Alternatively, we could say that

$$\pi(x) = (1 + o(1))\frac{x}{\log x},$$

which is to say that $\pi(x)$ is $x/\log x$ plus an error term that is in the limit negligible compared with $x/\log x$. More generally, we say, '$f(x)$ is small oh of $g(x)$', and write $f(x) = o(g(x))$, if $f(x)/g(x) \to 0$ as x tends to its limit.

The Prime Number Theorem can be put in a quantitative form,

$$\pi(x) = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right). \tag{1.6}$$

Here the last term denotes an implicitly defined function (the difference between the other members of the equation); the assertion is that this function has absolute value not exceeding $Cx(\log x)^{-2}$. That is, the above is equivalent to asserting that there is a constant $C > 0$ such that the inequality

$$\left|\pi(x) - \frac{x}{\log x}\right| \le \frac{Cx}{(\log x)^2}$$

holds for all $x \ge 2$. In general, we say that $f(x)$ is 'big oh of $g(x)$', and write $f(x) = O(g(x))$ if there is a constant $C > 0$ such that $|f(x)| \le Cg(x)$ for all x in the appropriate domain. The function f may be complex-valued, but g is necessarily non-negative. The constant C is called the *implicit constant*; it is an absolute constant unless the contrary is indicated. For example, if C is liable to depend on a parameter α, we might say, 'For any fixed value of α, $f(x) = O(g(x))$'. Alternatively, we might say, '$f(x) = O(g(x))$ where the implicit constant may depend on α', or more briefly, $f(x) = O_\alpha(g(x))$.

When there is no main term, instead of writing $f(x) = O(g(x))$ we save a pair of parentheses by writing instead $f(x) \ll g(x)$. This is read, '$f(x)$ is less-than-less-than $g(x)$', and we write $f(x) \ll_\alpha g(x)$ if the implicit constant may depend on α. To provide an example of this notation, we recall that Chebyshev

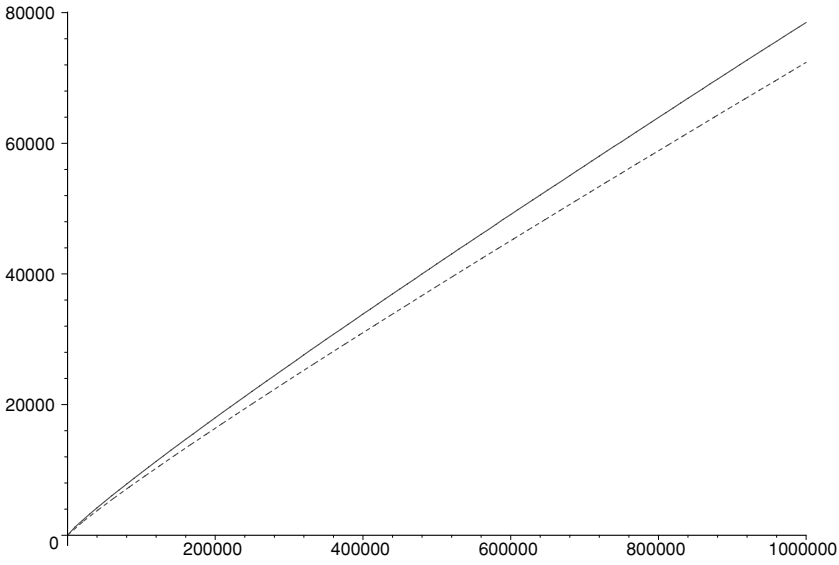

Figure 1.1 Graph of $\pi(x)$ (solid) and $x/\log x$ (dotted) for $2 \le x \le 10^6$.

proved that $\pi(x) \ll x/\log x$. This is of course weaker than the Prime Number Theorem, but it was derived much earlier, in 1852. Chebyshev also showed that $\pi(x) \gg x/\log x$. In general, we say that $f(x) \gg g(x)$ if there is a positive constant c such that $f(x) \ge cg(x)$ and g is non-negative. In this situation both f and g take only positive values. If both $f \ll g$ and $f \gg g$ then we say that f and g have the same order of magnitude, and write $f \asymp g$. Thus Chebyshev's estimates can be expressed as a single relation,

$$\pi(x) \asymp \frac{x}{\log x}.$$

The estimate (1.6) is best possible to the extent that the error term is not $o(x(\log x)^{-2})$. We have also a special notation to express this:

$$\pi(x) - \frac{x}{\log x} = \Omega\left(\frac{x}{(\log x)^2}\right).$$

In general, if $\limsup_{x\to\infty} |f(x)|/g(x) > 0$ then we say that $f(x)$ is 'Omega of $g(x)$', and write $f(x) = \Omega(g(x))$. This is precisely the negation of the statement '$f(x) = o(g(x))$'. When studying numerical values, as in Figure 1.1, we find that the fit of $x/\log x$ to $\pi(x)$ is not very compelling. This is because the error term in the approximation is only one logarithm smaller than the main term. This error term is not oscillatory – rather there is a second main term of this

size:

$$\pi(x) = \frac{x}{\log x} + \frac{x}{(\log x)^2} + O\left(\frac{x}{(\log x)^3}\right).$$

This is also best possible, but the main term can be made still more elaborate to give a smaller error term. Gauss was the first to propose a better approximation to $\pi(x)$. Numerical studies led him to observe that the density of prime numbers in the neighbourhood of x is approximately $1/\log x$. This suggests that the number of primes not exceeding x might be approximately equal to the *logarithmic integral*,

$$\mathrm{li}(x) = \int_2^x \frac{1}{\log u}\, du.$$

(Orally, 'li' rhymes with 'pi'.) By repeated integration by parts we can show that

$$\mathrm{li}(x) = x \sum_{k=1}^{K-1} \frac{(k-1)!}{(\log x)^k} + O_K\left(\frac{x}{(\log x)^K}\right)$$

for any positive integer K; thus the secondary main terms of the approximation to $\pi(x)$ are contained in li(x).

In Chapter 6 we shall prove the Prime Number Theorem in the sharper quantitative form

$$\pi(x) = \mathrm{li}(x) + O\left(\frac{x}{\exp(c\sqrt{\log x})}\right)$$

for some suitable positive constant c. Note that $\exp(c\sqrt{\log x})$ tends to infinity faster than any power of $\log x$. The error term above seems to fall far from what seems to be the truth. Numerical evidence, such as that in Table 1.1, suggests that the error term in the Prime Number Theorem is closer to $\sqrt{x}$ in size. Gauss noted the good fit, and also that $\pi(x) < \mathrm{li}(x)$ for all x in the range of his extensive computations. He proposed that this might continue indefinitely, but the numerical evidence is misleading, for in 1914 Littlewood showed that

$$\pi(x) - \mathrm{li}(x) = \Omega_{\pm}\left(\frac{x^{1/2}\log\log\log x}{\log x}\right).$$

Here the subscript $\pm$ indicates that the error term achieves the stated order of magnitude infinitely often, and in both signs. In particular, the difference $\pi - \mathrm{li}$ has infinitely many sign changes. More generally, we write $f(x) = \Omega_+(g(x))$ if $\limsup_{x\to\infty} f(x)/g(x) > 0$, we write $f(x) = \Omega_-(g(x))$ if $\liminf_{x\to\infty} f(x)/g(x) < 0$, and we write $f(x) = \Omega_\pm(g(x))$ if both these relations hold.

Table 1.1 Values of $\pi(x)$, li(x), $x/\log x$ *for* $x = 10^k$, $1 \le k \le 22$.

x	$\pi(x)$	li(x)	$x/\log x$
10	4	5.12	4.34
10^2	25	29.08	21.71
10^3	168	176.56	144.76
10^4	1229	1245.09	1085.74
10^5	9592	9628.76	8685.89
10^6	78498	78626.50	72382.41
10^7	664579	664917.36	620420.69
10^8	5761455	5762208.33	5428681.02
10^9	50847534	50849233.90	48254942.43
10^{10}	455052511	455055613.54	434294481.90
10^{11}	4118054813	4118066399.58	3948131653.67
10^{12}	37607912018	37607950279.76	36191206825.27
10^{13}	346065536839	346065458090.05	334072678387.12
10^{14}	3204941750802	3204942065690.91	3102103442166.08
10^{15}	29844570422669	29844571475286.54	28952965460216.79
10^{16}	279238341033925	279238344248555.75	271434051189532.39
10^{17}	2623557157654233	2623557165610820.07	2554673422960304.87
10^{18}	24739954287740860	24739954309690413.98	24127471216847323.76
10^{19}	234057667276344607	234057667376222382.22	228576043106974646.13
10^{20}	2220819602560918840	2220819602783663483.55	2171472409516259138.26
10^{21}	21127269486018731928	21127269486616126182.33	20680689614440563221.48
10^{22}	201467286689315906290	201467286691248261498.15	197406582683296285295.97

In the exercises below we give several examples of the use of generating functions, mostly power series, to establish relations between various counting functions.

1.1.1 Exercises

1. Let $r(n)$ be the number of ways that n cents of postage can be made, using only 1 cent, 2 cent, and 3 cent stamps. That is, $r(n)$ is the number of ordered triples (x_1, x_2, x_3) of non-negative integers such that $x_1 + 2x_2 + 3x_3 = n$.
   (a) Show that
   $$\sum_{n=0}^{\infty} r(n)z^n = \frac{1}{(1-z)(1-z^2)(1-z^3)}$$
   for $|z| < 1$.
   (b) Determine the partial fraction expansion of the rational function above.

That is, find constants $a, b, \dots, f$ so that the above is

$$\frac{a}{(z-1)^3} + \frac{b}{(z-1)^2} + \frac{c}{z-1} + \frac{d}{z+1} + \frac{e}{z-\omega} + \frac{f}{z-\overline{\omega}}$$

where $\omega = e^{2\pi i/3}$ and $\overline{\omega} = e^{-2\pi i/3}$ are the primitive cube roots of unity.

(c) Show that $r(n)$ is the integer nearest $(n+3)^2/12$.

(d) Show that $r(n)$ is the number of ways of writing $n = y_1 + y_2 + y_3$ with $y_1 \geq y_2 \geq y_3 \geq 0$.

2. Explain why

$$\prod_{k=0}^{\infty} \left(1 + z^{2^k}\right) = 1 + z + z^2 + \cdots$$

for $|z| < 1$.

3. (L. Mirsky & D. J. Newman) Suppose that $0 \leq a_k < m_k$ for $1 \leq k \leq K$, and that $m_1 < m_2 < \cdots < m_K$. This is called a *family of covering congruences* if every integer x satisfies at least one of the congruences $x \equiv a_k \pmod{m_k}$. A system of covering congruences is called *exact* if for every value of x there is exactly one value of k such that $x \equiv a_k \pmod{m_k}$. Show that if the system is exact then

$$\sum_{k=1}^{K} \frac{z^{a_k}}{1 - z^{m_k}} = \frac{1}{1-z}$$

for $|z| < 1$. Show that the left-hand side above is

$$\sim \frac{e^{2\pi i a_K/m_K}}{m_K(1-r)}$$

when $z = re^{2\pi i/m_K}$ and $r \to 1^-$. On the other hand, the right-hand side is bounded for z in a neighbourhood of $e^{2\pi i/m_K}$ if $m_K > 1$. Deduce that a family of covering congruences is not exact if $m_k > 1$.

4. Let $p(n;k)$ denote the number of partitions of n into at most k parts, that is, the number of ordered k-tuples $(x_1, x_2, \dots, x_k)$ of non-negative integers such that $n = x_1 + x_2 + \cdots + x_k$ and $x_1 \geq x_2 \geq \cdots \geq x_k$. Let $p(n) = p(n;n)$ denote the total number of partitions of n. Also let $p_{\mathrm{o}}(n)$ be the number of partitions of n into an odd number of parts, $p_{\mathrm{o}}(n) = \sum_{2\nmid k} p(n;k)$. Finally, let $p_{\mathrm{d}}(n)$ denote the number of partitions of n into distinct parts, so that $x_1 > x_2 > \cdots > x_k$. By convention, put $p(0) = p_{\mathrm{o}}(0) = p_{\mathrm{d}}(0) = 1$.

(a) Show that there are precisely $p(n;k)$ partitions of n into parts not exceeding k.

(b) Show that

$$\sum_{n=0}^{\infty} p(n;k)z^n = \prod_{j=1}^{k}(1-z^j)^{-1}$$

for $|z| < 1$.

(c) Show that

$$\sum_{n=0}^{\infty} p(n)z^n = \prod_{k=1}^{\infty}(1-z^k)^{-1}$$

for $|z| < 1$.

(d) Show that

$$\sum_{n=0}^{\infty} p_{\mathrm{d}}(n)z^n = \prod_{k=1}^{\infty}(1+z^k)$$

for $|z| < 1$.

(e) Show that

$$\sum_{n=0}^{\infty} p_{\mathrm{o}}(n)z^n = \prod_{k=1}^{\infty}(1-z^{2k-1})^{-1}$$

for $|z| < 1$.

(f) By using the result of Exercise 2, or otherwise, show that the last two generating functions above are identically equal. Deduce that $p_{\mathrm{o}}(n) = p_{\mathrm{d}}(n)$ for all n.

5. Let $A(n)$ denote the number of ways of associating a product of n terms; thus $A(1) = A(2) = 1$ and $A(3) = 2$. By convention, $A(0) = 0$.

(a) By considering the possible positionings of the outermost parentheses, show that

$$A(n) = \sum_{k=1}^{n-1} A(k)A(n-k)$$

for all $n \geq 2$.

(b) Let $P(z) = \sum_{n=0}^{\infty} A(n)z^n$. Show that

$$P(z)^2 = P(z) - z.$$

Deduce that

$$P(z) = \frac{1-\sqrt{1-4z}}{2} = \sum_{n=1}^{\infty} \binom{1/2}{n} 2^{2n-1}(-1)^{n-1}z^n.$$

(c) Conclude that $A(n) = \binom{2n-2}{n-1}/n$ for all $n \geq 1$. These are called the *Catalan numbers*.

(d) What needs to be said concerning the convergence of the series used above?

6. (a) Let n_k denote the total number of monic polynomials of degree k in $\mathbb{F}_p[x]$. Show that $n_k = p^k$.

(b) Let $P_1, P_2, \dots$ be the irreducible monic polynomials in $\mathbb{F}_p[x]$, listed in some (arbitrary) order. Show that

$$\prod_{r=1}^{\infty}(1 + z^{\deg P_r} + z^{2\deg P_r} + z^{3\deg P_r} + \cdots) = 1 + pz + p^2z^2 + p^3z^3 + \cdots$$

for $|z| < 1/p$.

(c) Let g_k denote the number of irreducible monic polynomials of degree k in $\mathbb{F}_p[x]$. Show that

$$\prod_{k=1}^{\infty}(1 - z^k)^{-g_k} = (1 - pz)^{-1} \qquad (|z| < 1/p).$$

(d) Take logarithmic derivatives to show that

$$\sum_{k=1}^{\infty} k g_k \frac{z^{k-1}}{1 - z^k} = \frac{p}{1 - pz} \qquad (|z| < 1/p).$$

(e) Show that

$$\sum_{k=1}^{\infty} k g_k \sum_{m=1}^{\infty} z^{mk} = \sum_{n=1}^{\infty} p^n z^n \qquad (|z| < 1/p).$$

(f) Deduce that

$$\sum_{k|n} k g_k = p^n$$

for all positive integers n.

(g) (Gauss) Use the Möbius inversion formula to show that

$$g_n = \frac{1}{n} \sum_{k|n} \mu(k) p^{n/k}$$

for all positive integers n.

(h) Use (f) (not (g)) to show that

$$\frac{p^n}{n} - \frac{2p^{n/2}}{n} \le g_n \le \frac{p^n}{n}.$$

(i) If a monic polynomial of degree n is chosen at random from $\mathbb{F}_p[x]$, about how likely is it that it is irreducible? (Assume that p and/or n is large.)

(j) Show that $g_n > 0$ for all p and all $n \geq 1$. (If $P \in \mathbb{F}_p[x]$ is irreducible and has degree n, then the quotient ring $\mathbb{F}_p[x]/(P)$ is a field of p^n elements. Thus we have proved that there is such a field, for each prime p and integer $n \geq 1$. It may be further shown that the order of a finite field is necessarily a prime power, and that any two finite fields of the same order are isomorphic. Hence the field of order p^n, whose existence we have proved, is essentially unique.)

7. (E. Berlekamp) Let p be a prime number. We recall that polynomials in a single variable (mod p) factor uniquely into irreducible polynomials. Thus a monic polynomial $f(x)$ can be expressed uniquely (mod p) in the form $g(x)h(x)^2$ where $g(x)$ is square-free (mod p) and both g and h are monic. Let s_n denote the number of monic square-free polynomials (mod p) of degree n. Show that

$$\Big(\sum_{k=0}^{\infty} s_k z^k\Big)\Big(\sum_{m=0}^{\infty} p^m z^{2m}\Big) = \sum_{n=0}^{\infty} p^n z^n$$

for $|z| < 1/p$. Deduce that

$$\sum_{k=0}^{\infty} s_k z^k = \frac{1 - pz^2}{1 - pz},$$

and hence that $s_0 = 1$, $s_1 = p$, and that $s_k = p^k(1 - 1/p)$ for all $k \geq 2$.

8. (cf Wagon 1987) (a) Let $\mathcal{I} = [a, b]$ be an interval. Show that $\int_{\mathcal{I}} e^{2\pi i x}\, dx = 0$ if and only if the length $b - a$ of $\mathcal{I}$ is an integer.
   (b) Let $\mathcal{R} = [a, b] \times [c, d]$ be a rectangle. Show that $\iint_{\mathcal{R}} e^{2\pi i(x+y)}\, dx\, dy = 0$ if and only if at least one of the edge lengths of $\mathcal{R}$ is an integer.
   (c) Let $\mathcal{R}$ be a rectangle that is a union of finitely many rectangles $\mathcal{R}_i$; the $\mathcal{R}_i$ are disjoint apart from their boundaries. Show that if all the $\mathcal{R}_i$ have the property that at least one of their side lengths is an integer, then $\mathcal{R}$ also has this property.

9. (L. Moser) If $\mathcal{A}$ is a set of non-negative integers, let $r_{\mathcal{A}}(n)$ denote the number of representations of n as a sum of two distinct members of $\mathcal{A}$. That is, $r_{\mathcal{A}}(n)$ is the number of ordered pairs (a_1, a_2) for which $a_1 \in \mathcal{A}$, $a_2 \in \mathcal{A}$, $a_1 + a_2 = n$, and $a_1 \neq a_2$. Let $A(z) = \sum_{a \in \mathcal{A}} z^a$.
   (a) Show that $\sum_n r_{\mathcal{A}}(n) z^n = A(z)^2 - A(z^2)$ for $|z| < 1$.
   (b) Suppose that the non-negative integers are partitioned into two sets $\mathcal{A}$ and $\mathcal{B}$ in such a way that $r_{\mathcal{A}}(n) = r_{\mathcal{B}}(n)$ for all non-negative integers n. Without loss of generality, $0 \in \mathcal{A}$. Show that $1 \in \mathcal{B}$, that $2 \in \mathcal{B}$, and that $3 \in \mathcal{A}$.
   (c) With $\mathcal{A}$ and $\mathcal{B}$ as above, show that $A(z) + B(z) = 1/(1 - z)$ for $|z| < 1$.
   (d) Show that $A(z) - B(z) = (1 - z)\big(A(z^2) - B(z^2)\big)$, and hence by