# 1
# Foundations

In this chapter, we assemble a number of ideas and techniques that will eventually be fitted together to achieve our aim. Their only common feature is that they are needed to prove the prime number theorem, so the chapter has no single unifying theme. However, each *section* of the chapter is devoted to a very clearly defined topic. Some of these ideas are analytic, others number-theoretic, but there would be no advantage in trying to keep the two strands apart: they reinforce each other in a fruitful partnership.

Our objective is to find a formula that approximates $\pi(x)$, the number of primes not greater than $x$. We start, in section 1.1, by identifying some candidates as suggested by numerical evidence. We also give a brief account of the long history leading to the successful proof of the prime number theorem.

The term "arithmetic function" is used for a sequence defined using number-theoretic properties in some way. A great deal of number theory consists of the study of such functions. Now we can express $\pi(x)$ as the partial sum $\sum_{n\leq x} u_P(n)$, where $u_P$ is the arithmetic function defined as follows:

$$u_P(n) = \begin{cases} 1 & \text{if } n \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

Typically, arithmetic functions appear to be very irregular, but this is smoothed out by addition, and one can hope to find an estimate for their partial sums. This identifies our problem as one of a certain type.

We go on to describe two essential techniques for rewriting and estimating discrete sums, Abel summation and integral estimation. Both are used constantly in all that follows.

After this, we are in a position to describe the first real progress towards the prime number theorem, achieved by Chebyshev in 1850. Chebyshev recognised that an estimation of $\pi(x)$ can be deduced from an estimation of $\theta(x) = \sum_{p\in P[x]} \log p$ (where $P[x]$ denotes the set of primes not greater than

$x$), and showed that the latter sum can be estimated by a comparatively short (but ingenious) argument. In this way, he demonstrated that $\pi(x)$ lies between $cx/\log x$ and $Cx/\log x$ for two constants $c$, $C$.

Finally, we introduce a concept that will permeate the rest of our study to the extent that it could serve as a subtitle for this book. A *Dirichlet series* is a series of the form $\sum_{n=1}^{\infty} a(n)/n^s$, in which $s$ is a complex variable. The case $a(n) = 1$ defines the *Riemann zeta function*. Every arithmetic function has a corresponding Dirichlet series; multiplication of the series corresponds to "convolution" of the arithmetic functions. Our "fundamental theorems" in chapter 3 will derive information about the partial sums of $a(n)$ from the nature of the function defined by the series, with the prime number theorem appearing as a special case.

## 1.1 Counting prime numbers

As the reader surely knows, prime numbers are those that have no positive divisors except 1 and the number itself. The special significance of prime numbers is due to the following fact, which we will assume known:

*Every positive integer is expressible as a product of primes. The expression is unique if the primes are listed in increasing order.*

Effectively, this means that the primes are the basic "atoms" in the multipicative system of integers. (If $n$ is itself prime, we are regarding it as a "product" of one prime, itself.)

The first result on the number of primes was already known to Euclid. Here it is, with Euclid's beautiful proof.

**Proposition 1.1.1** *There are infinitely many prime numbers.*

*Proof* Choose finitely many primes $p_1, p_2, \ldots, p_n$. We will show that they cannot constitute the total set of primes. Consider the number

$$N = p_1 p_2 \ldots p_n + 1.$$

Then $N$ is not a multiple of any $p_j$, because it clearly leaves remainder 1 when divided by $p_j$. However, by the above statement, $N$ is expressible as a product of primes. Let $q$ be any one of these. Then $q$ is a further prime, different from all the $p_j$, which therefore indeed fail to constitute the total set of primes. □

**Note** This reasoning actually shows a bit more: if the primes are listed as $p_1, p_2, \ldots$ in increasing order, then $p_{n+1} \leq p_1 p_2 \ldots p_n + 1$.

With this settled, it is natural to ask how many prime numbers there are up to any given number. This is the topic of our study. Let us give it some notation:

$$\pi(x) = \text{the number of primes not greater than } x.$$

This notation is standard in number theory; there is no real danger of confusion with the number $\pi$. It will suit our purposes to regard $\pi(x)$ as a function of a real variable $x$. As such a function, it is, of course, constant between primes and jumps by 1 at each prime.

The first impression given by the sequence of primes

$$2, 3, 5, 7, 11, \ldots, 101, 103, 107, 109, 113, 127, \ldots, 163, 167, 173, 179, \ldots$$

is one of extreme irregularity. There are bunches, gaps and relatively uniform stretches. It would appear to be a daunting task to find a simple expression that approximates to $\pi(x)$ for all large enough $x$. The only simple observation is that the primes tend to become more sparse as one goes on. However, an examination of the numerical values of $\pi(x)$ suggests that a reasonable approximation is given by $x/(\log x)$, a considerably better one by

$$\frac{x}{\log x - 1},$$

and a still better one by the "logarithmic integral", defined as follows:

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

Some of these numerical values are as follows (given to the nearest integer):

| $n$ | $\pi(n)$ | $\frac{n}{\log n}$ | $\frac{n}{\log n - 1}$ | $\mathrm{li}(n)$ |
|---|---|---|---|---|
| 1,000 | 168 | 145 | 169 | 177 |
| 10,000 | 1,229 | 1,086 | 1,218 | 1,246 |
| 50,000 | 5,133 | 4,621 | 5,092 | 5,166 |
| 100,000 | 9,592 | 8,686 | 9,512 | 9,630 |
| 500,000 | 41,538 | 38,103 | 41,246 | 41,607 |
| 1,000,000 | 78,498 | 72,382 | 78,031 | 78,628 |
| 10,000,000 | 664,579 | 620,421 | 661,459 | 664,918 |

By the year 1800, long before the age of computers, mathematicians had performed the remarkable feat of calculating these figures by hand up to

$n = 400,000$. In the age of computers, it has of course become much easier to calculate values of $\pi(x)$. Some readers will be interested in doing so on their own computer: various methods for this are discussed in appendix F.

Let us formulate precisely the conjecture suggested by these figures. Given two functions $f(x)$, $g(x)$, both tending to infinity as $x \to \infty$, we write

$$f(x) \sim g(x) \qquad \text{as } x \to \infty$$

to mean that

$$\frac{f(x)}{g(x)} \to 1 \qquad \text{as } x \to \infty.$$

Our conjecture is the statement

$$\pi(x) \sim \mathrm{li}(x) \qquad \text{as } x \to \infty.$$

In fact, as we will show in section 1.5,

$$\frac{x}{\log x} \sim \frac{x}{\log x - 1} \sim \mathrm{li}(x) \qquad \text{as } x \to \infty,$$

so at this level it is equivalent to state the conjecture using any of the three functions.

The conjecture is in fact true. The statement $\pi(x) \sim \mathrm{li}(x)$ is called the *prime number theorem*. It is indisputably one of the most celebrated theorems in mathematics. Ways of proving it, together with related results, more precise versions and generalizations, form the subject of this book. Of course, numerical evidence of the above type can never constitute a proof of the general statement.

An informal interpretation of the theorem is that the "average density" of primes around a large number $x$ approximates to $1/(\log x)$, or that the "probability" of $n$ being prime is (in some sense) $1/(\log n)$.

Let us return to the historical trail (for a much more detailed historical account, see [Nar]). Legendre, in 1798, postulated the approximations $x/(\log x)$ and $x/(\log x - 1)$. He suggested (wrongly) that an even better approximation would be given by $x/(\log x - A)$, with $A = 1.0836$. Meanwhile, Gauss proposed $\mathrm{li}(x)$. It seems that Gauss recorded his conjecture around 1793 (at the age of 14!) but did not communicate it to anyone until 1849.

The search for a proof remained one of the main areas of mathematical endeavour during the rest of the nineteenth century. In 1850, a giant stride was made by Chebyshev, who showed, by essentially number-theoretic methods, that there are constants $c$ and $C$ (not very far from 1) such that

$$c\,\mathrm{li}(x) \le \pi(x) \le C\,\mathrm{li}(x)$$

for all large enough $x$. However, no refinement of his methods seemed to offer any hope of proving the desired limit.

A completely different approach was proposed by Riemann in 1859. His starting point was a remarkable identity already discovered by Euler in 1737, expressing the "zeta function"

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

as an infinite *product* involving the primes. Riemann considered this as a function of a *complex* variable $s$, defined by the above formula for $\operatorname{Re} s > 1$. He showed how to extend the definition of the function to the rest of the complex plane and outlined a programme showing how, if certain properties of the extended zeta function could be established, the prime number theorem would follow. His paper was a bold imaginitive leap; it was hardly an obvious idea to use the theorems of complex analysis to count prime numbers! However, Riemann was not able to justify all his steps, and one of them, the "Riemann hypothesis", has remained unsolved to this day, regarded by many as the most important unsolved problem in mathematics.

It was not until 1896 that Riemann's programme was successfully completed. It was then done so independently by the French mathematician Jacques Hadamard and the Belgian Charles-Jean de la Vallée Poussin. They were able to bypass the Riemann hypothesis and establish other properties of the zeta function that were sufficient for the purpose. Hadamard lived until 1963 (aged 97) and de la Vallée Poussin until 1962 (aged 95): their mathematical labours cannot have done any harm to their health!

Further variations and modifications of their methods were developed by Mertens, Landau and others, but to this day the simplest, and most powerful, proofs of the prime number theorem rely on the zeta function and complex analysis, as suggested by Riemann. In chapters 1–3, we present a version (and a variant) that benefits from a century of "tidying up", but which still recognisably owes its existence to Riemann.

After the successful outcome of Riemann's programme, it remained a matter of great interest to ask whether the theorem could after all be proved by number-theoretic methods, without complex analysis. This was eventually achieved in 1949, again independently by two people, A. Selberg and P. Erdös. Proofs of this sort are called "elementary" as opposed to "analytic". However, "elementary" does not mean "simple"! Half a century later, known proofs of this sort are still more complicated than analytic ones and are less successful in providing error estimates or in delivering other theorems of the same sort. A version is presented in chapter 6.

### Exercises

1 Let $n \geq 1$ and let $E = \{30n + r : 0 \leq r \leq 29\}$. For which values of $r$ is $30n + r$ not a multiple of 2, 3 or 5 ? By considering the possible positions of multiples of 7, show that $E$ contains at most seven primes (seven cases, no short cuts!).

2 Show that, for any $n \geq 2$, there is eventually a gap of length at least $n$ between successive primes. [Hint: Consider $n!+2$ or $p_1 p_2 \dots p_n + 2$.]

3 Let the primes be listed, in order, as $p_1, p_2, \dots$. Use Euclid's proof to show by induction that $p_n \leq 2^{2^{n-1}}$ for each $n$. Deduce that

$$\pi(x) \geq \frac{\log\log x}{\log 2}.$$

## 1.2 Arithmetic functions

Formally, an arithmetic function is simply a sequence, with real or complex values. A sequence is, of course, a *function* on the set $\mathbb{N}$ of positive integers. To emphasize that we are thinking of them as functions, we shall usually use notation like $a(n)$, rather than $a_n$, for the value corresponding to the integer $n$. The term "arithmetic function" is used especially when $a(n)$ is defined using number-theoretic properties in some way. A large part of number theory consists, in one way or another, of the study of these functions.

We list some examples. First, two very simple ones, mainly to establish the notation we will use:

$$u(n) = 1 \quad \text{for all } n \qquad \text{(the "unit function")};$$

$$e_j(n) = \begin{cases} 1 & \text{if } n = j, \\ 0 & \text{if } n \neq j. \end{cases}$$

Next, given any subset $E$ of $\mathbb{N}$ (for example, the set $P$ of primes), define

$$u_E(n) = \begin{cases} 1 & \text{if } n \in E, \\ 0 & \text{if } n \notin E. \end{cases}$$

Clearly, $u$ itself is the case $E = \mathbb{N}$. Third, three more obviously number-theoretic examples:

$\tau(n) =$ the number of (positive) divisors of $n$, including 1 and $n$;
$\omega(n) =$ the number of prime divisors of $n$;
$\Omega(n) =$ the number of prime factors of $n$, counted with repetitions.

(This notation is more or less standard, though some writers use $d$ instead of $\tau$.) Note that $\tau(1) = 1$ and $\omega(1) = \Omega(1) = 0$. For $n > 1$, these functions can easily be described in terms of the prime factorization of $n$, as follows.

**Proposition 1.2.1** *Suppose that $n > 1$, with prime factorization*

$$n = \prod_{j=1}^{m} p_j^{k_j}.$$

*Then*

$$\tau(n) = \prod_{j=1}^{m}(k_j + 1), \quad \omega(n) = m, \quad \Omega(n) = \sum_{j=1}^{m} k_j.$$

*Proof* The expressions for $\omega(n)$ and $\Omega(n)$ are just the definition. Divisors of $n$ are of the form $\prod_{j=1}^{m} p_j^{r_j}$, where, for each $j$, the possible values of $r_j$ are $0, 1, \ldots, k_j$. This gives the expression for $\tau(n)$. □

In particular, if $p$ is prime, then $\tau(p^k) = k+1$, $\omega(p^k) = 1$ and $\Omega(p^k) = k$. To give another example, since $72 = 2^3.3^2$, we have $\tau(72) = 12$, $\omega(72) = 2$ and $\Omega(72) = 5$.

Given arithmetic functions $a$,$b$, we denote the pointwise product by $ab$, so that $(ab)(n) = a(n)b(n)$. Obviously, $au = a$ for any $a$.

**Summation functions.** Given an arithmetic function $a(n)$, its *summation function* $A(x)$ is defined by

$$A(x) = \sum_{n \le x} a(n).$$

It is useful to regard $A(x)$ as a function of a *real* variable $x$. As such a function, it is, of course, constant between integers and has a jump discontinuity at each integer where $a(n) \neq 0$. Clearly, $\pi(x)$ is the summation function of $u_P(n)$ (note: in particular cases, the established notation will not usually allow a notational device like the substitution of $A$ for $a$).

Individual values of arithmetic functions may fluctuate wildly – as in most of the examples just given. However, in many cases summation smooths out the fluctuation, and it may be possible to find an asymptotic expression for the summation function for large $x$. In the case of $\tau(n)$ and $\omega(n)$, the first step is to apply a bit of "lateral thinking" to obtain alternative expressions for the summation functions, as in the next result. The notation $[x]$ means the largest integer not greater than $x$. We shall use the notation $P[x]$ to mean the set of primes not greater than $x$ (but there is no generally agreed notation for this). Also, $j|n$ means that $j$ divides into $n$.

**Proposition 1.2.2** *Write* $S_\tau(x) = \sum_{n\le x} \tau(n)$ *and* $S_\omega(x) = \sum_{n\le x} \omega(n)$. *Then*

$$S_\tau(x) = \sum_{j\le x} \left[\frac{x}{j}\right], \qquad S_\omega(x) = \sum_{p\in P[x]} \left[\frac{x}{p}\right].$$

*Proof* Clearly, $S_\tau(x)$ is the number of ordered pairs $(j,n)$ such that $j|n$ and $n \le x$. For fixed $j$ (instead of fixed $n$), the number of such pairs is the number of multiples $rj$ not greater than $x$. This number is obviously $[x/j]$. The stated expression follows.

The argument for $S_\omega(x)$ is similar, counting the number of pairs $(p,n)$ as above, but with $p$ prime. □

The "double counting" principle seen in this proof is often useful. We shall see later how the identities in 1.2.2 can be used to derive asymptotic expressions for $S_\tau(x)$ and $S_\omega(x)$, and similar results will be obtained for some other arithmetic functions. Since $\pi(x)$ is itself a summation function, our main objective, the prime number theorem, is a result of exactly this type. But, as the reader may suspect, this case will cost us a lot more effort than most of the others.

**Multiplicative functions.** We denote by $(m,n)$ the greatest common divisor of $m$ and $n$. An arithmetic function $a$ is said to be

*completely multiplicative* if $a(mn) = a(m)a(n)$ for all $m,n$;

*multiplicative* if $a(mn) = a(m)a(n)$ whenever $(m,n) = 1$.

Clearly, if $a$ is multiplicative and not identically zero, then $a(1) = 1$. Also, $a$ is fully determined by the values $a(p^k)$ for prime $p$, since if the prime factorization of $n$ is $\prod_{j=1}^r p_j^{k_j}$, then $a(n) = \prod_{j=1}^r a(p_j^{k_j})$. Of course, if $a$ is completely multiplicative, then $a(p^k) = a(p)^k$, and the function is already fully determined by the values $a(p)$.

We list some examples.

(i) For any $s$, let $a(n) = n^s$. Then $a$ is completely multiplicative.
(ii) $e_1$ is completely multiplicative, but $e_j$ is not multiplicative for $j \ge 2$, since $e_j(1) = 0$.
(iii) $\tau$ is multiplicative. This follows from 1.2.1, since if $(m,n) = 1$, then $m$ and $n$ have different prime divisors. It is not completely multiplicative, since $\tau(2) = 2$, $\tau(4) = 3$.
(iv) $u_P$ is not multiplicative, since $u_P(1) = 0$.
(v) Neither $\omega$ nor $\Omega$ is multiplicative; however, we have $\Omega(mn) = \Omega(m) + \Omega(n)$, and similarly for $\omega$ when $(m,n) = 1$.

(vi) *Liouville's function* is defined by $\lambda(n) = (-1)^{\Omega(n)}$. It is completely multiplicative, by the statement in (v).

(vii) Let

$$\chi(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \equiv 1 \pmod 4 \\ -1 & \text{if } n \equiv -1 \pmod 4. \end{cases}$$

By considering the different cases, one checks easily that $\chi$ is completely multiplicative.

As the reader may already know, there are many further interesting arithmetic functions. Some will make their appearance in later sections.

### Exercises

1 Find the smallest $n$ such that: (i) $\Omega(n) = 4$, (ii) $\omega(n) = 4$, (iii) $\tau(n) = 4$.

2 Show that $\sum_{n=1}^{30} \tau(n) = 111$ without calculating individual values of $\tau(n)$.

3 Calculate $\sum_{n=1}^{100} \omega(n)$ without calculating individual values of $\omega(n)$.

4 Show that $\tau(n)$ is odd if and only if $n$ is a square.

5 Show that, for any $n \geq 2$,

$$2^{\omega(n)} \leq \tau(n) \leq 2^{\Omega(n)} \leq n.$$

[You may assume that $k + 1 \leq 2^k$ for all $k \geq 0$.]

6 Let $S$ be the set of squares. Show that $u_S$ is multiplicative.

7 Let $a(n) = (-1)^{n-1}$ for $n \geq 1$. Show that $a$ is multiplicative.

8 Prove that, for any $\varepsilon > 0$, we have $\tau(n)/n^{\varepsilon} \to 0$ as $n \to \infty$. [Again use $k+1 \leq 2^k$. For each prime $p < 2^{1/\varepsilon}$, show that there is a constant $C_p$ such that $k + 1 \leq C_p\, p^{\varepsilon k}$ for all $k$.]

## 1.3 Abel summation

### *Discrete version*

Abel summation, in its various forms, will be a very basic tool in all that follows, so we will describe it rather thoroughly. It is the process of expressing a sum of products $\sum a(r)f(r)$ in terms of *partial sums* of the $a(r)$'s and *differences* of the $f(r)$'s. Our choice of notation reflects the different roles played by $a(r)$ and $f(r)$. The process is exactly analogous to integration by

parts for functions, and indeed it is sometimes called "summation by parts" or "partial summation". As already mentioned, a central theme in analytic number theory is the estimation of partial sums (rather than individual values) of arithmetic functions. This explains why Abel summation is so often appropriate. Throughout the following, we assume that $a(r)$, $f(r)$ are given numbers (real or complex) for $r \geq 1$, and write $A(n) = \sum_{r=1}^{n} a(r)$ for $n \geq 1$ (also $A(0) = 0$). If we have another sequence $b(r)$, then $B(n)$ is defined similarly. The basic result is very simple, as follows.

**Proposition 1.3.1** *For integers $n > m \geq 0$,*

$$\sum_{r=m+1}^{n} a(r)f(r) = \sum_{r=m}^{n-1} A(r)[f(r) - f(r+1)] + A(n)f(n) - A(m)f(m).$$

*In particular,*

$$\sum_{r=1}^{n} a(r)f(r) = \sum_{r=1}^{n-1} A(r)[f(r) - f(r+1)] + A(n)f(n).$$

*Proof* The proof looks nicer if we write $A_r$ and $f_r$ instead of $A(r)$ and $f(r)$! For all $r \geq 1$, we have $a_r = A_r - A_{r-1}$ (recall $A_0 = 0$). Hence

$$\begin{aligned}\sum_{r=m+1}^{n} a_r f_r &= (A_{m+1} - A_m)f_{m+1} + (A_{m+2} - A_{m+1})f_{m+2} + \cdots \\ &\quad \cdots + (A_n - A_{n-1})f_n \\ &= -A_m f_{m+1} + \sum_{r=m+1}^{n-1} A_r(f_r - f_{r+1}) + A_n f_n \qquad (1.1) \\ &= -A_m f_m + \sum_{r=m}^{n-1} A_r(f_r - f_{r+1}) + A_n f_n. \qquad (1.2)\end{aligned}$$

The second statement is the case $m = 0$. □

This simple identity has numerous corollaries and applications.

**Corollary 1.3.2** *Suppose that $f(r)$ is real and non-negative, and decreases with $r$. Suppose that $a(r)$, $b(r)$ are such that $A(r) \leq CB(r)$ for all $r$. Then*

$$\sum_{r=1}^{n} a(r)f(r) \leq C\sum_{r=1}^{n} b(r)f(r).$$

*Proof* This follows at once from 1.3.1, because $f(r) - f(r+1)$ and $f(n)$ are non-negative. □