5

The distribution of primes

This chapter concerns itself with the question: how many primes are there? In Chapter 1, we proved that there are infinitely many primes; however, we are interested in a more quantitative answer to this question; that is, we want to know how "dense" the prime numbers are.

This chapter has a bit more of an "analytical" flavor than other chapters in this text. However, we shall not make use of any mathematics beyond that of elementary calculus.

5.1 Chebyshev's theorem on the density of primes

The natural way of measuring the density of primes is to count the number of primes up to a bound x, where x is a real number. To this end, we introduce the function $\pi(x)$, whose value at each real number $x \geq 0$ is defined to be the number of primes up to (and including) x. For example, $\pi(1) = 0$, $\pi(2) = 1$, and $\pi(7.5) = 4$. The function $\pi(x)$ is an example of a "step function," that is, a function that changes values only at a discrete set of points. It might seem more natural to define $\pi(x)$ only on the integers, but it is the tradition to define it over the real numbers (and there are some technical benefits in doing so).

Let us first take a look at some values of $\pi(x)$. Table 5.1 shows values of $\pi(x)$ for $x = 10^{3i}$ and $i = 1, \ldots, 6$. The third column of this table shows the value of $x/\pi(x)$ (to five decimal places). One can see that the differences between successive rows of this third column are roughly the same — about 6.9 — which suggests that the function $x/\pi(x)$ grows logarithmically in x. Indeed, as $\log(10^3) \approx 6.9$, it would not be unreasonable to guess that $x/\pi(x) \approx \log x$, or equivalently, $\pi(x) \approx x/\log x$ (as discussed in the Preliminaries, $\log x$ denotes the natural logarithm of x).

The following theorem is a first — and important — step towards making the above guesswork more rigorous (the statements of this and many other results in this chapter make use of the asymptotic notation introduced in §3.1):

Table 5.1. *Some values of* $\pi(x)$

x	$\pi(x)$	$x/\pi(x)$
10^3	168	5.95238
10^6	78498	12.73918
10^9	50847534	19.66664
10^{12}	37607912018	26.59015
10^{15}	29844570422669	33.50693
10^{18}	24739954287740860	40.42045

Theorem 5.1 (Chebyshev's theorem). *We have*

$$\pi(x) = \Theta(x/\log x).$$

It is not too difficult to prove this theorem, which we now proceed to do in several steps. We begin with some elementary bounds on binomial coefficients (see §A2):

Lemma 5.2. *If m is a positive integer, then*

$$\binom{2m}{m} \geq 2^{2m}/2m \quad \text{and} \quad \binom{2m+1}{m} < 2^{2m}.$$

Proof. As $\binom{2m}{m}$ is the largest binomial coefficient in the binomial expansion of $(1+1)^{2m}$, we have

$$2^{2m} = \sum_{i=0}^{2m} \binom{2m}{i} = 1 + \sum_{i=1}^{2m-1} \binom{2m}{i} + 1 \leq 2 + (2m-1)\binom{2m}{m} \leq 2m\binom{2m}{m}.$$

The proves the first inequality. For the second, observe that the binomial coefficient $\binom{2m+1}{m}$ occurs twice in the binomial expansion of $(1+1)^{2m+1}$, and is therefore less than $2^{2m+1}/2 = 2^{2m}$. □

Next, recalling that $\nu_p(n)$ denotes the power to which a prime p divides an integer n, we continue with the following observation:

Lemma 5.3. *Let n be a positive integer. For every prime p, we have*

$$\nu_p(n!) = \sum_{k\geq 1} \lfloor n/p^k \rfloor.$$

Proof. For all positive integers j, k, define $d_{jk} := 1$ if $p^k \mid j$, and $d_{jk} := 0$, otherwise. Observe that $\nu_p(j) = \sum_{k\geq 1} d_{jk}$ (this sum is actually finite, since $d_{jk} = 0$

for all sufficiently large k). So we have

$$\nu_p(n!) = \sum_{j=1}^{n} \nu_p(j) = \sum_{j=1}^{n} \sum_{k\geq 1} d_{jk} = \sum_{k\geq 1} \sum_{j=1}^{n} d_{jk}.$$

Finally, note that $\sum_{j=1}^{n} d_{jk}$ is equal to the number of multiples of p^k among the integers $1, \ldots, n$, which by Exercise 1.3 is equal to $\lfloor n/p^k \rfloor$. □

The following theorem gives a lower bound on $\pi(x)$.

Theorem 5.4. *$\pi(n) \geq \frac{1}{2}(\log 2)n/\log n$ for every integer $n \geq 2$.*

Proof. Let m be a positive integer, and consider the binomial coefficient

$$N := \binom{2m}{m} = \frac{(2m)!}{(m!)^2}.$$

It is clear that N is divisible only by primes p up to $2m$. Applying Lemma 5.3 to the identity $N = (2m)!/(m!)^2$, we have

$$\nu_p(N) = \sum_{k\geq 1} (\lfloor 2m/p^k \rfloor - 2\lfloor m/p^k \rfloor).$$

Each term in this sum is either 0 or 1 (see Exercise 1.4), and for $k > \log(2m)/\log p$, each term is zero. Thus, $\nu_p(N) \leq \log(2m)/\log p$. So we have

$$\begin{aligned} \pi(2m)\log(2m) &= \sum_{p\leq 2m} \frac{\log(2m)}{\log p} \log p \\ &\geq \sum_{p\leq 2m} \nu_p(N) \log p = \log N, \end{aligned}$$

where the summations are over the primes p up to $2m$. By Lemma 5.2, we have $N \geq 2^{2m}/2m \geq 2^m$, and hence

$$\pi(2m)\log(2m) \geq m \log 2 = \tfrac{1}{2}(\log 2)(2m).$$

That proves the theorem for even n. Now consider odd $n \geq 3$, so $n = 2m - 1$ for some $m \geq 2$. It is easily verified that the function $x/\log x$ is increasing for $x \geq 3$; therefore,

$$\begin{aligned} \pi(2m-1) &= \pi(2m) \\ &\geq \tfrac{1}{2}(\log 2)(2m)/\log(2m) \\ &\geq \tfrac{1}{2}(\log 2)(2m-1)/\log(2m-1). \end{aligned}$$

That proves the theorem for odd n. □

As a consequence of the above theorem, we have $\pi(x) = \Omega(x/\log x)$ for real numbers x. Indeed, setting $c := \frac{1}{2}(\log 2)$, for every real number $x \geq 2$, we have

$$\pi(x) = \pi(\lfloor x \rfloor) \geq c\lfloor x \rfloor / \log \lfloor x \rfloor \geq c(x-1)/\log x;$$

from this, it is clear that $\pi(x) = \Omega(x/\log x)$.

To obtain a corresponding upper bound for $\pi(x)$, we introduce an auxiliary function, called **Chebyshev's theta function**:

$$\vartheta(x) := \sum_{p \leq x} \log p,$$

where the sum is over all primes p up to x.

Chebyshev's theta function is an example of a summation over primes, and in this chapter, we will be considering a number of functions that are defined in terms of sums or products over primes (and indeed, such summations already cropped up in the proof of Theorem 5.4). To avoid excessive tedium, we adopt the usual convention used by number theorists: if not explicitly stated, summations and products over the variable p are always understood to be over primes. For example, we may write $\pi(x) = \sum_{p \leq x} 1$.

Theorem 5.5. *We have*

$$\vartheta(x) = \Theta(\pi(x) \log x).$$

Proof. On the one hand, we have

$$\vartheta(x) = \sum_{p \leq x} \log p \leq \log x \sum_{p \leq x} 1 = \pi(x) \log x.$$

On the other hand, we have

$$\begin{aligned} \vartheta(x) &= \sum_{p \leq x} \log p \geq \sum_{x^{1/2} < p \leq x} \log p \geq \tfrac{1}{2} \log x \sum_{x^{1/2} < p \leq x} 1 \\ &= \tfrac{1}{2} \log x \left(\pi(x) - \pi(x^{1/2}) \right) = \tfrac{1}{2} \left(1 - \pi(x^{1/2})/\pi(x) \right) \pi(x) \log x. \end{aligned}$$

It will therefore suffice to show that $\pi(x^{1/2})/\pi(x) = o(1)$. Clearly, $\pi(x^{1/2}) \leq x^{1/2}$. Moreover, by the previous theorem, $\pi(x) = \Omega(x/\log x)$. Therefore,

$$\pi(x^{1/2})/\pi(x) = O(\log x / x^{1/2}) = o(1),$$

and the theorem follows. □

Theorem 5.6. *$\vartheta(x) < 2(\log 2)x$ for every real number $x \geq 1$.*

Proof. It suffices to prove that $\vartheta(n) < 2(\log 2)n$ for every positive integer n, since then $\vartheta(x) = \vartheta(\lfloor x \rfloor) < 2(\log 2)\lfloor x \rfloor \leq 2(\log 2)x$. We prove this by induction on n.

For $n = 1$ and $n = 2$, this is clear, so assume $n > 2$. If n is even, then using the induction hypothesis for $n - 1$, we have

$$\vartheta(n) = \vartheta(n-1) < 2(\log 2)(n-1) < 2(\log 2)n.$$

Now consider the case where n is odd. Write $n = 2m + 1$, where m is a positive integer, and consider the binomial coefficient

$$M := \binom{2m+1}{m} = \frac{(2m+1)\cdots(m+2)}{m!}.$$

Observe that M is divisible by all primes p with $m + 1 < p \leq 2m + 1$. Moreover, be Lemma 5.2, we have $M < 2^{2m}$. It follows that

$$\vartheta(2m+1) - \vartheta(m+1) = \sum_{m+1<p\leq 2m+1} \log p \leq \log M < 2(\log 2)m.$$

Using this, and the induction hypothesis for $m + 1$, we obtain

$$\begin{aligned}\vartheta(n) &= \vartheta(2m+1) - \vartheta(m+1) + \vartheta(m+1) \\ &< 2(\log 2)m + 2(\log 2)(m+1) = 2(\log 2)n. \quad \square\end{aligned}$$

Another way of stating the above theorem is:

$$\prod_{p\leq x} p < 4^x.$$

Theorem 5.1 follows immediately from Theorems 5.4, 5.5 and 5.6. Note that we have also proved:

Theorem 5.7. *We have*

$$\vartheta(x) = \Theta(x).$$

EXERCISE 5.1. For each positive integer n, let p_n denote the nth prime. Show that $p_n = \Theta(n \log n)$.

EXERCISE 5.2. For each positive integer n, let $\omega(n)$ denote the number of distinct primes dividing n. Show that $\omega(n) = O(\log n / \log\log n)$.

EXERCISE 5.3. Show that $\sum_{p\leq x} 1/\log p = \Theta(x/(\log x)^2)$.

5.2 Bertrand's postulate

Suppose we want to know how many primes there are of a given bit length, or more generally, how many primes there are between m and $2m$ for a given positive integer m. Neither the statement, nor our proof, of Chebyshev's theorem imply that

there are *any* primes between m and $2m$, let alone a useful density estimate of such primes.

Bertrand's postulate is the assertion that for every positive integer m, there exists a prime between m and $2m$. We shall in fact prove a stronger result: there is at least one prime between m and $2m$, and moreover, the number of such primes is $\Omega(m/\log m)$.

Theorem 5.8 (Bertrand's postulate). *For every positive integer m, we have*

$$\pi(2m) - \pi(m) > \frac{m}{3\log(2m)}.$$

The proof uses Theorem 5.6, along with a more careful re-working of the proof of Theorem 5.4. The theorem is clearly true for $m \leq 2$, so we may assume that $m \geq 3$. As in the proof of the Theorem 5.4, define $N := \binom{2m}{m}$, and recall that N is divisible only by primes less than $2m$, and that we have the identity

$$\nu_p(N) = \sum_{k \geq 1} (\lfloor 2m/p^k \rfloor - 2\lfloor m/p^k \rfloor), \tag{5.1}$$

where each term in the sum is either 0 or 1. We can characterize the values $\nu_p(N)$ a bit more precisely, as follows:

Lemma 5.9. *Let $m \geq 3$ and $N := \binom{2m}{m}$. For all primes p, we have:*

$$p^{\nu_p(N)} \leq 2m; \tag{5.2}$$

$$\text{if } p > \sqrt{2m}, \text{ then } \nu_p(N) \leq 1; \tag{5.3}$$

$$\text{if } 2m/3 < p \leq m, \text{ then } \nu_p(N) = 0; \tag{5.4}$$

$$\text{if } m < p < 2m, \text{ then } \nu_p(N) = 1. \tag{5.5}$$

Proof. For (5.2), all terms with $k > \log(2m)/\log p$ in (5.1) vanish, and hence $\nu_p(N) \leq \log(2m)/\log p$, from which it follows that $p^{\nu_p(N)} \leq 2m$.

(5.3) follows immediately from (5.2).

For (5.4), if $2m/3 < p \leq m$, then $2m/p < 3$, and we must also have $p \geq 3$, since $p = 2$ implies $m < 3$. We have $p^2 > p(2m/3) = 2m(p/3) \geq 2m$, and hence all terms with $k > 1$ in (5.1) vanish. The term with $k = 1$ also vanishes, since $1 \leq m/p < 3/2$, from which it follows that $2 \leq 2m/p < 3$, and hence $\lfloor m/p \rfloor = 1$ and $\lfloor 2m/p \rfloor = 2$.

For (5.5), if $m < p < 2m$, it follows that $1 < 2m/p < 2$, so $\lfloor 2m/p \rfloor = 1$. Also, $m/p < 1$, so $\lfloor m/p \rfloor = 0$. It follows that the term with $k = 1$ in (5.1) is 1, and it is clear that $2m/p^k < 1$ for all $k > 1$, and so all the other terms vanish. □

We now have the necessary technical ingredients to prove Theorem 5.8. Define

$$P_m := \prod_{m<p<2m} p,$$

and define Q_m so that

$$N = Q_m P_m.$$

By (5.4) and (5.5), we see that

$$Q_m = \prod_{p \le 2m/3} p^{\nu_p(N)}.$$

Moreover, by (5.3), $\nu_p(N) > 1$ for at most those $p \le \sqrt{2m}$, so there are at most $\sqrt{2m}$ such primes, and by (5.2), the contribution of each such prime to the above product is at most $2m$. Combining this with Theorem 5.6, we obtain

$$Q_m < (2m)^{\sqrt{2m}} \cdot 4^{2m/3}.$$

We now apply Lemma 5.2, obtaining

$$P_m = NQ_m^{-1} \ge 2^{2m}(2m)^{-1}Q_m^{-1} > 4^{m/3}(2m)^{-(1+\sqrt{2m})}.$$

It follows that

$$\begin{aligned}\pi(2m) - \pi(m) &\ge \log P_m / \log(2m) > \frac{m \log 4}{3\log(2m)} - (1 + \sqrt{2m}) \\ &= \frac{m}{3\log(2m)} + \frac{m(\log 4 - 1)}{3\log(2m)} - (1 + \sqrt{2m}).\end{aligned}$$

Clearly, for all sufficiently large m, we have

$$\frac{m(\log 4 - 1)}{3\log(2m)} > 1 + \sqrt{2m}. \tag{5.6}$$

That proves Theorem 5.8 for all sufficiently large m. Moreover, a simple calculation shows that (5.6) holds for all $m \ge 13{,}000$, and one can verify by brute force (with the aid of a computer) that the theorem holds for $m < 13{,}000$.

5.3 Mertens' theorem

Our next goal is to prove the following theorem, which turns out to have a number of applications.

Theorem 5.10. *We have*

$$\sum_{p \le x} \frac{1}{p} = \log\log x + O(1).$$

The proof of this theorem, while not difficult, is a bit technical, and we proceed in several steps.

Theorem 5.11. *We have*

$$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1).$$

Proof. Let $n := \lfloor x \rfloor$. The idea of the proof is to estimate $\log(n!)$ in two different ways. By Lemma 5.3, we have

$$\log(n!) = \sum_{p \le n} \sum_{k \ge 1} \lfloor n/p^k \rfloor \log p = \sum_{p \le n} \lfloor n/p \rfloor \log p + \sum_{k \ge 2} \sum_{p \le n} \lfloor n/p^k \rfloor \log p.$$

We next show that the last sum is $O(n)$. We have

$$\begin{aligned} \sum_{p \le n} \log p \sum_{k \ge 2} \lfloor n/p^k \rfloor &\le n \sum_{p \le n} \log p \sum_{k \ge 2} p^{-k} \\ &= n \sum_{p \le n} \frac{\log p}{p^2} \cdot \frac{1}{1 - 1/p} = n \sum_{p \le n} \frac{\log p}{p(p-1)} \\ &\le n \sum_{k \ge 2} \frac{\log k}{k(k-1)} = O(n). \end{aligned}$$

Thus, we have shown that

$$\log(n!) = \sum_{p \le n} \lfloor n/p \rfloor \log p + O(n).$$

Since $\lfloor n/p \rfloor = n/p + O(1)$, applying Theorem 5.6 (and Exercise 3.12), we obtain

$$\log(n!) = \sum_{p \le n} (n/p) \log p + O\Big(\sum_{p \le n} \log p \Big) + O(n) = n \sum_{p \le n} \frac{\log p}{p} + O(n). \tag{5.7}$$

We can also estimate $\log(n!)$ by estimating a sum by an integral (see §A5):

$$\log(n!) = \sum_{k=1}^{n} \log k = \int_1^n \log t \, dt + O(\log n) = n \log n - n + O(\log n). \tag{5.8}$$

Combining (5.7) and (5.8), and noting that $\log x - \log n = o(1)$ (see Exercise 3.11), we obtain

$$\sum_{p \le x} \frac{\log p}{p} = \log n + O(1) = \log x + O(1),$$

which proves the theorem. □

We shall also need the following theorem, which is a very useful tool in its own right; it is essentially a discrete variant of "integration by parts."

Theorem 5.12 (Abel's identity). *Let $\{c_i\}_{i=k}^{\infty}$ be a sequence of real numbers, and for each real number t, define*

$$C(t) := \sum_{k \le i \le t} c_i.$$

Further, suppose that $f(t)$ is a function with a continuous derivative $f'(t)$ on the interval $[k, x]$, where x is a real number, with $x \ge k$. Then

$$\sum_{k \le i \le x} c_i f(i) = C(x)f(x) - \int_k^x C(t)f'(t)\,dt.$$

Note that since $C(t)$ is a step function, the integrand $C(t)f'(t)$ is piece-wise continuous on $[k, x]$, and hence the integral is well defined (see §A4).

Proof. Let $n := \lfloor x \rfloor$. We have

$$\begin{aligned}\sum_{i=k}^{n} c_i f(i) &= C(k)f(k) + \sum_{i=k+1}^{n} [C(i) - C(i-1)]f(i) \\ &= \sum_{i=k}^{n-1} C(i)[f(i) - f(i+1)] + C(n)f(n) \\ &= \sum_{i=k}^{n-1} C(i)[f(i) - f(i+1)] + C(n)[f(n) - f(x)] + C(x)f(x).\end{aligned}$$

Observe that for $i = k, \dots, n-1$, we have $C(t) = C(i)$ for all $t \in [i, i+1)$, and so

$$C(i)[f(i) - f(i+1)] = -C(i)\int_i^{i+1} f'(t)\,dt = -\int_i^{i+1} C(t)f'(t)\,dt;$$

likewise,

$$C(n)[f(n) - f(x)] = -\int_n^x C(t)f'(t)\,dt,$$

from which the theorem directly follows. □

Proof of Theorem 5.10. For $i \ge 2$, set

$$c_i := \begin{cases} (\log i)/i & \text{if } i \text{ is prime,} \\ 0 & \text{otherwise.} \end{cases}$$

By Theorem 5.11, we have

$$C(t) := \sum_{2 \le i \le t} c_i = \sum_{p \le t} \frac{\log p}{p} = \log t + R(t),$$

where $R(t) = O(1)$. Applying Theorem 5.12 with $f(t) := 1/\log t$ (and using Exercise 3.13), we obtain

$$\begin{aligned}\sum_{p\le x}\frac{1}{p} &= \sum_{2\le i\le x} c_i f(i) = \frac{C(x)}{\log x} + \int_2^x \frac{C(t)}{t(\log t)^2}dt \\ &= 1 + \frac{R(x)}{\log x} + \int_2^x \frac{dt}{t\log t} + \int_2^x \frac{R(t)}{t(\log t)^2}dt \\ &= 1 + O(1/\log x) + (\log\log x - \log\log 2) + O(1) \\ &= \log\log x + O(1). \ \square\end{aligned}$$

Using Theorem 5.10, we can easily show the following:

Theorem 5.13 (Mertens' theorem). *We have*

$$\prod_{p\le x}(1 - 1/p) = \Theta(1/\log x).$$

Proof. Using parts (i) and (iii) of §A1, for any fixed prime p, we have

$$-\frac{1}{p^2} \le \frac{1}{p} + \log(1 - 1/p) \le 0. \tag{5.9}$$

Moreover, since

$$\sum_{p\le x}\frac{1}{p^2} \le \sum_{i\ge 2}\frac{1}{i^2} < \infty,$$

summing the inequality (5.9) over all primes $p \le x$ yields

$$-C \le \sum_{p\le x}\frac{1}{p} + \log g(x) \le 0,$$

where C is a positive constant, and $g(x) := \prod_{p\le x}(1 - 1/p)$. From this, and from Theorem 5.10, we obtain $\log g(x) = -\log\log x + O(1)$, which implies that $g(x) = \Theta(1/\log x)$ (see Exercise 3.11). That proves the theorem. $\square$

EXERCISE 5.4. For each positive integer k, let P_k denote the product of the first k primes. Show that $\varphi(P_k) = \Theta(P_k/\log\log P_k)$ (here, φ is Euler's phi function).

EXERCISE 5.5. The previous exercise showed that $\varphi(n)$ could be as small as (about) $n/\log\log n$ for infinitely many n. Show that this is the "worst case," in the sense that $\varphi(n) = \Omega(n/\log\log n)$.

EXERCISE 5.6. Show that for every positive integer constant k,

$$\int_2^x \frac{dt}{(\log t)^k} = \frac{x}{(\log x)^k} + O\Big(\frac{x}{(\log x)^{k+1}}\Big).$$

This fact may be useful in some of the following exercises.

EXERCISE 5.7. Use Chebyshev's theorem and Abel's identity to prove a stronger version of Theorem 5.5: $\vartheta(x) = \pi(x)\log x + O(x/\log x)$.

EXERCISE 5.8. Use Chebyshev's theorem and Abel's identity to show that

$$\sum_{p \le x} \frac{1}{\log p} = \frac{\pi(x)}{\log x} + O(x/(\log x)^3).$$

EXERCISE 5.9. Show that

$$\prod_{2 < p \le x} (1 - 2/p) = \Theta(1/(\log x)^2).$$

EXERCISE 5.10. Show that if $\pi(x) \sim cx/\log x$ for some constant c, then we must have $c = 1$.

EXERCISE 5.11. Strengthen Theorem 5.10: show that for some constant A, we have $\sum_{p \le x} 1/p = \log\log x + A + o(1)$. You do not need to estimate A, but in fact $A \approx 0.261497212847643$.

EXERCISE 5.12. Use the result from the previous exercise to strengthen Mertens' theorem: show that for some constant B_1, we have $\prod_{p \le x}(1 - 1/p) \sim B_1/(\log x)$. You do not need to estimate B_1, but in fact $B_1 \approx 0.561459483566885$.

EXERCISE 5.13. Strengthen the result of Exercise 5.9: show that for some constant B_2, we have

$$\prod_{2 < p \le x} (1 - 2/p) \sim B_2/(\log x)^2.$$

You do not need to estimate B_2, but in fact $B_2 \approx 0.832429065662$.

EXERCISE 5.14. Use Abel's identity to derive **Euler's summation formula**: if $f(t)$ has a continuous derivative $f'(t)$ on the interval $[a, b]$, where a and b are integers, then

$$\sum_{i=a}^{b} f(i) - \int_a^b f(t)\,dt = f(a) + \int_a^b (t - \lfloor t \rfloor) f'(t)\,dt.$$

EXERCISE 5.15. Use Euler's summation formula (previous exercise) to show that

$$\log(n!) = n\log n - n + \tfrac{1}{2}\log n + O(1),$$

and from this, conclude that $n! = \Theta((n/e)^n\sqrt{n})$. This is a weak form of **Stirling's approximation**; a sharper form states that $n! \sim (n/e)^n\sqrt{2\pi n}$.

EXERCISE 5.16. Use Stirling's approximation (previous exercise) to show that

$$\binom{2m}{m} = \Theta(2^{2m}/\sqrt{m}).$$

5.4 The sieve of Eratosthenes

As an application of Theorem 5.10, consider the **sieve of Eratosthenes**. This is an algorithm that generates all the primes up to a given bound n. It uses an array $A[2 \ldots n]$, and runs as follows.

```
for k ← 2 to n do A[k] ← 1
for k ← 2 to ⌊√n⌋ do
    if A[k] = 1 then
        i ← 2k
        while i ≤ n do
            A[i] ← 0,  i ← i + k
```

When the algorithm finishes, we have $A[k] = 1$ if and only if k is prime, for $k = 2, \ldots, n$. This can easily be proven using the fact (see Exercise 1.2) that a composite number k between 2 and n must be divisible by a prime that is at most $\sqrt{n}$, and by proving by induction on k that at the beginning of each iteration of the main loop, $A[i] = 0$ if and only if i is divisible by a prime less than k, for $i = k, \ldots, n$. We leave the details of this to the reader.

We are more interested in the running time of the algorithm. To analyze the running time, we assume that all arithmetic operations take constant time; this is reasonable, since all the numbers computed are used as array indices and thus should fit in single machine words. Therefore, we can assume that built-in arithmetic instructions are used for operating on such numbers.

Every time we execute the inner loop of the algorithm, we perform $O(n/k)$ steps to clear the entries of A indexed by multiples of k. Pessimistically, then, we could bound the total running time by $O(n\,T(n))$, where

$$T(n) := \sum_{k \le \sqrt{n}} 1/k.$$

Estimating the sum by an integral (see §A5), we have

$$T(n) = \sum_{k=1}^{\lfloor \sqrt{n} \rfloor} 1/k = \int_1^{\lfloor \sqrt{n} \rfloor} \frac{dy}{y} + O(1) \sim \frac{1}{2} \log n.$$

This implies a $O(n \operatorname{len}(n))$ bound on the running time of the algorithm. However, this rather crude analysis ignores the fact that the inner loop is executed only for

prime values of k; taking this fact into account, we see that the running time is $O(n\,T_1(n))$, where

$$T_1(n) := \sum_{p \le \sqrt{n}} 1/p.$$

By Theorem 5.10, $T_1(n) = \log\log n + O(1)$, which implies a $O(n\,\mathrm{len}(\mathrm{len}(n)))$ bound on the running time of the algorithm. This is a substantial improvement over the above, rather crude analysis.

EXERCISE 5.17. Give a detailed proof of the correctness of the above algorithm.

EXERCISE 5.18. One drawback of the above algorithm is its use of space: it requires an array of size n. Show how to modify the algorithm, without substantially increasing its running time, so that one can enumerate all the primes up to n, using an auxiliary array of size just $O(\sqrt{n})$.

EXERCISE 5.19. Design and analyze an algorithm that on input n outputs the table of values $\tau(k)$ for $k = 1, \ldots, n$, where $\tau(k)$ is the number of positive divisors of k. Your algorithm should run in time $O(n\,\mathrm{len}(n))$.

5.5 The prime number theorem ... and beyond

In this section, we survey a number of theorems and conjectures related to the distribution of primes. This is a vast area of mathematical research, with a number of very deep results. We shall be stating a number of theorems from the literature in this section without proof; while our intent is to keep the text as self contained as possible, and to avoid degenerating into "mathematical tourism," it nevertheless is a good idea to occasionally have a somewhat broader perspective. In the subsequent chapters, we shall not make any critical use of the theorems in this section.

5.5.1 The prime number theorem

The main theorem in the theory of the density of primes is the following.

Theorem 5.14 (Prime number theorem). *We have*

$$\pi(x) \sim x/\log x.$$

Proof. Literature—see §5.6. □

As we saw in Exercise 5.10, if $\pi(x)/(x/\log x)$ tends to a limit as $x \to \infty$, then the limit must be 1, so in fact the hard part of proving the prime number theorem is to show that $\pi(x)/(x/\log x)$ does indeed tend to some limit.

EXERCISE 5.20. Using the prime number theorem, show that $\vartheta(x) \sim x$.

EXERCISE 5.21. Using the prime number theorem, show that $p_n \sim n \log n$, where p_n denotes the nth prime.

EXERCISE 5.22. Using the prime number theorem, show that Bertrand's postulate can be strengthened (asymptotically) as follows: for every $\varepsilon > 0$, there exist positive constants c and x_0, such that for all $x \geq x_0$, we have

$$\pi((1+\varepsilon)x) - \pi(x) \geq c\frac{x}{\log x}.$$

5.5.2 The error term in the prime number theorem

The prime number theorem says that

$$|\pi(x) - x/\log x| \leq \delta(x),$$

where $\delta(x) = o(x/\log x)$. A natural question is: how small is the "error term" $\delta(x)$? It can be shown that

$$\pi(x) = x/\log x + O(x/(\log x)^2). \tag{5.10}$$

This bound on the error term is not very impressive, but unfortunately, cannot be improved upon. The problem is that $x/\log x$ is not really the best "simple" function that approximates $\pi(x)$. It turns out that a better approximation to $\pi(x)$ is the **logarithmic integral**, defined for all real numbers $x \geq 2$ as

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

It is not hard to show (see Exercise 5.6) that

$$\mathrm{li}(x) = x/\log x + O(x/(\log x)^2). \tag{5.11}$$

Thus, $\mathrm{li}(x) \sim x/\log x \sim \pi(x)$. However, the error term in the approximation of $\pi(x)$ by $\mathrm{li}(x)$ is much better. This is illustrated numerically in Table 5.2; for example, at $x = 10^{18}$, $\mathrm{li}(x)$ approximates $\pi(x)$ with a relative error just under 10^{-9}, while $x/\log x$ approximates $\pi(x)$ with a relative error of about 0.025.

The sharpest proven result on the error in approximating $\pi(x)$ by $\mathrm{li}(x)$ is the following:

Theorem 5.15. *Let $\kappa(x) := (\log x)^{3/5}(\log\log x)^{-1/5}$. Then for some $c > 0$, we have*

$$\pi(x) = \mathrm{li}(x) + O(xe^{-c\kappa(x)}).$$

Proof. Literature—see §5.6. □

Table 5.2. *Values of* $\pi(x)$, $\mathrm{li}(x)$, *and* $x/\log x$

x	$\pi(x)$	$\mathrm{li}(x)$	$x/\log x$
10^3	168	176.6	144.8
10^6	78498	78626.5	72382.4
10^9	50847534	50849233.9	48254942.4
10^{12}	37607912018	37607950279.8	36191206825.3
10^{15}	29844570422669	29844571475286.5	28952965460216.8
10^{18}	24739954287740860	24739954309690414.0	24127471216847323.8

Note that the error term $xe^{-c\kappa(x)}$ is $o(x/(\log x)^k)$ for every fixed $k \geq 0$. Also note that (5.10) follows directly from (5.11) and Theorem 5.15.

Although the above estimate on the error term in the approximation of $\pi(x)$ by $\mathrm{li}(x)$ is pretty good, it is conjectured that the actual error term is much smaller:

Conjecture 5.16. *For all* $x \geq 2.01$, *we have*

$$|\pi(x) - \mathrm{li}(x)| < x^{1/2} \log x.$$

Conjecture 5.16 is equivalent to the famous **Riemann hypothesis**, which is a conjecture about the location of the zeros of a certain function, called **Riemann's zeta function**. We give a *very* brief, high-level account of this conjecture, and its connection to the theory of the distribution of primes.

For all real numbers $s > 1$, the zeta function is defined as

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{5.12}$$

Note that because $s > 1$, the infinite series defining $\zeta(s)$ converges. A simple, but important, connection between the zeta function and the theory of prime numbers is the following:

Theorem 5.17 (Euler's identity). *For every real number* $s > 1$, *we have*

$$\zeta(s) = \prod_{p} (1 - p^{-s})^{-1}, \tag{5.13}$$

where the product is over all primes p.

Proof. The rigorous interpretation of the infinite product on the right-hand side of (5.13) is as a limit of finite products. Thus, if p_i denotes the ith prime, for $i = 1, 2, \ldots$, then we are really proving that

$$\zeta(s) = \lim_{r \to \infty} \prod_{i=1}^{r} (1 - p_i^{-s})^{-1}.$$

Now, from the identity

$$(1 - p_i^{-s})^{-1} = \sum_{e=0}^{\infty} p_i^{-es},$$

we have

$$\prod_{i=1}^{r}(1 - p_i^{-s})^{-1} = \left(1 + p_1^{-s} + p_1^{-2s} + \cdots\right) \cdots \left(1 + p_r^{-s} + p_r^{-2s} + \cdots\right)$$
$$= \sum_{n=1}^{\infty} \frac{h_r(n)}{n^s},$$

where

$$h_r(n) := \begin{cases} 1 & \text{if } n \text{ is divisible only by the primes } p_1, \ldots, p_r; \\ 0 & \text{otherwise.} \end{cases}$$

Here, we have made use of the fact (see §A7) that we can multiply term-wise infinite series with non-negative terms.

Now, for every $\varepsilon > 0$, there exists n_0 such that $\sum_{n=n_0}^{\infty} n^{-s} < \varepsilon$ (because the series defining $\zeta(s)$ converges). Moreover, there exists an r_0 such that $h_r(n) = 1$ for all $n < n_0$ and $r \geq r_0$. Therefore, for all $r \geq r_0$, we have

$$\left| \sum_{n=1}^{\infty} \frac{h_r(n)}{n^s} - \zeta(s) \right| \leq \sum_{n=n_0}^{\infty} n^{-s} < \varepsilon.$$

It follows that

$$\lim_{r\to\infty} \sum_{n=1}^{\infty} \frac{h_r(n)}{n^s} = \zeta(s),$$

which proves the theorem. □

While Theorem 5.17 is nice, things become much more interesting if one extends the domain of definition of the zeta function to the complex plane. For the reader who is familiar with just a little complex analysis, it is easy to see that the infinite series defining the zeta function in (5.12) converges absolutely for all complex numbers s whose real part is greater than 1, and that (5.13) holds as well for such s. However, it is possible to extend the domain of definition of $\zeta(s)$ even further—in fact, one can extend the definition of $\zeta(s)$ in a "nice way " (in the language of complex analysis, *analytically continue*) to the entire complex plane (except the point $s = 1$, where there is a simple pole). Exactly how this is done is beyond the scope of this text, but assuming this extended definition of $\zeta(s)$, we can now state the Riemann hypothesis:

Conjecture 5.18 (Riemann hypothesis). *Suppose s is a complex number with $s = x + yi$, where $x, y \in \mathbb{R}$, such that $\zeta(s) = 0$ and $0 < x < 1$. Then $x = 1/2$.*

A lot is known about the zeros of the zeta function in the "critical strip," which consists of those points s whose real part is greater than 0 and less than 1: it is known that there are infinitely many such zeros, and there are even good estimates about their density. It turns out that one can apply standard tools in complex analysis, like contour integration, to the zeta function (and functions derived from it) to answer various questions about the distribution of primes. Indeed, such techniques may be used to prove the prime number theorem. However, if one assumes the Riemann hypothesis, then these techniques yield much sharper results, such as the bound in Conjecture 5.16.

EXERCISE 5.23. For any arithmetic function a (mapping positive integers to reals), we can form the **Dirichlet series**

$$F_a(s) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s}.$$

For simplicity we assume that s takes only real values, even though such series are usually studied for complex values of s.

(a) Show that if the Dirichlet series $F_a(s)$ converges absolutely for some real s, then it converges absolutely for all real $s' \geq s$.

(b) From part (a), conclude that for any given arithmetic function a, there is an **interval of absolute convergence** of the form (s_0, ∞), where we allow $s_0 = -\infty$ and $s_0 = \infty$, such that $F_a(s)$ converges absolutely for $s > s_0$, and does not converge absolutely for $s < s_0$.

(c) Let a and b be arithmetic functions such that $F_a(s)$ has an interval of absolute convergence (s_0, ∞) and $F_b(s)$ has an interval of absolute convergence (s_0', ∞), and assume that $s_0 < \infty$ and $s_0' < \infty$. Let $c := a \star b$ be the Dirichlet product of a and b, as defined in §2.9. Show that for all $s \in (\max(s_0, s_0'), \infty)$, the series $F_c(s)$ converges absolutely and, moreover, that $F_a(s)F_b(s) = F_c(s)$.

5.5.3 Explicit estimates

Sometimes, it is useful to have explicit estimates for $\pi(x)$, as well as related functions, like $\vartheta(x)$ and the nth prime function p_n. The following theorem presents a number of bounds that have been proved without relying on any unproved conjectures.

Theorem 5.19. *We have:*

(i) $\dfrac{x}{\log x}\Big(1+\dfrac{1}{2\log x}\Big) < \pi(x) < \dfrac{x}{\log x}\Big(1+\dfrac{3}{2\log x}\Big)$, *for* $x \geq 59$;

(ii) $n(\log n + \log\log n - 3/2) < p_n < n(\log n + \log\log n - 1/2)$, *for* $n \geq 20$;

(iii) $x\Big(1-\dfrac{1}{2\log x}\Big) < \vartheta(x) < x\Big(1+\dfrac{1}{2\log x}\Big)$, *for* $x \geq 563$;

(iv) $\log\log x + A - \dfrac{1}{2(\log x)^2} < \displaystyle\sum_{p\leq x} 1/p < \log\log x + A + \dfrac{1}{2(\log x)^2}$,
for $x \geq 286$, *where* $A \approx 0.261497212847643$;

(v) $\dfrac{B_1}{\log x}\Big(1-\dfrac{1}{2(\log x)^2}\Big) < \displaystyle\prod_{p\leq x}\Big(1-\frac{1}{p}\Big) < \dfrac{B_1}{\log x}\Big(1+\dfrac{1}{2(\log x)^2}\Big)$,
for $x \geq 285$, *where* $B_1 \approx 0.561459483566885$.

Proof. Literature—see §5.6. □

5.5.4 Primes in arithmetic progressions

In Theorems 2.35 and 2.36, we proved that there are infinitely many primes $p \equiv 1 \pmod 4$ and infinitely many primes $p \equiv 3 \pmod 4$. These results are actually special cases of a much more general result.

Let d be a positive integer, and let a be any integer. An **arithmetic progression** with first term a and common difference d consists of all integers of the form

$$a + dm, \quad m = 0, 1, 2, \ldots.$$

The question is: under what conditions does such an arithmetic progression contain infinitely many primes? An equivalent formulation is: under what conditions are there infinitely many primes $p \equiv a \pmod d$? If a and d have a common factor $c > 1$, then every term in the progression is divisible by c, and so there can be at most one prime in the progression. So a necessary condition for the existence of infinitely many primes $p \equiv a \pmod d$ is that $\gcd(a, d) = 1$. A famous theorem due to Dirichlet states that this is a sufficient condition as well.

Theorem 5.20 (Dirichlet's theorem). *Let* $a, d \in \mathbb{Z}$ *with* $d > 0$ *and* $\gcd(a, d) = 1$. *Then there are infinitely many primes* $p \equiv a \pmod d$.

Proof. Literature—see §5.6. □

We can also ask about the density of primes in arithmetic progressions. One might expect that for a fixed value of d, the primes are distributed in roughly equal

measure among the $\varphi(d)$ different residue classes $[a]_d$ with $\gcd(a,d) = 1$ (here, φ is Euler's phi function). This is in fact the case. To formulate such assertions, we define $\pi(x;d,a)$ to be the number of primes p up to x with $p \equiv a \pmod{d}$.

Theorem 5.21. *Let $a, d \in \mathbb{Z}$ with $d > 0$ and $\gcd(a,d) = 1$. Then*

$$\pi(x;d,a) \sim \frac{x}{\varphi(d)\log x}.$$

Proof. Literature—see §5.6. □

The above theorem is only applicable in the case where d and a are fixed as $x \to \infty$. For example, it says that roughly half the primes up to x are congruent to 1 modulo 4, and roughly half the primes up to x are congruent to 3 modulo 4. However, suppose $d \to \infty$, and we want to estimate, say, the number of primes $p \equiv 1 \pmod{d}$ up to d^3. Theorem 5.21 does not help us here. The following conjecture does, however:

Conjecture 5.22. *Let $x \in \mathbb{R}$, $a, d \in \mathbb{Z}$ with $x \geq 2$, $d \geq 2$, and $\gcd(a,d) = 1$. Then*

$$\left| \pi(x;d,a) - \frac{\operatorname{li}(x)}{\varphi(d)} \right| \leq x^{1/2}(\log x + 2\log d).$$

The above conjecture is in fact a consequence of a generalization of the Riemann hypothesis — see §5.6. This conjecture implies that for every constant $\alpha < 1/2$, if $2 \leq d \leq x^\alpha$, then $\pi(x;d,a)$ is closely approximated by $\operatorname{li}(x)/\varphi(d)$ (see Exercise 5.24). It can also be used to get an upper bound on the least prime $p \equiv a \pmod{d}$ (see Exercise 5.25). The following theorem is the best rigorously proven upper bound on the smallest prime in an arithmetic progression:

Theorem 5.23. *There exists a constant c such that for all $a, d \in \mathbb{Z}$ with $d \geq 2$ and $\gcd(a,d) = 1$, the least prime $p \equiv a \pmod{d}$ is at most $cd^{11/2}$.*

Proof. Literature—see §5.6. □

EXERCISE 5.24. Assuming Conjecture 5.22, show that for all α, ε satisfying $0 < \alpha < 1/2$ and $0 < \varepsilon < 1$, there exists an x_0, such that for all $x > x_0$, for all $d \in \mathbb{Z}$ with $2 \leq d \leq x^\alpha$, and for all $a \in \mathbb{Z}$ relatively prime to d, the number of primes $p \leq x$ such that $p \equiv a \pmod{d}$ is at least $(1-\varepsilon)\operatorname{li}(x)/\varphi(d)$ and at most $(1+\varepsilon)\operatorname{li}(x)/\varphi(d)$.

EXERCISE 5.25. Assuming Conjecture 5.22, show that there exists a constant c such that for all $a, d \in \mathbb{Z}$ with $d \geq 2$ and $\gcd(a,d) = 1$, the least prime $p \equiv a \pmod{d}$ is at most $c\varphi(d)^2(\log d)^4$.

5.5.5 Sophie Germain primes

A **Sophie Germain prime** is a prime p such that $2p+1$ is also prime. Such primes are actually useful in a number of practical applications, and so we discuss them briefly here.

It is an open problem to prove (or disprove) that there are infinitely many Sophie Germain primes. However, numerical evidence, and heuristic arguments, strongly suggest not only that there are infinitely many such primes, but also a fairly precise estimate on the density of such primes.

Let $\pi^*(x)$ denote the number of Sophie Germain primes up to x.

Conjecture 5.24. *We have*

$$\pi^*(x) \sim C\frac{x}{(\log x)^2},$$

where C is the constant

$$C := 2\prod_{p>2}\frac{p(p-2)}{(p-1)^2} \approx 1.32032,$$

and the product is over all primes $p > 2$.

The above conjecture is a special case of the following, more general conjecture.

Conjecture 5.25 (Dickson's conjecture). *Let $(a_1, b_1), \ldots, (a_k, b_k)$ be distinct pairs of integers, where each a_i is positive. Let $P(x)$ be the number of positive integers m up to x such that $a_i m + b_i$ are simultaneously prime for $i = 1, \ldots, k$. For each prime p, let $\omega(p)$ be the number of integers $m \in \{0, \ldots, p-1\}$ that satisfy*

$$\prod_{i=1}^{k}(a_i m + b_i) \equiv 0 \pmod{p}.$$

If $\omega(p) < p$ for each prime p, then

$$P(x) \sim D\frac{x}{(\log x)^k},$$

where

$$D := \prod_{p}\frac{1-\omega(p)/p}{(1-1/p)^k},$$

the product being over all primes p.

In Exercise 5.26 below, you are asked to verify that the quantity D appearing in Conjecture 5.25 satisfies $0 < D < \infty$. Conjecture 5.24 is implied by Conjecture 5.25 with $k := 2$, $(a_1, b_1) := (1, 0)$, and $(a_2, b_2) := (2, 1)$; in this case,

$\omega(2) = 1$ and $\omega(p) = 2$ for all $p > 2$. The above conjecture also includes (a strong version of) the famous **twin primes conjecture** as a special case: the number of primes p up to x such that $p + 2$ is also prime is $\sim Cx/(\log x)^2$, where C is the same constant as in Conjecture 5.24.

A heuristic argument in favor of Conjecture 5.25 runs as follows. In some sense, the chance that a large positive integer m is prime is about $1/\log m$. Since $\log(a_i m + b_i) \sim \log m$, the chance that $a_1 m + b_1, \ldots, a_k m + b_k$ are all prime should be about $1/(\log m)^k$. But this ignores the fact that $a_1 m + b_1, \ldots, a_k m + b_k$ are not quite random integers. For each prime p, we must apply a "correction factor" r_p/s_p, where r_p is the chance that for random m, none of $a_1 m + b_1, \ldots, a_k m + b_k$ is divisible by p, and s_p is the chance that for k truly random, large integers, none of them is divisible by p. One sees that $r_p = 1 - \omega(p)/p$ and $s_p = (1 - 1/p)^k$. This implies (using §A5 and Exercise 5.6) that $P(x)$ should be about

$$D \sum_{m \le x} 1/(\log m)^k \sim D \int_2^x dt/(\log t)^k \sim Dx/(\log x)^k.$$

Although Conjecture 5.25 is well supported by numerical evidence, there seems little hope of it being proved any time soon, even under the Riemann hypothesis or any of its generalizations.

EXERCISE 5.26. Show that the quantity D appearing in Conjecture 5.25 satisfies $0 < D < \infty$. Hint: first show that $\omega(p) = k$ for all sufficiently large p.

EXERCISE 5.27. Derive Theorem 5.21 from Conjecture 5.25.

EXERCISE 5.28. Show that the constant C appearing in Conjecture 5.24 satisfies

$$2C = B_2/B_1^2,$$

where B_1 and B_2 are the constants from Exercises 5.12 and 5.13.

5.6 Notes

The prime number theorem was conjectured by Gauss in 1791. It was proven independently in 1896 by Hadamard and de la Vallée Poussin. A proof of the prime number theorem may be found, for example, in the book by Hardy and Wright [46].

Theorem 5.19, as well as the estimates for the constants A, B_1, and B_2 mentioned in that theorem and Exercises 5.11, 5.12, and 5.13, are from Rosser and Schoenfeld [83].

Theorem 5.15 is from Walfisz [102].

Theorem 5.17, which made the first connection between the theory of prime numbers and the zeta function, was discovered in the 18th century by Euler. The Riemann hypothesis was made by Riemann in 1859, and to this day, remains one of the most vexing conjectures in mathematics. Riemann in fact showed that his conjecture about the zeros of the zeta function is equivalent to the conjecture that for each fixed $\varepsilon > 0$, $\pi(x) = \mathrm{li}(x) + O(x^{1/2+\varepsilon})$. This was strengthened by von Koch in 1901, who showed that the Riemann hypothesis is true if and only if $\pi(x) = \mathrm{li}(x) + O(x^{1/2} \log x)$. See Chapter 1 of the book by Crandall and Pomerance [30] for more on the connection between the Riemann hypothesis and the theory of prime numbers; in particular, see Exercise 1.36 in that book for an outline of a proof that Conjecture 5.16 follows from the Riemann hypothesis.

A warning: some authors (and software packages) define the logarithmic integral using the interval of integration $(0, x)$, rather than $(2, x)$, which increases its value by a constant $c \approx 1.0452$.

Theorem 5.20 was proved by Dirichlet in 1837, while Theorem 5.21 was proved by de la Vallée Poussin in 1896. A result of Oesterlé [73] implies that Conjecture 5.22 for $d \geq 3$ is a consequence of an assumption about the location of the zeros of certain generalizations of Riemann's zeta function; the case $d = 2$ follows from the bound in Conjecture 5.16 under the ordinary Riemann hypothesis. Theorem 5.23 is from Heath-Brown [47]. The bound in Exercise 5.25 can be improved to $c\varphi(d)^2(\log d)^2$ (see Theorem 8.5.8 of [11]).

Conjecture 5.25 originates from Dickson [33]. In fact, Dickson only conjectured that the quantity $P(x)$ defined in Conjecture 5.25 tends to infinity. The conjectured formula for the rate of growth of $P(x)$ is a special case of a more general conjecture stated by Bateman and Horn [12], which generalizes various, more specific conjectures stated by Hardy and Littlewood [45].

For the reader who is interested in learning more on the topics discussed in this chapter, we recommend the books by Apostol [8] and Hardy and Wright [46]; indeed, many of the proofs presented in this chapter are minor variations on proofs from these two books. Our proof of Bertrand's postulate is based on the presentation in Section 9.2 of Redmond [80]. See also Bach and Shallit [11] (especially Chapter 8), as well as Crandall and Pomerance [30] (especially Chapter 1), for a more detailed overview of these topics.

The data in Tables 5.1 and 5.2 was obtained using the computer program *Maple.*