Chapter 9
Hidden in Plain Sight

Chebyshev said it, and I'll say it again,
There's always a prime between n and 2n

Nathan Fine (1916–1994)

Take any number and keep finding factors of that number that cannot be factored themselves. For example, $84 = 2 \cdot 2 \cdot 3 \cdot 7$, $455 = 5 \cdot 7 \cdot 13$ or $897 = 3 \cdot 13 \cdot 23$. These examples show that a number can be written as the product of prime numbers.[1] This is called a *prime factorization*. A separate argument, that we will shortly get to, shows that this factorization is unique. This result has far reaching consequences and is called the *Fundamental Theorem of Arithmetic*. This theorem shows that primes are the DNA of the number system. Essentially all of the results of number theory are theorems of the primes, the topic of this chapter.

9.1 Properties of Prime Numbers

Do primes ever end? To address this question, let $p_1, p_2, \ldots, p_n$ be a list of successive primes that end with an assumed maximal prime p_n. Consider a *primorial number*, denoted by the somewhat strange notation $p_n\#$, that corresponds to the product of the first n consecutive primes

$$p_n\# = p_1 \cdot p_2 \cdots p_{n-1} \cdot p_n \tag{9.1}$$

[1] Just keep dividing until it is not possible to continue without having a remainder.

R. Nelson, *A Brief Journey in Discrete Mathematics*,
https://doi.org/10.1007/978-3-030-37861-5_9

This is not a prime number but how about $p_n\# + 1$? If $p_n\# + 1$ is divided by p_j:

$$\frac{p_n\# + 1}{p_j} = p_1 \cdot p_2 \cdots p_{j-1} \cdot p_{j+1} \cdots p_{n-1} \cdot p_n + \frac{1}{p_j}$$

then the result is a whole number with a remainder. But if no previous prime divides $p_n\# + 1$, then it must be prime and it is clearly larger than p_n, the presumed largest prime. This contradicts the assumption that there is a maximal prime. This clever argument was first put forth sometime around 300 BC by Euclid of Alexandria, the father of *Euclidean geometry*. There are literally dozens of proofs that the primes go on infinitely and we will see a couple more in this chapter.

How does one generate a list of prime numbers? Let us discuss one way proposed by another Greek mathematician, Eratosthenes (276–194 BC), who developed a technique sometime around 200 BC. It is a simple idea called a *sieve*. For a variety of reasons the integer 1 is not considered to be prime.[2] A sieve starts by writing all the integers starting from 2

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, \ldots$$

The first number in the list, 2, is the first prime and this means that all subsequent multiples of 2 can be crossed out as candidate primes;

$$2, 3, \not{4}, 5, \not{6}, 7, \not{8}, 9, \not{10}, 11, \not{12}, 13, \not{14}, 15, \not{16}, 17, \not{18}, 19, \not{20}, 21, \not{22}, 23, \ldots$$

This leaves the next prime, 3. Repeating this process, cross out all multiples of 3 yielding

$$2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \ldots$$

Notice that 6 is already crossed out because it was divisible by 2 and would again be crossed out because it is also divisible by 3. The first remaining number is the next prime, 5, and the process continues by crossing out multiples of 5

$$2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, \ldots$$

This leaves 7 as the next prime. The algorithm continues on from here.

[2] Essentially it makes too many trivial exceptions in theorems in number theory.

Eventually the only numbers left not crossed are the set of primes. This sieve shows how primes emerge as the essential components of the integers. There are other methods to generate primes and long lists of primes can be found on the Internet. Its maddening, however, that there is no equation for the n'th prime. No one who has walked the earth, and even perhaps who will ever walk the earth, knows the 17 quadragintillion'th prime.

We next return to the fundamental theorem of arithmetic and prove that the representation of an integer as a product of primes is unique. For small values of n this is easily established so assume the first time uniqueness does not hold is at integer m. It is clear that m cannot be prime. Assume that composite m has two different prime factorizations. In these factorizations, order the primes in increasing value so that p is the smallest prime in the first factorization and q is the smallest in the second. Let the remaining portion of the factorizations of m be denoted by P and Q, respectively. Thus we can write

$$m = pP = qQ$$

Note that P is composed of primes at least as large as p and, similarly, Q consists of primes at least as large as q. If $p = q$, then we reach a contradiction since $P = m/p = m/q = Q$ is an integer smaller than m which is assumed to have a unique factorization. Since p and q differ, one has to be greater so assume that $p > q$. Note, from the two factorizations above, m is divisible by both p and q. It clearly is divisible by p but what about q? If q divides m, then it must divide either p or P. But this is impossible since both of these terms consist of products of primes that are strictly larger than q. Thus we reach a contradiction—prime factorizations are unique.

From now we will talk about integers in terms of their prime factorization. Let $\omega_i(n)$ be the exponent of the i'th prime, p_i, in the representation of the integer n, thus

$$n = 2^{\omega_1(n)} \cdot 3^{\omega_2(n)} \cdot 5^{\omega_3(n)} \cdot 7^{\omega_4(n)} \cdots p_i^{\omega_i(n)} \cdots = \prod_{i=1}^{\infty} p_i^{\omega_i(n)}$$

To multiply two numbers using this representation one simply adds exponents

$$n \cdot m = \prod_{i=1}^{\infty} p_i^{\omega_i(n)+\omega_i(m)}$$

More conveniently we can write n as the infinite vector of values $\omega(n) = (\omega_1(n),\ \omega_2(n),\ \ldots)$ where the j'th place corresponds to the exponent of p_j. Thus $n \cdot m$ is represented as the vector addition: $\omega(n \cdot m) = (\omega_1(n) + \omega_1(m),\ \omega_2(n) + \omega_2(m),\ \ldots)$. As an example,

$$198 = (1, 2, 0, 0, 1, 0, \ldots) = 2 \cdot 3^2 \cdot 11 \tag{9.2}$$

Note that $w_i(n/m) = w_i(n) - w_i(m)$ (provided n is divisible by m) and $w_i(n^k) = kw_i(n)$ for integer k.

9.1.1 Properties of Integer Divisors

This notation allows us to specify the total number of divisors as well as the sum of all the divisors with simple arithmetic expressions. Define $\sigma_k(n)$ be the

$$\sigma_k(n) = \sum_{d|n} d^k \tag{9.3}$$

where $d|n$ means that the summation occur over all possible integer values of d that evenly divide n. Thus, $\sigma_0(n)$ is the number of total divisors of n and $\sigma_1(n)$ is the sum of the total divisors. For the example (9.2) above there are 12 divisors given by

$$\{1, 2, 3, 11, 2 \cdot 3, 2 \cdot 11, 3^2, 3 \cdot 11, 2 \cdot 3^2, 2 \cdot 3 \cdot 11, 3^2 \cdot 11, 2 \cdot 3^2 \cdot 11\}$$

To calculate an expression for $\sigma_0(n)$, concentrate on the i'th prime which has an exponent of $\omega_i(n)$. The total number of possible divisors due to this prime is given by

$$p_i^0,\ p_i^1, \ldots, p_i^{\omega_i(n)}$$

leading to a total of $1 + \omega_i(n)$ possibilities. Since this is true for all i we have

$$\sigma_0(n) = (1 + \omega_1(n))(1 + \omega_2(n)) \cdots = \prod_{i=1}^{\infty} (1 + \omega_i(n)) \tag{9.4}$$

Note the special case for primes raised to a power:

$$\sigma_0(p_i^k) = k + 1 \tag{9.5}$$

The value sum of the divisors for the example can be expressed by

$$\sigma_1(198) = (2^0 + 2^1)(3^0 + 3^1 + 3^2)(11^0 + 11^1)$$

To explain this, note that expanding this multiplication into its individual factors corresponds to summing all possible products of the form $2^{k_1}3^{k_2}11^{k_5}$, where $k_1 = 0, 1,\ \ k_2 = 1, 2, 3$, and $k_5 = 1, 2$. Following this pattern we can write the sum of all the divisors for n as the product of the sum of all the divisors for the i'th prime

$$1 + p_i^1 + p_i^2 + \cdots + p_i^{\omega_i(n)} = \frac{p_i^{\omega_i(n)+1} - 1}{p_i - 1}$$

Thus $\sigma_1(n)$ is given by

$$\sigma_1(n) = \prod_{i=1}^{\infty} \frac{p_i^{\omega_i(n)+1} - 1}{p_i - 1} \tag{9.6}$$

For the example above, we obtain $\sigma_1(198) = 468$. Note the special case for primes raised to a power:

$$\sigma_1(p_i^k) = 1 + p_i^1 + \cdots + p_i^k = \frac{p_i^{k+1} - 1}{p_i - 1} \tag{9.7}$$

The prime factorization of $n! = n(n-1)\cdots 2 \cdot 1$ can be obtained from the factorizations of all the integers less than or equal to n. For prime p_i, let $\Omega_i(n) = \omega_i(n!)$ which is given by

$$\Omega_i(n) = \sum_{k=2}^{n} \omega_i(k)$$

A modification of a sieve argument allows us to calculate a closed form expression for $\Omega_i(n)$. To motivate this argument, consider the prime factorization of 10! and concentrate on the value of the exponent of 2 in that factorization. Every step of size $2^i,\ i = 1, \ldots$ corresponds to a multiplication by 2 which has to be counted in the final value of

the exponent. For 10! we have factors associated with 2^1, arising from $2, 4, 6, 8, 10$, factors associated with 2^2, from 4 and 8, and associated with 2^3, from 8. Counting all of these shows that the final exponent of 2 equals 8. Mathematically, we can write the contribution to the final exponent for factors associated with 2^i by the integer portion of $n/2^i$. Generalization of this argument shows that

$$\Omega_i(n) = \sum_{\ell : p_i^\ell \le n} \left\lfloor \frac{n}{p_i^\ell} \right\rfloor \tag{9.8}$$

The prime factorization can therefore be written as

$$n! = \prod_{i=1}^{\infty} p_i^{\Omega_i(n)} \tag{9.9}$$

From this equation it is clear that $n!$ cannot be prime (indeed all factorial numbers are even), but $n! \pm 1$ could be. Such primes are called *factorial primes*. Less than a hundred of these primes have been discovered.

Recall the definition of a primorial number defined in equation (9.1), values of which are given by

n	1	2	3	4	5	6	7	8	9
p_n	2	3	5	7	11	13	17	19	23
$p_n\#$	2	6	30	210	2,310	30,030	510,510	9,699,690	223,092,870

9.2 The Prime Counting Function

A closely related function to $p_n\#$, denoted by $z\#$, is the product of all primes less than or equal to a value z:

$$z\# = \prod_{i=1}^{\pi(z)} p_i \tag{9.10}$$

where $\pi(z)$, the *prime counting function*, is the number of primes less than or equal to z

$$\pi(z) = \sum_{i:p_i \le z} 1 \tag{9.11}$$

Since $z\#$ only depends on primes, if the largest prime less than or equal to z is p_n (equivalently $\pi(z) = n$), then $p_n\# = z\#$. From equations (9.5) and (9.7) we can write $\sigma_0(p_n\#) = 2^n$ and

$$\sigma_1(p_n\#) = \prod_{i=1}^{n}(p_i + 1) \tag{9.12}$$

or, expressing this in a different notation, that

$$\sigma_1(z\#) = \prod_{i=1}^{\pi(z)}(p_i + 1) \tag{9.13}$$

We wish to show that an upper bound of $z\#$ is given by

$$z\# \le 4^{z-1} \tag{9.14}$$

Since $\lfloor z \rfloor \# = z\#$ and $4^{\lfloor z \rfloor - 1} \le 4^{z-1}$ we can, without loss of generality, restrict z to be integer when deriving the bound. It is easy to check that (9.14) holds for small values of z. Assume then, inductively, that it holds for all values up to z. Since the value of $z\#$ only depends on primes less than or equal to z, it suffices to show that (9.14) holds for the largest odd prime less than or equal to z. Let this prime be given by $2\ell + 1$ and decompose $(2\ell + 1)\#$ into disjoint multiplications:

$$\begin{aligned}(2\ell+1)\,\# &= (\ell+1)\,\# \prod_{i:\ell+1<p_i\le 2\ell+1} p_i \\ &\le 4^{\ell} \prod_{i:\ell+1<p_i\le 2\ell+1} p_i\end{aligned} \tag{9.15}$$

The induction hypothesis is used to create the inequality in the first term of the last equation.

The second product term in (9.15) reminds one of a portion of a binomial coefficient. In particular, recall the computational form for binomial coefficients given in equation (2.11):

$$\binom{2\ell+1}{\ell} = \prod_{j=0}^{\ell-1} \frac{2\ell+1-j}{\ell-j} \tag{9.16}$$

There are two things to note: each term of this product is a fraction that is greater than 1 and primes in the range $i : \ell+1 < p_i \leq 2\ell+1$ are contained in the numerator of (9.16) but not in the denominator. This shows that the binomial coefficient is larger or equal to the multiplication of consecutive primes from $\ell+1$ to $2\ell+1$ and thus that

$$\prod_{i:\ell+1<p_i\leq 2\ell+1} p_i < \binom{2\ell+1}{\ell} \tag{9.17}$$

Since

$$\binom{2\ell+1}{\ell} = \binom{2\ell+1}{\ell+1}$$

we can use the binomial summation formula of (2.21) to write

$$2\binom{2\ell+1}{\ell} = 2^{2\ell+1} - \sum_{j\neq\ell,\ell+1} \binom{2\ell+1}{j}$$

Dividing by 2 and eliminating the subtraction shows that

$$\binom{2\ell+1}{\ell} < 2^{2\ell} = 4^{\ell}$$

Combining this with (9.15) yields the final bound

$$(2\ell+1)\,\# \leq 4^{2\ell} \tag{9.18}$$

For z not restricted to being integer or prime, this bound can be rewritten in the form of equation (9.14).

9.3 There Is Always a Prime Between n and $2n$

A generalization of a primorial number is one consisting of the multiplication of primes (not necessarily consecutive). Such numbers are said to be *square-free* since the exponents in their prime factorization are less than or equal to 1. The following proof shows that all integers can be factorized as the product of an integer and a square-free number. Let n be an integer and write

$$n = m^2 \ell \tag{9.19}$$

where m^2 is the largest square divisor of n (possibly equal to 1) and ℓ is a square-free integer. Recall that $\omega_i(n)$ is the exponent of p_i in the prime factorization of n. Let $a_i(n)$ and $b_i(n)$ solve

$$\omega_i(n) = 2a_i(n) + b_i(n), \quad 0 \leq b_i(n) \leq 1 \tag{9.20}$$

If $b_i(n) = 1$, then the i'th exponent has odd parity.

With this notation, the factorization of n given by (9.19) follows for m and ℓ that satisfy $\omega_i(m) = a_i(n)$ and $\omega_i(\ell) = b_i(n)$. To illustrate this with an example, consider

$$2,156,000 = 2^5\, 5^3\, 7^2\, 11$$

Then $m = 140 = 2^2 \cdot 5 \cdot 7$ and $\ell = 110 = 2 \cdot 5 \cdot 11$ and thus $2,156,000 = 140^2 \cdot 110$.

How many square-free numbers are there less than n? To answer this, note that since all products of primes less than n are square-free, the total number corresponds to the number of subsets of $\pi(n)$ items which is given by $2^{\pi(n)}$.[3] We have just showed that any number can be written as product of a square with a square-free number. There are at most $\sqrt{n}$ square numbers less than n. Thus, it must be the case that $n \leq \sqrt{n}\ 2^{\pi(n)}$. After taking the natural logarithm of both sides, this implies that

$$\pi(n) \geq \frac{\ln(n)}{2\ln(2)} \tag{9.21}$$

[3] A consequence of the binomial theorem, see equation (2.21).

Equation (9.21) is not only another proof of the infinitude of the primes but it also provides a lower bound for the n'th prime. You should note that this strong result is a direct consequence of the simple factorization given in (9.19).

Equation (9.9) proves useful in deriving an upper bound on the central binomial coefficient:

$$\begin{aligned}(9.22)\qquad \binom{2n}{n} &= \frac{(2n)!}{(n!)^2} = \prod_{i=1}^{\infty} p_i^{\Omega_i(2n)} \Big/ \left(\prod_{i=1}^{\infty} p_i^{\Omega_i(n)}\right)^2 \\ &= \prod_{i=1}^{\infty} p_i^{\Omega_i(2n)} \Big/ \prod_{i=1}^{\infty} p_i^{2\Omega_i(n)} = \prod_{i=1}^{\infty} p_i^{\Omega_i(2n)-2\Omega_i(n)} \\ &= \prod_{i=1}^{\infty} p_i^{m_i}\end{aligned}$$

where we have defined

$$(9.23)\qquad m_i = \sum_{\ell: p_i^\ell \le 2n} \psi_{i,\ell}$$

and

$$(9.24)\qquad \psi_{i,\ell} = \left\lfloor \frac{2n}{p_i^\ell} \right\rfloor - 2\left\lfloor \frac{n}{p_i^\ell} \right\rfloor$$

Equations (9.23) and (9.24) are the keys to calculating the upper bound. Clearly (9.24) shows that $\psi_{i,\ell} = 0$ if $p_i^\ell > 2n$. The same equation also shows that $\psi_{i,\ell}$ can at most equal 1. To establish this, observe that if x and a are positive and a integer, then[4]

$$\lfloor ax \rfloor - a\lfloor x \rfloor < a$$

Setting $x = n/p_i^\ell$ and $a = 2$ and using this inequality shows that $\psi_{i,\ell} < 2$, thus establishing the claim.

To derive the upper bound, write (9.9) in disjoint ranges as

[4] A quick proof goes as follows: let $x = \lfloor x \rfloor + r$, where $0 \le r < 1$. Then the inequality follows from $a\lfloor \lfloor x \rfloor + r \rfloor = a\lfloor x \rfloor$ and $\lfloor a(\lfloor x \rfloor + r) \rfloor < a\lfloor x \rfloor + a$.

(9.25)
$$\binom{2n}{n} = \prod_{p_i \le \sqrt{2n}} p_i^{m_{i,\ell}} \prod_{\sqrt{2n} < p_i \le 2n/3} p_i^{m_{i,\ell}} \prod_{2n/3 < p_i \le n} p_i^{m_{i,\ell}} \prod_{n < p_i \le 2n} p_i^{m_{i,\ell}}$$

We now proceed to calculate a bound for each range in (9.25). There are at most $\sqrt{2n}$ primes less than or equal to $\sqrt{2n}$ and each of them is clearly less than $2n$. Thus a bound for the first range is given by

$$\prod_{p_i \le \sqrt{2n}} p_i^{m_{i,\ell}} < (2n)^{\sqrt{2n}} \tag{9.26}$$

For primes that satisfy $\sqrt{2n} < p_i \le 2n/3$ we claim that $m_i \le 1$. Since $\psi_{i,\ell}$ can be at most 1, to show that $m_i \le 1$ it suffices to show that $\psi_{i,2} = 0$ in this range. This follows immediately since the smallest square prime in this range is larger than $2n$. Thus, at most, this range consists of the multiplication of consecutive primes from $\sqrt{2n} + 1$ to $2n/3$. This corresponds to a primordial number and thus, using the inequality (9.14), we can write

$$\prod_{\sqrt{2n} < p_i \le 2n/3} p_i^{m_{i,\ell}} \le 4^{2n/3 - 1} < 4^{2n/3} \tag{9.27}$$

There are no primes in the third range: $m_i = 0$ if $2n/3 < p_i \le n$. To show this, note that this range can be rewritten as $1 \le n/p_i < 3/2$. Thus setting

$$n = p_i + r, \quad 0 \le r < p_i/2 \tag{9.28}$$

implies that $\lfloor 2n/p_i \rfloor = 2$ and $2\lfloor n/p_i \rfloor = 2$ showing that $\psi_{i,1} = 0$. To show that $\psi_{i,\ell} = 0$ for $\ell > 1$, note that (9.28) implies that

$$\frac{n}{p_i^\ell} = \frac{1}{p_i^{\ell-1}} \left(1 + \frac{r}{p_i}\right) < \frac{3}{2p_i^{\ell-1}} < 1$$

Collecting the results of (9.26) and (9.27) and substituting into (9.25) shows that

$$\binom{2n}{n} < (2n)^{\sqrt{2n}} 4^{2n/3} \prod_{n < p_i \le 2n} p_i^{m_{i,\ell}} \tag{9.29}$$

Previously a lower bound was derived for the number of coin tossing games of length $2n$ that end even, see equation (6.5) . Incorporating this into (9.29):

$$\frac{4^n}{2n} < \binom{2n}{n} < (2n)^{\sqrt{2n}} 4^{2n/3} \prod_{n<p_i\le 2n} p_i^{m_{i,\ell}}$$

uncovers the result mentioned in the beginning quote by Fine since it shows that

$$\frac{4^{n/3}}{(2n)^{\sqrt{2n}+1}} < \prod_{n<p_i\le 2n} p_i^{m_{i,\ell}} \tag{9.30}$$

Two quick computer programs now complete the result. The left-hand side of (9.30) increases with n and, solving it numerically, shows that it crosses 1 for $n = 468$. This guarantees that there is a prime between n and $2n$ for all $n \ge 468$. A trivial program then can be used to verify the result for values of n less than 468. Giving credit to Paul Erdős for the above analysis allows us to rephrase Fine's quote as:

Chebyshev found them, then Paul Erdős again,
Primes trying to hide within n and 2n

Equivalent ways of expressing this theorem are: $p_{n+1} < 2p_n$ and $\pi(z) - \pi(z/2) \ge 1$.

There are a couple direct consequences of this result. First, it is another proof that there is no largest prime. Next, it also suggests a method to write any integer as the sum of distinct primes along with the possible addition of 1. To quickly sketch a way to construct such a sum, let p_{k_1} denote the largest prime less than or equal to n. The theorem shows that $\lfloor n/2 \rfloor + 1 \le p_{k_1} \le n$. If $p_{k_1} = n$, then the construction is finished. Otherwise, we are left to write $n - p_{k_1}$ as the sum of distinct primes. Again, select the largest prime less than or equal to this value and denote it by p_{k_2}. Applying the theorem again shows that $\lfloor (n - p_{k_1})/2 \rfloor + 1 \le p_{k_2} \le n - p_{k_1}$. If $p_{k_2} = n - p_{k_1}$, then we are done since $n = p_{k_1} + p_{k_2}$. Otherwise, the construction continues sequentially until it stops at the m'th step where either $n = p_{k_1} + \cdots + p_{k_m}$ or $n = p_{k_1} + \cdots + p_{k_m} + 1$. To illustrate the output, note that the algorithm produces the following representations: $212,506,133 = 212,506,123 + 7 + 3$ and $212,506,135 = 212,506,123 + 11 + 1$.

This construction says nothing more about the representation of an integer as the sum of primes other than constructing one.

We should mention Goldbach's conjecture, named after Christian Goldbach (1690–1764). This conjecture claims that every even integer larger than 2 can be written as the sum of two primes. This conjecture has not yet been proved (computers have not found a counter example up to about 10^{18}). The above algorithm, most frequently yields two summands, although this is clearly not mandated in its specification.

You may not have noticed that the arguments leading to equation (9.30) utilized coarse inequalities that could be substantially far from their exact values. For example, inequality (9.26) is tantamount to assuming that all positive integers less than $\sqrt{2n}$ are primes with the value $2n$ and inequality (9.27) assumes that the product of primes in the range $\sqrt{2n}$ to $2n/3$ equals the product of all primes less than n. These are extremely crude approximations to the actual values, and yet, these arguments are sufficient to establish a deep result—that a prime lies between any number and its double. How is this possible?

Let me answer the question with a question. Did you ever get an F on a test? Okay, probably not if you are reading this book. But if you did, then you would know that it is almost impossible to pass the course, and this is especially true if your F was a result of getting 0 points out of 100. This is the case for this bound. The range $2n/3$ to n grows linearly as n increases and, as proved above, there are no primes in the binomial coefficient within this range. The overestimations in the previous ranges eventually are dwarfed by the lack of primes in this range. This is the genius of the argument and shows that *even when mathematics is used as a blunt tool, it can achieve a result of fine precision.*

9.3.1 The Prime Number Theorem with a Controversy

There is a glaring hole now left in this chapter. We know that there are an infinite number of primes, know that the n'th prime must grow as $\ln(n)$ (equation (9.21)) and know that a prime always exists between a number and its double. The question left hanging concerns the asymptotic distribution of the primes among the integers. Is there a function $f(n)$, so that as n grows without bound the ratio $\pi(n)/f(n)$ converges to a non-zero value? If so, then this tell us something about the regularity of the appearance of primes in the integers. As mentioned before, there is little hope of finding a more precise answer to this question since there is no formula for

the n'th prime. In the chapter, *As Simple as 2+2=1* , we discussed Fermat's little theorem (8.5) which can be used to test if an integer is a prime, and Wilson's theorem, equation (8.9), which provided necessary and sufficient conditions for an integer to be prime. These theorems, however, do not address the distribution question. Like the decimal digits of π which are completely deterministic but essentially unpredictable, primes occur among the integers seemingly popping up at random but leaving behind a madding trace of *regularity*.

The search for understanding how this series of surprises achieves a mathematical uniformity resulted in the *prime number theorem* which finally put the matter to rest by showing that

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} \to 1 \tag{9.31}$$

The following table shows the value of the ratio of (9.31) converges towards 1 for values of n from 10^1 to 10^8:

$n = 10^k$	2	4	6	8
$\pi(n)/(n/\ln(n))$	1.1513	1.1320	1.0845	1.0613

There is a long history of the discovery of this theorem, most of which utilizes advanced mathematics. In 1948, Atle Selberg (1917–2007) established an *elementary* approach that promised to be pivotal in proving the result. This was achieved by both Selberg and Erdős and resulted in a controversial interchange regarding the ownership of the result. Even though these later techniques are elementary, they lie outside the scope of this book.