1.1.5. Use repeated removal of the largest unit fraction to show

$$\frac{6}{19}=\frac{1}{4}+\frac{1}{16}+\frac{1}{304}.$$

It is worth mentioning that Fibonacci obtained the simpler decomposition $\frac{6}{19}=\frac{1}{4}+\frac{1}{19}+\frac{1}{76}$. After removal of the largest unit fraction, $\frac{1}{4}$, he was left with $\frac{5}{76}$. Rather than repeat the process of removing the largest unit fraction, he took advantage of the fact that 76 has the divisor 4 to split $\frac{5}{76}$ into $\frac{4}{76}+\frac{1}{76}=\frac{1}{19}+\frac{1}{76}$.

It is also worth mentioning that there are still some unsolved problems with Egyptian fractions. For example, it is not known whether each fraction of the form $\frac{4}{n}$ is the sum of three or fewer unit fractions. (For more information on problems with Egyptian fractions, see Guy (1994).)

1.2 Division, Divisors, and Primes

So far we have taken addition, multiplication, and fractions more or less for granted, and we shall continue to do so until a deeper investigation is called for (Section 1.9*). However, we cannot take division for granted, because it cannot always be done in the natural numbers. As you learned in primary school, 3 into 7 "won't go," so we are forced to consider the more complicated concept of *division with remainder*. The exact relation between 3 and 7 is that

$$7=2\times 3+1,$$

which we express by saying that 2 is the *quotient* when 7 is divided by 3, and 1 is the *remainder*. Only when there is no remainder, as when 3 divides 6, is true division possible in the natural numbers.

If a and b are any natural numbers, we say that *b divides a* if there is a natural number q such that

$$a=qb.$$

In this case, we also say that a is *divisible* by b, or that b is a *divisor* of a, or that a is a *multiple* of b.

If b does not divide a then $a\neq b, 2b, 3b, \ldots$, hence if we descend through the numbers $a, a-b, a-2b, a-3b, \ldots$ we eventually reach (because we cannot descend indefinitely), a natural number $r = a - qb$ smaller than b. We then have the result

$$a = qb + r, \quad \text{with } r < b.$$

The natural number q is called the quotient on division of a by b, and r is called the remainder. The fact that a can be expressed as a multiple of b plus a remainder smaller than b is often called the *division algorithm*, though we prefer to use that name for the *process* of division (namely, repeated subtraction of b until the remainder is smaller than b), and call the fact the *division property*.

The relation of division with remainder includes true division, of course, when we allow $r = 0$. In fact, some people include 0 among the natural numbers, but it is helpful to distinguish it as a new number: the first of several extensions of the number concept.[2] The fractions, for example, are an extension of the natural numbers because the natural numbers n are just the special fractions $\frac{n}{1}$. At this point you may wonder why we do not move to fractions immediately and make division easier. After all,

$$7 = \frac{7}{3} \times 3,$$

so 3 *does* divide 7 in the world of fractions. The reason is that fractions do not overcome the difficulty of division, they only conceal it. The problem comes back when we have to decide when a fraction is in lowest terms. We know $\frac{6}{3}$ is not in lowest terms, for example, because we know that 3 divides 6 *in the natural numbers*.

This example helps to clarify what is "natural" about the natural numbers. Apart from being the medium for counting, they are also the natural setting for division, divisors, and *factorization* —the process of writing numbers as products. When a natural number is written as a product, say,

$$a = n_1 n_2 \cdots n_k,$$

[2] The only disadvantage in taking 0 to be new is that there is then no name for the enlarged set "natural numbers together with 0." This is only a temporary inconvenience; we soon need further extensions of the natural numbers, which *do* have names.

the divisors n_j of a are called *factors*. The simplest numbers, from the standpoint of factorization, are the *primes* —the natural numbers p divisible only by 1 and p. They may be regarded as "atoms" because they cannot be split into smaller factors. Factors of 1 are redundant, so 1 is not classed as a prime. The first few prime numbers are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \ldots .$$

Exercises

In the proof that $\sqrt{2}$ is irrational (Section 1.1), we used the fact that m^2 is even if and only if m is even, or in other words that 2 divides m^2 if and only if 2 divides m. This is easily checked, but it is worth spelling out, because algebra is involved, and the idea of "algebraic factorization" has many other applications.

$$\begin{aligned} 2 \text{ divides } m &\Rightarrow m = 2l \text{ for some } l \\ &\Rightarrow m^2 = (2l)^2 = 2(2l^2) \\ &\Rightarrow 2 \text{ divides } m^2. \end{aligned}$$

$$\begin{aligned} 2 \text{ does not divide } m &\Rightarrow m = 2l + 1 \text{ for some } l \\ &\Rightarrow m^2 = (2l+1)^2 = 4l^2 + 4l + 1 = 2(2l^2 + 2l) + 1 \\ &\Rightarrow 2 \text{ does not divide } m^2. \end{aligned}$$

This idea has a generalization to multiples of 3.

1.2.1. Show that m^2 is a multiple of 3 only if m is a multiple of 3. Hence prove that there are no natural numbers m and n such that $m^2 = 3n^2$.

This proves the irrationality of $\sqrt{3}$; there are other ways to prove it, some of which are more general and apply to $\sqrt{5}, \sqrt{6}, \ldots$ as well. We shall see them in Section 1.6. Another important algebraic factorization is the following.

1.2.2. Check that $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$.

This enables us to find divisors of certain large numbers.

1.2.3. Deduce from Exercise 1.2.2 that, if $m = np$, then $2^m - 1$ is divisible by $2^p - 1$.

1.2.4. Conclude that $2^p - 1$ is prime only if p is prime.

Primes of the form $2^p - 1$ are known as *Mersenne primes* after Marin Mersenne (1588–1648), who first drew attention to them. About 35 Mersenne primes have been found, but it is not known whether there are infinitely many.

1.2.5. Check that $2^p - 1$ is prime when $p = 2, 3, 5, 7$, but not when $p = 11$.

1.2.6.* By similarly factorizing $x^n + 1$ when n is odd, deduce that $2^m + 1$ is prime only if m has no odd divisors, that is, only if m is a power of 2.

1.2.7. Check that $2^{2^h} + 1$ is prime for $h = 0, 1, 2, 3, 4$, but that 641 divides $2^{2^5} + 1$.

Primes of the form $2^{2^h} + 1$ are called *Fermat primes*, after Pierre de Fermat. Apart from those with $h = 0, 1, 2, 3, 4$, no other Fermat primes are known.

1.3 The Mysterious Sequence of Primes

It is relatively easy to continue the list of primes, especially with the help of a computer, but one never gets a clear picture of where it is going. Somehow, the two simplest aspects of the natural numbers—their ability to be ordered and their ability to be factored—interact in an incredibly complex way. Listing the primes in increasing order produces no apparent pattern; one cannot even be sure the list continues indefinitely. On the other hand, the *concept* of prime is surely simple, so maybe we can prove that there are infinitely many primes, without knowing their pattern.

This is in fact what Euclid did, more than 2000 years ago. You can read his simple proof in Proposition 20, Book IX of the *Elements*, which is available in English in the excellent edition of Heath (1925). Here is a slightly modernized version.

Euclid's Theorem *There are infinitely many primes.*

Proof First we need to see that any natural number n has a prime divisor.

Take any divisor d of n. If d is prime, we have found a prime divisor. If not, d has a smaller divisor $e \neq 1$. This divisor e of d is also a divisor of n, because $n = dq$ and $d = er$ for some natural numbers q and r, and therefore $n = erq$. If e is not prime, we repeat the argument, finding a smaller divisor $f \neq 1$. Because we cannot descend indefinitely, we eventually find a prime divisor of n.

Now we use a prime divisor to extend any given list of primes. Given primes $p_1, p_2, \ldots, p_k$, consider the number

$$n = p_1 p_2 \cdots p_k + 1.$$

This number is not divisible by any of the given primes $p_1, p_2, \ldots, p_k$, because they all leave remainder 1. But we have just seen that n has some prime divisor p. Thus, if $p_1, p_2, \ldots, p_k$ are any given primes, we can find a prime $p \neq p_1, p_2, \ldots, p_k$. □

This proof is one of the most admired in mathematics, and one's admiration for it only increases the more one knows about primes. Euclid, like us, did not know any pattern in the sequence of primes, so he devised a proof that did not *need* to know. If he and later mathematicians had waited for someone to find a pattern, we still would not know the first thing about primes.

Exercises

Euclid's proof is the simplest way to see that infinitely many primes *exist*, though not the most practical way to find them. Still, it is fun to produce new primes by multiplying known primes together and adding 1. Starting with the single prime $p_1 = 2$, for example, we get $n = 2 + 1 = 3$, which is a second prime p_2. Then p_1, p_2 give $n = 2 \times 3 + 1 = 7$, which is a third prime p_3; p_1, p_2, p_3 give $n = 2 \times 3 \times 7 + 1 = 43$, and so on.

1.3.1. Continue this process, and find the first stage where $n = p_1 p_2 p_3 \cdots p_k + 1$ is not itself a prime.

If you take the *least* prime divisor of n at each stage, you should be able to continue long enough to find an n in this sequence whose least prime divisor is 5. With some computer help, you might be able to continue long enough to reach an n whose least prime divisor is 11. (It is preceded by some huge prime values of n.) It is not known whether *each* prime is eventually produced by this process.

Apart from the number 2, all prime numbers are odd, and odd numbers are of two types: those of the form $4n + 1$ and those of the form $4n + 3$. It turns out to be helpful to split the odd primes in this way as well, because the two types of odd prime often behave differently. For a start, we can extend Euclid's idea to prove that there are infinitely many primes of the form $4n + 3$.

1.3.2. Show that the product of $4a + 1$ and $4b + 1$ is a number of the form $4n + 1$.

1.3.3. Deduce from Exercise 1.3.2 that any number of the form $4m + 3$ has a prime factor of the form $4n + 3$.

1.3.4. Show that $p_1, p_2, \ldots, p_k$ do not divide $2p_1p_2 \cdots p_k + 1$.

1.3.5. Show, however, that if $p_1, p_2, \ldots, p_k$ are all odd primes then *some prime of the form* $4n + 3$ divides $2p_1p_2 \cdots p_k + 1$. Deduce that there are infinitely many primes of the form $4n + 3$.

It is also true that there are infinitely many primes of the form $4n+1$, but this is harder to prove. The best possible result in this direction was proved by Peter Lejeune Dirichlet (1837). He showed that any sequence of the form $an + b$, where a and b are natural numbers with no common divisor, contains infinitely many primes. For example, Dirichlet's theorem says there are infinitely many primes of the form $6n + 1$ and of the form $6n + 5$, but there are none of the form $6n + 3$ (because 3 divides any number of the form $6n + 3$). In general, if a and b have a common divisor, there are no primes of the form $an + b$.

The form $an + b$ is called a *linear* form, so Dirichlet's theorem settles the question of how many primes there are in a given linear form. Virtually nothing is known about primes in higher-degree forms. For example, we do not know whether there are infinitely many primes of the form $n^2 + 1$.

1.4 Integers and Rationals

Everyone will agree that the natural numbers $1, 2, 3, 4, \ldots$ deserve the name "natural," but mathematicians feel they are not natural enough. $1, 2, 3, 4, \ldots$ are fine for counting, but not for arithmetic, because they do not permit unlimited subtraction. We cannot take

7 from 3, for example. To make this possible, we extend the set $\mathbb{N}$ of natural numbers to the set $\mathbb{Z}$ of *integers*[3] by adjoining 0 and the *negative integers* $-1, -2, -3, -4, \ldots$. The negative integers can be viewed as the result of subtracting $1, 2, 3, 4, \ldots$ respectively from 0, but it is simpler to regard attachment of the negative sign as the basic operation, and to *define* subtraction by $a - b = a + (-b)$.

The natural numbers now start a new life as the *positive integers*. Each positive integer a has an *additive inverse* $-a$, and the additive inverse of $-a$ is defined to be a. If we also define $-0 = 0$, then it follows that in all cases $-(-a) = a$.

The integers are a more natural home for arithmetic because they permit addition, subtraction, and multiplication without restriction. However, questions arise about the meaning of these operations on the newly introduced numbers. What is $(-1) - (-4)$ for example, or $(-1) \times (-1)$? The best way to answer these questions is by "keeping things natural." We ask ourselves how $+$, $-$, and $\times$ behave on $\mathbb{N}$ and insist that they behave the same on $\mathbb{Z}$.

First, we can summarize how $+$ and $-$ behave by the following rules, which hold for all positive integers a, b and c:

$$\begin{aligned} a + (b + c) &= (a + b) + c && \text{(associative law)} \\ a + b &= b + a && \text{(commutative law)} \\ a + (-a) &= 0 && \text{(additive inverse property)} \\ a + 0 &= a && \text{(identity property of 0)} \end{aligned}$$

These are nothing but the rules we use unconsciously when doing addition and subtraction on positive integers. We have to become conscious of them now, to see what they imply for integers in general.

It follows, for example, that we have *uniqueness of additive inverse*: $-a$ is the *only* integer b such that $a+b = 0$. This is what we normally call "solving for b," but with more awareness of the individual steps:

$$\begin{aligned} a + b = 0 &\Rightarrow (-a) + (a + b) = -a && \text{adding } -a \text{ to both sides} \\ &\Rightarrow ((-a) + a) + b = -a && \text{by the associative law} \\ &\Rightarrow (a + (-a)) + b = -a && \text{by the commutative law} \end{aligned}$$

[3] The letter $\mathbb{Z}$ is the initial of the German word "Zahlen" meaning "numbers."