For example, to prove irrationality of $\sqrt{2}$, we observe that the equation

$$m^2 = 2n^2$$

contradicts unique prime factorization. Why? The prime 2 necessarily occurs an even number of times in the prime factorization of the left-hand side, namely, twice the number of times it occurs in m. But it occurs an odd number of times on the right-hand side: the visible occurrence, plus twice the number of times it occurs in n.

Exactly the same argument applies to the equation $m^2 = 3n^2$, but with the prime 3 in place of the prime 2, and hence proves the irrationality of $\sqrt{3}$. Likewise for the equation $m^2 = 5n^2$, and the irrationality of $\sqrt{5}$. The irrationality of $\sqrt{6}$ is a little different, of course, because 6 is not a prime. But in this case it still works to consider the prime factors in the hypothetical equation $m^2 = 6n^2$.

1.6.1. Prove the irrationality of $\sqrt{6}$, that is, the impossibility of $m^2 = 6n^2$.

The irrationality of many other numbers can be proved by the same idea—showing that a hypothetical equation has some prime occurring to different exponents on the left- and right-hand sides.

1.6.2. Prove the irrationality of $\sqrt[3]{2}$, that is, the impossibility of $m^3 = 2n^3$.

1.6.3. Prove the irrationality of $\log_{10} 2$, that is, the impossibility of $2 = 10^{m/n}$.

In the *Disquisitiones Arithmeticae* (arithmetical investigations) of Carl Friedrich Gauss (1801) there is an interesting direct proof of the prime divisor property, by descent.

1.6.4. First show that a prime p cannot divide a product of smaller numbers. Suppose that p divides $a_1 b_1$, where $a_1, b_1 < p$, and deduce that p also divides $a_1 b_2$, where

$$b_2 = \text{remainder when } p \text{ is divided by } b_1,$$

which gives an infinite descent.

1.6.5. Use Exercise 1.6.4 to deduce the prime divisor property, by showing that if p divides ab, and p divides neither a nor b, then p divides an $a_1 b_1$ with $a_1, b_1 < p$.

Gauss remarked that the prime divisor property was already proved by Euclid,

however we did not wish to omit it, because many modern authors have offered up feeble arguments in place of proof or have neglected the theorem completely. *(Gauss (1801), article 14)*

1.7 Prime Factorization and Divisors

Unique prime factorization is called the *fundamental theorem of arithmetic*, and was first stated by Gauss (1801). Gauss also pointed out how unique prime factorization allows us to describe all the divisors of a given natural number.

For example, because $30 = 2 \times 3 \times 5$, the numbers $1, 2, 3, 5, 2 \times 3$, $2 \times 5, 3 \times 5$, and $2 \times 3 \times 5$ are all divisors of 30. Conversely, any natural number divisor a of 30 satisfies

$$2 \times 3 \times 5 = ab$$

for some natural number b. By uniqueness, the prime factorization of ab is also $2 \times 3 \times 5$, and a is part of it, hence a is one of the numbers listed.

In general, if

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where $p_1, p_2, \ldots, p_k$ are the distinct prime divisors of n, and $e_1, e_2, \ldots, e_k$ are their exponents, then the natural number divisors of n are numbers of the form

$$n = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k},$$

where $0 \leq d_1 \leq e_1, 0 \leq d_2 \leq e_2, \ldots, 0 \leq d_k \leq e_k$. This is because the prime factorization of a divisor is (by uniqueness) part of the prime factorization of n.

It may be that general statements about prime factorization and divisors were not made by Euclid because he lacked a notation for exponents. The same goes for the following description of greatest common divisors and least common multiples, which first appear in Gauss (1801), although they were probably known much earlier. They follow immediately from the description of divisors in terms of prime factors. The idea of finding the $\gcd(m, n)$ by collecting all

the common prime factors m and n is certainly an obvious one, sometimes taught in primary school, because it works well for small numbers.

$$\gcd(p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}, p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}) = p_1^{\min(e_1,f_1)}p_2^{\min(e_2,f_2)}\cdots p_k^{\min(e_k,f_k)}.$$

The least common multiple of m and n is abbreviated $\operatorname{lcm}(m, n)$, and we have

$$\operatorname{lcm}(p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}, p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}) = p_1^{\max(e_1,f_1)}p_2^{\max(e_2,f_2)}\cdots p_k^{\max(e_k,f_k)}.$$

Putting these two formulas together, we get the elegant formula

$$\gcd(m, n)\operatorname{lcm}(m, n) = mn,$$

which apparently was not noticed by Euclid. This formula shows, incidentally, how to compute $\operatorname{lcm}(m, n)$ *without* prime factorizations of m and n: compute $\gcd(m, n)$ by the Euclidean algorithm, then divide it into mn.

The climax of Euclid's number theory occurs at the end of Book IX of the *Elements*, where he proves a famous theorem about perfect numbers. A natural number n is called *perfect* if it is the sum of its proper divisors, that is, the natural number divisors apart from itself. The Greeks thought of the proper divisors as the "parts" of a number, hence a perfect number was the "sum of its parts." Only a few examples were then known, the smallest being $6 = 1+2+3$ and the next being $28 = 1+2+4+7+14$. Euclid found a general formula that includes these and all other known examples by finding all the divisors of numbers of the form $2^{n-1}p$, where p is prime.

Euclid's theorem on perfect numbers *If p is a prime of the form $2^n - 1$, then the number $2^{n-1}p$ is perfect.*

Proof By the preceding remarks, the proper divisors of $2^{n-1}p$ are

$$1, 2, 2^2, \ldots, 2^{n-1}, p, 2p, 2^2p, \ldots, 2^{n-2}p.$$

To find the sum of these we need to know that $1+2+2^2+\cdots+2^{n-1} = 2^n - 1$. This can be done by the formula for the sum of a geometric series or, more naively, by adding 1 to the left-hand side and "folding it up" to 2^n as follows:

$$\begin{aligned} &1 + 1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} \\ &= 2 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} \end{aligned}$$

$$\begin{aligned} &= 2^2 + 2^2 + 2^3 + \cdots + 2^{n-1} \\ &= 2^3 + 2^3 + \cdots + 2^{n-1} \\ &\vdots \\ &= 2^{n-1} + 2^{n-1} \\ &= 2^n \end{aligned}$$

But now $2^n - 1 = p$, so when we add this to the other proper divisors the sum continues to fold up:

$$\begin{aligned} &p + p + 2p + 2^2p + 2^3p + \cdots + 2^{n-2}p \\ &= 2p + 2p + 2^2p + 2^3p + \cdots + 2^{n-2}p \\ &= 2^2p + 2^2p + 2^3p + \cdots + 2^{n-2}p \\ &= 2^3p + 2^3p + \cdots + 2^{n-2}p \\ &\vdots \\ &= 2^{n-2}p + 2^{n-2}p \\ &= 2^{n-1}p, \end{aligned}$$

which is the number we started with. □

Exercises

Euclid's theorem shifts the focus of attention from perfect numbers to primes of the form $2^n - 1$. These are called *Mersenne primes* (as mentioned in connection with Exercise 1.2.4) because Mersenne recognized that they are prime only for prime n, and boldly conjectured that $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ give primes and $n = 89, 107$ do not. His conjectures were far from correct but were nevertheless important because they inspired Fermat to devise methods for finding factors of numbers of the form $2^n - 1$. Fermat's ideas turned out to be useful far outside this special problem, as we shall see in Chapter 6.

Although Euclid did not explicitly state unique prime factorization, there is evidence that the Greeks were aware of it and even of its implications for the description of divisors. Plato pointed out, in his *Laws* around 360 BC, that 5040 is a convenient number because it is divisible by all numbers from 1 to 10. He also mentioned that it has 59 divisors altogether.

The number of divisors is correct (if 5040 itself is omitted) and would be very hard to check except by using the fact that $5040 = 2^4 \times 3^2 \times 5 \times 7$.

1.7.1. Use the prime factorization of 5040 to show that it has $5 \times 3 \times 2 \times 2 = 60$ natural number divisors (including itself).

1.7.2. Show that $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ has $(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$ natural number divisors.

Before leaving the subject of perfect numbers, it is worth mentioning that Leonhard Euler proved a converse of Euclid's theorem: *every even perfect number is of the form* $2^{n-1}p$, *where* $p = 2^n - 1$ *is prime.* An elegant proof of Euler's theorem, due to Leonard Eugene Dickson (1874–1934), goes as follows.

1.7.3. For any natural number $N = 2^{n-1}q$, where q is odd, let Σ be the sum of all natural number divisors of q. Show that the sum of all proper divisors of N is $(2^n - 1)\Sigma - N$.

1.7.4. Deduce from Exercise 1.7.3 that, if N is perfect, then $2N = 2^n q = (2^n - 1)\Sigma$ and hence $\Sigma = q + q/(2^n - 1)$.

1.7.5. Deduce from Exercise 1.7.4 that $2^n - 1$ divides q, that q and $q/(2^n - 1)$ are the only divisors of q, and hence that q is a prime with $q = 2^n - 1$.

It remains an open problem whether there are any odd perfect numbers.

1.8 Induction

We began this book by claiming that arithmetic rests on the counting process and that proofs in arithmetic draw their strength from the logical essence of counting, *mathematical induction*. We gave one version of induction, called *descent*, and a few examples, and then said no more about it. So you may wonder whether induction is actually as important as we claimed. It is. Induction has been quietly intervening at crucial moments ever since we first mentioned it.

Look again over the previous sections, and you will see that descent was used to prove the following fundamental results:

- The division "algorithm" (or property) (Section 1.2).
- Existence of a prime divisor (Section 1.3).

- Termination of the Euclidean algorithm (Section 1.5).
- Unique prime factorization (Section 1.6).

It is also needed for Exercise 1.1.4 on Egyptian fractions, and Exercise 1.5.4 on $\gcd(F_{n+1}, F_n)$.

In addition to descent, which says that any descending sequence of natural numbers has a least member, we have used a form of induction that could be called *ascent*: if a sequence of natural numbers includes 1, and includes $i+1$ when it includes i, then the sequence includes all natural numbers. This principle is immediate from the definition of the natural numbers by counting.

Ascent is normally used to prove a statement about n, $S(n)$ say, by proving that the sequence of numbers n for which $S(n)$ holds includes all natural numbers. One has to prove

1. $S(n)$ is true for $n = 1$
   (the so-called *base step*) and
2. $S(n)$ is true for $n = i + 1$ when it is true for $n = i$
   (the so-called *induction step*).

Then it follows by ascent that $S(n)$ is true for all natural numbers n. This form of induction was used in two crucial results.

- Correctness of the Euclidean algorithm (Section 1.5). To do this, we proved the statement S_n: $\gcd(a_n, b_n) = \gcd(a, b)$. It is true for $n = 1$, because $(a_1, b_1) = (a, b)$; and it is true for $n = i + 1$ when it is true for $n = i$, because $\gcd(a_i, b_i) = \gcd(a_{i+1}, b_{i+1})$.
- $\gcd(a, b) = ax + by$ for some integers x and y (Section 1.5). We actually proved the statement that a_n and b_n are of this form: proving it true for $n = 1$, because $a_1 = a$ and $b_1 = b$; then proving it true for $n = i + 1$ when it is true for $n = i$, because differences of numbers of the form $ax + by$ are still of this form.

Exercises

The ascent form of induction is often used to prove equations involving a sum of n terms, such as $S(n) : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

1.8.1. For this particular equation $S(n)$, check the base step $S(1)$. Then add $(i+1)$ to both sides of $S(i)$ to prove the induction step $S(i) \Rightarrow S(i+1)$.

1.8.2. Similarly use induction to prove that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

and

$$1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2 = (1 + 2 + \cdots + n)^2.$$

On the other hand, a frequent complaint about such proofs is that one has to guess the right-hand side correctly before it is possible to get started. One would prefer a method that *discovers* the right-hand side, as well as proves it. For example, one can discover the form of $1 + 2 + \cdots + n$ by writing it a second time, in reverse:

$$1 + 2 + \cdots + (n-1) + n$$
$$n + (n-1) + \cdots + 2 + 1.$$

It is then clear, by adding the two rows, that there is a sum of $n + 1$ in each of the n columns, hence

$$2(1 + 2 + \cdots + n) = n(n+1),$$

and therefore

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

The latter kind of proof is often called *noninductive*, but what has really happened is that induction has been redeployed to prove that each column has sum $n + 1$. This is so easy that the base step and induction step need not be spelled out.

1.8.3. Use induction directly to prove the formula for the geometric series:

$$1 + r + r^2 + r^3 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r},$$

and describe a proof that leads to the discovery of this formula.

According to Hasse (1928), Zermelo found an interesting inductive proof of unique prime factorization along the following lines. Assuming there is a natural number with two different prime factorizations, there is a *least* such number n, by descent. It follows that n has two prime factorizations with no common prime factor, otherwise we could cancel to get a smaller number with two prime factorizations. Next ...