1

Preliminary Considerations

Number theory is one of the most appealing and esthetically pleasing of all branches of mathematics. Carl Friedrick Gauss (1777 – 1855), one of the greatest mathematicians, physicists, and astronomers of all time, once remarked that "mathematics is the queen of the sciences, but number theory is the queen of mathematics." Again referring to number theory, Gauss extolled "the enchanting charms of this sublime science. . . ." As the reader is almost surely aware, mathematics has a substance and beauty all its own, and it is this quality that has continually attracted the attention of people such as Gauss. The matter is well summed up by W. F. White, who wrote: "The beautiful has its place in mathematics for here are triumphs of the creative imagination, beautiful theorems, proofs and processes whose perfection of form has made them classic. He must be a 'practical' man who can see no poetry in mathematics."

Beauty, of course, is a matter of taste and it is not for anyone to determine the taste of another. Yet surprising results, economically stated and subtly proved, have been a source of pleasure and satisfaction to the human mind throughout the ages. Our hope is that readers will derive similar enjoyment from the following pages.

Not all of the succeeding theorems can appropriately be classed as beautiful, nor are all the proofs neat and elegant, but the theory of numbers has more than its fair share of such results. It *is* a fascinating study and our hope is that as readers of this book penetrate more deeply into it, they too will be pleasantly surprised and pleased at the statement of a theorem or the turn of a proof. Even more, we hope that they may know the special pleasure of discovering and proving results for themselves.

But there are other reasons for studying number theory quite apart from intel-

lectual satisfaction. In our modern computer-oriented society it is widely recognized that discrete mathematics, of which number theory is an integral part, is increasingly the applicable mathematics of the day. Important notions in computer science which depend in significant ways on number-theoretic results include large integer arithmetic; binary, octal, and hexadecimal representations of integers; factoring integers; generation of pseudo-random numbers; recursion; computational complexity; cryptography, including public-key encryption systems, and much more. Indeed, the references to number-theoretic ideas in Donald Knuth's definitive three-volume work, *The Art of Computer Programming,* are legion, and it is safe to say that no one ignorant of number theory can be a serious student of computer science.

Finally, we note that the art of solving problems is of paramount importance to students of both mathematics and computer science. How *does* one reasonably proceed to analyze an unusual situation never encountered before, to pose it as a well-defined problem, and then to solve it? The answer to this question is difficult indeed, since there are many approaches and diverse heuristics, and it is rarely clear which will be effective at any given time. Perhaps the best way to become a capable problem solver is to solve many nonroutine problems, and a course in number theory provides ample opportunity to practice this skill. Solving problems and proving theorems can certainly be frustrating, but as one's skill improves and insight and ingenuity increase, the activity can also be the source of great satisfaction. Thus, a final hope for our readers is that they will come increasingly to enjoy this special pleasure as they grapple with the interesting problems with which the theory of numbers is replete.

1.1 SUMMATION AND MULTIPLICATION NOTATION

From time to time as our development proceeds we shall have occasion to use special notation to simplify the writing of sums and products. The notation is standard but it may not be amiss to begin our study by reviewing its essential features.

Summation Notation

For $r \leq s$, we use $\sum_{i=r}^{s} a_i$ to represent the sum

$$a_r + a_{r+1} + \cdots + a_s;$$

s and r are called the *upper* and the *lower limits* of summation, and i is called the *index* of summation. For example,

$$\sum_{i=0}^{4} a_i = a_0 + a_1 + a_2 + a_3 + a_4$$

and analogously,

$$\sum_{j=1}^{3} j^2 = 1^2 + 2^2 + 3^2.$$

The idea is to replace the index of summation in the expression being summed by consecutive integers, starting with the lower limit of summation and stopping with the upper limit, and then to add the resulting expressions.

With this in mind, it is not difficult to derive a number of interesting results of a general nature. In each of the following cases, we shall use 1 and n for the lower and upper limits, but it is clear that any integers r and s could be used just as well. First we consider

$$\sum_{i=1}^{n} a_i b_i = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n. \tag{1.1}$$

If we set $b_i = k$ for $i = 1, 2, \ldots, n$ in (1.1), we obtain

$$\sum_{i=1}^{n} k a_i = k \cdot \sum_{i=1}^{n} a_i. \tag{1.2}$$

This simply notes that a constant factor (independent of the index of summation) can be factored out of the entire summation. Moreover, if $a_i = 1$ as well as $b_i = k$ for each $i = 1, 2, \ldots, n$ in (1.1), we obtain

$$\sum_{i=1}^{n} k = nk. \tag{1.3}$$

Thus, the summation of a constant (i.e., a quantity independent of the index of summation) is equal to the value of the constant times the *number of values the index assumes.* For example,

$$\sum_{i=5}^{17} 3 = 3 \cdot 13 = 39 \quad \text{and} \quad \sum_{j=0}^{5} 7b = 42b.$$

It is sometimes necessary to use multiple summation. If $k = b_j$ in (1.2), we have

$$\sum_{i=1}^{n} a_i b_j = b_j \cdot \sum_{i=1}^{n} a_i, \tag{1.4}$$

and if we now sum both sides as j runs from 1 to m, we obtain

$$\sum_{j=1}^{m} \sum_{i=1}^{n} a_i b_j = \sum_{j=1}^{m} \left(b_j \cdot \sum_{i=1}^{n} a_i \right). \tag{1.5}$$

Since with regard to the summation on j, the entire sum $\Sigma_{i=1}^{n} a_i$ is constant, it follows from (1.2) that

$$\sum_{j=1}^{m} \left(b_j \cdot \sum_{i=1}^{n} a_i \right) = \left(\sum_{j=1}^{m} b_j \right) \cdot \left(\sum_{i=1}^{n} a_i \right) = \left(\sum_{i=1}^{n} a_i \right) \cdot \left(\sum_{j=1}^{m} b_j \right). \tag{1.6}$$

Combining this with (1.5), we obtain the very important result

$$\sum_{j=1}^{m}\sum_{i=1}^{n} a_i b_j = \sum_{i=1}^{n} a_i \cdot \sum_{j=1}^{m} b_j. \tag{1.7}$$

Another important and useful summation formula is

$$\begin{aligned}\sum_{i=1}^{n}(a_i + b_i) &= (a_1 + b_1) + (a_2 + b_2) + \cdots + (a_n + b_n)\\ &= (a_1 + \cdots + a_n) + (b_1 + \cdots + b_n)\\ &= \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i.\end{aligned} \tag{1.8}$$

Multiplication Notation

For $r \le s$, we use

$$\prod_{i=r}^{s} a_i$$

to represent the product of the numbers $a_r, a_{r+1}, \ldots, a_s$. For example,

$$\prod_{i=1}^{5} a_i = a_1 a_2 a_3 a_4 a_5$$

and

$$n! = \prod_{i=1}^{n} i.$$

As in the case of sums, it is possible to derive a number of useful formulas for special types of products. As before, we use n and 1 for upper and lower limits in the following products, but other limits can be used just as well. The derivations in each case are analogous to the ones for the corresponding sums. In the first place,

$$\begin{aligned}\prod_{i=1}^{n} a_i b_i &= (a_1 b_1)(a_2 b_2) \cdots (a_n b_n)\\ &= (a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_n)\\ &= \prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{n} b_i.\end{aligned} \tag{1.9}$$

If we set $b_i = k$ for $i = 1, 2, \ldots, n$ in (1.9), we obtain

$$\prod_{i=1}^{n} k a_i = k^n \cdot \prod_{i=1}^{n} a_i. \tag{1.10}$$

Moreover, if we set $a_i = 1$ for $i = 1, 2, \ldots, n$ in (1.10), we obtain

$$\prod_{i=1}^{n} k = k^n, \tag{1.11}$$

which says that the product of a constant is equal to the constant raised to a power equal to the number of values that the index of multiplication assumes.

As examples of the preceding results, we note that

$$\begin{aligned}\prod_{i=1}^{n} i(i+1) &= \prod_{i=1}^{n} i \cdot \prod_{i=1}^{n} (i+1) \\ &= n!(n+1)!,\end{aligned}$$

that

$$\prod_{i=1}^{n} 2i = 2^n \cdot n!,$$

and that

$$\prod_{i=1}^{n} 2 = 2^n.$$

One final result concerning products is suggested by (1.9). If $a_i = b_i$, then (1.9) becomes

$$\prod_{i=1}^{n} a_i^2 = \prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n} a_i\right)^2.$$

This suggests that, in general,

$$\prod_{i=1}^{n} a_i^k = \left(\prod_{i=1}^{n} a_i\right)^k. \tag{1.12}$$

The easy proof of this is left to the reader as Exercise 10 of Section 1.4.

Finally, we observe that it is often useful to make a change of indices in either summations or products much as one changes variables in algebra or in integration problems in calculus. For example, if we set $j + 1 = i$, we have that

$$\sum_{i=1}^{r} i^2 = \sum_{j=0}^{r-1} (j+1)^2; \tag{1.13}$$

in both cases we are referring to the sum

$$1^2 + 2^2 + 3^2 + \cdots + r^2. \tag{1.14}$$

Note that to transform the first sum in (1.13) into the second we replace the i in i^2 by $j + 1$ to obtain $(j + 1)^2$ and adjust the limits by noting that when $i = 1$, $j = 0$ and when $i = r$, $j = r - 1$. As an additional example, suppose that we set $i = r - k$. Then

when $i = 1, k = r - 1$ and when $i = r, k = 0$. Thus, substituting $r - k$ for i on the left side of (1.13), we obtain

$$\sum_{i=1}^{r} i^2 = \sum_{k=r-1}^{0} (r-k)^2 = \sum_{k=0}^{r-1} (r-k)^2 \tag{1.15}$$

since a sum is the same if we sum either forward or backward. In this case the substitution seems to make the sum more involved, but the idea is important and the device of substitution of indices is often useful in manipulating with sums and products.

EXERCISES 1.1

1. Write out the following sums.

   (a) $\sum_{i=1}^{5} (2i-1)$ **(b)** $\sum_{i=0}^{6} \sin ix$ **(c)** $\sum_{i=0}^{0} f(i)$

   (d) $\sum_{j=1}^{n} \frac{2}{j(j+1)}$ **(e)** $\sum_{k=5}^{10} 3$ **(f)** $\sum_{i=3}^{3} \frac{3}{i}$

2. Use the change of indices $i = j + 1$ to rewrite the summations in Exercise 1(a)–(d).
3. Write the following in summation notation.
   (a) $2 + 4 + 6 + 8 + 10$
   (b) $1 + 8 + 27 + 64 + 125$
   (c) $28 + 31 + 34 + 37 + 40 + 43$
   (d) $n + (n+2) + (n+4) + \cdots + (n+2m)$
4. Evaluate $\Sigma_{i=1}^{n} (a_i - a_{i-1})$ given that $a_0 = 0$.
5. Use the result of Exercise 4 to prove that $\Sigma_{i=1}^{n} i = n(n+1)/2$.
   Hint: Let $a_i = i(i+1)/2$.
6. Use the result of Exercise 4 to prove that

$$\sum_{i=1}^{n} i(i+1) = n(n+1)(n+2)/3.$$

7. With only slight modifications, the equations in Exercises 5 and 6 could have been written in the form

$$\sum_{i=1}^{n} \binom{i}{1} = \binom{n+1}{2} \quad \text{and} \quad \sum_{i=1}^{n} \binom{i+1}{2} = \binom{n+2}{3},$$

where

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

is the usual binomial coefficient notation. What more general result do these suggest?

8. Use simple algebraic manipulation to show that

$$\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$$

for all integers n and k with $0 \le k \le n$.

9. Prove that

$$\sum_{i=1}^{n}\binom{i+k-1}{k}=\binom{n+k}{k+1},$$

where n and k are integers with $n \ge 1$ and $k \ge 0$. Note that it is customary to set $\binom{a}{b}=0$ for integers a and b if $0 \le a < b$.

10. Evaluate $\sum_{i=0}^{n}\binom{i}{k}$ where n and k are nonnegative integers.

Hint: Note that $\binom{i}{k}=0$ for $0 \le i < k$ and use the substitution $i = j+k-1$, where j is the new index of summation.

11. Use the results of Exercises 5 and 6 to derive a formula for

$$\sum_{i=1}^{n} i^2.$$

12. Write out the following products:

(a) $\prod_{j=1}^{4}(2j-1)$ **(b)** $\prod_{j=0}^{5}\frac{j}{j+1}$

(c) $\prod_{i=p}^{p+n} i$ **(d)** $\prod_{i=2}^{2} e^i$

13. Use the change of indices $i = j-1$ to rewrite all the products in Exercise 12.

14. Write the following in product notation.

(a) $2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12$

(b) $(-1)^n \cdot n!$

(c) $\left(1-\frac{1}{4}\right)\left(1-\frac{1}{9}\right)\left(1-\frac{1}{16}\right)\cdots\left(1-\frac{1}{n^2}\right)$

15. Evaluate $\prod_{i=1}^{n} a^i$ and $\prod_{i=1}^{n} a^{i(i+1)}$.

16. Evaluate $\prod_{i=1}^{n}\frac{a_i}{a_{i-1}}$ given that $a_0 = 1$.

17. Use the result of Exercise 16 to prove the following:

(a) $\prod_{i=1}^{n}\frac{i}{i+1}=\frac{1}{n+1}$ **(b)** $\prod_{i=1}^{n}\left[1-\frac{1}{(i+1)^2}\right]=\frac{n+2}{2(n+1)}$

Computer Exercise

18. **(a)** Write a computer program to compute and print

$$S_n = \sum_{i=1}^{n} i^3 \qquad \text{for } 1 \le n \le 20.$$

(b) On the basis of the printout, endeavor to guess a general formula for S_n.
(c) Use Exercise 5 to prove that your guess in part (b) is correct.

1.2 INDUCTIVE REASONING AND THE FIBONACCI SEQUENCE

It should not surprise any reader to assert that the learning of mathematics involves acquiring an array of manipulative skills, learning a substantial battery of theorems, and learning how to prove theorems. Appropriately, these matters are stressed in mathematics classes from kindergarten through college.

On the other hand, it is not the case that axiomatics and proof are the sum total of mathematics or even its most important part. Contrary to popular belief, mathematics is not a body of material discovered by the Greeks some 2000 years ago and long since embalmed in textbooks. It is a vital, vibrant, living subject, currently being created at a rate unprecedented in all of history. Unless students of mathematics understand something of this process of creation, it can be rather effectively argued that they really understand very little of what mathematics is all about. It is well and good to know a particular theorem, say the Pythagorean theorem; one ought to know something about the proof of the theorem and ought also to be able to use it to solve a variety of theoretical and practical problems. But where did the Pythagorean theorem come from, and how does one go about devising other theorems that might be useful in solving other theoretical and practical problems of importance? It is precisely at this point that *guessing* or *inductive reasoning* enters into mathematics. No one told Pythagoras that the Pythagorean theorem was true, and he did not simply look in a crystal ball and say, "Aha! I see a theorem!"; and again, "Aha! I see the proof!" No, Pythagoras or one of his contemporaries had to guess that the Pythagorean theorem was true, and then had to guess how to arrive at a proof. Without the guess there would have been no theorem, and without more guessing there would have been no proof. This has always been the case and this will always be the case. Without guessing there would be no theorems; without guessing there would be no mathematics! Thus, as indicated in the introduction, an important aim of this book will be to develop mastery of the art of intelligent guessing and of problem solving. For intelligent guessing and problem solving are the spirit of inquiry, and inquiry is the spirit of mathematics.

Of course, the latter aim should be pursued in other courses as well. But it is particularly suitable for a course in number theory. The great Euler (1707–1783) once wrote:

> As I shall show here with very good reasons, the properties of the numbers known today have been mostly discovered by observation, and discovered long before their truth has been confirmed by rigid demonstrations. There are even many properties of the numbers with which we are well acquainted but which we are not yet able to prove; only observations have led us to their knowledge. Hence we see that in the theory of numbers, which is still very imperfect, we can place our highest hopes in observations; they will lead us continually to new properties which we shall endeavor to prove afterwards.

Now how does one go about making an intelligent guess in a given situation? How does one go about solving a difficult problem in an unusual setting, and how does one go about guessing the key to a proof even if a result has been guessed or stated? No doubt many things can be said by way of answer,† but perhaps one of the best things that can be done is to consider a series of specific examples. Because they have so many elegant properties that can easily be discovered by the simple expedient of scrutinizing examples, we begin by considering the famous Fibonacci sequence, named after Leonardo of Pisa (c. 1170–1250), who was also called Fibonacci, and the closely related sequence of Lucas named after the French mathematician E. Lucas (1842–1891). The two sequences are defined, respectively, by the equations

$$\begin{aligned} &F_1 = F_2 = 1, \qquad F_{n+2} = F_{n+1} + F_n, \\ &L_1 = 1, \qquad L_2 = 3, \qquad L_{n+2} = L_{n+1} + L_n \end{aligned} \tag{1.16}$$

for all $n \geq 1$ and their first few terms (called Fibonacci and Lucas numbers, respectively) are given in the accompanying table.

THE FIRST 25 FIBONACCI AND LUCAS NUMBERS

n	F_n	L_n	n	F_n	L_n
1	1	1	14	377	843
2	1	3	15	610	1,364
3	2	4	16	987	2,207
4	3	7	17	1,597	3,571
5	5	11	18	2,584	5,778
6	8	18	19	4,181	9,349
7	13	29	20	6,765	15,127
8	21	47	21	10,946	24,476
9	34	76	22	17,711	39,603
10	55	123	23	28,657	64,079
11	89	199	24	46,368	103,682
12	144	322	25	75,025	167,761
13	233	521			

† The reader should see in particular the excellent book *Mathematics and Plausible Reasoning*, Vol. 1, by G. Polya (Princeton, N.J.: Princeton University Press, 1954), or the more recent two-volume work, *Mathematical Discovery*, by the same author (New York: John Wiley & Sons, Inc., 1981).

With the data at hand, suffice it to say that one considers examples, tries to identify regular and consistent patterns, and finally formulates general statements which one then endeavors to prove. For example, if we consider the table for a moment, we may note that

$$1 + 2 = 3,$$
$$1 + 3 = 4,$$
$$2 + 5 = 7,$$
$$3 + 8 = 11,$$
$$5 + 13 = 18,$$

and be led to guess that

$$F_n + F_{n+2} = L_{n+1} \tag{1.17}$$

for all $n \geq 1$. This is not hard to prove, but in this section we devote our attention to guessing, and the proofs will be postponed until Section 1.3 and even later for the more difficult results. As another example, we note that

$$1 + 1 = 2,$$
$$1 + 4 = 5,$$
$$4 + 9 = 13,$$
$$9 + 25 = 34,$$
$$25 + 64 = 89,$$

and a moment's reflection suggests that

$$F_n^2 + F_{n+1}^2 = F_{2n+1}, \qquad n \geq 1. \tag{1.18}$$

In the exercises that follow, the reader will find many examples of this sort. Sometimes the guess is easy to make; sometimes it is relatively difficult. In any case, all are interesting and somewhat surprising, and the more difficult ones will provide the greater opportunity for readers to strengthen their mathematical muscles and better prepare themselves for the rigors yet to come in this and other courses.

EXERCISES 1.2

1. Guess a formula suggested by each of the following sets of equations.

(a)
$$1 + 4 = 5$$
$$3 + 7 = 10$$
$$4 + 11 = 15$$
$$7 + 18 = 25$$
$$11 + 29 = 40$$

(b)
$$1 + 1 = 2$$
$$1 + 3 = 4$$
$$2 + 4 = 6$$
$$3 + 7 = 10$$
$$5 + 11 = 16$$

(c)
$$1-1=0$$
$$4-1=3$$
$$9-4=5$$
$$25-9=16$$
$$64-25=39$$

(d)
$$1\cdot 1=1$$
$$1\cdot 3=3$$
$$2\cdot 4=8$$
$$3\cdot 7=21$$
$$5\cdot 11=55$$

2. Exercise 1(c) suggests that it might be useful to define $F_0 = 0$.
   (a) Is this consistent with the pattern established by the defining equations (1.16)?
   (b) Define F_{-1}, F_{-2}, F_{-3}, F_{-4}, and F_{-5} in a way that is also consistent with (1.16).
   (c) Can you guess a relation between F_n and F_{-n}?

3. Exercise 1(c) also suggests that it is sometimes interesting to look at the differences of squares. What formulas are suggested by the following sets of equations? Note that more than one correct answer may be possible.

(a)
$$4-1=3$$
$$9-1=8$$
$$25-4=21$$
$$64-9=55$$

(b)
$$9-1=8$$
$$25-1=24$$
$$64-4=60$$
$$169-9=160$$

(c)
$$25-1=24$$
$$64-1=63$$
$$169-4=165$$
$$441-9=432$$
$$1156-25=1131$$

(d)
$$9-1=8$$
$$16-9=7$$
$$49-16=33$$
$$121-49=72$$
$$324-121=203$$

(e)
$$16-1=15$$
$$49-9=40$$
$$121-16=105$$
$$324-49=275$$

4. Exercise 3(d) suggests that it might be useful to define $L_0 = 2$.
   (a) Is this consistent with equations (1.16)?
   (b) How would you define L_{-1}, L_{-2}, and L_{-3}?
   (c) Can you guess a relationship between L_{-n} and L_n?

5. What formulas are suggested by the following arrays? Use summation notation in expressing your answer.

(a)
$$1=1$$
$$1+1=2$$
$$1+1+2=4$$
$$1+1+2+3=7$$

(b)
$$1=1$$
$$1+2=3$$
$$1+2+5=8$$
$$1+2+5+13=21$$

(c)
$$1=1$$
$$1+3=4$$
$$1+3+8=12$$
$$1+3+8+21=33$$

(d)
$$1=1$$
$$1-2=-1$$
$$1-2+5=4$$
$$1-2+5-13=-9$$

6. Guess formulas like those in Exercise 5 for the following summations.

(a) $\sum_{i=1}^{n} (-1)^{i-1} F_{2i}$ (b) $\sum_{i=1}^{n} L_i$

(c) $\sum_{i=1}^{n} F_{2i-1}$ (d) $\sum_{i=1}^{n} F_{2i}$

(e) $\sum_{i=1}^{n} (-1)^{i-1} F_{2i-1}$ (f) $\sum_{i=1}^{n} (-1)^{i-1} L_{2i}$

(g) $\sum_{i=1}^{n} (-1)^{i-1} F_i$ (h) $\sum_{i=1}^{n} (-1)^{i-1} L_i$

7. Guess formulas for the following summations.

(a) $\sum_{i=1}^{n} F_{3i-2}$ (b) $\sum_{i=1}^{n} F_{3i-1}$

(c) $\sum_{i=1}^{n} F_{3i}$ (d) $\sum_{i=1}^{n} (-1)^{i-1} F_{3i-2}$

(e) $\sum_{i=1}^{n} (-1)^{i-1} F_{3i-1}$ (f) $\sum_{i=1}^{n} (-1)^{i-1} F_{3i}$

8. Guess formulas for the following summations.

(a) $\sum_{i=1}^{n} F_i^2$ (b) $\sum_{i=1}^{n} F_i F_{i+1}$

(c) $\sum_{i=1}^{n} F_i F_{i+2}$ (d) $\sum_{i=1}^{n} F_i F_{i+3}$

(e) $\sum_{i=1}^{n} F_i F_{i+d}$, where d is any nonnegative integer

9. Let $f_1 = a$, $f_2 = b$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$. Find f_3, f_4, and f_5 and guess a general formula for f_n.

10. Consider the following arrays and guess the formula they suggest.

$$\begin{aligned} 8^2 - 5 \cdot 13 &= -1 & \qquad 13^2 - 8 \cdot 21 &= 1 \\ 8^2 - 3 \cdot 21 &= 1 & \qquad 13^2 - 5 \cdot 34 &= -1 \\ 8^2 - 2 \cdot 34 &= -4 & \qquad 13^2 - 3 \cdot 55 &= 4 \\ 8^2 - 1 \cdot 55 &= 9 & \qquad 13^2 - 2 \cdot 89 &= -9 \\ 8^2 - 1 \cdot 89 &= -25 & \qquad 13^2 - 1 \cdot 144 &= 25 \end{aligned}$$

11. Let n, k, and r be positive integers with $k < n$. See if you can guess how to complete the following equation:

$$F_n F_{n+r} - F_{n-k} F_{n+r+k} = \underline{\qquad\qquad}.$$

12. One of the most important phrases in a mathematician's vocabulary is "what if." For example, what if one replaces all the Fibonacci numbers in the formulas

in Exercises 6, 7, and 8 by Lucas numbers? Will valid formulas result, or at least similar formulas? Try some.

13. Note that Exercise 8(e) is a generalization of 8(a)–(d) and that Exercise 11 is a generalization of Exercise 10. Could you find generalizations of other results in this section?
14. What Fibonacci numbers are evenly divisible by (a) 3, (b) 4, (c) 5, and (d) 6? Can you make a general guess?

Computer Exercises

15. Write a computer program to generate the first 100 Fibonacci numbers; the first 100 Lucas numbers.
16. Write a computer program to find all positive integer solutions (x, y) to $x^2 - 5y^2 = 4$. Can you make a general guess?
17. Write a computer program to find all positive integer solutions to $x^2 - 5y^2 = -4$. Can you make a general guess?

1.3 THE POSTULATES OF MATHEMATICAL INDUCTION AND WELL-ORDERING

Like the rest of mathematics, the set of positive integers is a postulational system. For example, one might take the integers themselves and the operations of addition and multiplication as undefined terms and statements such as the closure law for addition, which states that the sum of any two positive integers is a positive integer, as postulates. In general, these postulates are well understood and we will not consider them here. However, we do consider one postulate that is often found confusing. The postulate in question is the *principle of mathematical induction* or its equivalent, the *well-ordering principle.* We list three alternative statements and then suggest some further variations on the general theme.

I_1. *First form of the principle of mathematical induction.* Any set of positive integers that contains the integer 1, and that contains $k + 1$ whenever it contains the positive integer k, contains all positive integers.

I_2. *Second form of the principle of mathematical induction.* Any set of positive integers that contains the integer 1, and that contains $k + 1$ whenever it contains the positive integers 1 to k inclusive, contains all positive integers.

I_3. *The well-ordering principle.* Every nonempty set of positive integers contains a least element.

The reader should bear in mind that one or another of these principles must be taken as a postulate for the system of positive integers, and we shall show that the other two can then be proved as theorems. Thus, all three hold for the set of positive

integers. What do they tell us about the system of positive integers, and how can we make use of this information?

In effect, the first form of the principle of mathematical induction, I_1, simply says that the set of all positive integers can be generated by starting with 1, and adding 1 successively ad infinitum; that is, that the infinite sequence $1, 1 + 1 = 2, 2 + 1 = 3, 3 + 1 = 4, \ldots$ contains all positive integers. The reader should note that this is said in I_1 by giving two conditions which guarantee that a set of positive integers is the set of all positive integers. The first condition specifies that the integer 1 be in the set, while the second condition states that if any particular integer is in the set, then so is its successor. But if 1 is in the set and the successor of 1 is in the set, then 2 is in the set. And if 2 is in the set, then so is 3, and so on. Thus we have an infinite sequence that contains all the positive integers.

The second form of the principle of mathematical induction, I_2, says the same thing about the system of positive integers as does I_1, but in a slightly different way. Again, there are two conditions which guarantee that a set of positive integers is the set of all positive integers. This time, however, the second condition states that if all positive integers from 1 up to and including any given integer are in the set, then the successor to that integer is also in the set. The first condition, as before, specifies that 1 be in the set. Taken together, these conditions imply that 2 is in the set. But then 1 and 2 are in the set and so 3 is in the set, and so on, as before.

Finally, the well-ordering principle, I_3, guarantees that if one has a set actually containing positive integers and only positive integers, then the set contains a smallest member. At first thought, it might seem that this would be true of any nonempty set of numbers, but this is not the case. For example, the set of positive real numbers fails to have a least element and so does the set of negative integers.

As noted earlier, it is not difficult to show that in the presence of the other postulates for the positive integers, these three principles are equivalent. First it may be worthwhile to see how they can be used in the formulation of proofs.

1.4 MATHEMATICAL INDUCTION

We illustrate the use of I_1 by assuming it as a postulate and using it to prove the following theorem.

THEOREM 1.1. For every positive integer n, $\sum_{i=1}^{n} i = n(n+1)/2$.

Proof. Let C be the set of all positive integral values of n for which the formula of the theorem is true. Clearly, 1 is in C since for $n = 1$, the assertion is simply that $1 = (1 + 1)/2$. Now suppose that k is in C, where k is a fixed but unspecified positive integer; that is, suppose that $1 + 2 + \cdots + k = k(k+1)/2$. Then

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

Thus, if the formula is true for $n=k$, it is also true for $n=k+1$; so $k+1$ is in C if k is in C. Finally, since C satisfies both conditions of I_1, it must contain all positive integers. Hence, the given formula is true for all positive integers n, as claimed.

In practice, one does not usually frame a proof based on I_1 (such proofs are called proofs by mathematical induction, as are those based on I_2) in terms of a set C, as in the preceding argument. It was done here only to make its dependence on I_1 completely clear. The essential features of the proof are that one must show that (step 1) the result in question holds for $n=1$ and that (step 2) it holds for $n=k+1$ whenever it holds for $n=k$, and this is all that is usually written down. Thus, for example, the preceding proof would more often be written in the following more abbreviated form.

Proof. For $n=1$, the assertion of the theorem is clearly true. Now, assume that $\Sigma_{i=1}^{k} i = k(k+1)/2$, where k is any fixed but unspecified positive integer. Then

$$\sum_{i=1}^{k+1} i=\frac{k(k+1)}{2}+(k+1)=\frac{(k+1)(k+2)}{2}.$$

Thus, since the assertion is true for $n=k+1$ if it is true for $n=k$, it is true for every positive integer n by the principle of mathematical induction.

The reader should note that *both* steps in a proof based on I_1 must be carried out before the desired conclusion can be drawn. For example, step 1 can be completed for the false formula

$$\sum_{i=1}^{n} i=\frac{n(n+1)}{2}+(n-1),$$

whereas step 2 cannot, and step 2 can be completed for the false formula

$$\sum_{i=1}^{n} i=\frac{n(n+1)}{2}+5,$$

whereas step 1 cannot.

One must also be sure that the argument made in step 2 of the proof does not depend on any particular value for k. The argument must hold for *any* fixed but unspecified positive integer k or else the "and so on" of the preceding paragraph will

break down. For example, let us "prove" that all positive integers are equal. The statement "any n positive integers are equal" is certainly true in case $n = 1$. Let us now assume it to be true for $n = k$ and prove that it must, therefore, be true for $n = k + 1$. Let

$$\overbrace{a_1, \underbrace{a_2, a_3, \ldots, a_k}, a_{k+1}}$$

be any $k + 1$ positive integers. By assumption, the first k must be equal and also the last k must be equal, as indicated above by the braces. But then, because of the overlap, it is apparent that all the numbers must be equal. Thus, the assertion is true for $n = k + 1$ if it is true for $n = k$ and the "proof" is complete. The difficulty, of course, is that there is no overlap between the first k numbers and the last k numbers in the foregoing diagram in case $k = 1$. Thus, step 2 of the argument is valid only for $k \geq 2$ and cannot be used to conclude that the result claimed is true for $n = 2$ if it is true for $n = 1$. However, it might be noted that if a separate argument could be given to prove the validity of the assertion for $n = 2$, then step 2 could be used to extend the result upward from 2.

The preceding remark suggests that the method of proof based on I_1 can be modified to prove that a result is true for all integers greater than or equal to any fixed integer, so that the induction does not have to begin with $n = 1$. For example, if one wanted to prove that a result were true for all integers greater than or equal to 29, it would suffice to prove it for $n = 29$ and for $n = k + 1$ on the basis of the assumption of its truth for $n = k$, where k is any fixed but unspecified integer greater than or equal to 29.

A proof based on I_2 is exactly like one based on I_1, with one exception. In step 2 of the proof, one assumes the truth of the assertion for all values of n from 1 to k inclusive and, on the basis of this assumption, must then prove its truth for $n = k + 1$. The point is that the truth of the $(k + 1)$st case often does not follow directly from the truth of the kth case, but does follow from the truth of the assertion for some or all of the positive integers preceding $k + 1$. Even in such cases, it is possible (by a devious trick) to use I_1, but a proof based on I_2 would be much more natural.

Before giving an example of such a situation, we note that the same general remarks apply to proofs based on I_2 as to those based on I_1. By this we mean that both steps of the proof must be carried out before the conclusion can be drawn, and that the argument in the second step of the proof must not depend on any particular value of k. Also, as indicated in the discussion of I_1, the induction can begin with 2, or 29, or any other integer in place of 1. For example, if 2 were used in place of 1, this would amount to saying that I_2 could be modified to read as follows: Any set of integers not less than 2 which contains 2 and contains $k + 1$ whenever it contains the integers 2 to k inclusive contains all integers not less than 2. We mention this case in particular since one of the simplest examples of a result that lends itself in a natural way to proof based on I_2 is a theorem true for all integers not less than 2. Before discussing this theorem, it will be necessary to introduce some terminology.

DEFINITION 1.1. If a and b are integers with $a \neq 0$ and there exists an integer c such that $b = ac$, then we say that a *divides* b and write $a|b$. We also call a a *divisor* of b and b a *multiple* of a. If $1 \leq a < b$ and $a|b$, then a is called a *proper divisor* of b. If a does not divide b, we write $a \nmid b$.

DEFINITION 1.2. If p is an integer greater than 1 whose only positive divisors are 1 and p itself, then p is called a *prime*. If p exceeds 1 and is not a prime, then it is called *composite*.

As examples of these definitions, we note that 1, 2, 3, and 6 are all divisors of 6, and all but 6 are proper divisors. Also, 2 and 3 are primes and 6 is composite. The integer 1 is neither prime nor composite.

We now illustrate the method of proof based on I_2. Note that we assume I_2, as modified above, as a postulate and prove the theorem in the simplified form without introducing a set C as in the first proof of Theorem 1.1

THEOREM 1.2. Every integer $n \geq 2$ is either a prime or can be represented as a product of primes.

Proof. The assertion is trivially true for $n = 2$ since 2 is a prime. Assume that it is true for all integers n with $2 \leq n \leq k$, where k is any fixed but unspecified integer not less than 2. We must show that, on the basis of this assumption, the assertion of the theorem is also true for $n = k + 1$. If $k + 1$ is a prime, there is nothing to show. If $k + 1$ is composite, there exist integers r and s with $2 \leq r \leq k$ and $2 \leq s \leq k$ such that $k + 1 = rs$. Since r and s both lie between 2 and k, we have, by assumption, that both are either primes or products of primes. Therefore, in this case, $k + 1$ must be a product of at least two primes. In any case, $k + 1$ is a prime or a product of primes and the assertion of the theorem is true for $n = k + 1$ if it is true for all integers n with $2 \leq n \leq k$. Thus, by I_2 as modified, it is true for all $n \leq 2$.

The reader should observe that the second part of the preceding proof depended on knowing that the assertion of the theorem held for both r and s. Since we knew only that r and s lay somewhere between 2 and k it was necessary to assume that the assertion of the theorem held for all integers in this range. Using I_1 in a natural way and making the induction assumption only for $n = k$ would not have sufficed.

It turns out that a wide variety of other variations on the theme of mathematical induction are possible. If we consider the definition of the Fibonacci numbers in Section 1.2, for example, F_3 can be computed since we know its *two* predecessors F_1 and F_2. Then F_4 can be computed from F_2 and F_3, and so on. This suggests that the logic of mathematical induction is essentially the same as the logic of constructing a DO LOOP in computing. It also suggests an alternative principle of mathematical induction.

I_4. *Third form of the principle of mathematical induction.* Any set of positive integers that contains 1 and 2, and that contains $k + 2$ whenever it contains the positive integers k and $k + 1$, contains all positive integers.

In making a proof based on I_4 one would begin by proving the desired result true for $n = 1$ and $n = 2$. One would then assume that the result is true for $n = k$ and $n = k + 1$, where k is any fixed but unspecified positive integer and, on the basis of this assumption, prove that the result must also hold for $n = k + 2$. Of course, as usual, both parts of the proof are necessary and the second part of the argument must not depend on k having some particular value.

Finally, how does one decide whether to use I_1, I_2, I_4, or some other variation of mathematical induction? Actually, perhaps on scratch paper, one has to do the second part of the proof to see what is required to get "the next case." Let $P(n)$ be a proposition about the integer n. If the truth of $P(k + 1)$ follows from the truth of $P(k)$, I_1 will do nicely. If the truth of $P(k + 1)$ depends on the truth of $P(i)$ for $1 \leq i \leq k$, one must use I_2. If the truth of $P(k + 2)$ follows from the truth of $P(k)$ and $P(k + 1)$, then clearly I_4 is needed. But suppose that the truth of $P(k + 2)$ depends on the truth of $P(k)$; what then? A moment's reflection makes it clear that it will suffice to begin by proving that both $P(1)$ and $P(2)$ are true. This would be yet another variation of mathematical induction.

EXERCISES 1.4

1. Show that none of the following sets contains a least element:
   (a) The set of positive real numbers.
   (b) The set of all integers.
   (c) The set of all real numbers greater than 2.
2. Find the least element in the set
$$F = \{1, 1/2, 1/2^2, \ldots, 1/2^n, \ldots\}.$$
3. The following equalities are false for most positive integers n. Try to prove each by the method of mathematical induction and show why the method fails. Also, in each case, give a positive integral value for n for which the equality is false.
   (a) $\sum_{i=1}^{n} (2i + 1) = n^2 + 2$ (b) $\sum_{i=1}^{n} (i + 3) = n^2 + n + 2$
   (c) $\sum_{i=1}^{n} 2^{i-1} = \frac{n(n+1)}{2}$ (d) $\sum_{i=1}^{n} (3i - 2) = n^2 + n + 1$

4. Prove that

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$$

for every positive integer n.

5. Prove that

$$\sum_{i=1}^{n} i^3 = \left[\frac{n(n+1)}{2}\right]^2$$

for every positive integer n.

6. Use I_1 to prove that $2^{2n} - 1$ is divisible by 3 for every positive integer n.
Hint: For the second part of the proof make your assumption by assuming that there exists an integer q such that $2^{2k} - 1 = 3q$. Then consider

$$2^{2(k+1)} - 1 = 4 \cdot 2^{2k} - 1 = 3 \cdot 2^{2k} + 2^{2k} - 1 = 3 \cdot 2^{2k} + 3q.$$

7. Prove that $2^{2n-1} + 1$ is divisible by 3 for every positive integer n.

8. Prove that $f(n) = 3n^5 + 5n^3 + 7n$ is divisible by 15 for *every* integer n.
Hint: Note that $f(-n) = -f(n)$.

9. Prove that $3^{2n+1} + 2^{n+2}$ is divisible by 7 for every nonnegative integer n.

10. Prove that $\prod_{i=1}^{n} a_i^r = (\prod_{i=1}^{n} a_i)^r$ for every positive integer n [see (1.12)].

11. For any positive integer n, prove in two different ways that

$$\sum_{i=1}^{n} i(i!) = (n+1)! - 1.$$

Hint: For one way, note that the first i of the expression being summed can be written as $(i+1) - 1$ and then see Exercise 4 of Section 1.1.

12. Let F_n denote the nth Fibonacci number and prove that the following are true for every positive integer n.

(a) $\sum_{i=1}^{n} F_i = F_{n+2} - 1$

(b) $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$

(c) $\sum_{i=1}^{n} F_{2i-1} = F_{2n}$

(d) $\sum_{i=1}^{n} F_{2i} = F_{2n+1} - 1$

(e) $\sum_{i=1}^{n} (-1)^{i-1} F_i = (-1)^{n-1} F_{n-1} + 1$

13. Let $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$ so that α and β are the roots of $x^2 = x + 1$; that is, $\alpha^2 = \alpha + 1$ and $\beta^2 = \beta + 1$. Prove that $F_n = (\alpha^n - \beta^n)/\sqrt{5}$ for all $n \geq 0$.
Hint: You may use either I_2 or I_4; *in either case* start by proving the result for $n = 1$ and $n = 2$. Why? This formula is due to J. P. M. Binet in 1843.
Note: $F_0 = 0$.

14. Prove that $L_n = \alpha^n + \beta^n$ for all integers $n \geq 0$.
Note: $L_0 = 2$.

15. Use I_4 to prove that $\alpha^{n-2} \leq F_n \leq \alpha^{n-1}$ for every positive integer n. Note that it is again necessary to make the first part of the proof for $n = 1$ and $n = 2$.

16. Prove that $\alpha^n = F_{n-1} + \alpha F_n$ for $n \geq 1$, provided that we define $F_0 = 0$.

17. Prove that $F_{n+m+1} = F_n F_m + F_{n+1} F_{m+1}$ for $m \geq 0$, $n \geq 0$.
Hint: Hold m constant and use induction on n.

18. Deduce from Exercise 17 that F_n divides F_{2n} for every $n \geq 1$.

19. Prove that F_n divides F_{mn} for $n \geq 1$, $m \geq 1$.
Hint: Fix n and use induction on m.

20. Let $P(n)$ be a statement about n such that for every positive integer k, the truth of $P(k)$ implies the truth of $P(k + 3)$. What must be done to prove that $P(n)$ is true for every positive integer n?

21. Let $P(n)$ be an assertion about the positive integer n such that for every positive integer k, the truth of $P(k)$ implies the truth of $P(k + 1)$ for all $k \geq 5$. What must be done to show that $P(n)$ is true for every positive integer n?

22. Let $P(n)$ be a statement about n such that $P(1)$ is true, that the truth of $P(k)$ implies the truth of $P(k + 1)$ and $P(k + 2)$ if k is odd. What can you conclude about $P(n)$?

23. Prove that

$$\sum_{i=1}^{n} F_i F_{i+1} = \begin{cases} F_n F_{n+2} & \text{for } n \text{ even,} \\ F_{n+1}^2 & \text{for } n \text{ odd,} \end{cases}$$

where n is positive.
Hint: Use Exercise 22.

24. Prove that

$$\sum_{i=1}^{n} F_i F_{i+d} = \begin{cases} F_n F_{n+1+d} & \text{for } n \text{ even,} \\ F_{n+1} F_{n+d} & \text{for } n \text{ odd,} \end{cases}$$

where n is positive and d is a fixed positive integer.

Computer Exercise

25. What would the following program compute?

```
      J = 1
      DO 1 I = 2, 51
      J = (I - 1)*J
1     PRINT, J
      STOP
      END
```

1.5 THE WELL-ORDERING PRINCIPLE

We now illustrate the method of proof based on the well-ordering principle, I_3, by proving the following little result concerning the number 1.

THEOREM 1.3. If a is a positive integer, then $a \geq 1$; that is, 1 is the least positive integer.

Proof. Suppose, on the contrary, that there exists an integer a such that $0 < a < 1$. Then, if C is the set of such integers, it is not empty. Therefore, by I_3, C must have a least element. Let b be the least element of C. Then $0 < b < 1$ and, on multiplication by b, $0 < b^2 < b$. But then b^2 is an element of C which is smaller than b and this contradicts the fact that b was the least element of C. Because of this contradiction, our original assumption must be false, so that $a \geq 1$ for every positive integer a.

As in this case, many proofs based on the well-ordering principle involve the method of proof by contradiction. To prove a theorem by contradiction, one proceeds, in general, as follows. One begins by assuming that the theorem is false, and then deduces from this assumption a result that is *known* to be false, or that contradicts the primary assumption. We shall have many occasions in the discussions that follow to use this method of proof.

The proof of Theorem 1.3 also provides an easy illustration of the method of proof due to P. Fermat (1601–1665) and known as *Fermat's method of infinite descent.* In general, such a proof has the following form. One assumes that there is a positive integer r possessing some property P. One then deduces that there is some positive integer $s < r$ which also has property P. But since this argument could be repeated ad infinitum, it contradicts the fact that there must be a smallest positive integer with property P. Hence, there must be no positive integer possessing property P.

Also, it should be observed that the well-ordering principle can be generalized along the same lines as I_1 and I_2. For example, it could be shown from the well-ordering principle as stated that any nonempty set of integers, none of which is less than some fixed integer b, has a least element. Also, one could prove that any nonempty set of integers, none of which is greater than some fixed integer c, has a greatest element.

A second example of proof based on the well-ordering principle is the following interesting demonstration that $\sqrt{2}$ is irrational, due originally to Hugo Steinhaus.

THEOREM 1.4. The number $\sqrt{2}$ is irrational.

Proof. Since $1 < 2 < 4$, it follows that $1 < \sqrt{2} < 2$. Now suppose that $\sqrt{2}$ is rational. Then by the well-ordering principle, there exists a least positive integer b and an integer a such that $\sqrt{2} = a/b$. This implies that $1 < a/b < 2$ and hence that

$b < a < 2b$ and that $0 < a - b < b$. Thus, $a - b$ is a positive integer less than b. But since $\sqrt{2} = a/b$, it follows that

$$2 = \frac{a^2}{b^2},$$

$$2b^2 = a^2,$$

$$2b^2 - ab = a^2 - ab,$$

$$b(2b - a) = a(a - b),$$

$$\sqrt{2} = \frac{a}{b} = \frac{2b - a}{a - b}.$$

But this gives $\sqrt{2}$ as a ratio of two integers with positive integer denominator less than b. Since this is a contradiction, the theorem is true.

EXERCISES 1.5

1. Use the well-ordering principle to prove that $\sqrt{5}$ is irrational.
2. The Archimedean axiom states that if a and b are positive integers, there exists an integer n such that $an \geq b$. Use the well-ordering principle to prove that this is so. *Hint:* Suppose that the assertion is false and consider the set C of all positive integers of the form $b - ma$.
3. Use the well-ordering principle to prove that any nonempty set C of integers none of which is less then a specified integer a has a least element.
   Hint: Consider the set D of all integers of the form $c - a + 1$, where c is an element of C.
4. Use the well-ordering principle (as modified in Exercise 3 with $a = 2$) to prove that every integer $n \geq 2$ is either a prime or a product of primes.
5. Use Fermat's method of descent to prove that $\Sigma_{i=1}^{n} i = n(n + 1)/2$. Note that the critical arithmetic of the argument is essentially the same as in the proof of this result by I_1 in Section 1.4.
6. Use Fermat's method of descent to prove that

$$\sum_{i=1}^{n} i^3 = n^2(n + 1)^2/4.$$

Computer Exercise

7. Write a program to determine the least positive integer that can be written (nontrivially) as the sum of two cubes of positive integers in two different ways.

1.6 EQUIVALENCE OF THE PRINCIPLES OF INDUCTION AND WELL-ORDERING

In this section we show that in the presence of the other postulates for the positive integers, I_1, I_2, and I_3 are equivalent. First, to avoid circular proofs of Theorems 1.6 and 1.7, we give an alternative proof of Theorem 1.3 based on either I_1 or I_2 and then deduce a needed corollary.

Proof of Theorem 1.3 Using I_1 or I_2. It is clear that $1 \geq 1$. For the proof based on I_1, assume that $k \geq 1$, where k is any fixed but unspecified positive integer. (For the proof based on I_2, assume that $i \geq 1$ for all positive integers i from 1 to k inclusive, where k is any fixed but unspecified positive integer.) Then $k + 1 \geq k \geq 1$ and it follows by I_1 (I_2) that $n \geq 1$ for every positive integer n. Thus, both I_1 and I_2 imply that 1 is the least positive integer, as claimed.

COROLLARY 1.5. If k is any positive integer, then there exists no positive integer n such that $k < n < k + 1$.

Proof. This is an immediate consequence of Theorem 1.3 and hence of any one of I_1, I_2, and I_3. To see this, observe that if there exists a positive integer n such that $k < n < k + 1$, then $0 < n - k < 1$, so that $n - k$ is a positive integer less than 1, in contradiction to Theorem 1.3. Thus, no such n can exist.

We now proceed to the equivalence of I_1, I_2, and I_3.

THEOREM 1.6. I_1 implies I_2.

Proof. We take I_1 as a postulate and must prove I_2 as a theorem. Let C be any set of positive integers satisfying the conditions of I_2. The problem is to show that C contains all positive integers.

Let A_n denote the statement "the integers 1 to n inclusive are in C." A_1 is true by hypothesis. Now, assume that A_k is true where k is any fixed but unspecified positive integer. Then 1 to k inclusive are in C. Hence, again by hypothesis, $k + 1$ is in C and A_{k+1} is true. Therefore, by I_1, A_n is true for every positive integer n, so C contains all positive integers.

THEOREM 1.7. I_2 implies I_3.

Proof. We now take I_2 as a postulate and prove I_3 as a theorem. Let C be a nonempty set of positive integers. We must show that C has a least element.

Assume that C has no least element and let A_n denote the statement "n is not an element of C." Then A_1 is true, for otherwise 1 would be the least element of C by Theorem 1.3, which we just proved using I_2. Assume that A_n is true for all n from 1 to k inclusive. Then, by Corollary 1.5, A_{k+1} must also be true, for otherwise $k + 1$ would be the least element in C. Thus, by I_2, A_n is true for every positive integer n.

But this implies that C is empty, contrary to hypothesis. Therefore, the assumption that C has no least element is false and the theorem is proved.

THEOREM 1.8. I_3 implies I_1.

Proof. Let C be a set of positive integers satisfying the conditions of I_1. Assuming I_3 as a postulate, we must prove that C contains all positive integers.

Suppose that C does not contain all positive integers. Then the set C^* of all positive integers not in C is nonempty. Therefore, by I_3, C^* has a least element. It follows from Theorem 1.3, which we proved by using I_3, that no elements of C^* are less than 1 and, hence, that the least element of C^* is not less than 1. Moreover, the least element of C^* cannot be 1 since, by hypothesis, 1 is in C. Thus, again by Corollary 1.5, the least element in C^* can be written in the form $k + 1$, where k is a positive integer. But this says that k is in C whereas $k + 1$ is not, in direct contradiction to the hypothesis. Thus, the assumption that C does not contain all positive integers is false and the theorem is proved.

Theorems 1.6 to 1.8 show that I_1 implies I_2, that I_2 implies I_3, and that I_3 implies I_1. Thus, if any of these propositions is assumed as a postulate for the positive integers, the others are immediately available as theorems. We shall have a number of occasions to use each of these principles in what follows.

1.7 THE DIVISION ALGORITHM

To simplify notation here and throughout the remainder of the book, we shall always use lowercase Latin letters to denote integers unless explicitly stated to the contrary.

THEOREM 1.9. (The Division Algorithm). For any $b > 0$ and a, there exist unique integers q and r with $0 \leq r < b$ such that $a = bq + r$.

Proof. The proof depends on the modification of the well-ordering principle discussed in Section 1.5.

Let C be the set of all nonnegative integers of the form $a - sb$. If $a \geq 0$, then $a - 0b$ is an element of C. If $a < 0$, then $a - ab = a(1 - b) \geq 0$ is an element of C since $b \geq 1$. Thus, in either case, C is not empty. Hence, by the well-ordering principle, C has a least element. Let q denote that value of s which yields the least element of C and set $a - bq = r$. Thus, since r is the least nonnegative element of this form, it follows that $0 \leq r$ and

$$r - b = a - bq - b = a - (q + 1) \cdot b < 0,$$

since $r - b$ is of the form $a - sb$ and yet is less than the least nonnegative integer of this form. Thus, $0 \leq r < b$, as claimed.

The first part of the proof has shown that q and r with the desired properties must exist. To show that q and r are unique, we must show that they are the *only*

integers with the desired properties. Suppose that $a = bq' + r'$, where $0 \leq r' < b$. It suffices to show that $r = r'$ and $q = q'$. If $q' < q$, then $q' + 1 \leq q$ since q and q' are both integers. Therefore,

$$r = a - bq \leq a - b(q' + 1) = a - bq' - b = r' - b < 0,$$

and this is a contradiction. Similarly, we obtain a contradiction if $q' > q$. Thus, it must be the case that $q = q'$. But then $bq + r = a = bq + r'$, so $r = r'$ as well.

Stated somewhat differently, this theorem simply says that if one divides a by the positive integer b, one obtains a quotient q and a remainder r where r is nonnegative and less than b. However, the restriction that b be positive is not strictly necessary, and the theorem could also be written in the form: Given integers a and b with $b \neq 0$, there exist unique integers q and r with $0 \leq r < |b|$ such that $a = bq + r$.

The division algorithm is surprisingly useful, as we shall see subsequently. As a first example, note that with $b = 2$, the theorem implies that every integer a is either of the form $2k$ or of the form $2k + 1$ (i.e., even or odd). Thus, a^2 is either of the form $4k^2 = 4r$ or $4k^2 + 4k + 1 = 4s + 1$. Hence, the square of an integer must leave a remainder of 0 or 1 when divided by 4; it cannot leave a remainder of 2 or 3. Similarly, any integer a must be of the form $3k$, or $3k + 1$, or $3k + 2$. Thus, a^2 must be of the form $9k^2 = 3u$, or $9k^2 + 6k + 1 = 3v + 1$, or $9k^2 + 12k + 4 = 3w + 1$. Hence, the square of an integer must leave a remainder of 0 or 1 when divided by 3; it cannot leave a remainder of 2. Admittedly, these are only small results, but they are not without interest and they indicate an important way in which the division algorithm can be used.

EXERCISES 1.7

1. Prove that no number in the sequence 11, 111, 1111, 11111, . . . , is a perfect square.
2. If p is a prime other than 2 or 5, prove that p must be one of the forms $10k + 1$, $10k + 3$, $10k + 7$, or $10k + 9$.
3. Prove that the product of any two odd numbers must be odd.
4. Prove that one of any two consecutive integers must be even.
5. Prove that one of any three consecutive integers must be divisible by 3.
6. If a is an integer, prove that one of the numbers a, $a + 2$, and $a + 4$ is divisible by 3.
7. If n is an integer not divisible by 2 or 3, show that $n^2 + 23$ must be divisible by 24. *Hint:* Any integer must be of the form $6k$, $6k + 1$, . . . , or $6k + 5$.
8. If a, b, and c are integers with $a^2 + b^2 = c^2$, show that a and b cannot both be odd.
9. If a and b are integers with $b < 0$, prove that there exist unique integers q and r with $0 \leq r < |b|$ such that $a = bq + r$.

10. If a and b are integers with $b \neq 0$, prove that there exist unqiue integers q and r with $-|b|/2 < r \leq |b|/2$ such that $a = bq + r$.

Computer Exercise

11. **(a)** Write a program to compute and print n, $f(n)$, $f(f(n))$, $f(f(f(n)))$, . . . for $1 \leq n \leq 100$, where $f(n) = n/2$ if n is even and $f(n) = 3n + 1$ if n is odd.
(b) Make a conjecture based on part (a).

1.8 POSITIONAL NOTATION

For many theoretical purposes in the theory of numbers it is immaterial what system one uses for the representation of numbers. The Greeks, for example, with a very cumbersome notation, were able to discover and prove many basic properties of the integers. For practical purposes, however, and for theoretical matters requiring detailed computation, it is important to have a notation that facilitates calculation. The Hindu–Arabic system of notation, in worldwide use today, certainly meets this requirement, and although it is well known from constant usage, it may not be amiss to discuss it here in some detail.

In the first place, the Hindu–Arabic system is a *positional* system of notation. For example, we write 2922 as shorthand for the much more cumbersome expression $2 \cdot 10^3 + 9 \cdot 10^2 + 2 \cdot 10 + 2$ and let the position of each *digit* determine its contribution to the total value of the number being represented. Thus, the three 2's above contribute, respectively, two thousand, twenty, and two, and the nine contributes nine hundred to the total value of two thousand nine hundred twenty-two.

In the second place, the Hindu–Arabic system is said to have the *base* 10, since all numbers are expressed as sums of multiples of powers of 10, as in the preceding example. Incidentally, it is not difficult to imagine how this all came about. Members of the human race normally come equipped with built-in calculators with 10 keys and, quite naturally, count large numbers by repeatedly counting the 10 fingers. Indeed, the numbers we use as multipliers of the powers of 10 in our present system are called digits, as are the fingers and toes.

The great power of this system of notation is that any integer, however large, can be represented conveniently by repeated use of only 10 symbols and that simple algorithms, or orderly methods of computation, can be devised for carrying out arithmetical computations. Other systems, such as the Roman, for example, require the creation of more and more symbols for the representation of ever-larger numbers, and even such simple operations as addition and multiplication are quite tedious, to say nothing about division: for example,

$$\begin{aligned} \text{XXVIII} + \text{XXXIV} &= \text{XXVIII} + \text{XXXIIII} \\ &= \text{XXXXXVIIIIIII} \\ &= \text{LVVII} \\ &= \text{LXII} \end{aligned}$$

and

$$\begin{aligned}(\text{XIX}) \cdot (\text{II}) &= (\text{XVIIII}) \cdot (\text{II}) \\ &= \text{XVIIII} + \text{XVIIII} \\ &= \text{XXVVIIIIIII} \\ &= \text{XXXVIII}.\end{aligned}$$

One need only compare these calculations with the corresponding ones using ordinary base 10 arithmetic to appreciate the advantage positional notation affords. The usual simple rules for borrowing and carrying in subtraction and addition, as well as the methods for multiplication, and division, depend entirely on this notion.

The following theorem shows that it is always possible to represent an integer in decimal form and also suggests some interesting alternatives.

THEOREM 1.10. Let b be greater than 1. Then every $a > 0$ can be uniquely represented in the form

$$a = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0$$

with $c_n \neq 0$, $n \geq 0$, and $0 \leq c_i < b$ for $i = 0, 1, 2, \ldots, n$.

Proof. We first show that every $a > 0$ has a representation of the desired form and then show that the representations are unique.

(i) For $a = 1$, it suffices to take $n = 0$, $c_0 = 1$.

(ii) Assume that every integer from 1 to k inclusive can be represented in the desired way. On the basis of this assumption, it must be shown that $k + 1$ can also be represented in this way. By Theorem 1.9, there exist integers c_0 and q with $0 \leq c_0 < b$ such that $k + 1 = bq + c_0$. If $q = 0$, then $c_0 \neq 0$ and $k + 1 = c_0$, so that $k + 1$ is represented in the desired form. If $q > 0$, then $q = (k + 1 - c_0)/b \leq (k + 1)/2 \leq k$, since $b \geq 2$ and $k \geq 1$. Thus, by the induction assumption, q can be represented in the desired way; that is, there exist constants which we may denote by $c_1, c_2, \ldots, c_m$ with $c_m \neq 0$ and $0 \leq c_i < b$ for $i = 1, 2, \ldots, m$ such that

$$q = c_m b^{m-1} + c_{m-1} b^{m-2} + \cdots + c_2 b + c_1.$$

Hence,

$$k + 1 = bq + c_0 = c_m b^m + \cdots + c_1 b + c_0$$

and so can be represented in the desired way. Thus, by mathematical induction, every positive integer a can be represented in this way.

(iii) We must still show that the representation of each integer a is unique. Suppose that some a can be represented in two essentially different ways, say

$$\begin{aligned}a &= c_0 + c_1 b + \cdots + c_n b^n \\ &= d_0 + d_1 b + \cdots + d_m b^m\end{aligned}$$

with $c_n \neq 0$, $d_m \neq 0$, $0 \leq c_i < b$ for each i, $0 \leq d_j < b$ for each j, and with $m \geq n$. Then by subtraction,

$$0 = e_0 + e_1 b + \cdots + e_m b^m$$

where $e_i = d_i - c_i$ for $i = 0, \ldots, n$, and $e_i = d_i$ for $i = n+1, \ldots, m$ if $m > n$. In view of the inequalities on the c's and d's, it follows that $-(b-1) \le e_i \le (b-1)$ for each i. Also, $e_i \neq 0$ for some i since we assumed that the two representations for a were essentially different. Let e_k be the nonzero e with the largest subscript. Then

$$-e_k b^k = e_0 + e_1 b + \cdots + e_{k-1} b^{k-1}$$

and

$$\begin{aligned} b^k \le |-e_k b^k| &= |e_0 + e_1 b + \cdots + e_{k-1} b^{k-1}| \\ &\le |e_0| + |e_1| b + \cdots + |e_{k-1}| b^{k-1} \\ &\le (b-1) + (b-1)b + \cdots + (b-1)b^{k-1} = b^k - 1. \end{aligned}$$

Since this is a clear contradiction, it must be the case that $m = n$ and $c_i = d_i$ for all i. Thus, the representation is unique.

Theorem 1.10 shows that positional representation of numbers is possible with any integer $b > 1$ as base. For example, if $b = 8$, Theorem 1.10 guarantees that any positive integer can be written uniquely as a sum of multiples of powers of 8 where the multipliers come from among the integers 0 through 7. Thus, one hundred thirty-one can be written as $2 \cdot 8^2 + 0 \cdot 8 + 3$ and just as the representations of integers as sums of multiples of powers of 10 are abbreviated to decimal notation, this might be abbreviated in *octal* notation to 203. Indeed, this is almost certainly the way the number would have been written if human beings had been equipped with four digits instead of five on each hand. To avoid confusion, we shall frequently use a subscript, written in base 10 notation, to indicate the base. For the example above, we have that $131_{10} = 203_8$. Incidentally, 203_8 should be read "two zero three, base eight" and not "two hundred three" since our language for numbers is already oriented to base 10.

Since our rules for numerical computation, by hand or by machine, depend on the positional character of decimal notation and not on the base, calculations with numbers written in octal notation would be carried out as usual except that we would have to use different addition and multiplication tables, as shown below.

ADDITION TABLE FOR BASE 8

+	1	2	3	4	5	6	7
1	2	3	4	5	6	7	10
2	3	4	5	6	7	10	11
3	4	5	6	7	10	11	12
4	5	6	7	10	11	12	13
5	6	7	10	11	12	13	14
6	7	10	11	12	13	14	15
7	10	11	12	13	14	15	16

MULTIPLICATION TABLE FOR BASE 8

×	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	10	12	14	16
3	3	6	11	14	17	22	25
4	4	10	14	20	24	30	34
5	5	12	17	24	31	36	43
6	6	14	22	30	36	44	52
7	7	16	25	34	43	52	61

For example, the product of twenty-five and twenty would be found, in base 8, as follows, where the notation is octal:

$$\begin{array}{r} 31 \\ \underline{24} \\ 144 \\ \underline{62} \\ 764 \end{array}$$

Thus, $764_8 = 7 \cdot 8^2 + 6 \cdot 8 + 4 = 500_{10}$. Similarly, the sum of thirty-five and thirty would appear in octal notation as

$$\begin{array}{r} {\scriptstyle 1} \\ 43 \\ \underline{36} \\ 101 \end{array}$$

and $101_8 = 1 \cdot 8^2 + 0 \cdot 8 + 1 = 65_{10}$, as it should. The reader should work through these calculations with the help of the tables above to see what is involved at each step.

As almost everyone knows, modern computers do arithmetic in binary (base 2) notation. Octal (base 8) and hexadecimal (base 16) notation are also used in computing. Base 2 is the natural notation for the internal workings of a machine since only the digits 0 and 1 are required, and these can easily be expressed in the machine by a switch being either on or off, a spot on a magnetic tape being magnitized or not magnetized, a spot on the face of an electrostatic tube being either charged or not charged, and so on. Of course, arithmetic to base 2 is greatly simplified since one need only learn the addition and multiplication tables through the ones. For example, multiplying eleven by seven in base 2, one would have

$$\begin{array}{r} 1011 \\ \underline{111} \\ 1011 \\ 1011 \\ \underline{1011} \\ 1001101 \end{array}$$

Sixty is divided by 10 as follows:

$$\begin{array}{r} 110 \\ 1010\overline{)\,111100} \\ \underline{1010} \\ 1010 \\ \underline{1010} \end{array}$$

The reader should check to see that all these calculations are correct.

Now, it happens that there is a very simple method for obtaining the positional representation of any positive integer a to any base $b > 1$. By Theorem 1.9, we are assured that there exist integers q_1 and r_1 such that $a = bq_1 + r_1$ and $0 \leq r_1 < b$. Also, there exist q_2 and r_2 such that $q_1 = bq_2 + r_2$ with $0 \leq r_2 < b$. Again, there exists q_3 and r_3 such that $q_2 = bq_3 + r_3$ with $0 \leq r_3 < b$, and so on. Now, it is clear that $a > q_1 > q_2 > q_3 > \cdots$. Thus, we must finally reach the place where some q is smaller than b, though still positive; that is, for some k, $0 < q_k < b$. If we divide once more by b, we obtain $q_k = 0 \cdot b + r_{k+1}$ with $0 < r_{k+1} < b$ and this ends the process. Now

$$\begin{aligned} a &= bq_1 + r_1 \\ &= b(bq_2 + r_2) + r_1 = b^2q_2 + br_2 + r_1 \\ &= b^2(bq_3 + r_3) + br_2 + r_1 = b^3q_3 + b^2r_3 + br_2 + r_1 \\ &= \cdots \\ &= b^k r_{k+1} + b^{k-1}r_k + \cdots + br_2 + r_1, \end{aligned}$$

which is a representation of a in the form described in Theorem 1.10. But since a is *uniquely* expressible in the form, this must be *the* desired representation.

For example, if we want to write 356_{10} in positional notation to base 7, we perform the successive division as follows:

$$\begin{aligned} 7\underline{|356} & \\ 7\underline{|50} = q_1, & \quad r_1 = 6 \\ 7\underline{|7} = q_2, & \quad r_2 = 1 \\ 7\underline{|1} = q_3, & \quad r_3 = 0 \\ 0 = q_4, & \quad r_4 = 1. \end{aligned}$$

Thus, $356_{10} = 1016_7$.

Octal (base 8) and hexadecimal (base 16) notation are used in computing since binary representations tend to be quite lengthy and can be greatly shortened by using octal or hexadecimal notation. Also, it is very easy to change from binary notation to either octal or hexadecimal, and conversely. To illustrate this we note that 171_{10} is written in base 2 as 10101011_2. Now

$$\begin{aligned} 10{,}101{,}011_2 &= 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1 \\ &= (1 \cdot 2 + 0)2^6 + (1 \cdot 2^2 + 0 \cdot 2^1 + 1)2^3 + (0 \cdot 2^2 + 1 \cdot 2 + 1) \\ &= 2 \cdot 8^2 + 5 \cdot 8 + 3 \\ &= 253_8. \end{aligned}$$

Thus, to go from base 8 to base 2 we replace each digit in base 8 by the triple of digits that give its representation in base 2 and conversely. Of course,

$$2 = 10_2, \quad 5 = 101_2, \quad \text{and} \quad 3 = 11_2 = 011_2$$

since initial 0's may or may not be needed to fill out a triple. The hexadecimal digits for 10, 11, 12, 13, 14, and 15 are normally represented by A, B, C, D, E, and F and their four-digit binary representations are given by

$$\begin{aligned} 0 &= 0000_2 & 8 &= 1000_2 \\ 1 &= 0001_2 & 9 &= 1001_2 \\ 2 &= 0010_2 & A &= 1010_2 \\ 3 &= 0011_2 & B &= 1011_2 \\ 4 &= 0100_2 & C &= 1100_2 \\ 5 &= 0101_2 & D &= 1101_2 \\ 6 &= 0110_2 & E &= 1110_2 \\ 7 &= 0111_2 & F &= 1111_2. \end{aligned}$$

Since $16 = 2^4$, we may go from hexadecimal to binary notation by replacing each digit by its *four*-digit binary representation, and conversely. Thus 171_{10} is represented in binary by $\underbrace{1010}\,\underbrace{1011}_2$

and in hexadecimal by AB_{16}.

EXERCISES 1.8

1. Express 247_{10} to **(a)** base 7, **(b)** base 2, **(c)** base 8, and **(d)** base 16.
2. What number to base 10 is represented by **(a)** 324_8, **(b)** 324_{16}, **(c)** 10_7, **(d)** 10_5, **(e)** 100_8, and **(f)** $D9B_{16}$?
3. What number to base 10 is represented by 21.7_8? (This has not been discussed, but the extension should be clear.)

4. Carry out the following computations using octal notation throughout. Check your work by converting to decimal notation.
   (a) $257_8 + 361_8$ **(b)** $257_8 \times 361_8$
   (c) $361_8 - 257_8$ **(d)** $1356_8 \div 31_8$
5. Construct addition and multiplication tables for base 5 and in that base carry out the following calculations.
   (a) $423_5 + 242_5$ **(b)** $423_5 \times 242_5$
   (c) $331_5 \div 23_5$
6. Convert the following to octal notation and hexadecimal notation.
   (a) 111100101_2 **(b)** 1100101_2
7. Convert the following to binary notation.
   (a) 257_8 **(b)** 301_8
   (c) $AF3_{16}$ **(d)** $10C_{16}$
8. Let b be greater than 1. Show that every integer a (positive, negative, or zero) can be represented uniquely in base $-b$, that is, in the form
$$a = c_n(-b)^n + c_{n-1}(-b)^{n-1} + \cdots + c_1(-b) + c_0$$
with $c_n \neq 0$ if $a \neq 0$ and $0 \leq c_i < b$ for $0 \leq i \leq n$. If $a < 0$, show that n is odd. If $a > 0$, show that n is even.
9. Show that the method for changing from base 10 notation to base b is also valid for changing to base $-b$. For example, to write 392_{10} in base -10, we have that
$$\begin{aligned} 392 &= (-10)(-39) + 2 \\ -39 &= (-10)(4) + 1 \\ 4 &= (-10) \cdot 0 + 4, \end{aligned}$$
so that $392_{10} = 412_{-10}$. In short form as above, this could have been written
$$\begin{aligned} -10|\underline{392} & \\ -10|\underline{-39} = q_1, &\quad r_1 = 2 \\ -10|\underline{4} = q_2, &\quad r_2 = 1 \\ 0 = q_3, &\quad r_3 = 4. \end{aligned}$$
10. Write **(a)** 82_{10} and **(b)** -761_{10} in base -10 notation.
11. Write the numbers from one through 20 in base -10 notation.
12. Show that, in adding or multiplying numbers to base -10, one must *subtract* the "carries." For example, 87_{-10} and 206_{-10} are added in the following way:
$$\begin{array}{r} {\scriptstyle 1} \\ 87 \\ \underline{206} \\ 273 \end{array}$$
Write these numbers in base 10 notation and check that the addition is correct.

13. In subtracting to base -10, show that when one borrows, one must increase rather than decrease the digit borrowed from. For example, in subtracting 29_{-10} from 57_{-10}, one proceeds as follows:

$$\begin{array}{r} {\scriptstyle 6} \\ 5\!\!\not{7}^{1}7 \\ 2\ 9 \\ \hline 4\ 8 \end{array}$$

Write these numbers in base 10 notation and check that the subtraction is correct.

14. Carry out the following calculations using base -10 notation throughout.

(a) $347_{-10} + 58_{-10}$ **(b)** $347_{-10} - 58_{-10}$
(c) $78_{-10} + 86_{-10}$ **(d)** $28_{-10} \times 57_{-10}$
(e) $534_{-10} - 2476_{-10}$ **(f)** $193600_{-10} \div 35_{-10}$

15. Write the following in base 10 notation.

(a) 276_{-10} **(b)** 27.6_{-10} **(c)** $27.6\overline{90}_{-10}$
(d) $27.5\overline{09}_{-10}$ **(e)** $0.\overline{90}_{-10}$ **(f)** $19.\overline{09}_{-10}$

Note that $27.6\overline{90}$ indicates the infinite repeating decimal 27.6909090 . . . where the 90 repeats ad infinitum.

Computer Exercises

16. Write a program to print any number n in base b notation, where b is an integer and $2 \le b \le 9$. Your program should print out the base b representation of n. In particular, write 18456203 in base 2.

17. **(a)** Let $s(n)$ denote the sum of the squares of the digits of n. Write a program to investigate the behavior of n, $s(n)$, $s(s(n))$, $s(s(s(n)))$, . . . for $1 \le n \le 100$. Be careful not to get caught in an infinite loop.
(b) Make a conjecture on the basis of part (a).

1.9 COMPUTATIONAL COMPLEXITY

In Section 1.8 we discussed positional notation for integers in any base and pointed out that base 2, base 8, and base 16 are particularly important and useful in computer science. The usual algorithms for integer computation are, of course, essentially the same in any base, and it is easy enough to write out careful proofs that they produce correct results. Of course, no claim is made for uniqueness of method and there are a number of alternatives for each of the basic operations of integer arithmetic. In the case of multiplication, for example, one reasonably well-known, but rather surprising algorithm is the method known variously as Russian peasant multiplication or Egyp-

tian multiplication. To multiply 27 times 38, for example, one divides 27 and its successive quotients by 2 (ignoring any remainders that might result) until a quotient of 1 is obtained, and simultaneously doubles 38 and its successive doubles, as illustrated:

27	38
13	76
~~6~~	~~152~~
3	304
1	608
	1026

One then deletes the even numbers in the "halving" column and the corresponding numbers in the "doubling" column and adds the remaining numbers in the "doubling" column to obtain the desired result. Thus, $27 \cdot 38 = 1026$. The question is not correctness but quickness or efficiency.

In general, in computing, it is important that jobs be done as efficiently as possible. Because of the cost of computing, this is particularly true of large jobs that must be run repeatedly. But it is equally true of very large and/or complicated jobs if they *are to be completed at all.* As fast as they are, as we will see later, there exist computational problems of sufficient size and complexity that they cannot yet be calculated in "finite time" on even the largest, fastest, and most sophisticated of today's computers. To obtain a bit deeper understanding of the problem, we investigate briefly the complexity of the usual algorithms of integer arithmetic. The needed definitions follow.

DEFINITION 1.3. If f and g are positive-valued functions with domain D, we say that f is $O(g)$ and write $f = O(g)$ if there is a positive constant C such that $f(x) < Cg(x)$ for all x in D. $O(g)$ is usually read "big-O of g" and we say that f is big-O of g or that f is of the order of g.

THEOREM 1.11. If $f = O(g)$ on the domain D and c is a positive constant, then $cf = O(g)$ on D; that is, $cO(g) = O(g)$.

Proof. If $f = O(g)$, there is a positive C such that $f(x) < Cg(x)$ for all x in D. Therefore, $cf(x) < cCg(x)$ for all x in D, so $cf = O(g)$.

THEOREM 1.12. If $f = O(cg)$ on the domain D and $c > 0$, then $f = O(g)$ on D; that is, $O(cg) = O(g)$.

Proof. $f = O(cg)$ implies that there exists a positive constant C such that $f(x) < Ccg(x)$ for all x in D. But then $f = O(g)$, as claimed.

THEOREM 1.13. If $f_1 = O(g_1)$ and $f_2 = O(g_2)$ on the domain D, then $f_1 + f_2 = O(g_1 + g_2)$ and $f_1 f_2 = O(g_1 g_2)$ on D.

Proof. Since $f_1 = O(g_1)$ and $f_2 = O(g_2)$, there exist positive constants C_1 and C_2 such that $f_1(x) < C_1 g_1(x)$ and $f_2(x) < C_2 g_2(x)$ for all x in D. But then

$$f_1(x) + f_2(x) < C_1 g_1(x) + C_2 g_2(x) < C[g_1(x) + g_2(x)],$$

where C is the larger of C_1 and C_2. Also,

$$f_1(x) f_2(c) < C_1 C_2 g_1(x) g_2(x)$$

for all x in D. These two inequalities imply that $f_1 + f_2 = O(g_1 + g_2)$ and $f_1 f_2 = O(g_1 g_2)$.

COROLLARY 1.14. If f_1 and f_2 are $O(g)$ on the domain D, then $f_1 + f_2 = O(g)$ and $f_1 f_2 = O(g^2)$ on D.

Proof. Setting $g = g_1 = g_2$ in Theorem 1.13, we have that $f_1 + f_2 = O(2g) = O(g)$ and $f_1 f_2 = O(g^2)$, as claimed.

THEOREM 1.15. If $g(x) \leq h(x)$ for all x in a domain D, then $O(g) + O(h) = O(h)$ and $O(g)O(h) = O(gh)$.

Proof. If $f_1 = O(g)$ and $f_2 = O(h)$ on D, then there exist positive constants C_1 and C_2 such that $f_1(x) < C_1 g(x) \leq C_1 h(x)$ and $f_2(x) < C_2 h(x)$ for all x in D. Therefore, $f_1(x) + f_2(x) < (C_1 + C_2)h(x)$ and $f_1(x) f_2(x) < C_1 C_2 g(x) h(x)$ for all x in D. But this implies that $f_1 + f_2 = O(h)$ and $f_1 f_2 = O(gh)$, as claimed.

We mentioned that it is natural that computers should represent integers and do calculations in binary notation — they represent numbers using *bits,* or binary digits. Thus, we can discuss the *computational complexity* of an algorithm in terms of *bit operations,* by which we mean the addition, subtraction, or multiplication of two binary digits, the division of a two-bit integer by a one-bit integer, or the shifting by one place of an integer written in binary notation.

Consider the operation of addition, for example. In adding two n-bit integers by the usual algorithm, we add the digits two at a time, and even allowing for a "carry" each time, the number of bit operations is clearly at most $3n$. Hence, addition and also subtraction of two n-bit integers takes $O(n)$ operations. On the other hand, the usual multiplication algorithm clearly requires n^2 bit multiplications and $O(n)$ additions, carries, and shifts. Thus, since $n \leq n^2$, it follows from Theorem 1.15 that $O(n^2)$-bit operations are required.

Somewhat surprisingly, however, faster algorithms for multiplication are available. Suppose, for example, that $P(n)$ denotes the number of bit operations required to multiply two n-bit integers and that we want to multiply two $2n$-bit integers

$$a = \sum_{i=0}^{2n-1} a_i 2^i \quad \text{and} \quad b = \sum_{i=0}^{2n-1} b_i 2^i.$$

Note that

$$a = A_1 \cdot 2^n + A_0 \quad \text{and} \quad b = B_1 \cdot 2^n + B_0,$$

where $A_0 = \sum_{i=0}^{n-1} a_i 2^i$, $A_1 = \sum_{i=n}^{2n-1} a_i 2^{i-n}$, $B_0 = \sum_{i=0}^{n-1} b_i 2^i$, and $B_1 = \sum_{i=n}^{2n-1} b_i 2^{i-n}$. The straightforward multiplication of a and b gives

$$ab = A_1 B_1 \cdot 2^{2n} + A_1 B_0 \cdot 2^n + A_0 B_1 \cdot 2^n + A_0 B_0,$$

which is the sum of the four products of two n-bit integers with appropriate shifts and carries. This gives $P(2n) = 4P(n) + cn$, where c is a positive constant, so $P(2n) = 4 \cdot O(n^2) = O(n^2)$ by Theorem 1.11. A little ingenuity, however, improves the result. One has only to do the algebra to see that

$$ab = (2^{2n} + 2^n)A_1 B_1 + 2^n(A_1 - A_0)(B_0 - B_1) + (2^n + 1)A_0 B_0. \tag{1.19}$$

This clearly requires the computation of three products of n-bit integers, $A_1 B_1$, $(A_1 - A_0)(B_0 - B_1)$, and $A_0 B_0$, in addition to a number of shifts and additions. Thus,

$$P(2n) \leq 3P(n) + cn, \tag{1.20}$$

where c is a positive constant since the additions and shifts clearly require only $O(n)$ operations.

Now it follows from (1.20) that

$$P(2^n) \leq q(3^n - 2^n), \tag{1.21}$$

where q is the larger of $P(2)$ and c. For $n = 1$, this is clearly true since $P(1) = 0$ and, by (1.20), $P(2) \leq 3P(1) + c = c(3^1 - 2^1)$. Assume that

$$P(2^k) \leq q(3^k - 2^k),$$

where $k \geq 1$ is fixed. Then, again by (1.20),

$$\begin{aligned} P(2^{k+1}) &\leq 3P(2^k) + c \cdot 2^k \\ &\leq 3q(3^k - 2^k) + c \cdot 2^k \\ &\leq q3^{k+1} - q \cdot 3 \cdot 2^k + q \cdot 2^k \\ &= q(3^{k+1} - 2^{k+1}), \end{aligned}$$

and the result is true for all $n \geq 1$ by mathematical induction.

Before showing that the algorithm of (1.19) is more efficient than the usual algorithm, we note that for any real α, by $[\alpha]$ we mean the integer satisfying $[\alpha] \leq \alpha < [\alpha] + 1$; that is, $[\alpha]$ is the largest integer not exceeding α.

THEOREM 1.16. $P(n) = O(n^{\log_2 3})$.

Proof. Since $n = 2^{\log_2 n} \leq 2^{[\log_2 n]+1}$, it follows from (1.19) that

$$\begin{aligned} P(n) &\leq P(2^{[\log_2 n]+1}) \\ &\leq q(3^{[\log_2 n]+1} - 2^{[\log_2 n]+1}) \\ &< 3q \cdot 3^{\log_2 n} \\ &= 3qn^{\log_2 3} \end{aligned}$$

since $\log_2 n \cdot \log_2 3 = \log_2 3 \cdot \log_2 n$ implies that

$$\log_2 3^{\log_2 n} = \log_2 n^{\log_2 3},$$

which in turn implies that $3^{\log_2 n} = n^{\log_2 3}$. But then $P(n) = O(n^{\log_2 3})$, as claimed.

Note that $\log_2 3 = 1.5849 \ldots$, so that the algorithm of (1.19) is considerably better than the usual algorithm, which requires $O(n^2)$ operations, as we have already seen. But even better algorithms exist. The best algorithm to date can multiply two n-bit integers in $O(n \cdot \log n \cdot \log \log n)$ operations, and $n \cdot \log n \cdot \log \log n$ is much smaller than $n^{\log_2 3}$ for large values of n.

Note, by the way, that $O(\log_{10} n) = O(\log_b n)$, where b is any real number greater than 1. To see this, we have only to note that $\log_{10} n = \log_{10} b \cdot \log_b n$.

Finally, although we choose not to prove it here, the following theorem shows that the number of bit operations for division and multiplication are related.

THEOREM 1.17. If a is a $2n$-bit integer and b has no more than n bits, there is an algorithm for computing the quotient and remainder of the division of a by b in $P(n)$ steps, the same number of steps as required for multiplying two n-bit integers.

For our purposes, it will suffice to take $P(n) = O(n^2)$ rather than one of the sharper estimates given above.

EXERCISES 1.9

1. **(a)** Find the base 10 analog to identity (1.19).
   (b) Using part (a), multiply 63 by 57 using only addition, subtraction, shifts, and just three multiplications of one-digit integers.
   (c) Use part (a) twice to multiply 7431 by 7283 using only additions, subtractions, shifts, and just nine multiplications of one-digit integers.
2. If $n = \sum_{i=0}^{r} n_i b^i$ with $0 \le n_i < b$ and $n_r \neq 0$ is the base b representation of n, show that $r = [\log_b n] + 1$.
3. Use Exercise 2 to determine the number of digits in the base 10 representation of 2^{64}.
4. If $f_i = O(g)$ on some domain D for $i = 1, 2, \ldots, n$, prove that $\sum_{i=1}^{n} f_i = O(g)$ and $\prod_{i=1}^{n} f_i = O(g^n)$ on D for every positive integer n.
5. If $a > 1$, $b > 1$, and $f(n) = O(a^n)$ for all positive integers n, under what circumstances does it follow that $f(n) = O(b^n)$?
6. If F_n denotes the nth Fibonacci number, prove that $F_n = O(\alpha^{n-1})$, where $\alpha = (1 + \sqrt{5})/2$ and the domain is the set of all positive integers.

7. If L_n denotes the nth Lucas number, show that $L_n = O(\alpha^n)$, where the domain is the set of all positive integers.

Computer Exercises

8. Write a computer program to add two arbitrarily large positive integers.
9. Write a computer program to multiply two arbitrarily large positive integers.

2

Divisibility Properties of Integers

Among the most important ideas in the theory of numbers is that of the divisibility of integers; we introduced this concept in Definitions 1.1 and 1.2 in Section 1.4. Questions concerning primes and divisors were among the earliest to be considered when human beings first began to reflect on the properties of numbers, and the search for answers continues to this day. How many primes are there? How many divisors does an integer have? Are there any other integers like $6 = 1 + 2 + 3$, where the sum of the proper divisors of the number is equal to the original number? Can one find a formula for the nth prime? Does the formula $F(n) = 2^{2^n} + 1$ yield prime values for every positive integer n? For what values of n does $2^n - 1$ give prime values? We shall consider these and other questions concerning divisibility as we develop the theory.

2.1 BASIC PROPERTIES

The first consequences of Definition 1.1, which should be reviewed at this time, are contained in the following theorems. Recall that we are using lowercase Latin letters to designate integers unless expressly stated to the contrary.

THEOREM 2.1

(i) If $a \neq 0$, then $a|0$ and $a|a$.
(ii) $1|b$ for any b.
(iii) If $a|b$, then $a|bc$ for any c.
(iv) If $a|b$ and $b|c$, then $a|c$.
(v) If $a|b$ and $a|c$, then $a|(bx + cy)$ for any x and y.

Proof. Parts (i) and (ii) are trivial since $a \cdot 0 = 0$, $a \cdot 1 = a$, and $1 \cdot b = b$.

(iii) If $a|b$, there exists q such that $aq = b$. Therefore, $a(qc) = bc$, so $a|bc$ for any c.

(iv) If $a|b$ and $b|c$, there exist integers r and s such that $ar = b$ and $bs = c$. But then $c = a(rs)$, so $a|c$, as claimed.

(v) If $a|b$ and $a|c$, there exist u and v such that $au = b$ and $av = c$. Then $bx + cy = aux + avy = a(ux + vy)$, so that $a|(bx + cy)$ for any x and y.

Property (v) in Theorem 2.1 is especially useful in solving many divisibility problems. In particular, we may note that if $a|b$ and $a|c$, then $a|(b + c)$ and $a|(b - c)$. Also, property (v) extends to sums of more than two terms. Thus, if $a|b_i$ for $i = 1, \ldots, n$, then $a|(b_1x_1 + \cdots + b_nx_n)$ for any integers $x_1, x_2, \ldots, x_n$.

THEOREM 2.2. If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

Proof. If $a|b$ and $b \neq 0$, there exists $c \neq 0$ such that $ac = b$. But then $|b| = |a| \cdot |c| \geq |a|$ since $|c| \geq 1$.

COROLLARY 2.3. If a and b are positive and $a|b$ and $b|a$, then $a = b$.

Proof. By Theorem 2.2, $|a| \leq |b|$ and $|b| \leq |a|$. But since a and b are positive, the absolute value bars are superfluous. Thus, $a \leq b \leq a$, so $a = b$.

In what follows, we shall have a number of occasions to use this corollary as a simple but effective tool in proving equality of numbers.

EXERCISES 2.1

1. If $a|b$ and $a + b = c$, prove that $a|c$.
2. If $a|c$ and $a + b = c$, prove that $a|b$.
3. If $m|(35n + 26)$, $m|(7n + 3)$, and $m > 1$, prove that $m = 11$.
4. If $m|(8n + 7)$ and $m|(6n + 5)$, prove that $m = \pm 1$.
5. If $a > 0$, $b > 0$, and $\frac{1}{a} + \frac{1}{b}$ is an integer, prove that $a = b$. Also, show that $a = 1$ or 2.
6. If $a = bq + r$ with $0 \leq r < b$ and $b|a$, prove that $r = 0$.
7. Let S be the set of all positive integers of the form $ax + by$. Suppose that S is not empty and let $d = ax_0 + by_0$ be the least element in S. Show that every element of S is divisible by d.
   Hint: Let n be an element of S. Then there exist integers q and r, with $0 \leq r < d$, such that $n = qd + r$. Using the special nature of n and d, argue that $r = 0$.

8. Let S be the set of Exercise 7; show that S contains *all* positive integral multiples of $d = ax_0 + by_0$.
9. Let N_n be the integer whose decimal expansion consists of n consecutive ones. For example, $N_2 = 11$ and $N_7 = 1{,}111{,}111$. Show that $N_n | N_m$ if and only if $n | m$.

Computer Exercise

10. Write a program to determine if one positive integer divides another.

2.2 THE GREATEST COMMON DIVISOR

If $d|a$ and $d|b$, then d is said to be a *common divisor* of a and b. If a and b are both equal to zero, it follows from property (i) of Theorem 2.1 that they have infinitely many common divisors. However, if at least one of a and b is different from zero, it follows from Theorem 2.2 that the number of common divisors is finite and hence that there must be a largest common divisor.

DEFINITION 2.1. If d is the largest common divisor of a and b, it is called the *greatest common divisor* of a and b and is denoted by (a, b).

In view of the preceding discussion, it is clear that (a, b) is defined only in case a and b are not both zero. Thus, when we subsequently have occasion to write (a, b), we shall always imply that a and b are not both zero. Also, it is clear that (a, b) is a positive integer.

If either a or b is small, the problem of finding (a, b) is not difficult since there are only a few alternatives. For example, it is easy to see that $\pm 1, \pm 2, \pm 3$, and ± 6 are the only common divisors of 12 and 18 and that $6 = (12, 18)$. However, trial-and-error methods are not very efficient when it comes to large values of a and b. There is an efficient and systematic way for computing (a, b), but before discussing it, it will be convenient to present two interesting and very useful alternative characterizations of the greatest common divisor.

THEOREM 2.4. If a and b are not both zero and if $d = (a, b)$, then d is the least element in the set of all positive integers of the form $ax + by$.

Proof. Consider the set C of all positive integers of the form $ax + by$. By hypothesis, at least one of a and b is different from zero. For definiteness, suppose that $a \neq 0$. If $a > 0$, then a itself is a member of C, and if $a < 0$, $-a$ is a member of C. Therefore, C is not empty, and so, by the well-ordering principle, must have a least element. Let

$$e = ax_0 + by_0$$

be the least element of C. It suffices to show that $d = e$.

By Theorem 1.9, there exist integers q and r with $0 \leq r < e$ such that $a = eq + r$. Thus,

$$\begin{aligned} r &= a - eq \\ &= a - (ax_0 + by_0)q \\ &= a(1 - qx_0) + b(-qy_0), \end{aligned}$$

which is of the form $ax + by$. If r were not zero, it would be a member of C, and this would contradict our assumption that e is the smallest member of C. Thus, $r = 0$ and $e|a$. Similarly, one can show that $e|b$. Thus, e is a common divisor of a and b, so that, by Definition 2.1, $e \leq d$. On the other hand, since $e = ax_0 + by_0$ and $d|a$ and $d|b$, it follows from property (v) of Theorem 2.1 that $d|e$. Hence, $d \leq e$ by Theorem 2.2, so $d = e$.

THEOREM 2.5. $d = (a, b)$ if and only if $d > 0$, $d|a$, $d|b$, and $f|d$ for every common divisor f of a and b.

Proof. As noted earlier, since we are discussing (a, b), we are tacitly assuming that a and b are not both zero.

(i) Suppose, first, that $d = (a, b)$. Then $d|a$, $d|b$, and by Theorem 2.4, $d = ax + by > 0$ for some integers x and y. But then, if $f|a$ and $f|b$, $f|d$ by property (v) of Theorem 2.1.

(ii) Conversely, suppose that $d > 0$, $d|a$, $d|b$, and $f|d$ for every common divisor f of a and b. Then d is a common divisor of a and b and, by Theorem 2.2, $|f| \leq d$. Thus, $d = (a, b)$ by Definition 2.1.

2.3 THE EUCLIDEAN ALGORITHM

We are now in a position to discuss an orderly and systematic process for finding the greatest common divisor of two nonzero integers. Such a method is given in Book VI of Euclid's *Elements* and is now known as *Euclid's algorithm.*

For $a > b > 0$, we proceed as follows. Divide a by b getting, according to Theorem 1.9, a quotient q_1 and remainder r_1 such that $a = bq_1 + r_1$ with $0 \leq r_1 < b$. If $r_1 = 0$, then $b|a$ and $(a, b) = b$. If $r_1 \neq 0$, we divide b by r_1, getting a quotient q_2 and remainder r_2 such that $b = q_2r_1 + r_2$ with $0 \leq r_2 < r_1$. If $r_2 = 0$, the process stops. If $r_2 \neq 0$, we continue and get $r_1 = q_3r_2 + r_3$ with $0 \leq r_3 < r_2$, and so on. Eventually, the process must terminate with a zero remainder since the decreasing sequence of nonnegative numbers $b > r_1 > r_2 > r_3 > \cdots$ can extend for at most b terms before reaching zero. Suppose that r_{k+1} is the first zero remainder, so that we have the equations

$$
\begin{aligned}
a &= bq_1 + r_1, \\
b &= r_1q_2 + r_2, \\
r_1 &= r_2q_3 + r_3, \\
&\cdots\cdots\cdots\cdots, \\
r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1}, \\
r_{k-2} &= r_{k-1}q_k + r_k, \\
r_{k-1} &= r_kq_{k+1}.
\end{aligned}
$$

It is easy to show that r_k, the last nonzero remainder, is the desired greatest common divisor of a and b. We have that $r_k|r_{k-1}$ and $r_k|r_k$ so, using the next-to-last of the preceding equations and property (v) of Theorem 2.1, $r_k|r_{k-2}$. But then $r_k|r_{k-1}$ and $r_k|r_{k-2}$, so, using the third equation from the last and property (v) of Theorem 2.1, $r_k|r_{k-3}$. This process may be continued to show that $r_k|a$ and $r_k|b$. On the other hand, if $f|a$ and $f|b$, it follows from the first of the preceding equations and property (v) of Theorem 2.1 that $f|r_1$. But then $f|b$ and $f|r_1$ and it follows from the second equation and property (v) of Theorem 2.1 that $f|r_2$. Continuing this argument step by step, one finally has that $f|r_k$. Thus, r_k satisfies the conditions of Theorem 2.5, so $r_k = (a, b)$, as claimed.

To make the method clear, we find the greatest common divisor of 288 and 51. Performing the appropriate divisions, we obtain

$$
\begin{aligned}
288 &= 51 \cdot 5 + 33, \\
51 &= 33 \cdot 1 + 18, \\
33 &= 18 \cdot 1 + 15, \\
18 &= 15 \cdot 1 + 3, \\
15 &= 3 \cdot 5.
\end{aligned}
$$

Thus, according to the preceding discussion, $3 = (288, 51)$. Moreover, one can use the preceding equations to find x and y such that $3 = 288x + 51y$, which we know exist by Theorem 2.4. Starting with the next-to-last equation and eliminating successive remainders, we obtain

$$
\begin{aligned}
3 &= 18 - 15 \\
&= 18 - (33 - 18) \\
&= 2 \cdot 18 - 33 \\
&= 2(51 - 33) - 33 \\
&= 2 \cdot 51 - 3 \cdot 33 \\
&= 2 \cdot 51 - 3(288 - 5 \cdot 51) \\
&= 288(-3) + 51 \cdot 17.
\end{aligned}
$$

Thus, $3 = 288x + 51y$, where $x = -3$ and $y = 17$. In passing, it may be noted that the x and y are not unique. For example,

$$\begin{aligned} 3 &= 288(-3) + 51 \cdot 17 \\ &= 288(-3) + 288 \cdot 51 - 288 \cdot 51 + 51 \cdot 17 \\ &= 288 \cdot 48 + 51(-271), \end{aligned}$$

so that $x = 48$, $y = -271$ would do just as well. In fact, it is easy to see that there are infinitely many pairs of values that x and y may assume.

Note that while the preceding calculation of x and y is easily accomplished by hand if the number of steps is not large, it is not the most efficient for machine computation. To do it this way by machine, one has to create a file to store the successive quotients and remainders and then compute backward, as above. This can be avoided if at each successive division, we immediately update by writing the new remainder as a combination of a and b. For 288 and 51, we would proceed as follows.

$$\begin{aligned} 288 &= 51 \cdot 5 + 33 & 33 &= 288 - 5 \cdot 51 \\ 51 &= 33 \cdot 1 + 18 & 18 &= 51 - 33 \\ & & &= 51 - (288 - 5 \cdot 51) \\ & & &= -288 + 6 \cdot 51 \\ 33 &= 18 \cdot 1 + 15 & 15 &= 33 - 18 \\ & & &= (288 - 5 \cdot 51) - (-288 + 6 \cdot 51) \\ & & &= 2 \cdot 288 - 11 \cdot 51 \\ 18 &= 15 \cdot 1 + 3 & 3 &= 18 - 15 \\ & & &= (-288 + 6 \cdot 51) - (2 \cdot 288 - 11 \cdot 51) \\ & & &= -3 \cdot 288 + 17 \cdot 51 \\ 15 &= 3 \cdot 5 \end{aligned}$$

Thus, $3 = (288, 51) = 288x + 51y$ with $x = -3$ and $y = 17$, as above.

The point of Theorem 2.4 is not so much the fact that $d = (a, b)$ is the least positive integer of the form $ax + by$, but that d can be written in this form at all. This fact was needed in the proof of Theorem 2.5, which formed the basis for the discussion of Euclid's algorithm, and it will prove useful at other points as we continue to develop the theory. Note, by the way, that if a and b are both positive, then $d < a + b$, so one of x and y in $d = ax + by$ must be positive and the other negative.

Incidentally, an expression of the form $ax + by$ is said to be a *linear combination* of a and b since each term is of *first degree* in a and b. Thus, Theorem 2.4 implies that (a, b) can be represented as a linear combination of a and b. It is important to note, however, that the converse of this statement is not true. That is, if $d = ax + by$, it *does not follow* that $d = (a, b)$. For if $d = ax + by$, then $kd = a(kx) + b(ky)$ is a linear combination of a and b for every k, and not all these values can equal (a, b). From $d = ax + by$ one can conclude that $(a, b) | d$, but without further information,

this is all that can be said. On the other hand, if $1 = ax + by$, then $(a, b)|1$, and since (a, b) is a positive integer, it follows that $(a, b) = 1$. Thus, we have proved the following little theorem.

THEOREM 2.6. $(a, b) = 1$ if and only if there exist integers x and y such that $1 = ax + by$.

COROLLARY 2.7. If $d = (a, b)$ and A and B are defined by the equations $a = Ad$, $b = Bd$, then $(A, B) = 1$.

Proof. Since $d = (a, b)$, there exist integers x and y such that $d = ax + by$. Therefore,

$$1 = \frac{a}{d}x + \frac{b}{d}y = Ax + By$$

and $(A, B) = 1$, by Theorem 2.6.

DEFINITION 2.2. If $(a, b) = 1$, then a and b are said to be *relatively prime.* More generally, if $(a_i, a_j) = 1$ for $i \neq j$, $1 \leq i \leq r$, $1 \leq j \leq r$, the integers a_1, a_2, . . . , a_r are said to be *pairwise relatively prime.*

A great deal more can be said about the special case when two numbers are relatively prime than is contained in Theorem 2.6 and Corollary 2.7. Further results appear in the following sequence of theorems, and we shall have occasion to return to the idea again and again.

THEOREM 2.8. If $a|bc$ and $(a, b) = 1$, then $a|c$.

Proof. Since $(a, b) = 1$, there exist integers x and y such that $1 = ax + by$. Therefore, $c = acx + bcy$. But $a|bc$, by hypothesis, so $a|(acx + bcy)$ by property (v) of Theorem 2.1. Therefore, $a|c$ and the proof is complete.

COROLLARY 2.9. If p is a prime and $p|bc$, then $p|b$, or $p|c$.

Proof. If $p|b$, there is nothing to show. If $p \nmid b$, then $(p, b) = 1$ since the only positive divisors of p are 1 and p itself. But then $p|c$, by Theorem 2.8.

COROLLARY 2.10. If p is a prime and $p|a_1a_2 \cdots a_n$, then $p|a_i$ for some i, $1 \leq i \leq n$.

This corollary can easily be proved by mathematical induction and the proof is left for the reader.

COROLLARY 2.11. If $p, p_1, p_2, \ldots, p_n$ are primes and $p|p_1p_2 \cdots p_n$, then $p = p_i$ for some i, $1 \leq i \leq n$.

Proof. By Corollary 2.10, $p|p_i$ for some i, $1 \le i \le n$. But $p \ne 1$ and the only positive divisors of p_i are 1 and p_i. Therefore, $p = p_i$ and the proof is complete.

THEOREM 2.12. If $(a, b_i) = 1$ for $i = 1, 2, \ldots, n$, then
$$(a, b_1 b_2 \ldots b_n) = 1.$$

Proof. Suppose that $(a, b_1 b_2 \cdots b_n) = d > 1$. Then, by Theorem 1.2, there exists a prime p such that $p|d$. Since $d|a$ and $d|b_1 b_2 \cdots b_n$, it follows from property (iv) of Theorem 2.1 that $p|a$ and $p|b_1 b_2 \cdots b_n$. Therefore, by Corollary 2.10, $p|b_i$ for some i, $1 \le i \le n$. But then $p|a$ and $p|b_i$, and this contradicts $(a, b_i) = 1$ for all $i = 1, 2, \ldots, n$. Therefore, it must be the case that $d = 1$.

THEOREM 2.13. If $a|c$, $b|c$, and $(a, b) = 1$, then $ab|c$.

Proof. Since $a|c$ and $b|c$, there exist integers r and s such that $ar = c = bs$. From this it follows that $b|ar$. But $(a, b) = 1$ and so, by Theorem 2.8, $b|r$. Thus, $bt = r$ for some t and $c = ar = abt$. Therefore, $ab|c$ and the proof is complete.

COROLLARY 2.14. If $m_1, m_2, \ldots, m_n$ are pairwise relatively prime and $m_i|a$ for $i = 1, 2, \ldots, n$, then $m|a$ where $m = m_1 m_2 \cdots m_n$.

Proof. The result is certainly true for $n = 1$. Suppose that it is also true for $n = k$ and consider the integers $m_1, m_2, \ldots, m_{k+1}$ with $(m_i, m_j) = 1$ for $i \ne j$, $1 \le i \le k+1, 1 \le j \le k+1$. By Theorem 2.12, $(m', m_{k+1}) = 1$ where $m' = m_1 m_2 \cdots m_k$, and by the induction assumption, $m'|a$. But then, by Theorem 2.13, $m' m_{k+1}|a$ and $m' m_{k+1} = m_1 m_2 \cdots m_{k+1}$. Thus, the result is true for all $n \ge 1$, by mathematical induction.

We close this section by proving a theorem due to Gabriel Lamé in 1844 which gives an upper bound on the number of steps needed to complete the Euclidean algorithm for computing (a, b). First we need to prove a small result about Fibonacci numbers.

LEMMA 2.15. Let $\alpha = (1 + \sqrt{5})/2$. Then $F_n > \alpha^{n-2}$ for $n \ge 3$.

Proof. Note that $F_3 = 2 > 1.618 \ldots = (1 + \sqrt{5})/2$ and that $F_4 = 3 > 2.618 \ldots = \{(1 + \sqrt{5})/2\}^2$. Thus, the result is true for $n = 3$ and $n = 4$. Assume that $F_k > \alpha^{k-2}$ and $F_{k+1} > \alpha^{k-1}$ for some fixed $k \ge 3$. Then
$$F_{k+2} = F_{k+1} + F_k > \alpha^{k-1} + \alpha^{k-2} = \alpha^{k-2}(\alpha + 1) = \alpha^k$$
since $\alpha + 1 = \alpha^2$. Thus, the result is true for all $n \ge 3$ by mathematical induction.

THEOREM 2.16. Let $a > b > 0$. The number of divisions needed to find (a, b) by the Euclidean algorithm is at most 5 times the number of decimal digits in b.

Proof. Referring to the set of equations describing the Euclidean algorithm at the beginning of Section 2.3, we note that we have used $k + 1$ divisions. Moreover,

$q_i \geq 1$ for $1 \leq i \leq k$ and $q_{k+1} \geq 2$ since $r_k < r_{k-1}$. As usual, let F_n denote the nth Fibonacci number. Then, by the equations at the top of page 43,

$$\begin{aligned} r_k &\geq 1 = F_2, \\ r_{k-1} &\geq 2r_k \geq 2 = F_3, \\ r_{k-2} &\geq r_{k-1} + r_k \geq F_3 + F_2 = F_4, \\ &\cdots\cdots\cdots, \\ r_1 &\geq r_2 + r_3 \geq F_k + F_{k-1} = F_{k+1}, \\ b &\geq r_1 + r_2 \geq F_{k+1} + F_k = F_{k+2}. \end{aligned}$$

Thus, if there are $k+1$ divisions, it follows that $b \geq F_{k+2} > \alpha^k$ for $k \geq 1$ by Lemma 2.15. Hence,

$$\log_{10} b > k \log_{10} \alpha > \frac{k}{5}$$

since $\log_{10} \alpha = 0.208\ldots$. Let r be the number of decimal digits in b. Then $b < 10^r$ and $\log_{10} b < r$. Thus, from above,

$$k < 5 \log_{10} b < 5r$$

and

$$k + 1 \leq 5r$$

since r and k are integers. This completes the proof.

COROLLARY 2.17. The number of bit operations needed to find (a, b) with $a > b > 0$ is $O((\log_2 a)^3)$.

Proof. Since $b < a$, it follows from Lamé's theorem that the number of divisions required to compute (a, b) is $O(\log_{10} b) = O(\log_2 b) = O(\log_2 a)$. Also, by Theorem 1.16, the number of bit operations required to perform each of these divisions is $O((\log_2 a)^2)$. Thus, (a, b) can be found in $O((\log_2 a)^2)O(\log_2 a) = O((\log_2 a)^3)$ bit operations, as claimed.

EXERCISES 2.3

1. **(a)** Compute (357, 629) and determine x and y such that

$$(357, 629) = 357x + 629y.$$

(b) Compute $(-357, 629)$ and find x and y such that

$$(-357, 629) = -357x + 629y.$$

2. **(a)** Compute (7700, 2233) and determine x and y such that

$$(7700, 2233) = 7700x + 2233y.$$

(b) Compute (7700, -2233) and determine x and y such that

$$(7700, -2233) = 7700x - 2233y.$$

3. If a is an integer, prove that $(14a + 3, 21a + 4) = 1$.

4. If $b \neq 0$, prove that $(0, b) = |b|$.

5. Prove that $b|a$ if and only if $(a, b) = |b|$.

6. If $b|c$, prove that $(a, b) = (a + c, b)$.
Hint: Let $d = (a, b)$, $e = (a + c, b)$ and show that $d|e$ and $e|d$.

7. If $(a, c) = 1$ and $b|c$, prove that $(a, b) = 1$.

8. If $(a, c) = 1$, prove that $(a, bc) = (a, b)$.

9. If $c > 0$, prove that $(ac, bc) = c(a, b)$.

10. If $(a, b) = 1$, prove that $(a + b, a - b) = 1$ or 2.
Hint: Suppose that $d = (a + b, a - b)$. Show that $d|2b$, $d|2a$, and use the result of Exercise 9.

11. If $(a, b) = 1$, prove that $(2a + b, a + 2b) = 1$ or 3.

12. If $d|mn$ and $(m, n) = 1$, prove that $d = d_1d_2$, where $d_1|m$, $d_2|n$ and $(d_1, d_2) = 1$.
Hint: Let $d_1 = (d, m)$.

13. If $(a, b) = (c, d) = 1$, $b > 0$, $d > 0$, and $a/b + c/d$ is an integer, prove that $b = d$.

14. Prove that the product of any three consecutive integers is divisible by 6.
Suggestion: Use Theorem 2.13 and Exercises 4 and 5 of Section 1.7.

15. If $(a, b) = r$, $(a, c) = s$, and $(b, c) = 1$, prove that $(a, bc) = rs$. Give an example to show that this need not be true if $(b, c) > 1$.

16. For the Fibonacci sequence (see Section 1.2), prove that $(F_n, F_{n+1}) = 1$ for every positive integer n.

17. For the Fibonacci sequence, prove that $(F_n, F_{n+3}) = 1$ or 2 for $n \geq 1$.
Hint: Let $d|(F_n, F_{n+3})$ and show that $d|2$.

***18.** In Exercise 17, $(F_n, F_{n+3}) = 2$ if and only if $2|F_n$. Show that $2|F_n$ if and only if $n = 3q$ for some positive integer q.
Hint: For the "if" part, note that $2 = F_3$ and use Exercise 19 of Section 1.4. For the "only if" part, deduce from Exercise 17 of Section 1.4 that $F_n = F_{3q-1}F_r + F_{3q}F_{r+1}$ for $n = 3q + r$ and argue by contradiction using the results of Exercises 16 and 7.

***19.** Exercise 18 can be generalized. For $m > 2$, show that $F_m|F_n$ if and only if $m|n$.
Hint: For the "only if" part of the proof, deduce from Exercise 17 of Section 1.4 that $F_n = F_{mq-1}F_r + F_{mq}F_{r+1}$, where $n = mq + r$ and again argue by contradiction using Exercises 16 and 7.

*20. Let $t \geq 2$ and suppose that m is the least positive integer such that $t|F_m$. Prove that $t|F_n$ if and only if $m|n$.
Note: That such an m always exists is guaranteed by Exercise 28 of Section 4.1.

*21. Let N_n be the integer whose decimal expansion consists of n consecutive ones as in Exercise 9 of Section 2.1. Show that $(N_n, N_m) = N_{(n,m)}$.

*22. If $(a, b) = 1$, and $a > b > 0$, prove that

$$(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$$

for any positive integers m and n.

Computer Exercises

23. Write a computer program to compute $d = (a, b)$ and to determine x and y such that $d = ax + by$ for any positive integers a and b.

24. Use your program to compute (F_m, F_n) for $1 \leq n < m \leq 35$, where F_n denotes the nth Fibonacci number. Make a conjecture on the basis of this computation and prove that your conjecture is correct.

2.4 THE LEAST COMMON MULTIPLE

If $a|m$ and $b|m$, then m is called a *common multiple* of a and b. Since division by zero is meaningless, it is clear that this definition has meaning only if a and b are both different from zero. In this case it is clear that ab and $-ab$ are both common multiples of a and b and that one of them is positive. Therefore, by the well-ordering principle, there must exist a least positive common multiple.

DEFINITION 2.3. If m is the smallest positive common multiple of a and b, it is called the *least common multiple* of a and b and is denoted by $[a, b]$.

In view of the preceding discussion, when we write $[a, b]$ we shall always understand that a and b are different from zero. The following two theorems provide alternative characterizations of the least common multiple as well as a method for computing it.

THEOREM 2.18. $m = [a, b]$ if and only if $m > 0$, $a|m$, $b|m$ and $m|n$ for every common multiple n of a and b.

Proof. Since we are discussing $[a, b]$, we tacitly assume that a and b are different from zero.

(i) Suppose, first, that $m = [a, b]$ and that n is any common multiple of a and b. By definition, $m > 0$, $a|m$, and $b|m$, so we have only to show that $m|n$. There is no loss in generality in assuming that n is positive, for if n were negative, we would consider $-n$. Since, by definition, m is the least positive common multiple of a and b,

it follows that $m \leq n$. By Theorem 1.9, there exist q and r with $0 \leq r < m$ such that $n = qm + r$. Then $r = n - qm$ and it follows from property (v) of Theorem 2.1 that r is a common multiple of a and b since both m and n are common multiples of a and b. If $r \neq 0$, this violates the given condition that m is the least common multiple. Therefore, $r = 0$ and $m|n$, as claimed.

(ii) Suppose that $m > 0$, $a|m$, $b|m$, and that $m|n$ for every common multiple n of a and b. Clearly, m is a positive common multiple of a and b, so we have only to show that it is the least positive common multiple. Since $m|n$, where n is any common multiple, it follows from Theorem 2.2 that $m \leq |n|$. Thus, m is the least positive common multiple of a and b and the proof is complete.

THEOREM 2.19. If $ab \neq 0$, then $[a, b] = |ab/(a, b)|$.

Proof. Let $d = (a, b)$, $a = Ad$, $b = Bd$, and $m = |ab/d|$. Then $m = |Ab| = |aB|$, so that $m > 0$, $a|m$, and $b|m$. If $a|n$ and $b|n$, then there exist r and s such that $ar = n = bs$. Therefore, $Adr = Bds$ and $Ar = Bs$. This implies that $A|Bs$. But $(A, B) = 1$ by Corollary 2.7, so, by Theorem 2.8, $A|s$ and there exists t such that $At = s$. But then $n = bs = Abt = \pm mt$, so $m|n$. Thus, m satisfies the conditions of Theorem 2.18 and $m = [a, b]$, as we were to prove.

In view of Theorem 2.19, the computation of the least common multiple of two nonzero integers can be made to depend on the computation of their greatest common divisor, which, in turn, can be computed by Euclid's algorithm. For example, since we found earlier that $(288, 51) = 3$, we now have that

$$[288, 51] = \frac{288 \cdot 51}{3} = 4896.$$

Of course, the ideas of greatest common divisor (g.c.d.) and least common multiple can be extended in a natural way to more than two numbers. Thus, if $a_1, a_2, \ldots, a_r$ are not all zero, they have a largest positive common divisor which we denote by $(a_1, a_2, \ldots, a_r)$. It can be shown that d is the g.c.d. of $a_1, a_2, \ldots, a_r$ if and only if $d > 0$, $d|a_i$, for $i = 1, 2, \ldots, r$, and $f|d$ for every common divisor f of $a_1, a_2, \ldots, a_r$. Also, it can be shown that d is the least positive integer of the form $a_1x_1 + a_2x_2 + \cdots + a_rx_r$. The integers $a_1, a_2, \ldots, a_r$ are said to be *relatively prime* in case $(a_1, a_2, \ldots, a_r) = 1$. As before,

$$(a_1, a_2, \ldots, a_r) = 1$$

if and only if there exist integers $x_1, x_2, \ldots, x_r$ such that

$$a_1x_1 + \cdots + a_rx_r = 1.$$

Similarly, if none of $a_1, a_2, \ldots, a_r$ are zero, they have a least positive common multiple which we denote by $[a_1, a_2, \ldots, a_r]$. It can be shown that $m = [a_1, a_2, \ldots, a_r]$ if and only if $m > 0$, $a_i|m$ for each $i = 1, 2, \ldots, r$, and $m|n$ for every common multiple n of the a's.

The calculation of the greatest common divisor and least common multiple of more than two integers can be accomplished in successive steps in accordance with the following theorems.

THEOREM 2.20. If none of $a_1, a_2, \ldots, a_r$ is zero, then

$$(a_1, a_2, \ldots, a_r) = ((a_1, \ldots, a_{r-1}), a_r).$$

Proof. Let $d = (a_1, a_2, \ldots, a_r)$ and $e = ((a_1, \ldots, a_{r-1}), a_r)$; then d and e are both positive. By Corollary 2.3, it suffices to show that $d|e$ and $e|d$. Since $d = (a_1, \ldots, a_r)$, $d|a_i$ for $i = 1, 2, \ldots, r$. Therefore, $d|(a_1, \ldots, a_{r-1})$ and $d|a_r$. But then $d|e$ by Theorem 2.5. On the other hand, $e|a_r$ and $e|(a_1, \ldots, a_{r-1})$. Therefore, $e|a_i$ for $1 \leq i \leq r$, so $e|d$. This completes the proof.

THEOREM 2.21. If none of $a_1, a_2, \ldots, a_r$ is zero, then

$$[a_1, a_2, \ldots, a_r] = [[a_1, \ldots, a_{r-1}], a_r].$$

The proof of this theorem, which is exactly analogous to that of Theorem 2.20, is left to the reader.

Theorems 2.20 and 2.21 provide a systematic method for computing the greatest common divisor and least common multiple of more than two integers. For example, to find (108, 84, 78) we first use the Euclidean algorithm to find that (108, 84) = 12 and that (12, 78) = 6. Hence, by Theorem 2.20, (108, 84, 78) = 6. Also, from the equations of the Euclidean algorithm used to compute (108, 84) = 12 and (12, 78) = 6, it is easy to find x_1, x_2, x_3 such that $6 = 108x_1 + 84x_2 + 78x_3$. These equations give $12 = 4 \cdot 84 - 3 \cdot 108$ and $6 = 78 - 6 \cdot 12$, which can be combined to give

$$\begin{aligned} 6 &= 78 - 6(4 \cdot 84 - 3 \cdot 108) \\ &= 18 \cdot 108 - 24 \cdot 84 + 78. \end{aligned}$$

Thus, we can take $x_1 = 18, x_2 = -24$, and $x_3 = 1$. As before, it is easy to see that x_1, x_2, and x_3 are not unique.

By Theorem 2.19,

$$[108, 84] = \frac{108 \cdot 84}{12} = 756.$$

Using the Euclidean algorithm, we find that (756, 78) = 6. Again, by Theorem 2.19,

$$[756, 78] = \frac{756 \cdot 78}{6} = 9828.$$

Therefore, by Theorem 2.21,

$$[108, 84, 78] = [756, 78] = 9828.$$

EXERCISES 2.4

1. Find the following.
   (a) [357, 629] **(b)** [−357, 629] **(c)** [299, 377]
2. Find (357, 629, 221) and determine x, y, and z such that
$$(357, 629, 221) = 357x + 629y + 221z.$$
3. Find [357, 629, 221].
4. Find (299, 377, 403) and x, y, and z such that
$$(299, 377, 403) = 299x + 377y + 403z.$$
5. Find [299, 377, 403].
6. If $c > 0$, prove that $[ac, bc] = c[a, b]$.
7. Prove that $a|b$ if and only if $[a, b] = |b|$.
8. For any integer n, prove that $[9n + 8, 6n + 5] = 54n^2 + 93n + 40$.
9. Find $(12n^2 + 16n + 6, 6n + 5)$ and $[12n^2 + 16n + 6, 6n + 5]$, where n is an integer.
10. Let $a_1, a_2, \ldots, a_r$ be nonzero integers. Let $d = a_1x_1 + a_2x_2 + \cdots + a_rx_r$ be the smallest positive linear combination of $a_1, a_2, \ldots, a_r$. Prove that
$$d = (a_1, a_2, \ldots, a_r).$$
11. Prove that $(a_1, a_2, \ldots, a_r) = 1$ if and only if there exist integers $x_1, x_2, \ldots, x_r$ such that $1 = a_1x_1 + a_2x_2 + \cdots + a_rx_r$.
12. Give an example to show that the equation
$$(a_1, a_2, \ldots, a_r)[a_1, a_2, \ldots, a_r] = a_1a_2 \cdots a_r$$
is not necessarily true.
13. Give an example to show that the equation of Exercise 12 is sometimes true. Can you discover under what conditions the equation is generally true?

Computer Exercise

14. Write a computer program to determine the positive integer solutions to the equation $y^2 - xy - x^2 = 1$ and $y^2 - xy - x^2 = -1$. Make a conjecture on the basis of the printout of your program. Try to prove at least part of your conjecture.

2.5 THE FUNDAMENTAL THEOREM OF ARITHMETIC

As shown in Theorem 1.2, every positive integer greater than 1 either is a prime or can be successively factored into a product of primes. For example, $36 = 4 \cdot 9 =$

$2 \cdot 2 \cdot 3 \cdot 3$ where 2 and 3 are primes. Again, $36 = 6 \cdot 6 = 2 \cdot 3 \cdot 2 \cdot 3$ and we see that the same prime factors occur in each case. Indeed, it is common experience that apart from the order in which the factors occur, factorization of an integer into a product of primes can be carried out in one and only one way. Common experience, however, is a poor substitute for proof. To illustrate this point, it is our present purpose to exhibit systems of numbers possessing many of the same properties as the set of positive integers, but where factorization into primes is not unique.

We begin by letting I denote the set of all positive integers, and considering the set T of all positive integers of the form $3k+1$, where k is a nonnegative integer. That is, $T = \{1, 4, 7, 10, 13, 16, 19, 22, 25, 28, \ldots\}$ consists of just those positive integers which leave a remainder of 1 when divided by 3. Since

$$(3r + 1)(3s + 1) = 3(3rs + r + s) + 1,$$

it follows that the product of any two elements of T is again an element of T or, in more technical terms, that T is *closed* with respect to multiplication. Also, since T is a subset of I, certain properties of I necessarily hold in T. Thus, we need no further argument to be sure that the commutative and associative laws for multiplication hold in T and that 1 is the multiplicative identity for T, just as it is for I.

In addition to the similarities already mentioned, it is clear that T also contains prime and composite numbers, just as I does. That is, some elements in T can be factored into products of other elements in T and some cannot. For example, $16 = 4 \cdot 4$ and $28 = 4 \cdot 7$, so 16 and 28 are composite in T. On the other hand, none of 4, 7, 10, 13, 19, 22, or 25 can be further factored in T and so are called primes in T. But the similarity between I and T ceases at this point since it is easy to see that factorization into primes in T is not unique. For example, $100 = 4 \cdot 25 = 10 \cdot 10$, yet 4, 10, and 25 are all prime in T. Of course, none of 4, 10, and 25 are prime in the ordinary sense, but they are prime in T and so we have a legitimate example of a multiplicative system where prime factorization is not unique.

Since T and I possess precisely the same multiplicative properties, it is apparent that some other property must be basic to unique factorization. Of course, one suspects that some additive property, or at least some property involving both addition and multiplication, may be the crux of the matter, and it is certainly true that I and T differ considerably in this respect. In fact, since

$$(3r + 1) + (3s + 1) = 3(r + s) + 2,$$

it is clear that T does not contain the sum of any two of its elements and so is not even closed with respect to addition.

If we consider additive properties as well as multiplicative properties, then, in addition to the laws already mentioned, it is well known that I is closed with respect to addition, that the commutative and associative laws for addition hold, and that the distributive law involving both addition and multiplication is valid in I. However, not even all of these properties are sufficient to guarantee unique factorization, as the following example shows.

We consider the set C of all complex numbers of the form $a + b\sqrt{5}i$, where a

and b are integers. Typical elements of C include such numbers as $2 + 3\sqrt{5}i$, $1 - \sqrt{5}i$, $2\sqrt{5}i = 0 + 2\sqrt{5}i$, and $4 = 4 + 0\sqrt{5}i$. In particular, we note that $a = a + 0\sqrt{5}i$, so that all integers are themselves members of C.

It is easy to see that the closure, commutative, and associative laws for both addition and multiplication hold in C, that the distributive law holds, and that one is the multiplicative identity. For example,

$$(a + b\sqrt{5}i) + (c + d\sqrt{5}i) = (a + c) + (b + d)\sqrt{5}i$$

and

$$(a + b\sqrt{5}i)(c + d\sqrt{5}i) = (ac - 5bd) + (ad + bc)\sqrt{5}i,$$

so that C is closed with respect to both addition and multiplication. The reader should check to see that the other properties hold as well.

Since we have closure under multiplication, it is obvious that C contains composite elements. Although not as easy to see, it is also true that some numbers are prime in C. Since $21 = 3 \cdot 7 = (1 + 2\sqrt{5}i)(1 - 2\sqrt{5}i)$, it will follow that prime factorization in C is not unique, provided we show that 3, 7, $1 + 2\sqrt{5}i$, and $1 - 2\sqrt{5}i$ are all prime in C.

To show that 3 is prime in C, we must show that it is impossible to find elements α and β in C, both different from ± 1, such that $3 = \alpha\beta$. This is most easily accomplished in the following way. If $\alpha = a + b\sqrt{5}i$ is any element of C, define $N(\alpha)$, called the *norm* of α, by the equation $N(\alpha) = a^2 + 5b^2$. The reader can easily show by direct calculation that for any two numbers α and β in C, $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$. Now, suppose that $\alpha = a + b\sqrt{5}i$, $\beta = c + d\sqrt{5}i$ with a, b, c, and d integers, and that $3 = \alpha\beta$. Then $9 = N(3) = N(\alpha) \cdot N(\beta) = (a^2 + 5b^2)(c^2 + 5d^2)$. Since this is an equation in integers and $1 \cdot 9 = 9 \cdot 1 = 3 \cdot 3$ are the only possibilities for factoring 9 in positive integers, it follows that $N(\alpha) = 1$, or $N(\beta) = 1$, or $N(\alpha) = N(\beta) = 3$. In the first case, it is clear that $a = \pm 1$, $b = 0$, so that $\alpha = \pm 1$ and we have the trivial factorizations $3 = 1 \cdot 3$ or $3 = (-1)(-3)$. Similarly, $N(\beta) = 1$ implies the trivial factorization $3 = 3 \cdot 1$ or $3 = (-3)(-1)$. Finally, $N(\alpha) = 3$ is impossible since if $|b| > 0$, then $N(\alpha) \geq 5$; if $b = 0$ and $a = \pm 1$, then $N(\alpha) = 1$; and if $b = 0$ and $|a| \geq 2$, then $N(\alpha) \geq 4$. Thus, it is impossible to find a nontrivial factorization of 3 in C and 3 is prime in C, as claimed.

Similar calculations which the reader can easily perform suffice to show that 7, $1 + 2\sqrt{5}i$, and $1 - 2\sqrt{5}i$ are also prime in C. Thus, we may finally say that unique factorization does not hold in C, even though C apparently satisfies most of the same arithmetical laws as does I, where prime factorization is unique.

The preceding examples clearly demonstrate the need for giving a careful and rigorous proof of the fact that prime factorization in I is unique, even though we are quite certain, by "common experience," that this is true. There have been cases where claims supported by equally firm convictions have been proved false.

THEOREM 2.22. (The Fundamental Theorem of Arithmetic). Every integer $n \geq 2$ is either a prime or a product of primes, and the product is unique apart from the order in which the factors appear.

Proof. Since the first part of the theorem is simply a restatement of Theorem 1.2, we have only to show that the representation of any integer greater than 1 as a product of primes is unique. Suppose that for some integer $a \geq 2$,

$$a = p_1 p_2 \cdot \cdot \cdot p_m = q_1 q_2 \cdot \cdot \cdot q_n,$$

where the p's and q's are primes, $m \geq 1$, and $n \geq 1$. It is no restriction to assume that $m \leq n$ and that

$$p_1 \leq p_2 \leq \cdot \cdot \cdot \leq p_m \quad \text{and} \quad q_1 \leq q_2 \leq \cdot \cdot \cdot \leq q_n.$$

Since the equality above implies that $p_1 | q_1 q_2 \cdot \cdot \cdot q_n$, it follows from Corollary 2.11 that $p_1 = q_i$ for some i with $1 \leq i \leq n$. This implies that $p_1 = q_i \geq q_1$. Similarly, it can be shown that $q_1 \geq p_1$, so, in fact, $q_1 = p_1$. Dividing these equal factors out of the initial equality, we obtain

$$p_2 p_3 \cdot \cdot \cdot p_m = q_2 q_3 \cdot \cdot \cdot q_n.$$

But the argument can now be repeated to show that $p_2 = q_2$ and, similarly, that $p_i = q_i$ for $i = 3, 4, \ldots, m$. At this stage, if m were less than n, one would have $1 = q_{m+1} q_{m+2} \cdot \cdot \cdot q_n$, which is clearly false since $q_i > 1$ for each i. Therefore, $m = n$, $p_i = q_i$ for each i, and the representation is unique, as claimed.

Since the primes into which an integer can be factored need not be distinct, it follows from the Fundamental Theorem of Arithmetic that each integer $a \geq 2$ can be represented as a product $a = \prod_{i=1}^{r} p_i^{a_i}$ of prime powers. This representation is called the *canonical representation* of a. Thus $2^2 \cdot 3$, $2^4 \cdot 3^4$, and $2^2 \cdot 5 \cdot 11$ are the canonical representations of 12, 1296, and 220 in that order. If, in a given problem, only one number is represented in this way, we usually require a_i to be positive for each i. However, for notational convenience when two or more numbers are involved, we sometimes allow some of the exponents to be zero. If $a_1 = 0$, for example, the prime p_1 simply does not occur in the canonical representation of a. This device makes it possible to write the canonical representation of any two positive integers so that they *appear* to involve the same prime factors even though they may, in fact, fail to have any nontrivial common factors. For example, we could write $12 = 2^2 \cdot 3 \cdot 5^0$ and $20 = 2^2 \cdot 3^0 \cdot 5$; and one could even write $1 = 2^0 \cdot 3^0 \cdot 5^0$. The usefulness of this device is apparent in the following important theorem.

THEOREM 2.23. Let $a = \prod_{i=1}^{r} p_i^{a_i}$ with $a_i > 0$ for each i be the canonical representation for a and let $b > 0$. Then $b | a$ if and only if $b = \prod_{i=1}^{r} p_i^{b_i}$ with $0 \leq b_i \leq a_i$ for each i.

Proof. If $b = \prod_{i=1}^{r} p_i^{b_i}$ with $0 \le b_i \le a_i$, then

$$\begin{aligned} a &= \prod_{i=1}^{r} p_i^{a_i} \\ &= \prod_{i=1}^{r} p_i^{a_i - b_i + b_i} \\ &= \prod_{i=1}^{r} p_i^{a_i - b_i} p_i^{b_i} \\ &= \prod_{i=1}^{r} p_i^{a_i - b_i} \cdot \prod_{i=1}^{r} p_i^{b_i} \\ &= c \cdot b, \end{aligned}$$

where $c = \prod_{i=1}^{r} p_i^{a_i - b_i}$ and $c \ge 1$ since $a_i - b_i \ge 0$ for each i. Therefore, $b|a$, as we wished to prove.

To prove the converse, suppose that $b|a$. Then, since there exists c such that $bc = a$, the canonical representation of a can be formed by taking the product of the canonical representations of b and c. (A canonical representation for a can be formed in this way, and since the canonical representation must be unique by Theorem 2.22, this must be *the* canonical representation.) Thus, the primes that appear in the canonical representations of b and c must be the same as those in the canonical representation of a; that is, $b = \prod_{i=1}^{r} p_i^{b_i}$ and $c = \prod_{i=1}^{r} p_i^{c_i}$ with $b_i \ge 0$ and $c_i \ge 0$. Since $bc = a$, it follows that $a_i = b_i + c_i$, so $a_i \ge b_i$. This completes the proof.

Theorem 2.23 makes it extremely easy to write down all the positive divisors of a positive integer once its canonical representation has been obtained. For example, since $72 = 2^3 \cdot 3^2$, the divisors of 72 are

$$\begin{array}{lll} 1 \cdot 1 & 1 \cdot 3 & 1 \cdot 3^2 \\ 2 \cdot 1 & 2 \cdot 3 & 2 \cdot 3^2 \\ 2^2 \cdot 1 & 2^2 \cdot 3 & 2^2 \cdot 3^2 \\ 2^3 \cdot 1 & 2^3 \cdot 3 & 2^3 \cdot 3^2. \end{array}$$

It may be noticed that there are $4 \cdot 3 = 12$ such divisors and that they are the terms in the expansion of the product $(1 + 2 + 2^2 + 2^3)(1 + 3 + 3^2)$. In fact, this product gives the *sum* of the positive divisors of 72. In general, if $a = \prod_{i=1}^{r} p_i^{a_i}$, it is clear that $\prod_{i=1}^{r} (a_i + 1)$ is the number of positive divisors of a and that the sum of these divisors is given by the product

$$\prod_{i=1}^{r} (1 + p_i + p_i^2 + \cdots + p_i^{a_i}) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

It is customary to denote the number of positive divisors of a by $\tau(a)$ and their sum by $\sigma(a)$. Thus, we have obtained the following theorem.

THEOREM 2.24. If $a = \prod_{i=1}^{r} p_i^{a_i}$ with $a_i > 0$ for each i is the canonical representation of a, then

$$\tau(a) = \prod_{i=1}^{r} (a_i + 1) \qquad \text{and} \qquad \sigma(a) = \prod_{i=1}^{r} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Also, $\tau(1) = \sigma(1) = 1$.

Canonical representations also make it very easy to find greatest common divisors and least common multiples.

THEOREM 2.25. If $a = \prod_{i=1}^{r} p_i^{a_i}$ and $b = \prod_{i=1}^{r} p_i^{b_i}$ and $a_i \geq 0$ and $b_i \geq 0$ for each i are the canonical representations of a and b, then

$$(a, b) = \prod_{i=1}^{r} p_i^{u_i} \qquad \text{and} \qquad [a, b] = \prod_{i=1}^{r} p_i^{v_i},$$

where u_i is the smaller of a_i and b_i and v_i is the larger of a_i and b_i for each i.

Proof. Let $d = \prod_{i=1}^{r} p_i^{u_i}$. Since u_i is the smaller of a_i and b_i, $u_i \leq a_i$ and $u_i \leq b_i$ for each i. Therefore, by Theorem 2.23, $d|a$ and $d|b$. Suppose that $f|a$ and $f|b$. Then $|f| = \prod_{i=1}^{r} p_i^{f_i}$ with $f_i \leq a_i$ and $f_i \leq b_i$ for each i. But since u_i is the smaller of a_i and b_i, this implies that $f_i \leq u_i$ for each i. Therefore, again by Theorem 2.23, $|f||d$, so $f|d$. Since $d > 0$, it follows from Theorem 2.5 that $\prod_{i=1}^{r} p_i^{u_i} = d = (a, b)$, as claimed.

To complete the proof, note that by definition of u_i and v_i, $a_i + b_i - u_i = v_i$. Thus, by Theorem 2.19,

$$\begin{aligned}
[a, b] &= \frac{ab}{(a, b)} \\
&= \frac{\prod_{i=1}^{r} p_i^{a_i} \cdot \prod_{i=1}^{r} p_i^{b_i}}{\prod_{i=1}^{r} p_i^{u_i}} \\
&= \prod_{i=1}^{r} p_i^{a_i+b_i-u_i} \\
&= \prod_{i=1}^{r} p_i^{v_i},
\end{aligned}$$

as claimed.

For example, since $1296 = 2^4 \cdot 3^4$ and $9720 = 2^3 \cdot 3^5 \cdot 5$, we immediately have that

$$(1296, 9720) = 2^3 \cdot 3^4 = 648$$

and

$$[1296, 9720] = 2^4 \cdot 3^5 \cdot 5 = 19{,}440.$$

EXERCISES 2.5

1. Find the canonical representation of each of the following numbers.
   (a) 4725 **(b)** 3718 **(c)** 3234
2. Find (4725, 3234) and [4725, 3234].
3. Find (3718, 3234) and [3718, 3234].
4. Find $\tau(4725)$ and $\sigma(4725)$.
5. Find $\tau(3718)$ and $\sigma(3718)$.
6. Find the sum of the squares of the positive divisors of 4725.
7. If $a = \prod_{i=1}^{r} p_i^{a_i}$ with $a_i > 0$ for each i is the canonical representation of a, deduce a formula for the sum of the squares of the positive divisors of a.
8. Let $a = \prod_{i=1}^{r} p_i^{a_i}$ with $a_i > 0$ for each i be the canonical representation of a. Prove that a is the square of an integer if and only if a_i is even for each i.
9. Show that the number of positive divisors of a positive integer a is odd if and only if a is the square of the integer.
10. Let $a = \prod_{i=1}^{r} p_i^{a_i}$ and $b = \prod_{i=1}^{r} p_i^{b_i}$ with $a_i \geq 0$, $b_i \geq 0$ for each i be the canonical representations of a and b. Prove that $(a, b) = 1$ if and only if $a_i b_i = 0$ for each i, that is, if and only if a_i or b_i is zero for each i.
11. If $a = \prod_{i=1}^{r} p_i^{a_i}$, $b = \prod_{i=1}^{r} p_i^{b_i}$, $c = \prod_{i=1}^{r} p_i^{c_i}$, with $a_i \geq 0$, $b_i \geq 0$, $c_i \geq 0$ are the canonical representation of a, b, and c, prove that $(a, b, c) = \prod_{i=1}^{r} p_i^{u_i}$ and $[a, b, c] = \prod_{i=1}^{r} p_i^{v_i}$, where u_i is the smallest of a_i, b_i, c_i and v_i is the largest of a_i, b_i, c_i for each i. This result could be extended in the same way to more than three integers.
12. State the most general conditions which assure that for $r \geq 3$,
$$(a_1, a_2, \ldots, a_r)[a_1, a_2, \ldots, a_r] = a_1 a_2 \cdots a_r.$$
13. Let a, b, c be positive integers.
   (a) Prove that $abc = (a, b, c)[(a, b), (a, c), (b, c)][a, b, c]$.
   (b) Prove that $abc = (a, b, c)[ab, bc, ac]$.
   (c) Prove that $abc = (ab, ac, bc)[a, b, c]$.
14. Find a result like any one of those in Exercise 13 for integers a, b, c, and d.
15. Let C be the set of all complex numbers of the form $a + b\sqrt{5}i$, where a and b are integers. Prove that 7, $1 + 2\sqrt{5}i$, and $1 - 2\sqrt{5}i$ are all prime in C.

Computer Exercise

16. For each n write a computer program to determine the minimum number of squares needed to write n as a sum of nonzero perfect squares. Execute the program for $1 \leq n \leq 200$ and print out the representations of each n as the sum of the minimum number of squares. Make a conjecture on the basis of the printout.

2.6 PYTHAGOREAN TRIPLES

Everyone is familiar with the fact that the triangle with sides 3, 4, and 5 is a right triangle, or, what is the same thing, that

$$3^2 + 4^2 = 5^2.$$

Only slightly less familiar is the fact that

$$5^2 + 12^2 = 13^2 \quad \text{and} \quad 8^2 + 15^2 = 17^2.$$

The problem we wish to consider here is that of finding all such triples of positive integers, called *Pythagorean triples.*

In the first place, it is clear that if a, b, c is a Pythagorean triple, then so is ka, kb, kc, for any integer k. Thus 6, 8, 10 and 9, 12, 15 are such triples, although neither is essentially different from the parent triple 3, 4, 5. In view of this fact, it is clear that our chore will be essentially completed if we find all Pythagorean triples whose elements are relatively prime. Such triples are called *primitive* Pythagorean triples.

Suppose, now, that x, y, z is a primitive Pythagorean triple so that $x^2 + y^2 = z^2$ and $(x, y, z) = 1$. We first show that this implies that $(x, y) = (x, z) = (y, z) = 1$. For example, if $(x, z) = d > 1$, then, by the Fundamental Theorem of Arithmetic, there exists a prime p such that $p|d$. Since $d|x$ and $d|z$, it follows that $p|x, p|z, p|z^2, p|x^2$, and $p|z^2 - x^2$. But $z^2 - x^2 = y^2$. Thus, $p|y^2$ and, by Corollary 2.9, $p|y$. This contradicts $(x, y, z) = 1$, so it must be the case that $(x, z) = 1$. Similarly, one can show that $(x, y) = (y, z) = 1$.

From the preceding paragraph, it follows that x and y cannot both be even. It is also true that they cannot both be odd. This follows from the fact, discussed in Section 1.7, that the square of an odd integer must be of the form $4q+ 1$ and the square of an even integer must be of the form $4q$, so that the square of an integer cannot be of the form $4q + 2$ or $4q + 3$. Thus, if x and y were both odd, then $x^2 = 4r + 1$ and $y^2 = 4s + 1$ for some r and s and $z^2 = x^2 + y^2 = 4(r + s) + 2$. This says that z^2 is of the form $4q + 2$, and this is impossible, as noted above. Hence, it must be the case that one of x and y is even, the other odd.

For definiteness, take x even and y odd. Of course, z^2 will then be of the form $4q + 1$, so z is also odd. Hence, $z - y$ and $z + y$ are both even and

$$x^2 = z^2 - y^2 = (z - y)(z + y).$$

Let $z - y = 2u$ and $z + y = 2v$. Then

$$z = v + u \quad \text{and} \quad y = v - u,$$

and it can be shown that one of u and v is even, the other odd, and that $(u, v) = 1$. For if $(u, v) = d > 1$, then $d|u$, $d|v$, so $d|z$ and $d|y$, in contradiction to the fact that $(z, y) = 1$. Moreover, if u and v are both odd, then z and y are even, and this is also a contradiction.

Since x is even, $x/2$ is an integer and

$$\left(\frac{x}{2}\right)^2 = \frac{z-y}{2} \cdot \frac{z+y}{2} = u \cdot v.$$

Let $x/2 = \prod_{i=1}^{r} p_i^{a_i}$ be the canonical representation of $x/2$. Then $u \cdot v = \prod_{i=1}^{r} p_i^{2a_i}$. It follows from Theorem 2.23 that $u = \prod_{i=1}^{r} p_i^{b_i}$, $v = \prod_{i=1}^{r} p_i^{c_i}$, $b_i \geq 0$, $c_i \geq 0$, and that $b_i + c_i = 2a_i$. If b_i and c_i are both different from zero for some i, then $p_i | u$ and $p_i | v$, in contradiction to the fact that $(u, v) = 1$. Thus, one of b_i and c_i is zero for each i. It follows that b_i and c_i are even for each i, say $b_i = 2u_i$ and $c_i = 2v_i$. Then $u = s^2$, $v = t^2$, where $s = \prod_{i=1}^{r} p_i^{u_i}$ and $t = \prod_{i=1}^{r} p_i^{v_i}$. Also $(s, t) = 1$ and one of s and t is even and the other odd, since the same statements are true about u and v.

Since $x > 0$ and $x = 2\sqrt{uv}$, it follows that if x, y, z is a primitive Pythagorean triple, then there exist integers s and t, with $(s, t) = 1$ and with one of s and t even and the other odd, such that

$$x = 2st,$$
$$y = t^2 - s^2,$$
$$z = t^2 + s^2.$$

Of course, we must also choose $t > s$ since $y > 0$.

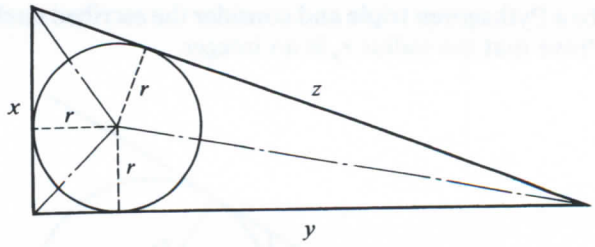
It is not difficult to prove that the converse of this result is also true. In the first place, if x, y, z are defined by the preceding formulas,

$$\begin{aligned} x^2 + y^2 &= (2st)^2 + (t^2 - s^2)^2 \\ &= t^4 + 2t^2s^2 + s^4 \\ &= (t^2 + s^2)^2 \\ &= z^2. \end{aligned}$$

Also, if $(s, t) = 1$ with one of s and t even and the other odd, then x is even and y and z are both odd. Suppose that $(y, z) = d > 1$. Then there exists a prime p such that $p | d$. Therefore, $p | y$, $p | z$, so p divides $z + y = 2t^2$ and $z - y = 2s^2$. But p must be odd since $p | z$ and z is odd. Therefore, $p | t^2$ and $p | s^2$, so $p | t$ and $p | s$ by Corollary 2.9. This contradicts $(s, t) = 1$, so it must be the case that $(y, z) = 1$. Similarly, it can be shown that $(x, y) = (x, z) = 1$. Therefore, x, y, z defined as above form a primitive Pythagorean triple and we have proved the following theorem.

THEOREM 2.26. The positive integers x, y, and z with x even form a primitive Pythagorean triple if and only if there exist integers s and t, with $s < t$, with $(s, t) = 1$ and with one of s and t even and the other odd, such that $x = 2st$, $y = t^2 - s^2$, and $z = t^2 + s^2$.

Since $A = xy/2$ and x is even, it is obvious that the area of the right triangle associated with a Pythagorean triple is always an integer. It is interesting that the inradius of the associated right triangle also is always an integer. This is easily seen by computing the area of the triangle shown in two different ways.



Suppose that x, y, z is a primitive Pythagorean triple so that $x = 2st$, $y = t^2 - s^2$, and $z = t^2 + s^2$. Then, if r is the inradius,

$$A = \frac{xy}{2} = \frac{rx}{2} + \frac{ry}{2} + \frac{rz}{2}$$

and

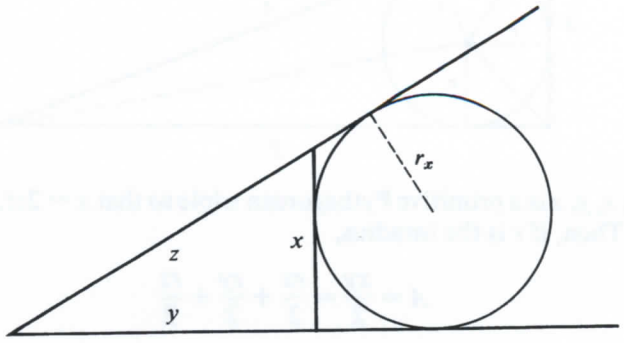
$$\begin{aligned} r = \frac{xy}{x+y+z} &= \frac{2st(t^2 - s^2)}{2st + (t^2 - s^2) + (t^2 + s^2)} \\ &= \frac{2st(t-s)(t+s)}{2t(s+t)} \\ &= s(t-s), \end{aligned}$$

which is an integer. If x, y, z is not a primitive triple, then $x = k \cdot 2st$, $y = k(t^2 - s^2)$, $z = k(t^2 + s^2)$ for some k and the argument still holds.

EXERCISES 2.6

1. Construct a table of primitive Pythagorean triples for the following values of (s, t): (1, 2), (1, 4), (2, 3), (1, 6), (2, 5), (3, 4), (1, 8), (2, 7), and (4, 5).
2. The table of Exercise 1 suggests that one of the numbers in any primitive Pythagorean triple is divisible by 4, one (not necessarily a different one) is divisible by 3, and one (again not necessarily different) is divisible by 5. Prove that this is so.
   Hint: By Theorem 1.9, every integer can be written in the form $3q$, $3q + 1$, or $3q + 2$. Similarly, any integer is of the form $5q$, $5q + 1$, $5q + 2$, $5q + 3$, or $5q + 4$.
3. Give values of x, y, z such that $(x, y, z) = 1$ and yet $(x, y) > 1$, $(x, z) > 1$, and $(y, z) > 1$.
4. If $x^2 + y^2 = z^2$ and $(x, y, z) = 1$, prove that $(x, y) = (y, z) = 1$.
5. If $(s, t) = 1$ and one of s and t is even, the other odd, prove that $(x, y) = (x, z) = 1$, where $x = 2st$, $y = t^2 - s^2$, and $z = t^2 + s^2$.

6. Let x, y, z be a Pythagoren triple and consider the escribed circle as shown in the diagram. Prove that the radius r_x is an integer.



Hint: Calculate the area of the triangle in two different ways.

7. Prove that the radii r_y and r_z of the other two escribed circles for the triangle of Exercise 6 also have integral values.
8. Show that (3, 4, 5) is the only primitive Pythagorean triple consisting of consecutive integers.
9. Show that the only Pythagorean triples in arithmetic progression are of the form $(3k, 4k, 5k)$ for $k \geq 1$.
10. Show that any positive odd integer can be the side of a primitive Pythagorean triangle whose other side and hypotenuse are consecutive integers.
11. Prove that if the sum of two consecutive integers is a square, then the smaller of the two integers is a side and the larger of the two integers is the hypotenuse of a primitive Pythagorean triangle.

Computer Exercise

12. Write a computer program to find all Pythagorean triples (x, y, z) such that $|x - y| = 1$. Note that this implies that $x = y \pm 1$ and hence that the triple found is primitive. Thus, $x = 2st$, $y = t^2 - s^2$, and $z = t^2 + s^2$ for suitable integers s and t with $t > s$, as noted above. Print a table of values of t, s, x, y, and z ordered by increasing values of z. Carefully consider this table and make a conjecture concerning the values of t and s that generate the triples found.

2.7 THE GREATEST INTEGER FUNCTION

The greatest integer function is frequently quite useful in treating number-theoretic problems. In this section we define the function, develop its principal properties, and exhibit some interesting and surprising applications. The reader should note that we continue to use small Latin letters to represent integers.

DEFINITION 2.4. If α is a real number, then $[\alpha]$ denotes the *greatest integer not exceeding* α. Alternatively, $[\alpha]$ is the integer satisfying the inequality

$$[\alpha] \leq \alpha < [\alpha] + 1.$$

THEOREM 2.27. In the following, α, β, and θ denote real numbers.

(i) $\alpha - 1 < [\alpha] \leq \alpha$
(ii) If $a \leq \alpha$, then $a \leq [\alpha]$.
(iii) If $a > \alpha$, then $a \geq [\alpha] + 1 > [\alpha]$.
(iv) If $\alpha \leq \beta$, then $[\alpha] \leq [\beta]$.
(v) If $\theta = \alpha - [\alpha]$, then $0 \leq \theta < 1$.
(vi) If $\alpha = n + \theta$ with $0 \leq \theta < 1$, then $n = [\alpha]$.
(vii) For any integer n, $[\alpha + n] = [\alpha] + n$.
(viii) If $a = bq + r$ with $0 \leq r < b$, then $q = [a/b]$.

Proof. (i) The inequality $\alpha - 1 < [\alpha] \leq \alpha$ is simply a restatement of the defining inequality for $[\alpha]$.

(ii) If $a + 1 > \alpha$, then $a \leq \alpha < a + 1$ and $a = [\alpha]$ by Definition 2.4. If $a + 1 \not> \alpha$, then $a + 1 \leq \alpha$ and $a \leq \alpha - 1 < [\alpha]$, by part (i).

(iii) By definition, $[\alpha] \leq \alpha$. Since $a > \alpha$, it follows that $a > [\alpha]$. Thus, $a \geq [\alpha] + 1$ since a and $[\alpha]$ are both integers.

(iv) By definition, $[\alpha] \leq \alpha$. Therefore, since $\alpha \leq \beta$, it follows that $[\alpha] \leq \beta$. But $[\alpha]$ is an integer and so, by part (ii), $[\alpha] \leq [\beta]$.

(v) The inequality $0 \leq \alpha - [\alpha] < 1$ follows immediately from part (i). Thus, $0 \leq \theta < 1$, since $\theta = \alpha - [\alpha]$.

(vi) Since $0 \leq \theta < 1$ and $\alpha = n + \theta$, it follows that $n \leq \alpha < n + 1$. But then $n = [\alpha]$ by Definition 2.4.

(vii) By part (v), $\alpha = [\alpha] + \theta$ with $0 \leq \theta < 1$. Therefore, $\alpha + n = [\alpha] + n + \theta$ and $[\alpha + n] = [\alpha] + n$ by part (vi).

(viii) Since $a = bq + r$ with $0 \leq r < b$, it follows that

$$\frac{a}{b} = q + \frac{r}{b}$$

with $0 \leq r/b < 1$. Therefore, by part (vi), $q = [a/b]$.

THEOREM 2.28. For any real number α and any integer $n > 0$,

$$\left[\frac{[\alpha]}{n}\right] = \left[\frac{\alpha}{n}\right].$$

Proof. By definition

$$\left[\frac{\alpha}{n}\right] \leq \frac{\alpha}{n} < \left[\frac{\alpha}{n}\right] + 1.$$

Therefore,

$$n \cdot \left[\frac{\alpha}{n}\right] \leq \alpha < n \cdot \left[\frac{\alpha}{n}\right] + n,$$

and it follows from properties (i) and (iii) of Theorem 2.27 that

$$n \cdot \left[\frac{\alpha}{n}\right] \leq [\alpha] < n \cdot \left[\frac{\alpha}{n}\right] + n.$$

But this implies that

$$\left[\frac{\alpha}{n}\right] \leq \frac{[\alpha]}{n} < \left[\frac{\alpha}{n}\right] + 1,$$

so

$$\left[\frac{\alpha}{n}\right] = \left[\frac{[\alpha]}{n}\right]$$

by Definition 2.4, since $[\alpha/n]$ is an integer.

DEFINITION 2.5. Let p be any prime and n any positive integer. If $p^f | n$ and $p^{f+1} \nmid n$, we say that p^f *exactly divides* n and write $p^f \| n$.

An alternative way of expressing Definition 2.4 is to say that $p^f \| n$ if and only if p^f appears in the canonical representation of n. That is, if $n = \prod_{i=1}^{r} p_i^{n_i}$ is the canonical representation of n, than $p^{n_i} \| n$ for each i. Again one can say that $p^f \| n$ if and only if p^f is the highest power of p dividing n. Of course, if $p \nmid n$, then $f = 0$ and we could still write $p^0 \| n$. As we will see immediately, this notational device is concise and useful.

THEOREM 2.29. If n is a positive integer and p is a prime, then $p^e \| n!$, where

$$e = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^r}\right]$$

and r is determined by n by the inequality $p^r \leq n < p^{r+1}$.

Proof. For a given integer k, the multiples of p^k that do not exceed n are p^k, $2p^k$, . . . , qp^k, where q is the largest integer such that $qp^k \leq n$. But this says that q is the largest integer not exceeding n/p^k, so that $q = [n/p^k]$. Thus, $[n/p^k]$ gives the number of positive multiples of p^k that do not exceed n. Now, if $1 \leq m \leq n$, then $m = qp^k$ with $(q, p) = 1$, $0 \leq k \leq r$, and m contributes precisely k to the total exponent e with which p appears in the canonical representation of $n!$ Moreover, m is counted precisely k times by the sum

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^r}\right],$$

once as a multiple of p, once as a multiple of p^2, . . . , once as a multiple of p^k, and no more. Of course, if $k = 0$, then m is not counted in the sum. Therefore, the sum

above accounts exactly for the contribution of each m between 1 and n to the exponent e, as claimed.

As an example of Theorem 2.29, consider the case for $n = 28$, $p = 3$. For $0 \le k \le 3$, let S_k denote the set of integers m with $1 \le m \le 28$ of the form $m = q \cdot 3^k$, $(q, 3) = 1$. Thus,

$$S_0 = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 28\},$$
$$S_1 = \{3, 6, 12, 15, 21, 24\}$$
$$S_2 = \{9, 18\},$$
$$S_3 = \{27\},$$

and this accounts for all the integers n, $1 \le n \le 28$, each appearing precisely once. Clearly, each element of S_0 contributes nothing to the exponent e with which 3 appears in the canonical representation of 28! Each element of S_1 contributes 1 to e, each element of S_2 contributes 2, and each element of S_3 contributes 3. Thus, in this case

$$e = 6 + 4 + 3 = 13.$$

Moreover, $[28/3] = 9$, the number of elements in S_1, S_2, and S_3; $[28/9] = 3$, the number of elements in S_2 and S_3; $[28/27] = 1$, the number of elements in S_3; and

$$9 + 3 + 1 = 13 = e.$$

Now, by Theorem 2.28,

$$\left[\frac{n}{p^2}\right] = \left[\frac{[n/p]}{p}\right],$$
$$\left[\frac{n}{p^3}\right] = \left[\frac{[n/p^2]}{p}\right],$$
$$\cdots\cdots\cdots$$

Also, by property (viii) of Theorem 2.27, $[n/p]$ is the quotient obtained when n is divided by p, $\left[\frac{[n/p]}{p}\right]$ is the quotient obtained when $[n/p]$ is divided by p, and so on. Thus, the work of determining the exponent of p in the canonical representation of $n!$ can be conveniently arranged as a sequence of divisions by p, the sum of the successive quotients yielding the desired exponent. For example, for $p = 3$ and $n = 28$, one would have

$$\begin{array}{r|l} 3 & 28 \\ 3 & 9 \\ 3 & 3 \\ 3 & 1 \\ & 0, \end{array}$$

where 28 is divided by 3, and then each successive quotient (ignoring remainders) is divided by 3 until a quotient of 0 is obtained. Thus, $[28/3] = 9$, $[28/3^2] = 3$, $[28/3^3] = 1$, and the desired exponent is 13, as before.

The preceding computation of the exponent of 3 in the canonical representation of 28! bears a marked resemblance to the calculation of the digits in the positional representation of 28 to base 3. That this resemblance is more than superficial is shown by the following theorem.

THEOREM 2.30. If p is prime, if

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_r p^r$$

with $a_r \neq 0$ and $0 \leq a_i < p$ for each i, and if $p^e \| n!$, then

$$e = \frac{n - (a_0 + a_1 + \cdots + a_r)}{p - 1}.$$

Proof. Since

$$n = a_0 + a_1 p + \cdots + a_r p^r$$

with $a_r \neq 0$ and $0 \leq a_i < p$ for each i, it is clear that

$$\left[\frac{n}{p}\right] = a_1 + a_2 p + \cdots + a_r p^{r-1},$$

$$\left[\frac{n}{p^2}\right] = a_2 + a_3 p + \cdots + a_r p^{r-2},$$

$$\cdots\cdots\cdots$$

$$\left[\frac{n}{p^r}\right] = a_r.$$

From these equations, it readily follows that

$$a_0 + p\left[\frac{n}{p}\right] = n,$$

$$a_1 + p\left[\frac{n}{p^2}\right] = \left[\frac{n}{p}\right],$$

$$a_2 + p\left[\frac{n}{p^3}\right] = \left[\frac{n}{p^2}\right],$$

$$\cdots\cdots$$

$$a_{r-1} + p\left[\frac{n}{p^r}\right] = \left[\frac{n}{p^{r-1}}\right],$$

$$a_r = \left[\frac{n}{p^r}\right].$$

If we now add these equations and make use of the fact that

$$e = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^r}\right],$$

we obtain

$$(a_0 + a_1 + \cdots + a_r) + pe = n + e,$$

from which the desired result immediately follows.

Note that $28_{10} = 1001_3$. Therefore, using the formula of Theorem 2.30, we again obtain

$$e = \frac{28 - (1 + 0 + 0 + 1)}{3 - 1} = 13$$

as the exponent of 3 such that $3^e \| 28!$

In computer science, it is typical to denote $[\alpha]$ by the symbol $\lfloor \alpha \rfloor$ and to denote the least integer not less than α by $\lceil \alpha \rceil$. The notation used here is standard in mathematics and the reader should understand both. Note, by the way, that $\lceil \alpha \rceil = -[-\alpha]$, as the reader is asked to show in Exercise 3 below. Thus, the least integer notation, $\lceil \alpha \rceil$, is actually not necessary. However, it is regularly used in computer science and should be familiar to all students of both mathematics and computer science.

EXERCISES 2.7

1. Evaluate the following.
   (a) $[2.7]$ **(b)** $[-3.5]$ **(c)** $[-\sqrt{2}]$ **(d)** $[\frac{75}{4}]$
   (e) $-[-2.7]$ **(f)** $-[3.5]$ **(g)** $-[\sqrt{2}]$ **(h)** $-[-\frac{75}{4}]$
   (i) $[2.7 + 0.5]$ **(j)** $[-3.5 + 0.5]$ **(k)** $[-\sqrt{2} + 0.5]$ **(l)** $[\frac{75}{4} + \frac{1}{2}]$
2. **(a)** Under what conditions is $[\alpha] + [\alpha] = [2\alpha]$?
   (b) Under what conditions is $[\alpha] + [-\alpha] \neq 0$?
3. Prove that $-[-\alpha]$ is the least integer not less than α, that is, that $-[-\alpha] = \lceil \alpha \rceil$.
4. Prove that no integer is nearer α than $[\alpha + \frac{1}{2}]$. If two integers are equally near, show that $[\alpha + \frac{1}{2}]$ is the larger of the two integers.
5. Prove that no integer is nearer α than $-[-\alpha + \frac{1}{2}]$. If two integers are equally near α, show that $-[-\alpha + \frac{1}{2}]$ is the smaller of the two integers.
6. Prove that $[\alpha] + [\alpha + \frac{1}{2}] = [2\alpha]$ for every real number α.
   Hint: $\alpha = [n] + \theta$ with $0 \leq \theta < 1$. Consider two cases: $0 \leq \theta < \frac{1}{2}$ and $\frac{1}{2} \leq \theta < 1$.
7. Prove that $[\alpha] + [\alpha + \frac{1}{3}] + [\alpha + \frac{2}{3}] = [3\alpha]$ for every real number α.

8. Prove that

$$[\alpha] + \left[\alpha + \frac{1}{k}\right] + \left[\alpha + \frac{2}{k}\right] + \cdots + \left[\alpha + \frac{k-1}{k}\right] = [k\alpha]$$

for every real number α and any integer $k \geq 1$.
Hint: $\alpha = [\alpha] + \theta$ with $0 \leq \theta < 1$ and there exists r with $0 \leq r < k$ such that $r/k \leq \theta < (r+1)/k$.

9. Find the exponent e such that $3^e \| 91!$

10. Show that 3 does not divide the binomial coefficient $\binom{91}{10}$.

11. Find the highest power of 10 that divides 91!

12. If α and β are real numbers, prove that

$$[\alpha] + [\beta] \leq [\alpha + \beta].$$

Hint: Use property (ii) of Theorem 2.27.

13. Use the result of Exercise 12 to prove that

$$\frac{(a+b)!}{a!b!}$$

is an integer for any positive integers a and b.

14. Prove that the product of any k consecutive positive integers is divisible by $k!$.

15. Let a and b be positive integers and suppose that $a = \sum_{i=0}^{r} a_k p^i$, $b = \sum_{i=0}^{r} b_i p^i$, and $a + b = \sum_{i=0}^{r} c_i p^i$, respectively, are the representations of a, b, and $a + b$ to the base p. If $p^f \| \binom{a+b}{a}$, show that $f = \sum_{i=0}^{r} (a_i + b_i - c_i)/(p-1)$.

16. Let a, b, $a + b$, p and f be as in Exercise 15. Show that f is the sum of the carries one makes when adding a to b in base p.
Hint: Let $d_0, d_1, \ldots, d_r$ be the carries in the aforementioned addition and note that $a_0 + b_0 = c_0 + d_0 p$, $d_0 + a_1 + b_1 = c_1 + d_1 p$, $\ldots$, $d_{r-1} + a_r + b_r = c_r + d_r p$. Note that $d_r = 0$.

17. Suppose that we number the rows of Pascal's triangle starting with zero so that the zeroth row consists of a single 1, the first row consists of two ones, the second row is the triple, 1, 2, 1 in that order, and so on. Show that the number of odd entries in the nth row of Pascal's triangle is 2^s, where s is the number of 1's in the positional representation of n to base 2.

18. It is only natural to extend Exercise 17 and ask how many entries in the nth row of Pascal's triangle are not divisible by a given prime p. If $n = \sum_{i=0}^{r} a_i p^i$ is the positional representation of n to base p, show that the number in question is $\prod_{i=0}^{r} (a_i + 1)$.

19. If p is a prime and $p^\alpha \| n$, prove that $p \nmid \binom{n}{p^\alpha}$.

20. Let $S = \{s_1, s_2, \ldots, s_m\}$ be a set of m nonnegative integers, and for each $i \geq 1$, let $f(i)$ denote the number of s_j in S for which $s_j \geq i$. Then $\sum_{j=1}^{m} s_j = \sum_{i=1}^{\infty} f(i)$.

(a) Illustrate the result for the set

$$S = \{3, 1, 5, 2\}.$$

(b) Prove the equality claimed.

***21.** Use the result of Exercise 20 to give an alternative proof of Theorem 2.27.
Hint: For each j, with $1 \leq j \leq n$, let s_j be the largest integer such that $p^{s_j} | j$. Then $e = \sum_{j=1}^{n} s_j = \sum_{i=1}^{\infty} f(i)$ and it is only necessary to argue that $f(i) = [n/p^i]$ for each i.

***22.** If $n \geq 0$, $\alpha = (1 + \sqrt{5})/2$, and F_n is the nth Fibonacci number, prove that

$$F_n = \left[\frac{\alpha^n}{\sqrt{5}} + \frac{1}{2}\right],$$

that is, that F_n is the integer nearest to $\alpha^n/\sqrt{5}$.
Hint: Note that $|(1 - \sqrt{5})/2| < 1$ and use Binet's formula developed in Exercise 13 of Section 1.4.

***23.** For $n \geq 2$, prove that $L_n = [\alpha^n + \frac{1}{2}]$ where L_n is the nth Lucas number.
Hint: See Exercise 14 of Section 1.4.

***24.** For $n \geq 2$, prove that $F_{n+1} = [\alpha F_n + \frac{1}{2}]$.

***25.** For $n \geq 4$, prove that $L_{n+1} = [\alpha L_n + \frac{1}{2}]$.

***26.** For $n \geq 0$, prove that

$$F_{n+1} = \sum_{i=0}^{[n/2]} \binom{n-i}{i}.$$

Hint: Consider the two cases $n = 2m + 1$ and $n = 2m + 2$ and prove them simultaneously by induction on m.

Computer Exercises

27. Write a computer program to generate and print Pascal's triangle.

28. Write a computer program to determine and print the product of the six entries surrounding any given entry in Pascal's triangle. Make a conjecture based on the printout of your program.

29. Try to generalize your conjecture in Exercise 28. Write a program to test special cases of your more general conjecture.

30. Let $a_1, a_2, a_3, a_4, a_5, a_6$ be the six entries in order around any given entry in Pascal's triangle. Write a program to calculate and print (a_1, a_3, a_5) and (a_2, a_4, a_6) for any given a. Make a conjecture based on the printout of this program.

3

Prime Numbers

The study of prime numbers naturally begins with the problem of determining whether a given integer n is prime or composite. Innocent as it may seem, this problem has no simple general solution, and we shall have to be content with partial answers. In view of the Fundamental Theorem of Arithmetic, it is clear that in any given case, the determination could be made by successively dividing the integer in question by each of the primes that precede it, provided that these primes are known. In fact, since it is evident that each composite positive integer must have a nontrivial factor not exceeding its own square root, the answer could be found for any n by successively dividing by each of the primes not exceeding $\sqrt{n}$. This greatly reduces the amount of work that must be done, but the process is still not feasible for extremely large values of n since the primes are not known much beyond 10^7.

3.1 THE SIEVE OF ERATOSTHENES

A simple and ingenious approach to the problem which enables one to find all the primes up to any prescribed limit is the one called the *Sieve of Erathosthenes,* after the Greek mathematician Eratosthenes (276 – 194 B.C.). This method consists of writing down all the integers from 2 up to the given limit n and then sieving out, as it were, the composite numbers. We note first that 2 is the smallest prime and that the multiples of 2,

$$2 \cdot 2, 2 \cdot 3, 2 \cdot 4, \ldots, 2k, \ldots,$$

occur in the list of integers at intervals of two following 2. Thus, if we strike from the list every second number after 2, we "sieve out" all multiples of 2 not exceeding n, and

we retain only multiples of larger primes. Now 3, the next largest integer not struck out, is clearly a prime since it is not a multiple of the only prime smaller than itself. Again, the multiples of 3 occur in the list of integers at intervals of three following 3, so we now strike out each of these numbers not yet deleted as multiples of 2. The next number not already deleted must also be a prime, since it is not a multiple of 2 or 3, the only primes that precede it. Thus, 5 is a prime and every fifth number after 5 must be deleted as a multiple of 5. Since every composite number must have a prime factor not exceeding its own square root, every composite number in our list must have a prime factor not exceeding $\sqrt{n}$. Thus, by the time we have deleted all multiples of all primes not exceeding $\sqrt{n}$, we shall have sieved out all composite numbers and those that remain will be *all* of the primes not exceeding n.

The table that follows shows the completed sieve for $n = 200$. Note that since $17^2 = 289$, the process is completed by the time all multiples of 13 have been struck from the list. The prime numbers have been circled to make them stand out in the table.

THE SIEVE OF ERATOSTHENES FOR $n = 200$

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	157	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	163	~~164~~	~~165~~	~~166~~	167	~~168~~	~~169~~	~~170~~
~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	193	~~194~~	~~195~~	~~196~~	197	~~198~~	199	~~200~~

Variations on the sieve method still provide the most effective means for computing factor tables and tables of prime numbers. Probably the best such tables (and certainly the best accessible) are those by D. N. Lehmer [Carnegie Institution of Washington, D.C., Publications No. 105 (1909) and No. 165 (1914); New York: Hafner Publishing Company, 1956], which extend to somewhat beyond 10 million. Unpublished tables by J. P. Kulik (1773–1863) in possession of the Academy of Sciences of Vienna extend up to 100 million, but there is some doubt as to their accuracy.

For easy reference in connection with material in this text, a table of primes less than 10,000 is given on pages 235–238 and a table of complete factorizations of positive integers less than 1000 is given on pages 239–243.

3.2 THE INFINITUDE OF PRIMES

Careful study of the tables of primes suggests many interesting conjectures, some of which have been proved, whereas others still resist attack. For example, in the first five groups of 1000 positive integers there are, respectively,

168, 135, 127, 120, and 119

primes. However, if we skip over to the last five groups of 1000 integers preceding 10,000,000, we find that they contain

62, 58, 67, 64, and 53

primes, respectively. This suggests that the primes occur less and less frequently among the larger integers, and it also suggests that there is no end to the sequence of primes. It is, in fact, relatively easy to prove that there are infinitely many primes. Many such proofs exist, and the first proof is due to Euclid (?330–265 B.C.). It is also possible to prove that the primes occur less and less frequently among the larger integers, but the proofs are much more difficult. The first results along this line were obtained by the Russian mathematician P. L. Tchebychef in 1850. We consider Tchebychef's work in Section 3.3. The proof of the following theorem is a variant of that of Euclid.

THEOREM 3.1. There are infinitely many primes.

Proof. We first note that some primes do exist, so that the following argument is not vacuous.

Suppose that there are only a finite number of primes, say $p_1, p_2, \ldots, p_r$, and consider the integer $n = p_1 p_2 \cdots p_r + 1$. Clearly, $n > p_i$ for $i = 1, 2, \ldots, r$, so n must be composite. By the Fundamental Theorem of Arithmetic, n must have prime divisors. Thus, $p_i | n$ for some i. But then $p_i | 1$, and this is impossible. Therefore, there must be infinitely many primes.

A glance at the table on page 71 shows that except for 2 and 5, all the primes occur in the first, third, seventh, and ninth columns of the table and that there are nearly the same number of primes in each column. Larger tables show that this trend continues, so that one might reasonably guess that if the table on page 71 were extended ad infinitum, there would be infinitely many primes in each of these columns. More neatly put, one might guess that there are infinitely many primes of the form $10k + 1$, infinitely many of the form $10k + 3$, infinitely many of the form $10k + 7$, and infinitely many of the form $10k + 9$. Similarly, if the primes are arranged according to divisibility by 4, all except the prime 2 are of the form $4k + 1$ or $4k + 3$ and there seem to be about equally many of each type. Thus, one might reasonably guess that there are infinitely many primes of the form $4k + 1$ and infinitely many of the form $4k + 3$. The fact is that all these guesses are correct; the results mentioned are all special cases of a most remarkable theorem proved by G. L. Dirichlet in 1837. The proof, which depends on the analytic methods of complex function theory, is much too difficult for inclusion here, so we must be content with just the statement of the theorem.

THEOREM 3.2. (Dirichlet's Theorem). If $(a, d) = 1$ with $a > 0$ and $d > 0$, then there are infinitely many primes of the form $a + kd$.

It is clear that the conditions of Dirichlet's theorem are necessary since if $(a, d) = r > 1$, then $r|(a + kd)$ for every k and $a + kd$ is never a prime for $k \geq 1$. The difficulty arises in showing that the conditions are sufficient. However, certain special cases of Dirichlet's theorem can be handled by arguments similar to that of Theorem 3.1. The following theorem provides an example.

Note that, by the division algorithm, all odd primes must be of the form $4k + 1$ or $4k + 3$. But $4k + 3 = 4(k + 1) - 1$ is of the form $4k - 1$. Thus, it is also true that all odd primes must be of the form $4k \pm 1$.

THEOREM 3.3. There are infinitely many primes of the form $4k - 1$.

Proof. Since 3, 7, and 11 are of this form, the following argument is not vacuous. Suppose that there are only finitely many primes of this form, say $p_1, p_2, \ldots, p_r$, and consider the number

$$m = 4p_1p_2 \cdots p_r - 1.$$

Since m is of the form $4k - 1$ and $m > p_i$ for each i, it follows that m is composite and must have prime factors of the form $4k + 1$ or $4k - 1$. Since the product of any two numbers of the form $4k + 1$ is again of that form, it follows that m has at least one prime divisor of the form $4k - 1$. Thus, $p_i|m$ for some i. But then $p_i|1$, and this is impossible. Therefore, there must be infinitely many primes of the form $4k - 1$.

Another conjecture suggested by the tables of primes is that there are infinitely many so-called *twin primes,* that is, pairs p and $p + 2$ which are *both* primes. The

table on page 71 contains 15 such pairs, and more extensive tables show that these pairs continue to appear. There are, in fact, 36 pairs of twin primes between $10^{12} - 10^4$ and $10^{12} + 10^4$, and 1,000,000,009,649 and 1,000,000,009,651 are the largest in this range. However, unlike the proof that there are infinitely many primes, no proof that there are infinitely many twin primes has been found. A number of criteria for their existence have been established, but a proof that twin primes are infinite in number has resisted the efforts of the best mathematicians over the years. The most significant, though inconclusive, result was obtained in 1921 by Viggo Brun, using a variation on the method of the Sieve of Eratosthenes. Again, we must be content to state the theorem without proof.

THEOREM 3.4. (Brun's Theorem). If q runs through the sequence of twin primes, then $\Sigma(1/q)$ converges.

If the preceding series were divergent, there would necessarily be infinitely many twin primes. As it is, one can only infer that the twin primes are relatively scarce and, possibly, only finite in number. This, by the way, can be contrasted with the corresponding theorem for all primes.

THEOREM 3.5. If p runs through all prime values, then $\Sigma(1/p)$ diverges.

Proof. Let x and j be any two positive integers, let p_i denote the ith prime, and let $N(x, j)$ denote the number of positive integers $n \leq x$ such that $p_i \nmid n$ for any $i > j$. If n is such an integer, we may write $n = rs^2$, where r and s are positive integers and where r is square-free, that is, r is not divisible by the square of any prime. We may now estimate $N(x, j)$ by considering the number of ways of choosing r and s so as to construct n's of the desired type. In the first place, $s \leq \sqrt{n} \leq \sqrt{x}$, so that there are at most $\sqrt{x}$ possible choices for s. Also, since r is square-free,

$$r = \prod_{i=1}^{j} p_i^{\alpha_i}$$

with $\alpha_i = 0$ or 1 for each i. Since there are two choices for each α_i, it follows that there are precisely 2^j possible choices for r. Thus, we finally have that there exist at most $2^j \cdot \sqrt{x}$ positive integers n satisfying the given conditions. Thus,

$$N(x, j) \leq 2^j \cdot \sqrt{x} \tag{3.1}$$

for any two positive integers x and j.

Now, suppose that $\Sigma_{i=1}^{\infty} 1/p_i$ converges. Then, by the general theory of infinite series, there must exist some j such that

$$\sum_{i=j+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}. \tag{3.2}$$

For this particular value of j, we reestimate $N(x, j)$ by estimating the number of integers $n \leq x$ that are divisible by some p_i with $i > j$ and that are, therefore, not

counted by $N(x, j)$. For such an i, the integers $p_i, 2p_i, \ldots, kp_i$, where k is the largest integer such that $kp_i \leq x$, are the values of $n \leq x$ that are divisible by p_i. Thus, for each $i > j$, there are at most x/p_i such values of n. It follows that the number of values of $n \leq x$ not counted by $N(x, j)$ is at most $\sum_{i=j+1}^{\infty} x/p_i$. Thus, using (3.2), we obtain

$$x - N(x, j) \leq \sum_{i=j+1}^{\infty} \frac{x}{p_i} < \frac{x}{2}, \tag{3.3}$$

and it follows that

$$\frac{x}{2} < N(x, j). \tag{3.4}$$

Combining this result with (3.1), we obtain

$$\frac{x}{2} < 2^j \cdot \sqrt{x} \qquad \text{or} \qquad x < 2^{2j+2}$$

for every positive integer x. But this is clearly false, since the set of positive integers is unbounded. Therefore, the assumption that $\sum_{i=1}^{\infty} 1/p_i$ converges is false and the proof is complete.

Although it is obvious from Theorems 3.4 and 3.5 that the set of twin primes is much less numerous than the set of all primes, the inductive evidence that there are infinitely many twin primes is quite strong. On the other hand, it is easy to show that there are arbitrarily long stretches of consecutive composite numbers; so the distribution of the primes among the integers must be extremely irregular. To see that this last assertion is true, consider the sequence $n! + 2, n! + 3, \ldots, n! + n$ for $n \geq 2$. The first of these numbers is clearly divisible by 2, the second by 3, the third by 4, and so on. Thus, we have $n - 1$ consecutive composite integers for any $n \geq 2$.

In view of this great irregularity in the occurrence of primes, it is not surprising that no general formula has been found for finding the nth prime. It has not even been possible to find simple functions that assume only prime values for integral arguments, and the only simple functions that are known to assume infinitely many prime values are the linear functions $f(n) = a + nd$ of Dirichlet's theorem. While the function

$$f(n) = n^2 - 81n + 1681 = (n - 40)^2 - (n - 40) + 41$$

yields prime values for all $n = 1, 2, \ldots, 80$, it is not presently known whether even such a simple quadratic function as $h(n) = n^2 + 1$ assumes infinitely many prime values for integral values of n. That no polynomial can assume *only* prime values is shown in the following theorem.

THEOREM 3.6. If $f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0$ is a non-constant polynomial with integral coefficients, then $f(n)$ must be composite for infinitely many values of the integer n.

Proof. It is no restriction to assume that $a_k > 0$ so that $\lim_{n\to\infty} f(n) = \infty$. Hence, for an integer m sufficiently large, the integer $f(m) > 1$. Let $y = f(m)$. Then, for any r,

$$\begin{aligned} f(m + ry) &= a_k(m + ry)^k + \cdots + a_1(m + ry) + a_0 \\ &= f(m) + y \cdot g(r) \\ &= y + y \cdot g(r) \\ &= y\{1 + g(r)\}, \end{aligned}$$

where $g(r)$ is a polynomial in r with integral coefficients whose leading term is $a_k y^{k-1} r^k$. Therefore, $\lim_{r\to\infty} g(r) = \infty$, and there must exist an integer r_0 such that $g(r) > 1$ for all $r \geq r_0$. Thus, $f(m + ry)$ is composite for all integers $r \geq r_0$ and the theorem is proved.

EXERCISES 3.2

1. If p is a prime different from 2 or 3, show that it must be of the form $6k + 1$ or $6k + 5$. Note that $6k + 5 = 6(k + 1) - 1$ is of the form $6k - 1$. Thus, it is also true that all primes but 2 or 3 are of the form $6k \pm 1$.
2. Prove that there are infinitely many primes of the form $6k - 1$.
3. Try to prove that there are infintely many primes of the form $4k + 1$ by imitating the proof of Theorem 3.3. Why does the proof break down?
4. How many twin primes lie in the range $9000 \leq n < 10{,}000$?
5. If p and $p + 2$ are twin primes and $p > 3$, prove that $6|(p + 1)$.
6. If $p \geq q \geq 5$ and p and q are both primes, show that $24|(p^2 - q^2)$.
   Hint: Use Theorem 2.12.
7. Let $N = p_1 p_2 \cdots p_r + p_{r+1} p_{r+2} \cdots p_{r+s}$ with $r \geq 1$ and $s \geq 1$ and where the p_i are distinct primes. Show that $p_i \nmid N$ for $1 \leq i \leq r + s$ and hence deduce again that there exist infinitely many primes.
8. Show that we cannot have a prime triplet of the form $p, p + 2, p + 4$ for $p > 3$.
   Hint: See Exercise 6 of Section 1.7.
9. What would you conjecture about prime pairs of the form $p, p + 4$? $p, p + 6$? $p, p + 8$? Check the table of primes at the back of the book.

Computer Exercise

10. Write a computer program implementing the Sieve of Eratosthenes for $1 \leq n \leq 500$.

*3.3 THE PRIME NUMBER THEOREM

As we have seen, the distribution of the primes considered individually appears to be most erratic. Over all, however, their distribution turns out to be amazingly regular. One measure of the distribution of the primes is the function $\pi(x)$ that denotes the number of primes not exceeding x. For example, $\pi(1) = 0$, $\pi(2) = 1$, $\pi(4) = 2$, and $\pi(p_n) = n$, where p_n denotes the nth prime. An explicit formula for $\pi(n)$ for every n would be equivalent to a formula for p_n and, as mentioned earlier, no such formula is known. However, $\pi(x)$ was studied in much detail as early as the latter part of the eighteenth century by Legendre and also by Gauss, then still in his teens, with a view toward finding a relatively simple function whose value *approximated* that of $\pi(x)$. In particular, both men sought a function $f(x)$ such that, for large values of x, the difference between $\pi(x)$ and $f(x)$ was small in relation to $\pi(x)$. In fact, they hoped to find $f(x)$ such that

$$\lim_{x\to\infty} \frac{\pi(x) - f(x)}{\pi(x)} = \lim_{x\to\infty} \left\{1 - \frac{f(x)}{\pi(x)}\right\} = 0,$$

or what amounts to the same thing, such that

$$\lim_{x\to\infty} \frac{\pi(x)}{f(x)} = 1.$$

Legendre conjectured that for the natural logarithm, $\ln x = \log_e x$,

$$\frac{x}{\ln x - 1.08366}$$

was such an approximating function, and Gauss guessed that both $x/\ln x$ and

$$Li(x) = \int_2^x \frac{du}{\ln u}$$

were good approximating functions, with $Li(x)$ giving the better results. Although neither had a proof that his function was a good approximation to $\pi(x)$ in the sense described above, it is interesting to see what actually happens for various values of x. In the accompanying table, the values in the last three columns are given to the nearest integer.

x	$\pi(x)$	$\frac{x}{\ln x}$	$\frac{x}{\ln x - 1.08366}$	$Li(x)$
1,000	168	145	172	178
10,000	1,229	1,086	1,231	1,246
100,000	9,592	8,686	9,588	9,630
1,000,000	78,498	72,382	78,543	78,628
10,000,000	664,579	620,419	665,138	664,918

This line of research finally culminated in the following two very remarkable theorems, which we must offer here without proof.

THEOREM 3.7. (Tchebychef's Inequality). There exist positive constants c_1 and c_2 such that, for all $x \geq 2$,

$$\frac{c_1 x}{\ln x} < \pi(x) < \frac{c_2 x}{\ln x}.$$

THEOREM 3.8. (The Prime Number Theorem)

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1.$$

It follows from Tchebychef's inequality that there exist positive constants c_3 and c_4 such that

$$c_3 n \ln n < p_n < c_4 n \ln n$$

for all $n \geq 2$, where p_n denotes the nth prime. This, in turn, yields an alternative proof of Theorem 3.5 since

$$\frac{1}{p_n} > \frac{1}{c_4 n \ln n}$$

and $\Sigma_{n=2}^{\infty} 1/n \ln n$ diverges.

Also, it follows from the prime number theorem (Theorem 3.8) that

$$\lim_{n \to \infty} \frac{p_n}{n \ln n} = 1,$$

and conversely, so that this statement is equivalent to that of the prime number theorem. It may be of interest to see how the implication goes in at least one direction. Suppose we assume that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1.$$

Setting $x = p_n$, we have $\pi(p_n) = n$ and it follows that

$$\lim_{n \to \infty} \frac{n \ln p_n}{p_n} = 1. \tag{3.5}$$

Since the logarithm is a continuous function, the logarithm of the limit of a function is the limit of the logarithm of the function, provided that the limit of the function is positive. Thus, taking the logarithm of the preceding limit, we have that

$$\lim_{n \to \infty} \{\ln n + \ln \ln p_n - \ln p_n\} = 0$$

and, hence, that

$$\lim_{n\to\infty} \ln p_n \cdot \left\{ \frac{\ln n}{\ln p_n} + \frac{\ln \ln p_n}{\ln p_n} - 1 \right\} = 0.$$

For this is to be true, the limit of the quantity in braces must be zero, and since

$$\lim_{n\to\infty} \frac{\ln \ln p_n}{\ln p_n} = 0,$$

it follows that

$$\lim_{n\to\infty} \frac{\ln n}{\ln p_n} = 1.$$

Using this result in (3.5), we finally obtain

$$\begin{aligned} 1 &= \lim_{n\to\infty} \frac{n \ln p_n}{p_n} \\ &= \lim_{n\to\infty} \frac{n \ln n}{p_n} \cdot \frac{\ln p_n}{\ln n} \\ &= \lim_{n\to\infty} \frac{n \ln n}{p_n}, \end{aligned}$$

as claimed. The reader will find it interesting to prove the implication in the other direction.

It is also of interest to note that the prime number theorem is equivalent to the assertion that

$$\lim_{n\to\infty} \frac{\pi(x)}{Li(x)} = 1,$$

where $Li(x) = \int_2^x dt/\ln t$ is the approximating function of Gauss. To see this, it is only necessary to show that

$$\lim_{x\to\infty} \frac{Li(x)}{x/\ln x} = 1.$$

For if this is so, we have

$$\begin{aligned} 1 &= \lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} \\ &= \lim_{x\to\infty} \frac{\pi(x)}{Li(x)} \cdot \frac{Li(x)}{x/\ln x} \\ &= \lim_{x\to\infty} \frac{\pi(x)}{Li(x)}. \end{aligned}$$

Integrating by parts, we obtain

$$\int_2^x \frac{dt}{\ln t} = \frac{x}{\ln x} - \frac{2}{\ln 2} + \int_2^x \frac{dt}{\ln^2 t}. \tag{3.6}$$

Since $1/\ln^2 t$ is positive and decreasing for $t > 1$, it follows that for $x \geq 4$,

$$\begin{aligned} 0 < \int_2^x \frac{dt}{\ln^2 t} &= \int_2^{\sqrt{x}} \frac{dt}{\ln^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\ln^2 t} \\ &< \frac{\sqrt{x}-2}{\ln^2 2} + \frac{x-\sqrt{x}}{\frac{1}{4}\ln^2 x} < \frac{\sqrt{x}}{\ln^2 2} + \frac{4x}{\ln^2 x}. \end{aligned}$$

From this it follows that

$$0 < \frac{\int_2^x (dt/\ln^2 t)}{x/\ln x} < \frac{\ln x}{\sqrt{x} \cdot \ln^2 2} + \frac{4}{\ln x},$$

so that

$$\lim_{x\to\infty} \frac{\int_2^x (dt/\ln^2 t)}{x/\ln x} = 0. \tag{3.7}$$

Finally, since $\lim_{x\to\infty} x/\ln x = \infty$, if we divide both sides of (3.6) by $x/\ln x$ and make use of (3.7), we obtain

$$\lim_{x\to\infty} \frac{\int_2^x (dt/\ln t)}{x/\ln x} = \lim_{x\to\infty} \frac{Li(x)}{x/\ln x} = 1,$$

as claimed.

EXERCISES 3.3

***1.** Deduce from the prime number theorem that

$$\lim_{x\to\infty} \frac{\pi(x)}{x/(\ln x - c)} = 1$$

for any constant c.

***2.** Assume that

$$\lim_{n\to\infty} \frac{n \ln n}{p_n} = 1,$$

where p_n denotes the nth prime and deduce the prime number theorem.

Hint: For $x \geq 2$, determine n by $p_n \leq x < p_{n+1}$ so that

$$n = \pi(p_n) \leq \pi(x) \leq \pi(p_{n+1}) = n + 1$$

and $x \to \infty$ as $n \to \infty$.

Computer Exercises

3. Using the program of Exercise 10 of Section 3.2 as a subroutine, write a computer program to see which of the primes less than 500 can be represented as the sum of two squares of positive integers. Endeavor to make a general guess based on the output of your program.
4. Write a computer program to ascertain which of the primes less than 500 can serve as the length of the hypotenuse of a primitive Pythagorean triangle. Endeavor to make a general guess based on the output of your program.

3.4 MERSENNE, FERMAT, AND PERFECT NUMBERS

Various methods have been developed for determining whether certain special types of numbers are prime or composite, and the largest primes known have been discovered in this way. The current champion is $2^{859,433} - 1$, an enormous giant with 258,716 digits in its decimal expansion. Determining that $2^{859,433} - 1$ is prime is only the latest in a long and interesting series of events that started in 1644 when a French monk, Father Marin Mersenne, found that the first few primes p for which $M_p = 2^p - 1$ is prime are $p = 2, 3, 5, 7, 13, 17$, and 19. Beyond this, he conjectured that M_p would be prime for $p = 31, 67, 127$, and 257 and that no other such primes would occur for p in this range. Mersenne was later found to be mistaken in the five cases $p = 61, 67, 89, 107$, and 257; that is, M_{61}, M_{89}, and M_{107} are prime and M_{67} and M_{257} are not. Nevertheless, in his honor, numbers of the form $2^n - 1$ are called *Mersenne numbers* and primes of this form are called *Mersenne primes.* We show below that if $a^n - 1$ is a prime, then it must, in fact, be a Mersenne prime.

M_{127} was shown to be prime in 1876 by a Frenchman, Edouard Lucas, who developed a neat and efficient method of attack. In 1930, D. H. Lehmer improved Lucas's algorithm and began to use computers to test M_p for further values of p. By 1963, the list of known Mersenne primes had grown to 23, with the additions corresponding to the primes $p = 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941$, and 11,213. When $2^{11,213} - 1$ was shown to be prime at the University of Illinois, the result was subtly announced to the world by using the metered stamp cancellation shown on all university mail for a period of several months. The next

numbers added to the list were $M_{19,937}$ in 1971; $M_{21,701}$ in 1978 after a three-year effort by two teenagers, Laura Nickel and Curt Noll, then first-year students at California State University at Hayward; $M_{23,209}$ in February 1979, also by Nickel and Noll; $M_{44,497}$ in April 1979; $M_{86,243}$ and $M_{132,049}$ in 1983; $M_{216,091}$ in 1985; $M_{110,503}$ in 1988; $M_{756,839}$ in 1992; and $M_{859,433}$ in January 1994.

Determining $M_{859,433}$ prime took several hours on the latest Cray supercomputer. Indeed, searching for new Mersenne primes has become a standard test to demonstrate the speed of newly developed computers. Historically, it has required about four times as much computer time to discover each new Mersenne prime as it would to rediscover *all* previously known Mersenne primes. However, human nature being what it is, we can expect that the search for these extremely large primes will not end here. In fact, the Lucas–Lehmer test for primality of Mersenne primes is given in the exercises of Section 4.2. Thus, if sufficient running time on a sufficiently powerful machine can be secured, the reader can happily enter the competition and perhaps at least briefly receive recognition in the *Guinness Book of World Records.*

But what about other numbers of the form $a^n - 1$? Might they provide even more huge primes? The answer, in the negative, is given in the following theorem.

THEOREM 3.9. If $a^n - 1$ is a prime, $n > 1$, and $a > 1$, then $a = 2$ and n is a prime.

Proof. Since

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$$

and the second factor is clearly greater than 1, it follows that $a - 1 = 1$ and $a = 2$. Otherwise, the first factor would also exceed 1 and $a^n - 1$ would be composite. Moreover, if n were composite so that $n = rs$ with $r > 1$, $s > 1$, then

$$2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1)$$

and each factor on the right clearly exceeds 1. This is again a contradiction, so n must be a prime.

A statement similar to that of Mersenne was made by Fermat, who conjectured that $2^{2^n} + 1$ is a prime for every nonnegative integer n. This is certainly true for $n = 0, 1, 2, 3,$ and 4. But in 1732, Euler showed that $2^{2^5} + 1$ is divisible by 641 and so is not a prime. Indeed, in spite of extensive theoretical and computational efforts, no more Fermat primes have been discovered and many number theorists suspect that no more exist. Still, Fermat's guess was not unreasonable, as the following theorem shows.

THEOREM 3.10. If $a^n + 1$ is a prime, $a > 1$, $n > 0$, then a is even and $n = 2^r$ for some r.

Proof. If a were odd, then $a^n + 1 \geq 4$ would be even and so would not be a prime. Moreover, suppose that n had an odd factor greater than 1, say $n = mq$ with q

odd and $q > 1$. Then

$$\begin{aligned} a^n + 1 &= a^{mq} + 1 \\ &= (a^m + 1)(a^{m(q-1)} - a^{m(q-2)} + \cdots - a^m + 1). \end{aligned}$$

Since $q \geq 3$, both factors are greater than 1 and this contradicts the fact that $a^n + 1$ is a prime. Therefore, n has no odd factor and so must be of the form $n = 2^r$ for some nonnegative integer r.

Finally, we consider an interesting set of numbers called *perfect numbers* which were certainly studied by the Greeks and possibly even before and which are intimately related to Mersenne primes. Most simply, a perfect number is one such as $6 = 1 + 2 + 3$ which is equal to the sum of its proper divisors. Using more modern notation, we give the following definition in terms of the function $\sigma(n)$, the sum of the positive divisors of n (see Section 2.5).

DEFINITION 3.1. A positive integer a is called *perfect* in case $\sigma(a) = 2a$.

For example, since

$$\sigma(6) = 1 + 2 + 3 + 6 = 12$$

and

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56,$$

it follows that 6 and 28 are both perfect. Similarly, 496 and 8128 are perfect, and the reader may notice that each of these numbers is even. Indeed, the only known perfect numbers are even, and all of these are as characterized in the following theorem, the first part of which was known to Euclid.

THEOREM 3.11. If $2^n - 1$ is a prime, then $a = 2^{n-1}(2^n - 1)$ is perfect and every even perfect number is of this form.

Proof. Let $a = 2^{n-1}(2^n - 1)$, where $2^n - 1$ is a prime. Then, by Theorem 2.24,

$$\begin{aligned} \sigma(a) &= \sigma[2^{n-1}(2^n - 1)] \\ &= \frac{2^n - 1}{2 - 1} \cdot (2^n - 1 + 1) \\ &= 2^n(2^n - 1) \\ &= 2a, \end{aligned}$$

and it follows that a is perfect.

Conversely, suppose that a is an even perfect number. Determine n and m by the equation

$$a = m2^{n-1}$$

and the conditions $n \geq 2$, m odd, $m > 0$. Since a is perfect, we have again

$$\begin{aligned} m2^n &= 2a \\ &= \sigma(a) \\ &= \sigma(m2^{n-1}) \\ &= \sigma(m)\sigma(2^{n-1}) \\ &= \sigma(m)(2^n - 1). \end{aligned}$$

Therefore,

$$\sigma(m) = \frac{m2^n}{2^n - 1}.$$

Since

$$\sigma(m) = \frac{m2^n}{2^n - 1}$$

is an integer and $(2^n, 2^n - 1) = 1$, this implies that $(2^n - 1) | m$ and hence that

$$\left| \frac{m}{2^n - 1} \right| m.$$

Moreover,

$$\sigma(m) = \frac{m2^n}{2^n - 1} = m + \frac{m}{2^n - 1},$$

so that $\sigma(m)$ is equal to the sum of m and one other positive divisor of m. Thus, m must have *only* two positive divisors, and so must be a prime. Also, it must be the case that

$$\frac{m}{2^n - 1} = 1.$$

Therefore, $m = 2^n - 1$ and $a = 2^{n-1}(2^n - 1)$, where $2^n - 1$ is a prime.

Of course, it is not known if there exist infinitely many even perfect numbers since, as Theorem 3.11 shows, there is a one-to-one correspondence between even perfect numbers and Mersenne primes and it is not known if the set of Mersenne primes is infinite. Also, it is not presently known if *any* odd perfect numbers exist, although, curiously, theorems do exist which show that if m is an odd perfect number, then m must be very large. Peter Hagis has shown that every odd perfect number m must have at least 8 distinct prime factors and G. Cohen has shown that m must exceed 10^{80}. In 1977, M. Buxton and S. Elmore announced that, in fact, m must exceed 10^{200} but they have never published a paper to this effect. In any case, it seems increasingly likely that no odd perfect numbers exist.

EXERCISES 3.4

1. If n is even, show by exhibiting the other factor that $a + 1$ is also a factor of $a^n - 1$.
2. Show that $a + 1$ is not a factor of $a^n + 1$ if n is even and $a > 1$.
3. If $\mathcal{F}(n)$ is the nth Fermat number, show that $(\mathcal{F}(n), \mathcal{F}(n+k)) = 1$ for every pair of positive integers n and k.
   Hint: Show that $\mathcal{F}(n) | \{\mathcal{F}(n+k) - 2\}$.
4. Deduce from Exercise 3 that there are infinitely many primes.
5. **(a)** If $\mathcal{F}(n)$ is the nth Fermat number, prove that $\prod_{i=0}^{n-1} \mathcal{F}(k) = \mathcal{F}(n) - 2$ for every positive integer n.
   (b) Use part (a) to again deduce that $(\mathcal{F}(n), \mathcal{F}(n+k)) = 1$ for all positive integers n and k.
6. Test for primality each of the numbers $2 + 1$, $2^2 + 1$, $2^{2^2} + 1$, $2^{2^{2^2}} + 1$. Since 251 is the largest prime not exceeding the square root of $2^{2^{2^2}} + 1$, it will probably be easier to do this problem by checking Lehmer's table of primes mentioned in Section 3.1, which, hopefully, is in your library.
7. On the basis of Exercise 6, could you make a conjecture?
8. Let $q = 2^{n-1} \cdot p$, where $p = 2^n - 1$ is a Mersenne prime. List all the divisors of q and show directly that q is a perfect number.
9. Is either of 523,776 or 33,550,336 a perfect number? It may help to refer to the table of primes at the back of the book.
10. The following triangular arrays of dots

led the early Greeks to call the numbers 1, 3, 6, 10, 15, . . . triangular numbers just as 1, 4, 9, 16, . . . are called square numbers and can be associated with square arrays of dots. Since $1 = 1$, $1 + 2 = 3$, $1 + 2 + 3 = 6$, $1 + 2 + 3 + 4 = 10$, and so on, it is clear that the nth triangular number is given by the formula

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

Prove that every even perfect number is a triangular number.

11. Which triangular number is $2^{n-1}(2^n - 1)$?
12. If $\sigma(a) = ra$, a is called *multiply perfect* or more accurately, *r-perfect*. Verify that 120 and 672 are 3-perfect and that 2,178,540 is 4-perfect. In making the last

verification it may be helpful to consult the small factor table at the back of the book.

*13. Let r and s be even positive integers such that $\sigma(r) = 2s$ and $\sigma(s) = 2r$. Prove that there exist Mersenne primes $2^p - 1$ and $2^q - 1$ such that $r = 2^{q-1}(2^p - 1)$ and $s = 2^{p-1}(2^q - 1)$, and conversely.

Computer Exercises

14. The positive integer a is called *abundant* if $\sigma(a) > 2a$ and *deficient* if $\sigma(a) < 2a$. Write a computer program to classify a as abundant, perfect, or deficient for $1 \leq a \leq 100$. Study the output carefully and make several conjectures.

15. Use a modified version of the program of Exercise 14 to see if there are any odd abundant numbers less than 10,000. Can you make any conjecture on the basis of these data?