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 $n$, $\Sigma_{i=1}^{n} i = n(n+1)/2$.

**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 $\Sigma_{i=1}^{n-1} i = k(k+1)/2$, where $k$ is any fixed but unspecified positive integer. Then

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

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

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

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

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

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

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

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 $k = 2$ 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 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 $I_1$ 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 $(k + 1)$th case often does not follow directly from the truth of the $k$th 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 $I_1$ 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 $I_2$ were used in place of 1, this would amount to saying that $I_1$ 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 $a \not{|} b$.

**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 $n \geq 2$; then $n = k$, 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 $n \geq 2$.

- The reader should observe that the second part of the preceding proof depends 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 $I_2$ 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, $F_n$ can be computed since we know its two predecessors $F_1$ and $F_2$. Then $F_3$ can be computed from $F_2$ and $F_1$, 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.
1. 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 \( I_n \) 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 \( k \), 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 \( I_1 \), \( I_2 \), \( I_3 \), 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 \( I_3 \) is needed. But suppose that the truth of \( P(k + 2) \) depends on the truth of \( P(i) \); 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
   \[ F = \{1, \sqrt{2}, 1/2, \ldots, 1/2^n, \ldots \}. \]

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) \[ \sum_{i=1}^{n} 2^{-i} = \frac{n(n + 1)}{2} \]
   (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 \( 2^{3n} - 1 \) is divisible by 3 for every positive integer \( n \).
   \textit{Hint:} For the second part of the proof make your assumption by assuming that there exists an integer \( k \) such that \( 2^{3k} - 1 = 3q \). Then consider
   \[ 2^{3(k+1)} - 1 = 8 \cdot 2^{3k} - 1 = 2 \cdot (2^{3k} - 1) + 1 = 2 \cdot 3q + 1 = 3 \cdot 2^{3k} + 3q. \]

7. Prove that \( 2^{3n+1} + 1 \) is divisible by 3 for every positive integer \( n \).

8. Prove that \( f(n) = 3n^3 + 5n^2 + 7n \) is divisible by 15 for every positive integer \( n \).
   \textit{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 \( \Pi_{k=1}^{n} a_k = (\Pi_{k=1}^{n} a_k)^2 \) for every positive integer \( n \) (see (1,12)).

11. For any positive integer \( n \), prove in two different ways that
   \[ \sum_{i=1}^{n} i(i+1) = (n+1)^2 - 1. \]
   \textit{Hint:} For one way, note that the first \( i \) of the expression being summed can be written as \( i(i+1) = i^2 + i \) and then see Exercise 4 of Section 1.1.

12. Let \( F_n \) denote the \( n \)th 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) \[ \sum_{i=1}^{n} F_i^2 = F_{n+1}F_{n+2} \]
   (c) \[ \sum_{i=1}^{n} F_{2i} = F_{2n} \]
   (d) \[ \sum_{i=1}^{n} F_{2i-1} = F_{2n-1} - 1 \]
   (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 \( \alpha \) and \( \beta \) 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 \( n \geq 0 \).
   \textit{Hint:} You may use either \( I_1 \) or \( I_2 \); 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 1845.
   \textit{Note:} \( F_0 = 0 \).
1.5 THE WELL-ORDERING PRINCIPLE

We now illustrate the method of proof based on the well-ordering principle, 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 $I_1$, $C$ 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 $s$ 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 H. 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...
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, I₁, I₂, and I₃ 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 I₁, or I₂ and then deduce a needed corollary.

Proof of Theorem 1.3 Using I₁ or I₂. It is clear that 1 ≡ 1. For the proof based on I₁, assume that k ≡ 1, where k is any fixed but unspecified positive integer. (For the proof based on I₂, assume that i ≡ 1 for all positive integers i from 1 to k inclusive, where k is any fixed but unspecified positive integer.) Then k + 1 ≡ k + 1 and it follows by I₁ (I₂) that n ≡ 1 for every positive integer n. Thus, both I₁ and I₂ 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 I₁, I₂, and I₃. 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 I₁, I₂, and I₃.

THEOREM 1.6. * I₁ implies I₂.

Proof. We take I₁ as a postulate and must prove I₂ as a theorem. Let C be any set of positive integers satisfying the conditions of I₂. The problem is to show that C contains all positive integers.

Let Aₖ denote the statement “the integers 1 to n inclusive are in C.” A₁ is true by hypothesis. Now, assume that Aₖ 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 Aₖ+₁ is true. Therefore, by I₁, Aₖ is true for every positive integer n, so C contains all positive integers.

THEOREM 1.7. I₂ implies I₁.

Proof. We now take I₂ as a postulate and prove I₁ 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 Aₖ denote the statement “n is not an element of C.” Then A₁ is true, for otherwise 1 would be the least element of C by Theorem 1.3, which we just proved using I₂. Assume that Aₖ is true for all n from 1 to k inclusive. Then, by Corollary 1.5, Aₖ+₁ must also be true, for otherwise k + 1 would be the least element in C. Thus, by I₂, Aₖ is true for every positive integer n.

EXERCISES 1.5

1. Use the well-ordering principle to prove that \( \sqrt{2} \) is irrational.
2. The Archimedean axiom states that if a and b are positive integers, there exists an integer n such that an > 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 than 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 ≥ 2 is either a prime or a product of primes.
5. Use Fermat's method of descent to prove that \( \sum_{i=1}^{n} i = n(n+1)/2 \). Note that the critical arithmetic of the argument is essentially the same as in the proof of this result by I₁ in Section 1.4.
6. Use Fermat's method of descent to prove that \( \sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6 \).
   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.
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.** $I_1$ implies $I_2$.

**Proof.** Let $C$ be a set of positive integers satisfying the conditions of $I_1$. Assuming $I_2$ 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 $I_1$, $C^*$ has a least element. It follows from Theorem 1.3, which we proved by using $I_1$, 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 $I_4$. 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 $a = 0$, then $a - 0b = a(1 - b) = 0$ 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 $a$ 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

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

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

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

and this is a contradiction. Similarly, we obtain a contradiction if $q' > q$. Thus, it must be the case that $q = q'$. But then $bq + r = bq' + r'$, 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 $4k^2$ 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, $a^3$ must be of the form $9k^3$, or $9k^3 + 6k + 1 = 3e + 1$, or $9k^3 + 12k + 4 = 3w + 1$. 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 $11, 111, 1111, 11111, \ldots$ 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 $x$ is an integer not divisible by 3, show that $x^2 + 23$ must be divisible by 24. [Hint: Any integer must be of the form $6k$, $6k + 1$, $6k + 2$, $6k + 3$, $6k + 4$, 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 $a = bq + r$. 


7. If $L_n$ denotes the $n$th Lucas number, show that $L_n = O(n^p)$, 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 $n$th prime? Does the formula $F(n) = 2^n + 1$ 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 $a = 0$, 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 $y$. 

39
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 \( bx + cy = aux + any = a(ux + vy) \), 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 \( a|b \) 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 \( |b| = |a| \cdot |c| \leq |a| \) 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 $N_m | N_n$ 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 $\pm 1, \pm 2, \pm 3, \pm 6$ 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{align*}
r &= a - eq \\
    &= a - (ax_0 + by_0)q \\
    &= d(1 - qx_0) + b(-y_0),
\end{align*}
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, $f|d$. 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 $a$ and $b$. 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 $b$ 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 $0 > r_1 > r_2 > r_3 > \cdots$ can extend for at most $b$ terms before reaching zero. Suppose that $r_{n+1}$ is the first zero remainder, so that we have the equations
\[ a = bq_1 + r_1, \]
\[ b = rq_2 + r_2, \]
\[ r_1 = q_3r_2 + r_3, \]
\[ \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \]
\[ r_{n-2} = q_{n-1}r_{n-1} + r_{n-1}, \]
\[ r_{n-1} = q_nr_n + r_n, \]
\[ r_n = r_{n+1}. \]

It is easy to show that $r_n$, the last nonzero remainder, is the desired greatest common divisor of $a$ and $b$. We have that $r_0 | r_{n-1}$ and $r_1 | r_{n-2}$ so, using the next-to-last of the preceding equations and property (v) of Theorem 2.1, $r_1 | r_{n-2}$. But then $r_1 | r_{n-1}$ and $r_1 | r_{n-2}$, so, using the third equation from the last and property (v) of Theorem 2.1, $r_1 | r_{n-3}$. This process may be continued to show that $r_1 | a$ and $r_1 | b$. 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 $f|r_n$. Thus, $r_n$ satisfies the conditions of Theorem 2.5, so $r_n = (a, b)$, as claimed.

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

Performing the appropriate divisions, we obtain
\[ 288 = 51 \cdot 5 + 33, \]
\[ 51 = 3 \cdot 16 + 3, \]
\[ 33 = 16 \cdot 2 + 1, \]
\[ 18 = 15 \cdot 1 + 3, \]
\[ 15 = 3 \cdot 5. \]

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
\[ 3 = 18 - 15, \]
\[ = 18 - (33 - 18), \]
\[ = 2 \cdot 18 - 33, \]
\[ = 2 \cdot (51 - 33) - 33, \]
\[ = 2 \cdot 51 - 3 \cdot 33, \]
\[ = 2 \cdot 51 - 3 \cdot (288 - 5 \cdot 51), \]
\[ = 288 (-3) + 51 \cdot 17. \]
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,

\[
3 = 288(-3) + 51 \cdot 17 \\
= 288(-3) + 288 \cdot 51 - 288 \cdot 51 + 51 \cdot 17 \\
= 288 + 51(-271),
\]

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 of x and y may assume.

Note that 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.

\[
\begin{align*}
288 &= 51 \cdot 5 + 33 \\
33 &= 18 \cdot 1 + 15 \\
15 &= 8 \cdot 1 + 7 \\
7 &= 3 \cdot 2 + 1 \\
1 &= 3 \cdot 3 + 0
\end{align*}
\]

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 fashioned 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 of these values can equal \( (a, b) \).

From \( d = ax + by \) one can conclude that \( (a, b) \) divides d, but without further information,
Proof. By Corollary 2.10, \( p | p_i \) for some \( i \), \( 1 \leq i \leq n \). But \( p \neq 1 \) 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 \( (a, b_1 b_2 \ldots b_n) = d > 1 \). Then, by Theorem 1.2, there exists a prime \( p \) such that \( p | d \). Since \( d | a \) and \( d | b_1 b_2 \ldots b_n \), it follows from property (iv) of Theorem 2.1 that \( p | a \) and \( p | b_i \) for some \( i \), \( 1 \leq i \leq n \). 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 \( m = m_1 m_2 \ldots m_n \).

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 \( i \neq j \), \( 1 \leq i \leq k+1, 1 \leq j \leq k+1 \). By Theorem 2.12, \( (m', m_{k+1}) = 1 \) where \( m' = m_1 m_2 \ldots m_k \), and by the induction assumption, \( m' | a \). But then, by Theorem 2.13, \( m' m_{k+1} | a \) and \( m' m_{k+1} = m_1 m_2 \ldots m_{k+1} \). Thus, the result is true for all \( n \geq 1 \), 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 \( n \geq 3 \).

Proof. Note that \( F_2 = 2 > 1.618 \ldots = (1 + \sqrt{5})/2 \) and that \( F_3 = 3 > 2.618 \ldots = ((1 + \sqrt{5})/2)^3 \). 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 \( k \geq 3 \). 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 \( n \geq 3 \) 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,
EXERCISES 2.3

The number of operations needed to find \( q \) with

\[ \log_q a \quad \text{is} \quad q > a > 0 \]

COROLLARY 2.17

Since \( x \) and \( k \) are integers, this completes the proof.

\[ 35 = 1 + k \]

and

\[ 35 > q \log_{q} a \quad \text{and} \quad \log_{q} a > k \]

Thus, from above,

\[ 10^{0.208} \quad \text{is the number of decimal digits in} \quad \log_{q} a \]

Thus, if there are \( k \) divisions, it follows from \( q \log_{q} a > k \) for \( k \) is an integer.

Thus, by the algorithm at the top of page 43, the greatest common divisor of \( a \) and \( b \) is equal to \( d \).
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 \(d = (a, b), c' = (a + c, b)\) and show that \(d|c\) and \(c|d\).
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 \(d|m\) 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 \(a|b + c\) and \(b|d\), show that \(b = d\).
14. Prove that the product of any three consecutive integers is divisible by 6.
15. If \((a, c) = 1\), \((b, c) = 1\), \((a, bc) = rs\). 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 \((F_n, F_{n+2}) = 2\) or 12 for \(n \geq 1\).

**Hint:** Show that \(2|F_m\) if and only if \(m = 3q\) for some positive integer \(q\).
18. In Exercise 17, \((F_m, F_{m+2}) = 2\) or 12. Show that \(2|F_n\) if and only if \(n = 3q\) for some positive integer \(q\).

**Hint:** For the "if" part, note that \(2 = F_1\), and use Exercise 19 of Section 1.4. For the "only if" part, deduce from Exercise 17 of Section 1.4 that \(F_m + F_{m+2} = F_{m+1}\), for \(m = 3q + r\) and \(r\) 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 \(F_m + F_{m+2} = F_{m+1}\), where \(n = mq + r\) and again argue by contradiction using the results of Exercises 16 and 7.

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 at least one 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 \(m|a\) and \(b|n\) 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, \(m > 0\), \(a|m\), \(b|m\), 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 \( a \) and \( r \) with \( 0 \leq r < m \) such that \( n = qn + r \). 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 \( r = 0 \), this violates the given condition that \( m \) is the least common multiple.

Therefore, \( r = 0 \) and \( m | n \), as claimed.

(ii) Suppose that \( m > 0 \), \( a | m \), and \( b \mid m \), 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 \( m = \lbrack n \rbrack \). Thus, \( m \) is the least positive common multiple of \( a \) and \( b \) and the proof is complete.

**THEOREM 2.19.** If \( ab = 0 \), then \( \lbrack a, b \rbrack = \lbrack ab/(a, b) \rbrack \).

**Proof.** Let \( d = \lbrack a, b \rbrack \). Then \( m = \lbrack ab \rbrack = \lbrack ab/d \rbrack \). If \( m \geq 0 \), then \( a/d \) and \( b/d \) are integers, so there exist \( r \) and \( s \) such that \( ar = bn = bs \). Therefore, \( Adr = Bds \) and \( Ar = Bs \). This implies that \( Ads \). But \( (A, B) = 1 \) by Corollary 2.7, so, by Theorem 2.8, \( A/s \) and there exists \( i \) such that \( Ai = s \). But then \( n = bs = ad \) and \( m/n \), so \( m \). Thus, \( m \) satisfies the conditions of Theorem 2.18 and \( m = \lbrack a, b \rbrack \), 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 \( \lbrack 288, 51 \rbrack = 5 \), we now have that

\[
\frac{288}{51} = \frac{51 \cdot 5}{3} = 4986.
\]

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 \( a_1, a_2, \ldots, a_n \) are not all zero, they have a largest common divisor which we denote by \( \langle a_1, a_2, \ldots, a_n \rangle \). It can be shown that \( \langle a_1, a_2, \ldots, a_n \rangle \) if and only if \( n \geq 2 \), \( d \), and \( d \) for every common divisor of \( a_1, a_2, \ldots, a_n \). Also, it can be shown that \( d \) is the least positive integer of the form \( a_1x_1 + a_2x_2 + \cdots + a_nx_n \). The integers \( a_1, a_2, \ldots, a_n \) are said to be relatively prime in case \( \langle a_1, a_2, \ldots, a_n \rangle = 1 \). As before,

\[
\langle a_1, a_2, \ldots, a_n \rangle = 1
\]

if and only if there exist integers \( x_1, x_2, \ldots, x_n \) such that

\[
a_1x_1 + \cdots + a_nx_n = 1.
\]

Similarly, if none of \( a_1, a_2, \ldots, a_n \) are zero, they have a least positive common multiple which we denote by \( \{ a_1, a_2, \ldots, a_n \} \). It can be shown that \( \{ a_1, a_2, \ldots, a_n \} \) if and only if \( n \geq 2 \) and \( a_1 \cdot a_2 \cdots a_n \) for every common multiple \( n \) of the \( a_i \).
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 \([a, b] = \gcd(a, b)\).

8. For any integer \(n\), prove that \([2n + 8, 6n + 5] = 54n^2 + 93n + 40\).

9. Find \([12n^2 + 16n + 6, 6n + 5]\) and \([12n^2 + 16n + 6, 6n + 5]\), where \(n\) is an integer.

10. Let \(a_1, a_2, \ldots, a_n\) be nonzero integers. Let \(d = a_1x_1 + a_2x_2 + \cdots + a_nx_n\) be the smallest positive linear combination of \(a_1, a_2, \ldots, a_n\). Prove that
    \(d = (a_1, a_2, \ldots, a_n)\).

11. Prove that \((a_1, a_2, \ldots, a_n) = 1\) if and only if there exist integers \(x_1, x_2, \ldots, x_n\) such that
    \(1 = a_1x_1 + a_2x_2 + \cdots + a_nx_n\).

12. Give an example to show that the equation
    \((a_1, a_2, \ldots, a_n)(a_1, a_2, \ldots, a_n) = a_1a_2 \cdots a_n\)
    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 \(y^2 = x^2 - 1\) and \(z^2 = x^2 - 1\). 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, \(36 = 4 \cdot 9 = \)

Sec. 2.5 The Fundamental Theorem of Arithmetic

2 \cdot 3 \cdot 3 \cdot 3\) where 2 and 3 are primes. Again, \(36 = 6 \cdot 6 = 2 \cdot 3 \cdot 3\) 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

\((3r + 1)(3s + 1) = 3(3(r + s) + 1),\)

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

\((3r + 1) + (3s + 1) = 3(r + s + 1),\)

it is clear that \(T\) does not contain the sum of any 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 \(T\) 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 \(T\). However, not even all of those properties are sufficient to guarantee unique factorization, as the following example shows.

We consider the set \(C\) of all complex numbers of the form \(a + \sqrt{3}i\), where \(a\) and