4-1
DIVISIBILITY

You can imagine how surprised the author was when an experienced teacher revealed that he did not know the meanings of "greatest common factor" and "least common multiple," though these terms could be found repeatedly in the sixth grade mathematics text from which the teacher taught. Since these concepts belong (and are!) in the elementary school mathematics curriculum, we will present them, along with some other important ideas, in this chapter. Later we will see that comparing fractions, adding fractions, and reducing fractions are just some of the arithmetic problems that involve these concepts.

A useful technique to help in understanding number theory is to take given whole numbers and view them as products of smaller whole numbers. One illustration of how this can be of use is given in Example 4-1. Others will be given in Chapter 5.

[illegible]

Devise a way of multiplying 12 × 25 in your head.

[illegible]

Observe that each four 25's make 100 and think as follows:

$$\begin{aligned} 12 \times 25 &= 3 \times 4 \times 25 \\ &= 3 \times 100 \\ &= 300 \end{aligned}$$

(It may help to visualize 12 quarters. Each 4 quarters make a dollar, so 12 quarters make 3 dollars.)

Notice in Example 4-1 that it helps to think of 12 as 3 times 4. Central to the idea of expressing a given whole number as the product of smaller whole numbers is the following definition:

☐ Definition of Divisibility

> Given whole numbers a and b (a can't be 0), we say that b **divides** a if there is a whole number c such that $a = b \times c$. The symbol " | " is used to indicate "divides" and "∤" is used to indicate "does not divide."

[illegible]

Which are true?

(a) $3 \mid 15$ (b) $8 \mid 4$ (c) $10 \mid 10$

(d) $2 \mid 7$ (e) $2 \nmid 3$ (f) $3 \mid 9$

"24 is a multiple of 8," and

"24 is divisible by 8."

Two closely related facts are valuable both for reinforcing the basic notion of divisibility and for their usefulness later. They are the following:

☐ Divisibility Properties for Sums and Differences

If $b \mid a$ and $b \mid d$, then $b \mid (a + d)$, and
If $b \mid a$ and $b \mid d$, then $b \mid (a - d)$ (provided $a - d$ is defined).

We wish to show that these results hold for any whole numbers a, b, and d that satisfy the given conditions. To illustrate the method of proof, we will first consider a numerical example. Specifically, we will verify that since $11 \mid 99$ and $11 \mid 55$, $11 \mid (99 + 55)$. To argue that $11 \mid (99 + 55)$, we must find a whole number c such that $99 + 55 = 11 \times c$. How can we use our given information? We are given that $11 \mid 99$, so there is some whole number e (we have already used c to represent something else) such that $99 = 11 \times e$. Clearly e is 9; namely, $99 = 11 \times 9$. We are also given that $11 \mid 55$, so there is some whole number f such that $55 = 11 \times f$. Clearly f is 5; namely, $55 = 11 \times 5$. Thus $99 + 55 = 11 \times 9 + 11 \times 5$, which by the distributive property is $11 \times (9 + 5)$, or 11×14. So the number c which we sought is 14. Summarizing, we said that if 99 is 9 elevens and 55 is 5 elevens, then 99 + 55 must be 9 elevens + 5 elevens, or 14 elevens.

We can do a proof for arbitrary whole numbers a, b, and d in exactly the same way. Let us prove that

If $b \mid a$ and $b \mid d$, then $b \mid (a + d)$.

To argue that $b \mid (a + d)$, we must find a whole number c such that $a + d = b \times c$. How can we use our given information? We are given that $b \mid a$, so there is some whole number e such that $a = b \times e$. We are also given that $b \mid d$, so there is some whole number f such that $d = b \times f$. Thus $a + d = b \times e + b \times f$, which by the distributive property is $b \times (e + f)$. Since e and f are whole numbers, their sum must be a whole number, according to the closure property for addition. So the number c which we sought is $e + f$.

This result can also be stated another way: If a number divides each of two numbers, then it divides their sum. You will have the opportunity to prove the companion result in the problems; namely, that if a number divides each of two numbers, then it divides their difference. The proof is quite similar.

These two divisibility properties will be called upon many times. One way in which they are helpful is shown in Example 4-3.

EXAMPLE 4-3

(a) Is 156 divisible by 13?

(b) Is 692 divisible by 7?

(g) $17 \mid (23 \times 17 \times 73)$

(h) $(3^4 \times 5^2) \mid (2^{10} \times 3^{10} \times 5^{10})$

SOLU

(a) The problem says "three divides fifteen," which is true, since $15 = 3 \times 5$. (There is a whole number which when multiplied by 3 gives 15.)

(b) $8 \mid 4$ is false, since $4 = 8 \times c$ holds for no *whole number c*. There is no whole number which when multiplied by 8 gives 4.

(c) $10 \mid 10$ is true, since $10 = 10 \times 1$. (1 is a whole number.)

(d) $2 \mid 7$ is false, since $7 = 2 \times c$ holds for no *whole number c*.

(e) The problem says "two does *not* divide three," which is true, since $3 = 2 \times c$ holds for no *whole number c*.

(f) $3 \mid 9$ is true, since $9 = 3 \times 3$. (3 is a whole number.)

(g) $17 \mid (23 \times 17 \times 73)$ is true provided there is a whole number c which when multiplied by 17 gives $23 \times 17 \times 73$. Since $23 \times 17 \times 73$ can be thought of as $17 \times (23 \times 73)$ (after applying the commutative and associative properties of multiplication), the whole number c that we sought is 23×73.

h) $(3^4 \times 5^2) \mid (2^{10} \times 3^{10} \times 5^{10})$ is true provided there is a whole number c which when multiplied by $3^4 \times 5^2$ gives $2^{10} \times 3^{10} \times 5^{10}$. What quantity, when multiplied by the product of four 3's and two 5's, gives the product of ten 2's, ten 3's, and ten 5's? We need the product of ten 2's, six more 3's, and eight more 5's, so $c = 2^{10} \times 3^6 \times 5^8$.

We can make two helpful observations from the examples. First, the whole umbers a, b, and c of the definition of "divides" need not be different, as can e seen in parts (c) and (f). Second, "$3 \mid 15$" is a *statement*, which in this case is ue. Regarding this second point, note that

"$3 \mid 15$" says "3 divides 15"

hich is a true statement, while the symbolism

"$15 \div 3$" means "15 divided by 3"

hich is a number, namely 5.

If b divides a we also say that

b is a **divisor** of a

b is a **factor** of a and

a is a **multiple** of b

a is **divisible** by b

r example, all the following statements are true:

"8 is a divisor of 24,"

"8 is a factor of 24,"

SOLUTION

We could use long division (or a calculator) to answer each of these questions, but it is not necessary.

(a) Look for a number about the size of 156 which is known to be divisible by 13. For instance, 156 is 26 more than 130, which is clearly divisible by 13. Since both 130 and 26 are divisible by 13, their sum, which is 156, is also divisible by 13.

(b) Look for a number about the size of 692 which is known to be divisible by 7. Observe that 692 is 8 less than 700, a known multiple of 7. If 692 were divisible by 7, then the difference 700 − 692 (which is 8) would have to be divisible by 7. Since 8 is not divisible by 7, 692 cannot be divisible by 7.

Not all problems will work out this well, but there are enough instances where the method of Example 4-3 is helpful to make it worthwhile.

Another application of these two divisibility properties is establishing the validity of certain divisibility tests, such as the well-known **divisibility test for 2**, which says:

A number is divisible by 2 if and only if its last digit is 0, 2, 4, 6, or 8.

We will prove this result for three-digit numbers. Arguments for bigger or smaller numbers would be similar. Suppose we have a three-digit number n whose hundreds digit is p, whose tens digit is q, and whose ones digit is r. Then, recalling some facts about place value, we have $n = p \times 100 + q \times 10 + r$. Now

$$2 \mid (p \times 100), \text{ since } p \times 100 = 2 \times (50 \times p), \text{ and}$$
$$2 \mid (q \times 10), \text{ since } q \times 10 = 2 \times (5 \times q), \text{ so}$$
$$2 \mid (p \times 100 + q \times 10), \text{ by the sum property.}$$

It will be helpful to think of $(p \times 100 + q \times 10)$ as a single whole number that is divisible by 2. Using parentheses for emphasis we can write

$$n = (p \times 100 + q \times 10) + r.$$

Now it will be easy to see that if r is 0, 2, 4, 6, or 8, then $2 \mid n$; and if $2 \mid n$, then r is 0, 2, 4, 6, or 8. First, if r is 0, 2, 4, 6, or 8, then $2 \mid r$. But since $2 \mid (p \times 100 + q \times 10)$ and $2 \mid r$, it follows by the sum property that $2 \mid (p \times 100 + q \times 10) + r$; namely, $2 \mid n$. Conversely, if $2 \mid n$, rewrite

$$n = (p \times 100 + q \times 10) + r, \text{ as}$$
$$r = n - (p \times 100 + q \times 10).$$

Observe that $2 \mid n$ and $2 \mid (p \times 100 + q \times 10)$ implies $2 \mid n - (p \times 100 + q \times 10)$, so $2 \mid r$. But if the one-digit number r is divisible by 2, r must be 0, 2, 4, 6, or 8.

Is there a divisibility test for 3? Each of the numbers 30, 21, 12, 33, 24, 15, 36, 27, 18, and 39 is divisible by 3, so it doesn't seem to matter what the last digit is. Yet there *is* a good **divisibility test for 3**:

> A number is divisible by 3 if and only if the sum of its digits is divisible by 3.

Notice that the sum of the digits of each of the numbers listed above is divisible by 3. Here are some examples:

The sum of the digits of 30 is $3 + 0 = 3$.

The sum of the digits of 21 is $2 + 1 = 3$.

The sum of the digits of 24 is $2 + 4 = 6$.

The sum of the digits of 39 is $3 + 9 = 12$.

In each case, the sum of the digits is divisible by 3.

We will sketch a proof for three-digit numbers. Other cases are similar. Suppose our three-digit number $n = p \times 100 + q \times 10 + r$ as in the previous proof. After applying some of the properties developed in the preceding chapter, we have

$$\begin{aligned} n &= p \times 100 + q \times 10 + r \\ &= p \times (99 + 1) + q \times (9 + 1) + r \\ &= p \times 99 + p + q \times 9 + q + r \\ &= p \times 99 + q \times 9 + p + q + r \\ &= (p \times 99 + q \times 9) + (p + q + r) \end{aligned}$$

where parentheses were added in the last step for emphasis. Now $(p \times 99 + q \times 9)$ is clearly divisible by 3, so if $(p + q + r)$ is divisible by 3, so is n; and, if n is divisible by 3, so is $(p + q + r)$, which can be expressed as the difference $n - (p \times 99 + q \times 9)$.

Other divisibility tests will be considered in the problems.

EXERCISES AND PROBLEMS 4-1

DEFINITION

1. Which are true?
   (a) $6 \mid 12$ (b) $12 \mid 6$ (c) $6 \mid 6$
   (d) 8 is a multiple of 4. (e) 8 is a factor of 4.
2. Use the definition of "divides" (find c) to show
   (a) $5 \mid 120$ (b) $5 \mid 2^3 \times 3 \times 5$
   (c) $5 \mid 2^{11} \times 3^8 \times 5^7 \times 13^{67}$ (d) $10 \mid 2^{11} \times 3^8 \times 5^7 \times 13^{67}$
   (e) $1000000 \mid 2^{11} \times 3^8 \times 5^7 \times 13^{67}$
   (f) $p^2q^3 \mid p^6q^6r^6$, where p, q, and r are whole numbers
   (g) $3 \mid 6 \times 4$ (h) $3 \mid (6 \times 4 + 3)$
3. If 12 divides n, what else must divide n?
4. (a) Obviously 2 divides 86. Why?
   (b) Find c (in the definition of "divides") to show that 2 divides 86.
   (c) Is the number c a divisor of 86? Prove it.

5. The previous problem illustrates how divisors occur "in pairs." This can be helpful in finding divisors of a number. For example, it is easy to see from the divisibility tests that 2 and 3 (and thus 6) are divisors of 222. From each of these divisors we obtain a "c" (from the definition of divides).

$$222 = 2 \times 111 \qquad (c = 111)$$

$$222 = 3 \times 74 \qquad (c = 74)$$

$$222 = 6 \times 37 \qquad (c = 37)$$

This technique tells us that 111, 74, and 37 are also divisors of 222, so a complete list of divisors of 222 is 1, 2, 3, 6, 37, 74, 111, 222. Use this technique to find a list of all divisors of (a) 78, (b) 170, (c) 266, (d) 36. (e) Which divisor of 36 is "paired with" 6?

6. (a) Find the smallest whole number divisible by all of the numbers 2, 3, 4, 5, and 6.
   (b) Describe the smallest whole number divisible by all of the numbers 2, 3, 4, 5, 6, 7, . . . , 20. (Do not do any computation.)

DIVISIBILITY TESTS AND PROPERTIES

7. You should be able to answer each of these questions without actually performing any divisions (or using a calculator) — just using divisibility ideas. Tell whether each is true or false and how you know:
   (a) $15 \mid 1000$ (b) $8 \mid 1000$ (c) $17 \mid 168$
   (d) $35 \mid 1092$ (e) $18 \mid 6372$ (f) $6 \mid 10{,}000{,}002$

8. (a) An employer promises to pay a new employee $14,000 per year. For easy bookkeeping, the actual salary is to be the smallest whole number ≥ 14,000 which is divisible by 12. (Why 12?) Find this number.
   (b) Repeat part (a) replacing $14,000 by $13,000.
   (c) The secretary in charge of payroll frequently faces similar problems. Devise a divisibility test for 12. (Hint: See Problem 3.)

9. (a) Devise a divisibility test for 9. Prove it works for three-digit numbers (of the form $100a + 10b + c$).
   (b) Do the same for 5. (c) Do the same for 4. (d) Do the same for 11.
   (Hint for part (d): $100a + 10b + c = 99a + a + 11b - b + c$.)

10. Which of the following are divisible by 3? by 4? by 9?
    (a) 225 (b) 348 (c) 31687452 (d) 7001936

11. Take any three-digit number. Rearrange the digits in any order. Subtract the smaller number from the larger. (a) Show that the result is divisible by 9. *(b) Will this work for *all* three-digit numbers? *(c) Prove it.

12. Give an example of each of the following properties. Use the example to find a proof that each is true for all non-zero whole numbers a, b, and c. (See the discussion and proof of the sum property given in this section to see how a numerical example can help to discover a general proof.)
    (a) If $b \mid a$ and $b \mid d$, then $b \mid (a - d)$ (provided $a - d$ is defined). (difference property of divisibility)
    (b) If $b \mid a$ and $a \mid d$, then $b \mid d$. (**transitive property of divisibility**)
    (c) If $b \mid a$, then $b \mid ad$.
    (d) If $b \mid a$ and $b \mid d$, then $b \mid (ra + sd)$ for any whole numbers r and s.
    (e) If $ab \mid d$, then $a \mid d$.

13. True or False? Give reasons.
    (a) If $b \mid a$ and $b \nmid d$, then $b \nmid (a + d)$.
    (b) If $b \nmid a$ and $b \nmid d$, then $b \nmid (a + d)$.

14. The sum $1^2 + 2^2 + 3^2 + 4^2 + \ldots + n^2$ can be shown to equal $n(n + 1)(2n + 1)/6$. Verify this result for
    (a) $n = 1$ (b) $n = 2$ (c) $n = 3$ (d) $n = 4$
    *(e) Show that for every whole number n, 6 divides $n(n + 1)(2n + 1)$. (In other words, show that $[n(n + 1)(2n + 1)/6]$ is a whole number for each n.)

15. Prove every number of the form ABCABC, such as 957957 or 100100, is divisible by 7, by 11, and by 13.

*16. (a) Show that $3 \mid (n^3 - n)$ for each whole number n.
    (b) Show that $5 \mid (n^5 - n)$ for each whole number n.
    (c) Show that $9 \mid (n^9 - n)$ for each whole number n *is false*.

CALCULATORS

*C*17. Suppose we compute $p \div d$ using a dependable calculator. (a) If $p \div d$ gives an answer of 233, is it necessarily true that $d \mid p$? (b) If $p \div d$ gives an answer of 3.8, is it possible that $d \mid p$? (c) If $p \div d$ gives an answer of 3.8, is it possible that $p \mid d$?

PROBLEM SOLVING EXTENSIONS

18. Devise a way to multiply each of these mentally:
    (a) 15 × 18 (b) 15 × 42 (c) 25 × 32 (d) 25 × 33 (e) 25 × 34

19. In Example 4-1, the term 3 × 4 × 25 is thought of both as 12 × 25 and as 3 × 100. Which of the basic properties of multiplication is being used implicitly here?

20. The symbol 5! is called five factorial (see Problem 22, Section 3-5) and means $5 \times 4 \times 3 \times 2 \times 1$; namely, $5! = 120$. Also $3! = 3 \times 2 \times 1 = 6$. Which of the following are true? If the statement is true, find the value of c in the definition of "divides."
    (a) $5 \mid 5!$ (b) $4 \mid 5!$ (c) $7 \mid 6!$ (d) $6 \mid 5!$
    (e) $5 \mid (5! + 1)$ (f) $4 \mid 7!$ (g) $50 \mid 50!$ (h) $50 \mid (50! + 1)$
    (Do not multiply out parts g and h.)

21. (Note: It is recommended that you do the parts to this question in sequence, since they are related. See Problem 20.)
    How many zeros are at the end of each of the following?
    (a) 4! (b) 5! (c) 9! (d) 10! (e) 11! (f) 20! (g) 100!

22. An old invoice showed that 72 turkeys had been purchased for $_67.9_. The first and last digits were illegible. Assuming that the total amount (expressed in cents) is divisible a whole number of times by 72, what are the missing digits!

23. We say that 6 is a **perfect number**, since it equals the sum of its proper divisors (divisors other than 6 itself):

$$6 = 1 + 2 + 3$$

    (a) There is another perfect number less than 35. Find it.
    (b) Euclid knew that $N = (2^{n-1})(2^n - 1)$ is an even perfect number whenever $2^n - 1$ is prime. For example, if $n = 5$, then

$$N = (2^4)(2^5 - 1) = 16 \times 31 = 496,$$

which is a perfect number. Use Euclid's formula to find two more perfect numbers. (Verify that they are perfect numbers.)

(c) Perfect numbers are always triangular numbers. (See Problem 27, Section 3-5.) For example, 6 is a triangular number. Show that your answer to part (a) is a triangular number.

(d) Notice that $496 = 1^3 + 3^3 + 5^3 + 7^3$. Is $1^3 + 3^3$ a perfect number? Is $1^3 + 3^3 + 5^3$ a perfect number? Express your answer to part (a) as the sum of odd cubes.

For more information on perfect numbers see references [20] and [25].

4-2
PRIME NUMBERS

With this background in the concept of divisibility, we return to the question of expressing whole numbers as products of smaller whole numbers. An embodiment of this concept that is quite appropriate for elementary school children is the task of building rectangle-shaped "houses" with a specified number of blocks. For instance, children might be asked to build as many different kinds of (rectangular) "houses" as possible using exactly six blocks. The only possibilities (in which no block is placed on top of another) are given in Figure 4-1. Among the things a child might learn from this example is that the factors of six are one, two, three, and six.

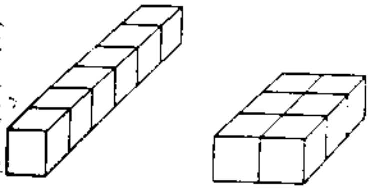


FIGURE 4-1

What rectangles are possible using exactly seven blocks? Since seven is not the product of two smaller whole numbers, the only possible rectangles are 1 × 7 (or 7 × 1). The classification of whole numbers according to which numbers can be expressed as the product of smaller factors leads us to the following definitions:

If a whole number can be expressed as the product of two smaller whole numbers, it is called **composite**.

If a whole number (other than 1 or 0) cannot be expressed as the product of two smaller whole numbers, it is called **prime**.

0 and 1 are exceptions and are not considered either prime or composite.

EXAMPLE 4-4

(a) List the first five composites. (b) List the first five primes.

0 is excluded from both categories.

1 is excluded from both categories.

2 is prime

3 is prime

4 = 2 × 2

5 is prime

6 = 2 × 3

7 is prime

8 = 2 × 4

9 = 3 × 3

10 = 2 × 5

11 is prime

Thus (a) the first five composites are 4, 6, 8, 9, and 10, and (b) the first five primes are 2, 3, 5, 7, and 11.

Some composites can be written as the product of two smaller whole numbers in more than one way. For example, 12 = 2 × 6 and 12 = 3 × 4. If we continue the factoring process, observing that 6 = 2 × 3 and 4 = 2 × 2, we have

$$12 = 2 \times 6 = 2 \times 2 \times 3 \quad \text{and} \quad 12 = 3 \times 4 = 3 \times 2 \times 2.$$

In each case, we arrive at exactly the same list of factors (except for the order in which they appear). These factors are primes, so the process terminates. We choose to ignore factors of 1, for though it is true that 12 = 12 × 1 and that 12 = 2 × 2 × 3 × 1 × 1 × 1, the 1's don't provide any useful information about the number 12. This is why we do not consider 1 to be prime, for now we can make the following remark: there is exactly one way to write 12 as the product of primes, except for the order of the factors.

Is this true for other whole numbers? For all whole numbers? We shall investigate these interesting and important questions further.

First, we examine a few more examples, borrowing a technique often used in elementary school texts. We draw a **prime factor tree** to help factor numbers into primes. Figure 4-2 shows two of the possible prime factor trees for 12. In either case, we collect the prime factors from the ends of the branches. Some prime factor trees for 60 are shown in Figure 4-3. In each of the prime factor

FIGURE 4-2

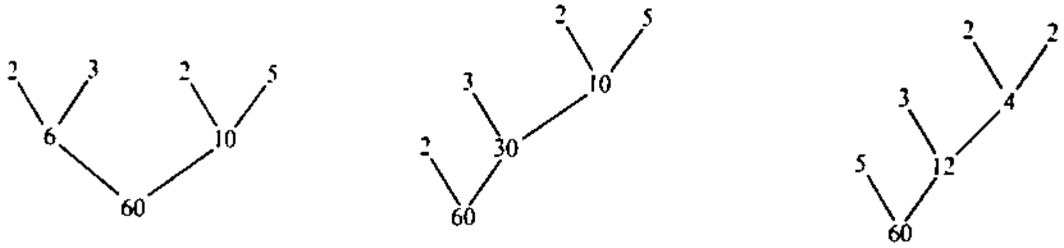


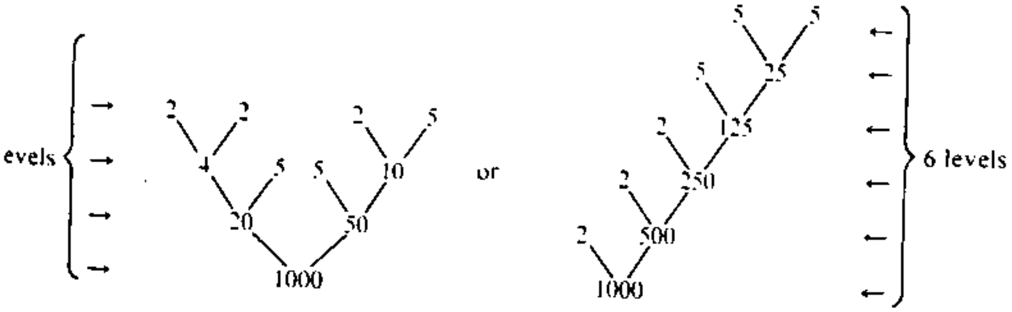
FIGURE 4-3

trees for 60, we arrived at the same prime factors: 2, 2, 3, and 5. (Are there other ways to factor 60? Do they lead to the same prime factors?)

While we are far from exhausting all the possibilities in determining which numbers factor into primes *in just one way* (except for the order of the factors), the prime factor trees suggest one conclusion:

> A whole number (larger than 1) is either prime or can be written as the product of primes.

f the given whole number is larger than 1 and is not itself a prime, it can be vritten as the product of two smaller whole numbers. (In terms of our picture, f it is not the end of a branch, it will split into further branches.) Now if either or both) of these two smaller whole numbers is not prime, then it (they) can be vritten as the product of two still smaller whole numbers. We continue until all he factors are primes. But since the supply of whole numbers smaller than the riginal number is limited, the process must eventually terminate. For stance, if we start with the whole number 1000, the first branches must consist f two numbers each not more than 999, the next branches must consist of two umbers each not more than 998, and so on, so there can be no more than 1000 levels." (See Figure 4-4.) While the actual number is far less, the important ing is that the process must end. The preceding argument shows that a whole umber (larger than 1) is either prime or can be written as the product of primes *at least one way.*



GURE 4-4

The problem of determining whether there is *at most one way* to do this, ough it is quite interesting, is not presented here. You will be given ample portunity to investigate whether this unique factorization into primes holds certain subsets of the whole numbers. We will clarify the issue for the whole mbers themselves by stating the Unique Factorization Theorem (also called e Fundamental Theorem of Arithmetic):

Unique Factorization Theorem

> Any whole number (greater than 1) is either prime or can be written as the product of primes in exactly one way, except for the order of the factors.

Oystein Ore in *Invitation to Number Theory* [23] provides a straightforward proof of this theorem for the interested reader.

The Unique Factorization Theorem tells us that numbers which are not already prime factor into primes in a unique way, but it doesn't tell us how to find them. Our next example provides a number of helpful hints for this process.

EXAMPLE 4-5

Write (a) 231, (b) 229, and (c) 279 each as a product of primes.

SOLUTION

(a) We try to find prime factors of 231 beginning with 2:

2 is not a factor, as the last digit is 1.

3 is a factor, since the sum of the digits is 6.

Write $231 = 3 \times 77$. We recognize 77 as 7×11, so $231 = 3 \times 7 \times 11$. Since 3, 7, and 11 are all primes, no further factorization is possible.

(b) We try to find prime factors of 229 beginning with 2:

2 is not a factor, as the last digit is 9.

3 is not a factor, since the sum of the digits is 13.

5 is not a factor. Why?

7 is not a factor, since 229 is 19 more than 210.

(We know $7 \mid 210$, so if $7 \mid 229$ it would have to divide the difference $229 - 210$, which is 19.)

11 is not a factor, since 229 is 9 more than 220.

(We know $11 \mid 220$, so if $11 \mid 229$ it would have to divide the difference $229 - 220$, which is 9.)

13 is not a factor, since 229 is 31 less than 260.

(We know $13 \mid 260$, so if $13 \mid 229$ it would have to divide the difference $260 - 229$, which is 31.)

The next prime is 17. We know 229 has no factors (other than 1) smaller than 17, because we have already tried all the primes less than 17. But multiplying two factors, each one at least 17, would give a product which is at least $17 \times 17 = 289$. Hence 229 is not the product of two smaller primes, so 229 must itself be a prime.

(c) We try to find prime factors of 279 beginning with 2:

2 is not a factor, as the last digit is 9.

3 is a factor since the sum of the digits is 18.

Write $279 = 3 \times 93$. Now we wish to check if 93 has any prime factors. We have already eliminated 2 as a possibility, but there could be another factor of 3. In fact there is, and we get $279 = 3 \times 3 \times 31$, or $3^2 \times 31$.

Some observations from this rather long example are in order.

(1) *We test only primes as divisors.* We didn't try 4 or 6. Why? If some composite divides the number, so would the prime factors of this composite number. For instance, if a number is divisible by 6, it is divisible by 2 and by 3. In part (a) of Example 4-5 it is true that $21 \mid 231$, but $21 = 3 \times 7$. Long before it would have been necessary to try 21 as a divisor, we found that $3 \mid 231$ and $7 \mid 231$.

(2) *There is no need to try primes which when squared exceed the given number.* This situation was dealt with in part (b). Another way of looking at it is like this: Suppose in factoring 229 that 31 is one of the prime factors. What would the other factor be? Since 31 goes into 229 about 7 or 8 times, the other factor would be about 7 or 8. But 7 is not a factor (we tried it), and 8 is not a factor (because a number divisible by 8 is divisible by 2, which we tried). In fact we accounted for all factors up to 17, and 17×31 is much too big.

(3) *A particular prime may occur more than once* in the factorization. This is clear in view of part (c).

We now turn to the question of how many primes there are. Example 4-6 will construct a sequence of four consecutive whole numbers, none of which is prime, in order to illustrate a technique to use to show that there are strings of consecutive composites which are as (finitely) long as we may like.

EXAMPLE 4-6

Construct a string of at least four consecutive composite numbers.

SOLUTION

Consider the number $1 \times 2 \times 3 \times 4 \times 5$, which is 120. Since it has factors of 2, 3, 4, and 5, clearly each of the numbers 2, 3, 4, and 5 divides 120. By the divisibility property for sums we have:

$2 \mid 120$ and $2 \mid 2$, so $2 \mid 122$

$3 \mid 120$ and $3 \mid 3$, so $3 \mid 123$

$4 \mid 120$ and $4 \mid 4$, so $4 \mid 124$

$5 \mid 120$ and $5 \mid 5$, so $5 \mid 125$

Now the numbers 122, 123, 124, and 125 each have a divisor other than 1 which is smaller than that number, so none of them is prime.

Actually this is only part of a longer sequence of consecutive composites 114, 115, 116, 117, . . . , 126, which might be easy to find by trial and error, but the method of the previous example can provide impressive results without trial and error, as shown in Example 4-7.

Construct a string of at least 100 consecutive composite numbers.

Consider the number $1 \times 2 \times 3 \times 4 \times \ldots \times 100 \times 101$, which we will call m. Since m has factors of 2, 3, 4, . . . , 100, 101, clearly each of the numbers 2, 3, 4, . . . , 100, 101 divides m. By the divisibility property for sums, we have

$$\begin{array}{rcrcr}
2 \mid m & \text{and} & 2 \mid 2, & \text{so} & 2 \mid (m + 2) \\
3 \mid m & \text{and} & 3 \mid 3, & \text{so} & 3 \mid (m + 3) \\
4 \mid m & \text{and} & 4 \mid 4, & \text{so} & 4 \mid (m + 4) \\
 & & & \ldots & \\
100 \mid m & \text{and} & 100 \mid 100, & \text{so} & 100 \mid (m + 100) \\
101 \mid m & \text{and} & 101 \mid 101, & \text{so} & 101 \mid (m + 101)
\end{array}$$

Now the 100 consecutive numbers $m + 2, m + 3, m + 4, \ldots, m + 100, m + 101$ each have a divisor other than 1 which is smaller than that number, so none of them is prime.

Of course, the technique of Examples 4-6 and 4-7 could be used to find a string of composites of any desired (finite) length. It might appear that prime numbers would eventually vanish altogether. It may be surprising, therefore, that a proof using a similar technique shows that the list of primes never ends! In other words, we will show that

There is no largest prime.

To establish this result, we will argue, as Euclid did thousands of years ago, that as soon as we assume that there is a largest prime we can find another prime which is larger. Suppose there *were* a largest prime. Call it p. Let k be the product of all the primes including p. Then $k = 2 \times 3 \times 5 \times 7 \times 11 \times \ldots \times p$, so every prime number from 2 through p divides k. Now consider the number $k + 1$.

This number is not divisible by 2, for if 2 divided both k and $k + 1$ it would have to divide their difference, which is 1. But $2 \nmid 1$, hence $2 \nmid (k + 1)$. In the same way, 3 cannot divide $k + 1$, nor can 5, 7, 11, or any of the primes up to and including p. Thus, either $k + 1$ has no prime factors (other than itself) so it is a prime, or it has prime factors larger than those listed. Either way, there is a prime larger than p; hence, the assumption that there is a largest prime is impossible. Since there is no largest prime, it follows that the list of primes continues indefinitely; namely, the number of primes is infinite.

Methods of finding primes and other related questions have intrigued athematicians for centuries. For instance, the deceptively simple statement alled **Goldbach's conjecture**) that every even number greater than 2 is the :m of two primes has yet to be proven true or false. It is easy to see that it holds r the first few even numbers greater than 2:

$$4 = 2 + 2$$
$$6 = 3 + 3$$
$$8 = 3 + 5$$
$$10 = 5 + 5$$
$$12 = 5 + 7$$

is and some other interesting queries will be raised in the problems.

EXERCISES AND PROBLEMS 4-2

DEFINITION

1. The process for finding primes described below, called the **sieve of Eratosthenes**, was in use thousands of years ago and is still used today in computer programs written to generate primes. To find all primes less than or equal to 100, list the numbers 1 through 100.

1	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

Cross off 1, since the definition of prime excludes it. Beginning with the number 4, cross off every second number, since these are each divisible by 2. Cross off every third number, beginning with 6. Then the first three rows will look like this:

~~1~~	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~~

(a) Which numbers are crossed off more than once?

(b) In continuing the process it is unnecessary, after doing the above, to cross off the multiples of 4; namely, 8, 12, 16, . . . , 100. Why?

(c) Cross off all multiples of 5 (except 5 itself). Do the same for multiples of other primes.

- (d) What was the smallest prime for which you found all its multiples (other than itself) already crossed off? Compare this result with the observations which follow Example 4-5.
- (e) Examine your sieve and list all primes less than 100.

2. Use the sieve method to find all primes less than 200.

3. The sieve of Eratosthenes is based on which divisibility property?

4. Find (if possible)
   - (a) the smallest prime (b) the largest prime
   - (c) all primes between 90 and 100
   - (d) $\{1, 2, 3, 4, \ldots, 10\} \setminus \{\text{primes less than } 10\}$

5. Mathematicians have long tried to find a formula which consistently yields primes. The formula $p(n) = n^2 - n + 41$ yields primes for $n = 0, 1, 2, 3, 4, \ldots, 40$. For instance $p(0) = 0^2 - 0 + 41 = 41$ is prime, $p(1) = 1^2 - 1 + 41 = 41$ is prime, $p(2) = 2^2 - 2 + 41 = 43$ is prime.
   - (a) Find $p(3)$, $p(4)$, $p(5)$, $p(6)$, and $p(7)$.
   - (b) Find $p(41)$. Is it prime? Support your answer.

6. (a) Show that the formula $f(n) = n^2 + n + 11$ yields primes for $n = 0, 1, 2$, and 3. (See Problem 5.) Find the smallest whole number n for which $f(n) = n^2 + n + 11$ is *not* a prime.
   - (b) Repeat part (a) for $f(n) = n^2 + n + 17$.
   - (c) $f(n) = n^2 - 79n + 1601$ yields primes for $n = 0, 1, 2, 3, \ldots, 79$. Show that $f(80)$ is *not* a prime. (Hint: It's a perfect square.)

   (Note: There is no known formula that consistently yields different primes for all values of n.)

PRIME FACTORIZATION

7. Find a factor tree for 60 different from those in Figure 4-3.

8. Find a factor tree for (a) 28 (b) 168.

9. When factoring a given number into primes, some students like to organize their work like this:

$$\begin{array}{r} 5 \\ 3\overline{)15} \\ 2\overline{)30} \\ 2\overline{)60} \end{array}$$

   Divide by 2 as often as possible, then 3, then 5, and so on for each prime to conclude $60 = 2 \times 2 \times 3 \times 5$. This method is used below to factor 294 into primes:

$$\begin{array}{r} 7 \\ 7\overline{)\ 49} \\ 3\overline{)147} \\ 2\overline{)294} \end{array}$$

   Thus $294 = 2 \times 3 \times 7 \times 7$.
   Use this method to factor the following into primes:
   (a) 66 (b) 72 (c) 153 (d) 459 (e) 1000.

10. Write the number whose prime factorization is given by
    - (a) $2 \times 3 \times 5 \times 7$ (b) $2^3 \times 3^2$
    - (c) $2^5 \times 5^5$ (d) $3^4 \times 7 \times 11$

11. Select the best answers from the choices given in parentheses: To test whether 149 is prime, one could divide by all (*whole numbers, primes, odd numbers*) less than (*11, 13, 15, 75, 149, 150*).

12. Factor each of the following into primes: (a) 143 (b) 151 (c) 493

13. Make a flowchart for factoring a given number into primes, using the observations which follow Example 4-5.

14. (a) Factor 100 into primes. (b) Factor each divisor of 100 into primes.
    (c) What relationship exists between parts (a) and (b)?
    (d) Suppose $n = 17^5 \times 19^7$. If m is a divisor of n, what can you say about the prime factorization of m?

COUNTING DIVISORS

15. (a) How many divisors does 0 have? (b) 0 divides how many numbers?

16. Complete the following chart:

Number	Prime Decomposition	Divisors	Number of Divisors
2	2	1, 2	2
3	3	1, 3	2
4	2^2	1, 2, 4	3
5			
6			
7			
8			
9			
10			
11			
12			
16			
20			
24	$2^3 \times 3$	1, 2, 3, 4, 6, 8, 12, 24	8
32			
60			
72			
100			

17. Which whole number from 1 through 100 has the most divisors? Which has the most prime factors?

18. Tell how many divisors each of the following numbers has:
    (a) $5^2 \times 3$ (b) $5^2 \times 3^2$ (c) $5^2 \times 3^3$ (d) $13^5 \times 17^{11}$
    (e) $2^3 \times 3^4 \times 5 \times 7^{30}$

19. Find the smallest whole number that has exactly
    (a) 1 divisor
    (b) 2 divisors
    (c) 3 divisors
    (d) 4 divisors
    (e) 5 divisors
    (f) 6 divisors
    (g) 7 divisors
    (h) 8 divisors.

20. Characterize (describe by some rule) all whole numbers which have exactly
    (a) 2 divisors
    (b) 3 divisors
    (c) 5 divisors
    *(d) 4 divisors
    *(e) 6 divisors
    *(f) 12 divisors.

PROPERTIES

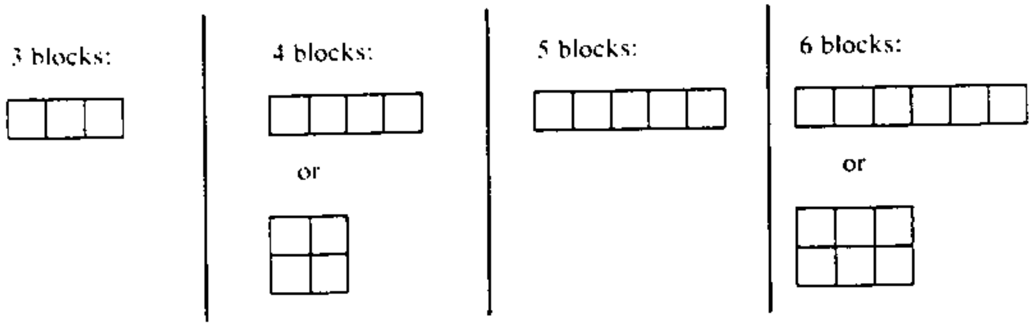
21. Refer to the proof that there is no largest prime. Note that if p were assumed to be 5, $k = 2 \times 3 \times 5 = 30$, so $k + 1 = 31$, which is a prime larger than 5. Find $k + 1$ if p were assumed to be 7.

22. True or False? Support your answer. "Every whole number (greater than 1) is either prime or can be expressed as the *sum* of primes in exactly one way."

*23. Let $S = \{\text{whole numbers}\} \setminus \{2\}$; that is, S is the set of all whole numbers except 2. Then $S = \{0, 1, 3, 4, 5, 6, 7, 8, \ldots\}$. We will call a member of S an **S-prime** if it is greater than 1 and cannot be written as the product of two smaller members *of* S. Thus the first few S-primes are 3, 4, 5, 6, and 7. (Though $6 = 2 \times 3$ it is an S-prime since the factor 2 is not in S.)
   - (a) Do the closure, commutative, associative, and identity properties for multiplication hold for the set S?
   - (b) Find the smallest member of S which is not an S-prime.
   - (c) Find a member of S which factors into S-primes in two ways. This shows that S fails to satisfy what property or theorem?
   - (d) Find a member of S which factors into S-primes in three ways.
   - (e) When does a member of S factor into S-primes in exactly one way?
   - (f) Does the sum property of divisibility hold in S? Support your answer.
   - (g) Does the difference property of divisibility hold in S? Support your answer.
   - (h) What happens if instead of 2 some other prime, like 7, is removed?
   - (i) What happens if two or more primes are simultaneously removed?

MATERIALS AND CALCULATORS

*L*24. Use a set of blocks (cubes) in this problem. Show all "houses" (rectangles) which can be made from up to 12 blocks, as in the examples below. (See also Figure 4-1.)



Which whole numbers will have more than one representation?

*C*25. Notice that for the first few values of n, the number obtained by adding 1 to the product of the first n primes is itself a prime.

n	(Product of First n Primes) + 1
1	$2 + 1 = 3$
2	$2 \times 3 + 1 = 7$
3	$2 \times 3 \times 5 + 1 = 31$
4	$2 \times 3 \times 5 \times 7 + 1 = 211$

- (a) Determine the value when n is 5.
- (b) Determine the value when n is 6. Show that this value is not prime by finding a factor between 50 and 60.

*C*26. (Note: It is recommended that you do the parts to this question in sequence, since they are related.) Use repeated multiplication on a calculator to help answer these questions.
   (a) What are the last two digits of 2^{22}?
   (b) What are the last two digits of 2^{23}?
   (c) What are the last two digits of 2^{24}?
   (d) What are the last two digits of 102^{22}?
   (e) What are the last two digits of 12^{22}?
   (f) What are the last two digits of 372^{22}?
   (g) What is the last digit of $39{,}407^{99}$?
   (h) What are the last two digits of $39{,}407^{99}$?
   (i) What is the last digit of $83{,}903^{99}$?
   (j) What are the last two digits of $83{,}903^{99}$?

*P*27. Write a program that finds the first 50 prime numbers.

*P*28. Write a program that factors a given number into primes.

*P*29. Use your program of Problem 28 to factor these numbers into primes:
   (a) 221 (b) 441 (c) 899 (d) 907 (e) 99,299 (f) 2,893,443

PROBLEM SOLVING EXTENSIONS

30. Two primes whose difference is 2 are called **twin primes**. Thus 5 and 7, 11 and 13, and 29 and 31 are three pairs of twin primes. Find all pairs of twin primes less than 100.

31. 2 and 3 are primes whose difference is 1. Find all such pairs of primes less than 1,000,000.

32. An elusive result that mathematicians have been unable to prove either true or false is older than the U.S. Declaration of Independence. Called Goldbach's conjecture, it claims that each even number greater than 2 is the sum of two primes. Some examples were given on page 133.
   (a) Verify that it holds for even numbers through 50.
   (b) Assuming Goldbach's conjecture is true, prove that each odd whole number greater than 6 is the sum of three primes.

33. Can you find whole numbers m and n such that $3^m = 7^n$?

34. For what type of whole numbers n is it true that n divides $(n - 1)!$? For example, 8 divides $7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$, but 5 does not divide $4 \times 3 \times 2 \times 1$. (See Problem 20, Section 4-1.)

35. Find a string of 1000 consecutive composite numbers.

36. Is it possible to make a magic square with the first nine prime numbers? (In a magic square all rows, columns, and main diagonals have the same sum. (See Problems 20 and 21, Section 3-2.) Do it or explain why it cannot be done.

4-3

GREATEST COMMON DIVISOR AND LEAST COMMON MULTIPLE

The discussion and problems of the previous section provide several techniques that enable us to split a given whole number into primes, the "building blocks" the whole numbers with respect to multiplication. Once we have the prime ctors, it is easy to find all the divisors of a given number.

With respect to our goals, finding common divisors (and multiples) of two or more numbers is most important. For instance, 18 and 24 have several common divisors:

divisors of 18 = 1, 2, 3, 6, 9, 18

divisors of 24 = 1, 2, 3, 4, 6, 8, 12, 24

common divisors of 18 and 24 = 1, 2, 3, 6

Any two whole numbers will always have at least one common divisor. (What is it?) Among all the common divisors, there will always be a largest one, since the divisors cannot exceed the numbers themselves. For these reasons, it is meaningful to talk about a greatest common divisor for two (or more) numbers.

> The **greatest common divisor** of two (or more) whole numbers is the largest whole number which divides both (all) of them.

The greatest common divisor is usually abbreviated **GCD**. It is sometimes called the **greatest common factor (GCF)**.

EXAMPLE 4-8

Find each of the following:

(a) GCD (6, 8) (b) GCD (20, 30) (c) GCD (24, 28, 30)

(d) GCD (4, 9) (e) GCD (153, 204)

SOLUTION

(a) divisors of 6 = 1, 2, 3, 6
divisors of 8 = 1, 2, 4, 8
common divisors of 6 and 8 = 1, 2
GCD (6, 8) = 2

(b) divisors of 20 = 1, 2, 4, 5, 10, 20
divisors of 30 = 1, 2, 3, 5, 6, 10, 15, 30
common divisors of 20 and 30 = 1, 2, 5, 10
GCD (20, 30) = 10

(c) divisors of 24 = 1, 2, 3, 4, 6, 8, 12, 24
divisors of 28 = 1, 2, 4, 7, 14, 28
divisors of 30 = 1, 2, 3, 5, 6, 10, 15, 30
common divisors of 24, 28, and 30 = 1, 2
GCD (24, 28, 30) = 2

(d) divisors of 4 = 1, 2, 4
divisors of 9 = 1, 3, 9
common divisors of 4 and 9 = 1
GCD (4, 9) = 1 (When no prime divides both of the given numbers, they are called **relatively prime**.)

(e) divisors of 153 = 1, 3, 9, 17, 51, 153
divisors of 204 = 1, 2, 3, 4, 6, 12, 17, 34, 51, 68, 102, 204
common divisors of 153 and 204 = 1, 3, 17, 51
GCD (153, 204) = 51

[redacted]

While the method of Example 4-8 is satisfactory for many problems, other procedures work better in some cases, especially for larger numbers. Among them is a process where the GCD is constructed from the prime factors. Another method is the Euclidean algorithm, where the GCD is calculated directly by successive applications of the division algorithm.

We introduce the construction method by recalling that the exercises of the previous section revealed a relationship between the prime factors of a number and the prime factors of its divisors. As one example (see also Problem 14, Section 4-2) consider the divisors of 84, whose prime factorization is $2^2 \times 3 \times 7$.

Divisor of 84	*Prime Factorization of Divisor*
1	1
2	2
3	3
4	2^2
6	2×3
7	7
12	$2^2 \times 3$
14	2×7
21	3×7
28	$2^2 \times 7$
42	$2 \times 3 \times 7$
84	$2^2 \times 3 \times 7$

Note that each divisor of 84 (except 1, the trivial divisor) is either a prime factor of 84 or it factors into a product consisting of some or all of the prime factors of 84. Suppose, to the contrary, that 84 had some other divisor *d*, and that *d* had a different prime factor, say 13. Then 13 would divide *d* and *d* would divide 84, so by the transitive property of divisibility 13 would divide 84. This means 84 would equal 13 multiplied by some other primes. But then 84 would factor into primes in two ways (with and without the prime factor 13), which is impossible according to the Unique Factorization Theorem. Thus it is absurd for any divisor of 84 to have a factor of 13. By a similar argument, each divisor of 84 (except 1) must have as its prime factors some choice from among 2, 3, and 7. What is argued here for 84 is valid as well for all whole numbers; namely, the divisors (other than 1) of a whole number *w* must either be prime factors of *w* or be products of some of the prime factors which give *w* itself.

This observation makes finding the GCD of two or more numbers considerably easier, for we can construct it from the common prime factors of the numbers.

EX

Use prime factorization to find the GCD of

(a) 20 and 30 (b) 153 and 204

(c) $2^5 \times 3^6 \times 11^8$ and $2^3 \times 3^{17} \times 7^2 \times 11$ (d) 261 and 377

SOLU

(a) $20 = 2^2 \times 5$, so any divisor of 20 can have at most two 2's and one 5 (and no other primes) as prime factors. Since $30 = 2 \times 3 \times 5$, any divisor of 30 can have at most one 2, one 3, and one 5 (and no other primes) as prime factors. Thus a number which is a common factor of 20 and 30 must satisfy all these conditions and can have at most one 2 and one 5 (and no other primes) as prime factors, so the common factors are 1, 2, 5, and 10. To find the GCD, the *greatest* of the common divisors, we use both of the possible factors, 2 and 5, and obtain 10. As we would expect, the list of common divisors and the GCD are consistent with the results of Example 4-8.

(b) $153 = 3^2 \times 17$ and $204 = 2^2 \times 3 \times 17$. As before, to find the GCD we construct the number that uses as many of the common prime factors as possible. We may select no 2's, one 3, and one 17, so GCD (153, 204) = $3 \times 17 = 51$.

(c) A common divisor of $2^5 \times 3^6 \times 11^8$ and $2^3 \times 3^{17} \times 7^2 \times 11$ can have at most three 2's, six 3's, no 7's, one 11, and no other prime factors. The greatest number satisfying these conditions is $2^3 \times 3^6 \times 11$, and we are content to leave our answer in this form.

(d) $261 = 3^2 \times 29$ is easy to factor by applying the divisibility test for 3 (or for 9). We could painstakingly factor 377, which is more difficult, but the only possible *common* prime factors (which are all we care about at this point) are 3 and 29. 377 fails the divisibility test for 3, but it does divide by 29 ($377 = 29 \times 13$). So GCD (261, 377) = 29.

These examples suggest a three-step procedure to construct the GCD of two (or more) numbers.

To Construct the GCD of Two (or More) Numbers

1. Factor each number into primes.
2. Select each prime the least number of times that it appears on any of the lists.
3. Express the GCD as the product of the primes that result from step 2.

Our next example applies this process to finding the GCD of three numbers.

EXAMPLE 4

Use prime factorization to find

(a) GCD (54, 72, 90) (b) GCD (36, 49, 56)

SOLUTION

(a) $54 = 2 \times 3^3$

$72 = 2^3 \times 3^2$

$90 = 2 \times 3^2 \times 5$

$\text{GCD}(54, 72, 90) = 2 \times 3^2 = 18$

(b) $36 = 2^2 \times 3^2$

$49 = 7^2$

$56 = 2^3 \times 7$

The least number of times 2 occurs is zero (on the list for 49).

The least number of times 3 occurs is zero (on the list for 49).

The least number of times 7 occurs is zero (on the list for 36).

Thus there are no common prime factors, so GCD (36, 49, 56) = 1.

The **Euclidean algorithm** is a good method for finding the GCD of two numbers that are hard to factor. We will present an example and then analyze how and why it works.

EXAMPLE 4-11

Use the Euclidean algorithm to find the GCD (493, 221).

SOLUTION

(1) $493 = 221 \times 2 + 51$

(2) $221 = 51 \times 4 + 17$

(3) $51 = 17 \times 3 + 0$

Therefore GCD (493, 221) = 17.

We now offer an explanation of what happened!

(1) Divide 493 by 221. Use the division algorithm to express 493 as a multiple of 221 plus a remainder that is less than 221.

(2) Divide 221 by 51. Use the division algorithm to express 221 as a multiple of 51 plus a remainder that is less than 51.

(3) Divide 51 by 17. Use the division algorithm to express 51 as a multiple of 17 plus a remainder that is less than 17. This time the remainder is 0, so the process terminates.

So why is 17 the GCD (493, 221)? We will answer this by examining the Euclidean algorithm one step at a time. In the first step we wrote

$$493 = 221 \times 2 + 51.$$

We show that the list of divisors of both 493 and 221 is precisely the same as the list of divisors of both 221 and 51:

Suppose $p \mid 493$ and $p \mid 221$. Then $p \mid (221 \times 2)$ (see Problem 12c, Section 4-1), and consequently $p \mid (493 - 221 \times 2)$ (see Problem 12a, Section 4-1). In other words, $p \mid 51$. This shows that any number that divides both 493 and 221 will also divide both 221 and 51.

Now suppose $s \mid 221$ and $s \mid 51$. Then $s \mid (221 \times 2)$ and consequently $s \mid (221 \times 2 + 51)$, by the divisibility of a sum property. In other words, $s \mid 493$. This shows that any number that divides both 221 and 51 will also divide both 493 and 221.

Summarizing, we see that the list of divisors of both 493 and 221 and the list of divisors of both 221 and 51 must be identical, so in particular, GCD (493, 221) = GCD (221, 51).

In this same way we can show that in general, if $a = b \times q + r$, then GCD (a, b) = GCD (b, r). Returning to our original example, we can apply this principle several times to obtain

$$\begin{aligned} \text{GCD } (493, 221) &= \text{GCD } (221, 51) \\ &= \text{GCD } (51, 17) \\ &= \text{GCD } (17, 0) \\ &= 17 \end{aligned}$$

Let's double our number of examples of the Euclidean algorithm by presenting another one:

EXAMPLE 4.12

Use the Euclidean algorithm to find the GCD (1776, 1492).

SOLUTION

$$\begin{tikzcd}[column sep=small]
1776 & = & 1492 \arrow[dll] & \times 1 + & 284 \arrow[dll] \\
1492 & = & 284 \arrow[dll] & \times 5 + & 72 \arrow[dll] \\
284 & = & 72 \arrow[dll] & \times 3 + & 68 \arrow[dll] \\
72 & = & 68 \arrow[dll] & \times 1 + & 4 \arrow[dll] \\
68 & = & 4 & \times 17 + & 0
\end{tikzcd}$$

Applying our new principle five times gives:

$$\begin{aligned} \text{GCD } (1776, 1492) &= \text{GCD } (1492, 284) \\ &= \text{GCD } (284, 72) \\ &= \text{GCD } (72, 68) \\ &= \text{GCD } (68, 4) \\ &= \text{GCD } (4, 0) \\ &= 4 \end{aligned}$$

With three methods of finding common divisors at our disposal, we will now investigate the topic of common multiples.

Finding the multiples of a single number is straightforward. For example, the multiples of 6 are

$$\begin{aligned} 6 \times 0 &= 0 \\ 6 \times 1 &= 6 \\ 6 \times 2 &= 12 \\ 6 \times 3 &= 18 \\ 6 \times 4 &= 24 \end{aligned}$$

We can find common multiples of two (or more) numbers by methods much like those used to find common divisors. For instance, to find common multiples of 18 and 24, we could list the multiples of each and search for common ones:

multiples of 18: 0, 18, 36, 54, 72, 90, 108, 126, 144, 162, . . .

multiples of 24: 0, 24, 48, 72, 96, 120, 144, 168, . . .

common multiples of 18 and 24: 0, 72, 144, . . .

One difference between these results and those for finding common divisors is immediately noticeable: the list of multiples is endless, as is the list of common multiples. To show that the list of common multiples never ends, we will show that every multiple of 72 is a common multiple of 18 and 24.

Let $72k$ be a multiple of 72, where k is a whole number. Then

$$72k = (18 \times 4)k = 18 \times 4k \text{ and}$$

$$72k = (24 \times 3)k = 24 \times 3k$$

Since k is a whole number, so are $4k$ and $3k$. Thus there is a whole number ($4k$) which multiplied by 18 gives $72k$, so 18 divides $72k$ ($72k$ is a multiple of 18). Also there is a whole number ($3k$) which shows that 24 divides $72k$ ($72k$ is a multiple of 24).

Clearly, there is no greatest common multiple of 18 and 24. If $72k$ is some multiple of 72, then $72(k + 1)$ will be a larger multiple. It so happens (as when finding lowest common denominators for fractions) that we are interested this time in the *least* common multiple. Since 0 is a multiple of each whole number, 0 is technically the least of all common multiples for any two (or more) numbers. This fact is of little use to us. So henceforth when we use the term "least common multiple" we exclude 0.

Is there always a least common multiple for any two whole numbers? Given some whole numbers, their product is always a common multiple. For instance, given 7 and 9, 63 is a multiple of 7 and 63 is a multiple of 9. Similarly, the product of any two whole numbers is a common multiple. Now, among all of the common multiples (we exclude 0), there will always be a smallest one, since every (non-empty) set of whole numbers has a least member. This makes the following definition meaningful:

> The **least common multiple** of two (or more) whole numbers is the smallest whole number (other than 0) which is a multiple of both (all) of them.

The least common multiple is usually abbreviated **LCM**.

Find each of the following:

(a) LCM (6, 8) (b) LCM (20, 30) (c) LCM (24, 28, 30)

(a) multiples of 6 = 0, 6, 12, 18, 24, 30, 36, 42, 48, 54, . . .
multiples of 8 = 0, 8, 16, 24, 32, 40, 48, 56, . . .
common multiples of 6 and 8 = 0, 24, 48, . . .
LCM (6, 8) = 24

(b) multiples of 20 = 0, 20, 40, 60, 80, 100, 120, . . .
multiples of 30 = 0, 30, 60, 90, 120, 150, 180, . . .
common multiples of 20 and 30 = 0, 60, 120, 180, . . .
LCM (20, 30) = 60

(c) multiples of 24 = 0, 24, 48, 72, 96, 120, 144, 168, 192, 216, 240, . . .
multiples of 28 = 0, 28, 56, 84, 112, 140, 168, 196, 224, 252, 280, . . .
multiples of 30 = 0, 30, 60, 90, 120, 150, 180, 210, 240, 270, 300, . . .
common multiples of 24, 28, and 30 = 0, ?, . . .

Writing out eleven multiples of each did not produce a single non-trivial common multiple. We do know that 24 × 28 × 30 = 20160 is a common multiple, but is it the smallest?! We will defer the solution of this problem in hopes of finding a better way.

This last example shows the need for other methods. We found when considering the GCD that it was helpful to factor the given numbers into primes. Will this help us here? Let's go back to the easier example. We found LCM (6, 8) = 24. Factoring these three numbers into primes, we see

$$6 = 2 \times 3$$
$$8 = 2^3$$
$$24 = 2^3 \times 3$$

What is the relationship between the prime factors of 6 and 8 and the prime factors of 24, the LCM of 6 and 8? If you do not recognize the pattern at this point, you might try several more examples. Additional clues for determining how to construct the LCM from the prime factors will be given in the problems.

We know that the Euclidean algorithm always yields the GCD of two numbers. Once the GCD is known, a simple computation gives the LCM, but again we will give you the opportunity to discover this for yourself.

EXERCISES AND PROBLEMS 4-3

DEFINITION

1. Which are bigger, divisors of 12 or multiples of 12? Are there any exceptions? Which is bigger, GCD (12, 15) or LCM (12, 15)? If *a* and *b* are two different whole numbers, which is bigger, GCD (*a*, *b*) or LCM (*a*, *b*)?

2. Use the method of Example 4-8 to find
   (a) GCD (8, 10) (b) GCD (40, 60) (c) GCD (25, 36)
   (d) GCD (24, 36, 42) (e) GCD (232, 261).

3. Any two whole numbers have one common divisor. What is it?

4. Find the GCD of each pair of numbers by any method. (This problem is adapted from a sixth grade text.)
   (a) 36, 42 (b) 20, 36 (c) 90, 315 (d) 72, 450
   (e) 175, 105 (f) 525, 441 (g) 152, 228

5. Find by any method:
   (a) GCD (14, 28) (b) GCD (72, 90, 96) (c) GCD (312, 468, 1092)

6. Determine a three-step procedure for constructing the LCM of two (or more) numbers based on factoring each of the numbers into primes. (Hint: Beginning with the three-step construction of the GCD given on page 140, few words need to be replaced to make this a method for finding the LCM.)

7. Use the method of construction from prime factorization that you have developed to find the LCM of each pair of numbers.
   (a) 15, 20 (b) 63, 72 (c) 98, 126 (d) 152, 228
   (e) 21, 6 (f) 20, 24 (g) 14, 28 (h) 136, 153

8. (a) Use this method to show LCM (24, 28, 30) = 840.
   (b) Find LCM (90, 105, 120).

9. True or False? The LCM of any two positive whole numbers m and n is the smallest positive multiple of m that has n as a factor.

10. (a) When does LCM $(a, b) = a \times b$? (b) When does LCM $(a, b) = a$?
    (c) When does GCD $(a, b) = a \times b$? (d) When does GCD $(a, b) = a$?

11. According to the definition of LCM, what is
    (a) LCM (0, 5) (b) LCM (0, 0)?

EUCLIDEAN ALGORITHM

12. Use the Euclidean algorithm to find the GCD of each pair of numbers:
    (a) 36, 42 (b) 737, 871 (c) 4189, 4307
    (d) 89, 144 (e) 1746, 9846

13. The Euclidean algorithm works to find the GCD of two numbers. Is it possible to find the GCD of three (or four or five) numbers by finding the GCD's for two numbers at a time? Explain. (Hint: It may help to think in terms of the method of factoring into primes. Try some examples by this method.)

*14. Draw a flowchart for using the Euclidean algorithm to find the GCD of two numbers.

15. (a) If $493 = 221 \times 2 + 51$, show that GCD (493, 221) = GCD (221, 51).
    (b) If $a = b \times q + r$, show that GCD (a, b) = GCD (b, r).

PROPERTIES AND RELATIONSHIPS

16. (a) What are the prime factors of 10?
    (b) 10, 20, and 30 are some of the positive multiples of 10. List all of the positive multiples of 10 up to 100.
    (c) Factor each of these multiples of 10 into primes.
    (d) Which prime factors occur on every one of the lists?

17. As in the previous problem, examine the prime factors of 12 and the prime factors of the positive multiples of 12 (up to 120).

18. Based on the two preceding problems (and other examples, if you wish), state a relationship between the prime factors of a number and the prime factors of its multiples. Give an argument to show that this relationship is generally true.

19. (a) Complete the following chart:

a	b	GCD (a, b)	LCM (a, b)	GCD (a, b) × LCM (a, b)
2	3	1	6	6
3	4			
4	6			
8	12			
42	56			
50	60			

(b) Look for a relationship between the last column and the first two.
(c) Does this relationship hold for all whole numbers? Why?

20. Use the results of the preceding problem to answer the following:
(a) If GCD (493, 221) = 17 (see Example 4-11), find LCM (493, 221).
(b) If GCD (1492, 1776) = 4 (see Example 4-12), find LCM (1492, 1776).
(c) Find LCM (737, 871). (See Problem 12b.)

21. The LCM of two numbers is $2^3 \times 3^2 \times 7 \times 11 \times 13$. The GCD of the same two numbers is $2 \times 3 \times 7$. If one of the numbers is $2^3 \times 3 \times 7 \times 11$, what is the other number?

22. We said earlier that two numbers are called relatively prime if their GCD is 1. Thus 4 and 9 are relatively prime (though neither is prime). Find all numbers less than 20 which are relatively prime with 12.

23. What property of multiplication justifies each of the following statements that were made in showing that 72 is a common multiple of 18 and 24?
(a) $(18 \times 4)\,k = 18 \times 4k$
(b) Since k is a whole number, so are $4k$ and $3k$.

24. Suppose we write "aLb" to mean LCM (a, b) and "aGb" to mean GCD (a, b). For example, 3L4 = 12, 6L8 = 24, 6G8 = 2, 4G9 = 1. Which of the following properties hold?
(a) The set of whole numbers is closed under L.
(b) The set of whole numbers is closed under G.
(c) L is commutative.
(d) G is commutative.
(e) L is associative.
(f) G is associative.
(g) L distributes over G; namely, aL(bGc) = (aLb) G (aLc).
(h) G distributes over L; namely, aG(bLc) = (aGb) L (aGc).

MATERIALS AND CALCULATORS

*L*25. Which "train" involving Cuisenaire rods represents each of the following?
(a) GCD of a purple rod and a dark green rod.
(b) LCM of a purple rod and a dark green rod.

(c) GCD of a dark green rod and a blue rod.
(d) Describe the rod (or "train") which is the GCD of any two rods (or "trains").
(e) Describe the rod (or "train") which is the LCM of any two rods (or "trains").

26. Read "Star Patterns," in the January 1978 *Arithmetic Teacher* [47] and answer these questions:
  (a) How many paths are there for the star (10,4)? the star (15,6)?
  (b) How many orbits will there be in completing one path of (10,4)? of (15,6)?
  (c) Draw (10,4) and (15,6).
  (d) Construct a star having three paths and four orbits for each path.

*C*27. (a) Use a calculator to list the first ten positive multiples of 56 and of 42. Use this process to find LCM (56, 42).
  (b) Repeat for 133 and 209.

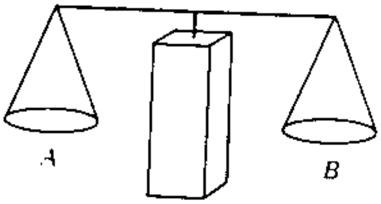
*C*28. Outline a systematic procedure for finding the GCD of two numbers on a calculator.

*P*29. Write a program which uses the Euclidean algorithm to find the GCD of two numbers. (Hint: See Problem 31, Section 3-6.)

*P*30. Use your program of Problem 29 to find the GCD of
  (a) 664 and 747
  (b) 65,039 and 78,091
  (c) 323 and 493
  (d) 9991 and 48,791
  (e) 1597 and 2584
  (f) 4,084,361 and 18,399,131

PROBLEM SOLVING EXTENSIONS

31.



You have a balance scale with an unlimited supply of 3-lb and 5-lb weights (but no other denominations). Examples: You can weigh 11 lb of potatoes on pan *A* by placing two 3-lb weights and one 5-lb weight on pan *B*. You can weigh 2 lb of potatoes by placing a 3-lb weight on one pan and a 5-lb weight on the other.
Is it possible to weigh the following amounts of potatoes? If so, tell how.
(a) 9 lb (b) 22 lb (c) 17 lb (d) 1 lb (e) 7 lb
(f) Describe all possible values which can be weighed, assuming there are no other limitations.

32. Repeat Problem 31 when there is an unlimited supply of 4-lb and 6-lb weights (but no other denominations).

33. Repeat Problem 31 when there is an unlimited supply of 6-lb and 9-lb weights.

34. Generalize the results of the three previous problems.