while 4, 8, 12, 16, ... are not. It is not difficult to see that the integer 60 can be factored into e-primes in two distinct ways; namely,

$$60 = 2 \cdot 30 = 6 \cdot 10.$$

Part of the trouble arises from the fact that Theorem 3-1 is lacking in the set E: $6 \mid 2 \cdot 30$, but $6 \nmid 2$ and $6 \nmid 30$.

This is an opportune moment to insert a famous result of Pythagoras. Mathematics as a science began with Pythagoras (569–500 B.C.), and much of the content of Euclid's *Elements* is due to Pythagoras and his School. The Pythagoreans deserve the credit for being the first to classify numbers into odd and even, prime and composite.

THEOREM 3-3 (Pythagoras). *The number $\sqrt{2}$ is irrational.*

Proof: Suppose to the contrary that $\sqrt{2}$ is a rational number; say, $\sqrt{2} = a/b$, where a and b are both integers with $\gcd(a, b) = 1$. Squaring, we get $a^2 = 2b^2$, so that $b \mid a^2$. If $b > 1$, then the Fundamental Theorem of Arithmetic guarantees the existence of a prime p such that $p \mid b$. It follows that $p \mid a^2$ and, by Theorem 3-1, that $p \mid a$; hence, $\gcd(a, b) \geq p$. We therefore arrive at a contradiction, unless $b = 1$. But if this happens, then $a^2 = 2$, which is impossible (we assume that the reader is willing to grant that no integer can be multiplied by itself to give 2). Our supposition that $\sqrt{2}$ is a rational number is untenable and so $\sqrt{2}$ must be irrational.

PROBLEMS 3.1

1. It has been conjectured that there are infinitely many primes of the form $n^2 - 2$. Exhibit five such primes.
2. Give an example to show that the following conjecture is not true: Every positive integer can be written in the form $p + a^2$, where p is either a prime or 1, and $a \geq 0$.
3. Prove each of the assertions below:
   (a) Any prime of the form $3n + 1$ is also of the form $6m + 1$.
   (b) Each integer of the form $3n + 2$ has a prime factor of this form.
   (c) The only prime of the form $n^3 - 1$ is 7. [*Hint:* Write $n^3 - 1$ as $(n - 1)(n^2 + n + 1)$.]
   (d) The only prime p for which $3p + 1$ is a perfect square is $p = 5$.

4. If $p \geq 5$ is a prime number, show that $p^2 + 2$ is composite. [*Hint:* p takes one of the forms $6k + 1$ or $6k + 5$.]
5. (a) Given that p is a prime and $p \mid a^n$, prove that $p^n \mid a^n$.
   (b) If gcd $(a, b) = p$, a prime, what are the possible values of gcd (a^2, b^2), gcd (a^2, b) and gcd (a^3, b^2)?
6. Establish each of the following statements:
   (a) Every integer of the form $n^4 + 4$, with $n > 1$, is composite.
   (b) If $n > 4$ is composite, then n divides $(n - 1)!$.
   (c) Any integer of the form $8^n + 1$, where $n \geq 1$, is composite. [*Hint:* $2^n + 1 \mid 2^{3n} + 1$.]
   (d) Each integer $n > 11$ can be written as the sum of two composite numbers. [*Hint:* If n is even, say $n = 2k$, then $n - 6 = 2(k - 3)$; for n odd, consider the integer $n - 9$.]
7. Find all prime numbers that divide 50!.
8. If $p \geq q \geq 5$ and p and q are both primes, prove that $24 \mid p^2 - q^2$.
9. (a) An unanswered question is whether there are infinitely many primes which are 1 more than a power of 2, such as $5 = 2^2 + 1$. Find two more of these primes.
   (b) A more general conjecture is that there exist infinitely many primes of the form $n^2 + 1$; for example, $257 = 16^2 + 1$. Exhibit five more primes of this type.
10. If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10. [*Hint:* p takes one of the forms $5k + 1$, $5k + 2$, $5k + 3$ or $5k + 4$.]
11. Another unproven conjecture is that there are an infinitude of primes which are 1 less than a power of 2, such as $3 = 2^2 - 1$.
   (a) Find four more of these primes.
   (b) If $p = 2^k - 1$ is prime, show that k is an odd integer, except when $k = 2$. [*Hint:* $3 \mid 4^n - 1$ for all $n \geq 1$.]
12. Find the prime factorization of the integers 1234, 10140, and 36000.
13. Consider the set S of all positive integers of the form $3k + 1$; that is, $S = \{1, 4, 7, 10, 13, 16, \ldots\}$. An integer $a > 1$ of S is said to be prime if it cannot be factored into two smaller integers, each of which belongs to S (thus, 10 and 25 are prime, while $16 = 4 \cdot 4$ and $28 = 4 \cdot 7$ are not).
   (a) Prove that any member of S is either a prime or a product of primes.
   (b) Give an example to show that it is possible for an integer in S to be factored into primes in more than one way.
14. It has been conjectured that every even integer can be written as the difference of two consecutive primes in infinitely many ways. For example,

$$6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013 = \cdots.$$

Express the integer 10 as the difference of two consecutive primes in fifteen ways.

15. Prove that a positive integer $a > 1$ is a square if and only if in the canonical form of a all the exponents of the primes are even integers.
16. An integer is said to be *square-free* if it is not divisible by the square of any integer greater than 1. Prove that
    (a) an integer $n > 1$ is square-free if and only if n can be factored into a product of distinct primes;
    (b) every integer $n > 1$ is the product of a square-free integer and a perfect square. [*Hint:* If $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ is the canonical factorization of n, write $k_i = 2q_i + r_i$ where $r_i = 0$ or 1 according as k_i is even or odd.]
17. Verify that any integer n can be expressed as $n = 2^k m$, where $k \geq 0$ and m is an odd integer.
18. Numerical evidence makes it plausible that there are infinitely many primes p such that $p + 50$ is also prime. List fifteen of these primes.

3.2 THE SIEVE OF ERATOSTHENES

Given a particular integer, how can we determine whether it is prime or composite and, in the latter case, how can we actually find a nontrivial divisor? The most obvious approach consists of successively dividing the integer in question by each of the numbers preceeding it; if none of them (except 1) serves as a divisor, then the integer must be prime. Although this method is very simple to describe, it cannot be regarded as useful in practice. For even if one is undaunted by large calculations, the amount of time and work involved may be prohibitive.

There is a property of composite numbers which allows us to reduce materially the necessary computations—but still the above process remains cumbersome. If an integer $a > 1$ is composite, then it may be written as $a = bc$, where $1 < b < a$ and $1 < c < a$. Assuming that $b \leq c$, we get $b^2 \leq bc = a$ and so $b \leq \sqrt{a}$. Since $b > 1$, Theorem 3-2 ensures that b has at least one prime factor p. Then $p \leq b \leq \sqrt{a}$; furthermore, because $p \mid b$ and $b \mid a$, it follows that $p \mid a$. The point is simply this: a composite number a will always possess a prime divisor p satisfying $p \leq \sqrt{a}$.

In testing the primality of a specific integer $a > 1$, it therefore suffices to divide a by those primes not exceeding $\sqrt{a}$ (presuming, of course, the availability of a list of primes up to $\sqrt{a}$). This may be clarified by considering the integer $a = 509$. Inasmuch as $22 < \sqrt{509} < 23$, we

need only try out the primes which are not larger than 22 as possible divisors; namely, the primes 2, 3, 5, 7, 11, 13, 17, 19. Dividing 509 by each of these in turn, we find that none serves as a divisor of 509. The conclusion is that 509 must be a prime number.

Example 3-1

The foregoing technique provides a practical means for determining the canonical form of an integer, say $a = 2093$. Since $45 < \sqrt{2093} < 46$, it is enough to examine the multiples $2p$, $3p$, $5p$, $7p$, $11p$, $13p$, $17p$, $19p$, $23p$, $29p$, $31p$, $37p$, $41p$, $43p$. By trial, the first of these to divide 2093 is 7 and $2093 = 7 \cdot 299$. As regards the integer 299, the seven primes which are less than 18 (note that $17 < \sqrt{299} < 18$) are 2, 3, 5, 7, 11, 13, 17. The first prime divisor of 299 is 13 and, carrying out the required division, we obtain $299 = 13 \cdot 23$. But 23 is itself a prime, whence 2093 has exactly three prime factors, 7, 13, and 23:

$$2093 = 7 \cdot 13 \cdot 23.$$

Another Greek mathematician whose work in number theory remains significant is Eratosthenes of Cyrene (276–194 B.C.). While posterity remembers him mainly as the director of the world-famous library at Alexandria, Eratosthenes was gifted in all branches of learning, if not of first rank in any; in his own day, he was nicknamed "Beta" because, it was said, he stood at least second in every field. Perhaps the most impressive feat of Eratosthenes was the accurate measurement of the earth's circumference by a simple application of Euclidean geometry.

We have seen that if an integer $a > 1$ is not divisible by a prime $p \leq \sqrt{a}$, then a is of necessity a prime. Eratosthenes used this fact as the basis of a clever technique, called the "Sieve of Eratosthenes," for finding all primes below a given integer n. The scheme calls for writing down the integers from 2 to n in their natural order and then systematically eliminating all the composite numbers by striking out all multiples $2p$, $3p$, $4p$, $5p$,... of the primes $p \leq \sqrt{n}$. The integers that are left on the list—those that do not fall through the "sieve"—are primes.

To see an example of how this works, suppose that we wish to find all primes not exceeding 100. Consider the sequence of consecutive integers 2, 3, 4, ..., 100. Recognizing that 2 is a prime, we begin by crossing out all even integers from our listing, except 2 itself. The first of the remaining integers is 3, which must be a prime. We keep 3, but strike out all higher multiples of 3, so that 9, 15, 21, ... are now