In this algorithm, the expression \([n]\) denotes the smallest positive integer greater than or equal to \(n\).

We began this section by saying that many mathematicians are trying to find larger and larger primes. The largest prime known today has a special form, \(2^p - 1\), where \(p\) is a prime integer. These types of primes are called Mersenne primes after a seventeenth-century French monk who studied the positive integers of the form \(2^m - 1\), where \(m > 1\). For any positive integer \(m > 1\), \(M_n = 2^m - 1\) is called the \(n\)th Mersenne number, and if \(p\) is prime and \(M_p = 2^p - 1\) is also prime, then \(M_p\) is called a Mersenne prime. For example, \(M_2 = 2^2 - 1 = 3\), \(M_3 = 2^3 - 1 = 7\), \(M_5 = 2^5 - 1 = 31\), and \(M_7 = 2^7 - 1 = 127\), whereas \(M_{11} = 2^{11} - 1 = 2047 = 25 \cdot 89\) is composite.

We conclude the section with the following information.

- In 1992, David Slowinski and Paul Gage verified using a computer that \(2^{536851} - 1\) is prime.
- In 1994, David Slowinski and Paul Gage verified using a computer that \(2^{89433} - 1\) is prime.
- In 1996, Joel Armengaud, a computer programmer, discovered by computer that \(2^{1993702} - 1\) is prime.
- In 1997, Gordon Spence of Hampshire, England, discovered by computer that \(2^{2976221} - 1\) is prime.
- In 1999, Nayan Hajratwala discovered by the Lucas-Lehmer test that \(2^{6972593} - 1\) is prime.

**Remark 2.4.14** Determining if a given number is prime has fascinated mathematicians for several centuries and, more recently, computer scientists for several decades. The first recorded algorithm for this was given by Eratosthenes ca. 250 B.C. However, his algorithm is very inefficient on large numbers. Since then several efforts have been made to design an efficient (in other words, polynomial-time) algorithm. In 2002, the first deterministic polynomial-time algorithm that determines whether an input number is prime or composite was found by an Indian professor, Manindra Agrawal, and two graduate students, Neeraj Kayal and Nitin Saxena.

**Worked-Out Exercises**

**Exercise 1:** Show that for any integer \(n > 4\), \(n^4 + 64\) is a composite integer.

**Solution:** We have \(n^4 + 64 = (n^2 + 8)^2 - (8^2) = (n^2 + 8 + 4n)(n^2 + 8 - 4n) = (n^2 + 8 + 4n)((n - 4)n + 8)\).

Because \(n > 4\), \(n - 4 > 0\), so \((n - 4)n + 8 > 1\). Again, \((n^2 + 8 + 4n) > 1\). Hence, for any integer \(n > 4\), \(n^4 + 64\) is a composite integer.

**Exercise 2:** Determine which of the following integers are prime.

(a) \(293\)  
(b) \(9823\)

**Solution:**

(a) We first find all primes \(p\) such that \(p^2 < 293\). These primes are \(2, 3, 5, 7, 11, 13,\) and \(17\). Now none of these primes divide 293. Hence, 293 is a prime.

(b) We consider primes \(p\) such that \(p^2 < 9823\). These primes are \(2, 3, 5, 7, 11, 13, 17,\ldots\). None of 2, 3, 5, 7 divide 9823. However, 11 divides 9823. Hence, 9823 is not a prime.

**Exercise 3:** Find all prime divisors of \(60!\), where \(60!\) denotes the factorial of 60, i.e., the product all integers from 1 to 60.
Solution: Because 60! is the product of all integers from 1 to 60, the prime divisors of 60! are those primes that are less than 60. Hence, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, and 59 are the only prime divisors of 60!.

Exercise 4: Let $p$ be a prime such that $p \mid a^2$, $p \mid (a^2 + b^2)$. Prove that $p \mid b$.

Solution: Because $p \mid a^2$, by Corollary 2.4.5, $p \mid a$. Now $p \mid a$ and $p \mid (a^2 + b^2)$. Therefore, by Theorem 2.1.14(iii), $p \mid b^2$. This implies that $p \mid b$, because $p$ is a prime integer.

Exercise 5: Let $p$ be a prime integer such that $\gcd(a, p^2) = p$ and $\gcd(b, p^2) = p$. Find $\gcd(ab, p^3)$.

Solution: By the given condition, $\gcd(a, p^2) = p$. Therefore, $p \mid a$. Also, $p^2 \nmid a$. (For if $p^2 \mid a$, then $\gcd(a, p^2) \geq p^2 > p$, which is a contradiction.) Now $a$ can be written as a product of prime powers. Because $p \mid a$ and $p^2 \nmid a$, it follows that $p$ appears as a factor in the prime factorization of $a$, but $p^2$, where $k \geq 2$, does not appear in that prime factorization.

In a similar manner, $\gcd(b, p^2) = p$ implies that $p \mid b$ and $p^2 \nmid b$. As before, it follows that $p$ appears as a factor in the prime factorization of $b$, but $p^2$, where $k \geq 2$, does not appear in that prime factorization.

It now follows that $p^3 \mid ab$ and $p^3 \mid ab$. Hence, $\gcd(ab, p^3) = p^3$.

Exercise 6: Show that every odd prime is the form $4n + 1$ or $4n + 3$. Also, show that the number of primes of the form $4n + 3$ is infinite.

Solution: Any integer is one of the forms $4n$, $4n + 1$, $4n + 2$, or $4n + 3$. Now $4n$ cannot be prime for any integer $n$ and $4n + 2 = 2(2n + 1)$ is prime only for $n = 0$, which is even. Hence, every odd prime is the form $4n + 1$ or $4n + 3$. Next, we show that the number of primes of the form $4n + 3$ is infinite.

Notice that 3, 7, 11, and 19 are primes of the form $4n + 3$. Suppose there exist only a finite number of primes of the form $4n + 3$. Let $p_1, p_2, p_3, \ldots$, and $p_k$ be the complete list of all primes of the form $4n + 3$. Consider the integer

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

Observe that none of the primes $p_1, p_2, p_3, \ldots, p_k$ and 2 divide $m$. Because $m > 1$, we find that $m$ has an odd prime divisor.

Now any odd prime is either of the form $4n + 1$ or of the form $4n + 3$. Because the product of any two integers of the form $4n + 1$ is again an integer of the form $4n + 1$, it follows that all the prime divisors of $m$ cannot be of the form $4n + 1$. Hence, $m$ has a prime divisor of the form $4n + 3$, which must be one of $p_1, p_2, p_3, \ldots, p_k$. This contradicts the fact that none of $p_i$ divides $m$. Hence, the number of primes of the form $4n + 3$ is infinite.

Exercise 7: Justify that for any positive integer $n$, $f(n) = n^2 + n + 41$ may not always be prime.

Solution: Because $f(41) = 41^2 + 41 + 41 = 41(41 + 1 + 1)$, it follows that $f(41)$ is not prime.

Exercise 8: Let $n$ be a positive integer such that $n^3 - 1$ is prime. Prove that $n = 2$.

Solution: We can write

$$n^3 - 1 = (n - 1)(n^2 + n + 1).$$

Because $n^3 - 1$ is prime, either $n - 1 = 1$ or $n^2 + n + 1 = 1$. Now $n \geq 1$, so $n^2 + n + 1 > 1$, i.e., $n^2 + n + 1 \neq 1$. Thus, we must have $n - 1 = 1$. This implies that $n = 2$.

Exercise 9: For any positive integer $n$, if $2^n - 1$ is a prime, then prove that $n$ is also prime.

Solution: Suppose that $2^n - 1$ is prime, but $n$ is not prime. If $n = 1$, then $2 - 1 = 1$, which is not prime, a contradiction. If $n > 1$ and not prime, then there exist integers $m$ and $k$ such that $1 < m < n, 1 < k < n$, and $n = mk$.

Now,

$$2^n - 1 = 2^{mk} - 1 = (2^m - 1)(2^{mk - 1} + 2^{mk - 2} + \cdots + 2^m + 1).$$

Because $m > 1$, we find that $2^n - 1 > 1$. Also, $k > 1$, and so we have

$$2^{mk - 1} + 2^{mk - 2} + \cdots + 2^m + 1 > 1.$$ 

Thus, $2^n - 1$ is expressed as the product of two integers both of which are greater than one. Hence, $2^n - 1$ is not prime. This is a contradiction to our assumption. Consequently, if $2^n - 1$ is a prime, then $n$ is also prime.

SECTION REVIEW

Key Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>prime number</td>
<td>A number that is only divisible by 1 and itself</td>
</tr>
<tr>
<td>prime</td>
<td>A number that is only divisible by 1 and itself</td>
</tr>
<tr>
<td>composite</td>
<td>A number that is divisible by numbers other than 1 and itself</td>
</tr>
<tr>
<td>Fundamental Theorem of Arithmetic</td>
<td>Every integer greater than 1 is either a prime or can be uniquely factored into primes</td>
</tr>
<tr>
<td>trivial positive divisor</td>
<td>A positive divisor that is less than the number</td>
</tr>
<tr>
<td>standard factorization</td>
<td>The unique prime factorization of a number</td>
</tr>
</tbody>
</table>


Key Definition

1. An integer \( p > 1 \) is called a prime number, or prime, if the only positive divisors of \( p \) are 1 and \( p \). An integer \( q > 1 \) that is not prime is called composite.

Some Key Results

1. An integer \( p > 1 \) is prime if and only if for all integers \( a \) and \( b \), \( p \) divides \( ab \) implies either \( p \) divides \( a \) or \( p \) divides \( b \).
2. Every integer \( n \geq 2 \) has a prime factor.
3. There are infinitely many primes.
4. If \( n \) is a composite integer, then \( n \) has a prime factor not exceeding \( \sqrt{n} \).
5. Fundamental Theorem of Arithmetic: Every integer \( n \geq 2 \) can be expressed uniquely as a product of (one or more) primes, up to the order of the factors. More precisely, any integer \( n \geq 2 \) can be expressed as \( n = p_1 p_2 \cdots p_r \), where \( p_1, p_2, \ldots, p_r \) are primes. Moreover, if \( n = p_1 p_2 \cdots p_r \) and \( n = q_1 q_2 \cdots q_t \) are two factorizations of \( n \) as a product of primes, then \( r = s \) and the \( q_i \) can be relabeled so that \( p_i = q_i \) for all \( i = 1, 2, \ldots, r \).

Exercises

1. Determine which of the following integers are primes.
   a. 391  b. 1999  c. 2083
2. Express 873, 675, and 1617 as a product of primes.
3. Find all prime numbers \( p \) such that \( 100 \leq p \leq 140 \).
4. Let \( p \) be a prime such that \( p | a^5 \), \( p | a^2 + b^2 \). Prove that \( p | a \).
5. If \( p \) is a prime integer such that \( p = n^2 - 9 \) for some integer \( n \), then show that \( p = 7 \).
6. Let \( p \) be a prime integer such that \( \gcd(a, p^4) = p \) and \( \gcd(b, p^3) = p \). Find the \( \gcd(ab, p^7) \).
7. If \( n \) is a positive integer such that \( n^3 + 1 \) is prime, then show that \( n = 1 \).
8. Find all prime factors of 90!
9. If \( a > 0 \) and \( n \geq 2 \) are integers such that \( a^n - 1 \) is prime, then show that \( a = 2 \).
10. Let \( p_n \) denote the \( n \)th prime. Prove that \( p_{n+1} \leq 2p_n + 1 \) and hence show that \( p_n \leq 2^{2^{n-1}} - 2 \).
11. If \( p \) is a prime, prove that there exist no positive integers \( m \) and \( n \) such that \( m^2 = pn^2 \).
12. Let \( k \) be a positive integer. Prove that the following integers

\[(k + 1)! + 2, (k + 1)! + 3, \ldots, (k + 1)! + k, (k + 1)! + (k + 1)\]

are \( k \) consecutive composite integers.
13. Find five consecutive composite integers.
14. Prove that any prime \( p \) of the form \( 7k + 1 \) is also of the form \( 14t + 1 \).
15. Prove that there are infinitely many primes of the form \( 4n - 1 \).
16. Prove that there are infinitely many primes of the form \( 3n + 2 \).
17. Let \( a, b \) be two integers such that \( 3 | (a^2 + b^2) \). Then prove that \( 3 | a \) and \( 3 | b \).
18. Prove that the only prime of the form \( n^2 - 4 \) is 5.
19. Prove that the only prime of the form \( n^2 - 1 \) is 7.
20. Factor the numbers 8067 and 9,970,716 by Fermat's method.
21. If \( p_n \) is the \( n \)th prime, then prove that

\[
\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}
\]

is not an integer.