The famous German mathematician Carl Friedrich Gauss once remarked, “Mathematics is the Queen of Science, and number theory is the Queen of Mathematics.” This chapter is centered around the study of number theory. Number theory is the branch of mathematics devoted to the study of the properties of the natural numbers,

**Prime and Composite Numbers**

In earlier chapters we discussed the set of natural numbers, also called the counting numbers or the positive integers:

\[ \{1, 2, 3, \ldots \} \]

Number theory deals with the study of the properties of this set of numbers, and a key concept of number theory is the idea of divisibility. Informally, we say that one counting number is divisible by another if the operation of dividing the first by the second leaves a remainder 0. A formal definition follows.

### Divisibility

The natural number \(a\) is divisible by the natural number \(b\) if there exists a natural number \(k\) such that \(a = bk\). If \(b\) divides \(a\), then we write \(b \mid a\).

Notice that if \(b\) divides \(a\), then the quotient \(a/b\) is a natural number. For example, 4 divides 20 since there exists a natural number \(k\) such that \(20 = 4k\). The value of \(k\) here is 5, since \(20 = 4 \cdot 5\). (A dot is used here to denote multiplication.) The natural number 20 is not divisible by 7, for example, since there is no natural number \(k\) satisfying \(20 = 7k\). Alternatively, we think “20 divided by 7 gives quotient 2 with remainder 6” and since there is a nonzero remainder, divisibility does not hold. We write \(7 \notdivides 20\) to indicate that 7 does not divide 20.

If the natural number \(a\) is divisible by the natural number \(b\), then \(b\) is a factor (or divisor) of \(a\), and \(a\) is a multiple of \(b\). For example, 5 is a factor of 30, and 30 is a multiple of 5. Also, 6 is a factor of 30, and 30 is a multiple of 6. The number 30 equals \(6 \cdot 5\); this product \(6 \cdot 5\) is called a factorization of 30. Other factorizations of 30 include \(3 \cdot 10, 2 \cdot 15, 1 \cdot 30,\) and \(2 \cdot 3 \cdot 5\).

The ideas of even and odd natural numbers are based on the concept of divisibility. A natural number is even if it is divisible by 2, and odd if it is not.

### Example 1

Decide whether the first number listed is divisible by the second.

(a) \(45; 9\)

Is there a natural number \(k\) that satisfies \(45 = 9k\)? The answer is yes, since \(45 = 9 \cdot 5\), and 5 is a natural number. Therefore, 9 divides 45, written \(9 \divides 45\).

(b) \(60; 7\)

Since the quotient \(60 \div 7\) is not a natural number, 60 is not divisible by 7, written \(7 \notdivides 60\).
Prime and Composite Numbers

A natural number greater than 1 that has only itself and 1 as factors is called a **prime number**. A natural number greater than 1 that is not prime is called **composite**.

Mathematicians agree that the natural number 1 is neither prime nor composite. The following alternative definition of a prime number clarifies that 1 is not a prime.

**Alternative Definition of a Prime Number**

A **prime number** is a natural number that has *exactly* two different natural number factors.

This alternative definition excludes the possibility of 1 being prime, since 1 has only one natural number factor (namely, 1).

There is a systematic method for identifying prime numbers in a list of numbers: 2, 3, … , n. The method, known as the **Sieve of Eratosthenes**, is named after the
Greek geographer, poet, astronomer, and mathematician, who lived from about 276 to 192 B.C. To construct such a sieve, list all the natural numbers from 2 through some given natural number \( n \), such as 100. The number 2 is prime, but all other multiples of 2 (4, 6, 8, 10, and so on) are composite. Circle the prime 2, and cross out all other multiples of 2. The next number not crossed out and not circled is 3, the next prime. Circle the 3, and cross out all other multiples of 3 (6, 9, 12, 15, and so on) that are not already crossed out. Circle the next prime, 5, and cross out all other multiples of 5 not already crossed out. Continue this process for all primes less than or equal to the square root of the last number in the list. For this list, we may stop with 7, since the next prime, 11, is greater than the square root of 100, which is 10. At this stage, simply circle all remaining numbers that are not crossed out. Table 1 shows the Sieve of Eratosthenes for 2, 3, 4, …, 100, identifying the 25 primes in that range. Theoretically, such a sieve can be constructed for any value of \( n \).

<table>
<thead>
<tr>
<th>TABLE 1</th>
<th>Sieve of Eratosthenes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>14</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>16</td>
</tr>
<tr>
<td>17</td>
<td>18</td>
</tr>
<tr>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>21</td>
<td>22</td>
</tr>
<tr>
<td>23</td>
<td>24</td>
</tr>
<tr>
<td>25</td>
<td>26</td>
</tr>
<tr>
<td>27</td>
<td>28</td>
</tr>
<tr>
<td>29</td>
<td>30</td>
</tr>
<tr>
<td>31</td>
<td>32</td>
</tr>
<tr>
<td>33</td>
<td>34</td>
</tr>
<tr>
<td>35</td>
<td>36</td>
</tr>
<tr>
<td>37</td>
<td>38</td>
</tr>
<tr>
<td>39</td>
<td>40</td>
</tr>
<tr>
<td>41</td>
<td>42</td>
</tr>
<tr>
<td>43</td>
<td>44</td>
</tr>
<tr>
<td>45</td>
<td>46</td>
</tr>
<tr>
<td>47</td>
<td>48</td>
</tr>
<tr>
<td>49</td>
<td>50</td>
</tr>
<tr>
<td>51</td>
<td>52</td>
</tr>
<tr>
<td>53</td>
<td>54</td>
</tr>
<tr>
<td>55</td>
<td>56</td>
</tr>
<tr>
<td>57</td>
<td>58</td>
</tr>
<tr>
<td>59</td>
<td>60</td>
</tr>
<tr>
<td>61</td>
<td>62</td>
</tr>
<tr>
<td>63</td>
<td>64</td>
</tr>
<tr>
<td>65</td>
<td>66</td>
</tr>
<tr>
<td>67</td>
<td>68</td>
</tr>
<tr>
<td>69</td>
<td>70</td>
</tr>
<tr>
<td>71</td>
<td>72</td>
</tr>
<tr>
<td>73</td>
<td>74</td>
</tr>
<tr>
<td>75</td>
<td>76</td>
</tr>
<tr>
<td>77</td>
<td>78</td>
</tr>
<tr>
<td>79</td>
<td>80</td>
</tr>
<tr>
<td>81</td>
<td>82</td>
</tr>
<tr>
<td>83</td>
<td>84</td>
</tr>
<tr>
<td>85</td>
<td>86</td>
</tr>
<tr>
<td>87</td>
<td>88</td>
</tr>
<tr>
<td>89</td>
<td>90</td>
</tr>
<tr>
<td>91</td>
<td>92</td>
</tr>
<tr>
<td>93</td>
<td>94</td>
</tr>
<tr>
<td>95</td>
<td>96</td>
</tr>
<tr>
<td>97</td>
<td>98</td>
</tr>
<tr>
<td>99</td>
<td>100</td>
</tr>
</tbody>
</table>

**Example 3**

Decide whether each number is prime or composite.

(a) 97

Since the only factors of 97 are 97 and 1, the number 97 is prime.

(b) 59,872

The number 59,872 is even, so it is divisible by 2. It is composite. (There is only one even prime, the number 2 itself.)

(c) 697

For 697 to be composite, there must be a number other than 697 and 1 that divides into it with remainder 0. Start by trying 2, and then 3. Neither works. There is no need to try 4. (If 4 divides with remainder 0 into a number, then 2 will also.) Try 5. There is no need to try 6 or any succeeding even number. (Why?) Try 7. Try 11. (Why not try 9?) Try 13. Keep trying numbers until one works, or until a number is tried whose square exceeds the given number. Try 17:

\[
697 \div 17 = 41.
\]

The number 697 is composite.

An aid in determining whether a natural number is divisible by another natural number is called a **divisibility test**. Some simple divisibility tests exist for small...
Writing in the October 1, 1994 issue of Science News, Ivars Peterson gives a fascinating account of the recent discovery of a 75-year-old factoring machine ("Cranking Out Primes: Tracking Down a Long-lost Factoring Machine"). In 1989, Jeffrey Shallit of the University of Waterloo in Ontario came across an article in an obscure 1920 French journal, in which the author, Eugene Olivier Carissan, reported his invention of the factoring apparatus. Shallit and two colleagues embarked on a search for the machine. They contacted all telephone subscribers in France named Carissan and received a reply from Eugene Carissan’s daughter. The machine was still in existence and in working condition, stored in a drawer at an astronomical observatory in Floirac, near Bordeaux.

Peterson explains in the article how the apparatus works. Using the machine, Carissan took just ten minutes to prove that 708,158,977 is a prime number, and he was able to factor a 13-digit number. While this cannot compare to what technology can accomplish today, it was a significant achievement for Carissan’s day.

As mentioned earlier, a number such as 15, which can be written as a product of prime factors (15 = 3 · 5), is called a composite number. An important theorem in mathematics states that there is only one possible way to write the prime factorization of a composite natural number. This theorem is called the fundamental theorem of arithmetic, a form of which was known to the ancient Greeks.*

* A theorem is a statement that can be proved true from other statements. For a proof of this theorem, see What Is Mathematics? by Richard Courant and Herbert Robbins (Oxford University Press, 1941), p. 23.
The following program, written by Charles W. Gantner and provided courtesy of Texas Instruments, can be used on the TI-83 Plus calculator to list all primes less than or equal to a given natural number \( N \).

**PROGRAM: PRIMES**

: Disp "INPUT \( N \geq 2 \)"
: Disp "TO GET"
: Disp "PRIMES \( \leq N \)"
: Input N
: 2 → T
: Disp T
: 1 → A
:Lbl 1
: A + 2 → A
: 3 → B
: If A > N
: Stop
: Lbl 2
: If B ≤ √(A)
: Goto 3
: Disp A
: Pause
: Goto 1
: Lbl 3
: If A/B ≤ int (A/B)
: Goto 1
: B + 2 → B
: Goto 2

The display indicates that the primes less than or equal to 6 are 2, 3, and 5.

**The Fundamental Theorem of Arithmetic**

Every composite natural number can be expressed in one and only one way as a product of primes (if the order of the factors is disregarded).

This theorem is sometimes called the **unique factorization theorem** to reflect the idea that there is only one (unique) prime factorization possible for any given natural number.

A composite number can be factored into primes by using a “factor tree” as illustrated in the next example.

**EXAMPLE 5** Find the prime factorization of the composite number 504.

Since 2 is a factor of 504, we can begin the first branches of the factor tree by writing 504 as 2 \( \cdot 252 \). Then factor 252 as 2 \( \cdot 126 \). When a composite factor appears that does not have 2 as a factor, try 3, then 5, then 7, and so on, until there is a prime number at the end of each branch.

![Factor Tree Diagram]

The prime factors are circled. Using exponents, the prime factorization of 504 is 2\(^3\) \( \cdot 3^2 \) \( \cdot 7 \). (Note: Because the fundamental theorem of arithmetic guarantees that this prime factorization is unique, we could have started the factor tree with 3 \( \cdot 168 \), or 8 \( \cdot 63 \), or several other possibilities, as long as we had continued until all factors were prime. In every case, the same final factorization would be obtained.)

As an alternative to the factor tree method, we may divide 504 by primes over and over, using the compact form shown below.

\[
\begin{array}{c|c}
\text{Prime} & \text{Factorization} \\
\hline
2 & 504 \\
2 & 252 \\
2 & 126 \\
3 & 63 \\
3 & 21 \\
7 & \\
\end{array}
\]

Keep going, using as necessary the primes 2, 3, 5, 7, 11, and so on, until the last number is a prime. Read the prime factors as shown in color, to get 504 = 2\(^3\) \( \cdot 3^2 \) \( \cdot 7 \).

**The Infinitude of Primes** Since prime numbers are, in a sense, the building blocks of the entire number system, mathematicians (amateur as well as professional) have sought for thousands of years to learn as much as possible about them. Although much still is unknown, there is one important basic result that was proved...
by Euclid around 300 B.C., namely that there are infinitely many primes. This means, for one thing, that no matter how large a prime we identify, there are always others even larger. Euclid’s proof remains today as one of the most elegant proofs in all of mathematics. (An elegant mathematical proof is one that exhibits the desired result in a most direct, concise manner. Mathematicians strive for elegance in their proofs.) It is called a proof by contradiction.

A statement can be proved by contradiction as follows: We assume that the negation of the statement is true. The assumption that the negation is true is used to produce some sort of contradiction, or absurdity. The fact that the negation of the original statement leads to a contradiction means that the original statement must be true.

In order to better understand a particular part of the proof that there are infinitely many primes, it is helpful to examine the following argument.

Suppose that \( M = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 \). Now \( M \) is the product of the first four prime numbers, plus 1. If we divide 211 by each of the primes 2, 3, 5, and 7, the remainder is always 1.

\[
\begin{array}{cccc}
105 & 70 & 42 & 30 \\
2\overline{211} & 3\overline{211} & 5\overline{211} & 7\overline{211} \\
210 & 210 & 210 & 210 \\
1 & 1 & 1 & 1 \\
\end{array}
\]

So 211 is not divisible by any of the primes 2, 3, 5, and 7.

Now we are ready to prove that there are infinitely many primes. If it can be shown that there is no largest prime number, then there must be infinitely many primes.

**Theorem** There is no largest prime number.

**Proof:** Suppose that there is a largest prime number and call it \( P \). Now form the number \( M \) such that

\[ M = p_1 \cdot p_2 \cdot p_3 \cdots P + 1, \]

where \( p_1, p_2, p_3, \ldots, P \) represent all the primes less than or equal to \( P \). Now the number \( M \) must be either prime or composite.

1. Suppose that \( M \) is prime.
   - \( M \) is obviously larger than \( P \), so if \( M \) is prime, it is larger than the assumed largest prime \( P \). We have reached a contradiction.

2. Suppose that \( M \) is composite.
   - If \( M \) is composite, it must have a prime factor. But none of \( p_1, p_2, p_3, \ldots, P \) are factors of \( M \), since division by each will leave a remainder of 1. (Recall the above argument.) So if \( M \) has a prime factor, it must be greater than \( P \). But this is a contradiction, since \( P \) is the assumed largest prime.

In either case 1 or 2, we reach a contradiction. The whole argument was based upon the assumption that a largest prime exists, but since this leads to contradictions, there must be no largest prime, or equivalently, there are infinitely many primes.

**The Search for Large Primes** Identifying larger and larger prime numbers and factoring large composite numbers into their prime components is of great practical importance today since it is the basis of modern cryptography systems (secret codes). Various codes have been used for centuries in military applications.
Prime Search  At one time, 211,213 − 1 was the largest known Mersenne prime. To honor its discovery, the Urbana, Illinois, post office used the cancellation picture above. Since then, larger prime numbers have been found.

Marin Mersenne (1588–1648), in his Cogitata Physico-Mathematica (1644), claimed that Mₙ was prime for n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, and 257, and composite for all other prime numbers n less than 257. Other mathematicians at the time knew that Mersenne could not have actually tested all these values, but no one else could prove or disprove them either. It was more than 300 years later before all primes up to 257 were legitimately checked out, and Mersenne was finally revealed to have made five errors:

- M₂ is prime.
- M₅ is composite.
- M₁₀ is prime.
- M₁₂ is prime.
- M₂² is composite.

Today the security of industrial and business data also depends upon the theory of prime numbers.

As mathematicians continue to search for larger and larger primes, a formula for generating all the primes would be nice (something similar, for example, to the formula 2ⁿ, which generates all even counting numbers for n = 1, 2, 3, . . ., or the formula n², which generates all the perfect squares). Numbers generated by the formula Mₙ = 2ⁿ − 1 are called Mersenne numbers to honor the French monk Marin Mersenne (1588–1648). It was long known that a composite value of n would always generate a composite Mersenne number. (See Exercises 81–86.) And some early mathematicians believed that a prime value of n would always generate a prime Mersenne number. That is, starting with any known prime number n, one could always produce another, larger prime number 2ⁿ − 1. (Although “always generate a prime” is not the same as “generate all primes,” at least it would be a source of primes.)

**Example 6** Evaluate the Mersenne number Mₙ for n = 2, 3, and 5.

\[ M₂ = 2² − 1 = 3 \quad M₃ = 2³ − 1 = 7 \quad M₅ = 2⁵ − 1 = 31 \]

Note that all three values, 3, 7, and 31, are indeed primes.

It turns out that M₇ is also a prime (see Exercise 26), but it was discovered in 1536 that M₁₁ = 2¹¹ − 1 = 2047 is not prime (since it is 2³ · 89). So prime values of n do not always produce prime Mₙ. The question then became which prime values of n do produce prime Mersenne numbers (the so-called Mersenne primes). Since no way was ever found to identify, in general, which prime values of n result in Mersenne primes, it became a matter of checking out each prime n value individually—not an easy task given that the Mersenne numbers rapidly become very large.

The Mersenne prime search yielded results slowly. By about 1600, Mₙ had been verified as prime for all prime n up to 19 (except for 11, as mentioned above). The next one was M₃₁, verified by Euler in 1732. About 100 years later, M₁₂⁷ was shown to be prime. No larger Mersenne prime was discovered until 1952, when an early computer verified that M₃₂¹, M₆⁰⁷, M₁₂⁷⁹, M₂₃²⁰⁳, and M₂₃⁸⁵ are all primes.

Over the last 50 years, most new record-breaking primes have been identified by mathematicians expert in devising algorithms and programming them to run on the most powerful computers available. In early 1996, the Great Internet Mersenne Prime Search (GIMPS) was launched. By early 2002, more than 130,000 individuals had signed on, receiving free software and source code to run during slack time on more than 205,000 personal computers throughout the world. The latest Mersenne prime was \( M_{13,466,917} = 2^{13,466,917} − 1 \), a number with 4,053,946 decimal digits. It was the 39th known Mersenne prime. (In a BBC online article it was reckoned that the accomplishment by GIMPS had utilized a combined 13,000 years of computer time.)

During the same general period that Mersenne was thinking about prime numbers, Pierre de Fermat (about 1601–1665) conjectured that the formula \( 2^{2^n} + 1 \) would always produce a prime, for any whole number value of n. Table 3 shows how this formula generates the first four Fermat numbers, which are indeed all primes. The fifth Fermat number (from n = 4) is likewise prime, but the sixth Fermat number (from n = 5) turns out to be 4,294,967,297, which is not prime. (See Exercises 75 and 76.) To date, no more primes have been found among the Fermat numbers.
Of historical note are a couple of polynomial formulas that produce primes. In 1732, Leonhard Euler offered the formula \( n^2 - n + 41 \), which generates primes for \( n \) up to 40 and fails at \( n = 41 \). In 1879, E. B. Escott produced more primes with the formula \( n^2 - 79n + 1601 \), which first fails at \( n = 80 \).

\[
\begin{array}{cccc}
 n & 2^n & 2^{2n} & 2^{2n} + 1 \\
 0 & 1 & 2 & 3 \\
 1 & 2 & 4 & 5 \\
 2 & 4 & 16 & 17 \\
 3 & 8 & 256 & 257 \\
\end{array}
\]

Table 3 shows the generation of Fermat Numbers.

\[
\begin{array}{cccc}
 n & \text{Euler formula} & \text{Escott formula} \\
 & n^2 - n + 41 & n^2 - 79n + 1601 \\
 1 & 41 & 1523 \\
 2 & 43 & 1447 \\
 3 & 47 & 1373 \\
 4 & 53 & 1301 \\
 5 & 61 & 1231 \\
\end{array}
\]

Table 4 shows the required numbers.

All values found here are primes. (Use Table 1 to verify the Euler values.)

Actually, it is not hard to prove that there can be no polynomial that will consistently generate primes. More complicated mathematical formulas do exist for generating primes, but none produced so far can be practically applied in a reasonable amount of time, even using the fastest computers.

---

Prime Does Pay  On November 14, 2001, Michael Cameron’s computer, an 800 MHz AMD T-Bird, found the 39th known Mersenne prime, after just 42 days of idle time computing. The number contains 4,053,946 decimal digits. Starting with the first million-digit prime, the Electronics Frontier Foundation has paid rewards of $50,000 for record-breaking primes. The first discoverer of a ten-million-digit prime will receive $100,000.

If you would like to join the Great Internet Mersenne Prime Search, check out http://www.mersenne.org.

---

An Addison-Wesley product. Copyright © 2004 Pearson Education, Inc.