

## 4

## Number Theory and Cryptography

4.1 Divisibility and Modular Arithmetic

4.2 Integer Representations and Algorithms

4.3 Primes and Greatest Common Divisors

4.4 Solving Congruences

4.5 Applications of Congruences

4.6 Cryptography

The part of mathematics devoted to the study of the set of integers and their properties is known as number theory. In this chapter we will develop some of the important concepts of number theory including many of those used in computer science. As we develop number theory, we will use the proof methods developed in Chapter 1 to prove many theorems.

We will first introduce the notion of divisibility of integers, which we use to introduce modular, or clock, arithmetic. Modular arithmetic operates with the remainders of integers when they are divided by a fixed positive integer, called the modulus. We will prove many important results about modular arithmetic which we will use extensively in this chapter.

Integers can be represented with any positive integer  $b$  greater than 1 as a base. In this chapter we discuss base  $b$  representations of integers and give an algorithm for finding them. In particular, we will discuss binary, octal, and hexadecimal (base 2, 8, and 16) representations. We will describe algorithms for carrying out arithmetic using these representations and study their complexity. These algorithms were the first procedures called algorithms.

We will discuss prime numbers, the positive integers that have only 1 and themselves as positive divisors. We will prove that there are infinitely many primes; the proof we give is considered to be one of the most beautiful proofs in mathematics. We will discuss the distribution of primes and many famous open questions concerning primes. We will introduce the concept of greatest common divisors and study the Euclidean algorithm for computing them. This algorithm was first described thousands of years ago. We will introduce the fundamental theorem of arithmetic, a key result which tells us that every positive integer has a unique factorization into primes.

We will explain how to solve linear congruences, as well as systems of linear congruences, which we solve using the famous Chinese remainder theorem. We will introduce the notion of pseudoprimes, which are composite integers masquerading as primes, and show how this notion can help us rapidly generate prime numbers.

This chapter introduces several important applications of number theory. In particular, we will use number theory to generate pseudorandom numbers, to assign memory locations to computer files, and to find check digits used to detect errors in various kinds of identification numbers. We also introduce the subject of cryptography. Number theory plays an essential role both in classical cryptography, first used thousands of years ago, and modern cryptography, which plays an essential role in electronic communication. We will show how the ideas we develop can be used in cryptographic protocols, introducing protocols for sharing keys and for sending signed messages. Number theory, once considered the purest of subjects, has become an essential tool in providing computer and Internet security.

Finally, it should be noted that this chapter is designed to introduce some key aspects of number theory. As with all the topics covered in this book, there is a great deal more to learn. Interested students can consult [Ro11], the author's number theory text, to explore this fascinating subject more fully.

## 4.1

## Divisibility and Modular Arithmetic

## 4.1.1 Introduction

The ideas that we will develop in this section are based on the notion of divisibility. Division of an integer by a positive integer produces a quotient and a remainder. Working with these remainders leads to modular arithmetic, which plays an important role in mathematics and which

is used throughout computer science. We will discuss some important applications of modular arithmetic later in this chapter, including generating pseudorandom numbers, assigning computer memory locations to files, constructing check digits, and encrypting messages.

### 4.1.2 Division

When one integer is divided by a second nonzero integer, the quotient may or may not be an integer. For example,  $12/3 = 4$  is an integer, whereas  $11/4 = 2.75$  is not. This leads to Definition 1.

#### Definition 1

If  $a$  and  $b$  are integers with  $a \neq 0$ , we say that  $a$  divides  $b$  if there is an integer  $c$  such that  $b = ac$  (or equivalently, if  $\frac{b}{a}$  is an integer). When  $a$  divides  $b$  we say that  $a$  is a *factor* or *divisor* of  $b$ , and that  $b$  is a *multiple* of  $a$ . The notation  $a \mid b$  denotes that  $a$  divides  $b$ . We write  $a \nmid b$  when  $a$  does not divide  $b$ .

**Remark:** We can express  $a \mid b$  using quantifiers as  $\exists c(ac = b)$ , where the universe of discourse is the set of integers.

In Figure 1 a number line indicates which integers are divisible by the positive integer  $d$ .

**EXAMPLE 1** Determine whether  $3 \mid 7$  and whether  $3 \mid 12$ .

**Solution:** We see that  $3 \nmid 7$ , because  $7/3$  is not an integer. On the other hand,  $3 \mid 12$  because  $12/3 = 4$ .

**EXAMPLE 2** Let  $n$  and  $d$  be positive integers. How many positive integers not exceeding  $n$  are divisible by  $d$ ?

**Extra Examples** ➤

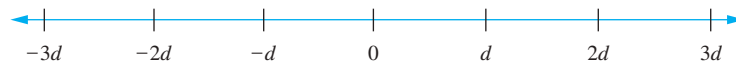
**Solution:** The positive integers divisible by  $d$  are all the integers of the form  $dk$ , where  $k$  is a positive integer. Hence, the number of positive integers divisible by  $d$  that do not exceed  $n$  equals the number of integers  $k$  with  $0 < dk \leq n$ , or with  $0 < k \leq n/d$ . Therefore, there are  $\lfloor n/d \rfloor$  positive integers not exceeding  $n$  that are divisible by  $d$ .

Some of the basic properties of divisibility of integers are given in Theorem 1.

#### THEOREM 1

Let  $a$ ,  $b$ , and  $c$  be integers, where  $a \neq 0$ . Then


- (i) if  $a \mid b$  and  $a \mid c$ , then  $a \mid (b + c)$ ;
- (ii) if  $a \mid b$ , then  $a \mid bc$  for all integers  $c$ ;
- (iii) if  $a \mid b$  and  $b \mid c$ , then  $a \mid c$ .



**FIGURE 1** Integers divisible by the positive integer  $d$ .

**Proof:** We will give a direct proof of (i). Suppose that  $a \mid b$  and  $a \mid c$ . Then, from the definition of divisibility, it follows that there are integers  $s$  and  $t$  with  $b = as$  and  $c = at$ . Hence,


$$b + c = as + at = a(s + t).$$

Therefore,  $a$  divides  $b + c$ . This establishes part (i) of the theorem. The proofs of parts (ii) and (iii) are left as Exercises 3 and 4. 

Theorem 1 has this useful consequence.

### COROLLARY 1

If  $a$ ,  $b$ , and  $c$  are integers, where  $a \neq 0$ , such that  $a \mid b$  and  $a \mid c$ , then  $a \mid mb + nc$  whenever  $m$  and  $n$  are integers.

**Proof:** We will give a direct proof. By part (ii) of Theorem 1 we see that  $a \mid mb$  and  $a \mid nc$  whenever  $m$  and  $n$  are integers. By part (i) of Theorem 1 it follows that  $a \mid mb + nc$ . 

## 4.1.3 The Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder, as the division algorithm shows.

### THEOREM 2

**THE DIVISION ALGORITHM** Let  $a$  be an integer and  $d$  a positive integer. Then there are unique integers  $q$  and  $r$ , with  $0 \leq r < d$ , such that  $a = dq + r$ .

We defer the proof of the division algorithm to Section 5.2. (See Example 5 and Exercise 37 in that section.)

**Remark:** Theorem 2 is not really an algorithm. (Why not?) Nevertheless, we use its traditional name.

### Definition 2

In the equality given in the division algorithm,  $d$  is called the *divisor*,  $a$  is called the *dividend*,  $q$  is called the *quotient*, and  $r$  is called the *remainder*. This notation is used to express the quotient and remainder:

$$q = a \text{ div } d, \quad r = a \text{ mod } d.$$

**Remark:** Note that both  $a \text{ div } d$  and  $a \text{ mod } d$  for a fixed  $d$  are functions on the set of integers. Furthermore, when  $a$  is an integer and  $d$  is a positive integer, we have  $a \text{ div } d = \lfloor a/d \rfloor$  and  $a \text{ mod } d = a - d \lfloor a/d \rfloor$ . (See Exercise 24.)


Examples 3 and 4 illustrate the division algorithm.

### EXAMPLE 3

What are the quotient and remainder when 101 is divided by 11?

**Solution:** We have

$$101 = 11 \cdot 9 + 2.$$

Hence, the quotient when 101 is divided by 11 is  $9 = 101 \text{ div } 11$ , and the remainder is  $2 = 101 \text{ mod } 11$ . 

**EXAMPLE 4** What are the quotient and remainder when  $-11$  is divided by  $3$ ?

*Extra  
Examples* 


*Solution:* We have

$$-11 = 3(-4) + 1.$$

Hence, the quotient when  $-11$  is divided by  $3$  is  $-4 = -11 \text{ div } 3$ , and the remainder is  $1 = -11 \text{ mod } 3$ .

Note that the remainder cannot be negative. Consequently, the remainder is *not*  $-2$ , even though

$$-11 = 3(-3) - 2,$$

because  $r = -2$  does not satisfy  $0 \leq r < 3$ . 

Note that the integer  $a$  is divisible by the integer  $d$  if and only if the remainder is zero when  $a$  is divided by  $d$ .

**Remark:** A programming language may have one, or possibly two, operators for modular arithmetic, denoted by `mod` (in BASIC, Maple, Mathematica, EXCEL, and SQL), `%` (in C, C++, Java, and Python), `rem` (in Ada and Lisp), or something else. Be careful when using them, because for  $a < 0$ , some of these operators return  $a - m[a/m]$  instead of  $a \text{ mod } m = a - m[a/m]$  (as shown in Exercise 24). Also, **unlike  $a \text{ mod } m$ , some of these operators are defined when  $m < 0$ , and even when  $m = 0$ .**

#### 4.1.4 Modular Arithmetic

In some situations we care only about the remainder of an integer when it is divided by some specified positive integer. For instance, when we ask what time it will be (on a 24-hour clock) 50 hours from now, we care only about the remainder when 50 plus the current hour is divided by 24. Because we are often interested only in remainders, we have special notations for them. We have already introduced the notation  $a \text{ mod } m$  to represent the remainder when an integer  $a$  is divided by the positive integer  $m$ . We now introduce a different, but related, notation that **indicates that two integers have the same remainder** when they are divided by the positive integer  $m$ .

##### Definition 3

If  $a$  and  $b$  are integers and  $m$  is a positive integer, then  **$a$  is congruent to  $b$  modulo  $m$**  if  **$m$  divides  $a - b$** . We use the notation  $a \equiv b \pmod{m}$  to indicate that  $a$  is congruent to  $b$  modulo  $m$ . We say that  $a \equiv b \pmod{m}$  is a **congruence** and that  $m$  is its **modulus** (plural **moduli**). If  $a$  and  $b$  are not congruent modulo  $m$ , we write  **$a \not\equiv b \pmod{m}$** .

Although both notations  $a \equiv b \pmod{m}$  and  $a \text{ mod } m = b$  include “mod,” they represent fundamentally different concepts. The **first represents a relation** on the set of integers, whereas the **second represents a function**. However, the relation  $a \equiv b \pmod{m}$  and the  **$\text{mod } m$  function** are closely related, as described in Theorem 3.

##### THEOREM 3

Let  $a$  and  $b$  be integers, and let  $m$  be a positive integer. Then  **$a \equiv b \pmod{m}$  if and only if  $a \text{ mod } m = b \text{ mod } m$ .**

The proof of Theorem 3 is left as Exercises 21 and 22. Recall that  $a \bmod m$  and  $b \bmod m$  are the remainders when  $a$  and  $b$  are divided by  $m$ , respectively. Consequently, Theorem 3 also says that  $a \equiv b \pmod{m}$  if and only if  $a$  and  $b$  have the same remainder when divided by  $m$ .

**EXAMPLE 5** Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

**Solution:** Because 6 divides  $17 - 5 = 12$ , we see that  $17 \equiv 5 \pmod{6}$ . However, because  $24 - 14 = 10$  is not divisible by 6, we see that  $24 \not\equiv 14 \pmod{6}$ . ◀

The great German mathematician Karl Friedrich Gauss developed the concept of congruences at the end of the eighteenth century. The notion of congruences has played an important role in the development of number theory.

Theorem 4 provides a useful way to work with congruences.

**THEOREM 4** Let  $m$  be a positive integer. The integers  $a$  and  $b$  are congruent modulo  $m$  if and only if there is an integer  $k$  such that  $a = b + km$ .

**Proof:** If  $a \equiv b \pmod{m}$ , by the definition of congruence (Definition 3), we know that  $m \mid (a - b)$ . This means that there is an integer  $k$  such that  $a - b = km$ , so that  $a = b + km$ . Conversely, if there is an integer  $k$  such that  $a = b + km$ , then  $km = a - b$ . Hence,  $m$  divides  $a - b$ , so that  $a \equiv b \pmod{m}$ . ◀

The set of all integers congruent to an integer  $a$  modulo  $m$  is called the **congruence class** of  $a$  modulo  $m$ . In Chapter 9 we will show that there are  $m$  pairwise disjoint equivalence classes modulo  $m$  and that the union of these equivalence classes is the set of integers.

Theorem 5 shows that additions and multiplications preserve congruences.

**THEOREM 5** Let  $m$  be a positive integer. If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

### Links



©Hulton Archive/Getty Images

**KARL FRIEDRICH GAUSS (1777–1855)** Karl Friedrich Gauss, the son of a bricklayer, was a child prodigy. He demonstrated his potential at the age of 10, when he quickly solved a problem assigned by a teacher to keep the class busy. The teacher asked the students to find the sum of the first 100 positive integers. Gauss realized that this sum could be found by forming 50 pairs, each with the sum 101:  $1 + 100, 2 + 99, \dots, 50 + 51$ . This brilliance attracted the sponsorship of patrons, including Duke Ferdinand of Brunswick, who made it possible for Gauss to attend Caroline College and the University of Göttingen. While a student, he invented the method of least squares, which is used to estimate the most likely value of a variable from experimental results. In 1796 Gauss made a fundamental discovery in geometry, advancing a subject that had not advanced since ancient times. He showed that a 17-sided regular polygon could be drawn using just a ruler and compass.

In 1799 Gauss presented the first rigorous proof of the fundamental theorem of algebra, which states that a polynomial of degree  $n$  has exactly  $n$  roots in the complex numbers (counting multiplicities). Gauss achieved worldwide fame when he successfully calculated the orbit of the first asteroid discovered, Ceres, using scanty data.

Gauss was called the Prince of Mathematics by his contemporary mathematicians. Although Gauss is noted for his many discoveries in geometry, algebra, analysis, astronomy, and physics, he had a special interest in number theory, which can be seen from his statement “Mathematics is the queen of the sciences, and the theory of numbers is the queen of mathematics.” Gauss laid the foundations for modern number theory with the publication of his book *Disquisitiones Arithmeticae* in 1801.

**Proof:** We use a direct proof. Because  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , by Theorem 4 there are integers  $s$  and  $t$  with  $b = a + sm$  and  $d = c + tm$ . Hence,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

and

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

Hence,

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}. \quad \triangleleft$$

**EXAMPLE 6** Because  $7 \equiv 2 \pmod{5}$  and  $11 \equiv 1 \pmod{5}$ , it follows from Theorem 5 that

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

and that

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}. \quad \triangleleft$$



You cannot always divide both sides of a congruence by the same number!

We must be careful working with congruences. Some properties we may expect to be true are not valid. For example, if  $ac \equiv bc \pmod{m}$ , the congruence  $a \equiv b \pmod{m}$  may be false. Similarly, if  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , the congruence  $a^c \equiv b^d \pmod{m}$  may be false. (See Exercise 43.)

Corollary 2 shows how to find the values of the **mod**  $m$  function at the sum and product of two integers using the values of this function at each of these integers. We will use this result in Section 5.4.

## COROLLARY 2

Let  $m$  be a positive integer and let  $a$  and  $b$  be integers. Then

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

and

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$



**Proof:** By the definitions of **mod**  $m$  and of congruence modulo  $m$ , we know that  $a \equiv (a \bmod m) \pmod{m}$  and  $b \equiv (b \bmod m) \pmod{m}$ . Hence, Theorem 5 tells us that

$$a + b \equiv (a \bmod m) + (b \bmod m) \pmod{m}$$

and


$$ab \equiv (a \bmod m)(b \bmod m) \pmod{m}.$$

The equalities in this corollary follow from these last two congruences by Theorem 3. \triangleleft

In Section 4.6 we will carry out a variety of computations using the **mod** function when we study cryptography. Example 7 illustrates a type of computation involving the **mod** function that we will encounter.

**EXAMPLE 7** Find the value of  $(19^3 \bmod 31)^4 \bmod 23$ .

**Solution:** To compute  $(19^3 \bmod 31)^4 \bmod 23$ , we will first evaluate  $19^3 \bmod 31$ . Because  $19^3 = 6859$  and  $6859 = 221 \cdot 31 + 8$ , we have  $19^3 \bmod 31 = 6859 \bmod 31 = 8$ . So,  $(19^3 \bmod 31)^4 \bmod 23 = 8^4 \bmod 23$ .

Next, note that  $8^4 = 4096$ . Because  $4096 = 178 \cdot 23 + 2$ , we have  $4096 \bmod 23 = 2$ . Hence,  $(19^3 \bmod 31)^4 \bmod 23 = 2$ . 

### 4.1.5 Arithmetic Modulo $m$

We can define arithmetic **operations on  $\mathbf{Z}_m$** , the set of nonnegative **integers less than  $m$** , that is, the set  $\{0, 1, \dots, m-1\}$ . In particular, we define addition of these integers, denoted by  $+_m$  by

$$a +_m b = (a + b) \bmod m,$$

where the addition on the right-hand side of this equation is the ordinary addition of integers, and we define multiplication of these integers, denoted by  $\cdot_m$  by

$$a \cdot_m b = (a \cdot b) \bmod m,$$

where the multiplication on the right-hand side of this equation is the ordinary multiplication of integers. The operations  $+_m$  and  $\cdot_m$  are called addition and multiplication modulo  $m$  and when we use these operations, we are said to be doing **arithmetic modulo  $m$** .


**EXAMPLE 8** Use the definition of addition and multiplication in  $\mathbf{Z}_m$  to find  $7 +_{11} 9$  and  $7 \cdot_{11} 9$ .

**Solution:** Using the definition of addition modulo 11, we find that

$$7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5,$$

and

$$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8.$$

Hence,  $7 +_{11} 9 = 5$  and  $7 \cdot_{11} 9 = 8$ . 

The operations  $+_m$  and  $\cdot_m$  satisfy many of the same properties of ordinary addition and multiplication of integers. In particular, they satisfy these properties:

**Closure** If  $a$  and  $b$  belong to  $\mathbf{Z}_m$ , then  $a +_m b$  and  $a \cdot_m b$  belong to  $\mathbf{Z}_m$ .

**Associativity** If  $a$ ,  $b$ , and  $c$  belong to  $\mathbf{Z}_m$ , then  $(a +_m b) +_m c = a +_m (b +_m c)$  and  $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$ .

**Commutativity** If  $a$  and  $b$  belong to  $\mathbf{Z}_m$ , then  $a +_m b = b +_m a$  and  $a \cdot_m b = b \cdot_m a$ .

**Identity elements** The elements 0 and 1 are identity elements for addition and multiplication modulo  $m$ , respectively. That is, if  $a$  belongs to  $\mathbf{Z}_m$ , then  $a +_m 0 = 0 +_m a = a$  and  $a \cdot_m 1 = 1 \cdot_m a = a$ .

**Additive inverses** If  $a \neq 0$  belongs to  $\mathbf{Z}_m$ , then  $m - a$  is an additive inverse of  $a$  modulo  $m$  and 0 is its own additive inverse. That is,  $a +_m (m - a) = 0$  and  $0 +_m 0 = 0$ .



**Distributivity** If  $a$ ,  $b$ , and  $c$  belong to  $\mathbf{Z}_m$ , then  $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$  and  $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$ .

These properties follow from the properties we have developed for congruences and remainders modulo  $m$ , together with the properties of integers; we leave their proofs as Exercises 48–50. Note that we have listed the property that every element of  $\mathbf{Z}_m$  has an additive inverse, but no analogous property for multiplicative inverses has been included. This is because multiplicative inverses do not always exist modulo  $m$ . For instance, there is no multiplicative inverse of 2 modulo 6, as the reader can verify. We will return to the question of when an integer has a multiplicative inverse modulo  $m$  later in this chapter.

**Remark:** Because  $\mathbf{Z}_m$  with the operations of addition and multiplication modulo  $m$  satisfies the properties listed,  $\mathbf{Z}_m$  with modular addition is said to be a **commutative group** and  $\mathbf{Z}_m$  with both of these operations is said to be a **commutative ring**. Note that the set of integers with ordinary addition and multiplication also forms a commutative ring. Groups and rings are studied in courses that cover abstract algebra.

**Remark:** In Exercise 36, and in later sections, we will use the notations  $+$  and  $\cdot$  for  $+_m$  and  $\cdot_m$  without the subscript  $m$  on the symbol for the operator whenever we work with  $\mathbf{Z}_m$ .

## Exercises

- Does 17 divide each of these numbers?  
a) 68    b) 84    c) 357    d) 1001
- Prove that if  $a$  is an integer other than 0, then  
a) 1 divides  $a$ .    b)  $a$  divides 0.
- Prove that part (ii) of Theorem 1 is true.
- Prove that part (iii) of Theorem 1 is true.
- Show that if  $a \mid b$  and  $b \mid a$ , where  $a$  and  $b$  are integers, then  $a = b$  or  $a = -b$ .
- Show that if  $a, b, c$ , and  $d$  are integers, where  $a \neq 0$ , such that  $a \mid c$  and  $b \mid d$ , then  $ab \mid cd$ .
- Show that if  $a, b$ , and  $c$  are integers, where  $a \neq 0$  and  $c \neq 0$ , such that  $ac \mid bc$ , then  $a \mid b$ .
- Prove or disprove that if  $a \mid bc$ , where  $a, b$ , and  $c$  are positive integers and  $a \neq 0$ , then  $a \mid b$  or  $a \mid c$ .
- Prove that if  $a$  and  $b$  are integers and  $a$  divides  $b$ , then  $a$  is odd or  $b$  is even.
- Prove that if  $a$  and  $b$  are nonzero integers,  $a$  divides  $b$ , and  $a + b$  is odd, then  $a$  is odd.
- Prove that if  $a$  is an integer that is not divisible by 3, then  $(a + 1)(a + 2)$  is divisible by 3.
- Prove that if  $a$  is a positive integer, then 4 does not divide  $a^2 + 2$ .
- What are the quotient and remainder when  
a) 19 is divided by 7?    b)  $-111$  is divided by 11?  
c) 789 is divided by 23?    d) 1001 is divided by 13?  
e) 0 is divided by 19?    f) 3 is divided by 5?  
g)  $-1$  is divided by 3?    h) 4 is divided by 1?
- What are the quotient and remainder when  
a) 44 is divided by 8?  
b) 777 is divided by 21?  
c)  $-123$  is divided by 19?
- $-1$  is divided by 23?  
e)  $-2002$  is divided by 87?  
f) 0 is divided by 17?  
g) 1,234,567 is divided by 1001?  
h)  $-100$  is divided by 101?
- What time does a 12-hour clock read  
a) 80 hours after it reads 11:00?  
b) 40 hours before it reads 12:00?  
c) 100 hours after it reads 6:00?
- What time does a 24-hour clock read  
a) 100 hours after it reads 2:00?  
b) 45 hours before it reads 12:00?  
c) 168 hours after it reads 19:00?
- Suppose that  $a$  and  $b$  are integers,  $a \equiv 4 \pmod{13}$ , and  $b \equiv 9 \pmod{13}$ . Find the integer  $c$  with  $0 \leq c \leq 12$  such that  
a)  $c \equiv 9a \pmod{13}$ .  
b)  $c \equiv 11b \pmod{13}$ .  
c)  $c \equiv a + b \pmod{13}$ .  
d)  $c \equiv 2a + 3b \pmod{13}$ .  
e)  $c \equiv a^2 + b^2 \pmod{13}$ .  
f)  $c \equiv a^3 - b^3 \pmod{13}$ .
- Suppose that  $a$  and  $b$  are integers,  $a \equiv 11 \pmod{19}$ , and  $b \equiv 3 \pmod{19}$ . Find the integer  $c$  with  $0 \leq c \leq 18$  such that  
a)  $c \equiv 13a \pmod{19}$ .  
b)  $c \equiv 8b \pmod{19}$ .  
c)  $c \equiv a - b \pmod{19}$ .  
d)  $c \equiv 7a + 3b \pmod{19}$ .  
e)  $c \equiv 2a^2 + 3b^2 \pmod{19}$ .  
f)  $c \equiv a^3 + 4b^3 \pmod{19}$ .



19. Show that if  $a$  and  $d$  are positive integers, then  $(-a) \operatorname{div} d = -a \operatorname{div} d$  if and only if  $d$  divides  $a$ .
20. Prove or disprove that if  $a$ ,  $b$ , and  $d$  are integers with  $d > 0$ , then  $(a + b) \operatorname{div} d = a \operatorname{div} d + b \operatorname{div} d$ .
21. Let  $m$  be a positive integer. Show that  $a \equiv b \pmod{m}$  if  $a \bmod m = b \bmod m$ .
22. Let  $m$  be a positive integer. Show that  $a \bmod m = b \bmod m$  if  $a \equiv b \pmod{m}$ .
23. Show that if  $n$  and  $k$  are positive integers, then  $\lceil n/k \rceil = \lfloor (n-1)/k \rfloor + 1$ .
24. Show that if  $a$  is an integer and  $d$  is an integer greater than 1, then the quotient and remainder obtained when  $a$  is divided by  $d$  are  $\lfloor a/d \rfloor$  and  $a - d\lfloor a/d \rfloor$ , respectively.
25. Find a formula for the integer with smallest absolute value that is congruent to an integer  $a$  modulo  $m$ , where  $m$  is a positive integer.
26. Evaluate these quantities.
 

a) $-17 \bmod 2$	b) $144 \bmod 7$
c) $-101 \bmod 13$	d) $199 \bmod 19$
27. Evaluate these quantities.
 

a) $13 \bmod 3$	b) $-97 \bmod 11$
c) $155 \bmod 19$	d) $-221 \bmod 23$
28. Find  $a \operatorname{div} m$  and  $a \bmod m$  when
 

a) $a = -111, m = 99$ .	b) $a = -9999, m = 101$ .
c) $a = 10299, m = 999$ .	d) $a = 123456, m = 1001$ .
29. Find  $a \operatorname{div} m$  and  $a \bmod m$  when
 

a) $a = 228, m = 119$ .	b) $a = 9009, m = 223$ .
c) $a = -10101, m = 333$ .	d) $a = -765432, m = 38271$ .
30. Find the integer  $a$  such that
 

a) $a \equiv 43 \pmod{23}$ and $-22 \leq a \leq 0$ .	b) $a \equiv 17 \pmod{29}$ and $-14 \leq a \leq 14$ .
c) $a \equiv -11 \pmod{21}$ and $90 \leq a \leq 110$ .	
31. Find the integer  $a$  such that
 

a) $a \equiv -15 \pmod{27}$ and $-26 \leq a \leq 0$ .	b) $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$ .
c) $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$ .	
32. List five integers that are congruent to 4 modulo 12.
33. List all integers between  $-100$  and  $100$  that are congruent to  $-1$  modulo 25.
34. Decide whether each of these integers is congruent to 3 modulo 7.
 

a) 37	b) 66
c) $-17$	d) $-67$
35. Decide whether each of these integers is congruent to 5 modulo 17.
 

a) 80	b) 103
c) $-29$	d) $-122$
36. Find each of these values.
 

a) $(177 \bmod 31 + 270 \bmod 31) \bmod 31$	b) $(177 \bmod 31 \cdot 270 \bmod 31) \bmod 31$
---	---
37. Find each of these values.
 

a) $(-133 \bmod 23 + 261 \bmod 23) \bmod 23$	b) $(457 \bmod 23 \cdot 182 \bmod 23) \bmod 23$
--	---
38. Find each of these values.
 

a) $(19^2 \bmod 41) \bmod 9$	b) $(32^3 \bmod 13)^2 \bmod 11$
c) $(7^3 \bmod 23)^2 \bmod 31$	d) $(21^2 \bmod 15)^3 \bmod 22$
39. Find each of these values.
 

a) $(99^2 \bmod 32)^3 \bmod 15$	b) $(3^4 \bmod 17)^2 \bmod 11$
c) $(19^3 \bmod 23)^2 \bmod 31$	d) $(89^3 \bmod 79)^4 \bmod 26$
40. Show that if  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , where  $a, b, c, d$ , and  $m$  are integers with  $m \geq 2$ , then  $a - c \equiv b - d \pmod{m}$ .
41. Show that if  $n \mid m$ , where  $n$  and  $m$  are integers greater than 1, and if  $a \equiv b \pmod{m}$ , where  $a$  and  $b$  are integers, then  $a \equiv b \pmod{n}$ .
42. Show that if  $a, b, c$ , and  $m$  are integers such that  $m \geq 2$ ,  $c > 0$ , and  $a \equiv b \pmod{m}$ , then  $ac \equiv bc \pmod{mc}$ .
43. Find counterexamples to each of these statements about congruences.
 

a) If $ac \equiv bc \pmod{m}$ , where $a, b, c$ , and $m$ are integers with $m \geq 2$ , then $a \equiv b \pmod{m}$ .	b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ , where $a, b, c, d$ , and $m$ are integers with $c$ and $d$ positive and $m \geq 2$ , then $a^c \equiv b^d \pmod{m}$ .
---	---
44. Show that if  $n$  is an integer then  $n^2 \equiv 0$  or  $1 \pmod{4}$ .
45. Use Exercise 44 to show that if  $m$  is a positive integer of the form  $4k + 3$  for some nonnegative integer  $k$ , then  $m$  is not the sum of the squares of two integers.
46. Prove that if  $n$  is an odd positive integer, then  $n^2 \equiv 1 \pmod{8}$ .
47. Show that if  $a, b, k$ , and  $m$  are integers such that  $k \geq 1$ ,  $m \geq 2$ , and  $a \equiv b \pmod{m}$ , then  $a^k \equiv b^k \pmod{m}$ .
48. Show that  $\mathbf{Z}_m$  with addition modulo  $m$ , where  $m \geq 2$  is an integer, satisfies the closure, associative, and commutative properties, 0 is an additive identity, and for every nonzero  $a \in \mathbf{Z}_m$ ,  $m - a$  is an inverse of  $a$  modulo  $m$ .
49. Show that  $\mathbf{Z}_m$  with multiplication modulo  $m$ , where  $m \geq 2$  is an integer, satisfies the closure, associative, and commutativity properties, and 1 is a multiplicative identity.
50. Show that the distributive property of multiplication over addition holds for  $\mathbf{Z}_m$ , where  $m \geq 2$  is an integer.
51. Write out the addition and multiplication tables for  $\mathbf{Z}_5$  (where by addition and multiplication we mean  $+_5$  and  $\cdot_5$ ).
52. Write out the addition and multiplication tables for  $\mathbf{Z}_6$  (where by addition and multiplication we mean  $+_6$  and  $\cdot_6$ ).
53. Determine whether each of the functions  $f(a) = a \operatorname{div} d$  and  $g(a) = a \bmod d$ , where  $d$  is a fixed positive integer, from the set of integers to the set of integers, is one-to-one, and determine whether each of these functions is onto.