4

The Integers

4.1 The Division Algorithm

What are some of the important properties of the real numbers? Most of us learned early in life that they have a definite order. Later, we met the symbol $\leq$, whose properties are best summarized by saying that it is a partial order; that is, the binary relation $\leq$ is

reflexive: $a \leq a$ for all $a \in \mathsf{R}$,

antisymmetric: if $a \leq b$ and $b \leq a$ for $a, b \in \mathsf{R}$, then $a = b$, and

transitive: if $a \leq b$ and $b \leq c$, for $a, b, c \in \mathsf{R}$, then $a \leq c$.

(See Section 2.5.)

Readers should ensure that they agree with the following inequalities:

$$-15 \leq -8 \leq -\frac{1}{3} \leq -0.3 \leq -\frac{1}{4} \leq -0.25 \leq 0 \leq 1 \leq 3.14 \leq \pi \leq \frac{22}{7} \leq 4.$$

Which of the $\leq$ signs in the preceding list could be changed to the strict inequality $<$? The answer is all of them, except for $-\frac{1}{4} \leq -0.25$. Since $-\frac{1}{4} = -0.25$, the strict inequality $-\frac{1}{4} < -0.25$ is not true. Is it clear why each of the remaining $\leq$ signs could be replaced by $<$ signs?

Pause 1

Why is $-\frac{1}{3} < -0.3$? Why is $3.14 < \pi < \frac{22}{7}$? ∎

We can add two real numbers a and b and obtain their sum $a + b$, or we can multiply two real numbers a and b and obtain their product $a \cdot b$ (usually written ab, without the centered dot). These operations of addition and multiplication satisfy a number of important properties, the last three of which relate to order.

4.1.1 PROPERTIES OF + AND ·

Let a, b, and c be real numbers. Then

1. (**closure**) $a + b$ and ab are both real numbers.
2. (**commutativity**) $a + b = b + a$ and $ab = ba$.
3. (**associativity**) $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.
4. (**identities**) $a + 0 = a$ and $a \cdot 1 = a$.
5. (**distributivity**) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.
6. (**additive inverse**) $a + (-a) = 0$.

7. **(multiplicative inverse)** $a(\frac{1}{a}) = 1$ if $a \neq 0$.
8. $a \leq b$ implies $a + c \leq b + c$.
9. $a \leq b$ and $c \geq 0$ implies $ac \leq bc$.
10. $a \leq b$ and $c \leq 0$ implies $ac \geq bc$.

A third well-known operation, *subtraction*, is defined in terms of addition by the rule

$$a - b = a + (-b).$$

It is not unusual for a set of real numbers to have no smallest element; for example, there is no smallest element in the set $\{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots\}$. Similarly, there is no smallest positive number. On the other hand, this sort of thing does not occur with sets of natural numbers, according to the *Well-Ordering Principle*.

4.1.2 WELL-ORDERING PRINCIPLE

Any nonempty set of natural numbers has a smallest element.

In the rest of this section, we concentrate on the integers. All the properties of paragraph 4.1.1 (with closure suitably rephrased) hold for the integers, in most instances because they hold for all real numbers. The closure property for the integers says that the sum and product of integers are integers. Equivalently, we also say that the integers are *closed* under addition and under multiplication. Not all sets of real numbers are closed under these operations: The set of odd integers is not closed under addition since, for example, $1 + 3 = 4$, which is not odd.

Pause 2

Is the set of negative integers closed under multiplication? Is the set of natural numbers closed under multiplication? Is the set of natural numbers closed under subtraction? ∎

When some of us were schoolchildren, division of 58 by 17 was performed with a configuration like this,

$$\begin{array}{r} 3 \\ 17\overline{)58} \\ \underline{51} \\ 7 \end{array}$$

which served to illustrate that the answer is "3 remainder 7." When 58 is divided by 17, the *quotient* is 3 and the *remainder* is 7; equivalently,

$$58 = 3(17) + 7.$$

It is also true that $58 = 2(17) + 24$, but we were taught that the remainder must be less than the divisor. We now prove that this sort of division is always possible and, moreover, the quotient and the remainder are unique.

4.1.3 THEOREM

Given natural numbers a and b, there are unique nonnegative integers q and r, with $0 \leq r < b$, such that $a = qb + r$.

Proof

Consider the sequence of nonnegative multiples of b; that is, $0 \cdot b = 0$, $1 \cdot b = b$, $2 \cdot b = 2b$, $3 \cdot b = 3b$, ... The first term in this increasing sequence of numbers is 0, which is less than a since a is a natural number. On the other hand, some term is bigger than a [for example, $(2a)b > a$ because $2b > 1$], so, by the Well-Ordering Principle, the set of multiples of b that exceed a has a smallest element, say $(q+1)b$.

So we have $qb \le a < (q+1)b$. (See Fig. 4.1.) Set $r = a - qb$. Since $qb \le a$, we have $r \ge 0$. Since $(q+1)b > a$, we have $r < b$. Hence, $0 \le r < b$, and we have found q and r as required.

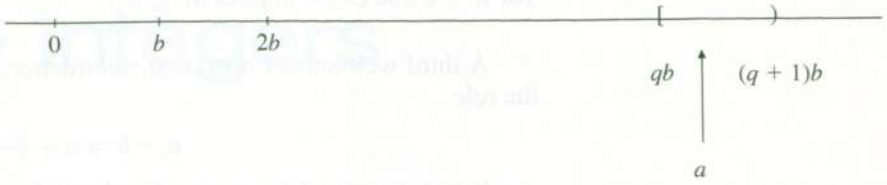


Figure 4.1

To see that q and r are unique, assume that a can be expressed in the given form in two ways; that is, suppose that $a = q_1 b + r_1$ and $a = q_2 b + r_2$ with $0 \le r_1 < b$ and $0 \le r_2 < b$. Then $(q_1 - q_2)b = r_2 - r_1$. Now $(q_1 - q_2)b$ is an integral multiple of b, while $-b < r_2 - r_1 < b$. The only possibility is that this multiple is 0, and so $q_1 = q_2, r_1 = r_2$ as desired. ●

4.1.4 DEFINITIONS

If a and b are natural numbers and $a = qb + r$ for nonnegative integers q and r with $0 \le r < b$, the integer q is called the *quotient* and the integer r is called the *remainder* when a is divided by b. ❖

When a and b are both positive and a is divided by b, it is useful to note that the quotient is the integer part of the number displayed by a calculator used to divide a by b. (The remainder is $a - qb$.)

PROBLEM 1. Find the quotient q and the remainder r and write $a = qb + r$ when $a = 19$ is divided by $b = 7$. Find the quotient and remainder when 589,621 is divided by 7893 and when 11,109,999,999 is divided by 1111.

Solution. When 19 is divided by 7, the quotient is 2 and the remainder is 5. We have $19 = 2(7) + 5$.

Dividing 589,621 by 7893, one author's calculator displayed 74.701761. Thus, $q = 74$ and $r = 589{,}621 - 74(7893) = 5539$.

For the last part of the question, we have to be a little resourceful since one of the numbers here is too large for the author's unsophisticated calculator! Instead, we note that

$$\begin{aligned} 11{,}109{,}999{,}999 &= 11{,}110{,}000{,}000 - 1 \\ &= 1111(10{,}000{,}000) - 1 \\ &= 1111(9{,}999{,}999 + 1) - 1 \\ &= 1111(9{,}999{,}999) + 1110. \end{aligned}$$

So the quotient is 9,999,999 and the remainder is 1110. ▲

With only slight modifications, Theorem 4.1.3 can be generalized to situations where a and b are integers, not just natural numbers. Note, however, that to preserve the uniqueness of q the possibility $b = 0$ must be excluded.[1] (Also, in this case, the condition $0 \le r < b$ would be impossible to meet.)

---

[1] Division by 0 always causes problems!

4.1.5 THE DIVISION ALGORITHM

Let $a, b \in \mathbf{Z}$, $b \neq 0$. Then there exist unique integers q and r, with $0 \leq r < |b|$, such that $a = qb + r$.

Proof In Theorem 4.1.3, we proved this in the case when a and b are both positive. If $a = 0$, then $q = 0$, $r = 0$ gives a solution. We will consider the other cases individually.

Case 1: $b > 0$ and $a < 0$.
Since $-a > 0$, we can apply Theorem 4.1.3 to $-a$ and b obtaining q and r, with $0 \leq r < b$, such that $-a = qb + r$. Therefore, $a = (-q)b - r$. If $r = 0$, $a = (-q)b$, while if $r > 0$, $a = (-q - 1)b + (b - r)$ with $0 < b - r < b = |b|$. In either case, we have expressed a in the desired form.

Case 2: $b < 0$ and either $a > 0$ or $a < 0$.
Here $-b > 0$, so Theorem 4.1.3 and Case 1 tell us that there exist integers q and r, $0 \leq r < -b = |b|$, such that $a = q(-b) + r = (-q)b + r$. Again we have expressed a in the desired form.

The proof of uniqueness follows as in Theorem 4.1.3. ●

Chapter 8 is devoted to the subject of *algorithms*. Here, we simply remark that *algorithm* means "definite procedure" and that the theorem known as the *Division Algorithm* takes its name from the fact that there is a definite procedure for determining q and r, given a and b. For $a, b > 0$, $q = \lfloor \frac{a}{b} \rfloor$ is the integer part of $\frac{a}{b}$ and $r = a - qb$, as illustrated in Problem 1. For possibly negative a and/or b, the procedure is given in Proposition 4.1.6.

EXAMPLE 2 Verify that $a = qb + r$ in each of the following cases and, in the process, notice that q is not always what we might expect.

a	b	q	r
58	17	3	7
58	−17	−3	7
−58	17	−4	10
−58	−17	4	10

■

When a is written in the form $a = qb + r$, with $0 \leq r < |b|$, we shall show that q is the floor or ceiling of $\frac{a}{b}$ according as b is positive or negative. (The *floor* and *ceiling* functions were defined in paragraph 3.1.7.) In the preceding table, for instance, when $a = -58$, $b = 17$, $\lfloor -\frac{58}{17} \rfloor = \lfloor -3.41\ldots \rfloor = -4$, the value recorded for q. When $a = -58$, $b = -17$, $\lceil \frac{-58}{-17} \rceil = \lceil 3.41 \rceil = 4$, again the recorded value of q.

4.1.6 PROPOSITION If $a = qb + r$, with $0 \leq r < |b|$, then

$$q = \begin{cases} \lfloor \frac{a}{b} \rfloor & \text{if } b > 0 \\ \lceil \frac{a}{b} \rceil & \text{if } b < 0. \end{cases}$$

Proof We consider the case $b > 0$ and leave the other possibility to the exercises. By definition of floor, $x - 1 < \lfloor x \rfloor \leq x$ for any x. Let $x = \frac{a}{b}$ and $\lfloor x \rfloor = k$. Then

$$\frac{a}{b} - 1 < k \leq \frac{a}{b}.$$

Multiplying by the positive number b (and using Property 9 of paragraph 4.1.1), we obtain $a - b < kb \leq a$ and then, multiplying by -1,

$$-a \leq -kb < -a + b$$

(by Property 10). Adding a gives $0 \leq a - kb < b$ so, letting $r = a - kb$, we have $a = kb + r$ with $0 \leq r < |b|$. By uniqueness of q, $q = k = \lfloor \frac{a}{b} \rfloor$, as asserted. ●

EXAMPLE 3 With $a = -1027$ and $b = 38$, we have

$$\left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor -\frac{1027}{38} \right\rfloor = \lfloor -27.026\ldots \rfloor = -28 = q.$$

It is straightforward now to determine r: $r = a - qb = -1027 + 1064 = 37$. Thus, $-1027 = -28(38) + 37$. With $a = 1{,}234{,}567$ and $b = -103$, we have $\lceil \frac{a}{b} \rceil = \lceil -11{,}986.087\ldots \rceil = -11{,}986 = q$. As before, we note that $r = a - qb = 1{,}234{,}567 - (-11{,}986)(-103) = 9$. Thus, $1{,}234{,}567 = -103(-11{,}986) + 9$. ■

Representing Natural Numbers in Various Bases

As an application of some of the ideas we have presented so far, we discuss briefly the representation of natural numbers in bases other than the familiar one.

Unless they have reason to suspect otherwise, most people expect that the numbers they encounter in their day-to-day lives are presented in *base* 10. The integer 2159, for example, is assumed to mean

$$2 \cdot 10^3 + 1 \cdot 10^2 + 5 \cdot 10 + 9.$$

The digits 9, 5, 1, and 2 are called, respectively, the *units*, *tens*, *hundreds*, and *thousands* digits of this integer. If we lived in a base 12 world, however, we would interpret 2159 as

$$2 \cdot 12^3 + 1 \cdot 12^2 + 5 \cdot 12 + 9.$$

When we represent a number in a base other than 10, we shall employ notation such as $(2159)_{12}$. Thus,

$$(2159)_{12} = 2 \cdot 12^3 + 1 \cdot 12^2 + 5 \cdot 12 + 9.$$

4.1.7 DEFINITION Given a fixed natural number $b > 1$, the *base b representation* of a natural number N is the expression $(a_{n-1}a_{n-2}\ldots a_0)_b$, where $a_0, a_1, \ldots, a_{n-1}$ are those integers $0 \leq a_i < b$ that satisfy $N = a_{n-1}b^{n-1} + a_{n-2}b^{n-2} + \cdots + a_1 b + a_0$. Thus,

$$(a_{n-1}a_{n-2}\ldots a_0)_b = a_{n-1}b^{n-1} + a_{n-2}b^{n-2} + \cdots + a_1 b + a_0. \quad ❖$$

The base 5 representation of 117 is 432, written $117 = (432)_5$, because $117 = 4(5^2) + 3(5) + 2$. In base 3, $117 = (11{,}100)_3$ because $117 = 1(3^4) + 1(3^3) + 1(3^2)$. While 10 is the most familiar base, nowadays bases 2, 8, and 16 are also common. Base 2 is also known as *binary*, base 8 as *octal*, and base 16 as *hexadecimal*. The basic hexadecimal digits are 0–9, A, B, C, D, E, and F. For example, $10 = \mathrm{A}_{16}$, $11 = \mathrm{B}_{16}$, and $(4\mathrm{C})_{16} = 4 \cdot 16 + 12 = 76$.

To convert from base b to base 10 is easy: Use the definition of $(\ldots)_b$ in 4.1.7. What about converting from base 10 to base b?

Suppose that $N = (a_{n-1}a_{n-2}\ldots a_0)_b$ is a number given in base b. Then

$$\begin{aligned} N &= a_{n-1}b^{n-1} + a_{n-2}b^{n-2} + \cdots + a_1 b + a_0 \\ &= (a_{n-1}b^{n-2} + a_{n-2}b^{n-3} + \cdots + a_1)b + a_0 = q_0 b + a_0, \end{aligned}$$

where $q_0 = a_{n-1}b^{n-2} + a_{n-2}b^{n-3} + \cdots + a_1$. Since $0 \le a_0 < b$, when N is divided by b, the remainder is a_0 and the quotient is q_0. Similarly,

$$q_0 = (a_{n-1}b^{n-3} + a_{n-2}b^{n-4} + \cdots + a_2)b + a_1 = q_1 b + a_1$$

with $q_1 = a_{n-1}b^{n-3} + a_{n-2}b^{n-4} + \cdots + a_2$, so when q_0 is divided by b, the remainder is a_1 and the quotient is q_1. In a similar way, we see that a_2 is the remainder when q_1 is divided by b. Thus, the digits in the representation of N in base b are, from right to left, the remainders when first N and then successive quotients are divided by b.

PROBLEM 4. Find the binary, octal, and hexadecimal representations of the number 2159.

Solution. We have $2159 = 1079(2) + 1$, $1079 = 539(2) + 1$, $539 = 269(2) + 1$, $269 = 134(2) + 1$, $134 = 67(2) + 0$, $67 = 33(2) + 1$, $33 = 16(2) + 1$, $16 = 8(2) + 0$, $8 = 4(2) + 0$, $4 = 2(2) + 0$, $2 = 2(1) + 0$, and $1 = 0(2) + 1$. The sequence of remainders is 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 1, so, writing these in reverse order, $2159 = (100{,}001{,}101{,}111)_2$.

The base 8 and base 16 representations can be obtained by similar means or from the base 2 representation. Having determined that $2159 = 2^{11} + 2^6 + 2^5 + 2^3 + 2^2 + 2 + 1$, we have

$$\begin{aligned} 2159 &= 2^2(2^3)^3 + (2^3)^2 + (2^2)2^3 + 2^3 + 7 \\ &= 4(8^3) + 1(8^2) + 5(8) + 7 = (4157)_8 \end{aligned}$$

and

$$\begin{aligned} 2159 &= 2^{11} + 2^6 + 2^5 + 2^3 + 2^2 + 2 + 1 \\ &= 2^3(2^4)^2 + 2^2(2^4) + 2(2^4) + 15 \\ &= 8(16)^2 + 6(16) + 15 = (86\text{F})_{16}. \end{aligned}$$

▲

PROBLEM 5. Convert 21,469 to octal and to hexadecimal notation.

Solution. We have $21{,}469 = 2683(8) + 5$, $2683 = 335(8) + 3$, $335 = 41(8) + 7$, $41 = 5(8) + 1$ and $5 = 0(8) + 5$. Thus, $21{,}469 = (51{,}735)_8$. Similarly, $21{,}469 = 1341(16) + 13$, $1341 = 83(16) + 13$, $83 = 5(16) + 3$, and $5 = 0(16) + 5$, so $21{,}469 = (53\text{DD})_{16}$. ▲

The authors have a colleague who figures it's time to retire now that he is 1,000,000. How old do you think this fellow is? ▮

Answers to Pauses

1. $\frac{1}{3}$ is the same as the decimal $0.333\ldots$. The three dots "..." mean that the 3's continue indefinitely. We often write $\frac{1}{3} = 0.\dot{3}$ and say that $\frac{1}{3}$ equals "point 3 repeated." Since $0.\dot{3}$ is larger than 0.3, its **negative**, $-0.\dot{3}$, is less than -0.3. The number π is perhaps the most fascinating number of all. Its decimal expansion begins 3.14159, so it is definitely bigger than 3.14. As a decimal, $\frac{22}{7} = 3.\overline{142857}$, where the line indicates that the sequence of numbers underneath is repeated indefinitely; thus,

$$\frac{22}{7} = 3.\underbrace{142857}\,\underbrace{142857}\,\underbrace{142857}\,142857\ldots.$$

Thus, we see that $\pi < \frac{22}{7}$. Unlike $\frac{1}{3}$ and $\frac{22}{7}$, the decimal expansion of π continues indefinitely, without any kind of pattern.

2. The set of negative integers is not closed under multiplication since, for example, $(-2)(-3) = 6$ is not a negative integer. The set of natural numbers is closed under multiplication since the product of natural numbers is a natural number. The natural numbers are not closed under subtraction since, for example, $4 - 7$ is not a natural number.
3. We think he is $64 = 1{,}000{,}000_2$.

True/False Questions

(Answers can be found in the back of the book.)

1. $-\pi \leq -\frac{22}{7}$
2. The Well-Ordering Principle states that any nonempty set of natural numbers has a smallest element.
3. The equation $15 = (2 \times 4) + 7$ is correct.
4. The equation in Question 3 with $a = 15$, $b = 4$, $q = 2$, and $r = 7$ satisfies the requirements of the Division Algorithm.
5. The equation $-15 = ((-3) \times 4)) + (-3)$ satisfies the requirements of the Division Algorithm (with $a = -15$ and $b = 4$).
6. The equation $-15 = ((-4) \times 4) + 1$ satisfies the requirements of the Division Algorithm (with $a = -15$ and $b = 4$).
7. If $a, b > 0$ and q, r are chosen to satisfy the requirements of the Division Algorithm, then $q = \lceil \frac{a}{b} \rceil$.
8. The base 3 representation of 91 is 3101.
9. The base 5 representation of 91 is 3301.
10. The base 10 representation of $(124)_7$ is 67.

Exercises

*The answers to exercises marked [BB] can be found in the **B**ack of the **B**ook.*

1. [BB] Use the properties given in paragraph 4.1.1 to derive a second distributive law: $(a+b)c = ac+bc$ for any real numbers a, b, c.
2. True or false? If false, give a counterexample.
   (a) [BB] Subtraction is a closed operation on the real numbers.
   (b) Subtraction of real numbers is commutative.
   (c) Subtraction of real numbers is associative.
3. Show (by means of a counterexample) that Property 9 of paragraph 4.1.1 does not hold if $c < 0$.
4. [BB] Find the quotient q and the remainder r as defined in the Division Algorithm, 4.1.5, in each of the following cases.
   (a) $a = 500; b = 17$ (b) $a = -500; b = 17$
   (c) $a = 500; b = -17$ (d) $a = -500; b = -17$
5. Find q and r as defined in the Division Algorithm, 4.1.5, in each of the following cases.
   (a) $a = 5286; b = 19$ (b) $a = -5286; b = 19$
   (c) $a = 5286; b = -19$ (d) $a = -5286; b = -19$
   (e) $a = 19; b = 5286$ (f) $a = -19; b = 5286$
6. Find integers q and r, with $0 \leq r < |b|$, such that $a = bq + r$ in each of the following cases.
   (a) $a = 12{,}345; b = -39$
   (b) $a = -27{,}361; b = -977$
   (c) $a = -102{,}497; b = -1473$
   (d) $a = 98{,}764; b = 4789$
   (e) $a = -41{,}391; b = -755$
   (f) $a = 555{,}555{,}123; b = 111{,}111{,}111$
   (g) $a = 81{,}538{,}416{,}000; b = 38{,}754$
7. [BB] Let a be an integer. Prove that there exists an integer k such that $a^2 = 3k$ or $a^2 = 3k + 1$.
8. [BB] Fix a natural number $n > 1$ and define $f: \mathbb{Z} \to \mathbb{Z}$ by setting $f(a)$ equal to the quotient when a is divided by n; that is, $f(a) = q$, where $a = qn + r$ with $0 \leq r < n$.
   (a) Find the domain and range of f.
   (b) Is f one-to-one?
   (c) Is f onto?
   Explain your answers.

9. Suppose $n > 1$ is a natural number and $f: \mathbb{Z} \to \mathbb{N} \cup \{0\}$ is the function that associates with each $a \in \mathbb{Z}$ its remainder upon division by n; thus, if $a = qn + r$ with $0 \leq r < n$, then $f(a) = r$.

(a) Find the domain and range of f.

(b) Is f one-to-one?

(c) Is f onto?

Explain your answers.

10. [BB] Complete the proof of Proposition 4.1.6 by showing that, if $a = qb + r$ with $0 \leq r < |b|$ and $b < 0$, then $q = \lceil a/b \rceil$.

11. Find the binary, octal, and hexadecimal representations for each of the following integers (given in base 10).

(a) [BB] 4034 **(b)** 57,483 **(c)** 185,178

12. **(a)** Suppose the natural number N is $(a_{n-1} \ldots a_0)_b$ (in base b). Prove that $n - 1 = \lfloor \log_b N \rfloor$ (and hence that N has $1 + \lfloor \log_b N \rfloor$ digits in base b).

(b) How many digits does 7^{254} have in its base 10 representation?

(c) How many digits does the number 319^{566} have in its base 10 representation?

4.2 Divisibility and the Euclidean Algorithm

When we say that one integer *divides* another, we mean "divides exactly," that is, with a remainder of 0.

4.2.1 DEFINITION Given integers a and b with $b \neq 0$, we say that b is a *divisor* or a *factor* of a and that a *is divisible by* b if and only if $a = qb$ for some integer q. We write $b \mid a$ to signify that a is divisible by b and say "b divides a." ❖

For example, 3 is a divisor of 18, -7 is a divisor of 35, $16 \mid -64$, $-4 \nmid 38$. (As always, a slash through a symbol negates the meaning of that symbol. Just as $\neq$ means "not equal" and $\notin$ means "does not belong to," so $\nmid$ means "does not divide.")

Note that $1 \mid n$ for any integer n because $n = n \cdot 1$.

Pause 4 Show that $n \mid 0$ for any integer $n \neq 0$. ∎

PROBLEM 6. Given three consecutive integers a, $a+1$, $a+2$, prove that one of them is divisible by 3.

Solution. By the division algorithm, we can write $a = 3q + r$ with $0 \leq r < 3$. Since r is an integer, we must have $r = 0$, $r = 1$, or $r = 2$. If $r = 0$, then $a = 3q$ is divisible by 3. If $r = 1$, then $a = 3q + 1$, so $a + 2 = 3q + 3$ is divisible by 3. If $r = 2$, then $a = 3q + 2$, so $a + 1 = 3q + 3$ is divisible by 3. ▲

The most important properties of "divides" are summarized in the next proposition.

4.2.2 PROPOSITION The binary relation $\mathcal{R}$ on $\mathbb{N}$ defined by $(a, b) \in \mathcal{R}$ if and only if $a \mid b$ is a partial order.

Proof We have to show that the relation is reflexive, antisymmetric, and transitive.

Reflexive: For any $a \in \mathbb{N}$, $a \mid a$ because $a = 1 \cdot a$.

Antisymmetric: Suppose $a, b \in \mathbb{N}$ are such that $a \mid b$ and $b \mid a$. Then $b = q_1 a$ for some natural number q_1 and $a = q_2 b$ for some natural number q_2. Thus, $a = q_2(q_1 a) = (q_1 q_2)a$. Since $a \neq 0$, $q_1 q_2 = 1$, and, since q_1 and q_2 are natural numbers, we must have $q_1 = q_2 = 1$; thus, $a = b$.

Transitive: If $a, b, c \in \mathbb{N}$ are such that $a \mid b$ and $b \mid c$, then $b = q_1 a$ and $c = q_2 b$ for some natural numbers q_1 and q_2. Thus, $c = q_2 b = q_2(q_1 a) = (q_1 q_2)a$, with $q_1 q_2$ a natural number. So $a \mid c$. ●

The proposition says that $(\mathbb{N}, |)$ is a partially ordered set. In fact, $(A, |)$ is a poset for any set A of natural numbers. At this point, we encourage you to review Section 2.5 and, in particular, the terminology associated with posets.

EXAMPLE 7 Let $A = \{1, 2, 3, 4, 5, 6\}$. In the poset $(A, |)$, the element 4 is maximal because there is no $a \in A$ satisfying $4 \mid a$ except $a = 4$. This element is not a maximum however, since, and for example, $5 \nmid 4$. Similarly, 5 and 6 are maximal elements that are not maximum. ■

Pause 5 Draw the Hasse diagram for this poset and find all minimal, minimum, maximal, and maximum elements. ▮

Another property of "divides" is the content of the next proposition, whose proof is a straightforward consequence of the definition.

4.2.3 PROPOSITION Suppose a, b, and c are integers such that $c \mid a$ and $c \mid b$. Then $c \mid (xa + yb)$ for any integers x and y.

Proof Since $c \mid a$, we know that $a = q_1 c$ for some integer q_1. Since $c \mid b$, we also have $b = q_2 c$ for some integer q_2. Thus, $xa + yb = xq_1 c + yq_2 c = (q_1 x + q_2 y)c$. Since $q_1 x + q_2 y$ is an integer, $c \mid (xa + yb)$, as required. ●

The Greatest Common Divisor

4.2.4 DEFINITION Let a and b be integers not both of which are 0. An integer g is the *greatest common divisor (gcd)* of a and b if and only if g is the largest common divisor of a and b; that is, if and only if

1. $g \mid a$, $g \mid b$ and,
2. if c is any integer such that $c \mid a$ and $c \mid b$, then $c \leq g$.

We write $g = \gcd(a, b)$ to signify that g is the greatest common divisor of a and b. ❖

EXAMPLE 8

- The greatest common divisor of 15 and 6 is 3,
- $\gcd(-24, 18) = 6$,
- $\gcd(756, 210) = 42$,
- $\gcd(-756, 210) = 42$,
- $\gcd(-756, -210) = 42$. ■

Pause 6 If a and b are integers such that $a \mid b$, what is the greatest common divisor of a and b? ▮

Pause 7 Suppose a is a nonzero integer. What is $\gcd(a, 0)$? ▮

It follows almost immediately from the definition that two integers, not both 0, have exactly one greatest common divisor. (See Exercise 15.) Also, since 1 is a common divisor of any two integers, the greatest common divisor of two integers is always positive.

The seventh book of Euclid's *Elements* (300 B.C.) describes a procedure now known as the Euclidean algorithm for finding the gcd of two integers a and b. It is based on the fact that when $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$. For instance, since $\underline{58} = 3(\underline{17}) + \underline{7}$, it must be that $\gcd(58, 17) = \gcd(17, 7)$. Also, since $\underline{75} = 3(\underline{21}) + \underline{12}$, it must be that $\gcd(75, 21) = \gcd(21, 12)$.

4.2.5 LEMMA If $a = qb + r$ for integers a, b, q, and r, then $\gcd(a, b) = \gcd(b, r)$.

Proof If $a = b = 0$, then $a = qb + r$ says $r = 0$. Similarly, if $b = r = 0$, then $a = 0$. In either case, the result is true since neither $\gcd(a, b)$ nor $\gcd(b, r)$ is defined. Thus, it remains to consider the case that $g_1 = \gcd(a, b)$ and $g_2 = \gcd(b, r)$ are both well-defined integers. First, $g_2 \mid b$ and $g_2 \mid r$, so $g_2 \mid (qb + r)$; that is, $g_2 \mid a$. Thus, g_2 is a common divisor of a and b and, since g_1 is the greatest common divisor of a and b, we have $g_2 \leq g_1$.

On the other hand, since $g_1 \mid a$ and $g_1 \mid b$, we know that $g_1 \mid (a - qb)$; that is, $g_1 \mid r$. As a common divisor of b and r, it cannot exceed the gcd of these numbers. Thus, $g_1 \leq g_2$, so $g_1 = g_2$, as desired. ●

The Euclidean algorithm involves nothing more than a repeated application of this lemma.

4.2.6 EUCLIDEAN ALGORITHM Let a and b be natural numbers with $b < a$. To find the greatest common divisor of a and b, write

$$a = q_1 b + r_1, \quad \text{with } 0 \leq r_1 < b.$$

If $r_1 \neq 0$, write $b = q_2 r_1 + r_2$, with $0 \leq r_2 < r_1$.

If $r_2 \neq 0$, write $r_1 = q_3 r_2 + r_3$, with $0 \leq r_3 < r_2$.

If $r_3 \neq 0$, write $r_2 = q_4 r_3 + r_4$, with $0 \leq r_4 < r_3$.

Continue this process until some remainder $r_{k+1} = 0$. Then the greatest common divisor of a and b is r_k, the last nonzero remainder. ❖

Why does this process work? Why must some remainder be 0? To answer the second question, suppose no remainder is zero. Then $\{r_1, r_2, r_3, \dots\}$ is a nonempty set of natural numbers and hence has a smallest element, r_k, by the Well-Ordering Principle. Since the next remainder is smaller than r_k, we have a contradiction. So some remainder, $r_{k+1} = 0$ and, by Lemma 4.2.5, the last nonzero remainder r_k is the gcd of a and b because

$$\begin{aligned}\gcd(a, b) = \gcd(b, r_1) &= \gcd(r_1, r_2) \\ &= \gcd(r_2, r_3) = \cdots = \gcd(r_k, r_{k+1}) = \gcd(r_k, 0) = r_k.\end{aligned}$$

PROBLEM 9. Find the greatest common divisor of 630 and 196.

Solution. We have

$$\begin{aligned} 630 &= 3(196) + 42 \\ 196 &= 4(42) + 28 \\ 42 &= 1(28) + 14 \\ 28 &= 2(14) + 0. \end{aligned}$$

The last nonzero remainder is 14, so this is $\gcd(630, 196)$. ▲

Let us write down these same equations in a different way, expressing each of the remainders ($r_1 = 42$, $r_2 = 28$, $r_3 = 14$) in terms of $a = 630$ and $b = 196$. We have

$$\begin{aligned} 42 &= 630 - 3(196) && = a - 3b \\ 28 &= 196 - 4(42) \\ (1) \qquad &= b - 4r_1 = b - 4(a - 3b) && = -4a + 13b \\ 14 &= 42 - 28 \\ &= r_1 - r_2 = (a - 3b) - (-4a + 13b) = 5a - 16b. \end{aligned}$$

Recording only the remainders and the coefficients a and b, these equations can be neatly coded by the array

$$\begin{array}{rrr} 42 & 1 & -3 \\ 28 & -4 & 13 \\ 14 & 5 & -16. \end{array}$$

Adding to the top of this array the rows

$$\begin{array}{rrr} 630 & 1 & 0 \\ 196 & 0 & 1, \end{array}$$

which correspond to the equations $630 = 1a + 0b$ and $196 = 0a + 1b$, respectively, we obtain the array

$$\begin{array}{rrr} 630 & 1 & 0 \\ 196 & 0 & 1 \\ 42 & 1 & -3 \\ 28 & -4 & 13 \\ 14 & 5 & -16, \end{array}$$

which is easy to remember. Each row after the first two is of the form $x - qy$, where x and y are the two rows preceding it and q is the quotient when the first number in x is divided by the first number in y. When 630 is divided by 196, the quotient is 3, so the third row is

$$(630\ 1\ 0) - 3(196\ 0\ 1) = 42\ 1\ -3.$$

When 196 is divided by 42, the quotient is 4, so the fourth row is

$$(196\ 0\ 1) - 4(42\ 1\ -3) = 28\ -4\ 13.$$

When 42 is divided by 28, the quotient is 1; so the last row is

$$(42\ 1\ -3) - (28\ -4\ 13) = 14\ 5\ -16.$$

Since the last remainder, 14, divides the previous remainder, 28, the next remainder is 0. So gcd(630, 196) = 14, the last nonzero remainder.

Here is another example of this procedure.

PROBLEM 10. Find gcd(1800, 756).

Solution.

$$\begin{array}{rrr} 1800 & 1 & 0 \\ 756 & 0 & 1 \\ 288 & 1 & -2 \\ 180 & -2 & 5 \\ 108 & 3 & -7 \\ 72 & -5 & 12 \\ 36 & 8 & -19 \end{array}$$

Since the last nonzero remainder is 36, gcd(1800, 756) = 36. ▲

4.2.7 DEFINITION Nonzero integers are *relatively prime* if and only if their greatest common divisor is 1, in other words, if and only if 1 is the only positive integer that divides both the given integers. ❖

Pause 8 Show that 17,369 and 5472 are relatively prime. ∎

There is a very important property of the greatest common divisor that we have so far overlooked. As seen most clearly in equations (1), each remainder that arises in the course of applying the algorithm is an *integral linear combination* of the given two numbers a and b; that is, each remainder can be written in the form $ma+nb$ for integers m and n. In particular, the greatest common divisor of a and b, being the last nonzero remainder, is an integral linear combination of a and b. For example, as we saw in (1), $\gcd(630, 196) = 14 = 5a - 16b = 5(630) - 16(196)$. Similarly, the calculations of Problem 10 show that $\gcd(1800, 756) = 36 = 8(1800) - 19(756)$.

Pause 9

In PAUSE 8 we asked you to show that the integers 17,369 and 5472 are relatively prime. Find integers m and n so that $17{,}369m + 5472n = 1$. ∎

4.2.8 REMARK

Since, by definition, the greatest common divisor of two integers a and b, which are not both 0, is a positive number, it is clear that $\gcd(a, b) = \gcd(|a|, |b|)$. For example, $\gcd(15, -36) = \gcd(15, 36) = 3$ and $\gcd(-18, -99) = \gcd(18, 99) = 9$. Since $|a|$ and $|b|$ are natural numbers, the Euclidean algorithm in fact can be used to find the greatest common divisor of *any* pair of nonzero integers a and b. ❖

We have been illustrating through examples a general fact: The greatest common divisor of two natural numbers a and b is a linear combination of a and b. If $a = 0$ and $b \geq 1$, then $\gcd(a, b) = b = 0(a)+1(b)$ is also a linear combination of a and b. If $\gcd(|a|, |b|)$ is a linear combination of $|a|$ and $|b|$, then our remark shows that $\gcd(a, b) = \gcd(|a|, |b|)$ is a linear combination of a and b (since $|a| = \pm a$ and $|b| = \pm b$). For example, since $\gcd(1800, 756) = 36 = 8(1800) - 19(756)$, $\gcd(1800, -756) = 36 = 8(1800) + 19(-756)$. The following theorem, the proof of which follows by noting that each remainder in the Euclidean algorithm is a linear combination of the previous two, describes the most important property of the greatest common divisor. (See also Exercise 26.)

4.2.9 THEOREM

The greatest common divisor of integers a and b is an integral linear combination of them; that is, if $g = \gcd(a, b)$, then there are integers m and n such that $g = ma + nb$.

The corollaries that follow illustrate ways in which this theorem is used.

4.2.10 COROLLARY

Suppose a, b, and x are integers such that $a \mid bx$. If a and b are relatively prime, then $a \mid x$.

Proof

We know that there are integers m and n so that $ma + nb = 1$ [because $\gcd(a, b) = 1$]. Multiplying by x, we obtain $max + nbx = x$. But $a \mid max$ and $a \mid nbx$ because $nbx = n(bx)$, and we are given that $a \mid bx$. Thus, a divides the sum $max + nbx = x$.

●

4.2.11 COROLLARY

The greatest common divisor of nonzero integers a and b is divisible by every common divisor of a and b.

Proof

Let $g = \gcd(a, b)$. By Theorem 4.2.9, $g = ma + nb$ for integers m and n. Thus, by Proposition 4.2.3, if c is a common divisor of a and b, then $c \mid g$. ●

PROBLEM 11. Suppose a, b and c are three nonzero integers with a and c relatively prime. Show that $\gcd(a, bc) = \gcd(a, b)$.

Solution. Let $g_1 = \gcd(a, bc)$ and $g_2 = \gcd(a, b)$. Since $g_2 \mid b$, we know that $g_2 \mid bc$. Since also $g_2 \mid a$, we have $g_2 \leq g_1$. On the other hand (and just as in Corollary 4.2.10), since $\gcd(a, c) = 1$, there are integers m and n such that $ma + nc = 1$. Multiplying by b, we obtain $mab + nbc = b$. Since $g_1 \mid a$ and $g_1 \mid bc$, it must also be the case that $g_1 \mid b$. Then, since $g_1 \mid a$, $g_1 \leq g_2$. Therefore, $g_1 = g_2$. ▲

The Least Common Multiple

In paragraph 2.5.6, the greatest lower bound of two elements a and b in a partially ordered set $(A, \preceq)$ was defined to be an element $g = a \wedge b \in A$ with the properties

1. $g \preceq a$, $g \preceq b$, and
2. if $c \preceq a$ and $c \preceq b$ for some $c \in A$, then $c \preceq g$.

Corollary 4.2.11 therefore shows that every pair of natural numbers has a glb in the poset $(\mathbb{N}, \mid)$, that is, their greatest common divisor: For $a, b \in \mathbb{N}$,

$$a \wedge b = \gcd(a, b).$$

It is also true that every pair of natural numbers has a least upper bound.

4.2.12 DEFINITION If a and b are nonzero integers, we say that ℓ is the *least common multiple (lcm)* of a and b and write $\ell = \operatorname{lcm}(a, b)$ if and only if ℓ is a positive integer satisfying

1. $a \mid \ell$, $b \mid \ell$ and,
2. if m is any positive integer such that $a \mid m$ and $b \mid m$, then $\ell \leq m$. ❖

EXAMPLE 12

- The least common multiple of 4 and 14 is 28.
- $\operatorname{lcm}(-6, 21) = 42$.
- $\operatorname{lcm}(-5, -25) = 25$. ■

Since $|ab|$ is a common multiple of a and b, the least common multiple always exists and does not exceed $|ab|$. Remember also that a least common multiple is always positive (by definition).

In the exercises (see also Exercise 30 of Section 4.3), we ask you to derive the formula

$$\gcd(a, b) \operatorname{lcm}(a, b) = |ab|, \tag{2}$$

which holds for any nonzero integers a and b and gives a quick way of computing least common multiples.

EXAMPLE 13

- Since $\gcd(6, 21) = 3$, it follows that $\operatorname{lcm}(6, 21) = \frac{6(21)}{3} = \frac{126}{3} = 42$.
- Since $\gcd(630, -196) = 14$ (Problem 9), it follows that $\operatorname{lcm}(630, -196) = \frac{630(196)}{14} = 8820$. ■

Just as the greatest common divisor of a and b is divisible by all common divisors of a and b, we can show that the least common multiple of a and b is a divisor of all common multiples of a and b (see Exercise 29). Thus, the least common multiple of natural numbers a and b is their least upper bound in the poset $(\mathbb{N}, \mid)$ (see again paragraph 2.5.6). For $a, b \in \mathbb{N}$,

$$a \vee b = \operatorname{lcm}(a, b).$$

Remembering that a lattice is a partially ordered set in which every two elements have a greatest lower bound and a least upper bound, the following proposition is immediate.

4.2.13 PROPOSITION The poset $(\mathbb{N}, \mid)$ is a lattice.

The Lattice of Divisors of a Natural Number

Implicit in the definition of lattice is the fact that the greatest lower bound and least upper bound of every pair of elements should lie in the set. The poset $(\{2, 3, 4\}, \mid)$, for instance, is not a lattice because, while, for example, 2 and 3 have a glb in N, this element is not in $\{2, 3, 4\}$.

We have seen that $(\mathbb{N}, \mid)$ is a lattice. Also, for many subsets A of N, $(A, \mid)$ is a lattice. For example, if n is any natural number and $A = \{d \in \mathbb{N} \mid d \mid n\}$ is the set of positive divisors of n, then $(A, \mid)$ is a lattice. (See Exercise 35.)

EXAMPLE 14 With $A = \{1, 2, 3, 5, 6, 10, 15, 30\}$, the set of positive divisors of $n = 30$, $(A, \mid)$ is a lattice whose Hasse diagram is shown in Fig. 4.2. Notice that every pair of elements of A has a glb and a lub. For every pair of elements $a, b \in A$, $a \wedge b$ is the unique element below (and connected with lines to) both a and b, and $a \vee b$ is the unique element above (and connected with lines to) both a and b. ■

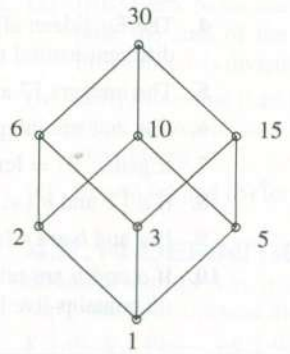
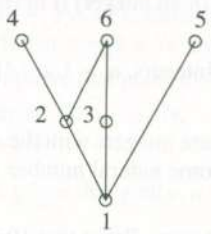


Figure 4.2 The Hasse diagram for $(A, \mid)$, where A is the set of divisors of 30. Compare with Fig. 2.4, p. 66.

Answers to Pauses



4. For any integer n, we have $0 = qn$ for the integer $q = 0$.
5. Since $1 \mid a$ for all $a \in A$, no $a \neq 1$ can be minimal. The only minimal element is 1, and it is a minimum. The elements 4, 5, and 6 are maximal. For instance, 4 is maximal because there is no $a \in A$ such that $4 \mid a$, except $a = 4$. There are no maximum elements; for example, 4 is not maximum because $a \mid 4$ for all $a \in A$ is not true.
6. The largest divisor of a is $|a|$. Since $|a|$ is a common divisor of a and b, this must be their gcd.
7. Since a is a common divisor of a and 0, the greatest common divisor of these numbers is $|a|$.

8.

17,369	1	0
5472	0	1
953	1	−3
707	−5	16
246	6	−19
215	−17	54
31	23	−73
29	−155	492
2	178	−565
1	−2647	8402

The last nonzero remainder, 1 in this case, is the gcd. So 17,369 and 5472 are relatively prime.

9. $1 = -2647(17{,}369) + 8402(5472)$.

True/False Questions

(Answers can be found in the back of the book.)

1. Given two consecutive integers a, $a+1$, one of them must be divisible by 2.
2. If a, b, c are nonzero integers such that $c \mid a$ and $c \mid b$, then $\gcd(a, b) \leq c$.
3. $\gcd(a, 1) = 1$ for any integer a.
4. The Euclidean algorithm is an algorithm that finds the greatest common divisor of two different natural numbers.
5. The integers 77 and 105 are relatively prime.
6. If a, b, c are integers such that $a \mid bc$, then either $a \mid b$ or $a \mid c$.
7. If $\gcd(a, b) = \text{lcm}(a, b)$, then $a = b$.
8. If $a \mid c$ and $b \mid c$, then $\text{lcm}(a, b) \leq c$.
9. If a and b are relatively prime natural numbers, then $\text{lcm}(a, b) = ab$.
10. If a and b are relatively prime, the Hasse diagram for the lattice of positive divisors of ab contains five lines.

Exercises

*The answers to exercises marked [BB] can be found in the **B**ack of the **B**ook.*

1. [BB] We have seen in this section that $(\mathbb{N}, \mid)$ is a partially ordered set.
   (a) Is it totally ordered?
   (b) Does it have a maximum? A minimum?
   Explain your answers.
2. Consider the partially ordered set $(\{2, 4, 6, 8\}, \mid)$.
   (a) Explain why every pair of elements in this poset has a greatest lower bound.
   (b) Does every pair of elements have a least upper bound?
   (c) Is the poset a lattice?
   Explain your answers.
3. Draw the Hasse diagrams for each of the following partially ordered sets.
   (a) [BB] $(\{2, 3, 4, 5, 6, 7\}, \mid)$
   (b) $(\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}, \mid)$
4. List all minimal, minimum, maximal, and maximum elements for each of the posets in Exercise 3.
5. [BB] Let n be a natural number. Given n consecutive integers, $a, a+1, a+2, \ldots, a+n-1$, show that one of them is divisible by n.
6. [BB] Prove that $n^2 - 2$ (n an integer) is never divisible by 4.
7. Given that a and x are integers, $a > 1$, $a \mid (11x+3)$, and $a \mid (55x+52)$, find a.
8. [BB] Suppose a and b are integers with the same remainder upon division by some natural number n. Prove that $n \mid (a-b)$.
9. [BB] Let a and b be integers. Prove that $10a+b$ is divisible by 7 if and only if $a+5b$ is divisible by 7.

10. True or false? In each case, justify your answer with a proof or a counterexample (all variables represent integers).

(a) [BB] If $a \mid b$ and $b \mid (-c)$, then $a \mid c$.

(b) If $a \mid b$ and $c \mid b$, then $ac \mid b$.

(c) If $a \mid b$ and $a \mid c$, then $a \mid bc$.

(d) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

(e) If $a \mid b$ and $c \mid \frac{b}{a}$, then $c \mid b$ and $a \mid \frac{b}{c}$.

11. Suppose a and b are relatively prime integers and c is an integer such that $a \mid c$ and $b \mid c$. Prove that $ab \mid c$.

12. In each of the following cases, find the greatest common divisor of a and b and express it in the form $ma + nb$ for suitable integers m and n.

(a) [BB] $a = 93, b = 119$

(b) [BB] $a = -93, b = 119$

(c) [BB] $a = -93, b = -119$

(d) $a = 1575, b = 231$ **(e)** $a = 1575, b = -231$

(f) $a = -1575, b = -231$ **(g)** $a = -3719, b = 8416$

(h) $a = 100{,}996, b = 20{,}048$

(i) $a = 28{,}844, b = -15{,}712$

(j) $a = 12{,}345, b = 54{,}321$

13. Which of the pairs of integers in Exercise 12 are relatively prime?

14. [BB] If a and b are relatively prime integers, prove that $\gcd(a + b, a - b) = 1$ or 2.

15. [BB] Prove that integers a and b can have at most one greatest common divisor.

16. Prove that, for integers a and b, $\gcd(a, a + b) = \gcd(a, b)$. [*Hint*: Mimic the proof of Lemma 4.2.5.]

17. **(a)** [BB] Find a pair of integers x and y such that $17{,}369x + 5472y = 4$. (See PAUSE 9.)

(b) Find integers x and y such that $154x + 260y = 4$.

(c) [BB] Show that no integers x, y satisfy $154x + 260y = 3$.

(d) Show that no integers x, y satisfy $196x + 260y = 14$.

18. **(a)** [BB] Given integers d, x and y, suppose there exist integers m and n such that $d = mx + ny$. Prove that $\gcd(x, y) \mid d$.

(b) Is the converse of (a) true? If $\gcd(x, y) \mid d$, need there exist integers m and n such that $d = mx + ny$?

19. **(a)** Exhibit integers x and y such that $7x + 5y = 3$.

(b) If $7x + 5y = 3$, show that there exists an integer k such that $y = 9 + 7k$ and $x = -6 - 5k$.

20. If $k \in \mathbb{N}$, prove that $\gcd(3k + 2, 5k + 3) = 1$.

21. [BB] Let $a, b, c \in \mathbb{N}$. Prove that $\gcd(ac, bc) = c(\gcd(a, b))$.

22. If $a \in \mathbb{N}$, prove that $\gcd(a, a+2) = \begin{cases} 1 & \text{if } a \text{ is odd} \\ 2 & \text{if } a \text{ is even.} \end{cases}$

23. [BB] Prove that $\gcd(n, n + 1) = 1$ for any $n \in \mathbb{N}$. Find integers x and y such that $nx + (n + 1)y = 1$.

24. Prove that if a, b, and c are natural numbers, $\gcd(a, c) = 1$, and $b \mid c$, then $\gcd(a, b) = 1$.

25. Let n and s be positive integers and suppose k is the least positive integer such that $n \mid ks$. Prove that $k = \frac{n}{\gcd(n, s)}$.

26. [BB] Use the Well-Ordering Principle to prove Theorem 4.2.9. [*Hint*: Consider the set of positive linear combinations of a and b.]

27. [BB] Find $\operatorname{lcm}(63, 273)$ and $\operatorname{lcm}(56, 200)$. [*Hint*: An easy method takes advantage of formula (2) of this section.]

28. [BB; (a)] Find the lcm of each of the pairs of integers given in Exercise 12.

29. Let a and b be nonzero integers with $\operatorname{lcm}(a, b) = \ell$. Let m be any common multiple of a and b. Prove that $\ell \mid m$.

30. [BB] Prove that $\gcd(a, b) \mid \operatorname{lcm}(a, b)$ for any nonzero integers a and b.

31. Establish formula (2) of this section by proving that the least common multiple of nonzero integers a and b is $\frac{|ab|}{\gcd(a, b)}$.

32. **(a)** [BB] Let x be an integer expressed in base 10. Suppose the sum of the digits of x is divisible by 3. Prove that x is divisible by 3.

(b) [BB] Prove that if an integer x is divisible by 3 then, when written in base 10, the sum of the digits of x is divisible by 3.

(c) Repeat (a) and (b) for the integer 9.

4.2.14 DEFINITION The greatest common divisor of n integers $a_1, a_2, \ldots, a_n$, not all zero, is a number g that is a common divisor of these integers (that is, $g \mid a_1, g \mid a_2, \ldots, g \mid a_n$) and that is the largest of all such common divisors (that is, if $c \mid a_1, c \mid a_2, \ldots, c \mid a_n$, then $c \leq g$). It is denoted $\gcd(a_1, \ldots, a_n)$. ❖

33. **(a)** Suppose a, b, c are nonzero integers. Show that $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$.

(b) Show that the gcd of nonzero integers a, b, c is an integral linear combination of them.

(c) Find $\gcd(105, 231, 165)$ and express this as an integral linear combination of the given three integers.

(d) Answer (c) for the integers 6279, 8580, and 2873.

(e) Answer (c) for the integers 5577, 18,837, and 25,740.

34. Suppose that $(A_1, \preceq_1)$ and $(A_2, \preceq_2)$ are partial orders.

(a) Show that the definition

$$(x_1, x_2) \preceq (y_1, y_2)$$
if and only if $x_1 \preceq_1 y_1$ and $x_2 \preceq_2 y_2$

for $(x_1, x_2), (y_1, y_2) \in A_1 \times A_2$ makes $A_1 \times A_2$ a partially ordered set.

(b) Let $A_1 = A_2 = \{2, 3, 4\}$. Assign to A_1 the partial order $\leq$ and to A_2 the partial order $|$. Partially order $A_1 \times A_2$ as in part (a). Show all relationships of the form $(x_1, x_2) \precneqq (y_1, y_2)$.

(c) Draw the Hasse diagram for the partial order in (b).

(d) Find any maximal, minimal, maximum, and minimum elements that may exist in the partial order of (b).

(e) With A_1 and A_2 as in part (b), find the glbs and lubs that exist for each of the following pairs of elements.

i. $(2, 2), (3, 3)$ ii. $(4, 2), (3, 4)$
iii. $(3, 2), (2, 4)$ iv. $(3, 2), (3, 4)$

(f) Show, by example, that if $(A_1, \preceq_1)$ and $(A_2, \preceq_2)$ are total orders then $(A_1 \times A_2, \preceq)$ need not be a total order.

35. (a) Let n be a natural number, $n > 1$. Let $A = \{a \in \mathbb{N} \mid a \mid n\}$. Prove that $(A, |)$ is a lattice.

(b) [BB] Draw the Hasse diagram associated with the poset given in (a) for $n = 12$.

(c) Draw the Hasse diagram associated with the poset given in (a) for $n = 36$.

(d) Draw the Hasse diagram associated with the poset given in (a) for $n = 90$.

36. (a) [BB] Let g be the greatest common divisor of integers m and n, not both 0. Show that there are infinitely many pairs a, b of integers such that $g = am + bn$.

(b) Suppose m and n are relatively prime integers each greater than 1.

i. Show that there exist unique integers a, b with $0 < b < m$ such that $am + bn = 1$.

ii. Show that there exist unique integers a, b with $0 < a < n$ and $0 < b < m$ such that $am = bn + 1$.

4.3 Prime Numbers

In Section 4.2, we saw what it means to say that one integer "divides" another. The basic building blocks of divisibility are the famous prime numbers. We examine some of the properties of prime numbers in this section.

4.3.1 DEFINITION

A natural number $p \geq 2$ is called *prime* if and only if the only natural numbers that divide p are 1 and p. A natural number $n > 1$ that is not prime is called *composite*. Thus, $n > 1$ is composite if $n = ab$, where a and b are natural numbers with $1 < a, b < n$. ❖

Table 4.3 The primes less than 100.

2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

The integers 2, 3, and 5 are primes while 4, 6, and 10 are composite. The natural number 1 is neither prime nor composite. It is interesting to note that exactly one-quarter of the numbers between 1 and 100 (inclusive) are prime. These primes are shown in Table 4.3.

You may have needed more than a few seconds to verify that some of the entries in Table 4.3 are, in fact, prime. Such verification gets increasingly more difficult as the numbers get bigger. One of the great challenges of mathematics and an active area of research today is that of finding efficient algorithms for checking whether large integers are primes. By the end of 1988, the largest known prime number was $2^{216,091} - 1$. This was discovered in 1985 by computer scientists working at Geosciences Corporation, Houston, who required just three hours on a Cray X-MP computer to verify that this number was, indeed, prime. Not everyone was impressed. A vice president of Chevron Oil was apparently quoted as saying, "The results are interesting, if true, but they are certainly not going to help me find oil."

The discovery of new primes is viewed as both a test of humankind's ingenuity and the reliability of new computers, so, when a new prime is discovered, it is widely publicized. Early in 1992, David Slowinski and Paul Gage of Cray Research, Inc., announced that $2^{756,839} - 1$ is prime. Then in 1994 the same people announced the primality of $2^{859,433} - 1$, a number with a mere 258,716 digits. On November 13, 1996, Joel Armengaud, a 29-year-old computer programmer working in France, discovered that $2^{1,398,269} - 1$ is prime. A year later, Gordon Spence of Hampshire, England, with a Pentium PC running a program downloaded over the World Wide

Web,[2] found that $2^{2,976,221} - 1$ is prime. This number, with 895,932 digits, would fill a 450-page book all by itself! New primes are currently being discovered at such a rate that it is difficult for the authors of textbooks to keep pace.

As this book goes to press, the world's largest prime is $2^{24,036,583} - 1$, a number with 7,235,733 decimal digits. This was discovered on May 15, 2004, by Josh Findley after two weeks of calculation on a 2.4-GHz Pentium 4 computer.[3] Now the search continues for a prime still bigger, a process that will never end because it has been known since the time of Euclid that the number of primes is infinite. To prove this fact, we first need a short lemma.

4.3.2 LEMMA Given any natural number $n > 1$, there exists a prime p such that $p \mid n$.

Proof We give a proof by contradiction. Thus, we suppose the lemma is false. In this case, the set of natural numbers greater than 1 that are not divisible by any prime is not empty. By the Well-Ordering Principle, the set contains a smallest element m. Since $m \mid m$, but m is not divisible by any prime, m itself cannot be prime, so m is divisible by some natural number a, with $1 < a < m$. By minimality of m, a must be divisible by a prime p. Since $p \mid a$ and $a \mid m$, we have $p \mid m$, a contradiction. ●

Now we can easily show that there is an infinite number of primes. The wonderfully simple argument we present has been known since 300 B.C. and is commonly attributed to Euclid since it appears in Euclid's *Elements*. It is a model of a proof by contradiction.

4.3.3 THEOREM There are infinitely many primes.

Proof If the theorem is not true, there is just a finite number of primes $p_1, p_2, \ldots, p_t$. Let $n = (p_1 p_2 \cdots p_t) + 1$. By Lemma 4.3.2, n is divisible by some prime and hence by some p_i. Since $p_1 p_2 \cdots p_t$ is also divisible by p_i, the number $n - (p_1 p_2 \cdots p_t)$ must also be divisible by p_i. Thus, 1 is divisible by p_i, a contradiction. ●

Pause 10 Although the number of primes is infinite, the number of natural numbers that are not prime is infinite too. Find an easy way to see this. ▮

We now return to the question of determining whether a given integer is prime. Several elementary observations can be made at the outset. Any even integer is divisible by 2 and so is not prime (unless it equals 2). Similarly, any integer larger than 5 whose units digit is 0 or 5 is divisible by 5 and hence not prime. If n is not prime, Lemma 4.3.2 tells us that n is divisible by some prime. So, to verify that n is not prime, it is enough just to test the **prime** numbers less than n (rather than **all** numbers less than n) when searching for a divisor of n.

Here is another fact that decreases considerably the amount of testing that must be done when checking for divisors of an integer.

4.3.4 LEMMA If a natural number $n > 1$ is not prime, then n is divisible by some prime number $p \leq \sqrt{n}$.

[2]The World Wide Web is full of information about large primes. For instance, there is lots of up-to-the-minute news in "The Prime Pages:" **www.utm.edu/research/primes/**.

[3]For more information about the exciting projects that lead to the discovery of enormous prime numbers visit **www.mersenne.org**.

Proof Since n is not prime, n can be factored $n = ab$ with $1 < a \leq b < n$. Then $a \leq \sqrt{n}$ since otherwise, $ab > \sqrt{n}\sqrt{n} = n$, a contradiction. As a natural number greater than 1, it follows that a is divisible by some prime p. Since $p \mid a$ and $a \mid n$, $p \mid n$ by transitivity. Also, since $a \leq \sqrt{n}$ and $p \mid a$, we must have $p \leq \sqrt{n}$. Thus, p is the desired prime factor of n. ●

As a consequence of Lemma 4.3.4, when testing a natural number n for primality, we need only consider the possibility of a prime divisor less than or equal to the square root of n. For example, to verify that 97 is prime, we need only check the prime numbers less than or equal to $\sqrt{97}$. Since none of 2, 3, 5, 7 is a divisor of 97, we are assured that 97 is a prime number. It is apparent that Lemma 4.3.4 reduces dramatically the work involved in a primality check.

One simple procedure that goes back over 2000 years for finding all the primes less than or equal to some given integer is named after the Greek Eratosthenes (ca. 200 B.C.), chief librarian of the great library at Alexandria and a contemporary of Archimedes. Reportedly, Eratosthenes was the first person to estimate the circumference of the earth.

Pause 11 Who was Archimedes? ▮

4.3.5 THE SIEVE OF ERATOSTHENES

To find all the prime numbers less than or equal to a given natural number n,

- list all the integers from 2 to n,
- circle 2 and then cross out all multiples of 2 in the list,
- circle 3, the first number not yet crossed out or circled, and then cross out all multiples of 3,
- circle 5, the first number not yet crossed out or circled, and cross out all multiples of 5,
- at the general stage, circle the first number that is neither crossed out nor circled and cross out all its multiples,
- continue until all numbers less than or equal to $\sqrt{n}$ have been circled or crossed out.

When the procedure is finished, those integers not crossed out are the primes not exceeding n.

EXAMPLE 15 As an example of this procedure, we verify that the list of primes $p < 100$ given in Table 4.3 is correct. All the integers from 2 to 100 are listed in Fig. 4.4. Initially, 2 was circled and then all even integers were crossed out with a single stroke. At the second stage, 3 was circled and all multiples of 3 not yet crossed out were crossed out with two strokes. Then 5 was circled and all multiples of 5 not yet crossed out were crossed out with three strokes. Finally, 7 was circled and all multiples of 7 not previously crossed out were crossed out with four strokes. The primes less than 100 are those not crossed out. ■

The prime numbers are considered building blocks because of the following important theorem, which generalizes observations such as $8 = 2 \cdot 2 \cdot 2$, $15 = 3 \cdot 5$ and $60 = 2 \cdot 2 \cdot 3 \cdot 5$.

4.3.6 THEOREM Every natural number $n \geq 2$ can be written $n = p_1 p_2 \cdots p_r$ as the product of prime numbers $p_1, p_2, \ldots, p_r$ or, by grouping equal primes, in the form $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s}$ as the product of powers of distinct primes $q_1, q_2, \ldots, q_s$.

Proof If the result is false, then the set of integers $n \geq 2$ that cannot be written as the

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~~	

Figure 4.4 The Sieve of Eratosthenes used to determine the primes $p \leq 100$.

product of primes is not empty and so, by the Well-Ordering Principle, contains a smallest element m. This number cannot be prime, so $m = ab$ with $1 < a, b < m$. By minimality of m, each of a and b is the product of primes, hence so is m, a contradiction. ●

EXAMPLE 16

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$
$1176 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7 = 2^3 \cdot 3 \cdot 7^2$
$21340 = 2 \cdot 2 \cdot 5 \cdot 11 \cdot 97 = 2^2 \cdot 5 \cdot 11 \cdot 97.$ ■

Theorem 4.3.6 can be strengthened. There is, in fact, just one way to express a natural number as the product of primes, but to prove this, we need a preliminary result that is a special case of something we proved earlier (see Corollary 4.2.10). Notice that $3 \mid 12$ and, regardless of how 12 is factored, $12 = 2(6) = 3(4)$, 3 always divides one of the factors. The next proposition describes the most important property of a prime number.

4.3.7 PROPOSITION Suppose a and b are integers and p is a prime such that $p \mid ab$. Then $p \mid a$ or $p \mid b$.

This indeed follows from Corollary 4.2.10 because, if $p \nmid a$, then p and a are relatively prime.

Now suppose a prime p divides the product $a_1 a_2 \cdots a_k$ of k integers. By Proposition 4.3.7, $p \mid a_1$ or $p \mid a_2 \cdots a_k$. In the latter case, applying the proposition again, we see that $p \mid a_2$ or $p \mid a_3 \cdots a_k$. In this way, we obtain the following corollary.

4.3.8 COROLLARY If a prime p divides the product $a_1 a_2 \cdots a_k$ of integers, then p divides one of the a_i.

Now to prove that a natural number $n > 1$ can be factored in just one way as the product of primes, assume that n can be factored in two different ways:

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell \tag{3}$$

with all the p_i and q_j primes. After canceling equal factors on each side of this equation, we either have an equation that says that the product of certain primes is 1 (an absurdity) or another equation like (3), where none of the primes p_i is among the primes q_j. Then, since $p_1 \mid p_1 p_2 \cdots p_k$, it would follow that $p_1 \mid q_1 q_2 \cdots q_\ell$. By Corollary 4.3.8, $p_1 \mid q_j$ for one of the primes q_j. Since both p_1 and q_j are primes, this forces $p_1 = q_j$, a contradiction.

The fact that every integer $n > 1$ can be written uniquely as the product of prime numbers is called the Fundamental Theorem of Arithmetic. Because of its importance, we state it again.

4.3.9 THE FUNDAMENTAL THEOREM OF ARITHMETIC

Every integer $n \geq 2$ can be written in the form

$$n = p_1 p_2 \cdots p_r \tag{4}$$

for a unique set of primes $\{p_1, p_2, \ldots, p_r\}$; equivalently, every integer $n \geq 2$ can be written

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s} \tag{5}$$

(the *prime decomposition* of n)

as the product of powers of distinct prime numbers $q_1, q_2, \ldots, q_s$. These primes and the exponents $\alpha_1, \alpha_2, \ldots, \alpha_s$ are unique.

As noted, the decomposition in (5) is called the *prime decomposition* of n. For example, the prime decomposition of 120 is $2^3 \cdot 3 \cdot 5$.

4.3.10 DEFINITION

The *prime factors* or *prime divisors* of an integer $n \geq 2$ are the prime numbers that divide n. The *multiplicity* of a prime divisor p of n is the largest number α such that $p^\alpha \mid n$. ❖

Thus, the prime factors of an integer n are the primes p_i or q_i given in (4) and (5) and the multiplicities of $q_1, \ldots, q_s$ are the exponents $\alpha_1, \ldots, \alpha_s$, respectively. The prime factors of 14 are 2 and 7 and each has multiplicity 1. The prime factors of 120 are 2, 3, and 5; 2 has multiplicity 3, while 3 and 5 each have multiplicity 1.

PROBLEM 17. Find the prime decomposition of the greatest common divisor of nonzero integers a and b.

Solution. By the Fundamental Theorem of Arithmetic, a and b can be expressed in the form

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

for certain primes $p_1, p_2, \ldots, p_r$ and integers $\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_r$. (By allowing the possibility that some of the α_i or β_i are 0, we can assume that the same r primes occur in the decompositions of both a and b.) We claim that the greatest common divisor of a and b is

$$g = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_r^{\min(\alpha_r, \beta_r)},$$

where $\min(\alpha_i, \beta_i)$ denotes the smaller of the two nonnegative integers α_i and β_i.

Note that $g \mid a$ since the exponent $\min(\alpha_i, \beta_i)$ does not exceed α_i, the exponent of the prime p_i in a. Similarly, $g \mid b$. Next, assume that $c \mid a$ and $c \mid b$. Since any prime that divides c also divides a and b, the only primes dividing c must be among $p_1, p_2, \ldots, p_r$. Thus, $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$ for some integers γ_i. Since $c \mid a$, however, we must have $\gamma_i \leq \alpha_i$ for each i and, similarly, $\gamma_i \leq \beta_i$ for each i because $c \mid b$. Hence, $\gamma_i \leq \min(\alpha_i, \beta_i)$ for each i, so $c \mid g$ and the result follows. ▲

Prime numbers have held a special fascination for humankind ever since the Greeks realized there were infinitely many of them. They are so familiar, yet there are many questions concerning them that are easy to state but hard to answer. Many remain unsolved today. In the rest of this section, we briefly survey some of what is known and some of what is unknown about primes, but few details and no proofs

will be given. For more information, the interested reader might consult Silverman's book,[4] for example.

Mersenne Primes

While it is very difficult to determine whether a given large integer is prime, the problem may be easier for special classes of integers. For example, integers of the form $7n$, $n \in \mathbb{N}$, are never prime if $n > 1$ since they are obviously divisible by 7. What about integers of the form $n^2 - 1$? Well, since $n^2 - 1 = (n-1)(n+1)$, these cannot be prime either as long as $n > 2$. Father Marin Mersenne (1588–1648) was interested in integers of the form $2^n - 1$. He showed that these could only be prime if n itself was prime. (See Exercise 18.) Then he noted that it wasn't sufficient just for n to be prime since $2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime. He conjectured that $2^p - 1$ is prime if p is any of the primes 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 and composite for the other primes $p \leq 257$. Unfortunately, he was wrong on several counts. For example, $2^{61} - 1$ is prime while $2^{257} - 1$ is not. (Resist the urge to factor!) In Mersenne's honor, primes of the form $2^p - 1$ are called *Mersenne primes*. Interestingly, all the large primes that have been discovered in recent years have been primes of this form. Late in 2001, the 39th Mersenne prime was discovered by Michael Cameron, a 20-year-old Canadian working on one of over 200,000 networked PCs that had been systematically checking increasingly larger numbers of the form $2^p - 1$ to see if they might be prime. Cameron's prime, with $p = 13466917$, is a number with 4,053,946 digits. It was found after two and a half years of testing 100,000 other similar candidates. Will more Mersenne primes be discovered in the future? Nobody really knows.

4.3.11 OPEN PROBLEM Are there infinitely many Mersenne primes?

Fermat Primes

Another interesting class of prime numbers is the set of *Fermat primes*, these being prime numbers of the form $2^{2^n} + 1$. For $n = 0, 1, 2, 3, 4$, indeed $2^{2^n} + 1$ is prime and it was a guess of the seventeenth-century lawyer Pierre de Fermat (1601–1665), perhaps the most famous amateur mathematician of all time, that $2^{2^n} + 1$ is prime for all $n \geq 0$. In 1732, however, the great Swiss mathematician Léonhard Euler (1707–1783) showed that $2^{2^5} + 1$ is not prime (it is divisible by 641) and, to this day, no further Fermat primes have been discovered.

When a Cray supercomputer tires of hunting for Mersenne primes, it turns to a search for Fermat primes! In a number of cases, complete factorizations of $2^{2^n} + 1$ are known; in other cases, one or two prime factors are known. There are Fermat *numbers*, of the form $2^{2n} + 1$, known to be composite, though no one knows a single factor! As of 1995, the smallest Fermat number whose primality was unsettled was $2^{2^{24}} + 1$. More details, together with an indication as to how testing huge numbers for primality is used to check the reliability of some of the world's largest computers, can be found in an article by Jeff Young and Duncan A. Buell.[5]

Pause 12 What are the first five Fermat primes? ∎

4.3.12 OPEN PROBLEM Are there more than five Fermat primes?

[4] Joseph H. Silverman, *A Friendly Introduction to Number Theory*, 2nd ed. (Prentice Hall, 2001).
[5] "The Twentieth Fermat Number Is Composite," *Mathematics of Computation* **50** (1988), 261–263.

How Many Primes Are There?

We have discussed Euclid's observation that there are infinitely many primes (Theorem 4.3.3), so what does the question just posed really mean?

There is great interest in the proportion of natural numbers that are prime. Students who have enjoyed advanced calculus will know that the series

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots$$

diverges (the partial sums increase without bound as more and more terms are added), while the series

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots$$

converges (to $\frac{\pi^2}{6}$ in fact).[6] Notice that the second sum here is part of the first. So the fact that the second sum is finite while the first is infinite shows that the sequence of perfect squares $1^2, 2^2, 3^2, \ldots$ forms only a tiny part of the sequence of all natural numbers $1, 2, 3, \ldots$.

Which of these sequences does the set of primes most resemble? Does the sum of reciprocals of the primes

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\cdots$$

converge or diverge? As a matter of fact, it diverges, so, in some sense, there really are a "lot" of prime numbers, many more than there are perfect squares, for example.

A sophisticated result concerning the number of primes is the important Prime Number Theorem, which was proved independently by Jacques Hadamard and Charles-Jean de la Vallée-Pousin in 1896. It gives an approximation to the function $\pi(x)$, which is the number of primes $p \le x$. For example, $\pi(5) = 3$ since there are three primes $p \le 5$. We have earlier noted that there are 25 primes $p \le 100$; thus, $\pi(100) = 25$.

4.3.13 PRIME NUMBER THEOREM

Let $\pi(x)$ denote the number of primes $p \le x$. Then

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1; \quad \text{equivalently,} \quad \pi(x) \sim \frac{x}{\ln x}.$$

Students uncertain about limits might wish a translation! First, we say "is asymptotic to" for $\sim$. So the second statement of the theorem reads "$\pi(x)$ is asymptotic to $\frac{x}{\ln x}$," from which we infer that $\pi(x)$ is approximately equal to $\frac{x}{\ln x}$ for large x, the approximation getting better and better as x grows. Setting $x = 100$, Theorem 4.3.13 asserts that the number of primes $p \le 100$ is roughly $\frac{100}{\ln 100} \approx 21.715$. Note that

$$\frac{\pi(100)}{100/\ln 100} \approx \frac{25}{21.715} \approx 1.151.$$

(The symbol $\approx$ means "approximately.") Setting $x = 1{,}000{,}000$, the theorem says that the number of primes under 1 million is roughly $\frac{1{,}000{,}000}{\ln 1{,}000{,}000} \approx 72{,}382$. In fact, there are 78,498 such primes. Note that

$$\frac{\pi(1{,}000{,}000)}{1{,}000{,}000/\ln 1{,}000{,}000} \approx \frac{78{,}498}{72{,}382} \approx 1.084.$$

As x gets larger, the fraction $\frac{\pi(x)}{x/\ln x}$ gets closer and closer to 1.

[6] The reader who has not studied advanced calculus can relax! The ideas to which we make reference here are not critical to an overall appreciation of the mysteries of the primes.

On June 23, 1993, at a meeting at the Isaac Newton Institute in Cambridge, England, Andrew Wiles of Princeton University announced a proof of Fermat's Last Theorem, arguably the most famous open mathematics problem of all time.

4.3.14 FERMAT'S LAST THEOREM

For any integer $n > 2$, the equation $a^n + b^n = c^n$ has no nonzero integer solutions a, b, c.

Notice that it is sufficient to prove this theorem just for the case that n is a prime. For example, if we knew that $a^3 + b^3 = c^3$ had no integral solutions, then neither would $A^{3n} + B^{3n} = C^{3n}$. If the latter had a solution, so would the former, with $a = A^n, b = B^n, c = C^n$.

When we first learned the Theorem of Pythagoras for right-angled triangles, we discovered that there are many triples a, b, c of integers that satisfy $a^2 + b^2 = c^2$; for example, 3, 4, 5 and 5, 12, 13. But are there triples of integers a, b, c satisfying $a^3 + b^3 = c^3$ or $a^7 + b^7 = c^7$ or $a^n + b^n = c^n$ for any values of n except $n = 2$?

Pierre de Fermat was notorious for scribbling ideas in the margins of whatever he was reading. In 1637, he wrote in the margin of Diophantus's book *Arithmetic* that he had found a "truly wonderful" proof that $a^n + b^n = c^n$ had no solutions in the positive integers for $n > 2$, but that there was insufficient space to write it down. Truly wonderful it must have been, because for over 350 years, mathematicians were unable to find a proof, though countless many tried!

Amateur and professional mathematicians alike devoted years and even lifetimes to working on Fermat's Last Theorem. The theorem owes its name, by the way, to the fact that it is the last of the many conjectures made by Fermat during his lifetime to have resisted resolution. By now, most of Fermat's unproven suggested theorems have been settled (and found to be true).

In 1983, Gerd Faltings proved that, for each $n > 2$, the equation $a^n + b^n = c^n$ could have at most a finite number of solutions. While this was a remarkable achievement, it was a long way from showing that this finite number was zero. Then, in 1985, Kenneth Ribet of Berkeley showed that Fermat's Last Theorem was a consequence of a conjecture first proposed by Yutaka Taniyama in 1955 and clarified by Goro Shimura in the 1960s. It was a proof of the Shimura-Taniyama conjecture that Andrew Wiles announced on June 23, 1993, a truly historic day in the world of mathematics. The months following this announcement were extremely exciting as mathematicians all over the world attempted to understand Wiles's proof. Not unexpectedly, in such a complex and lengthy argument, a few flaws were found. By the end of 1994, however, Wiles and one of his former graduate students, Richard Taylor, had resolved the remaining issues to the satisfaction of all.

Among the many exciting accounts of the history of Fermat's Last Theorem and of Wiles's work, we draw special attention to an article by Barry Cipra, "Fermat's Theorem—at Last!", which was the leading article in *What's Happening in the Mathematical Sciences*, Vol. **3** (1995–1996), published by the American Mathematical Society. Faltings himself wrote "The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles" for the *Notices of the American Mathematical Society*, Vol. 42 (1995), No. 7. In fact, many excellent accounts have been written. There is one entitled "The Marvelous Proof" by Fernando Q. Gouvêa, which appeared in the *American Mathematical Monthly*, Vol. 101 (1994), and others by Ram Murty, *Notes of the Canadian Mathematical Society*, Vol. 25 (September 1993) and by Keith Devlin, Fernando Gouvêa, and Andrew Granville, *Focus*, Vol. 13, Mathematical Association of America (August 1993).

Pause 13 Show that $\sqrt[n]{2}$ is irrational for $n \geq 3$.[7] ∎

More Open Problems

So far, we have only peeked into the Pandora's box of fascinating but unanswered problems concerning prime numbers. Here are a few more.

There are intriguing questions concerning prime *gaps*, the distances between consecutive primes. On the one hand, there are arbitrarily long gaps in the list of primes. One way to see this is to observe that, if the first $n+1$ primes are p_1, p_2, $\ldots$, p_{n+1}, then all the numbers between $p_1 p_2 \cdots p_n + 2$ and $p_1 p_2 \cdots p_n + p_{n+1} - 1$ are composite. (See Exercise 27.) On the other hand, there are also very small gaps in the primes, for example, gaps of length 2 such as between 3 and 5 or 11 and 13.

Integers p and $p+2$ that are both prime are called *twin primes*. For example, 3 and 5, 5 and 7, 11 and 13, 41 and 43 are twin primes. So are $4{,}648{,}619{,}711{,}505 \times 2^{60{,}000} \pm 1$, a 1999 discovery of Heinz-Georg Wassing, Antal Jarai, and Karl-Heinz Indlekofer. As of mid-2000, these numbers, each with 18,075 digits, remained the largest known pair of twin primes. It is possible, though not likely, that there are no more. Unlike prime numbers, it is not known whether there are infinitely many twin primes. One tantalizing result, proved by Viggo Brun in 1921 using a variation of the Sieve of Eratosthenes, is that the sum of the reciprocals of just the twin primes converges. Having noted that the sum of the reciprocals of all the primes diverges, Brun's result is evidence that the number of twin primes is "small." On the other hand, there are 224,376,048 twin prime pairs less than 100 billion, and this seems like a pretty big number. Is the total number finite? No one knows.

4.3.15 THE TWIN PRIME CONJECTURE

There are infinitely many twin primes.

Observe that $4 = 2+2$, $6 = 3+3$, $8 = 5+3$, $28 = 17+11$, and $96 = 43+53$. Every even integer **appears** to be the sum of two primes. Is this really right? The conjecture that it is, first made by Christian Goldbach in 1742 in a letter to Euler, has proved remarkably resistant to solution. In 1937, I. M. Vinogradov showed that every sufficiently large integer can be written as the sum of at most **four** primes. *Sufficiently large* means that there is a positive integer n_0 such that every integer larger than n_0 satisfies the condition. In 1966, J. Chen showed that every sufficiently large **even** integer can be written as $x + y$, where x is prime and y is either prime or the product of two primes. So we seem to be close to a solution of Goldbach's conjecture, though the last step is often the hardest.

4.3.16 THE GOLDBACH CONJECTURE

Every even integer greater than 2 is the sum of two primes.

Answers to Pauses

10. For instance, numbers of the form $7n$, $n \in \mathbb{N}$, $n > 1$, are not prime, and there are infinitely many of these.

11. Archimedes was a Greek scientist of the third century B.C. perhaps best known for the Principle of Archimedes. This states that the weight of the fluid displaced by a floating object is equal to the weight of the object itself.

12. The first five Fermat primes are $2^{(2^0)} + 1 = 2^1 + 1 = 3$, $2^{(2^1)} + 1 = 2^2 + 1 = 5$, $2^{(2^2)} + 1 = 2^4 + 1 = 17$, $2^{(2^3)} + 1 = 2^8 + 1 = 257$, and $2^{(2^4)} + 1 = 2^{16} + 1 = 65{,}537$.

[7] In the *American Mathematical Monthly* **110** (2003), no. 5, p. 423, this problem is credited to William Henry Schultz, then an undergraduate at the University of North Carolina at Charlotte.

13. If $\sqrt[n]{2}$ were rational, there would exist positive integers a and b such that $\sqrt[n]{2} = \frac{a}{b}$. Thus $a = b\sqrt[n]{2}$, so $a^n = 2b^n = b^n + b^n$, contradicting Fermat's Last Theorem!

True/False Questions

(Answers can be found in the back of the book.)

1. 127 is a prime number.

2. 1 is a prime number.

3. The Sieve of Archimedes is a method of determining all primes less than or equal to a given natural number n.

4. Every natural number $n \geq 2$ can be written $n = p_1 p_2 \cdots p_r$ as the product of distinct prime numbers $p_1, p_2, \ldots, p_r$.

5. If a is divisible by at most three distinct primes and b is divisible by four distinct primes, then $\gcd(a, b)$ is divisible by at most three distinct primes.

6. If a is divisible by at most three distinct primes and b is divisible by four distinct primes, then $\text{lcm}(a, b)$ is divisible by at most four distinct primes.

7. $15 = 2^4 - 1$ is a Mersenne prime.

8. $17 = 2^4 + 1$ is a Fermat prime.

9. Fermat's Last Theorem is still an open problem.

10. The Goldbach Conjecture is still an open problem.

Exercises

The answers to exercises marked [BB] can be found in the ***B****ack of the* ***B****ook.*

1. Determine whether each of the following integers is a prime.

(a) [BB] 157 **(b)** [BB] 9831

(c) 9833 **(d)** 55,551,111

(e) $2^{216,090} - 1$

2. Can Lemma 4.3.4 be strengthened? In other words, does there exist a number $r < \sqrt{n}$ such that if n is not prime then n has a prime factor $p \leq r$?

3. **(a)** [BB] Suppose p is the smallest prime factor of an integer n and $p > \sqrt{n/p}$. Prove that n/p is prime.

(b) [BB] Express 16,773,121 as the product of primes given that 433 is this number's smallest prime factor.

4. Find the prime decomposition of each of the following natural numbers.

(a) [BB] 856 **(b)** 2323

(c) 6647 **(d)** 9970

(e) [BB] $(2^8 - 1)^{20}$ **(f)** 55,551,111

5. [BB] Use the Fundamental Theorem of Arithmetic to prove that for no natural number n does the integer 14^n terminate in 0.

6. Let $A = \{\frac{m}{n} \in \mathbb{Q} \mid 3 \nmid n\}$.

(a) List five different elements of A at most one of which is an integer.

(b) [BB] Prove that A is closed under addition.

(c) Prove that A is closed under multiplication.

7. Let A be any subset of $\mathbb{Z} \setminus \{0\}$ and, for $a, b \in A$, define $a \sim b$ if ab is a *perfect square* (that is, $ab = x^2$ for some integer x). Show that $\sim$ defines an equivalence relation on A.

8. True or false? Explain your answers.

(a) For all $n \in \mathbb{N}$, $n > 1$, there exists a prime p such that $p \mid n$.

(b) [BB] There exists a prime p such that $p \mid n$ for all $n \in \mathbb{N}, n > 1$.

(The position of the universal quantifier makes a world of difference!)

9. Define $f: \mathbb{N} \setminus \{1\} \to \mathbb{N}$ by setting $f(n)$ equal to the largest prime divisor of n.

(a) Find the range of f.

(b) Is f one-to-one?

(c) Is f onto?

(d) Why did we not express f as a function $\mathbb{N} \to \mathbb{N}$? Explain your answers.

10. Determine whether each of the following functions $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is one-to-one. Explain your answers.

(a) [BB] $f(n, m) = 2^m 6^n$ **(b)** $f(n, m) = 36^m 6^n$

11. **(a)** [BB] Find $\pi(10)$ and approximate values of $10/\ln 10$ and $\frac{\pi(10)}{10/\ln 10}$ (three decimal place accuracy).

(b) Find $\pi(50)$ and approximate values of $50/\ln 50$ and $\frac{\pi(50)}{50/\ln 50}$.

(c) Find $\pi(95)$ and approximate values of $95/\ln 95$ and $\frac{\pi(95)}{95/\ln 95}$.

12. **(a)** Use the Sieve of Eratosthenes to list all the primes less than 200. Find $\pi(200)$ and the values of $200/\ln 200$ and $\frac{\pi(200)}{200/\ln 200}$ (to three decimal places).

(b) Use the Sieve of Eratosthenes to list all the primes less than 500. Find $\pi(500)$ and the values of $500/\ln 500$ and $\frac{\pi(500)}{500/\ln 500}$ (to three decimal places).

13. Estimate the number of primes less than 5000, less than 50,000, less than 500,000, and less than 5,000,000.

14. [BB] Let p and q be distinct primes and n a natural number. If $p \mid n$ and $q \mid n$, why must pq divide n?

15. Suppose $2x_0 + 5y_0 = 19 = 2x + 5y$ for certain integers x_0, y_0, x, y.

(a) Show that there exists an integer k such that $x = x_0 + 5k$ and $y = y_0 - 2k$.

(b) If $2x + 5y = 19$, show that there exists an integer k such that $x = 2 + 5k$ and $y = 3 - 2k$.

16. [BB] Given distinct positive integers a and b, show that there exists an integer $n \geq 0$ such that $a + n$ and $b + n$ are relatively prime.

17. For any natural number n, let $d(n)$ denote the number of positive divisors of n. For example, $d(4) = 3$ because 4 has three positive divisors: 1, 2, and 4.

(a) Describe those natural numbers n for which $d(n) = 2$.

(b) [BB] Describe those natural numbers n for which $d(n) = 3$.

(c) Describe those natural numbers n for which $d(n) = 5$.

18. **(a)** [BB] Is $2^{15} - 1$ prime? Explain your answer.

(b) Is $2^{91} - 1$ prime? Explain your answer.

(c) Show that if $2^n - 1$ is prime then necessarily n is prime.

(d) Is the converse of (c) true? (If n is prime, need $2^n - 1$ be prime?)

19. **(a)** [BB] Show that $2^6 + 1$ is not prime.

(b) Show that $2^{20} + 1$ is not prime.

(c) Show that if $2^n + 1$ is prime then necessarily n is a power of 2.

20. **(a)** Show that the sum of two odd prime numbers is never prime.

(b) Is (a) true if the word odd is deleted?

21. [BB] Show that the sum of two consecutive primes is never twice a prime.

22. If n is an odd integer, show that $x^2 - y^2 = 2n$ has no integer solutions.

23. [BB] True or false: $\{n \in \mathbb{N} \mid n > 2 \text{ and } a^n + b^n = c^n \text{ for some } a, b, c \in \mathbb{N}\} = \emptyset$?

24. [BB] Suppose that a, b, and c are integers each two of which are relatively prime. Prove that $\gcd(ab, bc, ac) = 1$.

25. Let a, b, and c be integers each relatively prime to another integer n. Prove that the product abc is relatively prime to n.

26. Given that p is prime, $\gcd(a, p^2) = p$ and $\gcd(b, p^3) = p^2$, find

(a) [BB] $\gcd(ab, p^4)$ **(b)** $\gcd(a + b, p^4)$

27. Let $p_1, p_2, \ldots, p_{n+1}$ denote the first $n + 1$ primes (in order). Prove that every number between $p_1 p_2 \cdots p_n + 2$ and $p_1 p_2 \cdots p_n + p_{n+1} - 1$ (inclusive) is composite. How does this show that there are gaps of arbitrary length in the sequence of primes?

28. If the greatest common divisor of integers a and b is the prime p, what are the possible values of

(a) [BB] $\gcd(a^2, b)$?

(b) $\gcd(a^3, b)$?

(c) $\gcd(a^2, b^3)$?

29. [BB] Let a and b be natural numbers with $\gcd(a, b) = 1$ and ab a perfect square. Prove that a and b are also perfect squares.

30. Let a and b be natural numbers.

(a) Find the prime decomposition of $\text{lcm}(a, b)$ in terms of the prime decompositions of a and b and prove your answer. (See Problem 17, p. 118.)

(b) Use (a) to prove formula (2) of Section 4.2 in the case $a, b > 0$: $\gcd(a, b)\,\text{lcm}(a, b) = ab$.

31. [BB] Prove that an integer that is both a square (a^2 for some a) and a cube (b^3 for some b) is also a sixth power.

32. Let a and b be integers. Let p be a prime. Answer true or false and explain:

(a) [BB] If $p \mid a^{11}$, then $p \mid a$.

(b) If $p \mid a$ and $p \mid (a^2 + b^2)$, then $p \mid b$.

(c) If $p \mid (a^9 + a^{17})$, then $p \mid a$.

33. [BB] Show that there are infinitely many triples of integers a, b, c that satisfy $a^2 + b^2 = c^2$.

34. **(a)** [BB] Prove that every odd positive integer of the form $3n + 2$, $n \in \mathbb{N}$, has a prime factor of the same form. What happens if the word odd is omitted?

(b) Repeat (a) for positive integers of the form $4n + 3$.

(c) Repeat (a) for positive integers of the form $6n + 5$.

(d) Prove that there are infinitely many primes of the form $6n + 5$.

35. Suppose p and $p + 2$ are twin primes and $p > 3$. Prove that $6 \mid (p + 1)$.

36. Let $\mathbb{Q}^+$ denote the set of positive rational numbers. If $\frac{m}{n}$ is in $\mathbb{Q}^+$, then

- either $m = 1$ or $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the product of powers of distinct primes $p_1, p_2, \ldots, p_k$;

- either $n = 1$ or $n = q_1^{f_1} q_2^{f_2} \cdots q_\ell^{f_\ell}$ is the product of powers of distinct primes $q_1, q_2, \ldots, q_\ell$

and, in the case $m \neq 1$ and $n \neq 1$, we may assume that no p_i equals any q_j. Now define $f: \mathbb{Q}^+ \to \mathbb{N}$ by

$$f(1) = 1$$

$$f\left(\frac{m}{n}\right) = \begin{cases} p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k} & \text{if } n = 1, m \neq 1 \\ q_1^{2f_1-1} q_2^{2f_2-1} \cdots q_\ell^{2f_\ell-1} & \text{if } m = 1, n \neq 1 \\ p_1^{2e_1} \cdots p_k^{2e_k} q_1^{2f_1-1} \cdots q_\ell^{2f_\ell-1} & \text{if } m \neq 1, n \neq 1 \end{cases}$$

(a) Find $f(8)$ [BB], $f(\frac{1}{8})$, $f(100)$ and $f(\frac{40}{63})$.

(b) Find x such that $f(x) = 1{,}000{,}000$ [BB], t such that $f(t) = 10{,}000{,}000$, and s such that $f(s) = 365{,}040$.

(c) Show that f is a bijection.

(This exercise, which gives a direct proof that the positive rationals are countable, is due to Yoram Sagher. See the *American Mathematical Monthly*, Vol. 96 (1989), no. 9, p. 823.)

37. For positive integers a and b, define $a \sim b$ if there exist integers $n \geq 1$ and $m \geq 1$ such that $a^m = b^n$.

(a) Prove that $\sim$ defines an equivalence relation on $\mathbb{N}$.

(b) Find $\overline{3}$, $\overline{4}$, and $\overline{144}$.

(c) Find the equivalence class of $a \in \mathbb{N}$. [*Hint*: Write $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.]

38. (a) Write a computer program that implements the Sieve of Eratosthenes as described in the text.

(b) Use your program to enumerate all primes less than 1000.

(c) What is $\pi(1000)$? Compare this with approximate values (three decimal place accuracy) of $1000/\ln 1000$ and $\frac{\pi(1000)}{1000/\ln 1000}$.

4.4 Congruence

If it is 11 P.M. in Los Angeles, what time is it in Toronto? If he or she were aware that Los Angeles is three time zones west of Toronto, a person might well respond (correctly) "2 A.M." The process by which the time in Toronto was obtained is sometimes called *clock arithmetic*; more properly, it is *addition modulo* 12: $11+3 = 14 = 2$ (modulo 12). It is based on the idea of *congruence*, the subject of this section.

4.4.1 DEFINITION Let $n > 1$ be a fixed natural number. Given integers a and b, we say that a is *congruent to b modulo n* (or a is *congruent to b mod n* for short) and we write $a \equiv b \pmod{n}$, if and only if $n \mid (a - b)$. The number n is called the *modulus* of the congruence. ❖

EXAMPLE 18 $3 \equiv 17 \pmod{7}$ because $3-17 = -14$ is divisible by 7; $-2 \equiv 13 \pmod{3}$ because $-2 - 13 = -15$ is divisible by 3; $60 \equiv 10 \pmod{25}$; $-4 \equiv -49 \pmod{9}$. ■

As a binary relation on $\mathbb{Z}$, congruence is

reflexive: $a \equiv a \pmod{n}$ for any integer a,

symmetric: if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$ and

transitive: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Congruence is reflexive because $a - a = 0$ is divisible by n. It is symmetric because if $n \mid (a - b)$ then $n \mid (b - a)$ because $b - a = -(a - b)$. It is transitive because, if both $a - b$ and $b - c$ are divisible by n, then so is their sum, which is $a - c$. Thus, for any $n > 1$, congruence mod n is an equivalence relation on $\mathbb{Z}$.

We urge you to review the basic features of equivalence relations that were discussed in Section 2.4. Recall, for instance, that an equivalence relation partitions the underlying set into subsets called equivalence classes, the equivalence class of an element being the set of those elements to which it is equivalent. The equivalence classes of congruence mod n are called *congruence classes*.

4.4.2 DEFINITION The *congruence class mod n* of an integer a is the set of all integers to which a is congruent mod n. It is denoted $\overline{a}$. Thus,

$$\overline{a} = \{b \in \mathbf{Z} \mid a \equiv b \pmod{n}\}.$$

[Since congruence mod n is symmetric, we do not have to remember whether to write $a \equiv b \pmod{n}$ or $b \equiv a \pmod{n}$ in this definition. You can't have one without the other!] ❖

EXAMPLE 19 Let $n = 5$. Since $-8 - 17 = -25$ is divisible by 5, we have $-8 \equiv 17 \pmod{5}$. Thus, -8 belongs to the congruence class of 17; in symbols, $-8 \in \overline{17}$. Notice also that $17 \in \overline{-8}$. In fact, you should check that $\overline{-8} = \overline{17}$. (See Proposition 4.4.3.) ■

Let us find all congruence classes of integers mod 5. To begin,

$$\begin{aligned}\overline{0} &= \{b \in \mathbf{Z} \mid b \equiv 0 \pmod{5}\} \\ &= \{b \in \mathbf{Z} \mid 5 \mid (b-0)\} \\ &= \{b \in \mathbf{Z} \mid b = 5k \text{ for some integer } k\}\end{aligned}$$

and

$$\begin{aligned}\overline{1} &= \{b \in \mathbf{Z} \mid b \equiv 1 \pmod{5}\} \\ &= \{b \in \mathbf{Z} \mid 5 \mid (b-1)\} \\ &= \{b \in \mathbf{Z} \mid b - 1 = 5k \text{ for some integer } k\} \\ &= \{b \in \mathbf{Z} \mid b = 5k + 1 \text{ for some integer } k\}.\end{aligned}$$

In Section 2.4, we introduced the notation $5\mathbf{Z}$ and $5\mathbf{Z} + 1$ for these sets $\overline{0}$ and $\overline{1}$, respectively. Continuing, we find that

$$\overline{2} = \{b \in \mathbf{Z} \mid b = 5k + 2 \text{ for some } k \in \mathbf{Z}\} = 5\mathbf{Z} + 2,$$

$$\overline{3} = \{b \in \mathbf{Z} \mid b = 5k + 3 \text{ for some } k \in \mathbf{Z}\} = 5\mathbf{Z} + 3,$$

and

$$\overline{4} = \{b \in \mathbf{Z} \mid b = 5k + 4 \text{ for some } k \in \mathbf{Z}\} = 5\mathbf{Z} + 4.$$

Note that the five congruence classes determined so far *partition* the integers, as they must: They are equivalence classes.

Equivalence classes are always pairwise disjoint. Here, for instance, if $a \in (5\mathbf{Z} + r) \cap (5\mathbf{Z} + s)$ for $0 \le r, s \le 4$, then $a = 5k + r = 5\ell + s$ for some integers k and ℓ, and so $r - s = 5(\ell - k)$ would be a multiple of 5. For r, s between 0 and 4, this can only happen if $r = s$.

The union of all the congruence classes is $\mathbf{Z}$. For any $a \in \mathbf{Z}$, by the Division Algorithm (Theorem 4.1.5), we can write $a = 5q + r$ with q, r integers and $0 \le r < 5$. Since $r \in \{0, 1, 2, 3, 4\}$, the integer a is in $5\mathbf{Z}$, $5\mathbf{Z} + 1$, $5\mathbf{Z} + 2$, $5\mathbf{Z} + 3$, or $5\mathbf{Z} + 4$.

$$\mathbf{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4} = 5\mathbf{Z} \cup 5\mathbf{Z}+1 \cup 5\mathbf{Z}+2 \cup 5\mathbf{Z}+3 \cup 5\mathbf{Z}+4$$

In general, two equivalence classes are disjoint or equal (Proposition 2.4.4). Here then, for any integer n, $\overline{n}$ must be one of $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, or $\overline{4}$. With which of these classes, for example, does $\overline{5}$ coincide? Observe that $5 \in \overline{5}$, since $5 \equiv 5 \pmod{5}$. Also, as noted previously, $5 \in \overline{0}$. Since the classes $\overline{0}$ and $\overline{5}$ are not disjoint, they are equal: $\overline{5} = \overline{0}$.

Similarly, since 6 belongs to both $\overline{6}$ and $\overline{1}$, we have $\overline{6} = \overline{1}$. You should also see that $\overline{7} = \overline{2}$, $\overline{8} = \overline{3}$, $\overline{-14} = \overline{1}$, and so on.

Our next few results are almost immediate consequences of the theory of equivalence relations.

4.4.3 PROPOSITION Let a, b, and n be integers with $n > 1$. Then the following statements are equivalent.

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $a \in \overline{b}$
4. $b \in \overline{a}$
5. $\overline{a} = \overline{b}$

Proof Each of the implications (1) $\rightarrow$ (2) $\rightarrow$ (3) is a direct consequence of definitions and (3) $\rightarrow$ (4) follows from the symmetry of congruence. We may therefore complete the proof by establishing (4) $\rightarrow$ (5) and (5) $\rightarrow$ (1). To see that (4) $\rightarrow$ (5), let $b \in \overline{a}$. Then $b \equiv a \pmod{n}$, so $\overline{a} = \overline{b}$ by Proposition 2.4.3. To see that (5) $\rightarrow$ (1), suppose that $\overline{a} = \overline{b}$. Then $a \in \overline{b}$ because $a \in \overline{a}$, so $a \equiv b \pmod{n}$ and $n \mid (a - b)$. ●

Of all the equivalences established in Proposition 4.4.3, we emphasize perhaps the most important one.

4.4.4 COROLLARY For integers a, b, and n with $n > 1$,

$$a \equiv b \pmod{n} \text{ if and only if } \overline{a} = \overline{b}.$$

The next proposition generalizes the special case $n = 5$, which we have already investigated.

4.4.5 PROPOSITION Any integer is congruent mod n to its remainder upon division by n. Thus, there are n congruence classes of integers mod n corresponding to each of the n possible remainders

$$\begin{aligned} \overline{0} &= n\mathbf{Z} \\ \overline{1} &= n\mathbf{Z} + 1 \\ \overline{2} &= n\mathbf{Z} + 2 \\ &\vdots \\ \overline{n-1} &= n\mathbf{Z} + (n-1). \end{aligned}$$

These congruence classes partition $\mathbf{Z}$; that is, they are disjoint sets whose union is the set of all integers.

Proof Suppose a is an integer. The remainder when a is divided by n is the number r, $0 \leq r < n$, obtained when we write $a = qn + r$ according to the Division Algorithm (Theorem 4.1.5). Since $a - r = qn$ is divisible by n, we obtain $a \equiv r \pmod{n}$, as claimed.

Since $0 \leq r < n$, the integer r is one of $0, 1, 2, \ldots, n - 1$. Thus, a belongs to one of the specified classes. It remains only to show that these classes are disjoint. For this, note that if $r_1, r_2 \in \{0, 1, \ldots, n-1\}$ then $r_1 \not\equiv r_2 \pmod{n}$. Thus, $r_1 \in \overline{r_1}$, but $r_1 \notin \overline{r_2}$, so the congruence classes $\overline{r_1}$ and $\overline{r_2}$ are not equal. Since congruence

classes are equivalence classes, $\overline{r_1} \cap \overline{r_2} = \emptyset$, by Proposition 2.4.4. Thus, the classes $\overline{0}, \ldots, \overline{n-1}$ are indeed disjoint. ●

EXAMPLE 20 Suppose $n = 32$. There are 32 congruence classes of integers mod 32:

$$\overline{0} = 32\mathbb{Z}, \quad \overline{1} = 32\mathbb{Z} + 1, \quad \ldots, \quad \overline{31} = 32\mathbb{Z} + 31.$$

To determine the class to which a specific integer belongs, say 3958, we use the Division Algorithm to write $3958 = 123(32) + 22$.[8] Thus, 22 is the remainder, so $3958 \equiv 22 \pmod{32}$ by Proposition 4.4.5 and $3958 \in \overline{22}$. ■

Pause 14 Find an integer r, $0 \leq r < 18$, such that $3958 \equiv r \pmod{18}$. Do the same for -3958. ▮

Proposition 4.4.5 says that every integer is congruent modulo n to one of the n integers $0, 1, 2, \ldots, n-1$. Therefore, when working mod n, it is customary to assume that all integers are between 0 and $n-1$ (inclusive) and to replace any integer a outside this range by its remainder upon division by n. This remainder is called "$a \pmod{n}$," and the process of replacing a by $a \pmod{n}$ is called *reduction modulo* n.

4.4.6 DEFINITION If $n > 1$ is a natural number and a is any integer, $a \pmod{n}$ is the remainder r, $0 \leq r < n$, obtained when a is divided by n. ❖

EXAMPLE 21

- $-17 \pmod{5} = 3$, $28 \pmod{6} = 4$ and $-30 \pmod{9} = 6$.
- The integer 29 is 5 mod 6. ■

Just as for equations, to "solve" a congruence or a system of congruences involving one or more unknowns means to find all possible values of the unknowns that make the congruences true, always respecting the convention given in Definition 4.4.6. Without this convention, any even number is a solution to the congruence $2x \equiv 0 \pmod{4}$. With the convention, however, we give only $x = 0$ and $x = 2$ as solutions.

PROBLEM 22. Solve each of the following congruences if possible. If no solution exists, explain why not.

(a) $3x \equiv 1 \pmod{5}$
(b) $3x \equiv 1 \pmod{6}$
(c) $3x \equiv 3 \pmod{6}$

Solution. Simple congruences like these with small moduli are probably best solved by trying all possible values of x mod n.

(a) If $x = 0$, $3x = 0 \equiv 0 \pmod{5}$.
If $x = 1$, $3x = 3 \equiv 3 \pmod{5}$.
If $x = 2$, $3x = 6 \equiv 1 \pmod{5}$.
If $x = 3$, $3x = 9 \equiv 4 \pmod{5}$.
If $x = 4$, $3x = 12 \equiv 2 \pmod{5}$.

Since the modulus is 5, we want x in the range $0 \leq x < 5$. Thus, the only solution to the congruence is $x = 2$.

[8] Remember the easy way to see this. Use a calculator to compute $\frac{3958}{32} = 123.68\ldots$. The integer part of this number (the floor of $\frac{3958}{32}$) is the quotient given by the Division Algorithm. See Proposition 4.1.6.

(b) There is no solution to this congruence because the values of $3x \pmod 6$ are just 0 and 3:

$$3(0) = 0, \quad 3(1) = 3, \quad 3(2) = 6 \equiv 0,$$
$$3(3) = 9 \equiv 3, \quad 3(4) = 12 \equiv 0, \quad 3(5) = 15 \equiv 3.$$

(c) The calculations in part (b) show that $3x \equiv 3 \pmod 6$ has solutions $x = 1$, $x = 3$, and $x = 5$. ▲

Suppose we want to find the sum $1017 + 2876 \pmod 7$. This can be accomplished in two ways. We could evaluate $1017 + 2876 = 3893 \equiv 1 \pmod 7$, but, equally, we could reduce the integers 1017 and 2876 modulo 7 first like this:

$$1017 \equiv 2 \pmod 7$$
$$2876 \equiv 6 \pmod 7$$
$$1017 + 2876 \equiv 2 + 6 = 8 \equiv 1 \pmod 7.$$

The second approach is particularly useful when forming products since it keeps the numbers involved small. Observe:

$$(1017)(2876) \equiv (2)(6) = 12 \equiv 5 \pmod 7.$$

Computing powers of an integer modulo a natural number n is often just a mental (rather than calculator) exercise if we continually work mod n. For example,

$$(1017)^2 \equiv 2^2 = 4 \pmod 7$$
$$(1017)^3 = (1017)^2(1017) \equiv 4(2) = 8 \equiv 1 \pmod 7$$
$$(1017)^4 = (1017)^3(1017) \equiv 1(2) = 2 \pmod 7$$
$$(1017)^5 = (1017)^4(1017) \equiv 2(2) = 4 \pmod 7$$

and so on. Here is an easy way to compute $(1017)^{12}$:

$$(1017)^{12} = ((1017)^4)^3 \equiv 2^3 = 8 \equiv 1 \pmod 7.$$

The following proposition describes the general principles that guarantee that the sorts of calculations we have been performing are valid.

4.4.7 PROPOSITION If $a \equiv x \pmod n$ and $b \equiv y \pmod n$, then

(a) $a + b \equiv x + y \pmod n$ and
(b) $ab \equiv xy \pmod n$.

Proof Direct proofs of each part are suggested.

(a) We have to check that $(a + b) - (x + y)$ is divisible by n. This difference is $(a - x) + (b - y)$, which is the sum of two numbers each divisible by n, so the difference itself is divisible by n.

(b) We have to check that $ab - xy$ is divisible by n. Subtracting and adding ay, we notice that

$$ab - xy = ab - ay + ay - xy = a(b - y) + (a - x)y,$$

each term on the right again being divisible by n. Thus, $ab - xy$ is divisible by n. ●

PROBLEM 23. Suppose a and b are integers and $3 \mid (a^2 + b^2)$. Show that $3 \mid a$ and $3 \mid b$.

Solution. We wish to prove that $a \equiv 0 \pmod 3$ and $b \equiv 0 \pmod 3$ and do so by contradiction. Thus we assume the result is false: so either $a \not\equiv 0 \pmod 3$ or $b \not\equiv 0 \pmod 3$. Assume $a \not\equiv 0 \pmod 3$. Then $a \equiv 1$ or $a \equiv 2 \pmod 3$, so part (b) of Proposition 4.4.7 says $a^2 \equiv 1$ or $a^2 \equiv 2^2 = 4 \equiv 1 \pmod 3$. In each case, $a^2 \equiv 1 \pmod 3$. Now $b \equiv 0, 1, 2 \pmod 3$, so $b^2 \equiv 0^2, 1^2, 2^2 \pmod 3$; that is, $b^2 \equiv 0$ or $1 \pmod 3$. It follows that the possible values of $a^2 + b^2 \pmod 3$ are $1 + 0$ and $1 + 1$. This is a contradiction, since we are given that $a^2 + b^2 \equiv 0 \pmod 3$. Thus $a \equiv 0 \pmod 3$ and, similarly, $b \equiv 0 \pmod 3$. ▲

While addition and multiplication of congruences behave as we would hope, we must be exceedingly careful when **dividing** each side of a congruence by an integer. Dividing each side of the congruence $30 \equiv 12 \pmod 9$ by 3, for example, produces the false statement $10 \equiv 4 \pmod 9$. In general, we can only divide a congruence by an integer that is **relatively prime** to the modulus, as asserted by the next proposition. (We leave its proof to the exercises.)

4.4.8 PROPOSITION If $ac \equiv bc \pmod n$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod n$.

For example, given $28 \equiv 10 \pmod 3$, we can divide by 2 and obtain $14 \equiv 5 \pmod 3$ because $\gcd(2, 3) = 1$. The linear congruences $2x \equiv 1 \pmod 7$ and $6x \equiv 3 \pmod 7$ have the same solutions, since we can divide each side of the second congruence by 3, this being relatively prime to 7. On the other hand, multiplying a congruence by a number not relatively prime to the modulus changes the congruence. For example, the solutions to $2x \equiv 1 \pmod 9$ and $6x \equiv 3 \pmod 9$ are different!

Pause 15 Solve $2x \equiv 1 \pmod 9$ and $6x \equiv 3 \pmod 9$. ▮

PROBLEM 24. Solve each of the following pairs of congruences, if possible. If no solution exists, explain why not.

(a) $2x + 3y \equiv 1 \pmod 6$
$x + 3y \equiv 4 \pmod 6$

(b) $2x + 3y \equiv 1 \pmod 6$
$x + 3y \equiv 5 \pmod 6$

Solution. We solve simple systems of linear congruences by the ad hoc methods with which we first solved systems of linear equations, by adding and subtracting and occasionally multiplying, though only by numbers relatively prime to the modulus (for a reason illustrated by PAUSE 15).

(a) Adding the two congruences gives $3x + 6y \equiv 5 \pmod 6$. Since $6y \equiv 0 \pmod 6$, we have $3x \equiv 5 \pmod 6$. This congruence has no solution because the values of $3x \pmod 6$ are 0 and 3. Thus, no x, y satisfy the given pair of congruences.

(b) This time, adding the two congruences gives $3x \equiv 0 \pmod 6$ and hence $x \equiv 0$, $x \equiv 2$, or $x \equiv 4 \pmod 6$. If $x \equiv 0$, then the second congruence says $3y \equiv 5 \pmod 6$, to which there is no solution. If $x \equiv 2$, the second congruence says $2 + 3y \equiv 5$; hence $3y \equiv 3 \pmod 6$, so $y \equiv 1 \pmod 6$, $y \equiv 3 \pmod 6$, or $y \equiv 5 \pmod 6$. If $x \equiv 4$, the second congruence reads $4 + 3y \equiv 5$, so $3y \equiv 1 \pmod 6$ and there is no solution. The pair of congruences has three solutions: $x \equiv 2 \pmod 6$ and $y \equiv 1 \pmod 6$, $y \equiv 3 \pmod 6$, or $y \equiv 5 \pmod 6$. ▲

Every integer a has an *additive inverse* modulo n; that is, there exists an integer x satisfying $a + x \equiv 0 \pmod{n}$. For example, take $x = -a$ or $x = n - a$ to respect the convention in 4.4.6 above. The existence of additive inverses means that congruences of the form $a + x \equiv b \pmod{n}$ always have a solution obtained by adding the additive inverse of a to each side: $x = b + (-a) = b - a$. On the other hand, not every congruence of the form $ax \equiv b \pmod{n}$ has a solution.

The congruence $3x \equiv b \pmod{6}$ may not have a solution (for example, when $b = 1$). Contrast this with the congruence $3x \equiv b \pmod{7}$, which has a solution for any b since each of the integers 0, 1, 2, 3, 4, 5, 6 is $3x \pmod{7}$ for some x:

$$3(0) = 0, \quad 3(1) = 3, \quad 3(2) = 6, \quad 3(3) = 9 \equiv 2,$$
$$3(4) = 12 \equiv 5, \quad 3(5) = 15 \equiv 1, \quad 3(6) = 18 \equiv 4 \pmod{7}.$$

A solution to $3x \equiv 1 \pmod{7}$, for instance, is $x = 5$. The difference between $3x \equiv b \pmod{6}$ and $3x \equiv b \pmod{7}$ is the modulus. In the second case, 3 is relatively prime to the modulus, 7, whereas in the first case it is not.

4.4.9 PROPOSITION Let $n > 1$ be a natural number and let a be an integer with $\gcd(a, n) = 1$.

(a) There exists an integer s such that $sa \equiv 1 \pmod{n}$.
(b) For any integer b, the congruence $ax \equiv b \pmod{n}$ has a solution.
(c) The solution to $ax \equiv b \pmod{n}$ is unique mod n in the sense that, if $ax_1 \equiv b \pmod{n}$ and $ax_2 \equiv b \pmod{n}$, then $x_1 \equiv x_2 \pmod{n}$.

Proof

(a) By Theorem 4.2.9, the greatest common divisor of two integers is a linear combination of them. Here, since $\gcd(a, n) = 1$, we know there are integers s and t such that $sa + tn = 1$. Since $sa - 1$ is divisible by n, $sa \equiv 1 \pmod{n}$.

(b) By part (a), we know that a has an inverse $s \pmod{n}$. Multiplying the congruence $ax \equiv b$ by s, we have $sax \equiv sb \pmod{n}$ and so $x \equiv sb$. It is straightforward to verify that $x = sb$ is indeed a solution to $ax \equiv b \pmod{n}$ since $a(sb) = (as)b \equiv 1(b) \equiv b \pmod{n}$.

(c) Uniqueness follows directly from Proposition 4.4.8. Since $\gcd(a, n) = 1$, if $ax_1 \equiv ax_2 \pmod{n}$, then $x_1 \equiv x_2 \pmod{n}$. ●

The integer s satisfying $sa \equiv 1 \pmod{n}$, whose existence is part (a) and whose uniqueness is established in part (c), is called the multiplicative *inverse* of $a \pmod{n}$. We write $s = a^{-1}$.

Observe that our proof [in part (b)] that the **congruence** $ax \equiv b \pmod{n}$ has a solution essentially repeats the steps by which we solve the **equation** $ax = b$ in real numbers. To solve $ax = b$, with a, b real numbers and $a \neq 0$, we multiply both sides by the (multiplicative) inverse of a to obtain $x = a^{-1}b$. We solve the congruence $ax \equiv b \pmod{n}$ exactly the same way: If a has a multiplicative inverse $\pmod{n}$, multiply both sides of the congruence by a^{-1}, the inverse of $a \pmod{n}$, obtaining $x \equiv a^{-1}b \pmod{n}$.

It remains to show how to find the inverse of $a \pmod{n}$, when this exists. For this, we use the method described in the proof of Proposition 4.4.9. If $\gcd(a, n) = 1$, we know there exist integers s and t such that $sa + tn = 1$. Thus $sa \equiv 1 \pmod{n}$, so $s = a^{-1}$.

PROBLEM 25. Solve the congruence $20x \equiv 101 \pmod{637}$.

Solution. We have $-7(637) + 223(20) = 1$, so $223(20) \equiv 1 \pmod{637}$ and $223 = 20^{-1} \pmod{637}$. Multiplying each side of the given congruence by 223 gives $x \equiv$

$223(101) = 22{,}523 \equiv 228 \pmod{637}$. Thus, $x = 228$ provides a solution and one that is unique mod 637: Any other solution is congruent mod 637 to 228. ▲

PROBLEM 26. Part (a) of Proposition 4.4.9 says that if $\gcd(a, n) = 1$ then a has an inverse mod n. Show that the converse is also true: If a has an inverse mod n, then $\gcd(a, n) = 1$.

Solution. If a has an inverse mod n, there is an integer s such that $sa \equiv 1 \pmod{n}$, so $sa - 1 = qn$ for some integer q. Writing this as $1 = sa - qn$, it follows that any natural number that divides both n and a must divide 1 and hence be 1. So $\gcd(a, n) = 1$. ▲

As another application of Proposition 4.4.8, we derive *Fermat's Little Theorem.*

Pause 16

What is Fermat's best known theorem? ▮

4.4.10 FERMAT'S LITTLE THEOREM

If p is a prime and $p \nmid c$, then $c^{p-1} \equiv 1 \pmod{p}$.

Proof

We have $\gcd(c, p) = 1$. Thus, by Proposition 4.4.8, no two of the integers c, $2c$, $\ldots$, $(p-1)c$ are congruent mod p. The same proposition also shows that none of the elements $c, 2c, \ldots, (p-1)c$ is $0 \pmod{p}$. Thus, modulo p, the $p-1$ integers $c, 2c, \ldots, (p-1)c$ are precisely $1, 2, \ldots, p-1$, in some order. Thus,

$$c \cdot 2c \cdot 3c \cdots (p-1)c \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

Letting $x = 1 \cdot 2 \cdot 3 \cdots (p-1)$,[9] this equation reads

$$xc^{p-1} \equiv x \pmod{p}$$

and, since $\gcd(p, x) = 1$, we can cancel x and obtain $c^{p-1} \equiv 1$, as required. ●

Because of Fermat's Little Theorem, none of the congruences $2^2 \equiv 1 \pmod{3}$, $4^6 \equiv 1 \pmod{7}$, $9^{10} \equiv 1 \pmod{11}$ are surprises. Similarly, since 13,331 is prime, Fermat's Little Theorem shows $4^{13{,}330} \equiv 1 \pmod{13{,}331}$, $4^{13{,}331} \equiv 4 \pmod{13{,}331}$, and $4^{13{,}332} \equiv 16 \pmod{13{,}331}$.

Pause 17

Explain the last two congruences here. ▮

Answers to Pauses

14. An integer a is congruent (mod 18) to its remainder when it is divided by 18. Since $\frac{3958}{18} = 219.8$, $\lfloor \frac{3958}{18} \rfloor = 219$, and we find $3958 = 219(18) + 16$. The remainder is 16, so $3958 \equiv 16 \pmod{18}$. Similarly, $\lfloor -\frac{3958}{18} \rfloor = -220$, so $-3958 = -220(18) + 2$ and $-3958 \equiv 2 \pmod{18}$.

15. $2x \equiv 1 \pmod{9}$ implies $x = 5$, but $6x \equiv 3 \pmod{9}$ implies $x = 2$, $x = 5$, or $x = 8$.

16. Theorem 4.3.14.

17. $4^{13{,}331} = 4(4^{13{,}330}) \equiv 4(1) = 4 \pmod{13{,}331}$; $4^{13{,}332} = 4(4)(4^{13{,}330}) \equiv 16(1) = 16 \pmod{13{,}331}$, using Fermat's Little Theorem in each case to deduce that $4^{13{,}330} \equiv 1 \pmod{13{,}331}$.

[9] The product of all the integers from 1 to n inclusive is commonly denoted $n!$ (read "n factorial"), so we could also write $(p-1)!$ instead of x. See Definition 5.1.2.

True/False Questions

(Answers can be found in the back of the book.)

1. A 2003 country music hit by Alan Jackson and Jimmy Buffett contains a line that states (roughly) that, while the clock might read only 12:30, it's 5:00 somewhere (and so it's OK to start the evening's entertainment). Unfortunately, it's impossible to meet the conditions of this song within North America.
2. $55 \equiv 7 \pmod 3$.
3. $55 \in \overline{7} \pmod 3$.
4. $55 \equiv 2 \pmod 3$.
5. $\overline{55} = \overline{2} \pmod 3$.
6. There are 72 congruence classes of integers mod 73.
7. $5x \equiv 3 \pmod{10}$ has no solution.
8. $49x \equiv 1 \pmod{81}$ has no solution.
9. If $a \equiv x \pmod n$ and $b \equiv y \pmod n$, then $ab \equiv xy \pmod n$.
10. $84^{10} \equiv 1 \pmod{11}$.

Exercises

*The answers to exercises marked [BB] can be found in the **B**ack of the **B**ook.*

1. [BB] This question concerns congruence mod 7.
   (a) List three positive and three negative integers in $\overline{5}$ and in $\overline{-3}$.
   (b) What is the general form of an integer in $\overline{5}$ and of an integer in $\overline{-3}$?
2. This question concerns congruence mod 13.
   (a) List four positive and five negative integers in $\overline{3}$ and in $\overline{-2}$.
   (b) What is the general form of an integer in $\overline{3}$ and of an integer in $\overline{-2}$?
3. Find $a \pmod n$ in each of the following cases.
   (a) [BB] $a = 1286, n = 39$
   (b) $a = 43{,}197, n = 333$
   (c) [BB] $a = -545{,}608, n = 51$
   (d) $a = -125{,}617, n = 315$
   (e) $a = 11{,}111{,}111{,}111, n = 1111$
4. True or false? Give a reason for each answer.
   (a) [BB] $\overline{2} = \overline{18} \pmod{10}$
   (b) $7 \in \overline{-13} \pmod 5$
   (c) [BB] $-8 \equiv 44 \pmod{13}$
   (d) With respect to congruence mod 29, $\overline{17} \cap \overline{423} = \emptyset$
   (e) $-18 \notin \overline{400} \pmod{19}$
5. List all congruence classes, giving the most usual and one other name for each.
   (a) [BB] congruence mod 3
   (b) congruence mod 5 (c) congruence mod 8
6. Carry out each of the indicated calculations, giving the answer mod n.
   (a) [BB] $21{,}758{,}623 + 17{,}123{,}055, n = 6$
   (b) $(21{,}758{,}623)(17{,}123{,}055), n = 6$
   (c) $(17{,}123)^{50}, n = 6$
   (d) $10^4, 10^8, 10^{12}, 10^{20}, 10^{24}, n = 7$
   (e) [BB] $2, 2^2, 2^3, \ldots, 2^{10}, n = 11$
   (f) $4, 4^2, 4^3, 4^4, 4^5, 4^6, 4^7, 4^8, 4^9, 4^{10}, n = 11$
7. Find $a + b \pmod n$, $ab \pmod n$ and $(a + b)^2 \pmod n$ in each of the following situations:
   (a) $a = 4003, b = -127, n = 85$
   (b) $a = 17{,}891, b = 14{,}485, n = 143$
   (c) $a = -389{,}221, b = 123{,}450, n = 10{,}000$
8. [BB] If $a \in \mathbf{Z}$ and $a \not\equiv 0 \pmod 7$, show that $a \equiv 5^k \pmod 7$ for some integer k.
9. Find all integers $x, 0 \le x < n$, satisfying each of the following congruences mod n. If no such x exists, explain why not.
   (a) [BB] $3x \equiv 4 \pmod n, n = 6$
   (b) $4x \equiv 2 \pmod n, n = 6$
   (c) $4x \equiv 3 \pmod n, n = 7$
   (d) $4x \equiv 3 \pmod n, n = 6$
   (e) [BB] $2x \equiv 18 \pmod n, n = 50$
   (f) [BB] $5x \equiv 1 \pmod n, n = 11$
   (g) $5x \equiv 5 \pmod n, n = 25$
   (h) $4x \equiv 301 \pmod n, n = 592$
   (i) $65x \equiv 27 \pmod n, n = 169$
   (j) $4x \equiv 320 \pmod n, n = 592$
   (k) [BB] $16x \equiv 301 \pmod n, n = 595$
   (l) $79x \equiv 15 \pmod n, n = 722$
   (m) $155x \equiv 1185 \pmod n, n = 1404$
   (n) $58x \equiv 6 \pmod n, n = 78$

10. **(a)** Given integers a, b, c, d, x, and a prime p, suppose $(ax + b)(cx + d) \equiv 0 \pmod{p}$. Prove that $ax + b \equiv 0 \pmod{p}$ or $cx + d \equiv 0 \pmod{p}$.

(b) Find all integers x, $0 \leq x < n$, that satisfy each of the following congruences. If no x exists, explain why not.

i. [BB] $x^2 \equiv 4 \pmod{n}, n = 13$
ii. $(2x + 1)(3x + 4) \equiv 0 \pmod{n}, n = 17$
iii. $3x^2 + 14x - 5 \equiv 0 \pmod{n}, n = 97$
iv. [BB] $x^2 \equiv 2 \pmod{n}, n = 6$
v. $x^2 \equiv -2 \pmod{n}, n = 6$
vi. $4x^2 + 3x + 7 \equiv 0 \pmod{n}, n = 5$

11. Find all integers x and y, $0 \leq x, y < n$, that satisfy each of the following pairs of congruences. If no x, y exist, explain why not.

(a) [BB] $2x + y \equiv 1 \pmod{n}$, $x + 3y \equiv 3 \pmod{n}$, $n = 6$

(b) [BB] $x + 5y \equiv 3 \pmod{n}$, $4x + 5y \equiv 1 \pmod{n}$, $n = 9$

(c) $x + 5y \equiv 3 \pmod{n}$, $4x + 5y \equiv 1 \pmod{n}$, $n = 8$

(d) $7x + 2y \equiv 3 \pmod{n}$, $9x + 4y \equiv 6 \pmod{n}$, $n = 15$

(e) $3x + 5y \equiv 14 \pmod{n}$, $5x + 9y \equiv 6 \pmod{n}$, $n = 28$

12. [BB] Prove Proposition 4.4.8.

13. [BB] If $a \equiv b \pmod{n}$, show that $\gcd(a, n) = \gcd(b, n)$.

14. Suppose a and b are integers, $n > 1$ is a natural number, and $a \equiv b \pmod{n}$. True or false? In each case, prove or give a counterexample.

(a) [BB] $3a \equiv b^2 \pmod{n}$

(b) $a^2 \equiv b^2 \pmod{n}$

(c) $a^2 \equiv b^3 \pmod{n}$ **(d)** $a^2 \equiv b^2 \pmod{n^2}$

15. Let a and n be natural numbers with $n > 1$. Let r and s be integers and suppose $r \equiv s \pmod{n}$. True or false? Explain.

(a) [BB] $a^r \equiv a^s \pmod{n}$

(b) $r^a \equiv s^a \pmod{n}$

16. Prove that an integer $(a_{n-1}a_{n-2}\ldots a_0)_{10}$ is divisible by 11 if and only if $a_0 + a_2 + a_4 + \cdots \equiv a_1 + a_3 + a_5 + \cdots \pmod{11}$. [*Hint*: $10 \equiv -1 \pmod{11}$.]

17. **(a)** [BB] Use the result of Problem 23 to prove that $\sqrt{2}$ is irrational; that is, show that it is impossible to write $\sqrt{2} = \frac{a}{b}$ for integers a, b. [*Hint*: Without loss of generality, assume that a and b have no common factors other than ± 1. Why is there no loss of generality?]

(b) Let n be a natural number, $n \equiv 2 \pmod{3}$. Use Problem 23 to prove that $\sqrt{n}$ is irrational.

18. **(a)** Find all integers x, $0 \leq x < n$, that satisfy each of the following congruences.

i. $x^2 \equiv 1 \pmod{n}$, $n = 5$
ii. $x^2 \equiv 1 \pmod{n}$, $n = 7$
iii. $x^2 \equiv 1 \pmod{n}$, $n = 13$

(b) [BB] Suppose $p \neq 2$ is a prime. Find all integers x, $0 \leq x < p$, such that $x^2 \equiv 1 \pmod{p}$.

19. **(a)** Find all integers x, $0 \leq x < n$, that satisfy each of the following congruences.

i. [BB] $x^2 \equiv 1 \pmod{n}, n = 5^2$
ii. $x^2 \equiv 1 \pmod{n}, n = 5^3$
iii. $x^2 \equiv 1 \pmod{n}, n = 7^2$

(b) Suppose $p \neq 2$ is a prime and k is any natural number. Find all integers x, $0 \leq x < p^k$, that satisfy $x^2 \equiv 1 \pmod{p^k}$.

20. **(a)** Find all integers x, $0 \leq x < n$, that satisfy each of the following congruences.

i. $x^2 \equiv 1 \pmod{n}, n = 2$
ii. $x^2 \equiv 1 \pmod{n}, n = 2^2$
iii. $x^2 \equiv 1 \pmod{n}, n = 2^3$
iv. $x^2 \equiv 1 \pmod{n}, n = 2^4$

(b) Let k be a natural number. Find all integers x, $0 \leq x < 2^k$, that satisfy $x^2 \equiv 1 \pmod{2^k}$.

21. In each case, find the inverse of $a \pmod{n}$ and use this to solve the given congruence.

(a) $a = 7, n = 11, 7x \equiv 3 \pmod{11}$
(b) $a = 15, n = 22, 15x \equiv 9 \pmod{22}$
(c) $a = 32, n = 53, 32x \equiv 19 \pmod{53}$
(d) $a = 8, n = 111, 8x \equiv 28 \pmod{111}$

22. In each of the following, the given integer p is a prime.

(a) [BB] Find 18^{8970}, 18^{8971}, and 18^{8972}, each mod p, $p = 8971$.

(b) Find $53^{20,592}$, $53^{20,593}$, $53^{20,594}$, each mod p, $p = 20{,}593$.

(c) Find 3^{508}, 3^{509}, 3^{512}, each mod p, $p = 509$.

(d) Find $6^{10,588}$, $6^{10,589}$, $6^{10,594}$, each mod p, $p = 10{,}589$.

(e) Find 8^{4056}, 8^{4058}, 8^{4060}, each mod p, $p = 4057$.

(f) Find 2^{3948} and $2^{3941} \pmod{p}$, $p = 3943$.

23. [BB] Show that $x^{97} - x + 1 \equiv 0 \pmod{97}$ has no solutions.

24. Let A be the set of congruence classes of integers modulo some natural number n. For $\overline{a}, \overline{b} \in A$, define $\overline{a} \preceq \overline{b}$ if $ab \equiv a^2 \pmod{n}$. Prove or disprove that $\preceq$ is a partial order in each of the following cases.

(a) $n = p$ is a prime.

(b) $n = pq$ is the product of two distinct primes.

(c) n is divisible by the square of a prime. [*Hint*: It might be helpful first to consider the case $n = 12$.]

4.5 Applications of Congruence

International Standard Book Numbers

Since 1968, most published books have been assigned a 10-digit number called the *International Standard Book Number* (ISBN), which identifies the country of publication, the publisher, and the book itself. The second edition of this book, for example, had ISBN 0-13-092000-2.

In fact, all relevant information in an ISBN is stored in the first nine digits; the tenth digit is a *check digit* whose sole purpose is to give us confidence that the first nine digits are correct.

When a university department wishes to place an order for textbooks for a forthcoming semester, it is common for each faculty member to send to some administrative person the ISBNs of the books he or she will use and then for a single list of all desired ISBNs to be produced and sent to the bookstore. These lists from many departments are collected, grouped in various ways, and sent to publishers. It is not hard to see that there are many opportunities for numbers to be copied incorrectly. Thus, some easy way to encourage accuracy is essential. If the digits of an ISBN are denoted $a_1, a_2, \ldots, a_{10}$, with the first nine in the range 0–9, then a_{10} is chosen in the range 0–10 so that

$$a_1 + 2a_2 + 3a_3 + \cdots + 9a_9 + 10a_{10} \equiv 0 \pmod{11}. \tag{6}$$

If a_{10} happens to be 10, it is recorded as an X.

Checking the ISBN of the second edition of this text, we have

$$1(0) + 2(1) + 3(3) + 4(0) + 5(9) + 6(2) + 7(0) + 8(0) + 9(0) + 10(2) = 88 \equiv 0 \pmod{11}.$$

If an ISBN begins 0-93-603103, the tenth digit is chosen so that

$$1(0) + 2(9) + 3(3) + 4(6) + 5(0) + 6(3) + 7(1) + 8(0) + 9(3) + 10a_{10} \equiv 0 \pmod{11};$$

thus, $103 + 10a_{10} \equiv 0 \pmod{11}$, so $a_{10} = 4$. The ISBN would be recorded as 0-93-603103-4. If this number were copied to another list with an error in the fourth digit, say as 0-93-503103-4, a computer could easily check that

$$1(0) + 2(9) + 3(3) + 4(5) + 5(0) + 6(3) + 7(1) + 8(0) + 9(3) + 10(4) = 139 \equiv 7 \not\equiv 0 \pmod{11},$$

so the existence of a mistake would come to light. Of course, it would be necessary to check previous lists to determine the precise error. Obtaining 7 instead of 0 as the result of our calculation provides no clue as to which digit was in error. For instance, the number 0-93-603153-4 also differs from the correct ISBN in one digit, and for it we again have

$$1(0) + 2(9) + 3(3) + 4(6) + 5(0) + 6(3) + 7(1) + 8(5) + 9(3) + 10(4) = 183 \equiv 7 \pmod{11}.$$

We can show that the test given in (6) always detects errors in single digits (see Exercise 5), although it is possible for errors in two digits to cancel each other and go undetected.

Change two digits in 0-93-603103-4 so that $a_1 + 2a_2 + 3a_3 + \cdots + 9a_9 + 10a_{10} \equiv 0 \pmod{11}$ (and hence the changes would not be detected by our test). ∎

On the other hand, when a number is copied, a common error is for consecutive digits to be transposed: We might dial the phone number 754-3628 instead of 754-3268, for instance.

PROBLEM 27. Show that the test in (6) detects transpositions of consecutive digits.

Solution. If $a_1a_2\cdots a_{10}$ is a correct ISBN number, then

$$a = a_1 + 2a_2 + \cdots + ia_i + (i+1)a_{i+1} + \cdots + 10a_{10} \equiv 0 \pmod{11}.$$

Suppose that the digits a_i and a_{i+1} are transposed. We claim that the miscopied number $a_1a_2\cdots a_{i+1}a_i\cdots a_{10}$ does not satisfy (6). To see this, let

$$b = a_1 + 2a_2 + \cdots + ia_{i+1} + (i+1)a_i + \cdots + 10a_{10}$$

and note that $a - b = i(a_i - a_{i+1}) + (i+1)(a_{i+1} - a_i) = a_{i+1} - a_i$. Thus $b \equiv a_i - a_{i+1} \pmod{11}$. Since $0 \le a_i, a_{i+1} \le 9$, the difference $a_{i+1} - a_i$ cannot be 0 (mod 11) (unless $a_i = a_{i+1}$, in which case there was no transposition error), and so $b \not\equiv 0 \pmod{11}$. The miscopied number does not pass the test. ▲

We conclude this section by observing that the test given in (6) can be abbreviated by writing it in the form $\mathsf{w} \cdot \mathsf{a} \equiv 0 \pmod{11}$, where a is the *vector* $(a_1, a_2, \ldots, a_{10})$, w the *weight vector* $(1, 2, \ldots, 10)$, and $\cdot$ denotes *dot product*. For readers unfamiliar with the concepts of vector and dot product, a *vector* is an n-tuple of numbers, $(a_1, a_2, \ldots, a_n)$ (n can be any natural number), and the dot product of $\mathsf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathsf{b} = (b_1, b_2, \ldots, b_n)$ is the number

$$\mathsf{a} \cdot \mathsf{b} = a_1b_1 + a_2b_2 + \cdots + a_nb_n.$$

These notions are not critical to an understanding of this section but useful, perhaps, to students with some linear algebra background.

Figure 4.5 A universal product code.

Universal Product Codes

Check digits permeate today's society. Besides forming part of an ISBN, they are attached to identification numbers of airline tickets, money orders, credit cards, bank accounts, drivers' licenses, and most items found in stores.

Figure 4.5 shows the kind of *universal product code* (UPC) with which North American consumers are familiar. Most goods for sale today can be identified uniquely by a special number called a *universal product number*. A universal product **code** is a way to represent a universal product **number** as a pattern of black and white stripes of various thicknesses. For obvious reasons, a universal product code is also called a *bar code*. (Later we shall see how this code works.)

The universal product numbers we want to discuss are 12-digit numbers of the form x-xxxxx-xxxxx-x, where each x stands for a single digit between 0 and 9; for example, 0-12345-67890-1. The last digit is a check digit that serves to affirm (with some degree of confidence) the accuracy of the preceding 11. For example, the universal product number shown in Fig. 4.5 is 0-64200-11589-6 and 6 is the check digit. It is not unusual for a scanning device to misread a bar code. The use of a check digit, therefore, provides a way to alert the cashier that the number must be read again.

The check digit is determined by the rule

(7) 3(sum of digits in odd positions)
+ (sum of digits in even positions) $\equiv 0 \pmod{10}$.

For the number encoded by the bar code in Fig. 4.5, for instance, we have

$$\text{sum of digits in odd positions} = 0 + 4 + 0 + 1 + 5 + 9 = 19$$

$$\text{sum of digits in even positions} = 6 + 2 + 0 + 1 + 8 + 6 = 23$$

and $3(19) + 23 = 80 \equiv 0 \pmod{10}$.

As with ISBNs, the rule for determining the check digit of a universal product number can be phrased in the language of vectors. If a_1–$a_2 \cdots a_6$–$a_7 \cdots a_{11}$–a_{12} is a universal product number and $\mathbf{a}$ denotes the vector $(a_1, a_2, \ldots, a_{12})$, then (7) just says $\mathbf{w} \cdot \mathbf{a} \equiv 0 \pmod{10}$ for a certain weight vector $\mathbf{w}$.

Pause 19

What is $\mathbf{w}$? ∎

Finally, we consider the nature of a bar **code** itself. Notice that the bar code in Fig. 4.5 begins and ends with a black–white–black sequence of thin stripes and is separated into distinct halves by a white–black–white–black–white sequence of thin stripes. In each half of the code, each of the digits 0–9 corresponds to a sequence of four stripes of varying thicknesses. In the **left** half, the pattern is white–black–white–black; in the **right** half, it is black–white–black–white.

Using 0 to denote a thin white stripe and 00, 000, 0000 to denote increasingly thicker white stripes and, similarly, using 1 to denote a thin black stripe and 11, 111, 1111 to denote increasingly thicker black stripes, Table 4.6 shows the right and left stripe sequences to which each digit in the range 0–9 corresponds. For example, on the left, 6 is encoded 0101111, that is, by

thin white (0)–thin black (1)–thin white (0)–thickest black (1111).

Note that the stripe sequence that encodes a digit on the right can be obtained from the stripe sequence on the left by interchanging black and white. (Also note that there is no connection between the sequences used to encode a digit and the base 2 representation of that digit.)

Only for convenience of the consumer is the universal product number sometimes written beneath the sequence of stripes that encodes it. The scanning device

Table 4.6 The pattern of stripes used to encode each of the digits 0–9 on the left and right sides of a bar code.

	Encoding	
Digit	On left side	On right side
0	0001101	1110010
1	0011001	1100110
2	0010011	1101100
3	0111101	1000010
4	0100011	1011100
5	0110001	1001110
6	0101111	1010000
7	0111011	1000100
8	0110111	1001000
9	0001011	1110100

used by the cashier to read the code is, of course, only able to detect light and dark stripes.

How does such a device know whether a bar code has been passed over it from left to right or from right to left? Suppose the first four stripes read by the scanner are 0011101. At first thought, we might assume that this was the code for a digit on the left (after all, it begins with a white stripe), but it could also be the code for a digit on the right read backward (since it ends with a black stripe). Notice, however, that there is **no** digit whose left code is 0011101; thus, the scanner has read from right to left and the **last** digit in the product number has been coded 1011100 (the digits of 0011101 in reverse); the last digit in the product number must be 4. Since the sequence of stripes used to encode a digit, when taken in reverse order, is not the sequence of any other encoding, the scanner always knows the direction in which it is reading the code.

There is a simpler way to tell whether the code is being read left to right or right to left. Can you find it? (Study the sum of the digits in the codes given in Table 4.6.)∎

We refer readers who wish to learn more about check digits to a very interesting article by Joseph A. Gallian that appeared in 1991 in an issue of *The College Mathematics Journal*. [10]

The Chinese Remainder Theorem

The notion of congruence is so basic and useful that some people just have to spread the word. In the lunch room the other day, a discrete math student (DMS) boasted to his friend as follows:

DMS: Calculators are neat, but there are lots of ways to work with numbers without having to use one. The trick is to keep the numbers small by working with remainders.

Friend: What do you mean?

DMS: I'm thinking of a three-digit number. When I divide it by 12, I get a remainder of 4.

Friend: So what?

DMS: When I divide the same number by 25, I get a remainder of 15.

Friend: So what?

DMS: What was my number? I'll give you a hint. It's bigger than 200.

Friend (10 minutes later): I give up.

DMS: It's easy. I'll show you how to do it. (*See Exercise 20.*)

We conclude this section by considering certain systems of simultaneous congruences. The system

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 0 \pmod{30}, \end{aligned}$$

for example, has no solution because the first congruence says x is odd while the second says x is even. This situation occurs precisely because the moduli, 4 and 30, are not relatively prime.

[10] Joe Gallian, "The Mathematics of Identification Numbers," *The College Mathematics Journal* **22**, No. 3 (May 1991).

Suppose m and n are relatively prime natural numbers. Then, for any integers a and b, the pair of congruences

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned} \tag{8}$$

has a solution. One way to see this is to note that there are integers s and t such that $sm + tn = 1$, by Theorem 4.2.9. Thus, $x = a(tn) + b(sm)$ is a solution to (8) since $tn \equiv 1 \pmod{m}$ and $sm \equiv 1 \pmod{n}$. Moreover, x is unique mod mn in the sense that, if x' is another solution, then $x \equiv x' \pmod{mn}$. For this, observe that if x and x' both satisfy (8), then $x - x'$ is divisible by both m and n and hence by mn. (See Exercise 11 of Section 4.2.)

PROBLEM 28. Solve the system $\begin{aligned} x &\equiv 2 \pmod{4} \\ x &\equiv 6 \pmod{7}. \end{aligned}$

Solution. We write $1 = (-1)(7) + 2(4)$ and obtain $x = 2(-1)(7) + 6(2)(4) = 34$. Thus, mod 28, $34 \equiv 6$ is the unique solution to the given pair of congruences. ▲

We have been investigating a special case of the *Chinese Remainder Theorem*, named after the country where it was first discovered (circa A.D. 350).

4.5.1 CHINESE REMAINDER THEOREM

Suppose $m_1, m_2, \ldots, m_t$ are pairwise relatively prime integers, that is, any two of them are relatively prime. Then, for any integers $a_1, a_2, \ldots, a_t$, the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_t \pmod{m_t} \end{aligned}$$

has a solution that is unique modulo the product $m_1 m_2 \cdots m_t$.

The proof, which is just an extension of the $t = 2$ case already discussed and a straightforward exercise in mathematical induction, is left to the exercises of Section 5.1.

The Chinese Remainder Theorem has many practical consequences, two of which we now describe. Each provides a convincing example of how "pure" mathematics can have very relevant applications.

Determining Numbers by Their Remainders

Let n be a natural number. By the Fundamental Theorem of Arithmetic (Theorem 4.3.9), n can be written $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$, where $p_1, p_2, \ldots, p_t$ are unique distinct primes and the exponents $\alpha_i > 0$. Let $a > 1$ be some integer and let a_i be the remainder when a is divided by $p_i^{\alpha_i}$. By Proposition 4.4.5, $a \equiv a_i \pmod{p_i^{\alpha_i}}$; in other words,

$$\begin{aligned} a &\equiv a_1 \pmod{p_1^{\alpha_1}} \\ a &\equiv a_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ a &\equiv a_t \pmod{p_t^{\alpha_t}}. \end{aligned}$$

Since the numbers $p_1^{\alpha_1}, \ldots, p_t^{\alpha_t}$ are relatively prime, the Chinese Remainder Theorem says that a is unique mod n. Thus, if $0 < a < n$, then the integer a itself is uniquely determined. This idea is crucial for the manipulation of "large" numbers in computers, since it implies that to store a number a larger than a given computer's capacity it is sufficient to store the set of remainders that a leaves upon division by a set of prime powers. We illustrate.

PROBLEM 29. Let $n = 90 = 2 \cdot 5 \cdot 9$. Suppose a is an integer, $0 < a < 90$, that has remainders 1, 3, and 4 upon division by the prime powers 2, 5, and 9, respectively. We claim that a has been identified uniquely. Why?

Solution. We are given that a is a solution to the system

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 9. \end{aligned}$$

The Chinese Remainder Theorem says that x is unique mod 90. Thus, x is congruent to exactly one a in the range $0 < a < 90$.

To find a, we solve the first two congruences by the method proposed earlier. We write $1(5) - 2(2) = 1$ and obtain $x \equiv 1(5) - 3(2)(2) = -7 \equiv 3 \pmod{10}$. Solving this congruence and the third one, we write $1(10) - 1(9) = 1$ and determine $a \equiv 4(10) - 3(9) = 13 \pmod{90}$. Thus, $a = 13 + 90t$ for some t. Since $0 < a < 90$, we must have $a = 13$. ▲

Suppose that a and b are integers and that $m_1, \ldots, m_t$ are pairwise relatively prime. (Typically, the m_i are powers of distinct prime numbers.) Let a_i and b_i be the remainders when a and b are divided by m_i, respectively. Since $a \equiv a_i \pmod{m_i}$ and $b \equiv b_i \pmod{m_i}$, we know that $ab \equiv a_i b_i \pmod{m_i}$ by Proposition 4.4.7. The Chinese Remainder Theorem says that ab is determined uniquely, mod mn, by the remainders $a_1 b_1, \ldots, a_t b_t$. This idea can be exploited when a and b are (very) large to find the product ab in shorter time than is possible by conventional methods. Again, we illustrate with an example.

EXAMPLE 30 Let $a = 64$ and $b = 79$. We have

$$\begin{aligned} a &\equiv 0 \pmod 4 \\ a &\equiv 1 \pmod 9 \\ a &\equiv 14 \pmod{25} \end{aligned} \qquad \text{and} \qquad \begin{aligned} b &\equiv 3 \pmod 4 \\ b &\equiv 7 \pmod 9 \\ b &\equiv 4 \pmod{25}. \end{aligned}$$

Thus, ab is a solution to the set of congruences

$$\begin{aligned} x &\equiv 0(3) \equiv 0 \pmod 4 \\ x &\equiv 1(7) \equiv 7 \pmod 9 \\ x &\equiv 14(4) = 56 \equiv 6 \pmod{25}. \end{aligned}$$

We solve the first two congruences by writing $1 = 9 - 2(4)$ and obtaining $x \equiv 0(9) - 7(2)(4) = -56 \equiv 16 \pmod{36}$. Then $-9(36) + 13(25) = 1$ gives $x \equiv 6(-9)(36) + 16(13)(25) = 3256 \equiv 556 \pmod{900}$ as a solution to all three. Thus, $ab = 556 + 900t$ for some integer t. Since crude estimates give $4200 < ab < 5600$, we could determine $ab = 556 + 900(5) = 5056$, this being the only value of $556 + 900t$ in this range. ■

Cryptography

Cryptography (also known as cryptology) is the study of ways in which messages can be coded so that a third party, intercepting the code, will have great difficulty recovering the original text. Such coding is of importance not just to the military. Today, when so much information is transmitted electronically, secrecy is of paramount concern to us all. As a second application of the Chinese Remainder Theorem (and of other ideas introduced in this section), we discuss the *RSA Algorithm*, a method of encoding a message discovered in 1977 by Ronald Rivest, Adi Shamir, and Leonard Adleman.

By assigning to the letters of the alphabet the numbers 01, 02, . . . , 26, to a space the number 27 and to various punctuation marks numbers beyond 27, it is apparent that any message determines a number M. "HELLO," for instance, would determine the number $M = 0805121215$. Here is how the RSA Algorithm converts M to another number E.

Choose two different primes p and q and a natural number s relatively prime to both $p-1$ and $q-1$. Let $r = pq$. Let E be the remainder when M^s is divided by r, and use E to encode M; that is, transmit E instead of M. Since $E \equiv M^s \pmod{r}$, we have $E \equiv M^s \pmod{p}$ and $E \equiv M^s \pmod{q}$.

Using the RSA Algorithm and publicizing the values of r and s, anybody can send you an encoded message that you can decode by the following scheme. Since $\gcd(s, p-1) = 1$, there exist integers a and x such that $as + x(p-1) = 1$, so $M = M^{as+x(p-1)} = (M^s)^a (M^{p-1})^x \equiv E^a \pmod{p}$ (by Fermat's Little Theorem). Similarly, $M \equiv E^b \pmod{q}$ for an integer b that you can determine because you know s and q. Since $M \equiv E^a \pmod{p}$ and $M \equiv E^b \pmod{q}$, by the Chinese Remainder Theorem, M is uniquely determined modulo r and, if $M < r$, then M is a uniquely determined integer. The success of this decoding procedure lies in knowing the factorization $r = pq$. Finding the prime factors of a large integer is practically impossible if r is, say, a 100-digit number. Thus, we have described a procedure that can be public knowledge, but that ensures that messages transmitted to you are secure.

PROBLEM 31. Suppose $r = 17 \cdot 59 = 1003$ and $s = 3$. A secret agent wishes to send you the message "GO." In this case, $M = 715$. The agent calculates $M^s = (715)^3$ and, since $(715)^3 \equiv 579 \pmod{1003}$, she transmits the number $E = 579$. You receive this number and must decode it. How is this done?

Solution. First, note that $\gcd(3, 16) = 1$ and $11(3) + (-2)(16) = 1$, so $a = 11$. Also, $39(3) + (-2)(58) = 1$, so $b = 39$. (It is always possible to choose a and b positive. See Exercise 22.) Then $E^a = (579)^{11} \equiv 1^{11} \equiv 1 \pmod{17}$, while $E^b = (579)^{39} \equiv (48)^{39} \equiv 48(3)^{19} \equiv 48(27)22^4 \equiv 7 \pmod{59}$. The problem is then reduced to solving the pair of congruences

$$\begin{aligned} x &\equiv 1 \pmod{17} \\ x &\equiv 7 \pmod{59}. \end{aligned} \tag{9}$$

Using the methods described earlier, we obtain $x \equiv 715 \pmod{1003}$, which was the word transmitted. ▲

What "methods described earlier"? Show how to get 715 as the solution. ▮

As a final remark, we note that, in practice, we do not convert a message to a single enormous number M and then encode M. Instead we divide the message into blocks of characters of a fixed length, convert each block to a number, and then

encode these numbers. For example, the message

THE PROJECT IS DELAYED TWO MONTHS

might be divided into blocks of length 4,

THEP ROJE CTIS DELA YEDT WOMO NTHS

and then into numbers

20080516 18151005 03200919 04051201 25050420 23151315 14200819

each of which could be coded as described previously.

Readers interested in learning more about cryptography might consult the excellent little book *Cryptology*, by Albrecht Beutelspacher, published by the Mathematical Association of America in 1994.

Answers to Pauses

18. We have seen that changing the fourth digit from 6 to 5 gives a number with $a_1 + 2a_2 + \cdots + 9a_9 + 10a_{10} \equiv 7 \pmod{11}$, so if we also change the first digit from 0 to 4, we should get $a_1 + 2a_2 + \cdots + 9a_9 + 10a_{10} \equiv 0 \pmod{11}$, as desired. It is easy to check that the incorrect ISBN 4-93-503103-4, which has errors in two digits, would pass our test.

19. $w = (3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$.

20. The sum of the digits that code a number on the left is odd, whereas the sum of the digits that code a number on the right is even. If the scanner at first reads 0011101, for example, the sum of digits being even implies that the number is on the right.

21.
$$\begin{array}{rrr} 59 & 1 & 0 \\ 17 & 0 & 1 \\ 8 & 1 & -3 \\ 1 & -2 & 7 \end{array}$$

So $1 = -2(59) + 7(17)$ and $1(-2)(59) + 7(7)(17) = 715$ is a solution.

True/False Questions

(Answers can be found in the back of the book.)

1. 0-78-521421-6 is a valid ISBN.

2. 1-25534-32141-1 is a valid universal product number.

3. Vectors are useful in the study of ISBNs and UPCs.

4. The system $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{6}$ has a solution.

5. The system $x \equiv 7 \pmod{9}$, $x \equiv 5 \pmod{10}$, $x \equiv 8 \pmod{11}$ has a unique solution.

6. A natural number a that is less than 105 can be identified uniquely by finding its remainders when divided by 3, 5, and 7.

7. A natural number a that is less than 1000 can be identified uniquely by finding its remainders when divided by 3, 7, and 11.

8. A natural number a that is less than 1000 can be identified uniquely by finding its remainders when divided by 3, 5, 7, and 11.

9. The RSA algorithm uses Fermat's Last Theorem.

10. The RSA algorithm uses the Chinese Remainder Theorem.

Exercises

*The answers to exercises marked [BB] can be found in the **B**ack of the **B**ook.*

1. Which of the following are valid ISBNs and which are not? Explain.
   (a) [BB] 0-12-345678-9
   (b) [BB] 0-43-209105-5
   (c) 1-66-713242-6
   (d) 9-41-288319-6
   (e) 3-49-216627-X
2. Find the digit A so that each of the following numbers is a valid ISBN number.
   (a) [BB] 3-41-610927-A
   (b) A-46-122837-4
   (c) 9-12-3A4551-X
   (d) [BB] 2-72-9188A6-2
   (e) 8-9A-539828-4
3. Is there an ISBN number of the form A-31-526678-2? Explain.
4. [BB] Show that the test given in (6) to detect an error in an ISBN is equivalent to the test $a_1+2a_2+\cdots+9a_9 \equiv a_{10} \pmod{11}$.
5. (a) Show that an error in any single digit of an ISBN will always be detected by the test in (6).
   (b) If an error is made in a single digit, will the test identify which digit is wrong?
6. (a) [BB] Change the third and sixth digits of the ISBN 2-42-978329-0 so that the resulting number is not a valid ISBN.
   (b) Change the third and sixth digits of the ISBN in (a) so that the resulting number is still valid.
   (c) Show that any two digits of an ISBN can always be changed so that the errors would not be detected by the test in (6).
7. Consider the following alternative check for correctness of an ISBN number. Instead of (6), the check digit a_{10} is determined by the rule $a_1 + a_2 + \cdots + a_9 + a_{10} \equiv 0 \pmod{11}$.
   (a) [BB] Express this rule in the form $\mathbf{w} \cdot \mathbf{a} \equiv 0 \pmod{11}$ for some vectors w and a.
   (b) Show that this rule detects an error in a single digit.
   (c) Show that this rule does not detect a transposition of two (different) digits.
8. Try to identify the universal product numbers defined by each of the bar codes in Fig. 4.7.
9. Which of the following are valid universal product numbers and which are not? Explain.
   (a) [BB] 0-12345-67890-1
   (b) 1-66326-73551-5
   (c) [BB] 2-52998-17394-9
   (d) 9-53889-22687-3
   (e) 8-41285-19384-2
10. In each of the following cases, find the digit x so that the given number is a valid universal product number.
    (a) [BB] 0-12x89-29109-4
    (b) 1-29347-49x26-8
    (c) 4-29217-10258-x
    (d) 5-91057-x9332-2
    (e) x-79154-91937-6
11. [BB] This exercise concerns the universal product number test labeled (7) on page 136.
    (a) Show that the test will detect a single error in an even-position digit of a universal product number.
    (b) Show by example that the test will not necessarily detect two errors in even positions.
12. Repeat both parts of Exercise 11 for odd positions.
13. A mistake is made in a single digit of a universal product number.

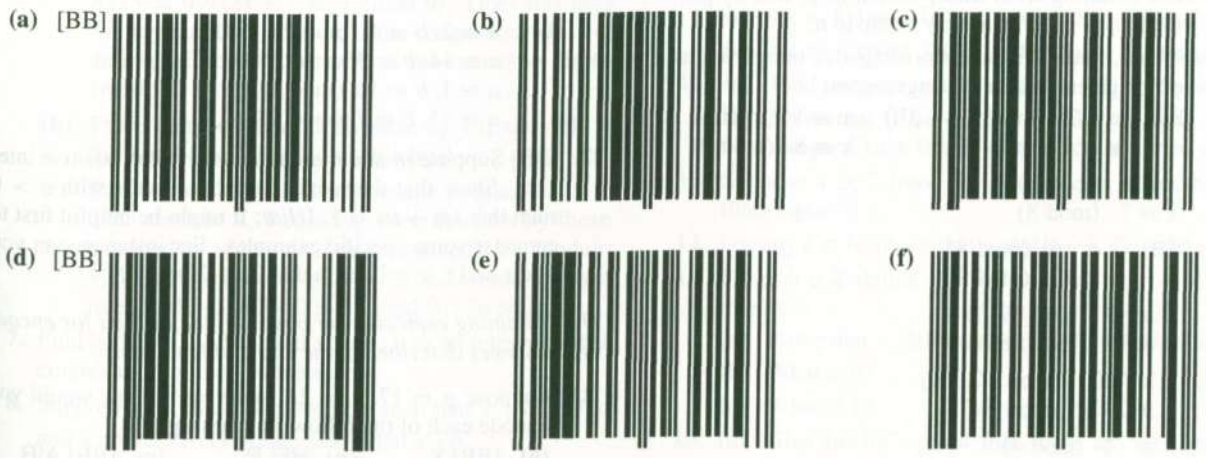


Figure 4.7 Bar codes for Exercise 8.

(a) Will the test described in this section identify the digit that is wrong?

(b) Will it identify whether the error is an odd or an even position?

14. (a) [BB] Give an example of a valid universal product number that differs from the valid number 1-23456-98732-6 in the fourth and fifth positions.

(b) [BB] Give an example of an invalid product number that differs from the valid number 1-23456-98732-6 in the fourth and fifth positions.

15. Does the test in (7) detect transposition errors; that is, will it notice if two (different) adjacent digits have been interchanged? Explain.

16. A certain state proposes to determine the check digit a_{12} of a 12-digit driver's license number $a_1a_2\cdots a_{12}$ by the rule

$$12a_1 + 11a_2 + 10a_3 + \cdots + 2a_{11} + a_{12} \equiv 0 \pmod{10}.$$

(a) Express this test in the form $\mathsf{w}\cdot\mathsf{a} \equiv 0 \pmod{10}$ for vectors w and a.

(b) [BB] Does this test detect an error in a single digit?

(c) Does this test detect the error resulting from the transposition of consecutive digits?

(d) Does it detect transposition errors in general?

Explain your answers.

17. Consider the general test

$$\mathsf{w}\cdot\mathsf{a} \equiv 0 \pmod{n}$$

for correctness of a k-digit number $a_1a_2\ldots a_k$, $0 \le a_i \le 9$, where $\mathsf{a} = (a_1, a_2, \ldots, a_k)$, $\mathsf{w} = (w_1, w_2, \ldots, w_k)$ is a weight vector, and $n > 1$.

(a) [BB] If this is to be a sensible test, we should have $n > 9$. Why?

(b) Assume $n > 9$. If w_i is relatively prime to n for all i, show that the test will detect single-digit errors.

(c) Assume $n > 9$. Show that the test will detect the error resulting from transposition of a_i and a_j provided $w_i - w_j$ is relatively prime to n.

18. In each case, find the smallest nonnegative integer x that satisfies the given system of congruences.

(a) [BB] $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$

(b) $x \equiv 1 \pmod 4$, $x \equiv 8 \pmod 9$

(c) $x \equiv 3 \pmod 5$, $x \equiv 7 \pmod 8$

(d) [BB] $x \equiv 6 \pmod 8$, $x \equiv 17 \pmod{25}$

(e) $x \equiv 3 \pmod{1917}$, $x \equiv 75 \pmod{385}$

(f) $x \equiv 1003 \pmod{17{,}369}$, $x \equiv 2974 \pmod{5472}$

(g) $x \equiv 1 \pmod 4$, $x \equiv 8 \pmod 9$, $x \equiv 10 \pmod{25}$

19. For each of the following, find the smallest positive integer that has the given sequence of remainders when divided by the prime powers 4, 3, and 25, respectively.

(a) [BB] 1, 2, 3

(b) 2, 0, 6

(c) 3, 1, 17

(d) [BB] 0, 2, 10

(e) 3, 2, 24

20. [BB] Think about the conversation between discrete math student and friend on page 138. What was the number?

21. In each of the following cases, find a positive integer x such that $ab \equiv x$ modulo a suitable integer. Assuming that $ab < 50{,}000$, find ab itself, if possible, and explain your reasoning.

(a) [BB] $a \equiv 3, b \equiv 3 \pmod 4$; $a \equiv 0, b \equiv 8 \pmod 9$; $a \equiv 4, b \equiv 18 \pmod{25}$

(b) $a \equiv 7, b \equiv 7 \pmod 8$; $a \equiv 9, b \equiv 8 \pmod{27}$; $a \equiv 29, b \equiv 18 \pmod{125}$

(c) $a \equiv 1, b \equiv 2 \pmod 8$; $a \equiv 8, b \equiv 1 \pmod{27}$; $a \equiv 55, b \equiv 82 \pmod{125}$

(d) $a \equiv 1, b \equiv 6 \pmod 8$; $a \equiv 2, b \equiv 6 \pmod{27}$; $a \equiv 12, b \equiv 97 \pmod{125}$

(e) [BB] $a \equiv 1, b \equiv 3 \pmod 4$; $a \equiv 3, b \equiv 4 \pmod{25}$; $a \equiv 10, b \equiv 79 \pmod{343}$

(f) $a \equiv 3, b \equiv 1 \pmod 4$; $a \equiv 17, b \equiv 6 \pmod{25}$; $a \equiv 78, b \equiv 122 \pmod{343}$

(g) $a \equiv 3, b \equiv 4 \pmod 5$; $a \equiv 36, b \equiv 42 \pmod{49}$; $a \equiv 7, b \equiv 8 \pmod{11}$; $a \equiv 1, b \equiv 3 \pmod{13}$

(h) $a \equiv 2, b \equiv 4 \pmod 5$; $a \equiv 14, b \equiv 36 \pmod{49}$; $a \equiv 1, b \equiv 10 \pmod{11}$; $a \equiv 11, b \equiv 7 \pmod{13}$

22. [BB] Suppose m and n are relatively prime positive integers. Show that there exist integers s and t with $s > 0$ such that $sm + tn = 1$. [*Hint*: It might be helpful first to consider some specific examples. For instance, can you find s and t, $s > 0$, such that $7s + 22t = 1$?]

The remaining exercises are based on the method for encoding messages described at the end of this section.

23. Suppose $p = 17$, $q = 23$, and $s = 5$. How would you encode each of the following "messages"?

(a) [BB] X

(b) HELP

(c) [BB] AIR

(d) BYE

(e) NOW

24. Suppose $p = 5$, $q = 7$, and $s = 5$. Decode each of the following encoded "messages."

(a) [BB] 31 **(b)** 24 **(c)** [BB] 7

(d) 11 **(e)** 23

25. Suppose $p = 17$, $q = 59$, and $s = 3$.

(a) [BB] If you receive $E = 456$, what is the message?

(b) If you receive $E = 926$, what is the message?

Key Terms & Ideas

Here are some technical words and phrases that were used in this chapter. Do you know the meaning of each? If you're not sure, check the glossary or index at the back of the book.

base b
composite
congruence class
congruence mod n
divides
divisor
equivalence relation
factor
greatest common divisor
least common multiple
multiplicity
prime decomposition
prime divisor
prime factor
prime number
quotient
relatively prime
remainder
Well-Ordering Principle

Review Exercises for Chapter 4

1. Find the quotient and remainder when 11,109,999,999,997 is divided by 1111.

2. **(a)** Convert $(1100101)_2$ to base 10.

(b) Convert 32,145 to octal.

3. Buddy claims $31 + 156 = 220$. Could this be true? [*Hint*: Buddy may not be working in base 10.]

4. An integer n, which has exactly eight factors, is divisible by 6 and 14. What is n?

5. Can $(987654321)_b$ be even? Explain.

6. **(a)** The sum of the digits of the number 8215 is $8 + 2 + 1 + 5 = 16 \equiv 7 \pmod 9$. Observe also that $8215 = 9(912) + 7 \equiv 7 \pmod 9$. Does this hold for any number? That is, is the congruence class of an integer (mod 9) the same as the sum of its digits (mod 9)? Explain.

(b) Prove that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9.

(c) Suppose we want to compute the product 8215×3567 modulo 9. Replacing these integers by those obtained by adding their digits and reducing modulo 9 gives $16 \times 21 \equiv 7 \times 3 = 21 \equiv 3 \pmod 9$. Is it true that $8215 \times 3567 \equiv 3 \pmod 9$? Explain.

7. Find $\gcd(2700, -504)$ and express it as an integral linear combination of the given integers.

8. Suppose x, a, and b are integers such that $x \mid ab$. If x and a are relatively prime, prove that $x \mid b$.

9. **(a)** Illustrate the Euclidean algorithm by showing that 571 and 386 are relatively prime.

(b) Find integers a and b such that $571a + 386b = 10$.

(c) Find the smallest positive integer a such that $571a + 386b = 10$. What is the corresponding value of b? Justify your answer. [*Hint*: You may find Exercise 8 helpful.]

10. **(a)** Express 1 as an integral linear combination of 17 and 97.

(b) Solve the congruence $17x \equiv 10 \pmod{97}$.

11. Solve the following congruences; that is, in each case find all values of x between 0 and the given modulus that satisfy the congruence.

(a) $8x \equiv 1 \pmod{27}$ **(b)** $8x \equiv 15 \pmod{27}$

(c) $4x \equiv 8 \pmod{16}$ **(d)** $4x \equiv 9 \pmod{16}$

(e) $6x \equiv 7 \pmod{380}$ **(f)** $6x \equiv 8 \pmod{380}$

12. **(a)** Find integers x_0 and y_0 so that $6x_0 + 25y_0 = 13$.

(b) Show that if $6x + 25y = 13$ then there exists an integer k such that $x = x_0 + 25k$ and $y = y_0 - 6k$.

13. Suppose $n \equiv 7 \pmod 8$. Show that n is not the sum of three squares.

14. For any $k \in \mathbb{N}$, prove that $\gcd(4k + 3, 7k + 5) = 1$.

15. For $a, b \in \mathbb{Z}$, define $a \sim b$ if and only if $a^2 - b^2$ is divisible by 3.

(a) Prove that $\sim$ defines an equivalence relation on $\mathbb{Z}$.

(b) What is $\overline{0}$?

(c) What is $\overline{1}$?

16. **(a)** Give Euclid's proof that there are infinitely many primes.

(b) State the Fundamental Theorem of Arithmetic.

17. Is $2^{119} - 1$ prime? What about $3^{109} - 1$? What about $4^{109} - 1$? Explain your answers.

18. What is the last digit of 7^{355}? [*Hint*: You want the integer k with the property that $7^{355} \equiv k \pmod{10}$.]

19. True or false (and justify):

(a) If $b \mid a$ and $\frac{a}{b} \mid c$, then $bc \mid a$.

(b) If $b \mid a$ and $\frac{a}{b} \mid c$, then $a \mid bc$.

20. Suppose a and b are integers with $1 \leq a < b$. Suppose $a \mid b$ and $(a+1) \mid (b+1)$. Prove that $a^2 < b$.

21. **(a)** Compute $3^{80} \pmod{7}$.

(b) Find all integers x such that $5x \equiv 1 \pmod{100}$. Briefly explain your answer.

22. Find all integers $x \pmod{12}$ that satisfy $9x \equiv 3 \pmod{12}$.

23. Find all integers x, $0 \leq x < 243$ that satisfy $36x \equiv 9 \pmod{243}$.

24. Find all integers x and y, $0 \leq x, y < 10$, that satisfy

$$x + 5y \equiv 5 \pmod{10}$$
$$5x + 3y \equiv 1 \pmod{10}.$$

25. **(a)** Find the digit A so that A-25-322846-7 is a valid ISBN number.

(b) Find the digit x so that 3-25814-39x75-6 is a valid universal product code.

26. Find the smallest nonnegative integer that satisfies

$$x \equiv 5 \pmod{341}$$
$$x \equiv 11 \pmod{189}.$$

27. Find the smallest positive integer x that satisfies

$$x \equiv 3 \pmod{5}$$
$$x \equiv 5 \pmod{7}$$
$$x \equiv 7 \pmod{11}.$$