CHAPTER 4
Number Theory and Cryptography

SECTION 4.1 Divisibility and Modular Arithmetic

Number theory is playing an increasingly important role in computer science. This section and these exercises just scratch the surface of what is relevant. Many of these exercises are simply a matter of applying definitions. It is sometimes hard for a beginning student to remember that in order to prove something about a concept (such as modular arithmetic), it is usually necessary to invoke the definition! Exercises 34–44 hint at the rich structure that modular arithmetic has (sometimes resembling real number arithmetic more than integer arithmetic). In many contexts in mathematics and computer science, modular arithmetic is more relevant and convenient than ordinary integer arithmetic.

1. **a)** yes, since $68 = 17 \cdot 4$ **b)** no, remainder $= 16$
c) yes, since $357 = 17 \cdot 21$ **d)** no, remainder $= 15$

3. If $a \mid b$, then we know that $b = at$ for some integer t. Therefore $bc = a(tc)$, so by definition $a \mid bc$.

5. The given conditions imply that there are integers s and t such that $a = bs$ and $b = at$. Combining these, we obtain $a = ats$; since $a \neq 0$, we conclude that $st = 1$. Now the only way for this to happen is for $s = t = 1$ or $s = t = -1$. Therefore either $a = b$ or $a = -b$.

7. The given condition means that $bc = (ac)t$ for some integer t. Since $c \neq 0$, we can divide both sides by c to obtain $b = at$. This is the definition of $a \mid b$, as desired.

9. In each case we need to find (the unique integers) q and r such that $a = dq + r$ and $0 \leq r < d$, where a and d are the given integers. In each case $q = \lfloor a/d \rfloor$.
a) $19 = 7 \cdot 2 + 5$, so $q = 2$ and $r = 5$ **b)** $-111 = 11 \cdot (-11) + 10$, so $q = -11$ and $r = 10$
c) $789 = 23 \cdot 34 + 7$, so $q = 34$ and $r = 7$ **d)** $1001 = 13 \cdot 77 + 0$, so $q = 77$ and $r = 0$
e) $0 = 19 \cdot 0 + 0$, so $q = 0$ and $r = 0$ **f)** $3 = 5 \cdot 0 + 3$, so $q = 0$ and $r = 3$
g) $-1 = 3 \cdot (-1) + 2$, so $q = -1$ and $r = 2$ **h)** $4 = 1 \cdot 4 + 0$, so $q = 4$ and $r = 0$

11. We are doing arithmetic modulo 12 for this exercise.
a) Because $11 + 80 \textbf{ mod } 12 = 7$, the clock reads 7:00.
b) Because $12 - 40 \textbf{ mod } 12 = -28 \textbf{ mod } 12 = -28 + 36 \textbf{ mod } 12 = 8$, the clock reads 8:00.
c) Because $6 + 100 \textbf{ mod } 12 = 10$, the clock reads 10:00.

13. In each case we merely have to compute the expression on the right **mod** 13. This means dividing it by 13 and taking the (nonnegative) remainder.
a) $9 \cdot 4 \textbf{ mod } 13 = 36 \textbf{ mod } 13 = 10$ **b)** $11 \cdot 9 \textbf{ mod } 13 = 99 \textbf{ mod } 13 = 8$
c) $4 + 9 \textbf{ mod } 13 = 13 \textbf{ mod } 13 = 0$ **d)** $2 \cdot 4 + 3 \cdot 9 \textbf{ mod } 13 = 35 \textbf{ mod } 13 = 9$
e) $4^2 + 9^2 \textbf{ mod } 13 = 97 \textbf{ mod } 13 = 6$
f) $4^3 - 9^3 \textbf{ mod } 13 = -665 \textbf{ mod } 13 = 11$ (because $-665 = -52 \cdot 13 + 11$)

15. The given condition, that a **mod** $m = b$ **mod** m, means that a and b have the same remainder when divided by m. In symbols, $a = q_1 m + r$ and $b = q_2 m + r$ for some integers q_1, q_2, and r. Subtracting these two equations gives us $a - b = (q_1 - q_2)m$, which says that m divides (is a factor of) $a - b$. This is precisely the definition of $a \equiv b \pmod{m}$.

17. The quotient n/k lies between two consecutive integers, say $b-1$ and b, possibly equal to b. In symbols, there exists a positive integer b such that $b - 1 < n/k \leq b$. In particular, $\lceil n/k \rceil = b$. Also, since $n/k > b - 1$, we have $n > k(b-1)$, and so (since everything is an integer) $n - 1 \geq k(b-1)$. This means that $(n-1)/k \geq b-1$, so $\lfloor (n-1)/k \rfloor \geq b-1$. On the other hand, $\lfloor (n-1)/k \rfloor \leq (n-1)/k < n/k \leq b$, so $\lfloor (n-1)/k \rfloor < b$. Therefore $\lfloor (n-1)/k \rfloor = b - 1$. The desired conclusion follows.

19. Let's first look at an example or two. If $m = 7$, then the usual set of values we use for the congruence classes modulo m is $\{0, 1, 2, 3, 4, 5, 6\}$. However, we can replace 6 by -1, 5 by -2, and 4 by -3 to get the collection $\{-3, -2, -1, 0, 1, 2, 3\}$. These will be the values with smallest absolute values. Similarly, if $m = 8$, then the collection we want is $\{-3, -2, -1, 0, 1, 2, 3, 4\}$ ($\{-4, -3, -2, -1, 0, 1, 2, 3\}$ would do just as well). In general, in place of $\{0, 1, 2, \ldots, m-1\}$ we can use $\{\lceil -m/2 \rceil, \lceil -m/2 \rceil + 1, \ldots, -1, 0, 1, 2, \ldots, \lceil m/2 \rceil\}$, omitting either $\lceil -m/2 \rceil$ or $\lceil m/2 \rceil$ if m is even. Note that the values in $\{0, 1, 2, \ldots, m-1\}$ greater than $\lceil m/2 \rceil$ have had m subtracted from them to produce the negative values in our answer. As for a formula to produce these values, we can use a two-part formula:

$$f(x) = \begin{cases} x \textbf{ mod } m & \text{if } x \textbf{ mod } m \leq \lceil m/2 \rceil \\ (x \textbf{ mod } m) - m & \text{if } x \textbf{ mod } m > \lceil m/2 \rceil. \end{cases}$$

Note that if m is even, then we can, alternatively, take $f(m/2) = -m/2$.

21. For these problems, we need to perform the division (as in Exercise 9) and report the remainder.

a) $13 = 3 \cdot 4 + 1$, so 13 **mod** $3 = 1$ **b)** $-97 = 11 \cdot (-9) + 2$, so -97 **mod** $11 = 2$

c) $155 = 19 \cdot 8 + 3$, so 155 **mod** $19 = 3$ **d)** $-221 = 23 \cdot (-10) + 9$, so -221 **mod** $23 = 9$

23. Recall that a **div** m and a **mod** m are the integer quotient and remainder when a is divided by m.

a) Because $228 = 1 \cdot 119 + 109$, we have 228 **div** $119 = 1$ and 228 **mod** $119 = 109$.

b) Because $9009 = 40 \cdot 223 + 89$, we have 9009 **div** $223 = 40$ and 9009 **mod** $223 = 89$.

c) Because $-10101 = -31 \cdot 333 + 222$, we have -10101 **div** $333 = -31$ and -10101 **mod** $333 = 222$. (Note that $10101 \div 333$ is $30\frac{111}{333}$, so without the negative dividend we would get a different absolute quotient and different remainder. But we have to round the negative quotient here, $-30\frac{111}{333}$, *down* to -31 in order for the remainder to be nonnegative.)

d) Because $-765432 = -21 \cdot 38271 + 38259$, we have -765432 **div** $38271 = -21$ and -765432 **mod** $38271 = 38259$.

25. **a)** Because -15 already satisfies the inequality, the answer is -15.

b) Because 24 is too large to satisfy the inequality, we subtract 31 and obtain the answer is -7.

c) Because 99 is too small to satisfy the inequality, we add 41 and obtain the answer is 140.

27. We just need to start at -1 and repeatedly subtract or add 25 until we exceed the desired range. Thus the negative values we seek are -1, -26, -51, and -76, and the positive values are 24, 49, 74, and 99.

29. For these problems, we need to divide by 17 and see whether the remainder equals 5. Remember that the quotient can be negative, but the remainder r must satisfy $0 \leq r < 17$.

a) $80 = 17 \cdot 4 + 12$, so $80 \not\equiv 5 \pmod{17}$ **b)** $103 = 17 \cdot 6 + 1$, so $103 \not\equiv 5 \pmod{17}$

c) $-29 = 17 \cdot (-2) + 5$, so $-29 \equiv 5 \pmod{17}$ **d)** $-122 = 17 \cdot (-8) + 14$, so $-122 \not\equiv 5 \pmod{17}$

31.

a) Working modulo 23, we have $-133 + 261 = 128 \equiv 13$, so the answer is 13.

b) Working modulo 23, we have $457 \cdot 182 \equiv 20 \cdot 21 = 420 \equiv 6$.

33. **a)** $(99^2 \textbf{ mod } 32)^3 \textbf{ mod } 15 = (3^2 \textbf{ mod } 32)^3 \textbf{ mod } 15 = 9^3 \textbf{ mod } 15 = 729 \textbf{ mod } 15 = 9$

b) $(3^4 \textbf{ mod } 17)^2 \textbf{ mod } 11 = (81 \textbf{ mod } 17)^2 \textbf{ mod } 11 = 13^2 \textbf{ mod } 11 = 2^2 \textbf{ mod } 11 = 4$

c) $(19^3 \textbf{ mod } 23)^2 \textbf{ mod } 31 = ((-4)^3 \textbf{ mod } 23)^2 \textbf{ mod } 31 = (-64 \textbf{ mod } 23)^2 \textbf{ mod } 31 = 5^2 \textbf{ mod } 31 = 25$

d) $(89^3 \textbf{ mod } 79)^4 \textbf{ mod } 26 = (10^3 \textbf{ mod } 79)^4 \textbf{ mod } 26 = (1000 \textbf{ mod } 79)^4 \textbf{ mod } 26 = 52^4 \textbf{ mod } 26 = 0^4 \textbf{ mod } 26 = 0$

35. The hypothesis $a \equiv b \pmod{m}$ means that $m \,|\, (a - b)$. Since we are given that $n \,|\, m$, Theorem 1(*iii*) implies that $n \,|\, (a - b)$. Therefore $a \equiv b \pmod{n}$, as desired.

37. **a)** To show that this conditional statement does not necessarily hold, we need to find an example in which $ac \equiv bc \pmod{m}$, but $a \not\equiv b \pmod{m}$. Let $m = 4$ and $c = 2$ (what is important in constructing this example is that m and c have a nontrivial common factor). Let $a = 0$ and $b = 2$. Then $ac = 0$ and $bc = 4$, so $ac \equiv bc \pmod{4}$, but $0 \not\equiv 2 \pmod{4}$.

b) To show that this conditional statement does not necessarily hold, we need to find an example in which $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, but $a^c \not\equiv b^d \pmod{m}$. If we try a few randomly chosen positive integers, we will soon find one. Let $m = 5$, $a = 3$, $b = 3$, $c = 1$, and $d = 6$. Then $a^c = 3$ and $b^d = 729 \equiv 4 \pmod{5}$, so $3^1 \not\equiv 3^6 \pmod{5}$, even though $3 \equiv 3 \pmod{5}$ and $1 \equiv 6 \pmod{5}$.

39. By Exercise 38 the sum of two squares must be either $0 + 0$, $0 + 1$, or $1 + 1$, modulo 4. Therefore the sum cannot be 3 modulo 4, which means that it cannot be of the form $4k + 3$.

41. There are at least two ways to prove this. One way is to invoke Theorem 5 repeatedly. Since $a \equiv b \pmod{m}$, Theorem 5 implies that $a \cdot a \equiv b \cdot b \pmod{m}$, i.e., $a^2 \equiv b^2 \pmod{m}$. Invoking Theorem 5 again, since $a \equiv b \pmod{m}$ and $a^2 \equiv b^2 \pmod{m}$, we obtain $a^3 \equiv b^3 \pmod{m}$. After $k - 1$ applications of this process, we obtain $a^k \equiv b^k \pmod{m}$, as desired. (This is really a proof by mathematical induction, a topic to be considered formally in Chapter 5.)

Alternately, we can argue directly, using the algebraic identity $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1})$. Specifically, the hypothesis that $a \equiv b \pmod{m}$ means that $m \,|\, (a - b)$. Therefore by Theorem 1(*ii*), m divides the right-hand side of this identity, so $m \,|\, (a^k - b^k)$. This means precisely that $a^k \equiv b^k \pmod{m}$.

43. The closure property states that $a \cdot_m b \in \mathbf{Z}_m$ whenever $a, b \in \mathbf{Z}_m$. Recall that $\mathbf{Z}_m = \{0, 1, 2, \ldots, m - 1\}$ and that $a \cdot_m b$ is defined to be $(a \cdot b) \textbf{ mod } m$. But this last expression will by definition be an integer in the desired range. To see that multiplication is associative, we must show that $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$. This is equivalent to

$$((a \cdot b \textbf{ mod } m) \cdot c) \textbf{ mod } m = (a \cdot (b \cdot c \textbf{ mod } m)) \textbf{ mod } m.$$

This is true, because both sides equal $(a \cdot b \cdot c) \textbf{ mod } m$ (multiplication of integers is associative). Similarly, multiplication in $\mathbf{Z}_m$ is commutative because multiplication in $\mathbf{Z}$ is commutative, and 1 is the multiplicative identity for $\mathbf{Z}_m$ because 1 is the multiplicative identity for $\mathbf{Z}$.

45. We will use $+$ and $\cdot$ for these operations to save space and improve the appearance of the table. Notice that we really can get by with a little more than half of this table if we observe that these operations are commutative; then we would need to list $a + b$ and $a \cdot b$ only for $a \leq b$.

$$
\begin{array}{lllll}
0+0=0 & 0+1=1 & 0+2=2 & 0+3=3 & 0+4=4 \\
1+0=1 & 1+1=2 & 1+2=3 & 1+3=4 & 1+4=0 \\
2+0=2 & 2+1=3 & 2+2=4 & 2+3=0 & 2+4=1 \\
3+0=3 & 3+1=4 & 3+2=0 & 3+3=1 & 3+4=2 \\
4+0=4 & 4+1=0 & 4+2=1 & 4+3=2 & 4+4=3
\end{array}
$$

$$
\begin{array}{lllll}
0\cdot 0=0 & 0\cdot 1=0 & 0\cdot 2=0 & 0\cdot 3=0 & 0\cdot 4=0 \\
1\cdot 0=0 & 1\cdot 1=1 & 1\cdot 2=2 & 1\cdot 3=3 & 1\cdot 4=4 \\
2\cdot 0=0 & 2\cdot 1=2 & 2\cdot 2=4 & 2\cdot 3=1 & 2\cdot 4=3 \\
3\cdot 0=0 & 3\cdot 1=3 & 3\cdot 2=1 & 3\cdot 3=4 & 3\cdot 4=2 \\
4\cdot 0=0 & 4\cdot 1=4 & 4\cdot 2=3 & 4\cdot 3=2 & 4\cdot 4=1
\end{array}
$$

47. If $d = 1$, then $f(a) = a$ and $g(a) = 0$. Therefore f is clearly one-to-one and onto, and g is neither. If $d > 1$, then f is still onto, because $f(db) = b$ for any desired $b \in \mathbf{Z}$, but it is clearly not one-to-one, because $f(0) = f(1) = 0$. Furthermore, g is clearly not onto, because its range is just $\{0, 1, 2, \ldots, d-1\}$, and it is not one-to-one because $g(0) = g(d) = 0$.

SECTION 4.2 Integer Representations and Algorithms

In addition to having some routine calculation exercises, this exercise set introduces other forms of representing integers. These are **balanced ternary expansion**, **Cantor expansion**, **binary coded decimal** *(or* **BCD***) representation, and* **one's** *and* **two's complement** *representations. Each has practical and/or theoretical importance in mathematics or computer science. If all else fails, one can carry out an algorithm by "playing computer" and mechanically following the pseudocode step by step.*

1. We divide repeatedly by 2, noting the remainders. The remainders are then arranged from right to left to obtain the binary representation of the given number.

a) We begin by dividing 231 by 2, obtaining a quotient of 115 and a remainder of 1. Therefore $a_0 = 1$. Next $115/2 = 57$, remainder 1. Therefore $a_1 = 1$. Similarly $57/2 = 28$, remainder 1. Therefore $a_2 = 1$. Then $28/2 = 14$, remainder 0, so $a_3 = 0$. Similarly $a_4 = 0$, after we divide 14 by 2, obtaining 7 with remainder 0. Three more divisions yield quotients of 3, 1, and 0, with remainders of 1, 1, and 1, respectively, so $a_5 = a_6 = a_7 = 1$. Putting all this together, we see that the binary representation is $(a_7a_6a_5a_4a_3a_2a_1a_0)_2 = (1110\ 0111)_2$. As a check we can compute that $2^0 + 2^1 + 2^2 + 2^5 + 2^6 + 2^7 = 231$.

b) Following the same procedure as in part **(a)**, we obtain successive remainders 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1. Therefore $4532 = (1\ 0001\ 1011\ 0100)_2$.

c) By the same method we obtain $97644 = (1\ 0111\ 1101\ 0110\ 1100)_2$.

3. **a)** $(1\ 1111)_2 = 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 16 + 8 + 4 + 2 + 1 = 31$. An easier way to get the answer is to note that $(1\ 1111)_2 = (10\ 0000)_2 - 1 = 2^5 - 1 = 31$.

b) $(10\ 0000\ 0001)_2 = 2^9 + 2^0 = 513$

c) $(1\ 0101\ 0101)_2 = 2^8 + 2^6 + 2^4 + 2^2 + 2^0 = 256 + 64 + 16 + 4 + 1 = 341$

d) $(110\ 1001\ 0001\ 0000)_2 = 2^{14} + 2^{13} + 2^{11} + 2^8 + 2^4 = 16384 + 8192 + 2048 + 256 + 16 = 26896$

5. In each case we follow the idea given in Example 7, converting each octal digit to its binary equivalent (including leading 0's where necessary). Note that by convention we then group the binary digits into groups of fours, starting at the right.

a) Since $(5)_8 = (101)_2$, $(7)_8 = (111)_2$, and $(2)_8 = (010)_2$, we have $(572)_8 = (1\ 0111\ 1010)_2$.

b) We concatenate 1, 110, 000, and 100 to obtain $(11\ 1000\ 0100)_2$.

c) $(1\ 0001\ 0011)_2$ **d)** $(101\ 0000\ 1111)_2$

7. Following Example 7, we simply write the binary equivalents of each digit: $(\text{A})_{16} = (1010)_2$, $(\text{B})_{16} = (1011)_2$, $(\text{C})_{16} = (1100)_2$, $(\text{D})_{16} = (1101)_2$, $(\text{E})_{16} = (1110)_2$, and $(\text{F})_{16} = (1111)_2$. Note that the blocking by groups of four binary digits is just for readability by humans.

a) $(80\text{E})_{16} = (1000\ 0000\ 1110)_2$

b) $(135\text{AB})_{16} = (0001\ 0011\ 0101\ 1010\ 1011)_2$

c) $(\text{ABBA})_{16} = (1010\ 1011\ 1011\ 1010)_2$

d) $(\text{DEFACED})_{16} = (1101\ 1110\ 1111\ 1010\ 1100\ 1110\ 1101)_2$

9. Following Example 7, we simply write the binary equivalents of each digit. Since $(\text{A})_{16} = (1010)_2$, $(\text{B})_{16} = (1011)_2$, $(\text{C})_{16} = (1100)_2$, $(\text{D})_{16} = (1101)_2$, $(\text{E})_{16} = (1110)_2$, and $(\text{F})_{16} = (1111)_2$, we see that $(\text{ABCDEF})_{16} = (101010111100110111101111)_2$. Following the convention shown in Exercise 3 of grouping binary digits by fours, we can write this in a more readable form as 1010 1011 1100 1101 1110 1111.

11. Following Example 7, we simply write the hexadecimal equivalents of each group of four binary digits. Thus we have $(1011\ 0111\ 1011)_2 = (\text{B7B})_{16}$.

13. We adopt a notation that will help with the explanation. Adding up to three leading 0's if necessary, write the binary expansion as $(\ldots b_{23}b_{22}b_{21}b_{20}b_{13}b_{12}b_{11}b_{10}b_{03}b_{02}b_{01}b_{00})_2$. The value of this numeral is $b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + 2^4b_{10} + 2^5b_{11} + 2^6b_{12} + 2^7b_{13} + 2^8b_{20} + 2^9b_{21} + 2^{10}b_{22} + 2^{11}b_{23} + \cdots$, which we can rewrite as $b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + (b_{10} + 2b_{11} + 4b_{12} + 8b_{13}) \cdot 2^4 + (b_{20} + 2b_{21} + 4b_{22} + 8b_{23}) \cdot 2^8 + \cdots$. Now $(b_{i3}b_{i2}b_{i1}b_{i0})_2$ translates into the hexadecimal digit h_i. So our number is $h_0 + h_1 \cdot 2^4 + h_2 \cdot 2^8 + \cdots = h_0 + h_1 \cdot 16 + h_2 \cdot 16^2 + \cdots$, which is the hexadecimal expansion $(\ldots h_1h_1h_0)_{16}$.

15. We adopt a notation that will help with the explanation. Adding up to two leading 0's if necessary, write the binary expansion as $(\ldots b_{22}b_{21}b_{20}b_{12}b_{11}b_{10}b_{02}b_{01}b_{00})_2$. The value of this numeral is $b_{00} + 2b_{01} + 4b_{02} + 2^3b_{10} + 2^4b_{11} + 2^5b_{12} + 2^6b_{20} + 2^7b_{21} + 2^8b_{22} + \cdots$, which we can rewrite as $b_{00} + 2b_{01} + 4b_{02} + (b_{10} + 2b_{11} + 4b_{12}) \cdot 2^3 + (b_{20} + 2b_{21} + 4b_{22}) \cdot 2^6 + \cdots$. Now $(b_{i2}b_{i1}b_{i0})_2$ translates into the octal digit h_i. So our number is $h_0 + h_1 \cdot 2^3 + h_2 \cdot 2^6 + \cdots = h_0 + h_1 \cdot 8 + h_2 \cdot 8^2 + \cdots$, which is the octal expansion $(\ldots h_1h_1h_0)_8$.

17. In each case we follow the method of Example 7, blocking by threes instead of fours. We replace each octal digit of the given numeral by its 3-digit binary equivalent and string the digits together. The first digit is $(7)_8 = (111)_2$, the next is $(3)_8 = (011)_2$, and so on, so we obtain $(1\ 1101\ 1100\ 1010\ 1101\ 0001)_2$. For the other direction, we split the given binary numeral into blocks of three digits, adding initial 0's to fill it out: 001 010 111 011. Then we replace each block by its octal equivalent, obtaining the answer $(1273)_8$.

19. Since we have procedures for converting both octal and hexadecimal to and from binary (Example 7), to convert from octal to hexadecimal, we first convert from octal to binary and then convert from binary to hexadecimal.

21. We can just add and multiply using the grade-school algorithms, working with these very simple addition and multiplication tables: $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, $1 + 1 = 10$, which means that we "carry" the 1 into the

next column; $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$. See Examples 8 and 10. Note that we can check our work by converting everything to decimal numerals (the check is shown in parentheses below). For convenience, we leave off the "2" subscripts throughout.

a) $100\ 0111 + 111\ 0111 = 1011\ 1110$ (decimal: $71 + 119 = 190$)
$100\ 0111 \cdot 111\ 0111 = 10\ 0001\ 0000\ 0001$ (decimal: $71 \cdot 119 = 8449$)

b) $1110\ 1111 + 1011\ 1101 = 1\ 1010\ 1100$ (decimal: $239 + 189 = 428$)
$1110\ 1111 \cdot 1011\ 1101 = 1011\ 0000\ 0111\ 0011$ (decimal: $239 \cdot 189 = 45{,}171$)

c) $10\ 1010\ 1010 + 1\ 1111\ 0000 = 100\ 1001\ 1010$ (decimal: $682 + 496 = 1178$)
$10\ 1010\ 1010 \cdot 1\ 1111\ 0000 = 101\ 0010\ 1001\ 0110\ 0000$ (decimal: $682 \cdot 496 = 338{,}272$)

d) $10\ 0000\ 0001 + 11\ 1111\ 1111 = 110\ 0000\ 0000$ (decimal: $513 + 1023 = 1536$)
$10\ 0000\ 0001 \cdot 11\ 1111\ 1111 = 1000\ 0000\ 0001\ 1111\ 1111$ (decimal: $513 \cdot 1023 = 524{,}799$)

23. We can just add and multiply using the grade-school algorithms (working column by column starting at the right), using the addition and multiplication tables in base eight (for example, $5 + 6 = 13$ and $5 \cdot 6 = 36$). When a digit-by-digit answer is too large to fit (i.e., greater than 7), we "carry" into the next column. Note that we can check our work by converting everything to decimal numerals (the check is shown in parentheses below). For convenience, we leave off the "8" subscripts throughout.

a) $763 + 147 = 1132$ (decimal: $499 + 103 = 602$)
$763 \cdot 147 = 144{,}305$ (decimal: $499 \cdot 103 = 51{,}397$)

b) $6001 + 272 = 6273$ (decimal: $3073 + 186 = 3259$)
$6001 \cdot 272 = 2{,}134{,}272$ (decimal: $3073 \cdot 186 = 571{,}578$)

c) $1111 + 777 = 2110$ (decimal: $585 + 511 = 1096$)
$1111 \cdot 777 = 1{,}107{,}667$ (decimal: $585 \cdot 511 = 298{,}935$)

d) $54321 + 3456 = 57{,}777$ (decimal: $22{,}737 + 1838 = 24{,}575$)
$54321 \cdot 3456 = 237{,}326{,}216$ (decimal: $22{,}737 \cdot 1838 = 41{,}790{,}606$)

25. In effect, this algorithm computes 7 **mod** 645, 7^2 **mod** 645, 7^4 **mod** 645, 7^8 **mod** 645, 7^{16} **mod** 645, ..., and then multiplies (modulo 645) the required values. Since $644 = (1010000100)_2$, we need to multiply together 7^4 **mod** 645, 7^{128} **mod** 645, and 7^{512} **mod** 645, reducing modulo 645 at each step. We compute by repeatedly squaring: 7^2 **mod** $645 = 49$, 7^4 **mod** $645 = 49^2$ **mod** $645 = 2401$ **mod** $645 = 466$, 7^8 **mod** $645 = 466^2$ **mod** $645 = 217156$ **mod** $645 = 436$, 7^{16} **mod** $645 = 436^2$ **mod** $645 = 190096$ **mod** $645 = 466$. At this point we see a pattern with period 2, so we have 7^{32} **mod** $645 = 436$, 7^{64} **mod** $645 = 466$, 7^{128} **mod** $645 = 436$, 7^{256} **mod** $645 = 466$, and 7^{512} **mod** $645 = 436$. Thus our final answer will be the product of 466, 436, and 436, reduced modulo 645. We compute these one at a time: $466 \cdot 436$ **mod** $645 = 203176$ **mod** $645 = 1$, and $1 \cdot 436$ **mod** $645 = 436$. So 7^{644} **mod** $645 = 436$. A computer algebra system will verify this; use the command "`7 &^ 644 mod 645;`" in *Maple*, for example. The ampersand here tells *Maple* to use modular exponentiation, rather than first computing the integer 7^{644}, which has over 500 digits, although it could certainly handle this if asked. The point is that modular exponentiation is much faster and avoids having to deal with such large numbers.

27. In effect, this algorithm computes 3 **mod** 99, 3^2 **mod** 99, 3^4 **mod** 99, 3^8 **mod** 99, 3^{16} **mod** 99, ..., and then multiplies (modulo 99) the required values. Since $2003 = (11111010011)_2$, we need to multiply together 3 **mod** 99, 3^2 **mod** 99, 3^{16} **mod** 99, 3^{64} **mod** 99, 3^{128} **mod** 99, 3^{256} **mod** 99, 3^{512} **mod** 99, and 3^{1024} **mod** 99, reducing modulo 99 at each step. We compute by repeatedly squaring: 3^2 **mod** $99 = 9$, 3^4 **mod** $99 = 81$, 3^8 **mod** $99 = 81^2$ **mod** $99 = 6561$ **mod** $99 = 27$, 3^{16} **mod** $99 = 27^2$ **mod** $99 = 729$ **mod** $99 = 36$, 3^{32} **mod** $99 = 36^2$ **mod** $99 = 1296$ **mod** $99 = 9$, and then the pattern repeats, so 3^{64} **mod** $99 = 81$, 3^{128} **mod** $99 = 27$, 3^{256} **mod** $99 = 36$, 3^{512} **mod** $99 = 9$, and 3^{1024} **mod** $99 = 81$. Thus

our final answer will be the product of 3, 9, 36, 81, 27, 36, 9, and 81. We compute these one at a time modulo 99: $3 \cdot 9$ is 27, $27 \cdot 36$ is 81, $81 \cdot 81$ is 27, $27 \cdot 27$ is 36, $36 \cdot 36$ is 9, $9 \cdot 9$ is 81, and finally $81 \cdot 81$ is 27. So $3^{2003} \bmod 99 = 27$.

29. The binary expansion of an integer represents the integer as a sum of distinct powers of 2. For example, since $21 = (1\ 0101)_2$, we have $21 = 2^4 + 2^2 + 2^0$. Since binary expansions are unique, each integer can be so represented uniquely.

31. Let the decimal expansion of the integer a be given by $a = (a_{n-1}a_{n-2}\ldots a_1a_0)_{10}$. Thus $a = 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \cdots + 10a_1 + a_0$. Since $10 \equiv 1 \pmod 3$, we have $a \equiv a_{n-1} + a_{n-2} + \cdots + a_1 + a_0 \pmod 3$. Therefore $a \equiv 0 \pmod 3$ if and only if the sum of the digits is congruent to 0 (mod 3). Since being divisible by 3 is the same as being congruent to 0 (mod 3), we have proved that a positive integer is divisible by 3 if and only if the sum of its decimal digits is divisible by 3.

33. Let the binary expansion of the positive integer a be given by $a = (a_{n-1}a_{n-2}\ldots a_1a_0)_2$. Thus $a = a_0 + 2a_1 + 2^2a_2 + \cdots + 2^{n-1}a_{n-1}$. Since $2^2 \equiv 1 \pmod 3$, we see that $2^k \equiv 1 \pmod 3$ when k is even, and $2^k \equiv 2 \equiv -1 \pmod 3$ when k is odd. Therefore we have $a \equiv a_0 - a_1 + a_2 - a_3 + \cdots \pm a_{n-1} \pmod 3$. Thus $a \equiv 0 \pmod 3$ if and only if the sum of the binary digits in the even-numbered positions minus the sum of the binary digits in the odd-numbered positions is congruent to 0 modulo 3. Since being divisible by 3 is the same as being congruent to 0 (mod 3), our proof is complete.

35. **a)** Since the leading bit is a 1, this represents a negative number. The binary expansion of the absolute value of this number is the complement of the rest of the expansion, namely the complement of 1001, or 0110. Since $(0110)_2 = 6$, the answer is -6.

b) Since the leading bit is a 0, this represents a positive number, namely the number whose binary expansion is the rest of this string, 1101. Since $(1101)_2 = 13$, the answer is 13.

c) The answer is the negative of the complement of 0001, namely $-(1110)_2 = -14$.

d) $-(0000)_2 = 0$; note that 0 has two different representations, 0000 and 1111

37. We must assume that the sum actually represents a number in the appropriate range. Assume that n bits are being used, so that numbers strictly between -2^{n-1} and 2^{n-1} can be represented. The answer is almost, but not quite, that to obtain the one's complement representation of the sum of two numbers, we simply add the two strings representing these numbers using Algorithm 3. Instead, after performing this operation, there may be a carry out of the left-most column; in such a case, we then add 1 more to the answer. For example, suppose that $n = 4$; then numbers from -7 to 7 can be represented. To add -5 and 3, we add 1010 and 0011, obtaining 1101; there was no carry out of the left-most column. Since 1101 is the one's complement representation of -2, we have the correct answer. On the other hand, to add -4 and -3, we add 1011 and 1100, obtaining 1 0111. The 1 that was carried out of the left-most column is instead added to 0111, yielding 1000, which is the one's complement representation of -7. A proof that this method works entails considering the various cases determined by the signs and magnitudes of the addends.

39. If m is positive (or 0), then the leading bit (a_{n-1}) is 0, so the formula reads simply $m = \sum_{i=0}^{n-2} a_i 2^i$, which is clearly correct, since this is the binary expansion of m. (See Section 2.4 for the meaning of summation notation. This symbolism is a shorthand way of writing $a_0 + 2a_1 + 4a_2 + \cdots + 2^{n-2}a_{n-2}$.) Now suppose that m is negative. The one's complement expansion for m has its leading bit equal to 1. By the definition of one's complement, we can think of obtaining the remaining $n-1$ bits by subtracting $-m$, written in binary, from $111\ldots1$ (with $n-1$ 1's), since subtracting a bit from 1 is the same thing as complementing it. Equivalently, if we view the bit string $(a_{n-2}a_{n-1}\ldots a_0)$ as a binary number, then it represents $(2^{n-1} - 1) - (-m)$. In

symbols, this says that $(2^{n-1}-1)-(-m)=\sum_{i=0}^{n-2}a_i2^i$. Solving for m gives us the equation we are trying to prove (since $a_{n-1}=1$).

41. Following the definition, if the first bit is a 0, then we just evaluate the binary expansion. If the first bit is a 1, then we find what number x is represented by the remaining four bits in binary; the answer is then $-(2^4-x)$.

a) Since the first bit is a 1, and the remaining bits represent the number 9, this string represents the number $-(2^4-9)=-7$.

b) Since the first bit is a 0 and this is just the binary expansion of 13, the answer is 13.

c) Since the first bit is a 1, and the remaining bits represent the number 1, this string represents the number $-(2^4-1)=-15$.

d) Since the first bit is a 1, and the remaining bits represent the number 15, this string represents the number $-(2^4-15)=-1$. Note that 10000 would represent $-(2^4-0)=-16$, so in fact we can represent one extra negative number than positive number with this notation.

43. The nice thing about two's complement arithmetic is that we can just work as if it were all in base 2, since $-x$ (where x is positive) is represented by 2^n-x; in other words, modulo 2^n, negative numbers represent themselves. However, if overflow occurs, then we must recognize an error. Let us look at some examples, where $n=5$ (i.e., we use five bits to represent numbers between -15 and 15). To add $5+7$, we write $00101+00111=01100$ in base 2, which gives us the correct answer, 12. However, if we try to add $13+7$ we obtain $01101+00111=10100$, which represents -12, rather than 20, so we report an overflow error. (Of course these two numbers are congruent modulo 32.) Similarly, for $5+(-7)$, we write $00101+11001=11110$ in base 2, and 11110 is the two's complement representation of -2, the right answer. For $(-5)+(-7)$, we write $11011+11001=110100$ in base 2; if we ignore the extra 1 in the left-most column (which doesn't exist), then this is the two's complement representation of -12, again the right answer. To summarize, to obtain the two's complement representation of the sum of two integers given in two's complement representation, add them as if they were binary integers, and ignore any carry out of the left-most column. However, if the left-most digits of the two addends agree and the left-most digit of the answer is different from their common value, then an overflow has occurred, and the answer is not valid.

45. If m is positive (or 0), then the leading bit (a_{n-1}) is 0, so the formula reads simply $m=\sum_{i=0}^{n-2}a_i2^i$, which is clearly correct, since this is the binary expansion of m. (See Section 2.4 for the meaning of summation notation. This symbolism is a shorthand way of writing $a_0+2a_1+4a_2+\cdots+2^{n-2}a_{n-2}$.) Now suppose that m is negative. The two's complement expansion for m has its leading bit equal to 1. By the definition of two's complement, the remaining $n-1$ bits are the binary expansion of $2^{n-1}-(-m)$. In symbols, this says that $2^{n-1}-(-m)=\sum_{i=0}^{n-2}a_i2^i$. Solving for m gives us the equation we are trying to prove (since $a_{n-1}=1$).

47. Clearly we need $4n$ digits, four for each digit of the decimal representation.

49. To find the Cantor expansion, we will work from left to right. Thus the first step will be to find the largest number n whose factorial is still less than or equal to the given positive integer x. Then we determine the digits in the expansion, starting with a_n and ending with a_1.

procedure *Cantor*(x : positive integer)
$n := 1$; *factorial* $:= 1$
while $(n+1) \cdot$ *factorial* $\leq x$
    $n := n + 1$
    factorial $:=$ *factorial* $\cdot\, n$
{at this point we know that there are n digits in the expansion}
$y := x$ {this is just so we do not destroy the original input}
while $n > 0$
    $a_n := \lfloor y/\textit{factorial} \rfloor$
    $y := y - a_n \cdot$ *factorial*
    factorial $:=$ *factorial*$/n$
    $n := n - 1$
{we are done: $x = a_n n! + a_{n-1}(n-1)! + \cdots + a_2 2! + a_1 1!$}

51. Note that $n = 5$. Initially the carry is $c = 0$, and we start the **for** loop with $j = 0$. Since $a_0 = 1$ and $b_0 = 0$, we set d to be $\lfloor (1+0+0)/2 \rfloor = 0$; then $s_0 = 1+0+0-2\cdot 0$, which equals 1, and finally $c = 0$. At the end of the first pass, then, the right-most digit of the answer has been determined (it's a 1), and there is a carry of 0 into the next column.

Now $j = 1$, and we compute d to be $\lfloor (a_1 + b_1 + c)/2 \rfloor = \lfloor (1+1+0)/2 \rfloor = 1$; whereupon s_1 becomes $1+1+0-2\cdot 1 = 0$, and c is set to 1. Thus far we have determined that the last two bits of the answer are 01 (from left to right), and there is a carry of 1 into the next column.

The next three passes through the loop are similar. As a result of the pass when $j = 2$ we set $d = 1$, $s_2 = 0$, and then $c = 1$. When $j = 3$, we obtain $d = 1$, $s_3 = 0$, and then $c = 1$. Finally, when $j = 4$, we obtain $d = 1$, $s_4 = 1$, and then $c = 1$. At this point the loop is terminated, and when we execute the final step, $s_5 = 1$. Thus the answer is 11 0001.

53. We will assume that the answer is not negative, since otherwise we would need something like the one's complement representation. The algorithm is similar to the algorithm for addition, except that we need to borrow instead of carry. Rather than trying to incorporate the two cases (borrow or no borrow) into one, as was done in the algorithm for addition, we will use an **if... then** statement to treat the cases separately. The notation is the usual one: $a = (a_{n-1} \ldots a_1 a_0)_2$ and $b = (b_{n-1} \ldots b_1 b_0)_2$

procedure *subtract*(a, b : nonnegative integers)
borrow $:= 0$
for $j := 0$ **to** $n - 1$
    if $a_j -$ *borrow* $\geq b_j$ **then**
        $s_j := a_j -$ *borrow* $- b_j$
        borrow $:= 0$
    else
        $s_j := a_j + 2 -$ *borrow* $- b_j$
        borrow $:= 1$
{assuming $a \geq b$, we have $a - b = (s_{n-1} s_{n-2} \ldots s_1 s_0)_2$}

55. To determine which of two integers (we assume they are nonnegative), given in binary as $a = (a_{n-1} \ldots a_1 a_0)_2$ and $b = (b_{n-1} \ldots b_1 b_0)_2$, is larger, we need to compare digits from the most significant end ($i = n-1$) to the least ($i = 0$), stopping if and when we find a difference. For variety here we record the answer as a character string; in most applications it would probably be better to set *compare* to one of three code values (such as -1, 1, and 0) to indicate which of the three possibilities held.

```
procedure compare(a, b : nonnegative integers)
i := n − 1
while i > 0 and a_i = b_i
        i := i − 1
if a_i > b_i then answer := "a > b"
else if a_i < b_i then answer := "a < b"
else answer := "a = b"
return answer
```

57. There is one division for each pass through the **while** loop. Also, each pass generates one digit in the base b expansion. Thus the number of divisions equals the number of digits in the base b expansion of n. This is just $\lfloor \log_b n \rfloor + 1$ (for example, numbers from 10 to 99, inclusive, have common logarithms in the interval $[1, 2)$). Therefore exactly $\lfloor \log_b n \rfloor + 1$ divisions are required, and this is $O(\log n)$. (We are counting only the actual division operation in the statement $q := \lfloor q/b \rfloor$. If we also count the implied division in the statement $a_k := q \bmod b$, then there are twice as many as we computed here. The big-O estimate is the same, of course.)

59. The only time-consuming part of the algorithm is the **while** loop, which is iterated q times. The work done inside is a subtraction of integers no bigger than a, which has $\log a$ bits. The results now follows from Example 9.

SECTION 4.3 Primes and Greatest Common Divisors

The prime numbers are the building blocks for the natural numbers in terms of multiplication, just as the elements (like carbon, oxygen, or uranium) are the building blocks of all matter. Just as we can put two hydrogen atoms and one oxygen atom together to form water, every composite natural number is uniquely constructed by multiplying together prime numbers. Analyzing numbers in terms of their prime factorizations allows us to solve many problems, such as finding greatest common divisors. Prime numbers have fascinated people for millennia, and many easy-to-state questions about them remain unanswered. Students interested in pursuing these topics more should definitely consider taking a course in number theory.

1. In each case we can just use trial division up to the square root of the number being tested.

a) Since $21 = 3 \cdot 7$, we know that 21 is not prime.

b) Since $2 \not| 29$, $3 \not| 29$, and $5 \not| 29$, we know that 29 is prime. We needed to check for prime divisors only up to $\sqrt{29}$, which is less than 6.

c) Since $2 \not| 71$, $3 \not| 71$, $5 \not| 71$, and $7 \not| 71$, we know that 71 is prime.

d) Since $2 \not| 97$, $3 \not| 97$, $5 \not| 97$, and $7 \not| 97$, we know that 97 is prime.

e) Since $111 = 3 \cdot 37$, we know that 111 is not prime.

f) Since $143 = 11 \cdot 13$, we know that 143 is not prime.

3. In each case we can use trial division, starting with the smallest prime and increasing to the next prime once we find that a given prime no longer is a divisor of what is left. A calculator comes in handy. Alternatively, one could use a factor tree.

a) We note that 2 is a factor of 88, and the quotient upon division by 2 is 44. We divide by 2 again, and then again, leaving a quotient of 11. Since 11 is prime, we are done, and we have found the prime factorization: $88 = 2^3 \cdot 11$.

b) $126 = 2 \cdot 63 = 2 \cdot 3 \cdot 21 = 2 \cdot 3 \cdot 3 \cdot 7 = 2 \cdot 3^2 \cdot 7$

c) $729 = 3 \cdot 243 = 3 \cdot 3 \cdot 81 = 3 \cdot 3 \cdot 3 \cdot 27 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 9 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 = 3^6$

d) $1001 = 7 \cdot 143 = 7 \cdot 11 \cdot 13$

e) $1111 = 11 \cdot 101$ (we know that 101 is prime because we have already tried all prime factors less than $\sqrt{101}$)
f) $909090 = 2 \cdot 454545 = 2 \cdot 3 \cdot 151515 = 2 \cdot 3 \cdot 3 \cdot 50505 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 16835 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 3367 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 481 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 37 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 37$

5. $10! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 2 \cdot 3 \cdot 2^2 \cdot 5 \cdot (2 \cdot 3) \cdot 7 \cdot 2^3 \cdot 3^2 \cdot (2 \cdot 5) = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$

7. The input is an integer n greater than 1. We try dividing it by all integers from 2 to $\sqrt{n}$, and if we find one that leaves no remainder then we know that n is not prime. The pseudocode below accomplishes this.

```
procedure primetester(n : integer greater than 1)
isprime := true
d := 2
while isprime and d ≤ √n
        if n mod d = 0 then isprime := false
        else d := d + 1
return isprime
```

9. We use what we know about factoring from algebra. In particular, we know that $a^m + 1 = (a+1)(a^{m-1} - a^{m-2} + a^{m-3} + \cdots - 1)$. (Notice that this works if and only if m is odd, because the final sign has to be a plus sign.) Because a and m are both greater than 1, we know that $1 < a + 1 < a^m + 1$. This provides a factoring of $a^m + 1$ into two proper factors, so $a^m + 1$ is composite.

11. We give a proof by contradiction. Suppose that in fact $\log_2 3$ is the rational number p/q, where p and q are integers. Since $\log_2 3 > 0$, we can assume that p and q are positive. Translating the equation $\log_2 3 = p/q$ into its exponential equivalent, we obtain $3 = 2^{p/q}$. Raising both sides to the q^{th} power yields $3^q = 2^p$. Now this is a violation of the Fundamental Theorem of Arithmetic, since it gives two different prime factorizations of the same number. Hence our assumption (that $\log_2 3$ is rational) must be wrong, and we conclude that $\log_2 3$ is irrational.

13. This is simply an existence statement. To prove that it is true, we need only exhibit the primes. Indeed, 3, 5, and 7 satisfy the conditions. (Actually, this is the only example, and a harder problem is to prove that there are no others.)

15. The prime factors of 30 are 2, 3, and 5. Thus we are looking for positive integers less than 30 that have none of these as prime factors. Since the smallest prime number other than these is 7, and 7^2 is already greater than 30, in fact only primes (and the number 1) will satisfy this condition. Therefore the answer is 1, 7, 11, 13, 17, 19, 23, and 29.

17. **a)** Since $\gcd(11, 15) = 1$, $\gcd(11, 19) = 1$, and $\gcd(15, 19) = 1$, these three numbers are pairwise relatively prime.
b) Since $\gcd(15, 21) = 3 > 1$, these three numbers are not pairwise relatively prime.
c) Since $\gcd(12, 17) = 1$, $\gcd(12, 31) = 1$, $\gcd(12, 37) = 1$, $\gcd(17, 31) = 1$, $\gcd(17, 37) = 1$, and $\gcd(31, 37) = 1$, these four numbers are pairwise relatively prime. (Indeed, the last three are primes, and the prime factors of the first are 2 and 3.)
d) Again, since no two of 7, 8, 9, and 11 have a common factor greater than 1, this set is pairwise relatively prime.

19. The identity shown in the hint is valid, as can be readily seen by multiplying out the right-hand side (all the terms cancel—telescope—except for 2^{ab} and -1). We will prove the assertion by proving its contrapositive. Suppose that n is *not* prime. Then by definition $n = ab$ for some integers a and b each greater than 1. Since $a > 1$, $2^a - 1$, the first factor in the suggested identity, is greater than 1. Clearly the second factor is greater than 1. Thus $2^n - 1 = 2^{ab} - 1$ is the product of two integers each greater than 1, so it is not prime.

21. We compute $\phi(n)$ here by enumerating the set of positive integers less than n that are relatively prime to n.
a) $\phi(4) = |\{1,3\}| = 2$ **b)** $\phi(10) = |\{1,3,7,9\}| = 4$
c) $\phi(13) = |\{1,2,3,4,5,6,7,8,9,10,11,12\}| = 12$

23. All the positive integers less than or equal to p^k (and there are clearly p^k of them) are less than p^k and relatively prime to p^k unless they are a multiple of p. Since the fraction $1/p$ of them are multiples of p, we have $\phi(p^k) = p^k(1 - 1/p) = p^k - p^{k-1}$.

25. To find the greatest common divisor of two numbers whose prime factorizations are given, we just need to take the smaller exponent for each prime.
a) The first number has no prime factors of 2, so the gcd has no 2's. Since the first number has seven factors of 3, but the second number has only five, the gcd has five factors of 3. Similarly the gcd has a factor of 5^3. So the gcd is $3^5 \cdot 5^3$.
b) These numbers have no common prime factors, so the gcd is 1. **c)** 23^{17} **d)** $41 \cdot 43 \cdot 53$
e) These numbers have no common prime factors, so the gcd is 1.
f) The gcd of any positive integer and 0 is that integer, so the answer is 1111.

27. To find the least common multiple of two numbers whose prime factorizations are given, we just need to take the larger exponent for each prime.
a) The first number has no prime factors of 2 but the second number has 11 of them, so the lcm has 11 factors of 2. Since the first number has seven factors of 3 and the second number has five, the lcm has seven factors of 3. Similarly the lcm has a factor of 5^9 and a factor of 7^3. So the lcm is $2^{11} \cdot 3^7 \cdot 5^9 \cdot 7^3$.
b) These numbers have no common prime factors, so the lcm is their product, $2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$.
c) 23^{31} **d)** $41 \cdot 43 \cdot 53$ **e)** $2^{12} \cdot 3^{13} \cdot 5^{17} \cdot 7^{21}$, as in part **(b)**
f) It makes no sense to ask for a positive multiple of 0, so this question has no answer. Least common multiples are defined only for positive integers.

29. First we find the prime factorizations: $92928 = 2^8 \cdot 3 \cdot 11^2$ and $123552 = 2^5 \cdot 3^3 \cdot 11 \cdot 13$. Therefore $\gcd(92928, 123552) = 2^5 \cdot 3 \cdot 11 = 1056$ and $\text{lcm}(92928, 123552) = 2^8 \cdot 3^3 \cdot 11^2 \cdot 13 = 10872576$. The requested products are $(2^5 \cdot 3 \cdot 11) \cdot (2^8 \cdot 3^3 \cdot 11^2 \cdot 13)$ and $(2^8 \cdot 3 \cdot 11^2) \cdot (2^5 \cdot 3^3 \cdot 11 \cdot 13)$, both of which are $2^{13} \cdot 3^4 \cdot 11^3 \cdot 13 = 11{,}481{,}440{,}256$.

31. The important observation to make here is that the smaller of any two numbers plus the larger of the two numbers is always equal to the sum of the two numbers. Since the exponent of the prime p in $\gcd(a,b)$ is the smaller of the exponents of p in a and in b, and since the exponent of the prime p in $\text{lcm}(a,b)$ is the larger of the exponents of p in a and in b, the exponent of p in $\gcd(a,b)\text{lcm}(a,b)$ is the sum of the smaller and the larger of these two values. Therefore by the observation, it equals the sum of the two values themselves, which is clearly equal to the exponent of p in ab. Since this is true for every prime p, we conclude that $\gcd(a,b)\text{lcm}(a,b)$ and ab have the same prime factorizations and are therefore equal.

33. **a)** By Lemma 1, $\gcd(12,18)$ is the same as the gcd of the smaller of these two numbers (12) and the remainder when the larger (18) is divided by the smaller. In this case the remainder is 6, so $\gcd(12,18) = \gcd(12,6)$. Now $\gcd(12,6)$ is the same as the gcd of the smaller of *these* two numbers (6) and the remainder when the larger (12) is divided by the smaller, namely 0. This gives $\gcd(12,6) = \gcd(6,0)$. But $\gcd(x,0) = x$ for all positive integers, so $\gcd(6,0) = 6$. Thus the answer is 6. In brief (the form we will use for the remaining parts), $\gcd(12,18) = \gcd(12,6) = \gcd(6,0) = 6$.
b) $\gcd(111,201) = \gcd(111,90) = \gcd(90,21) = \gcd(21,6) = \gcd(6,3) = \gcd(3,0) = 3$

c) $\gcd(1001, 1331) = \gcd(1001, 330) = \gcd(330, 11) = \gcd(11, 0) = 11$

d) $\gcd(12345, 54321) = \gcd(12345, 4941) = \gcd(4941, 2463) = \gcd(2463, 15) = \gcd(15, 3) = \gcd(3, 0) = 3$

e) $\gcd(1000, 5040) = \gcd(1000, 40) = \gcd(40, 0) = 40$

f) $\gcd(9888, 6060) = \gcd(6060, 3828) = \gcd(3828, 2232) = \gcd(2232, 1596) = \gcd(1596, 636) = \gcd(636, 324) = \gcd(324, 312) = \gcd(312, 12) = \gcd(12, 0) = 12$

35. In carrying out the Euclidean algorithm on this data, we divide successively by 55, 34, 21, 13, 8, 5, 3, 2, and 1, so nine divisions are required.

37. One can compute $\gcd(2^a - 1, 2^b - 1)$ using the Euclidean algorithm. Let us look at what happens when we do so. If $b = 1$, then the answer is just 1, which is the same as $2^{\gcd(a,b)} - 1$ in this case. Otherwise, we reduce the problem to computing $\gcd(2^b - 1, (2^a - 1) \bmod (2^b - 1))$. Now from Exercise 36 we know that this second argument equals $2^{a \bmod b} - 1$. Therefore the exponents involved in the continuing calculation are b and $a \bmod b$—exactly the same quantities that are involved in computing $\gcd(a, b)$! It follows that when the process terminates, the answer must be $2^{\gcd(a,b)} - 1$, as desired.

39. **a)** This first one is easy to do by inspection. Clearly 10 and 11 are relatively prime, so their greatest common divisor is 1, and $1 = 11 - 10 = (-1) \cdot 10 + 1 \cdot 11$.

b) In order to find the coefficients s and t such that $21s + 44t = \gcd(21, 44)$, we carry out the steps of the Euclidean algorithm.

$$44 = 2 \cdot 21 + 2$$
$$21 = 10 \cdot 2 + 1$$

Then we work up from the bottom, expressing the greatest common divisor (which we have just seen to be 1) in terms of the numbers involved in the algorithm, namely 44, 21, and 2. In particular, the last equation tells us that $1 = 21 - 10 \cdot 2$, so that we have expressed the gcd as a linear combination of 21 and 2. But now the first equation tells us that $2 = 44 - 2 \cdot 21$; we plug this into our previous equation and obtain

$$1 = 21 - 10 \cdot (44 - 2 \cdot 21) = 21 \cdot 21 - 10 \cdot 44.$$

Thus we have expressed 1 as a linear combination (with integer coefficients) of 21 and 44, namely $\gcd(21, 44) = 21 \cdot 21 + (-10) \cdot 44$.

c) Again, we carry out the Euclidean algorithm. Since $48 = 1 \cdot 36 + 12$, and $12 \mid 36$, we know that $\gcd(36, 48) = 12$. From the equation shown here, we can immediately write $12 = (-1) \cdot 36 + 48$.

d) The calculation of the greatest common divisor takes several steps:

$$55 = 1 \cdot 34 + 21$$
$$34 = 1 \cdot 21 + 13$$
$$21 = 1 \cdot 13 + 8$$
$$13 = 1 \cdot 8 + 5$$
$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$

Then we need to work our way back up, successively plugging in for the remainders determined in this

calculation:

$$\begin{aligned}1 &= 3 - 2\\ &= 3 - (5 - 3) = 2 \cdot 3 - 5\\ &= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5\\ &= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13\\ &= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13\\ &= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34\\ &= 13 \cdot (55 - 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34\end{aligned}$$

e) Here are the two calculations—down to the gcd using the Euclidean algorithm, and then back up by substitution until we have expressed the gcd as the desired linear combination of the original numbers.

$$\begin{aligned}213 &= 1 \cdot 117 + 96\\ 117 &= 1 \cdot 96 + 21\\ 96 &= 4 \cdot 21 + 12\\ 21 &= 1 \cdot 12 + 9\\ 12 &= 1 \cdot 9 + 3\end{aligned}$$

Since $3 \mid 9$, we have $\gcd(117, 213) = 3$.

$$\begin{aligned}3 &= 12 - 9\\ &= 12 - (21 - 12) = 2 \cdot 12 - 21\\ &= 2 \cdot (96 - 4 \cdot 21) - 21 = 2 \cdot 96 - 9 \cdot 21\\ &= 2 \cdot 96 - 9 \cdot (117 - 96) = 11 \cdot 96 - 9 \cdot 117\\ &= 11 \cdot (213 - 117) - 9 \cdot 117 = 11 \cdot 213 - 20 \cdot 117\end{aligned}$$

f) Clearly $\gcd(0, 223) = 223$, so we can write $223 = s \cdot 0 + 1 \cdot 223$ for any integer s.

g) Here are the two calculations—down to the gcd using the Euclidean algorithm, and then back up by substitution until we have expressed the gcd as the desired linear combination of the original numbers.

$$\begin{aligned}2347 &= 19 \cdot 123 + 10\\ 123 &= 12 \cdot 10 + 3\\ 10 &= 3 \cdot 3 + 1\end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}1 &= 10 - 3 \cdot 3\\ &= 10 - 3 \cdot (123 - 12 \cdot 10) = 37 \cdot 10 - 3 \cdot 123\\ &= 37 \cdot (2347 - 19 \cdot 123) - 3 \cdot 123 = 37 \cdot 2347 - 706 \cdot 123\end{aligned}$$

h) Here are the two calculations—down to the gcd using the Euclidean algorithm, and then back up by substitution until we have expressed the gcd as the desired linear combination of the original numbers.

$$\begin{aligned}4666 &= 3454 + 1212\\ 3454 &= 2 \cdot 1212 + 1030\\ 1212 &= 1030 + 182\\ 1030 &= 5 \cdot 182 + 120\\ 182 &= 120 + 62\\ 120 &= 62 + 58\\ 62 &= 58 + 4\\ 58 &= 14 \cdot 4 + 2\end{aligned}$$

Since $2 \mid 4$, the greatest common divisor is 2.

$$\begin{aligned}
2 &= 58 - 14 \cdot 4 \\
&= 58 - 14 \cdot (62 - 58) = 15 \cdot 58 - 14 \cdot 62 \\
&= 15 \cdot (120 - 62) - 14 \cdot 62 = 15 \cdot 120 - 29 \cdot 62 \\
&= 15 \cdot 120 - 29 \cdot (182 - 120) = 44 \cdot 120 - 29 \cdot 182 \\
&= 44 \cdot (1030 - 5 \cdot 182) - 29 \cdot 182 = 44 \cdot 1030 - 249 \cdot 182 \\
&= 44 \cdot 1030 - 249 \cdot (1212 - 1030) = 293 \cdot 1030 - 249 \cdot 1212 \\
&= 293 \cdot (3454 - 2 \cdot 1212) - 249 \cdot 1212 = 293 \cdot 3454 - 835 \cdot 1212 \\
&= 293 \cdot 3454 - 835 \cdot (4666 - 3454) = 1128 \cdot 3454 - 835 \cdot 4666
\end{aligned}$$

i) Here are the two calculations—down to the gcd using the Euclidean algorithm, and then back up by substitution until we have expressed the gcd as the desired linear combination of the original numbers.

$$\begin{aligned}
11111 &= 9999 + 1112 \\
9999 &= 8 \cdot 1112 + 1103 \\
1112 &= 1103 + 9 \\
1103 &= 122 \cdot 9 + 5 \\
9 &= 5 + 4 \\
5 &= 4 + 1
\end{aligned}$$

Thus 1 is the greatest common divisor.

$$\begin{aligned}
1 &= 5 - 4 \\
&= 5 - (9 - 5) = 2 \cdot 5 - 9 \\
&= 2 \cdot (1103 - 122 \cdot 9) - 9 = 2 \cdot 1103 - 245 \cdot 9 \\
&= 2 \cdot 1103 - 245 \cdot (1112 - 1103) = 247 \cdot 1103 - 245 \cdot 1112 \\
&= 247 \cdot (9999 - 8 \cdot 1112) - 245 \cdot 1112 = 247 \cdot 9999 - 2221 \cdot 1112 \\
&= 247 \cdot 9999 - 2221 \cdot (11111 - 9999) = 2468 \cdot 9999 - 2221 \cdot 11111
\end{aligned}$$

41. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1 = 0$, $r_2 = 26$, $q_2 = 3$, $r_3 = 13$, $q_3 = 2$. Note that $n = 3$. Thus we compute the successive s's and t's as follows, using the given recurrences:

$s_2 = s_0 - q_1 s_1 = 1 - 0 \cdot 0 = 1,$ $\qquad$ $t_2 = t_0 - q_1 t_1 = 0 - 0 \cdot 1 = 0$

$s_3 = s_1 - q_2 s_2 = 0 - 3 \cdot 1 = -3,$ $\qquad$ $t_3 = t_1 - q_2 t_2 = 1 - 3 \cdot 0 = 1$

Thus we have $s_3 a + t_3 b = (-3) \cdot 26 + 1 \cdot 91 = 13$, which is $\gcd(26, 91)$.

43. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1 = 1$, $r_2 = 55$, $q_2 = 1$, $r_3 = 34$, $q_3 = 1$, $r_4 = 21$, $q_4 = 1$, $r_5 = 13$, $q_5 = 1$, $r_6 = 8$, $q_6 = 1$, $r_7 = 5$, $q_7 = 1$, $r_8 = 3$, $q_8 = 1$, $r_9 = 2$, $q_9 = 1$, $r_{10} = 1$, $q_{10} = 2$. Note that $n = 10$. Thus we compute the successive s's and t's as follows, using the given recurrences:

$s_2 = s_0 - q_1 s_1 = 1 - 1 \cdot 0 = 1,$ $\qquad$ $t_2 = t_0 - q_1 t_1 = 0 - 1 \cdot 1 = -1$

$s_3 = s_1 - q_2 s_2 = 0 - 1 \cdot 1 = -1,$ $\qquad$ $t_3 = t_1 - q_2 t_2 = 1 - 1 \cdot (-1) = 2$

$s_4 = s_2 - q_3 s_3 = 1 - 1 \cdot (-1) = 2,$ $\qquad$ $t_4 = t_2 - q_3 t_3 = -1 - 1 \cdot 2 = -3$

$s_5 = s_3 - q_4 s_4 = -1 - 1 \cdot 2 = -3,$ $\qquad$ $t_5 = t_3 - q_4 t_4 = 2 - 1 \cdot (-3) = 5$

$s_6 = s_4 - q_5 s_5 = 2 - 1 \cdot (-3) = 5,$ $\qquad$ $t_6 = t_4 - q_5 t_5 = -3 - 1 \cdot 5 = -8$

$s_7 = s_5 - q_6 s_6 = -3 - 1 \cdot 5 = -8,$ $\qquad$ $t_7 = t_5 - q_6 t_6 = 5 - 1 \cdot (-8) = 13$

$s_8 = s_6 - q_7 s_7 = 5 - 1 \cdot (-8) = 13$, $t_8 = t_6 - q_7 t_7 = -8 - 1 \cdot 13 = -21$
$s_9 = s_7 - q_8 s_8 = -8 - 1 \cdot 13 = -21$, $t_9 = t_7 - q_8 t_8 = 13 - 1 \cdot (-21) = 34$
$s_{10} = s_8 - q_9 s_9 = 13 - 1 \cdot (-21) = 34$, $t_{10} = t_8 - q_9 t_9 = -21 - 1 \cdot 34 = -55$

Thus we have $s_{10}a + t_{10}b = 34 \cdot 144 + (-55) \cdot 89 = 1$, which is $\gcd(144, 89)$.

45. We start with the pseudocode for the Euclidean algorithm (Algorithm 1) and add variables to keep track of the s and t values. We need three of them, since the new s depends on the previous two s's, and similarly for t. We also need to keep track of q.

procedure *extended Euclidean*(a, b : positive integers)
$x := a$
$y := b$
$oldolds := 1$
$olds := 0$
$oldoldt := 0$
$oldt := 1$
while $y \neq 0$
    $q := x$ **div** y
    $r := x$ **mod** y
    $x := y$
    $y := r$
    $s := oldolds - q \cdot olds$
    $t := oldoldt - q \cdot oldt$
    $oldolds := olds$
    $oldoldt := oldt$
    $olds := s$
    $oldt := t$
{ $\gcd(a, b)$ is x, and the Bézout coefficients are given by $(oldolds)a + (oldoldt)b = x$ }

47. Obviously there are no definitive answers to these problems, but we present below a reasonable and satisfying rule for forming the sequence in each case.

a) There are 1's in the prime locations and 0's elsewhere. In other words, the n^{th} term of the sequence is 1 if n is a prime number and 0 otherwise.

b) The suspicious 2's occurring every other term and the appearance of the 11 and 13 lead us to discover that the n^{th} term is the smallest prime factor of n (and is 1 when $n = 1$).

c) The n^{th} term is the number of positive divisors of n. For example, the twelfth term is 6, since 12 has the positive divisors 1, 2, 3, 4, 6, and 12. A tip-off to get us going in the right direction is that there are 2's in the prime locations.

d) Perhaps the composer of the problem had something else in mind, but one rule here is that the n^{th} term is 0 if and only if n has a repeated prime factor; the 1's occur at locations for which n is "square-free" (has no factor, other than 1, that is a perfect square). For example, 12 has the square 2^2, so the twelfth term is 0.

e) We note that all the terms (after the first one) are primes. This leads us to guess that the n^{th} term is the largest prime less than or equal to n (and is 1 when $n = 1$).

f) Each term comes from the one before it by multiplying by a certain number. The multipliers are 2, 3, 5, 7, 11, 13, 17, 19, and 23—the primes. So the rule seems to be that we obtain the next term from the n^{th} term by multiplying by the n^{th} prime number (and we start at 1). In other words, the n^{th} term is the product of the smallest $n - 1$ prime numbers.

49. Consider the product $n(n+1)(n+2)$ for some integer n. Since every second integer is even (divisible by 2), this product is divisible by 2. Since every third integer is divisible by 3, this product is divisible by 3. Therefore this product has both 2 and 3 in its prime factorization and is therefore divisible by $2 \cdot 3 = 6$.

51. It is hard to know how to get started on this problem. To some extent, mathematics is an experimental science, so it would probably be a good idea to compute $n^2 - 79n + 1601$ for several positive integer values of n to get a feel for what is happening. Using a computer, or at least a calculator, would be helpful. If we plug in $n = 1, 2, 3, 4,$ and 5, then we get the values 1523, 1447, 1373, 1301, and 1231, all of which are prime. This may lead us to believe that the proposition is true, but it gives us no clue as to how to prove it. Indeed, it seems as if it would be very hard to prove that this expression *always* produces a prime number, since being prime means the absence of nontrivial factors, and nothing in the expression seems to be very helpful in proving such a negative assertion. (The fact that we cannot factor it algebraically is irrelevant—in fact, if it factored algebraically, then it would essentially *never* be prime.) Perhaps we should try some more integers. If we do so, we find a lot more prime numbers, but we are still skeptical. Well, perhaps there is some way to arrange that this expression will have a factor. How about 1601? Well, yes! If we let $n = 1601$, then all three terms will have 1601 as a common factor, so that 1601 is a factor of the entire expression. In fact, $1601^2 - 79 \cdot 1601 + 1601 = 1601 \cdot 1523$. So we have found a counterexample after all, and the proposition is false. Note that this was not a problem in which we could proceed in a calm, calculated way from problem to solution. Mathematics is often like that—lots of false leads and approaches that get us nowhere, and then suddenly a burst of insight that solves the problem. (The smallest n for which this expression is not prime is $n = 80$; this gives the value $1681 = 41 \cdot 41$.)

53. Here is one way to find a composite term in the sequence. If we set $k = 1$, then we get $a + b$. That number is greater than 1, but it may not be composite. So let's increase k by $a + b$, which will have the effect of adding a multiple of $a + b$ to our previous answer, and we will therefore get a composite number, because $a + b$ will be a nontrivial factor of it. So setting $k = a + b + 1$ should work. Indeed, with that choice we have $ak + b = a(a + b + 1) + b = a^2 + ab + a + b$, which factors nicely as $(a + 1)(a + b)$. Since a and b are both positive integers, both factors are greater than 1, and we have our composite number.

55. Recall that the proof that there are infinitely many primes starts by assuming that there are only finitely many primes $p_1, p_2, \ldots, p_n$, and forming the number $p_1 p_2 \cdots p_n + 1$. This number is either prime or has a prime factor different from each of the primes $p_1, p_2, \ldots, p_n$; this shows that there are infinitely many primes. So, let us suppose that there are only finitely many primes of the form $4k+3$, namely $q_1, q_2, \ldots, q_n$, where $q_1 = 3$, $q_2 = 7$, and so on.

What number can we form that is not divisible by any of these primes, but that must be divisible by a prime of the form $4k + 3$? We might consider the number $4q_1 q_2 \cdots q_n + 3$. Unfortunately, this number is not prime, as it is is divisible by 3 (because $q_1 = 3$). Instead we consider the number $Q = 4q_1 q_2 \cdots q_n - 1$. Note that Q is of the form $4k + 3$ (where $k = q_1 q_2 \cdots q_n - 1$). If Q is prime, then we have found a prime of the desired form different from all those listed. If Q is not prime, then Q has at least one prime factor not in the list $q_1, q_2, \ldots, q_n$, because the remainder when Q is divided by q_j is $q_j - 1$, and $q_j - 1 \neq 0$. Therefore $q_j \nmid Q$ for $j = 1, 2, \ldots, n$. Because all odd primes are either of the form $4k + 1$ or of the form $4k + 3$, and the product of primes of the form $4k + 1$ is also of this form (because $(4k + 1)(4m + 1) = 4(4km + k + m) + 1$), there must be a factor of Q of the form $4k + 3$ different from the primes we listed. This complete the proof.

57. We need to show that this function is one-to-one and onto. In other words, if we are given a positive integer x, we must show that there is exactly one positive rational number m/n (written in lowest terms) such that $K(m/n) = x$. To do this, we factor x into its prime factorization and then read off the m and n such that $K(m/n) = x$. The primes that occur to even powers are the primes that occur in the prime factorization of m, with the exponents being half the corresponding exponents in x; and the primes that occur to odd powers are the primes that occur in the prime factorization of n, with the exponents being half of one more than the exponents in x. Since this uniquely determines m and n, there is one and only one fraction, in

lowest terms, that maps to x under K.

SECTION 4.4 Solving Congruences

Many of these exercises are reasonably straightforward calculations, but the amount of arithmetic involved in some of them can be formidable. Look at the worked out examples in the text if you need help getting the hang of it. The theoretical exercises, such as #18 and #19 give you a good taste of the kinds of proofs in an elementary number theory course.

1. We simply need to show that $15 \cdot 7 \equiv 1 \pmod{26}$, or in other words, that $15 \cdot 7 - 1$ is divisible by 26. But this quantity is 104, which is $26 \cdot 4$.

3. We want to find an integer k such that $4k$ is 1 greater than a multiple of 9. We compute $4 \cdot 1 = 4 = 0 \cdot 9 + 4$, $4 \cdot 2 = 8 = 0 \cdot 9 + 8$, $4 \cdot 3 = 12 = 1 \cdot 9 + 3$, $4 \cdot 4 = 16 = 1 \cdot 9 + 7$, $4 \cdot 5 = 20 = 2 \cdot 9 + 2$, $4 \cdot 6 = 24 = 2 \cdot 9 + 6$, $4 \cdot 7 = 28 = 3 \cdot 9 + 1$. Therefore an inverse of 4 modulo 9 is 7.

5. **a)** Following the procedure of Example 2, we carry out the Euclidean algorithm to find $\gcd(4, 9)$:

$$9 = 2 \cdot 4 + 1$$
$$4 = 4 \cdot 1$$

Then we work backwards to rewrite the gcd (the last nonzero remainder, which is 1 here) in terms of 4 and 9:

$$1 = 9 - 2 \cdot 4$$

Therefore the Bézout coefficients of 9 and 4 are 1 and -2, respectively. The coefficient of 4 is our desired answer, namely -2, which is the same as 7 modulo 9. Note that this agrees with our answer in Exercise 3.

b) We proceed as above:

$$141 = 7 \cdot 19 + 8$$
$$19 = 2 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1$$

Then we work backwards to rewrite the gcd (the last nonzero remainder, which is 1 here) in terms of 141 and 19:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (8 - 2 \cdot 3) = 3 \cdot 3 - 1 \cdot 8 \\ &= 3 \cdot (19 - 2 \cdot 8) - 1 \cdot 8 = 3 \cdot 19 - 7 \cdot 8 \\ &= 3 \cdot 19 - 7 \cdot (141 - 7 \cdot 19) = (-7) \cdot 141 + 52 \cdot 19 \end{aligned}$$

Therefore the Bézout coefficient of 19 is 52, and that is an inverse of 19 modulo 141.

c) We proceed as above:

$$89 = 1 \cdot 55 + 34$$
$$55 = 1 \cdot 34 + 21$$
$$34 = 1 \cdot 21 + 13$$
$$21 = 1 \cdot 13 + 8$$
$$13 = 1 \cdot 8 + 5$$
$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 1 \cdot 2$$

Then we work backwards to rewrite the gcd (the last nonzero remainder, which is 1 here) in terms of 89 and 55:

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (5 - 1 \cdot 3) = 2 \cdot 3 - 1 \cdot 5 \\
&= 2 \cdot (8 - 1 \cdot 5) - 1 \cdot 5 = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (13 - 1 \cdot 8) = 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot (21 - 1 \cdot 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot (34 - 1 \cdot 21) = 13 \cdot 21 - 8 \cdot 34 \\
&= 13 \cdot (55 - 1 \cdot 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34 \\
&= 13 \cdot 55 - 21 \cdot (89 - 1 \cdot 55) = 34 \cdot 55 - 21 \cdot 89
\end{aligned}$$

Therefore the Bézout coefficient of 55 is 34, and that is an inverse of 55 modulo 89.

d) We proceed as above:

$$\begin{aligned}
232 &= 2 \cdot 89 + 54 \\
89 &= 1 \cdot 54 + 35 \\
54 &= 1 \cdot 35 + 19 \\
35 &= 1 \cdot 19 + 16 \\
19 &= 1 \cdot 16 + 3 \\
16 &= 5 \cdot 3 + 1 \\
3 &= 3 \cdot 1
\end{aligned}$$

Then we work backwards to rewrite the gcd (the last nonzero remainder, which is 1 here) in terms of 232 and 89:

$$\begin{aligned}
1 &= 16 - 5 \cdot 3 \\
&= 16 - 5 \cdot (19 - 1 \cdot 16) = 6 \cdot 16 - 5 \cdot 19 \\
&= 6 \cdot (35 - 1 \cdot 19) - 5 \cdot 19 = 6 \cdot 35 - 11 \cdot 19 \\
&= 6 \cdot 35 - 11 \cdot (54 - 1 \cdot 35) = 17 \cdot 35 - 11 \cdot 54 \\
&= 17 \cdot (89 - 1 \cdot 54) - 11 \cdot 54 = 17 \cdot 89 - 28 \cdot 54 \\
&= 17 \cdot 89 - 28 \cdot (232 - 2 \cdot 89) = 73 \cdot 89 - 28 \cdot 232
\end{aligned}$$

Therefore the Bézout coefficient of 89 is 73, and that is an inverse of 89 modulo 232.

7. We follow the hint. Suppose that we had two inverses of a modulo m, say b and c. In symbols, we would have $ba \equiv 1 \pmod{m}$ and $ca \equiv 1 \pmod{m}$. The first congruence says that m divides $ba - 1$, and the second says that m divides $ca - 1$. Therefore m divides the difference $(ba - 1) - (ca - 1) = ba - ca$. (The difference of two multiples of m is a multiple of m.) Thus $ba \equiv ca \pmod{m}$. It follows immediately from Theorem 7 in Section 4.3 (the roles of a, b, and c need to be permuted) that $b \equiv c \pmod{m}$, which is what we wanted to prove.

9. In Exercise 5a we found that an inverse of 4 modulo 9 is 7. Therefore we multiply both sides of this equation by 7, obtaining $x \equiv 35 \equiv 8 \pmod{9}$. As a check, we compute $4 \cdot 8 = 32 \equiv 5 \pmod{9}$.

11. Our answers are not unique, of course—anything in the same congruence class works just as well.

a) In Exercise 5b we found that an inverse of 19 modulo 141 is 52. Therefore we multiply both sides of this equation by 52, obtaining $x \equiv 208 \equiv 67 \pmod{141}$. As a check, we compute $19 \cdot 67 = 1273 \equiv 4 \pmod{141}$.

b) In Exercise 5c we found that an inverse of 55 modulo 89 is 34. Therefore we multiply both sides of this equation by 34, obtaining $x \equiv 1156 \equiv 88 \pmod{89}$. As a check, we compute $55 \cdot 88 \equiv 55 \cdot (-1) = -55 \equiv 34 \pmod{89}$.

c) In Exercise 5d we found that an inverse of 89 modulo 232 is 73. Therefore we multiply both sides of this equation by 73, obtaining $x \equiv 146 \pmod{232}$. As a check, we compute $89 \cdot 146 = 12994 \equiv 2 \pmod{232}$.

13. We follow the hint. Adding 6 to both sides gives the equivalent congruence $15x^2 + 19x + 6 \equiv 0 \pmod{11}$, because $5 + 6 = 11 \equiv 0 \pmod{11}$. This factors as $(5x + 3)(3x + 2) \equiv 0 \pmod{11}$. Because there are no non-zero divisors of 0 working modulo 11, we conclude that the solutions are precisely the solutions of $5x + 3 \equiv 0 \pmod{11}$ and $3x + 2 \equiv 0 \pmod{11}$. We solve these by the method of Example 3. By inspection (trial-and-error) or working it out through the Euclidean algorithm and back-substituting, we find that an inverse of 5 modulo 11 is 9, and multiplying both sides of $5x+3 \equiv 0 \pmod{11}$ by 9 yields $x+27 \equiv 0 \pmod{11}$, so $x \equiv -27 \equiv 6 \pmod{11}$. Similarly, an inverse of 3 modulo 11 is 4, and we get $x \equiv -8 \equiv 3 \pmod{11}$. So the solution set is $\{3, 6\}$ (and anything congruent to these modulo 11). Plugging these values into the original equation to check, we have $15 \cdot 3^2 + 19 \cdot 3 + 6 = 198 \equiv 0 \pmod{11}$ and $15 \cdot 6^2 + 19 \cdot 6 + 6 = 660 \equiv 0 \pmod{11}$.

15. The hypothesis tells us that m divides $ac - bc$, which is the product $(a - b)c$. Let m' be $m/\gcd(c, m)$. Then m' is a factor of m, so certainly $m' \mid (a - b)c$. Now since all the common factors of m and c were divided out of m to get m', we know that m' is relatively prime to c. It follows from Lemma 2 in Section 4.3 that $m' \mid a - b$. But this means that $a \equiv b \pmod{m'}$, exactly what we were trying to prove.

17. We want to find numbers x such that $x^2 \equiv 1 \pmod{p}$, in other words, such that p divides $x^2 - 1$. Factoring this expression, we see that we are seeking numbers x such that $p \mid (x+1)(x-1)$. By Lemma 3 in Section 4.3, this can only happen if $p \mid x + 1$ or $p \mid x - 1$. But these two congruences are equivalent to the statements $x \equiv -1 \pmod{p}$ and $x \equiv 1 \pmod{p}$.

19. **a)** If two of these integers were congruent modulo p, say ia and ja, where $1 \leq i < j < p$, then we would have $p \mid ja - ia$, or $p \mid (j - i)a$. By Lemma 2 (or Lemma 3) in Section 4.3, since a is not divisible by p, p must divide $j - i$. But this is impossible, since $j - i$ is a positive integer less than p. Therefore no two of these integers are congruent modulo p.

b) By part **(a)**, since no two of a, $2a$, ..., $(p - 1)a$ are congruent modulo p, each must be congruent to a different number from 1 to $p-1$. Therefore if we multiply them all together, we will obtain the same product, modulo p, as if we had multiplied all the numbers from 1 to $p - 1$. In symbols,

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

The left-hand side of this congruence is clearly $(p - 1)! \cdot a^{p-1}$, and the right-hand side is just $(p - 1)!$, as desired.

c) Wilson's theorem says that $(p - 1)!$ is congruent to -1 modulo p. Therefore the congruence in part **(b)** says that $(-1) \cdot a^{p-1} \equiv -1 \pmod{p}$. Multiplying both sides by -1, we see that $a^{p-1} \equiv 1 \pmod{p}$, as desired. Note that we already assumed the hypothesis that $p \nmid a$ in part **(a)**.

d) If $p \mid a$, then both sides of $a^p \equiv a \pmod{p}$ are 0 modulo p, so the congruence holds. If not, then we just multiply the result obtained in part **(c)** by a.

21. Since 2, 3, 5, and 11 are pairwise relatively prime, we can use the Chinese remainder theorem. The answer will be unique modulo $2 \cdot 3 \cdot 5 \cdot 11 = 330$. Using the notation in the text, we have $a_1 = 1$, $m_1 = 2$, $a_2 = 2$, $m_2 = 3$, $a_3 = 3$, $m_3 = 5$, $a_4 = 4$, $m_4 = 11$, $m = 330$, $M_1 = 330/2 = 165$, $M_2 = 330/3 = 110$, $M_3 = 330/5 = 66$, $M_4 = 330/11 = 30$. Then we need to find inverses y_i of M_i modulo m_i for $i = 1, 2, 3, 4$. This can be done by inspection (trial and error), since the moduli here are so small, or systematically using the Euclidean algorithm, as in Exercise 5; we find that $y_1 = 1$, $y_2 = 2$, $y_3 = 1$, and $y_4 = 7$ (for this last one, $30 \equiv 8 \pmod{11}$, so we want to solve $8y_4 = 1 \pmod{11}$, and we observe that $8 \cdot 7 = 56 \equiv 1 \pmod{11}$). Thus our solution is $x = 1 \cdot 165 \cdot 1 + 2 \cdot 110 \cdot 2 + 3 \cdot 66 \cdot 1 + 4 \cdot 30 \cdot 7 = 1643 \equiv 323 \pmod{330}$. So the solutions are all integers of the form $323 + 330k$, where k is an integer.

23. By definition, the first congruence can be written as $x = 3t + 2$ where t is an integer. Substituting this expression for x into the second congruence tells us that $3t + 2 \equiv 1 \pmod 4$, which can easily be solved to show that $t \equiv 1 \pmod 4$. From this we can write $t = 4u + 1$ for some integer u. Thus $x = 3t + 2 = 3(4u + 1) + 2 = 12u + 5$. We plug this into the third congruence to obtain $12u + 5 \equiv 3 \pmod 5$, which we easily solve to give $u \equiv 4 \pmod 5$. Hence $u = 5v + 4$, and so $x = 12u + 5 = 12(5v + 4) + 5 = 60v + 53$. We check our answer by confirming that $53 \equiv 2 \pmod 3$, $53 \equiv 1 \pmod 4$, and $53 \equiv 3 \pmod 5$.

25. We simply translate the steps of the calculation given in the proof of Theorem 2 into pseudocode. Of course, hidden in line 7 below is a multi-step process of finding inverses in modular arithmetic, which can be accomplished by using the Euclidean algorithm and back-substituting, as in Example 2. The last loop reduces the answer x to its simplest form modulo m. All solutions are then of the form $x + mk$, where m is the product of the moduli and k is an integer.

procedure *chinese*($m_1, m_2, \ldots, m_n$: relatively prime positive integers; $a_1, a_2, \ldots, a_n$: integers)
$m := 1$
for $k := 1$ **to** n
    $m := m \cdot m_k$
for $k := 1$ **to** n
    $M_k := m/m_k$
    $y_k := M_k^{-1}$ **mod** m_k
$x := 0$
for $k := 1$ **to** n
    $x := x + a_k M_k y_k$
while $x \geq m$
    $x := x - m$
return x {the smallest solution to the system $\{ x \equiv a_k \pmod{m_k},\ k = 1, 2, \ldots, n \}$}

27. We cannot apply the Chinese remainder theorem directly, since the moduli are not pairwise relatively prime. However, we can, using the Chinese remainder theorem, translate these congruences into a set of congruences that together are equivalent to the given congruence. Since we want $x \equiv 4 \pmod{12}$, we must have $x \equiv 4 \equiv 1 \pmod 3$ and $x \equiv 4 \equiv 0 \pmod 4$. Similarly, from the third congruence we must have $x \equiv 1 \pmod 3$ and $x \equiv 2 \pmod 7$. Since the first congruence is consistent with the requirement that $x \equiv 1 \pmod 3$, we see that our system is equivalent to the system $x \equiv 7 \pmod 9$, $x \equiv 0 \pmod 4$, $x \equiv 2 \pmod 7$. These can be solved using the Chinese remainder theorem (see Exercise 21 or Example 5) to yield $x \equiv 16 \pmod{252}$. Therefore the solutions are all integers of the form $16 + 252k$, where k is an integer.

29. We will argue for the truth of this statement using the Fundamental Theorem of Arithmetic. What we must show is that $m_1 m_2 \cdots m_n \mid a - b$. Look at the prime factorization of both sides of this proposition. Suppose that p is a prime appearing in the prime factorization of the left-hand side. Then $p \mid m_j$ for some j. Since the m_i's are relatively prime, p does not appear as a factor in any of the other m_i's. Now we know from the hypothesis that $m_j \mid a - b$. Therefore $a - b$ contains the factor p in its prime factorization, and p must appear to a power at least as large as the power to which it appears in m_j. But what we have just shown is that each prime power p^r in the prime factorization of the left-hand side also appears in the prime factorization of the right-hand side. Therefore the left-hand side does, indeed, divide the right-hand side.

31. We are asked to solve the simultaneous congruences $x \equiv 1 \pmod 2$ and $x \equiv 1 \pmod 3$. The solution will be unique modulo $2 \cdot 3 = 6$. By inspection we see that the answer is simply that $x \equiv 1 \pmod 6$. The solution set is $\{\ldots, -11, -5, 1, 7, 13, \ldots\}$.

33. Fermat's little theorem tells us that $7^{12} \equiv 1 \pmod{13}$. Note that $121 = 10 \cdot 12 + 1$. Therefore $7^{121} = 7^{12 \cdot 10} \cdot 7 = (7^{12})^{10} \cdot 7 \equiv 1^{10} \cdot 7 = 7 \pmod{13}$.

35. Fermat's little theorem tells us that under the given conditions $a^{p-1} \equiv 1 \pmod{p}$. Therefore $a^{p-2} \cdot a = a \cdot a^{p-2} = a^{p-1} \equiv 1 \pmod{p}$. This is precisely the definition that a^{p-2} is an inverse of a modulo p.

37. **a)** We calculate $2^{340} = (2^{10})^{34} \equiv 1^{34} = 1 \pmod{11}$, since Fermat's little theorem says that $2^{10} \equiv 1 \pmod{11}$.

b) We calculate $2^{340} = (2^5)^{68} = 32^{68} \equiv 1^{68} = 1 \pmod{31}$, since $32 \equiv 1 \pmod{31}$.

c) Since 11 and 31 are relatively prime, and $11 \cdot 31 = 341$, it follows from the first two parts and Exercise 29 that $2^{340} \equiv 1 \pmod{341}$.

39. **a)** By Fermat's little theorem we know that $5^6 \equiv 1 \pmod{7}$; therefore $5^{1998} = (5^6)^{333} \equiv 1^{333} \equiv 1 \pmod{7}$, and so $5^{2003} = 5^5 \cdot 5^{1998} \equiv 3125 \cdot 1 \equiv 3 \pmod{7}$. So 5^{2003} **mod** $7 = 3$. Similarly, $5^{10} \equiv 1 \pmod{11}$; therefore $5^{2000} = (5^{10})^{200} \equiv 1^{200} \equiv 1 \pmod{11}$, and so $5^{2003} = 5^3 \cdot 5^{2000} \equiv 125 \cdot 1 \equiv 4 \pmod{11}$. So 5^{2003} **mod** $11 = 4$. Finally, $5^{12} \equiv 1 \pmod{13}$; therefore $5^{1992} = (5^{12})^{166} \equiv 1^{166} \equiv 1 \pmod{13}$, and so $5^{2003} = 5^{11} \cdot 5^{1992} \equiv 48{,}828{,}125 \cdot 1 \equiv 8 \pmod{13}$. So 5^{2003} **mod** $13 = 8$.

b) We now apply the Chinese remainder theorem to the results of part **(a)**, as in Example 5. Let $m = 7 \cdot 11 \cdot 13 = 1001$, $M_1 = m/7 = 143$, $M_2 = m/11 = 91$, and $M_3 = m/13 = 77$. We see that 5 is an inverse of 143 modulo 7, since $143 \equiv 3 \pmod{7}$, and $3 \cdot 5 = 15 \equiv 1 \pmod{7}$. Similarly, 4 is an inverse of 91 modulo 11, and 12 is an inverse of 77 modulo 13. (An algorithm to compute inverses—if we don't want to find them by inspection as we've done here—is illustrated in Example 2.) Therefore the answer is $(3 \cdot 143 \cdot 5 + 4 \cdot 91 \cdot 4 + 8 \cdot 77 \cdot 12)$ **mod** $1001 = 10993$ **mod** $1001 = 983$.

41. Let q be a (necessarily odd) prime dividing $2^p - 1$. By Fermat's little theorem, we know that $q \mid 2^{q-1} - 1$. Then from Exercise 37 in Section 4.3 we know that $\gcd(2^p - 1, 2^{q-1} - 1) = 2^{\gcd(p,q-1)} - 1$. Since q is a common divisor of $2^p - 1$ and $2^{q-1} - 1$, we know that $\gcd(2^p - 1, 2^{q-1} - 1) > 1$. Hence $\gcd(p, q-1) = p$, since the only other possibility, namely $\gcd(p, q-1) = 1$, would give us $\gcd(2^p - 1, 2^{q-1} - 1) = 1$. Hence $p \mid q - 1$, and therefore there is a positive integer m such that $q - 1 = mp$. Since q is odd, m must be even, say $m = 2k$, and so every prime divisor of $2^p - 1$ is of the form $2kp + 1$. Furthermore, products of numbers of this form are also of this form, since $(2k_1p + 1)(2k_2p + 1) = 4k_1k_2p^2 + 2k_1p + 2k_2p + 1 = 2(2k_1k_2p + k_1 + k_2)p + 1$. Therefore all divisors of $2^p - 1$ are of this form.

43. To decide whether $2^{11} - 1 = 2047$ is prime, we need only look for a prime factor not exceeding $\sqrt{2047} \approx 45$. By Exercise 41 every such prime divisor must be of the form $22k + 1$. The only candidate is therefore 23. In fact $2047 = 23 \cdot 89$, so we conclude that 2047 is not prime.

We can take the same approach for $2^{17} - 1 = 131{,}071$, but we need either computer algebra software or patience with a calculator. By Exercise 41 every prime divisor of $2^{17} - 1$ must be of the form $34k + 1$, so we need to try all such divisors (or at least those that are not obviously nonprime) up to $\sqrt{131{,}071} \approx 362$, which means up to $k = 10$. No number of this form divides 131,071, so we conclude that it is prime.

45. First note that $2047 = 23 \cdot 89$, so 2047 is composite. To apply Miller's test, we write $2047 - 1 = 2046 = 2 \cdot 1023$, so $s = 1$ and $t = 1023$. We must show that either $2^{1023} \equiv 1 \pmod{2047}$ or $2^{1023} \equiv -1 \pmod{2047}$. To compute, we write $2^{1023} = (2^{11})^{93} = 2048^{93} \equiv 1^{93} = 1 \pmod{2047}$, as desired. (We could also compute this using the modular exponentiation algorithm given in Section 4.2—see Example 12 in that section.)

47. We factor $2821 = 7 \cdot 13 \cdot 31$. We must show that this number meets the definition of Carmichael number, namely that $b^{2820} \equiv 1 \pmod{2821}$ for all b relatively prime to 2821. Note that if $\gcd(b, 2821) = 1$, then $\gcd(b, 7) = \gcd(b, 13) = \gcd(b, 31) = 1$. Using Fermat's little theorem we find that $b^6 \equiv 1 \pmod{7}$, $b^{12} \equiv 1 \pmod{13}$, and $b^{30} \equiv 1 \pmod{31}$. It follows that $b^{2820} = (b^6)^{470} \equiv 1 \pmod{7}$, $b^{2820} = (b^{12})^{235} \equiv 1 \pmod{13}$, and $b^{2820} = (b^{30})^{94} \equiv 1 \pmod{31}$. By Exercise 29 (or the Chinese remainder theorem) it follows that $b^{2820} \equiv 1 \pmod{2821}$, as desired.

49. **a)** If we multiply out this expression, we get $n = 1296m^3 + 396m^2 + 36m + 1$. Clearly $6m \mid n-1$, $12m \mid n-1$, and $18m \mid n-1$. Therefore, the conditions of Exercise 48 are met, and we conclude that n is a Carmichael number.

b) Letting $m = 51$ gives $n = 172{,}947{,}529$. We note that $6m+1 = 307$, $12m+1 = 613$, and $18m+1 = 919$ are all prime.

51. It is straightforward to calculate the remainders when the integers from 0 to 14 are divided by 3 and by 5. For example, the remainders when 10 is divided by 3 and 5 are 1 and 0, respectively, so we represent 10 by the pair $(1,0)$. The exercise is simply asking us to tabulate these remainders, as in Example 7.

$0 = (0,0)$	$3 = (0,3)$	$6 = (0,1)$	$9 = (0,4)$	$12 = (0,2)$
$1 = (1,1)$	$4 = (1,4)$	$7 = (1,2)$	$10 = (1,0)$	$13 = (1,3)$
$2 = (2,2)$	$5 = (2,0)$	$8 = (2,3)$	$11 = (2,1)$	$14 = (2,4)$

53. The method of solving a system of congruences such as this is given in the proof of Theorem 2. Here we have $m_1 = 99$, $m_2 = 98$, $m_3 = 97$, and $m_4 = 95$, so that $m = 99 \cdot 98 \cdot 97 \cdot 95 = 89403930$. We compute the values $M_k = m/m_k$ and obtain $M_1 = 903070$, $M_2 = 912285$, $M_3 = 921690$, and $M_4 = 941094$. Next we need to find the inverses y_k of M_k modulo m_k. To do this we first replace each M_k by its remainder modulo m_k (to make the arithmetic easier), and then apply the technique shown in Example 2. For $k = 1$ we want to find the inverse of 903070 modulo 99, which is the same as the inverse of 903070 **mod** 99, namely 91. To do this we apply the Euclidean algorithm to express 1 as a linear combination of 91 and 99.

$$\begin{aligned} 99 &= 91 + 8 \\ 91 &= 11 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 2 + 1 \\ \therefore\ 1 &= 3 - 2 \\ &= 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8 \\ &= 3 \cdot (91 - 11 \cdot 8) - 8 = 3 \cdot 91 - 34 \cdot 8 \\ &= 3 \cdot 91 - 34 \cdot (99 - 91) = 37 \cdot 91 - 34 \cdot 99 \end{aligned}$$

We therefore conclude that the inverse of 91 modulo 99 is 37, so we have $y_1 = 37$. Similar calculations show that $y_2 = 33$, $y_3 = 24$, and $y_4 = 4$. Continuing with the procedure outlined in the proof of Theorem 2, we now form the sum of the products $a_k M_k y_k$, and this will be our solution. We have

$$65 \cdot 903070 \cdot 37 + 2 \cdot 912285 \cdot 33 + 51 \cdot 921690 \cdot 24 + 10 \cdot 941094 \cdot 4 = 3397886480.$$

We want our answer reduced modulo m, so we divide by 89403930 and take the remainder, obtaining 537140. (All of these calculations are not difficult using a scientific calculator.) Finally, let us check our answer: 537140 **mod** 99 = 65, 537140 **mod** 98 = 2, 537140 **mod** 97 = 51, 537140 **mod** 95 = 10.

55. For the first question we seek an exponent n such that $2^n \equiv 5 \pmod{19}$. For the second we want $2^n \equiv 6 \pmod{19}$. There is no known efficient algorithm for finding these exponents, so we might as well just start computing powers of 2 modulo 19. In each case, we just need to multiply the previous result by 2, working modulo 19. We have $2^2 = 4 \pmod{19}$, $2^3 = 2 \cdot 4 = 8 \pmod{19}$, $2^4 = 2 \cdot 8 = 16 \pmod{19}$, $2^5 = 2 \cdot 16 = 32 \equiv 13 \pmod{19}$, $2^6 = 2 \cdot 2^5 \equiv 2 \cdot 13 = 26 \equiv 7 \pmod{19}$, $2^7 \equiv 2 \cdot 7 = 14 \pmod{19}$, $2^8 \equiv 2 \cdot 14 = 28 \equiv 9 \pmod{19}$, $2^9 \equiv 2 \cdot 9 = 18 \pmod{19}$, $2^{10} \equiv 2 \cdot 18 = 36 \equiv 17 \pmod{19}$, $2^{11} \equiv 2 \cdot 17 = 34 \equiv 15 \pmod{19}$, $2^{12} \equiv 2 \cdot 15 = 30 \equiv 11 \pmod{19}$, $2^{13} \equiv 2 \cdot 11 = 22 \equiv 3 \pmod{19}$, $2^{14} \equiv 2 \cdot 3 = 6 \pmod{19}$. Finally! So we conclude that the discrete logarithm of 6 to the base 2 modulo 19 is 14. Continuing the calculation, we have $2^{15} \equiv 2 \cdot 6 = 12 \pmod{19}$, $2^{16} \equiv 2 \cdot 12 = 24 \equiv 5 \pmod{19}$. So the discrete logarithm of 5 to the base 2 modulo 19 is 16.

57. A computer algebra system such as *Maple* facilitates the modular arithmetic calculations. We repeatedly multiply by 3 and reduce modulo 17. We get $3^0 = 1 \pmod{17}$, $3^1 = 3 \pmod{17}$, $3^2 = 9 \pmod{17}$, $3^3 = 27 \equiv 10 \pmod{17}$, and so on. Thus $\log_3 1 = 0$, $\log_3 3 = 1$, $\log_3 9 = 2$, $\log_3 10 = 3$, and so on. If we collect the data and present them in order of increasing argument, we get the required table. (Of course $\log_3 0$ does not exist.)

$$\log_3 1 = 0 \quad \log_3 2 = 14 \quad \log_3 3 = 1 \quad \log_3 4 = 12 \quad \log_3 5 = 5 \quad \log_3 6 = 15 \quad \log_3 7 = 11 \quad \log_3 8 = 10$$

$$\log_3 9 = 2 \quad \log_3 10 = 3 \quad \log_3 11 = 7 \quad \log_3 12 = 13 \quad \log_3 13 = 4 \quad \log_3 14 = 9 \quad \log_3 15 = 6 \quad \log_3 16 = 8$$

59. We need to prove that if the congruence $x^2 \equiv a \pmod{p}$ has any solutions at all, then it has exactly two solutions. So let us assume that s is a solution. Clearly $-s$ is a solution as well, since $(-s)^2 = s^2$. Furthermore, $-s \not\equiv s \pmod{p}$, since if it were, we would have $2s \equiv 0 \pmod{p}$, which means that $p \mid 2s$. Since p is an odd prime, that means that $p \mid s$, so that $s \equiv 0 \pmod{p}$. Therefore $a \equiv 0 \pmod{p}$, contradicting the conditions of the problem.

It remains to prove that there cannot be more than two incongruent solutions. Suppose that s is one solution and that t is a second solution. We have $s^2 \equiv t^2 \pmod{p}$. This means that $p \mid s^2 - t^2$, that is, $p \mid (s+t)(s-t)$. Since p is prime, Lemma 3 in Section 4.3 guarantees that $p \mid s-t$ or $p \mid s+t$. This means that $t \equiv s \pmod{p}$ or $t \equiv -s \pmod{p}$. Therefore any solution t must be either the first solution or its negative. In other words, there are at most two solutions.

61. There is really almost nothing to prove here. The value $\left(\frac{a}{p}\right)$ depends only on whether or not a is a quadratic residue modulo p, i.e., whether or not the equivalence $x^2 \equiv a \pmod{p}$ has a solution. Obviously, this depends only on the equivalence class of a modulo p.

63. By Exercise 62 we know that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2} b^{(p-1)/2} = (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) \pmod{p}$. Since the only values either side of this equivalence can take on are ± 1, being congruent modulo p is the same as being equal.

65. We follow the hint. Working modulo 5, we want to solve $x^2 \equiv 4$. It is easy to see that there are exactly two solutions modulo 5, namely $x = 2$ and $x = 3$. Similarly there are only the solutions $x = 1$ and $x = 6$ modulo 7. Therefore we want to find values of x modulo $5 \cdot 7 = 35$ such that $x \equiv 2$ or 3 (mod 5) and $x \equiv 1$ or 6 (mod 7). We can do this by applying the Chinese remainder theorem (as in Example 5) four times, for the four combinations of these values. For example, to solve $x \equiv 2 \pmod{5}$ and $x \equiv 1 \pmod{7}$, we find that $m = 35$, $M_1 = 7$, $M_2 = 5$, $y_1 = 3$, $y_2 = 3$, so $x \equiv 2 \cdot 7 \cdot 3 + 1 \cdot 5 \cdot 3 = 57 \equiv 22 \pmod{35}$. Doing the similar calculation with the other three possibilities yields the other three solutions modulo 35: $x = 8$, $x = 13$, and $x = 27$.

67. To compute $\log_r a \pmod{p}$, we need to solve $r^e \equiv a \pmod{p}$ for e. The brute force approach is just to compute r^e **mod** p for $e = 0, 1, 2, \ldots, p-2$ until we get the answer a. This requires about p iterations, each of which can be done with $O(\log p)$ bit operations, since we need only multiply the previous value by r and find the remainder upon division by p. At worst, we require all p iterations; on average, only half that many. In either case, the time complexity is $O(p \log p)$, which is prohibitively large if p is, say, a 200-digit number.

SECTION 4.5 Applications of Congruences

The great British number theorist G. H. Hardy (1877–1947) once said, "I have never done anything 'useful.' No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world." He was wrong. Number theory has many applications, especially in cryptography (see Section 4.6). In the present section we saw applications to hashing functions (important for storing large amounts of information and being able to retrieve it efficiently), pseudorandom numbers (important for computer simulations), and check digits (important in our technological world). Hardy would be appalled! The exercises in this section are mostly routine.

1. We are simply asked to compute k **mod** 97 for each value of k. We do this by dividing the given number by 97 and taking the remainder, which can be found either by multiplying the decimal remainder by 97, or by subtracting 97 times the quotient from k. (See the solution to Exercise 3 below for details.)

a) 034567981 **mod** 97 = 91 **b)** 183211232 **mod** 97 = 57

c) 220195744 **mod** 97 = 21 **d)** 987255335 **mod** 97 = 5

3. a) We need to compute k **mod** 31 in each case. A good way to do this on a calculator is as follows. Enter k and divide by 31. The result will be a number with an integer part and a decimal fractional part. Subtract off the integer part, leaving a decimal fraction between 0 and 1. This is the remainder expressed as a decimal. To find out what whole number remainder that really represents, multiply by 31. The answer will be a whole number (or nearly so—it may require rounding, say from 4.9999 or 5.0001 to 5), and that number is k **mod** 31.

(i) 317 **mod** 31 = 7 (ii) 918 **mod** 31 = 19 (iii) 007 **mod** 31 = 7

(iv) 100 **mod** 31 = 7 (v) 111 **mod** 31 = 18 (vi) 310 **mod** 31 = 0

b) Take the next available space, where the next space is computed by adding 1 to the space number and pretending that $30 + 1 = 0$.

5. We apply the formula with $n = 0$ to obtain $x_1 = (3 \cdot x_0 + 2)$ **mod** 13 $= (3 \cdot 1 + 2)$ **mod** 13 $= 5$. Then $x_2 = (3 \cdot x_1 + 2)$ **mod** 13 $= (3 \cdot 5 + 2)$ **mod** 13 $= 17$ **mod** 13 $= 4$. Continuing in this way we have $x_3 = (3 \cdot 4 + 2)$ **mod** 13 $= 1$. Because this is the same as x_0, the sequence repeats from here on out. So the sequence is $1, 5, 4, 1, 5, 4, 1, 5, 4, \ldots$.

7. We compute until the sequence begins to repeat:

$$x_1 = 3 \cdot 2 \textbf{ mod } 11 = 6$$
$$x_2 = 3 \cdot 6 \textbf{ mod } 11 = 7$$
$$x_3 = 3 \cdot 7 \textbf{ mod } 11 = 10$$
$$x_4 = 3 \cdot 10 \textbf{ mod } 11 = 8$$
$$x_5 = 3 \cdot 8 \textbf{ mod } 11 = 2$$

Since $x_5 = x_0$, the sequence repeats forever: $2, 6, 7, 10, 8, 2, 6, 7, 10, 8, \ldots$.

9. We follow the instructions. Because $2357^2 = 5555449 = 05555449$, the middle four digits are 5554, so 5554 is our second pseudorandom number. Next $5554^2 = 30846916$, so our third pseudorandom number is 8469. Repeating the same procedure leads to the following five terms: $7239, 4031, 2489, 1951, 8064$.

11. We are told to apply the formula $x_{n+1} = x_n^3$ **mod** 7, starting with $x_0 = 2$. Thus $x_1 = 2^3$ **mod** 7 $= 1$, $x_2 = 1^3$ **mod** 7 $= 1$, and our sequence never gets off the ground! The sequence generated here is $2, 1, 1, 1, \ldots$.

13. A correctly transmitted bit string must have an even number of 1's. Therefore we can be sure that there is an error in (d), but because the other three strings have an even number of 1's, we cannot detect an error in any of them. (Of course that doesn't mean that there is no error, because it is possible that two bits were transmitted incorrectly, in which case the sum modulo 2 does not change.)

15. Let d be the check digit. Then we know that $1{\cdot}0{+}2{\cdot}0{+}3{\cdot}7{+}4{\cdot}1{+}5{\cdot}1{+}6{\cdot}9{+}7{\cdot}8{+}8{\cdot}8{+}9{\cdot}1{+}10{\cdot}d \equiv 0 \pmod{11}$. This simplifies to $213{+}10{\cdot}d \equiv 0 \pmod{11}$. But $213 \equiv 4 \pmod{11}$, and $10 \equiv -1 \pmod{11}$, so this is equivalent to $4 - d \equiv 0 \pmod{11}$, or $d = 4$.

17. The ISBN is 0073383090. To check its validity we compute, as in Example 6, $1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 3 + 5 \cdot 3 + 6 \cdot 8 + 7 \cdot 3 + 8 \cdot 0 + 9 \cdot 9 + 10 \cdot 0 = 198$. Because this is congruent to 0 modulo 11, the check digit was computed correctly.

19. To determine whether an 11-digit number is a valid USPS money order identification number, we need to verify that the sum of the first ten digits reduced modulo 9 gives the last digit.

a) $7 + 4 + 0 + 5 + 1 + 4 + 8 + 9 + 6 + 2 \bmod 9 = 46 \bmod 9 = 1 \neq 3$, so this is not a valid number.

b) $8 + 8 + 3 + 8 + 2 + 0 + 1 + 3 + 4 + 4 \bmod 9 = 41 \bmod 9 = 5$, which is the last digit, so this is a valid number.

c) $5 + 6 + 1 + 5 + 2 + 2 + 4 + 0 + 7 + 8 \bmod 9 = 40 \bmod 9 = 4$, which is the last digit, so this is a valid number.

d) $6 + 6 + 6 + 0 + 6 + 6 + 3 + 1 + 1 + 7 \bmod 9 = 42 \bmod 9 = 6 \neq 8$, so this is not a valid number.

21. In each case, we know that $x_{11} = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} \bmod 9$. (See the preamble to Exercise 18.) This is equivalent to $x_{11} \equiv x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} \pmod{9}$, with $0 \leq x_{11} \leq 8$. Therefore we will get an equation modulo 9 involving the unknown Q for each of these valid postal money order identification numbers.

a) $8 \equiv 4 + 9 + 3 + 2 + 1 + 2 + Q + 0 + 6 + 8 \pmod{9}$, which is equivalent to $8 \equiv Q + 35 \equiv Q + 8 \pmod{9}$. Therefore $Q \equiv 0 \pmod{9}$. There are two single-digit numbers Q that makes this true: $Q = 0$ and $Q = 9$, so it is impossible to know for sure what the smudged digit was.

b) $8 \equiv 8 + 5 + 0 + Q + 9 + 1 + 0 + 3 + 8 + 5 \pmod{9}$, which is equivalent to $8 \equiv Q + 39 \equiv Q + 3 \pmod{9}$. The only single-digit number Q that makes this true is $Q = 5$, so the smudged digit must have been a 5.

c) $4 \equiv 2 + Q + 9 + 4 + 1 + 0 + 0 + 7 + 7 + 3 \pmod{9}$, which is equivalent to $4 \equiv Q + 33 \equiv Q + 6 \pmod{9}$. The only single-digit number Q that makes this true is $Q = 7$, so the smudged digit must have been a 7.

d) $1 \equiv 6 + 6 + 6 + 8 + 7 + Q + 0 + 3 + 2 + 0 \pmod{9}$, which is equivalent to $1 \equiv Q + 38 \equiv Q + 2 \pmod{9}$. The only single-digit number Q that makes this true is $Q = 8$, so the smudged digit must have been an 8.

23. Because the first ten digits are added, any transposition error involving them will go undetected—the sum of the first ten digits will be the same for the transposed number as it is for the correct number. Suppose the last digit is transposed with another digit; without loss of generality, we can assume it's the tenth digit and that $x_{10} \neq x_{11}$. Then the correct equation will be

$$x_{11} \equiv x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{10} \pmod{9}$$

but the equation resulting from the error will read

$$x_{10} \equiv x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 + x_9 + x_{11} \pmod{9}.$$

Subtracting these two equations, we see that the erroneous equation will be true if and only if $x_{11} - x_{10} \equiv x_{10} - x_{11} \pmod{9}$. This is equivalent to $2x_{11} \equiv 2x_{10} \pmod{9}$, which, because 2 is relatively prime to 9, is equivalent to $x_{11} \equiv x_{10} \pmod{9}$, which is false. This tells us that the check equation will fail. Therefore we conclude that transposition errors involving the eleventh digits are detected.

25. From Example 5. we know that a valid UPC code must satisfy the equation

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}.$$

Therefore in each case we simply need to compute the left-hand side of this equation modulo 10 and see whether or not we get 0 as the answer.

a) $3 \cdot 0 + 3 + 3 \cdot 6 + 0 + 3 \cdot 0 + 0 + 3 \cdot 2 + 9 + 3 \cdot 1 + 4 + 3 \cdot 5 + 2 = 60 \equiv 0 \pmod{10}$, so this is a valid code.

b) $3 \cdot 0 + 1 + 3 \cdot 2 + 3 + 3 \cdot 4 + 5 + 3 \cdot 6 + 7 + 3 \cdot 8 + 9 + 3 \cdot 0 + 3 = 88 \not\equiv 0 \pmod{10}$, so this is not a valid code.

c) $3 \cdot 7 + 8 + 3 \cdot 2 + 4 + 3 \cdot 2 + 1 + 3 \cdot 8 + 4 + 3 \cdot 3 + 0 + 3 \cdot 1 + 4 = 90 \equiv 0 \pmod{10}$, so this is a valid code.

d) $3 \cdot 7 + 2 + 3 \cdot 6 + 4 + 3 \cdot 1 + 2 + 3 \cdot 1 + 7 + 3 \cdot 5 + 4 + 3 \cdot 2 + 5 = 90 \equiv 0 \pmod{10}$, so this is a valid code.

27. The digits with even subscripts appear in the formula with coefficient 1, whereas those with odd subscripts appear with coefficient 3. Therefore if two digits whose positions have the same parity (both odd or both even) are switched, then the sum will be unchanged and such an error cannot be detected. If two digits whose parities are different are transposed, say an x in an odd position and a y in an even position, then the new sum will differ from the old sum by $(x + 3y) - (3x + y)$, which equals $2(y - x)$. As long as the two transposed digits do not differ by 5, the sum will therefore be different modulo 10; if they do differ by 5, then the sum will be the same modulo 10. We conclude that transposition errors will be detected if and only if the transposed digits are an odd number of positions apart (in particular transposing neighboring digits) and do not differ by 5.

29. In each case we need to compute $a_1 a_2 \ldots a_{14}$ **mod** 7 and see if we get a_{15}. This may be inconvenient on a calculator with only 12 digits of precision, but one can always divide it out by hand (or, better, use computer algebra software).

a) $10133334178901 = 7 \cdot 1447619168414 + 3$. Therefore 10133334178901 **mod** $7 = 3 = a_{15}$, so this is a valid airline ticket number. (In *Maple* we could just type `10133334178901 mod 7` and get the response `3`.)

b) 00786234277044 **mod** $7 = 6 \neq 5 = a_{15}$, so this is not a valid number.

c) 11327343888253 **mod** $7 = 1 = a_{15}$, so this is a valid number.

d) 00012234732287 **mod** $7 = 1 = a_{15}$, so this is a valid number.

31. Let's solve a more general problem by ignoring the word "consecutive." First we look at the case in which the transposition does not involve the check digit itself. Suppose the erroneous number formed by the first 14 digits occurs when a_i is interchanged with a_j, where $1 \leq i < j \leq 14$. Because of our decimal place-value numeration system, before the switch, a_i was contributing $a_i \cdot 10^{14-i}$ to the value of the number, and a_j was contributing $a_j \cdot 10^{14-j}$. Therefore this change has increased the 14-digit number by $(a_j - a_i)10^{14-i} + (a_i - a_j)10^{14-j}$, which equals $(a_j - a_i)(10^{14-i} - 10^{14-j})$. In order for this to still check, this last expression must be equivalent to 0 modulo 7. Obviously this will happen if a_i and a_j differ by 7, but it will also happen if $(10^{14-i} - 10^{14-j})$ is a multiple of 7. A bit of calculation shows that this will happen if and only if $j - i = 6$ or 12. Thus we cannot detect the error if the columns in which the transposition occurs are 6 or 12 apart or the transposed digits differ by 7. Finally, if the digit a_{15} is transposed with the digit a_i, where $1 \leq i \leq 14$, then $a_1 a_2 \ldots a_{14}$ **mod** 7 has gone up by $(a_{15} - a_i)10^{14-i}$ and the check digit has gone up by $a_i - a_{15}$, so we will not be able to detect this error if and only if $(a_{15} - a_i)10^{14-i} \equiv a_i - a_{15} \pmod{7}$, which is equivalent to $(a_{15} - a_i)(10^{14-i} + 1) \equiv 0 \pmod{7}$. Because $10^{14-i} + 1 \equiv 0 \pmod{7}$ if and only if $i = 5$ or 11, we conclude that we cannot detect the transposition error if it interchanges the check digit with a_5 or a_{11} or interchanges it with a digit differing from it by 7. (Of course, the check digit must be 0 through 6, so an error that puts a 7, 8, or 9 in the last position can also be detected.)

Because transposing consecutive digits is not transposing digits whose positions differ by the quantities mentioned above, we can detect all transposition errors of consecutive digits unless the digits differ by 7.

33. In each case we will compute $3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7$ **mod** 11. If this matches the digit given for d_8, then the ISSN is valid, and conversely.

a) $3 \cdot 1 + 4 \cdot 0 + 5 \cdot 5 + 6 \cdot 9 + 7 \cdot 1 + 8 \cdot 0 + 9 \cdot 2 \bmod 11 = 107 \bmod 11 = 8$. Because $d_8 = 7 \neq 8$, this number is not valid.

b) $3 \cdot 0 + 4 \cdot 0 + 5 \cdot 0 + 6 \cdot 2 + 7 \cdot 9 + 8 \cdot 8 + 9 \cdot 9 \bmod 11 = 220 \bmod 11 = 0$. Because $d_8 = 0$, this number is valid.

c) $3 \cdot 1 + 4 \cdot 5 + 5 \cdot 3 + 6 \cdot 0 + 7 \cdot 8 + 8 \cdot 6 + 9 \cdot 6 \bmod 11 = 196 \bmod 11 = 9$. Because $d_8 = 9$, this number is valid.

d) $3 \cdot 1 + 4 \cdot 0 + 5 \cdot 0 + 6 \cdot 7 + 7 \cdot 1 + 8 \cdot 2 + 9 \cdot 0 \bmod 11 = 68 \bmod 11 = 2$. Because d_8 is "X" (representing 10 modulo 11), this number is not valid.

35. By subtracting d_8 from both sides and noting that $-1 \equiv 10 \pmod{11}$, we see that the checking congruence is equivalent to $3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 + 10d_8 \equiv 0 \pmod{11}$. It is now easy to see that transposing adjacent digits x and y (where x is on the left) causes the left-hand side to increase by x and decrease by y, for a net change of $x - y$. Because $x \not\equiv y \pmod{11}$, the congruence will no longer hold. Therefore errors of this type are always detected.

SECTION 4.6 Cryptography

In addition to exercises about the topics covered in this section, this exercise set introduces the Vigenère cipher (Exercises 18–22) and a protocol for key exchange (Exercise 33). There is a nice website for encoding and decoding with the affine cipher (for any function of the form $f(p) = ap + b$), which you can use to check your answers: `www.shodor.org/interactivate/activities/CaesarCipher/`. *A website for the Vigenère cipher can be found here:* `islab.oregonstate.edu/koc/ece575/02Project/Mun+Lee/VigenereCipher.html`

1. a) We need to replace each letter by the letter three places later in the alphabet. Thus D becomes G, O becomes R, and so on. The resulting message is GR QRW SDVV JR.

b) We need to replace each letter by the letter 13 places later in the alphabet. Thus D becomes Q, O becomes B (we cycle, with A following Z), and so on. The resulting message is QB ABG CNFF TB.

c) This one is a little harder, so it is probably easiest to work with the numbers. For D we have $p = 3$ because D is the fourth letter of the alphabet. Then $3 \cdot 3 + 7 \bmod 26 = 16$, so the encrypted letter is the 17^{th} letter, or Q (remember that we start the sequence at 0). Our original message has the following numerical values: 3-14 13-14-19 15-0-18-18 6-14. Multiplying each of these numbers by 3, adding 7, and reducing modulo 26 gives us 16-23 20-23-12 0-7-9-9 25-23. Translating back into letters we have QX UXM AHJJ ZX.

3. In each case, we translate the letters to numbers from 0 to 25, then apply the function, then translate back. (See the solution for Exercise 1c above for details.) In each case, the numerical message is 22-0-19-2-7 24-14-20-17 18-19-4-15.

a) Adding 14 to each number modulo 26 yields 10-14-7-16-21 12-2-8-5 6-7-18-3. Translating back into letters yields KOHQV MCIF GHSD.

b) Multiplying each number by 14, adding 21, and reducing modulo 26 yields 17-21-1-23-15 19-9-15-25 13-1-25-23. Translating back into letters yields RVBXP TJPZ NBZX.

c) Multiplying each number by -7, adding 1, and reducing modulo 26 yields 3-1-24-13-4 15-7-17-12 5-24-25-0. Translating back into letters yields DBYNE PHRM FYZA.

5. a) We need to undo the encryption operation, which was to choose the letter that occurred ten places later in the alphabet. Therefore we need to go backwards 10 places (or, what amounts to the same thing, forward 16 places). For example, the C decodes as S. Doing this for each letter, as in Exercise 1, gives us SURRENDER NOW.

b) BE MY FRIEND **c)** TIME FOR FUN

7. We need to play detective. First note that the two-letter word DY occurs twice. Because this was a shift cipher, we know that the first letter of this word occurs five places beyond the second letter in the alphabet. One of those letters has to be a vowel. This makes it very likely that the word is either UP or TO, corresponding to $k = 9$ or $k = 10$, respectively. Since TO is a more common word, let us assume $k = 10$. To decrypt, we shift each letter in the encrypted message backward 10 places (or forward 16 places) in the alphabet, obtaining TO SLEEP PERCHANCE TO DREAM (from *Hamlet*).

9. Following the same strategy as in Exercise 7, we try to figure out k from the fact that MW is a two-letter word in the encrypted text. What fits best is IS, with $k = 4$. If we apply that to the three-letter word, we get ANY, which seems quite promising. We now decode the entire message: ANY SUFFICIENTLY ADVANCED TECHNOLOGY IS INDISTINGUISHABLE FROM MAGIC.

11. We want to solve the congruence $c \equiv 15p + 13 \pmod{26}$ for p. To do that we will need an inverse of 15 modulo 26, which we can obtain using the Euclidean algorithm or by trial and error. It is 7, because $7 \cdot 15 = 105 = 4 \cdot 26 + 1$. Therefore we have $p = 7(c - 13)$ **mod** $26 = 7c - 91$ **mod** $26 = 7c + 13$ **mod** 26.

13. Because the most common letters are E and T, in that order, and the numerical values of E, T, Z, and J are 4, 19, 25, and 9, respectively, we will assume that $f(4) \equiv 25$ and $f(19) \equiv 9$. This means that $4a + b \equiv 25$ and $19a + b \equiv 9$, where we work modulo 26, of course. Subtracting the two equations gives $15a \equiv 10$, which simplifies to $3a \equiv 2$ (because 5 is not a factor of 26, we can divide both sides by 5). We can find an inverse of 3 modulo 26 using the Euclidean algorithm or by trial and error. It is 9, because $3 \cdot 9 = 27 = 26 + 1$. Therefore $a \equiv 9 \cdot 2 = 18$. Plugging this into $4a + b \equiv 25$ yields $b \equiv 25 - 4a = 25 - 72 \equiv 5$. We therefore guess that the encryption function is $f(p) = 18p + 5$ **mod** 26. As a check, we see that $f(4) = 25$ and $f(19) = 9$.

15. We permute each block of four by undoing the permutation σ. Because $\sigma(1) = 3$, we put the third letter first; because $\sigma(2) = 1$, we put the first letter second; and so on. This gives us BEWA REOF MART IANS, presumably meant to be BEWARE OF MARTIANS.

17. Presumably the message was translated letter by letter, such as by a shift cipher or affine cipher. (Other, nonlinear, bijections on $\mathbf{Z}_{26}$ are also possible.)

19. The numerical version of the encrypted text is 14-8-10-24-22-21-7-1-23. If we subtract the values for the key HOTHOTHOT, namely 7-14-19-7-14-19-7-14-19 and reduce modulo 26, we obtain 7-20-17-17-8-2-0-13-4, which translates to HURRICANE.

21. If l is the distance between the beginnings of the string that occurs several times, then it may be likely that the length of the key string is a factor of l. Thus if we have several such values of l, we can find their greatest common divisor and assume that the length of the key string is a factor of this gcd.

23. Suppose that we know $n = pq$ and $(p - 1)(q - 1)$, and we wish to find p and q. Here is how we do so. Expanding $(p - 1)(q - 1)$ algebraically we obtain $pq - p - q + 1 = n - p - q + 1$. Thus we know the value of $n - p - q + 1$, and so we can easily calculate the value of $p + q$ (since we know n). But we also know the value of pq, namely n. This gives us two simultaneous equations in two unknowns, and we can solve them using the quadratic formula. Here is an example. Suppose that we want to factor $n = 341$, and we are told that $(p - 1)(q - 1) = 300$. We want to find p and q. Following the argument just outlined, we know that $p + q = 341 + 1 - 300 = 42$. Plugging $q = 42 - p$ into $pq = 341$ we obtain $p(42 - p) = 341$, or $p^2 - 42p + 341 = 0$. The quadratic formula then tells us that $p = (42 + \sqrt{42^2 - 4 \cdot 341})/2 = 31$, and so the factors are 31 and $42 - 31 = 11$. Note that absolutely no trial divisions were involved here—it was just straight calculation.

25. First we translate UPLOAD into numbers: 2015 1114 0003. For each of these numbers, which we might call M, we need to compute $C = M^e$ **mod** $n = M^{17}$ **mod** 3233. Note that $n = 53 \cdot 61 = 3233$ and that $\gcd(e, (p-1)(q-1)) = \gcd(17, 52 \cdot 60) = 1$, as it should be. A computational aid tells us that 2015^{17} **mod** $3233 = 2545$, 1114^{17} **mod** $3233 = 2757$, and 0003^{17} **mod** $3233 = 1211$. Therefore the encrypted message is 2545 2757 1211.

27. This problem requires a great amount of calculation. Ideally, one should do it using a computer algebra package, such as *Mathematica* or *Maple*. Let us follow the procedure outlined in Example 9. It was computed there that the inverse of $e = 13$ modulo $n = 43 \cdot 59$ is $d = 937$. We need to compute 0667^{937} **mod** $2537 = 1808$, 1947^{937} **mod** $2537 = 1121$, and 0671^{937} **mod** $2537 = 0417$. (These calculations can in principle be done with a calculator, using the fast modular exponentiation algorithm, but it would probably take the better part of an hour and be prone to transcription errors.) Thus the original message is 1808 1121 0417, which is easily translated into letters as SILVER.

29. We follow the steps given in the text, with $p = 23$, $a = 5$, $k_1 = 8$, and $k_2 = 5$. Using *Maple*, we verify that 5 is a primitive root modulo 23, by noticing that 5^k as k runs from 0 to 21 produce distinct values (and of course 5^{22} **mod** $23 = 1$). We find that 5^8 **mod** $23 = 16$. So in Step (2), Alice sends 16 to Bob. Similarly, in Step (3), Bob sends 5^5 **mod** $23 = 20$ to Alice. In Step (4) Alice computes 20^8 **mod** $23 = 6$, and in Step (5) Bob computes 16^5 **mod** $23 = 6$. These are the same, of course, and thus 6 is the shared key.

31. See Example 10 for the procedure. First Alice translates her message into numbers: 1804 1111 0421 0417 2419 0708 1306. She then applies her decryption transformation sending each block x to x^{1183} **mod** 2867. (We should verify with *Maple* that $7 \cdot 1183$ **mod** $(60 \cdot 46) = 1$.) Using *Maple*, we see that the blocks become 1804^{1183} **mod** $2867 = 2186$, 1111^{1183} **mod** $2867 = 2087$, 0421^{1183} **mod** $2867 = 1279$, 0417^{1183} **mod** $2867 = 1251$, 2419^{1183} **mod** $2867 = 0326$, 0708^{1183} **mod** $2867 = 0816$, and 1306^{1183} **mod** $2867 = 1948$. If her friends apply Alice's encryption transformation to 2186 2087 1279 1251 0326 0816 1948, they will obtain the numbers of her original message.

33. Cathy knows the shared key $k_{\text{Alice,Bob}}$, but because she transmitted it to Alice encrypted, no one else knows it at the time Alice receives it. Alice can decrypt the first part of Cathy's message to find out what the key is. When Alice sends the second part of Cathy's message, which consists of $k_{\text{Alice,Bob}}$ encrypted with Bob's key, on to Bob, Bob can decrypt it to find the shared key, but it remains hidden from everyone else.

GUIDE TO REVIEW QUESTIONS FOR CHAPTER 4

1. Dividing 210 by 17 gives a quotient of 12 and a remainder of 6, which are the respective requested values.

2. **a)** $7 \mid a - b$ **b)** $0 \equiv -7$; $-1 \equiv -8$; $3 \equiv 17 \equiv -11$
c) $(10a + 13) - (-4b + 20) = 3(a - b) + 7(a + b - 1)$; note that 7 divides both terms

3. See Theorem 5 in Section 4.1.

4. See Example 5 in Section 4.2.

5. Octal: 154533; hexadecimal: D95B

6. 1110 1000 0110 and 1010 0000 1110 1011

7. See p. 258.

8. **a)** See Example 4 in Section 4.3 and the preceding paragraph on p. 258. **b)** $11^2 \cdot 23 \cdot 29$

9. **a)** See p. 265.
b) find all the common factors (not a good algorithm unless the numbers are really small); find the prime factorization of each integer (works well if the numbers aren't too big and therefore can be easily factored); use the Euclidean algorithm (really the best method)
c) 1 (use the Euclidean algorithm)
d) $2^3 3^5 5^5 7^3$

10. **a)** Use the Euclidean algorithm; see Example 17 in Section 4.3.
b) $7 = 5 \cdot 119 - 7 \cdot 84$

11. **a)** $a\overline{a} \equiv 1 \pmod{m}$
b) Express 1 as $sa + tm$ (see Review Question 10). Then s is the inverse of a modulo m.
c) 11

12. **a)** Multiply each side by the inverse of a modulo m. **b)** $\{\, 10 + 19k \mid k \in \mathbf{Z} \,\}$

13. **a)** See p. 278. **b)** $\{\, 17 + 140k \mid k \in \mathbf{Z} \,\}$

14. No; n could be a pseudoprime such as 341.

15. $9^{200} = 9^{18} \cdot 9^2 \cdot 9^{180} = 9^{18} \cdot 9^2 \cdot (9^{18})^{20} \equiv 1 \cdot 81 \cdot 1^{20} = 81 \equiv 5 \pmod{19}$

16. See Example 6 in Section 4.5.

17. NCCYRF NAQ BENATRF

18. **a)** See p. 298.
b) The amount of shift, k, is kept secret. It is needed both to encode and to decode messages.
c) Although the key for decoding, d, is kept secret, the keys for encoding, n and e, are published.

19. See pp. 299–301.

20. See p. 302.

SUPPLEMENTARY EXERCISES FOR CHAPTER 4

1. Because $89697 - 43179 = 46518$, we can conclude that the number of miles is congruent to 46,518 modulo 100,000. So it is $46518 + 100000k$ for some natural number k (the number of miles driven cannot be negative). Thus the actual number of miles driven is 46,518 or 146,518, or 246,518, or ....

3. Obviously there are an infinite number of possible answers. The numbers congruent to 5 modulo 17 include 5, 22, 39, 56, ..., as well as -12, -29, -46, ...

5. From the hypothesis $ac \equiv bc \pmod{m}$ we know that $ac - bc = km$ for some integer k. Divide both sides by c to obtain the equation $a - b = (km)/c$. Now the left-hand side is an integer, and so the right-hand side must be an integer as well. In other words, $c \mid km$. Letting $d = \gcd(m, c)$, we write $c = de$. Then the way that c divides km is that $d \mid m$ and $e \mid k$ (since no factor of e divides m/d). Thus our equation reduces to $a - b = (k/e)(m/d)$, where both factors on the right are integers. By definition, this means that $a \equiv b \pmod{m/d}$.

7. We give an indirect proof. If n is odd, then $n = 2k+1$ for some integer k. Therefore $n^2 + 1 = (2k+1)^2 + 1 = 4k^2 + 4k + 2 \equiv 2 \pmod{4}$. But perfect squares of even numbers are congruent to 0 modulo 4 (because $(2m)^2 = 4m^2$), and perfect squares of odd numbers are odd, so $n^2 + 1$ is not a perfect square.

9. The contribution of the digit in the kth column from the right in the binary expansion of a positive integer is 2^k, where we consider the units digit to be 0 columns from the right. Therefore for $k \geq 3$, the contribution is divisible by $2^3 = 8$. Any sequence of three digits other than 000 in the three right-most columns will contribute between 1 and 7, causing the number not to be divisible by 8. Thus a positive integer written in binary is divisible by 8 if and only if its last three digits are 000.

11. We assume that someone has chosen a positive integer less than 2^n, which we are to guess. We ask the person to write the number in binary, using leading 0's if necessary to make it n bits long. We then ask "Is the first bit a 1?", "Is the second bit a 1?", "Is the third bit a 1?", and so on. After we know the answers to these n questions, we will know the number, because we will know its binary expansion.

13. Without loss of generality, we may assume that the given integer is positive (since $n \mid a$ if and only if $n \mid (-a)$, and the case $a = 0$ is trivial). Let the decimal expansion of the integer a be given by $a = (a_{n-1}a_{n-2}\ldots a_1a_0)_{10}$. Thus $a = 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \cdots + 10a_1 + a_0$. Since $10 \equiv 1 \pmod 9$, we have $a \equiv a_{n-1} + a_{n-2} + \cdots + a_1 + a_0 \pmod 9$. Therefore $a \equiv 0 \pmod 9$ if and only if the sum of the digits is congruent to 0 (mod 9). Since being divisible by 9 is the same as being congruent to 0 (mod 9), we have proved that an integer is divisible by 9 if and only if the sum of its decimal digits is divisible by 9.

15. Note that $Q_n \geq 2$. By the Fundamental Theorem of Arithmetic, Q_n has a prime factorization. Because k is a factor of $n!$ for all $k \leq n$, when Q_n is divided by k the remainder will be 1; therefore k is not a factor of Q_n. Thus Q_n must have a prime factor greater than n. (We have shown that in fact all of the prime factors of Q_n will be greater than n.)

17. The numbers whose decimal expansion ends in 1 are precisely those integers in the arithmetic progression $10k + 1$. Dirichlet's theorem guarantees that this sequence includes infinitely many primes. The first few are 11, 31, 41, 61, 71, 101, 131, ...

19. Note that even numbers greater than 2 are composite and that 9 is composite. Therefore every odd number greater than 11 is the sum of two composite numbers ($13 = 4 + 9$, $15 = 6 + 9$, $17 = 8 + 9$, and so on). Similarly, because 8 is composite, so are all even numbers greater than 11: $12 = 4+8$, $14 = 6+8$, $16 = 8+8$, and so on.

21. Assume that every even integer greater than 2 is the sum of two primes, and let n be an integer greater than 5. If n is odd, then we can write $n = 3 + (n - 3)$, decompose $n - 3 = p + q$ into the sum of two primes (since $n - 3$ is an even integer greater than 2), and therefore have written $n = 3 + p + q$ as the sum of three primes. If n is even, then we can write $n = 2 + (n - 2)$, decompose $n - 2 = p + q$ into the sum of two primes (since $n - 2$ is an even integer greater than 2), and therefore have written $n = 2 + p + q$ as the sum of three primes. For the converse, assume that every integer greater than 5 is the sum of three primes, and let n be an even integer greater than 2. By our assumption we can write $n + 2$ as the sum of three primes. Since $n + 2$ is even, these three primes cannot all be odd, so we have $n + 2 = 2 + p + q$, where p and q are primes, whence $n = p + q$, as desired.

23. We give a proof by contradiction. For this proof we need a fact about polynomials, namely that a nonconstant polynomial can take on the same value only a finite number of times. (Think about its graph—a polynomial of degree n has at most n "wiggles" and so a horizontal line can intersect it at most n times. Alternatively, this statement follows from the Fundamental Theorem of Algebra, which guarantees that a polynomial of degree n has at most n 0's; if $f(x) = a$, then x is a zero of the polynomial $f(x) - a$.) Our given polynomial f can take on the values 0 and ± 1 only finitely many times, so if there is not some y such that $f(y)$ is composite,

then there must be some x_0 such that $\pm f(x_0)$ is prime, say p. Now look at $f(x_0 + kp)$. When we plug $x_0 + kp$ in for x in the polynomial and multiply it out, every term will contain a factor of p except for the terms that form $f(x_0)$. Therefore $f(x_0 + kp) = f(x_0) + mp = (m \pm 1)p$ for some integer m. As k varies, this value can be 0 or p or $-p$ only finitely many times; therefore it must be a different multiple of p and therefore a composite number for some values of k, and our proof is complete.

25. $\gcd(10223, 33341) = \gcd(10223, 2672) = \gcd(2672, 2207) = \gcd(2207, 465) = \gcd(465, 347) = \gcd(347, 118) = \gcd(118, 111) = \gcd(111, 7) = \gcd(7, 6) = \gcd(6, 1) = \gcd(1, 0) = 1$

27. By Lemma 1 in Section 4.3, $\gcd(2n + 1, 3n + 2) = \gcd(2n + 1, n + 1)$, since $2n + 1$ goes once into $3n + 2$ with a remainder of $n + 1$. Now if we divide $n + 1$ into $2n + 1$, we get a remainder of n, so the answer must equal $\gcd(n + 1, n)$. At this point, the remainder when dividing n into $n + 1$ is 1, so the answer must equal $\gcd(n, 1)$, which is clearly 1. Thus the answer is 1.

29. It might be helpful to read the solution to Exercise 55 in Section 4.3 to see the philosophy behind this approach. Suppose by way of contradiction that $q_1, q_2, \ldots, q_n$ are all the primes of the form $6k + 5$. Thus $q_1 = 5$, $q_2 = 11$, and so on. Let $Q = 6q_1q_2 \cdots q_n - 1$. We note that Q is of the form $6k+5$, where $k = q_1q_2 \cdots q_n - 1$. Now Q has a prime factorization $Q = p_1p_2 \cdots p_t$. Clearly no p_i is 2, 3, or any q_j, because the remainder when Q is divided by 2 is 1, by 3 is 2, and by q_j is $q_j - 1$. All odd primes other than 3 are of the form $6k + 1$ or $6k + 5$, and the product of primes of the form $6k + 1$ is also of this form. Therefore at least one of the p_i's must be of the form $6k + 5$, a contradiction.

31. Let's try the strategy used in the proof of Theorem 3 in Section 4.3. Suppose that $p_1, p_2, \ldots, p_n$ are the only primes of the form $4k + 1$. Notice that the product of primes of this form is again of this form, because $(4k_1 + 1)(4k_2 + 1) = 16k_1k_2 + 4k_1 + 4k_2 + 1 = 4(4k_1k_2 + k_1 + k_2) + 1$. We could try looking at $4p_1p_2 \cdots p_n + 1$, which is again of this form. By the Fundamental Theorem of Arithmetic, it has prime factors, and clearly no p_i is a factor. Unfortunately, we cannot be guaranteed that any of its prime factors are of the form $4k + 1$, because the product of two odd primes not of this form, namely of the form $4k + 3$, is of the form $4k + 1$; indeed, $(4k_1 + 3)(4k_2 + 3) = 16k_1k_2 + 12k_1 + 12k_2 + 9 = 4(4k_1k_2 + 3k_1 + 3k_2 + 2) + 1$. Thus the proof breaks down at this point.

33. **a)** Since 2 is a factor of all three of these integers, this set is not mutually relatively prime.

b) Since 12 and 25 share no common factors, this set has greatest common divisor 1, so it is mutually relatively prime. (It is possible for every pair of integers in a set of mutually relatively prime integers to have a nontrivial common factor (see Exercise 34), but certainly if two of the integers in a set are relatively prime, then the set is automatically mutually relatively prime.)

c) Since 15 and 28 share no common factors, this set has greatest common divisor 1, so it is mutually relatively prime.

d) Since 21 and 32 share no common factors, this set has greatest common divisor 1, so it is mutually relatively prime.

35. If n is even, then n^4+4^n is an even composite number, so we can restrict ourselves to n odd. The appearance of 4 suggests that we might work modulo 5, so let's try that. If n is not divisible by 5, then $n^4 \equiv 1 \pmod 5$ by Fermat's little theorem, and since n is odd, $4^n \equiv (-1)^n = -1 \pmod 5$. Therefore n^4+4^n is divisible by 5. So except for $n = 1$, in which case $n^4+4^n = 5$ is prime, the only possible values of n that can result in a prime value for $n^4 + 4^n$ are 5, 15, 25, and so on. *Maple* tells us that $5^4 + 4^5 = 17 \cdot 97$, $15^4 + 4^{15} = 36833 \cdot 29153$, and $25^4 + 4^{25} = 29 \cdot 373 \cdot 3121 \cdot 33350257$. So let us try to factor $n^4 + 4^n$ algebraically. It is not at all obvious how to discover these factors, but if we multiply out

$$(n^2 + 2^{\frac{n+1}{2}}n + 2^n)(n^2 - 2^{\frac{n+1}{2}}n + 2^n)$$

we get $n^4 + 4^n$. (Because n is odd, the exponent $\frac{n+1}{2}$ is an integer.) It only remains to show that each of these factors is greater than 1. The first is clearly so. The second factor takes on the values 5, 17, 65, and 305 for $n = 3$, 5, 7, and 9, respectively. Clearly for large n the 2^n term far exceeds the $-2^{\frac{n+1}{2}}n$ term, and our proof is complete.

37. The least common multiple of 6 and 15 is 30, so the set of solutions will be given modulo 30 (see Exercise 38). Since the numbers involved here are so small, it is probably best simply to write down the solutions of $x \equiv 4 \pmod 6$ and then see which, if any, of them are also solutions of $x \equiv 13 \pmod{15}$. The solutions of the first congruence, up to 30, are 4, 10, 16, 22, and 28. Only 28 is congruent to 13 modulo 15. Therefore the general solution is all numbers congruent to 28 modulo 30, i.e., ..., -32, -2, 28, 58, ...

39. *Maple* tells us that this is true, namely that $n^9 - n$ **mod** $30 = 0$ for all n (we need only check n from 0 to 29). For a more human-oriented proof (conceptual rather than computational), notice that it suffices to show that $n^9 - n \equiv 0 \pmod 2$, $n^9 - n \equiv 0 \pmod 3$, and $n^9 - n \equiv 0 \pmod 5$. The first is obvious (odd minus odd, and even minus even, are both even). The second follows from Fermat's little theorem, because $n^9 = (n^3)^3 \equiv n^3 \equiv n \pmod 3$. The third also follows from that theorem, because $n^9 = n^4 \cdot n^5 \equiv 1 \cdot n \equiv n \pmod 5$.

41. By Fermat's little theorem, $p^{q-1} \equiv 1 \pmod q$ and clearly $q^{p-1} \equiv 0 \pmod q$. Therefore $p^{q-1} + q^{p-1} \equiv 1 + 0 = 1 \pmod q$. Similarly, $p^{q-1} + q^{p-1} \equiv 1 \pmod p$. It follows from the Chinese remainder theorem that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

43. Because 1 and 3 are both relatively prime to 10, if the congruence is satisfied by the correct ISBN-13, it cannot be satisfied if one of the digits is changed. In particular, if a_i is changed from x to y, then the change in the left-hand side of the congruence is either $y - x$ or $3(y - x)$, modulo 10, neither of which can be 0. Therefore the sum can no longer be 0 modulo 10.

45. Subtract d_9 from both sides of the congruence and multiply through by -1 to obtain

$$-3(d_1 + d_4 + d_7) - 7(d_2 + d_5 + d_8) - (d_3 + d_6) \equiv d_9 \pmod{10}.$$

This is equivalent to

$$7(d_1 + d_4 + d_7) + 3(d_2 + d_5 + d_8) + 9(d_3 + d_6) \equiv d_9 \pmod{10}.$$

Because $0 \leq d_9 \leq 9$, it follows that $d_9 = 7(d_1 + d_4 + d_7) + 3(d_2 + d_5 + d_8) + 9(d_3 + d_6)$ **mod** 10. We calculate with the given eight digits to conclude that $d_9 = 7(1+0+0)+3(1+0+2)+9(1+0)$ **mod** $10 = 25$ **mod** $10 = 5$.

47. We need to find the inverse function. In other words, given $(ap + b)$ **mod** 26, how does one recover p? Working modulo 26, if we subtract b, then we will have ap. If we then multiply by an inverse of a (which must exist since we are assuming that $\gcd(a, 26) = 1$), we will have p back. Therefore the decryption function is $g(q) = \overline{a}(q - b)$ **mod** 26, where $\overline{a}$ is an inverse of a modulo 26. In this case, $a = 7$ and $b = 10$. Computing the inverse of 7 modulo 26 by the techniques of Section 4.4 (or by using *Maple*), we find $\overline{a} = 15$, so the decryption function is $g(q) = 15(q - 10)$ **mod** 26. Translating the letters into numbers, we see that the encrypted message is 11–9–12–10–6 12–6–12–23–5 16–4–23–12–22. Applying this function, we obtain the decrypted message 15–11–4–0–18 4–18–4–13–3 12–14–13–4–24. This translates into PLEAS ESEND MONEY, which, after correcting the spacing, is PLEASE SEND MONEY.

49. **a)** The seed is 23 (X); adding this to the first character of the plaintext, 19 (T), gives 16, which is Q. Therefore the first character of the ciphertext is Q. The next character of the keystream is the aforementioned T (19); add this to H (7) to get 0 (A), so the next character of the ciphertext is A. We continue in this manner, producing the encrypted message QAL HUVEM AT WVESGB.

b) Again the seed is 23 (X); adding this to the first character of the plaintext, 19 (T), gives 16, which is Q. Therefore the first character of the ciphertext is Q. The next character of the keystream is the aforementioned Q (16); add this to H (7) to get 23 (X), so the next character of the ciphertext is X. We continue in this manner, producing the encrypted message QXB EVZZL ZEVZZRFS.

WRITING PROJECTS FOR CHAPTER 4

Books and articles indicated by bracketed symbols below are listed near the end of this manual. You should also read the general comments and advice you will find there about researching and writing these essays.

1. As usual, the Web is an excellent resource here. Check out the GIMPS page and then follow its links: `www.mersenne.org/prime.htm`.

2. These primes are sometimes jokingly referred to as "industrial strength primes." Number theory textbooks, such as [Ro3], would be a place to start. See also the article [Le3].

3. One can often find mathematical news reported in *The New York Times* and other nontechnical media. Search an index to find a story about this topic. (While you're looking at back issues of the *Times*, read the January 31, 1995, article on the solution to Fermat's last theorem.)

4. Your essay should mention the RSA-129 project. See *The New York Times*, around the spring of 1994 (use its index). For an expository article, try [Po].

5. There are dozens of books on computer hardware and circuit design that discuss the algorithms and circuits used in performing these operations. If you are a computer science or computer engineering major, you probably have taken (or will take) a course that deals with these topics. See [Ko2] and similar books.

6. A traditional history of mathematics book should be helpful here; try [Bo4] or [Ev3].

7. This topic has taken on a lot of significance recently as randomized algorithms become more and more important. The August/September 1994 issue of *SIAM News* (the newsletter of the Society for Industrial and Applied Mathematics) has a provocative article on the subject. See also [La1], or for older material in a textbook try volume 2 of [Kn].

8. The Web has the answers. Try `www.skynet.ie/~martin/pages/iban.html` or Wikipedia.

9. The Web has the answers.

10. The author's number theory text ([Ro3]) has material on this topic. The amazing mathematician John H. Conway (inventor of the Game of Life, among other things) has devised what he calls the Doomsday Algorithm, and it works quite fast with practice. See [BeCo]. (Conway can determine any day of the week mentally in a second or two.)

11. This topic gets into the news on a regular basis. Try *The New York Times* index. See also Writing Project 4, above, and 12, below.

12. If I encrypt my signature with my private key, then I will produce something that will decrypt (using my public key) as my signature. Furthermore, no one else can do this, since no one else knows my private key. Good sources for cryptography include [Be], [MeOo], and [St2].

13. Several excellent books have appeared in the past decade on cryptography, such as [MeOo]. Many of them, including that one, will treat this topic.

14. Suppose that we use a prime for n. To find a private decryption key from the corresponding public encryption key e, one would need to find a number d that is an inverse for e modulo $n-1$ so that the calculation shown before Example 9 in Section 4.6 can go through. But finding such a d is easy using the Euclidean algorithm, because the person doing this would already know $n-1$. (In particular, to find d, one can work backward through the steps of the Euclidean algorithm to express 1 as a linear combination of e and $n-1$; then d is the coefficient of e in this linear combination.) The important point in the actual RSA system is that the person trying to find this inverse will not know $(p-1)(q-1)$ and therefore cannot simply use the Euclidean algorithm.

15. Start with Wikipedia.