CHAPTER 4
Number Theory and Cryptography

SECTION 4.1 Divisibility and Modular Arithmetic

2. **a)** $1 \mid a$ since $a = 1 \cdot a$. **b)** $a \mid 0$ since $0 = a \cdot 0$.

4. Suppose $a \mid b$, so that $b = at$ for some t, and $b \mid c$, so that $c = bs$ for some s. Then substituting the first equation into the second, we obtain $c = (at)s = a(ts)$. This means that $a \mid c$, as desired.

6. Under the hypotheses, we have $c = as$ and $d = bt$ for some s and t. Multiplying we obtain $cd = ab(st)$, which means that $ab \mid cd$, as desired.

8. The simplest counterexample is provided by $a = 4$ and $b = c = 2$.

10. In each case we can carry out the arithmetic on a calculator.
a) Since $8 \cdot 5 = 40$ and $44 - 40 = 4$, we have quotient 44 **div** $8 = 5$ and remainder 44 **mod** $8 = 4$.
b) Since $21 \cdot 37 = 777$, we have quotient 777 **div** $21 = 37$ and remainder 777 **mod** $21 = 0$.
c) As above, we can compute 123 **div** $19 = 6$ and 123 **mod** $19 = 9$. However, since the dividend is negative and the remainder is nonzero, the quotient is $-(6+1) = -7$ and the remainder is $19 - 9 = 10$. To check that -123 **div** $19 = -7$ and -123 **mod** $19 = 10$, we note that $-123 = (-7)(19) + 10$.
d) Since 1 **div** $23 = 0$ and 1 **mod** $23 = 1$, we have -1 **div** $23 = -1$ and -1 **mod** $23 = 22$.
e) Since 2002 **div** $87 = 23$ and 2002 **mod** $87 = 1$, we have -2002 **div** $87 = -24$ and 2002 **mod** $87 = 86$.
f) Clearly 0 **div** $17 = 0$ and 0 **mod** $17 = 0$.
g) We have 1234567 **div** $1001 = 1233$ and 1234567 **mod** $1001 = 334$.
h) Since 100 **div** $101 = 0$ and 100 **mod** $101 = 100$, we have -100 **div** $101 = -1$ and -100 **mod** $101 = 1$.

12. **a)** Because 100 **mod** $24 = 4$, the clock reads the same as 4 hours after 2:00, namely 6:00.
b) Essentially we are asked to compute $12 - 45$ **mod** $24 = -33$ **mod** $24 = -33 + 48$ **mod** $24 = 15$. The clock reads 15:00.
c) Because $168 \equiv 0 \pmod{24}$, the clock read 19:00.

14. This problem is equivalent to asking for the right-hand side **mod** 19. So we just do the arithmetic and compute the remainder upon division by 19.
a) $13 \cdot 11 = 143 \equiv 10 \pmod{19}$ **b)** $8 \cdot 3 = 24 \equiv 5 \pmod{19}$
c) $11 - 3 = 8 \pmod{19}$ **d)** $7 \cdot 11 + 3 \cdot 3 = 86 \equiv 10 \pmod{19}$
e) $2 \cdot 11^2 + 3 \cdot 3^2 = 269 \equiv 3 \pmod{19}$ **f)** $11^3 + 4 \cdot 3^3 = 1439 \equiv 14 \pmod{19}$

16. Assume that $a \equiv b \pmod{m}$. This means that $m \mid a - b$, say $a - b = mc$, so that $a = b + mc$. Now let us compute a **mod** m. We know that $b = qm + r$ for some nonnegative r less than m (namely, $r = b$ **mod** m). Therefore we can write $a = qm + r + mc = (q + c)m + r$. By definition this means that r must also equal a **mod** m. That is what we wanted to prove.

18. By Theorem 2 we have $a = dq + r$ with $0 \le r < d$. Dividing the equation by d we obtain $a/d = q + (r/d)$, with $0 \le (r/d) < 1$. Thus by definition it is clear that q is $\lfloor a/d \rfloor$. The original equation shows, of course, that $r = a - dq$, proving the second of the original statements.

20. In each case we just apply the division algorithm (carry out the division) to obtain the quotient and remainder, as in elementary school. However, if the dividend is negative, we must make sure to make the remainder positive, which may involve a quotient 1 less than might be expected.

a) Since $-17 = 2 \cdot (-9) + 1$, the remainder is 1. That is, -17 **mod** $2 = 1$. Note that we do not write $-17 = 2 \cdot (-8) - 1$, so -17 **mod** $2 \neq -1$.

b) Since $144 = 7 \cdot 20 + 4$, the remainder is 4. That is, 144 **mod** $7 = 4$.

c) Since $-101 = 13 \cdot (-8) + 3$, the remainder is 3. That is, -101 **mod** $13 = 3$. Note that we do not write $-101 = 13 \cdot (-7) - 10$; we can't have -101 **mod** $13 = -10$, because a **mod** b is always nonnegative.

d) Since $199 = 19 \cdot 10 + 9$, the remainder is 9. That is, 199 **mod** $19 = 9$.

22. In each case we do the division and report the quotient (a **div** m) and the remainder (a **mod** m). It is important to remember that the quotient needs to be rounded down, which means that if the dividend is negative, as in part **(a)**, the quotient is a number with a *larger* absolute value.

a) $111/99$ is between 1 and 2, so the quotient is -2 and the remainder is $-111-(-2)\cdot 99 = -111+198 = 87$.

b) $-9999/101 = -99$, so that is the quotient and the remainder is 0.

c) 10299 **div** $999 = 10$, 10299 **mod** $999 = 10299 - 10 \cdot 999 = 309$

d) 123456 **div** $1001 = 123$, 123456 **mod** $1001 = 333$

24. **a)** We can get into the desired range and stay within the same modular equivalence class by subtracting $2 \cdot 23$, so the answer is $a = 43 - 46 = -3$.

b) $17 - 29 = -12$, so $a = -12$. **c)** $a = -11 + 5 \cdot 21 = 94$

26. Among the infinite set of correct answers are 4, 16, -8, 1204, and -7016360.

28. We just subtract 3 from the given number; the answer is "yes" if and only if the difference is divisible by 7.

a) $37 - 3$ **mod** $7 = 34$ **mod** $7 = 6 \neq 0$, so $37 \not\equiv 3 \pmod 7$.

b) $66 - 3$ **mod** $7 = 63$ **mod** $7 = 0$, so $66 \equiv 3 \pmod 7$.

c) $-17 - 3$ **mod** $7 = -20$ **mod** $7 = 1 \neq 0$, so $-17 \not\equiv 3 \pmod 7$.

d) $-67 - 3$ **mod** $7 = -70$ **mod** $7 = 0$, so $-67 \equiv 3 \pmod 7$.

30. **a)** $(177$ **mod** $31 + 270$ **mod** $31)$ **mod** $31 = (22 + 22)$ **mod** $31 = 44$ **mod** $31 = 13$

b) $(177$ **mod** $31 \cdot 270$ **mod** $31)$ **mod** $31 = (22 \cdot 22)$ **mod** $31 = 484$ **mod** $31 = 19$

32. **a)** $(19^2$ **mod** $41)$ **mod** $9 = (361$ **mod** $41)$ **mod** $9 = 33$ **mod** $9 = 6$

b) $(32^3$ **mod** $13)^2$ **mod** $11 = (32768$ **mod** $13)^2$ **mod** $11 = 8^2$ **mod** $11 = 64$ **mod** $11 = 9$

c) $(7^3$ **mod** $23)^2$ **mod** $31 = (343$ **mod** $23)^2$ **mod** $31 = 21^2$ **mod** $31 = 441$ **mod** $31 = 7$

d) $(21^2$ **mod** $15)^3$ **mod** $22 = (441$ **mod** $15)^3$ **mod** $22 = 6^3$ **mod** $22 = 216$ **mod** $22 = 18$

34. From $a \equiv b \pmod m$ we know that $b = a + sm$ for some integer s. Similarly, $d = c + tm$. Subtracting, we have $b - d = (a - c) + (s - t)m$, which means that $a - c \equiv b - d \pmod m$.

36. From $a \equiv b \pmod m$ we know that $b = a + sm$ for some integer s. Multiplying by c we have $bc = ac + s(mc)$, which means that $ac \equiv bc \pmod{mc}$.

38. There are two cases. If n is even, then $n = 2k$ for some integer k, so $n^2 = 4k^2$, which means that $n^2 \equiv 0 \pmod 4$. If n is odd, then $n = 2k+1$ for some integer k, so $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, which means that $n^2 \equiv 1 \pmod 4$.

40. Write $n = 2k + 1$ for some integer k. Then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$. Since either k or $k+1$ is even, $4k(k+1)$ is a multiple of 8. Therefore $n^2 - 1$ is a multiple of 8, so $n^2 \equiv 1 \pmod 8$.

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

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

This is true, because both sides equal $(a+b+c)$ **mod** m, addition of integers is associative. Similarly, addition in $\mathbf{Z}_m$ is commutative because addition in $\mathbf{Z}$ is commutative, and 0 is the additive identity for $\mathbf{Z}_m$ because 0 is the additive identity for $\mathbf{Z}$. Finally, to see that $m - a$ is an inverse of a modulo m, we just note that $(m - a) +_m a = m - a + a$ **mod** $m = 0$. (It is also worth observing that 0 is its own additive inverse in $\mathbf{Z}_m$.)

44. The distributive property of multiplication over addition states that $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ whenever $a, b, c \in \mathbf{Z}_m$. By the definition of these modular operations and Corollary 2, the left-hand side equals $a(b + c)$ **mod** m and the right-hand side equals $ab + ac$ **mod** m. These are equal because multiplication is distributive over addition for integers.

46. 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; thus it would suffice to list $a + b$ and $a \cdot b$ only for $a \le b$.

$$\begin{array}{llllll}
0+0=0 & 0+1=1 & 0+2=2 & 0+3=3 & 0+4=4 & 0+5=5 \\
1+0=1 & 1+1=2 & 1+2=3 & 1+3=4 & 1+4=5 & 1+5=0 \\
2+0=2 & 2+1=3 & 2+2=4 & 2+3=5 & 2+4=0 & 2+5=1 \\
3+0=3 & 3+1=4 & 3+2=5 & 3+3=0 & 3+4=1 & 3+5=2 \\
4+0=4 & 4+1=5 & 4+2=0 & 4+3=1 & 4+4=2 & 4+5=3 \\
5+0=5 & 5+1=0 & 5+2=1 & 5+3=2 & 5+4=3 & 5+5=4
\end{array}$$

$$\begin{array}{llllll}
0 \cdot 0 = 0 & 0 \cdot 1 = 0 & 0 \cdot 2 = 0 & 0 \cdot 3 = 0 & 0 \cdot 4 = 0 & 0 \cdot 5 = 0 \\
1 \cdot 0 = 0 & 1 \cdot 1 = 1 & 1 \cdot 2 = 2 & 1 \cdot 3 = 3 & 1 \cdot 4 = 4 & 1 \cdot 5 = 5 \\
2 \cdot 0 = 0 & 2 \cdot 1 = 2 & 2 \cdot 2 = 4 & 2 \cdot 3 = 0 & 2 \cdot 4 = 2 & 2 \cdot 5 = 4 \\
3 \cdot 0 = 0 & 3 \cdot 1 = 3 & 3 \cdot 2 = 0 & 3 \cdot 3 = 3 & 3 \cdot 4 = 0 & 3 \cdot 5 = 3 \\
4 \cdot 0 = 0 & 4 \cdot 1 = 4 & 4 \cdot 2 = 2 & 4 \cdot 3 = 0 & 4 \cdot 4 = 4 & 4 \cdot 5 = 2 \\
5 \cdot 0 = 0 & 5 \cdot 1 = 5 & 5 \cdot 2 = 4 & 5 \cdot 3 = 3 & 5 \cdot 2 = 2 & 5 \cdot 5 = 1
\end{array}$$

SECTION 4.2 Integer Representations and Algorithms

2. To convert from decimal to binary, we successively divide by 2. We write down the remainders so obtained from right to left; that is the binary representation of the given number.

a) Since 321/2 is 160 with a remainder of 1, the rightmost digit is 1. Then since 160/2 is 80 with a remainder of 0, the second digit from the right is 0. We continue in this manner, obtaining successive quotients of 40, 20, 10, 5, 2, 1, and 0, and remainders of 0, 0, 0, 0, 1, 0, and 1. Putting all these remainders in order from right to left we obtain $(1\ 0100\ 0001)_2$ as the binary representation. We could, as a check, expand this binary numeral: $2^0 + 2^6 + 2^8 = 1 + 64 + 256 = 321$.

b) We could carry out the same process as in part **(a)**. Alternatively, we might notice that $1023 = 1024 - 1 = 2^{10} - 1$. Therefore the binary representation is 1 less than $(100\ 0000\ 0000)_2$, which is clearly $(11\ 1111\ 1111)_2$.

c) If we carry out the divisions by 2, the quotients are 50316, 25158, 12579, 6289, 3144, 1572, 786, 393, 196, 98, 49, 24, 12, 6, 3, 1, and 0, with remainders of 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 1, and 1. Putting the remainders in order from right to left we have $(1\ 1000\ 1001\ 0001\ 1000)_2$.

4. **a)** $1 + 2 + 8 + 16 = 27$ **b)** $1 + 4 + 16 + 32 + 128 + 512 = 693$

c) $2 + 4 + 8 + 16 + 32 + 128 + 256 + 512 = 958$

d) $1 + 2 + 4 + 8 + 16 + 1024 + 2048 + 4096 + 8192 + 16384 = 31775$

6. We follow the procedure of Example 7.

a) $(1111\ 0111)_2 = (011\ 110\ 111)_2 = (367)_8$

b) $(1010\ 1010\ 1010)_2 = (101\ 010\ 101\ 010)_2 = (5252)_8$

c) $(111\ 0111\ 0111\ 0111)_2 = (111\ 011\ 101\ 110\ 111)_2 = (73567)_8$

d) $(101\ 0101\ 0101\ 0101)_2 = (101\ 010\ 101\ 010\ 101)_2 = (52525)_8$

8. 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 have $(\text{BADFACED})_{16} = (10111010110111111010110011101101)_2$. Following the convention shown in Exercise 3 of grouping binary digits by fours, we can write this in a more readable form as 1011 1010 1101 1111 1010 1100 1110 1101.

10. We follow the procedure of Example 7.

a) $(1111\ 0111)_2 = (\text{F7})_{16}$ **b)** $(1010\ 1010\ 1010)_2 = (\text{AAA})_{16}$

c) $(111\ 0111\ 0111\ 0111)_2 = (7777)_{16}$ **d)** $(101\ 0101\ 0101\ 0101)_2 = (5555)_{16}$

12. Following Example 7, we simply write the hexadecimal equivalents of each group of four binary digits. Note that we group from the right, so the left-most group, which is just 1, becomes 0001. Thus we have $(0001\ 1000\ 0110\ 0011)_2 = (1863)_{16}$.

14. Let $(\ldots h_2h_1h_0)_{16}$ be the hexadecimal expansion of a positive integer. The value of that integer is, therefore, $h_0 + h_1 \cdot 16 + h_2 \cdot 16^2 + \cdots = h_0 + h_1 \cdot 2^4 + h_2 \cdot 2^8 + \cdots$. If we replace each hexadecimal digit h_i by its binary expansion $(b_{i3}b_{i2}b_{i1}b_{i0})_2$, then $h_i = b_{i0} + 2b_{i1} + 4b_{i2} + 8b_{i3}$. Therefore the value of the entire number is $b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + (b_{10} + 2b_{11} + 4b_{12} + 8b_{13}) \cdot 2^4 + (b_{20} + 2b_{21} + 4b_{22} + 8b_{23}) \cdot 2^8 + \cdots = b_{00} + 2b_{01} + 4b_{02} + 8b_{03} + 2^4b_{10} + 2^5b_{11} + 2^6b_{12} + 2^7b_{13} + 2^8b_{20} + 2^9b_{21} + 2^{10}b_{22} + 2^{11}b_{23} + \cdots$, which is the value of the binary expansion $(\ldots b_{23}b_{22}b_{21}b_{20}b_{13}b_{12}b_{11}b_{10}b_{03}b_{02}b_{01}b_{00})_2$.

16. Let $(\ldots d_2d_1d_0)_8$ be the octal expansion of a positive integer. The value of that integer is, therefore, $d_0 + d_1 \cdot 8 + d_2 \cdot 8^2 + \cdots = d_0 + d_1 \cdot 2^3 + d_2 \cdot 2^6 + \cdots$. If we replace each octal digit d_i by its binary expansion $(b_{i2}b_{i1}b_{i0})_2$, then $d_i = b_{i0} + 2b_{i1} + 4b_{i2}$. Therefore the value of the entire number is $b_{00} + 2b_{01} + 4b_{02} + (b_{10} + 2b_{11} + 4b_{12}) \cdot 2^3 + (b_{20} + 2b_{21} + 4b_{22}) \cdot 2^6 + \cdots = b_{00} + 2b_{01} + 4b_{02} + 2^3b_{10} + 2^4b_{11} + 2^5b_{12} + 2^6b_{20} + 2^6b_{21} + 2^8b_{22} + \cdots$, which is the value of the binary expansion $(\ldots b_{22}b_{21}b_{20}b_{12}b_{11}b_{10}b_{02}b_{01}b_{00})_2$.

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

20. Note that $64 = 2^6 = 8^2$. In base 64 we need 64 symbols, from 0 up to something representing 63 (maybe we could use, for example, digits up to 9, then lower and upper case letters from a to Z, and finally symbols @ and \$ to represent 62 and 63). Corresponding to each such symbol would be a binary string of six digits, from 000000 for 0, through 001010 for a, 100011 for z, 100100 for A, 111101 for Z, 111110 for @, and 111111 for \$. To translate from binary to base 64, we group the binary digits from the right in groups of 6 and use the list of correspondences to replace each six bits by one base-64 digit. To convert from base 64 to binary, we just replace each base-64 digit by its corresponding six bits.

For conversions between octal and base 64, we change the binary strings in our table to octal strings, replacing each 6-bit string by its 2-digit octal equivalent, and then follow the same procedures as above, interchanging base-64 digits and 2-digit strings of octal digits.

22. 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 three (for example, $2 + 1 = 10$ and $2 \cdot 2 = 11$). When a digit-by-digit answer is too large to fit (i.e., greater than 2), 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). A calculator or computer algebra system makes doing the conversions tolerable. For convenience, we leave off the "3" subscripts throughout.

a) $112 + 210 = 1022$ (decimal: $14 + 21 = 35$)
$112 \cdot 210 = 101{,}220$ (decimal: $14 \cdot 21 = 294$)

b) $2112 + 12021 = 21{,}210$ (decimal: $68 + 142 = 210$)
$2112 \cdot 12021 = 111{,}020{,}122$ (decimal: $68 \cdot 142 = 9656$)

c) $20001 + 1111 = 21{,}112$ (decimal: $163 + 40 = 203$)
$20001 \cdot 1111 = 22{,}221{,}111$ (decimal: $163 \cdot 40 = 6520$)

d) $120021 + 2002 = 122{,}100$ (decimal: $412 + 56 = 468$)
$120021 \cdot 2002 = 1{,}011{,}122{,}112$ (decimal: $412 \cdot 56 = 23{,}072$)

24. 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 sixteen (for example, $7 + 8 = \text{F}$ and $7 \cdot 8 = 38$). When a digit-by-digit answer is too large to fit (i.e., greater than F), 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). A calculator or computer algebra system makes doing the conversions tolerable, specially if we use built-in functions for doing so. For convenience, we leave off the "16" subscripts throughout.

a) $1\text{AB} + \text{BBC} = \text{D67}$ (decimal: $427 + 3004 = 3431$)
$1\text{AB} \cdot \text{BBC} = 139{,}294$ (decimal: $427 \cdot 3004 = 1{,}282{,}708$)

b) $20\text{CBA} + \text{A01} = 21{,}6\text{BB}$ (decimal: $134{,}330 + 2561 = 136{,}891$)
$20\text{CBA} \cdot \text{A01} = 14{,}815{,}0\text{BA}$ (decimal: $134{,}330 \cdot 2561 = 344{,}019{,}130$)

c) $\text{ABCDE} + 1111 = \text{AC{,}DEF}$ (decimal: $703{,}710 + 4369 = 708{,}079$)
$\text{ABCDE} \cdot 1111 = \text{B7{,}414{,}8BE}$ (decimal: $703{,}710 \cdot 4369 = 3{,}074{,}508{,}990$)

d) $\text{E0000E} + \text{BAAA} = \text{E0B{,}AB8}$ (decimal: $14{,}680{,}078 + 47{,}786 = 14{,}727{,}864$)
$\text{E0000E} \cdot \text{BAAA} = \text{A{,}354{,}CA3{,}54C}$ (decimal: $14{,}680{,}078 \cdot 47{,}786 = 701{,}502{,}207{,}308$)

26. In effect, this algorithm computes 11 **mod** 645, 11^2 **mod** 645, 11^4 **mod** 645, 11^8 **mod** 645, 11^{16} **mod** 645, ..., and then multiplies (modulo 645) the required values. Since $644 = (1010000100)_2$, we need to multiply

together $11^4 \bmod 645$, $11^{128} \bmod 645$, and $11^{512} \bmod 645$, reducing modulo 645 at each step. We compute by repeatedly squaring: $11^2 \bmod 645 = 121$, $11^4 \bmod 645 = 121^2 \bmod 645 = 14641 \bmod 645 = 451$, $11^8 \bmod 645 = 451^2 \bmod 645 = 203401 \bmod 645 = 226$, $11^{16} \bmod 645 = 226^2 \bmod 645 = 51076 \bmod 645 = 121$. At this point we notice that 121 appeared earlier in our calculation, so we have $11^{32} \bmod 645 = 121^2 \bmod 645 = 451$, $11^{64} \bmod 645 = 451^2 \bmod 645 = 226$, $11^{128} \bmod 645 = 226^2 \bmod 645 = 121$, $11^{256} \bmod 645 = 451$, and $11^{512} \bmod 645 = 226$. Thus our final answer will be the product of 451, 121, and 226, reduced modulo 645. We compute these one at a time: $451 \cdot 121 \bmod 645 = 54571 \bmod 645 = 391$, and $391 \cdot 226 \bmod 645 = 88366 \bmod 645 = 1$. So $11^{644} \bmod 645 = 1$. A computer algebra system will verify this; use the command "`1 &^ 644 mod 645;`" in *Maple*, for example. The ampersand here tells *Maple* to use modular exponentiation, rather than first computing the integer 11^{644}, which has over 600 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.

28. In effect this algorithm computes powers $123 \bmod 101$, $123^2 \bmod 101$, $123^4 \bmod 101$, $123^8 \bmod 101$, $123^{16} \bmod 101$, ..., and then multiplies (modulo 101) the required values. Since $1001 = (1111101001)_2$, we need to multiply together $123 \bmod 101$, $123^8 \bmod 101$, $123^{32} \bmod 101$, $123^{64} \bmod 101$, $123^{128} \bmod 101$, $123^{256} \bmod 101$, and $123^{512} \bmod 101$, reducing modulo 101 at each step. We compute by repeatedly squaring: $123 \bmod 101 = 22$, $123^2 \bmod 101 = 22^2 \bmod 101 = 484 \bmod 101 = 80$, $123^4 \bmod 101 = 80^2 \bmod 101 = 6400 \bmod 101 = 37$, $123^8 \bmod 101 = 37^2 \bmod 101 = 1369 \bmod 101 = 56$, $123^{16} \bmod 101 = 56^2 \bmod 101 = 3136 \bmod 101 = 5$, $123^{32} \bmod 101 = 5^2 \bmod 101 = 25$, $123^{64} \bmod 101 = 25^2 \bmod 101 = 625 \bmod 101 = 19$, $123^{128} \bmod 101 = 19^2 \bmod 101 = 361 \bmod 101 = 58$, $123^{256} \bmod 101 = 58^2 \bmod 101 = 3364 \bmod 101 = 31$, and $123^{512} \bmod 101 = 31^2 \bmod 101 = 961 \bmod 101 = 52$. Thus our final answer will be the product of 22, 56, 25, 19, 58, 31, and 52. We compute these one at a time modulo 101: $22 \cdot 56$ is 20, $20 \cdot 25$ is 96, $96 \cdot 19$ is 6, $6 \cdot 58$ is 45, $45 \cdot 31$ is 82, and finally $82 \cdot 52$ is 22. So $123^{1001} \bmod 101 = 22$.

30. **a)** $5 = 9 - 3 - 1$ **b)** $13 = 9 + 3 + 1$ **c)** $37 = 27 + 9 + 1$ **d)** $79 = 81 - 3 + 1$

32. The key fact here is that $10 \equiv -1 \pmod{11}$, and so $10^k \equiv (-1)^k \pmod{11}$. Thus 10^k is congruent to 1 if k is even and to -1 if k is odd. Let the decimal expansion of the integer a be given by $(a_{n-1}a_{n-2}\ldots a_3a_2a_1a_0)_{10}$. Thus $a = 10^{n-1}a_{n-1} + 10^{n-2}a_{n-2} + \cdots + 10a_1 + a_0$. Since $10^k \equiv (-1)^k \pmod{11}$, we have $a \equiv \pm a_{n-1} \mp a_{n-2} + \cdots - a_3 + a_2 - a_1 + a_0 \pmod{11}$, where signs alternate and depend on the parity of n. Therefore $a \equiv 0 \pmod{11}$ if and only if $(a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)$, which we obtain by collecting the odd and even indexed terms, is congruent to 0 (mod 11). Since being divisible by 11 is the same as being congruent to 0 (mod 11), we have proved that a positive integer is divisible by 11 if and only if the sum of its decimal digits in even-numbered positions minus the sum of its decimal digits in odd-numbered positions is divisible by 11.

34. **a)** Since the binary representation of 22 is 10110, the six bit one's complement representation is 010110.

b) Since the binary representation of 31 is 11111, the six bit one's complement representation is 011111.

c) Since the binary representation of 7 is 111, we complement 000111 to obtain 111000 as the one's complement representation of -7.

d) Since the binary representation of 19 is 10011, we complement 010011 to obtain 101100 as the one's complement representation of -19.

36. Every 1 is changed to a 0, and every 0 is changed to a 1.

38. We just combine the two ideas in Exercises 36 and 37: to form $a - b$, we compute $a + (-b)$, using Exercise 36 to find $-b$ and Exercise 37 to find the sum.

40. Following the definition, we find the two's complement expansion of a positive number simply by representing it in binary, using six bits; and we find the two's complement expansion of a negative number $-x$ by representing $2^5 - x$ in binary using five bits and preceding it with a 1.

a) Since 22 is positive, and its binary expansion is 10110, the answer is 010110.

b) Since 31 is positive, and its binary expansion is 11111, the answer is 011111.

c) Since -7 is negative, we first find the 5-bit binary expansion of $2^5 - 7 = 25$, namely 11001, and precede it by a 1, obtaining 111001.

d) Since -19 is negative, we first find the 5-bit binary expansion of $2^5 - 19 = 13$, namely 01101, and precede it by a 1, obtaining 101101.

42. We can experiment a bit to find a convenient algorithm. We saw in Exercise 40 that the expansion of -7 is 111001, while of course the expansion of 7 is 000111. Apparently to find the expansion of $-m$ from that of m we complement each bit and then add 1, working in base 2. Similarly, the expansion of -8 is 111000, whereas the expansion of 8 is 001000; again $110111 + 1 = 111000$. At the extremes (using six bits) we have 1 represented by 000001, so -1 is represented by $111110 + 1 = 111111$; and 31 is represented by 011111, so -31 is represented by $100000 + 1 = 100001$.

44. We just combine the two ideas in Exercises 42 and 43. To form $a - b$, we compute $a + (-b)$, using Exercise 42 to find $-b$ and Exercise 43 to find the sum.

46. If the number is positive (i.e., the left-most bit is 0), then the expansions are the same. If the number is negative (i.e., the left-most bit is 1), then we take the one's complement representation and add 1, working in base 2. For example, the one's complement representation of -19 using six bits is, from Exercise 34, 101100. Adding 1 we obtain 101101, which is the two's complement representation of -19 using six bits, from Exercise 40.

48. We obtain these expansions from the top down. For example in part **(e)** we compute that $7! > 1000$ but $6! \leq 1000$, so the highest factorial appearing is $6! = 720$. We use the division algorithm to find the quotient and remainder when 1000 is divided by 720, namely 1 and 280, respectively. Therefore the expansion begins $1 \cdot 6!$ and continues with the expansion of 280, which we find in the same manner.

a) $2 = 2!$ **b)** $7 = 3! + 1!$ **c)** $19 = 3 \cdot 3! + 1!$ **d)** $87 = 3 \cdot 4! + 2 \cdot 3! + 2! + 1!$

e) $1000 = 6! + 2 \cdot 5! + 4! + 2 \cdot 3! + 2 \cdot 2!$ **f)** $1000000 = 2 \cdot 9! + 6 \cdot 8! + 6 \cdot 7! + 2 \cdot 6! + 5 \cdot 5! + 4! + 2 \cdot 3! + 2 \cdot 2!$

50. The algorithm is essentially the same as the usual grade-school algorithm for adding. We add from right to left, one column at a time, carrying to the next column if necessary. A carry out of the column representing $i!$ is needed whenever the sum obtained for that column is greater than i, in which case we subtract $i + 1$ from that digit and carry 1 into the next column (since $(i + 1)! = (i + 1) \cdot i!$).

52. The partial products are 11100 and 1110000, namely 1110 shifted one place and three places to the left. We add these two numbers, obtaining 10001100.

54. Subtraction is really just like addition, so the number of bit operations should be comparable, namely $O(n)$. More specifically, if we analyze the algorithm for Exercise 53, we see that the loop is executed n times, and only a few operations are performed during each pass.

56. In the worst case, each bit of a has to be compared to each bit of b, so $O(n)$ comparisons are needed. An exact analysis of the procedure given in the solution to Exercise 55 shows that $n + 1$ comparisons of bits are needed in the worst case, assuming that the logical "and" condition in the **while** loop is evaluated efficiently from left to right (so that a_0 is not compared to b_0 there).

58. A multiplication modulo m consists of multiplying two integers, each at most $\log m$ bits long (since they are less than m), followed by a division by m, which is also $\log m$ bits long. Thus this takes $(\log m)^2$ bit operations by Example 11 and the analysis of Algorithm 4 mentioned in the text. This is what goes on inside the loop of Algorithm 5. The loop is iterated $\log n$ times. Therefore the total number of bit operations is $O((\log m)^2 \log n)$.

SECTION 4.3 Primes and Greatest Common Divisors

2. The numbers 19, 101, 107, and 113 are prime, as we can verify by trial division. The numbers $27 = 3^3$ and $93 = 3 \cdot 31$ are not prime.

4. We obtain the answers by trial division. The factorizations are $39 = 3 \cdot 13$, $81 = 3^4$, $101 = 101$ (prime), $143 = 11 \cdot 13$, $289 = 17^2$, and $899 = 29 \cdot 31$.

6. A 0 appears at the end of a number for every factor of 10 $(= 2 \cdot 5)$ the number has. Now 100! certainly has more factors of 2 than it has factors of 5, so the number of factors of 10 it has is the same as the number of factors of 5. Each of the twenty numbers 5, 10, 15, ..., 100 contributes a factor of 5 to 100!, and in addition the four numbers 25, 50, 75, and 100 contribute one more factor of 5. Therefore there are 24 factors of 5 in 100!, so 100! ends in exactly 24 0's.

8. The input is a positive integer n. We successively look for small factors d (starting with $d = 2$ and incrementing d once we know that d is no longer a factor of what remains), which will necessarily be prime. When we find a factor, we divide out by that factor and keep going. We will print the factors as we find them. (Alternatively, they could be stored in a list of some sort.) We stop when the remaining number is 1 (all factors have been found). The pseudocode below accomplishes this. Notice that we could be a little more sophisticated and use only prime trial divisors, but it hardly seems worth the effort, since it would take time to see which trial divisors are prime. Alternatively, we could handle $d = 2$ by itself and then loop through only odd values of d, starting at 3 and incrementing by 2.

```
procedure factorization(n : positive integer)
d := 2
while n > 1
        if n mod d = 0 then
                print d
                n := n/d
        else
                d := d + 1
```

10. We first establish the identity in the hint. If we let $y = x^k$, then the claimed identity is

$$(y^t + 1) = (y + 1)(y^{t-1} - y^{t-2} + y^{t-3} - \cdots - y + 1),$$

which is easily seen to be true by multiplying out the right-hand side and noticing the "telescoping" that occurs. We want to show that m is a power of 2, i.e., that its only prime factor is 2. Suppose to the contrary that m has an odd prime factor t and write $m = kt$, where k is a positive integer. Letting $x = 2$ in the identity given in the hint, we have $2^m + 1 = (2^k + 1)$(the other factor). Because $2^k + 1 > 1$ and the prime $2^m + 1$ can have no proper factor greater than 1, we must have $2^m + 1 = 2^k + 1$, so $m = k$ and $t = 1$, contradicting the fact that t is prime. This completes the proof by contradiction.

12. We follow the hint. There are n numbers in the sequence $(n+1)!+2$, $(n+1)!+3$, $(n+1)!+4$, $\ldots$, $(n+1)!+(n+1)$. The first of these is composite because it is divisible by 2; the second is composite because it is divisible by 3; the third is composite because it is divisible by 4; $\ldots$; the last is composite because it is divisible by $n+1$. This gives us the desired n consecutive composite integers.

14. We must find, by inspection with mental arithmetic, the greatest common divisors of the numbers from 1 to 11 with 12, and list those whose gcd is 1. These are 1, 5, 7, and 11. There are so few since 12 had many factors—in particular, both 2 and 3.

16. Since these numbers are small, the easiest approach is to find the prime factorization of each number and look for any common prime factors.

a) Since $21 = 3 \cdot 7$, $34 = 2 \cdot 17$, and $55 = 5 \cdot 11$, these are pairwise relatively prime.

b) Since $85 = 5 \cdot 17$, these are not pairwise relatively prime.

c) Since $25 = 5^2$, 41 is prime, $49 = 7^2$, and $64 = 2^6$, these are pairwise relatively prime.

d) Since 17, 19, and 23 are prime and $18 = 2 \cdot 3^2$, these are pairwise relatively prime.

18. **a)** Since $6 = 1+2+3$, and these three summands are the only proper divisors of 6, we conclude that 6 is perfect. Similarly $28 = 1+2+4+7+14$.

b) We need to find all the proper divisors of $2^{p-1}(2^p-1)$. Certainly all the numbers 1, 2, 4, 8, $\ldots$, 2^{p-1} are proper divisors, and their sum is 2^p-1 (this is a geometric series). Also each of these divisors times 2^p-1 is also a divisor, and all but the last is proper. Again adding up this geometric series we find a sum of $(2^p-1)(2^{p-1}-1)$. There are no other other proper divisors. Therefore the sum of all the divisors is $(2^p-1)+(2^p-1)(2^{p-1}-1) = (2^p-1)(1+2^{p-1}-1) = (2^p-1)2^{p-1}$, which is our original number. Therefore this number is perfect.

20. We need to find a factor if there is one, or else check all possible prime divisors up to the square root of the given number to verify that there is no nontrivial divisor.

a) $2^7-1 = 127$. Division by 2, 3, 5, 7, and 11 shows that these are not factors. Since $\sqrt{127} < 13$, we are done; 127 is prime.

b) $2^9-1 = 511 = 7 \cdot 73$, so this number is not prime.

c) $2^{11}-1 = 2047 = 23 \cdot 89$, so this number is not prime.

d) $2^{13}-1 = 8191$. Division by 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, and 89 (phew!) shows that these are not factors. Since $\sqrt{8191} < 97$, we are done; 8191 is prime.

22. Certainly if n is prime, then all the integers from 1 to $n-1$ are less than or equal to n and relatively prime to n, but no others are, so $\phi(n) = n-1$. Conversely, suppose that n is not prime. If $n = 1$, then we have $\phi(1) = 1 \neq 1-1$. If $n > 1$, then $n = ab$ with $1 < a < n$ and $1 < b < n$. Note that neither a nor b is relatively prime to n. Therefore the number of positive integers less than or equal to n and relatively prime to n is at most $n-3$ (since a, b, and n are not in this collection), so $\phi(n) \neq n-1$.

24. We form the greatest common divisors by finding the minimum exponent for each prime factor.

a) $2^2 \cdot 3^3 \cdot 5^2$ **b)** $2 \cdot 3 \cdot 11$ **c)** 17 **d)** 1 **e)** 5 **f)** $2 \cdot 3 \cdot 5 \cdot 7$

26. We form the least common multiples by finding the maximum exponent for each prime factor.

a) $2^5 \cdot 3^3 \cdot 5^5$ **b)** $2^{11} \cdot 3^9 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17^{14}$ **c)** 17^{17} **d)** $2^2 \cdot 5^3 \cdot 7 \cdot 13$

e) undefined (0 is not a positive integer) **f)** $2 \cdot 3 \cdot 5 \cdot 7$

28. We have $1000 = 2^3 \cdot 5^3$ and $625 = 5^4$, so $\gcd(1000, 625) = 5^3 = 125$, and $\text{lcm}(1000, 625) = 2^3 \cdot 5^4 = 5000$. As expected, $125 \cdot 5000 = 625000 = 1000 \cdot 625$.

30. By Exercise 31 we know that the product of the greatest common divisor and the least common multiple of two numbers is the product of the two numbers. Therefore the answer is $(2^7 \cdot 3^8 \cdot 5^2 \cdot 7^{11})/(2^3 \cdot 3^4 \cdot 5) = 2^4 \cdot 3^4 \cdot 5 \cdot 7^{11}$.

32. To apply the Euclidean algorithm, we divide the larger number by the smaller, replace the larger by the smaller and the smaller by the remainder of this division, and repeat this process until the remainder is 0. At that point, the smaller number is the greatest common divisor.

a) $\gcd(1,5) = \gcd(1,0) = 1$ **b)** $\gcd(100,101) = \gcd(100,1) = \gcd(1,0) = 1$

c) $\gcd(123,277) = \gcd(123,31) = \gcd(31,30) = \gcd(30,1) = \gcd(1,0) = 1$

d) $\gcd(1529,14039) = \gcd(1529,278) = \gcd(278,139) = \gcd(139,0) = 139$

e) $\gcd(1529,14038) = \gcd(1529,277) = \gcd(277,144) = \gcd(144,133) = \gcd(133,11) = \gcd(11,1) = \gcd(1,0) = 1$

f) $\gcd(11111,111111) = \gcd(11111,1) = \gcd(1,0) = 1$

34. We need to divide successively by 34, 21, 13, 8, 5, 3, 2, and 1, so eight divisions are required.

36. The statement we are asked to prove involves the result of dividing $2^a - 1$ by $2^b - 1$. Let us actually carry out that division algebraically—long division of these expressions. The leading term in the quotient is 2^{a-b} (as long as $a \geq b$), with a remainder at that point of $2^{a-b} - 1$. If now $a - b \geq b$ then the next step in the long division produces the next summand in the quotient, 2^{a-2b}, with a remainder at this stage of $2^{a-2b} - 1$. This process of long division continues until the remainder at some stage is less than the divisor, i.e., $2^{a-kb} - 1 < 2^b - 1$. But then the remainder is $2^{a-kb} - 1$, and clearly $a - kb$ is exactly a **mod** b. This completes the proof.

38. By Exercise 37, $2^a - 1$ and $2^b - 1$ are relatively prime precisely when $2^{\gcd(a,b)} - 1 = 1$, which happens if and only if $\gcd(a,b) = 1$. Thus it is enough to check here that 35, 34, 33, 31, 29, and 23 are relatively prime. This is clear, since the prime factorizations are, respectively, 35, $2 \cdot 17$, $3 \cdot 11$, 31, 29, and 23.

40. **a)** In order to find the coefficients s and t such that $9s + 11t = \gcd(9,11)$, we carry out the steps of the Euclidean algorithm.

$$11 = 9 + 2$$
$$9 = 4 \cdot 2 + 1$$

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 11, 9, and 2. In particular, the last equation tells us that $1 = 9 - 4 \cdot 2$, so that we have expressed the gcd as a linear combination of 9 and 2. But now the first equation tells us that $2 = 11 - 9$; we plug this into our previous equation and obtain

$$1 = 9 - 4 \cdot (11 - 9) = 5 \cdot 9 - 4 \cdot 11\,.$$

Thus we have expressed 1 as a linear combination (with integer coefficients) of 9 and 11, namely $\gcd(9,11) = 5 \cdot 9 - 4 \cdot 11$.

b) Again, we carry out the Euclidean algorithm. Since $44 = 33 + 11$, and $11 \mid 33$, we know that $\gcd(33,44) = 11$. From the equation shown here, we can immediately write $11 = (-1) \cdot 33 + 44$.

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

$$78 = 2 \cdot 35 + 8$$
$$35 = 4 \cdot 8 + 3$$
$$8 = 2 \cdot 3 + 2$$
$$3 = 2 + 1$$

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

$$\begin{aligned}1 &= 3 - 2\\ &= 3 - (8 - 2 \cdot 3) = 3 \cdot 3 - 8\\ &= 3 \cdot (35 - 4 \cdot 8) - 8 = 3 \cdot 35 - 13 \cdot 8\\ &= 3 \cdot 35 - 13 \cdot (78 - 2 \cdot 35) = 29 \cdot 35 - 13 \cdot 78\end{aligned}$$

d) 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.

$$\begin{aligned}55 &= 2 \cdot 21 + 13\\ 21 &= 13 + 8\\ 13 &= 8 + 5\\ 8 &= 5 + 3\\ 5 &= 3 + 2\\ 3 &= 2 + 1\end{aligned}$$

Thus the greatest common divisor is 1.

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

e) We compute the greatest common divisor in one step: $203 = 2 \cdot 101 + 1$. Therefore we have $1 = (-2) \cdot 101 + 203$.

f) We compute the greatest common divisor using the Euclidean algorithm:

$$\begin{aligned}323 &= 2 \cdot 124 + 75\\ 124 &= 75 + 49\\ 75 &= 49 + 26\\ 49 &= 26 + 23\\ 26 &= 23 + 3\\ 23 &= 7 \cdot 3 + 2\\ 3 &= 2 + 1\end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}1 &= 3 - 2\\ &= 3 - (23 - 7 \cdot 3) = 8 \cdot 3 - 23\\ &= 8 \cdot (26 - 23) - 23 = 8 \cdot 26 - 9 \cdot 23\\ &= 8 \cdot 26 - 9 \cdot (49 - 26) = 17 \cdot 26 - 9 \cdot 49\\ &= 17 \cdot (75 - 49) - 9 \cdot 49 = 17 \cdot 75 - 26 \cdot 49\\ &= 17 \cdot 75 - 26 \cdot (124 - 75) = 43 \cdot 75 - 26 \cdot 124\\ &= 43 \cdot (323 - 2 \cdot 124) - 26 \cdot 124 = 43 \cdot 323 - 112 \cdot 124\end{aligned}$$

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.

$$\begin{aligned}
2339 &= 2002 + 337 \\
2002 &= 5 \cdot 337 + 317 \\
337 &= 317 + 20 \\
317 &= 15 \cdot 20 + 17 \\
20 &= 17 + 3 \\
17 &= 5 \cdot 3 + 2 \\
3 &= 2 + 1
\end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (17 - 5 \cdot 3) = 6 \cdot 3 - 17 \\
&= 6 \cdot (20 - 17) - 17 = 6 \cdot 20 - 7 \cdot 17 \\
&= 6 \cdot 20 - 7 \cdot (317 - 15 \cdot 20) = 111 \cdot 20 - 7 \cdot 317 \\
&= 111 \cdot (337 - 317) - 7 \cdot 317 = 111 \cdot 337 - 118 \cdot 317 \\
&= 111 \cdot 337 - 118 \cdot (2002 - 5 \cdot 337) = 701 \cdot 337 - 118 \cdot 2002 \\
&= 701 \cdot (2339 - 2002) - 118 \cdot 2002 = 701 \cdot 2339 - 819 \cdot 2002
\end{aligned}$$

h) The procedure is the same:

$$\begin{aligned}
4669 &= 3457 + 1212 \\
3457 &= 2 \cdot 1212 + 1033 \\
1212 &= 1033 + 179 \\
1033 &= 5 \cdot 179 + 138 \\
179 &= 138 + 41 \\
138 &= 3 \cdot 41 + 15 \\
41 &= 2 \cdot 15 + 11 \\
15 &= 11 + 4 \\
11 &= 2 \cdot 4 + 3 \\
4 &= 3 + 1
\end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned}
1 &= 4 - 3 \\
&= 4 - (11 - 2 \cdot 4) = 3 \cdot 4 - 11 \\
&= 3 \cdot (15 - 11) - 11 = 3 \cdot 15 - 4 \cdot 11 \\
&= 3 \cdot 15 - 4 \cdot (41 - 2 \cdot 15) = 11 \cdot 15 - 4 \cdot 41 \\
&= 11 \cdot (138 - 3 \cdot 41) - 4 \cdot 41 = 11 \cdot 138 - 37 \cdot 41 \\
&= 11 \cdot 138 - 37 \cdot (179 - 138) = 48 \cdot 138 - 37 \cdot 179 \\
&= 48 \cdot (1033 - 5 \cdot 179) - 37 \cdot 179 = 48 \cdot 1033 - 277 \cdot 179 \\
&= 48 \cdot 1033 - 277 \cdot (1212 - 1033) = 325 \cdot 1033 - 277 \cdot 1212 \\
&= 325 \cdot (3457 - 2 \cdot 1212) - 277 \cdot 1212 = 325 \cdot 3457 - 927 \cdot 1212 \\
&= 325 \cdot 3457 - 927 \cdot (4669 - 3457) = 1252 \cdot 3457 - 927 \cdot 4669
\end{aligned}$$

i) The procedure is the same:

$$\begin{aligned} 13422 &= 10001 + 3421 \\ 10001 &= 2 \cdot 3421 + 3159 \\ 3421 &= 3159 + 262 \\ 3159 &= 12 \cdot 262 + 15 \\ 262 &= 17 \cdot 15 + 7 \\ 15 &= 2 \cdot 7 + 1 \end{aligned}$$

Thus the greatest common divisor is 1.

$$\begin{aligned} 1 &= 15 - 2 \cdot 7 \\ &= 15 - 2 \cdot (262 - 17 \cdot 15) = 35 \cdot 15 - 2 \cdot 262 \\ &= 35 \cdot (3159 - 12 \cdot 262) - 2 \cdot 262 = 35 \cdot 3159 - 422 \cdot 262 \\ &= 35 \cdot 3159 - 422 \cdot (3421 - 3159) = 457 \cdot 3159 - 422 \cdot 3421 \\ &= 457 \cdot (10001 - 2 \cdot 3421) - 422 \cdot 3421 = 457 \cdot 10001 - 1336 \cdot 3421 \\ &= 457 \cdot 10001 - 1336 \cdot (13422 - 10001) = 1793 \cdot 10001 - 1336 \cdot 13422 \end{aligned}$$

42. We take $a = 356$ and $b = 252$ to avoid a needless first step. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1 = 1$, $r_2 = 104$, $q_2 = 2$, $r_3 = 44$, $q_3 = 2$, $r_4 = 16$, $q_4 = 2$, $r_5 = 12$, $q_5 = 1$, $r_6 = 4$, $q_6 = 3$. Note that $n = 6$. Thus we compute the successive s's and t's as follows, using the given recurrences:

$$\begin{aligned} s_2 &= s_0 - q_1 s_1 = 1 - 1 \cdot 0 = 1, & t_2 &= t_0 - q_1 t_1 = 0 - 1 \cdot 1 = -1 \\ s_3 &= s_1 - q_2 s_2 = 0 - 2 \cdot 1 = -2, & t_3 &= t_1 - q_2 t_2 = 1 - 2 \cdot (-1) = 3 \\ s_4 &= s_2 - q_3 s_3 = 1 - 2 \cdot (-2) = 5, & t_4 &= t_2 - q_3 t_3 = -1 - 2 \cdot 3 = -7 \\ s_5 &= s_3 - q_4 s_4 = -2 - 2 \cdot 5 = -12, & t_5 &= t_3 - q_4 t_4 = 3 - 2 \cdot (-7) = 17 \\ s_6 &= s_4 - q_5 s_5 = 5 - 1 \cdot (-12) = 17, & t_6 &= t_4 - q_5 t_5 = -7 - 1 \cdot 17 = -24 \end{aligned}$$

Thus we have $s_6 a + t_6 b = 17 \cdot 356 + (-24) \cdot 252 = 4$, which is $\gcd(356, 252)$.

44. We take $a = 100001$ and $b = 1001$ to avoid a needless first step. When we apply the Euclidean algorithm we obtain the following quotients and remainders: $q_1 = 99$, $r_2 = 902$, $q_2 = 1$, $r_3 = 99$, $q_3 = 9$, $r_4 = 11$, $q_4 = 9$. Note that $n = 4$. Thus we compute the successive s's and t's as follows, using the given recurrences:

$$\begin{aligned} s_2 &= s_0 - q_1 s_1 = 1 - 99 \cdot 0 = 1, & t_2 &= t_0 - q_1 t_1 = 0 - 99 \cdot 1 = -99 \\ s_3 &= s_1 - q_2 s_2 = 0 - 1 \cdot 1 = -1, & t_3 &= t_1 - q_2 t_2 = 1 - 1 \cdot (-99) = 100 \\ s_4 &= s_2 - q_3 s_3 = 1 - 9 \cdot (-1) = 10, & t_4 &= t_2 - q_3 t_3 = -99 - 9 \cdot 100 = -999 \end{aligned}$$

Thus we have $s_4 a + t_4 b = 10 \cdot 100001 + (-999) \cdot 1001 = 11$, which is $\gcd(100001, 1001)$.

46. The number of (positive) factors that a positive integer n has can be determined from the prime factorization of n. If we write this prime factorization as $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then there are $(e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$ different factors. This follows from the ideas in Chapter 6. Specifically, in choosing a factor we can choose 0, 1, 2, $\ldots$, e_1 of the p_1 factors, a total of $e_1 + 1$ choices; for each of these there are $e_2 + 1$ choices as to how many p_2 factors to include, and so on. If we don't want to go through the analysis using the ideas given below, we could simply compute the number of factors for each n, starting at 1 (perhaps using a computer program), and thereby obtain the answers by "brute force."

a) If an integer is to have exactly three different factors (we assume "positive factors" is intended here), then n must be the square of a prime number; that is the only way to make $(e_1 + 1)(e_2 + 1) \cdots (e_r + 1) = 3$. The smallest prime number is 2. So the smallest positive integer with exactly three factors is $2^2 = 4$.

b) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=4$. We can do this with $r=1$ and $e_1=3$, or with $r=2$ and $e_1=e_2=1$. The smallest numbers obtainable in these ways are $2^3=8$ and $2\cdot 3=6$, respectively. So the smallest number with four factors is 6.

c) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=5$. We can do this only with $r=1$ and $e_1=4$, so the smallest such number is $2^4=16$.

d) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=6$. We can do this with $r=1$ and $e_1=5$, or with $r=2$ and $e_1=2$ and $e_2=1$. The smallest numbers obtainable in these ways are $2^5=32$ and $2^2\cdot 3=12$, respectively. So the smallest number with six factors is 12.

e) This time we want $(e_1+1)(e_2+1)\cdots(e_r+1)=10$. We can do this with $r=1$ and $e_1=9$, or with $r=2$ and $e_1=4$ and $e_2=1$. The smallest numbers obtainable in these ways are $2^9=512$ and $2^4\cdot 3=48$, respectively. So the smallest number with ten factors is 48.

48. 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) All the entries are primes. In fact, the n^{th} term is the smallest prime number greater than or equal to n.

b) Here we see that the sequence jumps at the prime locations. We can state this succinctly by saying that the n^{th} term is the number of prime numbers not exceeding n.

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

d) This sequence is actually important in number theory. The n^{th} term is -1 if n is prime, 0 if n has a repeated prime factor (for example, $12=2^2\cdot 3$, so 2 is a repeated prime factor of 12 and therefore the twelfth term is 0), and 1 otherwise (if n is not prime but is square-free).

e) The n^{th} term is 0 if n has two or more distinct prime factors, and is 1 otherwise. In other words the n^{th} term is 1 if n is a power of a prime number.

f) The n^{th} term is the square of the n^{th} prime.

50. From $a\equiv b \pmod m$ we know that $b=a+sm$ for some integer s. Now if d is a common divisor of a and m, then it divides the right-hand side of this equation, so it also divides b. We can rewrite the equation as $a=b-sm$, and then by similar reasoning, we see that every common divisor of b and m is also a divisor of a. This shows that the set of common divisors of a and m is equal to the set of common divisors of b and m, so certainly $\gcd(a,m)=\gcd(b,m)$.

52. We compute the first several of these: $2+1=3$ (which is prime), $2\cdot 3+1=7$ (which is prime), $2\cdot 3\cdot 5+1=31$ (which is prime), $2\cdot 3\cdot 5\cdot 7+1=211$ (which is prime), $2\cdot 3\cdot 5\cdot 7\cdot 11+1=2311$ (which is prime). However, $2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13+1=30031=59\cdot 509$, so the conjecture is false. Notice, however, that the prime factors in this last case were necessarily different from the primes being multiplied.

54. Suppose by way of contradiction that $q_1, q_2, \ldots, q_n$ are the only primes of the form $3k+2$. Notice that this list necessarily includes 2. Let $Q=3q_1q_2\cdots q_n-1$. Notice that neither 3 nor any prime of the form $3k+2$ is a factor of Q. But $Q\geq 3\cdot 2-1=5>1$, so it must have prime factors. Therefore all of its prime factors are of the form $3k+1$. However, the product of numbers of the form $3k+1$ is again of that form, because $(3k+1)(3l+1)=3(3kl+k+l)+1$. Patently Q is not of that form, and we have a contradiction, which completes the proof.

56. Define the function f as suggested from the positive rational numbers to the positive integers. This is a one-to-one function, because if we are given the value of $f(p/q)$, we can immediately recover p and q uniquely by writing $f(p/q)$ in base eleven and noting what appears to the left of the one and only A in the expansion and what appears to the right (and interpret these as numerals in base ten). Thus we have a one-to-one

correspondence between the set of positive rational numbers and an infinite subset of the natural numbers, which is countable; therefore the set of positive rational numbers is countable.

SECTION 4.4 Solving Congruences

2. We need to show that $13 \cdot 937 \equiv 1 \pmod{2436}$, or in other words, that $13 \cdot 937 - 1 = 12180$ is divisible by 2436. A calculator shows that it is, since $12180 = 2436 \cdot 5$.

4. We need a number that when multiplied by 2 gives a number congruent to 1 modulo 17. Since $18 \equiv 1 \pmod{17}$ and $2 \cdot 9 = 18$, it follows that 9 is an inverse of 2 modulo 17.

6. **a)** The first step of the procedure in Example 1 yields $17 = 8 \cdot 2 + 1$, which means that $17 - 8 \cdot 2 = 1$, so -8 is an inverse. We can also report this as 9, because $-8 \equiv 9 \pmod{17}$.
b) We need to find s and t such that $34s + 89t = 1$. Then s will be the desired inverse, since $34s \equiv 1 \pmod{89}$ (i.e., $34s - 1 = -89t$ is divisible by 89). To do so, we proceed as in Example 2. First we go through the Euclidean algorithm computation that $\gcd(34, 89) = 1$:

$$\begin{aligned} 89 &= 2 \cdot 34 + 21 \\ 34 &= 21 + 13 \\ 21 &= 13 + 8 \\ 13 &= 8 + 5 \\ 8 &= 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Then we reverse our steps and write 1 as the desired linear combination:

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

Thus $s = -34$, so an inverse of 34 modulo 89 is -34, which can also be written as 55.
c) We need to find s and t such that $144s + 233t = 1$. Then clearly s will be the desired inverse, since $144s \equiv 1 \pmod{233}$ (i.e., $144s - 1 = -233t$ is divisible by 233). To do so, we proceed as in Example 2. In fact, once we get to a certain point below, all the work was already done in part **(b)**. First we go through the

Euclidean algorithm computation that $\gcd(144, 233) = 1$:

$$\begin{aligned} 233 &= 144 + 89 \\ 144 &= 89 + 55 \\ 89 &= 55 + 34 \\ 55 &= 34 + 21 \\ 34 &= 21 + 13 \\ 21 &= 13 + 8 \\ 13 &= 8 + 5 \\ 8 &= 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

Then we reverse our steps and write 1 as the desired linear combination:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) = 2 \cdot 3 - 5 \\ &= 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3 \cdot (13 - 8) = 5 \cdot 8 - 3 \cdot 13 \\ &= 5 \cdot (21 - 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\ &= 5 \cdot 21 - 8 \cdot (34 - 21) = 13 \cdot 21 - 8 \cdot 34 \\ &= 13 \cdot (55 - 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34 \\ &= 13 \cdot 55 - 21 \cdot (89 - 55) = 34 \cdot 55 - 21 \cdot 89 \\ &= 34 \cdot (144 - 89) - 21 \cdot 89 = 34 \cdot 144 - 55 \cdot 89 \\ &= 34 \cdot 144 - 55 \cdot (233 - 144) = 89 \cdot 144 - 55 \cdot 233 \end{aligned}$$

Thus $s = 89$, so an inverse of 144 modulo 233 is 89, since $144 \cdot 89 = 12816 \equiv 1 \pmod{233}$.

d) The first step in the Euclidean algorithm calculation is $1001 = 5 \cdot 200 + 1$. Thus $-5 \cdot 200 + 1001 = 1$, and -5 (or 996) is the desired inverse.

8. If x is an inverse of a modulo m, then by definition $ax - 1 = tm$ for some integer t. If a and m in this equation both have a common divisor greater than 1, then 1 must also have this same common divisor, since $1 = ax - tm$. This is absurd, since the only positive divisor of 1 is 1. Therefore no such x exists.

10. We know from Exercise 6 that 9 is an inverse of 2 modulo 17. Therefore if we multiply both sides of this equation by 9 we will get $x \equiv 9 \cdot 7 \pmod{17}$. Since $63 \bmod 17 = 12$, the solutions are all integers congruent to 12 modulo 17, such as 12, 29, and -5. We can check, for example, that $2 \cdot 12 = 24 \equiv 7 \pmod{17}$. This answer can also be stated as all integers of the form $12 + 17k$ for $k \in \mathbf{Z}$.

12. In each case we multiply both sides of the congruence by the inverse found in Exercise 6 and simplify. Our answers are not unique, of course—anything in the same congruence class works just as well.

a) We found that 55 is an inverse of 34 modulo 89, so $x \equiv 77 \cdot 55 = 4235 \equiv 52 \pmod{89}$. Check: $34 \cdot 52 = 1768 \equiv 77 \pmod{89}$.

b) We found that 89 is an inverse of 144 modulo 233, so $x \equiv 4 \cdot 89 = 356 \equiv 123 \pmod{233}$. Check: $144 \cdot 123 = 17712 \equiv 4 \pmod{233}$.

c) We found that -5 is an inverse of 200 modulo 1001, so $x \equiv 13 \cdot (-5) = -65 \equiv 936 \pmod{1001}$. (We could also leave the answer as -65.) Check: $200 \cdot 936 = 187200 \equiv 13 \pmod{1001}$.

14. Adding 12 to both sides of the congruence yields $12x^2 + 25x + 12 \equiv 0 \pmod{11}$. (We chose something to add that would make the left-hand side easily factorable and the right-hand side equal to 0.) This is equivalent to $(3x + 4)(4x + 3) \equiv 0 \pmod{11}$. Because there are no non-zero divisors of 0 modulo 11, this congruence is true if and only if either $3x + 4 \equiv 0 \pmod{11}$ or $4x + 3 \equiv 0 \pmod{11}$. (This would have been more complicated modulo a non-prime modulus, because there would be nonzero divisors of 0.) We solve these linear congruences by inspection (guess and check) or using the Euclidean algorithm to find inverses of 3 and 4 (or using computer algebra software), to yield $x = 6$ or $x = 2$. In fact, typing "`msolve(12^2+25x=10,11)`" into *Maple* produces this solution set.

16. **a)** We can find inverses using the technique shown in Example 2. With a little work (or trial and error, which is actually faster in this case), we find that $2 \cdot 6 \equiv 1 \pmod{11}$, $3 \cdot 4 \equiv 1 \pmod{11}$, $5 \cdot 9 \equiv 1 \pmod{11}$, and $7 \cdot 8 \equiv 1 \pmod{11}$. Actually, the problem does not ask us to show these pairs explicitly, only to show that they exist. The general argument given in Exercise 18 shows this.

b) In this specific case we can compute $10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 10 = 10 \equiv -1 \pmod{11}$. Alternatively, we can use the proof in Exercise 18.

18. **a)** Every positive integer less than p has an inverse modulo p, and by Exercise 7 this inverse is unique among positive integers less than p. This follows from Theorem 1, since every number less than p must be relatively prime to p (because p is prime it has no smaller divisors). We can group each positive integer less than p with its inverse. The only issue is whether some numbers are their own inverses, in which case this grouping does not produce pairs. By Exercise 17 only 1 and -1 (which is the same as $p - 1$ modulo p) are their own inverses. Therefore all the other positive integers less than p can be grouped into pairs consisting of inverses of each other, and there are clearly $(p - 1 - 2)/2 = (p - 3)/2$ such pairs.

b) When we compute $(p - 1)!$, we can write the product by grouping the pairs of inverses modulo p. Each such pair produces the product 1 modulo p, so modulo p the entire product is the same as the product of the only unpaired elements, namely $1 \cdot (p - 1) = p - 1$. Since this equals -1 modulo p, our proof is complete.

c) By the contrapositive of what we have just proved, we can conclude that if $(n - 1)! \not\equiv -1 \pmod{n}$ then n is not prime.

20. Since 3, 4, and 5 are pairwise relatively prime, we can use the Chinese remainder theorem. The answer will be unique modulo $3 \cdot 4 \cdot 5 = 60$. Using the notation in the text, we have $a_1 = 2$, $m_1 = 3$, $a_2 = 1$, $m_2 = 4$, $a_3 = 3$, $m_3 = 5$, $m = 60$, $M_1 = 60/3 = 20$, $M_2 = 60/4 = 15$, $M_3 = 60/5 = 12$. Then we need to find inverses y_i of M_i modulo m_i for $i = 1, 2, 3$. This can be done by inspection (trial and error), since the moduli here are so small, or systematically using the Euclidean algorithm (as in Example 2); we find that $y_1 = 2$, $y_2 = 3$, and $y_3 = 3$. Thus our solution is $x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 233 \equiv 53 \pmod{60}$. So the solutions are all integers of the form $53 + 60k$, where k is an integer.

22. By definition, the first congruence can be written as $x = 6t + 3$ where t is an integer. Substituting this expression for x into the second congruence tells us that $6t + 3 \equiv 4 \pmod{7}$, which can easily be solved to show that $t \equiv 6 \pmod{7}$. From this we can write $t = 7u + 6$ for some integer u. Thus $x = 6t + 3 = 6(7u + 6) + 3 = 42u + 39$. Thus our answer is all numbers congruent to 39 modulo 42. We check our answer by confirming that $39 \equiv 3 \pmod{6}$ and $39 \equiv 4 \pmod{7}$.

24. By definition, the first congruence can be written as $x = 2t + 1$ where t is an integer. Substituting this expression for x into the second congruence tells us that $2t + 1 \equiv 2 \pmod{3}$, which can easily be solved to show that $t \equiv 2 \pmod{3}$. From this we can write $t = 3u + 2$ for some integer u. Thus $x = 2t + 1 = 2(3u + 2) + 1 = 6u + 5$. Next we have $6u + 5 \equiv 3 \pmod{5}$, which we solve to get $u \equiv 3 \pmod{5}$, so $u = 5v + 3$. Thus $x = 6(5v + 3) + 5 = 30v + 23$. For the last congruence we have $30v + 23 \equiv 4 \pmod{11}$; solving this is a

little harder but trial and error or the applying the methods of Example 2 to get an inverse and then Example 3 shows that $v \equiv 10 \pmod{11}$. Therefore $x = 30(11w + 10) + 23 = 330w + 323$. So our solution is all integers congruent to 323 modulo 330. We check our answer by confirming that $323 \equiv 1 \pmod 2$, $323 \equiv 2 \pmod 3$, $323 \equiv 3 \pmod 5$, and $323 \equiv 4 \pmod{11}$.

26. 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 $x \equiv 5 \pmod 6$, we must have $x \equiv 5 \equiv 1 \pmod 2$ and $x \equiv 5 \equiv 2 \pmod 3$. Similarly, from the second congruence we must have $x \equiv 1 \pmod 2$ and $x \equiv 3 \pmod 5$; and from the third congruence we must have $x \equiv 2 \pmod 3$ and $x \equiv 3 \pmod 5$. Since these six statements are consistent, we see that our system is equivalent to the system $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$. These can be solved using the Chinese remainder theorem (see Example 5) to yield $x \equiv 23 \pmod{30}$. Therefore the solutions are all integers of the form $23 + 30k$, where k is an integer.

28. This is just a restatement of the Chinese remainder theorem. Given any such a we can certainly compute $a \bmod m_1$, $a \bmod m_2$, ..., $a \bmod m_n$ to represent it. The Chinese remainder theorem says that there is only one nonnegative integer less than m yielding each n-tuple, so the representation is unique.

30. We follow the hint and suppose that there are two solutions to the set of congruences. Thus suppose that $x \equiv a_i \pmod{m_i}$ and $y \equiv a_i \pmod{m_i}$ for each i. We want to show that these solutions are the same modulo m; this will guarantee that there is only one nonnegative solution less than m. The assumption certainly implies that $x \equiv y \pmod{m_i}$ for each i. But then Exercise 29 tells us that $x \equiv y \pmod m$, as desired.

32. We are asked to solve $x \equiv 0 \pmod 5$ and $x \equiv 1 \pmod 3$. We know from the Chinese remainder theorem that there is a unique answer modulo 15. It is probably quickest just to look for it by dividing each multiple of 5 by 3, and we see immediately that $x = 10$ satisfies the condition. Thus the solutions are all integers congruent to 10 modulo 15. If the numbers involved were larger, then we could use the technique implicit in the proof of Theorem 2 (see Exercise 53).

34. Fermat's little theorem tells us that $23^{40} \equiv 1 \pmod{41}$. Therefore $23^{1002} = (23^{40})^{25} \cdot 23^2 \equiv 1^{25} \cdot 529 = 529 \equiv 37 \pmod{41}$.

36. By Exercise 35, an inverse of 5 modulo 41 is 5^{39}. We can stop there, but presumably we'd like a simpler answer. This could be calculated using modular exponentiation (or, from a practical point of view, with computer algebra software). The simplest form of this is 33, and it is easy to check that $5 \cdot 33 = 165 \equiv 1 \pmod{41}$.

38. **a)** By Fermat's little theorem we know that $3^4 \equiv 1 \pmod 5$; therefore $3^{300} = (3^4)^{75} \equiv 1^{75} \equiv 1 \pmod 5$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \cdot 1 = 9 \pmod 5$, so $3^{302} \bmod 5 = 4$. Similarly, $3^6 \equiv 1 \pmod 7$; therefore $3^{300} = (3^6)^{50} \equiv 1 \pmod 5$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod 7$, so $3^{302} \bmod 7 = 2$. Finally, $3^{10} \equiv 1 \pmod{11}$; therefore $3^{300} = (3^{10})^{30} \equiv 1 \pmod{11}$, and so $3^{302} = 3^2 \cdot 3^{300} \equiv 9 \pmod{11}$, so $3^{302} \bmod 11 = 9$.
b) Since 3^{302} is congruent to 9 modulo 5, 7, and 11, it is also congruent to 9 modulo 385. (This was a particularly trivial application of the Chinese remainder theorem.)

40. Note that the prime factorization of 42 is $2 \cdot 3 \cdot 7$. So it suffices to show that $2 \mid n^7 - n$, $3 \mid n^7 - n$, and $7 \mid n^7 - n$. The first is trivial ($n^7 - n$ is either "odd minus odd" or "even minus even," both of which are even), and each of the other two follows immediately from Fermat's little theorem, because $n^7 - n \equiv (n^2)^3 \cdot n - n \equiv 1 \cdot n - n = 0 \pmod 3$ and $n^7 - n \equiv n - n = 0 \pmod 7$.

42. To decide whether $2^{13}-1=8191$ is prime, we need only look for a prime factor not exceeding $\sqrt{8191}\approx 90.5$. By Exercise 41 every such prime divisor must be of the form $26k+1$. The only candidates are therefore 53 and 79. We easily check that neither is a divisor, and so we conclude that 8191 is prime.

We can take the same approach for $2^{23}-1=8{,}388{,}607$, but we might worry that there will be far too many potential divisors to test, since we must go as far as 2896. By Exercise 41 every prime divisor of $2^{23}-1$ must be of the form $46k+1$. The first candidate divisor is therefore 47. Luckily $47 \mid 8{,}388{,}607$, so we conclude that this Mersenne number is not prime.

44. Let $x_k = b^{(n-1)/2^k} = b^{2^{s-k}t}$, for $k = 0, 1, 2, \ldots, s$. Because n is prime and $n \not| b$, Fermat's little theorem tells us that $x_0 = b^{n-1} \equiv 1 \pmod{n}$. By Exercise 17, because $x_1^2 = (b^{(n-1)/2})^2 = x_0 \equiv 1 \pmod{n}$, either $x_1 \equiv -1 \pmod{n}$ or $x_1 \equiv 1 \pmod{n}$. If $x_1 \equiv 1 \pmod{n}$, because $x_2^2 = x_1 \equiv 1 \pmod{n}$, either $x_2 \equiv -1 \pmod{n}$ or $x_2 \equiv 1 \pmod{n}$. In general, if we have found that $x_0 \equiv x_1 \equiv x_2 \equiv \cdots \equiv x_k \equiv 1 \pmod{n}$, with $k < s$, then, because $x_{k+1}^2 = x_k \equiv 1 \pmod{n}$, we know that either $x_{k+1} \equiv -1 \pmod{n}$ or $x_{k+1} \equiv 1 \pmod{n}$. Continuing this procedure for $k = 1, 2, \ldots, s$, we find that either $x_s = b^t \equiv 1 \pmod{n}$, or $x_k \equiv -1 \pmod{n}$ for some integer k with $0 \le k \le s$. Hence, n passes Miller's test for the base b.

46. This follows from Exercise 49, taking $m = 1$. Alternatively, we can argue directly as follows. Factor $1729 = 7 \cdot 13 \cdot 19$. We must show that this number meets the definition of Carmichael number, namely that $b^{1728} \equiv 1 \pmod{1729}$ for all b relatively prime to 1729. Note that if $\gcd(b, 1729) = 1$, then $\gcd(b, 7) = \gcd(b, 13) = \gcd(b, 19) = 1$. Using Fermat's little theorem we find that $b^6 \equiv 1 \pmod{7}$, $b^{12} \equiv 1 \pmod{13}$, and $b^{18} \equiv 1 \pmod{19}$. It follows that $b^{1728} = (b^6)^{288} \equiv 1 \pmod{7}$, $b^{1728} = (b^{12})^{144} \equiv 1 \pmod{13}$, and $b^{1728} = (b^{18})^{96} \equiv 1 \pmod{19}$. By Exercise 29 (or the Chinese remainder theorem) it follows that $b^{1728} \equiv 1 \pmod{1729}$, as desired.

48. Let b be a positive integer with $\gcd(b, n) = 1$. The $\gcd(b, p_j) = 1$ for $j = 1, 2, \ldots, k$, and hence, by Fermat's little theorem, $b^{p_j - 1} \equiv 1 \pmod{p_j}$ for $j = 1, 2, \ldots, k$. Because $p_j - 1 \mid n - 1$, there are integers t_j with $t_j(p_j - 1) = n - 1$. Hence for each j we know that $b^{n-1} = b^{(p_j-1)t_j} = (b^{(p_j-1)})^{t_j} \equiv 1 \pmod{p_j}$. Therefore $b^{n-1} \equiv 1 \pmod{n}$, as desired.

50. We could use the technique shown in the proof of Theorem 2 to solve each part, or use the approach in our solution to Exercise 32, but since there are so many to do here, it is simpler just to write out all the representations of 0 through 27 and find those given in each part. This task is easily done, since the pattern is clear:

$0 = (0, 0)$	$7 = (3, 0)$	$14 = (2, 0)$	$21 = (1, 0)$
$1 = (1, 1)$	$8 = (0, 1)$	$15 = (3, 1)$	$22 = (2, 1)$
$2 = (2, 2)$	$9 = (1, 2)$	$16 = (0, 2)$	$23 = (3, 2)$
$3 = (3, 3)$	$10 = (2, 3)$	$17 = (1, 3)$	$24 = (0, 3)$
$4 = (0, 4)$	$11 = (3, 4)$	$18 = (2, 4)$	$25 = (1, 4)$
$5 = (1, 5)$	$12 = (0, 5)$	$19 = (3, 5)$	$26 = (2, 5)$
$6 = (2, 6)$	$13 = (1, 6)$	$20 = (0, 6)$	$27 = (3, 6)$

Now we can read off the answers.

a) 0 **b)** 21 **c)** 1 **d)** 22 **e)** 2 **f)** 24 **g)** 14 **h)** 19 **i)** 27

52. To add 4 and 7 we first find that 4 is represented by $(1, 4)$ and that 7 is represented by $(1, 2)$. Adding coordinate-wise, we see that the sum is represented by $(1+1, 4+2) = (2, 6) = (2, 1)$; we are working modulo 5 in the second coordinate. Then we find $(2, 1)$ in the table and see that it represents 11. Therefore we conclude that $4 + 7 = 11$. Note that we can only compute answers less than $3 \cdot 5 = 15$ using this method.

54. We calculate $2^i \bmod 19$ for $i = 1, 2, \ldots, 18$ and see that we get 18 different values. The values are 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1.

56. The proof is the same as the proof for the corresponding identity for the real numbers. To show that $\log_r(ab) \equiv \log_r a + \log_r b \pmod{p-1}$, it suffices (by definition) to show that $r^{\log_r a + \log_r b} \equiv ab \pmod{p-1}$. But $r^{\log_r a + \log_r b} = r^{\log_r a} \cdot r^{\log_r b} \equiv a \cdot b \pmod{p-1}$.

58. We square the first five positive integers and reduce modulo 11, obtaining 1, 4, 9, 5, 3. The squares of the next five are necessarily the same set of numbers modulo 11, since $(-x)^2 = x^2$, so we are done. Therefore the quadratic residues modulo 11 are all integers congruent to 1, 3, 4, 5, or 9 modulo 11.

60. Consider the list $x^2 \bmod p$ as x runs from 1 to $p-1$ inclusive. This gives us $p-1$ numbers between 1 and $p-1$ inclusive. By Exercise 59 every a that appears in this list appears exactly twice. Therefore exactly half of the $p-1$ numbers must appear in the list (i.e., be quadratic residues).

62. First assume that $\left(\frac{a}{p}\right) = 1$. Then the congruence $x^2 \equiv a \pmod{p}$ has a solution, say $x = s$. By Fermat's little theorem $a^{(p-1)/2} = (s^2)^{(p-1)/2} = s^{p-1} \equiv 1 \pmod{p}$, as desired. Next consider the case $\left(\frac{a}{p}\right) = -1$. Then the congruence $x^2 \equiv a \pmod{p}$ has no solution. Let i be an integer between 1 and $p-1$, inclusive. By Theorem 1, i has an inverse i' modulo p, and therefore there is an integer j, namely $i'a$, such that $ij \equiv a \pmod{p}$. Furthermore, since the congruence $x^2 \equiv a \pmod{p}$ has no solution, $j \neq i$. Thus we can group the integers from 1 to $p-1$ into $(p-1)/2$ pairs each with the product a. Multiplying these pairs together, we find that $(p-1)! \equiv a^{(p-1)/2} \pmod{p}$. But now Wilson's theorem (see Exercise 18) tells us that this latter value is -1, again as desired.

64. If $p \equiv 1 \pmod{4}$, then $(p-1)/2$ is even, so the right-hand side of the equivalence in Exercise 62 with $a = -1$ is $+1$, that is, -1 is a quadratic residue. Conversely, if $p \equiv 3 \pmod{4}$, then $(p-1)/2$ is odd, so the right-hand side of the equivalence in Exercise 62 with $a = -1$ is -1, that is, -1 is not a quadratic residue.

66. We follow the hint. Working modulo 3, we want to solve $x^2 \equiv 16 \equiv 1$. It is easy to see that there are exactly two solutions modulo 3, namely $x = 1$ and $x = 2$. Similarly we find the solutions $x = 1$ and $x = 4$ to $x^2 \equiv 16 \equiv 1 \pmod{5}$; and the solutions $x = 3$ and $x = 4$ to $x^2 \equiv 16 \equiv 2 \pmod{7}$. Therefore we want to find values of x modulo $3 \cdot 5 \cdot 7 = 105$ such that $x \equiv 1$ or $2 \pmod{3}$, $x \equiv 1$ or $4 \pmod{5}$ and $x \equiv 3$ or $4 \pmod{7}$. We can do this by applying the Chinese remainder theorem (as in Example 5) eight times, for the eight combinations of these values. For example, to solve $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$, and $x \equiv 3 \pmod{7}$, we find that $m = 105$, $M_1 = 35$, $M_2 = 21$, $M_3 = 15$, $y_1 = 2$, $y_2 = 1$, $y_3 = 1$, so $x \equiv 1 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 136 \equiv 31 \pmod{105}$. Doing the similar calculation with the other seven possibilities yields the other solutions modulo 105: $x = 4$, $x = 11$, $x = 46$, $x = 59$, $x = 74$, $x = 94$ and $x = 101$.

SECTION 4.5 Applications of Congruences

2. In each case we need to compute k **mod** 101 by dividing by 101 and finding the remainders. This can be done with a calculator that keeps 13 digits of accuracy internally. Just divide the number by 101, subtract off the integer part of the answer, and multiply the fraction that remains by 101. The result will be almost exactly an integer, and that integer is the answer.

a) 58 **b)** 60 **c)** 52 **d)** 3

4. We compute as follows: $h(k_1) = 1524$; $h(k_2) = 578$; $h(k_3) = 578$, which collides, $h(k_3, 1) = 2505$, so k_3 is assigned memory location 2505; $h(k_4) = 2376$; $h(k_5) = 3960$; $h(k_6) = 1526$; $h(k_7) = 2854$; $h(k_8) = 1526$, which collides, $h(k_8, 1) = 4927$, so k_8 is assigned memory location 4927; $h(k_9) = 3960$, which collides, $h(k_9, 1) = 6100 \equiv 1131 \pmod{4969}$, so k_9 is assigned memory location 1131; $h(k_{10}) = 3960$, which collides, $h(k_{10}, 1) = 4702$, so k_{10} is assigned memory location 4702. Notice that we never had to go above $i = 1$ in the probing sequence.

6. We just calculate using the formula. We are given $x_0 = 3$. Then $x_1 = (4 \cdot 3 + 1)$ **mod** $7 = 13$ **mod** $7 = 6$; $x_2 = (4 \cdot 6 + 1)$ **mod** $7 = 25$ **mod** $7 = 4$; $x_3 = (4 \cdot 4 + 1)$ **mod** $7 = 17$ **mod** $7 = 3$. At this point the sequence must continue to repeat 3, 6, 4, 3, 6, 4, ... forever.

8. We assume that the input to this procedure consists of a modulus ($m \geq 2$), a multiplier (a), an increment (c), a seed (x_0), and the number (n) of pseudorandom numbers desired. The output will be the sequence $\{x_i\}$.

procedure *pseudorandom*$(m, a, c, x_0, n$: nonnegative integers)
for $i := 1$ **to** n
$x_i := (ax_{i-1} + c)$ **mod** m

10. We follow the instructions. Because $3792^2 = 14379264$, the middle four digits are 3792, which is the number we started with. So this sequence is not random at all—it's constant! Similarly, $2916^2 = 08503056$, $5030^2 = 25300900$, $3009^2 = 09054081$, and $0540^2 = 00291600$, which gives us back the number we started with, so this sequence degenerates into a repeating sequence with period 4.

12. We are told to apply the formula $x_{n+1} = x_n^2$ **mod** 11, starting with $x_0 = 3$. Thus $x_1 = 3^2$ **mod** $11 = 9$, $x_3 = 9^2$ **mod** $11 = 4$, $x_4 = 4^2$ **mod** $11 = 5$, $x_5 = 5^2$ **mod** $11 = 3$, and we are back where we started. The sequence generated here is $3, 9, 4, 5, 3, 9, 4, 5, \ldots$.

14. If a string contains an odd number of errors, then the number of 1's in the string with its check bit will differ by an odd number from what it should be, which means it will be an odd number, rather than the expected even number, and we will know that there is an error. If the string contains an even number of errors, then the number of 1's in the string with its check bit will differ by an even number from what it should be, which means it will be an even number, as expected, and we will not know that anything is wrong.

16. We know that $1 \cdot 0 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 0 + 7 \cdot 0 + 8 \cdot Q + 9 \cdot 1 + 10 \cdot 8 \equiv 0 \pmod{11}$. This simplifies to $130 + 8Q \equiv 0 \pmod{11}$. We subtract 130 from both sides and simplify to $8Q \equiv 2 \pmod{11}$, since $-130 = -12 \cdot 11 + 2$. It is now a simple matter to use trial and error (or the methods of Section 4.4) to find that $Q = 3$ (since $24 \equiv 2 \pmod{11}$).

18. In each case we just have to compute $x_1 + x_2 + \cdots + x_{10}$ **mod** 9 The easiest way to do this by hand is to "cast out nines," i.e., throw away sums of 9 as we come to them.

a) $7 + 5 + 5 + 5 + 6 + 1 + 8 + 8 + 7 + 3$ **mod** $9 = 1$ **b)** 5 **c)** 2 **d)** 0

20. In each case we want to solve the equation $x_1 + x_2 + \cdots + x_{10} \equiv x_{11} \pmod 9$ for the missing digit, which is easily done by inspection (one can throw away 9's).

a) $Q + 1 + 2 + 2 + 3 + 1 + 3 + 9 + 7 + 8 \equiv 4 \pmod 9 \Rightarrow Q \equiv 4 \pmod 9 \Rightarrow Q = 4$

b) $6 + 7 + 0 + 2 + 1 + 2 + 0 + Q + 9 + 8 \equiv 8 \pmod 9 \Rightarrow Q + 8 \equiv 8 \pmod 9 \Rightarrow Q \equiv 0 \pmod 9$. 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.

c) $2 + 7 + Q + 4 + 1 + 0 + 0 + 7 + 7 + 3 \equiv 4 \pmod 9 \Rightarrow Q + 4 \equiv 4 \pmod 9 \Rightarrow Q \equiv 0 \pmod 9$. 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.

d) $2 + 1 + 3 + 2 + 7 + 9 + 0 + 3 + 2 + Q \equiv 1 \pmod 9 \Rightarrow Q + 2 \equiv 1 \pmod 9 \Rightarrow Q \equiv 8 \pmod 9 \Rightarrow Q = 8$

22. If one digit is changed to a value not congruent to it modulo 9, then the modular equivalence implied by the equation in the preamble will no longer hold. Therefore all single digit errors are detected except for the substitution of a 9 for a 0 or vice versa.

24. In each case we want to solve the equation $3x_1 + x_2 + 3x_3 + x_4 + \cdots + 3x_{11} + x_{12} \equiv 0 \pmod{10}$ for x_{12}, which can be done mentally, because we need to keep track of only the last digit.

a) $3 \cdot 7 + 3 + 3 \cdot 2 + 3 + 3 \cdot 2 + 1 + 3 \cdot 8 + 4 + 3 \cdot 4 + 3 + 3 \cdot 4 + x_{12} \equiv 0 \pmod{10} \Rightarrow x_{12} = 5$

b) $3 \cdot 6 + 3 + 3 \cdot 6 + 2 + 3 \cdot 3 + 9 + 3 \cdot 9 + 1 + 3 \cdot 3 + 4 + 3 \cdot 6 + x_{12} \equiv 0 \pmod{10} \Rightarrow x_{12} = 2$

c) $3 \cdot 0 + 4 + 3 \cdot 5 + 8 + 3 \cdot 7 + 3 + 3 \cdot 2 + 0 + 3 \cdot 7 + 2 + 3 \cdot 0 + x_{12} \equiv 0 \pmod{10} \Rightarrow x_{12} = 0$

d) $3 \cdot 9 + 3 + 3 \cdot 7 + 6 + 3 \cdot 4 + 3 + 3 \cdot 2 + 3 + 3 \cdot 3 + 4 + 3 \cdot 1 + x_{12} \equiv 0 \pmod{10} \Rightarrow x_{12} = 3$

26. Yes. Any single digit error will change, say, x to y, and one side of the congruence given in Example 5 will differ by either $x - y$ or $3(x - y)$ from its true value. Because $x - y \not\equiv 0$ and $3(x - y) \not\equiv 0 \pmod{10}$ (since 3 is relatively prime to 10), the congruence will no longer hold.

28. In each case we need to compute the remainder of the given 14-digit number upon division by 7.

a) 10237424413392 **mod** $7 = 1$ **b)** 00032781811234 **mod** $7 = 4$

c) 00611232134231 **mod** $7 = 5$ **d)** 00193222543435 **mod** $7 = 5$

30. A change in the digit in the n^{th} column from the right in the 14-digit number formed by the first 14 digits of the airline ticket identification number (with $n = 0$ corresponding to the units digit), say from x to y, will cause this 14-digit number to differ from its correct value by $(x - y)10^n$. If this equals 0 modulo 7, then the error will not be detected. Because 7 and 10 are relatively prime, that will happen if and only if $|x - y| = 7$; therefore we can detect errors except $0 \leftrightarrow 7$, $1 \leftrightarrow 8$, $2 \leftrightarrow 9$. The same reasoning applies to the check digit (although of course 7, 8, and 9 are invalid digits for the check digit anyway).

32. It follows from the preamble that we need to compute $3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7$ **mod** 11 in order to determine the check digit d_8.

a) $3 \cdot 1 + 4 \cdot 5 + 5 \cdot 7 + 6 \cdot 0 + 7 \cdot 8 + 8 \cdot 6 + 9 \cdot 8$ **mod** $11 = 3$

b) $3 \cdot 1 + 4 \cdot 5 + 5 \cdot 5 + 6 \cdot 3 + 7 \cdot 7 + 8 \cdot 3 + 9 \cdot 4$ **mod** $11 = 10$, so the check digit is X.

c) $3 \cdot 1 + 4 \cdot 0 + 5 \cdot 8 + 6 \cdot 9 + 7 \cdot 7 + 8 \cdot 0 + 9 \cdot 8$ **mod** $11 = 9$

d) $3 \cdot 1 + 4 \cdot 3 + 5 \cdot 8 + 6 \cdot 3 + 7 \cdot 8 + 8 \cdot 1 + 9 \cdot 1$ **mod** $11 = 3$

34. Yes. Any single digit error will change, say, x to y, and one side of the congruence given in the preamble will differ by $a(x - y)$, for some $a \in \{1, 3, 4, 5, 6, 7, 8, 9\}$, from its true value. Each of those values of a is relatively prime to 11, so $a(x - y) \not\equiv 0 \pmod{11}$ and the congruence will no longer hold.

SECTION 4.6 Cryptography

2. These are straightforward arithmetical calculations, as in Exercise 1.
a) WXST TSPPYXMSR **b)** NOJK KJHHPODJI **c)** QHAR RABBYHCAJ

4. We just need to "subtract 3" from each letter. For example, E goes down to B, and B goes down to Y.
a) BLUE JEANS **b)** TEST TODAY **c)** EAT DIM SUM

6. Under these assumptions we guess that the plaintext E became the ciphertext X. Since the number for E is 4 and the number for X is 23, $k = 23 - 4 = 19$.

8. Because of the word JVVU we guess that the ciphertext V might be the plaintext E or O. If it is the former, then the shift would have to be $21 - 4 = 17$. Applying the inverse of that shift to the message yields MEN LOVE TO WONDER, AND THAT IS THE SEED OF SCIENCE.

10. If the enciphering function is $f(p) = (p+k) \bmod 26$, then the deciphering function is $f^{-1}(p) = (p-k) \bmod 26$. Thus we seek a k such that $k \equiv -k \pmod{26}$, and the unique solution is $k = 13$.

12. If $\overline{a}$ is the inverse of a modulo 26, then the decryption function for the encryption function $c = (ap+b) \bmod 26$ is $p = \overline{a}(c-b) \bmod 26 = (\overline{a}c - \overline{a}b) \bmod 26$. Clearly two different pairs (a, b) cannot give the same encryption function, so we need to solve the system of congruences $\overline{a} \equiv a \pmod{26}$ and $b \equiv -\overline{a}b \pmod{26}$. Only 1 and -1 (which is the same as 25) are their own multiplicative inverses modulo 26 (this can be verified by asking a computer algebra system to compute all the inverses), so there are two cases. If $a = 1$, then the second congruence becomes $b \equiv -b \pmod{26}$, whose solutions are $b = 0$ and $b = 13$. This says that the identity function $c = p \bmod 26$ satisfies the given condition (although that was obvious and not very interesting), and so does $c = (p + 13) \bmod 26$. If $a = -1$, then the second congruence becomes $b \equiv b \pmod{26}$, which is satisfied by all values of b. Therefore all encryption functions of the form $c = (-p + b) \bmod 26$ also have themselves as the corresponding decryption function. The answer to the question phrased in terms of pairs is $(1, 0)$, $(1, 13)$, and $(-1, b)$ (or, equivalently, $(25, b)$) for all b.

14. Within each block of five letters (GRIZZ LYBEA RSXXX) we send the first letter to the third letter, the second letter to the fifth letter, and so on. So the encrypted message is IZGZR BELAY XXRXS.

16. One method, using technology, would be to try all possibilities. For $n = 2, 3, 4, \ldots$, have the computer go through all $n!$ permutations of $\{1, 2, 3, \ldots, n\}$ and for each one permute blocks of n letters of the ciphertext, printing out the resulting plaintext on the computer screen. You, a human, can look at them and figure out which ones make sense as a message.

18. The plaintext string in numbers is 18-13-14-22-5-0-11-11. We add the string for the key repeated twice, 1-11-20-4-1-11-20-4, to obtain the string 19-24-8-0-6-11-5-15, which in letters is TYIAGLFP.

20. A cryptosystem is a 5-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, as explained in Definition 1. We follow the discussion of Example 7. As there, $\mathcal{P}$ and $\mathcal{C}$ are strings of elements of $\mathbf{Z}_{26}$. The set of keys is the set of strings over $\mathbf{Z}_{26}$ as well. The set of encryption functions is the set of functions described in the preamble to Exercise 18. The set of decryption functions is the same, because decrypting with the string a-b-c-$\ldots$ is the same as encrypting with the string $(-a)$-$(-b)$-$(-c)$-$\ldots$

22. Suppose the length of the key string is l. We can apply the frequency method, explained in Example 5 and the preceding discussion, to the letters in positions 1, $1 + l$, $1 + 2l$, $\ldots$ to determine the first letter of the key string (viewed as a number from 0 to 25), then do the same for the second letter, and so on up to the l^{th} letter.

24. Translating the letters into numbers we have 0019 1900 0210. Thus we need to compute $C = P^{13}$ **mod** 2537 for $P = 19$, $P = 1900$, and $P = 210$. The results of these calculations, done by fast modular multiplication or a computer algebra system are 2299, 1317, and 2117, respectively. Thus the encrypted message is 2299 1317 2117.

26. First we find d, the inverse of $e = 17$ modulo $52 \cdot 60$. A computer algebra system tells us that $d = 2753$. Next we have the CAS compute c^d **mod** n for each of the four given numbers: 3185^{2753} **mod** $3233 = 1816$ (which are the letters SQ), 2038^{2753} **mod** $3233 = 2008$ (which are the letters UI), 2460^{2753} **mod** $3233 = 1717$ (which are the letters RR), and 2550^{2753} **mod** $3233 = 0411$ (which are the letters EL). The message is SQUIRREL.

28. If $M \equiv 0 \pmod{n}$, then $C \equiv M^e \equiv 0 \pmod{n}$ and so $C^d \equiv 0 \equiv M \pmod{n}$. Otherwise, $\gcd(M, p) = p$ and $\gcd(M, q) = 1$, or $\gcd(M, p) = 1$ and $\gcd(M, q) = q$. By symmetry it suffices to consider the first case, where $M \equiv 0 \pmod{p}$. We have $C^d \equiv (M^e)^d \equiv (0^e)^d \equiv 0 \equiv M \pmod{p}$. As in the case considered in the text, $de = 1 + k(p-1)(q-1)$ for some integer k, so

$$C^d \equiv M^{de} \equiv M^{1+k(p-1)(q-1)} \equiv M \cdot M^{(q-1)^{k(p-1)}} \equiv M \cdot 1 \equiv M \pmod{q}$$

by Fermat's little theorem. Thus by the Chinese remainder theorem, $C^d \equiv M \pmod{pq}$.

30. We follow the steps given in the text, with $p = 101$, $a = 2$, $k_1 = 7$, and $k_2 = 9$. Using *Maple*, we verify that 2 is a primitive root modulo 101, by noticing that 2^k as k runs from 0 to 99 produce distinct values (and of course 2^{100} **mod** $101 = 1$). We find that 2^7 **mod** $101 = 27$. So in Step (2), Alice sends 27 to Bob. Similarly, in Step (3), Bob sends 2^9 **mod** $101 = 7$ to Alice. In Step (4) Alice computes 7^7 **mod** $101 = 90$, and in Step (5) Bob computes 27^9 **mod** $101 = 90$. These are the same, of course, and thus 90 is the shared key.

32. When broken into blocks and translated into numbers the message is 0120 2413 1422. Alice applies her decryption transformation $D_{(2867,7)}(x) = x^{1183}$ **mod** 2867 to each block, which we compute with a CAS to give 1665 1728 2123. Next she applies Bob's encryption transformation $E_{(3127,21)}(x) = x^{21}$ **mod** 3127 to each block, which we compute with a CAS to give 2806 1327 0412. She sends that to Bob. Only Bob can read it, which he does by first applying his decryption transformation $D_{(3127,21)}(x) = x^{1149}$ **mod** 3127 to each block, recovering 1665 1728 2123, and then applying Alice's encryption transformation $E_{(2867,7)}(x) = x^7$ **mod** 2867 to each of these blocks, recovering the original 0120 2413 1422, BUY NOW.

SUPPLEMENTARY EXERCISES FOR CHAPTER 4

2. **a)** Each week consists of seven days. Therefore to find how many (whole) weeks there are in n days, we need to see how many 7's there are in n. That is exactly what n **div** 7 tells us.

b) Each day consists of 24 hours. Therefore to find how many (whole) days there are in n hours, we need to see how many 24's there are in n. That is exactly what n **div** 24 tells us.

4. Let $q = \left\lceil \frac{a}{d} - \frac{1}{2} \right\rceil$ and $r = a - dq$. Then we have forced $a = dq + r$, so it remains to prove that $-d/2 < r \leq d/2$. Now since $q - 1 < \frac{a}{d} - \frac{1}{2} \leq q$, we have (by multiplying through by d and adding $d/2$) $dq - \frac{d}{2} < a \leq dq + \frac{d}{2}$, so $-\frac{d}{2} < a - dq \leq \frac{d}{2}$, as desired.

6. By Exercise 38 in Section 4.1, the square of an integer is congruent to either 0 or 1 modulo 4, where obviously the odd integers have squares congruent to 1 modulo 4. The sum of two of these is therefore congruent to 2 modulo 4, so cannot be a square.

8. If there were integer solutions to this equation, then by definition we would have $x^2 \equiv 2 \pmod 5$. However we easily compute (as in Exercise 40 in Section 4.1) that the square of an integer of the form $5k$ is congruent to 0 modulo 5; the square of an integer of the form $5k+1$ is congruent to 1 modulo 5; the square of an integer of the form $5k+2$ is congruent to 4 modulo 5; the square of an integer of the form $5k+3$ is congruent to 4 modulo 5; and the square of an integer of the form $5k+4$ is congruent to 1 modulo 5. This is a contradiction, so no solutions exist.

10. The number 3 plays the same role in base two that the number 11 plays in base ten (essentially because $(11)_2 = 3$). The divisibility test for 11 in base ten is that $d_n d_{n-1} \ldots d_2 d_1 d_0$ is divisible by 11 if and only if the alternating sum $d_0 - d_1 + d_2 - \cdots + (-1)^n d_n$ is divisible by 11. The corresponding rule here is that $(d_n d_{n-1} \ldots d_2 d_1 d_0)_2$ is divisible by 3 if and only if the alternating sum $d_0 - d_1 + d_2 - \cdots + (-1)^n d_n$ is divisible by 3. For example, $27 = (11011)_2$ is divisible by 3 because $1 - 1 + 0 - 1 + 1 = 0$ is divisible by 3. The proof follows from the fact that $2^n - 1 \equiv 0 \pmod 3$ if n is even and $2^n + 1 \equiv 0 \pmod 3$ if n is odd. Thus we have

$$\begin{aligned}(d_n d_{n-1} \ldots d_2 d_1 d_0)_2 &= d_0 + 2d_1 + 2^2 d_2 + 2^3 d_3 + \cdots 2^n d_n \\ &= d_0 + (3k_1 - 1)d_1 + (3k_2 + 1)d_2 + (3k_3 - 1)d_3 + \cdots + (3k_n + (-1)^n)d_n \\ &= [d_0 - d_1 + d_2 - \cdots + (-1)^n d_n] + [3(k_1 d_1 + k_2 d_2 + k_3 d_3 + \cdots + k_n d_n)]\end{aligned}$$

for integers $k_1 = 1$, $k_2 = 1$, $k_3 = 3$, $k_4 = 5$, $k_5 = 11, \ldots$. The second bracketed expression is always divisible by 3, so the entire number is divisible by 3 if and only if the alternating sum is.

12. As we see from Exercise 11, at most n questions (guesses) are needed. Furthermore, at least this many yes/no questions are needed as well, since if we asked fewer questions, then by the pigeonhole principle, two numbers would produce the same set of answers and we would be unable to guess the number accurately. Thus the complexity is n questions. (The case $n = 0$ is not included, since in that case no questions are needed.) We are assuming throughout this exercise and the previous one that the inclusive sense of "between" was intended.

14. First note that since both a and b must be greater than 1, the sequences $\lfloor ka \rfloor$ and $\lfloor kb \rfloor$ do not list any positive integer twice. The issue is whether any positive integer is listed in both sequences, or whether some positive integer is omitted altogether. Let $N(x, n)$ denote the number of positive integers in the set $\{ \lfloor kx \rfloor \mid k \text{ is a positive integer} \}$ that are less than or equal to n. Then it is enough to prove that $N(a, n) + N(b, n) = n$ for all positive integers n. (That way no positive integer could be left out or appear twice when we consider all the numbers $\lfloor ka \rfloor$ and $\lfloor kb \rfloor$.) Now $N(a, n)$ is the number of positive integers k for which $\lfloor ka \rfloor \le n$, which is just the number of positive integers k for which $ka < n + 1$, since a is irrational, and this is clearly $\lfloor (n+1)/a \rfloor$. We have a similar result for b. Let $f(x)$ denote the fractional part of x (i.e., $f(x) = x - \lfloor x \rfloor$). Then we have

$$N(a, n) + N(b, n) = \left\lfloor \frac{n+1}{a} \right\rfloor + \left\lfloor \frac{n+1}{b} \right\rfloor = \frac{n+1}{a} - f\left(\frac{n+1}{a}\right) + \frac{n+1}{b} - f\left(\frac{n+1}{b}\right).$$

But the sum of the first and third terms of the right-hand side here is $n + 1$, since we are given that $(1/a) + (1/b) = 1$. The second and fourth terms are each fractions strictly between 0 and 1, and the entire expression is an integer, so they must sum to 1. Therefore the displayed value is $n + 1 - 1 = n$, as desired.

16. The first few of these are $Q_1 = 2$, $Q_2 = 3$, $Q_3 = 7$, $Q_4 = 25$, and $Q_5 = 121$. Although the first three are prime, the next two are not. In fact, a CAS tells us that Q_4 through $Q_{10} = 3{,}628{,}801 = 11 \cdot 329{,}891$ are all not prime. The only other primes among the first 100 are Q_{11}, Q_{27}, Q_{37}, Q_{41}, Q_{73}, and Q_{77}.

18. We can give a nice proof by contraposition here, by showing that if n is not prime, then the sum of its divisors is not $n + 1$. There are two cases. If $n = 1$, then the sum of the divisors is $1 \ne 1 + 1$. Otherwise n is composite, so can be written as $n = ab$, where both a and b are divisors of n different from 1 and from n

(although it might happen that $a = b$). Then n has at least the three distinct divisors 1, a, and n, and their sum is clearly not equal to $n + 1$. This completes the proof by contraposition. One should also observe that the converse of this statement is also true: if n is prime, then the sum of its divisors is $n + 1$ (since its only divisors are 1 and itself).

20. This question is asking for the smallest pair of primes that differ by 6. Looking at a table of prime numbers tells us that these are 23 and 29, so the five smallest consecutive composite integers are 24, 25, 26, 27, and 28.

22. Using a computer algebra system, such as *Maple* with its ability to loop and its built-in primeness tester, is the only reasonable way to solve this problem. The answer is 7, 37, 67, 97, 127, 157 (i.e., the common difference is 30). The analogous question for seven primes has common difference 150. A search for a string of eight primes in arithmetic progression found one with starting value 17 and common difference 6930.

24. There is one 0 at the end of this number for every factor of 2 in all of the numbers from 1 to 100. We count them as follows. All the even numbers have a factor of 2, and there are $100/2 = 50$ of these. All the multiples of 4 have another factor of 2, and there are $100/4 = 25$ of these. All the multiples of 8 have another factor of 2, and there are $\lfloor 100/8 \rfloor = 12$ of these, and so on. Thus the answer is $50 + 25 + 12 + 6 + 3 + 1 = 97$.

26. We need to divide successively by 233, 144, 89, 55, 34, 21, 13, 8, 5, 3, 2, and 1, a total of 12 divisions.

28. **a)** The first statement is clear. For the second, if a and b are both even, then certainly 2 is a factor of their greatest common divisor, and the complementary factor must be the greatest common divisor of the numbers obtained by dividing out this 2. For the third statement, if a is even and b is odd, then the factor of 2 in a will not appear in the greatest common divisor, so we can ignore it. Finally, the last statement follows from Lemma 1 in Section 4.3, taking $q = 1$ (despite the notation, nothing in Lemma 1 required q to be the quotient).

b) All the steps involved in implementing part **(a)** as an algorithm require only comparisons, subtractions, and divisions of even numbers by 2. Since division by 2 is a shift of one bit to the right, only the operations mentioned here are used. (Note that the algorithm needs two more reductions: if a is odd and b is even, then $\gcd(a, b) = \gcd(a, b/2)$, and if $a < b$, then interchange a and b.)

c) We show the operation of the algorithm as a string of equalities; each equation is one step.

$$\begin{aligned}
\gcd(1202, 4848) &= \gcd(4848, 1202) = 2\gcd(2424, 601) = 2\gcd(1212, 601) = 2\gcd(606, 601) \\
&= 2\gcd(303, 601) = 2\gcd(601, 303) = 2\gcd(298, 303) = 2\gcd(303, 298) \\
&= 2\gcd(303, 149) = 2\gcd(154, 149) = 2\gcd(77, 149) = 2\gcd(149, 77) \\
&= 2\gcd(72, 77) = 2\gcd(77, 72) = 2\gcd(77, 36) = 2\gcd(77, 18) \\
&= 2\gcd(77, 9) = 2\gcd(68, 9) = 2\gcd(34, 9) = 2\gcd(17, 9) \\
&= 2\gcd(8, 9) = 2\gcd(9, 8) = 2\gcd(9, 4) = 2\gcd(9, 2) \\
&= 2\gcd(9, 1) = 2\gcd(8, 1) = 2\gcd(4, 1) = 2\gcd(2, 1) \\
&= 2\gcd(1, 1) = 2
\end{aligned}$$

30. 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 $3k + 1$. Notice that the product of primes of this form is again of this form, because $(3k_1 + 1)(3k_2 + 1) = 9k_1k_2 + 3k_1 + 3k_2 + 1 = 3(3k_1k_2 + k_1 + k_2) + 1$. We could try looking at $3p_1p_2 \cdots p_n + 1$, 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 $3k + 1$,

because the product of two primes not of this form, namely of the form $3k+2$, is of the form $3k+1$; indeed, $(3k_1+2)(3k_2+2) = 9k_1k_2 + 6k_1 + 6k_2 + 4 = 3(3k_1k_2 + 2k_1 + 2k_2 + 1) + 1$. Thus the proof breaks down at this point.

32. We give a proof by contradiction. Suppose that $p > \sqrt[3]{n}$, where p is the smallest prime factor of n, but n/p is not prime and not equal to 1. Then $p^3 > n$, so $p^2 > n/p$. By our assumption, $n/p = a \cdot b$, where $a, b > 1$. Because $a \cdot b < p^2$, at least one of a and b is less than p; assume without loss of generality that it is a. Then a is a divisor of n smaller than p, so any prime factor of a is a prime divisor of n smaller than p, in contradiction to our assumptions.

34. We need to arrange that every pair of the four numbers has a factor in common. There are six such pairs, so let us use the first six prime numbers as the common factors. Call the numbers a, b, c, and d. We will give a and b a common factor of 2; a and c a common factor of 3; a and d a common factor of 5; b and c a common factor of 7; b and d a common factor of 11; and c and d a common factor of 13. The simplest way to accomplish this is to let $a = 2 \cdot 3 \cdot 5 = 30$; $b = 2 \cdot 7 \cdot 11 = 154$; $c = 3 \cdot 7 \cdot 13 = 273$; and $d = 5 \cdot 11 \cdot 13 = 715$. The numbers are mutually relatively prime, since no number is a factor of all of them (indeed, each prime is a factor of only two of them). Many other examples are possible, of course.

36. If $x \equiv 3 \pmod 9$, then $x = 3 + 9t$ for some integer t. In particular this equation tells us that $3 \mid x$. On the other hand the first congruence says that $x = 2 + 6s = 2 + 3 \cdot (2s)$ for some integer s, which implies that the remainder when x is divided by 3 is 2. Obviously these two conclusions are inconsistent, so there is no simultaneous solution to the two congruences.

38. **a)** There are two things to prove here. First suppose that $\gcd(m_1, m_2) \mid a_1 - a_2$; say $a_1 - a_2 = k \cdot \gcd(m_1, m_2)$. By Theorem 6 in Section 4.3, there are integers s and t such that $\gcd(m_1, m_2) = sm_1 + tm_2$. Multiplying both sides by k and substituting into our first equation we have $a_1 - a_2 = ksm_1 + ktm_2$, which can be rewritten as $a_1 - ksm_1 = a_2 + ktm_2$. This common value is clearly congruent to a_1 modulo m_1 and congruent to a_2 modulo m_2, so it is a solution to the given system. Conversely, suppose that there is a solution x to the system. Then $x = a_1 + sm_1 = a_2 + tm_2$ for some integers s and t. This says that $a_1 - a_2 = tm_2 - sm_1$. But $\gcd(m_1, m_2)$ divides both m_1 and m_2 and therefore divides the right-hand side of this last equation. Therefore it also divides the left-hand side, $a_1 - a_2$, as desired.

b) We follow the idea sketched in Exercises 29 and 30 of Section 4.4. First we show that if $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$, then $a \equiv b \pmod{\text{lcm}(m_1, m_2)}$. The first hypothesis says that $m_1 \mid a - b$; the second says that $m_2 \mid a - b$. Therefore $a - b$ is a common multiple of m_1 and m_2. If $a - b$ were not also a multiple of $\text{lcm}(m_1, m_2)$, then $(a - b)$ **mod** $\text{lcm}(m_1, m_2)$ would be a common multiple as well, contradicting the definition of $\text{lcm}(m_1, m_2)$. Therefore $a - b$ is a multiple of $\text{lcm}(m_1, m_2)$, i.e., $a \equiv b \pmod{\text{lcm}(m_1, m_2)}$. Now suppose that there were two solutions to the given system of congruences. By what we have just proved, since these two solutions are congruent modulo m_1 (since they are both congruent to a_1) and congruent modulo m_2 (since they are both congruent to a_2), they must be congruent to each other modulo $\text{lcm}(m_1, m_2)$. That is precisely what we wanted to prove.

40. Note that the prime factorization of 35 is $5 \cdot 7$. So it suffices to show that $5 \mid n^{12} - 1$ and $7 \mid n^{12} - 1$ for integers n relatively prime to 5 and 7. For such integers, Fermat's little theorem tells us that $n^4 \equiv 1 \pmod 5$ and $n^6 \equiv 1 \pmod 7$. Then we have $n^{12} - 1 \equiv (n^4)^3 - 1 \equiv 1^3 - 1 = 0 \pmod 5$ and $n^{12} - 1 \equiv (n^6)^2 - 1 \equiv 1^2 - 1 = 0 \pmod 7$.

42. In each case we just compute $(a_1 + a_3 + \cdots + a_{13}) + 3(a_2 + a_4 + \cdots + a_{12})$ **mod** 10 to make sure that it equals 0.

a) $(9+8+0+3+0+7+1)+3(7+0+7+2+6+9)$ **mod** $10=1$; invalid
b) $(9+8+4+4+4+2+1)+3(7+0+5+2+5+1)$ **mod** $10=2$; invalid
c) $(9+8+1+1+8+1+0)+3(7+3+6+4+4+0)$ **mod** $10=0$; valid
d) $(9+8+2+1+0+7+9)+3(7+0+0+1+1+9)$ **mod** $10=0$; valid

44. If two digits in odd locations, or two digits in even locations, are transposed, then the sum is the same, so this error will not be detected.

46. Because 3, 7, and 1 are all relatively prime to 10, changing a single digit to a different value will change the sum modulo 10 and the congruence will no longer hold. Transposition errors involving just d_1, d_4, and d_7 (and similarly for transpositions within $\{d_2, d_5, d_8\}$ or within $\{d_3, d_6, d_9\}$) clearly cannot be detected. If a transposition error occurs between two digits in different groups, it will be detected if the difference between the transposed values is not 5 but will not be detected if it is (i.e., transposing a 1 with a 6, or a 2 with a 7, and so on). To see why this is true in one case (the other cases are similar), suppose that $d_1 = x$ and $d_2 = y$ are interchanged. Then the sum is increased by $3(y-x)+7(x-y) = 4(x-y)$. This will be 0 modulo 10 if and only if $4(x-y)$ is not a multiple of 10, which is equivalent to $x-y$ not being a multiple of 5.

48. **a)** The seed is 23 (X); adding this mod 26 to the first character of the plaintext, 13 (N), gives 10, which is K. Therefore the first character of the ciphertext is K. The next character of the keystream is the aforementioned 13 (N); add this to O (14) to get 1 (B), so the next character of the ciphertext is B. We continue in this manner, producing the encrypted message KBK A LAL XBUQ XH RHGKLH.
b) Again the seed is 23 (X); adding this mod 26 to the first character of the plaintext, 13 (N), gives 10, which is K. Therefore the first character of the ciphertext is K. The next character of the keystream is the aforementioned K (10); add this to O (14) to get 24 (Y), so the next character of the ciphertext is Y. We continue in this manner, producing the encrypted message KYU CU NUY RZLP IW ZDFNQU.