SECTION 3.4 The Integers and Division

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 $44 \textbf{ div } 8 = 5$ and remainder $44 \textbf{ mod } 8 = 4$.

b) Since $21 \cdot 37 = 777$, we have quotient $777 \textbf{ div } 21 = 37$ and remainder $777 \textbf{ mod } 21 = 0$.

c) As above, we can compute $123 \textbf{ div } 19 = 6$ and $123 \textbf{ mod } 19 = 9$. 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 $-123 \textbf{ div } 19 = -7$ and $-123 \textbf{ mod } 19 = 10$, we note that $-123 = (-7)(19) + 10$.

d) Since $1 \textbf{ div } 23 = 0$ and $1 \textbf{ mod } 23 = 1$, we have $-1 \textbf{ div } 23 = -1$ and $-1 \textbf{ mod } 23 = 22$.

e) Since $2002 \textbf{ div } 87 = 23$ and $2002 \textbf{ mod } 87 = 1$, we have $-2002 \textbf{ div } 87 = -24$ and $2002 \textbf{ mod } 87 = 86$.

f) Clearly $0 \textbf{ div } 17 = 0$ and $0 \textbf{ mod } 17 = 0$.

g) We have $1234567 \textbf{ div } 1001 = 1233$ and $1234567 \textbf{ mod } 1001 = 334$.

h) Since $100 \textbf{ div } 101 = 0$ and $100 \textbf{ mod } 101 = 100$, we have $-100 \textbf{ div } 101 = -1$ and $-100 \textbf{ mod } 101 = 1$.

12. 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 $a \textbf{ mod } m$. We know that $b = qm + r$ for some nonnegative r less than m (namely, $r = b \textbf{ mod } m$). Therefore we can write $a = qm + r + mc = (q + c)m + r$. By definition this means that r must also equal $a \textbf{ mod } m$. That is what we wanted to prove.

14. 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.

16. 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, $-17 \textbf{ mod } 2 = 1$. Note that we do not write $-17 = 2 \cdot (-8) - 1$, so $-17 \textbf{ mod } 2 \ne -1$.

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

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

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

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

20. 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 $a - c \equiv b - d \pmod{m}$.

22. 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 $ac \equiv bc \pmod{mc}$.

24. 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 $n^2 \equiv 1 \pmod{8}$.

26. 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

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

30. 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

32. 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

34. We know that $1 \cdot 0 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 2 + 6 \cdot 3 + 7 \cdot Q + 8 \cdot 0 + 9 \cdot 7 + 10 \cdot 2 \equiv 0 \pmod{11}$. This simplifies to $127 + 7Q \equiv 0 \pmod{11}$. We subtract 127 from both sides and simplify to $7Q \equiv 5 \pmod{11}$, since $-127 = -12 \cdot 11 + 5$. It is now a simple matter to use trial and error (or the methods to be introduced in Section 3.7) to find that $Q = 7$ (since $49 \equiv 5 \pmod{11}$).