SECTION 3.4 The Integers and Division

Number theory is playing an increasingly important role in computer science. This section and these exercises just scratch the surface of what is relevant. Many of these exercises are simply a matter of applying definitions. It is sometimes hard for a beginning student to remember that in order to prove something about a concept (such as modular arithmetic), it is usually necessary to invoke the definition! Exercises 20–25 hint at the rich structure that modular arithmetic has (sometimes resembling real number arithmetic more than integer arithmetic). In many contexts in mathematics and computer science, modular arithmetic is more relevant and convenient than ordinary integer arithmetic.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

c) $-29 = 17 \cdot (-2) + 5$, so $80 \equiv 5 \pmod{17}$ **d)** $-122 = 17 \cdot (-8) + 14$, so $80 \not\equiv 5 \pmod{17}$

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

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

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

25. There are at least two ways to prove this. One way is to invoke Theorem 5 repeatedly. Since $a \equiv b \pmod{m}$, Theorem 5 implies that $a \cdot a \equiv b \cdot b \pmod{m}$, i.e., $a^2 \equiv b^2 \pmod{m}$. Invoking Theorem 5 again, since $a \equiv b \pmod{m}$ and $a^2 \equiv b^2 \pmod{m}$, we obtain $a^3 \equiv b^3 \pmod{m}$. After $k - 1$ applications of this process, we obtain $a^k \equiv b^k \pmod{m}$, as desired. (This is really a proof by mathematical induction, a topic to be considered formally in Chapter 4.)

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

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

(i) $317 \bmod 31 = 7$ (ii) $918 \bmod 31 = 19$ (iii) $007 \bmod 31 = 7$

(iv) $100 \bmod 31 = 7$ (v) $111 \bmod 31 = 18$ (vi) $310 \bmod 31 = 0$

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

29. We compute until the sequence begins to repeat:

$$x_1 = 3 \cdot 2 \bmod 11 = 6$$
$$x_2 = 3 \cdot 6 \bmod 11 = 7$$
$$x_3 = 3 \cdot 7 \bmod 11 = 10$$
$$x_4 = 3 \cdot 10 \bmod 11 = 8$$
$$x_5 = 3 \cdot 8 \bmod 11 = 2$$

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

31. **a)** The message in numbers is 3–14 13–14–19 15–0–18–18 6–14. Adding 3 to each number (no sum is greater than 25, so there is no need to reduce modulo 26), we obtain the numerical message 6–17 16–17–22 18–3–21–21 9–17. Then translating this back into letters (A = 0, ..., Z = 25), we obtain "GR QRW SDVV JR." Note that this really is easier to do without translating to numbers first—just recite the next three letters in the alphabet after the given letter (e.g., "D goes to E-F-G").

b) We follow the same procedure, except that we add 13 rather than 3, and we need to subtract 26 from some of the sums to reduce modulo 26. The encoded numerical message is 16–1 0–1–6 2–13–5–5 19–1, so the literal encoded message is "QB ABG CNFF TB."

c) This time we need to multiply by 3, add 7, and reduce modulo 26 to obtain the encoded numerical message: 16–23 20–23–12 0–7–9–9 25–23, which gives us "QX UXM AHJJ ZX."

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

35. The 10-digit ISBN number of this book is 0-07-288008-2. Therefore $1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 2 + 5 \cdot 8 + 6 \cdot 8 + 7 \cdot 0 + 8 \cdot 0 + 9 \cdot 8 + 10 \cdot 2$ should be congruent to 0 (mod 11). The sum is $209 = 11 \cdot 19$, so it checks.