

Solution **Section 2.3 – Divisibility and Modular Arithmetic**

Exercise

Does 17 divide each of these numbers?

a) 68 b) 84 c) 35 d) 1001

Solution

a) $68 = 17 \cdot 4$ *Yes*

b) $84 = 17 \cdot 4 + 16$ *No*, remainder 16

c) $357 = 17 \cdot 21$ *Yes*

d) $1001 = 17 \cdot 58 + 15$ *No*, remainder 15

Exercise

Prove that if a is an integer other than 0, then

a) 1 divides a b) a divides 0

Solution

a) $1|a$ since $a = 1 \cdot a$

b) $a|0$ since $0 = a \cdot 0$

Exercise

Show that if $a|b$ and $b|a$, where a and b are integers, then $a = b$ or $a = -b$.

Solution

Let s and t be integers such that $a = bs$ and $b = at$.

$a = bs = ats$. Since $a \neq 0$, we conclude that $st = 1$.

The only way for this to happen, since s and t are integers, is for $s = t = 1$ or $s = t = -1$.

Therefore, either $a = b$ or $a = -b$.

Exercise

Show that if a , b , and c are integers, where $a \neq 0$ and $c \neq 0$, such that $ac|bc$, then $a|b$

Solution

Since $ac|bc \Rightarrow bc = (ac)t$ for some integers t

Since $c \neq 0$, divide both sides by c to obtain $b = at$ and this result to $a|b$ ✓

Exercise

What are the quotient and remainder when

- 19 is divided by 7?
- 111 is divided by 11?
- 789 is divided by 23?
- 1001 is divided by 13?
- 0 is divided by 19?
- 3 is divided by 5?
- 1 is divided by 3?
- 4 is divided by 1?

Solution

- a)** $19 = 7 \cdot 2 + 5$ $q = 2$ and $r = 5$
b) $-111 = 11 \cdot (-11) + 10$ $q = -11$ and $r = 10$
c) $789 = 23 \cdot 34 + 7$ $q = 34$ and $r = 7$
d) $1001 = 13 \cdot 77 + 0$ $q = 77$ and $r = 0$
e) $0 = 19 \cdot 0 + 0$ $q = 0$ and $r = 0$
f) $3 = 5 \cdot 0 + 3$ $q = 0$ and $r = 3$
g) $-1 = 3 \cdot (-1) + 2$ $q = -1$ and $r = 2$
h) $4 = 1 \cdot 4 + 0$ $q = 4$ and $r = 0$

Exercise

What time does a 12-hour clock read

- 80 hours after it reads 11:00?
- 40 hours before it reads 12:00?
- 100 hours after it reads 6:00?

Solution

- a)** $11 - 80 \bmod 12 = 11 - 8 = 7$, the clock reads 7:00.
- b)** $12 - 40 \bmod 12 = -28 \bmod 12$ ($12 - 40 = -28$)
 $= -28 + 36 \bmod 12$
 $= 8$

The clock reads 8:00.

- c) $6 + 100 \bmod 12 = 6 + 4 = 10$, the clock reads 10:00.

Exercise

What time does a 24-hour clock read

- a) 100 hours after it reads 2:00?
- b) 45 hours before it reads 12:00?
- c) 168 hours after it reads 19:00?

Solution

- a) $2 + 100 \bmod 24 = 2 + 4 = 6$, the clock reads 6:00
- b) $12 - 45 \bmod 24 = -33 \bmod 24 = -33 + 48 \bmod 24 = 15$, the clock reads 15:00
- c) $168 \bmod 24 = 0$, the clock reads 19:00

Exercise

Suppose a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ such that

- a) $c \equiv 9a \pmod{13}$
- b) $c \equiv 11b \pmod{13}$
- c) $c \equiv a + b \pmod{13}$
- d) $c \equiv 2a + 3b \pmod{13}$
- e) $c \equiv a^2 + b^2 \pmod{13}$
- f) $c \equiv a^3 - b^3 \pmod{13}$

Solution

- a) $c = 9 \cdot 4 \bmod 13 = 36 \bmod 13 = 10$
- b) $c = 11 \cdot 9 \bmod 13 = 99 \bmod 13 = 8$
- c) $c = 4 + 9 \bmod 13 = 13 \bmod 13 = 0$
- d) $c = 2(4) + 3(9) \bmod 13 = 35 \bmod 13 = 9$
- e) $c = 4^2 + 9^2 \bmod 13 = 97 \bmod 13 = 6$
- f) $c = 4^3 - 9^3 \bmod 13 = -665 \bmod 13 = 11$ ($-665 = -52 \times 13 + 11$)

Exercise

Suppose a and b are integers, $a \equiv 11 \pmod{19}$, and $b \equiv 3 \pmod{19}$. Find the integer c with $0 \leq c \leq 10$ such that

- a) $c \equiv a - b \pmod{19}$
- b) $c \equiv 7a + 3b \pmod{19}$
- c) $c \equiv 2a^2 + 3b^2 \pmod{19}$
- d) $c \equiv a^3 + 4b^3 \pmod{19}$

Solution

- a) $c = 11 - 3 \pmod{19} = \underline{8}$
- b) $c = 7(11) + 3(3) \pmod{19} = 86 \pmod{19} = \underline{10}$ $7(11) + 3(3) = 86 \equiv 10 \pmod{19}$
- c) $2(11)^2 + 3(3)^2 = 263 \equiv \underline{3} \pmod{19}$
- d) $(11)^3 + (3)^3 = 1439 \equiv \underline{14} \pmod{19}$

Exercise

Let m be a positive integer. Show that $a \pmod{m} = b \pmod{m}$ if $a \equiv b \pmod{m}$

Solution

Given $a \pmod{m} = b \pmod{m}$ means that a and b have the same remainder $a = q_1 m + r$ and

$b = q_2 m + r$ for some integer q_1, q_2 and r .

$$\begin{aligned} a - b &= q_1 m + r - q_2 m - r \\ &= (q_1 - q_2)m \end{aligned}$$

Which says that m divides (is a factor). This precisely the definition of $a \equiv b \pmod{m}$

Exercise

Let m be a positive integer. Show that $a \equiv b \pmod{m}$ if $a \pmod{m} = b \pmod{m}$

Solution

Assume that $a \equiv b \pmod{m}$. This means that $m \mid a - b$, $a - b = mc \Rightarrow a = b + mc$.

Computing $a \pmod{m}$, we know that $b = qm + r$ for some nonnegative r less than m (namely, $r \equiv b \pmod{m}$). Therefore $a = qm + r + mc = (q + c)m + r$. By definition this means that r must also equal $a \pmod{m}$ ✓

Exercise

Show that if n and k are positive integers, then $\lceil n/k \rceil = \left\lfloor \frac{n-1}{k} \right\rfloor + 1$

Solution

The quotient $\frac{n}{k}$ lies between 2 consecutive integers, let say $b-1$ and b possibly equal to b . There exists a positive integer b such that $b-1 < \frac{n}{k} \leq b$. In particular $\frac{n}{k} = b$. Also since $\frac{n}{k} > b-1$ we have $n > k(b-1) \Rightarrow n-1 \geq k(b-1)$
 $\left\lfloor \frac{n-1}{k} \right\rfloor \leq \frac{n-1}{k} < \frac{n}{k} \leq b$ so $\left\lfloor \frac{n-1}{k} \right\rfloor < b$, therefore $\left\lfloor \frac{n-1}{k} \right\rfloor = b-1$

Exercise

Evaluate these quantities

- a) $-17 \bmod 2$
- b) $144 \bmod 7$
- c) $-101 \bmod 13$
- d) $199 \bmod 19$
- e) $13 \bmod 3$
- f) $-97 \bmod 11$

Solution

- a) $-17 = 2 \cdot (-9) + 1$, the remainder is 1. That is, $-17 \bmod 2 = 1$.
Note that we do not write $-17 = 2 \cdot (-8) - 1$ so $-17 \bmod 2 = -1$
- b) $144 = 7 \cdot 20 + 4$, the remainder is 4. That is, $144 \bmod 7 = 4$
- c) $-101 = 13 \cdot (-8) + 3$, the remainder is 3. That is, $-101 \bmod 13 = 3$
- d) $199 = 19 \cdot 10 + 9$, the remainder is 9. That is, $199 \bmod 19 = 9$
- e) $13 = 3 \cdot 4 + 1$, the remainder is 1. That is, $13 \bmod 3 = 1$
- f) $-97 = 11 \cdot (-9) + 2$, the remainder is 2. That is, $-97 \bmod 11 = 2$

Exercise

Find $a \text{ div } m$ and $a \bmod m$ when

- a) $a = 228, m = 119$
- b) $a = 9009, m = 223$
- c) $a = -10101, m = 333$
- d) $a = -765432, m = 38271$

Solution

a) $228 = 2 \cdot 119 + 109$

$228 \text{ div } 119 = 1 \text{ and } 228 \text{ mod } 119 = 109$.

b) $9009 = 40 \cdot 223 + 89$

$9009 \text{ div } 223 = 40 \text{ and } 9009 \text{ mod } 223 = 89$.

c) $-10101 = -31 \cdot 333 + 222$

$-10101 \text{ div } 333 = -31 \text{ and } -10101 \text{ mod } 333 = 222$.

d) $-765432 = -21 \cdot 38271 + 38259 \Rightarrow$

$-765432 \text{ div } 38271 = -11 \text{ and } -765432 \text{ mod } 38271 = 38259$.

Exercise

Find the integer a such that

a) $a \equiv -15 \pmod{27}$ and $-26 \leq a \leq 0$

b) $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$

c) $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$

d) $a \equiv 43 \pmod{23}$ and $-22 \leq a \leq 0$

e) $a \equiv 17 \pmod{29}$ and $-14 \leq a \leq 14$

Solution

a) -15 already satisfies the inequality, the answer $a = -15$

b) 24 is too large to satisfy the inequality, we subtract 31 and obtain $a = -7$

c) 24 is too small to satisfy the inequality, we add 41 and obtain $a = 140$

d) $a = 43 - 2 \cdot (23) = 43 - 46 = -3$

e) $a = 17 - 29 = -12$

Exercise

Decide whether each of these integers is congruent to 5 modulo 17 .

a) 37 b) 66 c) -17 d) -67

Solution

a) $37 - 3 \text{ mod } 7 = 34 \text{ mod } 7 = 6 \neq 0$, so $37 \not\equiv 3 \pmod{7}$

b) $66 - 3 \text{ mod } 7 = 63 \text{ mod } 7 = 0$, so $66 \equiv 3 \pmod{7}$

c) $-17 - 3 \text{ mod } 7 = -20 \text{ mod } 7 = 1 \neq 0$, so $-17 \not\equiv 3 \pmod{7}$

d) $-67 - 3 \text{ mod } 7 = -70 \text{ mod } 7 = 0$, so $-67 \equiv 3 \pmod{7}$

Exercise

Find each of these values.

a) $(-133 \bmod 23 + 261 \bmod 23) \bmod 23$

b) $(457 \bmod 23 \cdot 182 \bmod 23) \bmod 23$

c) $(177 \bmod 31 + 270 \bmod 31) \bmod 31$

d) $(19^2 \bmod 41) \bmod 9$

e) $(32^3 \bmod 13)^2 \bmod 11$

f) $(99^2 \bmod 32)^3 \bmod 15$

g) $(3^4 \bmod 17)^2 \bmod 11$

h) $(19^3 \bmod 23)^2 \bmod 31$

i) $(89^3 \bmod 79)^4 \bmod 26$

Solution

a) $-133 + 261 = 128 \equiv 13$

$$-133 + 261 \bmod 23 = 128 \bmod 23 = \underline{13} \quad 128 = 23 \cdot (5) + 13$$

b) $457 \cdot 182 \bmod 23 = 83174 \bmod 23 = \underline{6} \quad 83174 = 23 \cdot (3616) + 6$

c) $177 + 271 \bmod 31 = 448 \bmod 31 = \underline{14} \quad 448 = 31 \cdot (14) + 14$

d) $(19^2 \bmod 41) \bmod 9 = (361 \bmod 41) \bmod 9$

$$= 33 \bmod 9$$

$$= \underline{6}$$

e) $(32^3 \bmod 13)^2 \bmod 11 = (32768 \bmod 13)^2 \bmod 11$

$$= 8^2 \bmod 11$$

$$= 64 \bmod 11$$

$$= \underline{9}$$

f) $(99^2 \bmod 32)^3 \bmod 15 = (9801 \bmod 32)^3 \bmod 15$

$$= 9^3 \bmod 15$$

$$= 729 \bmod 15$$

$$= \underline{9}$$

g) $(3^4 \bmod 17)^2 \bmod 11 = (81 \bmod 17)^2 \bmod 11$

$$= 13^2 \bmod 11$$

$$= 169 \bmod 11$$

$$= 4$$

$$h) \left(19^3 \bmod 23 \right)^2 \bmod 31 = (6859 \bmod 23)^2 \bmod 31$$

$$= 5^2 \bmod 31$$

$$= 25 \bmod 31$$

$$= 25$$

$$i) \left(89^3 \bmod 79 \right)^4 \bmod 26 = (704969 \bmod 79)^4 \bmod 26$$

$$= 52^4 \bmod 26$$

$$= 7311616 \bmod 26$$

$$= 0$$