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

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

Exercise

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

Solution

Let s and t are 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 $ac \mid bc$, then $a \mid b$

Solution

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

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

Exercise

What are the quotient and remainder when

a) 19 is divided by 7?
b) −111 is divided by 11?
c) 789 is divided by 23?
d) 1001 is divided by 13?
e) 0 is divided by 19?
f) 3 is divided by 5?
g) −1 is divided by 3?
h) 4 is divided by 1?

Solution

a) $19 = 7 \cdot 2 + 5$ $\quad q = 2 \quad and \quad r = 5$

b) $-111 = 11 \cdot (-11) + 10$ $\quad q = -11 \quad and \quad r = 10$

c) $789 = 23 \cdot 34 + 7$ $\quad q = 34 \quad and \quad r = 7$

d) $1001 = 13 \cdot 77 + 0$ $\quad q = 77 \quad and \quad r = 0$

e) $0 = 19 \cdot 0 + 0$ $\quad q = 0 \quad and \quad r = 0$

f) $3 = 5 \cdot 0 + 3$ $\quad q = 0 \quad and \quad r = 3$

g) $-1 = 3 \cdot (-1) + 2$ $\quad q = -1 \quad and \quad r = 2$

h) $4 = 1 \cdot 4 + 0$ $\quad q = 4 \quad and \quad r = 0$

Exercise

What time does a 12-hour clock read

a) 80 hours after it reads 11:00?
b) 40 hours before it reads 12:00?
c) 100 hours after it reads 6:00?

Solution

a) $11 - 80 \ \boldsymbol{mod} \ 12 = 11 - 8 = 7$, the clock reads 7:00.

b) $12 - 40 \ \boldsymbol{mod} \ 12 = -28 \ \boldsymbol{mod} \ 12$ $\qquad (12 - 40 = -28)$

$$= -28 + 36 \ \boldsymbol{mod} \ 12$$
$$= 8$$

The clock reads 8:00.

c) $6 + 100 \ \boldsymbol{mod} \ 12 = 6 + 4 = 10$, 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) $2+100\ \boldsymbol{mod}\ 24 = 2+4 = 6$, the clock reads 6:00

b) $12-45\ \boldsymbol{mod}\ 24 = -33\ \boldsymbol{mod}\ 24 = -33+48\ \boldsymbol{mod}\ 24 = 15$, the clock reads 15:00

c) $168\ \boldsymbol{mod}\ 24 = 0$, 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 $0 \le c \le 12$ 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) $c = 9\cdot 4\ \boldsymbol{mod}\ 13 = 36\ \boldsymbol{mod}\ 13 = 10$

b) $c = 11\cdot 9\ \boldsymbol{mod}\ 13 = 99\ \boldsymbol{mod}\ 13 = 8$

c) $c = 4+9\ \boldsymbol{mod}\ 13 = 13\ \boldsymbol{mod}\ 13 = 0$

d) $c = 2(4)+3(9)\ \boldsymbol{mod}\ 13 = 35\ \boldsymbol{mod}\ 13 = 9$

e) $c = 4^2+9^2\ \boldsymbol{mod}\ 13 = 97\ \boldsymbol{mod}\ 13 = 6$

f) $c = 4^3-9^3\ \boldsymbol{mod}\ 13 = -665\ \boldsymbol{mod}\ 13 = 11$ $(-665 = -52\times 13 + 11)$

Exercise

Suppose a and b are integers, $a \equiv 11 \left(\boldsymbol{mod}\ 19\right)$, and $b \equiv 3 \left(\boldsymbol{mod}\ 19\right)$. Find the integer c with $0 \le c \le 10$ such that

a) $c \equiv a - b \left(\boldsymbol{mod}\ 19\right)$

b) $c \equiv 7a + 3b \left(\boldsymbol{mod}\ 19\right)$

c) $c \equiv 2a^2 + 3b^2 \left(\boldsymbol{mod}\ 19\right)$

d) $c \equiv a^3 + 4b^3 \left(\boldsymbol{mod}\ 19\right)$

Solution

a) $c = 11 - 3\ \boldsymbol{mod}\ 19 = \underline{8}$

b) $c = 7(11) + 3(3)\ \boldsymbol{mod}\ 19 = 86\ \boldsymbol{mod}\ 19 = \underline{10}$ $\qquad 7(11) + 3(3) = 86 \equiv 10 \left(\boldsymbol{mod}\ 19\right)$

c) $2(11)^2 + 3(3)^2 = 263 \equiv 3 \left(\boldsymbol{mod}\ 19\right)$

d) $(11)^3 + (3)^3 = 1439 \equiv 14 \left(\boldsymbol{mod}\ 19\right)$

Exercise

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

Solution

Given $a\ \boldsymbol{mod}\ m \equiv b\ \boldsymbol{mod}\ m$ 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.

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

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

Exercise

Let m be a positive integer. Show that $a \equiv b\left(\text{mod } m\right)$ if a **mod** $m = b$ **mod** m

Solution

Assume that $a \equiv b \left(\boldsymbol{mod}\ m\right)$. This means that $m | a - b$, $a - b = mc \Rightarrow a = b + mc$.

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

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 $b-1 < \frac{n}{k} \le b$. In particular $\frac{n}{k} = b$. Also since $\frac{n}{k} > b-1$ we have $n > k(b-1) \Rightarrow n-1 \ge k(b-1)$

$\left\lfloor \frac{n-1}{k} \right\rfloor \le \frac{n-1}{k} < \frac{n}{k} \le b$ 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 ***mod*** 2
b) 144 ***mod*** 7
c) -101 ***mod*** 13
d) 199 ***mod*** 19
e) 13 ***mod*** 3
f) -97 ***mod*** 11

Solution

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

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

c) $-101 = 13\cdot(-8)+3$, the remainder is 3. That is, -101 ***mod*** $13 = 3$

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

e) $13 = 3\cdot 4 + 1$, the remainder is 1. That is, 13 ***mod*** $3 = 1$

f) $-97 = 11\cdot(-9)+2$, the remainder is 2. That is, -97 ***mod*** $11 = 2$

Exercise

Find a **div** m and a **mod** m when

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

Solution

a) $228 = 2 \cdot 119 + 109 \Rightarrow 228 \; \textbf{div} \; 119 = 1 \quad \textit{and} \quad 228 \; \textbf{mod} \; 119 = 109$.

b) $9009 = 40 \cdot 223 + 89 \Rightarrow 9009 \; \textbf{div} \; 223 = 40 \quad \textit{and} \quad 9009 \; \textbf{mod} \; 223 = 89$.

c) $-10101 = -31 \cdot 333 + 222 \Rightarrow -10101 \; \textbf{div} \; 333 = -31 \quad \textit{and} \quad -10101 \; \textbf{mod} \; 333 = 222$.

d) $-765432 = -21 \cdot 38271 + 38259 \Rightarrow$
$-765432 \; \textbf{div} \; 38271 = -11 \quad \textit{and} \quad -765432 \; \textbf{mod} \; 38271 = 38259$.

Exercise

Find the integer a such that

a) $a \equiv -15 (\textbf{mod} \; 27) \;\; \textit{and} \;\; -26 \le a \le 0$

b) $a \equiv 24 (\textbf{mod} \; 31) \;\; \textit{and} \;\; -15 \le a \le 15$

c) $a \equiv 99 (\textbf{mod} \; 41) \;\; \textit{and} \;\; 100 \le a \le 140$

d) $a \equiv 43 (\textbf{mod} \; 23) \;\; \textit{and} \;\; -22 \le a \le 0$

e) $a \equiv 17 (\textbf{mod} \; 29) \;\; \textit{and} \;\; -14 \le a \le 14$

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.

$a)\; 37 \qquad b)\; 66 \qquad c)\; -17 \qquad d)\; -67$

Solution

a) $37 - 3 \; \textbf{mod} \; 7 = 34 \; \textbf{mod} \; 7 = 6 \ne 0$, so $37 \not\equiv 3 \left(\textbf{mod} \; 7\right)$

b) $66 - 3 \; \textbf{mod} \; 7 = 63 \; \textbf{mod} \; 7 = 0$, so $37 \equiv 3 \left(\textbf{mod} \; 7\right)$

c) $-17 - 3 \; \textbf{mod} \; 7 = -20 \; \textbf{mod} \; 7 = 1 \ne 0$, so $-17 \not\equiv 3 \left(\textbf{mod} \; 7\right)$

d) $-67 - 3 \; \textbf{mod} \; 7 = -70 \; \textbf{mod} \; 7 = 0$, so $-67 \equiv 3 \left(\textbf{mod} \; 7\right)$

Exercise

Find each of these values.

a) $(-133 \textbf{ mod } 23 + 261 \textbf{ mod } 23) \textbf{ mod } 23$

b) $(457 \textbf{ mod } 23 \cdot 182 \textbf{ mod } 23) \textbf{ mod } 23$

c) $(177 \textbf{ mod } 31 + 270 \textbf{ mod } 31) \textbf{ mod } 31$

d) $\left(19^2 \textbf{\textit{ mod }} 41\right) \textbf{\textit{ mod }} 9$

e) $\left(32^3 \textbf{\textit{ mod }} 13\right)^2 \textbf{\textit{ mod }} 11$

f) $\left(99^2 \textbf{\textit{ mod }} 32\right)^3 \textbf{\textit{ mod }} 15$

g) $\left(3^4 \textbf{\textit{ mod }} 17\right)^2 \textbf{\textit{ mod }} 11$

h) $\left(19^3 \textbf{\textit{ mod }} 23\right)^2 \textbf{\textit{ mod }} 31$

i) $\left(89^3 \textbf{\textit{ mod }} 79\right)^4 \textbf{\textit{ mod }} 26$

Solution

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

$-133 + 261 \textbf{\textit{ mod }} 23 = 128 \textbf{\textit{ mod }} 23 \underline{= 13}$ $\qquad 128 = 23 \cdot (5) + 13$

b) $457 \cdot 182 \textbf{\textit{ mod }} 23 = 83174 \textbf{\textit{ mod }} 23 \underline{= 6}$ $\qquad 83174 = 23 \cdot (3616) + 6$

c) $177 + 271 \textbf{\textit{ mod }} 31 = 448 \textbf{\textit{ mod }} 31 \underline{= 14}$ $\qquad 448 = 31 \cdot (14) + 14$

d) $\left(19^2 \textbf{\textit{ mod }} 41\right) \textbf{\textit{ mod }} 9 = (361 \textbf{\textit{ mod }} 41) \textbf{\textit{ mod }} 9 = 33 \textbf{\textit{ mod }} 9 \underline{= 6}$

e) $\left(32^3 \textbf{\textit{ mod }} 13\right)^2 \textbf{\textit{ mod }} 11 = (32768 \textbf{\textit{ mod }} 13)^2 \textbf{\textit{ mod }} 11 = 8^2 \textbf{\textit{ mod }} 11 = 64 \textbf{\textit{ mod }} 11 \underline{= 9}$

f) $\left(99^2 \textbf{\textit{ mod }} 32\right)^3 \textbf{\textit{ mod }} 15 = (9801 \textbf{\textit{ mod }} 32)^3 \textbf{\textit{ mod }} 15 = 9^3 \textbf{\textit{ mod }} 15 = 729 \textbf{\textit{ mod }} 15 \underline{= 9}$

g) $\left(3^4 \textbf{\textit{ mod }} 17\right)^2 \textbf{\textit{ mod }} 11 = (81 \textbf{\textit{ mod }} 17)^2 \textbf{\textit{ mod }} 11 = 13^2 \textbf{\textit{ mod }} 11 = 169 \textbf{\textit{ mod }} 11 \underline{= 4}$

h) $\left(19^3 \textbf{\textit{ mod }} 23\right)^2 \textbf{\textit{ mod }} 31 = (6859 \textbf{\textit{ mod }} 23)^2 \textbf{\textit{ mod }} 31 = 5^2 \textbf{\textit{ mod }} 31 = 25 \textbf{\textit{ mod }} 31 \underline{= 25}$

i) $\left(89^3 \textbf{\textit{ mod }} 79\right)^4 \textbf{\textit{ mod }} 26 = (704969 \textbf{\textit{ mod }} 79)^4 \textbf{\textit{ mod }} 26 = 52^4 \textbf{\textit{ mod }} 26 = 7311616 \textbf{\textit{ mod }} 26 \underline{= 0}$