# *Section* 2.3 – Divisibility and Modular Arithmetics

## *Division*

### *Definition*

If $a$ and $b$ are integers with $a \neq 0$, we say that $a$ divides $b$ if there is an integer $c$ such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integers. When $a$ divides $b$ we say that $a$ is a factor or divisor of $b$, and that $b$ is multiple of $a$. The notation $a \mid b$ denotes that $a$ divides $b$. We write $a \nmid b$ when $a$ does not divide $b$.

### *Example*

Determine whether $3 \mid 7$ and whether $3 \mid 12$.

***Solution***

We see that $3 \nmid 7$, because 7/3 is not integer.

$3 \mid 12$ because 12/3 = 4.

### *Example*

Let $n$ and $d$ be positive integers. How many positive integers not exceeding $n$ are divisible by $d$?

***Solution***

The positive integers divisible by $d$ are all the integers of the form $dk$, where $k$ is a positive integer. Hence, the number of positive integers divisible by $d$ that do not exceed $n$ equals the number of integers $k$ with $0 < k \leq n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding $n$ that are divisible by $d$.

### *Theroem*

Let $a$, $b$, and $c$ integers, where $a \neq 0$. Then

***i)*** If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

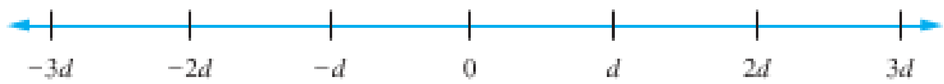
***ii)*** If $a \mid b$, then $a \mid bc$ for all integers $c$;

***iii)*** If $a \mid b$ and $b \mid c$, then $a \mid c$.

***Proof*** **(*i*)**

Suppose If $a \mid b$ and $a \mid c$. Then, from the definition of divisibility, it follows that there are integers $s$ and $t$ with $b = as$ and $c = at$. Hence,

$$b + c = as + at = a(s + t)$$




Therefore, $a$ divides $b + c$.

***Corollary***

If $a$, $b$, and $c$ integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever $m$ and $n$ are integers.

## The Division Algorithm

### *Theroem*

Let $a$ be an integer and $d$ a positive integer. Then there are unique integers $q$ and $r$, with $0 \leq r < d$, such that $a = dq + r$.

### *Definition*

In the equality given in the division algorithm, ***d*** is called the ***divisor***, ***a*** called the ***dividend***, ***q*** is called the ***quotient***, and ***r*** is called the ***remainder***. This notation is used to express the quotient and remainder:

$$q = a \textbf{ div } d, \qquad r = a \textbf{ mod } d$$

### *Example*

What are the quotient and remainder when 101 is divided by 11?

***Solution***

$101 = 11 \cdot 9 + 2$

Hence, the quotient when 101 is divided by 11 is 9 = 101 ***div*** 11,
and the remainder is 2 = 101 ***mod*** 11.

### *Example*

What are the quotient and remainder when –11 is divided by 3?

***Solution***

$-11 = 3(-4) + 1$

Hence, the quotient when –11 is divided by 3 is –4 = –11 ***div*** 3, and the remainder is 1 = –11 ***mod*** 3.

## Modular Arithmetic

### *Definition*

If *a* and *b* are integers and *m* is positive integer, then *a* is ***congruent*** to *b* ***modulo*** *m* if *m* divides *a* – *b*. We use the notation $a \equiv b \pmod{m}$ to indicate that *a* is *congruent* to *b modulo m*. We say that $a \equiv b \pmod{m}$ is a ***congruence*** and that m is its ***modulus*** (plural ***moduli***). If *a* and *b* are not congruent modulo *m*, we write $a \not\equiv b \pmod{m}$

### *Theorem*

Let *a* and *b* be integers, and let *m* be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \textbf{ mod } m = b \textbf{ mod } m$

### *Example*

Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

***Solution***

Because 6 divides 17 – 5 = 12, we see that $17 \equiv 5 \pmod{6}$.

24 – 14 = 10 is not divisible by 6, we see that $24 \not\equiv 14 \pmod{6}$

### *Theorem*

Let *m* be a positive integer. The integers *a* and *b* are congruent modulo *m* if and only if there is an integer *k* such that $a = b + km$.

### *Proof*

If $a \equiv b \pmod{m}$ that implies by the definition of congruence to $m \mid (a-b)$. Which is that there is an integer *k* such that $a - b = km \quad \Rightarrow \quad a = b + km$.

Conversely, if there is an integer $k$ such that $a = b + km$, then $km = a - b$. Hence, $m$ divides $a - b$, so that $a \equiv b \pmod{m}$

### *Theorem*

Let $m$ be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \qquad \textit{and} \qquad ac \equiv bd \pmod{m}$$

### *Proof*

Using direct proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by the theorem that are integers $s$ and $t$ with $b = a + sm \quad \textit{and} \quad d = c + tm$. Hence,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t) \qquad \Rightarrow \; a + c \equiv b + d \pmod{m}$$

And

$$bd = (a + sm)(c + tm) = ac + m(at + sc + stm) \qquad \Rightarrow \; ac \equiv bd \pmod{m}$$

### *Corollary*

Let $a$ and $b$ be integers, and let $m$ be a positive integer. Then

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

and

$$ab \textbf{ mod } m \; = \; ((a \textbf{ mod } m)(b \textbf{ mod } m)) \textbf{ mod } m$$

## *Arithmetic Modulo m*

We define addition by: $a +_m b = (a + b) \textbf{ mod } m$ and multiplication by $a \cdot_m b = (a \cdot b) \textbf{ mod } m$

# *Exercises* *Section* 2.3 – Divisibility and Modular Arithmetics

**1.** Does 17 divide each of these numbers?

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

**2.** Prove that if $a$ is an integer other than 0, then

***a***) $1$ *divides* $a$ ***b***) $a$ *divides* $0$

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

**4.** Show that if $a$, $b$, and $c$ are integers, where $a \neq 0$ and $c \neq 0$, such that $ac \mid bc$, then $a \mid b$

**5.** 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?

**6.** 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?

**7.** 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?

**8.** 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)* $c \equiv a^3 - b^3 \pmod{13}$

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

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

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

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

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

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

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

**12.** 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

**13.** 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

**14.** Find the integer $a$ such that

*a)* $a \equiv -15 (\boldsymbol{mod}\ 27)$ *and* $-26 \le a \le 0$

*b)* $a \equiv 24 (\boldsymbol{mod}\ 31)$ *and* $-15 \le a \le 15$

*c)* $a \equiv 99 (\boldsymbol{mod}\ 41)$ *and* $100 \le a \le 140$

*d)* $a \equiv 43 (\boldsymbol{mod}\ 23)$ *and* $-22 \le a \le 0$

*e)* $a \equiv 17 (\boldsymbol{mod}\ 29)$ *and* $-14 \le a \le 14$

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

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

**16.** Find each of these values.

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

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

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

*d)* $\left(19^2 \boldsymbol{mod}\ 41\right) \boldsymbol{mod}\ 9$

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

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

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

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

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