

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 integer. 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 $3 \nmid 7$ 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 .

Theorem

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:

$$q = a \text{ div } d, \quad r = a \text{ mod } d$$

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 $9 = 101 \text{ div } 11$, and the remainder is $2 = 101 \text{ mod } 11$.

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 $-4 = -11 \text{ div } 3$,
and the remainder is $1 = -11 \text{ mod } 3$.

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
 $a \bmod m = b \bmod m$

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 $a - b = km \Rightarrow a = b + km$.

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

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}$$

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 $b = a + sm$ and $d = c + tm$. Hence,

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

And

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

Corollary

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

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

and

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Arithmetic Modulo m

We define addition by: $a +_m b = (a + b) \bmod m$ and multiplication by $a \cdot_m b = (a \cdot b) \bmod m$

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, $a \equiv 11 \pmod{19}$, and $b \equiv 3 \pmod{19}$. Find the integer c with $0 \leq c \leq 10$ such that
- $c \equiv a - b \pmod{19}$
 - $c \equiv 7a + 3b \pmod{19}$
 - $c \equiv 2a^2 + 3b^2 \pmod{19}$
 - $c \equiv a^3 + 4b^3 \pmod{19}$
10. Let m be a positive integer. Show that $a \equiv b \pmod{m}$ if $a \bmod m = b \bmod m$
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
- $-17 \bmod 2$
 - $144 \bmod 7$
 - $-101 \bmod 13$
 - $199 \bmod 19$
 - $13 \bmod 3$
 - $-97 \bmod 11$
13. Find $a \div m$ and $a \bmod m$ when
- $a = 228, m = 119$
 - $a = 9009, m = 223$
 - $a = -10101, m = 333$
 - $a = -765432, m = 38271$
14. Find the integer a such that
- $a \equiv -15 \pmod{27}$ and $-26 \leq a \leq 0$
 - $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$
 - $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$
 - $a \equiv 43 \pmod{23}$ and $-22 \leq a \leq 0$
 - $a \equiv 17 \pmod{29}$ and $-14 \leq a \leq 14$
15. Decide whether each of these integers is congruent to 5 modulo 17.
- 37
 - 66
 - 17
 - 67
16. Find each of these values.
- $(-133 \bmod 23 + 261 \bmod 23) \bmod 23$

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

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

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

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

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

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

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

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