Number Theory

Chapter 4

Edited by: Dr. Meshal Alfarhood

Divisibility and Modular Arithmetic

Section 4.1

Section Summary

Division

Division Algorithm

Modular Arithmetic

Division

Definition: If a and b are integers with $a \neq 0$, then a *divides* b if there exists an integer c such that $b = ac$.

- The notation $a \mid b$ denotes that a divides b.
- If a does not divide b, we write $a \nmid b$.
- If $a \mid b$, then $\frac{b}{a}$ is an integer.

Examples: $3 \nmid 7$ and $3 \mid 12$.

Properties of Divisibility

Theorem: Let a, b, and c be integers, where $a \neq 0$.

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 of (i):

- **Direct proof:** Suppose $a \mid b$ and $a \mid c$. Then, there are integers s and t with $b=as$ and $c=at$.
- Hence, $b+c = as+at = a(s+t)$. Therefore, $a \mid (b+c)$

Division Algorithm

Division Algorithm: If *a* is an integer and *d* a positive integer, then there are unique integers *q* and *r*, with $\mathbf{0 \le r < d}$, such that $a = dq + r$.

- *a* is called the *dividend*.
- *d* is called the *divisor*.
- *q* is called the *quotient*.
- *r* is called the *remainder*.

$q = a$ **div** $d = \lfloor a/d \rfloor$

$r = a$ **mod** $d = a - d\lfloor a/d \rfloor$

Examples:

1. What are the quotient and remainder when 101 is divided by 11?
   - The quotient = 101 div 11 = $\lfloor 101/11 \rfloor = 9.$
   - The remainder = 101 mod 11 = $\mathbf{101 - 11\lfloor 101/11 \rfloor = 101 - 99 =}$ $2.$
   - $101 = 9 \cdot 11 + 2.$
2. What are the quotient and remainder when −11 is divided by 3?
   - The quotient = -11 div 3 = $\lfloor -11/3 \rfloor = -4.$
   - The remainder = -11 mod 3 = $\mathbf{-11 - 3\lfloor -11/3 \rfloor = -11 - (-12) =}$ $1.$
   - $-11 = (-4) \cdot 3 + 1.$

Modular Arithmetic

Definition: If a and b are integers and m is a positive integer, then a is *congruent* to b *modulo* m if m divides $a - b$.

- The notation $a \equiv b \pmod{m}$ says that <u>a is congruent to b modulo m</u>.
- If a is not congruent to b modulo m, we write $a \not\equiv b \pmod{m}$
- Two integers are congruent mod m **if and only if they have the same remainder when divided by m.** (a **mod** $m = b$ **mod** m).

Example: Determine whether 17 is congruent to 5 modulo 6? and whether 24 and 14 are congruent modulo 6?

Solution:

- **$17 \equiv 5 \pmod{6}$** → because 6 divides $17 - 5 = 12$.
- **$24 \not\equiv 14 \pmod{6}$** → because 6 does not divide $24 - 14 = 10$.

More on Congruence Relation

Theorem: Let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.

Proof:

- If $a \equiv b \pmod{m}$, then $m \mid a - b$. (by the definition of congruence) Hence, there is an integer k such that $a-b = km \rightarrow a = b+km$. (by the definition of division)
- Also, if there is an integer k such that $a=b+km$, then $a-b=km$. Hence, $m \mid a-b$ and $a \equiv b \pmod{m}$.

Congruence of Sums and Products

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

Proof:

- $a \equiv b \pmod{m} \rightarrow a = b + k_1 m$
- $c \equiv d \pmod{m} \rightarrow c = d + k_2 m$.
- Therefore,
  - $a + c = (b + k_1 m) + (d + k_2 m)$

    $a + c = (b + d) + m(k_1 + k_2)$

    $(a + c) - (b + d) = m(k_1 + k_2) \rightarrow m \mid ((a + c) - (b + d)) \rightarrow a+c \equiv b+d \pmod{m}$

Example: Because **7 ≡ 2 (mod 5)** and **11 ≡ 1 (mod 5)**, it follows from the previous Theorem that:

$18 \equiv 3 \pmod{5}$

$77 \equiv 2 \pmod{5}$

Algebraic Manipulation of Congruences

- **Multiplying** both sides of a valid congruence by an integer preserves validity. $a \cdot c \equiv b \cdot c \pmod{m}$
- **Adding** an integer to both sides of a valid congruence preserves validity. $a + c \equiv b + c \pmod{m}$
- **Dividing** a congruence by an integer does not always produce a valid congruence.
  - **Example**: The congruence **$14 \equiv 8 \pmod{6}$** holds. But dividing both sides by 2 does not produce a valid congruence since **$7 \not\equiv 4 \pmod{6}$**.

Exercise

Exercise 1: Find the remainder of the following:

1. **3 mod 7 =** 3 $[3 = 0 \cdot 7 + 3]$
2. **13 mod 7 =** 6 $[13 = 1 \cdot 7 + 6]$
3. **-3 mod 7 =** 4 $[-3 = (-1) \cdot 7 + 4]$
4. **-13 mod 7 =** 1 $[-13 = (-2) \cdot 7 + 1]$

Exercise 2: Is **112233 ≡ 123 (mod 10)?**

- Yes. Both numbers have the same remainder (=3) when divided by 10.

Exercise 3: Find the integer <u>a</u> such that **a ≡ 43 (mod 23)**, and $-22 \le$ **a** ≤ 0.

- $a - 43 = 23k$
- $a = 43+23k$ → This is the general solution of the value of **a**.
- Since the question asks for $[-22 \le a \le 0]$:
  - $a = 43 + 23(-2) =$ **-3**