Divisibility and Modular Arithmetic

Section 4.1

Section Summary [1]

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 $b = ac$.

- When a divides b we say that a is a *factor* or *divisor* of b and that b is a multiple of a.
- The notation $a \mid b$ denotes that a divides b.
- If $a \mid b$, then b/a is an integer.
- If a does not divide b, we write $a \nmid b$.

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

Properties of Divisibility

Theorem 1. 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: (i) Suppose $a \mid b$ and $a \mid c$, then it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$b + c = as + at = a(s + t)$. Hence, $a \mid (b + c)$

Corollary: If a, b, and c be 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.

It follows easily from (ii) and (i) of Theorem 1

Note. $mb + nc$ is called a linear combination of b and c.

Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder. This is traditionally called the “Division Algorithm,” but is really a theorem. We have proved it for natural numbers using induction.

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

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

Be careful when $a < 0$.
While $q < 0$, it must be that $r > 0$ or $r = 0$.

$-13 = 3(-4) + (-1)$ -13
$-13 = 3(-5) + 2$ so -13 divided by 3 is -5 with remainder 2.

Definitions of Functions **div** and **mod**

$q = a$ **div** d

$r = a$ **mod** d

Examples:

- What are the quotient and remainder when 101 is divided by 11?
- **Solution**: The quotient when 101 is divided by 11 is 9 = 101 **div** 11, and the remainder is 2 = 101 **mod** 11.
- What are the quotient and remainder when −11 is divided by 3?
- **Solution**: The quotient when −11 is divided by 3 is −4 = −11 **div** 3, and the remainder is 1 = −11 **mod** 3. This is because $-11 = 3(-4)+1$. While it is true that $-11 = 3(-3) - 2$, this second observation does not give the correct q and r.

Congruence Relation

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 a is congruent to b modulo m.
- We say that $a \equiv b \pmod{m}$ is a *congruence* and that m is its *modulus.*
- Two integers are congruent mod m if and only if they have the same remainder when divided by m.
- If a is not congruent to b modulo m, we write $a \not\equiv b \pmod{m}$

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 $17 - 5 = 12$.
- $24 \not\equiv 14 \pmod{6}$ since $24 - 14 = 10$ is not divisible by 6.

More on Congruences

Theorem 2. 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 $a \equiv b \pmod{m}$, then (by the definition of congruence) $m \mid (a - b)$. Hence, there is an integer k such that $a - b = km$ and equivalently $a = b + km$.
- Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, $m \mid (a - b)$ and $a \equiv b \pmod{m}$.

Note: In the text, m | a - b means m | (a - b).

The Relationship between (mod m) and **mod** m Notations

The use of "mod" in $a \equiv b \pmod{m}$ and a **mod** $m = b$ are different.

- $a \equiv b \pmod{m}$ is a relation on the set of integers.

  This means that m divides b - a or equivantly a = b+km for some integer k.

- In a **mod** $m = b$, the notation **mod** denotes a function.

  This means that the remainder is b when a is divided by m.

The relationship between these notations is made clear in this next theorem

Theorem 3. Suppose that each of a and b is an integer and m is a positive integer. Then $a \equiv b \pmod{m}$ if and only if a **mod** $m = b$ **mod** m.

Proof. $(\Rightarrow)$ If $a \equiv b \pmod{m}$ then $a - b = km$ for some integer k. Also $a = q_1 m + r_1$ and $b = q_2 m + r_2$ where each of q_1 and q_2 is an integer and each of r_1 and r_2 is a nonnegative integer less than m. Thus $a - b = (q_1 - q_2)m + r_1 - r_2$ where $-m < r_1 - r_2 < m$. Since $a - b$ is also km we have $km = (q_1 - q_2)m + r_1 - r_2$ so $(k - (q_1 - q_2))m = r_1 - r_2$. This shows that $r_1 - r_2$ is an integral multiple of m. Since $-m < r_1 - r_2 < m$ it must be that $r_1 - r_2 = 0$ so $r_1 = r_2$. Thus a **mod** $m = b$ **mod** m.

$(\Leftarrow)$ If a **mod** $m = b$ **mod** m then $a = q_1 m + r$ and $b = q_2 m + r$ where each of q_1 and q_2 is an integer and r is a nonnegative integer less than m. Thus $a - b = (q_1 - q_2)m$. So $a \equiv b \pmod{m}$.

Congruences of Sums and Products

Theorem 4: 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:

- Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, there is a pair of integers s and t with $b = a + sm$ and $d = c + tm$.
- Therefore,
  - $b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ and
  - $b\,d = (a + sm)\,(c + tm) = ac + m(at + cs + stm)$.
- Hence, $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

Example: Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows that

$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$ and

$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$

Algebraic Manipulation of Congruences

Multiplying both sides of a valid congruence by an integer preserves congruence.

If $a \equiv b \pmod{m}$ holds then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer.

Adding an integer to both sides of a valid congruence preserves validity.

If $a \equiv b \pmod{m}$ holds then $c + a \equiv (c + b) \pmod{m}$, where c is any integer.

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 $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod{6}$.

See Section 4.3 for conditions when division is ok.

Computing the **mod** *m* Function of Products and Sums

We use the following corollary to Theorem 4 to compute the remainder of the product or sum of two integers when divided by m from the remainders when each is divided by m.

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

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

and

$ab\ \mathbf{mod}\ m = ((a\ \mathbf{mod}\ m)\ (b\ \mathbf{mod}\ m))\ \mathbf{mod}\ m.$

Arithmetic Modulo m [1]

Definitions: Let $\mathbf{Z}_m$ be the set of nonnegative integers less than m: $\{0,1, \ldots., m-1\}$

- The operation $+_m$ is defined as $a +_m b = (a + b)$ **mod** m. This is *addition modulo m*.
- The operation $\cdot_m$ is defined as $a \cdot_m b = (a \cdot b)$ **mod** m. This is *multiplication modulo m*.
- Using these operations is said to be doing *arithmetic modulo m*.

Example: Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution: Using the definitions above:

- $7 +_{11} 9 = (7 + 9)$ **mod** $11 = 16$ **mod** $11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9)$ **mod** $11 = 63$ **mod** $11 = 8$

Arithmetic Modulo m 2

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication.

- *Closure*: If a and b belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.
- *Associativity*: If a, b, and c belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
- *Commutativity*: If a and b belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
- *Identity elements*: The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively.
  - If a belongs to $\mathbf{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Arithmetic Modulo m 3

- *Additive inverses*: If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse.
  - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$
- *Distributivity*: If a, b, and c belong to $\mathbf{Z}_m$, then
  - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Multiplicatative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6.