Ch 4.1 Divisibility and Modular Arithmetic

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 a *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 1 Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Solution:

$3 \nmid 7$, because $\dfrac{7}{3}$ is not an integer.

$3 \mid 12$, because $\dfrac{12}{3} = 4$.

THEOREM 1
Let a, b, and c be 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 $a \mid c$.

COLLARY 1
If a, b, and c are 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.

THEOREM 2 The Division Algorithm
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 $a = dq + r$.

In the equality given in the division algorithm, d is called the *divisor*, a is called the *dividend*, q is called the *quotient*, and r is called the *remainder*. This notation is used to express the equotient and remainder.
$q = a \textbf{ div } d, \quad r = a \textbf{ mod } d.$

If a and b are integers and m is a positive integer, then a is *congruent to b modulo m* if m divides $a - b$. 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 $a \not\equiv b \pmod{m}$.

Remark: Although both notations $a \equiv b \pmod{m}$ and $a \textbf{ mod } m = b$ include "mod", then represent fundamentally different concepts. The first represents a relation on the set of integers, whereas the second represents a function.

THEOREM 3
Let a and b be integers, let m be a positive integer. Then $a \equiv b \pmod{m}$ *iff* $a \textbf{ mod } m = b \textbf{ mod } m$.

THEOREM 4
Let m be a positive integer. Then integers a and b are congruent modulo m *iff* there is an integer k such that $a = b + km$.

THEOREM 5

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

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

You cannot always divide both sides of a congruence by the same number.

If $ac \equiv bc \pmod{m}$, the congruence $a \equiv b \pmod{m}$ may be false.

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, the congruence $a^c \equiv b^d \pmod{m}$ may be false.

COLLARY 2

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

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

▼ Example 7

Find the value of $(19^3 \mathbf{mod}\ 31)^4 \mathbf{mod}\ 23$.

Solution:

$19^3 \mathbf{mod}\ 31 = 6859 \mathbf{mod}\ 31 = 221 \cdot 31 + 8 \mathbf{mod}\ 31 = 8$

$(19^3 \mathbf{mod}\ 31)^4 \mathbf{mod}\ 23 = 8^4 \mathbf{mod}\ 23$

$8^4 \mathbf{mod}\ 23 = 4096 \mathbf{mod}\ 23 = 178 \cdot 23 + 2 \mathbf{mod}\ 23 = 2.$

Arithmetic Modulo m

Arithmetic operations (Z_m): the set $\{0, 1, \ldots, m-1\}$.

> $$a +_m b = (a + b) \mathbf{mod}\ m$$
> $$a \cdot_m b = (a \cdot b) \mathbf{mod}\ m$$

▼ Example 8

Use the definition of addition and multiplication in Z_m to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution:

Using the definition of addtion modulo 11, we find that

$7 +_{11} 9 = (7 + 9) \mathbf{mod}\ 11 = 16 \mathbf{mod}\ 11 = 5.$

$7 \cdot_{11} 9 = (7 \cdot 9) \mathbf{mod}\ 11 = 63 \mathbf{mod}\ 11 = 8$

Properties $+_m$ and $\cdot_m$ satisfy

- **Closure**: If a and b belong to Z_m, then $a +_m b$ and $a \cdot_m b$ belong to Z_m.
- **Associativity**: If a, b, and c belong to 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 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. That is, if a belongs to Z_m, then $a +_m 0 = 0 +_m a = a$ and $a \cdot_m 1 = 1 \cdot_m a = a$.
- **Additive inverses**: If $a \neq 0$ belongs to Z_m, then $m - a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is, $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.
- **Distributivity**: If a, b, and c belong to Z_m, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.