## Modular Arithmetic

1/23/12

Arithmetic of remainders resulting from divisions of integers by a positive integer.

**Definition** Let $a$ and $b$ be integers and $m$ be a positive integer. $a$ is congruent to $b$ modulo $m$ if $m \mid (a-b)$.

$a \equiv b \pmod{m}$ if $a$ is congruent to $b$ modulo $m$

$a \not\equiv b \pmod{m}$ if $a$ is not congruent to $b$ modulo $m$

**Examples:** is $2 \equiv 5 \pmod{3}$ ? Does $3 \mid (2-5)$? yes.

is $17 \equiv 7 \pmod{5}$ ? Does $5 \mid (17-7)$? yes.

(Practice Problems 20, 26, and 29)

**Section 4.1, problem 11**: 12-hour clock. What is the time shown by the clock

80 hours after 11:00? $80+11 \pmod{12} = 7$. The clock will show 7:00.

40 hours before 12:00? $12-40 \pmod{12} = -28 \bmod 12 = 36-28 \pmod{12} = 8$. The clock showed 8:00.

**Theorem 4.**

Let $a$ and $b$ be integers and $m$ be a positive integer. $a \equiv b \pmod{m}$ if and only if $a = b + km$ for some integer $k$.

**proof:** $\Rightarrow$ Let $a \equiv b \pmod{m}$

$\therefore m \mid (a-b)$ by def.

$\therefore (a-b) = k \cdot m$ (by def. of divide notation) $k$ is an int

$\therefore a = b + km$

$\Leftarrow$ Let $a = b + km$

$\therefore (a-b) = km$ or $(a-b)$ is a multiple of $m$

$\therefore m \mid (a-b)$

$\therefore a \equiv b \pmod{m}$

**Theorem 3.** Let $a, b$ be integers, $m$ be a positive integers.

$a \equiv b \pmod m$ if and only if $(a \bmod m) = (b \bmod m)$

$\Rightarrow$: Let $a \equiv b \pmod m \Rightarrow a = b + km$ (from Theorem 4) (1)

By Division Algorithm, there exist two integers $q$ and $r$, $0 \le r < m$, such that

$b = q \cdot m + r$ or $b \bmod m = r$

$\therefore a = (qm + r) + km$ [Substitute for $b$ in (1)]

$a = qm + km + r$

$a = (q + k)m + r$ $\therefore a \bmod m = r$

$\therefore (a \bmod m) = (b \bmod m) = r.$

$\Leftarrow$ Let $(a \bmod m) = (b \bmod m)$

Let $a \bmod m = b \bmod m = r$, $0 \le r < m$.

$\therefore a = q_1 \cdot m + r$ & $b = q_2 m + r$

for some ints. $q_1$ and $q_2$

$a - b = (q_1 m + r) - (q_2 m + r)$

$= (q_1 - q_2)m$

$\therefore m \mid a - b \Rightarrow a \equiv b \pmod m$

**Theorem 5.** Let $a, b, c, d$ be integers and $m$ be a positive int.

If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then

(i) $a + c \equiv b + d \pmod m$

(ii) $ac \equiv bd \pmod m$

(i) $a \equiv b \pmod m \Rightarrow a = b + km$ (for some int $k$, Thm. 4)

$c \equiv d \pmod m \Rightarrow c = d + l \cdot m$ (for some int. $l$)

$a + c = (b + km) + (d + lm)$

$a + c = b + d + (k + l)m$

$\therefore a + c \equiv b + d \pmod m$ (Theorem 4)

[Prove (ii)]

**Corollary 2** (i) $(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m$

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

(i).

Fact: $a \equiv (a \bmod m) \pmod m$. Why?

By the division algorithm, there exist two unique integers q and r such that

$a = q\,m + r$, $0 \le r < m$.

Since $m \mid a-r$, $a \equiv r \pmod m$, where $r = a \bmod m$ (by definition)

$a \equiv (a \bmod m) \pmod m$

$b \equiv (b \bmod m) \pmod m$

$\therefore a + b \equiv ((a \bmod m) + (b \bmod m)) \bmod m$ (Thm 5, i)

**Problem 26**

List 5 integers that are congruent to 4 modulo 12. $a \equiv 4 \pmod{12}$

4, 16, 28, 40, 52

$4 + k \cdot 12$ $\quad a = 4 + km$

**Arithmetic modulo m**

m is a positive int. For any int a,

a mod m $\quad 0, 1, 2, \ldots, m-1$

$Z_m = \{0, 1, 2, \ldots, m-1\}$

$+_m$: $\quad a +_m b = a + b \pmod{m}$

$\cdot_m$: $\quad a \cdot_m b = a \cdot b \pmod{m}$

$m = 11$ $\quad 7 +_{11} 9 = 16 \pmod{11} = 5$

$7 \cdot_m 9 = 63 \pmod{11} = 8$

**Properties of $+_m$ and $*_m$ operations**

**Closure:** if a and $b \in Z_m$, $a +_m b \in Z_m$ and $a \cdot_m b \in Z_m$

**Associativity:**

$$(a +_m b) +_m c = a +_m (b +_m c) = a +_m b +_m c$$

$$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c) = a \cdot_m b \cdot_m c$$

**Commutativity:** $a +_m b = b +_m a$

$a \cdot_m b = b \cdot_m a$

**Distributivity:** $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$

Identity elements 0 and 1 such that $a +_m 0 = a$

$a \cdot_m 1 = a$

**Additive inverse:** if $a \in \mathbb{Z}_m$, then there exists a $b \in \mathbb{Z}_m$ such that $a +_m b = 0$,

$a = 7$, $m = 11$, then $11 - 7 = 4$ is the additive inverse of $a$

multiplicative inverse if $m$ is prime

**Applications of congruences**

**1. Hash functions**

Store several records with keys. in m locations.

# keys $\leq$ m

key range >> m

Solution: Let m = 100

banner id = 00975681 $\xrightarrow{\text{Store it}}$ loc. 00975681 mod 100

= loc. 81

banner id 00687581 $\longrightarrow$ loc. 81

**2. pseudorandom numbers (RN)**

- a sequence of deterministically generated numbers such that

(i) consecutive numbers appear to be unrelated

(ii) repetition cycle is large

RN Sequence $x_0, x_1, \ldots, x_0, x_1, \ldots$

$x_{n+1} = (a \cdot x_n + c) \bmod m$ a, c constants,

$(n+1)$th number; $n$th number

(Linear congruential method)

**Problem 7, Section 4.5**

$x_{n+1} = 3x_n \pmod{11}$. Here $a=3$, $c=0$, $m=11$

$x_0 = 2$

$x_1 = 3 \cdot x_0 \pmod{11}$
$= 3 \cdot 2 \bmod 11$
$= 6$

$x_2 = 3 \cdot x_1 \pmod{11}$
$= 3 \cdot 6 \pmod{11}$
$= 18 \pmod{11}$
$= 7$

$x_3 = 3 \times 7 \bmod 11 = 10$

$x_4 = 3 \times 10 \bmod 11 = 8$

$x_5 = 3 \times 8 \bmod 11 = 2 = x_0$

The pseudorandom sequence is 2, 6, 7, 10, 8, 2, ...

**3. Encryption/decryption**

Alphabet A, ..., Z. Given a message, replace each letter by the third letter to the right. for X, Y and Z, use A, B and C, respectively.

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | | | | | | | | | | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | | | | | | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

clear Text U T S A

cipher text X W V D

replace each letter by the third letter to the left to get clear text. For A, B, C use X, Y, Z, respecitively.

Encrypt: $f(p) = p+3 \pmod{26}$

$p$: position of a letter in the alphabet

$f(p)$: position of the letter that replaces the letter in the clear text

Decrypt: $g(q) = q-3 \pmod{26}$

$q$: position of a letter in the alphabet

$g(q)$: position of the letter that replaces the letter in the cyphier text