CSE 20 Lecture 6
2/02/10

Residual Number System

1. Intro
2. Definitions
3. Operations
4. Conversions

2. Definitions

1. Relatively Prime: Two integers a & b are relatively prime if their greatest common divisor is 1.

e.g. 3 & 8, 4 & 9, but not 6 & 9

Residual number: Given $m_1, m_2, \ldots, m_k$ relatively prime and a positive integer $x < \prod_{i=1}^{k} m_i = M$

($0 \leqslant x \leqslant M$) represent x as

($x \% m_1, x \% m_2, \ldots, x \% m_k$)

Example

$k = 3 (m_1, m_2, m_3) = (2, 3, 7)$

$M = m_1 m_2 m_3 = 2 \times 3 \times 7 = 42$

Given $x = 30$ $(x \% m_1, x \% m_2, x \% m_3)$

$= (30 \% 2, 30 \% 3, 30 \% 7)$

$= (0, 0, 2)$

Given $y = 4$ $(y \% m_1, y \% m_2, y \% m_3)$

$= (4 \% 2, 4 \% 3, 4 \% 7)$

$= (0, 1, 4)$

Given $x + y = 34$ $((x + y) \% m_1, (x + y) \% m_2, (x + y) \% m_3)$

$= (34 \% 2, 34 \% 3, 34 \% 7)$

$= (0, 0, 6)$

Theorem: for all x, y in the domain [0, M – 1]

If $x \neq y$

($x \% m_1$, $x \% m_2$,…, $x \% m_k$)

($y \% m_1$, $y \% m_2$,…, $y \% m_k$)

& differ by at least one element in the representation

Proof: suppose $x > y$

Let $z = x - y > 0$

Then ($z \% m_1$, $z \% m_2$,…, $z \% m_k$)

Has at least one nonzero element.

3. Operations:

Decimal number	Residual Number
x	$(x \% m_1, x \% m_2, \ldots, x \% m_k)$
y	$(y \% m_1, y \% m_2, \ldots, y \% m_k)$
$x + y$	$((x + y) \% m_1, (x + y) \% m_2, \ldots, (x + y) \% m_k)$
$x - y \ (x > y)$	$((x - y) \% m_1, (x - y) \% m_2, \ldots, (x - y) \% m_k)$
$xy \quad (xy < M)$	$((xy) \% m_1, (xy) \% m_2, \ldots, (xy) \% m_k)$

Example

(m_1, m_2, m_3) = (2, 3, 7)

$x = 8$ (x_1, x_2, x_3) = (0, 2, 1)

$y = 5$ (y_1, y_2, y_3) = (1, 2, 5)

$x + y = 13$ → (1, 1, 6)

$x - y = 3$ → (-1%2, 0%3, -4%7) = (1, 0, 3)

$x \times y = 40$ → (0%2, 4%3, 5%7) = (0, 1, 5)

4. Conversions

Chinese Remainder Theorem

Let $M_i = M/m_i$

S_i be the solution that $(M_i \times S_i) \% m_i = 1$

Then $x = (\sum_{i=1}^{k} M_i S_i r_i) \% M$

Given (m_1, m_2, m_3) = (2, 3, 7)

M = $\prod_{i=1}^{k} m_i$ = 2 × 3 × 7 = 42

$M_1 = m_2 \times m_3 = 3 \times 7 = 21$ $\quad (M_1 \times S\text{-}_1) \% m_1 = (27 \times S_1) \% 2 = 1$

$M_2 = m_1 \times m_3 = 2 \times 7 = 14$ $\quad (M_2 \times S\text{-}_2) \% m_2 = (14 \times S_2) \% 3 = 1$

$M_3 = m_1 \times m_2 = 2 \times 3 = 6$ $\quad (M_3 \times S\text{-}_3) \% m_3 = (6 \times S_3) \% 7 = 1$

$(S_1, S_2, S_3) = (1,2,6)$

(0,2,1) $\quad (M_1 S_1 r_1 + M_2 S_2 r_2 + M_3 S_3 r_3) \% M$

(21 × 1 × 0 + 14 × 2 × 2 + 6 × 6 × 1) % 42

= (0 + 56 + 36) % 42

= 92 % 42 = 8

(1,2,5) $(M_1 S_1 r_1 + M_2 S_2 r_2 + M_3 S_3 r_3) \% M$

$(21 \times 1 \times 1 + 14 \times 2 \times 2 + 6 \times 6 \times 5) \% 42$

$= (21 + 56 + 180) \% 42$

$= 257 \% 42 = 5$

Proof: Let A = ($_i$ S_i r_i)

1. A % m_j = r_j
2. A % M is unique.

1. A % m_j = ($\sum_{i=1}^{k}$ M_i S_i r_i) & m_j $\qquad$ $M_i = \prod_{j \neq 1}^{1-k} m_j$

= ($\sum$ ($M_i S_i r_i$) % m_j) % m_j

= ($M_i S_i r_i$) % m_j

= [(M_j S_j) % m_j $\times$ (r_j $\times$ m_j)] % m_j

= r_j % m_j

= r_j

2. Let y = A % M

Suppose x $\neq$ y

We have { 0 < |x-y| < M

|x-y| % m_i = 0 for all *i* in { 1, 2,…, k }