CSE 20 – Discrete Math
Review before mid-term 2

CK Cheng

2.17.2010

Residual Number System

- Residual Number System: Show the operation of 19 x 15 in a residual number system with moduli (m_1, m_2, m_3) = (5, 13, 14).

Let's start by showing some basic work and expanding the problem:

19	(x_1, x_2, x_3)	=	(4, 6, 5)
x 15	(y_1, y_2, y_3)	=	x (0, 2, 1)
285(R_1, R_2, R_3)	(0, 12, 5)		

Just as we did for the multiplication of 19 and 15, we multiply each item of the top row with the corresponding value in the bottom row. Staring with 4 times 0, then 6 times 2, then 5 times 1.

- The Chinese Remainder Theorem states:

$$Z = \left(\sum_{i=1}^{N} M_i \cdot S_i \cdot R_i \right) \% M$$

Applying it to our problem we get…

$$19 \cdot 15 = \left(\sum_{i=1}^{3} M_i \cdot S_i \cdot R_i \right) \% M$$

- There are three things we really need to find: M_i, S_i, and R_i. Let's start with M_i.

$$M_1 = m2 \times m3 = 13 \times 14 = 182$$

$$M_2 = m3 \times m1 = 14 \times 5 = 70$$

$$M_3 = m1 \times m2 = 5 \times 13 = 65$$

Also note: (to find big M)

M = m1 x m2 x m3

M = 5 x 13 x 14

- Next up, find S_i

S_i is defined through the equation:

$$(M_i \times S_i) \% m_i = 1$$

Let's start off by finding S1

$$(M1 \times S1) \% m1 = 1$$

$$((13 \times 14) S1) \% 5 = 1$$

$$(182 S1) \% 5 = 1$$

$$(2 S1) \% 5 = 1$$

S1 must be equal to 3.

- Now let's find S_2 and S_3

(M2 x S2) % m2 = 1

((5 x 14) S2) % 13 = 1

(70 S2) % 13 = 1

(5 S2) % 13 = 1

S2 must be equal to 8

(M3 x S3) % m3 = 1

((5 x 13) S3) % 14 = 1

(65 S3) % 14 = 1

(9 S3) % 14 = 1

S3 must be equal to 11

- Last thing: we have to find R_i

It's pretty simple because that is simply the result from "vertically" multiplying the results found on the first page:

19	(x_1, x_2, x_3)	=	(4, 6, 5)
x 15	(y_1, y_2, y_3)	=	x (0, 2, 1)
285	(R_1, R_2, R_3)		(0, 12, 5)

R1, R2, and R3 are simply 0, 12, and 5.

- Plug them in

$$19 \cdot 15 = \left(\sum_{i=1}^{3} M_i \cdot S_i \cdot R_i\right) \% M$$

$$[(13 \times 14 \times 3 \times 0) + (5 \times 14 \times 8 \times 12) + (5 \times 13 \times 11 \times 5)] \% 910$$

$$= [(0) + (6720) + (3575)] \% 910$$

$$= [10295] \% 910$$

$$= 285$$

Number 5 (on practice exam 2)

- Chinese Remainder Theorem: given mutually prime numbers (m_1, m_2, … m_k) and remainder (r_1, r_2, … r_k), where $r_i = x \,\%\, m_i$.

$$0 \leq X < \prod_{i=1}^{k} m_i = M$$

Then…

$$X = \left(\sum_{i=1}^{N} M_i \cdot S_i \cdot R_i \right) \% M$$

Where $M_i = M / m_i$ and $S_i : (M_i S_i) \% m_i = 1$

Proof:

(part 1)

$$\left(\sum_{j=1}^{k} M_j S_j R_j \cdot \right) \% m_i = R_i$$

$$\left[\left(\sum_{j=1}^{k} M_j S_j R_j \cdot \right) \% m_i\right] \% m_i$$

$(M_i S_i R_i) \% mi$ By construction of m_j which is multiple of m_i if i does not equal j.

$R_i \% m_i$ By construction of S_i

Since $R_i < m_i$, the answer = R_i

(Part 2)

Prove X is unique

m_i are mutually prime and $0 \leq X < M$

Boolean Algebra

Boolean Algebra: Prove general associability holds for “+” in any Boolean algebra.

For n = 3,

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

Associativety

Set x = a + (b + c)

Set y = (a + b) + c

To prove x = y, we prove

1)ax = ay

2)a’x = a’y

Prove 1)

ax = ay ?

ax = a(a + (b + c)) = aa + a(b + c) (Distributive)

= a + a(b + c) (Idempotence)

= a (Absorption)

ay = a((a + (b + c)) = a(a + b) + ac (Distributive)

= aa + ab + ac (Distributive)

= a + ab + ac (Idempotence)

= a + ac (Absorption)

= a (Absorption)

Therefore: ax = a = ay

Prove 2)

a’x = a’y?

a’x = a’(a + (b + c)) = a’a + a’(b + c) (Distributive)

= a’(b + c) (Complement Identity)

a’y = a’((a+b) + c) = a’(a + b) + a’c (Distributive)

= a’a + a’b + a’c (Distributive)

= a’b + a’c (Complement Identity)

= a’(b + c) (Distributive)

a’x = a’(b +c) = a’y