

## Hw2 Solutions

11.2 (a)  $M=7 \times 5 \times 3=105$ . The range is  $[0, 104]$ .

(b)  $M=105$ ;  $m_3=7, m_2=5, m_1=3$

$$m_3^{\wedge}=M/m_3=15, m_2^{\wedge}=M/m_2=21, m_1^{\wedge}=M/m_1=35$$

$$|1/m_3^{\wedge}|_{m_3}=|1/15|_7=1, |1/m_2^{\wedge}|_{m_2}=|1/21|_5=1, |1/m_1^{\wedge}|_{m_1}=|1/35|_3=2$$

$$(2|3|2)\text{RNS}(7|5|3)=(2 \times 1 \times 15 + 3 \times 1 \times 21 + 2 \times 1 \times 35)|_{105}=23$$

(c)

$$a_1=x_1=2$$

$$a_2=((2|3|2)-(2|2|2)) \times |1/3|_5=(0|1|-) \times 2=(0|2|-)$$

$$a_3=((0|2|-)-(2|2|2)) \times |1/5|_7=(5|-|-) \times 3=(1|-|-)$$

$$\rightarrow (2|3|2)\text{RNS}(7|5|3)=(1|2|2)\text{MRS}(5|3)$$

(d)  $20=(6|0|2)\text{RNS}(7|5|3)$

$$a_3=20/15=1, \quad 20 \bmod 15=5$$

$$a_2=5/3=1, \quad a_1=5 \bmod 3=2$$

$$20=(1|1|2)\text{MRS}(5|3)$$

11.6  $35=(0|2|1)\text{RNS}(7|3|2)$

$$(1/5|_7)=3, (1/5|_3)=2, (1/5|_2)=1$$

$$35/5=(0|2|1)\text{RNS}(7|3|2) \times (3|2|1)\text{RNS}(7|3|2)=(0|1|1)\text{RNS}(7|3|2)=7$$

Because  $(1/7|_7)$  doesn't exist, so  $35/7$  is not easy to be calculated.

$34/5$  is not an integer number that can be represented by RNS.

The conditions of performing division in RNS are: 1) the divisor is not a multiple of a base number; 2) the result is integer.

11.7 If the shifted-out bit is 0, the number is multiplied by 2.

| C(X) | C(X') |
|------|-------|
| 0    | 0     |
| 1    | 2     |
| 2    | 1     |

If the shifted-out bit is 1, the number is multiplied by 2, then decreased by  $2^n$ . When  $n=5$ :

| C(X) | C(X') |
|------|-------|
| 0    | 1     |
| 1    | 0     |
| 2    | 2     |

For example,  $X=01101$ ,  $C(X)=|X|=1$ .

1st shift:  $X'=11010$   $C(X')=2$

2nd shift:  $X'=10100$   $C(X')=2$

3rd shift:  $X'=01000$   $C(X')=2$

4th shift:  $X'=10000$   $C(X')=1$

5th shift:  $X'=00000$   $C(X')=0$