Chapter 7. Residue Number Systems

7.1. Introduction to RNS

7.1.1. Definition, Representation and Range

Definition A residue number system (RNS) is defined by a set of k pairwise relatively prime moduli:

$$\{m_{k-1}, m_{k-2}, \ldots, m_1, m_0\},$$

where $m_{k-1} > \cdots > m_1 > m_0 > 1$.

- The representation of a given value X with respect to the above RNS is

  $$X = (x_{k-1}, x_{k-2}, \ldots, x_1, x_0),$$

  where $x_i = X \bmod m_i, i = 0, 1, \ldots, k-1$.

- Another way to represent X in RNS is

  $$X = (x_{k-1}|x_{k-2}|\cdots|x_1|x_0)_{RNS(m_{k-1}|m_{k-2}|\cdots|m_1|m_0)},$$

  where $x_i = \langle X \rangle_{m_i}, i = 0, 1, \ldots, k-1$.

- The dynamic range of the RNS is defined as

  $$M = m_{k-1} \times m_{k-2} \times \cdots \times m_1 \times m_0,$$

  which means that the RNS can represent M continuous integers. The representation range of the RNS by default is $[0, M-1]$. In order to let the RNS system be capable of representing negative integers, the representation range can also be made to include negative integers, *i.e.*, $[-M/2+1, M/2]$ or $[-M/2, M/2-1]$ for even M, or $[-(M-1)/2, (M-1)/2]$ for odd M.

Example 1 *Let an RNS be given by* $(9, 7, 5, 2)$. *Then* $M = 9 \times 7 \times 5 \times 2 = 630$ *and its range is* $[0, 629]$. *For given values of* $X_1 = 108_{10}$ *and* $X_2 = 500_{10}$, *their representations with respect to the given RNS are respectively:*

$$\begin{aligned} X_1 &= 108_{10} &= (0|3|3|0)_{RNS(9|7|5|2)}, \\ X_2 &= 500_{10} &= (5|3|0|0)_{RNS(9|7|5|2)}. \end{aligned}$$

- Note that $(X + M) \bmod m_i = X \bmod m_i$. Therefore, $X + M$ has the same RNS representation as X. So have $X + 2M, X + 3M, \ldots; X - M, X - 2M, \ldots$. To avoid ambivalence, by default the range is $[0, M - 1]$, unless it is specifically defined as something else.

- RNS representation of X can be viewed as a k-digit number, where the digit set for position i is $[0, m_i - 1]$.

7.1.2. RNS arithmetic

Given two operands in RNS:

$$\begin{aligned} X &= (x_{k-1}|x_{k-2}|\cdots|x_1|x_0)_{RNS(m_{k-1}|m_{k-2}|\cdots|m_1|m_0)}, \\ Y &= (y_{k-1}|y_{k-2}|\cdots|y_1|y_0)_{RNS(m_{k-1}|m_{k-2}|\cdots|m_1|m_0)}. \end{aligned}$$

Then arithmetic operations with respect to RNS are as follows:

$$\begin{aligned} X + Y &= (\langle x_{k-1} + y_{k-1}\rangle_{m_{k-1}}|\langle x_{k-2} + y_{k-2}\rangle_{m_{k-2}}|\cdots|\langle x_0 + y_0\rangle_{m_0})_{RNS(m_{k-1}|m_{k-2}|\cdots|m_0)} \\ X - Y &= (\langle x_{k-1} - y_{k-1}\rangle_{m_{k-1}}|\langle x_{k-2} - y_{k-2}\rangle_{m_{k-2}}|\cdots|\langle x_0 - y_0\rangle_{m_0})_{RNS(m_{k-1}|m_{k-2}|\cdots|m_0)} \\ X \times Y &= (\langle x_{k-1} \times y_{k-1}\rangle_{m_{k-1}}|\langle x_{k-2} \times y_{k-2}\rangle_{m_{k-2}}|\cdots|\langle x_0 \times y_0\rangle_{m_0})_{RNS(m_{k-1}|m_{k-2}|\cdots|m_0)} \\ X \div Y &= (\langle x_{k-1} \times y_{k-1}^{-1}\rangle_{m_{k-1}}|\langle x_{k-2} \times y_{k-2}^{-1}\rangle_{m_{k-2}}|\cdots|\langle x_0 \times y_0^{-1}\rangle_{m_0})_{RNS(m_{k-1}|m_{k-2}|\cdots|m_0)} \end{aligned}$$

Example 2 *Let an RNS be defined with moduli* $= (17, 13, 2)$. *Represent* $X = 75_{10}$ *and* $Y = 5_{10}$ *w.r.t. the RNS and then perform* $X + Y$, $X - Y$, $X \times Y$ *and* $X \div Y$. *The results are also w.r.t. the RNS.*

Solution:

$$\begin{aligned} X &= 75_{10} &= (7|10|1)_{RNS(17|13|2)}, \\ Y &= 5_{10} &= (5|5|1)_{RNS(17|13|2)}. \end{aligned}$$

The arithmetic operations are as follows:

$$\begin{aligned} X+Y &= (\langle 7+5\rangle_{17}|\langle 10+5\rangle_{13}|\langle 1+1\rangle_{2})_{RNS(17|13|2)} \\ &= (12|2|0)_{RNS(17|13|2)}, \end{aligned}$$

$$\begin{aligned} X-Y &= (\langle 7-5\rangle_{17}|\langle 10-5\rangle_{13}|\langle 1-1\rangle_{2})_{RNS(17|13|2)} \\ &= (2|5|0)_{RNS(17|13|2)}, \end{aligned}$$

$$\begin{aligned} X\times Y &= (\langle 7\times 5\rangle_{17}|\langle 10\times 5\rangle_{13}|\langle 1\times 1\rangle_{2})_{RNS(17|13|2)} \\ &= (1|11|1)_{RNS(17|13|2)}, \end{aligned}$$

$$\begin{aligned} X\div Y &= (\langle 7\times 5^{-1}\rangle_{17}|\langle 10\times 5^{-1}\rangle_{13}|\langle 1\times 1^{-1}\rangle_{2})_{RNS(17|13|2)} \\ &= (\langle 7\times 7\rangle_{17}|\langle 10\times 8\rangle_{13}|\langle 1\times 1\rangle_{2})_{RNS(17|13|2)} \\ &= (15|2|1)_{RNS(17|13|2)}. \end{aligned}$$

7.2. The Associated Mixed-Radix System (optional)

7.2.1. Definition and properties

- Mixed-radix system (MRS) associated with a given RNS: For example, associated with RNS: (m_3, m_2, m_1, m_0), there is the MRS that a given X represented with the MRS as

$$\begin{aligned} X &= (a_3|a_2|a_1|a_0)_{MRS(m_3|m_2|m_1|m_0)} \\ &= a_3\cdot(m_2m_1m_0)+a_2\cdot(m_1m_0)+a_1\cdot m_0+a_0, \end{aligned} \tag{7.1}$$

  where $a_i \in [0, m_i-1], i = 0, 1, 2, 3$.

- MRS can be viewed as an intermediate number system between RNS and a conventional number system, i.e., decimal or binary.

$$RNS \rightleftharpoons MRS \rightleftharpoons Decimal.$$

- Comparison, sign detection, and overflow detection are made easier with MRS.

- As MRS mainly serves as an intermediate number systems and usually is not used for major computation, we do not discuss its arithmetic operations here.

- In the following we will discuss conversions between MRS and some other representations, i.e., decimal and the RNS.

7.2.2. Conversion from Decimal to MRS

Example 3 *Given RNS*$(9|7|5|2)$ *and its associated MRS. Convert decimal number* $X = 151_{10}$ *into MRS*$(9|7|5|2)$.
Solution:
Let $X = (a_3|a_2|a_1|a_0)_{MRS(9|7|5|2)}$ *with respect to MRS*$(9|7|5|2)$. *It follows from eqn. (7.1),*

$$a_3(m_2m_1m_0) + a_2(m_1m_0) + a_1m_0 + a_0 = 151. \tag{7.2}$$

Take modulo $m_0 = 2$ *on both sides of equation (7.2), it follows*

$$a_0 = 151 \bmod m_0 = 151 \bmod 2 = 1.$$

Subtract $a_0 = 1$ *and then be divided by* $m_0 = 2$ *on both sides of (7.2), so we have:*

$$a_3(m_2m_1) + a_2(m_1) + a_1 = 75. \tag{7.3}$$

Take modulo $m_1 = 5$ *on both sides of the above equation, it follows* $a_1 = 75 \bmod m_1 = 75 \bmod 5 = 0$. *Divided by* $m_1 = 5$ *on the both sides of (7.3), it follows*

$$a_3(m_2) + a_2 = 15. \tag{7.4}$$

Take modulo $m_2 = 7$ *on both sides of the above equation, it follows* $a_2 = 15 \bmod 7 = 1$. *Subtract* $a_2 = 1$ *on both sides of (7.4) and then divided by* $m_2 = 7$, *it follows* $a_3 = (15 - 1) \div 7 = 2$. *So,* $X = (a_3|a_2|a_1|a_0)_{MRS(9|7|5|2)} = (2|1|0|1)_{MRS(9|7|5|2)}$.

7.2.3. Conversion from MRS to Decimal

Example 4 *Let* $X = (2|1|0|1)_{MRS(9|7|5|2)}$. *Find its decimal representation.*
Solution: It follows from eqn. (7.1),

$$\begin{aligned} & a_3(m_2m_1m_0) + a_2(m_1m_0) + a_1m_0 + a_0 \\ = \; & 2 \times (7 \times 5 \times 2) + 1 \times (5 \times 2) + 0 \times 2 + 1 \\ = \; & 151_{10}. \end{aligned}$$

7.2.4. Conversion from RNS to the associated MRS:

Algorithm 1 *Conversion from RNS to MRS*

```
  Input:   $X = (x_{k-1}|x_{k-2}|\cdots|x_0)_{RNS(m_{k-1}|m_{k-2}|\cdots|m_0)}$
  Output:  $X = (a_{k-1}|a_{k-2}|\cdots|a_0)_{MRS(m_{k-1}|m_{k-2}|\cdots|m_0)}$

$Y_0 := X$;
$a_0 = Y_0 \bmod m_0$;
FOR $i := 0$ to $k-2$
        $Y_{i+1} = (Y_i - a_i) \cdot |\frac{1}{m_i}|$;
        $a_{i+1} = Y_{i+1} \bmod m_{i+1}$;
EndFor
```

Example 5 *Let* $X = (7|4|1|1)_{RNS(9|7|5|2)}$. *Find its decimal representation and the MRS representation* $X = (a_3|a_2|a_1|a_0)_{MRS(9|7|5|2)}$.

Solution:

$$\begin{array}{l}
Y_0 = X = (7|4|1|1), \\
a_0 = Y_0 \bmod m_0 = 1; \\
Y_0 - a_0 = (7|4|1|-) - 1 = (7|4|1|-) - (1|1|1|-) = (6|3|0|-), \\
Y_1 = (Y_0 - a_0)|\frac{1}{m_0}| = (6|3|0|-)|\frac{1}{2}| = (6|3|0|-)(5|4|3|-) = (3|5|0|-), \\
a_1 = Y_1 \bmod m_1 = (3|5|0|-) \bmod 5 = 0; \\
Y_1 - a_1 = (3|5|-|-) - 0 = (3|5|-|-), \\
Y_2 = (Y_1 - a_1)|\frac{1}{m_1}| = (3|5|-|-)|\frac{1}{5}| = (3|5|-|-)(2|3|-|-) = (6|1|-|-), \\
a_2 = Y_2 \bmod m_2 = (6|1|-|-) \bmod 7 = 1; \\
Y_2 - a_2 = (6|-|-|-) - 1 = (5|-|-|-), \\
Y_3 = (Y_2 - a_2)|\frac{1}{m_2}| = (5|-|-|-)|\frac{1}{7}| = (5|-|-|-)(4|-|-|-) = (2|-|-|-), \\
a_3 = Y_3 \bmod m_3 = (2|-|-|-) \bmod 9 = 2.
\end{array}$$

So we have solved:

$$a_0 = 1, a_1 = 0, a_2 = 1, a_3 = 2$$

and

$$X = (7|4|1|1)_{RNS(9|7|5|2)} = (2|1|0|1)_{MRS(9|7|5|2)}.$$

7.2.5. Conversion from MRS to RNS:

Let an MRS associate with RNS: (m_3, m_2, m_1, m_0). Assume MRS representation of a number is

$$X = (a_3|a_2|a_1|a_0)_{\text{MRS}(m_3|m_2|m_1|m_0)}.$$

Find RNS representation $X = (x_3|x_2|x_1|x_0)_{\text{RNS}(m_3|m_2|m_1|m_0)}$.

From equation (7.1) it follows

$$X = a_3 \cdot (m_2 m_1 m_0) + a_2 \cdot (m_1 m_0) + a_1 \cdot m_0 + a_0.$$

Then

$$x_0 = X \bmod m_0 = a_0.$$

Similarly, we have

$$x_1 = X \bmod m_1 = a_1 m_0 + a_0 \bmod m_1.$$

x_2 and x_3 can be solved in simlar fashion.

7.3. Chinese Remainder Theorem (optional)

Given a RNS representation $X = (x_{k-1}|x_{k-2}|\cdots|x_0)_{RNS(m_{k-1}|m_{k-2}|\cdots|m_0)}$. How to evaluate X (convert it to decimal directly without resorting to MRS)?

Theorem 1 *Chinese Remainder Theorem: For RNS with moduli* $= (m_{k-1}, m_{k-2}, \ldots, m_0)$*, given RNS representation* $X = (x_{k-1}|x_{k-2}|\cdots|x_0)_{RNS(m_{k-1}|m_{k-2}|\cdots|m_0)}$*. Then an evaluation of* X *can be given as*

$$X = \left\langle \sum_{i=0}^{k-1} M_i \langle \alpha_i x_i \rangle_{m_i} \right\rangle_M ,$$

where $M_i = M/m_i, \alpha_i = \langle M_i^{-1} \rangle_{m_i}, i = 0, 1, \ldots, k-1.$

Chinese remainder theory is often abbreviated as CRT. We will use the following example to illustrate this theorem.

Example 6 *Given* $X = (4|6|2|1)_{RNS(9|7|5|2)}$*. Convert* X *into decimal number representation.*
Solution: (will be discussed in class)

Remark: Clearly, conversion of RNS representation to decimal can be done in the following two methods. The first method is to use MRS as the intermediate number system, where we convert RNS to MRS and then from MRS to decimal. The second method is to apply CRT that converts RNS to decimal in one single step.