Residue Number Systems

Sarah E. Ritchey

Youngstown State University

August 1, 2013

Residue Number Systems (RNS)

Definition

Define a modulus set to be $\{m_1, m_2, \ldots, m_n\}$ where m_j and m_k for $1 \le j \ne k \le n$ are odd pairwise relatively prime natural numbers. For any number $0 \le U < M = m_1 m_2 \ldots m_n$, let $u_j \equiv U \mod m_j$ for all $1 \le j \le n$. We will then call $\{u_1, u_2, \ldots, u_n\} = U$ the residue set for U.

Residue Number Systems (RNS)

Definition

Define a modulus set to be $\{m_1, m_2, \ldots, m_n\}$ where m_j and m_k for $1 \leq j \neq k \leq n$ are odd pairwise relatively prime natural numbers. For any number $0 \leq U < M = m_1 m_2 \ldots m_n$, let $u_j \equiv U \mod m_j$ for all $1 \leq j \leq n$. We will then call $\{u_1, u_2, \ldots, u_n\} = U$ the residue set for U.

For example, If $\{5, 7, 11\}$ is a modulus set and u=157, then

$$\begin{aligned} 157 &\equiv 2 \mod 5 \\ 157 &\equiv 3 \mod 7 \\ 157 &\equiv 3 \mod 11 \end{aligned}$$

so $U = \{2, 3, 3\}$ is our residue set and $M = 5 \cdot 7 \cdot 11 = 385$.

Why Use These

- Possible alternative method to perform arithmetic calculations on large numbers.

Why Use These

- Possible alternative method to perform arithmetic calculations on large numbers.
- Computers have parallel processors!

Why Use These

- Possible alternative method to perform arithmetic calculations on large numbers.

- Computers have parallel processors!

- Do arithmetic component-wise on each element in the residue set at the same time.

  Say we want to add $U = \{1, 2, 3\}$ and $V = \{4, 5, 6\}$ respectively as a residue set.
  $U + V = \{1 + 4, 2 + 5, 3 + 6\} = \{5, 7, 9\}$

Why Use These

- Possible alternative method to perform arithmetic calculations on large numbers.

- Computers have parallel processors!

- Do arithmetic component-wise on each element in the residue set at the same time.

  Say we want to add $U = \{1, 2, 3\}$ and $V = \{4, 5, 6\}$ respectively as a residue set.
  $U + V = \{1 + 4, 2 + 5, 3 + 6\} = \{5, 7, 9\}$

- It may be more efficient than only using a fraction of computational power.

Issues in an RNS

Because only the residue set is stored in a computers memory, new techniques are needed to handle:

Issues in an RNS

Because only the residue set is stored in a computers memory, new techniques are needed to handle:

- Conversion in and out of RNS
- Overflow Detection
- Parity Checking
- Sign of a Number

Converting into and out of RNS

To RNS:

- Use Modular Arithmetic
- Very Fast with computers

Converting into and out of RNS

To RNS:

- Use Modular Arithmetic
- Very Fast with computers

From RNS:

- Use Chinese Remainder Theorem
- Only efficient with very large numbers

Chinese Remainder Theorem

Theorem

Let $m_1, m_2, \ldots, m_n$ be odd positive integers which are pairwise relatively prime. Let $M = m_1 m_2 \ldots m_n$ and let $u_1, u_2, \ldots u_n$ be positive integers. There is only one integer U that satisfies

$$0 \leq U < M \quad \mathit{and} \quad U \equiv u_j \mod m_j \quad \mathit{for} \quad 1 \leq j \leq n.$$

Theorem

Let $m_1, m_2, \ldots, m_n$ be odd positive integers which are pairwise relatively prime. Let $M = m_1 m_2 \ldots m_n$ and let $u_1, u_2, \ldots u_n$ be positive integers. There is only one integer U that satisfies

$$0 \le U < M \quad \textit{and} \quad U \equiv u_j \mod m_j \quad \textit{for} \quad 1 \le j \le n.$$

Proof of Uniqueness.

Assume $U \equiv V \mod m_j$ for $1 \le j \le n$, then $U - V$ is a multiple of m_j for all j. Note $\gcd(m_j, m_k) = 1$ when $j \neq k$. This implies that $U - V$ is a multiple of $M = m_1 m_2 \ldots m_n$. This argument shows that there is **at most** one solution. □

Chinese Remainder Theorem Existence Proof

Proof.

We can find $\bar{m}_j$, with $1 \leq j \leq n$ such that,

$$\bar{m}_j \equiv 1 \mod m_j \qquad \text{and} \qquad \bar{m}_j \equiv 0 \mod m_k$$

for $k \neq j$. This follows because m_j and $\frac{M}{m_j}$ are relatively prime, so we may take

$$\bar{m}_j = \left(\frac{M}{m_j}\right)^{\varphi(m_j)}$$

by Euler's theorem. Now the number

$$U = u_1\bar{m}_1 + u_2\bar{m}_2 + \cdots + u_r\bar{m}_n \mod M$$

satisfies all the conditions. □

Converting Into and Out of an RNS

Let $\{5, 7\}$ be our modulus set and $M = 5 * 7 = 35$. Suppose we want to compute $11 + 17$.

$$11 = \{1, 4\}$$
$$17 = \{2, 3\}$$

Thus,

$$11 + 17 = \{(1 + 2) \mod 5, (4 + 3) \mod 7\} = \{3, 0\}$$

Using the chinese remainder theorem, we know:

$$\begin{aligned} 11 + 17 &= \left(3 * \left(\frac{35}{5}\right)^{\varphi(5)} + 0 * \left(\frac{35}{7}\right)^{\varphi(7)}\right) \mod 35 \\ &= \left(3 * 7^4 + 0 * 5^6\right) \mod 35 \\ &= 3 * 7^4 \mod 35 \\ &= 7{,}203 \mod 35 \\ &= 28 \end{aligned}$$

Overflow Detection

For any arithmetic operation $*$, let $Z = X * Y$. Overflow has occurred if $Z > M$.

Overflow Example

Let $\{5, 7\}$ be our modulus set and $M = 5 * 7 = 35$. Suppose we want to compute $32 + 17$.

$$32 = \{2, 4\}$$

$$17 = \{2, 3\}$$

Thus,

$$32 + 17 = \{4, 0\}$$

Overflow Example

Let $\{5, 7\}$ be our modulus set and $M = 5 * 7 = 35$. Suppose we want to compute $32 + 17$.

$$32 = \{2, 4\}$$

$$17 = \{2, 3\}$$

Thus,

$$32 + 17 = \{4, 0\}$$

Using the chinese remainder theorem, we know:

$$\begin{aligned} 32 + 17 &= \left(4 * \left(\frac{35}{5}\right)^{\varphi(5)} + 0 * \left(\frac{35}{7}\right)^{\varphi(7)}\right) \mod 35 \\ &= 14 \end{aligned}$$

Overflow Example

Let $\{5,7\}$ be our modulus set and $M = 5 * 7 = 35$. Suppose we want to compute $32 + 17$.

$$32 = \{2,4\}$$

$$17 = \{2,3\}$$

Thus,

$$32 + 17 = \{4,0\}$$

Using the chinese remainder theorem, we know:

$$\begin{aligned} 32 + 17 &= \left(4 * \left(\frac{35}{5}\right)^{\varphi(5)} + 0 * \left(\frac{35}{7}\right)^{\varphi(7)}\right) \mod 35 \\ &= 14 \end{aligned}$$

$32 + 17 = 49 \neq 14$

Overflow Detection

For any arithmetic operation $*$, let $Z = X * Y$. Overflow has occurred if $Z > M$.

Overflow Detection

For any arithmetic operation $*$, let $Z = X * Y$. Overflow has occurred if $Z > M$.

Why not simply compare magnitude of Z and M?

Overflow Detection

For any arithmetic operation $*$, let $Z = X * Y$. Overflow has occurred if $Z > M$.

Why not simply compare magnitude of Z and M?

Comparing magnitudes of two numbers is NOT efficient.

Overflow Detection

For any arithmetic operation $*$, let $Z = X * Y$. Overflow has occurred if $Z > M$.

Why not simply compare magnitude of Z and M?

Comparing magnitudes of two numbers is NOT efficient.

Use parity checking to detect overflow.

Parity Checking

Determining parity is telling whether a number is even or odd.

$$\mathcal{P}(X) \equiv X \mod 2 = |X|_2$$

Determining Parity

For integer $X \in [0, M)$ with residue representation $\{x_1, x_2, \ldots, x_n\}$ for the modulus set $\{m_1, m_2, \ldots, m_n\}$. Let $\hat{m}_i = \frac{M}{m_i}$. By the chinese remainder theorem, we know

$$|X|_M = \left| \sum_{i=1}^{n} \hat{m}_i \left| \frac{x_i}{\hat{m}_i} \right|_{m_i} \right|_M$$

$$|X|_M = \sum_{i=1}^{n} \hat{m}_i \left| \frac{x_i}{\hat{m}_i} \right|_{m_i} - rM$$

$$\mathcal{P}(|X|_M) = \mathcal{P}(\frac{x_1}{\hat{m}_1}) \oplus \mathcal{P}(\frac{x_2}{\hat{m}_2}) \oplus \ldots \mathcal{P}(\frac{x_n}{\hat{m}_n}) \oplus \mathcal{P}(r)$$

Calculating r

Define $S_i = |\frac{z_i}{\hat{m}_i}|_{m_i}$ for all $i \in \{1, \ldots, n\}$. Using the equation above, solve for r to get:

$$\sum_{i=1}^{n} \frac{S_i}{m_i} - \frac{|X|_M}{M} = r$$

Because $\frac{|X|_M}{M} < 1$, we can say:

$$\left\lfloor \sum_{i=1}^{n} \frac{S_i}{m_i} \right\rfloor = r$$

We can use the approximation

$$\frac{S_i}{m_i} = \frac{\lceil 2^t \frac{S_i}{m_i} \rceil}{2^t}.$$

It can be shown that to guarantee the accuracy of this function $t > \lceil \log_2(nM) \rceil$.

Signed Integers

Definition

In an RNS, a number X is considered non-negative if $0 \leq X \leq \frac{M}{2}$, and a number Y is considered negative if $\frac{M}{2} < X < M$.

Notice the additive inverse of X, is $M - X$.

For example, the inverse of 1 is $M - 1$.

Determining Sign with Parity Overflow Detection

Theorem

We know M is odd. Now for any $X < M$, X is non-negative if and only if $2X \mod M$ is even. Else if $2X \mod M$ is odd, then X is negative.

For example, say $M = 7$.
If X=3, then $2X \mod 7 \equiv 6$ which is even. Thus, X is positive.
If Y=5, then $2Y \mod 7 \equiv 3$ which is odd. Thus, Y is negative.

Overflow with Signed Integers

Check Sign of X and Y.

Theorem (Additive Overflow $X + Y$)

If X and Y have different signs, then no overflow occurs.
If X and Y are positive, check sign of $2(X + Y)$. If even, then no overflow.
If X and Y are negative, check sign of $2[(M - X) + (M - Y)]$. If even, then no overflow.

Theorem (Subtraction Overflow $X - Y$)

Consider $X + (M - Y)$. Follow addition algorithm.

Conclusions

- Parity checking has the potential to quickly solves many limitations in a residue number system.
- I would like to see if restricting the modulous set in some way will make converting out of an RNS more efficient.
- I would also like to test to see if keeping track of the relative magnitude of each number is more spatially efficent.

Thanks to Dr. Kramer for excellent advisement!

Bibliography

1. Knuth. *Semi numerical Algorithms: The Art of Computer Programming*. Vol 2.
2. Lu, Mi and Jen-Shiun Chaing, *A Novel Division Algorithm for the Residue Number System.* IEEE Transactions on Computers.
3. Hill, William. *A Spatially-Efficient Additive Overflow Detection Algorithm for the Residue Number System*.

Thanks to Dr. Kramer for excellent advisement!

Magnitude Comparison

Is $\{u_1, u_2, \ldots, u_r\} > \{v_1, v_2, \ldots, v_r\}$?

Theorem

Determine the signs of U an V.

If U and V are of different signs, then the positive number is larger.

If U and V are both positive, find the parity of each.

- *If U and V have the same parity, then $U - V$ is even if and only if $U \geq V$. Similarly $U - V$ is odd if and only if $U < V$.*

- *If U and V are of different parity, then $U - V$ is odd if and only if $U \geq V$. Similarly $U - V$ is even if and only if $U < V$.*

If U and V are both negative, find the additive inverse of each and compare the magnitude of the inverses. The number with the largest inverse, is the smallest in magnitude.