Residue Numbers

Choose a set of "relatively prime" moduli. e.g. \(2^{n-1}-1, 2^n-1, 2^n+1, 2^n-1, 2^n, 2^n+1\) but not both

For example \(\{5, 7, 8\}\)

The legitimate range is the product of the moduli set. (More specifically, the number of unique integer values that can be represented is \(\prod_{i=1}^{n} m_i\).)

A number is then represented as the remainder set (technically the residue set) obtained by applying each modulus to the number.

For instance, if the number is 220 its residue representation would be \(\{0, 3, 4\}\) for the moduli set of \(\{5, 7, 8\}\).

To reconstruct the original value from the residues use the Chinese Remainder Theorem.

First compute \(M_i = \frac{M}{m_i}\) where \(M = \prod_{i=1}^{n} m_i\), \(m_i\equiv\text{modulus } i\)

\[M_1 = \frac{m_1 \times m_2 \times m_3}{m_1} = m_2 \times m_3 = 7 \times 8 = 56\]

\[M_2 = \frac{m_1 \times m_2 \times m_3}{m_2} = m_1 \times m_3 = 5 \times 8 = 40\]

\[M_3 = \frac{m_1 \times m_2 \times m_3}{m_3} = m_1 \times m_2 = 5 \times 7 = 35\]
Now find the multiplicative inverse $K_i$, where $K_i$ is the smallest integer multiple of $M_i$ such that $(K_i \times M_i) \mod m_i = 1$

For our 220 example:

$1 \times M_1 \mod m_1 = 56 \mod 5 = 1 \quad \text{Thus } K_1 = 1$

$1 \times M_2 \mod m_2 = 40 \mod 7 = 5$
$2 \times M_2 \mod m_2 = 80 \mod 7 = 3$
$3 \times M_2 \mod m_2 = 120 \mod 7 = 1 \quad \text{Thus } K_2 = 3$

$1 \times M_3 \mod m_3 = 35 \mod 8 = 3$
$2 \times M_3 \mod m_3 = 70 \mod 8 = 6$
$3 \times M_3 \mod m_3 = 105 \mod 8 = 1 \quad \text{Thus } K_3 = 3$

**Chinese Remainder Theorem:**

\[
X = \left( \sum_{i=1}^{n} M_i \times \left[ \left( \frac{K_i \times r_i}{m_i} \mod m_i \right) \mod m_i \right] \right) \mod M
\]

\[
X = \left[ 56 \times \left[ (1 \times 0) \mod 5 \right] + 40 \times \left[ (3 \times 3) \mod 7 \right] + 35 \left[ (3 \times 4) \mod 8 \right] \right] \mod 280
\]

\[
= \left[ 56 \times 0 + (40 \times 2) + (35 \times 4) \right] \mod 280
\]

\[
= 140 \mod 280 = 220
\]

Another example: 221 $\rightarrow$ Residues = \{1, 4, 5\}

$M_1 = 56 \quad K_1 = 1$

$M_2 = 40 \quad K_2 = 3$

$M_3 = 35 \quad K_3 = 3$

\[
X = \left( \sum_{i=1}^{n} M_i \times \left[ \left( \frac{K_i \times r_i}{m_i} \mod m_i \right) \mod m_i \right] \right) \mod M
\]

\[
= \left[ 56 \left[ (1 \times 1) \mod 5 \right] + 40 \left[ (3 \times 4) \mod 7 \right] + 35 \left[ (3 \times 5) \mod 8 \right] \right] \mod 280
\]

\[
= \left[ 56 + 200 + 245 \right] \mod 280
\]

\[
= 501 \mod 280 = 221
\]
Addition and Subtraction of Residue Numbers
\[ |x \pm y|_m = |lx|m \pm |ly|m |_m \]

Multiplication of Residue Numbers
\[ |xy|_m = |lx|m \cdot |ly|m |_m \]

Translation: Operating on the original numbers and finding the residue is the same as operating on the residues.

Example: \( m = 5 \), \( x = 53 \), \( y = 19 \)
\[ |x|_5 = 3 \quad |y|_5 = 4 \]

Addition: \( |x+y|_5 = |53+19|_5 = |72|_5 = 2 \)
\[ |lx|_5 + |ly|_5 = |3 + 4|_5 = |17|_5 = 2 \]

Or we could work with residue sets. Let \( m = \{5, 7, 8\} \)
\[ x = 14 = \{ 4, 0, 6 \} \quad y = 9 = \{ 4, 2, 1 \} \]

\[
\begin{array}{cccc}
14 & 4 & 0 & 6 \\
+9 & +4 & +2 & +1 \\
\hline
23 & 3 & 2 & 7 \\
\end{array}
\]
Residues of 23 are \( \{3, 2, 7\} \mod 5 \), \( \mod 7 \), \( \mod 8 \)

\[
\begin{array}{cccc}
9 & 4 & 2 & 1 \\
-14 & -4 & -0 & -6 \\
-5 & 0 & 2 & 3 \\
\hline
\end{array}
\]
\( \mod 5 \), \( \mod 7 \), \( \mod 8 \)
(1-6) mod 8? What is this?

Formally, to find the residue of a number for a given modulus we must fulfill:

\[ Z_i = q_i \cdot m_i + r_i \quad \text{where} \]

\[ Z_i = \text{value or number} \]
\[ q_i = \text{integer} \]
\[ m_i = \text{modulus} \]
\[ r_i = \text{residue}, \quad q_i \text{ must be selected such that} \quad 0 \leq r_i < m_i \]

\[-5 = q_i \cdot 8 + r_i \]

Thus \( q_i = -1 \) so that \( r_i = 3 \)

What is the residue set for -5?

\[ m_1 = 5 \quad -5 = q_1 \cdot 5 + r_1 \quad \Rightarrow \quad q_1 = -1 \quad r_1 = 0 \]
\[ m_2 = 7 \quad -5 = q_2 \cdot 7 + r_2 \quad \Rightarrow \quad q_2 = -1 \quad r_2 = 2 \]
\[ m_3 = 8 \quad -5 = q_3 \cdot 8 + r_3 \quad \Rightarrow \quad q_3 = -1 \quad r_3 = 3 \]

\[-5 = \{0, 2, 3\}\]
What about multiplication?

\[
\begin{array}{cccc}
\text{14} & \text{4} & \text{0} & \text{6} \\
\times 9 & \times 4 & \times 2 & \times 1 \\
\hline
\text{126} & \text{0} & \text{0} & \text{6} \\
\text{mod 5} & \text{mod 7} & \text{mod 8} \\
\end{array}
\]

Residue set for 126 is \{1, 0, 6\}

Now try 14 and -9. First find residues of -9

m₁ = 5  \quad -9 = q₁ 5 + r₁  \Rightarrow q₁ = -2 \quad r₁ = 1

m₂ = 7  \quad -9 = q₂ 7 + r₂  \Rightarrow q₂ = -2 \quad r₂ = 5

m₃ = 8  \quad -9 = q₃ 8 + r₃  \Rightarrow q₃ = -2 \quad r₃ = 7

-9 = \{1, 5, 7\}

\[
\begin{array}{cccc}
\text{14} & \text{4} & \text{0} & \text{6} \\
\times (-9) & \times 1 & \times 5 & \times 7 \\
\hline
\text{-126} & \text{4} & \text{0} & \text{2} \\
\text{mod 5} & \text{mod 7} & \text{mod 8} \\
\end{array}
\]

Is this correct? Find residues of -126

-126 = q₁ 5 + r₁  \Rightarrow q₁ = -26 \quad r₁ = 4

-126 = q₂ 7 + r₂  \Rightarrow q₂ = -18 \quad r₂ = 0

-126 = q₃ 8 + r₃  \Rightarrow q₃ = -16 \quad r₃ = 2

-126 = \{4, 0, 2\}

This is all great and neat as long as finding the residues isn’t actually computationally expensive in terms of time or circuitry.
Low Cost Residues

These can be found directly for positive integers

\[ x \geq 2 \]

Choose \( m = 2^x - 1 \)

In this case the residue can be found without division.

1. Split the data up into groups of \( x \) bits.
2. Pad with zeros as necessary.
3. Add all groups using \( \text{mod}-m \) (i.e. \( \text{mod} \ 2^x-1 \)) additions.

For example, let \( x = 2 \) \( m = 3 \)

\[
\begin{align*}
\text{Data} & = 10011110 = 158_{10} \\
(10 + 01) \mod 3 & = 10 \mod 3 \\
(11 + 10) \mod 3 & = 10 \mod 3 \\
(00 + 10) \mod 3 & = 10 \mod 3 = 10_{10} = 2_{10}
\end{align*}
\]

Check: \( 158 \mod 3 = 2 \), Yes!

Examples:

\[
\begin{align*}
10101100101_z & = 1381_{10} \\
01 + 01 & = 10 \\
01 + 10 & = 01 \\
01 + 01 & = 01
\end{align*}
\]

\[
\begin{align*}
11111111_z & = 255_{10} \\
11 + 11 & = 10 \\
11 + 11 & = 00 \\
00 + 00 & = 00
\end{align*}
\]

\( 1381 \mod 3 = 1 \)

\( 255 \mod 3 = 0 \)

\[
\begin{align*}
3 \left[ \begin{array}{c}
416 \\
126 \\
15 \\
0
\end{array} \right] \\
\frac{85}{29} \frac{15}{15} \frac{15}{0}
\end{align*}
\]
Let \( y = 3 \) and thus \( m = 7 \) (so group 3 bits at a time).

\[
\begin{align*}
\overbrace{1111111}^z &= 255_{10} \\
\overbrace{0111111}^z &= 127_{10} \\
011 + 111 &\downarrow \\
011 + 111 &\downarrow \\
011 &
\end{align*}
\]

\( 255 \mod 7 = 3 \)

\( 127 \mod 7 = 1 \)

Of course order of residue additions is irrelevant.

Consider \( 183_{10} = 10110111_z \)

\[
\begin{align*}
010 + 110 &\downarrow \\
010 + 110 &\downarrow \\
001 &
\end{align*}
\]

\( 183 \mod 7 = 1 \)