CSE20 Lecture 6: Number Systems
5. Residual Numbers (cont) &
6. Cryptography

CK Cheng
UC San Diego
Residual Numbers
(NT-1 and Shaum’s Chapter 11)

• Introduction
• Definition
• Operations
• Inverse Conversion
Inverse Conversion

Number x

Mod Operation

Moduli \((m_1, m_2, \ldots, m_k)\)

Residual number \((x_1, x_2, \ldots, x_k)\)

+,-, x operations for each \(x_i\) under \(m_i\)

Results

Chinese Remainder Theorem
Chinese Remainder Theorem

Given a residual number \((r_1, r_2, ..., r_k)\) with moduli \((m_1, m_2, ..., m_k)\), where all \(m_i\) are mutually prime, set \(M = m_1 \times m_2 \times ... \times m_k\), and \(M_i = M / m_i\).

1. Find \(S_i\) that \((M_i \times S_i) \text{ mod } m_i = 1\) \((S_i\) an inverse of \(M_i\) in mod \(m_i\))

2. The corresponding number

\[ x = (\sum_{i=1,k}(M_i \times S_i \times r_i)) \text{ mod } M. \]
Example

Given \((m_1,m_2,m_3)=(2,3,7)\), \(M=2\times3\times7=42\), we have

\[M_1=m_2 \times m_3 = 3 \times 7 = 21\]
\[(M_1 S_1)\%m_1 = (21 S_1)\%2 = 1\]

\[M_2=m_1 \times m_3 = 2 \times 7 = 14\]
\[(M_2 S_2)\%m_2 = (14 S_2)\%3 = 1\]

\[M_3=m_1 \times m_2 = 2 \times 3 = 6\]
\[(M_3 S_3)\%m_3 = (6 S_3)\%7 = 1\]

Thus, \((S_1, S_2, S_3) = (1,2,6)\)

For a residual number \((0,2,1):\)

\[x=(M_1 S_1 r_1 + M_2 S_2 r_2 + M_3 S_3 r_3)\%M\]
\[=(21\times1\times0 + 14\times2\times2 + 6\times6\times1)\%42\]
\[= (0 + 56 + 36)\%42 = 92\%42 = 8\]
Example

For a residual number (1,2,5):

\[ x = (M_1 S_1 r_1 + M_2 S_2 r_2 + M_3 S_3 r_3) \mod M \]

\[ = (21 \times 1 \times 1 + 14 \times 2 \times 2 + 6 \times 6 \times 5) \mod 42 \]

\[ = (21 + 56 + 180) \mod 42 \]

\[ = 257 \mod 42 = 5 \]
Example: iClicker

Given \((m_1,m_2,m_3)=(2,3,5)\), \(M=2\times3\times5=30\), we have

\[M_1 = m_2 \times m_3 = 3 \times 5 = 15\]
\[(M_1 S_1) \mod m_1 = (15 S_1) \mod 2 = 1\]

\[M_2 = m_1 \times m_3 = 2 \times 5 = 10\]
\[(M_2 S_2) \mod m_2 = (10 S_2) \mod 3 = 1\]

\[M_3 = m_1 \times m_2 = 2 \times 3 = 6\]
\[(M_3 S_3) \mod m_3 = (6 S_3) \mod 5 = 1\]

Thus, \((S_1, S_2, S_3)\) is

A. \((1, 1, 1)\)

B. \((1, 2, 1)\)

C. \((2, 1, 2)\)

D. None of the above
Example: iClicker

Given \((m_1, m_2, m_3) = (2, 3, 5)\), \(M = 2 \times 3 \times 5 = 30\), we have

\[
\begin{align*}
M_1 &= m_2 \times m_3 = 3 \times 5 = 15 \quad (M_1 S_1) \mod m_1 = (15 S_1) \mod 2 = 1 \\
M_2 &= m_1 \times m_3 = 2 \times 5 = 10 \quad (M_2 S_2) \mod m_2 = (10 S_2) \mod 3 = 1 \\
M_3 &= m_1 \times m_2 = 2 \times 3 = 6 \quad (M_3 S_3) \mod m_3 = (6 S_3) \mod 5 = 1
\end{align*}
\]

For a residual number \((x_1, x_2, x_3) = (1, 2, 3)\), the corresponding number \(x\) is

A. 5
B. 19
C. 23
D. None of the above
Proof of Chinese Remainder Theorem

Let \( A = \sum_{i=1,k} (M_i S_i r_i) \), we show that

1. \( A \mod m_v = r_v \) and 2. \( x=A\mod M \) is unique.

1. \( A \mod m_v = \left[ \sum_{i=1,k} (M_i S_i r_i) \right] \mod m_v \)
   
   \[= \left[ \Sigma (M_i S_i r_i) \mod m_v \right] \mod m_v = (M_v S_v r_v) \mod m_v \]

   \[= [(M_v S_v) \mod m_v \times r_v \mod m_v] \mod m_v = r_v \mod m_v = r_v \]

2. Proof was shown in lecture 5.
6. Cryptography

1. Introduction
2. RSA Protocol
3. Remarks
6.1 Cryptography: Introduction

• Application of residual number systems
• Number theory (skip)
• Show the basic concept and process
• Many variations
6.2 RSA Protocol

- Function $P(X) = X^{e}\%N$ is public.
- Function $S(X) = X^{d}\%N$ is secret.
- Message $M$ is private, but $P(M)$ is observed by all.
- Desired feature: $S(P(M)) = M$.

Example: $(e,N) = (7,55), (d,N) = (23,55)$

- $M = 12 \Rightarrow P(12) = 12^7\%55 = 23 \Rightarrow S(23) = 23^{23}\%55 = 12$
- $M = 8 \Rightarrow P(8) = 8^7\%55 = 2 \Rightarrow S(2) = 2^{23}\%55 = ?$
6.2 RSA Protocol

1. \( N = pq \) where \( p \) & \( q \) are primes and kept secret.
2. \( e \) is mutually prime to \( f(N) = (p-1)(q-1) \)
3. \( d \) is the inverse of \( e \) mod \( f(N) \), i.e. \((ed)\%f(N) = 1\)

Theorem: \( S(P(M)) = P(S(M)) = M \) for \( 0 \leq M < N \)

Note that \( S(P(M)) = M^{ed} \% N \)

Theorem: \( M^{f(N)} \% N = 1 \) for \( 0 \leq M < N \)

Assumption: \( p \) & \( q \) are hard to find. Consequently, it is difficult to derive \( d \).
6.2 RSA Protocol

1. $N = pq$ where $p$ & $q$ are primes and kept secret.
2. $e$ is mutually prime to $f(N) = (p-1)(q-1)$
3. $d$ is the inverse of $e$ mod $f(N)$, i.e. $(ed)\%f(N) = 1$

Example: $N = pq = 3 \times 11 = 33$, $f(N) = (3-1)(11-1) = 20$
Let $e = 3$, then $d = 7$ ($3 \times 7 \% 20 = 1$).

$M = 9 \Rightarrow P(9) = 9^3 \% 33 = 3 \Rightarrow S(3) = 3^7 \% 33 = ?$
6.3 Remark

- Residual number system is used in cryptography.
- RSA protocol uses public key for coding $P(X)$ and secret key to decode $S(X)$.
- Use wide words (>1000 bits) so that the solution is computationally expensive without the knowledge of the function $S(X)$.