Residue Number Systems

A Puzzle

What number has the reminders 2, 3 and 2 when divided by the numbers 7, 5 and 3 ?

$$x \bmod 7 = 2$$

$$x \bmod 5 = 3$$

$$x \bmod 3 = 2$$

$$x = ???$$

Chinese mathematician Sun Tzu - third-century AD
(not the famous military strategist Sun Tzu)

Chinese Remainder Theorem

There exists an integer x solving the system of equations:

$$x \bmod m_1 = x_1$$

$$\ldots$$

$$x \bmod m_n = x_n$$

where numbers $m_1 \ldots m_n$ are relatively prime.

Residue Representation

- Convert X-value into RNS representation:
  - find a set of numbers (i.e. moduli), which are all **relatively prime** to each other (greatest common divisor is 1):

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

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

    e.g. 7, 5, 3
  - compute a set of residues with respect to moduli:

    $x_{k-1}, x_{k-2}, \ldots x_1, x_0$ where $x_i = X \bmod m_i = \langle x \rangle_{m_i}$

    e.g. $(X=12) \rightarrow 5, 2, 0$
  - residue list is treated as a k-digit RNS number:

    $X = (x_{k-1} | x_{k-2} | \ldots | x_1 | x_0)_{RNS(m_{k-1} | m_{k-2} | \ldots m_1 | m_0)}$ e.g. $(5|2|0)_{RNS(7|5|3)}$

RNS Examples

- Assume RNS(8|7|5|3)

$123 = (3|4|3|0)_{RNS}$

123				
moduli	8	7	5	3
residues	3	4	3	0

$5 = (5|5|0|2)_{RNS}$

5				
moduli	8	7	5	3
residues	5	5	0	2

$0 = (0|0|0|0)_{RNS}$

0				
moduli	8	7	5	3
residues	0	0	0	0

Congruency Relation

- Two integers a and b are said to be congruent modulo n, if their difference (a−b) is an integer multiple of n.

$$a \equiv b \pmod{n}$$

- $X \equiv x \pmod{m} \rightarrow x = X - km$

e.g.

$13 \equiv 3 \pmod{5} \rightarrow 3 = 13 - 2*5$

$13 \equiv 8 \pmod{5} \rightarrow 8 = 13 - 1*5$

$13 \equiv 13 \pmod{5} \rightarrow 13 = 13 - 0*5$

Operations on Congruent Numbers

For congruencies $A_i \equiv a_i$ (with modulus n):

- $\sum A_i \equiv \sum a_i$
- $A_i - A_j \equiv a_i - a_j$
- $\prod A_i \equiv \prod a_i$
- $A^s_i \equiv a^s_i$
- $v \cdot A_i \equiv v \cdot a_i$

(except division)

modulus = 5

A1 ≡ a1	13	3
A2 ≡ a2	9	4
sum	22	7 (2)
diff.	4	-1 (4)
mult.	117	12 (2)

Operations on RNS Numbers

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

$$X \equiv (x_{k-1} | x_{k-2} | \ldots | x_1 | x_0)$$

$$X \text{ oper } Y$$

$$(x_{k-1} \text{ oper } y_{k-1} | \ldots | x_1 \text{ oper } y_1 | x_0 \text{ oper } y_0)$$

Operations on RNS Numbers

- Operation (+,−,*,^) on RNS numbers is performed on all corresponding residues, totally in parallel
- Operation on residues at i-positions is performed modulo m_i
- The resulting RNS number uniquely identifies the result of operation (within the dynamic range)

Example of RNS Operations

- All operations are performed in parallel on corresponding residues (modulo m_i)

RNS		(8|7|5|3)
A	21	(5|0|1|0)
B	8	(0|1|3|2)
A+B	29	(5|1|4|2)
A−B	13	(5|6|3|1)
A*B	168	(0|0|3|0)
A^2	441	(1|0|1|0)
B^3	512	(0|1|2|2)
3*A	63	(7|0|3|0)

Representation Range

- RNS numbers may uniquely identify M numbers, where $M = (m_{k-1} * ... * m_1 * m_0) = \prod m_i$

  e.g. RNS(8|7|5|3) → 8*7*5*3 = 840 unique combinations

- M is called a dynamic range for a given RNS

- The range can cover any interval of M-consecutive numbers

  e.g. for M=840

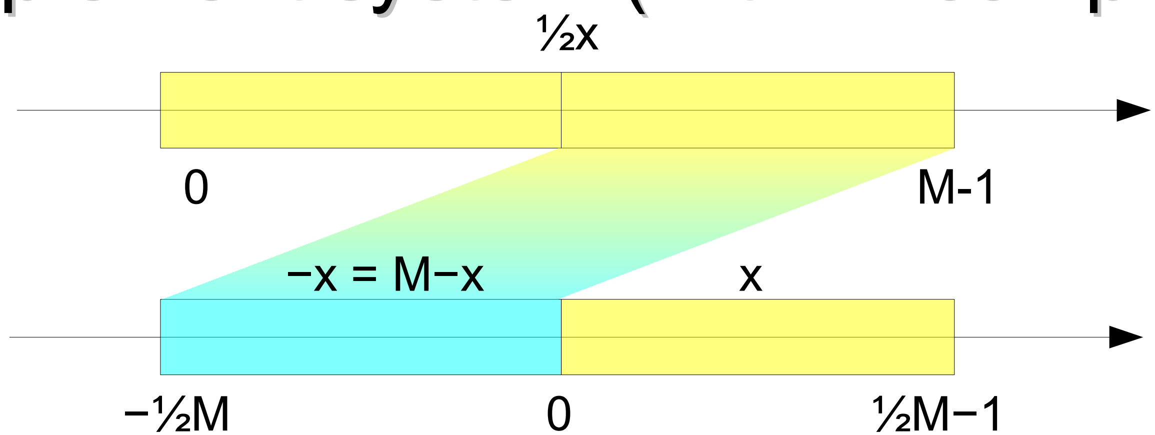
  0..839, −420..419, etc.

  $(0|0|0|0)_{RNS}$ = 0 or 840 or 1680 ...

  $(7|6|4|2)_{RNS}$ = 839 or -1

Negative RNS Numbers

- Negative numbers can be represented using a complement system (with M-complement)



- Residues of −x are equal to residues of M−x

$$(-x) \bmod m_i = (M-x) \bmod m_i$$

- Residues of −x are m_i-complements of x

$$x = (x_{k-1} | \ldots | x_0) \rightarrow -x = (m_{k-1} - x_{k-1} | \ldots | m_0 - x_0)$$

Negative RNS - Examples

- Take RNS representation of positive number

  $x = 21 = (5|0|1|0)_{RNS}$ ($RNS(8|7|5|3)$)

- Calculate m_i-complements of all residues

  $(8-5 \mid 7-0 \mid 5-1 \mid 3-0)_{RNS} = (3 \mid 0 \mid 4 \mid 0)_{RNS} = -21$

$0 = (0|0|0|0)_{RNS} \rightarrow -0 = (0|0|0|0)_{RNS}$

$1 = (1|1|1|1)_{RNS} \rightarrow -1 = (7|6|4|2)_{RNS}$

$419 = (3|6|4|2)_{RNS} \rightarrow -419 = (5|1|1|1)_{RNS}$

Difficult RNS Operations

- Speed of addition and multiplication in RNS is counterbalanced by difficulty of other important arithmetical operations:
  - division
  - sign test
  - magnitude comparison
  - overflow detection
- Applications of RNS are limited to fields with predominant use of addition and multiplication within the known range (FFT, DSP)

Efficiency of RNS Representation

- Residues are kept internally as separate binary numbers (bit-fields)

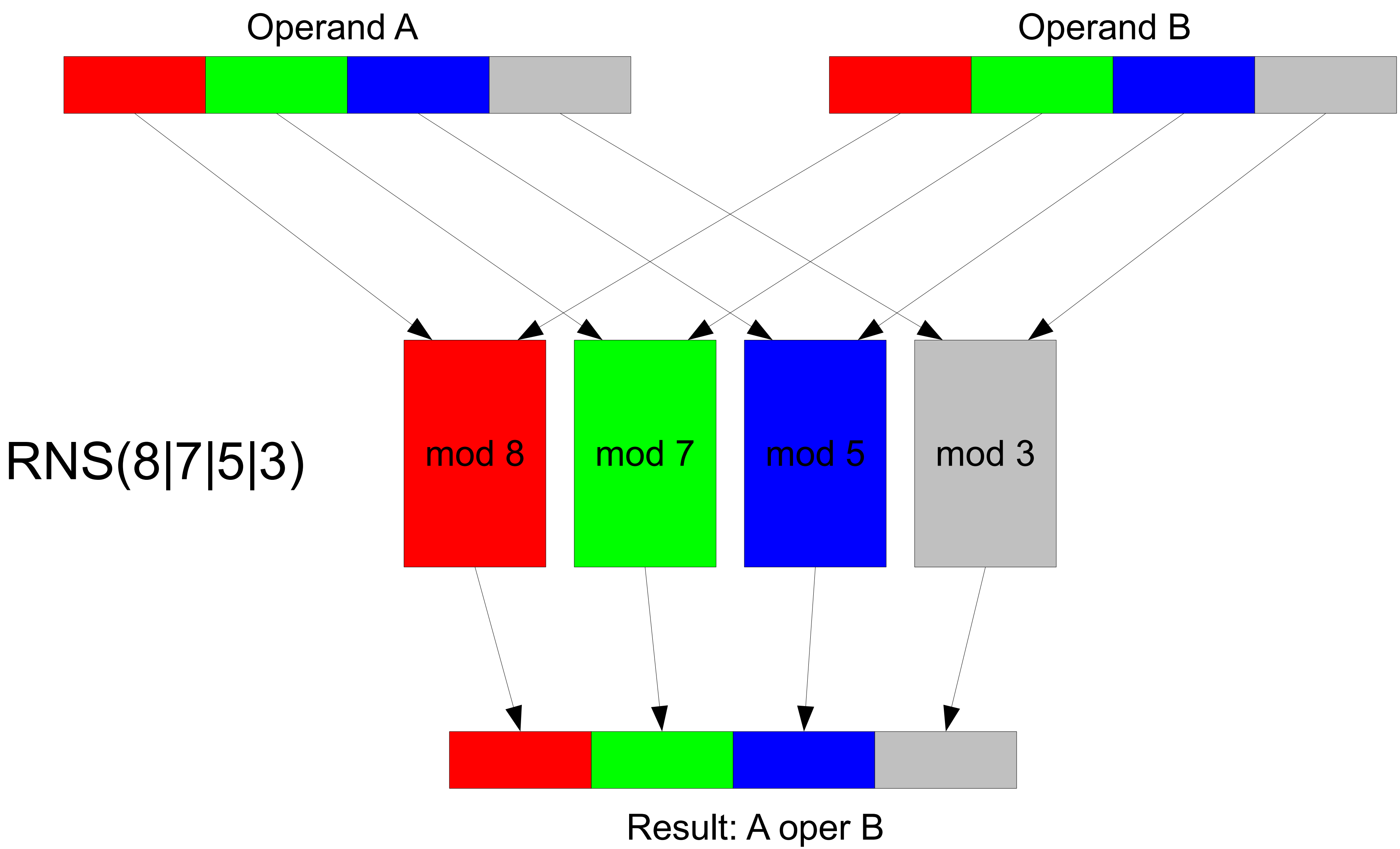
e.g. $5 = (5|5|0|2)_{RNS(8|7|5|3)} \rightarrow 10110100010$ (11-bits)

- How many bits are needed for M-different representations (in NBC)?

$$\log_2 M \rightarrow \log_2 840 = 9.714 \text{ bits}$$

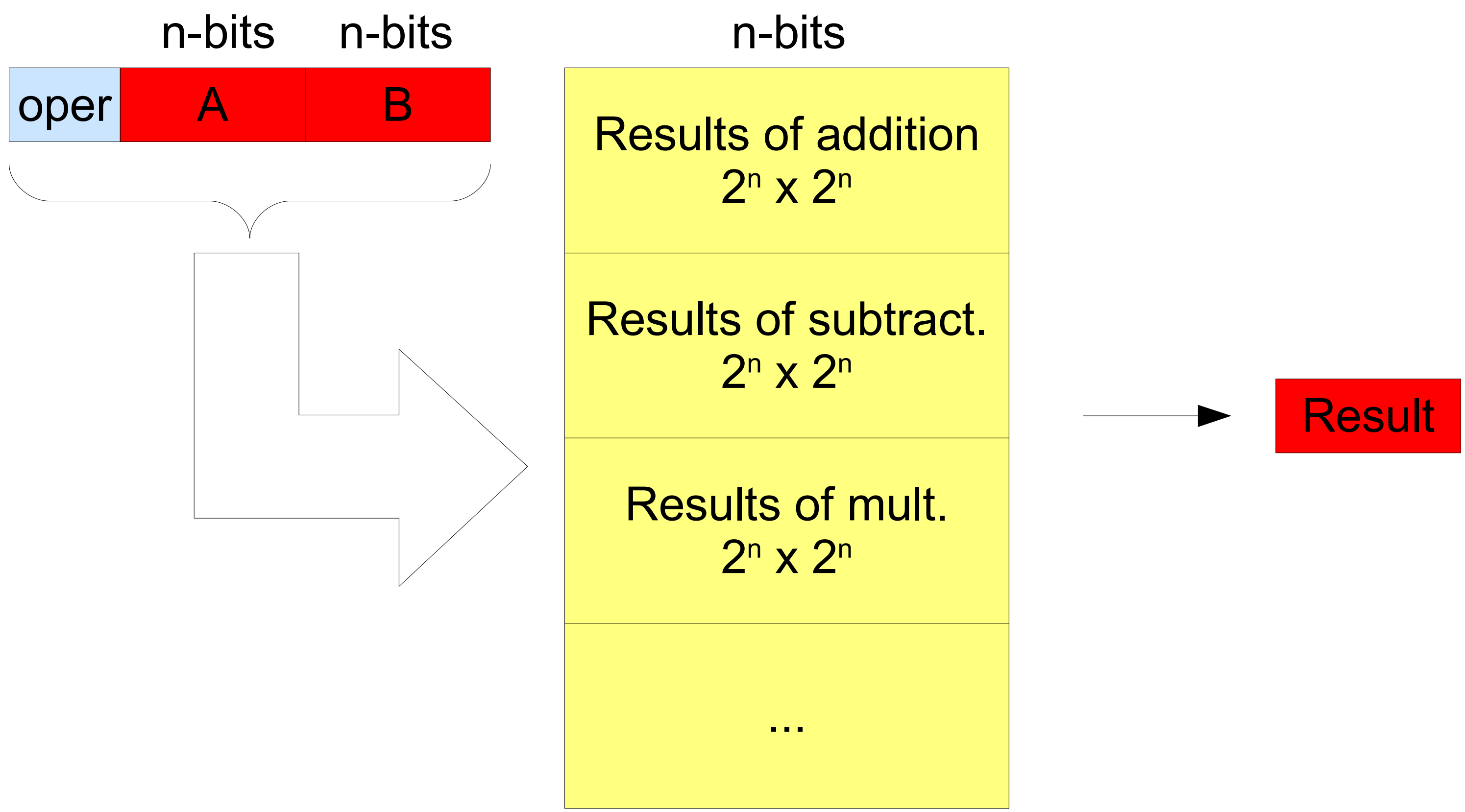
- Repr. efficiency is the ratio possible RNS representations related to NBC with the same bit-field length n
  - $\text{Eff} = M(n) / 2^n \rightarrow 840/2048 = 41\%$

RNS Arithmetical Unit



Fast Arithmetics with LUT

- Small size of operands permits the lookup-table implementation of residue arithm.units



e.g. 4-operations on 4-bits operands → 4 * (2^4 * 2^4) = 4*256 = 1024 4bit words (512B)

Choosing the RNS Moduli

- Moduli set (m_{k-1}...m_0) affects both
  - representation efficiency
  - complexity of arithmetical units
- For the chosen range M:
  - find the moduli: primes (or semi-primes) with product ≥ M
  - roughly equal bit-size of moduli should be favored (not an easy task)
  - moduli 2^n an 2^n-1 simplify arithmetic units

e.g. M=65535 → RNS(13|11|9|7|5|2), $\prod m_i$=90090, 20 bits :-(

Choosing the Moduli - Example

M = 100 000 (17 bits in NBC)

- Select consecutive primes

  RNS(17|13|11|7|5|3|2) → ∏=510510, 23 bits
- Remove primes to scale the result

  RNS(17|13|11|7|3|2) → ∏=102102, 20 bits
- Combine primes – equalize moduli length

  RNS(26|21|17|11) → ∏=102102, 19 bits
- Use powers of small primes

  RNS(15|13|11|2^3|7) → ∏=102102, 18 bits, max 4-bit field
- Favor 2^n an 2^n-1moduli

  RNS(2^5|2^5-1|2^4-1|2^3-1) → ∏=104160, 17 bits, eff≈100%

Conversion to RNS

Calculate the residues $m_{k-1} \ldots m_0$:

- From decimal – requires division
- From binary – requires addition of precomputed values from lookup table and simple division

$$\underbrace{\underbrace{b_{k-1} \ldots b_0}_{\text{NBC number}} \bmod m_i}_{\text{i-th residue of RNS representation}} = \underbrace{(\underbrace{2^{k-1} b_{k-1} \bmod m_i}_{\text{Precomputed for given RNS}} + \ldots + \underbrace{2^0 b_0 \bmod m_0}_{\text{Precomputed for given RNS}})}_{\text{requires division of relatively small number - can be implemented with LUT}} \bmod m_i$$

Binary to RNS - Example

- 164: $10100100_{NBC} \rightarrow$ RNS(8|7|5|3) ?

10100100_{NBC} mod 8 = 100_{NBC} = 4 (trivial)

10100100_{NBC} mod 7 = (2+4+4) mod 7 = 3

10100100_{NBC} mod 5 = (3+2+4) mod 5 = 4

10100100_{NBC} mod 3 = (2+2+1) mod 3 = 2

Final division uses small numbers and can also be implemented with LUT

- 164: $10100100_{NBC} \rightarrow$ (4|3|4|2)

Lookup table with precomputed partial residues for RNS with moduli (8|7|5|3)

k	2^k	2^k mod ... 8	7	5	3
0	1	1	1	1	1
1	2	2	2	2	2
2	4	4	4	4	1
3	8	0	1	3	2
4	16	0	2	1	1
5	32	0	4	2	2
6	64	0	1	4	1
7	128	0	2	3	2

Conversion from RNS

- Any RNS has associated mixed-radix system (MRS)

  $RNS(m_{k-1}|\ldots|m_0) = MRS(w_{k-1}|\ldots|w_0)$

- Conversion from RNS to any positional system is possible if the weights $w_{k-1}\ldots w_0$ are known
- Any RNS number $(x_{k-1}|\ldots|x_0)$ can be expressed as

  $x_{k-1}(1|0|\ldots|0) + x_{k-2}(0|1|\ldots|0) + \ldots + x_1(0|\ldots|1|0) + x_0(0|\ldots|0|1)$

- The weights $w_{k-1}\ldots w_0$ are equal to RNS numbers

  $(1|0|\ldots|0), (0|1|\ldots|0) \ldots (0|\ldots|1|0), (0|\ldots|0|1)$

Conversion from RNS

- Values of weights for the given RNS can be precomputed and used as constants

  $w_{k-1} = (1|0|...|0)_{RNS}$, ... $w_0 = (0|...|0|1)_{RNS}$

- All conversions are done modulo M.

  e.g. for RNS(8|7|5|3)

  $(1|0|0|0)_{RNS} = 105$

  $(0|1|0|0)_{RNS} = 120$

  $(0|0|1|0)_{RNS} = 336$

  $(0|0|0|1)_{RNS} = 280$

  $(3|2|4|2)_{RNS} = (3*105+2*120+4*336+2*280) \bmod 840 =$
  $(2459) \bmod 840 = 779$

Conversion from RNS

- How to calculate $(1|0|...|0)_{RNS}$ ...$(0|...|0|1)_{RNS}$?
- e.g. $(1|0|...|0)_{RNS}$ means the number that is dividable by moduli $m_{k-2}...m_0$
- $(1|0|...|0)_{RNS} = m_{k-2}*...*m_0 * n \quad (n=1,2...,m_{k-1}-1)$

  e.g $(1|0|0|0)_{RNS(8|7|5|3)} = 7*5*3*n$
- $(m_{k-2}*...*m_0 * n) \bmod m_{k-1} = 1 \rightarrow n=?$

  $(7*5*3*n) \bmod 8 = 1 \rightarrow n=1$

  $(1|0|...|0)_{RNS} = 7*5*3 = 105$

Selection of n is easy due to very limited range [1,...,m-1]