CSE20 Lecture 5: Number Systems
5. Residual Numbers

CK Cheng

UC San Diego

5. Residual Numbers

(NT-1 and Shaum's Chapter 11)

1. Introduction (parallel processing on huge numbers)
2. Definition (conversion)
3. Operations (+, -, x)
4. Inverse Conversion (recover the solution)

5. Residual Numbers: iClicker

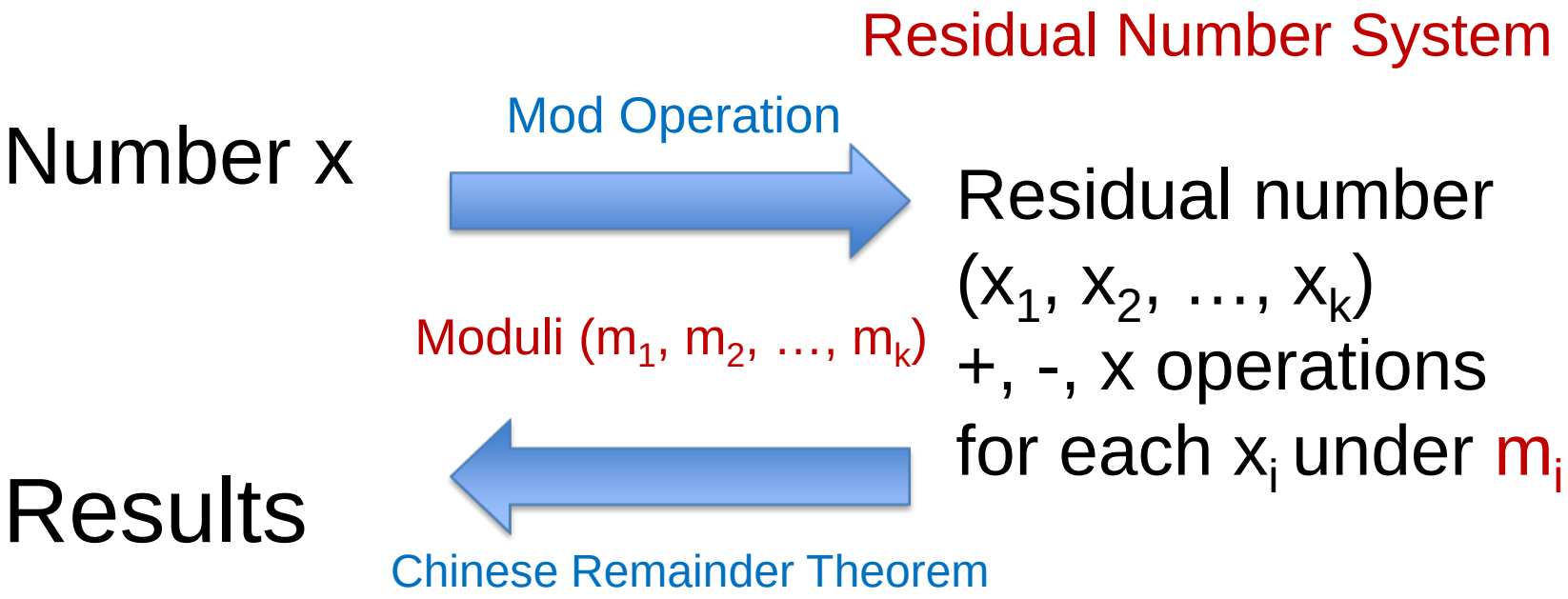
The statement about residual number system.

A. A counting system in ***Sun Tsu's Arithmetic Manual*** in the 4th century AD.
B. The system can be used for error correction.
C. The system is efficient for numbers with wide bit width.
D. All of the above
E. Two of the above.

5.1 Introduction

- Applications: communication, cryptography, and high performance signal processing
- Goal: Simplify arithmetic operations (+, -, x) when bit width n is huge, e.g. n= 1000. Note no division is involved.
- Usage in CSE: CSE20, CSE107, CSE127

5.1 Introduction: Flow



5.2 Definition

Mod (Modular) operation:

– Given integers x and d (d> 0), find q and r such that x = q*d+r, 0<= r <d,

where q: quotient, d: divisor, and r: remainder.

We define x%d= r.

Examples:

20=2*7+6 => 20%7=6

11=2*5+1 => 11%5=1

-8=(-2)*5+2 => (-8)%5=2

5.2 Definitions

Residual number: Conversion

Given $(m_1, m_2,\ldots,m_k)$ where m_i are mutually prime and a positive integer $x < M = m_1 m_2 \ldots m_k$ ($0 \le x < M$) represent x as

$$(x\%m_1, x\%m_2,\ldots, x\%m_k)$$

Mutually Prime:

- Two integers a & b are mutually (or relatively) prime if their greatest common divisor is 1.
- e.g. 3 & 8, 4 & 9, but not 6 & 9

Examples ($X\%m_i=r_i$)

Given moduli $(m_1, m_2, m_3) = (3, 5, 7)$, convert

X: (x_1, x_2, x_3), where $x_i=X\%m_i$.

- $X=0$; $x_1=x\%3=0$, $x_2=x\%5=0$, $x_3=x\%7= 0$.
  $=>(x_1,x_2,x_3)=(0,0,0)$
- $X=21$: $x_1=x\%3=0$, $x_2=x\%5=1$, $x_3=x\%7=0$.
  $=>(x_1,x_2,x_3)=(0,1,0)$
- X=18: $r_1=x\%3=$, $r_2=x\%5=$, $r_3=x\%7=$.
  $=>(x_1,x_2,x_3)=($, , $)$
- X=-9 : $x_1=x\%3=$, $x_2=x\%5=$, $x_3=x\%7=$
  $=>(x_1,x_2,x_3)=($, , $)$

5.2 Examples: iClicker

Can we compare the value of the residual numbers by comparing the residuals?

iClicker (A: Yes, B: No)

Given moduli $(m_1, m_2, m_3) = (2, 5, 7)$ and X=17, derive the corresponding residual number (x_1, x_2, x_3), where $r_i = X \% m_i$.

- A. (1, 3, 2)
- B. (1, 2, 3)
- C. (0, 1, 2)
- D. None of the above

Examples

A residual number system with $(m_1,m_2,m_3)=(2,3,7)$

- $M = m_1 * m_2 * m_3 = 2 * 3 * 7 = 42$
- Given X=30, $(X\%m_1, X\%m_2, X\%m_3)$
  $= (30\%2, 30\%3, 30\%7) = (0, 0, 2)$
- Given Y=4, $(Y\%m_1, Y\%m_2, Y\%m_3)$
  $= (4\%2, 4\%3, 4\%7) = (0, 1, 4)$
- Given X+Y=34,
  $((X+Y)\%m_1,(X+Y)\%m_2,(X+Y)\%m_3)$
  $= (34\%2, 34\%3, 34\%7) = (0, 1, 6)$

5.3 Modular Operations: Addition

Theorem 1: Given three integers x,y,d (d>0), we have (x+y)%d=(x%d+y%d)%d.

Proof:

Let $x = q_x d + r_x$ and $y = q_y d + r_y$

We have $(x+y)\%d = (q_x d + r_x + q_y d + r_y)\%d$

$=(r_x+r_y)\%d$

Therefore, (x+y)%d = (x%d+y%d)%d

5.3 Modular Operations: Multiplication

Theorem 2: Given three integers x,y,d (d>0), we have (x*y)%d=(x%d * y%d)%d.

Proof:

Let $x = q_x d + r_x$, $y = q_y d + r_y$

We have $(x*y)\%d = (q_x d + r_x)*(q_y d + r_y)\%d$

$$=(q_x q_y d^2+r_y q_x d+r_x q_y d+r_x * r_y)\%d$$

$$= (r_x * r_y)\%d$$

Therefore, (x*y)%d = (x%d * y%d)%d

5.3 Modular Operations

- What about division?
- Could we state the following equality?

  ((x%d)/(y%d))%d= (x/y)%d

E.g. try the case that x=6, y=3 & d=3

5.3 Modular Operations

- What about division?
- Could we state the following equality?

  ((x%d)/(y%d))%d= (x/y)%d

Answer: Not always! We have the following problems.

1. y%d can be zero.
2. (x%d)/(y%d) or x/y can be fractional.

5.3 Modular Operations: Examples

Given x=24 and y=19, derive x+y in the residual number system $(m_1,m_2,m_3)=(3,5,8)$.

I. $x+y=24+19=43$, $r_1=43\%3=1$, $r_2=43\%5=3$, $r_3=43\%8=3$. $\Rightarrow(r_1,r_2,r_3)=(1,3,3)$

II. Apply theorem 1.

$x\Rightarrow (x_1,x_2,x_3)=$

$y\Rightarrow (y_1,y_2,y_3)=$

$x+y\Rightarrow ((x_1+y_1)\%m_1,(x_2+y_2)\%m_2,(x_3+y_3)\%m_3)$

$=$

5.3 Modular Operations: Examples

Given x=9 and y=12, derive x*y in the residual number system $(m_1,m_2,m_3)=(3,5,8)$.

I. $x*y=9*12=108$, $r_1=108\%3=0$, $r_2=108\%5=3$, $r_3=108\%8=4$. $=>(r_1,r_2,r_3)=(0,3,4)$

II. Apply theorem 2.

$x=> (x_1,x_2,x_3)=$

$y=> (y_1,y_2,y_3)=$

$x*y=> ((x_1*y_1)\%m_1,(x_2*y_2)\%m_2,(x_3*y_3)\%m_3)$

$=$

5.3 Range of Numbers

Theorem 3: In a residual number system with $(m_1, m_2, \ldots, m_k)$, where all m_i are mutually prime, for any $0<=y<x<M=m_1m_2\ldots m_k$, we have the inequality $(x_1, x_2, \ldots, x_k)$!= $(y_1, y_2, \ldots, y_k)$, i.e.

there exists an $0<i<=k$ such that x_i!= y_i.

Proof: By contradiction. Suppose that

$(x_1, x_2, \ldots, x_k)=(y_1, y_2, \ldots, y_k)$, then x-y : (0,0, …,0) (theorem 1). However, for all numbers in the range of the interval, only 0 : (0,0, …,0) because the mods m_i are mutually prime.

5.3 Range of Numbers

Example: Let k=3 & $(m_1, m_2, m_3)=(3,4,5)$

1. M=3x4x5=60
2. Given X=45 and Y=40

   $(x_1,x_2,x_3)=(45\%3, 45\%4, 45\%5)=(0,1,0)$ and

   $(y_1,y_2,y_3)=(40\%3, 40\%4, 40\%5)=(1,0,0)$

3. Suppose Y=105 then

   $(y_1,y_2,y_3)=(105\%3, 105\%4, 105\%5)=(0,1,0)$