RESIDUE
CODES

CONTENT

01 RESIDUE CODES

02 RESIDUE NUMBER SYSTEM (RNS)

03 RESIDUE CODES ALGORITHMS

03.1 CHINESE REMAINDER THEOREM (CRT)

03.2 RESIDUE-TO-BINARY

04 IMPLEMENTATION OF RESİDUE CODE İN CRYPTOGRAPHY

05 ADVANTAGES AND DISADVANTAGES OF RESIDUE CODES

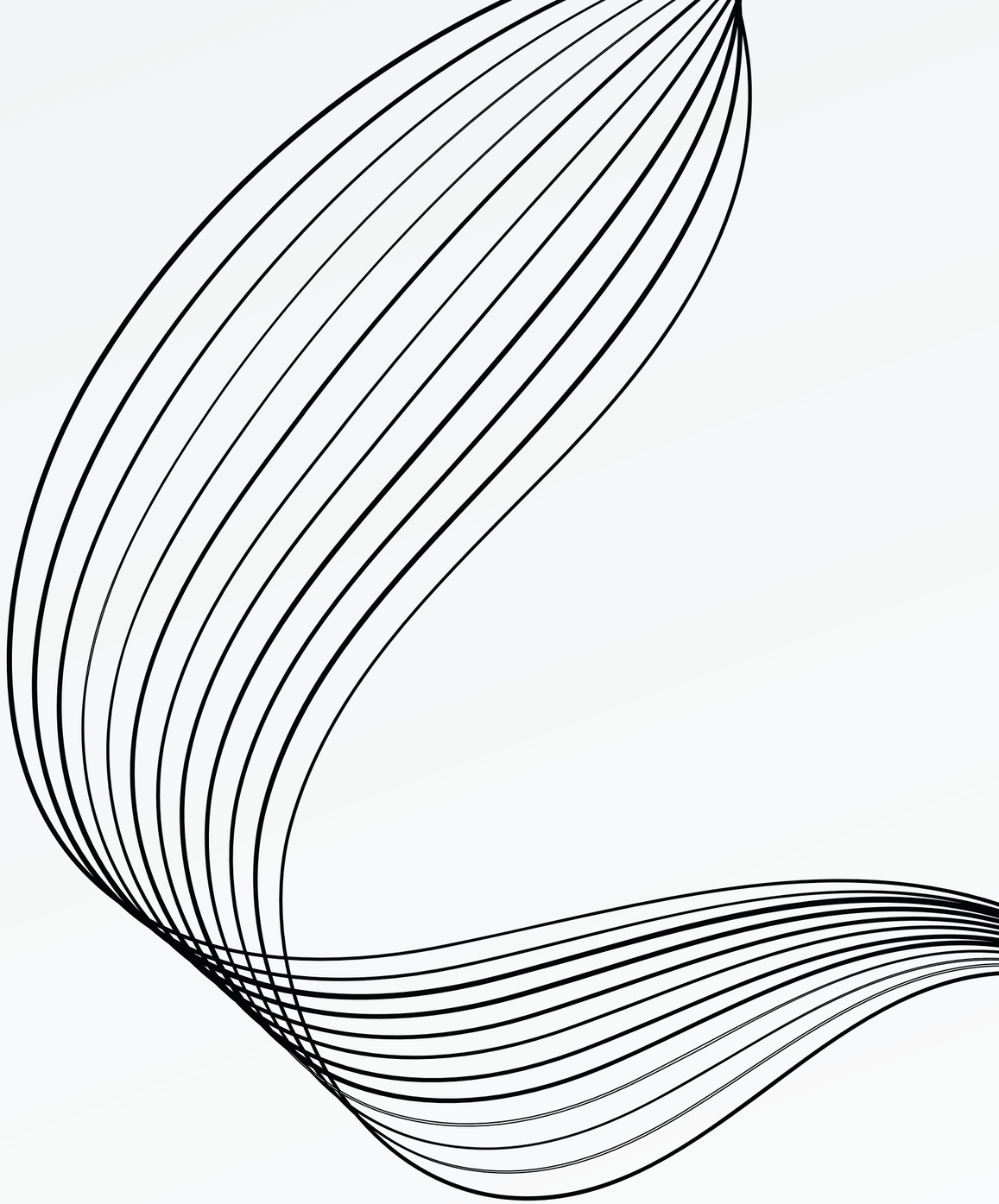
06 CODE PART

WHAT IS IT ?

It is a type of coding system used to check the entirety of a block of data/information and to detect errors. These codes represent a special value of the data block calculated according to a certain algorithm. On the receiver side, receiver can check the accuracy of the received data by calculating this value of the data block.

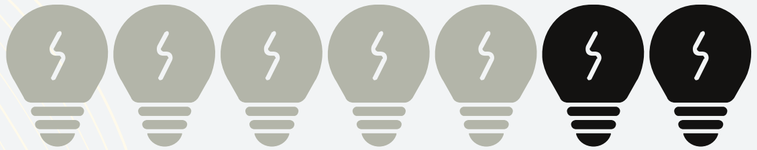
RESIDUE NUMBER SYSTEM

RNS (Residue Number System) uses modular arithmetic to represent numbers across different moduli. In this system, a number is represented as residue values based on the chosen moduli.



In RNS, the moduli are typically chosen to be relatively prime to each other. This ensures that operations performed on each modulus are independent from each other, enabling parallel computations.

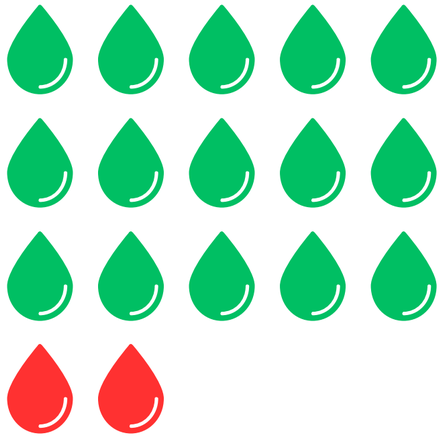
RNS



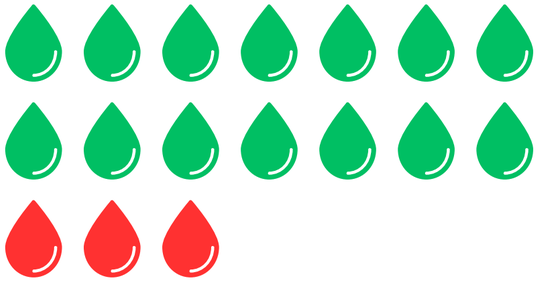
$7 \equiv 2 \pmod 5$

EXAMPLE

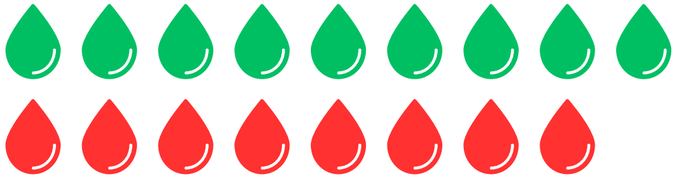
Definition: Let a,b,c ←ℤ with n>0 and a,b,c are relatively prime each other (gcd(a,b,c)=1). Let's say n = 17, a=5, b=7, c=9.



$17 \equiv 2 (\mathrm{mod}\ 5)$



$17 \equiv 3 (\mathrm{mod}\ 7)$



$17 \equiv 8 (\mathrm{mod}\ 9)$

So, in the RNS, the number 17 can be represented as (2, 3, 9) based on the residues obtained for each modulus.

RESIDUE CODE ALGORITHMS

CHINESE REMAINDER THEOREM

RESIDUE-TO-BINARY

CHINESE REMAINDER THEOREM (CRT)

The Chinese Remainder Theorem(CRT) is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime.

CRT CALCULATION

Equations

- $X \equiv a_1 (\text{mod } m_1)$
- $X \equiv a_2 (\text{mod } m_2)$
- $X \equiv a_3 (\text{mod } m_3)$

.

.

.

- $X \equiv a_x (\text{mod } m_x)$

Formula

- Chinese Remainder Theorem (CRT) gives a unique solution for the equations above when the modulis are relatively prime.($GCD(m_1, m_2, m_3 \dots m_x) = 1$)

- $\mathbf{X = (a_1 M_1 (M_1)^{-1} + a_2 M_2 (M_2)^{-1} + \dots + a_x M_x (M_x)^{-1}) Mod\ M}$

EXAMPLE

$X \equiv 2 \pmod 3$
$X \equiv 3 \pmod 5$
$X \equiv 2 \pmod 7$

SOLUTION

$$X = (a_1 M_1 (M_1)^{-1} + a_2 M_2 (M_2)^{-1} + a_3 M_3 (M_3)^{-1}) \text{Mod } M$$

SOLUTION OF EXAMPLE

$$X = (a_1 M_1 (M_1)^{-1} + a_2 M_2 (M_2)^{-1} + a_3 M_3 (M_3)^{-1}) \text{Mod } M$$

Given Data

To Find

$a_1 = 2$	$m_1 = 3$	M_1	$(M_1)^{-1}$	M
$a_2 = 3$	$m_2 = 5$	M_2	$(M_2)^{-1}$	
$a_3 = 2$	$m_3 = 7$	M_3	$(M_3)^{-1}$	

SOLUTION OF EXAMPLE

$M = m_1 * m_2 * m_3$ $M = 3 * 5 * 7$

Given Data To Find

$a_1 = 2$	$m_1 = 3$	M_1	$(M_1)^{-1}$	M=105
$a_2 = 3$	$m_2 = 5$	M_2	$(M_2)^{-1}$	
$a_3 = 2$	$m_3 = 7$	M_3	$(M_3)^{-1}$	

SOLUTION OF EXAMPLE

$M_1 = M / m_1$ $M_2 = M / m_2$ $M_3 = M / m_3$

$M_1 = 115/3$ $M_2 = 115/5$ $M_3 = 115/7$

Given Data

To Find

$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$(M_1)^{-1}$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$(M_2)^{-1}$
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$(M_3)^{-1}$

M=105

SOLUTION OF EXAMPLE

$m_1 = 3$	$M_1 = 35$	$(M_1)^{-1} = 2$
$m_2 = 5$	$M_2 = 21$	$(M_2)^{-1} = 1$
$m_3 = 7$	$M_3 = 15$	$(M_3)^{-1} = 1$

$M_1 \times (M_1)^{-1} = 1 \bmod m_1$

So:

$35 \times (M_1)^{-1} = 1 \bmod 3$

Assume $(M_1)^{-1} = 1,2$ respectively:

- $35 \times 1 \neq 1 \bmod 3$
- $35 \times 2 = 1 \bmod 3$

$(M_1)^{-1} = 2$

$M_2 \times (M_2)^{-1} = 1 \bmod m_2$

So:

$21 \times (M_2)^{-1} = 1 \bmod 5$

Assume $(M_1)^{-1} = 1$:

- $21 \times 1 = 1 \bmod 5$

$(M_2)^{-1} = 1$

$M_3 \times (M_3)^{-1} = 1 \bmod m_3$

So:

$21 \times (M_3)^{-1} = 1 \bmod 7$

Assume $(M_3)^{-1} = 1$:

- $15 \times 1 = 1 \bmod 7$

$(M_3)^{-1} = 1$

ANSWER

$$X = (a_1 M_1 (M_1)^{-1} + a_2 M_2 (M_2)^{-1} + a_3 M_3 (M_3)^{-1}) \text{Mod } M$$

$a_1 = 2$	$m_1 = 3$	$M_1 = 35$	$(M_1)^{-1} = 2$
$a_2 = 3$	$m_2 = 5$	$M_2 = 21$	$(M_2)^{-1} = 1$
$a_3 = 2$	$m_3 = 7$	$M_3 = 15$	$(M_3)^{-1} = 1$

$M = 105$

$$X = (2*35*2 + 3*21*1 + 2*15*1) \text{Mod } 105$$

Answer

$X \equiv 2 \pmod 3$
$X \equiv 3 \pmod 5$
$X \equiv 2 \pmod 7$

SOLUTION

X =(2*35*2 + 3*21*1 + 2*15*1)Mod 105

X = 233 mod 105

So:

X=23

RESIDUE-TO-BINARY

The conversion of a number from the residue number system to its binary equivalent is known as residue-to-binary conversion.

Residues modulo pairwise coprime integers serve as the building blocks of the residue number system, a nonstandard positional numeral system.

Residue to binary conversion steps

1

DETERMİNE THE MODULİ

Identify the set of pairwise coprime integers used in the residue number system.

2

CALCULATE THE RESİDUES

Divide the given residue number by each modulus and record the remainders.

3

CONVERT RESİDUES TO BİNARY

Convert each residue to its binary representation independently using standard binary conversion techniques like division by 2 or bit shifting.

4

COMBİNE THE BİNARY REPRESENTATİONS

Concatenate the binary representations of each residue to obtain the binary representation of the original residue number.

EXAMPLE

Let's consider a residue number system with two moduli: m1 = 5 and m2 = 7

Suppose we have a residue number with residues :

-r1 = 2 (mod 5)

- r2 = 4 (mod 7)

SOLUTION STEPS

1

Calculate the moduli product:
Compute the product of the moduli, M = m1 * m2 = 5 * 7 = 35.

To find the inverses of the moduli, do the following.
Determine the moduli's inverses in relation to the other modulus.
The inverses of 5 (mod 7) and 7 (mod 5) must be found in this situation.
Find a remainder of 1 when multiplying 5 by various numbers modulo 7 by looking at the remainders.
5*3=1(mod 7).

2

It is possible to find a remainder of 1 by applying the trial-and-error method to multiplying 7 by various numbers and looking at the remainders modulo 5.
5(-1) 3 (mod 7) is the inverse of 5 (mod 7).
7 (mod 5) reversed: 7 (-1) 3 (mod 5).

SOLUTION STEPS

3

Multiplying each residue by the corresponding modulus inverse will yield the residues multiplied by the inverses of the moduli.

For r1 = 2 (mod 5): r1 * 3 ≡ 2 * 3 ≡ 6 (mod 35)

For r2 = 4 (mod 7): r2 * 3 ≡ 4 * 3 ≡ 12 (mod 35)

4

To make the residues binary, follow these steps:.

Create a binary representation of the residues you got in the previous step.

6 (mod 35) ≡ 110 (in binary)

12 (mod 35) ≡ 1100 (in binary)

5

Combine the binary representations as follows.

The binary representations obtained in the previous step should be concatenated.

The original residue number is represented in binary as 1101100.

IMPLEMENTATİON OF RESİDUE CODE İN CRYPTOGRAPHY

Message Integrity

To guarantee the accuracy of transmitted messages, residue codes can be used.
It is possible to determine whether a message has been tampered with during transmission by computing and adding residue values to the message.

Error Detection and Correction

Use the appropriate algorithms based on the selected residue code if error detection or correction is necessary.
Comparing the calculated residue values to the anticipated values allows checksum or parity checks to be carried out for error detection.
Algorithms like Hamming or BCH can be used for error correction to find and fix errors in the residue values.

Integration into Cryptographic Systems:

Include the implementation of the residue code in the overall cryptographic architecture.
To do this, the cryptographic system's data transmission, storage, or computation processes may need to incorporate the encoding, error detection/correction, and decoding processes.

ADVANTAGES AND DİSADVANTAGES OF RESİDUE CODES

Advantages

- Speed and Efficiency
- Error Detection and Correction
- Hardware Utilization
- Security Enhancement

Disadvantages

- Complexity
- Limited Applicability
- Increased Storage Requirements
- Key Management

ADVANTAGES AND DİSADVANTAGES OF RESİDUE CODES

Speed and Efficiency

Compared to traditional binary codes, residue codes provide faster computations. They take advantage of the modularity of the residue number system, enabling distributed computations and parallel processing. This may lead to more effective mathematical operations and cryptographic algorithms.

Complexity

A thorough understanding of the residue number system and its related algorithms is necessary to implement and comprehend residue codes.
The complexity may make maintenance, debugging, and implementation more challenging.
The efficiency of encoding and decoding operations may also be impacted by the addition of computational steps.

ADVANTAGES AND DİSADVANTAGES OF RESİDUE CODES

Error Detection and Correction

Strong error control capabilities are offered by residue codes made for detecting and fixing errors. They have the ability to recognize and fix errors that are introduced into the residue number system's computations or transmissions.

Data integrity and dependability in cryptographic applications are improved by this.

Limited Applicability

Residue codes are created specifically for the residue number system and might not be directly applicable in all cryptographic applications.
When the underlying cryptographic algorithms can take advantage of the advantages of modular arithmetic and make use of the traits of the residue number system, they are most efficient.

OUR TEAM

IBRAHIM
ARDIC

SAMUEL
PORTO

ALIN
SEBASTIAN

REFERENCES

- HTTPS://ARXİV.ORG/ABS/2107.09245
- HTTPS://WWW.NESOACADEMY.ORG/CS/11-CRYPTOGRAPHY-AND-NETWORK-SECURİTY/02-ABSTRACT-ALGEBRA-AND-NUMBER-THEORY/19
- HTTPS://EN.WİKİPEDİA.ORG/WİKİ/QUADRATİC_RESİDUE_CODE
- HTTPS://İACR.ORG/ARCHİVE/CHES2008/51540128/51540128.PDF
- HTTPS://WWW.RESEARCHGATE.NET/PUBLİCATİON/233397710_A_NOVEL_APPROACH_CRYPTOGRAPHY_BY_USİNG_RESİDUE_NUMBER_SYSTEM
- HTTP://WWW.İNSİLİCASE.COM/WEB/CODE.ASPX
- HTTPS:/İETRESEARCH.ONLİNELİBRARY.WİLEY.COM/DOİ/FULL/10.1049/EL.2019.2143