CO-INS:Information and Network Security

Mathematics

Soma Saha (PhD)

Department of Computer Engineering
SGSITS Indore, India

February 25, 2021

Set of Integers

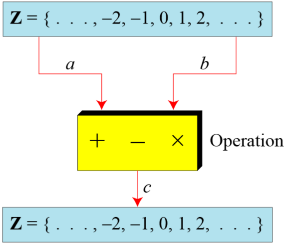
- The set of integers consists of zero (0), the positive natural numbers (1, 2, 3, ...), also called whole numbers or counting numbers, and their additive inverses (the negative integers, i.e., −1, −2, −3, ...).

$$\mathbf{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

Binary Operations on Set of Integers

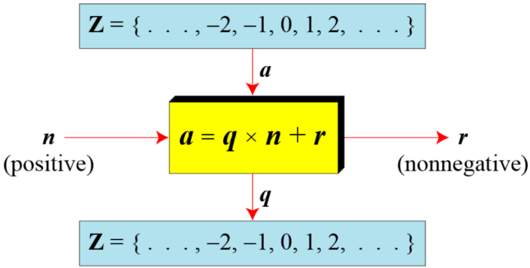
- A binary operation takes two inputs and creates one output.

Figure 1: Three Binary Operations for the set of integers:



Division Operation on Set of Integers

Figure 2: Division Algorithm for Integers.



Division Operation on Set of Integers: Example

- How can we add restriction that remainder **r** will always be **positive**?

$$-255 = (-\mathbf{23} \times 11) + (-\mathbf{2}) \quad \leftrightarrow \quad -255 = (-\mathbf{24} \times 11) + \mathbf{9}$$

Modular Arithmetic

- **The division relationship (a = q x n + r) has two inputs (a and n) and two outputs (q and r). In modular arithmetic, we are interested in only one of the outputs, the remainder r.**

1. Modular Operator
2. Set of Residues
3. Congruence
4. Operations in Z_n
5. Addition and Multiplication Tables
6. Different Sets

Modulo Operator

- The modulo operator is shown as **mod**.
- The second input (n) is called the modulus.
- The output r is called the residue.

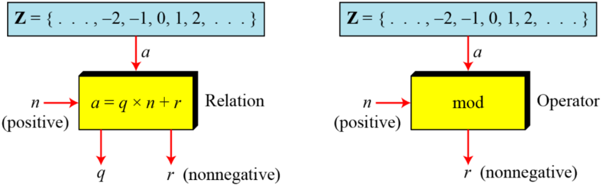


Figure 3: Division Algorithm and Modulo Operator.

Modulo Operator: Examples

- Find the result of the following operations:
  a. 27 mod 5
  b. 36 mod 12
  c. -18 mod 14
  d. -7 mod 10
  e. -36 mod 5
  f. -27 mod 12

Set of Residues: Z_n

- The result of the modulo operation with modulus n is always an integer between 0 and $n - 1$.
- The modulo oueartion creates a set, which in modular arithmetic is referred to as the **set of least residues modulo n,** or z_n.

$$\boxed{\mathbf{Z}_n = \{\ 0, 1, 2, 3, \ \ldots, \ (n-1)\ \}}$$

$$\boxed{\mathbf{Z}_2 = \{\ 0, 1\ \}} \quad \boxed{\mathbf{Z}_6 = \{\ 0, 1, 2, 3, 4, 5\ \}} \quad \boxed{\mathbf{Z}_{11} = \{\ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\ \}}$$

Figure 4: Some Z_n sets

Soma Saha

Congruence

- To show that two integers are congruent, we use the congruence operator ($\equiv$). For example, we write:

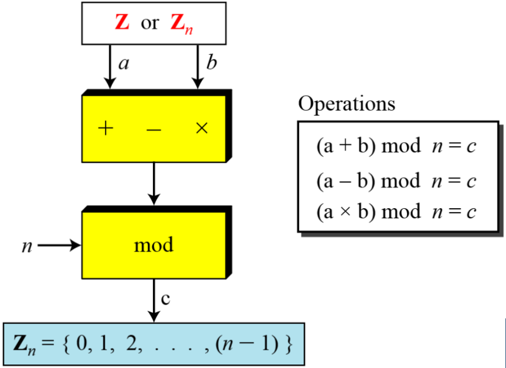
$$2 \equiv 12 \pmod{10} \qquad 13 \equiv 23 \pmod{10}$$
$$3 \equiv 8 \pmod{5} \qquad 8 \equiv 13 \pmod{5}$$

- 2 mod 10 = 2,
- 12 mod 10 = 2,
- 22 mod 10 = 2,

  In modular arithmetic, 2, 12, 22 are called congruent mod 10.

Operations in Z_n

- the three binary operations that we used for the set Z, can also be defined for the set Z_n.
- The result may need to be mapped to Z_n using the mod operator.



Operations in Z_n: Examples..1

- Perform the following operations (the inputs come from Z_n):

a. Add 7 to 14 in Z_{15}.

b. Subtract 11 from 7 in Z_{13}.

c. Multiply 11 by 7 in Z_{20}.

Operations in Z_n: Examples..1

- Perform the following operations (the inputs come from Z_n):

a. Add 7 to 14 in Z_{15}.
b. Subtract 11 from 7 in Z_{13}.
c. Multiply 11 by 7 in Z_{20}.

$$\begin{array}{lcl} (14 + 7) \bmod 15 & \rightarrow & (21) \bmod 15 = 6 \\ (7 - 11) \bmod 13 & \rightarrow & (-4) \bmod 13 = 9 \\ (7 \times 11) \bmod 20 & \rightarrow & (77) \bmod 20 = 17 \end{array}$$

Operations in Z_n: Examples..2

- Perform the following operations (the inputs come from either Z or Z_n):
  a. Add 17 to 27 in Z_{14}.
  b. Subtract 34 from 12 in Z_{13}.
  c. Multiply 123 by -10 in Z_{19}.

Soma Saha

Operations in Z_n: Examples..2

- Perform the following operations (the inputs come from either Z or Z_n):

a. Add 17 to 27 in Z_{14}.
b. Subtract 34 from 12 in Z_{13}.
c. Multiply 123 by -10 in Z_{19}.

---

a. (17 + 27) mod 14 —> (44) mod 14 = 2
b. (12 - 43) mod 13 —> (-31) mod 13 = 8
c. (123 x (-10)) mod 19 —> (-1230) mod 19 = 5

Properties of mod operations for Z_n

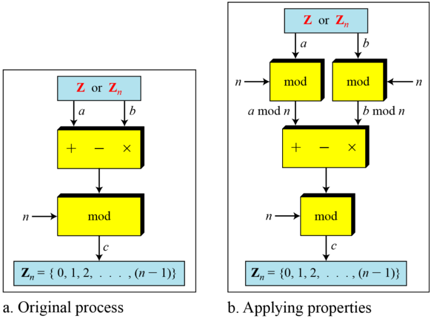
- **The following properties allow us to first map the two inputs to *Zn* (if they are coming from *Z*) before applying the three binary operations (+, -, x).**

First Property: $(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

Second Property: $(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

Third Property: $(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Properties of mod operator



- **The properties allow us to work with smaller/reduced numbers.**

Soma Saha

Application of mentioned properties:

$$(1{,}723{,}345 + 2{,}124{,}945) \bmod 11 = (8 + 9) \bmod 11 = 6$$

$$(1{,}723{,}345 - 2{,}124{,}945) \bmod 16 = (8 - 9) \bmod 11 = 10$$

$$(1{,}723{,}345 \times 2{,}124{,}945) \bmod 16 = (8 \times 9) \bmod 11 = 6$$

Soma Saha

Inverses

- When we are working with modular arithmetic, we often need to find the inverse of a number relative to an operation.
  - Additive Inverse (relative to addition operation).
  - Multiplicative Inverse (relative to multiplication operation)

Additive Inverse

- **In Z_n, two numbers a and b are additive inverses of each other if**

$$a + b \equiv 0 \pmod{n}$$

- In modular arithmetic, each integer has an additive inverse.
- The sum of an integer and its additive inverse is congruent to 0 modulo n.

Additive Inverse: Example

- Find all additive inverse pairs in Z_{10}.

Additive Inverse: Example

- Find all additive inverse pairs in Z_{10}.
- Six pairs: (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), (5, 5).

Multiplicative Inverse

- **In Z_n, two numbers a and b are multiplicative inverses of each other if**

$$a \times b \equiv 1 \pmod{n}$$

- In modular arithmetic, each integer may or may not have a multiplicative inverse.
- When there exists multiplicative inverse for an integer, the product of the integer and the multiplicative inverse is congruent to 1 modulo n.

Multiplicative Inverse: Example

1 Find the multiplicative inverse of 8 in Z_{10}.

Multiplicative Inverse: Example

1 Find the multiplicative inverse of 8 in Z_{10}.

– There is no multiplicative inverse, because gcd(10,8) = $2 \neq 1$. In other words, we cannot find a number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.

2. Find the multiplicative inverses in Z_{10}.

Multiplicative Inverse: Example

1 Find the multiplicative inverse of 8 in Z_{10}.

– There is no multiplicative inverse, because gcd(10,8) = 2 $\neq$ 1. In other words, we cannot find a number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.

2. Find the multiplicative inverses in Z_{10}.

– there are only 3 pairs: (1, 1), (3, 7), and (9, 9). The numbers 0,2,4,5,6, and 8 do not hce a multiplicative inverse. We can see that,
(1x1) mod 10 = 1,
(3x7) mod 10 = 1,
(9x9) mod 10 = 1

- **The integer a in Z_n has a multiplicative inverse if and only if gcd(n, a) $\equiv$ 1 (mod n)**

Soma Saha

Addition and Multiplication Tables

	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Addition Table in $\mathbf{Z}_{10}$

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	0	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Multiplication Table in $\mathbf{Z}_{10}$

Different Sets

- In cryptography, we often work with inverses.
- If the sender uses an integer (as the encryption key), the receiver uses the inverse of that integer (as the decryption key).
- If the operation (encryption/decryption algorithm) is addition, Z_n can be used as the set of possible keys because each integer in this set has an additive integer.
- if the operation (encryption/decryption algorithm) is multiplication, Z_n cannot be the set od possible keys because only some members of this set have a multiplicative inverse.
- We need another set; the new set, which is a subset of Z_n includes only integers in Z_n that have a unique multiplicative inverse. the set is called Z_n*.

Different Sets: Example

Figure 6: Some Z_n and Z_n* sets

$\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$\mathbf{Z}_6^* = \{1, 5\}$

$\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\mathbf{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$\mathbf{Z}_{10}^* = \{1, 3, 7, 9\}$

Bibliography: Books and Resources

- Cryptography and Network Security: Principles and Practice by William Stallings
- Cryptography and Network Security by Behrouz A Forouzan and Debdeep Mukhopadhyay
- Principles of Information Security by Michael E. Whitman and Herbert J. Mattord.
- Cisco platform, and Internet.
- Published research papers, study materials from researchers of security domain.

Soma Saha