# Modular Arithmetic

19CSE311 Computer Security

Jevitha KP
Department of CSE

# Modular Arithmetic

- define **modulo operator** `a mod n` to be remainder when a is divided by n
- use the term **congruence** for: $a \equiv b \bmod n$
  - when divided by *n,* a & b have same remainder
  - eg. 100 = 34 mod 11
- (a mod n) = (b mod n), then **a ≡ b (mod n)**
- b is called the **residue** of **a mod n**
  - since with integers can always write: $a = qn + b$
- usually have $0 <= b <= n-1$

  $-12 \bmod 7 \equiv -5 \bmod 7 \equiv 2 \bmod 7 \equiv 9 \bmod 7$

# Modular Arithmetic

- if $a \equiv 0 \pmod{n}$, then $n \mid a$
- **Properties of congruences**
  - $a \equiv b \pmod{n}$ if $n \mid (a - b)$.
  - $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
  - $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ ==> $a \equiv c \pmod{n}$.

| | | |
|---|---|---|
| $23 \equiv 8 \pmod{5}$ | because | $23 - 8 = 15 = 5 \times 3$ |
| $-11 \equiv 5 \pmod{8}$ | because | $-11 - 5 = -16 = 8 \times (-2)$ |
| $81 \equiv 0 \pmod{27}$ | because | $81 - 0 = 81 = 27 \times 3$ |

# Modular Arithmetic Operations

- The (mod n) operator maps all integers into the set of integers {0, 1, … , (n - 1)}
- Can we perform arithmetic operations within the confines of this set?
- We can; this technique is known as **modular arithmetic**.

# Properties of Modular Arithmetic

- Modular arithmetic exhibits the following properties:
  - **[(a mod n) + (b mod n)] mod n = (a + b) mod n**
  - **[(a mod n) - (b mod n)] mod n = (a - b) mod n**
  - **[(a mod n) * (b mod n)] mod n = (a * b) mod n**

$11 \bmod 8 = 3; 15 \bmod 8 = 7$

$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$

$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$

$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$

$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$

$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$

$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

# Modular Arithmetic

- Exponentiation is performed by repeated multiplication, as in ordinary arithmetic

To find $11^7 \bmod 13$, we can proceed as follows:

$$11^2 = 121 \equiv 4 \pmod{13}$$

$$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$$

$$11^7 = 11 \times 11^2 \times 11^4$$

$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$$

# Modulo 8 Example

- The rules for ordinary arithmetic involving addition, subtraction, and multiplication carry over into modular arithmetic.

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |

(a) Addition modulo 8

# Modulo 8 Example

- The rules for ordinary arithmetic involving addition, subtraction, and multiplication carry over into modular arithmetic.

| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
| 3 | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 |
| 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5 | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |
| 6 | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |
| 7 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

(b) Multiplication modulo 8

# Inverse

- As in ordinary addition, there is an **additive inverse, or negative**, to each integer in modular arithmetic.
- In this case, the negative of an integer x is the integer y such that (x + y) mod 8 = 0.
- To find the additive inverse of an integer in the left-hand column,
  - scan across the corresponding row of the matrix to find the value 0;
  - the integer at the top of that column is the additive inverse;
  - thus, **(2 + 6) mod 8 = 0**
  - **So 6 is the additive inverse of 2, in mod 8**

# Additive Inverse

- As in ordinary addition, there is an **additive inverse, or negative**, to each integer in modular arithmetic.
- In this case, the negative of an integer $x$ is the integer $y$ such that $(x + y) \bmod 8 = 0$.
- To find the additive inverse of an integer in the left-hand column,
  - scan across the corresponding row of the matrix to find the value 0;
  - the integer at the top of that column is the additive inverse;
  - thus, **$(2 + 6) \bmod 8 = 0$**
  - **So 6 is the additive inverse of 2, in mod 8**

# Multiplicative Inverse

- In modular arithmetic mod 8, the multiplicative inverse of x is the integer y such that **(x * y) mod 8 = 1 mod 8**.
- Now, to find the multiplicative inverse of an integer from the multiplication table,
  - scan across the matrix in the row for that integer to find the value 1;
  - the integer at the top of that column is the multiplicative inverse;
  - thus, (3 * 3) mod 8 = 1.

# Inverse

| $w$ | $-w$ | $w^{-1}$ |
|---|---|---|
| 0 | 0 | — |
| 1 | 7 | 1 |
| 2 | 6 | — |
| 3 | 5 | 3 |
| 4 | 4 | — |
| 5 | 3 | 5 |
| 6 | 2 | — |
| 7 | 1 | 7 |

(c) Additive and multiplicative inverse modulo 8

# Residue classes mod n

- Define the set $Z_n$ as the set of nonnegative integers less than n:
- $Z_n = \{0, 1, \ldots, (n - 1)\}$
- This is referred to as the **set of residues**, or **residue classes (mod n)**.
- Each integer in $Z_n$ represents a residue class.
- We can label the residue classes (mod n) as [0], [1], [2], … , [n - 1], where
- **$[r] = \{a: a \text{ is an integer}, a \equiv r \pmod{n}\}$**

# Residue class (mod 4)

The residue classes (mod 4) are

$$[0] = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$$
$$[1] = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$$
$$[2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$$
$$[3] = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$$

# Residue class

- Of all the integers in a residue class, the **smallest nonnegative integer** is the one used to represent the residue class.
- Finding the smallest nonnegative integer to which **k is congruent modulo n** is called **reducing k modulo n**.

# Properties of Modular arithmetic for integers in $Z_n$

- If we perform modular arithmetic within $Z_n$, the properties shown hold for integers in $Z_n$.

**Table 2.3** Properties of Modular Arithmetic for Integers in $Z_n$

| Property | Expression |
|---|---|
| Commutative Laws | $(w + x) \bmod n = (x + w) \bmod n$<br>$(w \times x) \bmod n = (x \times w) \bmod n$ |
| Associative Laws | $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$<br>$[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$ |
| Distributive Law | $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$ |
| Identities | $(0 + w) \bmod n = w \bmod n$<br>$(1 \times w) \bmod n = w \bmod n$ |
| Additive Inverse $(-w)$ | For each $w \in Z_n$, there exists a $z$ such that $w + z \equiv 0 \bmod n$ |

# Modular Arithmetic

- Note some peculiarities
  - if `(a+b)≡(a+c) mod n` then `b≡c mod n`

$$\textbf{if } (a + b) \equiv (a + c) \pmod{n} \textbf{ then } b \equiv c \pmod{n} \tag{2.4}$$

$$\boxed{(5 + 23) \equiv (5 + 7) \pmod{8};\ 23 \equiv 7 \pmod{8}}$$

Equation (2.4) is consistent with the existence of an additive inverse. Adding the additive inverse of $a$ to both sides of Equation (2.4), we have

$$((-a) + a + b) \equiv ((-a) + a + c) \pmod{n}$$
$$b \equiv c \pmod{n}$$

# Modular Arithmetic

- Note some peculiarities
  - $(ab) \equiv (ac) \bmod n$ then $b \equiv c \bmod n$ only if $a$ is relatively prime to $n$

$$\textbf{if } (a \times b) \equiv (a \times c) (\text{mod } n) \textbf{ then } b \equiv c (\text{mod } n) \textbf{ if } a \text{ is relatively prime to } n \qquad \textbf{(2.5)}$$

Recall that two integers are **relatively prime** if their only common positive integer factor is 1. Similar to the case of Equation (2.4), we can say that Equation (2.5) is consistent with the existence of a multiplicative inverse. Applying the multiplicative inverse of $a$ to both sides of Equation (2.5), we have

$$((a^{-1})ab) \equiv ((a^{-1})ac)(\text{mod } n)$$
$$b \equiv c(\text{mod } n)$$

# Residue class

To see this, consider an example in which the condition of Equation (2.5) does not hold. The integers 6 and 8 are not relatively prime, since they have the common factor 2. We have the following:

$$6 \times 3 = 18 \equiv 2 (\bmod 8)$$
$$6 \times 7 = 42 \equiv 2 (\bmod 8)$$

Yet $3 \not\equiv 7 \ (\bmod 8)$.

The reason for this result is that for any general modulus n,
a multiplier a that is applied in turn to the integers 0 through (n - 1) will fail to produce a complete set of residues **if a and n have any factors in common**

With $a = 6$ and $n = 8$,

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $Z_8$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Multiply by 6 | 0 | 6 | 12 | 18 | 24 | 30 | 36 | 42 |
| Residues | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |

Because we do not have a complete set of residues when multiplying by 6, more than one integer in $Z_8$ maps into the same residue. Specifically, $6 \times 0 \bmod 8 = 6 \times 4 \bmod 8$; $6 \times 1 \bmod 8 = 6 \times 5 \bmod 8$; and so on. Because this is a many-to-one mapping, there is not a unique inverse to the multiply operation.

However, if we take $a = 5$ and $n = 8$, whose only common factor is 1,

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| $Z_8$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Multiply by 5 | 0 | 5 | 10 | 15 | 20 | 25 | 30 | 35 |
| Residues | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |

The line of residues contains all the integers in $Z_8$, in a different order.

# Multiplicative Inverse

- In general, an integer has a multiplicative inverse in **Zn,** if and only if that integer is relatively prime to n.
- Table below shows that the integers 1, 3, 5, and 7 have a multiplicative inverse in Z8; but 2, 4, and 6 do not.

# Inverse

| $w$ | $-w$ | $w^{-1}$ |
|---|---|---|
| 0 | 0 | — |
| 1 | 7 | 1 |
| 2 | 6 | — |
| 3 | 5 | 3 |
| 4 | 4 | — |
| 5 | 3 | 5 |
| 6 | 2 | — |
| 7 | 1 | 7 |

(c) Additive and multiplicative inverse modulo 8

# Addition Modulo 7 Example

- Z7 = { 0,1,2,3,4,5,6} AInv = {0,6,5,4,3,2,1}

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

# Multiplication Modulo 7 Example

- Z7 = { 0,1,2,3,4,5,6} MInv = {-,1,4,5,2,3,6}

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |