Usage of Modular Arithmetic

Modular arithmetic is very well understood in terms of algorithms for various basic operations. That is one of the reason why we use finite fields (AES) in symmetric key cryptography. Cryptography requires hard problems. Some problems become hard with modular arithmetic. For example, algorithms are easy to compute over all integers but can become hard to compute when you introduce a modular reduction. Similarly with finding roots. Mod-arithmetic is the central mathematical concept in cryptography. Almost any cipher from the Caesar Cipher to the RSA Cipher use it.

There are two types of "mod":

- **The mod function**
- **The (mod) congruence**

Congruent modulo/congruence cryptography

Congruent numbers :
Integers that leave the same remainder when divided by the modulus m are somehow similar, however, not identical. Such numbers are called "congruent". For instance, 1 and 13 and 25 and 37 are congruent mod 12 since they all leave the same remainder when divided by 12.

To show that two integers are congruent, we use the congruence operator (≡).
For example, we write:
(a mod n) ≡ (b mod n)
This written as:
a ≡(b mod n) or b ≡(a mod n)

Example:
- **73 ≡4(mod 23) means:73 mod 23 ≡ 4 mod 23**
- **2 ≡ 12(mod 10)**

- **Is $6 \equiv 11 (\bmod 5)$? Yes, because 6 and 11 both belong to the same congruent/residue class 1 . That is to say when 6 and 11 are divided by 5 the remainder is 1.**
- **Is $7 \equiv 15 (\bmod 5)$? No, because 7 and 15 do not belong to the same congruent/residue class. Seven has a remainder of 2, while 15 has a remainder of 0, therefore 7 is not congruent to $15 (\bmod 5)$. That is $7 \not\equiv 15 (\bmod 5)$**

Set of Residues

The modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or Z_n.

Some Z_n sets

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

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

Properties of Congruence

1. $a \equiv b \pmod n$ if and only if $n|(a-b)$. **Note: (if n divides (a-b)** (Reflexive Property)

Example: a=a(mod n)

a-a/n=0/n

2. $a \equiv b \pmod n$ implies $b \equiv a \pmod n$ (Symmetric Property)

Example:12 ≡2 mod 5 **(mod 5 means 0 to n-1 i.e 0,1,2,3,4)**

b ≡a(mod n)

2 ≡12 mod 5

2-12=mod 5

-10= mod 5??? (in this situation add mode value with b-a(if b-a give result –value)until we will get first +ve number)

-10+5+5=0

So,0/5

3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$ (Transitive Property)

Example:

$$\underset{a}{\underset{\downarrow}{24}} \equiv \underset{b}{\underset{\downarrow}{12}} \bmod 3, \quad \underset{b}{\underset{\downarrow}{12}} \equiv \underset{c}{\underset{\downarrow}{6}} \bmod 3, \quad \underset{a}{\underset{\downarrow}{24}} \equiv \underset{c}{\underset{\downarrow}{6}} \bmod 3$$

Which of the following are true?

1. $3 \equiv 3 \pmod{17}$
2. $3 \equiv -3 \pmod{17}$
3. $172 \equiv 177 \pmod{5}$
4. $-13 \equiv 13 \pmod{26}$

Modular Arithmetic Operation properties

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

First property:
(A + B) mod C = (A mod C + B mod C) mod C

Example:

Let **A=14, B=17, C=5**

Let's verify: **(A + B) mod C = (A mod C + B mod C) mod C**
LHS = Left Hand Side of the Equation
RHS = Right Hand Side of the Equation

LHS = (A + B) mod C
LHS = (**14 + 17**) mod 5
LHS = **31** mod 5
LHS = 1
RHS = (A mod C + B mod C) mod C
RHS = (**14 mod 5 + 17 mod 5**) mod 5
RHS = (**4 + 2**) mod 5
RHS = 1
LHS = RHS = 1 **We will prove that (A + B) mod C = (A mod C + B mod C) mod C**

NOTE :
Second Property:
Modular Subtraction
A very similar proof holds for modular subtraction
(A - B) mod C = (A mod C - B mod C) mod C

Third property:
The multiplication property of modular arithmetic:
(A * B) mod C = (A mod C * B mod C) mod C

Example for Multiplication:
Let **A=4, B=7, C=6**
Let's verify: **(A * B)** mod C = (**A mod C** * **B mod C**) mod C
LHS= Left Hand Side of the Equation
RHS= Right Hand Side of the Equation

LHS = **(A * B)** mod C
LHS = **(4 * 7)** mod 6
LHS = **28** mod 6
LHS = **4**

RHS = (**A mod C** * **B mod C**) mod C
RHS = (**4 mod 6** * **7 mod 6**) mod 6
RHS = (**4 * 1**) mod 6
RHS = **4 mod 6**
RHS = **4**
LHS = RHS = 4
We will prove that (A * B) mod C = (A mod C * B mod C) mod C

TASK:

- Determine Whether 17 is congruent to 5 modulo 6, and Whether 24 and 14 are congruent modulo 6.

Solution:

Solution: 17 ≡ 5(mod 6) because 6 divides 17 − 5 = 12 but 24 !≡ 14(mod 6) since 24 − 14 = 10 is not divisible by 6.

Evaluate:

(i) 100 mod 26

(ii) (ii) 126 mod 26 (iii) 13 mod 26 (iv) −5 mod 26 (v) 12+18(mod 9)

Solve:

(i) 5 + 10 mod 26 (ii) 13 − 16 mod 26 (iii) 32 + 46 mod 26

(ii) Add 7 to 14 in Z15.

(iii) Subtract 11 from 7 in Z13.

(iv) Multiply 11 by 7 in Z20.

(v) 3*7(mod 11)

(vi) 7^2 (mod 13) ans 10

Evaluate:

(200+301) mod 11 = (2+4)mod11 = ans 6

(200-301) mod 11 = (2-4)mod11 = ans 9

(200*301) mod 11 = (2*4)mod11 = ans 8