Diffie-Hellman Algorithm

$$[6^5]^4 = [6^4]^5$$

A^B mod C =

((A mod C)^B) mod C

History

- The Diffie-Hellman algorithm was developed by Whitfield Diffie and Martin Hellman in 1976.
- This algorithm was devices not to encrypt the data but to generate same private cryptographic key at both ends so that there is no need to transfer this key from one communication end to another.

Modular Arithmetic

Modular exponentiation

A^B mod C = ((A mod C)^B) mod C

Modular Arithmetic

Modular operator

-29 mod 3 = 1

-14 mod 2 = 0

-4 mod 9 = 5

-17 mod 7 = 4

Modular Arithmetic **Congruence**

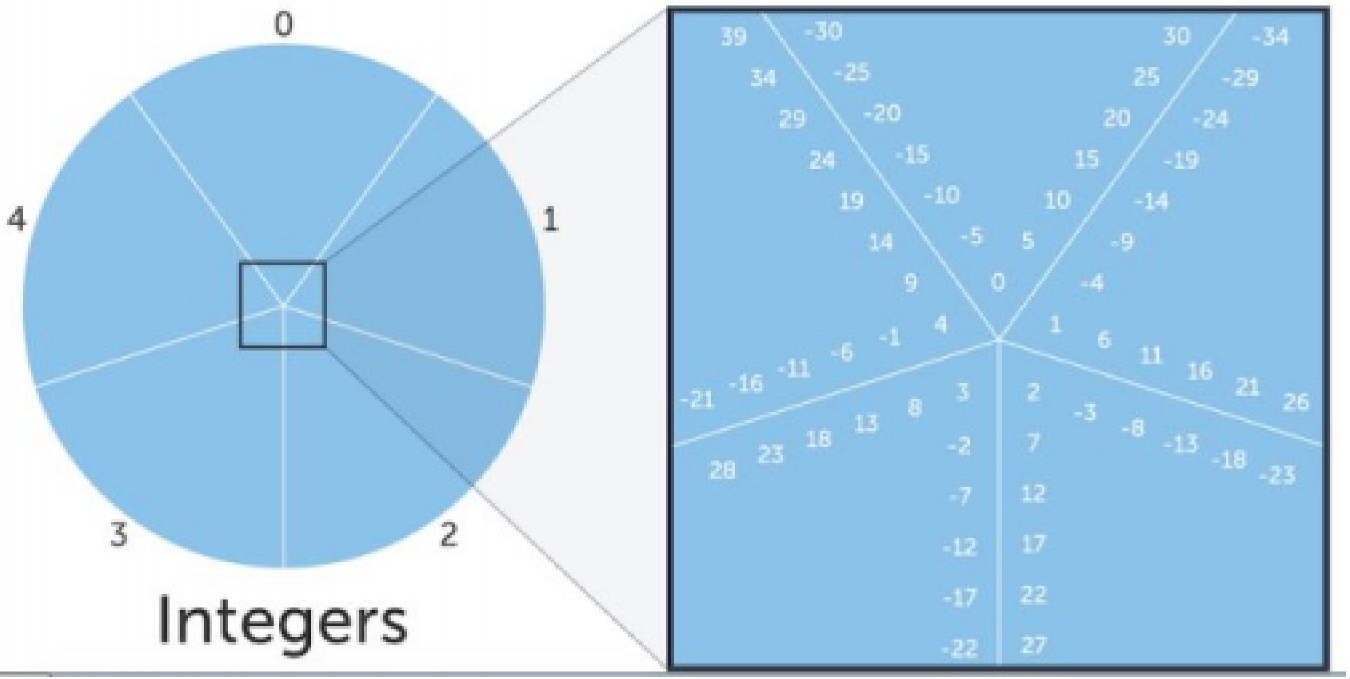
modulo

$$A \equiv B (\mathrm{mod}\ C)$$

This says that A is **congruent** to B modulo C.

Modular Arithmetic **Congruence modulo**

Let's imagine we were calculating mod 5 for all of the integers:



Modular Arithmetic

Congruence modulo

$$A \equiv B \pmod{C}$$

e.g. $26 \equiv 11 \pmod{5}$

$26 \bmod 5 = 1$ so it is in the equivalence class for 1,

$11 \bmod 5 = 1$ so it is in the equivalence class for 1, as well

$\equiv$ is the symbol for congruence, which means the values A and B a

the same **equivalence class**.

Modular Arithmetic

Modular multiplication

$$(A * B) \bmod C = (A \bmod C * B \bmod C) \bmod C$$

Modular Arithmetic **Modular**

addition, subtraction

$$(A + B) \bmod C = (A \bmod C + B \bmod C) \bmod C$$

$$(A - B) \bmod C = (A \bmod C - B \bmod C) \bmod C$$

Modular Arithmetic **Modular inverse**

Example: A=3, C=7

Step 1. Calculate A * B mod C for B values <u>0 through C-1</u>

3 * 0 ≡ 0 (mod 7)

3 * 1 ≡ 3 (mod 7)

3 * 2 ≡ 6 (mod 7)

3 * 3 ≡ 9 ≡ 2 (mod 7)

3 * 4 ≡ 12 ≡ 5 (mod 7)

3 * 5 ≡ 15 (mod 7) ≡ <u>1</u> (mod 7)   <------ FOUND INVERSE!

3 * 6 ≡ 18 (mod 7) ≡ 4 (mod 7)

5 is the modular inverse of 3 mod 7 since 5*3 mod 7 = 1