Yesterday

- On a clock with m hours the answer to any calculation is one of the integers $0, 1, 2, \ldots, m-1$.

- $a \equiv b \mod m$ means $a-b$ is an integer multiple of m

- $\boxed{3^{-1} \equiv 5 \mod 7}$

$\boxed{4^{-1} \equiv 2 \mod 7}$

$\boxed{5^{-1} \equiv 3 \mod 7}$

$\boxed{6^{-1} \equiv 6 \mod 7}$

- Suppose $2a \equiv 1$ and $2b \equiv 1$ mod 7. Then

$a \equiv 1.a \equiv 2b.a \equiv 2a.b \equiv 1.b \equiv b$

$\boxed{3^{-1} \equiv \qquad\qquad \bmod 12}$

3 has no inverse mod 12

- which numbers do have a multiplicative inverse on an m-hour clock.

- How do we find the inverse of say 15 mod 26 ?

i.e. how do we find a number k such that

$$15k \equiv 1 \mod 26 \,?$$

Answer :

Step 1 : use the Euclidean algorithm to find $\gcd(15, 26) = 1$

Step 2 use the output of the algorithm to find $15^{-1} \bmod 26$

$$26 = 1 \times 15 + 11$$

$$15 = 1 \times 11 + 4$$

$$11 = 2 \times 4 + 3$$

$$4 = 1 \times 3 + 1 \leftarrow \gcd(15, 26)$$

$$3 = 3 \times 1 + 0 \leftarrow \text{STOP}$$

$$1 = 4 - (1 \times 3)$$

$$= 4 - 3$$

$$= 4 - (11 - 2 \times 4)$$

$$= 3 \times 4 - 11$$

$$= 3(15 - 11) - 11$$

$$= 3 \times 15 - 4 \times 11$$

$$= 3 \times 15 - 4(26 - 15)$$

$$= 7 \times 15 - 4 \cdot 26$$

$$\equiv 7 \times 15 \mod 26$$

$$\boxed{\text{Hence } 15^{-1} \equiv 7 \mod 26}$$

Second Application

IBAN

$$\underbrace{\text{GB}}_{\text{Country Code}}\ \underbrace{82}_{\text{check digits}}\ \underbrace{\text{WEST}}_{\text{name}}\ \underbrace{123456}_{\text{bank Sort Code}}\ \underbrace{98765432}_{\text{account number.}}$$

There are 3 steps to validating an IBAN:

1) Rearrange

WEST 123456 98765432 GB 82

2) Convert letters to numbers:

A ~ 10, B ~ 11, ..., Z ~ 35

32 14 28 29 123456 98765432 10 11 82

3) Calculate this number on a clock with 97 hours, if the number is 1 mod 97 the IBAN is valid.