Yesterday

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

Since $2 \times 4 \equiv 1 \mod 7$

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

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

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

$6 \equiv 6 \mod 7$

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

$3^{-1} \equiv \quad \mod 12$

3 has no inverse mod 12.

Which numbers have an inverse on a clock with M hours?

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

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

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

Answer :

Step 1 : use the Euclidean algorithm to find

$\gcd(15, 26) = 1$

Step 2 : use the output of the Euclidean algorithm to find $15^{-1} \mod 26$.

STEP 1

$26 = 1 \times 15 + 11$

$15 = 1 \times 11 + 4$

$11 = 2 \times 4 + 3$

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

$3 = 3 \times 1 + 0 \leftarrow$ stop

STEP 2

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

$1 = 4 - (1 \cdot (11 - 2 \cdot 4))$

$= 3 \cdot 4 - 1 \cdot 11$

$= 3(15 - 11) - 1 \cdot 11$

$= -4 \cdot 11 + 3 \cdot 15$

$= -4(26 - 15) + 3 \cdot 15$

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

$\equiv 7 \cdot 15 \mod 26$

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

Second Application

IBAN:

GB 82 WEST 123456 98765432

- GB: country code
- 82: two check digits
- WEST: bank sort code
- 123456: bank sort code
- 98765432: account number

Three steps to validating the IBAN.

1) Rearrange:

WEST 123456 98765432 GB 82

2) Convert letters to numbers

A=10, B=11, C=12, ... Z=35

32 14 28 29 1 2 3 4 5 6 9 8 7 6

5 4 3 2 16 11 82

3) Calculate this number mod 97.
This number must be 1 mod 97
if the IBAN is valid.

But how can we quickly calculate big numbers mod 97 ?

Example Calculate

$4321 \mod 97$

Soln

$$4321 = 4\times1000 + 3\times100 + 2\times10 + 1$$

$$\equiv 4\times10\times3 + 3\times3 + 21 \mod 97$$

$$\equiv 23 + 9 + 21$$

$$\equiv 53 \mod 97$$