Yesterday

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

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

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

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

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

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

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

$5^{-1} \equiv 5 \mod 12$

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

3 has no inverse on a 12-hour clock !!

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

i.e. how do we find a 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 $15^{-1} \mod 26$.

$26 = 1 \times 15 + 11$

$15 = 1 \times 11 + 4$

$11 = 2 \times 4 + 3$

$4 = 1 \times 3 + \boxed{1} = \gcd(26, 15)$

$3 = 3 \times 1 + 0$

This is the Euclidean algorithm.

$1 = 4 - 1 \times 3$

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

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

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

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

$= 3 \cdot 15 - 4 \cdot (26 - 1 \cdot 15)$

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

$\equiv 7 \cdot 15 \mod 26$

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

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 validate an IBAN.

1) Rearranged

WEST 123456 98765432 GB 82

2) Convert letters to numbers

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

32 14 28 29 123456 98765432

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

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

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

$$= 23 + 9 + 21 \mod 97$$

$$= 53 \mod 97$$