Yesterday

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

because $2 \cdot 4 \equiv 1 \mod 7$

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

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

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

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

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

3 has no inverse mod 12

Which numbers have an inverse on a clock with m?

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 $15^{-1} \mod 26$

$26 = 1 \times 15 + 11$ ×

$15 = 1 \times 11 + 4$ ×

$11 = 2 \times 4 + 3$ ×

$4 = 1 \times 3 + 1$ ← gcd(15, 26) ×

$3 = 3 \times 1 + 0$ ← STOP

$$
\begin{aligned}
1 &= 4 - (1 \cdot 3) \\
&= 4 - 3 \\
&= 4 - (11 - 2 \cdot 4) \\
&= 3 \cdot 4 - 11 \\
&= 3(15 - 1 \cdot 11) - 11 \\
&= 3 \cdot 15 - 4 \cdot 11 \\
&= 3 \cdot 15 - 4(26 - 1 \cdot 15) \\
&= 7 \cdot 15 - 4 \cdot 26 \\
&\equiv 7 \cdot 15 \pmod{26}
\end{aligned}
$$

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

Second Applications

IBAN

GB 82 WEST 12 64 56 9 8 7 6 5 4 3 2

- GB: country code
- 82: two check digits
- WEST: name
- 12 64 56: bank sort code
- 9 8 7 6 5 4 3 2: account number

Three steps to validating an IBAN

1) Rearrange

WEST 12 34 56 9 8 7 6 5 4 3 2 1 GB 82

2) Convert letters to integers

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

3214282912345698765432116111 82

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

How can we quickly calculate a big number mod 97?

Example Calculate

$4321 \mod 97$.

Soln

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

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

$$= 23 + 9 + 21$$

$$= 53$$