

## Yesterday

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

- $a \equiv b \pmod{m}$  means  $a-b$  is an integer multiple of  $m$

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

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

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

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

- Suppose  $2a \equiv 1 \pmod{7}$  and  $2b \equiv 1 \pmod{7}$ . Then  $a \equiv 1, a \equiv 2b, a \equiv 2a \cdot b \equiv 1 \cdot b \equiv b$

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

3 has no inverse mod 12

- Which numbers do have a multiplicative inverse on an  $n$ -hour clock.
- How do we find the inverse of say 15 mod 26?  
i.e. how do we find a number  $k$  such that  
 $15k \equiv 1 \pmod{26}$ ?

Answer :

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

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

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

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

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

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

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

---

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

$$= 4 - 3$$

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

$$= 3 \times 4 - 11$$

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

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

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

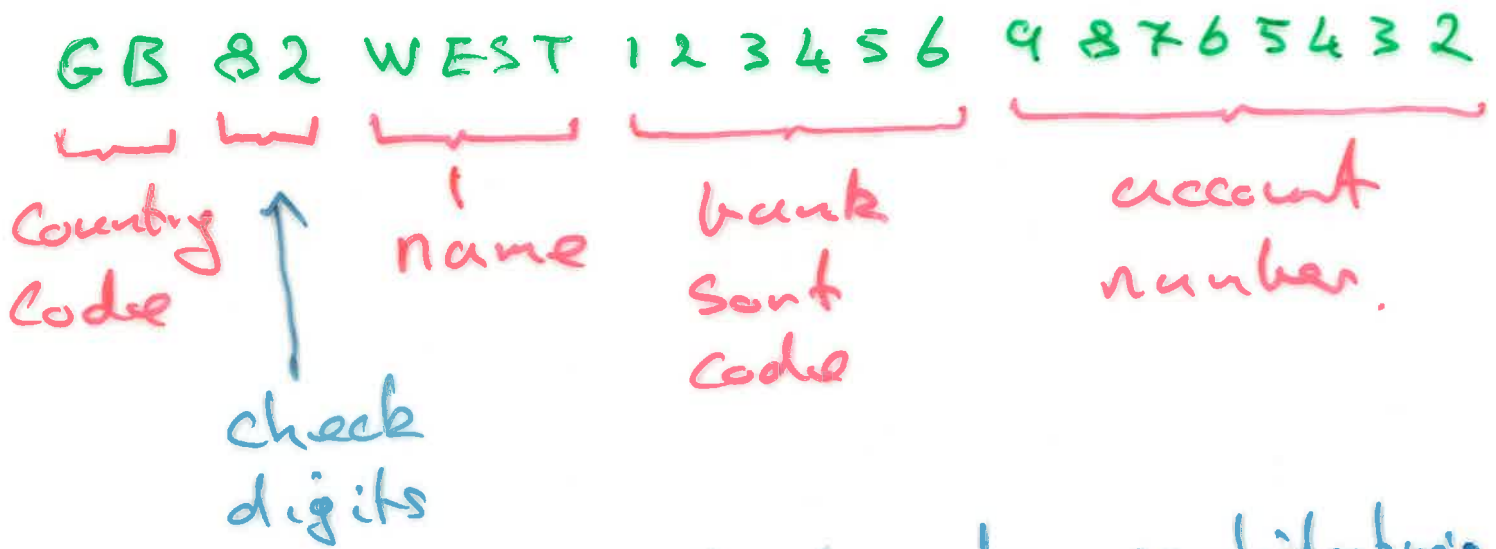
$$= 7 \times 15 - 4 \cdot 26$$

$$\equiv 7 \times 15 \pmod{26}$$

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

# Second Application

## IBAN



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 12 34 56 98765432 10 11 82

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