Modular Arithmetic (1)

- Calculation of the remainder is important.
- **Modular Arithmetic** provides a convenient method to calculate remainders.
- It was systematically studied by Gauss in the end of the 18^{th} century.

Carl Friedrich Gauss (1777-1855)

https://en.wikipedia.org/wiki/Carl_Friedrich_Gauss

Modular Arithmetic (2)

Definition

If A – B is divisible by N, we say

`**A and B are congruent (mod N)**′

or

`**A is congruent to B (mod N)**′.

We write

$$\mathbf{A \equiv B \pmod{N}}.$$

Example

$$2 + 3 \equiv 5 \equiv 0 \pmod{5}$$

$$4 \times 3 \equiv 12 \equiv 2 \pmod{5}$$

Modular Arithmetic (3)

Example

$A \backslash B$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$A + B \pmod 5$

$A \backslash B$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$A \times B \pmod 5$

Modular Arithmetic (4)

Basic Facts:

$$A \equiv B \pmod{N} \quad \text{and} \quad C \equiv D \pmod{N}$$

$$\Rightarrow \quad A + C \equiv B + D \pmod{N},$$

$$A - C \equiv B - D \pmod{N},$$

$$A \times C \equiv B \times D \pmod{N}.$$

- We can perform **addition (+)**, **subtraction (–)**, and **multiplication (×)** in the **(mod N)-world**.

Modular Arithmetic (5)

- $3 \times 2 \equiv 6 \equiv 1 \pmod 5$
  2 is the multiplicative inverse to 3 in the (mod 5)-world.

Theorem: Assume P is a **prime number**.
For $1 \leq A \leq P-1$, there is B satisfying

$$A \times B \equiv 1 \pmod P.$$

B is the **multiplicative inverse** to A (mod P).

Modular Arithmetic (6)

Examples (P=7)

- $1 \times 1 \equiv 1 \pmod 7$

  $\Rightarrow$ 1 is the **multiplicative inverse** to 1.
- $2 \times 4 \equiv 8 \equiv 1 \pmod 7$

  $\Rightarrow$ 2 is inverse to 4, and 4 is inverse to 2.
- $3 \times 5 \equiv 15 \equiv 1 \pmod 7$

  $\Rightarrow$ 3 is inverse to 5, and 5 is inverse to 3.
- $6 \times 6 \equiv 36 \equiv 1 \pmod 7$

  $\Rightarrow$ 6 is inverse to 6.

Modular Arithmetic (7)

Proof of Thm:

$$A \times B \pmod{P} \quad \text{for} \quad B = 1, 2, \cdots, P-1$$

are **not congruent** (mod P) to each other because if

$$A \times B \equiv A \times C \quad \text{for some } 1 \le B, C \le P-1$$

$$\Rightarrow \quad A \times (B - C) \equiv 0$$

$\Rightarrow$ $B - C$ is divisible by P (P is a **prime number**)

$$\Rightarrow \quad B \equiv C.$$

Hence $A \times B \equiv 1$ for some B.

Interlude: Queen of Mathematics

``Math is **the queen of the sciences**, and and number theory is **the queen of math**.”
(Carl Friedrich Gauss, 1777-1855)