Ex: $m = 4$. "$\mathbb{Z}$ mod 4"

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$.

For example

$31 \equiv 3 \pmod 4$

Of course: $31 = 7 \cdot 4 + 3$.

$-23 \equiv 1 \pmod 4$

~~$-23 =$~~ $-23 + 24 = 1$ equivalently $-23 = -6 \cdot 4 + 1$.

Ex: $m = 2$. $\mathbb{Z}_2 = \{0, 1\}$. Eq. cls are evens and odds.

We can do algebra with $\mathbb{Z}_m$.
Think + and ×. Let $a, b, c, m \in \mathbb{Z}$.

$$a+b \equiv c \pmod{m}$$

This means

$$m \mid (a+b-c).$$

For example, $m=8$:

$$12+7 = 19 \equiv 3 \pmod{8}$$

$$12+7 \equiv 3 \pmod{8}$$

Now multiplication:

$$ab \equiv c \pmod{m}$$

This means

$$m \mid (ab - c)$$

Ex: m=5:

$$7 \cdot 4 = 28 \equiv 3 \pmod{5}$$

$$7 \cdot 4 \equiv 3 \pmod{5}$$

Compatibility

$a \equiv a' \pmod{m}$

$b \equiv b' \pmod{m}$

Try to show the following are true yourself!

$$a + b \equiv a' + b' \pmod{m}$$

Idea: $f(x) = g(x) \equiv f(x) + a = g(x) + a$

$$a \cdot b \equiv a' \cdot b' \pmod{m}$$

Some examples $m = 5$

$$37 + 29 \equiv 2 + 4 = 6 \equiv 1 \pmod 5$$

$$37 \equiv 2 \pmod 5$$
$$29 \equiv 4 \pmod 5$$

$$37 \cdot 29 \equiv 2 \cdot 4 \equiv 8 \equiv 3 \pmod 5$$

Modular arithmetic is often much faster than integer arithmetic.

Applications

One application is a sanity check.

These occur in

- bar codes
- ISBNs
- CC numbers
- PPSNs

Sometimes called sum checks.

One algorithm for a sum check we look at is Luhn's algorithm.

Luhn's alg.

$d_n \cdots d_3 d_2 d_1$

where each $d_i \in \{0, \ldots, 9\}$.

1. Add every other digit, starting with the rightmost:

$$d_1 + d_3 + d_5 + \cdots$$

2. Double the intervening digits. If a double value has 2 digits, then add those 2 together.

$$\cdots \quad 2d_6 \quad 2d_4 \quad 2d_2$$

3. Add everything

$$d_1 + \underline{2d_2} + d_3 + \underline{\underline{2d_4}} + \cdots$$

4. The number passes the check if the total S (from (3)) satisfies

$$S \equiv 0 \pmod{10}.$$

Ex:

$$\begin{array}{c} \cdots\ 7\ 6\ 5\ 4\ 3\ 2\ 1 \\ 4907443752756013 \\ \downarrow \qquad 1+2 \\ 8907846712553023 \end{array}$$

$$0 \equiv 8907846712553023 \pmod{10}$$