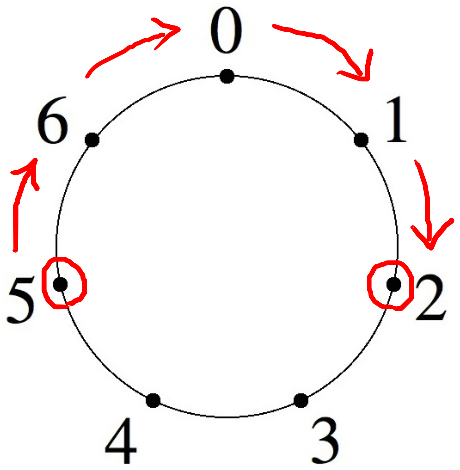
Number system $\mathbb{Z}_7$

Consider the number system $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$. (7 elements in $\mathbb{Z}_7$.)

Computations in $\mathbb{Z}_7$:



$1 + 3 = 4$

$5 + 4 = 2$ (shown on clock)

$2 - 6 = 3$

$3 \cdot 5 = 15 = 0 + 15 = 1$

Terminology. Because $3 \cdot 5 = 1$, we say that 3 and 5 are multiplicative inverses of each other in $\mathbb{Z}_7$.

Analogous to $\frac{1}{5} \cdot 5 = 1$ with real #'s.

Some notations

Be careful of the subtle distinctions:

- $16 \neq 30$ in $\mathbb{Z}$.
- $16 = 30$ in $\mathbb{Z}_7$. (Both equal to 2 in $\mathbb{Z}_7$.)

Notation: The two statements

$$a = b \text{ in } \mathbb{Z}_7 \quad \text{and} \quad a = b \pmod 7$$

mean the same thing.

Problem #4

Example: Let $a = 9876512340 6$ and $b = 98765123476$.

Then $a = b$ in $\mathbb{Z}_7$ because b is 70 more than a.

$a = b$ in $\mathbb{Z}_m$

More generally, let $a, b \in \mathbb{Z}$. Then $a = b$ in $\mathbb{Z}_7$ means...

- the difference between a and b is a multiple of 7, or
- $7 \mid (a - b)$, i.e., 7 is a divisor of the difference $a - b$.

$m \mid (a-b)$

Special case: $a = 0$ in $\mathbb{Z}_7$ means $7 \mid a$ (i.e., $b = 0$).

Note: This property is true in any $\mathbb{Z}_m$. (Replace 7 with m.)

$\times \quad \checkmark \quad \checkmark \quad \times \quad \checkmark \quad \times \quad \times \quad \checkmark \quad \checkmark \quad \times \quad \times \quad \checkmark \quad \times \quad \checkmark \quad \checkmark$

Problem #7: $\mathbb{Z}_{15} = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14\}$.

$12 = -3$

(In $\mathbb{Z}_{15}$: $3 \cdot x = 0, 3, 6, 9, 12 \neq 1$.)

Which elements have multiplicative inverses? $(a \cdot b = 1$ in $\mathbb{Z}_{15}.)$

- $1 \cdot 1 = 1$
- $4 \cdot 4 = 1$
- $11 \cdot 11 = 1$
- $14 \cdot 14 = (-1) \cdot (-1) = 1$
- $2 \cdot 8 = 1$
- $7 \cdot 13 = 1$

Note: 1, 4, 11, 14 are *self-inverses*.

Problem #7: $\mathbb{Z}_{15} = \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14\}$.

Elements with multiplicative inverses: 1, 2, 4, 7, 8, 11, 13, 14.

Elements without multiplicative inverses: 0, 3, 5, 6, 9, 10, 12.

Observations:

- $\gcd(4, 15) = 1 \implies$ 4 has a multiplicative inverse in $\mathbb{Z}_{15}$.
- $\gcd(6, 15) \neq 1 \implies$ 6 does not have a multiplicative inverse in $\mathbb{Z}_{15}$.

Conjecture: Let $a \in \mathbb{Z}_m$.

- If $\gcd(a, m) = 1$, then a has a multiplicative inverse in $\mathbb{Z}_m$.
- If $\gcd(a, m) \neq 1$, then a does not have a multiplicative inverse in $\mathbb{Z}_m$.