Recall: $U_7 = \{a \in \mathbb{Z}_7 \mid a \text{ has a multiplicative inverse in } \mathbb{Z}_7\}$

$$= \{1, 2, 3, 4, 5, 6\}.$$

- Note that U_7 is a group under multiplication.

Discuss in your group:

(a) Find the order of 2 in U_7.

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 1 \implies |2| = 3 \text{ or } \operatorname{ord}(2) = 3$$

(b) Find the order of 3 in U_7.

$3^1 = 3$ $\quad$ $3^4 = 4$

$3^2 = 2$ $\quad \xrightarrow{\times 3}$ $3^5 = 5$ $\quad \implies |3| = 6$ or $\operatorname{ord}(3) = 6$.

$3^3 = 6$ $\quad \xrightarrow{\times 3}$ $3^6 = 1$

Definition. Let g be an element of a group. The order of g is the *smallest* positive exponent n such that $g^n = \varepsilon$.

Notation. We often write $|g| = n$ or $\operatorname{ord}(g) = n$.

Example. In U_7, we have...

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 1,\ 2^4 = 2,\ 2^5 = 4,\ 2^6 = 1,\ \ldots$$

Thus, $\operatorname{ord}(2) = 3$. (Note that $\operatorname{ord}(2) \neq 6$.)

Problem #2: Suppose $\text{ord}(g) = 6$. $\boxed{\text{For which } k \text{ does } g^k = \varepsilon\text{?}}$

(a) $6 \mid 48$, because $48 = 6 \cdot 8$ (with remainder 0).

Then $g^{48} =$ $g^{6\cdot 8} = (g^6)^8 = \varepsilon^8 = \varepsilon$.

Thus, $g^{48} = \varepsilon$.

(b) $6 \nmid 263$, because $263 = 6 \cdot 43 + 5$ (with remainder $\neq 0$).

Then $g^{263} =$ $g^{6\cdot 43+5} = (g^6)^{43} \cdot g^5 = \varepsilon^{43} \cdot g^5 = g^5$.

But $g^5 \neq \varepsilon$, since $\text{ord}(g) = 6$. Thus, $g^{263} \neq \varepsilon$.

Theorem. Let g a group element with $\operatorname{ord}(g) = n$.
Then $n \mid k$ if and only if $g^k = \varepsilon$.

6

Example: Suppose $\operatorname{ord}(g) = 6$.

- $6 \mid 48 \implies g^{48} = \varepsilon$.
- $6 \nmid 263 \implies g^{263} \neq \varepsilon$.

Key: Only $\operatorname{ord}(g)$ or its multiples satisfy $g^k = \varepsilon$.

We have two implications to prove:

1. If $n \mid k$, then $g^k = \varepsilon$.

Problem #6.

2. If $g^k = \varepsilon$, then $n \mid k$. (Equivalently: If $n \nmid k$, then $g^k \neq \varepsilon$.)

Problem #4: Find the remainder when dividing 263 by 6.

- Elizabeth: $263 = 6 \cdot 42 + 11$, so the remainder is 11.
- Anita: $263 = 6 \cdot 44 + (-1)$, so the remainder is -1.
- **Answer:** $263 = 6 \cdot 43 + 5$, so the remainder is 5. ✓

Theorem (Division algorithm): Let $\overset{263}{a}$ and $\overset{6}{b}$ be integers, with $b \geq 1$. Then there exist $q, r \in \mathbb{Z}$ such that $a = b \cdot q + r$ with $0 \leq r < b$.

Remarks:

- The remainder must be less than the divisor and non-negative.
- This is helpful for showing $n \mid k$.

Theorem. Let g be a group element with $\mathrm{ord}(g) = n$.
If $g^k = \varepsilon$, then $n \mid k$.

Proof know-how: To prove that $n \mid k$...

- First write $k = n \cdot q + r$ with $0 \leq r < n$.
- Then show that $r = 0$ (so that we get $k = n \cdot q$).

Proof outline:

- n is the *smallest positive* integer such that $g^n = \varepsilon$.
- We'll show that $g^r = \varepsilon$, too.
- But $0 \leq r < n$. Thus, r must be zero.

Theorem. Let g be a group element with $\mathrm{ord}(g) = n$. If $g^k = \varepsilon$, then $n \mid k$.

Proof: Assume $g^k = \varepsilon$. We must show that $n \mid k$.

Write $k = n \cdot q + r$ where q, $r \in \mathbb{Z}$ with $\boxed{0 \leq r < n.}$ We'll show $r = 0$.

Since $g^k = \varepsilon$, we have $g^{n \cdot q + r} = \varepsilon$.

[Technical details for you to fill in. Or see the reading.]

Thus, $g^r = \varepsilon$.

But $r < n$ and n is the smallest positive integer such that $g^n = \varepsilon$.

So, r cannot be positive. But $r \geq 0$, and thus $r = 0$. Then, $k = n \cdot q$.

Therefore, $n \mid k$.