Recall: 1 is a *generator* of the additive group $\mathbb{Z}_{12}$, because its sums give all elements in the group.

$$1 = 1$$
$$1 + 1 = 2$$
$$1 + 1 + 1 = 3$$
$$\vdots$$
$$\underbrace{1 + 1 + 1 + \cdots + 1}_{12 \text{ terms}} = 0 \quad \longleftarrow \quad \text{ord}(1) = 12.$$

Definition:
We say that $\mathbb{Z}_{12}$ is *cyclic*, because it has a generator.

Discuss in your group:

(a) Is 2 a generator of $\mathbb{Z}_{12}$? Why or why not? No

(b) Find all the generators of $\mathbb{Z}_{12}$. **Ans:** 1, 5, 7, 11.

(c) Find all the generators of $\mathbb{Z}_{15}$. Do the same for $\mathbb{Z}_{20}$.

(d) What conjecture do you have? Can you *prove* it?

} See Chapter 13.

Consider the multiplicative group

$$U_{13} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}.$$

$$\begin{array}{llll} 2^1 = 2 & 2^4 = 3 & 2^7 = 11 & 2^{10} = 10 \\ 2^2 = 4 & 2^5 = 6 & 2^8 = 9 & 2^{11} = 7 \\ 2^3 = 8 & 2^6 = 12 & 2^9 = 5 & \boxed{2^{12} = 1} \end{array}$$

×2 ×2 ×2 ×2

$\longleftarrow$ $\text{ord}(2) = 12.$

Conclusion: U_{13} is cyclic, with generator 2.

$$U_{13} = \{ 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7 \}$$

$$= \{ 2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11} \}$$

$1 = 2^0 = 2^{12}.$

Let g be a group element $\text{ord}(g) = 12$. Thus, $g^{12} = \varepsilon$.

- $g^{-3} = g^{-3} \cdot \varepsilon = g^{-3} \cdot g^{12} = g^{9}$.
- $g^{197} = g^{12 \cdot 16 + 5} = (g^{12})^{16} \cdot g^{5} = \varepsilon^{16} \cdot g^{5} = g^{5}$.

Key: We can always reduce the *exponent* modulo 12.

Let g be a group element with $\operatorname{ord}(g) = 12$.

Notation: Let $\langle g \rangle$ be the set of *all* integer powers of g, i.e.,

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$$
$$= \{\ldots, g^{-4}, g^{-3}, g^{-2}, g^{-1}, g^0, g^1, g^2, g^3, g^4, \ldots\}$$ (Infinite set?)

ε

- $\langle g \rangle = \{\varepsilon, g^1, g^2, g^3, \ldots, g^{11}\}$, where $\varepsilon = g^0 = g^{12}$.

- The 12 elements in $\langle g \rangle$ are distinct.

  Reason: If $g^8 = g^5$, then $g^3 = \varepsilon$, which contradicts $\operatorname{ord}(g) = 12$.

- $\langle g \rangle$ behaves just like $\mathbb{Z}_{12}$ (e.g., $g^9 \cdot g^7 = g^{9+7} = g^4$).

Theorem: Let g be an element of a group G. Define $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$. Then $\langle g \rangle$ is a subgroup of G.

Proof: Let $\alpha, \beta \in \langle g \rangle$. Thus,

$\alpha = g^k$ and $\beta = g^j$ where $k, j \in \mathbb{Z}$.

Then $\alpha \cdot \beta = g^k \cdot g^j = g^{k+j} \in \langle g \rangle$.

Hence $\langle g \rangle$ is closed.

We have $\varepsilon = g^0 \in \langle g \rangle$.

Lastly, we have $\alpha^{-1} = (g^k)^{-1} = g^{-k} \in \langle g \rangle$.

Thus, $\langle g \rangle$ is a subgroup of G.

Scrap:

✓ 1. closure:

Let $\alpha, \beta \in \langle g \rangle$

$\Rightarrow \alpha = g^k, \beta = g^j$

$\Rightarrow \alpha\beta = g^{k+j} \in \langle g \rangle$

✓ 3. Identity: $\varepsilon = g^0 \in \langle g \rangle$.

✓ 4. Inverses:

$\alpha^{-1} = (g^k)^{-1}$

$= g^{-k} \in \langle g \rangle$