MATH 343 · GROUP THEORY · CHAPTER 4

Cyclic Groups

Properties · Orders of Powers · Classification of Subgroups

Fahd M. Alshammari

Part 1 — What a Cyclic Group Is

GOAL. Study the groups generated by a single element.

- Examples and one instructive non-example
- Theorem 4.1: when two powers of a are equal
- Why $|a| = |\langle a \rangle|$, which retires the notation collision of Chapter 3
- Why $\mathbb{Z}$ and $\mathbb{Z}_n$ are the only cyclic groups there are

Cyclic Groups — the Definition Recalled

From Chapter 3: a group G is **cyclic** if there is $a \in G$ with

$$G = \langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}.$$

Such an a is a **generator** of G.

- Every cyclic group is **Abelian**, since $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$
- A cyclic group may have many generators
- In additive notation a^n means na

The Basic Examples

EXAMPLE. $\mathbb{Z}$ under addition is cyclic. Its generators are exactly 1 and -1.

EXAMPLE. $\mathbb{Z}_n$ under addition modulo n is cyclic, with 1 and $-1 = n - 1$ among its generators. Unlike $\mathbb{Z}$, it may have many more.

EXAMPLE. $\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$. Indeed $\langle 3 \rangle = \{3,6,1,4,7,2,5,0\} = \mathbb{Z}_8$. But 2 is **not** a generator: $\langle 2 \rangle = \{0,2,4,6\}$.

A Cyclic Group and a Non-Example

EXAMPLE. $U(10) = \{1,3,7,9\}$ is cyclic:

$$\langle 3 \rangle = \{3^1, 3^2, 3^3, 3^4\} = \{3,9,7,1\} = U(10),$$

and 7 is also a generator.

NON-EXAMPLE. $U(8) = \{1,3,5,7\}$ is **not** cyclic, because

$$\langle 1 \rangle = \{1\}, \quad \langle 3 \rangle = \{1,3\}, \quad \langle 5 \rangle = \{1,5\}, \quad \langle 7 \rangle = \{1,7\},$$

and none of these is all of $U(8)$.

Theorem 4.1 — When Two Powers Agree

THEOREM 4.1. Let a be an element of a group G.

If a has **infinite order**, then $a^i = a^j$ if and only if $i = j$.

If a has **finite order** n, then

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\},$$

and $a^i = a^j$ if and only if n divides $i - j$.

Proof of Theorem 4.1 — the Infinite Case, and the List

PROOF (INFINITE ORDER). If $a^i = a^j$ then $a^{i-j} = e$. Since no nonzero power of a is the identity, $i - j = 0$.

PROOF (THE LIST). Let $|a| = n$. Certainly $e, a, \ldots, a^{n-1}$ lie in $\langle a \rangle$. Conversely let $a^k \in \langle a \rangle$. By the division algorithm $k = nq + r$ with $0 \leq r < n$, so

$$a^k = a^{nq+r} = (a^n)^q a^r = e\, a^r = a^r.$$

Hence $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$.

Proof of Theorem 4.1 — the Divisibility Criterion

PROOF (CONTINUED). Suppose $a^i = a^j$, so $a^{i-j} = e$. Write $i - j = nq + r$ with $0 \leq r < n$. Then

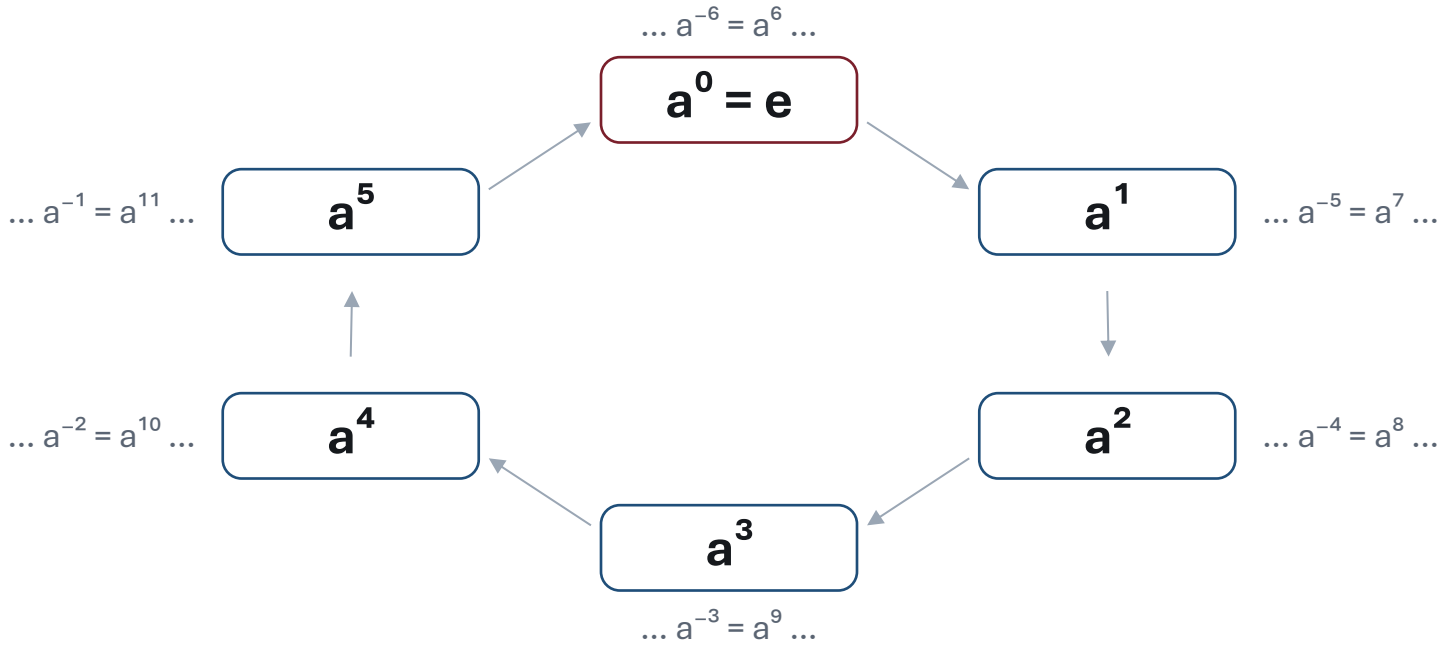
$$e = a^{i-j} = (a^n)^q a^r = a^r.$$

Since n is the **least** positive integer with $a^n = e$, we must have $r = 0$, so $n \mid i - j$.

Conversely, if $i - j = nq$ then $a^{i-j} = (a^n)^q = e$, so $a^i = a^j$.

The Powers of an Element of Order 6

For $|a| = 6$ the distinct powers are e, a, a^2, a^3, a^4, a^5, and every other integer power collapses onto one of these.



Multiplying by a walks one step around the circle; $a^i = a^j$ exactly when 6 divides $i - j$.

Corollary 1 — |a| = |⟨a⟩|

COROLLARY 1. For any group element a,

$$|a| = |\langle a \rangle|.$$

This is why the same notation and the same word are used for both: **they are the same number**.

- If $|a| = n$, the list $e, a, \ldots, a^{n-1}$ has exactly n distinct entries by Theorem 4.1
- If a has infinite order, all powers are distinct and $\langle a \rangle$ is infinite

Corollaries 2 and 3 — When Is a Power the Identity?

COROLLARY 2. For any group element a,

$$a^k = e \Leftrightarrow |a| \text{ divides } k.$$

COROLLARY 3. Equivalently, $a^k = e$ if and only if k is a **multiple** of $|a|$.

PROOF. By Theorem 4.1, $a^k = a^0 = e$ if and only if n divides $k - 0 = k$.

Interactive Exercise — Find the Error

FIND THE ERROR. A student writes: *"If* $a^{12} = e$ *then* $|a| = 12$."

- Always true, sometimes true, or never true?
- If it can fail, give the smallest counterexample
- Repair the statement so that it is correct

Work in pairs — three minutes.

Corollary 4 — The Order of a Product

COROLLARY 4. If a and b belong to a finite group and $ab = ba$, then $|ab|$ divides $|a|\,|b|$.

PROOF. Let $|a| = m$, $|b| = n$. Since a and b commute,

$$(ab)^{mn} = (a^m)^n (b^n)^m = e^n e^m = e,$$

so by Corollary 2, $|ab|$ divides mn.

WARNING. Without commutativity there is **no** relationship at all between $|ab|$ and $|a|, |b|$.

Why Z_n and Z Are the Only Cyclic Groups

Theorem 4.1 says that if $|a| = n$ then

$$a^i a^j = a^k \quad \text{where} \quad k = (i + j) \bmod n.$$

So multiplication in $\langle a \rangle$ **is** addition modulo n, whatever the group G and whatever the element a.

- If a has infinite order, multiplication in $\langle a \rangle$ is addition in $\mathbb{Z}$
- Hence there is essentially **one** cyclic group of each order
- $\mathbb{Z}$ and $\mathbb{Z}_n$ are the prototypes

Part 2 — The Order of a Power

GOAL. Compute $|a^k|$ and identify $\langle a^k \rangle$ knowing only $|a|$ and k.

- Theorem 4.2: $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$
- Four corollaries, ending in a complete description of the generators
- Worked examples where direct computation would be hopeless

Theorem 4.2 — The Order of a Power

THEOREM 4.2. Let a have order n and let k be a positive integer. Then

$$\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle \quad \text{and} \quad |a^k| = \frac{n}{\gcd(n,k)}.$$

Proof of Theorem 4.2 — the Subgroups Agree

PROOF. Write $d = \gcd(n, k)$ and $k = dr$.

One containment. $a^k = \left(a^d\right)^r$, so by closure $\langle a^k \rangle \subseteq \langle a^d \rangle$.

The other. By the gcd theorem (Theorem 0.2) there are integers s, t with $d = ns + kt$. Then

$$a^d = a^{ns+kt} = (a^n)^s \left(a^k\right)^t = e\left(a^k\right)^t \in \langle a^k \rangle,$$

so $\langle a^d \rangle \subseteq \langle a^k \rangle$. Hence $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$.

Proof of Theorem 4.2 — the Order

PROOF (CONTINUED). First, for **any** divisor d of n we show $|a^d| = n/d$:

$$(a^d)^{n/d} = a^n = e \quad \Rightarrow \quad |a^d| \leq n/d,$$

and if $0 < i < n/d$ then $(a^d)^i = a^{di} \neq e$ because $0 < di < n$. So $|a^d| = n/d$.

Applying this with $d = \gcd(n, k)$ and using Corollary 1,

$$|a^k| = |\langle a^k \rangle| = |\langle a^d \rangle| = |a^d| = n/\gcd(n, k).$$

Worked Example: an Element of Order 30

Let $|a| = 30$ .Find $|a^{26}|$, $|a^{17}|$, and $|a^{18}|$.

- $\gcd(30,26) = 2$,so $\langle a^{26} \rangle = \langle a^2 \rangle = \{e, a^2, a^4, \dots, a^{28}\}$ and
$$|a^{26}| = 30/2 = 15.$$
- $\gcd(30,17) = 1$,so $\langle a^{17} \rangle = \langle a \rangle$ and
$$|a^{17}| = 30.$$
- $\gcd(30,18) = 6$,so $\langle a^{18} \rangle = \langle a^6 \rangle = \{e, a^6, a^{12}, a^{18}, a^{24}\}$ and
$$|a^{18}| = 30/6 = 5.$$

Interactive Exercise — Find the Error

FIND THE ERROR(S). A student's solution, with $|a| = 30$:

(i) $\gcd(30,18) = 6,$ so $|a^{18}| = 6.$

(ii) $\gcd(30,25) = 5,$ so $\langle a^{25} \rangle$ has 5 elements.

Two minutes, then we compare.

Worked Example: an Element of Order 1000

Find $|a^{140}|$, $|a^{400}|$, and $|a^{62}|$.

Let $|a| = 1000 = 2^3 5^3$ .Use prime factorizations to get the gcd.

- $\gcd(1000,140) = \gcd(2^3 5^3, 2^2 5 \cdot 7) = 2^2 5 = 20$,so

$$|a^{140}| = 1000/20 = 50.$$

- $\gcd(1000,400) = \gcd(2^3 5^3, 2^4 5^2) = 2^3 5^2 = 200$,so

$$|a^{400}| = 1000/200 = 5.$$

- $\gcd(1000,62) = \gcd(2^3 5^3, 2 \cdot 31) = 2$,so

$$|a^{62}| = 1000/2 = 500.$$

Corollaries 1 and 2 — Comparing Powers

COROLLARY 1. In a finite cyclic group, the order of an element **divides** the order of the group.

COROLLARY 2. Let $|a| = n$. Then

$$\langle a^i \rangle = \langle a^j \rangle \Leftrightarrow \gcd(n, i) = \gcd(n, j),$$

and $\left|a^i\right| = \left|a^j\right|$ under the same condition.

Corollaries 3 and 4 — The Generators

COROLLARY 3. Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $\gcd(n, j) = 1$.

COROLLARY 4. An integer k in $\mathbb{Z}_n$ generates $\mathbb{Z}_n$ if and only if $\gcd(n, k) = 1$.

CONSEQUENCE. Once **one** generator is known, **all** of them are known.

Interactive Exercise — Sort Them

CLASSIFY. Which of $3,\ 4,\ 8,\ 9,\ 15,\ 18$ generate $\mathbb{Z}_{20}$?

- Sort all six by the **criterion** — no listing of elements
- For each non-generator, name $\langle k \rangle$
- How many generators has $\mathbb{Z}_{20}$ in all?

Three minutes in pairs.

The Power of Corollary 3 — Generators of U(50)

Direct computation shows $|U(50)| = 20$ and that 3 is a generator. By Corollary 3, the generators are exactly the 3^j with $\gcd(20, j) = 1$:

j	1	3	7	9	11	13	17	19
$3^j \bmod 50$	3	27	37	33	47	23	13	17

Part 3 — All the Subgroups, and How Many Elements of Each Order

GOAL. Settle the subgroup structure of a cyclic group completely, then count elements by order.

- Theorem 4.3, the **Fundamental Theorem of Cyclic Groups**
- The subgroup lattice of $\mathbb{Z}_{30}$
- The Euler phi function
- Theorem 4.4 and what survives for non-cyclic groups

Theorem 4.3 — Fundamental Theorem of Cyclic Groups

THEOREM 4.3. Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a\rangle| = n$, then the order of any subgroup of $\langle a\rangle$ divides n; and for **each** positive divisor k of n, $\langle a\rangle$ has **exactly one** subgroup of order k, namely

$$\langle a^{n/k}\rangle.$$

What Theorem 4.3 Says, Before the Proof

Suppose $G = \langle a \rangle$ has order 30.

- Parts one and two: every subgroup H has the form $\langle a^{30/k} \rangle$ for some divisor k of 30
- Part three: G has one subgroup of each of the orders

$$1,\ 2,\ 3,\ 5,\ 6,\ 10,\ 15,\ 30$$

and **no others** — eight subgroups, one for each divisor of 30

Interactive Exercise — Build One to Order

CONSTRUCT. Run Theorem 4.3 backwards. Build a cyclic group with exactly:

- **4** subgroups · **3** subgroups · **2** subgroups
- and decide whether **1** is possible

Justify each count without listing the subgroups.

Proof of Theorem 4.3 — Subgroups Are Cyclic

PROOF. Let $G = \langle a \rangle$ and let $H \leq G$. If $H = \{e\}$ it is cyclic, so assume not.

H contains a positive power of a. Every element of H is some a^t; if $t < 0$ then $a^{-t} \in H$ too.

Let m be least positive with $a^m \in H$. By closure $\langle a^m \rangle \subseteq H$. For the reverse, take $b = a^k \in H$ and write $k = mq + r$, $0 \leq r < m$. Then

$$a^r = a^{-mq} a^k \in H,$$

and minimality of m forces $r = 0$, so $b = (a^m)^q \in \langle a^m \rangle$.

Proof of Theorem 4.3 — Exactly One of Each Order

PROOF (CONTINUED). Let $|\langle a\rangle| = n$ and $H \leq \langle a\rangle$. By the previous step and Theorem 4.2, $H = \langle a^m\rangle$ with $m \mid n$ and $|a^m| = n/m$.

Now let k be any positive divisor of n. Then $\left|\langle a^{n/k}\rangle\right| = k$, so a subgroup of order k **exists**.

For **uniqueness**: if $K \leq \langle a\rangle$ has order k, then $K = \langle a^s\rangle$ with $|a^s| = n/s = k$, forcing $s = n/k$ and $K = \langle a^{n/k}\rangle$.

The Eight Subgroups of an Element of Order 30

For $|a| = 30$, the subgroups of $\langle a \rangle$ are exactly the $\langle a^m \rangle$ with $m \mid 30$:

subgroup	elements	order
$\langle a \rangle$	$e, a, a^2, \ldots, a^{29}$	30
$\langle a^2 \rangle$	$e, a^2, a^4, \ldots, a^{28}$	15
$\langle a^3 \rangle$	$e, a^3, a^6, \ldots, a^{27}$	10
$\langle a^5 \rangle$	$e, a^5, a^{10}, a^{15}, a^{20}, a^{25}$	6
$\langle a^6 \rangle$	$e, a^6, a^{12}, a^{18}, a^{24}$	5
$\langle a^{10} \rangle$	e, a^{10}, a^{20}	3
$\langle a^{15} \rangle$	e, a^{15}	2
$\langle a^{30} \rangle$	e	1

The Subgroups of Z_n

COROLLARY. For each positive divisor k of n, the set $\langle n/k \rangle$ is the **unique** subgroup of $\mathbb{Z}_n$ of order k — and these are the only subgroups.

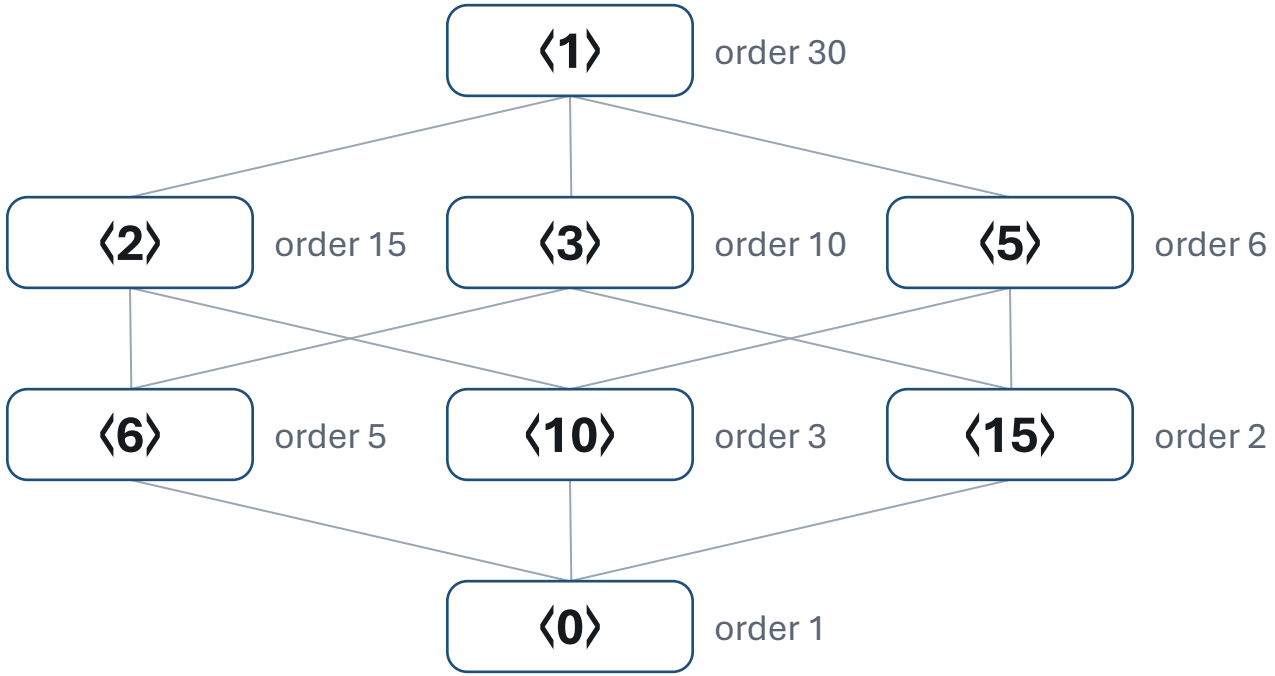
EXAMPLE. The subgroups of $\mathbb{Z}_{30}$ are

$$\langle 1 \rangle,\ \langle 2 \rangle,\ \langle 3 \rangle,\ \langle 5 \rangle,\ \langle 6 \rangle,\ \langle 10 \rangle,\ \langle 15 \rangle,\ \langle 30 \rangle = \{0\},$$

of orders $30,15,10,6,5,3,2,1$ respectively.

The Subgroup Lattice of Z_{30}

A **subgroup lattice** draws every subgroup and joins H up to K exactly when H is a proper subgroup of K.



One subgroup for each divisor of 30 — the divisor lattice, upside down.

Interactive Exercise — Draw the Lattice

BUILD. Draw the subgroup lattice of $\mathbb{Z}_{18}$ on paper.

- Decide the number of nodes **before** you draw
- Label each node with a generator and its order
- Why is the shape different from the $\mathbb{Z}_{30}$ lattice?

Five minutes; one pair draws theirs on the board.

Finding the Generators of a Subgroup

EXAMPLE. To find all generators of the subgroup of order 9 in $\mathbb{Z}_{36}$: one generator is $36/9 = 4$, and by Corollary 3 of Theorem 4.2 the others are the $4j$ with $\gcd(9, j) = 1$:

$$\langle 4 \rangle = \langle 8 \rangle = \langle 16 \rangle = \langle 20 \rangle = \langle 28 \rangle = \langle 32 \rangle.$$

IN GENERAL. Once $a^{n/d}$ generates the subgroup of order d, all its generators are $\left(a^{n/d}\right)^{j}$ with $j \in U(d)$.

The Euler Phi Function

DEFINITION. $\varphi(1) = 1$, and for $n > 1$, $\varphi(n)$ is the number of positive integers less than n and relatively prime to n.

By the definition of $U(n)$, $|U(n)| = \varphi(n)$.

n	1	2	3	4	5	6	7	8	9	10	11	12
ϕ(n)	1	1	2	2	4	2	6	4	6	4	10	4

Theorem 4.4 — Counting Elements by Order

THEOREM 4.4. If d is a positive divisor of n, then a cyclic group of order n has exactly $\varphi(d)$ elements of order d.

PROOF. By Theorem 4.3 the group has exactly one subgroup of order d, say $\langle b \rangle$. Every element of order d generates that subgroup, and by Corollary 3 of Theorem 4.2, b^k generates it precisely when $\gcd(k, d) = 1$. There are $\varphi(d)$ such k.

What Survives for Non-Cyclic Groups

COROLLARY. In **any** finite group, the number of elements of order d is a **multiple** of $\varphi(d)$.

WHY. If there are none, $\varphi(d)$ divides 0. Otherwise take a of order d; $\langle a \rangle$ contributes $\varphi(d)$ of them. If some b of order d lies outside $\langle a \rangle$, then $\langle b \rangle$ contributes another $\varphi(d)$, and the two sets are disjoint — a common element c of order d would give $\langle a \rangle = \langle c \rangle = \langle b \rangle$.

Interactive Exercise — Which Claim Is True?

COMPARE. Let G have order 8. **A.** G has exactly $\varphi(2) = 1$ element of order 2. **B.** The number of such elements is a multiple of $\varphi(2)$.

- Which holds for **every** group of order 8?
- Find a G where the two disagree
- What extra hypothesis would make A true?

Two minutes, then hands up for A or B.

Using Phi to Test Whether U(n) Is Cyclic

EXAMPLE. $\varphi(50) = \varphi(2)\varphi(5^2) = 1 \cdot (25 - 5) = 20$, so $|U(50)| = 20$ and $|3|$ must be $2,4,5,10$ or 20. Since $3^4 = 31$, the order is not 2 or 4; and modulo 50, $3^{10} = 3^5 3^5 \equiv (-7)(-7) = 49$, ruling out 5 and 10. Hence $|3| = 20$ and $U(50) = \langle 3 \rangle$.

A FASTER TEST. For $n > 2$, if $U(n)$ is cyclic it has exactly **one** element of order 2. But $9^2 \equiv 1$ in $U(80)$ and $11^2 \equiv 1$ in $U(120)$, alongside $n - 1$ — so neither is cyclic.

Why Cyclic Groups Matter

- Cyclic groups are a **narrow** class — most groups are not cyclic
- But in Chapter 11 they turn out to be the **BUILDING BLOCKS** of every finite Abelian group, as primes are for integers
- Theorem 4.3 is exceptionally strong: exactly one subgroup per divisor
- Almost nothing that clean survives: D_4 has order 8 with **five** subgroups of order 2 and **three** of order 4

What to Take Away

- $|a| = |\langle a \rangle|$, and $a^k = e$ exactly when $|a|$ divides k
- $\left|a^k\right| = n/\gcd(n,k)$ and $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ — the whole of Part 2 in one line
- a^j generates $\langle a \rangle$ exactly when $\gcd(n,j) = 1$; in $\mathbb{Z}_n$, k generates exactly when $\gcd(n,k) = 1$
- A cyclic group of order n has **one subgroup per divisor** of n, and $\varphi(d)$ elements of order d
- In any finite group the number of elements of order d is a multiple of $\varphi(d)$

Assigned exercises (Ch. 4): 1–7, 9, 16, 21, 27, 32, 35, 43, 45, 51, 61, 65, 66, 67, 69, 76.

Interactive Exercise — All Three Theorems at Once

GENERALISE. Let $\langle a \rangle$ be cyclic of order 36. Without listing any element:

- How many subgroups does $\langle a \rangle$ have?
- What is $\left|a^{20}\right|$, and which subgroup is $\langle a^{20} \rangle$?
- How many elements have order 12? How many generators has that subgroup?

Five minutes; name the result used at each step.