Exercise 1 Cheat Sheet
Multiplicative Groups of $(\mathbb{Z}/n\mathbb{Z})^*$

Recognition

Use this algorithm when asked to:

- Find the order of an element.
- Count elements of order k.
- Find all elements of order k.

If

$$n = pq,$$

then

$$\boxed{(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*}$$

Always split with the Chinese Remainder Theorem (CRT).

Facts

$$|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1, \qquad |(\mathbb{Z}/n\mathbb{Z})^*| = (p-1)(q-1).$$

Each $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

$$\boxed{\text{ord}(x) = \text{lcm}(\text{ord}(x_p), \text{ord}(x_q))}$$

A cyclic group has exactly

$$\boxed{\phi(d)}$$

elements of order d.

(a) Find the Order of a

1. Factor n.

$$n = pq$$

GAP:

```
FactorsInt(n);
```

2. Compute orders modulo each prime.
Since

$$a^{p-1} \equiv 1 \pmod{p},$$

the order divides $p - 1$.
Start with

$$t = p - 1.$$

Factor t.
For every prime divisor r:

$$\boxed{\text{while } a^{t/r} \equiv 1 \pmod{p}, \quad t \leftarrow t/r}$$

Idea: repeatedly shrink the exponent until it cannot be reduced.
Then

$$t = t_p = \text{ord}(a \bmod p).$$

Repeat for q to obtain t_q.
Useful GAP:

```
FactorsInt(p-1);
```

```
PowerMod(a,e,p);
```

```
OrderMod(a,p);
```
(verification)

3. Combine

$$\boxed{\text{ord}(a) = \text{lcm}(t_p, t_q)}$$

GAP:

```
Lcm(tp,tq);
```

(b) Count Elements of Order k

1. List divisors

$$d_1 \mid (p-1), \qquad d_2 \mid (q-1).$$

GAP:

```
DivisorsInt(p-1);
```

```
DivisorsInt(q-1);
```

2. Keep only

$$\boxed{\text{lcm}(d_1, d_2) = k.}$$

3. Count
A cyclic group contributes

$$\phi(d)$$

elements of order d.
Therefore

$$\boxed{\sum_{\text{lcm}(d_1,d_2)=k} \phi(d_1)\phi(d_2)}$$

GAP:

```
Phi(d);
```

(c) Find All Elements of Order k

1. Find valid sub-orders
List

$$d_1 \mid (p-1), \qquad d_2 \mid (q-1),$$

and keep only

$$\boxed{\operatorname{lcm}(d_1, d_2) = k.}$$

2. Find generators
Test small integers $(2, 3, 5, \ldots)$ until one passes:

$$g^{(p-1)/r} \not\equiv 1 \pmod{p}$$

for every prime divisor r of $p-1$.
Repeat for q.
GAP:

```
GeneratorsPrimeResidues(p);
```

3. Build all subgroup elements
For each valid pair (d_1, d_2):

$$a = g_p^{(p-1)/d_1}, \qquad b = g_q^{(q-1)/d_2}.$$

These produce one element of orders d_1 and d_2.
To obtain *all* elements:

$$a^m, \qquad 1 \le m < d_1, \qquad \gcd(m, d_1) = 1,$$

$$b^n, \qquad 1 \le n < d_2, \qquad \gcd(n, d_2) = 1.$$

There are exactly

$$\phi(d_1), \qquad \phi(d_2)$$

such elements.
Manual shortcut:

- List $1, \ldots, d-1$.
- Cross out multiples of every prime factor of d.
- Remaining exponents are exactly the coprime ones.

4. Combine with CRT
For every pair (a^m, b^n) solve

$$x \equiv a^m \pmod{p}, \qquad x \equiv b^n \pmod{q}.$$

Each CRT solution has order k.
GAP:

```
ChineseRem(a,p,b,q);
```

Workflow

$$\boxed{\begin{array}{c}\text{Factor } n\\ \downarrow\\ \text{CRT}\\ \downarrow\\ \begin{cases}(a)\ \text{Find } t_p, t_q \to \text{LCM}\\ (b)\ \text{Divisors} \to \phi(d_1)\phi(d_2)\\ (c)\ \text{Generators} \to g^{(p-1)/d} \to \text{CRT}\end{cases}\end{array}}$$

Common Mistakes

- Never compute the order directly modulo n; split with CRT first.
- Orders combine by **LCM**, never multiplication.
- $\phi(d)$ counts elements of order d only because each $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.
- To obtain *all* elements of order d, use every exponent coprime to d.
- Before counting or constructing elements of order k, verify there exist

  $$d_1 \mid (p-1), \qquad d_2 \mid (q-1)$$

  such that

  $$\text{lcm}(d_1, d_2) = k.$$