

# Cyclicity of $\mathbb{Z}_p^*$

Daochen Wang

November 1, 2025

**Definition 1** (Group). A *group*  $G := (S, \alpha)$  is defined by a set  $S$  and a function  $\alpha: S \times S \rightarrow S$  with the following conditions. (For  $g, h \in S$ , we write  $g \cdot h$  or simply  $gh$  as shorthand for  $\alpha(g, h)$ .)

1. Existence of identity. There exists an  $e \in S$  such that for all  $g \in S$ ,  $ge = eg = g$ .
2. Existence of inverses. For all  $g \in S$ , there exists  $h \in S$  such that  $gh = hg = e$ .
3. Associativity. For all  $g, h, k \in S$ ,  $(gh)k = g(hk)$ . (That is,  $\alpha(\alpha(g, h), k) = \alpha(g, \alpha(h, k))$ .)

The set  $S$  is known as the underlying set of  $G$  and the function  $\alpha$  is known as the group operation of  $G$ . The *order* of  $G$  is the size of the set underlying  $G$  and is denoted  $|G|$ . We say  $G$  is a *finite group* if its order is finite.

If we additionally have  $gh = hg$  for all  $g, h \in S$ , then we say  $G$  is *abelian*.

**Remark 1.** The definition implies: (i) the identity element  $e$  is unique, (ii) for all  $g \in S$ , there exists a unique  $h \in S$  such that  $gh = hg = e$  and we can denote it without ambiguity by  $g^{-1}$ . **Good exercise to check.**

**Example 1.** Our main working example is the group  $\mathbb{Z}_p^*$ , where  $p$  is prime. The underlying set is  $\{1, \dots, p-1\}$  and the group operation is *multiplication* modulo  $p$ . Consider  $\mathbb{Z}_5^*$ : the set is  $\{1, 2, 3, 4\}$  and  $3 \cdot 4 = 2$ ,  $2 \cdot 3 = 1$ ,  $3^{-1} = 2$ , etc. Note that it's not obvious that the existence-of-inverse requirement of a group is satisfied, but it can be shown using Bézout's identity and the assumption that  $p$  is prime. The group is also abelian, since multiplication (modulo  $p$ ) commutes.

**Definition 2** (Subgroup). Let  $G := (S, \alpha)$  be a group. We say  $T \subseteq S$  forms a *subgroup* of  $G$  if:

1.  $T$  contains the identity element of  $G$ .
2.  $T$  is closed under  $\alpha$ , i.e.,  $g, h \in T \implies gh \in T$ .
3.  $T$  contains inverses, i.e.,  $g \in T \implies g^{-1} \in T$ .

This definition means that  $(T, \alpha|_T)$  is a group, where  $\alpha|_T: T \times T \rightarrow T$  is the natural restriction of  $\alpha$  to  $T$  defined by  $\alpha|_T(x, y) = \alpha(x, y)$  for all  $x, y \in T$ . We say  $(T, \alpha|_T)$  is a subgroup of  $G$ . Often the function  $\alpha$  is implicit in which case it is common to abuse language and identify the set  $S$  with the group  $G$  and the set  $T$  with the subgroup  $(T, \alpha|_T)$ . We write  $H \leq G$  to mean  $H$  is a subgroup of  $G$ .

**Definition 3** (Coset). Let  $G$  be a group and  $H$  be a subgroup. A *coset* of  $H$  in  $G$  is a set of the form  $gH := \{gh \mid h \in H\}$ .

**Theorem 1** (Lagrange). *Let  $G$  be a finite group and  $H$  be a subgroup. Then the order of  $H$  divides the order of  $G$ .*

*Proof.* The cosets of  $H$  partition  $G$  and each have size  $|H|$ . □

**Definition 4.** Let  $G$  be a finite group and  $g \in G$ . The *order* of  $g$  in  $G$ , denoted  $o(g)$  or  $\text{ord}(g)$ , is the minimum positive integer  $r$  such that  $g^r = e$ . The *subgroup generated by  $g$* , denoted  $\langle g \rangle$ , is the subgroup formed by the subset  $\{e, g^1, \dots, g^{o(g)-1}\}$ .

**Exercise:** check  $o(g)$  is well-defined and that  $\langle g \rangle$  indeed forms a subgroup.

**Corollary 1.** *Let  $G$  be a finite group and  $g \in G$ , then  $o(g)$  divides  $|G|$ , written  $o(g) \mid |G|$ .*

*Proof.* Follows from Lagrange's theorem because  $\langle g \rangle$  is a subgroup of  $G$  of size  $o(g)$ . □

An immediate corollary of the above is:

**Corollary 2.** *Let  $G$  be a finite group and  $g \in G$ , then  $g^{|G|} = e$ . In particular, this implies Fermat's Little Theorem that for all  $a \in \mathbb{Z}_p^*$ , where  $p$  is prime, we have  $a^{p-1} = 1$ .*

**Definition 5.** Let  $n$  be a positive integer. We write  $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$ . We write  $\mathbb{Z}_n[X]$  for the set of polynomials with coefficients in  $\mathbb{Z}_n$ . Given  $0 \neq P \in \mathbb{Z}_n[X]$ , the degree of  $P$  is defined to be the exponent of the largest power of  $X$  that has a non-zero coefficient. We say  $x \in \mathbb{Z}_n$  is a root of  $P$  if  $P(x) = 0 \pmod n$ .

**Example 2.** The set  $\mathbb{Z}_4[X]$  contains polynomials like  $2X$ ,  $X^3$ , and  $3X^{100} + X^{42} + 1$ , which are of degrees 1, 3, 100, respectively. Note that 2 is a root of  $2X$  and  $X^3$  in  $\mathbb{Z}_4$ ; while  $3X^{100} + X^{42} + 1$  has no roots in  $\mathbb{Z}_4$ . **Why?**

**Proposition 1.** Let  $p$  be prime and  $P \in \mathbb{Z}_p[X]$ . If  $P$  has degree  $d \geq 1$ , then  $P$  has at most  $d$  distinct roots in  $\mathbb{Z}_p$ .

*Proof.* Proof by induction on  $d$ . For  $d = 1$ , the polynomial must be of the form  $P = \alpha X + \beta$  for some  $\alpha, \beta \in \mathbb{Z}_p$  with  $\alpha \neq 0$ . Since  $p$  is prime, this means  $\alpha$  is invertible and the only root to  $P(x) = 0$  is  $-\alpha^{-1}\beta$ . For  $d > 1$ , suppose  $x$  is a root of  $P$ , then use polynomial division to write  $P = (X - x)Q + r$ , where  $Q \in \mathbb{Z}_p[X]$  has degree  $d - 1$  and  $r \in \mathbb{Z}_p$ . Evaluating  $P$  at  $X = x$  shows  $r = 0$ . Thus  $P = (X - x)Q$ . Suppose  $y \in \mathbb{Z}_p$  is a root of  $P$ , then  $(y - x)Q(y) = 0$ , so  $y = x$  or  $Q(y) = 0$  as  $p$  is prime. (This uses the fact that if a prime divides a product of two integers, then it must divide at least one of them.) Therefore, by the inductive hypothesis,  $y$  can take one of at most  $1 + (d - 1) = d$  possible values since  $Q$  has degree  $d - 1$ . This completes the proof.  $\square$

**Remark 2.** Proposition 1 can be false if  $p$  is not prime:

1. The polynomial  $2X \in \mathbb{Z}_4[X]$  has two distinct roots in  $\mathbb{Z}_4$ , namely, 0 and 2.
2. The polynomial  $X^2 - 1 \in \mathbb{Z}_8[X]$  has four distinct roots in  $\mathbb{Z}_8$ , namely, 1, 3, 5, 7.

**Definition 6.** For positive integers  $a, b$ ,  $\text{lcm}(a, b)$  denotes the least common multiple of  $a$  and  $b$ .

**Example 3.**  $\text{lcm}(6, 21) = 42$ .  $\text{lcm}(7, 5) = 35$ .  $\text{lcm}(35, 7) = 35$ .

**Lemma 1.** Let  $G$  be a finite abelian group. Let  $g, h \in G$ . Suppose  $o(g), o(h)$  are coprime, then  $o(gh) = \text{lcm}(o(g), o(h)) = o(g) \cdot o(h)$ .

*Proof.* Since  $o(g)$  and  $o(h)$  are coprime, it directly follows that  $\text{lcm}(o(g), o(h)) = o(g) \cdot o(h)$ . Thus, it suffices to show  $o(gh) = \text{lcm}(o(g), o(h))$ . Write  $k := o(gh)$  and  $\ell := \text{lcm}(o(g), o(h))$ .

For  $k \leq \ell$ : we have

$$\begin{aligned} (gh)^\ell &= g^\ell h^\ell && G \text{ abelian} \\ &= e \cdot e = e && \ell \text{ is a multiple of } o(g) \text{ and } o(h) \end{aligned}$$

so  $k \leq \ell$  by the definition of  $k$  as the order of  $gh$ .

For  $\ell \leq k$ : as above, we have

$$(gh)^k = g^k h^k = e \tag{1}$$

and so

$$x := g^k = (h^{-1})^k \in \langle g \rangle \cap \langle h \rangle \tag{2}$$

Thus, Corollary 1 implies  $o(x) \mid o(g)$  and  $o(x) \mid o(h)$ . But  $o(g)$  and  $o(h)$  are coprime so  $o(x) = 1$ , so  $x = e$ . Therefore, the definition of  $x$  means  $g^k = e = h^k$ . Therefore,  $o(g) \mid k$  and  $o(h) \mid k$  (to see this, list powers of  $g, h$  in a sequence) so  $k$  is a common multiple of  $o(g)$  and  $o(h)$  so  $k \geq \ell$  by the definition of  $\ell$  as the least common multiple.  $\square$

**Remark 3.** The coprimality assumption is crucial in Lemma 1. For example, consider the group  $\mathbb{Z}_2$ , i.e.,  $\{0, 1\}$  under addition modulo 2. Then  $o(1 + 1) = o(0) = 1$  but  $\text{lcm}(o(1), o(1)) = 2$ .

From Lemma 1, we deduce the next proposition. (Based on this StackExchange answer.)

**Proposition 2.** Every finite abelian group  $G$  has an lcm-closed order set. That is, for all  $x, y \in G$ , there exists  $z \in G$  such that

$$o(z) = \text{lcm}(o(x), o(y)). \tag{3}$$

*Proof.* Proof by induction on  $o(x)o(y)$ . If  $o(x)o(y) = 1$ , then we can choose  $z = e$ . Otherwise,  $o(x)o(y) > 1$  and we can wlog factorize<sup>1</sup>

$$o(x) = AP, \quad o(y) = BP', \tag{4}$$

where  $P = p^m > 1$  for some prime  $p$  coprime to  $A, B$ ; and  $P' \mid P$ .

Then

$$o(x^{P'}) = A \quad \text{and} \quad o(y^{P'}) = B \tag{5}$$

By induction there exists  $z$  with  $o(z) = \text{lcm}(A, B)$ .

Now note that  $o(x^A) = P$  and  $P$  is coprime to  $o(z) = \text{lcm}(A, B)$ . Therefore,

$$\begin{aligned} o(x^A z) &= P \cdot \text{lcm}(A, B) && \text{Lemma 1} \\ &= \text{lcm}(AP, BP') && P' \mid P \\ &= \text{lcm}(o(x), o(y)), \end{aligned}$$

as required.  $\square$

<sup>1</sup>Intuition: this pulls out a fixed prime  $p$  from  $o(x)$  and  $o(y)$  as many times as possible. Can wlog assume  $o(x)$  has at least one prime factor  $p$  since  $o(x)o(y) > 1$ , and also that  $p$  appears more times in the prime factorization of  $o(x)$  than in that of  $o(y)$  else can relabel  $x \leftrightarrow y$ .

**Definition 7** (Cyclic groups and generators). Let  $G$  be a finite group, we say  $G$  is *cyclic* if there exists  $g \in G$ , such that  $o(g) = |G|$ . In this case, we call  $g$  a *generator* of  $G$ .

**Theorem 2.** For all  $p$  prime,  $\mathbb{Z}_p^*$  is a cyclic group.

**Example 4.** In  $\mathbb{Z}_5^*$ , we have  $o(1) = 1$ ,  $o(2) = 4$ ,  $o(3) = 4$ ,  $o(4) = 2$ . So 2 and 3 are the only generators.

*Proof.* Let  $\ell$  be the least common multiple of the orders of the elements of  $\mathbb{Z}_p^*$ . By Proposition 2,  $\ell$  must be the order of some element in  $\mathbb{Z}_p^*$ . Thus it suffices to show  $\ell = p - 1$ .

By Corollary 1,  $p - 1$  is a common multiple of the orders of the elements of  $\mathbb{Z}_p^*$ , so  $\ell \leq p - 1$ .

Moreover, the definition of  $\ell$  implies that every element of  $\mathbb{Z}_p^*$  is a root of  $P := X^\ell - 1 \in \mathbb{Z}_p[X]$  in  $\mathbb{Z}_p$ . Since  $P$  is of degree  $\ell$  and  $\mathbb{Z}_p^*$  has  $p - 1$  distinct elements, we must have  $p - 1 \leq \ell$  by Proposition 1.

Hence  $\ell = p - 1$  and the theorem follows. □