Classification of Cyclic Subgroups with the Fundamental Theorem of Cyclic Groups

Larine Ouyang, Bang Tam Ngo, Irene Choi

April 2024

Abstract

Group theory serves as a foundational part of modern mathematics, offering a profound understanding of the structure and relationships of various mathematical systems. This paper delves into the concepts of cyclic group subgroups using the Fundamental Theorem of Cyclic Groups as its cornerstone. Beginning with the definition of groups, subgroups, and cyclic groups, the paper explores their various properties, leveraging them to introduce the Fundamental Theorem of Cyclic Groups, which establishes the uniqueness and cyclical nature of subgroups within cyclic groups. Applying the theoretical framework provided by the Fundamental Theorem of Cyclic Groups, this paper explains further on identifying cyclic groups, overall providing insights into the diverse application of the subgroups of cyclic groups, contributing to a deeper understanding of group theory.

Contents

1. Group

Definition 1.1 (Group)**.** A group is defined as an ordered pair $(G, \star)$, where G is a set and $\star$ is a binary operation on G. $\star$ has to satisfy the three following axioms:

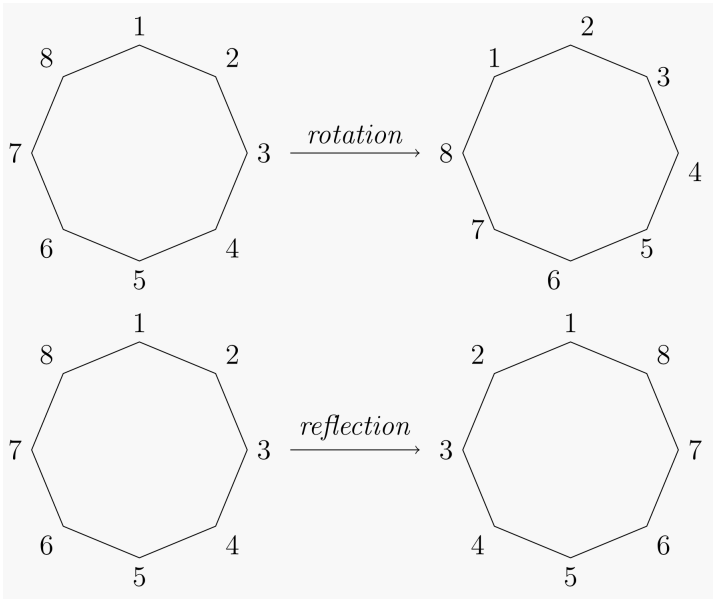
- Associativity: $(a \star b) \star c = a \star (b \star c)$.
- Existence of an identity: $\exists \ \ e \in G$ s.t. $\forall \ \ a \in G$, $a \star e = e \star a = a$.
- Existence of an inverse: $\forall \ \ a \in G$, $\exists \ \ a^{-1} \in G$ s.t. $a \star a^{-1} = a^{-1} \star a = e$.

Lemma 1.1. *Consider a group G under the operation $\star$. Then, the following five propositions are true:*
1. G has a unique identity
2. For all $a \in G$, there exists a^{-1} which is unique
3. For all $a \in G$, $(a^{-1})^{-1} = a$
4. $(a \star b)^{-1} = (b^{-1}) \star (a^{-1})$
5. The General Associative Law: $\forall\ a_1, a_2, ..., a_n \in G$, the value of $a_1 \star a_2 \star ... \star a_n$ is constant no matter how the terms are groups or bracketed.

Example 1.1 (Group $\mathbb{Z}$)**.** *The set of all integers, $\mathbb{Z}$ is a group as it exhibits the characteristics of a group under addition:*
1. The identity of $\mathbb{Z}$ is 0.
2. For all $a \in G$, the inverse is $-a$.
3. For all $a \in G$, $(a^{-1})^{-1} = a$.
4. $(a + b)^{-1} = b^{-1} + a^{-1}$
5. The fact that associativity holds under addition is trivial.

Example 1.2 (Dihedral Groups)**.** *A notable group is the Dihedral Group, denoted as D_n. A dihedral group consists of rotations and reflections in polygons, presented as*

$$D_{2n} = \ \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$



2. Cyclic Groups

In this section, we give the definition of cyclic and some important propositions involving the concept.

Definition 2.1 (Generator of a Group)**.** For a group H, some element x is a generator if $H = \{g^k : k \in \mathbb{Z}\}$.

Definition 2.2 (Cyclic Group)**.** A group H is a cyclic group if there is some element $x \in H$ that is a generator of group H, i.e, $H = \langle x \rangle$

Definition 2.3 (Order of Elements in a Group)**.** The order of an element X of a group H is defined as the least positive integer k, such that $x^k = x \cdot x \cdots x$**(k times)** $= e$, where e is the identity of group H. i.e. $\text{ord}(x) = k$

Lemma 2.1. *For all positive integers, r and $u \in (\mathbb{Z}/p\mathbb{Z})^\times$, define $d = \text{ord}(u)$, then $\text{ord}(u^r) = \frac{d}{\gcd(r,d)}$. We can get the order of u^r from the order of u.*

Proof. Let $m, r \in \mathbb{Z}^+$, $u \in (\mathbb{Z}/p\mathbb{Z})^\times$. Observe, $u^d \equiv 1 \pmod{m}$. Notice, $\text{ord}(u^r)$ must be the smallest $n \in \mathbb{Z}^+$ where $u^{rn} = u^{rn} \equiv 1 \pmod{m}$. As such, $d \mid rn$. We can write $d = d' \gcd(d, r)$, $r = r' \gcd(d, r)$, where $\gcd(d', r') = 1$. As such, $d' \mid r'n \implies d' \mid n$. Notice, $d' = \frac{d}{\gcd(d,r)}$, so $n = \frac{d}{\gcd(d,r)} \cdot k$ for $k \in \mathbb{Z}^+$. The smallest such k is 1, so the smallest n, or $\text{ord}(u^r) = \frac{d}{\gcd(r,d)}$. □

Let's see and example of what is not a cyclic group.

Example 2.1. *$(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic.*

Proof. Note that $(\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$. Because $1 = 3^2 = 5^2 = 7^2$, all elements of $(\mathbb{Z}/8\mathbb{Z})^\times$ have order 2 (except 1, which has order 1). Therefore, since there is no element of $(\mathbb{Z}/8\mathbb{Z})^\times$ with order 4, $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic. □

3. Subgroup

Definition 3.1 (Subgroup)**.** Let G be a group. The subset H of G is a **subgroup** of G if H is nonempty and H is closed under products and inverses (i.e. $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.

Definition 3.2 (Cyclic Subgroup)**.** A subgroup H of a group G is called cyclic if there exists $g \in G$ such that $H = \langle g \rangle = \{g^k : k \in \mathbb{Z}\}$.

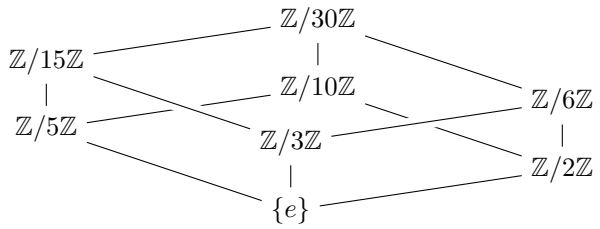
Lemma 3.1 (Uniqueness of the Identity Element in Subgroups)**.** *The identity element of a subgroup H of a group G is the same as the identity element of G.*

Proof. Let e_G denote the identity element of the group G, and suppose e_H is the identity element of the subgroup H. By definition of a subgroup, $H \subseteq G$, and therefore, $e_H \in G$. To show $e_H = e_G$, consider any element $a_H \in H$. Since e_H is the identity element in H, we have: $a_H \cdot e_H = e_H \cdot a_H = a_H$. Also, since H is a subgroup of G, each element in H including its identity must obey the identity laws of G as well. Therefore, for any $a_H \in H$, the group operation with e_G in G gives us: $a_H \cdot e_G = e_G \cdot a_H = a_H$. Now, consider the element a_H^{-1}, which is the inverse of a_H in H. Since H is a subgroup, a_H^{-1} is also an element of H. Hence, we apply the subgroup's identity element: $a_H \cdot a_H^{-1} = e_H$. But since the operation is taking place in G, and inverses and identity elements are consistent in the group, we also have $a_H \cdot a_H^{-1} = e_G$. Therefore, $e_H = e_G$, because the operation of a_H and its inverse gives the same identity element, whether considered within H or G. This shows that the identity element of H is the same as the identity element of G. □

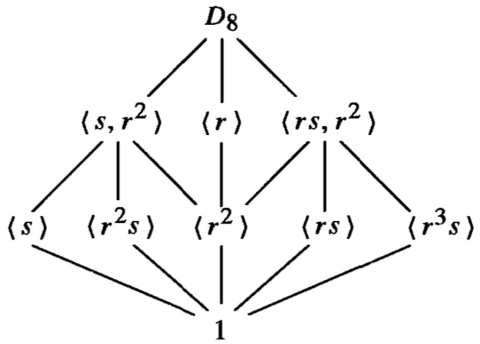
Definition 3.3 (Lattice of Subgroups)**.** The lattice of subgroups of a particular group G has its lattices composed of the subgroups of G. Each lattice is positioned in the following manner:

1. Start at the bottom with the element 1.
2. Ascending, place subgroups in a way such that the orders are continuously increasing until G is reached.
3. Connect any two vertices together if there exists no subgroups between the two.

Example 3.1 (Lattice of $\mathbb{Z}/30\mathbb{Z}$)**.** *The lattice of subgroups of* $\mathbb{Z}/30\mathbb{Z}$*:*



Example 3.2 (Lattice of D_8)**.** *The lattice of* D_8 *is as follows:*



As the rule for plotting the lattice of subgroup mentions, the lattice starts at the bottom with the element 1. Then, notice that the orders of the subgroups at each vertex increases as the lattice ascends, ending at the top with the group D_8*. Further note how the subgroups are connected; the subgroups with no other subgroups between are connected. For instance, between* $\langle r \rangle$ *and* $\langle r^2 \rangle$*, there are no subgroups between, requiring the connection between the two.*

Corollary 3.2.

Lemma 3.3 (Cyclicality of Subgroups of a Cyclic Group)**.** *Let* $G = \langle g \rangle$ *be a cyclic group generated by* g*. If* H *is any subgroup of* G*, then* H *can be written in the form of* $H = \langle g^d \rangle$*.*

Proof. Consider the set $S = \{k \in \mathbb{Z} \mid g^k \in H\}$. Since H is not empty, the set S is non-empty. Let d be the smallest element in set S. We claim that $H = \langle g^d \rangle$. By the division algorithm, any integer k can be expressed as $k = dq + r$ where $0 \leq r < d$. If $g^k \in H$, then $g^k = g^{dq+r} = (g^d)^q \cdot g^r$. Since H is closed under taking inverses and products, $g^{-dq} \in H$ and hence $g^r \in H$. However, by the choice of d as the smallest such integer, r must be zero. Thus, every $g^k \in H$ can be written as $(g^d)^q$, which follows $H = \langle g^d \rangle$. □

Lemma 3.4 (Subgroups Formed by Powers of a Generator)**.** *Let* $G = \langle g \rangle$ *be a cyclic group generated by an element* g *with finite order* n*. If* H *is any subgroup of* G*, then there exists an integer* d *such that* $H = \langle g^d \rangle$*, where the order of* H *divides* n *and* $d \mid n$*.*

Proof. By Definition 3.1, H itself must contain the identity element and be closed under the group operation and taking inverses. By Lemma 3.2, H can be generated by g and can be written in the form $H = \langle g^d \rangle$ for $d \in \mathbb{Z}$. Since $g^n = e$ in G and $g^{kd} \in H$ for any k, there exists$m \in \mathbb{Z}$ s.t. $(g^d)^m = g^{dm} = g^n = e$. Thus, $md = n$, which follows $d \mid n$ and $m \mid n$. □

4. Fundamental Theorem of Cyclic Groups

Definition 4.1 (Fundamental Theorem of Cyclic Groups)**.** Consider a cyclic group $G = \langle g \rangle$ of order n.

1. Every subgroup of G is cyclic.
2. If $\mid G \mid = n$, the order of all subgroups of G divides n.
3. $\forall \ \ k \mid n$, the subgroup $\langle g^{n/k} \rangle$ is a unique subgroup with order k.

Proof. By Lemma 3.3, we've proven that every subgroup of G is cyclic. By Lemma 3.4, we've proven that the order of all subgroups of G divides $|G|$. For subgroup H of G, if $H = \langle g^l \rangle$, by Lemma 3.4, $|H| = \frac{n}{l} = k$, and therefore $l = \frac{n}{k}$. This proves that the subgroup is a unique subgroup with order k. □

5. Applications

5.1. Application 1

Theorem 5.1. *The direct product $\mathbb{Z}_{n1} \times \mathbb{Z}_{n2} \times ... \times \mathbb{Z}_{nk}$ is a cyclic group if and only if the numbers $n1, n2, ..., nk$ are pairwise coprime.*

Proof. We first prove that if the numbers $n_1, n_2, ..., n_k$ are pairwise coprime, then $\mathbb{Z}n_1 \times \mathbb{Z}n_2 \times ... \times \mathbb{Z}_{n_k}$ is cyclic.

Let $m = \text{lcm}(n_1, n_2, ..., n_k)$. Since $n_1, n_2, ..., n_k$ are pairwise coprime, $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Thus, $m = n_1 \cdot n_2 \cdot ... \cdot n_k$. Consider the element $g = (1, 1, ..., 1)$ in $\mathbb{Z}n_1 \times \mathbb{Z}n_2 \times ... \times \mathbb{Z}n_k$. By the Chinese Remainder Theorem, g generates the entire group, meaning every element in $\mathbb{Z}n_1 \times \mathbb{Z}n_2 \times ... \times \mathbb{Z}n_k$ can be expressed as a power of g. Thus, the group is cyclic.

We next prove that if $\mathbb{Z}n_1 \times \mathbb{Z}n_2 \times ... \times \mathbb{Z}_{n_k}$ is cyclic, then the numbers $n_1, n_2, ..., n_k$ are pairwise coprime.

Let $g = (g_1, ..., g_k)$ be a generator of $\mathbb{Z}n_1 \times ... \times \mathbb{Z}_{n_k}$. Then the order of g must be the order of the group, which is $n_1 \cdot ... \cdot n_k$. Suppose there exists n_i, n_j such that $\gcd(n_i, n_j) = d > 1$. Then the order of the identity element, is $n_1 \cdot ... \cdot n_k / d < n_1 \cdot ... \cdot n_k$, contradicting that g is a generator of the group. $n_1, ..., n_k$ must be pairwise coprime.

□

Definition 5.1 (Chinese Remainder Theorem)**.** Consider two relatively prime integers k and l. $\forall\ m, n \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that

$$x \equiv m \pmod{k}$$
$$x \equiv n \pmod{l}$$

(k and l are coprime.)

5.2. Application 2

Theorem 5.2. *$(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic when $n = 1, 2, 4, p^k, 2p^k$*

Proof. First, we are going to look at the case of prime powers and later we further prove that we only need to look at $(\mathbb{Z}/p\mathbb{Z})^\times$. □

5.2.1. Case for even prime

Lemma 5.3. *$(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic for $n > 2$.*

Proof. In this first case we look at the case where n are the powers of 2. We can find 2 subgroups of order 2. Because cyclic groups all contain distinct elements, there can only be one element, x in it such that x^2 is the equal to the identity element. These subgroups in $(\mathbb{Z}/2^n\mathbb{Z})^\times$ are generated by the elements $2^k - 1$ and $2^{k-1} - 1$

$$\begin{aligned}
&(2^k - 1)^2 \equiv 1 \pmod{2^k} \\
&= (2^k)^2 - 2(2^k) + 1 \equiv 1 \pmod{2^k} \\
&= 1 \equiv 1 \pmod{2^k}
\end{aligned}$$

$$\begin{aligned}
&(2^{k-1} - 1)^2 \equiv 1 \pmod{2^k} \\
&= (2^{k-1})^2 - 2(2^{k-1}) + 1 \equiv 1 \pmod{2^k} \\
&= (2^{2k-2}) - 2^k) + 1 \equiv 1 \pmod{2^k} \\
&= 1 \equiv 1 \pmod{2^k}
\end{aligned}$$

□

5.2.2. Case for odd primes

The proof for this case is slightly irrelevant so you can read it in depth at this later section 5.3, but what came out of this case is the following theorem:

Corollary 5.4 (Cyclicity of $(\mathbb{Z}/p\mathbb{Z})^\times$)**.** *For all $p \in \mathbb{P}$, $k \in \mathbb{Z}$, there exists $u \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that the order of u is $\varphi\left(p^k\right)$.*

Corollary 5.5. *$(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic for $n = 1, 2, 4, p^k, 2p^k$*

Proof. We know that by Chinese Remainder Theorem, $(\mathbb{Z}/n\mathbb{Z})^\times = \prod_{i=0}^{k}(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$. So, all of the 'factors' of $(\mathbb{Z}/n\mathbb{Z})^\times$ must be cyclic as well by the Fundamental Theorem of Cyclic Groups.. By our previous application, no two factors, $(\mathbb{Z}/p_a^{k_a}\mathbb{Z})^\times$ and $(\mathbb{Z}/p_b^{k_b}\mathbb{Z})^\times$, for $a, b \leq i$ can have an even order, as it would imply $\gcd(p_a^{k_a}, p_b^{k_b}) > 1$. We know that $(\mathbb{Z}/p\mathbb{Z})^\times$ has size $\varphi\left(p^k\right) = (p-1)(p^k - 1)$ which is an even number when p is odd. This means that $(\mathbb{Z}/n\mathbb{Z})^\times$ can have at most a factor of one $(\mathbb{Z}/p\mathbb{Z})^\times$ along with some $(\mathbb{Z}/2^n\mathbb{Z})^\times$. We can check that $(\mathbb{Z}/2\mathbb{Z})^\times = 1$, so it is trivial, while $(\mathbb{Z}/4\mathbb{Z})^\times = 1, 3$ has an order of size 2. So the group, $(\mathbb{Z}/n\mathbb{Z})^\times$, is only cyclic when $n = 1, 2, 4, p^k, 2p^k$. □

5.3. Proof for the case of odd prime powers

Lemma 5.6. *For all odd primes, p, $t \in (\mathbb{Z}/p\mathbb{Z})^\times$, there are at most d solutions to $x^d \equiv t \pmod{p^k}$.*

Proof. Let $p \in \mathbb{P}$ where $p \neq 2$, $k, d \in \mathbb{Z}^+$, $t \in (\mathbb{Z}/p\mathbb{Z})^\times$. Suppose for contradiction that there exists a non-empty set $C = \{\, c \in \mathbb{Z}^+ \mid S_c := \{\, s : s^d \equiv t \pmod{p^c} \,\}| > d \,\}$. Then, by the Well-Ordering Principle, there exists a least element $l \in C$ such that, $l > 1$. Consider $l - 1$ which is in $\mathbb{Z}^+$ but not in C, so $|S_{l-1} := \{\, s : s^d \equiv t \pmod{p^{l-1}} \,\}| \leq d$. Take one such s. Consider $x \in S_l$. Since $x^d \equiv t \pmod{p^l}$, $x \equiv s \pmod{p^{l-1}}$, so $x = p^{l-1}m + s$ for some $m \in \mathbb{N}$. Then, $|S_l| = |S_{l-1}| \cdot \#m$ where $\#m$ is the number of distinct

m's possible.
Notice,

$$\begin{aligned} t \equiv x^d &= (p^{l-1}m + s)^d \\ &= \sum_{i=0}^{d} \binom{d}{i} p^{l-1} m^{d-i} s^i \\ &= \sum_{i=0}^{d} \binom{d}{i} s^i m^{d-i} p^{(l-1)(d-i)} \\ &= ds^{d-1}mp^{l-1} + s^d + \sum_{i=0}^{d-2} \binom{d}{i} s^i m^{d-i} p^{(l-1)(d-i)} \\ &\equiv ds^{d-1}mp^{l-1} + s^d \pmod{p^l}. \end{aligned}$$

Note in particular that $p^l \mid p^{(l-1)(d-i)}$, as $(l-1)(d-i) \geq (l-1)(d-(d-2)) = 2(l-1) \geq l$, given that $l > 1$. Since $s^d \equiv t \pmod{p^{l-1}}$, $s^d = p^{l-1}j + t \implies s^d - t = p^{l-1}j$ for some fixed $j \in \mathbb{N}$. By the previous results, we have

$$\begin{aligned} 0 &\equiv ds^{d-1}mp^{l-1} + (s^d - t) \\ &= ds^{d-1}mp^{l-1} + p^{l-1}j \\ &= p^{l-1}ds^{d-1}m + j \pmod{p^l}. \end{aligned}$$

As such, $ds^{d-1}m + j \equiv 0 \pmod{p}$. Since d and s^{d-1} are coprime to p and j is fixed, $\#m = 1$. As such, $|S_l| = |S_{l-1}| \leq d$, which is a contradiction. As such, $C = \varnothing$, so we are done. □

Lemma 5.7. *For all $m \in \mathbb{Z}^+$, $(\mathbb{Z}/p\mathbb{Z})^\times$, define $d = \operatorname{ord}(u)$, $R = \{1, \ldots, d\}$, then there are no distinct $r_1, r_2 \in R$ such that $u^{r_1} = u^{r_2}$.*

Proof. Let $m \in \mathbb{Z}^+$, $u \in (\mathbb{Z}/p\mathbb{Z})^\times$. Suppose for contradiction that $u^{r_1} = u^{r_2}$ for some distinct $r_1, r_2 \in R$. Supposing without loss of generality that $r_1 > r_2$, we have $u^{r_1 - r_2} = 1$. However, since $\max r_1 - r_2 = d - 1 < d$ and $\min r_1 - r_2 = 1 > 0$, this is a contradiction. □

Lemma 5.8. *For all $n \in \mathbb{Z}^+$, $n = \sum_{d \mid n} \varphi(d)$.*

Proof. Let $n \in \mathbb{Z}^+$. Consider the set of ordered pairs $S = \{(1, n), \ldots, (n, n)\}$, the cardinality of which is n. Since for all $a, b \in \mathbb{Z}^+$, $\gcd(a, b) \mid a, b$, each term (i, n) of it may be rewritten as $\gcd(i, n) \cdot (i', n_i') := (\gcd(i, n) \cdot i', \gcd(i, n) \cdot n_i')$ where $\gcd(i', n_i') = 1$, for $i \in \{1, \ldots, n\}$.
We put all ordered pairs of the same scalar factor into one subset. For every $d \mid n$, there is a subset with a scalar factor of d, and there exists no subset whose scalar factor is not a divisor of n. Note further that the cardinality of each subset is $\varphi(n_i') = \varphi\left(\frac{n}{\gcd(i,n)}\right) = \varphi\left(\frac{n}{d}\right)$, where $d \mid n$. As such, $n = \sum_{d \mid n} \varphi\left(\frac{n}{d}\right) = \sum_{d' \mid n} \varphi(d')$. □

Theorem 5.9. *For all $m, d \in \mathbb{Z}^+$, if $d \mid \varphi(m)$ and $m = p^k$ for some odd $p \in \mathbb{P}$, $k \in \mathbb{Z}^+$, then the number of elements in $(\mathbb{Z}/p\mathbb{Z})^\times$ of order d is equal to $\varphi(d)$.*

Proof. Let $m, d \in \mathbb{Z}^+$. Suppose $d \mid \varphi(m)$ and $m = p^k$ for some odd $p \in \mathbb{P}$, $k \in \mathbb{Z}^+$. Define $\delta(d) = |\{u \in (\mathbb{Z}/p\mathbb{Z})^\times \operatorname{ord}(u) = d\}|$. We try to show that $\delta(d) = \varphi(d)$.
We first aim to show that $\delta(d) \leq \varphi(d)$, so we suppose for contradiction that $\delta(d) > \varphi(d)$. Since $\varphi(d) \geq 1$, under this assumption, there is at least one element $u \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order d. By Lemma 2.1, for some $r \in \mathbb{Z}^+$, if $\gcd(r, d) = 1$, $\operatorname{ord}(u^r) = d$. Notice, if $r > d$, $u^r = u^{r \pmod d}$ where $r \pmod d \in \{1, \ldots, d\}$, so there are $\varphi(d)$ many u^r's whose order is d. Since $\delta(d) > \varphi(d)$, there exists some v that cannot be expressed

as a power of u whose order is d.
Consider the set $\{u^1, \ldots, u^d\}$, all of which, by Lemma 5.6, are distinct roots of $x^d = 1$ for $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. Note that the cardinality of the set is d. However, since $v \notin \{u^1, \ldots, u^d\}$ and the order of v is d, there exists an additional root of the polynomial. As such, the number of solutions to $x^d = 1$ is larger than d, which contradicts Proposition **??**. Thus, $\delta(d) \leq \varphi(d)$, so $\varphi(d) = \delta(d) + k_d$ for some $k_d \in \mathbb{N}$.
Notice, since all orders in $(\mathbb{Z}/p\mathbb{Z})^\times$ are divisors of $\varphi(m)$, $\sum_{d \mid \varphi(m)} \delta(d) = |(\mathbb{Z}/p\mathbb{Z})^\times| = \varphi(m)$. By Proposition 5.8, $\varphi(m) = \sum_{d \mid \varphi(m)} \varphi(d)$. As such, $\sum_{d \mid \varphi(m)} \delta(d) = \sum_{d \mid \varphi(m)} \varphi(d) = \sum_{d \mid \varphi(m)} \delta(d) + k_d$. Since all k_d are non-negative, this can only be true if all $k_d = 0$. Thus, $\delta(d) = \varphi(d)$ for all $d \in \mathbb{Z}$ where $d \mid \varphi(m)$. □

Corollary 5.10 (Cyclicity of $(\mathbb{Z}/p\mathbb{Z})^\times$)**.** *For all $p \in \mathbb{P}$, $k \in \mathbb{Z}$, there exists $u \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that the order of u is $\varphi(p^k)$.*

Proof. Let $p \in \mathbb{P}$, $k \in \mathbb{Z}^+$. Then by Theorem 5.9, there are exactly $\varphi(\varphi(p^k))$ of $u \in (\mathbb{Z}/p\mathbb{Z})^\times$ with order $\varphi(p^k)$. Since for all $n \in \mathbb{Z}^+$, $\varphi(n) \geq 1$, we are done. □