WHEN ARE ALL GROUPS OF ORDER n CYCLIC?

KEITH CONRAD

1. Introduction

For a prime number p, every group of order p is cyclic: each element in the group besides the identity has order p by Lagrange's theorem, so the group has a generator. In fact each nonidentity element of the group is a generator.

There are also composite n for which all groups of order n are cyclic, although the proof is not as simple as choosing an arbitrary nonidentity element and expecting it to be a generator. The first such n is 15: every group of order 15 is cyclic. Here is a proof by Jyrki Lahtonen [6]. If G is a group with order 15 then each element of G has order 1, 3, 5, or 15. By the Sylow theorems, G has a unique subgroup of order 3 and a unique subgroup of order 5, so it has 2 elements of order 3, 4 elements of order 5, and of course 1 element of order 1. That leaves $15 - 2 - 4 - 1 = 8$ elements unaccounted for, so they must all have order 15 and any of them is a generator of G. The same argument shows every group of order 35 is cyclic, and more generally every group of order pq where p and q are distinct primes with $p \not\equiv 1 \bmod q$ and $q \not\equiv 1 \bmod p$ is cyclic: the congruences imply there is one p-Sylow subgroup and one q-Sylow subgroup, making the number of elements of order 1, p, or q equal to $1 + (p-1) + (q-1) = p + q - 1$, so the number of remaining elements is $pq - (p+q-1) = (p-1)(q-1)$, which is positive. Each of these remaining elements must have order pq and thus generates the group.

The general question we want to address is: for which positive integers n is every group of order n cyclic? For each n there is a cyclic group of order n, and a group isomorphic to a cyclic group is cyclic, so a more abstract way of posing our question is: for which n are all groups of order n isomorphic? Whatever way the question is formulated, here is the answer.

Theorem 1.1. *For a positive integer n, all groups of order n are cyclic if and only if n is squarefree and, for each pair of distinct primes p and q dividing n, $q \not\equiv 1 \bmod p$.*

A positive integer n fitting the conclusion of Theorem 1.1 is called a *cyclic number*. It vacuously includes 1 and all primes. In Table 1 are the first five cyclic n with 2, 3, and 4 prime factors. The first 61 cyclic n are online at the OEIS: see https://oeis.org/A003277.

2 primes	3 primes	4 primes
$15 = 3 \cdot 5$	$255 = 3 \cdot 5 \cdot 17$	$5865 = 3 \cdot 5 \cdot 17 \cdot 23$
$33 = 3 \cdot 11$	$345 = 3 \cdot 5 \cdot 23$	$7395 = 3 \cdot 5 \cdot 17 \cdot 29$
$35 = 5 \cdot 7$	$435 = 3 \cdot 5 \cdot 29$	$7735 = 5 \cdot 7 \cdot 13 \cdot 17$
$51 = 3 \cdot 17$	$455 = 5 \cdot 7 \cdot 13$	$8645 = 5 \cdot 7 \cdot 13 \cdot 19$
$65 = 5 \cdot 13$	$561 = 3 \cdot 11 \cdot 17$	$10005 = 3 \cdot 5 \cdot 23 \cdot 29$

Table 1. Cyclic numbers with 2, 3, and 4 prime factors.

From the formula for $\varphi(n)$ in terms of the prime factorization of n, the criterion on n in Theorem 1.1 is equivalent to saying

$$(n, \varphi(n)) = 1,$$

which is a convenient way to generate a long list of cyclic numbers using a computer algebra system that knows the φ-function.

Dickson [2] determined in 1905 those n for which all groups of order n are abelian, from which Theorem 1.1 is a consequence. The earliest proof focusing specifically on n for which all groups of order n are cyclic (not just abelian) was given by Szele [8] in 1947.

Proving Theorem 1.1 has two directions:

(1) (necessity) if all groups of order n are cyclic then n is squarefree and $q \not\equiv 1 \bmod p$ for all distinct primes p and q dividing n,
(2) (sufficiency) if n is squarefree and $q \not\equiv 1 \bmod p$ for all distinct primes p and q dividing n then all groups of order n are cyclic.

We will prove necessity in Section 2 and prove sufficiency in two ways in Sections 3 and 4. Other proofs of Theorem 1.1 can be found in the references.

2. Necessity of n being a cyclic number

Assume all groups of order n are cyclic. To prove n is squarefree and $q \not\equiv 1 \bmod p$ for all distinct primes p and q dividing n, we want to show for every other n that there is a noncyclic group of order n. Those other n are either (i) not squarefree or (ii) have a pair of prime factors p and q where $q \equiv 1 \bmod p$ (so $q > p$). In the first case we have $p^2 \mid n$ for some prime p, and in the second case we have $pq \mid n$ where p and q are primes with $q \equiv 1 \bmod p$. The following two examples give us noncyclic groups of order p^2 and pq.

Example 2.1. For each prime p, the group $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$ has order p^2 and is not cyclic since each element has order 1 or p.

Example 2.2. Let p and q be distinct primes with $p < q$ and $q \equiv 1 \bmod p$. The group

$$\mathrm{Aff}(\mathbf{Z}/(q)) = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x \in (\mathbf{Z}/(q))^\times, y \in \mathbf{Z}/(q) \right\}$$

has order $(q-1)q$. Since $p \mid (q-1)$, by Cauchy's theorem $(\mathbf{Z}/(q))^\times$ contains a g with order p. The matrices in $\mathrm{Aff}(\mathbf{Z}/(q))$ with upper-left entry a power of g form a group of order pq:

$$H_{p,q} := \left\{ \begin{pmatrix} g^i & b \\ 0 & 1 \end{pmatrix} : i \in \mathbf{Z}/(p), b \in \mathbf{Z}/(q) \right\}.$$

This group is not cyclic since it is not even abelian: $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} g & 0 \\ 0 & 1 \end{smallmatrix}\right)$ are in $H_{p,q}$ and do not commute, as you can check.

With these examples we can prove all groups of order n are cyclic only when n is a cyclic number.

Proof. If n is divisible by p^2 for some prime p then the group $\mathbf{Z}/(p) \times \mathbf{Z}/(p) \times \mathbf{Z}/(n/p^2)$ has order n and is not cyclic since it has the noncyclic subgroup $\mathbf{Z}/(p) \times \mathbf{Z}/(p)$. If n has distinct prime factors p and q such that $p < q$ and $q \equiv 1 \bmod p$ then the group $H_{p,q} \times \mathbf{Z}/(n/pq)$ has order n and is not cyclic since it has the nonabelian (hence noncyclic) subgroup $H_{p,q}$. $\square$

3. Sufficiency of n being a cyclic number

Now assume that n is a cyclic number: it is squarefree and $q \not\equiv 1 \bmod p$ for all distinct primes p and q dividing n. We want to prove every group of order n is cyclic.

We will use induction on cyclic numbers n. If n is 1 or a prime then certainly all groups of order n are cyclic, so we can assume n is a cyclic number with at least two prime factors and, by induction, that all groups having order equal to a cyclic number less than n are cyclic groups. We want to show every group G of order n is also cyclic. We will assume G of order n is *not* a cyclic group and derive a contradiction. Another way of describing G is as a minimal counterexample: if there is a non-cyclic group having order equal to a cyclic number then there is a *non-cyclic group of least order equal to a cyclic number*, and let G be such a group (so $|G|$ must have at least two prime factors). This group G is not supposed to exist. We will prove it has various properties until we reach a contradiction.

Lemma 3.1. *The group G is not abelian.*

Proof. Suppose G is abelian. Let $|G| = p_1p_2\cdots p_r$ for distinct primes p_i and (by Cauchy's theorem) let $g_i \in G$ have order p_i. Since the g_i's commute and their orders are pairwise relatively prime, the order of the product $g_1\cdots g_r$ is the product of their orders, so $g_1\cdots g_r$ has order $p_1\cdots p_r = |G|$ and thus $g_1\cdots g_r$ generates G, which makes G cyclic, contradicting the defining condition that G is not cyclic. □

Every factor of a cyclic number is cyclic, so all proper subgroups and quotient groups of G are cyclic groups. We will use this multiple times below.

Next we strengthen Lemma 3.1 by showing G is very far from being abelian.

Lemma 3.2. *The group G has a trivial center.*

Proof. Let Z be the center of G, so $Z \lhd G$, and if Z is nontrivial then $|G/Z| < |G|$. Therefore G/Z is cyclic. It is a standard result in group theory that if G/Z is cyclic then G is abelian, so our group G is abelian, which contradicts Lemma 3.1. Thus Z is trivial. □

For $x \in G$, its *centralizer* is $Z(x) = \{g \in G : gx = xg\}$. If $x \neq e$ then $Z(x) \neq G$ since the center of G is trivial by Lemma 3.2. The rest of our argument will use centralizers a lot.

Lemma 3.3. *For nontrivial x in G, if $y \in Z(x)$ and $y \neq e$ then $Z(y) = Z(x)$.*

Proof. Since $Z(x) \neq G$, $Z(x)$ is cyclic and thus abelian. Therefore if $y \in Z(x)$, all elements of $Z(x)$ commute with y, which makes $Z(x) \subset Z(y)$. Now $x \in Z(y)$ and $y \neq e$, so by similar reasoning $Z(y) \subset Z(x)$. □

Lemma 3.4. *For nontrivial x and x' in G, if $Z(x) \neq Z(x')$ then $Z(x) \cap Z(x') = \{e\}$.*

Proof. We prove the contrapositive. If $Z(x) \cap Z(x') \neq \{e\}$, let y be a non-identity element of $Z(x) \cap Z(x')$. By Lemma 3.3, $Z(y) = Z(x)$ and $Z(y) = Z(x')$, so $Z(x) = Z(x')$. □

For a subgroup H of a finite group G, the number of subgroups of G that are conjugate to H is $|G|/|\mathrm{N}(H)|$, where $\mathrm{N}(H) = \{g \in G : gHg^{-1} = H\}$ is the normalizer of H.

Lemma 3.5. *If $x \in G$ has prime order then $Z(x) = \mathrm{N}(\langle x\rangle)$ and the number of subgroups of G conjugate to $Z(x)$ is $|G|/|Z(x)|$.*

Proof. Let p be the order of x. Since $Z(x)$ is abelian we have $\langle x\rangle \lhd Z(x)$, so $Z(x) \subset \mathrm{N}(\langle x\rangle)$. To prove $\mathrm{N}(\langle x\rangle) \subset Z(x)$, we adapt the argument from [4, Lemma 1].

Let $g \in \mathrm{N}(\langle x \rangle)$, so

$$gxg^{-1} = x^i, \tag{3.1}$$

where $i \not\equiv 0 \bmod p$. For $k \in \mathbf{Z}^+$ conjugate both sides of (3.1) k times by g to get

$$g^k x g^{-k} = x^{i^k}.$$

In this equation set $k = n = |G|$, so $x = x^{i^n}$ and therefore $i^n \equiv 1 \bmod p$. This implies the order of $i \bmod p$ divides n. Also the order of $i \bmod p$ divides $p-1$, a factor of $\varphi(n)$. Since n is a cyclic number, $(n, \varphi(n)) = 1$. Thus the order of $i \bmod p$ is 1, so $i \equiv 1 \bmod p$ and feeding this back into (3.1) gives us $gxg^{-1} = x$, so $g \in Z(x)$.

The number of subgroups of G conjugate to $Z(x)$ is $|G|/|\mathrm{N}(Z(x))|$. Since $|G|$ is squarefree, $\langle x \rangle$ is a p-Sylow subgroup of G. Therefore $\mathrm{N}(Z(x)) = Z(x)$ because the normalizer of every Sylow subgroup is its own normalizer. Thus $|G|/|\mathrm{N}(Z(x))| = |G|/|Z(x)|$. □

Now we are ready to show the minimal counterexample G leads to a contradiction.

Let p be a prime factor of $|G|$ and x be an element of G with order p (Cauchy's theorem). Then Lemma 3.5 tells us $Z(x)$ has $|G|/|Z(x)|$ conjugate subgroups in G, including itself.

Since $|Z(x)| < |G|$, there is a prime q dividing $|G|/|Z(x)|$ and q does not divide $|Z(x)|$ since $|G|$ is squarefree. Let $y \in G$ have order q (Cauchy again), so $|Z(y)|$ is divisible by q while $|Z(x)|$ is not divisible by q.

We will now look at the union of the subgroups of G conjugate to $Z(x)$ or to $Z(y)$:

$$\bigcup_{g \in G} gZ(x)g^{-1} \cup \bigcup_{h \in G} hZ(y)h^{-1}. \tag{3.2}$$

It will turn out that this subset of G has more than $|G|$ elements, a clear contradiction.

Since $gZ(x)g^{-1} = Z(gxg^{-1})$, Lemma 3.4 tells us that different subgroups conjugate to $Z(x)$ intersect trivially. Similarly, different subgroups conjugate to $Z(y)$ intersect trivially. How does a subgroup conjugate to $Z(x)$ compare to a subgroup conjugate to $Z(y)$? They can't be equal since subgroups of the second kind have order divisible by q and subgroups of the first kind do not, so Lemma 3.4 implies subgroups conjugate to $Z(x)$ and subgroups conjugate to $Z(y)$ intersect trivially.

We can now count the size of (3.2). Using Lemma 3.5 and counting the identity element separately,

$$\begin{aligned}
\left| \bigcup_{g \in G} gZ(x)g^{-1} \cup \bigcup_{h \in G} hZ(y)h^{-1} \right| &= 1 + \frac{|G|}{|Z(x)|}(|Z(x)| - 1) + \frac{|G|}{|Z(y)|}(|Z(y)| - 1) \\
&= 1 + |G| - \frac{|G|}{|Z(x)|} + |G| - \frac{|G|}{|Z(y)|} \\
&\geq 1 + |G| - \frac{|G|}{2} + |G| - \frac{|G|}{2} \\
&= 1 + |G|,
\end{aligned}$$

which is a contradiction and that completes our proof.

4. Second proof of sufficiency of n being a cyclic number

Most proofs I have read that show each group with order equal to a cyclic number is a cyclic group ([1, pp. 9–11], [3], [4], [5], and [10] and [11]) involve maximal subgroups, where a *maximal subgroup* of a group is a proper subgroup contained in no other proper

subgroup. (The proofs in [7], [8], and [9] are based on ideas other than maximal subgroups, *e.g.*, Burnside's normal complement theorem in [7].) In this section we will describe the approach via maximal subgroups, which is similar in many respects to the argument in Section 3, since the subgroups $Z(x)$ for $x \neq e$ in a minimal counterexample G turn out to be the maximal subgroups of G. We will borrow from Section 3 Lemmas 3.1 and 3.2, but otherwise develop what we need.

Here is the strategy. For a maximal subgroup M of a minimal counterexample G we will show that the size of

$$\bigcup_{g \in G} gMg^{-1}$$

is over half the size of G but is not all of G. Then we'll show there is a maximal subgroup M' not conjugate to M, and the union of its conjugate subgroups also fill up over half of G but not all of G. The conjugate subgroups of M and M' taken together have over $|G|$ distinct elements, and that will be a contradiction.

In a group of prime order the trivial subgroup is maximal, and in a group of non-prime order the trivial subgroup is not maximal since, for each element of prime order (which exist by Cauchy's theorem), the subgroup it generates is a proper subgroup containing the trivial subgroup. When G is a minimal counterexample its proper subgroups are cyclic, so all maximal subgroups of G are cyclic.

Lemma 4.1. *If x is nontrivial in G then $Z(x)$ is a maximal subgroup of G.*

Proof. Since $x \neq e$ and G has a trivial center (Lemma 3.2), $Z(x)$ is a proper subgroup of G. To prove $Z(x)$ is a maximal subgroup of G, suppose $Z(x) \subset H \subset G$ for a proper subgroup H. Since $|H| < |G|$, the subgroup H is cyclic, and hence abelian, so all of its elements commute with each other. Thus $y \in H \Rightarrow y \in Z(x)$, so $H \subset Z(x)$. Thus $H = Z(x)$. □

Lemma 4.2. *If M is a maximal subgroup of G then $M \neq \{e\}$ and $M = Z(x)$ for each nontrivial x in M.*

This is like Lemma 3.3.

Proof. The subgroup M is nontrivial since $|G|$ is not 1 or prime, and since M is cyclic its elements all commute with each other. So for x in M we have $M \subset Z(x)$. By the definition of maximal subgroups, $M \subset Z(x) \subset G \Rightarrow Z(x) = M$ or $Z(x) = G$. If $Z(x) = G$ then $x \in Z(G)$, and $Z(G)$ is trivial by Lemma 3.2, so $x \neq e \Rightarrow Z(x) = M$. □

Lemma 4.3. *If M and M' are different maximal subgroups of G then $M \cap M'$ is trivial.*

This is like Lemma 3.4.

Proof. We prove the contrapositive. If $M \cap M'$ is not trivial, let x be a non-identity element of $M \cap M'$. By Lemma 4.2, $M = Z(x)$ and $M' = Z(x)$, so $M = M'$. □

Lemma 4.4. *There are no normal subgroups in G other than $\{e\}$ and G.*

This is not like any lemma in Section 3, but it will substitute for the property $\mathrm{N}(P) = P$ of Sylow subgroups that was used in Section 3.

Proof. Let N be a proper normal subgroup of G, so N is cyclic, say of order m. For each $g \in G$ we have $gNg^{-1} = N$, so we can associate to each $g \in G$ the conjugation function $\gamma_g \colon N \to N$ by $\gamma_g(x) = gxg^{-1}$. Each γ_g is an automorphism of N (its inverse is $\gamma_{g^{-1}}$), so $g \mapsto \gamma_g$ is a homomorphism $G \to \mathrm{Aut}(N) \cong (\mathbf{Z}/(m))^\times$. We will show this is trivial!

Let K be the kernel, so $|G/K|$ divides $|G|$, which is n. Also G/K embeds into $\mathrm{Aut}(N)$, so $|G/K|$ divides $\varphi(m)$, which divides $\varphi(n)$ since $m \mid n$ (look at the formula for the φ-function, especially on squarefree numbers). Since n and $\varphi(n)$ are relatively prime and $|G/K|$ divides both, G/K is trivial. Thus $G = K$, which means every element of G conjugates like the identity on the elements of N. Thus $N \subset Z(G)$, so N is trivial by Lemma 3.2. □

Pick $x \neq e$ in G and set $M = Z(x)$, which is a maximal subgroup. Each gMg^{-1} has order $|M|$. Also gMg^{-1} is a maximal subgroup of G, either by checking for all finite groups that the conjugate of a maximal subgroup is a maximal subgroup, or by checking in our special case that $gMg^{-1} = gZ(x)g^{-1} = Z(gxg^{-1})$ and using Lemma 4.1. The number of different subgroups gMg^{-1} as g varies is $|G|/|\mathrm{N}(M)|$, and conjugate subgroups of M intersect trivially when they are distinct by Lemma 4.3, so by counting the identity element separately,

$$\left|\bigcup_{g\in G} gMg^{-1}\right| = 1 + \frac{|G|}{|\mathrm{N}(M)|}(|M| - 1).$$

We have $M \subset \mathrm{N}(M) \subset G$, so $\mathrm{N}(M) = M$ or $\mathrm{N}(M) = G$ by maximality of M. Nontrivial proper subgroups of G are not normal (Lemma 4.4), so $\mathrm{N}(M) \neq G$. Thus $\mathrm{N}(M) = M$,[1] so

$$\left|\bigcup_{g\in G} gMg^{-1}\right| = 1 + \frac{|G|}{|M|}(|M| - 1) = 1 + \left(1 - \frac{1}{|M|}\right)|G| \geq 1 + \frac{|G|}{2}.$$

That's a lower bound. We also have an upper bound:

$$\left|\bigcup_{g\in G} gMg^{-1}\right| = 1 + \left(1 - \frac{1}{|M|}\right)|G| < 1 + \left(1 - \frac{1}{|G|}\right)|G| = |G|.$$

By this strict inequality, there is some $x' \in G$ that is not in any conjugate subgroup of M.[2] Set $M' = Z(x')$. Since $x' \neq e$, by reasoning as above with conjugate subgroups of M' in place of M, we get

$$\left|\bigcup_{h\in G} hM'h^{-1}\right| \geq 1 + \frac{|G|}{2}.$$

Subgroups of G having the form gMg^{-1} and $hM'h^{-1}$ can't be equal, since otherwise M' is conjugate to M but $x' \in M'$ and x' is (by definition) in no conjugate subgroup of M. Thus every gMg^{-1} and $hM'h^{-1}$ intersect trivially (Lemma 4.3), so by counting the identity element separately,

$$\begin{aligned}\left|\bigcup_{g\in G} gMg^{-1} \cup \bigcup_{h\in G} hM'h^{-1}\right| &= 1 + \left|\bigcup_{g\in G} gMg^{-1}\right| - 1 + \left|\bigcup_{h\in G} hM'h^{-1}\right| - 1 \\ &\geq 1 + \frac{|G|}{2} + \frac{|G|}{2} \\ &= 1 + |G|,\end{aligned}$$

which is a contradiction.

[1] The step analogous to this in Section 3 is that $\mathrm{N}(P) = P$ when P is a Sylow subgroup of G.

[2] In fact, for every finite group G and proper subgroup H, the union of all gHg^{-1} is not all of G.

References

[1] L. Crew, On the characterization of the numbers n such that any group of order n has a given property P, https://arxiv.org/pdf/1501.03170.pdf. (See pp. 9–11.)

[2] L. E. Dickson, Definitions of a group and a field by independent postulates, *Trans. Amer. Math. Soc.* **6** (1905), 198–204. Online at http://www.ams.org/journals/tran/1905-006-02/S0002-9947-1905-1500706-2/S0002-9947-1905-1500706-2.pdf

[3] J. Gallian and D. Moulton, When is Z_n the only group of order n?, *Elem. Math.* **48** (1993), 117–119. http://gdz.sub.uni-goettingen.de/dms/load/img/?PID=GDZPPN002083140.

[4] Y. Ge, All Groups of Order n are cyclic iff. . ., https://yiminge.wordpress.com/2009/01/22/all-groups-of-order-n-are-cyclic-iff/.

[5] D. Jungnickel, On the Uniqueness of the Cyclic Group of Order n, *Amer. Math. Monthly* **99** (1992), 545–547, https://www.jstor.org/stable/2324062.

[6] J. Lahtonen, answer at https://math.stackexchange.com/questions/67407/group-of-order-15-is-abelian.

[7] Y. Sharifi, Groups of order n with gcd(n,phi(n))=1 are cyclic, https://ysharifi.wordpress.com/2010/12/13/groups-of-order-n-with-gcdn-phin1-are-cyclic/.

[8] T. Szele, Über die endlichen Ordnungszahlen, zu denen nur eine Gruppe gehört, *Comm. Math. Helv.* **20** (1947), 265–267, https://eudml.org/doc/138922.

[9] S. K. Upadhyay and S. D. Kumar, Existence of a Unique Group of Finite Order, *The Mathematics Student* **81** (2012), 215–218. http://www.indianmathsociety.org.in/mathstudent2012.pdf

[10] A. Youcis, A Classification of Integers n for Which the Only Groups of Order n are Cyclic (Pt. I), https://drexel28.wordpress.com/2011/09/13/a-classification-of-integers-n-for-which-the-only-groups-of-order-n- are-cyclic-pt-i/.

[11] A. Youcis, A Classification of Integers n for Which the Only Groups of Order n are Cyclic (Pt. II), https://drexel28.wordpress.com/2011/09/13/a-classification-of-integers-n-for-which-the-only-groups-of-order-n-are-cyclic-pt-ii/.