COUNTING GROUP ELEMENTS WHOSE ORDER DIVIDES k

Joseph Pollari
University of Wisconsin Oshkosh
Department of Mathematics
800 Algoma Boulevard
Oshkosh, Wisconsin 54901
joey.pollari@gmail.com

Kenneth L. Price
University of Wisconsin Oshkosh
Department of Mathematics
800 Algoma Boulevard
Oshkosh, Wisconsin 54901
pricek@uwosh.edu

1 Introduction

This work covers results of an independent study conducted in spring 2022 by the student coauthor, Pollari, under the direction of the faculty coauthor, Price. The research question was motivated by a formula in [4, Theorem 3.6], which involves counting the number of elements of a group that have certain orders. We provide an exact count for the class of finite abelian groups in Section 2 (see Theorem 8). Results on certain finite nonabelian groups are provided in Section 3. (See Theorems 9, 15, and 23, as well as Corollaries 18 and 24.)

As noted in Remark 16, deriving more precise results than the ones in Theorems 15 and 23 is impractical. However, this can be solved using technology in many cases. The software utilized in this investigation was prepared by the student coauthor (Pollari) in the programming language Python. The code is provided in Appendix 4.

We will reference Judson's undergraduate algebra textbook when necessary. There are several editions of this textbook, but we included citation information for [2], since it is the most recent edition that the faculty coauthor (Price) taught from.

Notation 1 *For a finite group G and a positive integer $k \leq |G|$, let $O_G(k)$ denote the number of elements of G whose order divides k.*

We may view O_G as a function from $\{1, 2, \ldots, |G|\}$ to $\mathbb{N}$. We consider the question: what are the range of values for O_G? To motivate this question, we note that $O_{G_1} = O_{G_2}$ for any isomorphic finite groups G_1 and G_2. This provides a method for distinguishing nonisomorphic groups, which we use in Corollary 5.

More motivation for the research question is provided by formula 1, which holds for any finite group G and prime number p. See [4, Corollary 3.8] for more details.

$$O_G(p) \equiv |G|^{p-1} \pmod{p} \tag{1}$$

This may remind you of Fermat's Little Theorem (see [2, Theorem 6.13]). It is indeed an extension of this famous result. Suppose p is a prime number and a is a positive integer such that $p \nmid a$. If we set $G = \mathbf{Z}_a$, then $|G| = a$ and, by Corollary 4, $O_{\mathbf{Z}_a}(p) = 1$. Thus equation 1 reduces to $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's Little Theorem.

As a consequence of formula 1, if p divides $|G|$, then p divides $O_G(p)$. However, if $p \nmid |G|$, then, by Lagrange's Theorem, G contains no elements of order p and $O_G(p) = 1$. In this case, equation 1 becomes $1 \equiv |G|^{p-1} \pmod{p}$, which also follows from Fermat's Little Theorem.

The proofs of all the results contained within are 'elementary,' which means they are accessible to anyone who has completed an undergraduate course on group theory. We conclude this introductory section with Lemma 2, which has an elementary proof and is repeatedly used throughout the remaining sections.

Lemma 2 *Suppose G is a finite group with identity e. and k is an integer with $1 \leq k \leq |G|$.*

1. *Let $H_G(k) = \left\{x \in G : x^k = e\right\}$. Then $O_G(k) = |H_G(k)|$*
2. *Suppose G is the external direct product of finite groups A and B, that is, $G = A \times B$. We have $H_G(k) = H_A(k) \times H_B(k)$ and $O_G(k) = O_A(k) \cdot O_B(k)$.*
3. *If G is abelian, then $H_G(k)$ is a subgroup of G and $O_G(k)$ divides $|G|$.*

Proof. (1) For $x \in G$, we have $x^k = e$ if and only if $\operatorname{ord}(x)$ divides k by Lagrange's Theorem. Thus, $H_G(k)$ is the set of elements of G whose order divides k and $O_G(k) = |H_G(k)|$, as claimed.

(2) By part 1, it is enough to show that $H_G(k) = H_A(k) \times H_B(k)$. The identity element of G is (e_A, e_B), where e_A is the identity element of A and e_B is the identity element of B.

Let $x \in H_A(k) \times H_B(k)$ be arbitrarily chosen. Then $x = (a, b)$ for some $a \in H_A(k)$ and $b \in H_B(k)$. We have $a^k = e_A$ and $b^k = e_B$ so $(a, b)^k = \left(a^k, b^k\right) = (e_A, e_B)$. This implies $(a,b) \in H_G(k)$ and $H_A(k) \times H_B(k) \subseteq H_G(k)$ since x was arbitrarily chosen in $H_A(k) \times H_B(k)$.

Let $y \in H_G(k)$ be arbitrarily chosen. Then $y^k = (e_A, e_B)$ and $y = (c,d)$ for some $c \in A$ and $d \in B$. Substituting $y = (c,d)$ into $y^k = (e_A, e_B)$ gives $\left(c^k, d^k\right) = (e_A, e_B)$. Thus $c^k = e_A$ and $d^k = e_B$, which implies $c \in H_A(k)$ and $d \in H_B(k)$. Therefore, $y \in H_A(k) \times H_B(k)$ and $H_G(k) \subseteq H_A(k) \times H_B(k)$ since y was arbitrarily chosen in $H_G(k)$. Therefore, $H_G(k) = H_A(k) \times H_B(k)$, as desired.

(3) We have $H_G(k) \neq \varnothing$ since $e \in H_G(k)$. Let $g, h \in H_G(k)$ be arbitrarily chosen. Then $g^k = h^k = e$ and $\left(gh^{-1}\right)^k = g^k \left(h^k\right)^{-1} = e$ since G is abelian. Thus $gh^{-1} \in H_G(k)$ and $H_G(k)$ is a subgroup of G by [2, Theorem 3.10]. Therefore, $O_G(k)$ divides $|G|$ by Lagrange's Theorem. ■

2 Finite Abelian Groups

2.1 Cyclic Groups

Theorem 3 *Suppose G is a cyclic group of order n and $a \in G$ is a generator of G. For any $k = 1, 2, \ldots, n$, we have $O_G(k) = \gcd(n,k)$.*

Proof. Set $\ell = n/\gcd(n,k)$. Note that $\left(a^\ell\right)^{\gcd(n,k)} = e$ so $\left(a^\ell\right)^k = e$ and $a^\ell \in H_G(k)$. Moreover, $\gcd(n,k)$ is the smallest power of a^ℓ that is equal to e since n is the smallest power of a that is equal to e. Thus $\operatorname{ord}\left(a^\ell\right) = \gcd(n,k)$. By part 3 of Lemma 2, $H_G(k)$ is a subgroup of G and $O_G(k) = |H_G(k)|$. Since $H_G(k)$ contains a^ℓ, which is an element of order $\gcd(n,k)$, we can conclude that $O_G(k) \geq \gcd(n,k)$.

A subgroup of a cyclic group is cyclic (see [2, Theorem 4.3]), Thus $H_G(k)$ is cyclic and there is a generator h for $H_G(k)$. Then $\operatorname{ord}(h)$ divides k since $h \in H_G(k)$. Moreover, $O_G(k) = |H_G(k)| = \operatorname{ord}(h)$ so $O_G(k)$ divides k. By part 3 of Lemma 2, $O_G(k)$ divides $|G| = n$. Therefore, $O_G(k)$ is a common divisor of k and n. Thus $O_G(k) \leq \gcd(k,n)$. ■

Corollary 4 *If n and k are integers such that $n \geq 2$ and $1 \leq k \leq n$, then $O_{\mathbb{Z}_n}(k) = \gcd(n,k)$.*

Corollary 5 *Let m and n be positive integers such that $m \geq 2$ and $n \geq 2$. If $\gcd(m,n) \neq 1$, then $\mathbb{Z}_{mn}$ is not isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$.*

Proof. Set $k = \gcd(m,n)$. By Theorem 3, $O_{\mathbb{Z}_m}(k) = \gcd(m,k) = k$, $O_{\mathbb{Z}_n}(k) = \gcd(n,k) = k$, and $O_{\mathbb{Z}_{mn}}(k) = \gcd(mn,k) = k$. By part 3 of Lemma 2, $O_{\mathbb{Z}_m \times \mathbb{Z}_n}(k) = O_{\mathbb{Z}_m}(k)\, O_{\mathbb{Z}_n}(k) = k^2$. If $\mathbb{Z}_{mn}$ is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_n$, then $O_{\mathbb{Z}_{mn}}(k) = O_{\mathbb{Z}_m \times \mathbb{Z}_n}(k)$, which implies $k = k^2$. Thus $k = 1$. ■

Remark 6 *A stronger result holds. As noted in [2, Theorem 9.10],* $\mathbb{Z}_{mn}$ *is isomorphic to* $\mathbb{Z}_m \times \mathbb{Z}_n$ *if and only if* $\gcd(m,n) = 1$*.*

2.2 Finite Abelian Groups

Definition 7 *Let* G *be a finite abelian group. As noted in [2, Theorem 13.3],* G *is isomorphic to a direct product of cyclic groups of prime power order, that is*

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}} \tag{2}$$

where n *and* $\alpha_1, \alpha_2, \ldots, a_n$ *are positive integers and* $p_1, p_2, \ldots, p_n$ *are primes (not necessarily distinct). We call* $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_n^{\alpha_n}$ *the* ***elementary divisors*** *of* G*.*

Theorem 8 *Suppose* G *is a finite group with elementary divisors* $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_n^{\alpha_n}$*. For any positive integer* $k \leq |G|$*, we have*

$$O_G(k) = \gcd\left(p_1^{\alpha_1}, k\right) \gcd\left(p_2^{a_2}, k\right) \cdots \gcd\left(p_n^{\alpha_n}, k\right).$$

Proof. Let G be expressed as shown in equation 7. By repeatedly applying part 2 of Lemma 2, we have

$$O_G(k) = O_{\mathbb{Z}_{p_1^{\alpha_1}}}(k) \cdot O_{\mathbb{Z}_{p_2^{\alpha_2}}}(k) \cdots O_{\mathbb{Z}_{p_n^{\alpha_n}}}(k).$$

By Theorem 3, $O_{\mathbb{Z}_{p_i^{\alpha_{1i}}}}(k) = \gcd\left(p_i^{\alpha_i}, k\right)$ for each $i = 1, \ldots, n$. The result follows immediately. ■

3 Finite Nonabelian Groups

3.1 Dihedral Groups

Recall the dihedral group of degree n, denoted by D_n, is defined to be the group of symmetries of a regular n-gon for any integer $n \geq 2$. The group operation is composition.

Theorem 9 *Let* n *and* k *be integers such that* $n \geq 2$ *and* $1 \leq k \leq n$*.*

$$O_{D_n}(k) = \begin{cases} \gcd(n,k) & \text{if } k \text{ is odd} \\ \gcd(n,k) + n & \text{if } k \text{ is even} \end{cases}$$

Proof. Let R_n be the set of rotational symmetries of a regular n-gon (including the identity). Let F_n be the set of reflection symmetries of a regular n-gon (not including the identity). The group D_n has order $2n$ and is the disjoint union of R_n and F_n. Note that R_n is a cyclic subgroup of D_n. It is generated by a rotation by $2\pi/n$ radians, so it has order n and $O_{R_n}(k) = \gcd(n,k)$ by Theorem 3. Moreover, every element of F_n has order 2.

If k is odd, then $H_{D_n}(k) = H_{R_n}(k)$. By part 1 of Lemma 2,

$$O_{D_n}(k) = O_{R_n}(k) = \gcd(n,k).$$

If k is even, then every reflection belongs to $H_{D_n}(k)$. Thus $H_{D_n}(k)$ is the disjoint union of $H_{R_n}(k)$ and F_n. By part 1 of Lemma 2,

$$O_{D_n}(k) = O_{R_n}(k) + |F_n| = \gcd(n,k) + n.$$

■

3.2 Symmetric Groups

Recall the symmetric group on n letters, denoted by S_n, is defined to be the group of permutations on the set $\{1,2,\ldots,n\}$ for any integer $n \geq 2$. We partition S_n following the construction and notation of principal characteristic polynomials described in [3]. Recall that for all $\sigma \in S_n$, there are disjoint cycles $\sigma_1,\ldots,\sigma_r \in S_n$ such that $\sigma = \sigma_1 \cdots \sigma_r$. This expression is unique in the sense that if there are disjoint cycles $\rho_1,\ldots,\rho_s \in S_n$ such that $\sigma = \rho_1 \cdots \rho_s$, then $r = s$ and there is a permutation $\pi \in S_r$ such that $\sigma_i = \rho_{\pi(i)}$ for $i = 1,\ldots,r$.

Definition 10 *The* cycle structure *of a permutation $\sigma \in S_n$ is an n-tuple $\alpha = (\alpha_1,\ldots,\alpha_n)$ such that σ is a (unique) product of disjoint α_1 cycles on one letter, α_2 cycles on two letters (i.e. transpositions), α_3 cycles on three letters (i.e. ternary cycles), and so on.*

Remark 11 *A cycle on one letter is equal to the identity. We use it for record keeping so that every number from 1 to n gets listed in the description of σ as a product of disjoint cycles.*

Notation 12 *Let P_α denote the number of all permutations with cycle structure α in S_n.*

Lemma 13 covers key properties about cycle structures that we use to calculate $O_{S_n}(k)$. Parts 1 and 4 appear in [3]. An elementary reference for integer partitions is [1].

Lemma 13 *Suppose $n \geq 2$ is an integer and $\sigma \in S_n$ has cycle structure $\alpha = (\alpha_1, \ldots, \alpha_n)$.*

1. An integer partition of n is given by $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n = n$.

2. The formula in part 1 induces a bijective correspondence between cycle structures on S_n and integer partitions on n.

3. The order of any permutation with cycle structure α is $\operatorname{lcm}\{j : 0 \neq \alpha_j\}$.

4. The number of all permutations with cycle structure α is given by formula 3.

$$P_\alpha = \frac{n!}{(1^{\alpha_1}\alpha_1!)(2^{\alpha_2}\alpha_2!)\cdots(n^{\alpha_n}\alpha_n!)} \tag{3}$$

Proof. (1) This is because all n letters are accounted for by the disjoint cycles.

(2) Cycle structures map to integer partitions by part (1). The inverse mapping takes an integer partition to the cycle structure whose i^{th} entry is the multiplicity of i for each i, $1 \leq i \leq n$.

(3) This is an easy exercise (see [2, Exercise 13, P. 75]). Note that in the cycle decomposition, the cycles are all disjoint and each of the α_j cycles of length j has order j.

(4) For each $\rho \in S_n$, the permutation $\rho\sigma\rho^{-1}$ is obtained by renumbering the entries of each disjoint cycle by replacing i with $\rho(i)$. Thus it also has cycle structure α. This gives up to $n!$ permutations with cycle structure α, but this is an overcount since the same cycle may be expressed in different ways. For $1 \leq r \leq n$, an r-cycle may be written in r^{α_r} different ways, depending on which letter is written first. Moreover, the r-cycles may be permuted amongst themselves in $\alpha_r!$ different ways. Formula 3 follows by multiplying the repetitions for each r-cycle in the denominator. ■

Notation 14 *For integers k and n with $n \geq 2$ and $1 \leq k \leq n$, we let $I_n(k)$ denote the set of all $\alpha = (\alpha_1, \ldots, \alpha_n)$ such that α is a cycle structure on S_n and $\operatorname{lcm}\{j : 0 \neq \alpha_j\} = k$.*

Theorem 15 *Suppose k and n are integers with $n \geq 2$ and $1 \leq k \leq n$.*

$$O_{S_n}(k) = \sum_{\alpha \in I_n(k)} P_\alpha = \sum_{\alpha \in I_n(k)} \frac{n!}{(1^{\alpha_1}\alpha_1!)(2^{\alpha_2}\alpha_2!)\cdots(n^{\alpha_n}\alpha_n!)} \tag{4}$$

Proof. By parts (1), (2), and (3) of Lemma 13,

$$H_{S_n}(k) = \cup_{\alpha \in I_n(k)} \{\sigma \in S_n : \sigma \text{ has cycle structure } \alpha\}.$$

Note that this is a union of disjoint sets. We obtain formula 4 by applying part (1) of Lemma 2 and part (4) of Lemma 13. ■

Remark 16 *There is no known formula for the number of integer partitions of a given integer n. This is a historically hard problem (see [1]). Thus we have no hope of finding the sets $I_n(k)$ for all values of k and n. An algorithm to calculate $O_{S_n}(k)$ using the result in Theorem 15 is contained in the appendix. Corollary 18 provides a formula for $O_{S_n}(2)$.*

Notation 17 *For any integer n, let $\lfloor n/2 \rfloor$ denote the greatest integer less than $n/2$.*

Corollary 18 *Suppose n is an integer and $n \geq 2$.*

$$O_{S_n}(2) = \sum_{h=0}^{\lfloor n/2 \rfloor} \frac{n!}{(n-2h)!\,(2^h)\,h!}$$

Proof. Note that $I_n(2) = \{(n-2h, h, 0, \ldots, 0) : 0 \leq h \leq \lfloor n/2 \rfloor\}$. Moreover, for all $h = 0, \ldots, \lfloor n/2 \rfloor$, $P(n-2h, h, 0, \ldots, 0) = \dfrac{n!}{(n-2h)!2^h h!}$. The result follows from Theorem 15. ∎

Example 19 *The values of $O_{S_n}(2)$ for $2 \leq n \leq 11$ are shown in the table below.*

n	2	3	4	5	6	7	8	9	10	11
$O_{S_n}(2)$	2	4	10	26	76	232	764	2620	9496	35696

Remark 20 *As noted in the introduction, if p is a prime number and p divides $|G|$, then p divides $O_G(p)$. Therefore, p divides $O_{S_n}(p)$ for any prime number $p \leq n$. In particular, $O_{S_n}(2)$ is even for all $n \geq 2$.*

3.3 Alternating Groups

Recall the alternating group on n letters, denoted A_n, is the subgroup of S_n containing all permutations that are the product of an even number of transpositions.

Lemma 21 *Suppose $n \geq 2$ is an integer and σ is a permutation in S_n with cycle structure $\alpha = (\alpha_1, \ldots, \alpha_n)$. Then $\sigma \in A_n$ if and only if $\alpha_2 + \alpha_4 + \cdots + \alpha_{\lfloor n/2 \rfloor}$ is even.*

Proof. The identity permutation is an element of A_n with cycle structure $(n, 0, \ldots, 0)$. Suppose σ is an arbitrarily chosen element of S_n with cycle structure $\alpha = (\alpha_1, \ldots, \alpha_n)$ such that $a_1 \neq n$. For each i, $1 < i \leq n$, if $0 < \alpha_i$ there are α_i cycles of length i in the cycle decomposition of σ. We denote them by $\sigma_{i,1}, \sigma_{i,2}, \ldots, \sigma_{i,\alpha_i}$. We can write the cycle decomposition of σ as

$$\sigma = \prod_{\substack{1<i\leq n \\ 0\neq\alpha_i}} \sigma_{i,1}\sigma_{i,2}\cdots\sigma_{i,\alpha_i}.$$

For each i, j, $1 < i \leq n$ and $1 \leq j \leq \alpha_i$, we can express $\sigma_{i,j}$ as a product of $i-1$ transpositions (see [2, Proposition 5.4]). Then the cycle decomposition of σ can also be rewritten as a product of transpositions and the number of transpositions is given by

$$\sum_{1<i\leq n} (i-1)\,\alpha_i = \sum_{\substack{1<i\leq n \\ i \text{ odd}}} (i-1)\,\alpha_i + \sum_{\substack{1<i\leq n \\ i \text{ even}}} (i-2)\,\alpha_i + \left(\alpha_2 + \alpha_4 + \cdots + \alpha_{\lfloor n/2 \rfloor}\right).$$

Note that $i-1$ is even when i is odd and $i-2$ is even when i is even, so the first two sums are even. Therefore, $\sigma \in A_n$ if and only if $\alpha_2 + \alpha_4 + \cdots + \alpha_{\lfloor n/2 \rfloor}$ is even. ■

Notation 22 *For integers k and n with $n \geq 2$ and $1 \leq k \leq n$, we let $J_n(k)$ denote the set of all $\alpha = (\alpha_1, \ldots, \alpha_n)$ such that α is a cycle structure on S_n, $\operatorname{lcm}\{j : 0 \neq \alpha_j\} = k$, and $\alpha_2 + \alpha_4 + \cdots + \alpha_{\lfloor n/2 \rfloor}$ is even.*

Theorem 23 *Suppose k and n are integers with $n \geq 2$ and $1 \leq k \leq n$.*

1. $O_{A_n}(k) = \sum_{\alpha \in J_n(k)} P_\alpha = \sum_{\alpha \in J_n(k)} \frac{n!}{(1^{\alpha_1}\alpha_1!)(2^{\alpha_2}\alpha_2!)\cdots(n^{\alpha_n}\alpha_n!)}$
2. *$O_{A_n}(k) = O_{S_n}(k)$ if and only if k is odd.*

Proof. Part (1) is proved in the same way as Theorem 15. To prove part (2), it is enough to show that $I_n(k) = J_n(k)$ if and only if k is odd.

Assume $I_n(k) \neq J_n(k)$ for some integer k, $1 \leq k \leq n$. Since $I_n(k) \subseteq J_n(k)$, there exists $\alpha \in J_n(k)$ such that $\alpha \notin I_n(k)$. This implies $\operatorname{lcm}\{j : 0 \neq \alpha_j\} = k$, and $\alpha_2 + \alpha_4 + \cdots + \alpha_{\lfloor n/2 \rfloor}$ is odd. The latter condition implies $\alpha_{2i} \neq 0$ for some $i > 0$. Thus $k = \operatorname{lcm}\{j : 0 \neq \alpha_j\}$ is even.

Now assume $I_n(k) = J_n(k)$ for some integer k, $1 \leq k \leq n$. Let $\beta = (\beta_1, \ldots, \beta_n)$ be the cycle structure whose entries are all 0 except $\beta_1 = n-k$, and $\beta_k = 1$. We have $\operatorname{lcm}\left\{j : 0 < \beta_j\right\} = k$, so $\beta \in I_n(k) = J_n(k)$. Thus $\beta_2 + \beta_4 + \cdots + \beta_{\lfloor n/2 \rfloor}$ is even. Thus k must be odd since $\beta_k = 1$ and $\beta_i = 0$ for all i such that $1 < i \leq n$ and $i \neq k$. ■

Corollary 24 *Suppose n is an integer and $n \geq 2$.*

$$O_{A_n}(2) = \sum_{\substack{h=0 \\ h \text{ even}}}^{\lfloor n/2 \rfloor} \frac{n!}{(n-2h)!\,(2^h)\,h!}$$

Proof. Note that $J_n(2) = \{(n-2h, h, 0, \ldots, 0) : h \text{ is even and } 0 \leq h \leq \lfloor n/2 \rfloor\}$. ■

Example 25 *The values of $O_{A_n}(2)$ for $2 \leq n \leq 11$ are shown in the table below.*

n	2	3	4	5	6	7	8	9	10	11
$O_{A_n}(2)$	1	1	4	16	46	106	316	1324	5356	18316

Remark 26 *As noted in the introduction, if p is a prime number and p divides $|G|$, then p divides $O_G(p)$. Therefore, $O_{A_n}(2)$ is even for all $n \geq 4$. If p is an odd prime, then p divides $O_{A_n}(p)$ for all $n \geq p$. For example, $O_{A_3}(3) = 3$, $O_{A_4}(3) = 9$, and $O_{A_5}(3) = 21$.*

4 Appendix: Python Code

Remark 27 *The following Python code calculates $O_{S_n}(k)$ for any integers n and k with $n \geq 2$ and $1 \leq k \leq n$.*

```
from math import factorial

def getFactors(a):  # generate factors of the input
    answer = []
    for alpha in range(1, a + 1):
    if a % alpha == 0:
        answer.append(alpha)
    return answer

def getPartitions(q):
# generate partitions of n, courtesy of
# https://jeromekelleher.net/category/combinatorics.html
    a = [0 for i in range(q + 1)]
    r = 1
    y = q - 1
    while r != 0:
        x = a[r - 1] + 1
        r -= 1
        while 2 * x <= y:
            a[r] = x
            y -= x
            r += 1
        l = r + 1
        while x <= y:
            a[r] = x
            a[l] = y
            yield a[:r + 2]
```

```
            x += 1
            y -= 1
        a[r] = x + y
        y = x + y - 1
        yield a[:r + 1]


n = int(input("Symmetric group on how many letters? "))
graphInput = input("Do you want to see a graph? ")
infoInput = input("Do you want to see detailed information regarding "
                  f"H_{{S_{{{n}}}}}(k)? ")
tableInput = input("Do you want to see an output table, "
                       "pre-formatted for LaTeX? ")

    graphMode = True if graphInput.casefold() == "yes" else False
    infoMode = True if infoInput.casefold() == "yes" else False
    tableMode = True if tableInput.casefold() == "yes" else False

    if graphMode:
        import matplotlib.pyplot as plotter
        # Package that allows us to plot data in Python.

    graph = {}  # This will be our map between k and O_Sn(k).
    for k in range(1, factorial(n) + 1):  # 1 <= k <= |G|
        # We'll filter our partitions for ones that only contain factors.
        factorsAndPartitions = []
        for currentPartition in getPartitions(n):
            works = 0  # This is the number of summands that are factors of k.
            for checkPartition in currentPartition:
                if checkPartition in getFactors(k):
                    works += 1
            # If all the numbers are factors of k...
            if works == len(currentPartition):
                # Put it in the list of working partitions.
                factorsAndPartitions.append(currentPartition)

        # This will be the list of factors and partitions,
        # but represented as cycle structures.
        cycleStructures = []
        for currFactorPartition in factorsAndPartitions:
            # Empty cycle structures, which we'll later
            # fill with the proper elements.
            cycleStructures.append([])
```

```
        for currStructure in range(len(cycleStructures)):
            for structureIndex in range(n):
                # Fill the empty cycle structure
                cycleStructures[currStructure].append\
                (factorsAndPartitions[currStructure].count\
                (structureIndex + 1))

        O_Sn = 0
        for currStructure in cycleStructures:
            currentPFunction = factorial(n)  # The numerator from [3]
            for currLength in range(1, n + 1):
                # Divide by first factor in the denominator from [3]
                currentPFunction /= currLength **\
                currStructure[currLength - 1]
            # Divide by second factor in the denominator from [3]
            currentPFunction /= factorial(currStructure[currLength - 1])
        O_Sn += currentPFunction
    graph.update({k: round(O_Sn)})

    if infoMode:
    print("k:", k)
    print(f"\t Partitions that only contain factors "
          "as summands: {factorsAndPartitions}")
    print(f"\t Represented as cycle structures: {cycleStructures}")
    print(f"\t O_{{S_{{{n}}}}}({k}) = {round(O_Sn)}")

if graphMode:  # This plots the data if we want to.
    plotter.plot(graph.keys(), graph.values())
    plotter.title(f"Number of elements of $S_{{{n}}}$ whose "
                  "order divides $k$")
    plotter.ylabel(f"$O_{{S{{{n}}}}}(k)$")
    plotter.xlabel("$k$")
    plotter.show()

if tableMode:  # This formats the LaTeX if we want a table.
    print("~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~"
          "~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~")
    print("Copy and paste into a LaTeX compiler:")
    print("\\begin{tabular}{|c|c|} \\hline")
    print(f"\t $k$ & $O_{{S_{{{n}}}}}(k)$ \\\\ \\hline")
    for keys in graph:
        print(f"\t {keys} & {graph[keys]} \\\\ \\hline")
    print("\\end{tabular}", end = "")
```

References

[1] G. E. Andrews & K. Eriksson, "Integer Partitions," Cambridge University Press (2004).

[2] T. Judson, "Abstract Algebra: Theory and Applications," https:\\abstract.ups.edu (2012).

[3] F. D. Murnaghan. On the Representations of the Symmetric Group, *American Journal of Mathematics* **59**(3) (1937), 437-488.

[4] J. DeWitt and K. Price, Induced Good Group Gradings of Structural Matrix Rings, *Communications in Algebra* **47** (2019), 1114-1124.