PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 101(115) (2017), 99–108 https://doi.org/10.2298/PIM1715099B

THE CYCLE INDEX OF THE AUTOMORPHISM GROUP OF $\mathbb{Z}_n$

Vladimir Bozovic and Žana Kovijanić Vukićević

Abstract. We consider the group action of the automorphism group $\mathcal{U}_n = \mathrm{Aut}(\mathbb{Z}_n)$ on the set $\mathbb{Z}_n$, that is the set of residue classes modulo n. Clearly, this group action provides a representation of $\mathcal{U}_n$ as a permutation group acting on n points. One problem to be solved regarding this group action is to find its cycle index. Once it is found, there appears a vast class of related enumerative and computational problems with interesting applications. We provide the cycle index of specified group action in two ways. One of them is more abstract and hence compact, while another one is basically a procedure of composing the cycle index from some building blocks. However, those building blocks are also well explained and finally presented in a very detailed fashion.

1. Introduction

Let $\mathcal{U}_n = \mathrm{Aut}(\mathbb{Z}_n)$ be the automorphism group of the cyclic additive group of residues modulo n. Throughout this paper, we treat $\mathbb{Z}_n$ interchangeably, merely as a set $\{0, 1, \ldots, n-1\}$ or as the additive, cyclic group. However, the context in which it is used will clearly determine its meaning.

As it is well known, $\mathcal{U}_n$ is isomorphic to the multiplicative group of those integers in $\mathbb{Z}_n$ that are relatively prime to n, i.e.,

$$\mathcal{U}_n = \{\pi_a \colon \mathbb{Z}_n \mapsto \mathbb{Z}_n \mid \pi_a(x) = ax \pmod{n},\ 1 \leqslant a \leqslant n,\ (a,n) = 1\}.$$

Based on that isomorphism, a mapping $\pi_a \in \mathcal{U}_n$, can be identified with an element $a \in \mathbb{Z}_n$, $(a,n) = 1$. Further, we will be frequently using that convenient isomorphic correspondence, without risk of misconception. Hence, the natural group action of the group $\mathcal{U}_n$ on the set of elements of $\mathbb{Z}_n$ could be seen as

$$(x, a) \mapsto ax \pmod{n} \quad (a \in \mathcal{U}_n,\ x \in \mathbb{Z}_n),$$

Clearly, the automorphism group, $\mathcal{U}_n$, represented in the described way is a permutation group acting on n points. Although elementary in its nature, it was a surprising fact that, to the best of our knowledge, the cycle index of the described

2010 *Mathematics Subject Classification:* Primary 05E99, Secondary: 20B40, 20C40.
Key words and phrases: cycle index, automorphism group of $\mathbb{Z}_n$.
Communicated by Zoran Petrović.

group action is still missing. We found only one paper, [**1**], that partially deals with the similar group action, and yet substantially different. Therefore, finding the cycle index, $\mathcal{Z}_{(\mathcal{U}_n,\mathbb{Z}_n)}$, of the described group action emerges as the main goal of this paper.

Based on somewhat distinct, although complement approaches, we get two forms of the same result. The first one that looks more general, whereas another one is technically more detailed, supplying raw structure of cycle index $\mathcal{Z}_{(\mathcal{U}_n,\mathbb{Z}_n)}$.

In the first approach, we get a nice, compact result from Corollary 3.1, while in the second approach, we use the fact of the direct decomposition of an additive Abelian group and corresponding decomposition of its automorphism group.

As n can be decomposed as a product of prime number powers, then we proceed by finding the cycle index $\mathcal{Z}_{(\mathcal{U}_{p^\alpha},\mathbb{Z}_{p^\alpha})}$, for a prime number p and $\alpha \in \mathbb{N}$, as a groundwork for utilization of a known result given in [**5**], that is an algorithm for finding cycle index of direct product of permutation groups.

Once the cycle index is found, there is a vast class of enumerative and combinatorial problems that could be related to it. For example, one of the classical enumerative, combinatorial "targets" is a number of orbits or equivalence classes of subsets of $\mathbb{Z}_n$.

2. Preliminaries

In this section, we bring up some basic, auxiliary results, notation and assumptions that will be used in the rest of the paper.

- By *natural number* we assume positive integer.
- By $\biguplus$ we denote disjoint union of sets.
- The label ϕ will be exclusively used for Euler's phi function.
- By C_n we denote a cyclic group of n elements.
- By $\mathrm{Sym}(M)$ we denote the full symmetric group on the set M.
- By $\mathrm{ord}(g)$ we denote the order of an element g in a group G.

Regarding a topic of group action, we slightly changed definitions of classical notions and accordingly, introduce new notation.

Definition 2.1 (Type of a permutation). Let P be a set with $|P| = n$. A permutation $\pi \in \mathrm{Sym}(P)$ is of the type $(\lambda_1, \lambda_2, \ldots, \lambda_n)$, iff π can be written as a composition of λ_i disjointed cycles of length i, for $i = 1, \ldots, n$.

Hence, by $\lambda_i(\pi)$ we mean the number of cycles of length i in the decomposition of π into disjoint cycles. We use the short and symbolic notation

$$\mathrm{ctype}(\pi) = \prod_{i=1}^{n} x_i^{\lambda_i(\pi)}$$

to mean that there are $\lambda_i(\pi)$ cycles of length i in the decomposition of π in product of disjoint cycles. Note that variable x_i has only formal meaning, referring to the cycle of the length i.

Definition 2.2 (Partial Cycle Index). Let P be a set of $|P| = n$ elements and let Γ be a subset of finite permutation group $\mathcal{G}_P$ acting on P. The *partial cycle* *index* of a subset $\Gamma \subseteq \mathcal{G}_P$ is defined as a polynomial in n indeterminates $x_1, \dots, x_n$, defined by

$$\mathcal{Z}_{(\Gamma,P)}(\mathcal{G}_P) := \frac{1}{|\mathcal{G}_P|} \sum_{\pi\in\Gamma} \operatorname{ctype}(\pi) = \frac{1}{|\mathcal{G}_P|} \sum_{\pi\in\Gamma} \prod_{i=1}^{n} x_i^{\lambda_i(\pi)}.$$

When $\Gamma = \mathcal{G}_P$, then $\mathcal{Z}_{(\mathcal{G}_P,P)}(\mathcal{G}_P)$ is called *the cycle index* of $\mathcal{G}_P$ on P, or shortly $\mathcal{Z}_{(\mathcal{G}_P,P)}$.

It should be emphasized that the natural number n, in the previous definition, is the upper limit regarding the number of indeterminates of cycle index polynomial. The actual number of indeterminates that could appear in the cycle index polynomial is $\lambda(n)$, that is the maximal order among of all orders of elements in $\mathcal{G}_P$.

Directly from the previous definition, we have this simple observation.

LEMMA 2.1. *Let $\mathcal{G}_P$ be a permutation group acting on a set P of n elements and let $\Gamma = \{\Gamma_i \subseteq \mathcal{G}_P \,|\, 1 \leqslant i \leqslant k, k \in N\}$ be a partition of the set of elements of $\mathcal{G}_P$. Then, the cycle index of $\mathcal{G}_P$ on P is $\mathcal{Z}_{(\mathcal{G}_P,P)} = \sum_{i=1}^{k} \mathcal{Z}_{(\Gamma_i,\mathcal{G}_P)}(\mathcal{G}_P)$.*

PROOF. It is a direct consequence of Definition 2.1 and the fact that $\mathcal{G}_P$ is disjoint union of Γ_i, $i = 1, 2, \dots, k$, i.e., $\mathcal{G}_P = \biguplus_{i=1}^{k} \Gamma_i$. □

This notion of partial cycle index will be helpful later. Let us introduce the notion of (r, k)-coprime residue set in $\mathbb{Z}_n$.

DEFINITION 2.3. Let n be a natural integer and let k be a divisor of n. Denote by r a natural integer less than k and coprime with k. The set of integers

$$\mathcal{U}_n^r(k) = \{x \in \mathcal{U}_n \mid x \equiv r \pmod{k}\}$$

is called (r, k)-coprime residue set in $\mathbb{Z}_n$.

We prove that any (r, k)-coprime set in $\mathbb{Z}_n$ is not empty. It is essentially restatement and slight modification of the result given in Lemma 2, page 32, [**6**]. This result will be helpful later, in the characterization of orbits of the examined group action.

LEMMA 2.2. *Let r, k, l, n be natural numbers such that* $\gcd(r, k) = 1$*, $r < k$ and $n = kl$. Then the (r, k)-coprime set $\mathcal{U}_n^r(k)$ is nonempty.*

PROOF. We prove for given r, k and n and $\gcd(r, k) = 1$, there exists t such that $\gcd(r + kt, n) = 1$ Let $p_i^{v_i}$ be a prime power dividing n. Then, there exists t_i such that $\gcd(r + kt_i, p_i^{v_i}) = 1$. Namely, if $p_i \mid k$, then $p_i \nmid r$ and $t_i = 0$ suffices. If $p_i \nmid k$, than any number t_i such that $t_i \not\equiv -r/k \pmod{p_i}$ will work.

By Chinese Reminder Theorem, there exists t such that $t \equiv t_i \pmod{p_i}$ and $\gcd(r + kt, n) = 1$. We need to prove that there exists $x \in \mathcal{U}_n$ such that $x \equiv r \pmod{k}$. Let $x \equiv r + kt \pmod{n}$. Since $k \mid n$ then $x \equiv r \pmod{k}$. Also, it is easy to see that $\gcd(x, n) = 1$ and therefore $x \in \mathcal{U}_n$. □

We introduce, without proof, the following textbook lemma.

LEMMA 2.3. *Let $C_n = \langle a \rangle$ be a cyclic group of n elements and let d be a natural number such that $d \mid n$. By A_d denote the set of all elements of C_n of order d. Then*

$$A_d = \{a^{\frac{n}{d}t} \mid t \in \mathbb{N} \text{ and } \gcd(t, d) = 1\}.$$

Hence, $|A_d| = \phi(d)$. Also, $C_n = \biguplus_{d|n} A_d$.

Let Ω_n^d, where $d \mid n$, be the set of elements of additive order d in the $\mathbb{Z}_n$. Then, according to Lemma 2.3, we have $\mathbb{Z}_n = \biguplus_{d|n} \Omega_n^d$ and $|\Omega_n^d| = \phi(d)$. The partition of $\mathbb{Z}_n$, we just specified, will play an important role in the analysis of the group action, we are dealing with.

3. Cycle index of $\mathcal{U}_n$ – general case

As pointed in Introduction, we consider the natural group action of the group $\mathcal{U}_n$ on the set of elements of $\mathbb{Z}_n$, given by $(x, a) \mapsto ax \pmod{n}$ $(a \in \mathcal{U}_n,\ x \in \mathbb{Z}_n)$.

Based on the results from the previous section, we prove that the typical orbit of the aforementioned group action is actually Ω_n^d.

LEMMA 3.1. *Let d, n be natural numbers, such that $d \mid n$. Then*

$$\Omega_n^d = \frac{n}{d} \cdot \mathcal{U}_d = \left\{ \frac{n}{d} t \mid 1 \leqslant t \leqslant d \text{ and } \gcd(t, d) = 1 \right\}.$$

Also, Ω_n^d is an orbit under the action of the group $\mathcal{U}_n$ on $\mathbb{Z}_n$.

PROOF. The first fact of the claim is a trivial consequence of Lemma 2.3, so we have $\Omega_n^d = \frac{n}{d} \cdot \mathcal{U}_d$. We prove that Ω_n^d is an orbit in the action of $\mathcal{U}_n$ on $\mathbb{Z}_n$.

Let x and y be elements of order d. Then we have $x = (n/d)k_1$ and $y = (n/d)k_2$ where $k_1, k_2 \in \mathcal{U}_d$. Therefore, there exists $k \in \mathcal{U}_d$ and $k_1 = kk_2$.

On the other hand, Lemma 2.2 claims that $\mathcal{U}_n^k(d)$ is nonempty, i.e., the existence of an element $h \in \mathcal{U}_n$ such that $h \equiv k \pmod{d}$. Clearly $k_1 \equiv hk_2 \pmod{d}$. By multiplying both sides by (n/d), we have $x \equiv hy \pmod{n}$. Thus, $\mathcal{U}_n$ is transitive on the set of elements of (additive) order d. $\square$

Let a, d be natural numbers such that $\gcd(a, d) = 1$. Denote by $o_d(a)$ the order of a with respect to modulo d, i.e., $o_d(a) = \min\{k \in \mathbb{N} \mid a^k \equiv 1 \pmod{d}\}$.

The following lemma has the key role in the description of how the mapping $\pi_a : \mathbb{Z}_n \mapsto \mathbb{Z}_n$, defined as $\pi_a(x) = ax \pmod{n}$, acts on an orbit Ω_n^d.

LEMMA 3.2. *Let d, n, a be natural numbers such that $d \mid n$ and $\gcd(a, n) = 1$. Consider $\tau = \pi_a|_{\Omega_n^d}$, that is restriction of the mapping $\pi_a : \mathbb{Z}_n \mapsto \mathbb{Z}_n$, defined as $\pi_a(x) = ax \pmod{n}$, on Ω_n^d. In other words, $\tau(x) = ax \pmod{n}$, where $x \in \Omega_n^d$.*

Then, τ is a permutation of Ω_n^d and $\operatorname{ctype}(\tau) = x_k^m$, where $k = o_d(a)$, $m = \frac{\phi(d)}{k}$.

PROOF. We know, from Lemma 3.1, that Ω_n^d is an orbit of π_a, so we conclude that $\tau : \Omega_n^d \mapsto \Omega_n^d$. Since, π_a is a bijection, then τ is certainly injection on Ω_n^d. However, Ω_n^d is a finite set, so τ must be a bijection.

According to Lemma 3.1, an arbitrary element $c \in \Omega_n^d$ is of the form $c = \frac{n}{d}v$, where $\gcd(v, d) = 1$. Let us consider the cycle that c belongs to, considering the mapping τ. Suppose that s is the length of the cycle $(c \mapsto ac \mapsto a^2c \mapsto \cdots \mapsto a^{s-1}c)$.

From $a^k v \equiv v \pmod{d}$ it follows $(a^k - 1)v = dt$, for some $t \in \mathbb{Z}$. Therefore, $(a^k - 1)\frac{n}{d}v = nt$, that means $a^k c \equiv c \pmod{n}$. Since s is the least number such that $a^s c \equiv c \pmod{n}$, then $s \leqslant k$.

On the other hand, from $a^s c \equiv c \pmod{n}$, it follows $a^s v \equiv v \pmod{d}$. Since $\gcd(v, d) = 1$, we conclude $a^s \equiv 1 \pmod{d}$. However, $k = o_d(a)$ and thus $k \leqslant s$, so we finally get $k = s$. Since c is an arbitrary element in Ω_n^d, we conclude that every cycle of τ is of the same length $k = o_d(a)$. □

Corollary 3.1. *Let n, a be natural numbers such that $d \mid n$ and $\gcd(a, n) = 1$. Then the bijection $\pi_a : \mathbb{Z}_n \mapsto \mathbb{Z}_n$, defined as $\pi_a(x) = ax \pmod{n}$, has cyclic structure* $\operatorname{ctype}(a) = \prod_{d|n} x_{o_d(a)}^{\phi(d)/o_d(a)}$.

Accordingly, the cycle index of $\mathcal{U}_n$, acting on the set $\mathbb{Z}_n$, is

$$\mathcal{Z}_{(\mathcal{U}_n,\mathbb{Z}_n)} = \frac{1}{\phi(n)} \sum_{a\in\mathcal{U}_n} \prod_{d|n} x_{o_d(a)}^{\frac{\phi(d)}{o_d(a)}}. \tag{3.1}$$

We should notice that the number of indeterminates in the polynomial $\mathcal{Z}_{(\mathcal{U}_n,\mathbb{Z}_n)}$ is actually equal to the maximal multiplicative order among elements in $\mathcal{U}_n$, that is $\lambda(n) = \max\{o_n(a) \mid a \in \mathcal{U}_n\}$.

In number theory, λ is known as Charmichael's lambda function. As it is principally analysed and resolved in [**8**], for a natural number n represented as a product of powers of prime numbers $n = \prod_{i=1}^k p_i^{e_i}$, we have that $\lambda(n)$ is equal to the least common multiplier of $\lambda(p_i^{e_i})$, for $i = 1, \dots, k$. Thus,

$$\lambda(n) = \operatorname{lcm}(\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \dots, \lambda(p_k^{e_k})),$$

where

$$\lambda(p^e) = \begin{cases} \phi(p^e) & \text{if } p \text{ an odd prime, } e \geqslant 1 \\ \phi(2^e) & \text{if } p = 2,\ e \leqslant 2 \\ 2^{e-2} & \text{if } p = 2,\ e > 2. \end{cases}$$

Therefore, only indeterminates $x_1, x_2, \dots, x_{\lambda(n)}$ appear in the cycle index $\mathcal{Z}_{(\mathcal{U}_n,\mathbb{Z}_n)}$.

4. Cycle index of $\mathcal{U}_{p^m}$

In this section, we present a more comprehensive look over the cycle index of the group $\mathcal{U}_{p^m}$ acting on $\mathbb{Z}_{p^m}$. Since the algebraic structure of $\mathcal{U}_{p^m}$ differs in two basic cases: when $p = 2$ and when p is an odd prime number, we will consider both in the course of finding cycle index of $\mathcal{U}_n$.

Once a cycle index of $\mathcal{U}_{p^m}$, for a prime number p, is found, it will serve as a building block for compounding cycle index of $\mathcal{U}_n$, where n is naturally represented as a product of powers of prime numbers.

4.1. Cycle index of $\mathcal{U}_{2^m}$. We start with the case of $\mathcal{U}_{2^m}$ acting on $\mathbb{Z}_{2^m}$. First of all, we need to determine how elements of $\mathcal{U}_{2^m}$ look like, considering the fact that it is not a cyclic group for $m \geqslant 3$, but direct product $C_2 \times C_{2^{m-2}}$. Still, there is a way for all elements of $\mathcal{U}_{2^m}$ to be represented in a functional form.

Definition 4.1. An integer a is said to be a semi-primitive root modulo n if the order of a modulo n is equal to $\phi(n)/2$, where ϕ is the Euler function.

It is shown in [**9**] that 3 is a semi-primitive root modulo 2^m. Thus, the order of 3 modulo 2^m is 2^{m-2}, for any integer $m \geqslant 3$ and

$$\mathcal{U}_{2^m} = \{\pm 3^i \pmod{2^m} : i = 1, \dots, 2^{m-2}\}.$$

Then, the following lemma is just rewording of the previous fact.

Lemma 4.1. *For an arbitrary element $w \in \mathcal{U}_{2^m}$, if $m \geqslant 3$, there exists a unique pair (a, b), $a \in \{0, 1\}$ and $b \in \{0, 1, \dots, 2^{m-2} - 1\}$ such that $w = (-1)^a 3^b$.*

It might be useful to mention that 5 is also a semi-primitive for $\mathcal{U}_{2^m}$, $m \geqslant 3$.
The following corollaries are either obvious or direct consequences of Lemma 4.1.

Corollary 4.1. *Let $a = 3^{2^s r}$, $d = 2^l$, where $s \geqslant 0$, $r = 1, 3, \dots, 2^{m-2-s} - 1$, $l \geqslant 1$. Then*

$$o_d(a) = \begin{cases} 1 & \text{if } l = 1; s \geqslant 0, \\ 2 & \text{if } l = 2; s = 0, \\ 1 & \text{if } l = 2; s \geqslant 1, \\ 2^{l-2-s} & \text{if } l \geqslant 3; s < l - 2, \\ 1 & \text{if } l \geqslant 3; s \geqslant l - 2. \end{cases}$$

Corollary 4.2. *Let $a = -3^{2^s r}$, $d = 2^l$, where $s \geqslant 0$, $r = 1, 3, \dots, 2^{m-2-s} - 1$, $l \geqslant 1$. Then*

$$o_d(a) = \begin{cases} 1 & \text{if } l = 1; s \geqslant 0, \\ 1 & \text{if } l = 2; s = 0, \\ 2 & \text{if } l = 2; s \geqslant 1, \\ 2^{l-2-s} & \text{if } l \geqslant 3; s < l - 2, \\ 2 & \text{if } l \geqslant 3; s \geqslant l - 2. \end{cases}$$

Lemma 4.2. *Let us consider*

$$\Gamma_1 = \{3^{2^s r} \mid s = 0, 1, \dots, m - 3, \; r = 0, 1, 3, \dots, 2^{m-2-s} - 1\}$$

as a subset of the group $\mathcal{U}_{2^m}$, for $m \geqslant 3$. Then, the partial cycle index of this set is

$$\mathcal{Z}_{(\Gamma_1, \mathbb{Z}_{2^m})}(\mathcal{U}_{2^m}) = \frac{1}{2^{m-1}} \left(x_1^{2^m} + 2^{m-3} x_1^2 x_2 \prod_{l=3}^{m} x_{2^{l-2}}^2 + \sum_{t=0}^{m-4} 2^t x_1^{2^{m-1-t}} \prod_{i=0}^{t} x_{2^{i+1}}^{2^{m-2-t}} \right).$$

Proof. Since all orbits of the multiplicative action of the group $\mathcal{U}_{2^m}$ on $\mathbb{Z}_{2^m}$ are of the form $\Omega_{2^m}^{2^l}$, where $0 \leqslant l \leqslant m$, it is important to find out the behaviour of particular mappings $x \mapsto 3^{2^s r} x \pmod{n}$, where $x \in \mathbb{Z}_{2^m}$, on those orbits. As stated before, we are interested in *ctypes* of those mappings on $\Omega_{2^m}^{2^l}$. In order to find *ctype* of the mappings $3^{2^s r}$ is restricted on orbit $\Omega_{2^m}^{2^l}$, we use the results of Corollary 4.1.

Firstly, all elements from Γ_1 are fixing $\Omega_{2^m}^1 = \{0\}$ and $\Omega_{2^m}^2 = \{2^{m-1}\}$ as one-element orbits.

By considering parameter l in the result of Corollary 4.1, we distinguish two major cases: when $l < 3$ and when $l \geqslant 3$. Accordingly, the orbits

$$\Omega^1_{2^m} = \{0\},\ \Omega^2_{2^m} = \{2^{m-1}\},\ \Omega^{2^2}_{2^m} = \{2^{m-2}, 2^m - 2^{m-2}\}$$

should be treated separately. For example, for the mappings of the form 3^r, where $r = 1, 3, \dots, 2^{m-2-s} - 1$, we have $\operatorname{ctype}(3^r) = x_1^2 x_2 \prod_{l=3}^{m} x^2_{2^{l-2}}$.

The total number of these mappings from Γ_1 is 2^{m-3}. For those mappings from Γ_1 of the form $3^{2^s r}$, when $s \geqslant 1$, we have

$$\operatorname{ctype}(3^{2^s r}) = x_1^4 \prod_{l=3}^{s+2} x_1^{2^{l-1}} \prod_{l=s+3}^{m} x^{2^{s+1}}_{2^{l-2-s}} = x_1^{2^{s+2}} \prod_{l=s+3}^{m} x^{2^{s+1}}_{2^{l-2-s}}.$$

The total number of these elements is 2^{m-3-s}. Clearly, for $r = 0$, we get identity and ctype of it is $x_1^{2^m}$.

Finally, by adding all them together, after some elementary algebraic manipulation, we get a partial cycle index of the subset Γ_1

$$\mathcal{Z}_{(\Gamma_1, \mathbb{Z}_{2^m})}(\mathcal{U}_{2^m}) = \frac{1}{2^{m-1}} \left(x_1^{2^m} + 2^{m-3} x_1^2 x_2 \prod_{l=3}^{m} x^2_{2^{l-2}} + \sum_{t=0}^{m-4} 2^t x_1^{2^{m-1-t}} \prod_{i=0}^{t} x^{2^{m-2-t}}_{2^{i+1}} \right). \ \square$$

Lemma 4.3. *Let us consider*

$$\Gamma_2 = -\{3^{2^s r} \mid s = 0, 1, \dots, m-3,\ r = 0, 1, 3, \dots, 2^{m-2-s} - 1\},$$

as a subset of the group $\mathcal{U}_{2^m}$, for $m \geqslant 3$. Then, the partial cycle index of this set, $\mathcal{Z}_{(\Gamma_2, \mathbb{Z}_{2^m})}(\mathcal{U}_{2^m})$, is

$$\frac{1}{2^{m-1}} \left(x_1^2 x_2^{2^m - 2} + 2^{m-3} x_1^4 \prod_{l=3}^{m} x^2_{2^{l-2}} + x_1^2 \sum_{t=0}^{m-4} 2^t x_2^{2^{m-t-1}-1} \prod_{i=1}^{t} x^{2^{m-t-2}}_{2^{i+1}} \right).$$

Proof. Similarly, as in the proof of Lemma 4.2, we use the result from Corollary 4.2. Note that $\operatorname{ctype}(-1) = x_1^2 x_2^{2^m - 2}$. By using the same type of reasoning used to prove Lemma 4.2, we get the result. $\square$

Corollary 4.3. *Let Γ_1 and Γ_2 be subsets of the group $\mathcal{U}_{2^m}$, $m \geqslant 3$, as introduced in Lemmas 4.2 and 4.3. Then $\mathcal{U}_{2^m} = \Gamma_1 \uplus \Gamma_2$.*

Proof. According to Lemma 4.1, every number from $\mathcal{U}_{2^m}$, if not -1 or 1, has the form $(-1)^a 3^{2^s r}$ where $a \in \{0, 1\}$, $s \in \{0, 1, \dots, m-3\}$ and r is an odd number, so $\Gamma_1 \cup \Gamma_2 = \mathcal{U}_{2^m}$. Also, from the same lemma it follows that $\Gamma_1 \cap \Gamma_2 = \emptyset$. Hence, $\Gamma_1 \uplus \Gamma_2$ is a disjoint union and equal to $\mathcal{U}_{2^m}$. $\square$

LEMMA 4.4. *The cycle index $\mathcal{Z} = \mathcal{Z}_{(\mathcal{U}_{2^m},\mathbb{Z}_{2^m})}$ of the permutation group $\mathcal{U}_{2^m}$ acting on $\mathbb{Z}_{2^m}$ is*

$$\mathcal{Z} = x_1^2 \quad \text{if } m = 1,$$

$$\mathcal{Z} = \frac{1}{2}(x_1^4 + x_1^2 x_2) \quad \text{if } m = 2,$$

$$\mathcal{Z} = \frac{1}{2^{m-1}}(\mathcal{Z}_1 + \mathcal{Z}_2) \quad \text{if } m \geqslant 3, \text{ where}$$

$$\mathcal{Z}_1 = x_1^{2^m} + 2^{m-3}x_1^2 x_2 \prod_{l=3}^{m} x_{2^{l-2}}^2 + \sum_{t=0}^{m-4} 2^t x_1^{2^{m-1-t}} \prod_{i=0}^{t} x_{2^{i+1}}^{2^{m-2-t}},$$

$$\mathcal{Z}_2 = x_1^2 x_2^{2^m-2} + 2^{m-3}x_1^4 \prod_{l=3}^{m} x_{2^{l-2}}^2 + x_1^2 \sum_{t=0}^{m-4} 2^t x_2^{2^{m-t-1}-1} \prod_{i=1}^{t} x_{2^{i+1}}^{2^{m-t-2}}.$$

PROOF. The claim follows trivially for $m = 1$ and $m = 2$. For the case $m \geqslant 3$, we use the results given in Lemmas 4.2 and 4.3, combined with the fact given in Corollary 4.3, that $\mathcal{U}_{2^m} = \Gamma_1 \uplus \Gamma_2$. □

4.2. Cycle index od $\mathcal{U}_{p^m}$, where p is an odd, prime number. The following lemma considers the case of $\mathcal{U}_{p^m}$, where p is an od prime number. As it has been already noted, this group is cyclic and consequently, it is much easier to find its cycle index.

LEMMA 4.5. *Let p be an odd prime. The cycle type of the permutation group $\mathcal{U}_{p^m}$ acting on $\mathbb{Z}_{p^m}$ is*

$$\mathcal{Z}_{(\mathcal{U}_{p^m},\mathbb{Z}_{p^m})} = \frac{1}{\phi(p^m)} \sum_{k=1}^{\phi(p^m)} \prod_{i=0}^{m} x_{u(i,k)}^{v(i,k)},$$

where $v(i,k) = (\phi(p^i), k)$ and $u(i,k) = \dfrac{\phi(p^i)}{v(i,k)}$.

PROOF. It is well known that in the case of an odd prime p, the automorphism group $\mathcal{U}_{p^m}$ is cyclic [**10**]. Let β be a generator of $\mathcal{U}_{p^m}$. Then, $\mathrm{ord}(\beta) = \phi(p^m)$. It is an elementary fact that in an arbitrary group G and $g \in G$, such that $\mathrm{ord}(g) = n$ it holds that $\mathrm{ord}(g^k) = n/(k, n)$.

Since $o_{p^i}(\beta) = \phi(p^i)$, for $i = 0, 1, \dots, m$, we conclude that

$$o_{p^i}(\beta^k) = \frac{\phi(p^i)}{(k, \phi(p^i))}, \text{ for } i = 0, 1, \dots, m.$$

Now, the claim follows directly from (3.1). □

4.3. Cycle index of direct product of permutation groups. Since we found the cycle indices of all groups $\mathcal{U}_{p^m}$ when p is a prime number, there is a natural question if there exists a way to combine them together in order to obtain the cycle index of $\mathcal{U}_n$, where n is the product of those prime power components. Hence, we need something like the cycle index of the direct product of permutation groups.

Let G_1, G_2 be permutation groups acting on sets X_1, X_2 respectively. Let $G = G_1 \times G_2$ and $X = X_1 \times X_2$ be the direct product of corresponding groups and sets. For an element $x = (x_1, x_2)$ of X and an element $g = (g_1, g_2)$ of G, we define the action of g on x by $(g, a) \mapsto (g_1x_1, g_2x_2)$.

Evidently, G is a permutation group on X. Let P and Q be polynomials

$$P(x_1, x_2, \ldots, x_u) = \sum a_{i_1 i_2 \ldots i_u} x_1^{i_1} x_2^{i_2} \ldots x_u^{i_u},$$
$$Q(x_1, x_2, \ldots, x_v) = \sum b_{j_1 j_2 \ldots j_v} x_1^{j_1} x_2^{j_2} \ldots x_v^{j_v}$$

In [**5**] the following product operator was defined

$$P \circledast Q = \sum a_{i_1 i_2 \ldots i_u} b_{j_1 j_2 \ldots j_v} \prod_{\substack{1 \leqslant l \leqslant u \\ 1 \leqslant m \leqslant v}} (x_l^{i_1} \circledast x_m^{j_m}),$$

where $x_l^{i_1} \circledast x_m^{j_m} = x_{\operatorname{lcm}(l,m)}^{i_1 j_m \gcd(l,m)}$.

We need the following lemma. For proof, see [**1, 5**].

Lemma 4.6. *The cycle index of the natural action of permutation group $G_1 \times G_2$ on $X_1 \times X_2$ induced by actions G_1 on X_1 and G_2 on X_2 can be expressed as:*

$$\mathcal{Z}_{(G_1 \times G_2, X_1 \times X_2)} = \mathcal{Z}_{(G_1, X_1)} \circledast \mathcal{Z}_{(G_2, X_2)}.$$

Let $n = \prod_{i=1}^{s} p_i^{\alpha_i}$. Applying the ring isomorphism $\mathbb{Z}_n \cong \bigoplus_{i=1}^{s} \mathbb{Z}_{p_i^{\alpha_i}}$, it follows that $\mathcal{U}_n \cong \bigoplus_{i=1}^{s} \mathcal{U}_{p_i^{\alpha_i}}$. Hence, according to Lemma 4.6, we have

$$\mathcal{Z}_{(\mathcal{U}_n, \mathbb{Z}_n)} = \mathcal{Z}_{(\mathcal{U}_{p_1^{\alpha_1}}, \mathbb{Z}_{p_1^{\alpha_1}})} \circledast \mathcal{Z}_{(\mathcal{U}_{p_2^{\alpha_2}}, \mathbb{Z}_{p_2^{\alpha_2}})} \circledast \cdots \circledast \mathcal{Z}_{(\mathcal{U}_{p_s^{\alpha_s}}, \mathbb{Z}_{p_s^{\alpha_s}})}.$$

Since the cycle indices of prime power components are given in Lemmas 4.4 and 4.5, the cycle index $\mathcal{Z}_{(\mathcal{U}_n, \mathbb{Z}_n)}$ can be calculated as above.

Example 4.1. Let us find the cycle index of $\mathcal{U}_{60}$. From Lemmas 4.4 and 4.5, we know that

$$\mathcal{Z}_{(\mathcal{U}_{2^2}, \mathbb{Z}_{2^2})} = \frac{1}{2}(x_1^4 + x_1^2 x_2), \mathcal{Z}_{(\mathcal{U}_3, \mathbb{Z}_3)} = \frac{1}{2}(x_1^3 + x_1 x_2), \mathcal{Z}_{(\mathcal{U}_5, \mathbb{Z}_5)} = \frac{1}{4}(x_1^5 + 2x_1 x_4 + x_1 x_2^2).$$

Therefore, and according to Lemma 4.6 $\mathcal{Z}_{(\mathcal{U}_{60}, \mathbb{Z}_{60})} = \mathcal{Z}_{(\mathcal{U}_{2^2}, \mathbb{Z}_{2^2})} \circledast \mathcal{Z}_{(\mathcal{U}_3, \mathbb{Z}_3)} \circledast \mathcal{Z}_{(\mathcal{U}_5, \mathbb{Z}_5)}$.

Firstly, we calculate the product of the first two cycle indices, that actually is $\mathcal{Z}_{(\mathcal{U}_{12}, \mathbb{Z}_{12})}$. So,

$$\begin{aligned}\mathcal{Z}_{(\mathcal{U}_{12}, \mathbb{Z}_{12})} &= \mathcal{Z}_{(\mathcal{U}_{2^2}, \mathbb{Z}_{2^2})} \circledast \mathcal{Z}_{(\mathcal{U}_3, \mathbb{Z}_3)} \\ &= \frac{1}{2}(x_1^4 + x_1^2 x_2) \circledast \frac{1}{2}(x_1^3 + x_1 x_2) = \frac{1}{4}(x_1^{12} + x_1^4 x_2^4 + x_1^2 x_2^5 + x_1^6 x_2^3).\end{aligned}$$

Finally, we get

$$\begin{aligned}\mathcal{Z}_{(\mathcal{U}_{60}, \mathbb{Z}_{60})} &= \mathcal{Z}_{(\mathcal{U}_{12}, \mathbb{Z}_{12})} \circledast \mathcal{Z}_{(\mathcal{U}_5, \mathbb{Z}_5)} \\ &= \frac{1}{4}(x_1^{12} + x_1^4 x_2^4 + x_1^2 x_2^5 + x_1^6 x_2^3) \circledast \frac{1}{4}(x_1^5 + 2x_1 x_4 + x_1 x_2^2) \\ &= \frac{1}{16}(x_1^{60} + 2x_1^4 x_2^4 x_4^{12} + x_1^4 x_2^{28} + 2x_1^2 x_2^5 x_4^{12} + x_1^2 x_2^{29} + 2x_1^6 x_2^3 x_4^{12} \\ &\qquad + x_1^6 x_2^{27} + 2x_1^{12} x_4^{12} + x_1^{12} x_2^{24} + x_1^{10} x_2^{25} + x_1^{20} x_2^{20} + x_1^{30} x_2^{15}).\end{aligned}$$

Certainly, the same result could be obtained by a simple application of (3.1).

5. Conclusions

We studied the group action of the automorphism group $\mathcal{U}_n = \mathrm{Aut}(\mathbb{Z}_n)$ on the set $\mathbb{Z}_n$, that is the set of residue classes modulo n. The main goal of the paper was to find the cycle index of that action. Based on some elementary number theory and algebraic techniques, we get a nice, compact result in Corollary 3.1. Also, in Lemmas 4.4 and 4.5, we provided a technically more detailed look at the building blocks of cycle index of the studied group action.

In the further research, as we announced in Introduction, it could be interesting to examine some combinatorial problems such as a problem of finding the number of orbits or equivalence classes of subsets of $\mathbb{Z}_n$. Namely, there is a natural way to induce the discussed group action on the set $\mathcal{O}_k$, standing for the set of all subsets of $\mathbb{Z}_n$ of size $k \leqslant n$ and then the task could be principally resolved by Pólya's theory application as in [**3**, **11**, **12**].

It is worth mentioning that the number of orbits of sets of $\mathcal{O}_k$ is related to the problem of factorizations of Abelian groups into the direct product of subsets that is examined in [**2**, **4**, **7**]. Hence, it seems that some further research in this topic could be very fruitful.

References

1. W. Wei, J. Xu, *Cycle index of direct product of permutation groups and number of equivalence classes of subsets of Z_v*, Discrete Math. **123**(1–3) (1993), 179–188.
2. V. Božović, N. Pace, *Factorization of groups using free mappings*, J. Algebra Appl. **7** (2008), 647–662.
3. N. G. De Bruijn, *A survey of generalizations of Pólya's enumeration theorem*, Nieuw Arch. Wiskd., III. Ser. **19** (1971), 89–112.
4. A. D. Sands, *On the factorization of finite groups*, J. Lond. Math. Soc. **2** (1974), 627–631.
5. M. A. Harrison, R. G. High, *On the cycle index of a product of permutation groups*, J. Comb. Theory **4** (1968), 277–299.
6. H. Cohn, *Advanced Number Theory*, Dover, 1980.
7. S. Szabó, *Topics in Factorization of Abelian Groups*, Birkhäuser, 2004.
8. R. D. Carmichael, *The Theory of Numbers*, Wiley, 1914.
9. C. F. Gauss, A. A. Clarke, *Disquisitiones Arithemeticae*, Springer, 1986.
10. H. J. Zassenhaus, *The Theory of Groups*, Dover, 1958.
11. G. Pólya, R. C. Read, *Combinatorial Enumeration of Groups, Graphs and Chemical Compounds*, Springer-Verlag, 1987.
12. N. G. De Bruijn, *Pólya Theory of Counting*, E. F. Wiley, 1964, 144–184.

Faculty of Natural Sciences and Mathematics
University of Montenegro
Podgorica
Montenegro
vladimirb@ac.me, vladobozovic@gmail.com
zanak@rc.pmf.ac.me

(Received 15 03 2016)
(Revised 06 11 2016)