ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 21 (2021) #P2.01
https://doi.org/10.26493/1855-3974.2129.ac1
(Also available at http://amc-journal.eu)

Classification of skew morphisms of cyclic groups which are square roots of automorphisms*

Kan Hu †

Department of Mathematics, Zhejiang Ocean University, Zhoushan, Zhejiang 316022, P.R. China, and
Key Laboratory of Oceanographic Big Data Mining & Application of Zhejiang Province, Zhoushan, Zhejiang 316022, P.R. China

Young Soo Kwon ‡

Department of Mathematics, Yeungnam University, Gyeongsan, 712-749, Republic of Korea

Jun-Yang Zhang §

School of Mathematical Sciences, Chongqing Normal University, Chongqing 401331, P.R. China

Received 29 September 2019, accepted 28 April 2021, published online 18 September 2021

Abstract

The auto-index of a skew morphism φ of a finite group A is the smallest positive integer h such that φ^h is an automorphism of A. In this paper we develop a theory of auto-index of skew morphisms, and as an application we present a complete classification of skew morphisms of finite cyclic groups which are square roots of automorphisms.

Keywords: Skew morphism, auto-index, period, square root.

Math. Subj. Class. (2020): 20B25, 05C10, 14H57

*The authors would like to thank Marston Conder for his suggestion of the concept of 'auto-index', and Kai Yuan for his help in verifying our examples by the Magma program.

†Supported by Natural Science Foundation of Zhejiang Province (LY16A010010, LQ17A010003).

‡Supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2018R1D1A1B05048450).

§Corresponding author. Supported by Basic Research and Frontier Exploration Project of Chongqing (No. cstc2018jcyjAX0010), Science and Technology Research Program of Chongqing Municipal Education Commission (No.KJQN201800512) and National Natural Science Foundation of China (11671276).

E-mail addresses: hukan@zjou.edu.cn (Kan Hu), ysookwon@ynu.ac.kr (Young Soo Kwon), jyzhang@cqnu.edu.cn (Jun-Yang Zhang)

1 Introduction

Throughout the paper, groups considered are all finite. A *skew morphism* of a group A is a permutation φ on A fixing the identity element of A and for which there is a function $\pi\colon A \to \mathbb{Z}_{|\varphi|}$ on A, called the *power function* of φ, such that $\varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b)$ for all $a, b \in A$. It is apparent the notion of skew morphism is a generalization of that of group automorphism. A skew morphism of A is called *proper* if it is not an automorphism. Two skew morphisms φ and φ' of A are *conjugate* if there exists an automorphism θ of A such that $\varphi' = \theta\varphi\theta^{-1}$.

The concept of skew morphism was first introduced by Jajcay and Širáň in [13] as an algebraic tool to study regular Cayley maps, which are regular embeddings of graphs on orientable closed surfaces admitting a regular subgroup of automorphisms on the vertices of the embedded graph. In this direction, regular Cayley maps of cyclic groups and dihedral groups have been classified, see [8, 21] and [14, 15, 16, 19, 28, 27]. In contrast, classification of regular Cayley maps of non-cyclic abelian groups and other metacyclic groups is still in progress; see [4, 5, 7, 20, 22, 26] for details.

The connection between skew morphisms and regular Cayley maps reveals a deep relationship between skew morphisms and group factorizations with cyclic complements. Indeed, if a group G is expressible as a product $A\langle y\rangle$ of a subgroup A and a cyclic subgroup $\langle y\rangle$ with $A \cap \langle y\rangle = 1$, then left multiplication of elements of A by y gives rise to a skew morphism φ of A, determined by $ya = \varphi(a)y^{\pi(a)}$ for all $a \in A$. Conversely, if φ is a skew morphism of a group A, then for any $a, b \in A$, we have

$$\varphi L_a(b) = \varphi(ab) = \varphi(a)\varphi^{\pi(a)}(b) = L_{\varphi(a)}\varphi^{\pi(a)}(b),$$

so $\langle\varphi\rangle L_A \subseteq L_A\langle\varphi\rangle$, where $L_A = \{L_a \mid a \in A\}$ is the left regular representation of A. Since $\langle\varphi\rangle \cap L_A = 1$, we have $|\langle\varphi\rangle L_A| = |L_A\langle\varphi\rangle|$, and hence $\langle\varphi\rangle L_A = L_A\langle\varphi\rangle$. Therefore, $G = L_A\langle\varphi\rangle$ is a factorization of a transitive permutation group with a cyclic complement, which is often referred to as the *skew-product group* of φ. The interested reader is referred to [6, 17] for more details.

A prominent problem in this field is the classification of skew morphisms of cyclic groups, which is closely related to regular Cayley maps [8] as well as edge-transitive embeddings of complete bipartite graphs [11]. Kovács and Nedela [17] showed that if $n = n_1n_2$ such that $\gcd(n_1, n_2) = 1$ and $\gcd(n_1, \phi(n_2)) = \gcd(\phi(n_1), n_2) = 1$, then every skew morphism φ of the cyclic additive group $\mathbb{Z}_n$ is a direct product $\varphi = \varphi_1 \times \varphi_2$ of skew morphisms φ_i of $\mathbb{Z}_{n_i}$, $i = 1, 2$. In a subsequent paper [18] the authors classified all skew morphisms of the cyclic groups $\mathbb{Z}_{p^e}$, where p is an odd prime. As for the case $p = 2$, the associated skew product groups are classified by Du and Hu in [9].

Recently, Bachratý and Jajcay introduced the notion of period of skew morphisms [1]. More precisely, the *period* of a skew morphism φ is the smallest positive integer d such that $\pi\big(\varphi^d(a)\big) = \pi(a)$ for all $a \in A$. In particular, if $d = 1$ then the skew morphism is said to be *smooth* (or *coset-preserving*). In [1, 23], it was shown that if φ is a skew morphism of period d, then φ^d is a smooth skew morphism. The smooth skew morphisms of cyclic groups and of dihedral groups were classified in [2] and [23] respectively. Let φ be a skew morphism of a group A with power function π. If for any $a \in A$ either $\pi(a) = \pi(\varphi(a)) = \cdots = \pi(\varphi^{|\varphi|-1}(a)) = 1$ or $\pi(a) = \pi(\varphi(a)) = \cdots = \pi(\varphi^{|\varphi|-1}(a)) = t$ where $|\varphi|$ is the order of φ and t is a fixed integer with $1 \le t < |\varphi|$, then φ is called *t-balanced*. Observe that every t-balanced skew morphism φ of a group A is necessarily smooth, and in particular φ^{t+1} is an automorphism of A (see [10] and Remark 3.2 in Section 3). Thus, any t-balanced skew morphism is a $(t+1)$-*th root* of a group automorphism.

Inspired by those results above, we propose the following two related problems:

Problem 1.1. Let A be a given group, and d a given positive integer.

(a) Classify all skew morphisms of A which are d-th roots of automorphisms of A.

(b) Classify all skew morphisms of A which have period d.

For $A = \mathbb{Z}_n$ and $d = 2$, the following main result of this paper is a solution to the first problem, and by Theorem 3.8 (a) in Section 4 it is also a partial solution to the second one (skew morphisms of period 2 of $\mathbb{Z}_n$ whose square is an automorphism are determined).

Theorem 1.2. *Every proper skew morphism of the cyclic additive group $\mathbb{Z}_n$ which is a square root of an automorphism is conjugate to a skew morphism of the form*

$$\varphi(x) \equiv sx - \frac{x(x-1)n}{2k} \pmod{n},$$

where the pair (k, s) of positive integers satisfy the following conditions:

(a) *k^2 divides n and $s \in \mathbb{Z}_n^*$ if k is odd, and $2k^2$ divides n and $s \in \mathbb{Z}_{n/2}^*$ if k is even,*

(b) *$s \equiv -1 \pmod{k}$, s has multiplicative order 2ℓ in $\mathbb{Z}_{n/k}$ and $\gcd(w, k) = 1$ where*

$$w = \frac{k}{n}(s^{2\ell} - 1) - \frac{s(s-1)}{2}\ell.$$

The power function of φ is given by $\pi(x) \equiv 1 + 2xw'\ell \pmod{m}$, where $w'w = 1 \pmod{k}$ and $m = 2k\ell$ is the order of φ. Moreover, two such skew morphisms corresponding to distinct integer pairs are not conjugate.

The paper is organized as follows. After a summary of preliminary results in Section 2, we develop a more comprehensive theory of powers of skew morphisms by defining a new notion called auto-index in Section 3. In Section 4 we show that if φ is a proper skew morphism of a group A which is a square root of an automorphism, then its power function has the property $\pi(xy) \equiv \pi(x) + \pi(y) - 1 \pmod{|\varphi|}$ for all $x, y \in A$; in particular, if $A = \mathbb{Z}_n$, then $\pi(x) \equiv (\pi(1) - 1)x + 1 \pmod{|\varphi|}$ for all $x \in \mathbb{Z}_n$. As an application of the theory, we present a proof of Theorem 1.2 in Section 5. Finally, for the special case when $n = p^e$ is a prime power, we enumerate proper skew morphisms of $\mathbb{Z}_n$ which are square roots of automorphisms in Section 6.

2 Preliminaries

In this section we summarize some preliminary results on skew morphisms for future reference.

Proposition 2.1 ([1, 13])**.** *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. Then for any positive integer k,*

$$\varphi^k(ab) = \varphi^k(a)\varphi^{\sigma(a,k)}(b), \qquad \text{for all} \quad a, b \in A,$$

where $\sigma(a,k) = \sum_{i=1}^{k} \pi(\varphi^{i-1}(a))$; moreover, φ^k is a skew morphism if and only if the congruence $kx \equiv \sigma(a,k) \pmod{m}$ is solvable for every $a \in A$.

Proposition 2.2 ([13]). *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. Then for any $a, b \in A$,*

$$\pi(ab) \equiv \sum_{i=1}^{\pi(a)} \pi(\varphi^{i-1}(b)) \pmod{m}.$$

Proposition 2.3 ([23]). *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. Then for any automorphism θ of A, $\varphi' = \theta\varphi\theta^{-1}$ is a skew morphism of A with power function $\pi' = \pi\theta^{-1}$.*

It follows that the automorphism group $\mathrm{Aut}(A)$ of A acts by conjugation on the set $\mathrm{Skew}(A)$ of all skew morphisms of A. Two skew morphisms of A are conjugate if they belong to the same orbit under such action.

An important subgroup related to skew morphisms is the *kernel* of φ defined by

$$\mathrm{Ker}\,\varphi = \{a \in A \mid \pi(a) \equiv 1 \pmod{m}\}.$$

It is well known that, for any $a, b \in A$, $\pi(a) \equiv \pi(b) \pmod{m}$ if and only if $ab^{-1} \in \mathrm{Ker}\,\varphi$, so π takes exactly $|A : \mathrm{Ker}\,\varphi|$ distinct values in $\mathbb{Z}_m$. The index $|A : \mathrm{Ker}\,\varphi|$ is called the *skew-type* of φ. It is obvious that φ is an automorphism if and only if it has skew-type 1. A skew morphism which is not an automorphism will be called *proper*.

The subset

$$\mathrm{Fix}\,\varphi = \{a \in A \mid \varphi(a) = a\}$$

of fixed-points of φ forms a subgroup of A. A subgroup N of A is *φ-invariant* if $\varphi(N) = N$. Clearly, $\mathrm{Fix}\,\varphi$ is φ-invariant, but $\mathrm{Ker}\,\varphi$ may not be. However, the subset

$$\mathrm{Core}\,\varphi = \bigcap_{i=1}^{m} \varphi^i(\mathrm{Ker}\,\varphi)$$

forms the largest φ-invariant subgroup of A contained in $\mathrm{Ker}\,\varphi$, and in particular, it is normal in A [28]. Thus $\mathrm{Ker}\,\varphi$ is φ-invariant if and only if $\mathrm{Ker}\,\varphi = \mathrm{Core}\,\varphi$, in which case the skew morphism is called *kernel-preserving*. It is apparent that if φ is kernel-preserving, then the restriction of φ to $\mathrm{Ker}\,\varphi$ is an automorphism of $\mathrm{Ker}\,\varphi$. The following result is well known.

Proposition 2.4 ([5]). *Every skew morphism of an abelian group is kernel-preserving.*

The importance of φ-invariant normal subgroups is reflected by the following result.

Proposition 2.5 ([29]). *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. If N a φ-invariant normal subgroup of A, then $\overline{\varphi}$ defined by $\overline{\varphi}(\overline{x}) = \overline{\varphi(x)}$ is a skew morphism of the quotient group $\overline{A} := A/N$. In particular, the order m_1 of $\overline{\varphi}$ is a divisor of m, and the power function $\overline{\pi}$ of $\overline{\varphi}$ is determined by $\overline{\pi}(\overline{a}) \equiv \pi(a) \pmod{m_1}$ for all $a \in A$.*

Since $\mathrm{Core}\,\varphi$ is a normal subgroup of A, φ induces a skew morphism $\overline{\varphi}$ of the quotient group $\overline{A} = A/\mathrm{Core}\,\varphi$. Define

$$\mathrm{Smooth}\,\varphi = \{a \in A \mid \overline{\varphi}(\overline{a}) = \overline{a}\},$$

which is the preimage of the fixed-point subgroup $\mathrm{Fix}\,\overline{\varphi}$ of $\overline{\varphi}$ under the natural epimorphism of A onto $A/\mathrm{Core}\,\varphi$. Since $\mathrm{Fix}\,\overline{\varphi}$ is a $\overline{\varphi}$-invariant subgroup of $\overline{A}$, $\mathrm{Smooth}\,\varphi$ is a φ-invariant subgroup of A.

In the extremal case that $\mathrm{Smooth}\,\varphi = A$, the skew morphism φ is called *smooth*. In [23] it is shown that a skew morphism φ of A is smooth if and only if $\pi(a) \equiv \pi(\varphi(a)) \pmod m$ for all $a \in A$. More generally, the *period* of φ is the smallest positive integer d such that $\pi(\varphi^d(a)) \equiv \pi(a) \pmod m$ for all $a \in A$. Thus, φ is smooth if and only if it has period 1. The following properties on the periodicity of skew morphisms are fundamental, see [23] for details.

Proposition 2.6 ([23])**.** *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. If φ has period d, then the following hold:*

(a) *d is equal to the order of the induced skew morphism $\overline{\varphi}$ of $\overline{A} = A/\mathrm{Core}\,\varphi$;*

(b) *d is the smallest positive integer such that φ^d is a smooth skew morphism of A;*

(c) *for any $a \in A$, $\sum_{i=1}^{d} \pi(\varphi^{i-1}(a)) \equiv 0 \pmod d$;*

(d) *conjugate skew morphisms have identical periods.*

Note that for any positive integer k, by Proposition 2.6 (a), if φ^k is a smooth skew morphism, then the period d of φ divides k.

3 Skew morphisms and automorphisms

Lemma 3.1. *Let φ be a skew morphism of a group A, and let $\pi\colon A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. Then for any positive integer k, φ^k is a group automorphism if and only if*

$$\sum_{i=1}^{k} \pi\big(\varphi^{i-1}(a)\big) \equiv k \pmod m$$

for all $a \in A$. In particular, if φ is smooth, then φ^k is an automorphism if and only if $k\pi(a) \equiv k \pmod m$ for all $a \in A$.

Proof. By Proposition 2.1, φ^k is a skew morphism of A if and only if the congruences

$$kx \equiv \sigma(a,k) \pmod m \tag{3.1}$$

are solvable for all $a \in A$, where

$$\sigma(a,k) = \sum_{i=1}^{k} \pi\big(\varphi^{i-1}(a)\big).$$

Note that if π_μ is the power function of $\mu := \varphi^k$, then $\pi_\mu(a)$ is the solution of (3.1), and therefore μ is an automorphism if and only if $\sigma(a,k) \equiv k \pmod m$ for all $a \in A$. In addition, if φ is smooth, then $\sigma(a,k) = k\pi(a)$, so μ is an automorphism if and only if $k\pi(a) \equiv k \pmod m$ for all $a \in A$. □

Remark 3.2. If φ is a t-balanced skew morphism of a group A, then φ is smooth and for all $a \in A\setminus\operatorname{Ker}\varphi$, $\pi(a) \equiv t \pmod m$ where $t^2 \equiv 1 \pmod m$ [5]. Therefore $(t+1)t \equiv t+1 \pmod m$. By Lemma 3.1, φ^{t+1} is a group automorphism. This is a generalization of [10, Lemma 3.4].

Definition 3.3. For a skew morphism φ of a group A, the *auto-index* of φ is defined to be the smallest positive integer h such that φ^h is a group automorphism of A.

Clearly, φ is an automorphism if and only if it has auto-index 1. Lower and upper bounds of the auto-index of a skew morphism are given as follows.

Lemma 3.4. *Let φ be a skew morphism of a group A. Suppose that φ has order m, period d and auto-index h, then d divides h and h divides m.*

Proof. Note that d is the smallest positive integer such that φ^d is a smooth skew morphism. Since φ^h is an automorphism which is necessarily smooth, the minimality of d implies that $d \mid h$. Since $\varphi^m = 1$ is the identity automorphism, the minimality of h implies that $h \mid m$, as required. □

Corollary 3.5. *If φ is a proper skew morphism of prime order, then it is smooth with auto-index equal to its order.*

Proof. Let d and h denote the period and auto-index of φ, respectively. As φ is proper, $d \le |A : \operatorname{Ker}\varphi| < |\varphi|$ and $h > 1$. By Lemma 3.4, d divides h and h divides $|\varphi|$. Since $|\varphi| = p$ is prime, we obtain $d = 1$ and $h = p$, as required. □

As an example of Corollary 3.5, $\varphi = (0)(153)(2)(4)$ is a proper skew morphism of the cyclic group $\mathbb{Z}_6$. It is smooth, and both its order and auto-index are equal to 3.

Lemma 3.6. *Let φ be a skew morphism of the cyclic group $\mathbb{Z}_n$ and let $\pi : \mathbb{Z}_n \to \mathbb{Z}_m$ be the associated power function, where m is the order of φ. If φ has period 2 and auto-index h, then h is an even positive divisor of m and there exists some $u \in \mathbb{Z}_h$ such that*

$$\pi(x) \equiv \big(\pi(1) - 1\big) \sum_{i=1}^{x} \Big(1 + \frac{um}{h}\Big)^{i-1} + 1 \pmod m, \quad \textit{for all } x \in \mathbb{Z}_n. \tag{3.2}$$

Proof. Since φ has period 2, by Proposition 2.6 (c), $\pi(x) + \pi(\varphi(x)) \equiv 0 \pmod 2$ for all $x \in \mathbb{Z}_n$. By Lemma 3.4, h is an even positive divisor of m. By Lemma 3.1, we have

$$h \equiv \sum_{i=1}^{h} \pi(\varphi^{i-1}(1)) \equiv \frac{1}{2}\Big(\pi(1) + \pi\big(\varphi(1)\big)\Big)h \pmod m,$$

and then

$$\frac{1}{2}\Big(\pi(1) + \pi\big(\varphi(1)\big)\Big) = 1 + um/h,$$

for some $u \in \mathbb{Z}_h$.

Moreover, since φ has period 2, by Proposition 2.6 (a), $\overline{\varphi}$ is an automorphism of order 2. Thus, $\pi(1) \equiv \overline{\pi}(\overline{1}) \equiv 1 \pmod 2$. Consequently, by Proposition 2.1, we have

$$\begin{aligned}\pi(2) \equiv& \sum_{i=1}^{\pi(1)} \pi\big(\varphi^{i-1}(1)\big)\\ \equiv& \pi(1) + \frac{\pi(1)-1}{2}\Big(\pi(1) + \pi\big(\varphi(1)\big)\Big)\\ \equiv& \pi(1) + \big(\pi(1)-1\big)(1+um/h)\\ \equiv& \big(\pi(1)-1\big)\big(1+(1+um/h)\big)+1 \pmod m.\end{aligned}$$

By induction, we obtain (3.2), as required. □

In what follows we study skew morphisms of auto-index 2. These skew morphisms are all square roots of automorphisms. Clearly, every permutation of order 2 on A is a square root of the identity automorphism of A. Generally, a square root of an automorphism of A maybe not a skew morphism of A. It seems too difficult to determine all square roots of automorphisms for a family of groups. In the following example, all square roots of nonidentity automorphisms of $\mathbb{Z}_8$ are determined.

Example 3.7. The cyclic group $\mathbb{Z}_8$ has three nonidentity automorphisms as follows:

$$\sigma_1 = (0)(2)(4)(6)(1,5)(3,7),\ \sigma_2 = (0)(4)(2,6)(1,3)(5,7),\ \sigma_3 = (0)(4)(2,6)(1,7)(5,3).$$

Since the square of every permutation of order 4 on $\mathbb{Z}_8$ either fixes no element or fixes 4 elements, σ_2 and σ_3 have no square roots. Set $\mu = (0)(2)(4)(6)(1,3,5,7)$ and use C_μ to denote the set of all square roots of the identity automorphism of $\mathbb{Z}_8$ which commute with μ. Then every square root of σ_1 can be represented as a product $\tau\mu$ where $\tau \in C_\mu$. It is straightforward to check that μ and μ^3 are the only two square roots of σ_1 which are skew morphisms. Since $\mu^3 = \sigma_3^{-1}\mu\sigma_3$, $\mathbb{Z}_8$ has a unique conjugate class of skew morphism of auto-index 2.

We are only concerned with square roots of automorphisms which are also skew morphisms. For convenience, skew morphisms of auto-index 2 are called *proper square roots of automorphisms* throughout this paper.

Theorem 3.8. *Let φ be a skew morphism of a group A, and let $\pi : A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. If φ is a proper square root of an automorphism, then*

(a) *φ is kernel-preserving of period at most 2;*

(b) *$\pi(x)$ is odd for all $x \in A$;*

(c) *$\pi(xy) \equiv \pi(x) + \pi(y) - 1 \pmod m$ for all $x, y \in A$;*

Proof. Take an arbitrary element $x \in A$. Since φ^2 is an automorphism and φ is not an automorphism, by Lemma 3.1, we have

$$\pi(x) + \pi(\varphi(x)) \equiv 2 \pmod m \quad \text{and} \quad \pi\big(\varphi(x)\big) + \pi\big(\varphi^2(x)\big) \equiv 2 \pmod m. \tag{3.3}$$

(a) From (3.3) we deduce $\pi(x) \equiv \pi\big(\varphi^2(x)\big) \pmod{m}$, so the period of φ is at most 2. In particular, we see that $\pi\big(\varphi(x)\big) = 1$ whenever $\pi(x) = 1$. It follows that φ is kernel-preserving.

(b) If φ has period 1, then $\pi(x) \equiv \pi\big(\varphi(x)\big) \pmod{m}$, and hence $2\pi(x) \equiv \pi(x) + \pi\big(\varphi(x)\big) \equiv 2 \pmod{m}$. Since φ is not an automorphism, m must be even. Since π is a group homomorphism from A to $\mathbb{Z}_m^*$ [23, Theorem 4.9], $\pi(x)$ is an odd integer. Now assume φ has period 2. Since φ is kernel-preserving, $\operatorname{Ker}\varphi = \operatorname{Core}\varphi$ is normal in A. By Proposition 2.6 (a), the induced skew morphism $\overline{\varphi}$ of $A/\operatorname{Ker}\varphi$ is an automorphism of order 2. Thus, $\pi(x) \equiv \overline{\pi}(\overline{x}) \equiv 1 \pmod{2}$, and $\pi(x)$ is also odd.

(c) By Proposition 2.2, we have

$$\begin{aligned}\pi(xy) \equiv &\sum_{i=1}^{\pi(x)} \pi(\varphi^{i-1}(y))\\ \equiv &\pi(y) + \frac{\pi(x)-1}{2}\big(\pi(y) + \pi(\varphi(y))\big)\\ \equiv &\pi(x) + \pi(y) - 1 \pmod{m}\end{aligned}$$

for all $x, y \in A$. □

Corollary 3.9. *Let φ be a proper square root of an automorphism of a group A, and let $\pi : A \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. Then*

(a) *if φ is smooth, then it has skew-type two, 4 divides m, and $\pi(x) = 1 + m/2$ for all $x \in A \setminus \operatorname{Ker}\varphi$;*

(b) *if φ is not smooth, then it has skew-type at least 3.*

Proof. If φ is smooth, then from the proof of Theorem 3.8, we see that m is even and $2\pi(x) \equiv 2 \pmod{m}$ for any $x \in A$. Hence $\pi(x) = 1$ or $1 + m/2$. Since φ is proper and $\pi(x)$ is odd, 4 divides m. If φ is not smooth, then the skew-type of φ is at least 3 since φ is kernel-preserving of period 2. □

Example 3.10 ([25])**.** The cyclic group $\mathbb{Z}_9$ has four skew morphisms of period 2:

$$\begin{aligned}
\varphi_1 &= (0)(1,2,7,5,4,8)(3,6), & \pi_1 &= [1][3,5,3,5,3,5][1,1];\\
\varphi_2 &= (0)(1,5,4,2,7,8)(3,6), & \pi_2 &= [1][3,5,3,5,3,5][1,1];\\
\varphi_3 &= (0)(1,8,4,5,7,2)(3,6), & \pi_3 &= [1][5,3,5,3,5,3][1,1];\\
\varphi_4 &= (0)(1,8,7,2,4,5)(3,6), & \pi_4 &= [1][5,3,5,3,5,3][1,1].
\end{aligned}$$

It can be directly verified that φ_i^2 $(i = 1,2,3,4)$ are automorphisms of $\mathbb{Z}_9$, so that all of these skew morphisms are proper square roots of automorphisms. Note that up to conjugation by automorphisms they are divided into two classes $\{\varphi_1, \varphi_4\}$ and $\{\varphi_2, \varphi_3\}$.

Example 3.11. Define two functions φ and π on the cyclic group $\mathbb{Z}_{8n}$ where n is a positive integer as follows:

$$\varphi(x) \equiv \begin{cases} 2i \pmod{8n}, & \text{if } x = 2i;\\ 2(n+i)+1 \pmod{8n}, & \text{if } x = 2i+1 \end{cases}$$

and

$$\pi(x) = \begin{cases} 1, & \text{if } x = 2i; \\ 3, & \text{if } x = 2i+1. \end{cases}$$

It is straightforward to check that φ is a skew morphism of $\mathbb{Z}_{8n}$ with power function π whose square is an involutory automorphism.

4 Technical lemmas

In what follows we restrict our discussion to proper square roots of automorphisms of the cyclic groups.

Lemma 4.1. *Let φ be a skew morphism of the cyclic group $\mathbb{Z}_n$, and let $\pi\colon \mathbb{Z}_n \to \mathbb{Z}_m$ be the power function of φ, where m is the order of φ. If φ is a proper square root of an automorphism and it has skew-type k, then the following hold:*

(a) *there is some integer $\ell \geq 1$ such that $m = 2k\ell$;*

(b) *there is some integer $u \in \mathbb{Z}_k^*$ such that $\pi(x) \equiv 1 + 2xu\ell \pmod m$ for all $x \in \mathbb{Z}_n$;*

(c) *the number $r = \varphi^2(1)$ is coprime to n and there exists some integer $v \in \mathbb{Z}_k^*$ such that $r^\ell \equiv 1 + vn/k \pmod n$;*

(d) *k^2 is a divisor of n;*

(e) *the multiplicative order of r in $\mathbb{Z}_{n/k}$ is equal to ℓ.*

Proof. By Theorem 3.8, φ has period 1 or 2 and

$$\pi(x+y) \equiv \pi(x) + \pi(y) - 1 \pmod m$$

for all $x, y \in \mathbb{Z}_n$. Thus $\pi(2) \equiv 2\pi(1) - 1 \equiv 2\big(\pi(1) - 1\big) + 1 \pmod m$ and by induction

$$\pi(x) \equiv x\big(\pi(1) - 1\big) + 1 \pmod m, \quad \forall x \in \mathbb{Z}_n.$$

In particular, $\pi(m) \equiv m\big(\pi(1) - 1\big) + 1 \equiv 1 \pmod m$, and therefore $m \in \operatorname{Ker}\varphi$. Since φ is of skew-type k, $\operatorname{Ker}\varphi = \langle k \rangle$, and hence $k \mid m$. Noting that

$$1 \equiv \pi(k) \equiv k\big(\pi(1) - 1\big) + 1 \pmod m,$$

we get $\pi(1) = 1 + um/k$ for some $u \in \mathbb{Z}_k$. Consequently, $\pi(x) \equiv 1 + xum/k \pmod m$. Since π takes k distinct values of the form $1 + im/k$ $(i = 0, 1, \ldots, k-1)$ in $\mathbb{Z}_m$, we have $u \in \mathbb{Z}_k^*$. By Theorem 3.8, $1 + m/k$ is odd, that is, m/k is even. Thus we can write $m = 2k\ell$, where ℓ is a positive integer. Then $\pi(x) \equiv 1 + 2xu\ell \pmod m$.

Set $r = \varphi^2(1)$. Since $\varphi^2 \in \operatorname{Aut}(\mathbb{Z}_n)$, r is coprime to n and $\varphi^2(x) \equiv rx \pmod n$ for all $x \in \mathbb{Z}_n$. In particular, $\varphi^{2\ell}(k) \equiv r^\ell k \pmod n$. On the other hand, there exists $u' \in \mathbb{Z}_n$ such that $\pi(u') \equiv 1 + 2\ell \pmod m$. Therefore

$$\varphi(k) + \varphi(u') \equiv \varphi(k + u') \equiv \varphi(u' + k) \equiv \varphi(u') + \varphi^{1+2\ell}(k) \pmod n$$

and then $\varphi^{2\ell}(k) = k$. Thus, $r^\ell \equiv 1 \pmod{n/k}$. Write $r^\ell = 1 + vn/k$. Recalling that φ has period at most 2, we have $\pi\big(\varphi^{2\ell}(1)\big) \equiv \pi(1) \pmod m$ and hence $\varphi^{2\ell}(1) \equiv 1$

$\pmod{k}$. It follows that $1 + vn/k \equiv r^\ell \equiv \varphi^{2\ell}(1) \equiv 1 \pmod{k}$, and hence k is a divisor of vn/k. Note that

$$\varphi^{2\ell j}(1) \equiv r^{\ell j} \equiv \Big(1 + \frac{vn}{k}\Big)^j \equiv 1 + \frac{jvn}{k} + \sum_{i=2}^{j} \binom{j}{i} \Big(\frac{vn}{k}\Big)^i \equiv 1 + \frac{jvn}{k} \pmod{n}$$

for any positive integer j. By [29, Lemma 3.1], the length of the orbit of 1 under φ is equal to the order $m = 2k\ell$ of φ. If $0 < j < k$, then $1 \not\equiv \varphi^{2j\ell}(1) \equiv 1 + jvn/k \pmod{n}$. Consequently, $v \in \mathbb{Z}_k^*$ and k^2 divides n.

If the multiplicative order of r in $\mathbb{Z}_{n/k}$ is i, then $r^i = 1 + tn/k$ for some positive integer t. Since $r^\ell \equiv 1 \pmod{n/k}$, we have $i \mid \ell$. On the other hand, since $k^2 \mid n$ for all $x \in \mathbb{Z}_n$, we have

$$\varphi^{2ik}(x) \equiv r^{ik}x \equiv (1 + tn/k)^k x \equiv x \pmod{n}.$$

Since the order of φ is $2k\ell$, we get $\ell \mid i$, and therefore $\ell = i$. □

Corollary 4.2. *Let φ be a skew morphism of the cyclic group $\mathbb{Z}_n$. If φ is a proper square root of an automorphism, then the induced skew morphism $\overline{\varphi}$ of $\mathbb{Z}_n/\mathrm{Ker}\,\varphi$ maps each $\overline{x}$ to $-\overline{x}$.*

Proof. Let m and k be the order and the skew-type of φ, respectively. By Lemma 4.1, $m = 2k\ell$ for some positive integer ℓ, and

$$2 \equiv \pi(x) + \pi\big(\varphi(x)\big) \equiv 2 + 2\big(x + \varphi(x)\big)u\ell \pmod{2k\ell}$$

for all $x \in \mathbb{Z}_n$, where $u \in \mathbb{Z}_k^*$. Thus $2\big(x + \varphi(x)\big)u\ell \equiv 0 \pmod{2k\ell}$ and then $\varphi(x) \equiv -x \pmod{k}$, as required. □

The converse of Corollary 4.2 is generally not true, see [6, Theorem 6.5] for a counterexample. However, we have the following result.

Lemma 4.3. *Let φ be a proper skew morphism of the cyclic group $\mathbb{Z}_n$. If the induced skew morphism $\overline{\varphi}$ of $\mathbb{Z}_n/\mathrm{Ker}\,\varphi$ maps each $\overline{x}$ to $-\overline{x}$, then φ^2 is a skew morphism of skew-type at most 2. In particular, if the skew-type of φ is odd, then φ^2 is an automorphism of $\mathbb{Z}_n$.*

Proof. Throughout the proof, we denote the order and the skew-type of φ by m and k, and the power functions of φ and $\overline{\varphi}$ by π and $\overline{\pi}$, respectively.

If $k = 2$, then the result is obviously true. In what follows we assume $k > 2$. Since $\overline{\varphi}$ maps each $\overline{x}$ to $-\overline{x}$, $\overline{\varphi}$ is an automorphism of order 2. By Proposition 2.6 (a), φ has period 2. It follows that m is even, $\pi\big(\varphi^2(x)\big) \equiv \pi(x) \pmod{m}$ and $\pi\big(\varphi(x)\big) \equiv \pi(-x) \pmod{m}$ for all $x \in \mathbb{Z}_n$. Since $\pi(x) \equiv \overline{\pi}(\overline{x}) \equiv 1 \pmod{2}$, $\pi(x)$ is odd.

Take two arbitrary elements $x, y \in \mathbb{Z}_n$. By Proposition 2.2, we have

$$\pi(x + y) \equiv \sum_{i=1}^{\pi(x)} \pi(\varphi^{i-1}(y)) \equiv \pi(y) + \frac{\pi(x) - 1}{2}\big(\pi(y) + \pi(-y)\big) \pmod{m}.$$

In particular,

$$1 = \pi(x - x) \equiv \pi(-x) + \frac{\pi(x) - 1}{2}\big(\pi(x) + \pi(-x)\big) \pmod{m}, \tag{4.1}$$

$$1 = \pi(-x + x) \equiv \pi(x) + \frac{\pi(-x) - 1}{2}\big(\pi(x) + \pi(-x)\big) \pmod{m}, \tag{4.2}$$

$$\pi(2x) \equiv \pi(x) + \frac{\pi(x) - 1}{2}\big(\pi(x) + \pi(-x)\big) \pmod{m}, \tag{4.3}$$

$$\pi(-2x) \equiv \pi(-x) + \frac{\pi(-x) - 1}{2}\big(\pi(x) + \pi(-x)\big) \pmod{m}, \tag{4.4}$$

$$\pi(2x + 1) \equiv \pi(2x) + \frac{\pi(1) - 1}{2}\big(\pi(2x) + \pi(-2x)\big) \pmod{m}, \tag{4.5}$$

$$\pi(-2x - 1) \equiv \pi(-2x) + \frac{\pi(-1) - 1}{2}\big(\pi(2x) + \pi(-2x)\big) \pmod{m}. \tag{4.6}$$

Adding (4.1) to (4.2) and (4.3) to (4.4), we get

$$\frac{1}{2}\big(\pi(x) + \pi(-x)\big)^2 \equiv 2 \pmod{m}$$

and

$$\frac{1}{2}\big(\pi(x) + \pi(-x)\big)^2 \equiv \pi(2x) + \pi(-2x) \pmod{m}.$$

Thus,

$$\pi(2x) + \pi(-2x) \equiv 2 \pmod{m}. \tag{4.7}$$

Substituting 2 for $\pi(2x) + \pi(-2x)$ in (4.5) and (4.6) we obtain

$$\pi(2x + 1) \equiv \pi(2x) + \pi(1) - 1 \pmod{m}$$

and

$$\pi(-2x - 1) \equiv \pi(-2x) + \pi(-1) - 1 \pmod{m}.$$

It follows that

$$\pi(2x + 1) + \pi(-2x - 1) \equiv \pi(1) + \pi(-1) \pmod{m}. \tag{4.8}$$

From (4.7) and (4.8) we deduce that

$$\varphi^2(x + y) = \varphi^2(x) + \varphi^2(y)$$

if x is even, and

$$\varphi^2(x + y) = \varphi^2(x) + \varphi^{\pi(1)+\pi(-1)}(y)$$

if x is odd. Thus, φ^2 is a skew morphism of skew-type at most 2. In particular, if the skew-type k of φ is an odd number, then

$$\pi(1) + \pi(-1) \equiv \pi(k + 1) + \pi(k - 1) \equiv 2 \pmod{m}$$

and therefore φ^2 is an automorphism, as claimed. □

5 Classification

In this section, we classify proper square roots of automorphisms of $\mathbb{Z}_n$.

Theorem 5.1. *Define a quadratic polynomial over the ring* $(\mathbb{Z}_n, +, \times)$ *by*

$$\varphi(x) \equiv sx - \frac{x(x-1)n}{2k} \pmod{n}, \quad x \in \mathbb{Z}_n, \tag{5.1}$$

where k and s are positive integers satisfying the following conditions:

(a) *k^2 divides n and $s \in \mathbb{Z}_n^*$ if k is odd, and $2k^2$ divides n and $s \in \mathbb{Z}_{n/2}^*$ if k is even,*

(b) *$s \equiv -1 \pmod{k}$, s has multiplicative order 2ℓ in $\mathbb{Z}_{n/k}$ and* $\gcd(w,k) = 1$ *where*

$$w = \frac{k}{n}(s^{2\ell} - 1) - \frac{s(s-1)}{2}\ell.$$

Then φ is a proper square root of an automorphism of the cyclic additive group $\mathbb{Z}_n$ whose skew-type is k and power function is given by

$$\pi(x) \equiv 1 + 2xw'\ell \pmod{m},$$

where $w'w \equiv 1 \pmod{k}$ and $m = 2k\ell$ is the order of φ. Moreover, up to conjugation φ is uniquely determined by the parameters k and s.

Proof. First, we show that φ is a permutation on $\mathbb{Z}_n$. Assume $\varphi(x) \equiv \varphi(y) \pmod{n}$ where $x, y \in \mathbb{Z}_n$. Then it suffices to prove that $x \equiv y \pmod{n}$. Since

$$sx - \frac{x(x-1)n}{2k} \equiv sy - \frac{y(y-1)n}{2k} \pmod{n},$$

we get

$$s(x-y) \equiv \frac{(x-y)(x+y-1)n}{2k} \pmod{n}.$$

By (a) and (b) we have $s \in \mathbb{Z}_n^*$. Thus, from the above equation we deduce that $x - y \equiv 0 \pmod{n/k}$. By (a) again we obtain

$$\frac{(x-y)(x+y-1)n}{2k} \equiv 0 \pmod{n},$$

and hence $x \equiv y \pmod{n}$.

Second, we show that φ^2 is an automorphism of $\mathbb{Z}_n$. By (a) and (b), we derive from formula (5.1) that

$$\varphi\Big(\frac{jn}{k}\Big) \equiv \frac{sjn}{k} - \frac{jn(jn-k)n}{2k^3} \equiv -\frac{jn}{k} \pmod{n} \tag{5.2}$$

for all positive integers j. Now for any $x, y \in \mathbb{Z}_n$,

$$\begin{aligned}\varphi(x+y) &\equiv s(x+y) - \frac{(x+y)(x+y-1)n}{2k} \\ &\equiv sx - \frac{x(x-1)n}{2k} + sy - \frac{y(y-1)n}{2k} - \frac{xyn}{k} \\ &\equiv \varphi(x) + \varphi(y) - \frac{xyn}{k} \pmod{n}.\end{aligned}$$

It follows that

$$\begin{aligned}
\varphi^2(x) &\equiv \varphi\Big(sx - \frac{x(x-1)n}{2k}\Big)\\
&\equiv \varphi(sx) + \varphi\Big(-\frac{x(x-1)n}{2k}\Big) + \frac{n}{k}\frac{sx^2(x-1)n}{2k}\\
&\equiv \varphi(sx) + \varphi\Big(-\frac{x(x-1)n}{2k}\Big)\\
&\overset{(5.2)}{\equiv} s^2x - \frac{sx(sx-1)n}{2k} + \frac{x(x-1)n}{2k}\\
&\equiv \Big(s^2 - \frac{s(s-1)n}{2k}\Big)x - \frac{(s^2-1)x(x-1)n}{2k}\\
&\overset{(b)}{\equiv} \Big(s^2 - \frac{s(s-1)n}{2k}\Big)x \pmod{n}.
\end{aligned}$$

Since $s \in \mathbb{Z}_n^*$ and $k^2 \mid n$, we have $\gcd\big(s^2 - \frac{s(s-1)n}{2k}, n\big) = 1$. Thus, φ^2 is an automorphism of $\mathbb{Z}_n$.

Next we show that φ is a skew morphism of $\mathbb{Z}_n$ with associated power function π defined by $\pi(x) \equiv 1 + 2w'\ell \pmod{m}$ for any $x \in \mathbb{Z}_n$, where $w'w \equiv 1 \pmod{k}$. Take arbitrary $x, y \in \mathbb{Z}_n$. By the conditions (a) and (b), we have

$$\begin{aligned}
\varphi(x) + \varphi^{\pi(x)}(y) \equiv \varphi(x) + \varphi^{1+2xw'\ell}(y) &\equiv \varphi(x) + \varphi^{2xw'\ell}(\varphi(y))\\
&\equiv \varphi(x) + \varphi(y)\Big(s^2 - \frac{s(s-1)n}{2k}\Big)^{\ell w'x}\\
&\equiv \varphi(x) + \varphi(y)\Big(s^{2\ell} - \frac{s(s-1)\ell n}{2k}\Big)^{w'x}\\
&\equiv \varphi(x) + \varphi(y)\Big(1 + \frac{wn}{k}\Big)^{w'x}\\
&\equiv \varphi(x) + \varphi(y)\Big(1 + \frac{nx}{k}\Big) \pmod{n}
\end{aligned}$$

and

$$\begin{aligned}
\varphi(x+y) \equiv \varphi(x) + \varphi(y) - \frac{nxy}{k} &\equiv \varphi(x) + \Big(sy - \frac{y(y-1)n}{2k}\Big) - \frac{nxy}{k}\\
&\equiv \varphi(x) + \Big(sy - \frac{y(y-1)n}{2k}\Big) + \frac{snxy}{k}\\
&\equiv \varphi(x) + \Big(sy - \frac{y(y-1)n}{2k}\Big)\Big(1 + \frac{nx}{k}\Big)\\
&\equiv \varphi(x) + \varphi(y)\Big(1 + \frac{nx}{k}\Big) \pmod{n}.
\end{aligned}$$

Therefore, $\varphi(x+y) \equiv \varphi(x) + \varphi^{\pi(x)}(y)$ and thus φ is a skew morphism of $\mathbb{Z}_n$.

Finally, we prove that up to conjugation φ is uniquely determined by the parameters k and s. It is evident that if two such skew morphism are conjugate, then they must have the same skew-type k. Suppose now that φ_i $(i = 1, 2)$ are two conjugate skew morphisms of $\mathbb{Z}_n$ defined by

$$\varphi_i(x) \equiv s_i x - \frac{x(x-1)n}{2k} \pmod{n},$$

where n, k and s_i satisfy the stated conditions. Then there exists an automorphism θ of $\mathbb{Z}_n$ such that $\varphi_1\theta = \theta\varphi_2$. Set $r = \theta(1)$. Then

$$s_1 rx - \frac{rx(rx-1)n}{2k} \equiv \varphi_1\theta(x) \equiv \theta\varphi_2(x) \equiv s_2 rx - \frac{rx(x-1)n}{2k} \pmod{n}.$$

Since $\gcd(r, n) = 1$, this is reduced to

$$s_1 x - \frac{x(rx-1)n}{2k} \equiv s_2 x - \frac{x(x-1)n}{2k} \pmod{n},$$

or equivalently,

$$(s_1 - s_2)x \equiv \frac{x(rx-1)n}{2k} - \frac{x(x-1)n}{2k} \equiv \frac{x^2(r-1)n}{2k} \pmod{n}.$$

If we choose $x = \pm 1$, then $\pm(s_1 - s_2) \equiv (r-1)n/2k \pmod{n}$. Therefore $2(s_1 - s_2) \equiv 0 \pmod{n}$ and $r \equiv 1 \pmod{k}$. If k is even, so is n, and hence $s_1 \equiv s_2 \pmod{n/2}$. If both k and n are odd, then $s_1 \equiv s_2 \pmod{n}$. If k is odd but n is even, then r is odd. Since $r \equiv 1 \pmod{k}$, we obtain $r - 1 \equiv 0 \pmod{2k}$. Thus, we also get $s_1 \equiv s_2 \pmod{n}$, as required. □

Now we are ready to prove the main result of the paper.

Proof of Theorem 1.2. By Theorem 5.1, the quadratic polynomial of the stated form is a proper square root of an automorphism of $\mathbb{Z}_n$, and distinct pairs (k, s) correspond to disconjugate skew morphisms.

Conversely, suppose that φ is a proper square root of an automorphism of $\mathbb{Z}_n$ of skew-type $k > 1$. By Lemma 4.1, $k^2 \mid n$, $|\varphi| = 2k\ell$ for some positive integer ℓ, and the power function of φ is given by $\pi(x) \equiv 1 + 2xu\ell \pmod{2k\ell}$ for some $u \in \mathbb{Z}_k^*$. Set $s = \varphi(1)$. By Lemma 3.1, we have

$$2 \equiv \pi(1) + \pi(\varphi(1)) \equiv (1 + 2u\ell) + (1 + 2su\ell) \equiv 2 + 2(1+s)u\ell \pmod{2k\ell},$$

which implies $2(1+s)u\ell \equiv 0 \pmod{2kl}$. Since $u \in \mathbb{Z}_k^*$, we obtain $s \equiv -1 \pmod{k}$.

Since φ^2 is an automorphism of $\mathbb{Z}_n$, $\varphi^2(x) \equiv rx \pmod{n}$ for some r coprime to n. By Lemma 4.1, $r^\ell \equiv 1 + vn/k \pmod{n}$ for some $v \in \mathbb{Z}_k^*$. Then

$$\begin{aligned}\varphi(x) &\equiv \varphi(x-1) + \varphi^{\pi(x-1)}(1) \equiv \varphi(x-1) + \varphi^{2\ell u(x-1)+1}(1)\\ &\equiv \varphi(x-1) + \varphi^{2\ell u(x-1)}(s) \equiv \varphi(x-1) + sr^{\ell u(x-1)}\\ &\equiv \varphi(x-1) + s\Big(1 + \frac{vn}{k}\Big)^{u(x-1)} \pmod{n}.\end{aligned}$$

By induction we obtain

$$\varphi(x) \equiv s\sum_{i=1}^{x}\Big(1 + \frac{vn}{k}\Big)^{u(i-1)} \pmod{n}, \quad x \in \mathbb{Z}_n.$$

Since $k^2 \mid n$, for any positive integer j, we have

$$\Big(1 + \frac{vn}{k}\Big)^j \equiv 1 + \frac{jvn}{k} + \sum_{i=2}^{j}\binom{j}{i}\Big(\frac{vn}{k}\Big)^i \equiv 1 + \frac{jvn}{k} \pmod{n}.$$

Thus,

$$\begin{aligned}\varphi(x) \equiv& s\sum_{i=1}^{x}\Big(1+\frac{vn}{k}\Big)^{u(i-1)} \equiv s\sum_{i=1}^{x}\Big(1+\frac{uvn(i-1)}{k}\Big)\\ \equiv& s\Big(x+\frac{uvnx(x-1)}{2k}\Big) \equiv sx-\frac{uvnx(x-1)}{2k} \pmod n.\end{aligned}$$

It follows that

$$r=\varphi^2(1)=\varphi(s)\equiv s^2-\frac{uvns(s-1)}{2k} \pmod n. \tag{5.3}$$

Hence, $r\equiv s^2 \pmod{n/k}$ and by Lemma 4.1 (e), s has multiplicative order 2ℓ in $\mathbb{Z}_{n/k}$.

Since

$$\begin{aligned}1+\frac{vn}{k} \equiv& r^\ell \equiv \Big(s^2-\frac{s(s-1)uvn}{2k}\Big)^\ell\\ \equiv& s^{2\ell}-\binom{\ell}{1}s^{2(\ell-1)}\frac{s(s-1)uvn}{2k}+\sum_{i=2}^{\ell}\binom{\ell}{i}s^{2(\ell-i)}\Big(-\frac{s(s-1)uvn}{2k}\Big)^i\\ \equiv& s^{2\ell}-\frac{s^{2(\ell-1)}s(s-1)\ell uvn}{2k} \equiv s^{2\ell}-\frac{s(s-1)\ell uvn}{2k} \pmod n,\end{aligned}$$

we have

$$s^{2\ell}\equiv 1+\Big(1+\frac{s(s-1)\ell u}{2}\Big)\frac{vn}{k} \pmod{n/k}.$$

By [12, Lemma 1], there exists $c\in\mathbb{Z}_n^*$ such that $c\equiv uv \pmod k$. Define $\varphi' := \theta_c\varphi\theta_c^{-1}$, where θ_c is the automorphism of $\mathbb{Z}_n$ taking 1 to c. By Proposition 2.3, φ' is a skew morphism of $\mathbb{Z}_n$. For all $x\in\mathbb{Z}_n$, we have

$$\begin{aligned}\varphi'(x) =& \theta_c\varphi\theta_c^{-1}(x)=\theta_c\varphi(c^{-1}x)\equiv c\Big(sc^{-1}x-\frac{c^{-1}x(c^{-1}x-1)cn}{2k}\Big)\\ \equiv& sx-\frac{x(x-c)n}{2k} \equiv \Big(s+\frac{(c-1)n}{2k}\Big)x-\frac{x(x-1)n}{2k} \pmod n.\end{aligned}$$

Let $s' = s+\frac{(c-1)n}{2k}$, then it is easily seen that $s'\equiv -1 \pmod k$, $s'\in\mathbb{Z}_n^*$, and s' has multiplicative order 2ℓ in $\mathbb{Z}_{n/k}$. Therefore, up to conjugation we can assume

$$\varphi(x)\equiv sx-\frac{x(x-1)n}{2k} \pmod n \quad \text{and} \quad \pi(x)\equiv 1+2w'\ell x \pmod{2k\ell},$$

where $s\equiv -1 \pmod k$, $s\in\mathbb{Z}_n^*$, $w'\in\mathbb{Z}_k^*$, and 2ℓ is the multiplicative order of s in $\mathbb{Z}_{n/k}$.

We show that $ww'\equiv 1 \pmod k$, that is, w' is the modular inverse of w in $\mathbb{Z}_k$. Noting that the congruence

$$w\equiv \frac{k}{n}(s^{2\ell}-1)-\frac{s(s-1)}{2}\ell \pmod k$$

is equivalent to

$$s^{2\ell}-\frac{s(s-1)\ell n}{2k}\equiv 1+\frac{nw}{k} \pmod n,$$

we have

$$\begin{aligned}
2s-\frac{n}{k} &\equiv \varphi(2)\equiv \varphi(1)+\varphi^{\pi(1)}(1)\\
&\equiv s+\varphi^{2w'\ell}(s)\\
&\equiv s+s\Big(s^2-\frac{s(s-1)n}{2k}\Big)^{\ell w'}\\
&\equiv s+s\Big(s^{2\ell}-\frac{s(s-1)\ell n}{k}\Big)^{w'}\\
&\equiv s+s\Big(1+\frac{nw}{k}\Big)^{w'}\\
&\equiv 2s+\frac{sww'n}{k}\equiv 2s-\frac{nww'}{k} \pmod{n},
\end{aligned}$$

which is reduced to $ww'\equiv 1 \pmod{k}$.

In what follows we consider the particular case that k is even. We have

$$\varphi^2(2)=2\varphi^2(1)\equiv 2s^2-\frac{s(s-1)n}{k}\equiv 2s^2-\frac{2n}{k} \pmod{n}$$

and

$$\begin{aligned}
\varphi^2(2) &\equiv \varphi\Big(2s-\frac{n}{k}\Big)\equiv s\Big(2s-\frac{n}{k}\Big)-\Big(2s-\frac{n}{k}\Big)\big(2s-\frac{n}{k}-1\big)\frac{n}{2k}\\
&\equiv 2s^2-\frac{sn}{k}-\Big(s-\frac{n}{2k}\Big)(2s-1)\frac{n}{k}\\
&\equiv 2s^2-\frac{sn}{k}-\Big(2s^2-s-\frac{sn}{k}+\frac{n}{2k}\Big)\frac{n}{k}\\
&\equiv 2s^2-\frac{2s^2n}{k}-\frac{n^2}{2k^2}\equiv 2s^2-\frac{2n}{k}-\frac{n^2}{2k^2} \pmod{n}.
\end{aligned}$$

Thus,

$$2s^2-\frac{2n}{k}\equiv 2s^2-\frac{2n}{k}-\frac{n^2}{2k^2} \pmod{n},$$

and therefore $2k^2 \mid n$. Moreover, if $s>n/2$, then we write $s'=s-n/2$ and define

$$\varphi'(x)\equiv s'x-\frac{x(x-1)n}{2k} \pmod{n}, \qquad x\in\mathbb{Z}_n.$$

It is easily seen that φ' is also a square root of an automorphism of $\mathbb{Z}_n$. We show that φ' is conjugate to φ. Since $2k^2\mid n$, $n=2^ekn_1$ where $e\geq 1$ and $2\nmid n_1$. Note that the number $c:=kn_1+1$ is coprime to n. Let θ_c be the automorphism of $\mathbb{Z}_n$ taking x to cx. Then, for any $x\in\mathbb{Z}_n$,

$$\begin{aligned}
\varphi'\theta_c(x) &\equiv s'cx-\frac{cx(cx-1)n}{2k}\\
&\equiv (s-\frac{n}{2})cx-\frac{\big(cx(x-1)+c(c-1)x^2\big)n}{2k}\\
&\equiv scx-\frac{cx(x-1)n}{2k}+\frac{nx}{2}-\frac{c(c-1)x^2n}{2k}\\
&\equiv scx-\frac{cx(x-1)n}{2k}\equiv \theta_c\varphi(x) \pmod{n}.
\end{aligned}$$

Thus, φ is conjugate to φ', as required. □

Corollary 5.2. *Every smooth proper square root of an automorphism of the cyclic group $\mathbb{Z}_n$ is conjugate to a skew morphism of the form*

$$\varphi(x) \equiv sx - \frac{x(x-1)n}{4} \pmod{n}, \quad x \in \mathbb{Z}_n,$$

with the associated power function given by

$$\pi(x) \equiv 1 + 2\ell x \pmod{4\ell}, \quad x \in \mathbb{Z}_n,$$

where $8 \mid n$, both s and $\frac{2}{n}(s^{2\ell}-1) - \frac{s(s-1)}{2}\ell$ are odd numbers, and the multiplicative order of s in $\mathbb{Z}_{n/2}$ is equal to 2ℓ. In particular, φ has order 4ℓ and skew-type 2.

Proof. By Corollary 3.9, every smooth proper square root of an automorphism has skew-type 2. The result follows immediately from Theorem 1.2. □

Remark 5.3. Note that if φ is proper skew morphism of $\mathbb{Z}_n$ and φ^2 is an involutory automorphism, then $|\varphi| = 4$, and by Theorem 1.2, $k = 2$, $\ell = 1$ and φ is smooth.

Corollary 5.4. *Let φ be a non-smooth skew morphism of the cyclic group $\mathbb{Z}_n$. If φ has skew-type 3, then it is conjugate to a skew morphism of the form*

$$\varphi(x) \equiv sx - \frac{n}{6}x(x-1) \pmod{n}, \qquad x \in \mathbb{Z}_n,$$

where $9 \mid n$, $s \in \mathbb{Z}_n^*$ has multiplicative order 2ℓ in $\mathbb{Z}_{n/3}$, $s \equiv -1 \pmod{3}$ and

$$\frac{3}{n}(s^{2\ell} - 1) - \ell \equiv w' \not\equiv 0 \pmod{3}.$$

Moreover, the order of φ is $m = 6\ell$ and the power function of φ is given by

$$\pi(x) \equiv 1 + \frac{m}{3}w'x \pmod{m}.$$

Proof. Since φ is a non-smooth skew morphism of $\mathbb{Z}_n$ of skew-type 3, the induced skew morphism $\overline{\varphi}$ of $\mathbb{Z}_n/\mathrm{Ker}\,\varphi$ is an automorphism of the form $\overline{\varphi} = (\overline{0})(\overline{1}, -\overline{1})$. By Lemma 4.3, φ^2 is an automorphism. The result then follows from Theorem 1.2. □

By Theorem 1.2, we have the following special property of a square root of an automorphism of the cyclic group $\mathbb{Z}_n$.

Corollary 5.5. *Let φ be a proper square root of an automorphism of the cyclic group $\mathbb{Z}_n$. Then every subgroup of $\mathbb{Z}_n$ is φ-invariant.*

Proof. Let $H = \langle h \rangle$ be a subgroup of $\mathbb{Z}_n$. If φ and φ' are conjugate by an automorphism of $\mathbb{Z}_n$ and H is φ-invariant, then H is also φ'-invariant. So it suffices to consider the skew morphisms φ given by Theorem 1.2. Let k be the skew-type of φ. For any integer j,

$$\varphi(jh) \equiv sjh - \frac{jh(jh-1)n}{2k} \equiv h\left(sj - \frac{j(jh-1)n}{2k}\right) \pmod{n}.$$

If n is even, $\frac{n}{2k}$ is a positive integer, and if n is odd, then h is also odd and $\frac{j(jh-1)n}{2k}$ is a positive integer. This means that $\varphi(jh) \in H$, and hence H is φ-invariant. □

6 The prime power case

In this section, for the case where $n = p^e$ is a prime power, we enumerate the conjugacy classes of proper square roots of automorphisms of $\mathbb{Z}_n$.

We need a technical result from number theory.

Proposition 6.1 ([3, 24]). *Suppose that $n = p^e$, where p is a prime and $e \geq 1$. Then*

(a) *if $p > 2$, then $\mathbb{Z}_{p^e}^* \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{e-1}}$ is cyclic of order $p^{e-1}(p-1)$. In particular, for each i, $1 \leq i \leq e-1$, an element of the form $1 + up^{e-i}$ in $\mathbb{Z}_{p^e}^*$ has order p^i if and only if $p \nmid u$,*

(b) *if $p = 2$, then $\mathbb{Z}_{2^e}^*$ is trivial if $e = 1$, $\mathbb{Z}_{2^e}^* \cong \mathbb{Z}_2$ if $e = 2$, and $\mathbb{Z}_{2^e}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{e-2}}$ if $e \geq 3$. In particular, in the last case for each i, $2 \leq i \leq e-1$, an element of the form $\pm 1 + u2^i$ in $\mathbb{Z}_{2^e}^*$ has order 2^{e-i} if and only if $2 \nmid u$.*

Let $N(p^e)$ denote the number of conjugacy classes of proper square roots of automorphisms of $\mathbb{Z}_{p^e}$. Then $N(p^e)$ is determined in the following theorem.

Theorem 6.2. *Suppose that p is a prime and $e \geq 1$. If $p \neq 2$, then*

$$N(p^e) = \begin{cases} \frac{1}{p-1}(p^{\frac{e}{2}} - 1)^2, & \text{if } e \text{ is even} \\ \frac{1}{p-1}(p^{\frac{e+1}{2}} - 1)(p^{\frac{e-1}{2}} - 1), & \text{if } e \text{ is odd}, \end{cases}$$

while if $p = 2$, then

$$N(2^e) = \begin{cases} 0, & \text{if } e < 3 \\ 1, & \text{if } e = 3 \\ 2^{e-1} - 3 \cdot 2^{\frac{e-2}{2}}, & \text{if } e > 3 \text{ is even} \\ 2^{e-1} - 2^{\frac{e+1}{2}}, & \text{if } e > 3 \text{ is odd}. \end{cases}$$

Proof. Denote $n = p^e$ and $k = p^f$. Then for fixed prime p and integer $e \geq 1$, by Theorem 1.2, $N(p^e)$ is equal to the number of pairs (f, s) which satisfy the following conditions:

(a) $2 \leq 2f \leq e$ and $s \in \mathbb{Z}_{p^e}^*$ if $p \neq 2$, and $2 \leq 2f \leq e-1$ and $s \in \mathbb{Z}_{2^{e-1}}^*$ if $p = 2$,

(b) $s \equiv -1 \pmod{p^f}$, s has multiplicative order 2ℓ in $\mathbb{Z}_{p^{e-f}}$ and $p \nmid w$, where

$$w = p^{f-e}(s^{2\ell} - 1) - \frac{1}{2}s(s-1)\ell.$$

For each admissible value of the parameter f, let $N(p^e, p^f)$ denote the number of admissible values of the parameter s. In what follows, we first determine $N(p^e, p^f)$, and then determine $N(p^e)$. We divide the proof into two cases according to the parity of p.

Case (A). $p \neq 2$.

Since $s \equiv -1 \pmod{p^f}$, we may write $s = tp^h - 1$ where $1 \leq f \leq h \leq e$ and $t \in \mathbb{Z}_{p^{e-h}}^*$. Then $s^2 = 1 + tp^h(tp^h - 2)$. According to the multiplicative order 2ℓ of s in $\mathbb{Z}_{p^{e-f}}$, we distinguish two subcases as follows.

If $h < e - f$, by Proposition 6.1 we have $\ell = p^{e-f-h}$. Since s has multiplicative ordr 2ℓ in $\mathbb{Z}_{p^{e-f}}$, we have $p^{e-f} \parallel s^{2\ell} - 1$. Since $p \mid \frac{1}{2}s(s-1)\ell$, we have $p \nmid w$.

If $h \geq e-f$, then $\ell = 1$. Recalling that $1 \leq f \leq h \leq e$, we have

$$w \equiv tp^{f+h-e}(tp^h - 2) - \frac{1}{2}(tp^h - 1)(tp^h - 2) \equiv -1 - 2tp^{f+h-e} \pmod{p}.$$

Thus, $p \mid w$ if and only if $h = e - f$ and $p \mid 1 + 2t$, where $t \in \mathbb{Z}_{p^f}^*$, in which case the number of such t is equal to p^{f-1}.

Consequently,

$$N(p^e, p^f) = \sum_{h=f}^{e} \phi(p^{e-h}) - p^{f-1} = 1 + \sum_{h=f}^{e-1} p^{e-h-1}(p-1) - p^{f-1} = p^{e-f} - p^{f-1},$$

where ϕ is the Euler's totient function. Therefore,

$$N(p^e) = \sum_{f=1}^{\lfloor e/2 \rfloor} N(p^e, p^f) = \sum_{f=1}^{\lfloor e/2 \rfloor} (p^{e-f} - p^{f-1}) = \frac{1}{p-1}(p^{\lfloor e/2 \rfloor} - 1)(p^{e-\lfloor e/2 \rfloor} - 1).$$

Note that $\lfloor e/2 \rfloor = e/2$ if e is even, and $\lfloor e/2 \rfloor = (e-1)/2$ if e is odd. The stated formula follows from substitution.

Case (B). $p = 2$.

It is straightforward to check that $N(2^2) = 0$, $N(2^3) = N(2^3, 2^1) = 1$ and $N(2^4) = N(2^4, 2^1) = 2$. In what follows, we assume $e \geq 5$ and distinguish two subcases.

Subcase (a). $s \equiv 1 \pmod 4$.

Since $s \equiv -1 \pmod{2^f}$, we have $f = 1$. Since $s \in \mathbb{Z}_{2^{e-1}}^*$, we may write $s = 1 + 2^h t$ where $2 \leq h \leq e-2$ and $t \in \mathbb{Z}_{2^{e-h-1}}^*$. By Proposition 6.1 (b), s has multiplicative order 2^{e-h-1} in $\mathbb{Z}_{2^{e-1}}$, and so $\ell = 2^{e-h-2}$. We have $2 \nmid w$ since

$$2^{e-1} \parallel (s^{2\ell} - 1) \quad \text{and} \quad 2 \mid \frac{1}{2}s(s-1)\ell.$$

Subcase (b). $s \equiv -1 \pmod 4$.

We may write $s = -1 + 2^h t$, where $2 \leq h \leq e-1$ and $t \in \mathbb{Z}_{2^{e-h-1}}^*$. Since $s \equiv -1 \pmod{2^f}$, we have $f \leq h$. Recall that s has multiplicative order 2ℓ in $\mathbb{Z}_{2^{e-f}}$.

If $h < e - f - 1$, then $e > f + h + 1 \geq 4$. By Proposition 6.1, s has multiplicative order 2^{e-f-h} in $\mathbb{Z}_{2^{e-f}}$, and hence $\ell = 2^{e-f-h-1}$. We also have $2 \nmid w$ since

$$2^{e-f} \parallel (s^{2\ell} - 1) \quad \text{and} \quad 2 \mid \frac{1}{2}s(s-1)\ell.$$

If $h \geq e - f - 1$, then $\ell = 1$ and hence

$$\begin{aligned} w &\equiv 2^{f-e}\big((-1+2^h t)^2 - 1\big) - (-1+2^h t)(-1+2^{h-1}t) \\ &\equiv (-1+2^{h-1}t)(2^{f-e+h+1}t - 2^h t + 1) \\ &\equiv 2^{f-e+h+1}t + 1 \pmod 2. \end{aligned}$$

It follows that $2 \nmid w$ if and only if $h > e - f - 1$. Therefore the case $h = e - f - 1$ should be excluded.

From the above discussion, we obtain

$$N(2^e, 2^1) = \sum_{h=2}^{e-2} \phi(2^{e-h-1}) + \sum_{h=2}^{e-1} \phi(2^{e-h-1}) - \phi(2) = 2^{e-2} - 2,$$

and for $f > 1$,

$$N(2^e, 2^f) = \sum_{h=f}^{e-f-2} \phi(2^{e-h-1}) + \sum_{h=e-f}^{e-1} \phi(2^{e-h-1}) = 2^{e-f-1} - 2^{f-1}.$$

Consequently, for $e \geq 5$, we get

$$\begin{aligned} N(2^e) = \sum_{f=1}^{\lfloor \frac{e-1}{2} \rfloor} N(2^e, 2^f) &= 2^{e-2} - 2 + \sum_{f=2}^{\lfloor \frac{e-1}{2} \rfloor} (2^{e-f-1} - 2^{f-1}) \\ &= 2^{e-2} - 2 + (2^{\lfloor \frac{e-1}{2} \rfloor - 1} - 1)(2^{e-1-\lfloor \frac{e-1}{2} \rfloor)} - 2). \end{aligned}$$

Note that $\lfloor \frac{e-1}{2} \rfloor = (e-2)/2$ if e if even, and $\lfloor \frac{e-1}{2} \rfloor = (e-1)/2$ if e is odd. The result follows from substitution for $\lfloor \frac{e-1}{2} \rfloor$ in the above formula, as required. □

Remark 6.3. By Theorem 1.2, one can enumerate the conjugacy classes of proper square roots of automorphisms of $\mathbb{Z}_n$ for any positive integer n in the following steps:

(a) Find the set of all positive integers k satisfying that k^2 divides n if k is odd, and $2k^2$ divides n if k is even. Denote this set by $A(n)$.

(b) For any $k \in A(n)$, find the set of all s satisfying (i) $s \equiv -1 \pmod{k}$ and (ii) $s \in \mathbb{Z}_n^*$ if k is odd, and $s \in \mathbb{Z}_{n/2}^*$ if k is even. Denote this set by $S(n, k)$.

(c) For any $s \in S(n, k)$, calculate the smallest positive integer ℓ such that $s^{2\ell} \equiv 1 \pmod{n/k}$ and check whether $\frac{k}{n}(s^{2\ell} - 1) - \frac{1}{2}s(s-1)\ell$ is coprime to k or not. Let $A(n, k)$ be the set of all $s \in S(n, k)$ satisfying that $\frac{k}{n}(s^{2\ell} - 1) - \frac{1}{2}s(s-1)\ell$ is coprime to k.

(d) Now (k, s) is admissible for proper square root of automorphism of $\mathbb{Z}_n$ if and only if $k \in A(n)$ and $s \in A(n, k)$. The number $N(n)$ of the conjugacy classes of proper square roots of automorphisms of $\mathbb{Z}_n$ is $\sum_{k \in A(n)} |A(n, k)|$.

Using the method above, we obtain $N(18) = 2$, $N(24) = 2$, $N(40) = 2$ and $N(72) = 16$. In each case the parameters (n, k, s) are given below (details are omitted):

(n, k)	$(18, 3)$	$(24, 2)$	$(40, 2)$	$(72, 2)$	$(72, 3)$	$(72, 6)$
s	$11, 17$	$7, 11$	$11, 19$	$7, 11, 19, 23, 31, 35$	$11, 17, 29, 35, 47, 53, 65, 71$	$23, 35$

We close the paper by attaching a full list of conjugacy classes of proper square roots of automorphisms of $\mathbb{Z}_n$ for some small values of n.

Table 1: Proper square roots of automorphisms of $\mathbb{Z}_n$.

n	$\varphi(x)$	$\pi(x)$	$\varphi^2(x)$
8	$6x^2 + 5x \pmod 8$	$1 + 2x \pmod 4$	$5x \pmod 8$
9	$3x^2 + 2x \pmod 9$	$1 + 2x \pmod 6$	$4x \pmod 9$
9	$3x^2 + 4x \pmod 9$	$1 + 2x \pmod 6$	$4x \pmod 9$
16	$12x^2 + 9x \pmod{16}$	$1 + 2x \pmod 4$	$9x \pmod{16}$
16	$12x^2 + 11x \pmod{16}$	$1 + 2x \pmod 4$	$9x \pmod{16}$
18	$15x^2 + 2x \pmod{18}$	$1 + 2x \pmod 6$	$13x \pmod{18}$
18	$15x^2 + 14x \pmod{18}$	$1 + 2x \pmod 6$	$7x \pmod{18}$
24	$18x^2 + 13x \pmod{24}$	$1 + 2x \pmod 4$	$23x \pmod{24}$
24	$18x^2 + 17x \pmod{24}$	$1 + 2x \pmod 4$	$13x \pmod{24}$
27	$9x^2 + 2x \pmod{27}$	$1 + 6x \pmod{18}$	$4x \pmod{27}$
27	$9x^2 + 5x \pmod{27}$	$1 + 6x \pmod{18}$	$25x \pmod{27}$
27	$9x^2 + 8x \pmod{27}$	$1 + 2x \pmod 6$	$10x \pmod{27}$
27	$9x^2 + 11x \pmod{27}$	$1 + 6x \pmod{18}$	$13x \pmod{27}$
27	$9x^2 + 14x \pmod{27}$	$1 + 12x \pmod{18}$	$7x \pmod{27}$
27	$9x^2 + 17x \pmod{27}$	$1 + 4x \pmod 6$	$19x \pmod{27}$
27	$9x^2 + 20x \pmod{27}$	$1 + 6x \pmod{18}$	$22x \pmod{27}$
27	$9x^2 + 23x \pmod{27}$	$1 + 12x \pmod{18}$	$16x \pmod{27}$
32	$24x^2 + 11x \pmod{32}$	$1 + 4x \pmod 8$	$25x \pmod{32}$
32	$24x^2 + 13x \pmod{32}$	$1 + 4x \pmod 8$	$25x \pmod{32}$
32	$24x^2 + 17x \pmod{32}$	$1 + 2x \pmod 4$	$17x \pmod{32}$
32	$24x^2 + 19x \pmod{32}$	$1 + 4x \pmod 8$	$9x \pmod{32}$
32	$24x^2 + 21x \pmod{32}$	$1 + 4x \pmod 8$	$9x \pmod{32}$
32	$24x^2 + 23x \pmod{32}$	$1 + 2x \pmod 4$	$17x \pmod{32}$
32	$28x^2 + 11x \pmod{32}$	$1 + 2x \pmod 8$	$9x \pmod{32}$
32	$28x^2 + 19x \pmod{32}$	$1 + 6x \pmod 8$	$25x \pmod{32}$
40	$30x^2 + 21x \pmod{40}$	$1 + 2x \pmod 4$	$31x \pmod{40}$
40	$30x^2 + 29x \pmod{40}$	$1 + 2x \pmod 4$	$21x \pmod{40}$
64	$48x^2 + 19x \pmod{64}$	$1 + 8x \pmod{16}$	$41x \pmod{64}$
64	$48x^2 + 21x \pmod{64}$	$1 + 8x \pmod{16}$	$25x \pmod{64}$
64	$48x^2 + 23x \pmod{64}$	$1 + 4x \pmod 8$	$17x \pmod{64}$
64	$48x^2 + 25x \pmod{64}$	$1 + 4x \pmod 8$	$17x \pmod{64}$
64	$48x^2 + 27x \pmod{64}$	$1 + 8x \pmod{16}$	$25x \pmod{64}$
64	$48x^2 + 29x \pmod{64}$	$1 + 8x \pmod{16}$	$41x \pmod{64}$
64	$48x^2 + 33x \pmod{64}$	$1 + 2x \pmod 4$	$33x \pmod{64}$
64	$48x^2 + 35x \pmod{64}$	$1 + 8x \pmod{16}$	$9x \pmod{64}$
64	$48x^2 + 37x \pmod{64}$	$1 + 4x \pmod{16}$	$57x \pmod{64}$
64	$48x^2 + 39x \pmod{64}$	$1 + 4x \pmod 8$	$49x \pmod{64}$
64	$48x^2 + 41x \pmod{64}$	$1 + 4x \pmod 8$	$49x \pmod{64}$
64	$48x^2 + 43x \pmod{64}$	$1 + 8x \pmod{16}$	$57x \pmod{64}$
64	$48x^2 + 45x \pmod{64}$	$1 + 8x \pmod{16}$	$9x \pmod{64}$
64	$48x^2 + 47x \pmod{64}$	$1 + 2x \pmod 4$	$33x \pmod{64}$
64	$56x^2 + 11x \pmod{64}$	$1 + 12x \pmod{16}$	$25x \pmod{64}$
64	$56x^2 + 19x \pmod{64}$	$1 + 4x \pmod{16}$	$9x \pmod{64}$
64	$56x^2 + 23x \pmod{64}$	$1 + 2x \pmod 8$	$17x \pmod{64}$
64	$56x^2 + 27x \pmod{64}$	$1 + 12x \pmod{16}$	$57x \pmod{64}$
64	$56x^2 + 35x \pmod{64}$	$1 + 4x \pmod{16}$	$41x \pmod{64}$
64	$56x^2 + 39x \pmod{64}$	$1 + 6x \pmod 8$	$49x \pmod{64}$

ORCID iDs

Kan Hu https://orcid.org/0000-0003-4775-7273
Young Soo Kwon https://orcid.org/0000-0002-1765-0806
Jun-Yang Zhang https://orcid.org/0000-0002-0871-2059

References

[1] M. Bachratý and R. Jajcay, Powers of skew-morphisms, in: *Symmetries in Graphs, Maps, and Polytopes*, Springer International Publishing, volume 159, pp. 1–25, 2016, doi:10.1007/978-3-319-30451-9.

[2] M. Bachratý and R. Jajcay, Classification of coset-preserving skew-morphisms of finite cyclic groups, *Australas. J. Comb.* **67** (2017), 259–280, https://ajc.maths.uq.edu.au/?page=get_volumes&volume=67.

[3] B. G. Basmaji, On the ismorphisms of two metacyclic groups, *Proc. Amer. Math. Soc.* **22** (1969), 175–182, doi:10.2307/2036947.

[4] M. Conder, R. Jajcay and T. Tucker, Regular Cayley maps for finite abelian groups, *J. Algebraic Combin.* **25** (2007), 259–283, doi:10.1007/s10801-006-0037-0.

[5] M. Conder, R. Jajcay and T. Tucker, Regular t-balanced Cayley maps, *J. Combin. Theory Ser. B* **97** (2007), 453–473, doi:10.1016/j.jctb.2006.07.008.

[6] M. D. E. Conder, R. Jajcay and T. W. Tucker, Cyclic complements and skew morphisms of groups, *J. Algebra* **453** (2016), 68–100, doi:10.1016/j.jalgebra.2015.12.024.

[7] M. D. E. Conder, Y. S. Kwon and J. Širáň, Reflexibility of regular Cayley maps for abelian groups, *J. Combin. Theory Ser. B* **99** (2009), 254–260, doi:10.1016/j.jctb.2008.07.002.

[8] M. D. E. Conder and T. W. Tucker, Regular Cayley maps for cyclic groups, *Trans. Amer. Math. Soc.* **366** (2014), 3585–3609, doi:10.1090/s0002-9947-2014-05933-3.

[9] S. Du and K. Hu, Skew-morphisms of cyclic 2-groups, *J. Group Theory* **22** (2019), 617–635, doi:10.1515/jgth-2019-2046.

[10] R. Feng, R. Jajcay and Y. Wang, Regular t-balanced Cayley maps for abelian groups, *Discrete Math.* **311** (2011), 2309–2316, doi:10.1016/j.disc.2011.04.012.

[11] Y.-Q. Feng, K. Hu, R. Nedela, M. Škoviera and N.-E. Wang, Complete regular dessins and skew-morphisms of cyclic groups, *Ars Math. Contemp.* **18** (2020), 289–307, doi:10.26493/1855-3974.1748.ebd.

[12] K. Hu, R. Nedela and N.-E. Wang, Nilpotent groups of class two which underly a unique regular dessin, *Geom. Dedicata* **179** (2015), 177–186, doi:10.1007/s10711-015-0074-8.

[13] R. Jajcay and J. Širáň, Skew-morphisms of regular Cayley maps, *Discrete Math.* **244** (2002), 167–179, doi:10.1016/s0012-365x(01)00081-4.

[14] I. Kovács and Y. S. Kwon, Regular Cayley maps on dihedral groups with the smallest kernel, *J. Algebraic Combin.* **44** (2016), 831–847, doi:10.1007/s10801-016-0689-3.

[15] I. Kovács and Y. S. Kwon, Classification of reflexible Cayley maps for dihedral groups, *J. Combin. Theory Ser. B* **127** (2017), 187–204, doi:10.1016/j.jctb.2017.06.002.

[16] I. Kovács and Y. S. Kwon, Regular Cayley maps for dihedral groups, *J. Comb. Theory Ser. B* **148** (2021), 84–124, doi:10.1016/j.jctb.2020.12.002.

[17] I. Kovács and R. Nedela, Decomposition of skew-morphisms of cyclic groups, *Ars Math. Contemp.* **4** (2011), 329–349, doi:10.26493/1855-3974.157.fc1.

[18] I. Kovács and R. Nedela, Skew-morphisms of cyclic p-groups, *J. Group Theory* **20** (2017), 1135–1154, doi:10.1515/jgth-2017-0015.

[19] J. H. Kwak, Y. S. Kwon and R. Feng, A classification of regular t-balanced Cayley maps on dihedral groups, *European J. Combin.* **27** (2006), 382–393, doi:10.1016/j.ejc.2004.12.002.

[20] J. H. Kwak and J.-M. Oh, A classification of regular t-balanced Cayley maps on dicyclic groups, *European J. Combin.* **29** (2008), 1151–1159, doi:10.1016/j.ejc.2007.06.023.

[21] Y. S. Kwon, A classification of regular t-balanced Cayley maps for cyclic groups, *Discrete Math.* **313** (2013), 656–664, doi:10.1016/j.disc.2012.12.012.

[22] J.-M. Oh, Regular t-balanced Cayley maps on semi-dihedral groups, *J. Combin. Theory Ser. B* **99** (2009), 480–493, doi:10.1016/j.jctb.2008.09.006.

[23] N.-E. Wang, K. Hu, K. Yuan and J.-Y. Zhang, Smooth skew morphisms of dihedral groups, *Ars Math. Contemp.* **16** (2019), 527–547, doi:10.26493/1855-3974.1475.3d3.

[24] M. Xu and Q. Zhang, A classification of metacyclic 2-groups, *Algebra Colloq.* **13** (2006), 25–34, doi:10.1142/s1005386706000058.

[25] K. Yuan, Y. Wang and J. H. Kwak, Enumeration of skew-morphisms of groups of small orders and their corresponding Cayley maps, *Adv. Math. (China)* **45** (2016), 21–36, doi:10.1103/physrevd.45.21.

[26] J.-Y. Zhang, Regular Cayley maps of skew-type 3 for abelian groups, *European J. Combin.* **39** (2014), 198–206, doi:10.1016/j.ejc.2014.01.006.

[27] J.-Y. Zhang, A classification of regular Cayley maps with trivial Cayley-core for dihedral groups, *Discrete Math.* **338** (2015), 1216–1225, doi:10.1016/j.disc.2015.01.036.

[28] J.-Y. Zhang, Regular Cayley maps of skew-type 3 for dihedral groups, *Discrete Math.* **338** (2015), 1163–1172, doi:10.1016/j.disc.2015.01.038.

[29] J.-Y. Zhang and S. Du, On the skew-morphisms of dihedral groups, *J. Group Theory* **19** (2016), 993–1016, doi:10.1515/jgth-2016-0027.