Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2013, Article ID 472350, 7 pages
http://dx.doi.org/10.1155/2013/472350

Research Article

Fixed Points of the Dickson Polynomials of the Second Kind

Adama Diene and Mohamed A. Salim

Department of Mathematical Sciences, United Arab Emirates University, P.O. Box 17551, Al Ain, Abu Dhabi 17551, UAE

Correspondence should be addressed to Adama Diene; adiene@uaeu.ac.ae

Received 12 December 2012; Revised 6 March 2013; Accepted 7 March 2013

Academic Editor: Roberto Barrio

The permutation behavior of Dickson polynomials of the first kind has been extensively studied, while such behavior for Dickson polynomials of the second kind is less known. Necessary and sufficient conditions for a polynomial of the second kind to be a permutation over some finite fields have been established by Cohen, Matthew, and Henderson. We introduce a new way to define these polynomials and determine the number of their fixed points.

1. Introduction

Let p be a prime, $e \geq 1$, $q = p^e$, and let $\mathbb{F}_q$ be the field of q elements. Denote the greatest integer function of n by $\lfloor n \rfloor$. For a fixed $a \in \mathbb{F}_q$, the polynomials

$$D_k(x,a) = \sum_{j=1}^{\lfloor k/2 \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j},$$
$$E_k(x,a) = \sum_{j=1}^{\lfloor k/2 \rfloor} \binom{k-j}{j} (-a)^j x^{k-2j} \tag{1}$$

are called the Dickson polynomials of the first and second kind, respectively.

It is well known (see [1]) that for any $x \in \mathbb{F}_q$, there exists $u \in \mathbb{F}_{q^2}$ such that $x = u + au^{-1}$ and the Dickson polynomials may be expressed as

$$D_k(x,a) = u^k + a^k u^{-k},$$
$$E_k(x,a) = \begin{cases} \dfrac{u^{k+1} - a^{k+1}u^{-(k+1)}}{u - au^{-1}}, & \text{if } u^2 \neq a, \\ (k+1)\left(\pm\sqrt{a}\right)^k, & \text{otherwise.} \end{cases} \tag{2}$$

For $a \in \mathbb{F}_q^*$, denote

$$\eta(a) = \begin{cases} 1, & \text{if } a \text{ is a square,} \\ -1, & \text{otherwise.} \end{cases} \tag{3}$$

According to [2], if $\eta(a) = 1$ and q is odd, then the sign class of k is defined to be the set $A = \{(\pm k_1, \pm k_2, \pm k_3) \in \mathbb{Z}^3\}$ if k satisfies the following congruences:

$$k_1 \equiv k+1 \pmod{p}, \qquad k_2 \equiv k+1 \pmod{\frac{q-1}{2}},$$
$$k_3 \equiv k+1 \pmod{\frac{q+1}{2}}. \tag{4}$$

If $\eta(a) = -1$ and q is odd, then the sign class of k is defined to be the set $A = \{(\pm k_1, \pm k_2) \in \mathbb{Z}^2\}$ if k satisfies the following congruences:

$$k_1 \equiv k+1 \pmod{q-1}, \qquad k_2 \equiv k+1 \pmod{q+1}. \tag{5}$$

If $E_k(x,1)$ is a permutation over $\mathbb{F}_q$, then k belongs to the class sign $(2,2,2)$ (see Henderson and Matthews [3]). Moreover (see Cohen in [4]), these conditions are necessary for $q \in \{p, p^2\}$, where p is an odd prime. Henderson and Matthew extended this result to all squares a such that $q \in \{p, p^2\}$. Later they found new classes of permutation

polynomials of the type $E_k(x,1)$ over $\mathbb{F}_q$. They proved that for $q = 3^e$, $E_k(x,1)$ permutes the elements of $\mathbb{F}_q$ if the sign class of k contains one of the following triples:

(i) $\{2, 10, 10\}$ for $e = 3$;

(ii) $\{2, 4, 4\}$ for e odd;

(iii) $\{2, ((3^s - 1)/2)^{-1} + 1, ((3^t - 1)/2)^{-1} + 1\}$, where $\gcd(s, e) = \gcd(t, 2e) = 1$.

They also proved that if $q = 5^e$ and if k belongs either to the sign class of $\{2, 2, (q-1)/4\}$ or $\{2, 2, 2\}$, then $E_k(x,1)$ permute the elements of $\mathbb{F}_q$. In general, for a large prime number p, few permutation polynomials of the form $E_k(x,a)$ have been identified.

For $a \in \{-1, 0, 1\}$, the cycle structure of $D_k(x,a)$ is well known. It was established by Ahmad in [5] for $a = 0$ and later by Lidl and Mullen [6] for $a \in \{-1, 1\}$. But the cycle structure of $E_k(x,a)$ remains unknown. We look partially to it by determining the number of fixed points of $E_k(x,a)$ over $\mathbb{F}_q$ for the Dickson polynomials of the second kind that are permutation polynomials over $\mathbb{F}_q$. For $a = 1$, it is well known that the first and second Chebyshev polynomials $T_n(x)$ and $U_n(x)$, over the field $\mathbb{Z}_p$, are, respectively, conjugates of $D_k(x,1)$ and $E_k(x,1)$. Namely, we have

$$D_k(x,1) = 2T_k\left(\frac{x}{2}\right), \qquad E_k(x,1) = U_k\left(\frac{x}{2}\right), \tag{6}$$

where

$$\begin{aligned} T_k(x) &= \cos(k \arccos(x)), \\ U_k(\cos(\theta)) &= \frac{\sin((k+1)\theta)}{\sin(\theta)}, \quad (k \in \mathbb{Z}). \end{aligned} \tag{7}$$

We use these relations between Dickson polynomials and Chebyshev polynomials along with a new approach to define $T_n(x)$ and $U_n(x)$ over $\mathbb{Z}_p$ to give a new approach of the Dickson polynomials $D_k(x,1)$ and $E_k(x,1)$ on $\mathbb{Z}_p$ in Section 2. In Section 3, we study the number of fixed points of $E_k(x,a)$.

2. The Dickson Polynomials $D_k(x,1)$ and $E_k(x,1)$

Now we present a theoretical approach of the family of Dickson polynomials $D_k(x,1)$ and $E_k(x,1)$ on $\mathbb{Z}_p$, which are essentially the first and the second Chebyshev polynomials $T_n(x)$ and $U_n(x)$ over $\mathbb{Z}_p$. We will provide a better way to look at these polynomials which can help to find many known properties. Let us recall that the first and the second Chebyshev polynomials defined in (7) can also be, respectively, defined by the following linear recurrence relations:

$$\begin{aligned} T_0(x) &= 1, \qquad T_1(x) = x, \\ T_k(x) &= 2xT_{k-1}(x) - T_{k-2}(x), \end{aligned} \tag{8}$$

$$\begin{aligned} U_0(x) &= 1, \qquad U_1(x) = 2x, \\ U_k(x) &= 2xU_{k-1}(x) - U_{k-2}(x). \end{aligned} \tag{9}$$

Obviously, $D_k(x,1) = 2T_k(x/2)$, $E_k(x,1) = U_k(x/2)$ and they can be derived as conjugates of $T_k(x)$ and $U_k(x)$, respectively. This implies that $D_k(x,1)$ and $T_k(x)$, as permutations of $\mathbb{Z}_p$, have the same number of cycles with the same length when written as a product of disjoint cycles, likewise for $E_k(x,1)$ and $U_k(x)$. Therefore to understand the permutation structure of $D_k(x,1)$ and $E_k(x,1)$, it suffices to know that of $T_k(x)$ and $U_k(x)$.

Put $\mathbb{R}_p = \mathbb{Z}_p[z]/(z^2+1)$. The structure of $\mathbb{R}_p$ depends on whether -1 is a square in $\mathbb{Z}_p$ or not. For a given ring R, we denote their group of units by $U(R)$.

Lemma 1. *Let $p \equiv 1 \pmod 4$. If $1 - x^2$ is a square in $\mathbb{Z}_p$, that is, $1 - x^2 = y^2$ for some $y \in \mathbb{Z}_p$, then there exists a group homomorphism $N : U(\mathbb{R}_p) \to U(\mathbb{Z}_p)$, such that for any $x + yz \in \mathrm{Ker}(N)$, the following equation*

$$(x + yz)^k = P_k(x,y) + Q_k(x,y)\,z \tag{10}$$

holds, where $T_k(x) = P_k(x,y)$ and $U_k(x) = (1/y)Q_k(x,y)$.

Proof. If $p \equiv 1 \pmod 4$, then -1 is a square in $\mathbb{Z}_p$. Let $\pm w$ be its roots in $\mathbb{Z}_p$. Then $\mathbb{R}_p \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, so $|U(\mathbb{R}_p)| = (p-1)^2$. If $X \in \mathbb{R}_p$, then X can be expressed as $X = a + bz$, where $a, b \in \mathbb{Z}_p$. Let N be the mapping from $\mathbb{R}_p$ to $\mathbb{Z}_p$ defined by

$$N(a + bz) = a^2 + b^2. \tag{11}$$

Clearly, N is a surjective group homomorphism from $U(\mathbb{R}_p)$ to $U(\mathbb{Z}_p)$. If $x + yz \in \mathrm{Ker}(N)$, then $(x + yz)^{-1} = x - yz$. Furthermore, $\mathrm{Ker}(N) \cong U(\mathbb{Z}_p)$ and it has order $p - 1$. If

$$(x + yz)^n = P_n(x,y) + Q_n(x,y)\,z, \quad (x + yz \in \mathrm{Ker}(N)), \tag{12}$$

then

$$\begin{aligned} (x + yz)^{n+1} &= (P_n(x,y) + Q_n(x,y)\,z)(x + yz) \\ &= (xP_n(x,y) - yQ_n(x,y)) \\ &\quad + (xQ_n(x,y) + yP_n(x,y))\,z. \end{aligned} \tag{13}$$

Therefore, $P_n(x,y)$ and $Q_n(x,y)$ satisfy the recurrence relations

$$\begin{aligned} P_{n+1}(x,y) &= (x+y)\,xP_n(x,y) - yQ_n(x,y), \\ Q_{n+1}(x,y) &= xQ_n(x,y) + yP_n(x,y), \end{aligned} \tag{14}$$

where

$$\begin{aligned} P_1(x) &= x, \qquad P_2(x) = 2x^2 - 1, \\ P_p(x) &= x, \qquad P_{k+n}(x) = P_n(x), \\ \frac{1}{y}Q_1(x) &= 1, \qquad \frac{1}{y}Q_2(x) = 2x, \\ \frac{1}{y}Q_p(x) &= 1, \qquad \frac{1}{y}Q_{k+n}(x) = Q_n(x), \end{aligned} \tag{15}$$

and k is the order of $x + yz$. That is, $P_n(x, y)$ and $Q_n(x, y)/y$ satisfy the recurrence (8), which means that $T_n(x) = P_n(x, y)$ is the first coordinate of $(x + yz)^n$ and

$$U_n(x) = \frac{Q_n(x, y)}{y}. \tag{16}$$

Notice that $Q_n(x, y)$ is uniquely determined by $P_n(x, y)$ up to a sign and we have

$$\begin{aligned} T_1(x) &= x, \qquad T_2(x) = 2x^2 - 1, \\ T_p(x) &= x, \qquad T_{k+n}(x) = T_n(x), \\ U_1(x) &= 1, \qquad U_2(x) = 2x, \\ U_p(x) &= 1, \qquad U_{k+n}(x) = U_n(x), \end{aligned} \tag{17}$$

where k is the order of $x + yz$. □

Remark 2. Let FC be the set of all the first coordinates of the elements in Ker(N). FC contains $(p + 1)/2 = (p - 1)/2 + 1$ elements including 0 and 1. Those elements are x in $\mathbb{Z}_p$ for which $1-x^2$ is a square in $\mathbb{Z}_p$. Moreover, FC is invariant under the actions of T_n and U_n. For a given element u in FC, we can find an element v in FC such that $u + vz$ is in Ker(N). The mapping which sends $u + vz$ to $u + vwu - vw$ is an isomorphism from Ker(N) to $U(\mathbb{Z}_p)$. Therefore, the order of $u + vz$ is simply determined by the least common multiple of the order of $u + vw$ and $u - vw$. However, since in $\mathbb{Z}_p$, $(u + vw)(u - vw) = 1$, the kernel Ker(N) is cyclic. For any element $u + vz$ in Ker(N), if $u + vw = g$, a generator of the group $U(\mathbb{Z}_p)$, then $u + vz$ is a generator of Ker(N).

Lemma 3. *Let $p \equiv 3 \pmod 4$. If $1 - x^2$ is a square in $\mathbb{Z}_p$, that is, $1 - x^2 = y^2$ for some $y \in \mathbb{Z}_p$, then there exists a group homomorphism $N : U(\mathbb{R}_p) \to U(\mathbb{Z}_p)$, such that*

$$(x + yz)^n = P_n(x, y) + Q_n(x, y)z, \quad (x + yz \in \mathrm{Ker}(N)), \tag{18}$$

where $T_n(x) = P_n(x, y)$ and $U_n(x) = Q_n(x, y)/y$.

Proof. In this case, -1 is not a square in $\mathbb{Z}_p$, and $|\mathbb{R}_p| = p^2$. Therefore, $|U(\mathbb{R}_p)| = p^2 - 1$. Again we can express every element $X \in \mathbb{R}_p$ as $X = a + bz$, where $a, b \in \mathbb{Z}_p$. Let $N : \mathbb{R}_p \to \mathbb{Z}_p$ be a map, defined by $N(a + bz) = a^2 + b^2$. Clearly, N is a surjective group homomorphism from $U(\mathbb{R}_p)$ to $U(\mathbb{Z}_p)$. The inverse of $x + yz \in \mathrm{Ker}(N)$ is $(x + yz)^{-1} = x - yz$ and for each element $x + yz \in \mathrm{Ker}(N)$ if $(x + yz)^n = P_n(x, y) + Q_n(x, y)$, then

$$\begin{aligned} (x + yz)^{n+1} &= (P_n(x, y) + Q_n(x, y)z)(x + yz) \\ &= (xP_n(x, y) - yQ_n(x, y)) \\ &\quad + (xQ_n(x, y) + yP_n(x, y))z. \end{aligned} \tag{19}$$

Therefore, $P_n(x, y)$ and $Q_n(x, y)$ satisfy the recurrence relations

$$\begin{aligned} P_{n+1}(x, y) &= (x, y)xP_n(x, y) - yQ_n(x, y), \\ Q_{n+1}(x, y) &= xQ_n(x, y) + yP_n(x, y), \end{aligned} \tag{20}$$

where

$$\begin{aligned} &P_1(x) = x, \qquad P_2(x) = 2x^2 - 1, \qquad P_{p+1}(x) = 1, \\ &P_{p+2}(x) = x, \qquad P_{k-n}(x) = P_n(x), \\ &\frac{1}{y}Q_1(x) = 1, \qquad \frac{1}{y}Q_2(x) = 2x, \qquad \frac{1}{y}Q_{p+2}(x) = 1, \\ &\frac{1}{y}Q_{p+3}(x) = 2x, \qquad \frac{1}{y}Q_{k+n}(x) = Q_n(x), \end{aligned} \tag{21}$$

and k is the order of $x+yz$. That is, $T_n(x) = P_n(x, y)$ is the first coordinate of $(x + yz)^n$ and $Q_n(x, y)$ is uniquely determined by $P_n(x, y)$ up to a sign. $U_n = Q_n(x, y)/y$ is the second Chebyshev polynomial. In this case, Ker(N) is a cyclic group of order $p + 1$, which also implies that

$$\begin{aligned} &T_{p+1}(x) = 1, \qquad T_{p+2}(x) = x, \qquad T_{k-n}(x) = T_n(x), \\ &U_{p+2}(x) = 1, \qquad T_{p+3}(x) = 2x, \qquad T_{k-n}(x) = T_n(x), \end{aligned} \tag{22}$$

where k is the order of $x + yz$. □

Remark 4. Since Ker(N) is a cyclic group, a good way to find a generator is to first find the generator of $U(\mathbb{R}_p)$ and then take the $(p - 1)$th power. If we let again FC to be the set of all the first coordinates of the elements of Ker(N), then it contains $((p + 1)/2) + 1$ elements including 0 and 1. The Ker(N) includes all the elements x in $\mathbb{Z}_p$ for which $1 - x^2$ is a square in $\mathbb{Z}_p$. It is invariant under the actions of T_n and U_n.

Finally, we assume that $1 - x^2$ is not a square in $\mathbb{Z}_p$. Put

$$\overline{\mathbb{Z}}_p = \frac{\mathbb{Z}_p[y]}{[y^2 - (1 - x^2)]}. \tag{23}$$

Clearly, $\overline{\mathbb{Z}}_p$ is a field of p^2 elements and $\mathbb{Z}_p$ can be embedded in $\overline{\mathbb{Z}}_p$ in the conventional way. For convenience, we will treat $\mathbb{Z}_p$ as a subset of $\overline{\mathbb{Z}}_p$ according to the standard embedding. Here, -1 becomes naturally a square in $\overline{\mathbb{Z}}_p$, and $\pm y$ are the two square roots of $(1 - x^2)$ in $\overline{\mathbb{Z}}_p$. The group of units $U(\overline{\mathbb{Z}}_p)$ of $\overline{\mathbb{Z}}_p$ is a cyclic group of order p^2-1. Let $\mathbb{H}_p = \overline{\mathbb{Z}}_p[z]/(z^2+1)$. Then $\mathbb{H}_p$ is a ring but not a field. Let $\overline{\mathbb{S}}_p$ denote the subset of all elements in $\mathbb{H}_p$ of the form of $a + byz$ where $a, b \in \mathbb{Z}_p$. Clearly, $\overline{\mathbb{S}}_p$ is a subring of $\mathbb{H}_p$.

Lemma 5. *Let $p \equiv 1 \pmod 4$. There exists a group homomorphism $N : U(\overline{\mathbb{S}}_p) \to U(\mathbb{Z}_p)$, such that*

$$(x + yz)^n = P_n(x, y) + Q_n(x, y)z, \quad (x + yz \in \mathrm{Ker}(N)), \tag{24}$$

where $T_n(x) = P_n(x, y)$ and $U_n(x) = Q_n(x, y)/y$.

Proof. In this case, -1 is a square in $\mathbb{Z}_p$ and the equation $a^2 + b^2(1 - x^2) = 0$ has no nonzero solutions for $a, b \in \mathbb{Z}_p$. Therefore, $\overline{\mathbb{S}}_p$ is a field.

Let N be the mapping from $U(\overline{\mathbb{S}}_p)$ to $U(\overline{\mathbb{Z}}_p)$, defined by

$$N(a + byz) = a^2 + b^2\left(1 - x^2\right). \tag{25}$$

Clearly, N is a surjective group homomorphism from $U(\overline{\mathbb{S}}_p)$ to $U(\overline{\mathbb{Z}}_p)$. Moreover, $\mathrm{Ker}(N)$ is a cyclic group of order $p + 1$, and for every element $x + yz \in \mathrm{Ker}(N)$, $(x + yz)^{-1} = x - yz$ and for each element of the form $x + yz \in \mathrm{Ker}(N)$ if

$$(x + yz)^n = P_n(x, y) + Q_n(x, y), \tag{26}$$

then

$$\begin{aligned}(x + yz)^{n+1} &= \left(P_n(x, y) + Q_n(x, y)\, z\right)(x + yz)\\ &= \left(xP_n(x, y) - yQ_n(x, y)\right)\\ &\quad + \left(xQ_n(x, y) + yP_n(x, y)\right) z.\end{aligned} \tag{27}$$

Therefore, $P_n(x, y)$ and $Q_n(x, y)$ satisfy the recurrence relations

$$\begin{aligned}P_{n+1}(x, y) &= (x, y)\, xP_n(x, y) - yQ_n(x, y),\\ Q_{n+1}(x, y) &= xQ_n(x, y) + yP_n(x, y),\end{aligned} \tag{28}$$

where

$$\begin{gathered}P_1(x) = x, \qquad P_2(x) = 2x^2 - 1, \qquad P_{p+1}(x) = 1,\\ P_{p+2}(x) = x, \qquad P_{k-n}(x) = P_n(x),\\ \frac{1}{y}Q_1(x) = 1, \qquad \frac{1}{y}Q_2(x) = 2x, \qquad \frac{1}{y}Q_{p+2}(x) = 1,\\ \frac{1}{y}Q_{p+3}(x) = 2x, \qquad \frac{1}{y}Q_{k+n}(x) = Q_n(x),\end{gathered} \tag{29}$$

and k is the order of $x + yz$. That is, $T_n(x) = P_n(x, y)$ is the first coordinate of $(x + yz)^n$ and $Q_n(x, y)$ is uniquely determined by $P_n(x, y)$ up to a sign. $U_n(x) = Q_n(x, y)/y$ is the second Chebyshev polynomial. Since $\mathrm{Ker}(N)$ is a cyclic group of order $p + 1$, we have

$$\begin{gathered}T_{p+1}(x) = 1, \qquad T_{p+2}(x) = x, \qquad T_{k-n}(x) = T_n(x),\\ U_{p+2}(x) = 1, \qquad T_{p+3}(x) = 2x, \qquad U_{k-n}(x) = U_n(x),\end{gathered} \tag{30}$$

where k is the order of $x + yz$. □

Remark 6. We can find a generator of $\mathrm{Ker}(N)$ by raising to the $(p - 1)$th a generator of $U(\overline{\mathbb{S}}_p)$. If $F_{C\overline{K}_p}$ denotes the set of all the first coordinates of the elements of $\mathrm{Ker}(N)$, then it contains $(p + 1)/2 + 1$ elements including ± 1, but not 0. $F_{C\overline{K}_p}$ without the elements ± 1 consists of all the elements x in $\mathbb{Z}_p$ for which $1 - x^2$ is not a square in $\mathbb{Z}_p$.

Lemma 7. *Let $p \equiv 3 \pmod 4$. There exists a group homomorphism $N : U(\mathbb{R}_p) \to U(\mathbb{Z}_p)$, such that $T_n(x) = P_n(x, y)$ and $U_n(x) = Q_n(x, y)/y$, whenever $x + yz \in \mathrm{Ker}(N)$ and $(x + yz)^n = P_n(x, y) + Q_n(x, y)z$.*

Proof. Here, we know that -1 is not a square in $\mathbb{Z}_p$ and $a^2 + b^2(1 - x^2) = 0$ has nonzero solutions for a and b. The total number of solutions is $2p - 1$. Therefore, $\overline{\mathbb{S}}_p$ is not a field.

Let $N : \overline{\mathbb{S}}_p \to \overline{\mathbb{Z}}_p^*$ be a map, defined by

$$N(a + byz) = a^2 + b^2\left(1 - x^2\right). \tag{31}$$

Clearly, N is a surjective group homomorphism from $U(\overline{\mathbb{S}}_p)$ to $U(\overline{\mathbb{Z}}_p)$. Also $\mathrm{Ker}(N)$ is a cyclic group of order $p - 1$ and for every element $x + yz \in \mathrm{Ker}(N)$, $(x + yz)^{-1} = x - yz$. Furthermore, if

$$(x + yz)^n = P_n(x, y) + Q_n(x, y) \quad (x + yz \in \mathrm{Ker}(N)), \tag{32}$$

then

$$\begin{aligned}(x + yz)^{n+1} &= \left(P_n(\mathrm{x}, y) + Q_n(x, y)\, z\right)(x + yz)\\ &= \left(xP_n(x, y) - yQ_n(x, y)\right)\\ &\quad + \left(xQ_n(x, y) + yP_n(x, y)\right) z.\end{aligned} \tag{33}$$

Therefore, $P_n(x, y)$ and $Q_n(x, y)$ satisfy the recurrence relations

$$\begin{aligned}P_{n+1}(x, y) &= (x, y)\, xP_n(x, y) - yQ_n(x, y),\\ Q_{n+1}(x, y) &= xQ_n(x, y) + yP_n(x, y),\end{aligned} \tag{34}$$

where

$$\begin{gathered}P_1(x) = x, \qquad P_2(x) = 2x^2 - 1, \qquad P_{p+1}(x) = 1,\\ P_{p+2}(x) = x, \qquad P_{k-n}(x) = P_n(x),\\ \frac{1}{y}Q_1(x) = 1, \qquad \frac{1}{y}Q_2(x) = 2x, \qquad \frac{1}{y}Q_{p+2}(x) = 1,\\ \frac{1}{y}Q_{p+3}(x) = 2x, \qquad \frac{1}{y}Q_{k+n}(x) = Q_n(x),\end{gathered} \tag{35}$$

and k is the order of $x + yz$. That is,

$$\begin{gathered}T_{p-1}(x) = 1, \qquad T_p(x) = x, \qquad T_{k-n}(x) = T_n(x),\\ U_{p+2}(x) = 1, \qquad U_{p+3}(x) = 2x, \qquad U_{k-n}(x) = U_n(x),\end{gathered} \tag{36}$$

where k is the order of $x + yz$. □

Remark 8. As in Remark 6, finding a generator $u + vz$ for $\mathrm{Ker}(N)$ is equivalent to finding a generator g in $U(\overline{\mathbb{S}}_p)$ such that $g = u + vw$. If $F_{C\overline{\mathbb{K}}_p}$ denotes the set of all the first coordinates of the elements of $\mathrm{Ker}(N)$, then it contains $(p + 1)/2$ elements including ± 1, but not 0. $F_{C\overline{\mathbb{K}}_p}$ without the element ± 1 consists of all the elements x in $\mathbb{Z}_p$ for which $1 - x^2$ is not a square in $\mathbb{Z}_p$.

As corollaries of the previous discussion, we obtain the following.

Corollary 9. *If $p \equiv 1 \pmod 4$, then the number of elements $x \in \mathbb{Z}_p$ for which $1 - x^2$ is a square in $\mathbb{Z}_p$ is $(p+1)/2$.*

If $p \equiv 3 \pmod 4$, then the number of elements $x \in \mathbb{Z}_p$ for which $1 - x^2$ is a square in $\mathbb{Z}_p$ is $(p+3)/2$.

3. Number of Fixed Points of $E_k(x, a)$

Since Dickson permutation polynomials are closed under composition of polynomials if and only if $a = 0, 1$, or -1 (see [7]), we will only focus on these 3 cases.

The case when $a = 0$ was proven by Ahmad [5]. His proof can also be found in [6]. The theorem is formulated as follows.

Theorem 10. *The number of fixed points of $E_k(x, 0)$ over $\mathbb{F}_q$ is given by*

$$\gcd(q-1, k-1) + 1. \tag{37}$$

In the next two theorems, we treat the cases $a = 1$ and $a = -1$. Their proofs follow the lines of the one of Lidl and Mullen [6] for the Dickson polynomials of the first kind.

Theorem 11. *For $x \neq \pm 2$, the number of fixed points of $E_k(x, 1)$ over $\mathbb{F}_q$ is given by*

$$\begin{aligned}\frac{1}{2}\big[&\gcd(q+1, k-1) + \gcd(q+1,2(k+3)) \\ &+ \gcd(q-1, k-1) + \gcd(q-1, 2(k+3)) \\ &- \gcd(q+1, k+3) - \gcd(q-1, k+3)\big] - \varepsilon_1,\end{aligned} \tag{38}$$

where

$$\varepsilon_1 = \begin{cases} 5, & \text{if } p \text{ and } n \text{ are odd}, 8 \mid q+1, \text{and } 8 \mid n-1, \\ 1, & \text{if } p \text{ and } n \text{ are odd}, 8 \nmid q+1, \text{and } 8 \nmid n-1, \\ 0, & \text{if } p \text{ is odd and } n \text{ are even.} \end{cases} \tag{39}$$

Proof. First we can notice that the only permutation polynomials of the form $E_k(x, 1)$ over $\mathbb{F}_q$ found are those for which q is odd and k belongs to the class sign $(2, a, b)$, where a, b vary depending on if $q = p, p^2, 3^e$, or 5^e. Let $\alpha \in \mathbb{F}_q$ be a fixed point of $E_k(x, 1)$. That is for all these permutations, we must have

$$\begin{aligned} k+1 &\equiv 2 \pmod p, \\ k+1 &\equiv -2 \pmod{\frac{q-1}{2}}. \end{aligned} \tag{40}$$

Then we have $E_k(\alpha, 1) = \alpha$; that is,

$$\frac{u^{k+1} - u^{-(k+1)}}{u - u^{-1}} = u + \frac{1}{u}, \tag{41}$$

which leads to

$$u^{k+1} - \frac{1}{u^{k+1}} - u^2 + \frac{1}{u^2} = 0. \tag{42}$$

Hence, we get

$$\left(u^{k+3} + 1\right)\left(u^{k-1} - 1\right) = 0. \tag{43}$$

Let $M = \{u \in \mathbb{F}_{q^2} : u^{q-1} = 1 \text{ or } u^{q+1} = 1\}$ be the set of all solutions of the q quadratic equations of the form $x^2 - \alpha x + 1 = 0$, with $\alpha \in \mathbb{F}_q$. Recall that if ω is a primitive element of $\mathbb{F}_{q^2}$ and if $M_1 = \{\omega^{(q-1)r} : r = 0, 1, \ldots, q\}$ and $M_2 = \{\omega^{(q+1)s} : s = 0, 1, \ldots, q-2\}$, then $M = M_1 \cup M_2$ and $M_1 \cap M_2 = \{\pm 1\}$. Also, u is a solution of $x^2 - \alpha x + 1 = 0$ if and only if u^{-1} is also a solution. So each fixed point $\alpha \in \mathbb{F}_q$ is associated with a pair (u, u^{-1}) in M. Therefore, the number of solutions is equal to half the sum of the solutions in both M_1 and M_2 excluding the common solutions.

Now $\omega^{(q-1)r} \in M_1$ is a solution if and only if $\omega^{(q-1)r(k+3)} = -1$ or $\omega^{(q-1)r(k-1)} = 1$.

Hence, we have

$$\begin{aligned} 2r(k+3) &\equiv 0 \pmod{q+1} \quad \text{or} \\ r(k-1) &\equiv 0 \pmod{q+1}. \end{aligned} \tag{44}$$

The numbers of solutions of these congruences in M_1 excluding the common solutions are, respectively, $\gcd(q+1, 2(k+3)) - \gcd(q+1, k+3)$ and $\gcd(q+1, k-1) - 2$ if p and n are odd. Therefore, the number of fixed points associated to the elements in M_1 is

$$\begin{aligned}\frac{1}{2}\big[&\gcd(q+1, 2(k+3)) - \gcd(q+1, k+3) \\ &+ \gcd(q+1, k-1) - 2\big].\end{aligned} \tag{45}$$

Similarly, if p and n are odd, the number of fixed points associated to elements in M_2 excluding the common solutions is

$$\begin{aligned}\frac{1}{2}\big[&\gcd(q-1, 2(k+3)) - \gcd(q-1, q+3) - 1 \\ &+ \gcd(q-1, k-1) - 2\big].\end{aligned} \tag{46}$$

Using the same argument, the numbers of solutions of these congruences in M_1 excluding the common solutions are, respectively, $\gcd(q+1, 2(k+3)) - \gcd(q+1, k+3)$ and $\gcd(q+1, k-1) - 2$ if p and n are even. Therefore, the number of fixed points associated to elements in M_1 is

$$\frac{1}{2}\left[\gcd(q+1, 2(k+3)) - \gcd(q+1, k+3) - 1\right]. \tag{47}$$

Similarly, if p and n are even, the number of fixed points associated to elements in M_2 excluding the common solutions is

$$\frac{1}{2}\left[\gcd(q-1, 2(k+3)) - \gcd(q-1, q+3) - 1\right]. \tag{48}$$

To complete the proof, we need to subtract the number of solutions when $\omega^{(q-1)r(k+3)} = -1$ and $\omega^{(q-1)r(k-1)} = 1$ at the same time. These are given by [7] and are equal to

$$\begin{cases} 8, & \text{if p and } n \text{ are odd}, 8 \mid q+1, \text{and } 8 \mid n-1, \\ 0, & \text{otherwise.} \end{cases} \tag{49}$$

Combine all the results above to conclude the answer. The case where q is even is pointless since in this case no permutation has been found. □

Theorem 12. *The number of fixed points of $E_k(x,-1)$ over $\mathbb{F}_q$ is given by*

$$\frac{1}{2}\left[a_1\cdot \gcd\left(k+3,2\left(q+1\right)\right)+a_2\cdot \gcd\left(k+3,q-1\right)\right.$$
$$\left.+a_3\cdot \gcd\left(k-1,2\left(q+1\right)\right)+\gcd\left(k-1,q-1\right)\right]-\varepsilon_{-1}, \tag{50}$$

where

$$a_1=\begin{cases}1, & \text{if } v_2\left(q+1\right)=v_2\left(k+3\right),\\ 0, & \text{otherwise},\end{cases}$$
$$a_2=\begin{cases}1, & \text{if } v_2\left(k+3\right)\le v_2\left(q-1\right)-1,\\ 0, & \text{otherwise},\end{cases}$$
$$a_3=\begin{cases}1, & \text{if } v_2\left(q+1\right)<v_2\left(k-1\right),\\ 0, & \text{otherwise},\end{cases} \tag{51}$$
$$\varepsilon_{-1}=\begin{cases}2, & \text{if } q\equiv 1 \pmod 4,\\ 0, & \text{otherwise}.\end{cases}$$

Proof. First of all, notice that for all permutations $E_k(x,-1)$ over $\mathbb{F}_q$ found so far, k is an odd integer. Let $\alpha\in\mathbb{F}_q$ be a fixed point of the permutation $E_k(x,-1)$ over $\mathbb{F}_q$. Then, $E_k(\alpha,-1)=\alpha$; that is,

$$E_k\left(x,-1\right)=\frac{u^{k+1}-u^{-(k+1)}}{u+u^{-1}}=u-\frac{1}{u}, \tag{52}$$

which implies

$$u^{k+1}-u^{-(k+1)}=u^2-u^{-2}. \tag{53}$$

Hence, we have

$$\left(u^{k+3}+1\right)\left(u^{k-1}-1\right)=0. \tag{54}$$

Let ω be a primitive element of $\mathbb{F}_{q^2}$. So we get $M_1(-1)=\{\omega^{(q-1)r/2}: r=1,3,...,2q+1\}$, $M_2(-1)=\{\omega^{(q+1)s}: s=0,1,....,q-2\}$, and $M(-1)=M_1(-1)\cup M_2(-1)$. For $i=0,1$, let $u_i=\omega^{(q^2-1)(1+2i)/4}$. From [6], we have $M_1(-1)\cap M_2(-1)=\{u_1,u_2\}$ if $q\equiv 1 \pmod 4$ and $M_1(-1)\cap M_2(-1)=\emptyset$ if $q\equiv 3 \pmod 4$. Therefore, as it was mentioned in [6], if we defined

$$N_3\left(-1\right)=\{u_1,u_2\}\quad \text{if } q\equiv 1 \pmod 4,$$
$$N_3\left(-1\right)=\emptyset\quad \text{if } q\equiv 3 \pmod 4 \tag{55}$$

and if

$$N_1\left(-1\right)=M_1\left(-1\right)\setminus N_3\left(-1\right),$$
$$N_2\left(-1\right)=M_2\left(-1\right)\setminus N_3\left(-1\right), \tag{56}$$

then

$$M\left(-1\right)=N_1\left(-1\right)\cup N_2\left(-1\right)\cup N_3\left(-1\right) \tag{57}$$

is a disjoint union.

Finally, from again [6], for $u\in\mathbb{F}_q$, if $u=u^{-1}$, then $u\in N_3(-1)$. Now a solution u of $(u^{k+3}+1)(u^{k-1}-1)=0$ is a solution of both $(u^{k+3}+1)$ and $(u^{k-1}-1)$ if and only if $u\in N_3(-1)$. Therefore, the number of solutions of (54) is the sum of the solutions in $N_1(-1)$, $N_2(-1)$, and $N_3(-1)$.

Let $v_p(m)$ denote the highest power of p dividing m if $m\neq 0$ and set $v_p(0)=\infty$. An element $u\in M_1(-1)$ is a solution of $u^{k+3}+1=0$ if and only if

$$r\left(k+3\right)\equiv q+1 \pmod{2\left(q+1\right)}, \tag{58}$$

which has solutions if and only if $\gcd(k+3,2(q+1))$ divides $(q+1)$ if and only if $v_2(k+3)\le v_2(q+1)$.

Let $d=\gcd(k+3,2(q+1))$. It is easy to see that

$$v_2\left(d\right)=\min\left\{v_2\left(\mathrm{k}+3\right),v_2\left(2\left(q+1\right)\right)\right\}=v_2\left(k+3\right). \tag{59}$$

Also let $\alpha,\beta\in\mathbb{Z}$, such that $\alpha(k+3)+2\beta(q+1)=d$. Then the solutions of (58) are

$$r=\frac{\alpha\left(q+1\right)}{d}+\frac{2\left(q+1\right)}{d}i,\quad (i=0,\ldots,d-1). \tag{60}$$

Using the same argument as in [6], α should be odd, because otherwise

$$v_2\left(d\right)\ge\min\left\{v_2\left(k+3\right)+1,v_2\left(2\left(q+1\right)\right)+1\right\}>v_2\left(k+3\right). \tag{61}$$

Now $v_2(q+1/d)=v_2(q+1)-v_2(d)=v_2(q+1)-v_2(k+1)$. Therefore, $(q+1)$ divides d if and only if $v_2(q+1)=v_2(k+3)$ and (58) has an odd solution r if and only if $v_2(q+1)=v_2(k+3)$. In this case, we have exactly $\gcd(k+3,2(q+1))$ solutions.

An element $u\in M_2(-1)$ is a solution of $u^{k+3}+1=0$ if and only if

$$\left(\omega^{(q+1)s}\right)^{k+3}=-1, \tag{62}$$

if and only if $((\omega^{(q+1)s})^{k+3})^2=1 \pmod{(q^2-1)}$, if and only if $(\omega^{(q+1)s(k+3)})^2=1 \pmod{q^2-1}$, if and only if

$$2\left(q+1\right)s\left(k+3\right)=0 \pmod{\left(q^2-1\right)}, \tag{63}$$

if and only $2s(k+3)=q-1 \pmod{(q-1)}$, and if and only if

$$s\left(k+3\right)=\frac{q-1}{2} \pmod{\left(q-1\right)}. \tag{64}$$

The last equation has a solution if and only if $\gcd(k+3,q-1))$ divides $(q-1)/2$, which is equivalent to the condition $v_2(k+3)\le v_2(q-1)-1$. Then the total number of those solutions is $\gcd(k+3,q-1)$.

An element $u\in M_1(-1)$ is a solution of $u^{k-1}-1=0$ if and only if

$$\omega^{(k-1)(q-1)r/2}=1 \pmod{\left(q^2-1\right)} \tag{65}$$

if and only if

$$r(k-1) \equiv 0 \pmod{2(q+1)}, \tag{66}$$

which has $\gcd((k-1), 2(q+1))$ solutions if it is solvable.

If $d = \gcd(k-1, 2(q+1))$, then

$$v_2(d) = \min\{v_2(k-1), v_2(2(q+1))\} = v_2(2(q+1)), \tag{67}$$

which implies that $2(q+1)/d$ is odd. But this can occur if and only if $v_2(q+1) < v_2(k-1)$, and the solutions of 8 in this case are

$$r = \frac{2(q+1)}{d} i, \quad (i = 0, \ldots, d-1). \tag{68}$$

An element $u \in M_2(-1)$ is a solution of $u^{k-1} - 1 = 0$ if and only if $(\omega^{(q+1)s})^{k-1} = 1$, if and only if

$$s(k-1) \equiv q-1 \pmod{q-1}, \tag{69}$$

if and only if

$$s(k-1) \equiv 0 \pmod{q-1}, \tag{70}$$

which has $\gcd(k-1, q-1)$ solutions.

To complete the proof, notice that by a similar method to that of the case $a = 1$, u is a solution of $u^{k+3} + 1 = 0$ (resp., $u^{k-1} - 1 = 0$) if and only if $-u^{-1}$ is also a solution, and the set of solutions of (58) and (66) on $N_3(-1)$ is the set of all solutions of $u^{k+3} + 1 = 0$ and $u^{k-1} - 1 = 0$ on $N_3(-1)$, which is empty if $q \equiv 3 \pmod 4$ and is equal to $\{u_1, u_2\}$ if $q \equiv 1 \pmod 4$. □

References

[1] R. Lidl, "Theory and applications of Dickson polynomials," in *Topics in Polynomials of One and Several Variables and Their Applications*, M. Rassias, H. M. Srivasta, and A. Yanushauskas, Eds., pp. 371–395, World Scientific Publishing, River Edge, NJ, USA, 1993.

[2] R. S. Coulter and R. W. Matthews, "On the permutation behaviour of Dickson polynomials of the second kind," *Finite Fields and their Applications*, vol. 8, no. 4, pp. 519–530, 2002.

[3] M. Henderson and R. Matthews, "Permutation properties of Chebyshev polynomials of the second kind over a finite field," *Finite Fields and their Applications*, vol. 1, no. 1, pp. 115–125, 1995.

[4] S. D. Cohen, "Dickson polynomials of the second kind that are permutations," *Canadian Journal of Mathematics*, vol. 46, no. 2, pp. 225–238, 1994.

[5] S. Ahmad, "Cycle structure of automorphisms of finite cyclic groups," *Journal of Combinatorial Theory A*, vol. 6, pp. 370–374, 1969.

[6] R. Lidl and G. L. Mullen, "Cycle structure of Dickson permutation polynomials," *Mathematical Journal of Okayama University*, vol. 33, pp. 1–11, 1991.

[7] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials*, vol. 65 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*, Longman Scientific & Technical, Essex, UK, 1993.