SIAM J. DISCRETE MATH.
Vol. 28, No. 2, pp. 722–735

DICKSON POLYNOMIALS OF THE SECOND KIND THAT PERMUTE $\mathbb{Z}_m$*

LONGJIANG QU† AND CUNSHENG DING‡

Abstract. In this paper, we investigate the permutation property of the Dickson polynomials $E_n(x,a)$ of the second kind over $\mathbb{Z}_m$. Due to a known result, it suffices to consider permutation polynomials $E_n(x,a)$ over $\mathbb{Z}_{p^t}$, where p is a prime and t is a positive integer. We identify all permutation polynomials of $E_n(x,a)$ over $\mathbb{Z}_{p^t}$ for (I) $p=2$ and (II) p is odd and a is a square over $\mathbb{Z}_p$. For odd p and nonsquares a in $\mathbb{Z}_p$, we determine a large class (if not all) of permutation polynomials $E_n(x,a)$ over $\mathbb{Z}_{p^t}$. A conjecture is also presented in this paper. If this conjecture is true, then all Dickson permutation polynomials $E_n(x,a)$ of the second kind over $\mathbb{Z}_m$ are determined.

Key words. Dickson polynomial of the second kind, permutation polynomial, residue class ring of integers

AMS subject classifications. 11C08, 05A05

DOI. 10.1137/130942589

1. Introduction.

A polynomial f over a finite ring R is called a *permutation polynomial* if f induces a one-to-one mapping on R. Permutation polynomials have been a hot topic of study for many years and have applications in coding theory [7, 13, 24], cryptography [15, 16, 19, 22, 23], combinatorial designs [7], and other areas of mathematics and engineering. Most studies have assumed that R is a finite field. There are also a few works on permutation polynomials modulo integers; see [6, 14, 20, 21].

Dickson polynomials would be important in both theory and applications. For instance, Dickson permutation polynomials of order five over $\mathbb{F}_{3^m}$, i.e., $D_5(x,a) = x^5 + ax^3 - a^2x$, led to a 70-year research breakthrough in combinatorics [8], gave a family of perfect nonlinear functions for cryptography [8], generated good linear codes [1, 25] for data communication and storage, and produced optimal signal sets for code division multiple access (CDMA) communications [9], to mention only a few applications of these Dickson permutation polynomials. For more information about Dickson polynomials, see the monograph [17] and the aforementioned references.

Let R be a ring. Dickson polynomials of the first kind (DPFK) and the second kind (DPSK) over R are defined by

$$D_n(X,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i X^{n-2i}$$

*Received by the editors October 23, 2013; accepted for publication (in revised form) March 5, 2014; published electronically May 1, 2014.
http://www.siam.org/journals/sidma/28-2/94258.html

†College of Science, National University of Defense Technology, Changsha, Hunan 410073, People's Republic of China (ljqu_happy@hotmail.com). This author's research was supported by the National Natural Science Foundation of China (61272484) and the Research Project of National University of Defense Technology (CJ 13-02-01).

‡Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong (cding@ust.hk). This author's research was supported by the Hong Kong Research Grants Council, project 601013.

and

$$E_n(X,a)=\sum_{i=0}^{\lfloor n/2\rfloor}\binom{n-i}{i}(-a)^iX^{n-2i},$$

respectively, where $\lfloor n/2\rfloor$ is the largest integer $\le n/2$, and $a\in R$. Dickson polynomials are also known as Chebyshev polynomials of the first and second kind due to their relations with Chebyshev polynomials.

Dickson permutation polynomials of the first kind over finite fields $\mathbb{F}_q$ have been completely determined. It is known that $D_n(X,a)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $\gcd(n,q^2-1)=1$ [17, Theorem 3.2]. Various results about the permutation behavior of Dickson polynomials of the second kind over $\mathbb{F}_q$ have also been established; see [3, 4] and the references therein. However, an explicit and simple characterization of the permutation property of Dickson polynomials of the second kind over $\mathbb{F}_q$ is missing. Henderson and Matthews showed that when $\eta(ab)=1$, where η is the quadratic multiplicative character of $\mathbb{F}_q$, $E_n(X,a)$ is a permutation polynomial over $\mathbb{F}_q$ if and only if $E_n(X,b)$ [11, Lemma 2.2] is also. Hence, the permutation behavior of the Dickson polynomials of the second kind splits into two distinct cases, according to whether a is a square or nonsquare. For odd primes p, Cohen proved the following result.

THEOREM 1.1 (see [5, Theorem 1.1]). *Let p be an odd prime and let a be a nonzero square in $\mathbb{F}_p$. Then $E_n(x,a)$ is a permutation polynomial of $\mathbb{F}_p$ if and only if*

$$\begin{cases} n+1\equiv\pm2 \pmod p,\\ n+1\equiv\pm2 \pmod{\frac{p-1}{2}},\\ n+1\equiv\pm2 \pmod{\frac{p+1}{2}}. \end{cases}\tag{1.1}$$

When a is a nonsquare, it can be easily verified that $E_n(x,a)$ is a permutation polynomial of $\mathbb{F}_p$ if n satisfies

$$\begin{cases} n+1\equiv\pm2 \pmod{p-1},\\ n+1\equiv\pm2 \pmod{p+1}. \end{cases}\tag{1.2}$$

In this paper, we study the permutation property of Dickson polynomials $E_n(x,a)$ of the second kind over $\mathbb{Z}_m$. This paper is organized as follows. Section 2 introduces known results on the permutation property of polynomials over $\mathbb{Z}_m$. Section 3 determines all Dickson permutation polynomials $E_n(x,a)$ over $\mathbb{Z}_{2^t}$, where t is any positive integer. Section 4 is a general discussion of Dickson permutation polynomials $E_n(x,a)$ over $\mathbb{Z}_{p^t}$ for odd primes p. Sections 5 and 6 deal with the cases that a is a nonsquare and square in $\mathbb{Z}_p$, respectively, where p is odd. Section 7 concludes this paper.

2. The permutation property of polynomials over $\mathbb{Z}_m$. We first recall the following lemma.

LEMMA 2.1 (see [17, Lemma 4.1]). *If $m=ab$, where $\gcd(a,b)=1$, then $g(x)$ is a permutation polynomial mod m if and only if $g(x)$ is a permutation polynomial mod a and mod b.*

By Lemma 2.1, the permutation property of the Dickson polynomials $E_n(x,a)$ over $\mathbb{Z}_m$ is equivalent to the permutation property of the polynomials $E_n(x,a)$s over $\mathbb{Z}_{p_i^{t_i}}$, where $m=\prod_{i=1}^s p_i^{t_i}$ and these p_i $(1\le i\le s)$ are pairwise distinct primes. Hence

we only need to discuss the permutation property of the polynomials $E_n(x,a)$ over $\mathbb{Z}_{p^t}$, where p is a prime.

LEMMA 2.2 (see [17, Corollary 4.3]). *A polynomial $g(x)$ is a permutation polynomial mod p^t, $t>1$, if and only if it is a permutation polynomial mod p and $g'(s)\not\equiv 0 \pmod p$ for every integer s, where $g'(x)$ denotes the derivative of $g(x)$.*

The following proposition follows directly from Lemma 2.2.

PROPOSITION 2.3. *Let $t\geq 2$ be an integer. Then a polynomial $g(x)$ is a permutation polynomial mod p^t if and only if it is a permutation polynomial mod p^2.*

Due to Lemma 2.2, we regard $E_n(x,a)$ and $E'_n(x,a)$ as two polynomials over $\mathbb{Z}_p$. Without loss of generality (w.l.o.g.), we can assume that $x,a\in\mathbb{Z}_p$. If $a=0$, then $E_n(x,a)=x^n$ and $E'_n(x)=nx^{n-1}$. It then follows from Lemma 2.2 that $E_n(x,0)$ is a permutation over $\mathbb{Z}_{p^t}$ if and only if $\gcd(n,p-1)=1$ and $\gcd(n,p)=1$. Thus in the rest of the paper, we always assume that $a\in\mathbb{Z}_p^*$, where $\mathbb{Z}_p^*$ is the set of nonzero elements of $\mathbb{Z}_p$.

The case $p=2$ will be dealt with separately and all Dickson permutation polynomials of the second kind over $\mathbb{Z}_{2^t}$ will be determined in what follows. When a is a square, thanks to Theorem 1.1 by Cohen, all the permutation polynomials $E_n(x,a)$ over $\mathbb{Z}_p$ are determined. Hence we only need to consider the case $\mathbb{Z}_{p^t}$, where $t\geq 2$. With Lemma 2.2 and Theorem 1.1, we will determine all permutation polynomials $E_n(x,a)$ over $\mathbb{Z}_{p^t}$ for all squares a. However, when a is a nonsquare, there does not exist a similar result as Theorem 1.1 [5]. In other words, we do not know whether there exists a permutation polynomial $E_n(x,a)$ over $\mathbb{Z}_p$ with n not satisfying (1.2). Experimental results show that for all $p<100$ and nonsquares a, all the permutation polynomial $E_n(x,a)$ over $\mathbb{Z}_p$ must satisfy (1.2). For convenience of subsequent discussions, we state the following conjecture.

CONJECTURE 2.4. *Let p be an odd prime and let a be a nonsquare of $\mathbb{Z}_p$. If $E_n(x,a)$ is a permutation polynomial of $\mathbb{Z}_p$, then* (1.2) *holds.*

3. The case that $p=2$. In this section, we describe all permutation polynomials $E_n(x,a)$ over $\mathbb{Z}_{2^t}$. By Lemma 2.2, w.l.o.g., we can assume that $a=1$. The following recurrence relation of the polynomials $E_n(x,a)$ will be needed.

LEMMA 3.1 (see [17, Lemma 2.3]). *$E_n(x,a)$ satisfies the second order recurrence relation*

$$E_{n+2}(x,a)=xE_{n+1}(x,a)-aE_n(x,a)$$

for $n\geq 0$ with initial values $E_0(x,a)=1$ and $E_1(x,a)=x$.

THEOREM 3.2.

(1) *$E_n(x,1)$ is a permutation polynomial over $\mathbb{Z}_2$ if and only if $n\equiv 1,2,3 \pmod 6$.*
(2) *$E_n(x,1)$ is a permutation polynomial over $\mathbb{Z}_{2^t}$ $(t\geq 2)$ if and only if $n\equiv 1,9 \pmod{12}$.*

Proof. (1) It is obvious that

$$E_n(0,1) \bmod 2 \equiv \begin{cases} 0 & \text{if } n \text{ is odd} \\ 1 & \text{otherwise.} \end{cases}$$

In other words, $(E_n(0,1) \bmod 2)_{n=0}^{\infty}$ forms the sequence

$$10,10,10,\ldots$$

with period 2. Now we compute $E_n(1,1) \bmod 2$. Plugging $a=1$ into the recurrence formula in Lemma 3.1, we obtain

$$E_{n+2}(x,1)=xE_{n+1}(x,1)-E_n(x,1)$$

for $n \geq 0$ with initial values $E_0(x,1) = 1$ and $E_1(x,1) = x$. It follows from this recurrence relation that the sequence $(E_n(1,1) \bmod 2)_{n=0}^{\infty}$ is

$$110, 110, \ldots, \tag{3.1}$$

which has period 3. Hence $E_n(0,1) \not\equiv E_n(1,1) \bmod 2$ if and only if $n \equiv 1,2,3 \pmod 6$. We have thus completed the proof of the first part.

(2) We now compute $E'_n(x,1) \bmod 2$ for $x \in \mathbb{Z}_2$. It is easy to see that

$$E'_n(0,1) \bmod 2 \equiv \begin{cases} 0 & \text{if } n \text{ is even,} \\ \frac{n+1}{2} \bmod 2 & \text{otherwise.} \end{cases}$$

Hence $E'_n(0,1) \not\equiv 0 \pmod 2$ if and only if $n \equiv 1 \pmod 4$. When n is odd, we have

$$\begin{aligned} E'_n(x,1) &\equiv \sum_{i=0}^{(n-1)/2} \binom{n-i}{i} (n-2i) x^{n-1-2i} \bmod 2 \\ &\equiv \sum_{i=0}^{(n-1)/2} \binom{n-i}{i} x^{n-1-2i} \bmod 2. \end{aligned}$$

Plugging $x = 1$ into the equivalence relation above, we have

$$E'_n(1,1) \equiv \sum_{i=0}^{(n-1)/2} \binom{n-i}{i} \equiv E_n(1,1) \bmod 2.$$

Then it follows from sequence (3.1) that $E'_n(1,1) \not\equiv 0 \pmod 2$ if and only if $n \equiv 0,1 \pmod 3$. Hence $E'_n(x,1) \not\equiv 0 \pmod 2$ for all $x \in \mathbb{Z}_2$ if and only if $n \equiv 1,9 \pmod{12}$. Combining this result with Lemma 2.2 and the first part of the theorem, we proved the second part. □

In this section, we determined all the permutation polynomials $E_n(x,a)$ over $\mathbb{Z}_{2^t}$. It should be noted that Theorem 3.2 can also be proved with [21, Theorem 1].

4. The case that p is an odd prime. Starting from now, we assume that $q = p^t$, where p is an odd prime and t is a positive integer.

When $t = 1$, all permutation polynomials $E_n(x,a)$ over $\mathbb{Z}_q$ are known for squares a due to Theorem 1.1, but not determined for nonsquares a as Conjecture 2.4 is not settled. In what follows we assume that $t \geq 2$.

By Lemma 2.2, $E_n(x,a)$ is a permutation polynomial over $\mathbb{Z}_{p^t} (t \geq 2)$ if and only if $E_n(x,a)$ is a permutation polynomial over $\mathbb{Z}_p$ and $E'_n(x,a) \not\equiv 0 \pmod p$ for any $x \in \mathbb{Z}_p$. Now we assume that $E_n(x,a)$ is a permutation polynomial over $\mathbb{Z}_p$. Then n is odd since $E_n(x,a)$ is an even or odd function depending on whether n is even or odd. First, we compute $E'_n(0,a)$. It follows from the definition of $E_n(x,a)$ that

$$E'_n(x,a) = \sum_{i=0}^{\frac{n-1}{2}} \binom{n-i}{i} (-a)^i (n-2i) x^{n-1-2i}.$$

Thus, we get

$$E'_n(0,a) = \frac{n+1}{2} (-a)^{\frac{n-1}{2}}.$$

Hence, we have the following lemma.

LEMMA 4.1. *$E'_n(0,a) \not\equiv 0 \pmod p$ if and only if*

$$n \not\equiv -1 \pmod p. \tag{4.1}$$

In the following, we assume that (4.1) holds and consider $E'_n(x,a) \bmod p$ for $x \in \mathbb{Z}_p^*$.

Note that any quadratic polynomial over $\mathbb{Z}_p$ factorizes over $\mathbb{F}_{p^2}$. Hence every $x \in \mathbb{Z}_p$ satisfies $x = u + au^{-1}$ for some $u \in \mathbb{F}_{p^2}$ and $a \in \mathbb{Z}_p$. As $x \in \mathbb{Z}_p$, we have $x^p = x$. Hence, $u^p + au^{-p} = u + au^{-1}$, which leads to $(u^{p-1}-1)(u^{p+1}-a) = 0$. We then have either $u^{p-1} = 1$ or $u^{p+1} = a$. Letting $x = u + au^{-1} \in \mathbb{Z}_p$, we have

$$E_n(x,a) = \begin{cases} \frac{u^{n+1} - a^{n+1}u^{-(n+1)}}{u - au^{-1}} & \text{if } u^2 \neq a \\ (n+1)(\pm\sqrt{a})^{n+1} & \text{if } \eta(a) = 1 \text{ and } u^2 = a, \end{cases} \tag{4.2}$$

where η is the quadratic multiplicative character over $\mathbb{Z}_p$. By definition, $u^2 \neq a$ if $\eta(a) = -1$. In connection with these definitions, as done in [12], we partition $\mathbb{Z}_p$ into disjoint S-sets, which are defined by

$$\begin{aligned} S_1 &= \{x = u + au^{-1} | u^{p-1} = 1 \text{ and } u \neq \pm\sqrt{a}\}, \\ S_2 &= \{x = u + au^{-1} | u^{p+1} = a \text{ and } u \neq \pm\sqrt{a}\}. \end{aligned} \tag{4.3}$$

If $\eta(a) = 1$, then $\mathbb{Z}_p = S_1 \cup S_2 \cup S_0$, where $S_0 = \{\pm 2\sqrt{a}\}$; if $\eta(a) = -1$, then $\mathbb{Z}_p = S_1 \cup S_2$. We can determine whether $x(\neq \pm 2\sqrt{a})$ is in S_1 or S_2 by calculating $\eta(x^2 - 4a)$. Precisely, $x \in S_1$ if $\eta(x^2 - 4a) = 1$, and $x \in S_2$ otherwise.

By [17, Lemma 2.4], $E_n(x,a)$ has the following generating function:

$$\sum_{n=0}^{\infty} E_n(x,a) z^n = \frac{1}{1 - xz + az^2}. \tag{4.4}$$

Hence $E'_n(x,a)$ has the generating function

$$\sum_{n=0}^{\infty} E'_n(x,a) z^n = \frac{z}{(1 - xz + az^2)^2}. \tag{4.5}$$

If $\eta(a) = 1$ and $x = \pm 2\sqrt{a}$, then

$$\frac{z}{(1 - xz + az^2)^2} = \frac{z}{(1 \mp \sqrt{a}z)^4} = \sum_{n=1}^{\infty} \binom{n+2}{3} (\pm\sqrt{a})^{n-1} z^n.$$

Hence, for $n \geq 1$ we have

$$E'_n(\pm 2\sqrt{a}, a) = \binom{n+2}{3} (\pm\sqrt{a})^{n-1}. \tag{4.6}$$

Now assume that $x = u + au^{-1} \neq \pm 2\sqrt{a}$. Let $d = u - au^{-1}$. Then $d^2 = x^2 - 4a$ and

$$\frac{1}{1 - xz + az^2} = \frac{1}{dz} \left(\frac{1}{1 - uz} - \frac{1}{1 - au^{-1}z} \right).$$

Furthermore,

$$\frac{z}{(1 - xz + az^2)^2} = \frac{1}{d^2 z} \left(\frac{1}{(1 - uz)^2} + \frac{1}{(1 - au^{-1}z)^2} \right) - \frac{2}{d^3 z^2} \left(\frac{1}{1 - uz} - \frac{1}{1 - au^{-1}z} \right).$$

Since $\frac{1}{1-bz} = \sum_{n=0}^{\infty} b^n z^n$ and $\frac{1}{(1-bz)^2} = \sum_{n=0}^{\infty} (n+1) b^n z^n$, we have

$$\sum_{n=0}^{\infty} E'_n(x,a) z^n = \sum_{n=0}^{\infty} \left[\frac{(n+2)}{d^2} \left(u^{n+1} + a^{n+1} u^{-(n+1)} \right) - \frac{2}{d^3} \left(u^{n+2} - a^{n+2} u^{-(n+2)} \right) \right] z^n.$$

Hence for $x = u + au^{-1} \neq \pm 2\sqrt{a}$, we have

$$E'_n(x,a) = \frac{(n+2)}{d^2} \left(u^{n+1} + (au^{-1})^{n+1} \right) - \frac{2}{d^3} \left(u^{n+2} - (au^{-1})^{n+2} \right). \tag{4.7}$$

Define

$$\begin{cases} r_1 = n+1 \pmod{p-1}, \\ r_2 = n+1 \pmod{p+1}, \end{cases} \tag{4.8}$$

where $-(p-1)/2 < r_1 \leq (p-1)/2$ and $-(p+1)/2 < r_2 \leq (p+1)/2$.

When $\eta(a) = -1$, we treat only the cases that $r_1, r_2 = \pm 2$ due to Conjecture 2.4. When $\eta(a) = 1$, it follows from Theorem 1.1 that $r_1 \in \{\pm 2, -\frac{p-1}{2} + 2, \frac{p-1}{2} - 2\}$ and $r_2 \in \{\pm 2, -\frac{p+1}{2} + 2, \frac{p+1}{2} - 2\}$. We assume first that $r_1, r_2 = \pm 2$. The other cases will be discussed later in the end of this section.

The following discussion is split into two cases according to whether $x \in S_1$ or $x \in S_2$. Note that we assume that $r_1, r_2 = \pm 2$ no matter what value of $\eta(a)$ is.

Case A: $x \in S_1$, i.e., $\eta(x^2 - 4a) = 1$.

Since $x = u + au^{-1} \in S_1$, we have $u^{p-1} = a^{p-1} = 1$. Hence $u^n = u^{r_1 - 1}$ and $a^n u^{-n} = a^{r_1 - 1} u^{1 - r_1}$.

Subcase A.I: $r_1 = 2$.

In this subcase, $n \equiv 1 \pmod{p-1}$. Then it follows from (4.7) that

$$\begin{aligned} E'_n(x,a) &\equiv \frac{n+2}{d^2} \left(u^2 + a^2 u^{-2} \right) - \frac{2}{d^3} \left(u^3 - a^3 u^{-3} \right) \pmod{p} \\ &\equiv \frac{n+2}{d^2} \left(x^2 - 2a \right) - \frac{2}{d^3} \cdot d \cdot \left(x^2 - a \right) \pmod{p}. \end{aligned}$$

Hence

$$\begin{aligned} & E'_n(x,a) \equiv 0 \pmod{p} \\ \Leftrightarrow\ & (n+2)(x^2 - 2a) \equiv 2(x^2 - a) \pmod{p} \\ \Leftrightarrow\ & nx^2 \equiv 2(n+1)a \pmod{p} \\ \Leftrightarrow\ & n \not\equiv 0 \pmod{p} \text{ and } x^2 \equiv \frac{2(n+1)a}{n} \pmod{p}. \end{aligned}$$

When $x^2 \equiv \frac{2(n+1)a}{n} \pmod{p}$, since $\eta(x^2 - 4a) = 1$, we deduce that $\eta(\frac{-2(n-1)a}{n}) = 1$. With Assumption (4.1), we have in this subcase the following conclusion:

There exists an $x \in S_1 \setminus \{0\}$ such that $E'_n(x,a) \equiv 0 \pmod{p}$

$$\Leftrightarrow \eta\left(\frac{2(n+1)a}{n} \right) = \eta\left(\frac{-2(n-1)a}{n} \right) = 1. \tag{4.9}$$

Subcase A.II: $r_1 = -2$.
In this subcase, $n \equiv -3 \pmod{p-1}$. Then it follows from (4.7) that

$$\begin{aligned} E'_n(x,a) &\equiv \frac{n+2}{d^2}\left(u^{-2}+a^{-2}u^2\right) - \frac{2}{d^3}\left(u^{-1}-a^{-1}u\right) \pmod p \\ &\equiv \frac{n+2}{d^2}\cdot\frac{x^2-2a}{a^2} + \frac{2}{d^3}\cdot\frac{d}{a} \pmod p. \end{aligned}$$

Hence,

$$\begin{aligned} & E'_n(x,a) \equiv 0 \pmod p \\ \Leftrightarrow\ & (n+2)(x^2-2a)+2a \equiv 0 \pmod p \\ \Leftrightarrow\ & (n+2)x^2 \equiv 2(n+1)a \pmod p \\ \Leftrightarrow\ & n \not\equiv -2 \pmod p \text{ and } x^2 \equiv \frac{2(n+1)a}{n+2} \pmod p. \end{aligned}$$

When $x^2 \equiv \frac{2(n+1)a}{n+2} \pmod p$, since $\eta(x^2-4a)=1$, we deduce that $\eta(\frac{-2(n+3)a}{n+2})=1$. With Assumption (4.1), we have in this subcase the following conclusion:

There exists an $x \in S_1 \setminus \{0\}$ such that $E'_n(x,a) \equiv 0 \pmod p$

$$\Leftrightarrow \eta\left(\frac{2(n+1)a}{n+2}\right) = \eta\left(\frac{-2(n+3)a}{n+2}\right) = 1. \tag{4.10}$$

Case B: $x \in S_2$, i.e., $\eta(x^2-4a) = -1$.
Since $x = u + au^{-1} \in S_2$, we have $u^{p+1} = a$ and $n \equiv r_2 - 1 \pmod{p+1}$. Let $n = k\cdot(p+1) + r_2 - 1$. Then $u^n = a^k u^{r_2-1}$ and $a^n u^{-n} = a^{2k+r_2-1}a^{-k}u^{1-r_2} = a^k a^{r_2-1}u^{1-r_2}$.

Subcase B.I: $r_2 = 2$.
In this subcase, $n \equiv 1 \pmod{p+1}$. Then it follows from (4.7) that

$$\begin{aligned} E'_n(x,a) &\equiv \frac{(n+2)a^k}{d^2}\left(u^2+a^2u^{-2}\right) - \frac{2a^k}{d^3}\left(u^3-a^3u^{-3}\right) \pmod p \\ &\equiv a^k\left(\frac{n+2}{d^2}\left(x^2-2a\right) - \frac{2}{d^3}\cdot d\cdot\left(x^2-a\right)\right) \pmod p. \end{aligned}$$

Similarly as in the subcase A.I, noting that $\eta(x^2-4a)=-1$, we have in this subcase the following conclusion:

There exists an $x \in S_2 \setminus \{0\}$ such that $E'_n(x,a) \equiv 0 \pmod p$

$$\Leftrightarrow \eta\left(\frac{2(n+1)a}{n}\right) = 1, \eta\left(\frac{-2(n-1)a}{n}\right) = -1. \tag{4.11}$$

Subcase B.II: $r_2 = -2$.
In this subcase, $n \equiv -3 \pmod{p+1}$. Then it follows from (4.7) that

$$\begin{aligned} E'_n(x,a) &\equiv \frac{(n+2)a^k}{d^2}\left(u^{-2}+a^{-2}u^2\right) - \frac{2a^k}{d^3}\left(u^{-1}-a^{-1}u\right) \pmod p \\ &\equiv a^k\left(\frac{n+2}{d^2}\frac{x^2-2a}{a^2} + \frac{2}{d^3}\cdot\frac{d}{a}\right) \pmod p. \end{aligned}$$

Similarly as in the subcase A.II, noting that $\eta(x^2-4a)=-1$, we have in this subcase the following conclusion:

There exists an $x \in S_2 \setminus \{0\}$ such that $E'_n(x,a) \equiv 0 \pmod p$

$$\Leftrightarrow \eta\left(\frac{2(n+1)a}{n+2}\right) = 1, \eta\left(\frac{-2(n+3)a}{n+2}\right) = -1. \tag{4.12}$$

At the end of this section, we consider the cases $r_1 \in \{-\frac{p-1}{2}+2, \frac{p-1}{2}-2\}$ and $r_2 \in \{-\frac{p+1}{2}+2, \frac{p+1}{2}-2\}$ when a is a nonzero square. We claim that for these values of r_1 and r_2, the conditions $E'_n(x,a) \not\equiv 0 \pmod p$ imply the same equations as $r_1, r_2 = \pm 2$ respectively. Only the case $r_1 = -\frac{p+1}{2}+2$ will be proved as an example. The proofs of the other cases are similar and omitted here.

Let $\eta(a) = 1$ and $r_1 = -\frac{p+1}{2}+2$. Then $n \equiv 1 - \frac{p-1}{2} \pmod{p-1}$. Hence

$$u^n = u^{1-\frac{p-1}{2}} = u \cdot \eta(u)$$

and

$$(au^{-1})^n = au^{-1} \cdot \eta(au^{-1}) = au^{-1} \cdot \eta(u).$$

It follows from (4.7) that

$$\begin{aligned} E'_n(x,a) &\equiv \eta(u)\left[\frac{(n+2)\left(u^2+a^2u^{-2}\right)}{d^2} - \frac{2\left(u^3-a^3u^{-3}\right)}{d^3}\right] \pmod p \\ &\equiv \eta(u)\left[\frac{(n+2)\left(x^2-2a\right)}{d^2} - \frac{2\left(x^2-a\right)}{d^2}\right] \pmod p. \end{aligned}$$

Plugging the above equation into $E'_n(x,a) \not\equiv 0 \pmod p$ will lead to the same equation as (4.9). The claim is proved. Hence we can assume that $r_1, r_2 = \pm 2$.

In the following two sections, we will distinguish two cases according to whether or not a is a square.

5. The case that p is odd and a is a nonsquare. We deal with the nonsquare case first. The result for $p = 3$ is presented first. The case $p \geq 5$ will be discussed later.

5.1. The subcase that $p = 3$. Let $p = 3$. Then $a = -1$ is the only nonsquare in $\mathbb{Z}_p$. The main result of this subcase is the following.

THEOREM 5.1.

(1) *$E_n(x,-1)$ is a permutation polynomial over $\mathbb{Z}_3$ if and only if $n \equiv 1 \pmod 4$.*

(2) *$E_n(x,-1)$ is a permutation polynomial over $\mathbb{Z}_{3^t}$ $(t \geq 2)$ if and only if $n \equiv 1, 9 \pmod{12}$.*

Proof. (1) Since n is odd, we have that $E_n(0,-1) = 0$. Hence $E_n(x,-1)$ is a permutation polynomial over $\mathbb{Z}_3$ if and only if

$$\{E_n(1,-1) \bmod 3, E_n(2,-1) \bmod 3\} = \{1,2\}. \tag{5.1}$$

Plugging $a = -1$ into Lemma 3.1, we get

$$E_{n+2}(x,-1) = xE_{n+1}(x,-1) + E_n(x,-1)$$

for $n \geq 0$ with initial values $E_0(x,-1) = 1$ and $E_1(x,-1) = x$. It follows from this recurrence relation that the sequence $(E_n(1,-1) \bmod 3)_{n=0}^{\infty}$ is

$$11202210, 11202210, \ldots,$$

whose period is 8. Similarly, the sequence $(E_n(2,-1) \pmod 3)_{n=0}^{\infty}$ is

$$12202110, 12202110, \ldots,$$

whose period is also 8. Hence (5.1) holds if and only if $n \equiv 1, 5 \pmod 8$, or, equivalently, if and only if $n \equiv 1 \pmod 4$.

(2) By Lemma 2.2 and the first part of this theorem, $E_n(x,-1)$ is a permutation polynomial over $\mathbb{Z}_{3^t}$ $(t \geq 2)$ if and only if $n \equiv 1 \pmod 4$ and $E_n'(x,-1) \not\equiv 0 \pmod 3$ for any $x \in \mathbb{Z}_3$. It follows from Lemma 4.1 that $E_n'(0,-1) \not\equiv 0 \pmod 3$ if and only if $n \equiv 0, 1 \pmod 3$. Now we consider $E_n'(\pm 1,-1) \bmod 3$. It can be easily verified that $S_1 = \{0\}$, $S_2 = \{\pm 1\}$, and $r_2 \equiv 2 \pmod{p+1=4}$. Similarly as the discussion in Subcase B.I, we can prove that $E_n'(\pm 1,-1) \equiv 0 \pmod 3$ if and only if

$$nx^2 \equiv 2(n+1)a \pmod 3.$$

Plugging $x^2 = 1$ and $a = -1$ into the above equation, we get $n \equiv n+1 \pmod 3$, which is impossible. Hence $E_n'(\pm 1,-1) \not\equiv 0 \pmod 3$ for any $n \geq 0$.

Summarizing the discussions above proves that $E_n(x,-1)$ is a permutation polynomial over $\mathbb{Z}_{3^t}$ $(t \geq 2)$ if and only if $n \equiv 1 \pmod 4$ and $n \equiv 0, 1 \pmod 3$, or, equivalently, $n \equiv 1, 9 \pmod{12}$. We are done. □

Remark. Note that when $p = 3$, $n \equiv 1 \pmod 4$ is consistent with (1.2). This means that Conjecture 2.4 holds for $p = 3$, which is consistent with the experimental result.

5.2. The subcase that $p \geq 5$. In this subsection we first assume that $p \geq 7$ is a prime. The case $p = 5$ will be treated later. Let n be an integer satisfying (1.2). As discussed earlier, for any $x \in \mathbb{Z}_p$, either $\eta(x^2 - 4a) = 1$ or $\eta(x^2 - 4a) = -1$. Noting that $\mathbb{Z}_p = S_1 \cup S_2$, and plugging $\eta(a) = -1$ into (4.9)–(4.12), with assumption (4.1) we arrive at the following conclusions:

1. When $(r_1, r_2) = (2, 2)$, there exists an $x \in \mathbb{Z}_p^*$ such that $E_n'(x,a) \equiv 0 \pmod p$ if and only if
$$\eta\left(\frac{2(n+1)}{n}\right) = -1.$$
2. When $(r_1, r_2) = (2, -2)$, there exists an $x \in \mathbb{Z}_p^*$ such that $E_n'(x,a) \equiv 0 \pmod p$ if and only if
$$\eta\left(\frac{2(n+1)}{n}\right) = \eta\left(\frac{-2(n-1)}{n}\right) = -1$$
or
$$\eta\left(\frac{2(n+1)}{n+2}\right) = -1 \text{ and } \eta\left(\frac{-2(n+3)}{n+2}\right) = 1.$$
3. When $(r_1, r_2) = (-2, 2)$, there exists an $x \in \mathbb{Z}_p^*$ such that $E_n'(x,a) \equiv 0 \pmod p$ if and only if
$$\eta\left(\frac{2(n+1)}{n+2}\right) = \eta\left(\frac{-2(n+3)}{n+2}\right) = -1$$
or
$$\eta\left(\frac{2(n+1)}{n}\right) = -1 \text{ and } \eta\left(\frac{-2(n-1)}{n}\right) = 1.$$

4. When $(r_1, r_2) = (-2, -2)$, there exists an $x \in \mathbb{Z}_p^*$ such that $E_n'(x, a) \equiv 0 \pmod{p}$ if and only if

$$\eta\left(\frac{2(n+1)}{n+2}\right) = -1.$$

Summarizing the discussions above, we obtain the following theorem.

THEOREM 5.2. *Let $p \geq 7$ be an odd prime and n be an integer satisfying* (1.2). *Let $\eta(a) = -1$. Then the following hold:*

1. *When $(r_1, r_2) = (2, 2)$, $E_n(x, a)$ is a permutation polynomial over $\mathbb{Z}_{p^t} (t \geq 2)$ if and only if*

$$n \equiv 0 \pmod{p} \text{ or } \eta\left(\frac{2(n+1)}{n}\right) = 1.$$

2. *When $(r_1, r_2) = (2, -2)$, $E_n(x, a)$ is a permutation polynomial over $\mathbb{Z}_{p^t} (t \geq 2)$ if and only if*

$$n \equiv 0, -2 \pmod{p}$$

or

$$\begin{cases} n \not\equiv 0, -1, -2 \pmod{p} \text{ and} \\ \left(\eta\left(\frac{2(n+1)}{n}\right) - 1\right)\left(\eta\left(\frac{-2(n-1)}{n}\right) - 1\right) = 0 \text{ and} \\ \left(\eta\left(\frac{2(n+1)}{n+2}\right) - 1\right)\left(\eta\left(\frac{-2(n+3)}{n+2}\right) + 1\right) = 0. \end{cases}$$

3. *When $(r_1, r_2) = (-2, 2)$, $E_n(x, a)$ is a permutation polynomial over $\mathbb{Z}_{p^t} (t \geq 2)$ if and only if*

$$n \equiv 0, -2 \pmod{p}$$

or

$$\begin{cases} n \not\equiv 0, -1, -2 \pmod{p} \text{ and} \\ \left(\eta\left(\frac{2(n+1)}{n+2}\right) - 1\right)\left(\eta\left(\frac{-2(n+3)}{n+2}\right) - 1\right) = 0 \text{ and} \\ \left(\eta\left(\frac{2(n+1)}{n}\right) - 1\right)\left(\eta\left(\frac{-2(n-1)}{n}\right) + 1\right) = 0. \end{cases}$$

4. *When $(r_1, r_2) = (-2, -2)$, $E_n(x, a)$ is a permutation polynomial over $\mathbb{Z}_{p^t} (t \geq 2)$ if and only if*

$$n \equiv -2 \pmod{p} \text{ or } \eta\left(\frac{2(n+1)}{n+2}\right) = 1.$$

Now we turn to the case $p = 5$. Let a be a nonsquare of $\mathbb{Z}_5$. According to (1.2), $E_n(x, a)$ is a permutation polynomial over $\mathbb{Z}_p$ if and only if $n \equiv 1, 9 \pmod{12}$. Noting that $p - 1 = 4$, we get $r_1 = 2$, where r_1 is defined in (4.8). Hence $n \equiv 1, 9 \pmod{12}$. Then it follows from $\eta(a) = -1$ that (4.9) holds if and only if $\eta(\frac{2(n+1)}{n}) = \eta(\frac{-2(n-1)}{n}) = -1$, which has no solution in Z_5. Let r_2 be defined as in (4.8). Then $r_2 = \pm 2$. If r_2=2, then $n \equiv 1 \pmod{12}$. With $\eta(a) = -1$, we have that (4.11) holds if and only if $\eta(\frac{2(n+1)}{n}) = -1$ and $\eta(\frac{-2(n-1)}{n}) = 1$, which holds if and only if $n \equiv 2$

(mod 5). Thus in this case $E_n(x,a)$ is a permutation polynomial over $\mathbb{Z}_{p^t}(t \geq 2)$ if and only if $n \not\equiv -1, 2 \pmod 5$. With $n \equiv 1 \pmod{12}$, we obtain that $n \equiv 1, 13, 25 \pmod{60}$. Similarly, if $r_2 = -2$, then $E_n(x,a)$ is a permutation polynomial over $\mathbb{Z}_{p^t}(t \geq 2)$ if and only if $n \equiv 21, 45, 57 \pmod{60}$.

Hence we arrive at the following conclusion.

THEOREM 5.3. *Let $p = 5$ and n be an integer satisfying (1.2), i.e., $n \equiv 1, 9 \pmod{12}$. Let $\eta(a) = -1$. Then $E_n(x,a)$ is a permutation polynomial over $\mathbb{Z}_{p^t}(t \geq 2)$ if and only if $n \equiv 1, 13, 21, 25, 45, 57 \pmod{60}$.*

Note that experimental results show that Conjecture 2.4 holds for $p < 100$. Theorem 5.2 provides all permutation polynomials of $E_n(x,a)$ over $\mathbb{Z}_{p^t}$ for $p < 100$ and nonsquare elements a. If Conjecture 2.4 holds, then all such permutation polynomials $E_n(x,a)$ over $\mathbb{Z}_{p^t}$ $(p \geq 7)$ are determined in Theorem 5.2 above.

6. The case that p is odd and a is a square. Similarly, we first give the result for $p = 3$. The case $p \geq 5$ will be discussed later.

6.1. The subcase that $p = 3$. Let $p = 3$. We assume $a = 1$ since a is a nonzero square.

THEOREM 6.1.

(1) *$E_n(x,1)$ is a permutation polynomial over $\mathbb{Z}_3$ if and only if*

$$n \equiv 1, 3 \pmod 6. \tag{6.1}$$

(2) *$E_n(x,1)$ is a permutation polynomial over $\mathbb{Z}_{3^t}$ $(t \geq 2)$ if and only if $n \equiv 1, 3, 13, 15 \pmod{18}$.*

Proof. (1) It follows directly from Theorem 1.1.

(2) By Lemma 2.2 and the first part of this theorem, $E_n(x,1)$ is a permutation polynomial over $\mathbb{Z}_{3^t}$ $(t \geq 2)$ if and only if $n \equiv 1, 3 \pmod 6$ and $E_n'(x,1) \not\equiv 0 \pmod 3$ for all $x \in \mathbb{Z}_3$. It follows from Lemma 4.1 that $E_n'(0,1) \not\equiv 0 \pmod 3$ if and only if $n \equiv 0, 1 \pmod 3$. Now we consider $E_n'(\pm 1, 1) \bmod 3$. Since $x^2 = 1 = 4a$, it follows from (4.6) that $E_n'(\pm 1, 1) \not\equiv 0 \pmod 3$ if and only if

$$\binom{n+2}{3} \not\equiv 0 \pmod 3. \tag{6.2}$$

By Lucas' formula, (6.2) holds if and only if

$$n \equiv 1, 2, 3, 4, 5, 6 \pmod 9. \tag{6.3}$$

It is easy to see that both (6.1) and (6.3) hold if and only if $n \equiv 1, 3, 13, 15 \pmod{18}$. We finish the proof. □

6.2. The subcase that $p \geq 5$. In this subsection we first assume that $p \geq 11$ is a prime. The cases $p = 5$ and $p = 7$ will be discussed later. Now $\eta(a) = 1$ and $\mathbb{Z}_p = S_1 \cup S_2 \cup S_0$, where $S_0 = \{\pm 2\sqrt{a}\}$. We define

$$\begin{cases} \bar{r}_1 = n + 1 \pmod{(p-1)/2}, \\ \bar{r}_2 = n + 1 \pmod{(p+1)/2}, \\ \bar{r}_3 = n + 1 \pmod p, \end{cases} \tag{6.4}$$

where $-(p-1)/4 < \bar{r}_1 \leq (p-1)/4$, $-(p+1)/4 < \bar{r}_2 \leq (p+1)/4$, and $-p/2 < \bar{r}_3 < p/2$.

Let $E_n(x,a)$ be a permutation polynomial over $\mathbb{Z}_{p^t}(t \geq 2)$. Then it is a permutation polynomial over $\mathbb{Z}_p$. Then it follows from Theorem 1.1 that $\bar{r}_i = \pm 2$ for each

i. If $\bar{r}_1 = 2$, then $r_1 = 2$ or $r_1 = -\frac{p-1}{2} + 2$, where r_1 is defined in (4.8). It follows from the discussion in section 4 that either case leads to the same equation, i.e., (4.9). Similarly, $\bar{r}_1 = -2$ and $\bar{r}_2 = \pm 2$ lead to (4.10)–(4.12), respectively. The following discussion is split into two cases according to the value of $\bar{r}_3$.

If $\bar{r}_3 = 2$, then $n \equiv 1 \pmod{p}$. For $x = \pm 2\sqrt{a}$, it follows from (4.6) that $E'_n(x,a) \equiv \binom{n+2}{3}(\pm\sqrt{a})^{n-1} \not\equiv 0 \pmod{p}$. For $x \in S_1 \cup S_2$, we have that $\frac{2(n+1)a}{n} \equiv 4a \pmod{p}$, $\frac{-2(n-1)a}{n} \equiv 0 \pmod{p}$, $\frac{2(n+1)a}{n+2} \equiv \frac{4}{3}a \pmod{p}$, and $\frac{-2(n+3)a}{n+2} \equiv \frac{-8}{3}a \pmod{p}$. Plugging these equations and $\eta(a) = 1$ into (4.9)–(4.12), we deduce that there exists an $x \in \mathbb{Z}_p$ such that $E'_n(x,a) \equiv 0 \pmod{p}$ if and only if

1. $\eta\left(\frac{4}{3}\right) = \eta\left(\frac{-8}{3}\right) = 1$ when $\bar{r}_1 = -2 \neq \bar{r}_3$;
2. $\eta\left(\frac{4}{3}\right) = 1$ and $\eta\left(\frac{-8}{3}\right) = -1$ when $\bar{r}_2 = -2 \neq \bar{r}_3$.

Similarly, if $\bar{r}_3 = -2$, then $n \equiv -3 \pmod{p}$. For $x = \pm 2\sqrt{a}$, it follows from (4.6) that $E'_n(x,a) \equiv \binom{n+2}{3}(\pm\sqrt{a})^{n-1} \not\equiv 0 \pmod{p}$. For $x \in S_1 \cup S_2$, we have that $\frac{2(n+1)a}{n} \equiv \frac{4}{3}a \pmod{p}$, $\frac{-2(n-1)a}{n} \equiv \frac{-8}{3}a \pmod{p}$, $\frac{2(n+1)a}{n+2} \equiv 4a \pmod{p}$, and $\frac{-2(n+3)a}{n+2} \equiv 0 \pmod{p}$. Plugging these equations and $\eta(a) = 1$ into (4.9)–(4.12), we deduce that there exists an $x \in \mathbb{Z}_p$ such that $E'_n(x,a) \equiv 0 \pmod{p}$ if and only if

1. $\eta\left(\frac{4}{3}\right) = \eta\left(\frac{-8}{3}\right) = 1$ when $\bar{r}_1 = 2 \neq \bar{r}_3$;
2. $\eta\left(\frac{4}{3}\right) = 1$ and $\eta\left(\frac{-8}{3}\right) = -1$ when $\bar{r}_2 = 2 \neq \bar{r}_3$.

Note that $\eta\left(\frac{4}{3}\right) = 1$ if and only if $\eta(3) = 1$, which is equivalent to $p \equiv 1, 11 \pmod{12}$; and $\eta(-2) = 1$ if and only if $p \equiv 1, 3 \pmod{8}$.

Now we turn to the cases $p = 5$ and $p = 7$. It is clear that $\eta(\frac{4}{3}) = -1$ holds for each case. Let $\bar{r}_3 = n + 1 \pmod{p}$, where $-p/2 < \bar{r}_3 < p/2$. Then $\bar{r}_3 = \pm 2$. If $\bar{r}_3 = 2$, then $n \equiv 1 \pmod{p}$. If $\bar{r}_3 = -2$, then $n \equiv -3 \pmod{p}$. Similarly as in the discussion above, we can deduce that $E'_n(x,a) \not\equiv 0 \pmod{p}$ holds for any $x \in \mathbb{Z}_p$. Hence $E_n(x,a)$ is a permutation polynomial over $\mathbb{Z}_{p^t} (t \geq 2)$ if and only if n is an integer satisfying (1.1).

The above discussions are summarized in the following theorem.

THEOREM 6.2. *Let $p \geq 5$ be an odd prime and let n be an integer satisfying* (1.1). *Let $\eta(a) = 1$. If $p = 5$ or $p = 7$, then $E_n(x,a)$ is always a permutation polynomial over $\mathbb{Z}_{p^t} (t \geq 2)$. If $p \geq 11$, the following four conclusions hold:*

1. *When $\bar{r}_1 = \bar{r}_2 = \bar{r}_3$, $E_n(x,a)$ is always a permutation polynomial over $\mathbb{Z}_{p^t} (t \geq 2)$.*
2. *When $\bar{r}_1 = \bar{r}_2 \neq \bar{r}_3$, $E_n(x,a)$ is a permutation polynomial over $\mathbb{Z}_{p^t} (t \geq 2)$ if and only if $\eta(3) = -1$, or, equivalently, if and only if*

$$p \equiv 5, 7 \pmod{12}.$$

3. *When $\bar{r}_1 = \bar{r}_3 \neq \bar{r}_2$, $E_n(x,a)$ is a permutation polynomial over $\mathbb{Z}_{p^t} (t \geq 2)$ if and only if $(\eta(3) + 1)(\eta(-2) - 1) = 0$, or, equivalently, if and only if*

$$p \not\equiv 13, 23 \pmod{24}.$$

4. *When $\bar{r}_2 = \bar{r}_3 \neq \bar{r}_1$, $E_n(x,a)$ is a permutation polynomial over $\mathbb{Z}_{p^t} (t \geq 2)$ if and only if $(\eta(3) + 1)(\eta(-2) + 1) = 0$, or, equivalently, if and only if*

$$p \not\equiv 1, 11 \pmod{24}.$$

All permutation polynomials $E_n(x,a)$ over $\mathbb{Z}_{p^t} (t \geq 2)$ for a being a square and $p \geq 5$ are determined by Theorem 6.2.

7. Summary and concluding remarks. In this paper, the permutation property of the Dickson polynomials $E_n(x, a)$ of the second kind over $\mathbb{Z}_m$ was investigated. All permutation polynomials of $E_n(x, a)$ over $\mathbb{Z}_{p^t}$ were determined except the case that $p \geq 7$ and a is a nonsquare.

In the case that $p \geq 7$ and a is a nonsquare, a large class of permutation polynomials of $E_n(x, a)$ over $\mathbb{Z}_{p^t}$ were also identified in Theorem 5.2. If Conjecture 2.4 is true, then all Dickson polynomials $E_n(x, a)$ of the second kind over $\mathbb{Z}_{p^t}$ and hence over $\mathbb{Z}_m$ were completely identified in this paper due to Lemma 2.1. So the only problem left regarding the permutation property of the Dickson polynomials $E_n(x, a)$ of the second kind over $\mathbb{Z}_m$ is the settlement of Conjecture 2.4. The reader is invited to attack this conjecture.

While Dickson polynomials of the first kind over finite fields have many applications in mathematics and engineering, it would also be interesting to look into applications of the Dickson permutation polynomials $E_n(x, a)$ of the second kind over $\mathbb{Z}_m$ in other areas of mathematics and engineering.

Acknowledgment. The authors would like to thank the reviewer for his/her detailed comments that much improved the technical and editorial quality of this paper.

REFERENCES

[1] C. Carlet, C. Ding, and J. Yuan, *Linear codes from highly nonlinear functions and their secret sharing schemes,* IEEE Trans. Inform. Theory, 51 (2005), pp. 2089–2102.
[2] M. Cipu, *Dickson polynomials that are permutations,* Serdica Math. J., 30 (2004), pp. 177–194.
[3] M. Cipu and S. D. Cohen, *Dickson polynomial permutations and Gröbner bases,* Contemp. Math., 461 (2008), pp. 79–90.
[4] R. S. Coulter and R. W. Matthews, *On the permutation behavior of Dickson polynomials of the second kind,* Finite Fields Appl., 8 (2002), pp. 519–530.
[5] S. D. Cohen, *Dickson polynomials of the second kind that are permutations,* Canad. Math. Bull., 46 (1994), pp. 225–238.
[6] J. Diaz-Vargas, C. J. Rubio-Barrios, J. A. Sozaya-Chan, and H. Tapia-Recillas, *Self-invertible permutation polynomials over Z_m,* Int. J. Algebra, 5 (2011), pp. 1135–1153.
[7] C. Ding and T. Helleseth, *Optimal ternary cyclic codes from monomials,* IEEE Trans. Inform. Theory, 59 (2013), pp. 5898–5904.
[8] C. Ding and J. Yuan, *A family of skew Hadamard difference sets,* J. Combin. Theory Ser. A, 113 (2006), pp. 1526–1535.
[9] C. Ding and J. Yin, *Signal sets from functions with optimum nonlinearity,* IEEE Trans. Comm., 55 (2007), pp. 936–940.
[10] M. Henderson, *A note on the permutation behaviour of the Dickson polynomials of the second kind,* Bull. Austr. Math. Soc., 56 (1997), pp. 499–505.
[11] M. Henderson and R. Matthews, *Permutation properties of Chebyshev polynomials of the second kind over a finite field,* Finite Fields Appl., 1 (1995), pp. 115–125.
[12] M. Henderson and R. Matthews, *Dickson polynomials of the second kind which are permutation polynomials over a finite field,* New Zealand J. Math., 27 (1998), pp. 227–244.
[13] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory,* Finite Fields Appl., 13 (2007), pp. 58–70.
[14] S. Li, *Permutation polynomials modulo m,* arXiv:0509523v6, 2005.
[15] R. Lidl, *On cryptosystems based on permutation polynomials and finite fields,* in Advances in Cryptology—EuroCrypt '84, T. Beth, N. Cot, and I. Ingemarsson, eds., Lecture Notes in Comput. Sci. 209, Springer-Verlag, Berlin, 1985, pp. 10–15.
[16] R. Lidl and W. B. Müller, *Permutation polynomials in RSA-cryptosystems,* in Advances in Cryptology, Plenum, New York, 1984, pp. 293–301.
[17] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials,* Longman Scientific and Technical, Harlow, UK, 1993.
[18] R. Lidl and H. Niederreiter, *Finite Fields,* 2nd ed., Encyclopedia Math. Appl. 20, Cambridge University Press, Cambridge, 1997.

[19] G. L. Mullen, *Permutation polynomials and nonsingular feedback shift registers over finite fields,* IEEE Trans. Inform. Theory, 35 (1989), pp. 900–902.
[20] G. Mullen and H. Stevens, *Permutation functions (mod m),* Acta Math. Hungar., 44 (1984), pp. 237–241.
[21] R. L. Rivest, *Permutation polynomials modulo* 2^w*,* Finite Fields Appl., 7 (2001), pp. 287–292.
[22] R. L. Rivest, A. Shamir, and L. M. Adelman, *A method for obtaining digital signatures and public-key cryptosystems,* Comm. ACM, 21 (1978), pp. 120–126.
[23] J. Schwenk and K. Huber, *Public key encryption and digital signatures based on permutation polynomials,* Electronic Lett., 34 (1998), pp. 759–760.
[24] J. Sun and O. Y. Takeshita, *Interleavers for turbo codes using permutation polynomials over integer rings,* IEEE Trans. Inform. Theory, 51 (2005), pp. 101–119.
[25] J. Yuan, C. Carlet, and C. Ding, *The weight distribution of a class of linear codes from perfect nonlinear functions,* IEEE Trans. Inform. Theory, 52 (2006), pp. 712–717.