Electronic Research Archive

http://www.aimspress.com/journal/era

ERA, 30(6): 2109–2120.
DOI: 10.3934/era.2022106
Received: 12 August 2021
Revised: 28 December 2021
Accepted: 30 December 2021
Published: 14 April 2022

Research article

Permutations involving squares in finite fields

Hai-Liang Wu[1] **and Li-Yuan Wang**[2,*]

[1] School of Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[2] School of Physical and Mathematical Sciences, Nanjing Tech University, Nanjing 211816, China

* **Correspondence:** Email: wly@smail.nju.edu.cn.

Abstract: Let p be an odd prime and let $\mathbb{F}_p$ be the finite field of p elements. In 2019, Sun studied some permutations involving squares in $\mathbb{F}_p$. In this paper, by the theory of local fields we generalize this topic to $\mathbb{F}_{p^2}$, which gives a partial answer to the question posed by Sun.

Keywords: quadratic residues; permutations; primitive roots; local fields

1. Introduction

Permutation is an important mathematical concept. Investigating permutations over finite fields is a classical topic in number theory, combinatorics and finite fields. Let $g(x)$ be a polynomial over a ring R. We say that $g(x)$ is a permutation polynomial if it acts as a permutation of all elements of the ring, i.e., the map

$$x \mapsto g(x)$$

is a bijection over R. By the Lagrange interpolation formula it is easy to see that every permutation over a finite field is induced by a permutation polynomial (for the recent progress on permutation polynomial readers may refer to the survey paper [1]).

Now we introduce some earlier work on this topic. Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. Clearly $f_a(x) = ax$ is a permutation polynomial over $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. The famous Zolotarev lemma [2] says that the sign of the permutation on $\mathbb{F}_p$ induced by $f_a(x)$ coincides with the Legendre symbol $(\frac{a}{p})$. This fact provides us with a different proof (see [3, 4]) of the law of quadratic reciprocity. Later G. Frobenius [5] generalized Zolotarev's result to the Jacobi symbols. Readers may refer to [6, 7] for more related information.

Let k be a positive integer with $\gcd(k, p-1) = 1$. Then clearly the polynomial $g_k(x) = x^k$ is a permutation polynomial over $\mathbb{F}_p$. The authors [8] determined the sign of this permutation induced by $g_k(x)$ via extending the method of Zolotarev. Moreover, with the tools in group representation theory, Duke and Hopkins [9] generalized this result to finite groups. They also gave the law of quadratic reciprocity on finite groups.

Recently, Sun [10, 11] studied some permutations involving squares in $\mathbb{F}_p$. For example, let $p = 2n + 1$ be an odd prime and let $b_1, \cdots, b_n$ be the sequence of all the n quadratic residues among $1, \cdots, p-1$ in ascending order. Then it is easy to see that the sequence

$$\overline{1^2}, \cdots, \overline{n^2}, \tag{1.1}$$

is a permutation τ_p of

$$\overline{b_1}, \cdots, \overline{b_n}, \tag{1.2}$$

where $\overline{a}$ denotes the element a mod $p\mathbb{Z}$ for each $a \in \mathbb{Z}$. Sun showed that

$$\operatorname{sgn}(\tau_p) = \begin{cases} 1 & \text{if } p \equiv 3 \pmod 8, \\ (-1)^{(h(-p)+1)/2} & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$ and $\operatorname{sgn}(\tau_p)$ denotes the sign of τ_p. While studying this topic, Sun and his collaborator [10, 12] also determined some products which concerns pth roots of unity. For instance, in the case $p \equiv 3 \pmod 4$ Sun [10] obtained

$$\prod_{0<j<k<p/2} \left(\zeta_p^{j^2} - \zeta_p^{k^2}\right) = \begin{cases} (-p)^{(p-3)/8} & \text{if } 8 \mid p-3, \\ (-1)^{\frac{p+1}{8}+\frac{h(-p)-1}{2}} p^{(p-3)/8}\mathbf{i} & \text{if } 8 \mid p-7. \end{cases} \tag{1.3}$$

Later Petrov and Sun [12] showed that if $p \equiv 1 \pmod 8$, then

$$\prod_{0<j<k<p/2} \left(\zeta_p^{j^2} + \zeta_p^{k^2}\right) = (-1)^{\#\left\{1\le k<\frac{p}{4}:\left(\frac{k}{p}\right)=-1\right\}}$$

and that if $p \equiv 5 \pmod 8$, then

$$\prod_{0<j<k<p/2} \left(\zeta_p^{j^2} + \zeta_p^{k^2}\right) = (-1)^{\#\left\{1\le k<\frac{p}{4}:\left(\frac{k}{p}\right)=-1\right\}}\varepsilon_p^{-h(p)},$$

where $\#S$ denotes the cardinality of a set S and $h(p)$ is the class number of $\mathbb{Q}(\sqrt{p})$. These products have close connections with permutations over $\mathbb{F}_p$. Readers may consult [10, 12] for details.

Along this line, the first author [13] determined the sign of τ_p in the case $p \equiv 1 \pmod 4$. Motivated by Sun's work, the first author also studied some permutations on $\mathbb{F}_p$ involving primitive roots modulo p. In fact, let $g_p \in \mathbb{Z}$ be a primitive root modulo p. Then the sequence

$$\overline{g_p^2}, \overline{g_p^4}, \cdots, \overline{g_p^{p-1}} \tag{1.4}$$

is a permutation on the sequence (1.2). In [13] the first author gave the sign of this permutation in the case $p \equiv 1 \pmod 4$.

Recently Sun posed the following problem:

In an arbitrary finite field $\mathbb{F}_q$ with $2 \nmid q$, can we get an analogue of the above permutation which involves non-zero squares over $\mathbb{F}_q$?

In this paper, we mainly generalize the above permutations to $\mathbb{F}_{p^2}$. To do this, we first need to construct two sequences of non-zero squares in $\mathbb{F}_{p^2}$ which are analogues of the sequences (1.1) and (1.4). We now introduce some notations and some basic facts involving local fields.

Let $p = 2n + 1$ be an odd prime, and let ζ_{p^2-1} be a primitive $(p^2 - 1)$th root of unity in the algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$. By [14, p.158 Propositon 7.12] it is easy to see that $[\mathbb{Q}_p(\zeta_{p^2-1}) : \mathbb{Q}_p] = 2$ and that the integral closure of $\mathbb{Z}_p$ in $\mathbb{Q}_p(\zeta_{p^2-1})$ is $\mathbb{Z}_p[\zeta_{p^2-1}]$. Noting that $p\mathbb{Z}_p$ is unramified in $\mathbb{Q}_p(\zeta_{p^2-1})$, we therefore obtain $\mathbb{Z}_p[\zeta_{p^2-1}]/p\mathbb{Z}_p[\zeta_{p^2-1}] \cong \mathbb{F}_{p^2}$. Let $\Delta \equiv 3 \pmod 4$ be an arbitrary quadratic non-residue modulo p in $\mathbb{Z}$. Then clearly p is inert in the field $\mathbb{Q}(\sqrt{\Delta})$. Hence $\mathbb{Z}[\sqrt{\Delta}]/p\mathbb{Z}[\sqrt{\Delta}] \cong \mathbb{F}_{p^2}$. Since $\mathbb{Q}_p(\zeta_{p^2-1})$ and $\mathbb{Q}_p(\sqrt{\Delta})$ are both quadratic unramified extensions of $\mathbb{Q}_p$, by the local existence theorem (cf. [14, p.321 Theorem 1.4]) we have

$$\mathbb{Q}_p(\zeta_{p^2-1}) = \mathbb{Q}_p(\sqrt{\Delta}).$$

By the structure of the unit group of a local field (cf. [14, p.136, Proposition 5.3]) we have

$$\mathbb{Z}_p[\zeta_{p^2-1}]^\times = \langle \zeta_{p^2-1} \rangle \times (1 + p\mathbb{Z}_p[\zeta_{p^2-1}]),$$

where $\mathbb{Z}_p[\zeta_{p^2-1}]^\times$ denotes the group of all invertible elements in $\mathbb{Z}_p[\zeta_{p^2-1}]$ and $\langle \zeta_{p^2-1} \rangle = \{\zeta_{p^2-1}^k : k \in \mathbb{Z}\}$. Hence we can let $g \in \mathbb{Z}_p[\zeta_{p^2-1}]$ be a primitive root modulo $p\mathbb{Z}_p[\zeta_{p^2-1}]$ with $g \equiv \zeta_{p^2-1} \pmod{p\mathbb{Z}_p[\zeta_{p^2-1}]}$. For all $x \in \mathbb{Z}[\sqrt{\Delta}]$ and $y \in \mathbb{Z}_p[\zeta_{p^2-1}]$ we use the symbols $\bar{x}$ and $\bar{y}$ to denote the elements x mod $p\mathbb{Z}[\sqrt{\Delta}]$ and y mod $p\mathbb{Z}_p[\zeta_{p^2-1}]$ respectively.

Set $a_k = k + \sqrt{\Delta}$ for $0 \le k \le p - 1$. Then it is easy to verify that

$$\{a_k^2 j^2 : 0 \le k \le p-1, 1 \le j \le n\} \cup \{j^2 : 1 \le j \le n\}$$

is a complete system of representatives of

$$\left(\mathbb{Z}[\sqrt{\Delta}]/p\mathbb{Z}[\sqrt{\Delta}]\right)^{\times 2} := \left\{\alpha^2 + p\mathbb{Z}[\sqrt{\Delta}] \ : \ \alpha \in Z[\sqrt{\Delta}] \setminus p\mathbb{Z}[\sqrt{\Delta}]\right\}.$$

By the isomorphism

$$\mathbb{Z}[\sqrt{\Delta}]/p\mathbb{Z}[\sqrt{\Delta}] \cong \mathbb{Z}_p[\zeta_{p^2-1}]/p\mathbb{Z}_p[\zeta_{p^2-1}]$$

which sends x mod $p\mathbb{Z}[\sqrt{\Delta}]$ to x mod $p\mathbb{Z}_p[\zeta_{p^2-1}]$, we can view the sequence

$$S := \overline{a_0^2 \cdot 1^2}, \overline{a_0^2 \cdot 2^2}, \cdots, \overline{a_0^2 \cdot n^2}, \cdots, \overline{a_{p-1}^2}, \cdots, \overline{a_{p-1}^2 n^2}, \cdots, \overline{1^2}, \cdots, \overline{n^2} \tag{1.5}$$

as a permutation π_p of the sequence

$$S^* := \overline{g^2}, \overline{g^4}, \cdots, \overline{g^{p^2-1}}. \tag{1.6}$$

Clearly the above two sequences are analogues of the sequences (1.1) and (1.4). We mainly study this permutation in this paper. To state our result, let $\beta_0 \in \{0, 1\}$ be the integer satisfying

$$(-1)^{\beta_0} \equiv \frac{(\sqrt{\Delta})^{\frac{p-1}{2}}}{\zeta_{p^2-1}^{\frac{p^2-1}{4}}} \pmod{p\mathbb{Z}_p[\zeta_{p^2-1}]}. \tag{1.7}$$

We also use the symbol $\operatorname{sgn}(\pi_p)$ to denote the sign of π_p. Now we state the main result of this paper.

Theorem 1.1.
$$\operatorname{sgn}(\pi_p) = \begin{cases} (-1)^{\beta_0 + \frac{p+3}{4}} & \textit{if } p \equiv 1 \pmod 4, \\ (-1)^{\frac{h(-p)+1}{2} + \beta_0} & \textit{if } p \equiv 3 \pmod 4 \textit{ and } p > 3, \\ (-1)^{1+\beta_0} & \textit{if } p = 3, \end{cases}$$

where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$.

The detailed proof of the above theorem will be given in next section.

2. Proof of the main result

Recall that $a_k = k + \sqrt{\Delta}$ for $k = 0, 1, \cdots, p-1$. We begin with several lemmas involving a_k. For convenience, we write $p = 2n + 1$ and $p\mathbb{Z}[\sqrt{\Delta}] = \mathfrak{p}$ in this section.

Lemma 2.1. *Let $A_p = \prod_{0 \le k \le p-1} a_k$. Then*

$$A_p^{n(n-1)} \equiv \begin{cases} \Delta^{-\frac{n}{2}} \pmod{\mathfrak{p}} & \textit{if } p \equiv 1 \pmod 4, \\ (-1)^{\frac{n-1}{2}} \pmod{\mathfrak{p}} & \textit{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. Since

$$\prod_{0 \le t \le p-1} (x + t) \equiv x^p - x \pmod{p\mathbb{Z}[x]},$$

we have

$$A_p^{n(n-1)} = \prod_{0 \le t \le p-1} (\sqrt{\Delta} + t)^{n(n-1)} \equiv (-2\sqrt{\Delta})^{n(n-1)} \pmod{\mathfrak{p}}.$$

Observing that $(\sqrt{\Delta})^{p-1} \equiv -1 \pmod{\mathfrak{p}}$, one may get the desired result. □

Lemma 2.2. *Let $B_p = \prod_{0 \le k \le p-1} (1 - a_k^{p-1})$. Then*

$$B_p^n \equiv 1 \pmod{\mathfrak{p}}.$$

Proof. For each $k = 0, \cdots, p-1$ we have

$$a_k^p = (k + \sqrt{\Delta})^p \equiv k + (\sqrt{\Delta})^{p-1}\sqrt{\Delta} \equiv k - \sqrt{\Delta} \pmod{\mathfrak{p}}. \tag{2.1}$$

Hence we have the following congruences

$$\begin{aligned} B_p^n &\equiv \prod_{0 \le k \le p-1} \left(1 - \frac{k - \sqrt{\Delta}}{k + \sqrt{\Delta}}\right)^n \\ &= 2^{pn} (\sqrt{\Delta})^{2n^2+n} \prod_{1 \le k \le n} \left(\frac{1}{k + \sqrt{\Delta}}\right)^n \left(\frac{1}{p - k + \sqrt{\Delta}}\right)^n \\ &\equiv \left(\frac{-2}{p}\right) \prod_{1 \le k \le n} \left(\frac{1}{\Delta - k^2}\right)^n \pmod{\mathfrak{p}}. \end{aligned}$$

Noting that

$$\prod_{1\le k\le n}(x-k^2)\equiv x^n-1 \pmod{p\mathbb{Z}[x]}, \tag{2.2}$$

we obtain

$$\prod_{1\le k\le n}\left(\frac{1}{\Delta-k^2}\right)^n\equiv\left(\frac{-2}{p}\right) \pmod{\mathfrak{p}}.$$

Hence

$$B_p^n\equiv 1 \pmod{\mathfrak{p}}.$$

□

Lemma 2.3. *Let* $C_p=\prod_{0<s<t<p}\frac{1}{(t+\sqrt{\Delta})(s+\sqrt{\Delta})}$. *Then*

$$C_p^n\equiv\left(\frac{-2}{p}\right) \pmod{\mathfrak{p}}.$$

Proof. Clearly we have

$$\begin{aligned}C_p=&\prod_{1\le s<t\le n}\frac{1}{(t+\sqrt{\Delta})(s+\sqrt{\Delta})}\frac{1}{(p-t+\sqrt{\Delta})(p-s+\sqrt{\Delta})}\\&\times\prod_{1\le s\le n}\prod_{1\le t\le n}\frac{1}{(p-t+\sqrt{\Delta})(s+\sqrt{\Delta})}.\end{aligned}$$

Hence we obtain that C_p^n mod $\mathfrak{p}$ is equal to

$$\prod_{1\le s<t\le n}\left(\frac{\Delta-t^2}{p}\right)\left(\frac{\Delta-s^2}{p}\right)\times\prod_{1\le s,t\le n}\left(\frac{1}{(\sqrt{\Delta}-t)(\sqrt{\Delta}+s)}\right)^n \pmod{\mathfrak{p}}.$$

We first handle the product

$$\prod_{1\le s\le n}\prod_{1\le t\le n}\left(\frac{1}{(\sqrt{\Delta}-t)(\sqrt{\Delta}+s)}\right)^n \pmod{\mathfrak{p}}.$$

Noting that

$$\prod_{1\le s\le n}(x+s)\prod_{1\le t\le n}(x-t)\equiv x^{p-1}-1 \pmod{p\mathbb{Z}[x]},$$

we therefore obtain

$$\prod_{1\le t\le n}(\sqrt{\Delta}-t)\equiv\frac{-2}{\prod_{1\le s\le n}(\sqrt{\Delta}+s)} \pmod{\mathfrak{p}}.$$

Hence

$$\prod_{1\le s\le n}\prod_{1\le t\le n}\left(\frac{1}{(\sqrt{\Delta}-t)(\sqrt{\Delta}+s)}\right)^n\equiv\left(\frac{-2}{p}\right)^n \pmod{\mathfrak{p}}. \tag{2.3}$$

We now turn to the product

$$\prod_{1\le s<t\le n}\Big(\frac{\Delta-t^2}{p}\Big)\Big(\frac{\Delta-s^2}{p}\Big).$$

Let $n_p = \#\{(x^2, y^2) : 1 \le x, y \le n, x^2 + y^2 \equiv \Delta \pmod p\}$. Then one can easily verify that

$$n_p = \begin{cases} n/2 & \text{if } 4 \mid p-1, \\ (n+1)/2 & \text{if } 4 \mid p-3. \end{cases} \tag{2.4}$$

Let $n'_p = \#\{(x^2, y^2) : 1 \le x, y \le n, x^2 + \Delta y^2 \equiv \Delta \pmod p\}$. Then

$$n'_p = \begin{cases} n/2 & \text{if } p \equiv 1 \pmod 4, \\ (n-1)/2 & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{2.5}$$

By the above we get

$$\#\Big\{(s,t) : 1 \le s < t \le n, \Big(\frac{\Delta-t^2}{p}\Big)\Big(\frac{\Delta-s^2}{p}\Big) = -1\Big\} = \begin{cases} \frac{n^2}{4} & \text{if } 4 \mid p-1, \\ \\ \frac{n^2-1}{4} & \text{if } 4 \mid p-3. \end{cases}$$

Therefore we have

$$\prod_{1\le s<t\le n}\Big(\frac{\Delta-t^2}{p}\Big)\Big(\frac{\Delta-s^2}{p}\Big) = \begin{cases} (-1)^{n/2} & \text{if } p \equiv 1 \pmod 4, \\ 1 & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{2.6}$$

Now our desired result follows from (2.3) and (2.6). □

Lemma 2.4. *Let* $D_p = \prod_{0\le s<t\le p-1}(a_t^{p-1} - a_s^{p-1})$*. Then* $D_p^n \pmod{\mathfrak{p}}$ *is equal to*

$$\begin{cases} (\sqrt{\Delta})^{-n^2} \pmod{\mathfrak{p}} & \text{if } p \equiv 1 \pmod 4, \\ (\sqrt{\Delta})^{-n^2}(-1)^{\frac{h(-p)+1}{2}} \cdot (\frac{2}{p}) \pmod{\mathfrak{p}} & \text{if } p \equiv 3 \pmod 4 \text{ and } p > 3, \\ -(\sqrt{\Delta})^{-1} \pmod{\mathfrak{p}} & \text{if } p = 3. \end{cases}$$

Proof. From (2.1) one may easily verify that $D_p^n \pmod{\mathfrak{p}}$ is equal to

$$\Big(\frac{t-\sqrt{\Delta}}{t+\sqrt{\Delta}} - \frac{s-\sqrt{\Delta}}{s+\sqrt{\Delta}}\Big)^n \equiv \prod_{0\le s<t\le p-1}\Big(\frac{2\sqrt{\Delta}(t-s)}{(t+\sqrt{\Delta})(s+\sqrt{\Delta})}\Big)^n \pmod{\mathfrak{p}}.$$

We further obtain

$$D_p^n \equiv \Big(\frac{-2}{p}\Big)^{n+1}\Big(\frac{-1}{\sqrt{\Delta}}\Big)^{n^2} C_p^n \prod_{0<t<p}\Big(\frac{1}{t+\sqrt{\Delta}}\Big)^n \prod_{0<s<t<p}(t-s)^n \pmod{\mathfrak{p}}.$$

We first handle the product

$$\prod_{1\le t\le p-1}\Big(\frac{1}{t+\sqrt{\Delta}}\Big)^n.$$

By (2.2) we have

$$\prod_{1\le t\le p-1}\left(\frac{1}{t+\sqrt{\Delta}}\right)^n \equiv \prod_{1\le t\le n}\left(\frac{1}{\Delta-t^2}\right)^n \equiv \left(\frac{-2}{p}\right) \pmod{\mathfrak{p}}. \tag{2.7}$$

We turn to the product

$$\prod_{1\le s<t\le p-1}(t-s)^n.$$

It is clear that

$$\prod_{1\le s<t\le p-1}(t-s)^n \pmod{\mathfrak{p}}$$

is equal to

$$\begin{aligned}&\prod_{1\le s<t\le n}\left(\frac{t-s}{p}\right)\left(\frac{-s+t}{p}\right)\prod_{1\le s\le n}\prod_{1\le t\le n}\left(\frac{-1}{p}\right)\left(\frac{t+s}{p}\right)\\ &\equiv(-1)^n\prod_{1\le s\le n}\prod_{1\le t\le n}\left(\frac{t+s}{p}\right) \pmod{\mathfrak{p}}.\end{aligned}$$

We now divide our proof into the following two cases.

Case 1. $p\equiv 1 \pmod 4$.

Let $1\le w\le n$ be an arbitrary quadratic non-residue modulo p. Then

$$\#\{(s,t): 1\le s,t\le n, s+t\equiv w \pmod p\}=w-1$$

and

$$\#\{(s,t): 1\le s,t\le n, s+t\equiv p-w \pmod p\}=w.$$

Hence when $p\equiv 1 \pmod 4$ we have

$$\prod_{1\le s\le n}\prod_{1\le t\le n}\left(\frac{t+s}{p}\right)=(-1)^{\#\{1\le w\le n:(\frac{w}{p})=-1\}}=(-1)^{n/2}. \tag{2.8}$$

Case 2. $p\equiv 3 \pmod 4$.

Let $1\le w\le n$ be an arbitrary quadratic non-residue modulo p and let $1\le v\le n$ be an arbitrary quadratic residue modulo p. Then

$$\#\{(s,t): 1\le s,t\le n, s+t\equiv w \pmod p\}=w-1$$

and

$$\#\{s,t): 1\le s,t\le n, s+t\equiv p-v \pmod p\}=v.$$

Hence

$$\prod_{1\le s\le n}\prod_{1\le t\le n}\left(\frac{t+s}{p}\right)=(-1)^{\#\{1\le w\le n:(\frac{w}{p})=-1\}}\cdot(-1)^{\frac{p^2-1}{8}}.$$

For each $p\equiv 3 \pmod 4$, let $h(-p)$ be the class number of $\mathbb{Q}(\sqrt{-p})$. When $p>3$, by the class number formula (cf. [15, Chapter 5]) we have

$$\left(2-\left(\frac{2}{p}\right)\right)h(-p)=n-2\#\left\{1\le w\le n:\left(\frac{w}{p}\right)=-1\right\}.$$

By this one may easily verify that

$$\#\left\{1 \le w \le n : \left(\frac{w}{p}\right) = -1\right\} \equiv \frac{h(-p)+1}{2} \pmod 2.$$

The readers may also see Mordell's paper [16] for details.

By the above, we obtain

$$\prod_{1\le s\le n}\prod_{1\le t\le n}\left(\frac{t+s}{p}\right) = \begin{cases} (-1)^{\frac{h(-p)+1}{2}} \cdot (\frac{2}{p}) & \text{if } p \equiv 3 \pmod 4 \text{ and } p > 3, \\ -1 & \text{if } p = 3. \end{cases} \tag{2.9}$$

In view of the above, we obtain the desired result. □

Let $\Phi_{p^2-1}(x) \in \mathbb{Z}[x]$ denote the (p^2-1)th cyclotomic polynomial. We also let

$$F(x) = \prod_{1\le s<t\le (p^2-1)/2} (x^{2t} - x^{2s}),$$

and let

$$T(x) = (-1)^{\frac{p^2+7}{8}}\left(\frac{p^2-1}{2}\right)^{\frac{p^2-1}{4}} \cdot x^{\frac{(p^2-1)}{4}} \in \mathbb{Z}[x].$$

Let $\zeta = e^{2\pi \mathbf{i}/(p^2-1)}$. The following result gives the explict value of $F(\zeta)$. As this result is the key element in the proof of our main result, we state this result as an individual theorem.

Theorem 2.5. *Let $\zeta = e^{2\pi \mathbf{i}/(p^2-1)}$ be a primitive (p^2-1)th root of unity. Then*

$$F(\zeta) = \mathbf{i}(-1)^{\frac{p^2+7}{8}}\left(\frac{p^2-1}{2}\right)^{\frac{p^2-1}{4}}.$$

Hence $\Phi_{p^2-1}(x) \mid F(x) - T(x)$ in $\mathbb{Z}[x]$.

Proof. It is sufficient to prove that $F(\zeta) = T(\zeta)$. We first compute $F(\zeta)^2$. We have the following equalities:

$$\begin{aligned} F(\zeta)^2 &= \prod_{1\le s<t\le \frac{p^2-1}{2}} (\zeta^{2t} - \zeta^{2s})^2 \\ &=(-1)^{\frac{(p^2-1)(p^2-3)}{8}} \cdot \prod_{1\le s\ne t\le \frac{p^2-1}{2}} (\zeta^{2t} - \zeta^{2s}) \\ &= \prod_{1\le t\le \frac{p^2-1}{2}} \left.\frac{x^{\frac{p^2-1}{2}} - 1}{x - \zeta^{2t}}\right|_{x=\zeta^{2t}} \\ &=\left(\frac{p^2-1}{2}\right)^{\frac{p^2-1}{2}} \prod_{1\le t\le \frac{p^2-1}{2}} \zeta^{-2t} = -1 \cdot \left(\frac{p^2-1}{2}\right)^{\frac{p^2-1}{2}}. \end{aligned}$$

Hence $F(\zeta) = \pm\mathbf{i} \cdot (\frac{p^2-1}{2})^{\frac{p^2-1}{2}}$. We now compute the argument of $F(\zeta)$. Note that for any $1 \le s < t \le (p^2-1)/2$ we have

$$\zeta^{2t} - \zeta^{2s} = \zeta^{t+s}(\zeta^{t-s} - \zeta^{-(t-s)}).$$

We therefore obtain

$$\mathrm{Arg}(\zeta^{2t} - \zeta^{2s}) = \frac{2\pi}{p^2-1}(t+s) + \frac{\pi}{2}.$$

By this we have

$$\begin{aligned}\mathrm{Arg}(F(\zeta)) = & \sum_{1\le s<t\le \frac{p^2-1}{2}} \left(\frac{2\pi}{p^2-1}(t+s) + \frac{\pi}{2}\right)\\ =& \frac{(p^2-1)(p^2-3)\pi}{16} + \frac{2\pi}{p^2-1} \cdot \sum_{1\le s<t\le \frac{p^2-1}{2}} (t+s)\\ \equiv & -\frac{\pi}{2} + \frac{p^2-1}{8}\pi \pmod{2\pi\mathbb{Z}}.\end{aligned}$$

Therefore

$$F(\zeta) = \mathbf{i}(-1)^{\frac{p^2+7}{8}}\left(\frac{p^2-1}{2}\right)^{\frac{p^2-1}{4}} = T(\zeta).$$

This completes the proof. □

Before the proof of our main result, we first observe the following fact. Let $S = \{\alpha_1, \cdots, \alpha_n\}$ be an arbitrary subset of a finite field and let τ be a permutation on S. Then it follows from definition that

$$\mathrm{sgn}(\tau) = \prod_{1\le s<t\le n} \frac{\tau(\alpha_t) - \tau(\alpha_s)}{\alpha_t - \alpha_s}.$$

Hence

$$\mathrm{sgn}(\pi_p) = \prod_{1\le s<t\le n} \frac{\overline{g^{2t}} - \overline{g^{2s}}}{\pi_p(\overline{g^{2t}}) - \pi_p(\overline{g^{2s}})}.$$

The next two propositions handle the numerator and the denominator respectively.

Proposition 2.6. *Set* $\mathfrak{P} = p\mathbb{Z}_p[\zeta_{p^2-1}]$. *Then*

$$\prod_{1\le s<t\le \frac{p^2-1}{2}} (g^{2t} - g^{2s}) \equiv -\left(\frac{2}{p}\right)\left(\frac{-2}{p}\right)^{\frac{p+1}{2}} g^{\frac{p^2-1}{4}} \pmod{\mathfrak{P}}. \tag{2.10}$$

Proof. Clearly $\Phi_{p^2-1}(x) \bmod p\mathbb{Z}_p[\zeta_{p^2-1}][x]$ splits completely in $(\mathbb{Z}_p[\zeta_{p^2-1}]/\mathfrak{P})[x]$. As $g \equiv \zeta_{p^2-1} \pmod{\mathfrak{P}}$, by Theorem 2.5 we see that

$$\prod_{1\le s<t\le \frac{p^2-1}{2}} (g^{2t} - g^{2s}) \pmod{\mathfrak{P}}$$

is equal to

$$-\left(\frac{2}{p}\right)\left(\frac{p^2-1}{2}\right)^{\frac{p^2-1}{4}} g^{\frac{p^2-1}{4}} \equiv -\left(\frac{2}{p}\right)\left(\frac{-2}{p}\right)^{\frac{p+1}{2}} g^{\frac{p^2-1}{4}} \pmod{\mathfrak{P}}.$$

This completes the proof. □

We now turn to the denominator.

Proposition 2.7.

$$\prod_{1\le s<t\le \frac{p^2-1}{2}} (\pi_p(g^{2t}) - \pi_p(g^{2s})) \pmod{\mathfrak{p}}$$

is equal to

$$\begin{cases} -\Delta^{-\frac{p-1}{4}}(\sqrt{\Delta})^{-\frac{(p-1)^2}{4}} \pmod{\mathfrak{p}} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{\frac{h(-p)-1}{2}}(\sqrt{\Delta})^{-\frac{(p-1)^2}{4}} \pmod{\mathfrak{p}} & \text{if } p \equiv 3 \pmod 4 \text{ and } p > 3, \\ -(\sqrt{\Delta})^{-1} \pmod{\mathfrak{p}} & \text{if } p = 3. \end{cases} \tag{2.11}$$

Proof. It is easy to verify that

$$\prod_{1\le s<t\le \frac{p^2-1}{2}} (\pi_p(g^{2t}) - \pi_p(g^{2s})) \pmod{\mathfrak{p}}$$

is equal to

$$A_p^{n(n-1)} B_p^n D_p^n \prod_{1\le s<t\le n} (t^2 - s^2)^2 \pmod{\mathfrak{p}}.$$

By [10, (1.5)] we have

$$\prod_{1\le s<t\le n} (t^2 - s^2)^2 \equiv (-1)^{n+1} \pmod p.$$

By the above we obtain that

$$\prod_{1\le s<t\le \frac{p^2-1}{2}} (\pi_p(g^{2t}) - \pi_p(g^{2s})) \pmod{\mathfrak{p}}$$

is equal to

$$\begin{cases} -\Delta^{-\frac{p-1}{4}}(\sqrt{\Delta})^{-\frac{(p-1)^2}{4}} \pmod{\mathfrak{p}} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{\frac{h(-p)-1}{2}}(\sqrt{\Delta})^{-\frac{(p-1)^2}{4}} \pmod{\mathfrak{p}} & \text{if } p \equiv 3 \pmod 4 \text{ and } p > 3, \\ -(\sqrt{\Delta})^{-1} \pmod{\mathfrak{p}} & \text{if } p = 3. \end{cases}$$

This completes the proof. □

Combining the above two propositions, we now state the proof of our main result.

Proof of Theorem 1.1. Set $\sqrt{\Delta} \equiv \zeta_{p^2-1}^{\alpha} \pmod{\mathfrak{P}}$ for some $\alpha \in \mathbb{Z}$. Since $(\sqrt{\Delta})^{p-1} \equiv -1 \pmod{\mathfrak{P}}$, we obtain

$$(p-1)\alpha \equiv \frac{p^2-1}{2} \pmod{p^2-1}.$$

Hence

$$\alpha \equiv \frac{p+1}{2} \pmod{p+1}.$$

Set $\alpha = \frac{p+1}{2} + (p+1)\beta$ for some $\beta \in \mathbb{Z}$. Then

$$(\sqrt{\Delta})^n \equiv \zeta_{p^2-1}^{\frac{p^2-1}{4}} \zeta_{p^2-1}^{\frac{p^2-1}{2}\beta} \pmod{\mathfrak{P}}.$$

By this we obtain

$$(-1)^{\beta} \equiv \frac{(\sqrt{\Delta})^n}{\zeta_{p^2-1}^{\frac{p^2-1}{4}}} \pmod{\mathfrak{P}}.$$

Hence $\beta \equiv \beta_0 \pmod 2$, where β_0 is defined as in (1.7). We divide the remaining proof into three cases.

Case 1. $p = 3$.

In this case by (2.10) and (2.11) it is easy to see that

$$\operatorname{sgn}(\pi_3) = (-1)^{1+\beta_0}.$$

Case 2. $p \equiv 1 \pmod 4$.

By (2.10) and (2.11) we have

$$\operatorname{sgn}(\pi_p) \equiv g^{\frac{p^2-1}{4} + \frac{p-1}{2}\alpha + \frac{(p-1)^2}{4}\alpha} \pmod{\mathfrak{P}}.$$

Replacing α by $\frac{p+1}{2} + (p+1)\beta$ and noting that $g^{\frac{p^2-1}{2}} \equiv -1 \pmod{\mathfrak{P}}$, we obtain that when $p \equiv 1 \pmod 4$

$$\operatorname{sgn}(\pi_p) = (-1)^{\beta_0 + \frac{p+3}{4}}.$$

Case 3. $p \equiv 3 \pmod 4$ and $p > 3$.

Similar to the Case 2, we have

$$\operatorname{sgn}(\pi_p) \equiv \left(\frac{2}{p}\right) g^{\frac{p^2-1}{4}} (-1)^{\frac{h(-p)+1}{2}} g^{\frac{(p-1)^2}{4}\alpha} \pmod{\mathfrak{P}}.$$

Then via a computation we obtain

$$\operatorname{sgn}(\pi_p) = (-1)^{\frac{h(-p)+1}{2} + \beta_0}.$$

In view of the above, we complete the proof. □

Acknowledgments

The first author was supported by the National Natural Science Foundation of China (Grant No. 12101321, Grant No. 11971222) and the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province (Grant No. 21KJB110002). The second author was supported by the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province (Grant No. 21KJB110001).

Conflict of interest

The authors declare there is no conflicts of interest.

References

1. X.-D. Hou, Permutation polynomials over finite fields-A survey of recent advances, *Finite Field Appl.*, **32** (2015), 82–119. https://doi.org/10.1016/j.ffa.2014.10.001
2. G. Zolotarev, Nouvelle démonstration de la loi de réciprocité de Legendre, *Nouvelles Ann. Math.*, **11** (1872), 354–362.
3. M. Riesz, Sur le lemme de Zolotareff et sur la loi de réciprocité des restes quadratiques, *Math. Scand.*, **1** (1953), 159–169. https://doi.org/10.7146/math.scand.a-10376
4. M. Szyjewski, Zolotarev's proof of Gauss reciprocity and Jacobi symbols, *Serdica Math. J.*, **37** (2011), 251–260.
5. G. Frobenius, *Über das quadratische Reziprozitdätsgesetz I,* Königliche Akademie der Wissenschaften, 1914, 335–349.
6. A. Brunyate, P. L. Clark, Extending the Zolotarev-Frobenius approach to quadratic reciprocity, *Ramanujan J.*, **37** (2015), 25–50. https://doi.org/10.1007/s11139-014-9635-y
7. R. E. Dressler, E. E. Shult, A simple proof of the Zolotarev-Frobenius theorem, *Proc. Amer. Math. Soc.*, **54** (1976), 53–54. https://doi.org/10.1090/S0002-9939-1976-0389732-8
8. L.-Y. Wang, H.-L. Wu, Applications of Lerch's theorem to permutations of quadratic residues, *Bull. Aust. Math. Soc.*, **100** (2019), 362–371. https://doi.org/10.1017/S000497271900073X
9. W. Duke, K. Hopkins, Quadratic reciprocity in a finite group, *Amer. Math. Monthly*, **112** (2005), 251–256. https://doi.org/10.1080/00029890.2005.11920190
10. Z.-W. Sun, Quadratic residues and related permutations and identities, *Finite Fields Appl.*, **59** (2019), 246–283. https://doi.org/10.1016/j.ffa.2019.06.004
11. Z.-W. Sun, On quadratic residues and quartic residues modulo primes, *Int. J. Number Theory*, **16** (2020), no. 8, 1833–1858. https://doi.org/10.1142/S1793042120500955
12. F. Petrov, Z.-W. Sun, Proof of some conjecture involving quadratic residues, *Electron. Res. Arch.*, **28** (2020), 589–597. https://doi.org/10.3934/era.2020031
13. H.-L. Wu, Quadratic residues and related permuations, *Finite Fields Appl.*, **60** (2019), Article 101576. https://doi.org/10.1016/j.ffa.2019.101576
14. J. Neukirch, Algebraic Number Theory, Springer-Verlag Berlin Heidelberg, 1999. https://doi.org/10.1007/978-3-662-03983-0
15. Z. I. Borevich, I. R. Shafarevich, Number Theory, Academic Press, 1966.
16. L. J. Mordell, The congruence $((p-1)/2)! \equiv \pm 1 \pmod{p}$, *Amer. Math. Monthly*, **68** (1961), 145–146. https://doi.org/10.2307/2312481

AIMS Press