SQUARES IN $\mathbb{F}_{p^2}$ AND PERMUTATIONS INVOLVING PRIMITIVE ROOTS

HAI-LIANG WU

Abstract. Let $p = 2n + 1$ be an odd prime, and let $\zeta_{p^2 - 1}$ be a primitive $(p^2 - 1)$-th root of unity in the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. We let $g \in \mathbb{Z}_p[\zeta_{p^2 - 1}]$ be a primitive root modulo $p\mathbb{Z}_p[\zeta_{p^2 - 1}]$. Let $\Delta \equiv 3 \pmod{4}$ be an arbitrary quadratic non-residue modulo $p$ in $\mathbb{Z}$. By the Local Existence Theorem of class field theory we have $\mathbb{Q}_p(\sqrt{\Delta}) = \mathbb{Q}_p(\zeta_{p^2 - 1})$. For all $x \in \mathbb{Z}[\sqrt{\Delta}]$ and $y \in \mathbb{Z}_p[\zeta_{p^2 - 1}]$ we use $\overline{x}$ and $\overline{y}$ to denote the elements $x \mod p\mathbb{Z}[\sqrt{\Delta}]$ and $y \mod p\mathbb{Z}_p[\zeta_{p^2 - 1}]$ respectively. If we set $a_k = k + \sqrt{\Delta}$ for $0 \leq k \leq p - 1$, then we can view the sequence

$S := a_0^2, \ldots, a_0^2n^2, \ldots, a_p^2n^2, \ldots, a_{p-1}^2n^2, \ldots, 1^2, \ldots, n^2$

as a permutation $\sigma_p(g)$ of the sequence

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

We determine the sign of $\sigma_p(g)$ completely in this paper.

1. Introduction

Investigating permutation problems in finite fields is a classical topic in number theory. First of all, many permutations on finite fields are induced by permutation polynomials over finite fields. For instance, 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 $\mathbb{F}_p$. The famous Zolotarev lemma [7] says that the sign of the permutation on $\mathbb{F}_p$ induced by $f_a(x)$ coincides with the Legendre symbol $(a/p)$. Also, When $k \in \mathbb{Z}^+$ and $\gcd(k, p - 1) = 1$, the polynomial $g_k(x) = x^k$ is a permutation polynomial over $\mathbb{F}_p$. L.-Y Wang and the author [5] determined the sign of this permutation induced by $g_k(x)$ by extending the method of G. Zolotarev. In addition, W. Duke and K. Hopkins [1] generalized this topic. They gave the law of quadratic reciprocity on finite groups by studying the signs of some permutations induced by permutation polynomials over finite groups.

2010 Mathematics Subject Classification. Primary 11A15; Secondary 05A05, 11R18.

Keywords. quadratic residues, permutations, primitive roots, local fields.

Supported by the National Natural Science Foundation of China (Grant No. 11971222).
In contrast with the above, Sun [4] investigated some permutations on \( \mathbb{F}_p \) involving squares in \( \mathbb{F}_p \). For example, let \( p = 2n + 1 \) be an odd prime and let \( b_1, \ldots, b_n \) be a sequence of all the \( n \) quadratic residues among \( 1, \ldots, p - 1 \) in the ascending order. Then it is easy to see that the sequence
\[
\overline{1^2}, \ldots, \overline{n^2}.
\] (1.1)
is a permutation \( \tau_p \) on
\[
\overline{b_1}, \ldots, \overline{b_n}.
\] (1.2)
Here \( \overline{a} \) denotes the element \( a \mod p\mathbb{Z} \) for each \( a \in \mathbb{Z} \). Sun first studied this permutation and he proved that
\[
\text{sgn}(\tau_p) = \begin{cases} 
1 & \text{if } p \equiv 3 \pmod{8}, \\
(-1)^{(h(-p)+1)/2} & \text{if } p \equiv 7 \pmod{8},
\end{cases}
\]
where \( h(-p) \) is the class number of \( \mathbb{Q}(\sqrt{-p}) \) and \( \text{sgn}(\tau_p) \) is the sign of \( \tau_p \). Sun also gave the explicit formula of the product
\[
\prod_{1 \leq j < k \leq \frac{p-1}{2}} (e^{2\pi ik^2/p} - e^{2\pi ij^2/p}).
\]
This product has deep connections with the class number of the quadratic field \( \mathbb{Q}(\sqrt{-p}) \). Readers may see [4] for details. Later the author [6] gave the sign of \( \tau_p \) in the case \( p \equiv 1 \pmod{4} \). Motivated by Sun’s work, the author 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
\[
\overline{g_p^2}, \overline{g_p^4}, \ldots, \overline{g_p^{p-1}}.
\] (1.3)
is a permutation on the sequence (1.2). In [6] the author gave the sign of this permutation in the case \( p \equiv 1 \pmod{4} \).

In view of the above, we actually investigated the permutations involving squares in \( \mathbb{F}_p \). Inspired by this, in this paper we mainly focus on the permutations concerning squares in \( \mathbb{F}_{p^2} \). We first introduce some notations and basic facts.

Let \( p = 2n + 1 \) be an odd prime, and let \( \zeta_{p^2-1} \) be a primitive \( (p^2 - 1) \)-th root of unity in the algebraic closure \( \overline{\mathbb{Q}_p} \) of \( \mathbb{Q}_p \). By [3, p.158 Proposition 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 unramified extensions of $\mathbb{Q}_p$ of degree 2, by the Local Existence Theorem (cf. [3, p.321 Theorem 1.4]) we see that

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

By the structure of the unit group of local field (cf. [3, p.136 Proposition 5.3]) we have

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

Here $(\zeta_{p^2-1}) = \{\zeta_{p^2-1}^k : k \in \mathbb{Z}\}$. 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. If we set $a_k = k + \sqrt{\Delta}$ for $0 \leq k \leq p-1$, then it is easy to verify that

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

is a complete system of representatives of $(\mathbb{Z}[\sqrt{\Delta}]/p\mathbb{Z}[\sqrt{\Delta}])^\times$. We can view the sequence

$$S := \overline{a_0^2}, \ldots, \overline{a_0^2n^2}, \ldots, \overline{a_{p-1}^2}, \ldots, \overline{a_{p-1}^2n^2}, \ldots, \overline{1^2}, \ldots, \overline{n^2} \quad (1.4)$$

as a permutation $\sigma_p$ of the sequence

$$S^* := g^2, g^4, \ldots, g^{p^2-1}. \quad (1.5)$$

To state our results, we let $\beta_0 \in \{0, 1\}$ be the integer satisfying

$$(-1)^\beta_0 \equiv \left(\frac{\sqrt{\Delta}}{\zeta_{p^2-1}}\right)^{\frac{p-1}{2}} \pmod{p\mathbb{Z}_p[\zeta_{p^2-1}]} \quad (1.6)$$

Throughout this paper, we use the symbol $\text{sgn}(\sigma_p(g))$ to denote the sign of $\sigma_p(g)$. Now we are in the position to state the main results of this paper.

**Theorem 1.1.**

$$\text{sgn}(\sigma_p(g)) = \begin{cases} (-1)^{\beta_0 + \frac{p+3}{4}} & \text{if } p \equiv 1 \pmod{4}, \\ (-1)^{h(-p) + \beta_0 + 1} & \text{if } p \equiv 3 \pmod{4} \text{ and } p > 3, \\ (-1)^1 & \text{if } p = 3, \end{cases}$$

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

The proof of the above Theorem will be given in Section 2.
2. Proof of the main result

Recall that $a_k = k + \sqrt{\Delta}$ for $k = 0, 1, \ldots, p - 1$. We need the following several lemmas involving $a_k$. For convenience, we write $p\mathbb{Z}[\sqrt{\Delta}] = \mathfrak{p}$.

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

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

*Proof.* Since

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

we have

$$A_p^{\frac{(p-1)(p-3)}{4}} = \prod_{0 \leq t \leq p - 1} (\sqrt{\Delta} + t)^{\frac{(p-1)(p-3)}{4}} \equiv (-2\sqrt{\Delta})^{\frac{(p-1)(p-3)}{4}} \pmod{\mathfrak{p}}.$$ 

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

**Lemma 2.2.** Let $B_p = \prod_{0 \leq k \leq p - 1} (1 - a_p^{-1})$. Then we have

$$B_p^{\frac{p-1}{2}} \equiv 1 \pmod{\mathfrak{p}}.$$ 

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

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

Hence we have the following congruences

$$B_p^{\frac{p-1}{2}} \equiv \prod_{0 \leq k \leq p - 1} \left(1 - \frac{k - \sqrt{\Delta}}{k + \sqrt{\Delta}}\right)^{\frac{p-1}{2}}$$

$$= 2^\frac{p-1}{2} (\sqrt{\Delta})^\frac{(p-1)^2}{2} \prod_{1 \leq k \leq \frac{p-1}{2}} \left(\frac{1}{k + \sqrt{\Delta}}\right)^{\frac{p-1}{2}} \left(\frac{1}{p - k + \sqrt{\Delta}}\right)^{\frac{p-1}{2}}$$

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

Noting that

$$\prod_{1 \leq k \leq \frac{p-1}{2}} (x - k^2) \equiv x^{\frac{p-1}{2}} - 1 \pmod{p\mathbb{Z}[x]}, \quad (2.2)$$

we obtain

$$\prod_{1 \leq k \leq \frac{p-1}{2}} \left(\frac{1}{\Delta - k^2}\right)^{\frac{p-1}{2}} \equiv \left(\frac{-2}{p}\right) \pmod{\mathfrak{p}}.$$
Hence
\[ B_p^{p-1} \equiv 1 \pmod{p}. \]
\[ \square \]

**Lemma 2.3.** Let \( C_p = \prod_{1 \leq s < t \leq p-1} \frac{1}{(t+\sqrt{\Delta})(s+\sqrt{\Delta})} \). Then
\[ C_p^{p-1} \equiv \left( \frac{-2}{p} \right) \pmod{p}. \]

**Proof.** Clearly we have
\[ C_p = \prod_{1 \leq s < t \leq \frac{p-1}{2}} \frac{1}{(t+\sqrt{\Delta})(s+\sqrt{\Delta})} \frac{1}{(p-t+\sqrt{\Delta})(p-s+\sqrt{\Delta})} \times \prod_{1 \leq s \leq \frac{p-1}{2}} \prod_{1 \leq t \leq \frac{p-1}{2}} \frac{1}{(p-t+\sqrt{\Delta})(s+\sqrt{\Delta})}. \]

Hence we obtain
\[ C_p^{p-1} \equiv \prod_{1 \leq s \leq \frac{p-1}{2}} \left( \frac{\Delta - t^2}{p} \right) \left( \frac{\Delta - s^2}{p} \right) \times \prod_{1 \leq s \leq \frac{p-1}{2}} \prod_{1 \leq t \leq \frac{p-1}{2}} \left( \frac{1}{(\sqrt{\Delta} - t)(\sqrt{\Delta} + s)} \right)^{p-1} \pmod{p}. \]

We first handle the product
\[ \prod_{1 \leq s \leq \frac{p-1}{2}} \prod_{1 \leq t \leq \frac{p-1}{2}} \left( \frac{1}{(\sqrt{\Delta} - t)(\sqrt{\Delta} + s)} \right)^{p-1} \pmod{p}. \]

Noting that
\[ \prod_{1 \leq s \leq \frac{p-1}{2}} (x + s) \prod_{1 \leq t \leq \frac{p-1}{2}} (x - t) \equiv x^{p-1} - 1 \pmod{p\mathbb{Z}[x]}, \]
we therefore get that
\[ \prod_{1 \leq t \leq \frac{p-1}{2}} (\sqrt{\Delta} - t) \equiv \frac{-2}{\prod_{1 \leq s \leq \frac{p-1}{2}} (\sqrt{\Delta} + s)} \pmod{p}. \]

Hence
\[ \prod_{1 \leq s \leq \frac{p-1}{2}} \prod_{1 \leq t \leq \frac{p-1}{2}} \left( \frac{1}{(\sqrt{\Delta} - t)(\sqrt{\Delta} + s)} \right)^{p-1} \equiv \left( \frac{-2}{p} \right)^{p-1} \pmod{p}. \] (2.3)

We now turn to the product
\[ \prod_{1 \leq s < t \leq \frac{p-1}{2}} \left( \frac{\Delta - t^2}{p} \right) \left( \frac{\Delta - s^2}{p} \right). \]
One can easily verify the following identities
\[
\#\{(x^2, y^2) : 1 \leq x, y \leq \frac{p-1}{2}, x^2 + y^2 \equiv \Delta \pmod{p}\} \tag{2.4}
\]
\[
= \begin{cases} 
\frac{p-1}{4} & \text{if } p \equiv 1 \pmod{4}, \\
\frac{p+1}{4} & \text{if } p \equiv 3 \pmod{4}.
\end{cases} \tag{2.5}
\]
and
\[
\#\{(x^2, y^2) : 1 \leq x, y \leq \frac{p-1}{2}, x^2 + \Delta y^2 \equiv \Delta \pmod{p}\} \tag{2.6}
\]
\[
= \begin{cases} 
\frac{p-1}{4} & \text{if } p \equiv 1 \pmod{4}, \\
\frac{p-3}{4} & \text{if } p \equiv 3 \pmod{4}.
\end{cases} \tag{2.7}
\]
From the above we see that
\[
\#\{(s, t) : 1 \leq s < t \leq \frac{p-1}{2} : \left(\frac{\Delta - t^2}{p}\right)\left(\frac{\Delta - s^2}{p}\right) = -1\}
\]
\[
= \begin{cases} 
\frac{(p-1)^2}{16} & \text{if } p \equiv 1 \pmod{4}, \\
\frac{p-3}{4} \cdot \frac{p+1}{4} & \text{if } p \equiv 3 \pmod{4}.
\end{cases} \tag{2.8}
\]
Therefore
\[
\prod_{1 \leq s < t \leq \frac{p-1}{2}} \left(\frac{\Delta - t^2}{p}\right)\left(\frac{\Delta - s^2}{p}\right) = \begin{cases} 
(-1)^{\frac{p-1}{4}} & \text{if } p \equiv 1 \pmod{4}, \\
1 & \text{if } p \equiv 3 \pmod{4}.
\end{cases} \tag{2.9}
\]
Then our desired result follows from (2.3) and (2.8).

**Lemma 2.4.** Let \(D_p = \prod_{0 \leq s < t < p-1} (a_t^{p-1} - a_s^{p-1})\). Then \(D_p^{\frac{p-1}{2}} \pmod{p}\) is equal to
\[
\begin{cases} 
\left(\sqrt{\Delta}\right)^{\left(\frac{-1}{4}\right)} (\pmod{p}) & \text{if } p \equiv 1 \pmod{4}, \\
\left(\sqrt{\Delta}\right)^{\left(\frac{-1}{4}\right)} (-1)^{\frac{h(p)+1}{2}} \cdot \left(\frac{2}{p}\right) (\pmod{p}) & \text{if } p \equiv 3 \pmod{4} \text{ and } p > 3, \\
-\left(\sqrt{\Delta}\right)^{-1} (\pmod{p}) & \text{if } p = 3.
\end{cases}
\]

**Proof.** From (2.1) one may easily verify that \(D_p^{\frac{p-1}{2}} \pmod{p}\) is equal to
\[
\left(\frac{t - \sqrt{\Delta}}{t + \sqrt{\Delta}} - \frac{s - \sqrt{\Delta}}{s + \sqrt{\Delta}}\right)^{\frac{p-1}{2}} = \prod_{0 \leq s < t < p-1} \left(\frac{2\sqrt{\Delta}(t-s)}{(t + \sqrt{\Delta})(s + \sqrt{\Delta})}\right)^{\frac{p-1}{2}} (\pmod{p})
\]
From this we further obtain that the above is equal to
\[
\left(\frac{-2}{p}\right)^{\frac{p-1}{2}} \left(\frac{-1}{\sqrt{\Delta}}\right)^{\left(\frac{-1}{4}\right)} \prod_{0 < t < p} \left(\frac{1}{t + \sqrt{\Delta}}\right)^{\frac{p-1}{2}} \prod_{0 < s < t < p} (t - s)^{\frac{p-1}{2}} (\pmod{p}).
\]
We first handle the product

$$\prod_{1 \leq t \leq p-1} \left( \frac{1}{t + \sqrt{\Delta}} \right)^{\frac{p-1}{2}}.$$ 

By (2.2) we have

$$\prod_{1 \leq t \leq p-1} \left( \frac{1}{t + \sqrt{\Delta}} \right)^{\frac{p-1}{2}} \equiv \prod_{1 \leq t \leq \frac{p-1}{2}} \left( \frac{1}{\Delta - t^2} \right)^{\frac{p-1}{2}} \equiv \left( \frac{-2}{p} \right) \pmod{p}. \quad (2.9)$$

We turn to the product

$$\prod_{1 \leq s < t \leq p-1} (t-s)^{\frac{p-1}{2}}.$$ 

It is clear that

$$\prod_{1 \leq s < t \leq p-1} (t-s)^{\frac{p-1}{2}} \pmod{p}$$

is equal to

$$\prod_{1 \leq s < t \leq \frac{p-1}{2}} \left( \frac{t-s}{p} \right) \prod_{1 \leq s \leq \frac{p-1}{2}, 1 \leq t \leq \frac{p-1}{2}} \left( \frac{t+s}{p} \right) \prod_{1 \leq s \leq \frac{p-1}{2}, 1 \leq t \leq \frac{p-1}{2}} \left( \frac{-1}{p} \right) \left( \frac{t+s}{p} \right) \equiv (-1)^{\frac{p-1}{2}} \prod_{1 \leq s \leq \frac{p-1}{2}, 1 \leq t \leq \frac{p-1}{2}} \left( \frac{t+s}{p} \right) \pmod{p}.$$ 

We now divide our proof into the following two cases.

**Case 1.** $p \equiv 1 \pmod{4}.$

Let $1 \leq w \leq \frac{p-1}{2}$ be an arbitrary quadratic non-residue modulo $p$. Then

$$\# \{(s, t) : 1 \leq s, t \leq \frac{p-1}{2}, s+t \equiv w \pmod{p}\} = w-1,$$

and

$$\# \{(s, t) : 1 \leq s, t \leq \frac{p-1}{2}, s+t \equiv p-w \pmod{p}\} = w.$$

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

$$\prod_{1 \leq s \leq \frac{p-1}{2}, 1 \leq t \leq \frac{p-1}{2}} \left( \frac{t+s}{p} \right) = (-1)^{\# \{1 \leq w \leq \frac{p-1}{2} : (\frac{w}{p}) = -1\}} = (-1)^{\frac{p-1}{4}} \quad (2.10)$$

**Case 2.** $p \equiv 3 \pmod{4}.$

Let $1 \leq w \leq \frac{p-1}{2}$ be an arbitrary quadratic non-residue modulo $p$, and let $1 \leq v \leq \frac{p-1}{2}$ be an arbitrary quadratic residue modulo $p$. Then

$$\# \{(s, t) : 1 \leq s, t \leq \frac{p-1}{2}, s+t \equiv w \pmod{p}\} = w-1,$$

and

$$\# \{(s, t) : 1 \leq s, t \leq \frac{p-1}{2}, s+t \equiv p-v \pmod{p}\} = v.$$
Hence
\[
\prod_{1 \leq s \leq \frac{p-1}{2}} \prod_{1 \leq t \leq \frac{p-1}{2}} \left( \frac{t+s}{p} \right) = (-1)^{\# \{ 1 \leq w \leq \frac{p-1}{2} : (w/p) = -1 \}} \cdot (-1)^{\frac{p^2-1}{8}}.
\]

For each \( p \equiv 3 \pmod{4} \) let \( h(-p) \) be the class number formula of \( \mathbb{Q}(\sqrt{-p}) \). When \( p > 3 \), by the class number formula we have
\[
(2 - \left(\frac{2}{p}\right))h(-p) = \frac{p-1}{2} - 2\# \{ 1 \leq w \leq \frac{p-1}{2} : (w/p) = -1 \}.
\]

From this one may easily verify that
\[
\# \{ 1 \leq w \leq \frac{p-1}{2} : (w/p) = -1 \} \equiv \frac{h(-p) + 1}{2} \pmod{2}.
\]

The readers may also see Mordell's paper [2] for details.

From the above, we obtain
\[
\prod_{1 \leq s \leq \frac{p-1}{2}} \prod_{1 \leq t \leq \frac{p-1}{2}} \left( \frac{t+s}{p} \right) = \begin{cases} 
(-1)^{\frac{h(-p)+1}{2}} \cdot \left(\frac{2}{p}\right) & \text{if } p \equiv 3 \pmod{4} \text{ and } p > 3, \\
-1 & \text{if } p = 3.
\end{cases}
\]

In view of the above, we obtain the desired result. \( \square \)

We let \( \Phi_{p^2-1}(x) \in \mathbb{Z}[x] \) denote the \((p^2 - 1)\)-th cyclotomic polynomial. We also let
\[
F(x) = \prod_{1 \leq s < t \leq (p^2-1)/2} (x^{2t} - x^{2s}),
\]
and let
\[
T(x) = (-1)^{\frac{p^2+1}{8}} \left( \frac{p^2-1}{2} \right)^{\frac{p^2-1}{4}} \cdot x^{(p^2-1)/4} \in \mathbb{Z}[x].
\]

We need the following lemma. We also set \( \zeta = e^{2\pi i/(p^2-1)} \).

**Lemma 2.5.** \( \Phi_{p^2-1}(x) \mid F(x) - T(x) \) 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:

$$F(\zeta)^2 = \prod_{1 \leq s < t \leq \frac{p^2-1}{2}} (\zeta^{2t} - \zeta^{2s})^2$$

$$= (-1)^{\frac{(p^2-1)(p^2-3)}{8}} \prod_{1 \leq s \neq t \leq \frac{p^2-1}{2}} (\zeta^{2t} - \zeta^{2s})$$

$$= \prod_{1 \leq t \leq \frac{p^2-1}{2}} \left( \frac{p^2-1}{2} \right)^{\frac{p^2-1}{2}} \prod_{1 \leq s \leq \frac{p^2-1}{2}} (\zeta - \zeta^{2t})$$

$$= (-1)^{\frac{(p^2-1)(p^2-3)}{8}} \prod_{1 \leq s \leq \frac{p^2-1}{2}} (\zeta - \zeta^{2t})$$

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

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

we therefore obtain

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

From this we have

$$\text{Arg}(F(\zeta)) = \sum_{1 \leq s < t \leq \frac{p^2-1}{2}} \left( \frac{2\pi}{p^2 - 1} (t + s) + \frac{\pi}{2} \right)$$

$$= \frac{(p^2-1)(p^2-3)\pi}{16} + \frac{2\pi}{p^2 - 1} \sum_{1 \leq s < t \leq \frac{p^2-1}{2}} (t + s)$$

$$= -\frac{\pi}{2} + \frac{p^2 - 1}{8} \pi \pmod{2\pi \mathbb{Z}}.$$ 

Therefore

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

This completes the proof. \qed

We are now in the position to prove Theorem 1.1.

**Proof of Theorem 1.1.** Let $S = \{\alpha_1, \cdots, \alpha_n\}$ be a finite subset of a finite field and let $\tau$ be a permutation on $S$. Then it follows from definition that
the sign of $\tau$ denoted by $\text{sgn}(\tau)$ is
\[ \prod_{1 \leq s < t \leq n} \frac{\tau(\alpha_t) - \tau(\alpha_s)}{\alpha_t - \alpha_s}. \]

From this we see that
\[ \text{sgn}(\sigma_p) = \prod_{1 \leq s < t \leq 2^{p-1}} \frac{\sigma_p(g^{2t}) - \sigma_p(g^{2s})}{g^{2t} - g^{2s}}. \]

We first handle the numerator. For convenience, we set
\[ B = p \mathbb{Z}_p[\zeta_p^{2^2 - 1}]. \]

Clearly $\Phi_p^{2^2 - 1}(x) \mod p\mathbb{Z}_p[\zeta_p^{2^2 - 1}][x]$ splits completely in $\mathbb{Z}_p[\zeta_p^{2^2 - 1}]/B[x]$. As $g \equiv \zeta_p^{2^2 - 1} \mod B$ by Lemma 2.5 we see that
\[ \prod_{1 \leq s < t \leq 2^{p-1}} (g^{2t} - g^{2s}) \mod B \]

is equal to
\[ - \left( \frac{2}{p} \right) \left( \frac{p^2 - 1}{2} \right)^{\frac{2^{p-1}}{4}} g^{\frac{2^{p-1}}{2}} \equiv - \left( \frac{2}{p} \right) \left( \frac{-2}{p} \right)^{\frac{2^{p-1}}{4}} g^{\frac{2^{p-1}}{2}} \mod B. \]  
(2.12)

We now turn to the denominator. It is easy to verify that
\[ \prod_{1 \leq s < t \leq 2^{p-1}} (\sigma_p(g^{2t}) - \sigma_p(g^{2s})) \mod p \]
is equal to
\[ A_p^{\frac{(p-3)(p-1)}{4}} B_p^{p-1} D_p^{p-1} \prod_{1 \leq s < t \leq 2^{p-1}} (t^2 - s^2)^2 \mod p. \]

By [4, (1.5)] we have
\[ \prod_{1 \leq s < t \leq 2^{p-1}} (t^2 - s^2)^2 \equiv (-1)^{\frac{2^{p-1}}{2}} \mod p. \]  
(2.13)

By the above, we obtain that
\[ \prod_{1 \leq s < t \leq 2^{p-1}} (\sigma_p(g^{2t}) - \sigma_p(g^{2s})) \mod p \]
is equal to
\[ \begin{cases} -\Delta^{-\frac{p-1}{2}}(\sqrt{\Delta})^{-\frac{(p-1)^2}{2}} \mod p & \text{if } p \equiv 1 \mod 4, \\ (-1)^{\frac{b(p-1)}{2}}(\sqrt{\Delta})^{-\frac{(p-1)^2}{4}} \mod p & \text{if } p \equiv 3 \mod 4 \text{ and } p > 3, \\ -(\sqrt{\Delta})^{-1} \mod p & \text{if } p = 3. \end{cases} \]  
(2.14)
Let $\sqrt{\Delta} \equiv \zeta_{p^2-1}^\alpha \pmod{B}$ for some $\alpha \in \mathbb{Z}$. Since $(\sqrt{\Delta})^{p^2-1} \equiv -1 \pmod{B}$, we obtain

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

Hence

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

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

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

From this we get

$$(-1)^\beta \equiv (\sqrt{\Delta})^{\frac{p^2-1}{2}} \pmod{B}.$$ 

Therefore $\beta \equiv \beta_0 \pmod{2}$, where $\beta_0$ is defined as in (1.6). We divide the remaining proof into three cases.

**Case 1.** $p \equiv 1 \pmod{4}$.

By (2.12) and (2.14) we have

$$\text{sgn}(\sigma_p) \equiv g^{\frac{p^2-1}{4} + \frac{p^2-1}{2} + \frac{(p - 1)^2}{4} \alpha} \pmod{B}.$$ 

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

$$\text{sgn}(\sigma_p) = (-1)^{\beta_0 + \frac{p^2-1}{4}}.$$ 

**Case 2.** $p \equiv 3 \pmod{4}$ and $p > 3$.

Similar to the Case 1, we have

$$\text{sgn}(\sigma_p) \equiv \left(\frac{2}{p}\right) g^{\frac{p^2-1}{4}} (-1)^{\frac{h(-p)+1}{2}} g^{\frac{(p - 1)^2}{4} \alpha} \pmod{B}.$$ 

Then via computation we obtain that

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

**Case 3.** $p = 3$.

In this case it is easy to see that

$$\text{sgn}(\sigma_3) = (-1)^{1 + \beta_0}.$$ 

In view of the above, we complete the proof. \qed

**Acknowledgments** This research was supported by the National Natural Science Foundation of China (Grant No. 11971222).
References

[1] W. Duke and K. Hopkins, Quadratic reciprocity in a finite group, Amer. Math. Monthly 112 (2005), 251–256.
[2] L. J. Mordell, The congruence \((p-1)/2)! \equiv \mp 1 \pmod{p}\), Amer. Math. Monthly 68 (1961), 145–146.
[3] J. Neukirch, Algebraic Number Theory, Springer-Verlag Berlin Heidelberg, 1999.
[4] Z.-W Sun, Quadratic residues and related permutations and identities, Finite Fields Appl. 59 (2019), 246–283.
[5] L.-Y Wang and H.-L Wu, Applications of Lerch’s theorem to permutations of quadratic residues, Bull. Aust. Math. Soc. 100 (2019), 362–371.
[6] H.-L Wu, Quadratic residues and related permutations, Finite Fields Appl. In press.
[7] G. Zolotarev, Nouvelle démonstration de la loi de réciprocité de Legendre, Nouvelles Ann. Math. 11 (1872), 354–362.