ON AN EXTENSION OF ZOLOTAREV’S LEMMA AND SOME PERMUTATIONS

LI-YUAN WANG AND HAI-LIANG WU

Abstract. Let $p$ be an odd prime, for each integer $a$ with $p \nmid a$, the famous Zolotarev’s Lemma says that the Legendre symbol $\left( \frac{a}{p} \right)$ is the sign of the permutation of $\mathbb{Z}/p\mathbb{Z}$ induced by multiplication by $a$. Then Frobenius extended Zolotarev’s result to all positive odd integers. Recently, Sun [5] studied the permutation problems involving quadratic residues.

Motivated by the above work, in this paper, we first extend the result of Frobenius to all positive integers. In addition, we discuss some permutation problems involving quadratic residues modulo an odd prime $p$. In particular, we confirm some conjectures posed by Sun. Finally, we study the permutation problems induced by primitive roots of a power of an odd prime $p$.

1. Introduction

Let $n$ be a positive integer, for any integer $a$. Throughout this paper, we use the symbol $\overline{a}$ to denote the element $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ and symbol $\text{sgn}(\pi)$ to denote the sign of the permutation $\pi$ on a finite set $\mathcal{S}$. In addition, let $\{a\}_n$ denote the least nonnegative residue of $a$ modulo $n$.

Given a positive integer $n$, for any integer $a$ with $\gcd(a, n) = 1$, it is clear that $\pi_a(k) = \overline{ak}$ with $0 \leq k \leq n - 1$ is a permutation on the set $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$. When $n = p$ for some odd prime $p$, in 1872, G. Zolotarev [7] showed that $\text{sgn}(\pi_a)$ is exactly equal to the Legendre symbol $\left( \frac{a}{p} \right)$ and with this result he proved the quadratic reciprocity law. This celebrated result now is well known as Zolotarev’s lemma. This result has many applications in modern number theory; readers may consult [1, 4] for more details. Later Frobenius extended Zolotarev’s result to all positive odd integers and showed that the sign of $\pi_a$ coincides with the Jacobi symbol $\left( \frac{a}{n} \right)$.

Recently, Sun [5] studied the permutation problems involving quadratic residues modulo an odd prime $p$. When $p \equiv 3 \pmod{4}$, he used the Galois

\bibitem{1} Zolotarev’s lemma, permutations, quadratic residues, primitive roots.

\bibitem{2} Supported by the National Natural Science Foundation of China (Grant No. 11571162).
Theory to determine the product
\[ \prod_{1 \leq j < k \leq (p-1)/2} \left( \zeta_p^j - \zeta_p^k \right), \]
where \( \zeta_p = e^{2\pi i/p} \), and he used this product to solve many permutation problems induced by quadratic residues modulo an odd prime (cf. \([5, \text{Theorem 1.3}]\)). Moreover, he posed some conjectures involving permutations of special form. Readers may consult \([5]\) for more details.

In this paper, we study the permutation problems involving three different aspects. Firstly, we extend the result of Frobenius to all positive integers. In addition, we investigate permutations related to quadratic residues modulo an odd prime. Finally, we show some results on the permutations induced by primitive roots of a power of an odd prime. Now, we state the main results of this paper.

**Theorem 1.1.** Let notations be as above, suppose that \( n = 2^rm' \) with \( 2 \nmid m' \) and \( r \geq 0 \), then we have
\[
\text{sgn}(\pi_a) = \begin{cases} 
\left( \frac{-1}{a} \right) & \text{if } r \geq 2, \\
1 & \text{if } r = 1, \\
\left( \frac{a}{m'} \right) & \text{if } r = 0.
\end{cases}
\]

**Remark 1.1.** (i) In fact, if \( r = 0 \), i.e., \( n \) is an odd positive integer, our result is indeed the result of Frobenius. For completeness, we list this result in Theorem 1.1.

(ii) \( \left( \frac{-1}{a} \right) \) is indeed the unique nontrivial Dirichlet Character modulo 4.

Using Theorem 1.1 we can easily obtain the following corollaries which will be proved in Section 2.

Let \( p \) be an odd prime and let \( A = \{1, 2, \ldots, (p-1)/2\} \), Sun \([5]\) defined a permutation \( \tau_p \) as follows: for each \( k \in A \), \( \tau_p(k) \) is the unique integer \( k^* \in A \) with \( kk^* \equiv \pm 1 \pmod{p} \). Sun \([5]\) proved that \( \text{sgn}(\tau_p) = -(\frac{2}{p}) \). Using Theorem 1.1 we can reprove Sun’s result.

**Corollary 1.1.** \([5, \text{Theorem 1.1(ii)}]\) Let notations be as above, then \( \text{sgn}(\tau_p) = -(\frac{2}{p}) \).

Now, we give another application of Theorem 1.1. Let \( p \equiv 2 \pmod{3} \) be an odd prime, it is easy to see that each element in \( \mathbb{Z}/p\mathbb{Z} \) is a cubic residue modulo \( p \). On the other hand, for any \( a, b \in \{0, 1, \ldots, p-1\} \) with \( a \neq b \), since \(-3\) is a non-quadratic residue modulo \( p \), one may easily verify that
\[ a^3 \not\equiv b^3 \pmod{p}. \]

Thus \( \sigma_3(k) = \overline{k^3} \) with \( 0 \leq k \leq p-1 \) is a permutation on the set \( \mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\} \). We obtain the following result which confirms a conjecture of Sun.

**Corollary 1.2.** Let notations be as above, then \( \text{sgn}(\sigma_3) = (-1)^{(p+1)/2} \).

Let \( G \) be a cyclic group of order \( n \), and let \( g \) be a generator of this group, then clearly \( \sigma_{-1}(g^k) = g^{-k} \) with \( 0 \leq k \leq n-1 \) is a permutation on \( G \). Determining \( \text{sgn}(\sigma_{-1}) \) is a classical exercise in algebra, with the help of Theorem 1.1, we can reprove this result.

**Corollary 1.3.** Let notations be as above, we have

\[
\text{sgn}(\sigma_{-1}) = \begin{cases} 
\left(-\frac{1}{2}\right) & \text{if } 2 \nmid n, \\
\left(-\frac{n+2}{2}\right) & \text{if } 2 \mid n.
\end{cases}
\]

We now turn to the permutation problems involving quadratic residues modulo an odd prime. Given an odd prime \( p \), let \( 1 = a_1 < a_2 < \ldots < a_{(p-1)/2} \leq p-1 \) be all quadratic residues modulo \( p \). Recently, Sun determined the product

\[
\prod_{1 \leq j < k \leq (p-1)/2} (\zeta_p^{j^2} - \zeta_p^{k^2}),
\]

where \( \zeta_p = e^{2\pi i/p} \), and he used this product to prove that the sign of the permutation \( \pi \) from \( a_1, a_2, \ldots, a_{(p-1)/2} \) to \( \{1^2\}_p, \{2^2\}_p, \ldots, \{(\frac{p-1}{2})^2\}_p \) is:

\[
\text{sgn}(\pi) = \begin{cases} 
1 & \text{if } p \equiv 3 \pmod{8}, \\
\left(-1\right)^{h(-p)+1} & \text{if } p \equiv 7 \pmod{8}.
\end{cases}
\]

Inspired by Sun’s work, we now consider the following sequences:

\[
A_0 : a_1, a_2, \ldots, a_{(p-1)/2}, \tag{1.1}
\]

\[
A_1 : \{1^2\}_p, \{2^2\}_p, \ldots, \left\{\left(\frac{p-1}{2}\right)^2\right\}_p, \tag{1.2}
\]

\[
A_2 : \{2^2\}_p, \{4^2\}_p, \ldots, \{(p-1)^2\}_p, \tag{1.3}
\]

\[
A_3 : \{1^2\}_p, \{3^2\}_p, \ldots, \{(p-2)^2\}_p, \tag{1.4}
\]

\[
A_4 : \{1\left(\frac{1}{p}\right)\}_p, \{2\left(\frac{2}{p}\right)\}_p, \ldots, \left\{\frac{p-1}{2}\left(\frac{p-1}{2}\right)\right\}_p, \tag{1.5}
\]

It is easy to see that \( A_i \) (\( i = 0, 1, 2, 3 \)) contains exactly all the quadratic residues modulo \( p \). And \( A_4 \) does only when \( p \equiv 3 \pmod{4} \). When \( A_i \) and \( A_j \) contains the same elements we denote the permutation from \( A_i \) to \( A_j \) by \( \sigma_{i,j} \). The following theorem gives the sign of \( \sigma_{2,1} \) and \( \sigma_{3,1} \) for all odd primes.
Theorem 1.2.

\[ \text{sgn}(\sigma_{2,1}) = \begin{cases} 
1 & \text{if } p \equiv 3 \pmod{4}, \\
\left(\frac{2}{p}\right) & \text{if } p \equiv 1 \pmod{4},
\end{cases} \]

and

\[ \text{sgn}(\sigma_{3,1}) = \begin{cases} 
-(\frac{2}{p}) & \text{if } p \equiv 3 \pmod{4}, \\
-1 & \text{if } p \equiv 1 \pmod{4}.
\end{cases} \]

Remark 1.2. By the above theorem, it is easy to see that \( \text{sgn}(\sigma_{2,3}) = \left(\frac{2}{p}\right) \).

When \( p \equiv 3 \pmod{4} \), we determined the sign of \( \sigma_{4,0} \) as follows:

Theorem 1.3. Given an odd prime \( p \equiv 3 \pmod{4} \), let \( h(-p) \) denote the class number of \( \mathbb{Q}(\sqrt{-p}) \), and let \( \lfloor \cdot \rfloor \) denote the floor function, then

\[ \text{sgn}(\sigma_{4,0}) = \begin{cases} 
(-1)^{\lfloor \frac{p+1}{8} \rfloor} & \text{if } p \equiv 3 \pmod{8}, \\
(-1)^{\lfloor \frac{p+1}{8} \rfloor + \frac{h(-p)+1}{2}} & \text{if } p \equiv 7 \pmod{8}.
\end{cases} \]

Remark 1.3. Here we note that combining Sun’s result and the above theorem gives

\[ \text{sgn}(\sigma_{4,1}) = (-1)^{\lfloor \frac{p+1}{8} \rfloor}. \]

In this direction, Sun ([5]) also posed several conjectures. One of which states as follows. Letting \( p \) be an odd prime and \( k \in \mathbb{Z} \) he defined \( R(k, p) \) to be the unique \( r \in \{0, 1, \ldots, (p - 1)/2\} \) with \( k \) congruent to \( r \) or \(-r\) modulo \( p \) and

\[ N_p := \# \{(i, j) : 1 \leq i < j \leq \frac{p-1}{2} \text{ and } R(i^2, p) > R(j^2, p)\}, \]

where \( \#S \) denotes the cardinality of a finite set \( S \). He conjectured that \( N_p \equiv \lfloor \frac{p+1}{8} \rfloor \pmod{2} \) for every odd prime \( p \). Although we cannot prove this conjecture completely, we are able to obtain the following result.

Theorem 1.4. Let notations be as above, for any prime \( p \equiv 3 \pmod{4} \), \( N_p \equiv \lfloor \frac{p+1}{8} \rfloor \pmod{2} \).

In 2018, S. Kohl posed a permutation problem involving primitive roots of an odd prime on Mathoverflow and F. Petrov solved his problem. In this paper, we generalize this problem to the primitive roots of a power of an odd prime. Given an odd prime \( p \) and a positive integer \( r \), let \( R_{p^r} \) denote the set of all primitive roots of \( p^r \). Let \( 1 = b_1 < b_2 < \ldots < b_n < p^r \) be the least nonnegative reduced residue system modulo \( p^r \) in ascending order, where
n = φ(p^r) = p^{r-1}(p - 1). Then for each $g \in R_{p^r}$, we define a permutation $\sigma_g$ on $\{b_1, .., b_n\}$ by

$$\sigma_g : b_i \mapsto g^i \pmod{p^r}.$$ 

We shall prove the following result.

**Theorem 1.5.** Let notations be as above, then

(i) If $p \equiv 1 \pmod{4}$, then

$$\#\{g \in R_{p^r} : \text{sgn}(\sigma_g) = 1\} = \#\{g \in R_{p^r} : \text{sgn}(\sigma_g) = -1\} = n/2.$$ 

(ii) If $p \equiv 3 \pmod{4}$, for each $g \in R_{p^r}$, then

$$\text{sgn}(\sigma_g) = (-1)^{\frac{h(-p) - 1}{2}},$$ 

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

Now, we give an outline of this paper. We will prove Theorem 1.1 and its corollaries in Section 2. The proofs of Theorem 1.2-1.4 will be given in Section 3. Finally, we prove Theorem 1.5 in Section 4.

### 2. Proofs of Theorem 1.1 and its corollaries

Given an integer $r \geq 1$, $R_r = \{0, 1, ..., 2^r - 1\}$ is a residue system modulo $2^r$ and $R^*_r = \{1, 3, ..., 2^r - 1\}$ is a reduced residue system modulo $2^r$. For each odd integer $a$, $\pi_a(k) = ak$ with $0 \leq k \leq 2^r - 1$ is a permutation on the set $\{0, 1, ..., 2^r - 1\}$. Also, $\pi^*_a := \pi_a |_{R^*_r}$ is a permutation on $R^*_r$. Then we have the following result

**Lemma 2.1.** Let notations be as above, then

$$\text{sgn}(\pi^*_a) = \begin{cases} (-1)^{\frac{a - 1}{2}} & \text{if } r = 2, \\ 1 & \text{if } r = 1 \text{ or } r \geq 3. \end{cases}$$

**Proof.** When $r = 1, 2$, via easy computation, one may get the desired result. Now, suppose that $r \geq 3$. It is well known that $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \{\pm 1\} \times C$, where $C$ is a cyclic group of order $2^{r-2}$. Let $g$ denote a generator of $C$. Then each element of $(\mathbb{Z}/2^r\mathbb{Z})^\times$ can be uniquely written as $\pm g^k$ with $0 \leq k \leq 2^{r-2} - 1$. Then we define two permutations $\pi_g$ and $\pi_{-1}$ on $(\mathbb{Z}/2^r\mathbb{Z})^\times$, where

$$\pi_g(\pm g^k) = \pm g^{k+1} \quad \text{and} \quad \pi_{-1}(\pm g^k) = \mp g^k.$$ 

It is easy to see that both sgn$(\pi_g)$ and sgn$(\pi_{-1})$ are equal to 1. Since $\pi_a$ can be decomposed into the product of $\pi_g$ and $\pi_{-1}$, we can easily get the desired result. □
Proof of Theorem 1.1 Since \( m = 2^r m' \) with \( 2 \nmid m' \), then \( \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/2^r \mathbb{Z} \times \mathbb{Z}/m'\mathbb{Z} \), thus it is easy to verify that 
\[
\text{sgn}(\pi_a) = \text{sgn}(\pi_a |_{\mathbb{Z}/2^r \mathbb{Z}})^{m'} \cdot \text{sgn}(\pi_a |_{\mathbb{Z}/m'\mathbb{Z}})^{2^r}.
\]
If \( r = 0 \), our result is indeed the Frobenius’ extension of Zolotarev’s Lemma. If \( r \geq 1 \), then \( \text{sgn}(\pi_a) = \text{sgn}(\pi_a |_{\mathbb{Z}/2^r \mathbb{Z}}) \). Thus we only need to consider the case when \( m = 2^r \) with \( r \geq 1 \). Now, we suppose that \( m = 2^r \) with \( r \geq 1 \). Since 
\[
\mathcal{R}_r = \bigcup_{l=0}^{r-1} 2^l \{1, 3, \ldots, 2^{r-l} - 1\},
\]
it is easy to see that 
\[
\pi_a = \prod_{l=0}^{r-1} \pi_a |_{\mathcal{R}_r^*}. \]
Hence, 
\[
\text{sgn}(\pi_a) = \prod_{l=0}^{r-1} \text{sgn}(\pi_a |_{\mathcal{R}_r^*}).
\]
By lemma 2.1
\[
\text{sgn}(\pi_a |_{\mathcal{R}_r^*}) = \begin{cases} 
(\frac{-1}{a}) & \text{if } r - l = 2, \\
1 & \text{if } r - l = 1 \text{ or } r - l \geq 3.
\end{cases}
\]
This implies Theorem 1.1. □

Proof of Corollary 1.1-1.3 (i) For each integer \( k \), recall that \( \{k\}_p \) denotes the least nonnegative residue of \( k \) modulo \( p \). Then for each \( k \in A = \{1, 2, \ldots, (p - 1)/2\} \), \( \tau_p(k) = \{\varepsilon k^{-1}\}_p \), where
\[
\varepsilon_k = \begin{cases} 
1 & \text{if } 1 \leq \{k^{-1}\}_p \leq (p - 1)/2, \\
-1 & \text{otherwise}.
\end{cases}
\]
Let
\[
B = \{\{1^2\}_p, \{2^2\}_p, \ldots, \{(\frac{p-1}{2})^2\}_p\}.
\]
We define a map \( f_1 \) from \( A \) to \( B \) as follows: for each \( k \in A \), \( f_1(k) = \{k^2\}_p \). Clearly, \( f_1 \) is a bijection. On the other hand, let
\[
A' = \{\{\varepsilon_1 1^{-1}\}_p, \ldots, \{\varepsilon_{\frac{p-1}{2}} (\frac{p-1}{2})^{-1}\}_p\},
\]
\[
B' = \{\{1^{-2}\}_p, \ldots, \{\frac{p-1}{2}^{-2}\}_p\}.
\]
Then, we define a map \( f_2 \) from \( A' \) to \( B' \) as follows: for each \( \{\varepsilon_k k^{-1}\}_p \),
\[
f_2(\{\varepsilon_k k^{-1}\}_p) = \{k^{-2}\}_p.
\]
Clearly, \( f_2 \) is a bijection. Moreover, \( f_2 \circ \tau_p \circ f_1^{-1} \) is a permutation on \( B \) with
\[
f_2 \circ \tau_p \circ f_1^{-1}(\{k^2\}_p) = \{k^{-2}\}_p.
\]
It is easy to see that
\[ \text{sgn}(\tau_p) = \text{sgn}(f_2 \circ \tau_p \circ f_1^{-1}). \]

On the other hand, if we let \( g \) be a primitive root of \( p \), then
\[ f_2 \circ \tau_p \circ f_1^{-1}(g^{2l}) = g^{-2l}. \]

Hence, \( f_2 \circ \tau_p \circ f_1^{-1} \) induces a permutation \( \pi_{-1} \) on \( \mathbb{Z}/(p-1)/2\mathbb{Z} = \{1,\ldots,(p-1)/2\} \). For each \( x \in \mathbb{Z}/(p-1)/2\mathbb{Z} \), \( \pi_{-1}(x) = -x \). Then corollary 1.1 follows from Theorem 1.1.

(ii) Let \( g \) be a primitive root of \( p \), then \( \mathbb{Z}/p\mathbb{Z} = \{0\} \cup \{g^k : 0 \leq k \leq p-1\} \).

Thus \( \sigma_3 \) induces a permutation \( \pi_3 \) on the set \( \mathbb{Z}/(p-1)\mathbb{Z} = \{0,1,\ldots,p-1\} \), where \( \pi_3(k) = 3k \). Then by Theorem 1.1 one may easily get the desired result.

(iii) Let \( g \) be a generator of \( G \), then clearly \( G = \{g^k : 0 \leq k \leq n-1\} \).

Thus \( \sigma_{-1} \) is a permutation on \( \mathbb{Z}/n\mathbb{Z} = \{0,1,\ldots,n-1\} \), where \( \sigma_{-1}(k) = -k \).

Then corollary 1.3 follows from Theorem 1.1. \( \square \)

3. Proof of Theorem 1.2–1.4

We begin with the following lemma which was originally appeared in [6, pp.364–365].

**Lemma 3.1.** Let \( p \) be a prime with \( p \equiv 3 \pmod{4} \). Then
\[ \prod_{1 \leq i < j \leq (p-1)/2} (i^2 + j^2) \equiv (-1)^{(p+1)/8} \pmod{p}. \]

For convenience, we write \( m = (p-1)/2 \) throughout this section.

**Proof of Theorem 1.2** By definition, we have
\[
\text{sgn}(\sigma_{2,1}) \equiv \prod_{1 \leq i < j \leq \frac{p-1}{2}} \frac{(2j)^2 - (2i)^2}{j^2 - i^2} \pmod{p} = \prod_{1 \leq i < j \leq \frac{p-1}{2}} 4 = 4^{\frac{p-1}{2}} \cdot 4^{\frac{p-3}{2}} \equiv \left( \frac{2}{p} \right)^{\frac{p-3}{2}} \pmod{p}
\]
\[
= \begin{cases} 
1 & \text{if } p \equiv 3 \pmod{4} \\
\left( \frac{2}{p} \right) & \text{if } p \equiv 1 \pmod{4}.
\end{cases}
\]

(3.1)

Now we calculate the sign of \( \sigma_{3,1} \). By definition,
\[
\text{sgn}(\sigma_{3,1}) = \prod_{1 \leq i < j \leq m} \frac{(2j - 1)^2 - (2i - 1)^2}{j^2 - i^2} \pmod{p}
\]
\[
\equiv \prod_{1 \leq i < j \leq m} 4 \cdot \frac{j + i - 1}{j + i} \pmod{p}
\]
\[
\equiv 2^{m-1} \cdot \frac{m}{m+1} \cdot \frac{m+2}{m+2} \cdots \frac{2m-2}{2m-1} \pmod{p}
\]
\[
\equiv 2^{m-1} \cdot \frac{m-1}{(2m-1)!} \cdot m! \pmod{p}
\]
\[
\equiv 2^{m-1} \cdot \frac{2}{p-1} \cdot (m!)^2 \pmod{p}.
\]

This gives
\[
\text{sgn}(\sigma_{3,1}) = \begin{cases} 
-1 & \text{if } p \equiv 1 \pmod{4} \\
-(\frac{2}{p}) & \text{if } p \equiv 3 \pmod{4}
\end{cases}
\] (3.2)

Now we turn to the proof of of Theorem 1.3. We assume \( p \equiv 3 \pmod{4} \) throughout the rest of this section.

**Proof of Theorem 1.3** Since \( a_1, a_2, \ldots, a_m \) is the list of all the \((p-1)/2\) quadratic residues among 1, ..., \( p - 1 \) in the ascending order, we only need to count the number of ordered pairs \((i, j)\) with \( 1 \leq i < j \leq m \) and \( \{i \left( \frac{i}{p} \right)\}_p > \{j \left( \frac{i}{p} \right)\}_p \). We denote this number by \( s(p) \). Given any \( 1 \leq i < m \), it is easy to check that if \( \left( \frac{i}{p} \right) = 1 \) the number of \( j \) with \( 1 \leq i < j \leq m \) and \( \{i \left( \frac{i}{p} \right)\}_p > \{j \left( \frac{i}{p} \right)\}_p \) is zero and if \( \left( \frac{i}{p} \right) = -1 \), this number is \( \frac{p-1}{2} - i \). Thus
\[
s(p) = \sum_{1 \leq i \leq (p-1)/2} \left( \frac{p-1}{2} - i \right) \cdot \frac{1}{2} \left( 1 - \left( \frac{i}{p} \right) \right)
\]
\[
= \frac{(p-1)(p-3)}{16} - \frac{p-1}{4} \sum_{1 \leq i \leq (p-1)/2} \left( \frac{i}{p} \right) + \frac{1}{2} \sum_{1 \leq i \leq (p-1)/2} i \left( \frac{i}{p} \right) \quad (3.3)
\]

By Dirichlet’s class number formula,
\[
-ph(-p) = \sum_{1 \leq i \leq p-1} i \left( \frac{i}{p} \right) = \sum_{1 \leq i \leq (p-1)/2} \left( i \left( \frac{i}{p} \right) + (p-i) \left( \frac{p-i}{p} \right) \right)
\]
\[
= \sum_{1 \leq i \leq (p-1)/2} \left( 2i \left( \frac{i}{p} \right) - p \left( \frac{i}{p} \right) \right). \quad (3.4)
\]
This implies,
\[ \sum_{1 \leq i \leq (p-1)/2} i \left( \frac{i}{p} \right) = \frac{1}{2} \left( -ph(-p) + p \sum_{1 \leq i \leq (p-1)/2} \left( \frac{i}{p} \right) \right) \]  
(3.5)

Thus
\[ s(p) = \frac{(p-1)(p-3)}{16} - \frac{1}{4} ph(-p) + \frac{1}{4} \sum_{1 \leq i \leq (p-1)/2} \left( \frac{i}{p} \right) \]
\[ = \frac{(p-1)(p-3)}{16} - \frac{1}{4} ph(-p) + \frac{1}{4} \left( h(-p) - \left( \frac{2}{p} \right) \right) \]  
(3.6)

The last equality follows from Dirichlet’s class number formula in another form:
\[ h(-p) = \frac{1}{2 - \left( \frac{2}{p} \right)} \sum_{1 \leq i \leq (p-1)/2} \left( \frac{i}{p} \right). \]

When \( p \equiv 3 \pmod{8} \), letting \( p = 8k + 3 \) we get
\[ s(p) \equiv k \pmod{2}. \]  
(3.7)

When \( p \equiv 7 \pmod{8} \), letting \( p = 8k + 7 \) we get
\[ s(p) \equiv k + 1 + \frac{h(-p) + 1}{2} \pmod{2}. \]  
(3.8)

This gives
\[ s(p) \equiv \begin{cases} \left\lfloor \frac{p+1}{8} \right\rfloor + \frac{h(-p) + 1}{2} \pmod{2} & \text{if } p \equiv 3 \pmod{8}, \\ \left\lfloor \frac{p+1}{8} \right\rfloor \pmod{2} & \text{if } p \equiv 7 \pmod{8}, \end{cases} \]

which ends the proof. \( \square \)

**Proof of Theorem 1.4** Let \( S \) be the set \( \{1, 2, ..., \frac{p-1}{2}\} \) and \( \tau : i \mapsto R(i^2, p) \) be a map from \( S \) to itself. Since \( p \equiv 3 \pmod{4} \), it is obvious that \( \tau \) is a bijection thus also a permutation on \( S \). Clearly, \( A_1 = \{\{1^2\}_p, \{2^2\}_p, ..., \left( \frac{p-1}{2} \right)^2 \}_p \} \) contains exactly all quadratic residues modulo \( p \). We define a map \( f \) from \( S \) to \( A_1 \) as follows: for each \( k \in S, f(k) = \{k^2\}_p \). Thus
\[ \text{sgn}(\sigma_{4, 1}) = \text{sgn}(f \circ \sigma_{4, 1} \circ f^{-1}) = \prod_{1 \leq i < j \leq \frac{p-1}{2}} \frac{j^4-i^4}{j^2-i^2} \pmod{p} \]
\[ = \prod_{1 \leq i < j \leq \frac{p-1}{2}} (j^2 + i^2) \pmod{p} \]
\[ = (-1)^{\left\lfloor \frac{p+1}{8} \right\rfloor} \pmod{p}. \]  
(3.9)

The last equality follows from Lemma 3.1. \( \square \)
4. Proof of Theorem 1.5

Throughout this section, we set \( n = \phi(p^r) = p^r - 1 \).

**Proof of Theorem 1.5**

(i) When \( p \equiv 1 \pmod{4} \), we have

\[
\sigma_{g^{-1}} \circ \sigma_g^{-1}(g^i) = g^{-i}.
\]

Thus \( \sigma_{g^{-1}} \circ \sigma_g^{-1} \) induces a permutation \( \pi^{-1} \) on \( \mathbb{Z}/n\mathbb{Z} = \{1, 2, \ldots, n\} \), where \( \pi^{-1}(k) = -k \). Hence, by Theorem 1.1 and the fact that \( p \equiv 1 \pmod{4} \), we obtain that \( \text{sgn}(\pi^{-1}) = -1 \). Thus \( \text{sgn}(\sigma_{g^{-1}}) \cdot \text{sgn}(\sigma_g) = -1 \), this implies (i) of Theorem 1.5.

(ii) Suppose \( p \equiv 3 \pmod{4} \), it follows from definition

\[
\text{sgn}(\sigma_g) = \prod_{1 \leq k < j \leq n} \frac{(g^j)^{p^r} - (g^k)^{p^r}}{b_j - b_k}.
\]

Thus, we only need to determine

\[
\prod_{1 \leq k < j \leq n} \frac{(g^j)^{p^r} - (g^k)^{p^r}}{b_j - b_k} \pmod{p} \quad (4.1)
\]

We first consider the numerator. Let

\[
f(z) = \prod_{1 \leq k < j \leq n} (z^j - z^k).
\]

Set \( \zeta_n = e^{2\pi i/n} \), then

\[
f(\zeta_n)^2 = (-1)^{\frac{n(n-1)}{2}} \prod_{1 \leq k \neq j \leq n} (\zeta_n^j - \zeta_n^k) = -1 \cdot \prod_{1 \leq j \leq n} \frac{z^n - 1}{z - \zeta_n^n} \big|_{z = \zeta_n^j}
\]

\[
= -1 \cdot \prod_{1 \leq j \leq n} n \zeta_n^{j(n-1)} = n^n.
\]

On the other hand, for each pair \((k, j)\) with \(1 \leq k < j \leq n\), it is easy to see that

\[
\text{Arg}(\zeta_n^j - \zeta_n^k) = \text{Arg}(\zeta_n^{(j+k)/2}(\zeta_n^{(j-k)/2} - \zeta_n^{-(j-k)/2})) \equiv \frac{j + k}{n}\pi + \frac{\pi}{2} \pmod{2\pi},
\]

where \( \text{Arg}(z) \) denotes the argument of complex number \( z \). Thus

\[
\text{Arg}(f(\zeta_n)) \equiv \sum_{1 \leq k < j \leq n} \left( \frac{j + k}{n}\pi + \frac{\pi}{2} \right) \equiv \frac{(3n + 2)(n-1)}{4}\pi \pmod{2\pi}.
\]

Hence,

\[
f(\zeta_n) = (-1)^{\frac{(3n+2)(n-1)}{4}}n^{n/2} = p^{(r-1)/2}(1)^{(3n+2)/4}(p-1)^{n/2}.
\]

Since \( (\mathbb{Z}/p^r\mathbb{Z})^\times \) is isomorphic to the group generated by \( \zeta_n \), we have

\[
p^{-n(r-1)/2} \prod_{1 \leq k < j \leq n} (\{g^j\}^{p^r} - \{g^k\}^{p^r}) \equiv (-1)^{(3n+2)/4 + n/2} \pmod{p}. \quad (4.3)
\]
Now, we consider the denominator. Since
\[ \prod_{1 \leq k < j \leq n} \frac{(g_j^2)^{p-1} - (g_k^2)^{p-1}}{b_j - b_k} = \pm 1. \]
Thus we only need to determine
\[ p^{-n(r-1)/2} \prod_{1 \leq k < j \leq n} (b_j - b_k) \pmod{p}. \tag{4.4} \]
Note that
\[ p^{-n(r-1)/2} \prod_{1 \leq k < j \leq n} (b_j - b_k) \equiv \prod_{1 \leq i < j \leq p-1} (j-i)^{p-1} \prod_{1 \leq i \neq j \leq p-1} (j-i)^{(p-1)/2} \pmod{p}. \tag{4.5} \]
It is known that
\[ \prod_{1 \leq i < j \leq p-1} (j-i) \equiv \left( \frac{p-1}{2} \right)! \cdot (-1)^{(p-3)/4} \pmod{p}. \tag{4.6} \]
By [2], we know that
\[ \left( \frac{p-1}{2} \right)! \equiv (-1)^{h(-p)+1} (mod \ p), \tag{4.7} \]
where \( h(-p) \) denotes the class number of \( \mathbb{Q}(\sqrt{-p}) \). Observe that
\[ \prod_{1 \leq i \neq j \leq p-1} (j-i) = -1 \cdot \prod_{1 \leq i < j \leq p-1} (j-i)^2. \tag{4.8} \]
Thus combining (4.5)-(4.8), we obtain that
\[ p^{-n(r-1)/2} \prod_{1 \leq k < j \leq n} (b_j - b_k) \equiv (-1)^{h(-p)+1 + \frac{p-3}{4} + r+1} \pmod{p}. \tag{4.9} \]
Combining (4.3) and (4.9), via computations, we can easily get the desired results. \( \square \)

Acknowledgment. We would like to thank Prof. Zhi-Wei Sun, Prof. Hao Pan, and Prof. Qing-Hu Hou for their indispensable suggestions. We appreciate the interest and feedback of He-Xia Ni, Guo-Shuai Mao, and Chen Wang.

This research was supported by the National Natural Science Foundation of China (Grant No. 11571162).

References

[1] A. Brunyate and P. L. Clark, Extending the Zolotarev-Frobenius approach to quadratic reciprocity, Ramanujan J. 37 (2015), 25–50.
[2] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory (Graduate Texts in Math.; 84), 2nd ed., Springer, New York, 1990.
[3] L. J. Mordell, *The congruence* \((p - 1)/2)! \equiv \pm 1 \pmod{p}*, Amer. Math. Monthly 68 (1961), 145–146.

[4] H. Pan, *A remark on Zolotarev’s theorem*, preprint, arXiv:0601026, 2006.

[5] Z.-W Sun, *Quadratic residues and related permutations*, preprint, arXiv:180907766, 2018.

[6] G. J. Szekely (ed.), *Contests in Higher Mathematics*, Springer, New York, 1996.

[7] G. Zolotarev, *Nouvelle démonstration de la loi de réciprocité de Legendre*, Nouvelles Ann. Math. 11(1872), 354–362.

(Li-Yuan Wang) Department of Mathematics, Nanjing University, Nanjing 210093, People’s Republic of China

E-mail address: wly@smail.nju.edu.cn

(Hai-Liang Wu) Department of Mathematics, Nanjing University, Nanjing 210093, People’s Republic of China

E-mail address: whl.math@smail.nju.edu.cn