SOME PERMUTATIONS OVER $\mathbb{F}_p$ CONCERNING PRIMITIVE ROOTS

LI-YUAN WANG AND HAO PAN

ABSTRACT. Let p be an odd prime and let $\mathbb{F}_p$ denote the finite field with p elements. Suppose that g is a primitive root of $\mathbb{F}_p$. Define the permutation $\tau_g : \mathcal{H}_p \to \mathcal{H}_p$ by

$$\tau_g(b) := \begin{cases} g^b, & \text{if } g^b \in \mathcal{H}_p, \\ -g^b, & \text{if } g^b \notin \mathcal{H}_p, \end{cases}$$

for each $b \in \mathcal{H}_p$, where $\mathcal{H}_p = \{1, 2, \ldots, (p-1)/2\}$ is viewed as a subset of $\mathbb{F}_p$. In this paper, we investigate the sign of τ_g. For example, if $p \equiv 5 \pmod 8$, then

$$(-1)^{|\tau_g|} = (-1)^{\frac{1}{4}(h(-4p)+2)}$$

for every primitive root g, where $h(-4p)$ is the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-4p})$.

1. INTRODUCTION

Suppose that p is an odd prime. Let $\mathbb{F}_p$ denote the finite field with p elements and let $\mathbb{F}_p^\times = \mathbb{F}_p \setminus \{0\}$. For convenience, we may identify $\mathbb{F}_p$ with $\{0, 1, \ldots, p-1\}$. Suppose that g is a primitive root of $\mathbb{F}_p$. Define

$$\sigma_g(b) := g^b \tag{1.1}$$

for each $b \in \{1, \ldots, p-1\}$. Since $\mathbb{F}_p^\times$ is identified with $\{1, \ldots, p-1\}$, we can view σ_g as a permutation over $\mathbb{F}_p^\times$. In [2], Kohl considered the sign of the permutation σ_g and proposed an interesting problem:

- *If $p \equiv 1 \pmod 4$, then*

$$|\{g \in \mathcal{R}_p : (-1)^{|\sigma_g|} = 1\}| = |\{g \in \mathcal{R}_p : (-1)^{|\sigma_g|} = -1\}|, \tag{1.2}$$

where $(-1)^{|\sigma_g|}$ denotes the sign of σ_g and

$$\mathcal{R}_p := \{g \in \mathbb{F}_p : g \textit{ is a primitive root}\}.$$

2010 *Mathematics Subject Classification.* Primary 11T22; Secondary 05A05, 11R29, 12E20 .

Key words and phrases. permutation; primitive root of a prime;

The first author is supported by the National Natural Science Foundation of China (Grant No. 11571162). The second author is supported by the National Natural Science Foundation of China (Grant No. 11671197).

- *If* $p \equiv 3 \pmod 4$, *then*

$$(-1)^{|\sigma_g|} \equiv -\left(\frac{p-1}{2}\right)! \pmod p \tag{1.3}$$

for each $g \in \mathcal{R}_p$.

Soon, (1.2) and (1.3) were confirmed by Ladisch and Petrov [2] respectively. In particular, the key ingredient of Petrov's proof is the formula

$$\prod_{1\le i<j\le p-1} (\zeta^j - \zeta^i) = e^{\frac{(p-2)(3p-1)}{4}\cdot \pi \mathbf{i}} \cdot (p-1)^{\frac{p-1}{2}}, \tag{1.4}$$

where $\mathbf{i} = \sqrt{-1}$ and $\zeta = e^{\frac{2\pi \mathbf{i}}{p-1}}$ is the $(p-1)$-th primitive root of unity. A classical result of Mordell [4] says that for any prime $p \equiv 3 \pmod 4$

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{1}{2}(h(-p)+1)} \pmod p,$$

where $h(d)$ denotes the class number of the quadratic field $\mathbb{Q}(\sqrt{d})$. Hence (1.3) also can be rewritten as

$$(-1)^{|\sigma_g|} \equiv (-1)^{\frac{1}{2}(h(-p)-1)} \pmod p. \tag{1.5}$$

In this note, we shall consider a variant of Kohl's problem. Let

$$\mathcal{H}_p := \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$$

and view $\mathcal{H}_p$ as a subset of $\mathbb{F}_p$. We shall define the permutation τ_g over $\mathcal{H}_p$ for every primitive root $g \in \mathcal{R}_p$. Define

$$\tau_g(b) := \begin{cases} g^b, & \text{if } g^b \in \mathcal{H}_p, \\ -g^b, & \text{if } g^b \notin \mathcal{H}_p, \end{cases} \tag{1.6}$$

for each $b \in \mathcal{H}_p$. Note that $-g^b = g^{\frac{1}{2}(p-1)+b}$. It is easy to see that τ_g is a permutation over $\mathcal{H}_p$. In fact, our definition of τ_g is motivated by the well-known Gauss lemma, which says that for each $a \in \mathbb{F}_p^\times$, the Legendre symbol

$$\left(\frac{a}{p}\right) = (-1)^{N_{a,p}},$$

where

$$N_{a,p} := |\{b \in \mathcal{H}_p : \, ab \notin \mathcal{H}_p\}|.$$

It is natural to ask what the sign of τ_g is. When $p = 3$, it is obvious that $\mathcal{R}_p = \{2\}$ and τ_2 is even. When $p > 3$, we have

Theorem 1.1. *(i) If $p \equiv 1 \pmod 8$, then for each $g \in \mathcal{R}_p$,*

$$(-1)^{|\tau_g|} = (-1)^{\frac{1}{4}h(-4p)} \cdot (-1)^{|\sigma_g|}. \tag{1.7}$$

(ii) If $p \equiv 5 \pmod 8$, then for each $g \in \mathcal{R}_p$,

$$(-1)^{|\tau_g|} = (-1)^{\frac{1}{4}(h(-4p)+2)}. \tag{1.8}$$

(iii) If $p = 18(2n+1)^2 + 1$ for some positive integer n, then

$$(-1)^{|\tau_g|} = (-1)^{n+1}. \tag{1.9}$$

(iv) If $p \equiv 3 \pmod 4$, $p > 3$ and not of the form $18(2n+1)^2 + 1$, then

$$|\{g \in \mathcal{R}_p : (-1)^{|\tau_g|} = 1\}| = |\{g \in \mathcal{R}_p : (-1)^{|\tau_g|} = -1\}|. \tag{1.10}$$

The proof of Theorem 1.1 will be given in the subsequent two sections. In fact, we shall use a modification of Petrov's discussions to prove (i)-(iii) of Theorem 1.1. And for the final case (iv), we shall find $1 \le a \le p-1$ with $(a, p-1) = 1$ such that τ_g and τ_{g^a} have the opposite parity for each $g \in \mathcal{R}_p$.

2. The case $p \equiv 1 \pmod 4$

In this section, we shall prove (i) and (ii) of Theorem1.1. First, suppose that p is an odd prime. Let

$$\mathcal{Q}_p = \{x^2 : x \in \mathbb{F}_p^*\},$$

i.e., $\mathcal{Q}_p$ is the set of all non-zero quadratic residues in $\mathbb{F}_p$. Define $\lambda : \mathcal{H}_p \to \mathcal{Q}_p$ by

$$\lambda(b) = b^2.$$

Since $\mathcal{H}_p = \{1, \dots, (p-1)/2\}$, clearly λ is a bijection. Let

$$\nu_g := \lambda \circ \tau_g \circ \lambda^{-1}.$$

Then ν_p is a permutation over $\mathcal{Q}_p$. Recall that the sign of a permutation is also determined by its decomposition into the product of disjoint cycles. So we must have

$$(-1)^{|\nu_g|} = (-1)^{|\tau_g|}. \tag{2.1}$$

Clearly for each $1 \le b \le (p-1)/2$, we have

$$\nu_g(b^2) = g^{2b}.$$

Hence

$$(-1)^{|\nu_g|} = \prod_{1 \le i < j \le \frac{p-1}{2}} \frac{g^{2j} - g^{2i}}{j^2 - i^2} \tag{2.2}$$

over $\mathbb{F}_p$.

Lemma 2.1. *Suppose that the prime $p \equiv 1 \pmod 4$. Then*

$$\prod_{1\le i<j\le \frac{p-1}{2}} (j^2-i^2) \equiv -\left(\frac{p-1}{2}\right)! \pmod p. \tag{2.3}$$

Proof. Evidently,

$$\begin{aligned}\prod_{1\le i<j\le \frac{p-1}{2}} (j^2-i^2) &= \prod_{1\le i\le \frac{p-3}{2}} \left(\prod_{i<j\le \frac{p-1}{2}} (j-i)\right)\cdot \prod_{1\le i\le \frac{p-3}{2}} \left(\prod_{i<j\le \frac{p-1}{2}} (j+i)\right)\\ &= \prod_{1\le i\le \frac{p-3}{2}} \left(\frac{p-1}{2}-i\right)!\cdot \prod_{1\le i\le \frac{p-3}{2}} \frac{(i+\frac{p-1}{2})!}{(2i)!}\\ &= \prod_{\substack{1\le k\le p-2\\ k\ne \frac{p-1}{2}}} k!\cdot \prod_{1\le i\le \frac{p-3}{2}} \frac{1}{(2i)!} = \frac{1}{(\frac{p-1}{2})!}\prod_{0\le k\le \frac{p-3}{2}} (2k+1)!. \end{aligned}\tag{2.4}$$

By the classical Wilson theorem, for each $1\le k\le p-2$,

$$k!(p-1-k)! \equiv (-1)^{p-1-k}k!\prod_{j=1}^{p-1-k}(p-j) = (-1)^k(p-1)! \equiv (-1)^{k+1} \pmod p. \tag{2.5}$$

Since $(p-1)/2$ is even now, we have

$$\prod_{1\le i<j\le \frac{p-1}{2}} (j^2-i^2) \equiv \frac{1}{(\frac{p-1}{2})!} \equiv -\left(\frac{p-1}{2}\right)! \pmod p.$$

□

In order to evaluate $\prod_{1\le i<j\le \frac{p-1}{2}}(g^{2j}-g^{2i})$, we may view g as an integer lying in $\{1,2,\ldots,p-1\}$. Let $\zeta = e^{\frac{2\pi \mathbf{i}}{p-1}}$ be a $(p-1)$-th primitive root of unity. Clearly

$$g^{p-1}-1 = \prod_{j=1}^{p-1}(g-\zeta^j) \equiv 0 \pmod p.$$

Hence there exists $1\le j_0\le p-1$ such that $g-\zeta^{j_0}$ is not prime to p, i.e.,

$$g-\zeta^{j_0} \equiv 0 \pmod{\mathfrak{p}}$$

for some prime ideal $\mathfrak{p}\subseteq \mathbb{Q}(\zeta)$ with $\mathfrak{p}\mid p$, where $\mathbb{Q}(\zeta)$ denotes the $(p-1)$-th cyclotomic field. For each $1\le k\le p-2$, since g^k-1 is prime to p , we must have $\zeta^{kj_0}\ne 1$. So j_0 is prime to $p-1$, i.e., ζ^{j_0} is also a $(p-1)$-th primitive root of unity. Recall that $\psi:\zeta\mapsto\zeta^{j_0}$ gives a Galois automorphism over $\mathbb{Q}(\zeta)$ (cf. [3, p. 71]). Hence without loss of generality, we may assume that $j_0=1$, i.e.,

$$g\equiv \zeta \pmod{\mathfrak{p}}. \tag{2.6}$$

Lemma 2.2. *Suppose that $p \equiv 1 \pmod 4$ is a prime. Then*

$$\prod_{1\le i<j\le \frac{p-1}{2}} (g^{2j}-g^{2i}) \equiv e^{\frac{(p-3)(3p+1)}{16}\cdot \pi \mathbf{i}} \cdot \left(\frac{p-1}{2}\right)^{\frac{p-1}{4}} \pmod{\mathfrak{p}}. \tag{2.7}$$

Proof. Let

$$\Upsilon(x) := \prod_{1\le i<j\le \frac{p-1}{2}} (x^{2j}-x^{2i}). \tag{2.8}$$

Clearly

$$\Upsilon(\zeta)^2 = \prod_{1\le i<j\le \frac{p-1}{2}} (\zeta^{2j}-\zeta^{2i})^2 = (-1)^{\frac{(p-1)(p-3)}{8}} \prod_{1\le i\ne j\le \frac{p-1}{2}} (\zeta^{2j}-\zeta^{2i}).$$

Note that

$$\prod_{i=1}^{\frac{p-3}{2}} (1-\zeta^{2i}) = \lim_{x\to 1} \prod_{i=1}^{\frac{p-3}{2}} (x-\zeta^{2i}) = \lim_{x\to 1} \frac{x^{\frac{p-1}{2}}-1}{x-1} = \frac{p-1}{2}.$$

It follows that

$$\begin{aligned}\prod_{j=1}^{\frac{p-1}{2}} \prod_{\substack{1\le i\le \frac{p-1}{2}\\ i\ne j}} (\zeta^{2j}-\zeta^{2i}) &= \prod_{j=1}^{\frac{p-1}{2}} \zeta^{(p-3)j} \prod_{\substack{1\le i\le \frac{p-1}{2}\\ i\ne j}} (1-\zeta^{2(i-j)}) \\ &= \prod_{j=1}^{\frac{p-1}{2}} \left(\zeta^{(p-3)j}\cdot \frac{p-1}{2}\right) = \zeta^{\frac{(p-3)(p^2-1)}{8}} \cdot \left(\frac{p-1}{2}\right)^{\frac{p-1}{2}}.\end{aligned}$$

Thus we get

$$\Upsilon(\zeta)^2 = (-1)^{\frac{(p-1)(p-3)}{8}+\frac{(p-3)(p+1)}{4}} \cdot \left(\frac{p-1}{2}\right)^{\frac{p-1}{2}}. \tag{2.9}$$

In particular,

$$|\Upsilon(\zeta)| = \left(\frac{p-1}{2}\right)^{\frac{p-1}{4}}.$$

Let $\alpha = \arg \Upsilon(\zeta)$ denote the argument of $\Upsilon(\zeta)$. Note that for any $\theta \in [0, 2\pi)$,

$$1-e^{\mathbf{i}\theta} = (1-\cos\theta) - \mathbf{i}\sin\theta = 2\sin\frac{\theta}{2}\left(\sin\frac{\theta}{2} - \mathbf{i}\cos\frac{\theta}{2}\right) = 2\sin\frac{\theta}{2}\cdot e^{\mathbf{i}(\frac{\theta}{2}-\frac{\pi}{2})},$$

i.e.,

$$\arg(1-e^{\mathbf{i}\theta}) \equiv \frac{\theta}{2} - \frac{\pi}{2} \pmod{2\pi},$$

where for $x, y, z \in \mathbb{R}$, $x \equiv y \pmod{z}$ means $x - y = nz$ for some integer n. Hence

$$\arg(\zeta^{2j} - \zeta^{2i}) = \arg\big(-\zeta^{2i}(1 - \zeta^{2j-2i})\big) \equiv (j+i) \cdot \frac{2\pi}{p-1} + \frac{\pi}{2} \pmod{2\pi}$$

for each $1 \le i < j \le (p-1)/2$. It follows that

$$\begin{aligned}\arg \Upsilon(\zeta) \equiv & \frac{2\pi}{p-1} \sum_{1 \le i < j \le \frac{p-1}{2}} (j+i) + \frac{\pi}{2} \sum_{1 \le i < j \le \frac{p-1}{2}} 1 \\ = & \frac{(p-3)(p^2-1)}{16} \cdot \frac{2\pi}{p-1} + \frac{(p-3)(p-1)}{8} \cdot \frac{\pi}{2} \\ = & \frac{(p-3)(3p+1)}{16} \cdot \pi \pmod{2\pi}.\end{aligned}$$

So

$$\Upsilon(\zeta) = e^{\frac{(p-3)(3p+1)}{16} \cdot \pi \mathbf{i}} \cdot \left(\frac{p-1}{2}\right)^{\frac{p-1}{4}}. \tag{2.10}$$

□

Furthermore, we also need a result of Williams and Currie (cf. [5, p. 972]).

Lemma 2.3. *Suppose that $p \equiv 1 \pmod 4$ is a prime. Then*

$$2^{\frac{p-1}{4}} \equiv (-1)^{\frac{h(-p)}{4} + \frac{p-1}{8}} \pmod p \tag{2.11}$$

if $p \equiv 1 \pmod 8$. And

$$2^{\frac{p-1}{4}} \cdot \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{1}{4}(h(-p)+2) + \frac{p-5}{8}} \pmod p \tag{2.12}$$

if $p \equiv 5 \pmod 8$.

First, assume that case $p \equiv 5 \pmod 8$. It is easy to check that

$$\frac{(p-3)(3p+1)}{16} \equiv \frac{p-5}{8} \pmod 2$$

when $p \equiv 5 \pmod 8$. So

$$\Upsilon(g) \equiv \Upsilon(\zeta) = \left(\frac{p-1}{2}\right)^{\frac{p-1}{4}} \cdot (-1)^{\frac{p-5}{8}} \pmod{\mathfrak{p}}. \tag{2.13}$$

Note that both sides of (2.13) are rational integers. So we have

$$\Upsilon(g) \equiv (-1)^{\frac{p-5}{8}} \cdot \left(\frac{p-1}{2}\right)^{\frac{p-1}{4}} \equiv \frac{(-1)^{\frac{p+3}{8}}}{2^{\frac{p-1}{4}}} \pmod p. \tag{2.14}$$

Combining (2.3), (2.7) and (2.12), we obtain that

$$(-1)^{|\nu_g|}\equiv\prod_{1\le i<j\le\frac{p-1}{2}}\frac{g^{2j}-g^{2i}}{j^2-i^2}\equiv(-1)^{\frac{1}{4}(h(-p)+2)}\pmod p$$

provided $p\equiv 5\pmod 8$. (1.8) is concluded.

Next, assume that $p\equiv 1\pmod 8$. Clearly now

$$\frac{(p-3)(3p+1)}{16}+\frac{1}{2}\equiv\frac{p-1}{8}\pmod 2.$$

According to (2.3), (2.7) and (2.11), we know that

$$(-1)^{|\tau_g|}\equiv\prod_{1\le i<j\le\frac{p-1}{2}}\frac{g^{2j}-g^{2i}}{j^2-i^2}\equiv(-1)^{\frac{1}{4}h(-p)+1}\mathbf{i}\cdot\left(\frac{p-1}{2}\right)!\pmod{\mathfrak{p}}.\tag{2.15}$$

On the other hand, by view of (2.5), we have

$$\prod_{1\le i<j\le p-1}(j-i)=\prod_{i=1}^{p-2}(p-1-i)!=\prod_{k=1}^{p-2}k!\equiv(-1)^{\frac{p^2-9}{8}}\cdot\left(\frac{p-1}{2}\right)!\pmod p.\tag{2.16}$$

So combining (2.16) with (1.4), we obtain that

$$\begin{aligned}(-1)^{|\sigma_g|}\equiv\prod_{1\le i<j\le p-1}\frac{g^j-g^i}{j-i}\equiv&\frac{(-1)^{\frac{p^2-9}{8}+\frac{p-1}{2}}\cdot e^{\frac{(p-2)(3p-1)}{4}\cdot\pi\mathbf{i}}}{(\frac{p-1}{2})!}\\ \equiv&(-1)^{\frac{p^2-1}{8}}\cdot e^{\frac{(p-2)(3p-1)}{4}\cdot\pi\mathbf{i}}\cdot\left(\frac{p-1}{2}\right)!\pmod{\mathfrak{p}}.\end{aligned}\tag{2.17}$$

Note that

$$\frac{p^2-1}{8}\equiv 0\pmod 2,\qquad\frac{(p-2)(3p-1)}{4}\equiv\frac{3}{2}\pmod 2$$

for any $p\equiv 1\pmod 8$. Thus (1.7) immediately follows from (2.15) and (2.17). □

3. The case $p\equiv 3\pmod 4$

Proof of (iii) of Theorem 1.1. Suppose that $p=18(2n+1)^2+1$ is a prime for some positive integer n. Let ζ and $\mathfrak{p}$ be the ones in (2.6). Note that (2.10) is factly valid for each odd prime p, i.e.,

$$\Upsilon(\zeta)=e^{\frac{(p-3)(3p+1)}{16}\cdot\pi\mathbf{i}}\cdot\left(\frac{p-1}{2}\right)^{\frac{p-1}{4}}.$$

Since $p=18(2n+1)^2+1\equiv 3\pmod{16}$ now, we have

$$\prod_{1\leq i<j\leq\frac{p-1}{2}}(g^{2j}-g^{2i})\equiv e^{\frac{(p-3)(3p+1)}{16}\cdot\pi\mathbf{i}}\cdot\left(\frac{p-1}{2}\right)^{\frac{p-1}{4}}=(6n+3)^{\frac{p-1}{2}}\pmod{\mathfrak{p}}. \quad (3.1)$$

Noting that both sides of (3.1) are rational integers, we factly get

$$\prod_{1\leq i<j\leq\frac{p-1}{2}}(g^{2j}-g^{2i})\equiv(6n+3)^{\frac{p-1}{2}}\pmod{p}. \quad (3.2)$$

On the other hand, in view of (2.4) and (2.5),

$$\prod_{1\leq i<j\leq\frac{p-1}{2}}(j^2-i^2)=\frac{1}{(\frac{p-1}{2})!}\prod_{k=0}^{\frac{p-3}{2}}(2k+1)!=\prod_{k=0}^{\frac{p-7}{4}}(2k+1)!(p-2-2k)!\equiv 1\pmod{p}.$$

Hence

$$(-1)^{|\tau_g|}=\prod_{1\leq i<j\leq\frac{p-1}{2}}\frac{g^{2j}-g^{2i}}{j^2-i^2}\equiv(6n+3)^{\frac{p-1}{2}}\equiv\left(\frac{6n+3}{p}\right)\pmod{p}.$$

Since $p\equiv 3\pmod 4$, by the law of quadratic reciprocity, we have

$$\left(\frac{6n+3}{p}\right)=(-1)^{3n+1}\cdot\left(\frac{p}{6n+3}\right)=(-1)^{n+1}\cdot\left(\frac{2(6n+3)^2+1}{6n+3}\right)=(-1)^{n+1}.$$

The proof of (1.9) is complete. □

Proof of (iv) of Theorem 1.1. Suppose that $p\equiv 3\pmod 4$ is a prime, $p>3$ and p is not of the form $18(2n+1)^2+1$. We mention that $(p-1)/2$ can't be a perfect square. Otherwise, assume on the contrary that $p=2m^2+1$ for some integer m. If $3\nmid m$, then

$$p=2m^2+1\equiv 2+1\equiv 0\pmod 3,$$

which is impossible since $p>3$ is prime. Suppose that $3\mid m$. Since $p\equiv 3\pmod 4$, m must be odd. So $m=3(2n+1)$ for some integer n. This also contradicts with our assumption that p isn't of the form $18(2n+1)^2+1$.

Let

$$h=\frac{p-1}{2}$$

and let $\mathbb{Z}_h=\mathbb{Z}/h\mathbb{Z}$ denote the cyclic group of order h. For convenience, we may write $\mathbb{Z}_h=\{1,2,\ldots,h\}$. On the other hand, recall that we have viewed $\mathcal{H}_p=\{1,2,\ldots,h\}$ as a subset of $\mathbb{F}_p$. Let ψ be the natural bijection from $\mathbb{Z}_h$ to $\mathcal{H}_p$.

Assume that $1\leq a\leq p-1$ is prime to $p-1$. Define

$$\eta_a(b):=ab$$

for each $b \in \mathbb{Z}_h$. Since a is also prime to h, η_a is a permutation over $\mathbb{Z}_h$. We claim that

$$\tau_{g^a} = \tau_g \circ \psi \circ \eta_a \circ \psi^{-1} \tag{3.3}$$

for each $g \in \mathcal{R}_p$. In fact, assume that $1 \le b \le h$ and $ab \equiv c \pmod h$ for some $1 \le c \le h$. Clearly

$$c = \psi \circ \eta_a \circ \psi^{-1}(b)$$

provided that both b and c are viewed as the elements of $\mathcal{H}_p$. Note that either $ab \equiv c \pmod{p-1}$ or $ab \equiv c + h \pmod{p-1}$ now. Hence, we must have

$$g^c \equiv (g^a)^b \pmod p$$

or

$$g^c \equiv (g^a)^b \cdot g^h \equiv -(g^a)^b \pmod p.$$

That is,

$$\tau_{g^a}(b) = \tau_g(c).$$

In view of (3.3), we get

$$(-1)^{\tau_{g^a}} = (-1)^{\tau_g} \cdot (-1)^{|\eta_a|}.$$

We shall find $1 \le a \le p-1$ with $(a, p-1) = 1$ such that η_a is an odd permutation. Since h is odd, according to the generalized Zolotarev lemma (cf. [1]), we know that

$$(-1)^{|\eta_a|} = \left(\frac{a}{h}\right),$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Jacobi symbol. We may write $h = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s}$, where $q_1, \ldots, q_s$ are distinct odd primes and $\alpha_1, \ldots, \alpha_s \ge 1$. Recall that h can't be a perfect square. Without loss of generality, assume that α_1 is odd. By the Chinese remainder theorem, there exists $1 \le a \le p-1$ with $(a, p-1) = 1$ such that a is a quadratic non-residue modulo q_1 and is a quadratic residue modulo q_i for each $2 \le i \le s$. Then

$$\left(\frac{a}{h}\right) = \prod_{j=1}^{s} \left(\frac{a}{q_j}\right)^{\alpha_j} = (-1)^{\alpha_1} = -1,$$

i.e., $(-1)^{|\eta_a|} = -1$.

Finally, since a is prime to $p-1$, clearly $\nu_a : g \mapsto g^a$ is a permutation over $\mathcal{R}_p$. So

$$|\{g : (-1)^{|\tau_g|} = 1\}| = |\{g : (-1)^{|\tau_{g^a}|} = -1\}| \le |\{g : (-1)^{|\tau_g|} = -1\}|,$$

and

$$|\{g : (-1)^{|\tau_g|} = -1\}| = |\{g : (-1)^{|\tau_{g^a}|} = 1\}| \le |\{g : (-1)^{|\tau_g|} = 1\}|.$$

Hence we must have $|\{g \in \mathcal{R}_p : (-1)^{|\tau_g|} = 1\}| = |\{g \in \mathcal{R}_p : (-1)^{|\tau_g|} = -1\}|$. $\square$

Acknowledgments. The authors thank Professor Zhi-Wei Sun for his very helpful comments. The first author also thanks Professors Henri Cohen and Will Jagy for informing him of the paper [5].

References

[1] A. Brunyate and P. L. Clark, *Extending the Zolotarev-Frobenius approach to quadratic reciprocity*, Ramanujan J., **37** (2015), 25-50.
[2] S. Kohl, Question 302865 in MathOverflow, solved by F. Ladisch and F. Petrov, available at https://mathoverflow.net/questions/302865/.
[3] S. Lang, *Algebraic number theory*, Graduate Texts in Math. 110, 2nd ed., Springer, New York, 1994.
[4] L. J. Mordell, *The congruence* $((p-1)/2)! \equiv \pm 1 \pmod{p}$, Amer. Math. Monthly, **68** (1961), 145-146.
[5] K. S. Williams and J. D. Currie, *Class numbers and biquadratic reciprocity*, Canad. J. Math., **34** (1982), 969-988.

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China
E-mail address: wly@smail.nju.edu.cn

School of Applied Mathematics, Nanjing University of Finance and Economics, Nanjing 210046, People's Republic of China
E-mail address: haopan79@zoho.com