ELECTRONIC RESEARCH ARCHIVE
Volume **28**, Number **2**, June **2020**

doi:10.3934/era.2020031
pp. **589–597**

# PROOF OF SOME CONJECTURES INVOLVING QUADRATIC RESIDUES

Fedor Petrov

St. Petersburg Department of Steklov
Mathematical Institute of Russian Academy of Sciences
Fontanka 27, 191023, St. Petersburg, Russia

Zhi-Wei Sun*

Department of Mathematics, Nanjing University
Nanjing 210093, China

(Communicated by Min Ru)

Abstract. We confirm several conjectures of Sun involving quadratic residues modulo odd primes. For any prime $p\equiv 1 \pmod 4$ and integer $a\not\equiv 0 \pmod p$, we prove that

$$(-1)^{|\{1\le k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}\prod_{1\le j<k\le (p-1)/2}(e^{2\pi iaj^2/p}+e^{2\pi iak^2/p})$$
$$=\begin{cases}1 & \text{if } p\equiv 1 \pmod 8,\\ \left(\frac{a}{p}\right)\varepsilon_p^{-(\frac{a}{p})h(p)} & \text{if } p\equiv 5 \pmod 8,\end{cases}$$

and that

$$\left|\left\{(j,k):\ 1\le j<k\le\frac{p-1}{2}\ \&\ \{aj^2\}_p>\{ak^2\}_p\right\}\right|$$
$$+\left|\left\{(j,k):\ 1\le j<k\le\frac{p-1}{2}\ \&\ \{ak^2-aj^2\}_p>\frac{p}{2}\right\}\right|$$
$$\equiv\left|\left\{1\le k<\frac{p}{4}:\ \left(\frac{k}{p}\right)=\left(\frac{a}{p}\right)\right\}\right| \pmod 2,$$

where $(\frac{a}{p})$ is the Legendre symbol, $\varepsilon_p$ and $h(p)$ are the fundamental unit and the class number of the real quadratic field $\mathbb{Q}(\sqrt{p})$ respectively, and $\{x\}_p$ is the least nonnegative residue of an integer $x$ modulo $p$. Also, for any prime $p\equiv 3 \pmod 4$ and $\delta=1,2$, we determine

$$(-1)^{|\{(j,k):\ 1\le j<k\le (p-1)/2 \text{ and } \{\delta T_j\}_p>\{\delta T_k\}_p\}|},$$

where $T_m$ denotes the triangular number $m(m+1)/2$.

---

2010 *Mathematics Subject Classification.* Primary: 11A15, 05A05; Secondary: 11R11, 33B10.

*Key words and phrases.* Quadratic residues modulo primes, quadratic fields, roots of unity, permutations, triangular numbers.

The work is supported by the NSFC-RFBR Cooperation and Exchange Program (grants NSFC 11811530072 and RFBR 18-51-53020-GFEN-a). The second author is also supported by the Natural Science Foundation of China (grant no. 11971222).

* Corresponding author: Zhi-Wei Sun.

1. **Introduction.** Let $p$ be an odd prime. It is well known that the numbers

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2$$

are pairwise incongruent modulo $p$, and they give all the $(p-1)/2$ quadratic residues modulo $p$. Recently Z.-W. Sun [7] initiated the study of permutations related to quadratic residues modulo $p$ as well as evaluations of related products involving $p$th roots of unity; many of his results in [7] are related to the class number of the quadratic field $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$. In this paper, we confirm some conjectures of Sun [7] in this new direction.

Let $p>3$ be a prime and let $\zeta=e^{2\pi i/p}$. Let $a\in\mathbb{Z}$ with $p\nmid a$. Recently, Z.-W. Sun [7, Theorem 1.3(ii)] showed that

$$\prod_{1\le j<k\le(p-1)/2}(\zeta^{aj^2}-\zeta^{ak^2})$$
$$=\begin{cases}\pm i^{(p-1)/4}p^{(p-3)/8}\varepsilon_p^{(\frac{a}{p})h(p)/2} & \text{if } p\equiv 1 \pmod 4,\\ (-p)^{(p-3)/8} & \text{if } p\equiv 3 \pmod 8,\\ (-1)^{(p+1)/8+(h(-p)-1)/2}(\frac{a}{p})p^{(p-3)/8}i & \text{if } p\equiv 7 \pmod 8,\end{cases}$$

where $(\frac{a}{p})$ is the Legendre symbol, $\varepsilon_p$ with $p\equiv 1 \pmod 4$ is the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$, and $h(d)$ with $d\equiv 0,1 \pmod 4$ not a square is the class number of the quadratic field with discriminant $d$. Sun [7, Theorem 1.5] also proved that

$$\begin{aligned}&(-1)^{a\frac{p+1}{2}\lfloor\frac{p-1}{4}\rfloor}2^{(p-1)(p-3)/8}\prod_{1\le j<k\le(p-1)/2}\cos\pi\frac{a(k^2-j^2)}{p}\\ &=\prod_{1\le j<k\le(p-1)/2}(\zeta^{aj^2}+\zeta^{ak^2})=\begin{cases}1 & \text{if } p\equiv 3 \pmod 4,\\ \pm\varepsilon_p^{(\frac{a}{p})h(p)((\frac{2}{p})-1)/2} & \text{if } p\equiv 1 \pmod 4.\end{cases}\end{aligned}\tag{1.1}$$

Our first theorem confirms [7, Conjecture 6.7].

**Theorem 1.1.** *Let $p$ be a prime with $p\equiv 1 \pmod 4$, and let $\zeta=e^{2\pi i/p}$. Let $a$ be an integer not divisible by $p$.*

(i) *If $p\equiv 1 \pmod 8$, then*

$$\prod_{1\le j<k\le(p-1)/2}(\zeta^{aj^2}+\zeta^{ak^2})=(-1)^{|\{1\le k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}.\tag{1.2}$$

(ii) *When $p\equiv 5 \pmod 8$, we have*

$$(-1)^{|\{1\le k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}\prod_{1\le j<k\le(p-1)/2}(\zeta^{aj^2}+\zeta^{ak^2})=\left(\frac{a}{p}\right)\varepsilon_p^{-(\frac{a}{p})h(p)}.\tag{1.3}$$

**Remark 1.1.** Let $p$ be a prime with $p\equiv 1 \pmod 4$. Then $(\frac{p-1}{2}!)^2\equiv -1 \pmod p$ by Wilson's theorem. We may write $p=x^2+y^2$ with $x,y\in\mathbb{Z}$, $x\equiv 1 \pmod 4$ and $y\equiv\frac{p-1}{2}!x \pmod p$. As $y^2\equiv p-1 \pmod 8$, we see that $y\equiv(\frac{2}{p})-1 \pmod 4$. By a result of K. Burde [3], we have

$$\left|\left\{1\le k<\frac{p}{4}:\ \left(\frac{k}{p}\right)=1\right\}\right|\equiv 0 \pmod 2\iff y\equiv\left(\frac{2}{p}\right)-1 \pmod 8.$$

Thus

$$(-1)^{|\{1\le k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}=(-1)^{\frac{p-1}{4}}(-1)^{\frac{1}{4}(y-(\frac{2}{p})+1)}=(-1)^{\lfloor\frac{y}{4}\rfloor}. \tag{1.4}$$

Let $p$ be an odd prime. For each $a\in\mathbb{Z}$ we let $\{a\}_p$ denote the least nonnegative residue of $a$ modulo $p$. Define

$$s(p):=\left|\left\{(j,k):\ 1\le j<k\le\frac{p-1}{2}\ \&\ \{j^2\}_p>\{k^2\}_p\right\}\right|$$

and

$$t(p):=\left|\left\{(j,k):\ 1\le j<k\le\frac{p-1}{2}\ \&\ \{k^2-j^2\}_p>\frac{p}{2}\right\}\right|$$

as in [7], where $(j,k)$ is an ordered pair. Sun [7, Theorem 1.4(i)] showed that

$$(-1)^{s(p)}=(-1)^{t(p)}=\begin{cases}1 & \text{if } p\equiv 3\ (\mathrm{mod}\ 8),\\ (-1)^{(h(-p)+1)/2} & \text{if } p\equiv 7\ (\mathrm{mod}\ 8).\end{cases}$$

He also conjectured that (cf. [7, Conjecture 6.1]) if $p\equiv 1\ (\mathrm{mod}\ 4)$ then

$$s(p)+t(p)\equiv\left|\left\{1\le k<\frac{p}{4}:\ \left(\frac{k}{p}\right)=1\right\}\right|\ (\mathrm{mod}\ 2). \tag{1.5}$$

Our second theorem in the case $a=1$ confirms this conjecture.

**Theorem 1.2.** *Let $p$ be a prime with $p\equiv 1\ (\mathrm{mod}\ 4)$, and let $a\in\mathbb{Z}$ with $p\nmid a$. Then*

$$\begin{aligned}&\left|\left\{(j,k):\ 1\le j<k\le\frac{p-1}{2}\ \&\ \{aj^2\}_p>\{ak^2\}_p\right\}\right|\\&+\left|\left\{(j,k):\ 1\le j<k\le\frac{p-1}{2}\ \&\ \{ak^2-aj^2\}_p>\frac{p}{2}\right\}\right|\\&\equiv\left|\left\{1\le k<\frac{p}{4}:\ \left(\frac{k}{p}\right)=\left(\frac{a}{p}\right)\right\}\right|\ (\mathrm{mod}\ 2).\end{aligned} \tag{1.6}$$

Our third theorem was first conjectured by Sun (cf. [7, Conjectures 6.3 and 6.4]).

**Theorem 1.3.** *Let $p$ be a prime with $p\equiv 3\ (\mathrm{mod}\ 4)$.*

(i) *We have*

$$(-1)^{|\{(j,k):\ 1\le j<k\le(p-1)/2\ \text{and}\ \{j(j+1)\}_p>\{k(k+1)\}_p\}|}=(-1)^{\lfloor(p+1)/8\rfloor}. \tag{1.7}$$

(ii) *Suppose $p>3$ and write $T_m=m(m+1)/2$ for $m\in\mathbb{N}$. Then*

$$(-1)^{|\{(j,k):\ 1\le j<k\le(p-1)/2\ \&\ \{T_j\}_p>\{T_k\}_p\}|}=(-1)^{\frac{h(-p)+1}{2}+|\{1\le k\le\lfloor\frac{p+1}{8}\rfloor:\ (\frac{k}{p})=1\}|}. \tag{1.8}$$

We will prove Theorems 1.1-1.2 in Section 2. Based on an auxiliary theorem given in Section 3, we are going to prove Theorem 1.3 in Section 4.

## 2. Proofs of Theorems 1.1-1.2.

In 2006, H. Pan [6] obtained the following lemma.

**Lemma 2.1.** (H. Pan [6]) *Let $n>1$ be an odd integer and let $c$ be any integer relatively prime to $n$. For each $j=1,\ldots,(n-1)/2$ let $\pi_c(j)$ be the unique $r\in\{1,\ldots,(n-1)/2\}$ with $cj$ congruent to $r$ or $-r$ modulo $n$. For the permutation $\pi_c$ on $\{1,\ldots,(n-1)/2\}$, its sign is given by*

$$\mathrm{sign}(\pi_c)=\left(\frac{c}{n}\right)^{(n+1)/2},$$

*where $(\frac{c}{n})$ is the Jacobi symbol.*

*Proof of the First Part of Theorem 1.1.* As $p\equiv 1 \pmod 8$, there is an integer $c$ with $c^2\equiv 2 \pmod p$. For $j=1,\ldots,(p-1)/2$ let $\pi_c(j)$ be the unique $r\in\{1,\ldots,(p-1)/2\}$ with $cj$ congruent to $r$ or $-r$ modulo $p$. Then $\pi_c$ is a permutation on $\{1,\ldots,(p-1)/2\}$, and

$$\prod_{1\le j<k\le (p-1)/2}\frac{\zeta^{2aj^2}-\zeta^{2ak^2}}{\zeta^{aj^2}-\zeta^{ak^2}}=\prod_{1\le j<k\le (p-1)/2}\frac{\zeta^{a\pi_c(j)^2}-\zeta^{a\pi_c(k)^2}}{\zeta^{aj^2}-\zeta^{ak^2}}$$
$$=(-1)^{|\{(j,k):\ 1\le j<k\le (p-1)/2\ \&\ \pi_c(j)>\pi_c(k)\}|}=\mathrm{sign}(\pi_c)=\left(\frac{c}{p}\right)$$

with the aid of Lemma 2.1. In view of K. S. Williams and J. D. Currie [8, (1.4)], we have

$$\left(\frac{c}{p}\right)\equiv c^{(p-1)/2}=(c^2)^{(p-1)/4}\equiv 2^{(p-1)/4}\equiv(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}\pmod p.$$

Therefore (1.2) holds in the case $p\equiv 1 \pmod 8$. □

**Remark 2.1.** Our method to prove part (i) of Theorem 1.1 does not work for part (ii) of Theorem 1.1.

*Proof of the Second Part of Theorem 1.1.* We distinguish two cases.

**Case** 1. $(\frac{a}{p})=1$.

In this case,

$$\left\{\{aj^2\}_p:\ 1\le j\le\frac{p-1}{2}\right\}=\left\{\{k^2\}_p:\ 1\le k\le\frac{p-1}{2}\right\}$$

So it suffices to show (1.3) for $a=1$. In view of (1.1) with $a=1$, we only need to prove that

$$(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}\prod_{1\le j<k\le(p-1)/2}(\zeta^{j^2}+\zeta^{k^2})>0. \tag{2.1}$$

As $(\frac{-1}{p})=1$, for each $1\le j\le(p-1)/2$ there is a unique integer $j_*\in\{1,\ldots,(p-1)/2\}$ such that $p-j^2\equiv j_*^2 \pmod p$. As $(\frac{2}{p})=-1$, we have $j\ne j_*$. For any distinct $j,k\in\{1,\ldots,(p-1)/2\}$, we have $\zeta^{j^2}+\zeta^{k^2}\ne 0$ (since $\zeta^{2j^2}\ne\zeta^{2k^2}$) and

$$(\zeta^{j^2}+\zeta^{k^2})(\zeta^{j_*^2}+\zeta^{k_*^2})=(\zeta^{j^2}+\zeta^{k^2})(\zeta^{-j^2}+\zeta^{-k^2})=|\zeta^{j^2}+\zeta^{k^2}|^2>0;$$

also,

$$\{j,k\}=\{j_*,k_*\}\iff j_*=k\text{ and }k_*=j\iff j_*=k.$$

For $1\le j\le(p-1)/2$, clearly

$$\zeta^{j^2}+\zeta^{j_*^2}=\zeta^{j^2}+\zeta^{-j^2}=2\cos 2\pi\frac{j^2}{p}=2\cos 2\pi\frac{j_*^2}{p}$$

and hence

$$\zeta^{j^2}+\zeta^{j_*^2}>0\iff\cos 2\pi\frac{j^2}{p}>0\iff\{j^2\}_p<\frac{p}{4}\text{ or }\{j_*^2\}_p<\frac{p}{4}.$$

Thus the sign of the product

$$\prod_{\substack{1\le j<k\le(p-1)/2\\ p\mid j^2+k^2}}(\zeta^{j^2}+\zeta^{k^2})=(-1)^{(p-1)/4}\prod_{1\le j<j_*\le(p-1)/2}(-\zeta^{j^2}-\zeta^{j_*^2})$$

is

$$(-1)^{(p-1)/4-|\{1\le k<\frac{p}{4}:\ (\frac{k}{p})=1\}|}=(-1)^{|\{1\le k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}.$$

So (2.1) holds and (1.3) follows.

**Case** 2. $(\frac{a}{p})=-1$.

By the discussion in Case 1, we have

$$(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}\prod_{1\le j<k\le (p-1)/2}(\zeta^{j^2}+\zeta^{k^2})=\varepsilon_p^{-h(p)}. \tag{2.2}$$

Let $\varphi_a$ be the element of the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with $\varphi_a(\zeta)=\zeta^a$. Then

$$\varphi_a(\sqrt{p})=\varphi_a\Big(\sum_{x=0}^{p-1}\zeta^{x^2}\Big)=\sum_{x=0}^{p-1}\zeta^{ax^2}=\Big(\frac{a}{p}\Big)\sqrt{p}=-\sqrt{p}$$

by the evaluation of quadratic Gauss sums (cf. [5, pp. 70-75]). Hence

$$\varphi_a(\varepsilon_p^{-h(p)})=\left(\frac{N(\varepsilon_p)}{\varepsilon_p}\right)^{-h(p)}=-\varepsilon_p^{h(p)}$$

where $N(\varepsilon_p)$ is the norm of $\varepsilon_p$ with respect to the field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$, and we have used the known results $N(\varepsilon_p)=-1$ and $2\nmid h(p)$ (cf. [4, p. 185 and p. 187]). Thus, by applying the automorphism $\varphi_a$ to the identity (2.2), we get

$$\begin{aligned}&(-1)^{|\{0<k<\frac{p}{4}:\ (\frac{k}{p})=-1\}|}\prod_{1\le j<k\le (p-1)/2}(\zeta^{aj^2}+\zeta^{ak^2})\\ =&\varphi_a(\varepsilon_p^{-h(p)})=-\varepsilon_p^{h(p)}=\Big(\frac{a}{p}\Big)\varepsilon_p^{-(\frac{a}{p})h(p)}.\end{aligned}$$

In view of the above, we have proven Theorem 1.1(ii). □

**Lemma 2.2.** *Let $p$ be an odd prime, and let $a\in\mathbb{Z}$ with $p\nmid a$. Then*

$$\begin{aligned}&\left|\left\{(j,k):\ 1\le j<k\le\frac{p-1}{2}\ \&\ \{aj^2\}_p>\{ak^2\}_p\right\}\right|\\ &+\left|\left\{(j,k):\ 1\le j<k\le\frac{p-1}{2}\ \&\ \{ak^2-aj^2\}_p>\frac{p}{2}\right\}\right|\\ \equiv&\left|\left\{(j,k):\ 1\le j<k\le\frac{p-1}{2}\ \&\ |\{aj^2\}_p-\{ak^2\}_p|>\frac{p}{2}\right\}\right|\ (\mathrm{mod}\ 2).\end{aligned} \tag{2.3}$$

*Proof.* This can be easily checked by distinguishing the cases $\{aj^2\}_p<\{ak^2\}_p$ and $\{aj^2\}_p>\{ak^2\}_p$ for $1\le j<k\le(p-1)/2$. □

*Proof of Theorem 1.2.* In view of Lemma 2.2, it suffices to show that

$$\begin{aligned}&\left|\left\{(j,k):\ 1\le j<k\le\frac{p-1}{2}\ \&\ |\{aj^2\}_p-\{ak^2\}_p|>\frac{p}{2}\right\}\right|\\ \equiv&\left|\left\{1\le k<\frac{p}{4}:\ \left(\frac{ak}{p}\right)=1\right\}\right|\ (\mathrm{mod}\ 2).\end{aligned} \tag{2.4}$$

As $(\frac{-1}{p})=1$, for each $1\le j\le(p-1)/2$ there is a unique integer $j_*\in\{1,\ldots,(p-1)/2\}$ such that $-j^2\equiv j_*^2\ (\mathrm{mod}\ p)$ and hence $-aj^2\equiv aj_*^2\ (\mathrm{mod}\ p)$. Clearly, $|\{1\le j\le(p-1)/2:\ j=j_*\}|\le 1$. Note that

$$|\{aj_*^2\}_p-\{ak_*^2\}_p|=|(p-\{aj^2\}_p)-(p-\{ak^2\}_p)|=|\{aj^2\}_p-\{ak^2\}_p|.$$

If $j$ and $k$ are distinct elements of $\{1,\ldots,(p-1)/2\}$, then $\{j,k\}=\{j_*,k_*\}$ if and only if $j_*=k$ and $k_*=j$. Thus

$$\begin{aligned}&\left|\left\{(j,k):\ 1\le j<k\le\frac{p-1}{2}\ \&\ |\{aj^2\}_p-\{ak^2\}_p|>\frac{p}{2}\right\}\right|\\ \equiv&\frac{1}{2}\left|\left\{1\le j\le\frac{p-1}{2}:\ |\{aj^2\}_p-\{aj_*^2\}|=|2\{aj^2\}_p-p|>\frac{p}{2}\right\}\right|\\ =&\frac{1}{2}\left|\left\{1\le j\le\frac{p-1}{2}:\ \{aj^2\}_p<\frac{p}{4}\text{ or }\{aj^2\}_p>\frac{3}{4}p\right\}\right|\\ =&\frac{1}{2}\left|\left\{1\le j\le\frac{p-1}{2}:\ \{aj^2\}_p<\frac{p}{4}\right\}\right|+\frac{1}{2}\left|\left\{1\le j\le\frac{p-1}{2}:\ \{aj_*^2\}_p<\frac{p}{4}\right\}\right|\\ =&\left|\left\{1\le j\le\frac{p-1}{2}:\ \{aj^2\}_p<\frac{p}{4}\right\}\right|=\left|\left\{1\le k<\frac{p}{4}:\ \left(\frac{ak}{p}\right)=1\right\}\right|\pmod 2.\end{aligned}$$

This proves the desired (2.4). So (1.6) holds. □

3. **An auxiliary theorem.** We first need a result of Sun [7].

**Lemma 3.1.** *Let $p=2n+1$ be a prime with $n$ odd, and let $a\in\mathbb{Z}$ with $p\nmid a$. Then*

$$\begin{aligned}&(-1)^{|\{(j,k):\ 1\le j<k\le n\ \&\ \{aj^2\}_p>\{ak^2\}_p\}|}\\ =&\begin{cases}1 & \text{if } p\equiv 3\pmod 8,\\ (-1)^{(h(-p)+1)/2}\left(\frac{a}{p}\right) & \text{if } p\equiv 7\pmod 8.\end{cases}\end{aligned}\tag{3.1}$$

*Proof.* By Sun [7, Theorem 1.4(ii)],

$$\begin{aligned}&\prod_{1\le j<k\le(p-1)/2}\left(\cot\pi\frac{aj^2}{p}-\cot\pi\frac{ak^2}{p}\right)\\ =&\begin{cases}(2^{p-1}/p)^{(p-3)/8} & \text{if } p\equiv 3\pmod 8,\\ (-1)^{(h(-p)+1)/2}\left(\frac{a}{p}\right)(2^{p-1}/p)^{(p-3)/8} & \text{if } p\equiv 7\pmod 8.\end{cases}\end{aligned}$$

This implies (3.1) since for any $1\le j<k\le(p-1)/2$ we have

$$\cot\pi\frac{aj^2}{p}<\cot\pi\frac{ak^2}{p}\iff\{aj^2\}_p>\{ak^2\}_p.$$

We are done. □

**Theorem 3.2.** *Let $p=2n+1$ be a prime with $n$ odd, and let $a,b\in\{1,\ldots,p-1\}$. Then*

$$\begin{aligned}&(-1)^{|\{(s,t):\ 0\le t<s\le n\ \&\ \{as^2-b\}_p>\{at^2-b\}_p\}|-|\{0<r<b:\ (\frac{r}{p})=(\frac{a}{p})\}|}\\ =&\begin{cases}1 & \text{if } p\equiv 3\pmod 8,\\ (-1)^{(h(-p)-1)/2}\left(\frac{a}{p}\right) & \text{if } p\equiv 7\pmod 8.\end{cases}\end{aligned}\tag{3.2}$$

*Proof.* Let $0\le t<s\le n$. By comparing $\{as^2\}_p$ and $\{at^2\}_p$ with $b$, we verify case by case that

$$[\{as^2-b\}_p>\{at^2-b\}_p]+[\{as^2\}_p>\{at^2\}_p]$$

is odd if and only if

$$\{as^2\}_p\ge b>\{at^2\}_p\ \text{ or }\ \{at^2\}_p\ge b>\{as^2\}_p,$$

where for an assertion $A$ we define

$$[A]=\begin{cases}1 & \text{if } A \text{ holds},\\ 0 & \text{otherwise}.\end{cases}$$

Note that

$$\begin{aligned}&|\{(s,t):\ 0\le t<s\le n,\ \{as^2\}_p\ge b>\{at^2\}_p \text{ or } \{as^2\}_p<b\le\{at^2\}_p\}|\\ =&\left|\left\{(r_1,r_2):\ 0\le r_1<b\le r_2\le p-1\ \&\ \left(\frac{ar_1}{p}\right),\left(\frac{ar_2}{p}\right)\ne -1\right\}\right|\\ =&\left|\left\{0\le r<b:\ \left(\frac{ar}{p}\right)\ne -1\right\}\right|\times\left(\frac{p+1}{2}-\left|\left\{0\le r<b:\ \left(\frac{ar}{p}\right)\ne -1\right\}\right|\right)\\ \equiv&\left|\left\{0\le r<b:\ \left(\frac{ar}{p}\right)\ne -1\right\}\right|=1+\left|\left\{0<r<b:\ \left(\frac{r}{p}\right)=\left(\frac{a}{p}\right)\right\}\right| \pmod 2\end{aligned}$$

and

$$\begin{aligned}&|\{(s,t):\ 0\le t<s\le n\ \&\ \{as^2\}_p>\{at^2\}_p\}|\\ =&\binom{n+1}{2}-|\{(s,t):\ 0\le t<s\le n\ \&\ \{as^2\}_p<\{at^2\}_p\}|\end{aligned}$$

with $\binom{n+1}{2}\equiv\frac{p+1}{4} \pmod 2$. Combining the above with (3.1), we finally obtain (3.2). □

## 4. **Proof of Theorem 1.3.**

**Lemma 4.1.** *Let $p$ be a prime with $p\equiv 3 \pmod 4$.*

(i) (Dirichlet (cf. [5, p. 238])) *If $p>3$ then*

$$\left(2-\left(\frac{2}{p}\right)\right)h(-p)=\sum_{k=1}^{(p-1)/2}\left(\frac{k}{p}\right).$$

(ii) (B. C. Berndt and S. Chowla [1]) *If $p\equiv 3 \pmod 8$, then $\sum_{0<k<p/4}(\frac{k}{p})=0$. If $p\equiv 7 \pmod 8$, then $\sum_{p/4<k<p/2}(\frac{k}{p})=0$.*

*Proof of Theorem 1.3.* We just prove the second part in details since the first part can be proved similarly.

Write $n=(p-1)/2$, and set

$$a=\frac{p+1}{2}\quad\text{and}\quad b=\begin{cases}(5p+1)/8 & \text{if } p\equiv 3 \pmod 8,\\ (p+1)/8 & \text{if } p\equiv 7 \pmod 8.\end{cases}$$

For any $r\in\mathbb{Z}$, we have

$$T_{n-r}=\frac{n(n+1)}{2}-(2n+1)\frac{r}{2}+\frac{r^2}{2}\equiv ar^2-b \pmod p.$$

Thus

$$\begin{aligned}&|\{(j,k):\ 0\le j<k\le n\ \&\ \{T_j\}_p>\{T_k\}_p\}|\\ =&|\{(t,s):\ 0\le t<s\le n\ \&\ \{T_{n-s}\}_p>\{T_{n-t}\}_p\}|\\ =&|\{(t,s):\ 0\le t<s\le n\ \&\ \{as^2-b\}_p>\{at^2-b\}_p\}|.\end{aligned}$$

Note that $(\frac{a}{p})=(\frac{2}{p})$. Set

$$B:=\left|\left\{0<r<b:\ \left(\frac{r}{p}\right)=\left(\frac{2}{p}\right)\right\}\right|. \tag{4.1}$$

Applying Theorem 3.2, from the above we obtain

$$\begin{aligned}&|\{(j,k):\ 1\le j<k\le n\ \&\ \{T_j\}_p>\{T_k\}_p\}|\\ \equiv& B+\begin{cases}0\pmod 2 & \text{if } p\equiv 3\pmod 8,\\ (h(-p)-1)/2\pmod 2 & \text{if } p\equiv 7\pmod 8.\end{cases}\end{aligned} \tag{4.2}$$

When $p\equiv 7\pmod 8$, we have

$$B+1=\left|\left\{1\le k\le\frac{p+1}{8}:\ \left(\frac{k}{p}\right)=1\right\}\right|$$

and hence (1.8) follows from (4.2).

Below we handle the case $p\equiv 3\pmod 8$. Observe that

$$\begin{aligned}B=&\sum_{k=1}^{(p-1)/2}\frac{1-(\frac{k}{p})}{2}+\left|\left\{\frac{p}{2}<k<\frac{5p+1}{8}:\ \left(\frac{2k-p}{p}\right)=1\right\}\right|\\ =&\frac{p-1}{4}-\frac12\sum_{k=1}^{(p-1)/2}\left(\frac{k}{p}\right)+\left|\left\{0<r<\frac{p+1}{4}:\ 2\nmid r\ \&\ \left(\frac{r}{p}\right)=1\right\}\right|.\end{aligned}$$

Applying Lemma 4.1, we obtain

$$\begin{aligned}B=&\frac{p-1}{4}-\frac{3h(-p)}{2}+\sum_{0<k<p/4}\frac{1+(\frac{k}{p})}{2}\\ &-\left|\left\{0<r<\frac{p+1}{4}:\ 2\mid r\ \&\ \left(\frac{r}{p}\right)=1\right\}\right|\\ \equiv&\frac{h(-p)+1}{2}+\frac{p-3}{8}-\left|\left\{0<k<\frac{p+1}{8}:\ \left(\frac{2k}{p}\right)=1\right\}\right|\\ =&\frac{h(-p)+1}{2}+\left|\left\{0<k<\frac{p+1}{8}:\ \left(\frac{2k}{p}\right)=-1\right\}\right|\\ =&\frac{h(-p)+1}{2}+\left|\left\{1\le k\le\left\lfloor\frac{p+1}{8}\right\rfloor:\ \left(\frac{k}{p}\right)=1\right\}\right|\pmod 2.\end{aligned}$$

So, in this case, (1.8) also follows from (4.2). □

**Acknowledgments.** We would like to thank the referee for helpful comments.

## REFERENCES

[1] B. C. Berndt and S. Chowla, Zero sums of the Legendre symbol, *Nordisk Mat. Tidskr.*, **22** (1974), 5–8.
[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, John Wiley & Sons, Inc., New York, 1998.
[3] K. Burde, Eine Verteilungseigenschaft der Legendresymbole, *J. Number Theory*, **12** (1980), 273–277.
[4] H. Cohn, *Advanced Number Theory*, Dover Publ., New York, 1962.
[5] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd Edition, Grad. Texts. Math., 84. Springer, New York, 1990.
[6] H. Pan, A remark on Zolotarev's theorem, preprint, arXiv:math/0601026.

[7] Z.-W. Sun, Quadratic residues and related permutations and identities, *Finite Fields Appl.*, **59** (2019), 246–283.
[8] K. S. Williams and J. D. Currie, Class numbers and biquadratic reciprocity, *Canad. J. Math.*, **34** (1982), 969–988.

Received December 2019; revised March 2020.

*E-mail address*: fedyapetrov@gmail.com
*E-mail address*: zwsun@nju.edu.cn