symmetry

MDPI

Article

The Quadratic Residues and Some of Their New Distribution Properties

Tingting Wang [1,†] and Xingxing Lv [2,*,†]

[1] College of Science, Northwest A&F University, No.22 Xinong Road, Yangling 712100, China; ttwang@nwafu.edu.cn
[2] School of Mathematics, Northwest University, Xi'an 710127, China
[*] Correspondence: lvxingxing@stumail.nwu.edu.cn
[†] These authors contributed equally to this work.

Received: 17 February 2020; Accepted: 3 March 2020; Published: 5 March 2020

Abstract: In this paper, we give some interesting identities and asymptotic formulas for one kind of counting function, by studying the computational problems involving the symmetry sums of one kind quadratic residues and quadratic non-residues mod p. The main methods we used are the properties of the Legendre's symbol mod p, and the estimate for character sums. As application, we solve two open problems proposed by Zhiwei Sun.

Keywords: quadratic residues; quadratic non-residues; Legendre's symbol; character sums; asymptotic formula

1. Introduction

Let p be an odd prime. For any integer a satisfying $(a, p) = 1$ (i.e., a co-prime to p), if there exists an integer x such that the congruence $x^2 \equiv a \bmod p$, then a is called a quadratic residue mod p. Otherwise, a is called a quadratic non-residue mod p. In order to facilitate the study of the properties of quadratic residues mod p, Legendre first introduced the characteristic function of the quadratic residues mod p. The defination of Legendre's symbol $\left(\frac{*}{p}\right)$ is that, for any integer a,

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residues mod } p; \\ -1, & \text{if } a \text{ is a quadratic non-residues mod } p; \\ 0 & \text{if } p \mid a. \end{cases}$$

We can find various interesting properties of the quadratic residues and Legendre's symbol in number theory books such as [1,2].

In fact, the properties of quadratic residues and Legendre's symbol mod p are very meaningful in number theory, which attract attention of many experts and scholars. Valuable research results about them have been obtained. For example, Burgess [3,4] proved that the least quadratic non-residue mod p is less than $p^{\frac{1}{4}+\varepsilon}$, where ε denotes any fixed positive number. The constant $\frac{1}{4}$ has been improved by some authors, see references [5–7].

Let $p \geq 3$ be a prime satisfying $p = 4k + 1$. For any quadratic residue r mod p and quadratic non-residue s mod p, it holds that (see [2]: Theorems 4–11)

$$\left(\frac{1}{2}\sum_{a=1}^{p-1}\left(\frac{a+r\bar{a}}{p}\right)\right)^2 + \left(\frac{1}{2}\sum_{a=1}^{p-1}\left(\frac{a+s\bar{a}}{p}\right)\right)^2 = p, \tag{1}$$

where $\bar{a}$ is satisfied with the equation $\bar{a} \cdot a \equiv 1 \bmod p$.

Some papers as regards quadratic residues and non-residues mod p can be found in references [8–16].

Recently, Zhiwei Sun proposed two conjectures during his communication with us:

A. For any prime $p \geq 101$, there is at least one integer a, such that a, $a+\bar{a}$ and $a-\bar{a}$ are all quadratic residues mod p?

B. For any prime $p \geq 18$, there is at least one quadratic non-residue a mod p, such that $a+\bar{a}$ and $a-\bar{a}$ are quadratic residues mod p?

Zhiwei Sun carried out some numerical tests to support his conjectures but cannot prove them. In this paper, we concern about problems involving quadratic residues and non-residues mod p.

We think Zhiwei Sun's conjectures not only show the symmetry of quadratic residues and non-residues but also reveal their profound distribution properties of the quadratic residues and non-residues mod p.

As application of our results, we solve them thoroughly. We actually proved two stronger conclusions. For narrative purposes, let p denote any odd prime $S(p,1)$ denote the number of all integers $1 \leq a \leq p-1$ such that a, $a+\bar{a}$, and $a-\bar{a}$ are all quadratic residues mod p, $S(p,-1)$ denotes the number of all integers $1 \leq a \leq p-1$ such that a is a quadratic non-residue mod p, $a+\bar{a}$ and $a-\bar{a}$ are quadratic residues mod p.

2. Results

The notations are as above. We prove our main results using elementary methods, the estimate for character sums, and the properties of Legendre's symbol mod p.

Theorem 1. *For any prime p with $p \equiv 3 \bmod 4$, we have the identities*

$$S(p,1) = \begin{cases} \frac{1}{8}\left(p-3\right), & \text{if } p \equiv 3 \bmod 8; \\ \frac{1}{8}\left(p-7\right), & \text{if } p \equiv 7 \bmod 8 \end{cases}$$

and

$$S(p,-1) = \begin{cases} \frac{1}{8}\left(p-3\right), & \text{if } p \equiv 3 \bmod 8; \\ \frac{1}{8}\left(p+1\right), & \text{if } p \equiv 7 \bmod 8. \end{cases}$$

Theorem 2. *For any prime p with $p \equiv 1 \bmod 4$, we have the asymptotic formulas*

$$S(p,1) = \begin{cases} \frac{1}{8}\left(p-3\right) + K(p,1), & \text{if } p \equiv 5 \bmod 8; \\ \frac{1}{8}\left(p-17\right) + K_1(p,1), & \text{if } p \equiv 1 \bmod 8 \end{cases}$$

and

$$S(p,-1) = \begin{cases} \frac{1}{8}\left(p+3\right) + K(p,-1), & \text{if } p \equiv 5 \bmod 8; \\ \frac{1}{8}\left(p+3\right) + K_1(p,-1), & \text{if } p \equiv 1 \bmod 8, \end{cases}$$

where we have the estimates $|K(p,1)| \leq \frac{3}{4}\cdot\sqrt{p}$, $|K_1(p,1)| \leq \frac{5}{4}\cdot\sqrt{p}$, $|K(p,-1)| \leq \frac{3}{4}\cdot\sqrt{p}$ *and* $|K_1(p,-1)| \leq \frac{5}{4}\cdot\sqrt{p}$.

From Theorems 1 and 2 and some simple calculations, we can deduce the following two corollaries:

Corollary 1. *For any prime $p \geq 101$, there is at least one integer a, such that a, $a+\bar{a}$ and $a-\bar{a}$ are all quadratic residues* mod p.

Corollary 2. *For any prime $p \geq 18$, there is at least one quadratic non-residue a* mod p, *such that $a+\bar{a}$ and $a-\bar{a}$ are quadratic residues* mod p.

Thus, we solved two problems proposed by professor Zhiwei Sun.

3. Several Lemmas

To complete the proofs of our main results, we need the following two basic lemmas.

Lemma 1. *Let p be a prime with $p \equiv 1 \bmod 4$; then, for any integer k with $(k, p) = 1$, we have the identity*

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

Proof of Lemma 1. Note that, for any integer a with $(a, p) = 1$, there is $\left(\frac{a}{p}\right) = \left(\frac{\bar{a}}{p}\right)$. Using the properties of the Legendre's symbol and reduced residue system mod p, we have

$$\begin{aligned} \sum_{a=1}^{p-1} \left(\frac{a^2+k}{p}\right) &= \sum_{a=1}^{p-1} \left(1 + \left(\frac{a}{p}\right)\right) \left(\frac{a+k}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{a+k}{p}\right) + \sum_{a=1}^{p-1} \left(\frac{a^2+ak}{p}\right) \\ &= \sum_{a=0}^{p-1} \left(\frac{a+k}{p}\right) + \sum_{a=1}^{p-1} \left(\frac{1+\bar{a}k}{p}\right) - \left(\frac{k}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{1+a}{p}\right) - \left(\frac{k}{p}\right) \\ &= \sum_{a=0}^{p-1} \left(\frac{1+a}{p}\right) - \left(\frac{k}{p}\right) - 1 = -1 - \left(\frac{k}{p}\right). \end{aligned}$$

This proves Lemma 1. □

Lemma 2. *Let p be a prime with $p \equiv 1 \bmod 4$; then, we have the estimate*

$$\left|\sum_{a=1}^{p-1} \left(\frac{a \pm \bar{a}}{p}\right)\right| \le 2 \cdot \sqrt{p} \quad \textit{and} \quad \left|\sum_{a=1}^{p-1} \left(\frac{a^4-1}{p}\right) \left(\frac{a}{p}\right)\right| \le 4 \cdot \sqrt{p}.$$

Proof of Lemma 2. Let $f(x) = x^3 \pm x$; then, $f(x)$ is not a complete square of an integral coefficient polynomial $g(x)$. Thus, from Weil's important work [17], we have

$$\left|\sum_{a=1}^{p-1} \left(\frac{a \pm \bar{a}}{p}\right)\right| = \left|\sum_{a=1}^{p-1} \left(\frac{a \pm \bar{a}}{p}\right) \left(\frac{a^2}{p}\right)\right| = \left|\sum_{a=1}^{p-1} \left(\frac{a^3 \pm a}{p}\right)\right| \le 2 \cdot \sqrt{p}.$$

Of course, for any prime $p = 4k + 1$, note that 1 and -1 are two quadratic residues mod p, so, from identity (1), we can also deduce the above estimate.

This proves the first estimate in Lemma 2.

Now, let $\chi_2 = \left(\frac{*}{p}\right)$, $e(y) = e^{2\pi i y}$, $\tau(\chi) = \sum_{a=1}^{p-1} \chi(a) e\left(\frac{a}{p}\right)$ denote the classical Gauss sums. Then, note that $\tau(\chi_2) = \sqrt{p}$; from the properties of $\tau(\chi)$, we have

$$\begin{aligned} \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{a^4-1}{p}\right) &= \frac{1}{\tau\left(\overline{\chi}_2\right)} \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \sum_{b=1}^{p-1} \left(\frac{b}{p}\right) e\left(\frac{b\left(a^4-1\right)}{p}\right) \\ &= \frac{1}{\sqrt{p}} \sum_{b=1}^{p-1} \left(\frac{b}{p}\right) e\left(\frac{-b}{p}\right) \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) e\left(\frac{ba^4}{p}\right). \end{aligned} \qquad (2)$$

Let g denote a primitive root mod p, $r = g^{\frac{p-1}{4}}$. It is clear that, if $p = 8k+5$, then r is a quadratic non-residue mod p and $r^4 \equiv 1 \bmod p$. Thus, in this case, for any integer $1 \le b \le p-1$, we have

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) e\left(\frac{ba^4}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{ar}{p}\right) e\left(\frac{b(ra)^4}{p}\right) = -\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) e\left(\frac{ba^4}{p}\right)$$

or

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) e\left(\frac{ba^4}{p}\right) = 0. \tag{3}$$

If $p = 8k+1$, then r is a quadratic residue mod p. Thus, in this case, there must be a character χ_1 mod p such that $\chi_1^4 = \left(\frac{*}{p}\right)$. Let λ be a fourth-order character mod p (That is, $\lambda^4 = \chi_0$ is the principal character mod p); then, from the properties of the Gauss sums and character sums mod p, we have

$$\begin{aligned} &\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) e\left(\frac{ba^4}{p}\right) = \sum_{a=1}^{p-1} \chi_1^4(a) e\left(\frac{ba^4}{p}\right) = \sum_{a=1}^{p-1} \chi_1\left(a^4\right) e\left(\frac{ba^4}{p}\right) \\ = &\sum_{a=1}^{p-1} \chi_1(a)\left(1+\lambda(a)+\lambda^2(a)+\lambda^3(a)\right) e\left(\frac{ba}{p}\right) = \overline{\chi}_1(b)\tau\left(\chi_1\right) \\ &+\overline{\chi}_1(b)\overline{\lambda}(b)\tau\left(\chi_1\lambda\right) + \overline{\chi}_1(b)\overline{\lambda}^2(b)\tau\left(\chi_1\lambda^2\right) + \overline{\chi}_1(b)\overline{\lambda}^3(b)\tau\left(\chi_1\lambda^3\right). \end{aligned} \tag{4}$$

For any character χ mod p, note that the estimate $|\tau(\chi)| \le \sqrt{p}$; from (2) and (4), we have the estimate

$$\begin{aligned} &\left|\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{a^4-1}{p}\right)\right| = \left|\frac{1}{\sqrt{p}} \sum_{b=1}^{p-1} \left(\frac{b}{p}\right) e\left(\frac{-b}{p}\right) \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) e\left(\frac{ba^4}{p}\right)\right| \\ \le &\frac{\left|\tau\left(\chi_1\right)\tau\left(\overline{\chi}_1\chi_2\right)\right|}{\sqrt{p}} + \frac{\left|\tau\left(\chi_1\lambda\right)\tau\left(\overline{\chi}_1\overline{\lambda}\chi_2\right)\right|}{\sqrt{p}} + \frac{\left|\tau\left(\chi_1\lambda^2\right)\tau\left(\overline{\chi}_1\overline{\lambda}^2\chi_2\right)\right|}{\sqrt{p}} \\ &+\frac{\left|\tau\left(\chi_1\lambda^3\right)\tau\left(\overline{\chi}_1\overline{\lambda}^3\chi_2\right)\right|}{\sqrt{p}} \le 4 \cdot \sqrt{p}. \end{aligned} \tag{5}$$

Now, the second estimate in Lemma 2 follows from (2), (3) and (5). □

4. Proofs of the Theorems

In this section, we shall complete the proofs of our main results.

Proof of Theorem 1. For any prime p with $p \equiv 3 \bmod 4$, note that $\left(\frac{-1}{p}\right) = -1$, so, for all integers $1 \le a \le p-1$, we have $(a+\overline{a}, p) = 1$ or $\left(a^2+1, p\right) = 1$. If $a = 1$ or $p-1$, then $a - \overline{a} = 0$, and $\left(a^2-1, p\right) = 1$ for all integers $2 \le a \le p-2$. Note that the identities

$$\sum_{a=1}^{p-1} \left(\frac{a^4-1}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{1-\overline{a}^4}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{1-a^4}{p}\right) = -\sum_{a=1}^{p-1} \left(\frac{a^4-1}{p}\right) = 0,$$

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{a^2-\overline{a}^2}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{-a}{p}\right) \left(\frac{a^2-\overline{a}^2}{p}\right) = -\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \left(\frac{a^2-\overline{a}^2}{p}\right) = 0,$$

$$\sum_{a=1}^{p-1} \left(\frac{a+\overline{a}}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{a-\overline{a}}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{-a-\overline{a}}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{-a+\overline{a}}{p}\right) = 0,$$

from Lemma 1, the definitions of S(p,1) and quadratic residues mod p we have

$$\begin{aligned}
S(p,1) &= \frac{1}{8}\sum_{a=2}^{p-2}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+\bar{a}}{p}\right)\right)\left(1+\left(\frac{a-\bar{a}}{p}\right)\right)\\
&= \frac{p-3}{8}+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a}{p}\right)+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a+\bar{a}}{p}\right)+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a-\bar{a}}{p}\right)+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a^2-\bar{a}^2}{p}\right)\\
&\quad+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a^2+1}{p}\right)+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a^2-1}{p}\right)+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a}{p}\right)\left(\frac{a^2-\bar{a}^2}{p}\right)\\
&= \frac{p-3}{8}+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a+\bar{a}}{p}\right)+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a-\bar{a}}{p}\right)-\frac{1}{4}\left(\frac{2}{p}\right)\\
&\quad+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a^2+1}{p}\right)+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a^2-1}{p}\right)+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(\frac{a^2-\bar{a}^2}{p}\right)+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a^4-1}{p}\right)\\
&= \frac{p-3}{8}-\frac{1}{4}\left(\frac{2}{p}\right)-\frac{1}{8}+\frac{1}{8}\sum_{a=0}^{p-1}\left(\frac{a^2+1}{p}\right)\\
&= \frac{1}{8}\left(p-5-2\left(\frac{2}{p}\right)\right)=\begin{cases}\frac{1}{8}(p-3), & \text{if } p\equiv 3 \bmod 8;\\ \frac{1}{8}(p-7), & \text{if } p\equiv 7 \bmod 8.\end{cases}
\end{aligned}\tag{6}$$

Similarly, from the methods of proving (6), we have the computational formula

$$\begin{aligned}
S(-1,p) &= \frac{1}{8}\sum_{a=2}^{p-2}\left(1-\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+\bar{a}}{p}\right)\right)\left(1+\left(\frac{a-\bar{a}}{p}\right)\right)\\
&= \frac{1}{4}\sum_{a=2}^{p-2}\left(1+\left(\frac{a+\bar{a}}{p}\right)\right)\left(1+\left(\frac{a-\bar{a}}{p}\right)\right)-S(p,1)\\
&= \frac{p-3}{4}+\frac{1}{4}\sum_{a=1}^{p-1}\left(\frac{a+\bar{a}}{p}\right)+\frac{1}{4}\sum_{a=1}^{p-1}\left(\frac{a-\bar{a}}{p}\right)+\frac{1}{4}\sum_{a=1}^{p-1}\left(\frac{a^2-\bar{a}^2}{p}\right)-S(p,1)\\
&= \frac{1}{8}\left(p-1+2\left(\frac{2}{p}\right)\right)=\begin{cases}\frac{1}{8}(p-3), & \text{if } p\equiv 3 \bmod 8;\\ \frac{1}{8}(p+1), & \text{if } p\equiv 7 \bmod 8.\end{cases}
\end{aligned}\tag{7}$$

It is clear that Theorem 1 follows from Formulas (6) and (7). □

Proof of Theorem 2. If $p \equiv 1 \bmod 4$, then $a+\bar{a} \equiv 0 \bmod p$ has two solutions λ and $-\lambda$ with $\lambda \neq \pm 1$. Thus, note that $\left(\frac{-1}{p}\right)=1$; from the definition of $S(p,1)$ and the properties of the Legendre's symbol mod p, we have

$$\begin{aligned}
S(p,1) &= \frac{1}{8}\sum_{\substack{a=2\\(a+\bar{a},p)=1}}^{p-1}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+\bar{a}}{p}\right)\right)\left(1+\left(\frac{a-\bar{a}}{p}\right)\right)\\
&= \frac{p-5}{8}+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a}{p}\right)+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a+\bar{a}}{p}\right)+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a-\bar{a}}{p}\right)+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a^2-\bar{a}^2}{p}\right)\\
&\quad+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a^2+1}{p}\right)+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a^2-1}{p}\right)+\frac{1}{8}\sum_{a=2}^{p-2}\left(\frac{a}{p}\right)\left(\frac{a^2-\bar{a}^2}{p}\right)\\
&\quad-\frac{1}{4}\left(1+\left(\frac{\lambda}{p}\right)\right)\left(1+\left(\frac{2\lambda}{p}\right)\right)\\
&= \frac{p-7}{8}+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a+\bar{a}}{p}\right)+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a-\bar{a}}{p}\right)-\frac{1}{2}\left(\frac{2}{p}\right)+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a^2+1}{p}\right)
\end{aligned}$$

$$
\begin{aligned}
&+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a^2-1}{p}\right)+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(\frac{a^2-\bar{a}^2}{p}\right)+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a^4-1}{p}\right)\\
&-\frac{1}{4}\left(1+\left(\frac{\lambda}{p}\right)+\left(\frac{2\lambda}{p}\right)+\left(\frac{2}{p}\right)\right)\\
= &\ \frac{p-13}{8}+\frac{1}{8}\left(1+\left(\frac{\lambda}{p}\right)\right)\sum_{a=1}^{p-1}\left(\frac{a+\bar{a}}{p}\right)-\frac{3}{4}\left(\frac{2}{p}\right)+\frac{1}{8}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(\frac{a^4-1}{p}\right)\\
&-\frac{1}{4}\left(1+\left(\frac{2}{p}\right)\right)\left(\frac{\lambda}{p}\right)+\frac{1}{8}\sum_{a=1}^{p-1}\left(1+\left(\frac{a}{p}\right)\right)\left(\frac{a^2-1}{p}\right). \qquad (8)
\end{aligned}
$$

When $p=8k+5$, we have $\left(\frac{2}{p}\right)=\left(\frac{\lambda}{p}\right)=-1$; from Lemma 2, we have

$$
\begin{aligned}
&\left|\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(\frac{a^4-1}{p}\right)\right|+\left|\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(\frac{a^2-1}{p}\right)\right|\\
&\le 4\cdot\sqrt{p}+\left|\sum_{a=1}^{p-1}\left(\frac{a-\bar{a}}{p}\right)\right|\le 6\cdot\sqrt{p}. \qquad (9)
\end{aligned}
$$

Combining (8) and (9) and Lemma 1, we have the asymptotic formula

$$S(p,1)=\frac{1}{8}(p-9)+K(p,1), \qquad (10)$$

where $|K(p,1)|\le\frac{3}{4}\cdot\sqrt{p}$.

If $p=8k+1$, then $\left(\frac{2}{p}\right)=\left(\frac{\lambda}{p}\right)=1$; from (8) and (9), Lemmas 1 and 2, we have the asymptotic formula

$$S(p,1)=\frac{1}{8}(p-25)+K_1(p,1), \qquad (11)$$

where $|K_1(p,1)|\le\frac{5}{4}\cdot\sqrt{p}$.

On the other hand, note that the identity

$$
\begin{aligned}
S(p,-1)=&\ \frac{1}{8}\sum_{\substack{a=2\\(a+\bar{a},p)=1}}^{p-1}\left(1-\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+\bar{a}}{p}\right)\right)\left(1+\left(\frac{a-\bar{a}}{p}\right)\right)\\
=&\ \frac{1}{4}\sum_{\substack{a=2\\(a+\bar{a},p)=1}}^{p-1}\left(1+\left(\frac{a+\bar{a}}{p}\right)\right)\left(1+\left(\frac{a-\bar{a}}{p}\right)\right)-S(p,1)\\
=&\ \frac{p-5}{4}+\frac{1}{4}\sum_{a=1}^{p-1}\left(\frac{a+\bar{a}}{p}\right)+\frac{1}{4}\sum_{a=1}^{p-1}\left(\frac{a-\bar{a}}{p}\right)-\left(\frac{2}{p}\right)-\frac{1}{2}\\
&+\frac{1}{4}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(\frac{a^2-1}{p}\right)-S(p,1). \qquad (12)
\end{aligned}
$$

From (8)–(12), we have the asymptotic formulas

$$S(p,-1)=\begin{cases}\frac{1}{8}(p+3)+K(p,-1), & \text{if } p\equiv 5 \bmod 8;\\ \frac{1}{8}(p+3)+K_1(p,-1), & \text{if } p\equiv 1 \bmod 8,\end{cases} \qquad (13)$$

where $|K(p,-1)|\le\frac{3}{4}\cdot\sqrt{p}$ and $|K_1(p,-1)|\le\frac{5}{4}\cdot\sqrt{p}$.

It is clear that Theorem 2 follows from asymptotic Formulas (10), (11) and (13). □

To prove Corollary 2, we only require $S(p,1) > 0$. That is,

$$\frac{1}{8}(p-17) > \frac{5}{4} \cdot \sqrt{p}.$$

This inequality implies that $S(p,1) > 0$ for all primes $p > 144$.

It is easy to verify $S(p,1) > 0$ for all $101 \leq p \leq 143$ by simple calculation.

Thus, Zhiwei Sun's problem A is correct for all primes $p \geq 101$.

Similarly, we can also prove that the problem B is also correct for all primes $p \geq 18$. This completes the proofs of our all results.

5. Conclusions

The main results of this paper are two theorems. Theorem 1 establishes two exact formulas for $S(p,1)$ and $S(p,-1)$ with $p = 4k+3$. Theorem 2 establishes two asymptotic formulas for $S(p,1)$ and $S(p,-1)$ with $p = 4k+1$. At the same time, we give two sharp upper bound estimates for the error terms. As application, we obtain two conclusions as follows:

i For any prime $p \geq 101$, there is at least one integer a, such that a, $a+\bar{a}$ and $a-\bar{a}$ are all quadratic residues mod p.

ii For any prime $p \geq 18$, there is at least one quadratic non-residue a mod p, such that $a+\bar{a}$ and $a-\bar{a}$ are quadratic residues mod p.

Therefore, we solved two problems proposed by Zhiwei Sun.

Author Contributions: All authors have equally contributed to this work. All authors read and approved the final manuscript.

Funding: This research was funded by the Y. S. T. N. S. P (2019KJXX-076), the N. S. B. R. P. (2019JM-207) of Shaanxi Province and the N. S. F. (11771351) of P. R. China.

Acknowledgments: The authors would like to thank the referee for their very helpful and detailed comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Apostol, T.M. *Introduction to Analytic Number Theory*; Springer: New York, NY, USA, 1976.
2. Zhang, W.P.; Li, H.L. *Elementary Number Theory*; Shaanxi Normal University Press: Xi'an, China, 2013.
3. Burgess, D.A. The distribution of quadratic residues and non-residues. *Mathematika* **1957**, *4*, 106–112. [CrossRef]
4. Burgess, D.A. A note on the distribution of residues and non-residues. *J. Lond. Math. Soc.* **1963**, *38*, 253–256. [CrossRef]
5. Balister, P.; Bollobas, B.; Jonathan, L.D. A note on Linnik's theorem on quadratic non-residues. *Arch. Math.* **2019**, *112*, 371–375. [CrossRef]
6. Schinzel, A. Primitive roots and quadratic non-residues. *Acta Arith.* **2011**, *149*, 161–170. [CrossRef]
7. Yuk-Kam, L.; Jie, W. On the least quadratic non-residue. *Int. J. Number Theory* **2008**, *4*, 423–435.
8. Ankeny, N.C. The least quadratic non-residue. *Ann. Math.* **1952**, *55*, 65–72. [CrossRef]
9. Graham, S.W.; Ringerse, C.J. Lower bound for least quadratic non-residues. In *Aanlytic Number Theory: Proceedings of a Conference in Honor of P. T. Bateman*; Book Series: Progress in Mathematics; Birkhäuser Boston: Cambridge, MA, USA, 1990; Volume 85, pp 269–309.
10. Peralta, R. On the distribution of quadratic residues and non-residues nodulo a prime number. *Math. Comput.* **1992**, *58*, 433–440. [CrossRef]
11. Wright, S. Quadratic residues and non-residues in arithmetic progression. *J. Number Theory* **2013**, *133*, 2398–2430. [CrossRef]
12. Soydan, G.; Demirci, M.; Ikikardes, N.Y. On the additive structure of the set of quadratic residues modulo p. *Adv. Stud. Contemp. Math.* **2007**, *14*, 251–257.

13. Kohnen, W. An elementary proof in the theory of quadratic residues. *Bull. Korean Math. Soc.* **2008**, *45*, 273–275. [CrossRef]
14. Hummel, P. On consecutive quadratic non-residues: a conjecture of Issai Schur. *J. Number Theory* **2003**, *103*, 257–266. [CrossRef]
15. Garaev, M.Z. A note on the least quadratic non-residue of the integer-sequences. *Bull. Aust. Math. Soc.* **2003**, *68*, 1–11. [CrossRef]
16. Hudson, R.H. On sequences of consecutive quadratic nonresidues. *J. Number Theory* **1971**, *3*, 178–181. [CrossRef]
17. Weil, A. On some exponential sums. *Proc. Natl. Acad. Sci. USA* **1948**, *34* , 203–210. [CrossRef] [PubMed]