


Article

On the Quartic Residues and Their New Distribution Properties

Juanli Su ¹ and Jiafan Zhang ^{2,*} 

¹ Department of Arts and Sciences, Yangling Vocational and Technical College, Yangling 712100, China; alic0229@126.com

² Research Center for Number Theory and Its Applications, Northwest University, Xi'an 710127, China

* Correspondence: zhangjiafan@stumail.nwu.edu.cn

Received: 3 July 2020; Accepted: 10 August 2020; Published: 11 August 2020



Abstract: In this paper, we use the analytic methods, the properties of the fourth-order characters, and the estimate for character sums to study the computational problems of one kind of special quartic residues modulo p , and give an exact calculation formula and asymptotic formula for their counting functions.

Keywords: quartic residues; fourth-order character; Gauss sums; counting function; calculation formula; asymptotic formula

1. Introduction

Let p be an odd prime and $k \geq 2$ be an integer. For any integer a with $(a, p) = 1$, if the congruence equation $x^k \equiv a \pmod{p}$ has solution, then we call a is a k -th residue modulo p . Otherwise, a is called a k -th non-residue modulo p . If $k = 2$, then we call a quadratic residue or quadratic non-residue modulo p . Legendre first introduced the characteristic function of the quadratic residues $\left(\frac{a}{p}\right)$, which was later called Legendre's symbol. It is defined as follows:

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

In particular, we have $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ and the quadratic reciprocity law

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

where p and q are two different odd primes.

The study of k -th residues modulo p is one of the important pieces of content in elementary number theory and analytic number theory, and many number theory problems are closely related to them. Because of this, many scholars have been engaged in the research work in this field, and have made rich research results. It is worth mentioning that Sun Zhihong [1–5] has done a lot of profound research on the quartic residues; these bring us to the study of the distribution properties of various k -th residues modulo p . Some other papers related to quadratic residues and cubic residues modulo p can be found in references [6–18]. For example, recently, Wang Tingting and Lv Xingxing [6] studied the distribution properties of some special quadratic residues and non-residues modulo p , who obtained an exact calculation formula and a sharp asymptotic formula for its counting function.

As some applications, they solved two problems proposed by Sun Zhiwei. That is, they proved the following two interesting results:

(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 modulo p .

(B). For any prime $p \geq 18$, there is at least one quadratic non-residue $a \bmod p$, such that $a + \bar{a}$ and $a - \bar{a}$ are quadratic residues modulo p , where \bar{a} is defined as $a\bar{a} \equiv 1 \bmod p$.

As an extension of Wang Tingting and Lv Xingxing's work [6], a natural problem is the quartic residues modulo p . It is clear that, if $p \equiv 3 \bmod 4$, then the quadratic residue is the same as the quartic residue modulo p . In this time, the problem is trivial. Thus, we just consider the non-trivial case $p \equiv 1 \bmod 4$.

Let p be a prime with $p \equiv 1 \bmod 4$, and $N(p)$ denotes the number of all integers $1 < a < p - 1$ such that $a + \bar{a}$ and $a - \bar{a}$ are quartic residues modulo p .

In this paper, we will use the analytic methods, the properties of the classical Gauss sums, and the estimate for character sums to study the computational problems of $N(p)$, and give an exact calculation formula and asymptotic formula for it. That is, we will prove the following two results:

Theorem 1. Let p be an odd prime with $p \equiv 5 \bmod 8$, then we have

$$N(p) = \frac{1}{16} \cdot \left(p - 7 - 2 \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a + \bar{a}}{p} \right) \right).$$

Theorem 2. Let p be an odd prime with $p \equiv 1 \bmod 8$, then we have the identity

$$N(p) = \frac{1}{16} \cdot (p - 17) + E(p),$$

where we have the estimates $|E(p)| \leq \frac{15}{4} \cdot \sqrt{p}$.

From our theorems, we can also deduce the following two corollaries:

Corollary 1. Let p be an odd prime with $p \equiv 5 \bmod 8$, and then we have the congruence

$$p \equiv 7 + 2 \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a + \bar{a}}{p} \right) \bmod 16,$$

which implies that

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a + \bar{a}}{p} \right) \equiv \begin{cases} -1 \bmod 8, & \text{if } p \equiv 5 \bmod 16; \\ 3 \bmod 8, & \text{if } p \equiv 13 \bmod 16. \end{cases}$$

Corollary 2. Let $p > 3700$ be a prime with $p \equiv 1 \bmod 4$, then there exists at least one integer a such that $a + \bar{a}$ and $a - \bar{a}$ are quartic residues modulo p .

Some notes: Prior work gave us great inspiration for the research of this paper, but the methods we used is completely different from the methods in [6] or [1–5], where they all use elementary methods, so they can only get some qualitative results or asymptotic formulas. We used some analytic methods and the properties of the classical Gauss sums. Thus, an accurate calculation formula is obtained.

In addition, Corollary 2 is a very rough estimate deduced directly from our theorems. If we use some mathematical software, then the constant 3700 in Corollary 2 can be made much smaller.

2. Several Lemmas

In this section, we need to prove several simple lemmas. For ease of understanding, we first define the symbols that appear below: $\tau(\chi)$ denotes the classical Gauss sum

$$\tau(\chi) = \sum_{a=1}^q \chi(a) e\left(\frac{a}{q}\right)$$

where $q \geq 3$ is an integer, χ is any Dirichlet character mod q , and $e(y) = e^{2\pi i y}$.

λ denotes any fourth-order character mod p , which is $\lambda \neq \chi_0$, $\lambda^4 = \chi_0$.

$\chi_2 = \left(\frac{*}{p}\right)$ denotes the Legendre's symbol mod p .

The basic knowledge required in this section can also be found in references [19,20]. We will decompose the proofs of our theorems into the following several lemmas by means of the characteristic function of the fourth-order character λ mod p . In the end, we only deal with some estimate for a certain character sums or calculations for some special Gauss sums. First, we have:

Lemma 1. *Let p be a prime with $p \equiv 1 \pmod{4}$. Then, for any fourth-order character λ mod p , one has the identity*

$$\tau^2(\lambda) + \tau^2(\bar{\lambda}) = 2\sqrt{p} \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a+\bar{a}}{p}\right),$$

where $\left(\frac{*}{p}\right)$ denotes the Legendre's symbol mod p and $a\bar{a} \equiv 1 \pmod{p}$.

Proof. This result is Theorem 1 in Chen and Zhang [21]. \square

Lemma 2. *Let p be an odd prime with $p \equiv 5 \pmod{8}$. Then, for any fourth-order character λ mod p , we have the identity*

$$\sum_{a=1}^{p-1} \lambda(a^2 - \bar{a}^2) = \sum_{a=1}^{p-1} \bar{\lambda}(a^2 - \bar{a}^2) = 0$$

and

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

Proof. Note that $p \equiv 5 \pmod{8}$, $\chi_2 = \lambda^2 = \bar{\lambda}^2$ and $\lambda(-1) = -1$, so, from the properties of the Legendre's symbol and complete residue system mod p , we have

$$\begin{aligned} & \sum_{a=1}^{p-1} \lambda(a^2 - \bar{a}^2) = \sum_{a=1}^{p-1} \lambda(a - \bar{a}) + \sum_{a=1}^{p-1} \chi_2(a) \lambda(a - \bar{a}) \\ &= \sum_{a=1}^{p-1} \lambda(-a + \bar{a}) + \sum_{a=1}^{p-1} \lambda^2(a) \bar{\lambda}(a) \lambda(a^2 - 1) \\ &= -\sum_{a=1}^{p-1} \lambda(a - \bar{a}) + \sum_{a=1}^{p-1} \lambda(a) \lambda(a^2 - 1) = \sum_{a=1}^{p-1} \lambda(-a) \lambda((-a)^2 - 1) \\ &= -\sum_{a=1}^{p-1} \lambda(a) \lambda(a^2 - 1) = 0. \end{aligned} \tag{1}$$

Similarly, we can also deduce that

$$\sum_{a=1}^{p-1} \bar{\lambda}(a^2 - \bar{a}^2) = 0. \tag{2}$$

It is clear that the first formula in Lemma 2 follows from (1) and (2).

Now, we prove the second one. Note that $\tau(\chi_2) = \sqrt{p}$, $\lambda(-1) = -1$, $\lambda^2 = \bar{\lambda}^2 = \chi_2$, from Lemma 1, and the properties of Gauss sums, we have

$$\begin{aligned} \sum_{a=1}^{p-1} \left(\frac{a - \bar{a}}{p} \right) &= \sum_{a=1}^{p-1} \lambda^2(a) \chi_2(a^2 - 1) \\ &= \sum_{a=1}^{p-1} \lambda(a) \chi_2(a - 1) + \sum_{a=1}^{p-1} \lambda(a) \chi_2(a) \chi_2(a - 1) \\ &= \frac{1}{\sqrt{p}} \sum_{b=1}^{p-1} \chi_2(b) \sum_{a=1}^{p-1} \lambda(a) e \left(\frac{b(a-1)}{p} \right) + \frac{1}{\sqrt{p}} \sum_{b=1}^{p-1} \chi_2(b) \sum_{a=1}^{p-1} \bar{\lambda}(a) e \left(\frac{b(a-1)}{p} \right) \\ &= -\frac{1}{\sqrt{p}} \left(\tau^2(\lambda) + \tau^2(\bar{\lambda}) \right) = -2 \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a + \bar{a}}{p} \right) = -\sum_{a=1}^{p-1} \left(\frac{a + \bar{a}}{p} \right), \end{aligned}$$

or

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

This proves the second formula in Lemma 2. \square

Lemma 3. Let p be an odd prime with $p \equiv 5 \pmod{8}$. Then, we have the identity

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

Proof. Note that $\lambda^2 = \bar{\lambda}^2 = \chi_2$, from the method of proving Lemma 2, the properties of the Gauss sums and the Legendre's symbol mod p we have

$$\begin{aligned} \sum_{a=1}^{p-1} \left(\frac{a^2 - \bar{a}^2}{p} \right) &= \sum_{a=1}^{p-1} \chi_2(a - \bar{a}) + \sum_{a=1}^{p-1} \chi_2(a) \chi_2(a - \bar{a}) \\ &= \sum_{a=1}^{p-1} \lambda^2(a) \chi_2(a^2 - 1) + \sum_{a=1}^{p-1} \chi_2(a^2 - 1) \\ &= \sum_{a=1}^{p-1} \lambda(a) \chi_2(a - 1) + \sum_{a=1}^{p-1} \lambda(a) \chi_2(a) \chi_2(a - 1) + \sum_{a=0}^{p-1} \chi_2((a+1)^2 - 1) - 1 \\ &= -\frac{\tau^2(\lambda)}{\sqrt{p}} - \frac{\tau^2(\bar{\lambda})}{\sqrt{p}} + \sum_{a=1}^{p-1} \chi_2(a^2 + 2a) - 1 \\ &= -2 \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a + \bar{a}}{p} \right) + \sum_{a=1}^{p-1} \chi_2(1 + 2\bar{a}) - 1 = -2 \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a + \bar{a}}{p} \right) - 2. \end{aligned}$$

This proves Lemma 3. \square

Lemma 4. Let p be an odd prime with $p \equiv 5 \pmod{8}$. Then, we have the identity

$$\sum_{a=1}^{p-1} \chi_2(a + \bar{a}) \lambda(a - \bar{a}) = \sum_{a=1}^{p-1} \chi_2(a - \bar{a}) \lambda(a + \bar{a}) = 0.$$

Proof. Note that $\lambda(-1) = -1$, $\lambda^2 = \bar{\lambda}^2 = \chi_2$, and for any integer a with $(a, p) = 1$, we have $\chi_2(a) = \chi_2(\bar{a})$. Thus,

$$\begin{aligned} & \sum_{a=1}^{p-1} \chi_2(a + \bar{a}) \lambda(a - \bar{a}) = \sum_{a=1}^{p-1} \lambda^2(a) \chi_2(a^2 + 1) \bar{\lambda}(a) \lambda(a^2 - 1) \\ &= \sum_{a=1}^{p-1} \lambda(a) \chi_2(a^2 + 1) \lambda(a^2 - 1) = \sum_{a=1}^{p-1} \lambda(-a) \chi_2((-a)^2 + 1) \lambda((-a)^2 - 1) \\ &= - \sum_{a=1}^{p-1} \lambda(a) \chi_2(a^2 + 1) \lambda(a^2 - 1) = 0. \end{aligned} \quad (3)$$

Similarly, we can also deduce the identity

$$\sum_{a=1}^{p-1} \chi_2(a - \bar{a}) \lambda(a + \bar{a}) = 0. \quad (4)$$

From (3) and (4), we can deduce Lemma 4. \square

Lemma 5. Let p be an odd prime with $p \equiv 5 \pmod{8}$. Then, for any fourth-order character $\lambda \pmod{p}$, we have the identities

$$\sum_{a=1}^{p-1} \lambda(a - \bar{a}) \bar{\lambda}(a + \bar{a}) = \sum_{a=1}^{p-1} \lambda(a + \bar{a}) \bar{\lambda}(a - \bar{a}) = 0.$$

Proof. Note that $\lambda(-1) = -1$, from the properties of the reduced residue system modulo p , we have the identity

$$\begin{aligned} & \sum_{a=1}^{p-1} \lambda(a^2 + 1) \bar{\lambda}(a^2 - 1) = \sum_{a=1}^{p-1} \lambda(1 + \bar{a}^2) \bar{\lambda}(1 - \bar{a}^2) \\ &= \sum_{a=1}^{p-1} \lambda(1 + a^2) \bar{\lambda}(1 - a^2) = - \sum_{a=1}^{p-1} \lambda(a^2 + 1) \bar{\lambda}(a^2 - 1), \end{aligned}$$

which implies that

$$\sum_{a=1}^{p-1} \lambda(a^2 + 1) \bar{\lambda}(a^2 - 1) = 0. \quad (5)$$

From (5), we may immediately get

$$\sum_{a=1}^{p-1} \lambda(a + \bar{a}) \bar{\lambda}(a - \bar{a}) = \sum_{a=1}^{p-1} \lambda(a^2 + 1) \bar{\lambda}(a^2 - 1) = 0.$$

This proves Lemma 5. \square

Lemma 6. Let p be an odd prime with $p \equiv 5 \pmod{8}$. For any fourth-order character $\lambda \pmod{p}$, if $r + \bar{r} \equiv 0 \pmod{p}$, then

$$\left(1 + \lambda(2r) + \lambda^2(2r) + \bar{\lambda}(2r)\right) + \left(1 + \lambda(-2r) + \lambda^2(-2r) + \bar{\lambda}(-2r)\right) = 4.$$

Proof. Since $\lambda^3 = \bar{\lambda}$, $\lambda(-1) = -1$ and $\left(\frac{2}{p}\right) = \lambda^2(2) = \chi_2(2) = (-1)^{\frac{p^2-1}{8}} = -1$, note that $r^2 \equiv -1 \pmod{p}$ or $r^3 \equiv -r \pmod{p}$, we have

$$\begin{aligned}\lambda(2r) &= \lambda(2)\bar{\lambda}^3(r) = \lambda(2)\bar{\lambda}(r^3) = \lambda(2)\bar{\lambda}(-r) \\ &= \lambda(-1)\lambda^2(2)\bar{\lambda}(2r) = -\chi_2(2) \cdot \bar{\lambda}(2r) = \bar{\lambda}(2r).\end{aligned}$$

Therefore, $\lambda(2r)$ is a real number. However, $|\lambda(2r)| = 1$, and we must have $\lambda(2r) = 1$ or -1 .

If $\lambda(2r) = 1$, then we have $1 + \lambda(2r) + \lambda^2(2r) + \bar{\lambda}(2r) = 1 + 1 + 1 + 1 = 4$ and

$$1 + \lambda(-2r) + \lambda^2(-2r) + \bar{\lambda}(-2r) = 1 - 1 + 1 - 1 = 0.$$

If $\lambda(2r) = -1$, then we have $1 + \lambda(2r) + \lambda^2(2r) + \bar{\lambda}(2r) = 1 - 1 + 1 - 1 = 0$ and

$$1 + \lambda(-2r) + \lambda^2(-2r) + \bar{\lambda}(-2r) = 1 + 1 + 1 + 1 = 4.$$

This proves Lemma 6. \square

3. Proofs of the Theorems

In this section, we shall complete the proofs of our main results. First, we prove Theorem 1. For any prime p with $p \equiv 5 \pmod{8}$, there must exist an integer $1 < r < p - 1$ such that $r^2 \equiv -1 \pmod{p}$ or $r + \bar{r} \equiv 0 \pmod{p}$. Let λ denote any fourth-order character modulo p . Then, for any integer n with $(n, p) = 1$, we have the characteristic function:

$$1 + \lambda(n) + \lambda^2(n) + \lambda^3(n) = \begin{cases} 4, & \text{if } n \text{ is a quartic residue modulo } p; \\ 0, & \text{if } n \text{ is not a quartic residue modulo } p. \end{cases}$$

Since $\lambda(2) = \bar{\lambda}^3(2) = \chi_2(2)\bar{\lambda}(2) = -\bar{\lambda}(2)$ and $\chi_2(\pm 2) = -1$, from Lemma 6 and the definition of $N(p)$, we have

$$\begin{aligned}N(p) &= \frac{1}{16} \sum_{\substack{a=2 \\ (a^2+1,p)=1}}^{p-2} (1 + \lambda(a + \bar{a}) + \chi_2(a + \bar{a}) + \bar{\lambda}(a + \bar{a})) \\ &\quad \times (1 + \lambda(a - \bar{a}) + \chi_2(a - \bar{a}) + \bar{\lambda}(a - \bar{a})) \\ &= \frac{1}{16} \sum_{a=1}^{p-1} (1 + \lambda(a + \bar{a}) + \chi_2(a + \bar{a}) + \bar{\lambda}(a + \bar{a})) \\ &\quad \times (1 + \lambda(a - \bar{a}) + \chi_2(a - \bar{a}) + \bar{\lambda}(a - \bar{a})) - \frac{4}{16} \\ &= \frac{1}{16} \sum_{a=1}^{p-1} (\lambda(a + \bar{a}) + \bar{\lambda}(a + \bar{a}) + \bar{\lambda}(a - \bar{a}) + \lambda(a - \bar{a}) + 1) \\ &\quad + \frac{1}{16} \sum_{a=1}^{p-1} (\lambda(a + \bar{a})\lambda(a - \bar{a}) + \bar{\lambda}(a + \bar{a})\bar{\lambda}(a - \bar{a}) + \chi_2(a^2 - \bar{a}^2)) \\ &\quad + \frac{1}{16} \sum_{a=1}^{p-1} (\lambda(a + \bar{a})\bar{\lambda}(a - \bar{a}) + \bar{\lambda}(a + \bar{a})\lambda(a - \bar{a})) \\ &\quad + \frac{1}{16} \sum_{a=1}^{p-1} (\chi_2(a + \bar{a})\lambda(a - \bar{a}) + \chi_2(a + \bar{a})\bar{\lambda}(a - \bar{a})) \\ &\quad + \frac{1}{16} \sum_{a=1}^{p-1} (\lambda(a + \bar{a})\chi_2(a - \bar{a}) + \bar{\lambda}(a + \bar{a})\chi_2(a - \bar{a})) \\ &\quad + \frac{1}{16} \sum_{a=1}^{p-1} (\chi_2(a + \bar{a}) + \chi_2(a - \bar{a})) - \frac{4}{16}. \tag{6}\end{aligned}$$

If $p \equiv 5 \pmod{8}$, then note that

$$\sum_{a=1}^{p-1} (\lambda(a + \bar{a}) + \lambda(a - \bar{a}) + \bar{\lambda}(a + \bar{a}) + \bar{\lambda}(a - \bar{a})) = 0,$$

from (6), Lemma 2–Lemma 5, we have

$$\begin{aligned} N(p) &= \frac{p-1}{16} - \frac{1}{16} \left(2 + 2 \sum_{a=1}^{p-1} \left(\frac{a + \bar{a}}{p} \right) \right) - \frac{4}{16} \\ &= \frac{1}{16} \cdot \left(p - 7 - 2 \sum_{a=1}^{p-1} \left(\frac{a + \bar{a}}{p} \right) \right). \end{aligned}$$

This proves Theorem 1.

If p is a prime with $p \equiv 1 \pmod{8}$, then note that $\chi_2(\pm 2) = 1$, $\lambda(\pm 1) = 1$, $\lambda(r) = \bar{\lambda}(r)$ and $\lambda(2) = \bar{\lambda}(2)$, from (6), we have

$$\begin{aligned} N(p) &= \frac{1}{16} \sum_{\substack{a=2 \\ (a^2+1, p)=1}}^{p-2} (1 + \lambda(a + \bar{a}) + \chi_2(a + \bar{a}) + \bar{\lambda}(a + \bar{a})) \\ &\quad \times (1 + \lambda(a - \bar{a}) + \chi_2(a - \bar{a}) + \bar{\lambda}(a - \bar{a})) \\ &= \frac{1}{16} \sum_{a=1}^{p-1} (1 + \lambda(a + \bar{a}) + \chi_2(a + \bar{a}) + \bar{\lambda}(a + \bar{a})) \\ &\quad \times (1 + \lambda(a - \bar{a}) + \chi_2(a - \bar{a}) + \bar{\lambda}(a - \bar{a})) - \frac{1 + \lambda(2)}{4} - \frac{1 + 2\lambda(2r) + \chi_2(r)}{8}. \end{aligned} \quad (7)$$

Since, in this case, we can not get those formulas like Lemma 3–Lemma 5. In this time, we only use the trivial estimates (see Weil's work [22] or Bourgain et al. [23]):

$$\left| \sum_{a=1}^{p-1} \lambda(a^2 - \bar{a}^2) \right| = \left| \sum_{a=1}^{p-1} \chi_2(a) \lambda(a^4 - 1) \right| \leq 5 \cdot \sqrt{p}, \quad (8)$$

$$\left| \sum_{a=1}^{p-1} \lambda(a + \bar{a}) \bar{\lambda}(a - \bar{a}) \right| = \left| \sum_{a=1}^{p-1} \lambda(a^2 + 1) \bar{\lambda}(a^2 - 1) \right| \leq 4 \cdot \sqrt{p}, \quad (9)$$

$$\left| \sum_{a=1}^{p-1} \chi_2(a + \bar{a}) \lambda(a - \bar{a}) \right| = \left| \sum_{a=1}^{p-1} \lambda(a) \chi_2(a^2 + 1) \lambda(a^2 - 1) \right| \leq 5 \cdot \sqrt{p}, \quad (10)$$

$$\left| \sum_{a=1}^{p-1} \chi_2(a - \bar{a}) \lambda(a + \bar{a}) \right| = \left| \sum_{a=1}^{p-1} \lambda(a) \chi_2(a^2 - 1) \lambda(a^2 + 1) \right| \leq 5 \cdot \sqrt{p}, \quad (11)$$

$$\left| \sum_{a=1}^{p-1} \lambda(a \pm \bar{a}) \right| = \left| \sum_{a=1}^{p-1} \bar{\lambda}(a) \lambda(a^2 \pm 1) \right| \leq 3 \cdot \sqrt{p}, \quad (12)$$

$$\left| \sum_{a=1}^{p-1} \chi_2(a^2 - \bar{a}^2) \right| \leq 4 \cdot \sqrt{p}, \quad (13)$$

$$\left| \sum_{a=1}^{p-1} \chi_2(a \pm \bar{a}) \right| \leq 3 \cdot \sqrt{p}, \quad (14)$$

$$0 \leq 1 + \lambda(2) \leq 2, \quad (15)$$

$$0 \leq 1 + 2\lambda(2r) + \chi_2(r) \leq 4. \quad (16)$$

Combining (7)–(16) we have asymptotic formula

$$N(p) = \frac{1}{16} \cdot (p - 17) + E(p),$$

where $E(p)$ satisfies the estimate $|E(p)| \leq \frac{15}{4} \cdot \sqrt{p}$.

Now, we prove Corollary 1. Since $N(p) \geq 0$ is an integer, from Theorem 1, we have

$$p - 7 - 2 \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a + \bar{a}}{p} \right) \equiv 0 \pmod{16}$$

or

$$p \equiv 7 + 2 \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a + \bar{a}}{p} \right) \pmod{16}.$$

In order to prove Corollary 2, we just have to make sure that $N(p) > 0$. From Theorem 1 and Theorem 2, we just have the inequalities

$$N(p) = \frac{1}{16} \left(p - 7 - 2 \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a + \bar{a}}{p} \right) \right) > 0 \quad (17)$$

and

$$N(p) = \frac{1}{16} (p - 17) + E(p) > \frac{1}{16} (p - 17) - \frac{15}{4} \cdot \sqrt{p} > 0. \quad (18)$$

Note that, from the estimate

$$\left| \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a + \bar{a}}{p} \right) \right| \leq \sqrt{p},$$

we can get $p > 3700$ for solving inequalities (17) and (18).

This completes the proofs of our all results.

4. Conclusions

The main results of this paper are two theorems and two corollaries. For prime p with $p \equiv 5 \pmod{8}$, Theorem 1 of this paper gives an exact calculation formula for $N(p)$, which contains an interesting constant

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

This $\alpha(p)$ is closely related to prime p . In fact, we have (see [20]: Theorem 4–11)

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

where s denotes any quadratic non-residue modulo p .

We know very little about the arithmetic properties of $\alpha(p)$, or even its parity. Obviously, for any prime p with $p \equiv 5 \pmod{8}$, Corollary 1 gives for the first time a nontrivial congruence property of $\alpha(p)$.

For any prime p with $p \equiv 1 \pmod{8}$, we naturally ask the following two problems:

- (1). Whether there exists an exact computing formula for $N(p)$?
- (2). What is the residue of $\alpha(p) \pmod{8}$?

Interested readers are advised to study them with us.

Author Contributions: Methodology, J.Z.; Writing original draft, J.S.; Writing review and editing, J.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the N.S.F. (11771351) and the Natural Science Basic Research Project in Shaanxi Province (2017JK1002) of P.R. China.

Acknowledgments: The authors would like to thank the referees for their very helpful and detailed comments. The authors also express their heartfelt thanks to their supervisor Wenpeng Zhang for his very helpful and detailed suggestion.

Conflicts of Interest: The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Sun, Z.H. Cubic congruences and sums involving $\binom{3k}{k}$. *Int. J. Number Theory* **2016**, *12*, 143–164. [\[CrossRef\]](#)
2. Sun, Z.H. Quartic residues and sums involving $\binom{4k}{2k}$. *Taiwan. J. Math.* **2015**, *19*, 803–818. [\[CrossRef\]](#)
3. Sun, Z.H. Cubic residues and binary quadratic forms. *J. Number Theory* **2007**, *124*, 62–104. [\[CrossRef\]](#)
4. Sun, Z.H. Quartic residues and binary quadratic forms. *J. Number Theory* **2005**, *113*, 10–52. [\[CrossRef\]](#)
5. Sun, Z.H. Supplements to the theory of quartic residues. *Acta Arith.* **2001**, *97*, 361–377. [\[CrossRef\]](#)
6. Wang, T.T.; Lv, X.X. The quadratic residues and some of their new distribution properties. *Symmetry* **2020**, *12*, 241. [\[CrossRef\]](#)
7. Graham, S.W.; Ringerse, C.J. Lower bound for least quadratic non-residues. In *Analytic Number Theory: Proceedings of a Conference in Honor of P. T. Bateman*; Book Series: Progress in Mathematics; Birkhäuser: Boston, MA, USA, 1990; Volume 85, 269–309.
8. Peralta, R. On the distribution of quadratic residues and non-residues modulo a prime number. *Math. Comput.* **1992**, *58*, 433–440. [\[CrossRef\]](#)
9. Wright, S. Quadratic residues and non-residues in arithmetic progression. *J. Number Theory* **2013**, *133*, 2398–2430. [\[CrossRef\]](#)
10. Kohnen, W. An elementary proof in the theory of quadratic residues. *Bull. Korean Math. Soc.* **2008**, *45*, 273–275. [\[CrossRef\]](#)
11. Hummel, P. On consecutive quadratic non-residues: a conjecture of Issai Schur. *J. Number Theory* **2003**, *103*, 257–266. [\[CrossRef\]](#)
12. Garaev, M.Z. A note on the least quadratic non-residue of the integer-sequences. *Bull. Aust. Math. Soc.* **2003**, *68*, 1–11. [\[CrossRef\]](#)
13. Schinzel, A. Primitive roots and quadratic non-residues. *Acta Arith.* **2011**, *149*, 161–170. [\[CrossRef\]](#)
14. Yuk-Kam, L.; Jie, W. On the least quadratic non-residue. *Int. J. Number Theory* **2008**, *4*, 423–435.
15. Dummit, D.S.; Dummit, E.P.; Kisilevsky, H. Characterizations of quadratic, cubic, and quartic residue matrices. *J. Number Theory* **2016**, *168*, 167–179. [\[CrossRef\]](#)
16. Xing, D. S.; Cao, Z. F.; Dong, X. L. Identity based signature scheme based on cubic residues. *Sci.-China-Inf. Sci.* **2011**, *54*, 2001–2012. [\[CrossRef\]](#)

17. Su, W. L.; Li, Q.; Luo, H. P. Lower bounds of Ramsey numbers based on cubic residues. *Discret. Math.* **2002**, *250*, 197–209. [[CrossRef](#)]
18. Deng, M.J.; Gu, J. Application of quartic residue character theory to the Diophantine equation $a(x) + b(y) = c(z)$. *Bull. Math. Soc. Sci. Math. Roum.* **2019**, *62*, 133–139.
19. Apostol, T.M. *Introduction to Analytic Number Theory*; Springer: New York, NY, USA, 1976.
20. Zhang, W.P.; Li, H.L. *Elementary Number Theory*; Shaanxi Normal University Press: Xi'an, China, 2013.
21. Chen, Z.Y.; Zhang, W. P. On the fourth-order linear recurrence formula related to classical Gauss sums. *Open Math.* **2017**, *15*, 1251–1255.
22. Weil, A. On some exponential sums. *Proc. Natl. Acad. Sci. USA* **1948**, *34*, 203–210. [[CrossRef](#)] [[PubMed](#)]
23. Bourgain, J.; Garaev, M.Z.; Konyagin, S.V.; Shparlinski, I.E. On the hidden shifted power problem. *Siam J. Comput.* **2012**, *41*, 1524–1557. [[CrossRef](#)]



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).