Research Article

On the Sixth Residues and Some New Properties of Their Distribution

Juanli Su[1] **and Jin Zhang** ![ORCID][2]

[1]*Department of Arts and Sciences, Yangling Vocational and Technical College, Yangling, China*
[2]*School of Information Engineering, Xi'an University, Xi'an, Shaanxi, China*

Correspondence should be addressed to Jin Zhang; zhangjin@xawl.edu.cn

In this paper, we use the analytic methods, the properties of the sixth-order characters, and the classical Gauss sums to study the computational problems of a certain special sixth residues' modulo p and give two exact calculating formulas for them.

1. Introduction

Let p be an odd prime and k be a fixed positive integer. For any integer a with $(a, p) = 1$, if the congruence equation $x^k \equiv a \bmod p$ has a solution x, then we call a is a kth residue modulo p. Otherwise, a is called a kth nonresidue modulo p. In particular, if $k = 2$, 3, and 4, we call a is a quadratic residue, cubic residue, and quartic residue modulo p, respectively. Undoubtedly, the research of quadratic residue is the most concerned topic. Legendre first introduced the characteristic function of the quadratic residues (a/p) modulo p, which later was called Legendre's symbol. It is defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadraticre sidue modulo } p, \\ -1, & \text{if } a \text{ is a quadratic nonresidue modulo } p, \\ 0, & \text{if } p|a. \end{cases} \tag{1}$$

Sometimes, we write Legendre's symbol $(*/p)$ as χ_2 for the sake of writing. This is because the introduction of this function greatly facilitated the study of quadratic residue properties and promoted the development of elementary number theory and analytic number theory. This is especially true in the study of primes and related problems. For example, if p is a prime with $p \equiv 1 \bmod 4$, then one has (see Theorem 4–11 in [1])

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

where $\overline{a}$ denotes the inverse of a. That is, $a \cdot \overline{a} \equiv 1 \bmod p$, and $(rs/p) = -1$.

Of course, there are many papers involving quadratic residues and primes, so we cannot cover all of them. Those who are interested can refer to [2–9].

In this paper, we are concerned with the problem of whether the special integers $a + \overline{a}$ and $a - \overline{a}$ both are kth residues' modulo p. Let $N_k(p)$ denote the number of all integers $1 < a < p - 1$ such that $a + \overline{a}$ and $a - \overline{a}$ both are kth residues' modulo p. Then, how are the values of $N_k(p)$ distributed?

Very recently, some authors had studied the calculating problem of $N_k(p)$ and obtained a series of interesting results. For example, Wang and Lv [10] obtained the identity

$$N_2(p) = \begin{cases} \dfrac{1}{8}(p - 3), & \text{if } p \equiv 3 \bmod 8, \\ \dfrac{1}{8}(p - 7), & \text{if } p \equiv 7 \bmod 8. \end{cases} \tag{3}$$

Hu and Chen [11] proved the following result: let p be an odd prime with $p \equiv 7 \bmod 12$. If 2 is a cubic residue mod p, then one has the identity

$$N_3(p) = \frac{1}{9} \cdot (p + 4d - 11). \tag{4}$$

If 2 is not a cubic residue mod p, then one has the asymptotic formula

$$N_3(p) = \frac{1}{9} \cdot (p - 5) + E(p), \tag{5}$$

where d is defined in (7) and $E(p)$ satisfies the estimates $|E(p)| \leq (2/3) \cdot \sqrt{p}$.

Su and Zhang [12] considered the case $p \equiv 5 \bmod 8$ and proved the identity

$$N_4(p) = \frac{1}{16} \cdot \left(p - 7 - 2 \sum_{a=1}^{p-1/2} \left(\frac{a + \overline{a}}{p} \right) \right). \tag{6}$$

As an extension of [10–12], a natural problem is what about sixth residues modulo p? It is clear that if $(p-1, 6) = 2$, then the problem is trivial. That is, any quadratic residue a modulo p is a sixth residue modulo p. So, we just consider the nontrivial case $p \equiv 1 \bmod 6$. In this case, we know that there are two integers d and b such that the identity

$$4p = d^2 + 27 \cdot b^2, \tag{7}$$

where d is uniquely determined by $d \equiv 1 \bmod 3$ (see [13]).

And, it is clear from (7) that the value of $N_6(p)$ must be related to d and b.

In this paper, we will use the analytic methods, the properties of the classical Gauss sums, and the estimate for some special character sums to study the computational problems of $N_6(p)$ and give an exact calculating formula for it. That is, we will prove the following two results.

Theorem 1. *Let p be an odd prime with $p \equiv 7 \bmod 12$. If 2 is a cubic residue modulo p, then we have the identity*

$$N_6(p) = \frac{1}{36} \cdot (p + 4d - 11), \tag{8}$$

where d is the same as defined in (7).

Theorem 2. *Let p be an odd prime with $p \equiv 7 \bmod 12$. If 2 is not a cubic residue modulo p, then we have*

$$N_6(p) = \frac{1}{72} \cdot (2p + 5d - 10 + 9b)$$

$$\tag{9}$$

$$\text{or } \frac{1}{72} \cdot (2p + 5d - 10 - 9b).$$

From our theorems, we may immediately deduce the following two corollaries.

Corollary 1. *Let p be an odd prime with $p \equiv 7 \bmod 12$. If 2 is a cubic residue modulo p, then we have the congruence*

$$p + 4d \equiv 11 \bmod 36. \tag{10}$$

Corollary 2. *Let p be an odd prime with $p \equiv 7 \bmod 12$. If 2 is not a cubic residue modulo p, then we have the congruence*

$$2p + 5d \equiv 10 + 9b \bmod 72$$

$$\text{or } 2p + 5d \equiv 10 - 9b \bmod 72. \tag{11}$$

First, in Theorems 1 and 2, we must distinguish whether 3 is a cubic residue modulo p because of the need to calculate the character sums. In different cases, the values of character sums are different.

Second, if p is a prime with $p \equiv 1 \bmod 12$, then, for some character sums, we can only use Weil's classical work [14, 15] to get some upper bound estimates and we cannot get their exact values. So, in this case, we can only deduce a sharp asymptotic formula for $N_6(p)$. That is,

$$N_6(p) = \frac{1}{36} \cdot p + O\left(p^{1/2}\right). \tag{12}$$

Third, if p is an odd prime with $p \equiv 7 \bmod 12$ and 2 is not a cubic residue modulo p, then our Theorem 2 also obtained an exact calculating formula for $N_6(p)$, which is obviously better than the corresponding result in [11].

Of course, our Theorem 2 is flawed, and it presents two possibilities. How to determine its correct value is an interesting open problem.

Finally, if p is a prime with $p \equiv 7 \bmod 12$, then we know that 2 is a cubic residue modulo p if and only if $2 \mid d$. That is, d is an even number. Otherwise, d is an odd number. Especially for primes $p = 7, 19, 67, 79, 103, 139, 151$, after some simple calculations, we have $4 \times 7 = 1^2 + 27 \cdot 1^2$, $4 \times 19 = 7^2 + 27 \cdot 1^2$, $4 \times 67 = (-5)^2 + 27 \cdot 3^2$, $4 \times 79 = (-17)^2 + 27 \cdot 1^2$, $4 \times 103 = 13^2 + 27 \cdot 3^2$, $4 \times 139 = (-23)^2 + 27 \cdot 1^2$, and $4 \times 151 = 19^2 + 27 \cdot 3^2$. Since $N_6(p)$ is an integer, so applying Corollary 2, we can get the congruences: $2 \cdot 7 + 5 \cdot 1 \equiv 10 + 9 \cdot 1 \bmod 72$, $2 \cdot 19 + 5 \cdot 7 \equiv 10 - 9 \cdot 1 \bmod 72$, $2 \cdot 67 + 5 \cdot (-5) \equiv 10 + 9 \cdot 3 \bmod 72$, $2 \cdot 79 + 5 \cdot (-17) \equiv 10 - 9 \cdot 1 \bmod 72$, $2 \cdot 103 + 5 \cdot 13 \equiv 10 - 9 \cdot 3 \bmod 72$, $2 \cdot 139 + 5 \cdot (-23) \equiv 10 + 9 \cdot 1 \bmod 72$, and $2 \cdot 151 + 5 \cdot 19 \equiv 10 + 9 \cdot 3 \bmod 72$.

Now, we consider Legendre's symbol $(d + b/p)$. Note that $(1 + 1/7) = 1$, $(7 + 1/19) = -1$, $(-5 + 3/67) = 1$, $(-17 + 1/79) = -1$, $(13 + 3/103) = -1$, $(-23 + 1/139) = 1$, and $(19 + 3/151) = 1$. From the above congruences and these values, we have a reason to believe the following.

Conjecture. *Let p be an odd prime with $p \equiv 7 \bmod 12$. If 2 is not a cubic residue modulo p, then we have the identity*

$$N_6(p) = \frac{1}{72} \cdot \left(2p + 5d - 10 + \left(\frac{d + b}{p} \right) \cdot 9b \right). \tag{13}$$

2. Several Lemmas

In this section, we decompose the proofs of our theorems into the following several lemmas. For the sake of simplicity, the basic knowledge required in this section is not listed, and

only three necessary references [1, 16, 17] are provided here. First, we have the following.

Lemma 1. *Let p be an odd prime with $p \equiv 1 \bmod 3$. Then, for any third-order character λ modulo p (i.e., $\lambda \neq \chi_0$ and $\lambda^3 = \chi_0$, the principal character modulo p), we have the identity*

$$\tau^3(\lambda) + \tau^3(\overline{\lambda}) = dp, \tag{14}$$

where $4p = d^2 + 27 \cdot b^2$, d is uniquely determined by $d \equiv 1 \bmod 3$, $\tau(\lambda) = \sum_{a=1}^{p-1} \lambda(a)e(a/p)$ denotes the classical Gauss sums, and $e(y) = e^{2\pi i y}$.

Proof. For the proof of this lemma, see Zhang and Hu [18] or Berndt and Evans [19]. □

Lemma 2. *Let p be a prime with $p \equiv 1 \bmod 6$. Then, for any third-order character $\lambda \bmod p$ and sixth-order character $\psi = \chi_2 \lambda$ (i.e., $\psi^i \neq \chi_0$, $1 \leq i \leq 5$, and $\psi^6 = \chi_0$), we have the identity*

$$\tau(\psi) = \frac{\lambda(2) \cdot \tau(\chi_2) \cdot \tau^2(\overline{\lambda})}{p}. \tag{15}$$

Proof. From the properties of the Gauss sums and the reduced residue system modulo p, note that the identity

$$\sum_{a=0}^{p-1} e\left(\frac{ba^2}{p}\right) = 1 + \sum_{a=1}^{p-1}(1 + \chi_2(a))e\left(\frac{ba}{p}\right) = \chi_2(b) \cdot \tau(\chi_2), \tag{16}$$

and we have

$$\sum_{a=0}^{p-1} \chi_2 \lambda(a^2 - 1) = \frac{1}{\tau(\chi_2\overline{\lambda})} \sum_{b=1}^{p-1} \chi_2\overline{\lambda}(b) \sum_{a=0}^{p-1} e\left(\frac{b(a^2-1)}{p}\right)$$

$$= \frac{\tau(\chi_2)}{\tau(\chi_2\overline{\lambda})} \sum_{b=1}^{p-1} \chi_2(b)\overline{\lambda}(b)\chi_2(b)e\left(\frac{-b}{p}\right) = \frac{\tau(\chi_2) \cdot \tau(\overline{\lambda})}{\tau(\chi_2\overline{\lambda})}. \tag{17}$$

On the contrary, we also have

$$\sum_{a=0}^{p-1} \chi_2 \lambda(a^2 - 1) = \sum_{a=1}^{p-1} \chi_2 \lambda(a^2 + 2a)$$

$$= \frac{1}{\tau(\chi_2\overline{\lambda})} \sum_{b=1}^{p-1} \chi_2\overline{\lambda}(b) \sum_{a=1}^{p-1} \chi_2(a)\lambda(a)e\left(\frac{b(a+2)}{p}\right)$$

$$= \frac{\tau(\chi_2\lambda)}{\tau(\chi_2\overline{\lambda})} \sum_{b=1}^{p-1} \chi_2(b)\overline{\lambda}(b)\chi_2(b)\overline{\lambda}(b)e\left(\frac{2b}{p}\right)$$

$$= \frac{\overline{\lambda}(2) \cdot \tau(\chi_2\lambda) \cdot \tau(\lambda)}{\tau(\chi_2\overline{\lambda})}. \tag{18}$$

Note that identity $\tau(\lambda) \cdot \tau(\overline{\lambda}) = p$, and from (17) and (18), we deduce the identity

$$\tau(\chi_2\lambda) = \tau(\psi) = \frac{\lambda(2) \cdot \tau(\chi_2) \cdot \tau^2(\overline{\lambda})}{p}. \tag{19}$$

This proves Lemma 2. □

Lemma 3. *Let p be an odd prime with $p \equiv 7 \bmod 12$. Then, for any third-order character $\lambda \bmod p$, we have the identity*

$$\sum_{a=1}^{p-1}\left(\lambda(a^2 - \overline{a}^2) + \overline{\lambda}(a^2 - \overline{a}^2)\right) = \frac{1 + \lambda(2)}{p} \cdot \left(\tau^3(\lambda) + \overline{\lambda}(2) \cdot \tau^3(\overline{\lambda})\right). \tag{20}$$

Proof. Note that $\lambda^2 = \overline{\lambda}$, $\lambda(-1) = 1$, and $\chi_2(-1) = -1$, and from Lemma 2, properties of the Gauss sums, and Legendre's symbol $\bmod p$, we have

$$\sum_{a=1}^{p-1} \lambda(a^2 - \overline{a}^2) = \sum_{a=1}^{p-1} \overline{\lambda}^2(a)\lambda(a^4 - 1) = \sum_{a=1}^{p-1}(1 + \chi_2(a)) \cdot \overline{\lambda}(a)\lambda(a^2 - 1)$$

$$= \sum_{a=1}^{p-1} \overline{\lambda}(a)\lambda(a^2 - 1) + \sum_{a=1}^{p-1} \chi_2(-a) \cdot \overline{\lambda}(-a)\lambda((-a)^2 - 1)$$

$$= \sum_{a=1}^{p-1} \lambda^2(a)\lambda(a^2 - 1) = \sum_{a=1}^{p-1}(1 + \chi_2(a))\lambda(a)\lambda(a - 1)$$

$$= \frac{1}{\tau(\overline{\lambda})} \sum_{a=1}^{p-1} \lambda(a) \sum_{b=1}^{p-1} \overline{\lambda}(b)e\left(\frac{b(a-1)}{p}\right) + \frac{1}{\tau(\overline{\lambda})} \sum_{a=1}^{p-1} \psi(a) \sum_{b=1}^{p-1} \overline{\lambda}(b)e\left(\frac{b(a-1)}{p}\right)$$

$$= \frac{\tau^2(\lambda)}{\tau(\overline{\lambda})} - \frac{\tau^2(\psi)}{\tau(\overline{\lambda})} = \frac{\tau^3(\lambda)}{p} - \frac{\tau^2(\psi) \cdot \tau(\lambda)}{p} = \frac{\tau^3(\lambda) + \overline{\lambda}(2) \cdot \tau^3(\overline{\lambda})}{p}, \tag{21}$$

where we have used the identity $\tau^2(\chi_2) = \chi_2(-1) \cdot p = -p$.

Similarly, we can also deduce that

$$\sum_{a=1}^{p-1} \overline{\lambda}(a^2 - \overline{a}^2) = \frac{\tau^3(\overline{\lambda}) + \lambda(2) \cdot \tau^3(\lambda)}{p}. \quad (22)$$

It is clear that Lemma 3 follows from (21) and (22). □

Lemma 4. *Let p be an odd prime with $p \equiv 7 \bmod 12$. Then, we have the identity*

$$\sum_{a=1}^{p-1} (\lambda(a + \overline{a}) + \overline{\lambda}(a + \overline{a})) = \frac{(1 - \lambda(2)) \cdot \tau^3(\lambda) + (1 - \overline{\lambda}(2)) \cdot \tau^3(\overline{\lambda})}{p}. \quad (23)$$

Proof. From the methods of proving Lemma 2 and the properties of the Gauss sums, we have

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

$$= \sum_{a=1}^{p-1} (1 + \chi_2(a)) \cdot \lambda(a)\lambda(a + 1) = \frac{\tau^3(\lambda)}{p} + \frac{\tau^2(\chi_2\lambda) \cdot \tau(\lambda)}{p}$$

$$= \frac{\tau^3(\lambda)}{p} - \frac{\overline{\lambda}(2) \cdot \tau^3(\overline{\lambda})}{p}. \quad (24)$$

So, from (24), we have

$$\sum_{a=1}^{p-1} (\lambda(a + \overline{a}) + \overline{\lambda}(a + \overline{a}))$$

$$= \frac{\tau^3(\lambda)}{p} - \frac{\overline{\lambda}(2) \cdot \tau^3(\overline{\lambda})}{p} + \frac{\tau^3(\overline{\lambda})}{p} - \frac{\lambda(2) \cdot \tau^3(\lambda)}{p} \quad (25)$$

$$= \frac{(1 - \lambda(2)) \cdot \tau^3(\lambda) + (1 - \overline{\lambda}(2)) \cdot \tau^3(\overline{\lambda})}{p}.$$

This proves Lemma 4. □

Lemma 5. *Let p be an odd prime with $p \equiv 7 \bmod 12$. Then, we have*

$$\sum_{a=1}^{p-1} (\lambda(a - \overline{a}) + \overline{\lambda}(a - \overline{a})) = \frac{(1 + \lambda(2)) \cdot \tau^3(\lambda) + (1 + \overline{\lambda}(2)) \cdot \tau^3(\overline{\lambda})}{p}. \quad (26)$$

Proof. It is the same as the proof of Lemma 4, so it is omitted. □

Lemma 6. *Let p be an odd prime with $p \equiv 7 \bmod 12$. Then, we have the identities*

$$\sum_{a=1}^{p-1} \psi(a + \overline{a})\overline{\psi}(a - \overline{a}) = \sum_{a=1}^{p-1} \psi(a - \overline{a})\overline{\psi}(a + \overline{a}) = 0. \quad (27)$$

Proof. Note that $\psi(-1) = \overline{\psi}(-1) = -1$, and from the properties of the reduced residue system modulo p, we have

$$\sum_{a=1}^{p-1} \psi(a + \overline{a})\overline{\psi}(a - \overline{a}) = \sum_{a=1}^{p-1} \psi(a^2 + 1)\overline{\psi}(a^2 - 1)$$

$$= \sum_{a=1}^{p-1} \psi(\overline{a}^2 + 1)\overline{\psi}(\overline{a}^2 - 1)$$

$$= \sum_{a=1}^{p-1} \psi(a^2 + 1)\overline{\psi}(1 - a^2) \quad (28)$$

$$= -\sum_{a=1}^{p-1} \psi(a^2 + 1)\overline{\psi}(a^2 - 1)$$

$$= -\sum_{a=1}^{p-1} \psi(a + \overline{a})\overline{\psi}(a - \overline{a}),$$

which implies that

$$\sum_{a=1}^{p-1} \psi(a + \overline{a})\overline{\psi}(a - \overline{a}) = 0. \quad (29)$$

This proves Lemma 6. □

Lemma 7. *Let p be an odd prime with $p \equiv 7 \bmod 12$. For any sixth-order character $\psi \bmod p$, we have*

$$\sum_{a=1}^{p-1} \psi(a + \overline{a}) \cdot \chi_2(a - \overline{a}) = \sum_{a=1}^{p-1} \overline{\psi}(a + \overline{a}) \cdot \chi_2(a - \overline{a}) = 0,$$

$$\sum_{a=1}^{p-1} \psi(a - \overline{a}) \cdot \chi_2(a + \overline{a}) = \sum_{a=1}^{p-1} \overline{\psi}(a - \overline{a}) \cdot \chi_2(a + \overline{a}) = 0. \quad (30)$$

Proof. Since $\psi = \chi_2\lambda$, $\chi_2(-1) = -1$, so, from the reduced residue system modulo p, we have

$$\sum_{a=1}^{p-1} \psi(a + \overline{a}) \cdot \chi_2(a - \overline{a}) = \sum_{a=1}^{p-1} \overline{\lambda}(a)\psi(a^2 + 1) \cdot \chi_2(a^2 - 1)$$

$$= \sum_{a=1}^{p-1} \lambda(a)\psi(\overline{a}^2 + 1) \cdot \chi_2(\overline{a}^2 - 1)$$

$$= \sum_{a=1}^{p-1} \lambda^2(a)\psi(a^2 + 1) \cdot \chi_2(1 - a^2)$$

$$= -\sum_{a=1}^{p-1} \overline{\lambda}(a)\psi(a^2 + 1) \cdot \chi_2(a^2 - 1)$$

$$= -\sum_{a=1}^{p-1} \psi(a + \overline{a}) \cdot \chi_2(a - \overline{a}), \quad (31)$$

which implies that

$$\sum_{a=1}^{p-1} \psi(a+\overline{a}) \cdot \chi_2(a-\overline{a}) = 0. \tag{32}$$

Similarly, we can also deduce the identity

$$\sum_{a=1}^{p-1} \psi(a-\overline{a}) \cdot \chi_2(a+\overline{a}) = 0. \tag{33}$$

This proves Lemma 7. $\qquad\square$

Lemma 8. *Let p be an odd prime with $p \equiv 7 \bmod 12$. Then, for any third-order character $\lambda \bmod p$ and $\psi = \chi_2\lambda$, we have*

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

$$\sum_{a=1}^{p-1} \psi(a-\overline{a}) \cdot \lambda(a+\overline{a}) = \sum_{a=1}^{p-1} \psi(a-\overline{a}) \cdot \overline{\lambda}(a+\overline{a}) = 0. \tag{34}$$

Proof. Note that $\lambda(-1) = 1$ and $\psi(-1) = -1$, we have

$$\sum_{a=1}^{p-1} \psi(a+\overline{a}) \cdot \lambda(a-\overline{a}) = \sum_{a=1}^{p-1} \psi(-a-\overline{a}) \cdot \lambda(-a+\overline{a}) \tag{35}$$

$$= -\sum_{a=1}^{p-1} \psi(a+\overline{a}) \cdot \lambda(a-\overline{a}).$$

So, we have the identity

$$\sum_{a=1}^{p-1} \psi(a+\overline{a}) \cdot \lambda(a-\overline{a}) = 0. \tag{36}$$

Similarly, we can also deduce the identity

$$\sum_{a=1}^{p-1} \psi(a-\overline{a}) \cdot \lambda(a+\overline{a}) = 0. \tag{37}$$

This proves Lemma 8. $\qquad\square$

Lemma 9. *Let p be an odd prime with $p \equiv 7 \bmod 12$. Then, for any third-order character $\lambda \bmod p$, we have*

$$\sum_{a=1}^{p-1} (\lambda(a+\overline{a}) \cdot \overline{\lambda}(a-\overline{a}) + \overline{\lambda}(a+\overline{a}) \cdot \lambda(a-\overline{a})) = -4. \tag{38}$$

Proof. From the properties of Legendre's symbol $\bmod p$, we have

$$\sum_{a=1}^{p-1} \lambda(a+\overline{a}) \cdot \overline{\lambda}(a-\overline{a}) = \sum_{a=1}^{p-1} \lambda(a^2+1) \cdot \overline{\lambda}(a^2-1)$$

$$= \sum_{a=1}^{p-1} (1+\chi_2(a))\lambda(a+1) \cdot \overline{\lambda}(a-1)$$

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

$$= -1 + \sum_{a=1}^{p-1} \lambda(a+2) \cdot \overline{\lambda}(a) - \sum_{a=1}^{p-1} \chi_2(a)\lambda(a-1) \cdot \overline{\lambda}(a+1)$$

$$= -1 + \sum_{a=1}^{p-1} \lambda(1+2 \cdot \overline{a}) - \sum_{a=1}^{p-1} \chi_2(a)\lambda(a-1) \cdot \overline{\lambda}(a+1)$$

$$= -2 + \sum_{a=0}^{p-1} \lambda(1+2 \cdot a) - \sum_{a=1}^{p-1} \chi_2(a)\lambda(a-1) \cdot \overline{\lambda}(a+1)$$

$$= -2 - \sum_{a=1}^{p-1} \chi_2(a)\lambda(a-1) \cdot \overline{\lambda}(a+1). \tag{39}$$

Similarly, we also have

$$\sum_{a=1}^{p-1} \overline{\lambda}(a+\overline{a}) \cdot \lambda(a-\overline{a}) = \sum_{a=1}^{p-1} \overline{\lambda}(a^2+1) \cdot \lambda(a^2-1)$$

$$= \sum_{a=1}^{p-1} (1+\chi_2(a))\overline{\lambda}(a+1) \cdot \lambda(a-1)$$

$$= -2 + \sum_{a=1}^{p-1} \chi_2(a)\overline{\lambda}(a+1) \cdot \lambda(a-1). \tag{40}$$

Combining (39) and (40), we have the identity

$$\sum_{a=1}^{p-1} (\lambda(a+\overline{a}) \cdot \overline{\lambda}(a-\overline{a}) + \overline{\lambda}(a+\overline{a}) \cdot \lambda(a-\overline{a})) = -4. \tag{41}$$

This proves Lemma 9. $\qquad\square$

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 $p \equiv 7 \bmod 12$, let λ denote a third-order character modulo p; then, $\psi = \chi_2\lambda$ is a sixth-order character modulo p. So, for any integer a with $(a, p) = 1$, from the characteristic function

$$1 + \psi(a) + \psi^2(a) + \psi^3(a) + \overline{\psi}^2(a) + \overline{\psi}(a) = \begin{cases} 6, & \text{if } a \text{ is a sixth residue modulo p,} \\ 0, & \text{if } a \text{ is not a sixth residue modulo p,} \end{cases} \tag{42}$$

and note that $\psi^2 = \overline{\lambda}$, $\psi^3 = \chi_2$, $\chi_2(-1) = -1$, $\lambda(-1) = 1$, $\psi(-1) = -1$, and $(a^2+1, p) = 1$, and we have the identity

$$N_6(p) = \frac{1}{36} \sum_{a=2}^{p-2} \left(1 + \psi(a + \overline{a}) + \overline{\lambda}(a + \overline{a}) + \chi_2(a + \overline{a}) + \lambda(a + \overline{a}) + \overline{\psi}(a + \overline{a})\right)$$

$$\times \left(1 + \psi(a - \overline{a}) + \overline{\lambda}(a - \overline{a}) + \chi_2(a - \overline{a}) + \lambda(a - \overline{a}) + \overline{\psi}(a - \overline{a})\right)$$

$$= \frac{1}{36} \sum_{a=1}^{p-1} \left(1 + \psi(a + \overline{a}) + \overline{\lambda}(a + \overline{a}) + \chi_2(a + \overline{a}) + \lambda(a + \overline{a}) + \overline{\psi}(a + \overline{a})\right)$$

$$\times \left(1 + \psi(a - \overline{a}) + \overline{\lambda}(a - \overline{a}) + \chi_2(a - \overline{a}) + \lambda(a - \overline{a}) + \overline{\psi}(a - \overline{a})\right) - \frac{1}{18} \cdot (1 + \lambda(2) + \overline{\lambda}(2))$$

$$= \frac{p-1}{36} + \frac{1}{36} \sum_{a=1}^{p-1} \left(\psi(a + \overline{a}) + \overline{\lambda}(a + \overline{a}) + \chi_2(a + \overline{a}) + \lambda(a + \overline{a}) + \overline{\psi}(a + \overline{a})\right)$$

$$+ \frac{1}{36} \sum_{a=1}^{p-1} \left(\psi(a - \overline{a}) + \overline{\lambda}(a - \overline{a}) + \chi_2(a - \overline{a}) + \lambda(a - \overline{a}) + \overline{\psi}(a - \overline{a})\right)$$

$$+ \frac{1}{36} \sum_{a=1}^{p-1} \left(\psi(a^2 - \overline{a}^2) + \overline{\lambda}(a^2 - \overline{a}^2) + \chi_2(a^2 - \overline{a}^2) + \lambda(a^2 - \overline{a}^2) + \overline{\psi}(a^2 - \overline{a}^2)\right) \qquad (43)$$

$$+ \frac{1}{36} \sum_{a=1}^{p-1} \psi(a + \overline{a}) \left(\overline{\lambda}(a - \overline{a}) + \chi_2(a - \overline{a}) + \lambda(a - \overline{a}) + \overline{\psi}(a - \overline{a})\right)$$

$$+ \frac{1}{36} \sum_{a=1}^{p-1} \overline{\lambda}(a + \overline{a}) \left(\psi(a - \overline{a}) + \lambda(a - \overline{a}) + \chi_2(a - \overline{a}) + \overline{\psi}(a - \overline{a})\right)$$

$$+ \frac{1}{36} \sum_{a=1}^{p-1} \chi_2(a + \overline{a}) \left(\psi(a - \overline{a}) + \overline{\lambda}(a - \overline{a}) + \lambda(a - \overline{a}) + \overline{\psi}(a - \overline{a})\right)$$

$$+ \frac{1}{36} \sum_{a=1}^{p-1} \lambda(a + \overline{a}) \left(\psi(a - \overline{a}) + \overline{\lambda}(a - \overline{a}) + \chi_2(a - \overline{a}) + \overline{\psi}(a - \overline{a})\right)$$

$$+ \frac{1}{36} \sum_{a=1}^{p-1} \overline{\psi}(a + \overline{a}) \left(\psi(a - \overline{a}) + \overline{\lambda}(a - \overline{a}) + \chi_2(a - \overline{a}) + \lambda(a - \overline{a})\right)$$

$$- \frac{1}{18} \cdot (1 + \lambda(2) + \overline{\lambda}(2)).$$

Note that $p \equiv 7 \bmod 12$ and $\chi_2(-1) = -1$, so we have

$$\sum_{a=1}^{p-1} \psi(a \pm \overline{a}) = \sum_{a=1}^{p-1} \overline{\psi}(a \pm \overline{a}) = \sum_{a=1}^{p-1} \chi_2(a \pm \overline{a}) = 0, \qquad (44)$$

$$\sum_{a=1}^{p-1} \psi(a^2 - \overline{a}^2) = \sum_{a=1}^{p-1} \overline{\psi}(a^2 - \overline{a}^2) = \sum_{a=1}^{p-1} \chi_2(a^2 - \overline{a}^2) = 0. \qquad (45)$$

From Lemma 1, 4, and 5, we have

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

$$= \frac{2}{p} \cdot \left(\tau^3(\lambda) + \tau^3(\overline{\lambda})\right) = 2d. \qquad (46)$$

Now, if 2 is a cubic residue modulo p, then $1 + \lambda(2) + \overline{\lambda}(2) = 3$. Combining (43)–(46), Lemma 3, and Lemma 6–9, we have

$$N_6(p) = \frac{p-1}{36} + \frac{1}{36} \cdot (2d + 2d - 4) - \frac{3}{18} = \frac{1}{36} \cdot (p + 4d - 11). \tag{47}$$

This proves Theorem 1.

Now, we prove Theorem 2. If 2 is not a cubic residue modulo p, then $1 + \lambda(2) + \overline{\lambda}(2) = 0$. That is to say,

$$\lambda(2) = -\frac{1}{2} \pm \frac{\sqrt{3}}{2} \cdot i, \tag{48}$$

$$\overline{\lambda}(2) = -\frac{1}{2} \mp \frac{\sqrt{3}}{2} \cdot i,$$

where $i^2 = -1$.

In this case, from Lemma 1, we have

$$
\begin{aligned}
&\left(\tau^3(\lambda) - \tau^3(\overline{\lambda})\right)^2 \\
&= d^2 \cdot p^2 - 4p^3 \\
&= -p^2 \cdot \left(4p - d^2\right) = -27 \cdot p^2 \cdot b^2,
\end{aligned} \tag{49}
$$

or

$$\tau^3(\lambda) - \tau^3(\overline{\lambda}) = \pm 3 \cdot \sqrt{3} \cdot p \cdot b \cdot i. \tag{50}$$

From (48), (50), and Lemma 3, we have

$$
\begin{aligned}
&\sum_{a=1}^{p-1}\left(\lambda\left(a^2 - \overline{a}^2\right) + \overline{\lambda}\left(a^2 - \overline{a}^2\right)\right) \\
&= \frac{1 + \lambda(2)}{p} \cdot \left(\tau^3(\lambda) + \overline{\lambda}(2) \cdot \tau^3(\overline{\lambda})\right) \\
&= -\frac{1}{p} \cdot \left(\overline{\lambda}(2) \cdot \tau^3(\lambda) + \lambda(2) \cdot \tau^3(\overline{\lambda})\right) \\
&= \frac{1}{2p} \cdot (pd \pm 9 \cdot p \cdot b) = \frac{1}{2} \cdot (d \pm 9b).
\end{aligned} \tag{51}
$$

Combining (43)–(46), (51), and Lemma 6–9, we have

$$
\begin{aligned}
N_6(p) &= \frac{p-1}{36} + \frac{1}{36} \cdot (2d - 4) + \frac{1}{72} \cdot (d + 9b) \\
&= \frac{1}{72} \cdot (2p + 5d - 10 + 9b),
\end{aligned} \tag{52}
$$

or

$$
\begin{aligned}
N_6(p) &= \frac{p-1}{36} + \frac{1}{36} \cdot (2d - 4) + \frac{1}{72} \cdot (d - 9b) \\
&= \frac{1}{72} \cdot (2p + 5d - 10 - 9b).
\end{aligned} \tag{53}
$$

This completes the proofs of our all results.

4. Conclusion

The main results of this paper are two theorems and two corollaries. Theorem 1 gives an exact computing formula for

$N_6(p)$ with $p \equiv 7 \bmod 12$ and 2 is a cubic residue modulo p. If $p \equiv 7 \bmod 12$ and 2 is not a cubic residue modulo p, then Theorem 2 established an identity for $N_6(p)$ and there are two possibilities. As some applications of these theorems, we also deduced two interesting congruences. For example, one of them is

$$p + 4d \equiv 11 \bmod 36, \tag{54}$$

where $p \equiv 7 \bmod 12$ and 2 is a cubic residue modulo p.

In addition, if $p \equiv 7 \bmod 12$ and 2 is not a cubic residue modulo p, then we also have an interesting conjecture. That is,

$$N_6(p) = \frac{1}{72} \cdot \left(2p + 5d - 10 + \left(\frac{d+b}{p}\right) \cdot 9b\right). \tag{55}$$

Data Availability

No data were used to support the findings of the study.

Conflicts of Interest

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

Authors' Contributions

All authors contributed equally to this work. All authors read and approved the final manuscript.

Acknowledgments

References

[1] W. P. Zhang and H. L. Li, *Elementary Number Theory*, Shaanxi Normal University Press, Xi'an, China, 2008.

[2] S. W. Graham and C. J. Ringerse, *Aanlytic Number Theory: Proceedings of a Conference in Honor of P. T. Bateman, Book Series: Progress in Mathematics*, Springer Nature, Cham, Switzerland, 1990.

[3] R. é. Peralta, "On the distribution of quadratic residues and nonresidues modulo a prime number," *Mathematics of Computation*, vol. 58, no. 197, pp. 433–440, 1992.

[4] S. Wright, "Quadratic residues and non-residues in arithmetic progression," *Journal of Number Theory*, vol. 133, no. 7, pp. 2398–2430, 2013.

[5] W. Kohnen, "An elementary proof in the theory of quadratic residues," *Bulletin of the Korean Mathematical Society*, vol. 45, no. 2, pp. 273–275, 2008.

[6] P. Hummel, "On consecutive quadratic non-residues: a conjecture of Issai Schur," *Journal of Number Theory*, vol. 103, no. 2, pp. 257–266, 2003.

[7] M. Z. Garaev, "A note on the least quadratic non-residue of the integer-sequences," *Bulletin of the Australian Mathematical Society*, vol. 68, no. 1, pp. 1–11, 2003.

[8] A. Schinzel, "Primitive roots and quadratic non-residues," *Acta Arithmetica*, vol. 149, no. 2, pp. 161–170, 2011.

[9] Y.-K. Lau and J. Wu, "On the least quadratic non-residue," *International Journal of Number Theory*, vol. 04, no. 03, pp. 423–435, 2008.

[10] T. T. Wang and X. X. Lv, "The quadratic residues and some of their new distribution properties," *Symmetry*, vol. 12, p. 241, 2020.

[11] J. Y. Hu and Z. Y. Chen, "On distribution properties of cubic residues," *AIMS Mathematics*, vol. 5, pp. 6051–6060, 2020.

[12] J. Su and J. Zhang, "On the quartic residues and their new distribution properties," *Mathematics*, vol. 8, no. 8, p. 1337, 2020.

[13] S. Chowla, J. Cowles, and M. Cowles, "On the number of zeros of diagonal cubic forms," *Journal of Number Theory*, vol. 9, no. 4, pp. 502–506, 1977.

[14] A. Weil, *Basic Number Theory*, Springer-Verlag, New York, NY, USA, 1974.

[15] A. Weil, "On some exponential sums," *Proceedings of the National Academy of Sciences of the USA*, vol. 34, pp. 203–210, 1948.

[16] M. Tom, *Apostol, Introduction to Analytic Number Theory*, Springer-Verlag, New York, NY USA, 1976.

[17] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, NY, USA, 1982.

[18] W. P. Zhang and J. Y. Hu, "The number of solutions of the diagonal cubic congruence equation mod p," *Mathematical Reports*, vol. 20, pp. 70–76, 2018.

[19] B. C. Berndt and R. J. Evans, "The determination of Gauss sums," *Bulletin of the American Mathematical Society*, vol. 5, no. 2, pp. 107–130, 1981.