AIMS Mathematics, 5(6): 6051–6060.
DOI:10.3934/math.2020388
Received: 09 April 2020
Accepted: 15 July 2020
Published: 23 July 2020

http://www.aimspress.com/journal/Math

Research article

On distribution properties of cubic residues

Hu Jiayuan[1] **and Chen Zhuoyu**[2,*]

[1] Department of Mathematics and Computer Science, Hetao College, Bayannur, P. R. China
[2] School of Mathematics, Northwest University, Xi'an, Shaanxi, P. R. China

* **Correspondence:** Email: chenzymath@163.com.

Abstract: In this paper, we use the elementary methods, the properties of the Gauss sums and the estimate for character sums to study the calculating problems of a certain cubic residues modulo p, and give some interesting identities and asymptotic formulas for their counting functions.

Keywords: cubic residues; third-order character; Gauss sums; identity; asymptotic formula
Mathematics Subject Classification:11A15, 11L40

1. Introduction

Let p be an odd prime, and a be an integer with $(a, p) = 1$. In order to study of the properties of quadratic residues modulo p, Legendre first introduced the characteristic function of the quadratic residues $\left(\frac{a}{p}\right)$, which was later called Legendre's symbol as follows:

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

The introduction of this symbol greatly promotes the research about the properties of the quadratic residues and non-residues modulo p. Therefore, a great number of scholars began to study related work and obtained a series of valuable research results. For example, if p be an odd prime with $p = 4k + 1$, then for any quadratic residue r and quadratic non-residue s modulo p, one has the identity (see [2]: Theorem 4–11)

$$\left(\frac{1}{2}\sum_{a=1}^{p-1}\left(\frac{a + ra^{-1}}{p}\right)\right)^2 + \left(\frac{1}{2}\sum_{a=1}^{p-1}\left(\frac{a + sa^{-1}}{p}\right)\right)^2 = p,$$

where a^{-1} is the inverse of a mod p. In detail, a^{-1} satisfy the equation $x \cdot a \equiv 1 \bmod p$.

Many other papers related to power residues and non-residues modulo p can also be found in references [4–20], here we will not describe it in detail.

Recently, Wang Tingting and Lv Xingxing [5] studied the distribution properties of a certain quadratic residues and non-residues modulo p, and proved the following two conclusions:

Theorem A. For any prime p with $p \equiv 3 \bmod 4$, one has the identities

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

and

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

where $N(p,1)$ denotes the number of all integers $1 \le a \le p-1$ such that a, $a+a^{-1}$ and $a-a^{-1}$ are all quadratic residues modulo p, $N(p,-1)$ denotes the number of all integers $1 \le a \le p-1$ such that a is a quadratic non-residue modulo p, $a+a^{-1}$ and $a-a^{-1}$ are quadratic residues modulo p.

Theorem B. For any prime p with $p \equiv 1 \bmod 4$, one has the asymptotic formulas

$$N(p,1) = \begin{cases} \frac{1}{8}(p-3) + E(p,1), & \text{if } p \equiv 5 \bmod 8; \\ \frac{1}{8}(p-17) + E_1(p,1), & \text{if } p \equiv 1 \bmod 8 \end{cases}$$

and

$$N(p,-1) = \begin{cases} \frac{1}{8}(p+3) + E(p,-1), & \text{if } p \equiv 5 \bmod 8; \\ \frac{1}{8}(p+3) + E_1(p,-1), & \text{if } p \equiv 1 \bmod 8, \end{cases}$$

where we have the estimates $|E(p,1)| \le \frac{3}{4} \cdot \sqrt{p}$, $|E_1(p,1)| \le \frac{5}{4} \cdot \sqrt{p}$, $|E(p,-1)| \le \frac{3}{4} \cdot \sqrt{p}$ and $|E_1(p,-1)| \le \frac{5}{4} \cdot \sqrt{p}$.

As two corollaries of these results, Wang Tingting and Lv Xingxing [5] solved two open problems proposed by professor Sun Zhiwei. That is, they proved:

For any prime $p \ge 101$, there is at least one integer a, such that a, $a+a^{-1}$ and $a-a^{-1}$ are all quadratic residues modulo p.

For any prime $p \ge 18$, there is at least one quadratic non-residue $a \bmod p$, such that $a+a^{-1}$ and $a-a^{-1}$ are quadratic residues modulo p.

In the field of the quadratic residues research, it is worth mentioning Z. H. Sun's important work [6]. We believe that Theorem A and B can also be derived from earlier results in [6]. All research works are very meaningful. In fact, the distribution of power residues plays an vital role in mathematics and cryptography, a number of important number theory and information security problems are closely related to it. A survey on this can be found in F. L. Ţiplea, S. Iftene, G. Teşeleanu, A. M. Nica [10]. Therefore, it is necessary to continue to study the distribution properties of the power residues.

Inspired by the works in [5] and [6], we will naturally ask that what happens to the cubic residues modulo p?

It is clear that if $(p-1,3) = 1$, then for any integer a with $(a,p) = 1$, the congruence equation $x^3 \equiv a \bmod p$ has one solution. So it is a trivial situation in the condition of $(p-1,3) = 1$. But if $p \equiv 1 \bmod 3$, then what happens?

This paper focuses on such problems. Let p be a prime with $p \equiv 1 \bmod 3$, and $N(p)$ denotes the number of all integers $1 < a < p-1$ such that $a + a^{-1}$ and $a - a^{-1}$ are cubic residues modulo p. In this paper, using the elementary methods, the properties of the third-order characters and Gauss sums, and the estimate for character sums, we are going to give an exact identity and some asymptotic formulas for $N(p)$. Our main results are summarized as following three conclusions:

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

$$N(p) = \frac{1}{9} \cdot (p + 4d - 11),$$

where d is uniquely determined by $4p = d^2 + 27b^2$ and $d \equiv 1 \bmod 3$.

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

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

where we have the estimates $|E(p)| \leq \frac{2}{3} \cdot \sqrt{p}$.

Theorem 3. Let p be an odd prime with $p \equiv 1 \bmod 12$, then we have the asymptotic formula

$$N(p) = \begin{cases} \frac{1}{9} \cdot (p - 13) + E_1(p), & \text{if 2 is a cubic residue mod } p; \\ \frac{1}{9} \cdot (p - 1) + E_1(p), & \text{if 2 is not a cubic residue mod } p. \end{cases}$$

where we have the estimates $|E_1(p)| < \frac{26}{9} \cdot \sqrt{p}$.

According to our theorems, we can deduce the following:

Corollary. Let $p > 700$ be a prime with $p \equiv 1 \bmod 3$, then there exists at least one integer $1 < a < p-1$ such that $a + a^{-1}$ and $a - a^{-1}$ are cubic residues mod p.

2. Several lemmas

To prove our main results, we need following several basic lemmas. For simplicity, there is no need to repeat some elementary knowledge of number theory and analytic number theory, which can be found in references [1–3].

Lemma 1. Let p be a prime with $p \equiv 1 \bmod 3$. Then for any third-order character $\lambda \bmod p$, we have the identity

$$\tau^3(\lambda) + \tau^3\left(\overline{\lambda}\right) = dp,$$

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

Proof. This result is Theorem 1 in Zhang Wenpeng and Hu Jiayuan [21].

Lemma 2. 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

$$\sum_{a=1}^{p-1} \lambda\left(a + a^{-1}\right) \overline{\lambda}\left(a - a^{-1}\right) + \sum_{a=1}^{p-1} \overline{\lambda}\left(a + a^{-1}\right) \lambda\left(a - a^{-1}\right) = -4.$$

Proof. Note that $p \equiv 3 \bmod 4$ and $\left(\frac{-1}{p}\right) = -1$, so based on the properties of the Legendre's symbol and complete residue system mod p, we obtain

$$\begin{aligned}
&\sum_{a=1}^{p-1} \lambda\left(a+a^{-1}\right)\overline{\lambda}\left(a-a^{-1}\right) = \sum_{a=1}^{p-1} \lambda\left(a^2+1\right)\overline{\lambda}\left(a^2-1\right)\\
=\ & \sum_{a=1}^{p-1}\left(1+\left(\frac{a}{p}\right)\right)\lambda(a+1)\,\overline{\lambda}(a-1)\\
=\ & \sum_{a=1}^{p-2}\lambda(a+2)\,\overline{\lambda}(a) + \sum_{a=1}^{p-1}\left(\frac{-a}{p}\right)\lambda(-a+1)\,\overline{\lambda}(-a-1)\\
=\ & \sum_{a=1}^{p-1}\lambda\left(1+2a^{-1}\right) - 1 - \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\lambda(a-1)\,\overline{\lambda}(a+1)\\
=\ & -2 - \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\lambda(a-1)\,\overline{\lambda}(a+1). \qquad (2.1)
\end{aligned}$$

Similarly, we can also deduce that

$$\sum_{a=1}^{p-1}\overline{\lambda}\left(a+a^{-1}\right)\lambda\left(a-a^{-1}\right) = -2 + \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\lambda(a-1)\,\overline{\lambda}(a+1). \qquad (2.2)$$

Combining (2.1) and (2.2) we have the identity

$$\sum_{a=1}^{p-1}\lambda\left(a+a^{-1}\right)\overline{\lambda}\left(a-a^{-1}\right) + \sum_{a=1}^{p-1}\overline{\lambda}\left(a+a^{-1}\right)\lambda\left(a-a^{-1}\right) = -4.$$

This proves Lemma 2.

Lemma 3. Let p be an odd prime with $p \equiv 1 \bmod 3$. Then for any third-order character λ mod p, we have the identity

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

Proof. Write $\chi_2 = \left(\frac{*}{p}\right)$. Note that the identities $\overline{\lambda} = \lambda^2$, from the properties of the Gauss sums and the Legendre's symbol mod p we have

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

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

$$= \frac{\tau^2(\lambda)}{\tau\left(\overline{\lambda}\right)}+\frac{\tau(\lambda\chi_2)}{\tau\left(\overline{\lambda}\right)}\sum_{b=1}^{p-1}\overline{\lambda}^2(b)\chi_2(b)e\left(\frac{-b}{p}\right)=\frac{\tau^2(\lambda)}{\tau\left(\overline{\lambda}\right)}+\left(\frac{-1}{p}\right)\frac{\tau^2(\lambda\chi_2)}{\tau\left(\overline{\lambda}\right)}. \tag{2.3}$$

Now according to the properties of complete residue system mod p, we have

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

$$= -1+\frac{1}{\tau\left(\overline{\lambda}\right)}\sum_{b=1}^{p-1}\overline{\lambda}(b)\sum_{a=1}^{p-1}\lambda(a)e\left(\frac{b(a+2)}{p}\right)=-1+\overline{\lambda}(2)\cdot\frac{\tau^2(\lambda)}{\tau\left(\overline{\lambda}\right)}. \tag{2.4}$$

On the other hand, from the properties of Legendre's symbol mod p we also have

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

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

$$= -1+\frac{\tau(\chi_2)}{\tau\left(\overline{\lambda}\right)}\sum_{b=1}^{p-1}\overline{\lambda}(b)\chi_2(b)e\left(\frac{-b}{p}\right)=-1+\left(\frac{-1}{p}\right)\frac{\tau(\chi_2)\tau\left(\overline{\lambda}\chi_2\right)}{\tau\left(\overline{\lambda}\right)}. \tag{2.5}$$

Since $\lambda^3(2)=1$, so applying (2.4) and (2.5) we can deduce the identity

$$\tau^2(\lambda)=\left(\frac{-1}{p}\right)\lambda(2)\tau(\chi_2)\tau\left(\overline{\lambda}\chi_2\right). \tag{2.6}$$

Note that $\tau^2(\chi_2)=\chi_2(-1)p$ and $\tau(\lambda)\tau\left(\overline{\lambda}\right)=\tau(\lambda)\overline{\tau(\lambda)}=p$, combining Lemma 1, (2.3) and (2.6) we can deduce the identity

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

$$= \frac{\tau^3(\lambda)}{p}+\frac{\tau^3\left(\overline{\lambda}\right)}{p}+\left(\frac{-1}{p}\right)\frac{\tau(\lambda)\tau^2(\lambda\chi_2)}{p}+\left(\frac{-1}{p}\right)\frac{\tau\left(\overline{\lambda}\right)\tau^2\left(\overline{\lambda}\chi_2\right)}{p}$$

$$= d+\left(\frac{-1}{p}\right)\frac{\lambda(2)\tau\left(\overline{\lambda}\right)\tau^4\left(\lambda\right)}{p\cdot\tau^2(\chi_2)}+\left(\frac{-1}{p}\right)\frac{\overline{\lambda}(2)\tau\left(\lambda\right)\tau^4\left(\overline{\lambda}\right)}{p\cdot\tau^2(\chi_2)}$$

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

This proves Lemma 3.

Lemma 4. Let p be an odd prime with $p \equiv 1 \bmod 3$. Then for any third-order character λ mod p, we have the identity

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

Proof. It can be deduced from the same methods of proving Lemma 3.

Lemma 5. Let p be an odd prime with $p \equiv 7 \bmod 12$. Then for any third-order character λ mod p, we have the identity

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

Proof. Note that the identity

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

From the properties of the Legendre's symbol mod p we have

$$\sum_{a=1}^{p-1}\lambda\left(a^2-a^{-2}\right)=\sum_{a=1}^{p-1}\lambda\left(a-a^{-1}\right)+\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\lambda\left(a-a^{-1}\right)=\sum_{a=1}^{p-1}\lambda\left(a-a^{-1}\right). \tag{2.7}$$

Applying (2.7) and Lemma 3 we may immediately get

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

This proves Lemma 5.

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 $p \equiv 7 \bmod 12$, note that $\left(\frac{-1}{p}\right)=-1$, so for all integers $1<a<p-1$, we have $(a+a^{-1},p)=1$. From Lemma 2–5 we have

$$\begin{aligned}N(p)&=\frac{1}{9}\sum_{a=2}^{p-2}\left(1+\lambda\left(a+a^{-1}\right)+\overline{\lambda}\left(a+a^{-1}\right)\right)\left(1+\lambda\left(a-a^{-1}\right)+\overline{\lambda}\left(a-a^{-1}\right)\right)\\ &=\frac{1}{9}\sum_{a=1}^{p-1}\left(1+\lambda\left(a+a^{-1}\right)+\overline{\lambda}\left(a+a^{-1}\right)\right)\left(1+\lambda\left(a-a^{-1}\right)+\overline{\lambda}\left(a-a^{-1}\right)\right)\\ &\quad-\frac{2}{9}\cdot\left(1+\lambda(2)+\overline{\lambda}(2)\right)\end{aligned}$$

$$
\begin{aligned}
&= \frac{p-1}{9} + \frac{1}{9}\sum_{a=1}^{p-1}\left(\lambda\left(a+a^{-1}\right)\overline{\lambda}\left(a-a^{-1}\right)+\overline{\lambda}\left(a+a^{-1}\right)\lambda\left(a-a^{-1}\right)\right)\\
&\quad+\frac{1}{9}\sum_{a=1}^{p-1}\left(\lambda\left(a+a^{-1}\right)+\lambda\left(a-a^{-1}\right)+\overline{\lambda}\left(a+a^{-1}\right)+\overline{\lambda}\left(a-a^{-1}\right)\right)\\
&\quad+\frac{1}{9}\sum_{a=1}^{p-1}\left(\lambda\left(a^2-a^{-2}\right)+\overline{\lambda}\left(a^2-a^{-2}\right)\right)-\frac{2}{9}\cdot\left(1+\lambda(2)+\overline{\lambda}(2)\right)\\
&= \frac{1}{9}\cdot\left(p+3d-7-2\lambda(2)-2\overline{\lambda}(2)\right)+\frac{1}{9p}\left(\lambda(2)\tau^3(\lambda)+\overline{\lambda}(2)\cdot\tau^3\left(\overline{\lambda}\right)\right). \qquad (3.1)
\end{aligned}
$$

If 2 is a cubic residue mod p, then $\lambda(2)=1$, from (3.1) and Lemma 1 we have

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

This proves Theorem 1.

If 2 is not a cubic residue mod p, then $1+\lambda(2)+\overline{\lambda}(2)=0$, note that the estimate $|\tau(\lambda)|=\sqrt{p}$, from (3.1) and Lemma 1 we have

$$
\begin{aligned}
N(p) &= \frac{p-7-2\lambda(2)-2\overline{\lambda}(2)}{9}+\frac{(3+\lambda(2))\tau^3(\lambda)+(3+\overline{\lambda}(2))\cdot\tau^3\left(\overline{\lambda}\right)}{9p}\\
&= \frac{p-5}{9}+\frac{\left(2-\overline{\lambda}(2)\right)\tau^3(\lambda)+(2-\lambda(2))\cdot\tau^3\left(\overline{\lambda}\right)}{9p}=\frac{p-5}{9}+E(p),
\end{aligned}
$$

where $|E(p)|=\frac{1}{9p}\cdot\left|\left(2-\overline{\lambda}(2)\right)\tau^3(\lambda)+(2-\lambda(2))\cdot\tau^3\left(\overline{\lambda}\right)\right|\le\frac{2}{3}\cdot\sqrt{p}$.
This proves Theorem 2.

If $p\equiv 1 \bmod 12$, then there exist integer r such that $r^2=(-r)^2\equiv -1 \bmod p$ and $r+r^{-1}\equiv 0 \bmod p$. For this integer $1<r<p-1$, we also have $\lambda(r)=\overline{\lambda}^2(r)=\overline{\lambda}(r^2)=\overline{\lambda}(-1)=1$, so we have

$$
\begin{aligned}
N(p) &= \frac{1}{9}\sum_{\substack{a=2\\(a^2+1,p)=1}}^{p-2}\left(1+\lambda\left(a+a^{-1}\right)+\overline{\lambda}\left(a+a^{-1}\right)\right)\left(1+\lambda\left(a-a^{-1}\right)+\overline{\lambda}\left(a-a^{-1}\right)\right)\\
&= \frac{1}{9}\sum_{a=1}^{p-1}\left(1+\lambda\left(a+a^{-1}\right)+\overline{\lambda}\left(a+a^{-1}\right)\right)\left(1+\lambda\left(a-a^{-1}\right)+\overline{\lambda}\left(a-a^{-1}\right)\right)\\
&\quad-\frac{4}{9}\cdot\left(1+\lambda(2)+\overline{\lambda}(2)\right)\\
&= \frac{p-1}{9}+\frac{1}{9}\sum_{a=1}^{p-1}\left(\lambda\left(a+a^{-1}\right)\overline{\lambda}\left(a-a^{-1}\right)+\overline{\lambda}\left(a+a^{-1}\right)\lambda\left(a-a^{-1}\right)\right)\\
&\quad+\frac{1}{9}\sum_{a=1}^{p-1}\left(\lambda\left(a+a^{-1}\right)+\lambda\left(a-a^{-1}\right)+\overline{\lambda}\left(a+a^{-1}\right)+\overline{\lambda}\left(a-a^{-1}\right)\right)\\
&\quad+\frac{1}{9}\sum_{a=1}^{p-1}\left(\lambda\left(a^2-a^{-2}\right)+\overline{\lambda}\left(a^2-a^{-2}\right)\right)-\frac{4}{9}\cdot\left(1+\lambda(2)+\overline{\lambda}(2)\right). \qquad (3.2)
\end{aligned}
$$

From the Weil's work [22] we have the estimates

$$\left|\sum_{a=1}^{p-1}\lambda\left(a^2-a^{-2}\right)\right| = \left|\sum_{a=1}^{p-1}\lambda(a)\lambda\left(a^4-1\right)\right| = \left|\sum_{a=1}^{p-1}\lambda\left(a^5-a\right)\right| \le 5\cdot\sqrt{p} \tag{3.3}$$

$$\left|\sum_{a=1}^{p-1}\lambda\left(a+a^{-1}\right)\overline{\lambda}\left(a-a^{-1}\right)\right| = \left|\sum_{a=1}^{p-1}\lambda\left(a^2+1\right)\overline{\lambda}\left(a^2-1\right)\right| \le 4\cdot\sqrt{p}. \tag{3.4}$$

If $\lambda(2)=1$, then note that $|d|\le 2\cdot\sqrt{p}$, applying (3.2–3.4) and Lemma 1–5 we have asymptotic formula

$$N(p) = \frac{1}{9}\cdot(p-13) + E_1(p), \tag{3.5}$$

where $|E_1(p)| \le \frac{26}{9}\cdot\sqrt{p}$.

If $\lambda(2)\ne 1$, then applying (3.2–3.4) and Lemma 2–5 we have asymptotic formula

$$N(p) = \frac{1}{9}\cdot(p-1) + E_1(p), \tag{3.6}$$

where $|E_1(p)| \le \frac{26}{9}\cdot\sqrt{p}$.

Now Theorem 3 follows from asymptotic formulas (3.5) and (3.6).

This completes the proofs of our all results.

4. Conclusion

The main results of this paper are three theorems and a corollary. Theorem 1 obtained an exact formula for $N(p)$ with $p = 12k+7$ and 2 is a cubic residue modulo p. Theorem 2 and Theorem 3 established two asymptotic formulas for $N(p)$ with $p\equiv 1 \bmod 3$ and 2 is not a cubic residue modulo p. At the same time, we also give two sharp upper bound estimates for the error terms. As some applications, we also deduced following corollary:

If $p > 700$ is a prime with $p\equiv 1 \bmod 3$, then there is at least one integer $1 < a < p-1$ such that $a+a^{-1}$ and $a-a^{-1}$ are cubic residues modulo p.

Acknowledgments

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

This work is supported by the N. S. F. (2017MS0114) of Inner Mongolia, Talent introduction research Foundation of Hetao College (HYRC2019007) and the N. S. F. (11771351) of P. R. China.

Conflict of interest

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

References

1. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer Science & Business Media, 1976.
2. W. P. Zhang, H. L. Li, *Elementary Number Theory*, Shaanxi Normal University Press, Xi'an, 2013.
3. W. Narkiewicz, *Classical Problems in Number Theory*, Polish Scientifc Publishers, WARSZAWA, 1986.
4. N. C. Ankeny, *The least quadratic non-residue*, Ann. Math., **55** (1952), 65–72.
5. T. Wang and X. Lv, *The quadratic residues and some of their new distribution properties*, Symmetry, **12** (2020), 1–8.
6. Z. H. Sun, *Consecutive numbers with the same Legendre symbol*, P. Am. Math. Soc., **130** (2002), 2503–2507.
7. Z. H. Sun, *Cubic residues and binary quadratic forms*, J. Number Theory, **124** (2007), 62–104.
8. Z. H. Sun, *Cubic congruences and sums involving* $\binom{3k}{k}$, Int. J. Number Theory, **12** (2016), 143–164.
9. Z. H. Sun, *On the theory of cubic residues and nonresidues*, Acta Arith., **84** (1998), 291–315.
10. F. L. Ţiplea, S. Iftene, G. Teşeleanu, et al. *On the distribution of quadratic residues and non-quadratic residues modulo composite integers and applications to cryptography*, Appl. Math. Comput., **372** (2020), 1–18.
11. R. Peralta, *On the distribution of quadratic residues and non-residues nodulo a prime number*, Math. Comput., **58** (1992), 433–440.
12. S. Wright, *Quadratic residues and non-residues in arithmetic progression*, J. Number Theory, **133** (2013), 2398–2430.
13. W. Kohnen, *An elementary proof in the theory of quadratic residues*, Bull. Korean Math. Soc., **45** (2008), 273–275.
14. P. Hummel, On consecutive quadratic non-residues: a conjecture of Issai Schur, J. Number Theory, **103** (2003), 257–266.
15. M. Z. Garaev, *A note on the least quadratic non-residue of the integer-sequences*, B. Aust. Math. Soc., **68** (2003), 1–11.
16. A. Schinzel, *Primitive roots and quadratic non-residues*, Acta Arith., **2** (2011), 161–170.
17. Y. K. Lau, J. Wu, *On the least quadratic non-residue*, Int. J. Number Theory, **4** (2008), 423–435.
18. D. S. Dummit, E. P. Dummit, H. Kisilevsky, *Characterizations of quadratic, cubic, and quartic residue matrices*, J. Number Theory, **168** (2016), 167–179.
19. D. S. Xing, Z. F. Cao, X. L. Dong, *Identity based signature scheme based on cubic residues*, Sci. China Inform. Sci., **54** (2011), 2001–2012.
20. W. L. Su, Q. Li, H. Luo, et al. *Lower bounds of Ramsey numbers based on cubic residues*, Discrete Math., **250** (2002), 197–209.
21. W. P. Zhang, J. Y. Hu, *The number of solutions of the diagonal cubic congruence equation* mod p, Math. Rep., **20** (2018), 73–80.

22. A. Weil, *On some exponential sums*, Proc. Natl. Acad. Sci. U. S. A., **34** (1948), 204–207.

AIMS Press