Computer Modeling in
Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.024363

check for updates

ARTICLE

On the Mean Value of High-Powers of a Special Character Sum Modulo a Prime

Xiaodan Yuan* and Wenpeng Zhang

School of Mathematics, Northwest University, Xi'an, China

*Corresponding Author: Xiaodan Yuan. Email: yuanxd@stumail.nwu.edu.cn

Received: 29 May 2022 Accepted: 07 September 2022

ABSTRACT

In this paper, we use the elementary methods, the properties of Dirichlet character sums and the classical Gauss sums to study the estimation of the mean value of high-powers for a special character sum modulo a prime, and derive an exact computational formula. It can be conveniently programmed by the "Mathematica" software, by which we can get the exact results easily.

KEYWORDS

Quadratic character; the classical gauss sums; the mean value of high-power; computational formula

1 Introduction

Let p be an odd prime, the quadratic character modulo p is called the Legendre symbol, which is defined by

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

Many mathematicians have studied the properties of the Legendre symbol and obtained a series of important results (see [1–13]). Perhaps the most representative properties of the Legendre's symbol are as follows:

Let p and q be two distinct odd primes, then one has the quadratic reciprocal formula (see [14]: Theorem 9.8 or [15]: Theorems 4–6)

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

For any odd prime p with $p \equiv 1 \bmod 4$, there exists two non-zero integers α_p and β_p such that (see [15]: Theorems 4–11)

$$p = \alpha_p^2 + \beta_p^2. \tag{1}$$

In fact, the integers α_p and β_p in Eq. (1) can be represented by the Jacobsthal sums $\phi_2(r)$, which is (see [16]: Definition of the Jacobsthal sums)

$$\phi_k(r) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right)\left(\frac{a^k + r}{p}\right) \text{ and } \alpha_p = \frac{1}{2}\phi_2(1), \ \beta_p = \frac{1}{2}\phi_2(s),$$

where s is any quadratic non-residue modulo p.

Now we consider a sum $A(r)$ be similar to β_p. For any integers r with $(r, p) = 1$ and $k \geq 0$, let $A(r)$ and $S_k(p)$ be defined as follows:

$$A(r) = 1 + \sum_{a=1}^{p-1} \left(\frac{a^2 + r\bar{a}}{p}\right) \text{ and } S_k(p) = \frac{1}{p-1}\sum_{r=1}^{p-1} A^k(r).$$

In this paper, we give an exact computational formula for $S_k(p)$ with $p \equiv 1 \bmod 6$, and prove the following result:

Theorem. Let p be a prime with $p \equiv 1 \bmod 6$, for any integer k, we have the identity

$$S_k(p) = \frac{1}{3} \cdot \left[d^k + \left(\frac{-d + 9b}{2}\right)^k + \left(\frac{-d - 9b}{2}\right)^k\right],$$

where d and b are uniquely determined by $4p = d^2 + 27b^2$, $d \equiv 1 \bmod 3$ and $b > 0$.

From this Theorem, we can immediately deduce the following four Corollaries:

Corollary 1. Let p be a prime with $p \equiv 1 \bmod 6$, then we have

$$\frac{1}{p-1}\sum_{r=1}^{p-1} \frac{1}{1 + \sum_{a=1}^{p-1}\left(\frac{a^2 + r\bar{a}}{p}\right)} = \frac{1}{p-1}\sum_{r=1}^{p-1} \frac{1}{1 + \sum_{a=1}^{p-1}\left(\frac{a^4 + ra}{p}\right)} = \frac{p}{d \cdot (3p - d^2)}.$$

Corollary 2. Let p be a prime with $p \equiv 1 \bmod 6$, we have

$$\frac{1}{p-1}\sum_{r=1}^{p-1} \frac{1}{\left[1 + \sum_{a=1}^{p-1}\left(\frac{a^2 + r\bar{a}}{p}\right)\right]^2} = \frac{1}{p-1}\sum_{r=1}^{p-1} \frac{1}{\left[1 + \sum_{a=1}^{p-1}\left(\frac{a^4 + ra}{p}\right)\right]^2} = \frac{3 \cdot p^2}{d^2 \cdot (3p - d^2)^2}.$$

Corollary 3. Let p be a prime with $p \equiv 1 \bmod 6$, then we have

$$\frac{1}{p-1}\sum_{r=1}^{p-1} \left[1 + \sum_{a=1}^{p-1}\left(\frac{a^2 + r\bar{a}}{p}\right)\right]^4 = \frac{1}{p-1}\sum_{r=1}^{p-1} \left[1 + \sum_{a=1}^{p-1}\left(\frac{a^4 + ra}{p}\right)\right]^4 = 6 \cdot p^2.$$

Corollary 4. Let p be a prime with $p \equiv 1 \bmod 6$, we have

$$\frac{1}{p-1}\sum_{r=1}^{p-1} \left[1 + \sum_{a=1}^{p-1}\left(\frac{a^2 + r\bar{a}}{p}\right)\right]^6 = \frac{1}{p-1}\sum_{r=1}^{p-1} \left[1 + \sum_{a=1}^{p-1}\left(\frac{a^4 + ra}{p}\right)\right]^6 = 18p^3 + d^2 \cdot \left(d^2 - 3p\right)^2.$$

Some notes: In our Theorem, we only discuss the case $p \equiv 1 \bmod 6$. If $p \equiv 5 \bmod 6$, the result is trivial, see Proposition 6.1.2 in [16]. In this case, for any integer r with $(r, p) = 1$, we have the identity

$$A(r) = 1 + \sum_{a=1}^{p-1} \left(\frac{a^2 + r\bar{a}}{p} \right) = 1 + \sum_{a=1}^{p-1} \left(\frac{a^3}{p} \right) \left(\frac{a^3 + r}{p} \right)$$
$$= 1 + \sum_{a=1}^{p-1} \left(\frac{1 + r\bar{a}}{p} \right) = \sum_{a=0}^{p-1} \left(\frac{1 + ra}{p} \right) = 0.$$

Thus, for all prime p with $p \equiv 5 \bmod 6$ and $k \geq 1$, we have $S_k(p) = 0$.

In addition, our Theorem holds for all negative integers.

Obviously, the advantage of our work is that it can transfer a complex mathematical computational problem into a simple form suitable for computer programming. It means that for any fixed prime p with $p \equiv 1 \bmod 6$ and integer k, the exact value of $S_k(p)$ can be calculated by our Theorem and a simple computer program. In Section 4, we give an example to calculate the exact results of the prime number p within 200 satisfying conditions $p \equiv 1 \bmod 6$ and $d \equiv 1 \bmod 3$. The exact results of calculation are summarised in Table 1.

Table 1: The calculation of $S_k(p)$

p	d	b	k	$S_k(p)$
7	1	1	1, 2, 3, 4, 5, 6, 7, 8	$S_1(7) = 0, S_2(7) = 14,$ $S_3(7) = -20, S_4(7) = 294,$ $S_5(7) = -700, S_6(7) = 6574$ $S_7(7) = -20580, S_8(7) = 152054$
19	7	1	1, 2, 3, 4, 5, 6, 7, 8	$S_1(19) = 0, S_2(19) = 38,$ $S_3(19) = -56, S_4(19) = 2166,$ $S_5(19) = -5329, S_6(19) = 126598$ $S_7(19) = -424536, S_8(19) = 7514006$
31	4	2	1, 2, 3, 4, 5, 6, 7, 8	$S_1(31) = 0, S_2(31) = 62,$ $S_3(31) = -308, S_4(31) = 5766,$ $S_5(31) = -47740, S_6(31) = 631102$ $S_7(31) = -6215748, S_8(31) = 73396406$
61	1	3	1, 2, 3, 4, 5, 6, 7, 8	$S_1(61) = 0, S_2(62) = 122,$ $S_3(61) = -182, S_4(61) = 22326,$ $S_5(61) = -55510, S_6(61) = 4118782$ $S_7(61) = -14221662, S_8(61) = 763839926$
73	7	3	1, 2, 3, 4, 5, 6, 7, 8	$S_1(73) = 0, S_2(73) = 146,$ $S_3(73) = -1190, S_4(73) = 31974,$ $S_5(73) = -434350, S_6(73) = 8418406$ $S_7(73) = -133171710, S_8(73) = 2360507414$
97	19	1	1, 2, 3, 4, 5, 6, 7, 8	$S_1(97) = 0, S_2(97) = 194,$ $S_3(97) = 1330, S_4(97) = 56454,$ $S_5(97) = 645050, S_6(97) = 18197014$ $S_7(97) = 262793370, S_8(97) = 6153247574$

(Continued)

Table 1 (continued)

p	d	b	k	$S_k(p)$
103	13	3	1, 2, 3, 4, 5, 6, 7, 8	$S_1(103) = 0$, $S_2(103) = 206$, $S_3(103) = -1820$, $S_4(103) = 63654$, $S_5(103) = -937300$, $S_6(103) = 22981486$ $S_7(103) = -405475980$, $S_8(103) = 8087165174$
151	19	3	1, 2, 3, 4, 5, 6, 7, 8	$S_1(151) = 0$, $S_2(151) = 302$, $S_3(151) = -1748$, $S_4(151) = 136806$, $S_5(151) = -1319740$, $S_6(151) = 65028622$ $S_7(151) = -836979108$, $S_8(151) = 31764871286$
163	25	1	1, 2, 3, 4, 5, 6, 7, 8	$S_1(163) = 0$, $S_2(163) = 326$, $S_3(163) = 3400$, $S_4(163) = 159414$, $S_5(163) = 2771000$, $S_6(163) = 89513446$ $S_7(163) = 1897026600$, $S_8(163) = 53193475094$
181	7	5	1, 2, 3, 4, 5, 6, 7, 8	$S_1(181) = 0$, $S_2(181) = 362$, $S_3(181) = -3458$, $S_4(181) = 196566$, $S_5(181) = -3129490$, $S_6(181) = 118693102$ $S_7(181) = -2379038298$, $S_8(181) = 75272130806$

2 Several Lemmas

In this section, we give some simple Lemmas, which are necessary in the proofs of our Theorem. In addition, we need some properties of the classical Gauss sums and character sums, which can be found in many number theory books, such as [14,15] or [17], and we will not repeat them. First, we have the following:

Lemma 1. Let p be a prime with $p \equiv 1 \bmod 3$, for any third-order character λ modulo 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 with $e(y) = e^{2\pi i y}$ and $i^2 = -1$, d is the same as the one in the Theorem.

Proof. See references [18] or [19].

Lemma 2. Let p be an odd prime, for any non-principal character χ modulo p, we have the identity

$$\tau\left(\chi^2\right) = \frac{\chi^2(2)}{\tau(\chi_2)} \cdot \tau(\chi) \cdot \tau(\chi\chi_2),$$

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

Proof. From the properties of the classical Gauss sums we have

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

On the other hand, for any integer b with $(b,p)=1$, from the identity

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

we also have

$$\sum_{a=0}^{p-1} \chi\left(a^2-1\right) = \frac{1}{\tau(\overline{\chi})} \sum_{a=0}^{p-1}\sum_{b=1}^{p-1} \overline{\chi}(b)\, e\left(\frac{b(a^2-1)}{p}\right)$$
$$= \frac{1}{\tau(\overline{\chi})} \sum_{b=1}^{p-1} \overline{\chi}(b)\, e\left(\frac{-b}{p}\right) \sum_{a=0}^{p-1} e\left(\frac{ba^2}{p}\right) = \frac{\tau(\chi_2)}{\tau(\overline{\chi})} \sum_{b=1}^{p-1} \overline{\chi}(b)\,\chi_2(b)\, e\left(\frac{-b}{p}\right)$$
$$= \frac{\chi_2(-1)\,\overline{\chi}(-1)\,\tau(\chi_2)\cdot\tau(\overline{\chi}\chi_2)}{\tau(\overline{\chi})}. \tag{3}$$

From Eqs. (2) and (3) we have the identity

$$\tau\left(\overline{\chi}^2\right) = \frac{\overline{\chi}^2(2)\cdot\chi_2(-1)\,\overline{\chi}(-1)\cdot\tau(\chi_2)\cdot\tau(\overline{\chi}\chi_2)}{\tau(\chi)}$$

or

$$\tau\left(\chi^2\right) = \frac{\chi^2(2)}{\tau(\chi_2)}\cdot\tau(\chi)\cdot\tau(\chi\chi_2).$$

This proves Lemma 2.

Lemma 3. Let p be a prime p with $p \equiv 1 \bmod 6$, then for any integer r with $(r,p)=1$ and three order character λ modulo p, we have the identity

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

Proof. From the characteristic function of the cubic residue modulo p, we have

$$\frac{1}{3}\cdot\left(1+\lambda(a)+\overline{\lambda}(a)\right) = \begin{cases} 1 & \text{if } a \text{ is a cubic residue modulo } p; \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

Applying Eq. (4) we have

$$\sum_{a=1}^{p-1}\left(\frac{a^2+r\overline{a}}{p}\right)=\sum_{a=1}^{p-1}\chi_2\left(\overline{a}^3\right)\chi_2\left(a^3+r\right)=\sum_{a=1}^{p-1}\chi_2\left(a^3\right)\chi_2\left(a^3+r\right)$$

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

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

$$=-1+\lambda\left(r\right)\sum_{a=1}^{p-1}\lambda\left(a\right)\chi_2\left(a\right)\chi_2\left(a+1\right)+\overline{\lambda}\left(r\right)\sum_{a=1}^{p-1}\overline{\lambda}\left(a\right)\chi_2\left(a\right)\chi_2\left(a+1\right). \tag{5}$$

From the properties of the classical Gauss sums, we have

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

$$=\frac{1}{\tau\left(\chi_2\right)}\cdot\tau\left(\lambda\chi_2\right)\cdot\tau\left(\overline{\lambda}\right). \tag{6}$$

Taking $\chi=\lambda$ in Lemma 2, we have

$$\tau\left(\overline{\lambda}\right)=\frac{\overline{\lambda}\left(2\right)}{\tau\left(\chi_2\right)}\cdot\tau\left(\lambda\right)\cdot\tau\left(\lambda\chi_2\right). \tag{7}$$

Note that $\tau\left(\lambda\right)\cdot\tau\left(\overline{\lambda}\right)=p$, from Eqs. (6) and (7) we have

$$\sum_{a=1}^{p-1}\lambda\left(a\right)\chi_2\left(a\right)\chi_2\left(a+1\right)=\frac{\lambda(2)}{p}\cdot\tau^3\left(\overline{\lambda}\right). \tag{8}$$

Similarly, we also have

$$\sum_{a=1}^{p-1}\overline{\lambda}\left(a\right)\chi_2\left(a\right)\chi_2\left(a+1\right)=\frac{\overline{\lambda}\left(2\right)}{p}\cdot\tau^3\left(\lambda\right). \tag{9}$$

Combining Eqs. (5), (8) and (9) we can deduce that

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

This proves Lemma 3.

Lemma 4. Let p be any odd prime with $p\equiv 1 \bmod 6$, then for any integers $k\geq 3$ and r with $(r,p)=1$, we have the third order recursive formula

$$A^k(r)=3p\cdot A^{k-2}(r)+\left(d^3-3dp\right)\cdot A^{k-3}(r),$$

where d is the same as defined in the Theorem.

Proof. Note that $\lambda^3 = \overline{\lambda}^3 = \chi_0$, the principal character modulo p, from Lemma 1 and Lemma 3 we have

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

$$= \frac{1}{p^3} \cdot \left[\tau^9(\lambda) + \tau^9\left(\overline{\lambda}\right) + 3p^3 \cdot \left(\overline{\lambda}(2r) \cdot \tau^3(\lambda) + \lambda(2r) \cdot \tau^3\left(\overline{\lambda}\right)\right)\right]$$

$$= \frac{1}{p^3} \cdot \left[\left(\tau^3(\lambda) + \tau^3\left(\overline{\lambda}\right)\right)^3 - 3p^3\left(\tau^3(\lambda) + \tau^3\left(\overline{\lambda}\right)\right) + 3p^4 \cdot A(r)\right]$$

$$= d^3 - 3dp + 3p \cdot A(r). \tag{10}$$

Indeed, for any integer $k \geq 3$, from Eq. (10) we have the third order recursive formula

$$A^k(r) = A^{k-3}(r) \cdot A^3(r) = 3p \cdot A^{k-2}(r) + \left(d^3 - 3dp\right) \cdot A^{k-3}(r).$$

This proves Lemma 4.

Lemma 5. Let p be any odd prime with $p \equiv 1 \bmod 6$, then we have

$S_0(p) = 1, S_1(p) = 0, S_2(p) = 2p,\ S_3(p) = d \cdot \left(d^2 - 3p\right)$ and

$S_k(p) = 3p \cdot S_{k-2}(p) + \left(d^3 - 3pd\right) \cdot S_{k-3}(p)$ for all $k \geq 4$.

Proof. From the definition

$$S_k(p) = \frac{1}{p-1}\sum_{r=1}^{p-1} A^k(r)$$

and the orthogonality of characters modulo p, we have

$$S_0(p) = 1, S_1(p) = \frac{1}{p(p-1)}\sum_{r=1}^{p-1}\left(\overline{\lambda}(2r) \cdot \tau^3(\lambda) + \lambda(2r) \cdot \tau^3\left(\overline{\lambda}\right)\right) = 0, \tag{11}$$

$$S_2(p) = \frac{1}{p^2(p-1)}\sum_{r=1}^{p-1}\left(\overline{\lambda}(2r) \cdot \tau^3(\lambda) + \lambda(2r) \cdot \tau^3\left(\overline{\lambda}\right)\right)^2 = 2p. \tag{12}$$

From Eq. (10) we also have

$$S_3(p) = \frac{1}{p^3(p-1)}\sum_{r=1}^{p-1}\left(\overline{\lambda}(2r) \cdot \tau^3(\lambda) + \lambda(2r) \cdot \tau^3\left(\overline{\lambda}\right)\right)^3$$

$$= \frac{1}{p-1}\sum_{r=1}^{p-1}\left(d^3 - 3dp + 3p \cdot A(r)\right) = d \cdot \left(d^2 - 3p\right). \tag{13}$$

If $k \geq 4$, then from Lemma 4 we have

$$S_k(p) = 3p \cdot S_{k-2}(p) + \left(d^3 - 3dp\right) \cdot S_{k-3}(p). \tag{14}$$

Now Lemma 5 follows from Eqs. (11)–(14).

3 Proof of the Theorem

In this section, we complete the proof of our Theorem. It is clear that the characteristic equation of the third order linear recursive formula

$$S_k(p) = 3p \cdot S_{k-2}(p) + \left(d^3 - 3dp\right) \cdot S_{k-3}(p) \tag{15}$$

is

$$x^3 - 3px - \left(d^3 - 3dp\right) = 0. \tag{16}$$

Note that $4p = d^2 + 27b^2$, from Eq. (16) we have

$$(x - d)\left(x + \frac{d + 9b}{2}\right)\left(x + \frac{d - 9b}{2}\right) = 0.$$

It is clear that the three roots of Eq. (16) are $x_1 = d$, $x_2 = \frac{-d+9d}{2}$ and $x_3 = \frac{-d-9d}{2}$. Indeed, the general term of Eq. (15) is

$$S_k(p) = C_1 \cdot d^k + C_2 \cdot \left(\frac{-d + 9b}{2}\right)^k + C_3 \cdot \left(\frac{-d - 9b}{2}\right)^k, \; k \geq 0. \tag{17}$$

From Lemma 5 we have

$$\begin{cases} C_1 + C_2 + C_3 = 1, \\ C_1 \cdot d + C_2 \cdot \left(\frac{-d+9b}{2}\right) + C_3 \cdot \left(\frac{-d-9b}{2}\right) = 0, \\ C_1 \cdot d^2 + C_2 \cdot \left(\frac{-d+9b}{2}\right)^2 + C_3 \cdot \left(\frac{-d-9b}{2}\right)^2 = 2p. \end{cases} \tag{18}$$

Solving the Eq. (18) we can get $C_1 = C_2 = C_3 = \frac{1}{3}$. From Eq. (17) we have

$$S_k(p) = \frac{1}{3}\left[d^k + \left(\frac{-d + 9b}{2}\right)^k + \left(\frac{-d - 9b}{2}\right)^k\right], \; k \geq 0.$$

This proves our Theorem.

Obviously, using Lemma 4 we can also extend k in Lemma 5 to all negative integers, which leads to the Corollary 1 and the Corollary 2.

This completes the proofs of our all results.

4 Conclusion

In this paper, we give an exact computational formula for $S_k(p)$ with $p \equiv 1 \bmod 6$, which is, for any integer k, we have the identity

$$S_k(p) = \frac{1}{3} \cdot \left[d^k + \left(\frac{-d + 9b}{2}\right)^k + \left(\frac{-d - 9b}{2}\right)^k\right],$$

where d and b are uniquely determined by $4p = d^2 + 27b^2$, $p \equiv 1 \bmod 6$ and $b > 0$.

Meanwhile, the problems of calculating the mean value of high-powers of quadratic character sums modulo a prime are given.

In the end, we use the mathematical software "Mathematica" to program and calculate the exact values of $S_1(p)$ to $S_8(p)$ of the prime number p within 200 satisfying conditions $p \equiv 1 \bmod 6$ and $d \equiv 1 \bmod 3$, as shown in Table 1. Its application can also extend to $S_k(p)$ that satisfies conditions $p \equiv 1 \bmod 6$ and $d \equiv 1 \bmod 3$ (where $4p = d^2 + 27b^2$) for any k. See the Appendix A for this specific computer program.

Acknowledgement: The authors would like to thank the editor and referees for their suggestions and critical comments that substantially improve the presentation of this work.

Funding Statement: This work was supported by the N. S. F. (12126357) of China.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Ankeny, N. C. (1952). The least quadratic non-residue. *Annals of Mathematics, 55,* 65–72. DOI 10.2307/1969420.
2. Peralta, R. (1992). On the distribution of quadratic residues and non-residues modulo a prime number. *Mathematics of Computation, 58,* 433–440. DOI 10.1090/S0025-5718-1992-1106978-9.
3. Sun, Z. H. (2002). Consecutive numbers with the same legendre symbol. *Proceedings of the American Mathematical Society, 130,* 2503–2507. DOI 10.1090/S0002-9939-02-06600-5.
4. Hummel, P. (2003). On consecutive quadratic non-residues: A conjecture of Issai Schur. *Journal of Number Theory, 103(2),* 257–266. DOI 10.1016/j.jnt.2003.06.003.
5. Garaev, M. Z. (2003). A note on the least quadratic non-residue of the integer-sequences. *Bulletin of the Australian Mathematical Society, 68(1),* 1–11. DOI 10.1017/S0004972700037369.
6. Kohnen, W. (2008). An elementary proof in the theory of quadratic residues. *Bulletin of the Korean Mathematical Society, 45(2),* 273–275. DOI 10.4134/BKMS.2008.45.2.273.
7. Yuk-Kam, L., Jie, W. (2008). On the least quadratic non-residue. *International Journal of Number Theory, 4,* 423–435. DOI 10.1142/S1793042108001432.
8. Schinzel, A. (2011). Primitive roots and quadratic non-residues. *Acta Arithmetica, 149,* 161–170. DOI 10.4064/aa149-2-5.
9. Wright, S. (2013). Quadratic residues and non-residues in arithmetic progression. *Journal of Number Theory, 133(7),* 2398–2430. DOI 10.1016/j.jnt.2013.01.004.
10. Dummit, D. S., Dummit, E. P., Kisilevsky, H. (2016). Characterizations of quadratic, cubic, and quartic residue matrices. *Journal of Number Theory, 168,* 167–179. DOI 10.1016/j.jnt.2016.04.014.
11. Ţiplea, F. L., Iftene, S., Teşeleanu, G., Nica, A. M. (2020). On the distribution of quadratic residues and non-quadratic residues modulo composite integers and applications to cryptography. *Applied Mathematics and Computation, 372,* 124993.
12. Wang, T. T., Lv, X. X. (2020). The quadratic residues and some of their new distribution properties. *Symmetry, 12(3),* 421.
13. Zhang, J. F., Meng, Y. Y. (2021). The mean values of character sums and their applications. *Mathematics, 9(4),* 318.
14. Apostol, T. M. (1976). *Introduction to analytic number theory*. New York: Springer-Verlag.
15. Zhang, W. P., Li, H. L. (2013). *Elementary number theory*. Xi'an, China: Shaanxi Normal University Press.

16. Berndt, B. C., Evans, R. J., Williams, K. S. (1999). Gauss and jacobi sums. *The Mathematical Gazette, 83(497),* 349–351.
17. Narkiewicz, W. (1986). *Classical problems in number theory*. Warszawa: Polish Scientifc Publishers.
18. Zhang, W. P., Hu, J. Y. (2018). The number of solutions of the diagonal cubic congruence equation mod p. *Mathematical Reports, 20(1),* 73–80.
19. Berndt, B. C., Evans, R. J. (1981). The determination of gauss sums. *Bulletin of the American Mathematical Society, 5(2),* 107–128.

Appendix A.

```
Clear[b]
Clear[p];
Clear[a];
Clear[d];
a = 1;
Array[p, 20];
For[i = 1, i <= 10000, i ++,
If[Mod[Prime[i], 6] == 1,
p[a] = Prime[i];
If[a == 20, Break[], ]
a ++;
, ]
]

a = 1;
Array[d, 20];
For[i = 1, i <= 10000, i ++,
If[Mod[i, 3] == 1,
d[a] = i;
If[a == 20, Break[], ]
a ++;
, ]
]
S[pi, di, bi, ki]: = (1/3) * (di^k i + ((−di + 9 * bi)/2)^k i + ((−di −9 * bi)/2)^k i)

For[i = 1, i <= 20, i ++,
For[j = 1, j <= 20, j ++,
b = Sqrt[(4 * p[i] − d[j] * d[j])/27];
If[Element[b, Integers],
```

```
For[k = 1, k <= 8, k++,
Print["p = ", p[i], "d = ", d[j], "b = ", b, "k = ", k,
"S = ", S[p[i], d[j], b, k]];
],
]
]
]
```