CrossMark

On the classical Gauss sum and the recursive properties

Hui Bai[1] and Jiayuan Hu[1*] (iD)

*Correspondence:
hujiayuan1986@163.com
[1]Department of Mathematics and
Computer Science, Hetao College,
Bayannur, P.R. China

Abstract

Let p be a prime with $p \equiv 1 \bmod 8$, ψ be an eighth character $\bmod p$, and $\tau(\psi)$ denote the classical Gauss sum $\bmod p$. The main purpose of this paper is using the analytic method and the properties of the classical Gauss sum to study the computational problem of one kind rational polynomial of $\tau(\psi)$. In the end, we prove an interesting second-order linear recursive formula for it.

MSC: 11L05

Keywords: The classical Gauss sum; Eighth character; Rational polynomial; Second-order linear recursive formula; Analytic method

1 Introduction

For any positive integer $q \geq 2$ and Dirichlet character $\chi \bmod q$, the classical Gauss sum $\tau(\chi)$ is defined as

$$\tau(\chi) = \sum_{a=1}^{q} \chi(a) e\left(\frac{a}{q}\right),$$
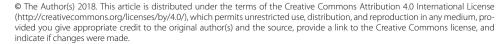
where $e(y) = e^{2\pi i y}$.

This sum is very important in the study of the analytic number theory, so many authors had studied its elementary properties, and obtained a series of important results. In fact, if χ is a primitive character $\bmod q$, then one has the identity $|\tau(\chi)| = \sqrt{q}$. For the general character $\chi \bmod q$, we have the estimate $|\tau(\chi)| \leq \sqrt{q}$. From some special characters $\chi \bmod q$, the Gauss sum $\tau(\chi)$ has some interesting properties. For example, if p is a prime with $p \equiv 1 \bmod 3$, and ψ is any third-order character $\bmod p$, then we have the identity [1, 2]

$$\tau^3(\psi) + \tau^3(\overline{\psi}) = dp,$$

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

Zhuoyu Chen and Wenpeng Zhang [3] obtained a similar formula for the quartic Gauss sum (see Lemma 2 below). Of course, there are also many similar results, and we are not going to list them here. The reader can refer to Refs. [4–7] and [8] for details.

In this paper, we are considering such a sequence $F_k(p)$ as follows: Let p be a prime with $p \equiv 1 \bmod 8$, ψ be any eighth-order character $\bmod p$. For any integer $k \geq 0$, we define the

sequence $F_k(p)$ as

$$F_k(p) = \frac{\tau^k(\psi)}{\tau^k(\psi^3)} + \frac{\tau^k(\psi^3)}{\tau^k(\psi)}. \tag{1}$$

The sequence $F_k(p)$ defined in (1) is clearly a second-order linear recurrence sequence. However, to find the exact value of this sequence, noting that $F_0(p) = 2$, we must know its first term $F_1(p)$. Generally, $F_1(p)$ is very difficult to calculate. But if ψ is an eighth-order character $\bmod\, p$, then we can deduce some interesting results. In this paper, we will focus on illustrating this point. That is, we shall prove the following two results.

Theorem 1 *Let p be a prime with $p \equiv 1 \bmod 8$, then, for any integer $k \geq 2$, we have the second-order linear recursive formula*

$$F_k(p) = C \cdot F_{k-1}(p) - F_{k-2}(p),$$

where $F_0(p) = 2$, $C = F_1(p) = \pm\sqrt{2 + \frac{2\alpha}{\sqrt{p}}}$, and the constant $\alpha = \alpha(p)$ is an integer, which is closely related to prime p.

In fact, we have a very important square-sum formula,

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

where $(\frac{*}{p})$ denotes the Legendre symbol $\bmod\, p$, r is any integer with $(\frac{r}{p}) = -1$ (see Theorem 4-11 in [9]).

Theorem 2 *Let p be a prime with $p \equiv 1 \bmod 8$, then, for any real number $k \geq 2$, we have the second-order linear recursive formula*

$$F_{2k}(p) = \frac{2\alpha}{\sqrt{p}} \cdot F_{2k-2}(p) - F_{2k-4}(p),$$

where $F_0(p) = 2$ and $F_2(p) = \frac{2\alpha}{\sqrt{p}}$.

Since $|\alpha| \leq \sqrt{p}$, the two roots of the equation $x^2 - \frac{2\alpha}{\sqrt{p}}x + 1 = 0$ are

$$x_1 = \frac{\alpha + i\sqrt{p - \alpha^2}}{\sqrt{p}} \quad \text{and} \quad x_2 = \frac{\alpha - i\sqrt{p - \alpha^2}}{\sqrt{p}},$$

where i is the imaginary unit. That is, $i^2 = -1$.

Therefore, from the properties of the second-order linear recursive sequence we have the computational formula

$$F_{2k}(p) = \left(\frac{\alpha + i\sqrt{p - \alpha^2}}{\sqrt{p}} \right)^k + \left(\frac{\alpha + i\sqrt{p - \alpha^2}}{\sqrt{p}} \right)^k.$$

Some notes: How to determine the positive or negative signs of $C = F_1(p)$ in Theorem 1 is an interesting open problem.

It is clear that $\phi(5) = \phi(8) = \phi(12) = 4$. Therefore, whether there is a similar second-order linear recurrence formula for the fifth-order (or twelfth-order) character $\bmod p$ remains to be further studied.

2 Several lemmas

In this section, we need to prove several simple lemmas, which is necessary in the proofs of our theorems. Hereinafter, we shall use many properties of the classical Gauss sum and Dirichlet characters $\bmod p$ (an odd prime); all of them can be found in Ref. [10], so they will not be repeated here.

Lemma 1 *Let p be a prime with $p \equiv 1 \bmod 8$, ψ be an eighth-order character $\bmod p$. Then we have the identity*

$$\tau^2(\overline{\psi}^2) = p \cdot \frac{\tau^2(\psi^3)}{\tau^2(\psi)}.$$

Proof Since $p \equiv 1 \bmod 8$, there exist 4 eighth-order characters $\bmod p$, let ψ be one of them; χ_2 denotes the Legendre symbol $\bmod p$. For any integer m with $(m, p) = 1$, note that we have the identities $\overline{\psi} \chi_2 = \psi^3$ and

$$\sum_{a=0}^{p-1} e\left(\frac{ma^2}{p}\right) = \sum_{a=0}^{p-1}\left(1 + \chi_2(a)\right)e\left(\frac{ma}{p}\right) = \chi_2(m)\tau(\chi_2) = \chi_2(m)\sqrt{p},$$

from the properties of the classical Gauss sum we have

$$\begin{aligned}
\sum_{a=0}^{p-1} \psi\left(a^2 - 1\right) &= \frac{1}{\tau(\overline{\psi})} \sum_{a=0}^{p-1}\sum_{b=1}^{p-1} \overline{\psi}(b)e\left(\frac{b(a^2 - 1)}{p}\right) \\
&= \frac{1}{\tau(\overline{\psi})} \sum_{b=1}^{p-1} \overline{\psi}(b)e\left(\frac{-b}{p}\right) \sum_{a=0}^{p-1} e\left(\frac{ba^2}{p}\right) \\
&= \frac{\sqrt{p}}{\tau(\overline{\psi})} \sum_{b=1}^{p-1} \overline{\psi}(b)\chi_2(b)e\left(\frac{-b}{p}\right) \\
&= \frac{\psi(-1)\sqrt{p}}{\tau(\overline{\psi})} \sum_{b=1}^{p-1} \psi^3(b)e\left(\frac{b}{p}\right) \\
&= \frac{\psi(-1)\sqrt{p} \cdot \tau(\psi^3)}{\tau(\overline{\psi})}.
\end{aligned} \tag{2}$$

On the other hand, from the properties of the classical Gauss sum we also have

$$\begin{aligned}
\sum_{a=0}^{p-1} \psi\left(a^2 - 1\right) &= \sum_{a=0}^{p-1} \psi\left((a+1)^2 - 1\right) = \sum_{a=1}^{p-1} \psi\left(a(a+2)\right) \\
&= \frac{1}{\tau(\overline{\psi})} \sum_{b=1}^{p-1} \overline{\psi}(b) \sum_{a=1}^{p-1} \psi(a)e\left(\frac{b(a+2)}{p}\right) = \frac{\tau(\psi)}{\tau(\overline{\psi})} \sum_{b=1}^{p-1} \overline{\psi}^2(b)e\left(\frac{2b}{p}\right) \\
&= \psi^2(2) \cdot \frac{\tau(\overline{\psi}^2)\tau(\psi)}{\tau(\overline{\psi})}.
\end{aligned} \tag{3}$$

Note that $\psi^4 = \chi_2$ and $\chi_2(2) = 1$, from (2) and (3) we have the identity

$$\tau^2(\overline{\psi}^2) = p \cdot \frac{\tau^2(\psi^3)}{\tau^2(\psi)}.$$

This proves Lemma 1. □

Lemma 2 *Let p be an odd prime with $p \equiv 1 \bmod 4$, λ be any fourth-order character $\bmod p$. Then we have the identity*

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

Proof See Lemma 2.2 in [3]. □

Lemma 3 *Let p be a prime with $p \equiv 1 \bmod 8$, ψ be an eighth-order character $\bmod p$. Then we have the identity*

$$\frac{\tau^2(\psi)}{\tau^2(\psi^3)} + \frac{\tau^2(\psi^3)}{\tau^2(\psi)} = \frac{2\alpha}{\sqrt{p}},$$

where α is defined as in Theorem 1.

Proof It it clear that if ψ is an eighth-order character $\bmod p$, then ψ^3 is also an eighth-order character $\bmod p$. So substituting ψ by ψ^3 in Lemma 1, and noting that $\psi^9 = \psi$, $\overline{\psi}^6 = \psi^2$, from Lemma 1 we have

$$\tau^2(\psi^2) = p \cdot \frac{\tau^2(\psi)}{\tau^2(\psi^3)}. \tag{4}$$

Note that ψ^2 is a fourth-order character $\bmod p$, from (4), Lemma 1 and Lemma 2 we may immediately deduce the identity

$$p\left(\frac{\tau^2(\psi)}{\tau^2(\psi^3)} + \frac{\tau^2(\psi^3)}{\tau^2(\psi)}\right) = \tau^2(\psi^2) + \tau^2(\overline{\psi}^2) = 2\sqrt{p} \cdot \alpha,$$

which implies the identity

$$\frac{\tau^2(\psi)}{\tau^2(\psi^3)} + \frac{\tau^2(\psi^3)}{\tau^2(\psi)} = \frac{2\alpha}{\sqrt{p}}.$$

This proves Lemma 3. □

3 Proofs of the theorems

Now we will complete the proofs of our main results. First we prove Theorem 1. Let p be a prime with $p \equiv 1 \bmod 8$, ψ be an eighth-order character $\bmod p$. For any integer $k \geq 0$, we define

$$F_k(p) = \frac{\tau^k(\psi)}{\tau^k(\psi^3)} + \frac{\tau^k(\psi^3)}{\tau^k(\psi)}.$$

It is clear that from Lemma 3 we have $F_0(p) = 2$ and

$$\frac{2\alpha}{\sqrt{p}} + 2 = \frac{\tau^2(\psi)}{\tau^2(\psi^3)} + \frac{\tau^2(\psi^3)}{\tau^2(\psi)} + 2 = \left(\frac{\tau(\psi)}{\tau(\psi^3)} + \frac{\tau(\psi^3)}{\tau(\psi)} \right)^2. \tag{5}$$

From (5) we can deduce that

$$F_1(p) = \pm\sqrt{2\left(1 + \frac{\alpha}{\sqrt{p}}\right)} = C. \tag{6}$$

If $k \geq 1$, then from the definition of $F_k(p)$ we have

$$F_k(p) \cdot F_1(p) = \left(\frac{\tau^k(\psi)}{\tau^k(\psi^3)} + \frac{\tau^k(\psi^3)}{\tau^k(\psi)} \right)\left(\frac{\tau(\psi)}{\tau(\psi^3)} + \frac{\tau(\psi^3)}{\tau(\psi)} \right) = F_{k+1}(p) + F_{k-1}(p)$$

or the second-order linear recursive formula

$$F_{k+1}(p) = C \cdot F_k(p) - F_{k-1}(p),$$

where $F_0(p) = 2$ and $F_1(p) = \pm\sqrt{2(1 + \frac{\alpha}{\sqrt{p}})}$.

This proves Theorem 1.

Similarly, we can deduce Theorem 2. In fact, for any integer $k \geq 1$, from Lemma 3 we have

$$\frac{2\alpha}{\sqrt{p}} \cdot F_{2k}(p) = \left(\frac{\tau^2(\psi)}{\tau^2(\psi^3)} + \frac{\tau^2(\psi^3)}{\tau^2(\psi)} \right)\left(\frac{\tau^{2k}(\psi)}{\tau^{2k}(\psi^3)} + \frac{\tau^{2k}(\psi^3)}{\tau^{2k}(\psi)} \right) = F_{2k+2}(p) + F_{2k-2}(p)$$

or the second-order linear recursive formula

$$F_{2k}(p) = \frac{2\alpha}{\sqrt{p}} \cdot F_{2k-2}(p) + F_{2k-4}(p),$$

where the first two terms are $F_0(p) = 2$ and $F_2(p) = \frac{2\alpha}{\sqrt{p}}$.

This completes the proof of Theorem 2.

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

Authors' contributions
All authors have equally contributed to this work. All authors read and approved the final manuscript.

Publisher's Note
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

References
1. Wenpeng, Z., Jiayuan, H.: The number of solutions of the diagonal cubic congruence equation $\mod p$. Math. Rep. **20**(1), 70–76 (2018)
2. Berndt, B.C., Evans, R.J.: The determination of Gauss sums. Bull. Am. Math. Soc. **5**, 107–128 (1981)
3. Zhuoyu, C., Wenpeng, Z.: On the fourth-order linear recurrence formula related to classical Gauss sums. Open Math. **15**, 1251–1255 (2017)
4. Shimeng, S., Wenpeng, Z.: On the quartic Gauss sums and their recurrence property. Adv. Differ. Equ. **2017**, 43 (2017)
5. Wenpeng, Z., Di, H.: On the sixth power mean of the two-term exponential sums. J. Number Theory **136**, 403–413 (2014)
6. Li, C., Jiayuan, H.: A linear recurrence formula involving cubic Gauss sums and Kloosterman sums. Acta Math. Sinica (Chin. Ser.) **61**, 67–72 (2018)
7. Chowla, S., Cowles, J., Cowles, M.: On the number of zeros of diagonal cubic forms. J. Number Theory **9**, 502–506 (1977)
8. Berndt, B.C., Evans, R.J.: Sums of Gauss, Jacobi, and Jacobsthal. J. Number Theory **11**, 349–389 (1979)
9. Wenpeng, Z., Hailong, L.: Elementary Number Theory. Shaanxi Normal University Press, Xi'an (2013)
10. Apostol, T.M.: Introduction to Analytic Number Theory. Springer, New York (1976)