AIMS Mathematics, 9(10): 26557–26578.
DOI: 10.3934/math.20241292
Received: 30 June 2024
Revised: 23 August 2024
Accepted: 30 August 2024
Published: 13 September 2024

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

Research article

Ternary cyclotomic numbers and ternary Jacobi sums

Zhichao Tang and Xiang Fan*

School of Mathematics, Sun Yat-sen University, Guangzhou 510275, China

* **Correspondence:** Email: fanx8@mail.sysu.edu.cn.

Abstract: Cyclotomic numbers and Jacobi sums, introduced over two centuries ago by Gauss and Jacobi, respectively, are pivotal in number theory and find wide applications in combinatorial designs, coding theory, cryptography, and information theory. The cyclotomic problem, focused on determining all cyclotomic numbers, or equivalently evaluating all Jacobi sums of a given order, has been a subject of extensive research. This paper explores their trivariate counterparts, termed "ternary cyclotomic numbers" and "ternary Jacobi sums", highlighting the fundamental properties that mirror those of the classical cases. We show the ternary versions of Fourier series expansions, two symmetry properties, and a summation equation. We further demonstrate that ternary Jacobi sums, with at least one trivial variable, can be evaluated in terms of classical Jacobi sums of the same order. These properties are established through elementary methods that parallel those utilized in classical cases. Based on these properties, then we offer explicit calculations for all ternary Jacobi sums and ternary cyclotomic numbers of order $e = 2$, and near-complete results for order $e = 3$, with the exception of the elusive integer $J_3(1, 1, 2)$ for us.

Keywords: cyclotomic number; Jacobi sum; cyclotomic problem; finite field
Mathematics Subject Classification: 11T22, 11T24

1. Introduction

Let $\mathbb{F}_q$ be the finite field of q elements, where $q = p^\alpha$ with a prime p and a positive integer α. Suppose that

$$q - 1 = ef$$

with positive integers e and f. Choose a generator γ of the multiplicative cyclic group

$$\mathbb{F}_q^* = \mathbb{F}_q - \{0\}.$$

For $v \in \mathbb{F}_q^*$, let $\mathrm{ind}_\gamma(v)$ denote the unique non-negative integer $m \leqslant q - 2$ such that $v = \gamma^m$.

For $0 \leqslant i, j \leqslant e-1$ (*or rather for* i, j *modulo* e), the e^2 **cyclotomic numbers** of order e, denoted by A_{ij} (*or* $A_{ij}^{(e)}$ *to indicate the order* e), are defined as the cardinality of the set X_{ij}, where

$$X_{ij} := \{v \in \mathbb{F}_q - \{0, -1\} \mid \mathrm{ind}_\gamma(v) \equiv i \,(\mathrm{mod}\, e),\ \mathrm{ind}_\gamma(v+1) \equiv j \,(\mathrm{mod}\, e)\}.$$

Introduced by Gauss [1,2] over two hundred years ago, cyclotomic numbers are a significant concept in number theory with deep connections to various mathematical areas. They have been extensively applied in combinatorial designs, coding theory, cryptography, and information theory (see [3–6]). For both theoretical and practical purposes, it is intriguing to determine all cyclotomic numbers of a given order e for all finite fields, a task usually called the **cyclotomic problem**.

In the case $q = p$, Gauss [1, §358] evaluated $A_{ij}^{(3)}$ in terms of (L, M) satisfying the Diophantine system

$$4p = L^2 + 27M^2, \quad \text{with} \quad L \equiv 1 \,(\mathrm{mod}\, 3).$$

This system determines L **uniquely** and M up to signs. Similarly, Gauss [2] evaluated $A_{ij}^{(4)}$ in terms of (a, b) satisfying

$$p = a^2 + b^2, \quad \text{with} \quad a \equiv 1 \,(\mathrm{mod}\, 4),$$

which fixes a **uniquely** and b up to signs. His results indicated that solving the cyclotomic problem over $\mathbb{F}_q$ generally requires more than just the value of q and order e; it also needs a quadratic partition of q.

Therefore, classical solutions to the cyclotomic problem are typically expressed using an appropriately chosen solution of a relevant Diophantine system (consisting of equations and congruences), often with the *sign ambiguity*. In this sense, many mathematicians have investigated the cyclotomic problem for various small orders $\leqslant 22$ (see Dickson's early foundational work [7–9] and a good recent survey [10]), as well as for special orders such as [11–13] for l, [13, 14] for $2l$, [15] for l^2, and [16, 17] for $2l^2$ (with an odd prime l).

While Gauss initially approached cyclotomy via Gauss sums, Dickson's use of Jacobi sums [7] laid the groundwork for modern cyclotomy. The cyclotomic problem is, in fact, equivalent to the explicit evaluation of Jacobi sums of the same order. Let us recall the definiton of Jacobi sums. Let ζ be a primitive complex e-th root of unity fixed once for all. We define a multiplicative character χ_e of order e on $\mathbb{F}_q^*$ by

$$\chi_e(\gamma^m) = \zeta^m \quad (\text{for any } m \in \mathbb{Z}),$$

and extend χ_e to a character on $\mathbb{F}_q$ by taking $\chi_e(0) = 0$. For convenience, we assume

$$\chi_e^m(0) = 0$$

for any integer m. The **Jacobi sums** $J(i, j)$ (*or* $J_e(i, j)$ *to indicate the order* e) of order e, for $0 \leqslant i, j \leqslant e-1$ (*or rather for* i, j *modulo* e), are defined by

$$J(i, j) = \sum_{v \in \mathbb{F}_q} \chi_e^i(v)\chi_e^j(v+1).$$

Jacobi sums and cyclotomic numbers are related by the following *finite Fourier series expansions*:

$$J(a, b) = \sum_{0 \leqslant i, j \leqslant e-1} A_{ij}\zeta^{ai+bj}, \quad e^2 A_{ab} = \sum_{0 \leqslant i, j \leqslant e-1} J(i, j)\zeta^{-(ai+bj)}.$$

To calculate all cyclotomic numbers of order e, it suffices to calculate all Jacobi sums of order e, and vice versa.

Jacobi made significant contributions to mathematics, including the Jacobi symbol, the Jacobi triple product, the Jacobi elliptic functions, and the Jacobian in variable transformations. Among his notable discoveries are Jacobi sums, which he proposed in 1827 in a letter to Gauss and published ten years later. These sums were later extended by Cauchy, Gauss, and Eisenstein. While Gauss sums are pivotal in proving quadratic reciprocity, Jacobi sums are essential for proving cubic reciprocity and were generalized by Eisenstein for biquadratic reciprocity. Jacobi sums are also used to estimate the number of integer solutions to congruences like

$$x^3 + y^3 \equiv 1 \pmod{p},$$

which are crucial for developing the Weil conjectures [18]. In modern mathematics, Jacobi sums have found applications in primality testing [19].

Wamelen [20] has provided an inductive arithmetic approach to characterize all Jacobi sums of any order, thereby solving the cyclotomic problem in theory. However, the Diophantine system he employed is notably large and intricate in general. In recent years, there has been growing interest in efficiently computing Jacobi sums [21], driven by their importance in applications such as primality testing, cryptosystems, combinatorial designs, and advanced number theory problems [19, 22].

For given $\mathbb{F}_q$, γ, and ζ, classical cyclotomic numbers and Jacobi sums are binary functions depending on two variables $i, j \in \mathbb{Z}/e\mathbb{Z}$. The purpose of this paper is to investigate their trivariate analogs, so-called "*ternary cyclotomic numbers*" and "*ternary Jacobi sums*", defined in Section 2. As classical cyclotomic numbers and Jacobi sums are important both theoretically and practically, we want to study their ternary counterparts in order to explore theoretically interesting problems or potential applications. In Section 2, we obtain some ternary properties, which are analogous to those of classical cyclotomic numbers and Jacobi sums, with proofs similar to those of classical ones. Then we use these properties to solve the cyclotomic problem for ternary cyclotomic numbers. Section 3 provides explicit evaluations of all ternary cyclotomic numbers and ternary Jacobi sums for order $e = 2$, and Section 4 nearly completes the evaluation for order $e = 3$, except for an integer $J_3(1, 1, 2)$, which remains unknown. Our calculations show that ternary Jacobi sums, which are some kind of character sums, cannot generally be transformed into classical Jacobi sums. So the cyclotomic problem for ternary cyclotomic numbers has its own interests in theory.

2. Ternary cyclotomic numbers and Jacobi sums with properties

Let $\mathbb{F}_q, \gamma, \zeta, \chi_e$ and

$$q = p^\alpha = ef + 1$$

be as described in Section 1. We further assume

$$q = ef + 1$$

is **odd** for convenience. (The upcoming definitions will be meaningless for $\mathbb{F}_{2^\alpha}$, where $v - 1 = v + 1$.) Specifically, either e or f is even.

For $0 \leqslant i, j, k \leqslant e-1$ (*or rather for* $i, j, k \in \mathbb{Z}/e\mathbb{Z}$), we define the **ternary cyclotomic numbers** of order e, denoted by A_{ijk} (*or* $A^{(e)}_{ijk}$ *to indicate the order* e), as the cardinality of the set

$$X_{ijk} := \{v \in \mathbb{F}_q - \{0, \pm 1\} \mid \mathrm{ind}_\gamma(v-1) \equiv i \,(\mathrm{mod}\, e),\ \mathrm{ind}_\gamma v \equiv j \,(\mathrm{mod}\, e),\ \mathrm{ind}_\gamma(v+1) \equiv k \,(\mathrm{mod}\, e)\}.$$

This definition relies on the choice of a multiplicative generator γ of $\mathbb{F}_q^*$. We also define the **ternary Jacobi sums** of order e, denoted by $J(i, j, k)$ (*or* $J_e(i, j, k)$ *to indicate the order* e), as

$$J(i, j, k) := \sum_{v \in \mathbb{F}_q} \chi_e^i(v-1)\chi_e^j(v)\chi_e^k(v+1).$$

This definition depends on the character χ_e on $\mathbb{F}_q$, which is determined by the selections of γ and ζ (as $\chi_e(\gamma^m) = \zeta^m$ and $\chi_e(0) = 0$). Clearly, we have

$$X_{ijk} = \{v \in \mathbb{F}_q \mid \chi_e(v-1) = \zeta^i,\ \chi_e(v) = \zeta^j,\ \chi_e(v+1) = \zeta^k\}.$$

Our definition of the ternary Jacobi sum can be viewed as a special case of the character sums studied in [23].

To calculate all ternary cyclotomic numbers of order e, it suffices to calculate all ternary Jacobi sums of order e, and vice versa, by the following *finite Fourier series expansions*.

Proposition 1. ***(Finite Fourier series expansions)*** *The ternary cyclotomic numbers and ternary Jacobi sums of the same order e are related by: for any* $a, b, c \in \mathbb{Z}/e\mathbb{Z}$,

$$J(a, b, c) = \sum_{i,j,k \in \mathbb{Z}/e\mathbb{Z}} A_{ijk}\zeta^{ai+bj+ck}, \tag{2.1}$$

$$e^3 A_{abc} = \sum_{i,j,k \in \mathbb{Z}/e\mathbb{Z}} J(i, j, k)\zeta^{-(ai+bj+ck)}. \tag{2.2}$$

Proof. Note that

$$\mathbb{F}_q = \{0, \pm 1\} \cup \bigcup_{i,j,k \in \mathbb{Z}/e\mathbb{Z}} X_{ijk}.$$

For $v \in \{0, \pm 1\}$,

$$\chi_e^a(v-1)\chi_e^b(v)\chi_e^c(v+1) = 0.$$

For the A_{ijk} elements $v \in X_{ijk}$,

$$\chi_e^a(v-1)\chi_e^b(v)\chi_e^c(v+1) = \zeta^{ai+bj+ck}.$$

Summing them all together, we obtain Eq (2.1). For the Eq (2.2), noting that $\zeta = \chi_e(\gamma)$, we have

$$\begin{aligned}\sum_{i,j,k \in \mathbb{Z}/e\mathbb{Z}} J(i, j, k)\zeta^{-(ai+bj+ck)} &= \sum_{i,j,k \in \mathbb{Z}/e\mathbb{Z}} \sum_{v \in \mathbb{F}_q} \chi_e^i(v-1)\chi_e^j(v)\chi_e^k(v+1)\chi_e(\gamma)^{-(ai+bj+ck)} \\ &= \sum_{v \in \mathbb{F}_q} \Big(\sum_{i=0}^{e-1} \chi_e^i\Big(\frac{v-1}{\gamma^a}\Big)\Big)\Big(\sum_{j=0}^{e-1} \chi_e^j\Big(\frac{v}{\gamma^b}\Big)\Big)\Big(\sum_{k=0}^{e-1} \chi_e^k\Big(\frac{v+1}{\gamma^c}\Big)\Big).\end{aligned}$$

Note that

$$\sum_{j=0}^{e-1}\chi_e^j\Big(\frac{v}{\gamma^b}\Big)=\begin{cases}e, & \text{if } v\neq 0 \text{ and } \mathrm{ind}_\gamma(v)\equiv b\,(\mathrm{mod}\,e),\\ 0, & \text{if } v=0 \text{ or } \mathrm{ind}_\gamma(v)\not\equiv b\,(\mathrm{mod}\,e),\end{cases}$$

and similar for $\sum_{i=0}^{e-1}\chi_e^i\Big(\frac{v-1}{\gamma^a}\Big)$ and $\sum_{j=0}^{e-1}\chi_e^k\Big(\frac{v+1}{\gamma^c}\Big)$. So the terms of the above sum are non-zero only when $v\in X_{abc}$, and thus

$$\sum_{i,j,k\in\mathbb{Z}/e\mathbb{Z}}J(i,j,k)\zeta^{-(ai+bj+ck)}=\sum_{v\in X_{abc}}e^3=e^3A_{abc}. \qquad \square$$

Following arguments often involve the value of $\chi_e(-1)$. Since

$$\gamma^{\frac{q-1}{2}}=-1\in\mathbb{F}_q,$$

and when e is even,

$$\zeta^{\frac{e}{2}}=-1\in\mathbb{C},$$

we have

$$\chi_e(-1)^{-1}=\chi_e(-1)=\chi_e(\gamma^{\frac{q-1}{2}})=\zeta^{\frac{ef}{2}}=\begin{cases}1, & \text{if } f \text{ is even},\\ \zeta^{\frac{e}{2}}=-1, & \text{if } f \text{ is odd},\end{cases}=(-1)^f.$$

Classical cyclotomic numbers exhibit a symmetry property in their two variables:

$$A_{ij}=A_{j+\frac{ef}{2},i+\frac{ef}{2}}=\begin{cases}A_{ji}, & \text{if } f \text{ is even},\\ A_{j+\frac{e}{2},i+\frac{e}{2}}, & \text{if } f \text{ is odd},\end{cases}$$

which implies that

$$J(a,b)=(-1)^{f(a+b)}J(b,a).$$

It is similar for ternary cyclotomic numbers and ternary Jacobi sums.

Proposition 2. *For any $i,j,k\in\mathbb{Z}/e\mathbb{Z}$,*

$$A_{ijk}=A_{k+\frac{ef}{2},j+\frac{ef}{2},i+\frac{ef}{2}}=\begin{cases}A_{kji}, & \textit{if } f \textit{ is even},\\ A_{k+\frac{e}{2},j+\frac{e}{2},i+\frac{e}{2}}, & \textit{if } f \textit{ is odd}.\end{cases}$$

Proof. For any $v\in\mathbb{F}_q$, let $w=-v$. Since

$$\chi_e(-1)=\zeta^{\frac{ef}{2}},$$

we have

$$\begin{aligned}v\in X_{ijk} &\iff (\chi_e(-w-1),\chi_e(-w),\chi_e(-w+1))=(\zeta^i,\zeta^j,\zeta^k)\\ &\iff (\chi_e(w-1),\chi_e(w),\chi_e(w+1))=(\chi_e(-1)\zeta^k,\chi_e(-1)\zeta^j,\chi_e(-1)\zeta^i)\\ &\iff w\in X_{k+\frac{ef}{2},j+\frac{ef}{2},i+\frac{ef}{2}}.\end{aligned}$$

So $v\mapsto -v$ induces a bijection from X_{ijk} to $X_{k+\frac{ef}{2},j+\frac{ef}{2},i+\frac{ef}{2}}$. $\square$

Corollary 3. *For any $a, b, c \in \mathbb{Z}/e\mathbb{Z}$,*

$$J(a,b,c) = (-1)^{f(a+b+c)} J(c,b,a).$$

As a consequence, when both f and b are odd, we have $J(a,b,a) = 0$.

Proof. By Propositions 1 and 2, as

$$\zeta^{-\frac{ef}{2}} = (-1)^f,$$

we have

$$\begin{aligned} J(a,b,c) &= \sum_{i,j,k \in \mathbb{Z}/e\mathbb{Z}} A_{k+\frac{ef}{2}, j+\frac{ef}{2}, i+\frac{ef}{2}} \zeta^{ai+bj+ck} \\ &= \sum_{l,m,n \in \mathbb{Z}/e\mathbb{Z}} A_{lmn} \zeta^{a(n-\frac{ef}{2})+b(m-\frac{ef}{2})+c(l-\frac{ef}{2})} \\ &= \zeta^{-\frac{ef}{2}(a+b+c)} \sum_{l,m,n \in \mathbb{Z}/e\mathbb{Z}} A_{lmn} \zeta^{cl+bm+an} \\ &= (-1)^{f(a+b+c)} J(c,b,a). \end{aligned}$$

□

Classical cyclotomic numbers exhibit another property

$$A_{ij} = A_{-i,j-i},$$

which implies that

$$J(a,b) = J(-a-b,b).$$

It is similar for ternary cases as follows:

Proposition 4. *For any $i, j, k \in \mathbb{Z}/e\mathbb{Z}$,*

$$A_{ijk} = A_{i-j+\frac{ef}{2},-j,k-j} = \begin{cases} A_{i-j,-j,k-j}, & \text{if } f \text{ is even}, \\ A_{i-j+\frac{e}{2},-j,k-j}, & \text{if } f \text{ is odd}. \end{cases}$$

Proof. For any $v \in \mathbb{F}_q$, let $w = v^{-1}$. Since

$$\chi_e(-1) = \zeta^{\frac{ef}{2}},$$

we have

$$\begin{aligned} v \in X_{ijk} &\iff (\chi_e(w^{-1}-1), \chi_e(w^{-1}), \chi_e(w^{-1}+1)) = (\zeta^i, \zeta^j, \zeta^k) \\ &\iff \left(\frac{\chi_e(w-1)}{\chi_e(-1)\chi_e(w)}, \chi_e(w), \frac{\chi_e(1+w)}{\chi_e(w)} \right) = (\zeta^i, \zeta^{-j}, \zeta^k) \\ &\iff (\chi_e(w-1), \chi_e(w), \chi_e(w+1)) = (\chi_e(-1)\zeta^{i-j}, \zeta^{-j}, \zeta^{k-j}) \\ &\iff w \in X_{i-j+\frac{ef}{2},-j,k-j}. \end{aligned}$$

So $v \mapsto v^{-1}$ induces a bijection from X_{ijk} to $X_{i-j+\frac{ef}{2},-j,k-j}$. □

Corollary 5. *For any $a, b, c \in \mathbb{Z}/e\mathbb{Z}$,*

$$J(a, b, c) = (-1)^{fa} J(a, -a - b - c, c).$$

Proof. By Propositions 1 and 4, as

$$\zeta^{-\frac{ef}{2}} = (-1)^f,$$

we have

$$\begin{aligned} J(a, b, c) &= \sum_{i,j,k \in \mathbb{Z}/e\mathbb{Z}} A_{i-j+\frac{ef}{2}, -j, k-j} \zeta^{ai+bj+ck} \\ &= \sum_{l,m,n \in \mathbb{Z}/e\mathbb{Z}} A_{l,m,n} \zeta^{a(l-m-\frac{ef}{2})-bm+c(n-m)} \\ &= (\zeta^{-\frac{ef}{2}})^a \sum_{l,m,n \in \mathbb{Z}/e\mathbb{Z}} A_{l,m,n} \zeta^{al+(-a-b-c)m+cn} \\ &= (-1)^{fa} J(a, -a - b - c, c). \end{aligned}$$

□

For classical cyclotomic numbers, we have

$$\sum_{i \in \mathbb{Z}/e\mathbb{Z}} A_{ij} = \begin{cases} f - 1, & \text{if } j \equiv 0 \pmod{e}, \\ f, & \text{otherwise,} \end{cases} \quad \text{and} \quad \sum_{j \in \mathbb{Z}/e\mathbb{Z}} A_{ij} = \begin{cases} f - 1, & \text{if } i \equiv \frac{ef}{2} \pmod{e}, \\ f, & \text{otherwise.} \end{cases} \tag{2.3}$$

We show similar equations for ternary cyclotomic numbers.

Proposition 6. *Let $g = \mathrm{ind}_\gamma(2)$. For any $i, j, k \in \mathbb{Z}/e\mathbb{Z}$,*

$$\begin{aligned} \sum_{t \in \mathbb{Z}/e\mathbb{Z}} A_{tjk} &= \begin{cases} A_{jk} - 1, & \textit{if } j \equiv 0 \pmod{e} \textit{ and } k \equiv g \pmod{e}, \\ A_{jk}, & \textit{otherwise}, \end{cases} \\ \sum_{t \in \mathbb{Z}/e\mathbb{Z}} A_{ijt} &= \begin{cases} A_{ij} - 1, & \textit{if } i \equiv g + \frac{ef}{2} \pmod{e} \textit{ and } j \equiv \frac{ef}{2} \pmod{e}, \\ A_{ij}, & \textit{otherwise}, \end{cases} \\ \sum_{t \in \mathbb{Z}/e\mathbb{Z}} A_{itk} &= \begin{cases} A_{i-g,k-g} - 1, & \textit{if } i \equiv \frac{ef}{2} \pmod{e} \textit{ and } k \equiv 0 \pmod{e}, \\ A_{i-g,k-g}, & \textit{otherwise}. \end{cases} \end{aligned}$$

Proof. Note that

$$\bigcup_{t \in \mathbb{Z}/e\mathbb{Z}} X_{tjk} = X_{jk} - \{1\}.$$

Also note that $1 \in X_{jk}$ if and only if

$$j \equiv 0 \pmod{e} \quad \text{and} \quad k \equiv g \pmod{e}.$$

These X_{tjk} are pairwise disjoint, which gives the first equation.

For the second equation,

$$\bigcup_{t \in \mathbb{Z}/e\mathbb{Z}} X_{ijt} = \{v \in \mathbb{F}_q - \{0, \pm 1\} \mid \chi_e(v - 1) = \zeta^i,\ \chi_e(v) = \zeta^j\}.$$

So

$$v \in \bigcup_{t\in\mathbb{Z}/e\mathbb{Z}} X_{ijt}$$

if and only if

$$v - 1 \in X_{ij} - \{-2\}.$$

Also note that $-2 \in X_{ij}$ if and only if

$$i \equiv g + \frac{ef}{2} \pmod{e} \text{ and } j \equiv \frac{ef}{2} \pmod{e}.$$

For the third equation,

$$\bigcup_{t\in\mathbb{Z}/e\mathbb{Z}} X_{itk} = \{v \in \mathbb{F}_q - \{0, \pm 1\} \mid \chi_e(v-1) = \zeta^i,\ \chi_e(v+1) = \zeta^k\}.$$

Then

$$v \in \bigcup_{t\in\mathbb{Z}/e\mathbb{Z}} X_{itk}$$

if and only if

$$\frac{v-1}{2} \in X_{i-g,k-g} - \{-2^{-1}\}.$$

Here

$$v \mapsto \frac{v-1}{2}$$

induces a bijection on $\mathbb{F}_q$. Also note that

$$-2^{-1} \in X_{i-g,k-g}$$

if and only if

$$i \equiv \frac{ef}{2} \pmod{e} \text{ and } k \equiv 0 \pmod{e}.$$ □

Note that

$$\sum_{v\in\mathbb{F}_q} \chi_e^i(v) = \sum_{m=0}^{q-2} \chi_e^i(\gamma^m) = \sum_{m=0}^{q-2} (\zeta^i)^m = \begin{cases} q-1, & \text{if } i \equiv 0 \pmod{e}, \\ 0, & \text{otherwise.} \end{cases}$$

So classical Jacobi sums $J(i, 0)$ and $J(0, i)$ can be easily evaluated by

$$\begin{aligned} (-1)^{fi} J(i,0) = J(0,i) &= \sum_{v\in\mathbb{F}_q} \chi_e^0(v)\chi_e^i(v+1) = \sum_{v\in\mathbb{F}_q} \chi_e^i(v+1) - \chi_e^i(1) \\ &= \begin{cases} q-2, & \text{if } i \equiv 0 \pmod{e}, \\ -1, & \text{otherwise.} \end{cases} \end{aligned} \tag{2.4}$$

Similarly, ternary Jacobi sums $J(i, j, k)$, with either i, j or k divided by e, can be evaluated in terms of classical Jacobi sums of the same order e.

Proposition 7. *Let $g = \mathrm{ind}_\gamma(2)$. For $i, j, k \in \mathbb{Z}/e\mathbb{Z}$, we have*

$$\begin{aligned} J(0, j, k) &= J(j, k) - \zeta^{gk}, \\ J(i, j, 0) &= J(i, j) - (-1)^{f(i+j)}\zeta^{gi}, \\ J(i, 0, k) &= \zeta^{g(i+k)}J(i, k) - (-1)^{fi}. \end{aligned}$$

Proof. Recall that

$$\chi_e^m(0) = 0$$

for any $m \in \mathbb{Z}$, we have

$$\chi_e(2) = \zeta^g \text{ and } \chi_e(-1) = (-1)^f.$$

So

$$\begin{aligned} J(0, j, k) &= \sum_{v\in\mathbb{F}_q} \chi_e^0(v-1)\chi_e^j(v)\chi_e^k(v+1) \\ &= \sum_{v\in\mathbb{F}_q-\{1\}} \chi_e^j(v)\chi_e^k(v+1) \\ &= \sum_{v\in\mathbb{F}_q} \chi_e^j(v)\chi_e^k(v+1) - \chi_e^j(1)\chi_e^k(2) \\ &= J(j, k) - \zeta^{gk}, \\ J(i, j, 0) &= \sum_{v\in\mathbb{F}_q-\{-1\}} \chi_e^i(v-1)\chi_e^j(v) \\ &= \sum_{v\in\mathbb{F}_q} \chi_e^i(v-1)\chi_e^j(v) - \chi_e^i(-2)\chi_e^j(-1) \\ &= J(i, j) - (-1)^{f(i+j)}\zeta^{gi}. \end{aligned}$$

In the following we let

$$w = \frac{v-1}{2}.$$

Note that

$$v \mapsto \frac{v-1}{2}$$

induces a bijection on $\mathbb{F}_q$. Then

$$\begin{aligned} J(i, 0, k) &= \sum_{v\in\mathbb{F}_q} \chi_e^i(v-1)\chi_e^k(v+1) - \chi_e^i(-1)\chi_e^k(1) \\ &= \sum_{w\in\mathbb{F}_q} \chi_e^i(2w)\chi_e^k(2w+2) - (-1)^{fi} \\ &= \zeta^{g(i+k)}J(i, k) - (-1)^{fi}. \end{aligned}$$

□

Corollary 8.

$$J(0, 0, 0) = q - 3.$$

For $i \not\equiv 0 \pmod{e}$, we have

$$J(i,0,0) = (-1)^{fi+1}(1+\zeta^{gi}),$$
$$J(0,i,0) = -1-(-1)^{fi},$$
$$J(0,0,i) = -1-\zeta^{gi}.$$

To conclude this section, it is important to highlight a key result that will facilitate our subsequent calculations, as it is self-evident from the definition.

Lemma 9. *Let k be an integer coprime to e, and σ_k denote the $\mathbb{Q}$-automorphism of the field $\mathbb{Q}(\zeta)$ with*

$$\sigma_k(\zeta) = \zeta^k.$$

Then for any $a, b, c \in \mathbb{Z}/e\mathbb{Z}$, we have

$$J(ka,kb) = \sigma_k(J(a,b)),$$
$$J(ka,kb,kc) = \sigma_k(J(a,b,c)).$$

3. Evaluation for order $e = 2$

In this section, assuming

$$e = 2 \quad \text{and} \quad q = p^\alpha = 2f+1,$$

we calculate all ternary cyclotomic numbers and ternary Jacobi sums of order 2 for a generator γ of $\mathbb{F}_q^*$. We fix $\zeta = -1$, and let

$$g = \mathrm{ind}_\gamma(2).$$

By Eq (2.4) and

$$J_2(a,b) = J_2(-a-b,b),$$

all classical Jacobi sums of order 2 are:

$$J_2(0,0) = q-2, \quad J_2(1,0) = (-1)^{f+1}, \quad J_2(1,1) = J_2(0,1) = -1. \tag{3.1}$$

First, let us calculate $J_2(1,1,1)$ when f is even (which is this section's most challenging part). We will see that it is related to classical Jacobi sums of order 4. Let us take the imaginary unit

$$\mathrm{i} = \sqrt{-1}$$

as the primitive 4-th root ζ_4 of unity. We write $J_4(i,j)$ (with $i, j \in \mathbb{Z}/4\mathbb{Z}$) for the classical Jacobi sums of order 4 with respect to γ and ζ_4. Let χ_4 be the character of $\mathbb{F}_q$ defined by

$$\chi_4(0) = 0, \quad \chi_4(\gamma^m) = \zeta_4^m = \mathrm{i}^m \ \text{(for any } m \in \mathbb{Z}).$$

By definition,

$$J_4(i,j) = \sum_{v\in\mathbb{F}_q} \chi_4^i(v)\chi_4^j(v+1).$$

A critical insight is that

$$\chi_2 = \chi_4^2$$

on $\mathbb{F}_q$. Also note that

$$\mathbb{F}_q^* = \{\gamma^m \mid 0 \leqslant m \leqslant 2f-1\}.$$

So

$$\begin{aligned} J_2(1,1,1) &= \sum_{v\in\mathbb{F}_q} \chi_2(v-1)\chi_2(v)\chi_2(v+1) = \sum_{v\in\mathbb{F}_q^*} \chi_2(v)\chi_2(v^2-1) \\ &= \sum_{v\in\mathbb{F}_q^*} \chi_4(v^2)\chi_4^2(v^2-1) = \sum_{m=0}^{2f-1} \chi_4(\gamma^{2m})\chi_4^2(\gamma^{2m}-1) \\ &= 2\sum_{m=0}^{f-1} \chi_4(\gamma^{2m})\chi_4^2(\gamma^{2m}-1). \end{aligned}$$

The final expression is a part of the following formula:

$$\begin{aligned} J_4(2,1) &= \sum_{v\in\mathbb{F}_q} \chi_4^2(v)\chi_4(v+1) = \sum_{w\in\mathbb{F}_q} \chi_4^2(w-1)\chi_4(w) \\ &= \sum_{w\in\mathbb{F}_q^*} \chi_4(w)\chi_4^2(w-1) = \sum_{n=0}^{2f-1} \chi_4(\gamma^n)\chi_4^2(\gamma^n-1) \\ &= \sum_{m=0}^{f-1} \chi_4(\gamma^{2m})\chi_4^2(\gamma^{2m}-1) + \sum_{m=0}^{f-1} \chi_4(\gamma^{2m+1})\chi_4^2(\gamma^{2m+1}-1). \end{aligned}$$

Since

$$\chi_4(\gamma^{2m}) = (-1)^m, \quad \chi_4(\gamma^{2m+1}) = \mathrm{i}^{2m+1} \in \{\pm\mathrm{i}\}$$

and

$$\chi_4^2(v) \in \{0, \pm 1\}$$

for any $v \in \mathbb{F}_q$,

$$\mathbf{Re}(J_4(2,1)) = \sum_{m=0}^{f-1} \chi_4(\gamma^{2m})\chi_4^2(\gamma^{2m}-1) = \frac{J_2(1,1,1)}{2},$$

where $\mathbf{Re}(z)$ represents the real component of a complex number z.

From [24], we extract the evaluation required. Take special note that the Jacobi sums as defined in [24, §2] are distinct from our own definitions. In fact, their Jacobi sums $R(m,n)$ equal our

$$J(n, -m-n) = (-1)^{fm} J(m,n).$$

So their finding for $R(1,1)$ [24, Propositions 1,2] can be reinterpreted as a result for our $J_4(1,2)$ as follows.

Lemma 10. [24, Propositions 1,2] *Let $q = p^\alpha \equiv 1 \pmod 4$ with p prime and $\alpha \geqslant 1$, and let*

$$s = -\mathbf{Re}(J_4(1,2)).$$

If $p \equiv 3 \pmod 4$, then α is even,

$$s = (-p)^{\alpha/2} \equiv 1 \pmod 4$$

and

$$J_4(1,2) = -s = -(-p)^{\alpha/2}.$$

*If $p \equiv 1 \pmod 4$, then s is the **unique** integer coprime to q such that $s \equiv 1 \pmod 4$ and $q - s^2$ is a perfect square.*

Remark 11. *The earlier literature* [25, p.298] *also presented the results of Lemma 10, but erred in the sign when $p \equiv 3 \pmod 4$.*

When

$$f = \frac{q-1}{2}$$

is even, by Lemma 10,

$$J_2(1,1,1) = 2\mathbf{Re}(J_4(2,1)) = 2\mathbf{Re}((-1)^{\frac{q-1}{4}} J_4(1,2)) = (-1)^{\frac{q-1}{4}}(-2s).$$

When f is odd, by Corollary 3, $J_2(1,1,1) = 0$.

Evaluating the ternary Jacobi sums of order 2, excluding $J_2(1,1,1)$, is now straightforward by Proposition 7, Corollary 8, and Eq (3.1). Combining all these, we formulate the results into the following theorem.

Theorem 12. *All ternary Jacobi sums of order 2 over $\mathbb{F}_q$ with respect to a generator γ of $\mathbb{F}_q^*$ are explicitly given as follows, with $g = \mathrm{ind}_\gamma(2)$ and s defined as in Lemma 10.*

$$\begin{aligned}
&J_2(0,0,0) = q-3, \qquad J_2(1,0,0) = (-1)^{f+1}(1+(-1)^g),\\
&J_2(0,0,1) = J_2(0,1,1) = J_2(1,1,0) = -1-(-1)^g,\\
&J_2(0,1,0) = J_2(1,0,1) = -1-(-1)^f,\\
&J_2(1,1,1) = \begin{cases} 0, & \text{if } q \equiv 3 \pmod 4,\\ -2s, & \text{if } q \equiv 1 \pmod 8,\\ 2s, & \text{if } q \equiv 5 \pmod 8. \end{cases}
\end{aligned}$$

Using finite Fourier series expansions from Proposition 1, along with Theorem 12, we derive a complete and explicit evaluation of all ternary cyclotomic numbers of order 2 as follows.

Theorem 13. *All ternary cyclotomic numbers of order 2 over $\mathbb{F}_q$, corresponding to a generator γ of $\mathbb{F}_q^*$, are explicitly evaluated as follows, with $g = \mathrm{ind}_\gamma(2)$ and s defined as in Lemma 10.*

If $q \equiv 3 \pmod 4$, then

$$A_{000}^{(2)} = A_{100}^{(2)} = A_{110}^{(2)} = A_{111}^{(2)} = \frac{q-5-2(-1)^g}{8},$$

$$A^{(2)}_{001} = A^{(2)}_{010} = A^{(2)}_{011} = A^{(2)}_{101} = \frac{q-1+2(-1)^g}{8}.$$

If $q \equiv 1 \pmod 8$, *then*

$$A^{(2)}_{000} = \frac{q-11-2s-4(-1)^g}{8}, \qquad A^{(2)}_{011} = A^{(2)}_{110} = \frac{q+1-2s}{8},$$
$$A^{(2)}_{101} = \frac{q-3-2s+4(-1)^g}{8}, \qquad A^{(2)}_{001} = A^{(2)}_{100} = A^{(2)}_{010} = A^{(2)}_{111} = \frac{q-3+2s}{8}.$$

If $q \equiv 5 \pmod 8$, *then*

$$A^{(2)}_{000} = A^{(2)}_{101} = \frac{q-7+2s}{8}, \qquad A^{(2)}_{011} = A^{(2)}_{110} = \frac{q+1+2s}{8},$$
$$A^{(2)}_{001} = A^{(2)}_{100} = A^{(2)}_{010} = A^{(2)}_{111} = \frac{q-3-2s}{8}.$$

4. Calculation for order $e = 3$

This section aims to compute as many ternary Jacobi sums of order 3 as feasible. Let

$$e = 3 \text{ and } q = p^\alpha = 3f + 1$$

be an odd prime power. Clearly, f is even. Let

$$g = \mathrm{ind}_\gamma(2).$$

We choose a cube root of unity $\zeta_3 \in \{e^{\pm\frac{2\pi}{3}\mathrm{i}}\}$. Then

$$\zeta_3^2 = -1 - \zeta_3.$$

Also note that

$$\sigma_2(\zeta_3) = \zeta_3^2 = \zeta_3^{-1} = \overline{\zeta_3},$$

for the $\mathbb{Q}$-automorphism σ_2: $\mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta)$. So σ_2 is just the complex conjugation.

First, recall the evaluation of classical Jacobi sums of order 3. Since f is even,

$$J_3(a,b) = J_3(b,a) = J_3(-a-b,b) = J_3(b,-a-b) = J_3(-a-b,a) = J_3(a,-a-b).$$

By Eq (2.4),

$$J_3(0,0) = q-2,$$

and

$$J_3(0,1) = J_3(1,0) = J_3(2,1) = J_3(1,2) = J_3(2,0) = J_3(0,2) = -1.$$

The value of

$$J_3(1,1) = \overline{J_3(2,2)}$$

is also known as the following lemma.

Lemma 14. [12, 25] *For*

$$q = p^{\alpha} = 3f + 1$$

with p odd prime and $\alpha \geqslant 1$, we can write

$$J_3(1,1) = \frac{L + 3M}{2} + 3M\zeta_3,$$

for some $L, M \in \mathbb{Z}$ with $L \equiv 1 \pmod 3$.

(1) *If $p \equiv 2 \pmod 3$, then α is even,*

$$M = 0, \quad L = -2(-p)^{\alpha/2}, \ \text{and} \ J_3(1,1) = -(-p)^{\alpha/2}.$$

(2) *If $p \equiv 1 \pmod 3$, then (L, M) is the **unique** solution of the Diophantine system:*

$$\begin{cases} 4q = L^2 + 27M^2, \\ L \equiv 1 \pmod 3, \quad p \nmid L, \\ \gamma^{\frac{q-1}{3}} \equiv (L + 9M)/(L - 9M) \pmod p. \end{cases} \tag{4.1}$$

Proof. For $p \equiv 1 \pmod 3$, this result is a part of [12, Proposition 1]. For $p \equiv 2 \pmod 3$, [25, p.297] provided the value of $J_3(1,1)$ but erred in the sign. To rectify this mistake, we present an elementary proof below.

By definition,

$$J_3(1,1) = a + b\zeta_3$$

with some $a, b \in \mathbb{Z}$. Write A_{ij} (with $0 \leqslant i, j \leqslant 2$) for the classical cyclotomic numbers of order 3. Note that f is even. So

$$A_{01} = A_{10} = A_{22} \ \text{ and } \ A_{02} = A_{20} = A_{11}.$$

By definition,

$$b = A_{01} + A_{10} + A_{22} - (A_{02} + A_{11} + A_{20}) = 3(A_{01} - A_{02}) \equiv 0 \pmod 3.$$

By Eq (2.3),

$$\begin{aligned} f - 1 &= A_{00} + A_{01} + A_{02}, \\ f &= A_{22} + A_{02} + A_{12} = A_{01} + A_{02} + A_{12}. \end{aligned}$$

So

$$A_{12} = A_{00} + 1.$$

By definition,

$$a = A_{00} + A_{12} + A_{21} - (A_{02} + A_{11} + A_{20}) = 2 + 3(A_{00} - A_{02}) \equiv 2 \pmod 3.$$

By [26, Theorem 2.1.3], if none of i, j, and $i + j$ are multiples of e, then

$$|J_e(i,j)| = \sqrt{q}.$$

Therefore,

$$p^\alpha = q = (a + b\zeta_3)(\overline{a + b\zeta_3}) = (a + b\zeta_3)(a + b\zeta_3^2).$$

The Eisenstein integer ring $\mathbb{Z}[\zeta_3]$ is a unique factorization domain (UFD), where the rational prime $p \equiv 2 \pmod 3$ is an Eisenstein prime, which is irreducible in $\mathbb{Z}[\zeta_3]$. So

$$a + b\zeta_3 = p^n u$$

for an integer $n \geqslant 0$ and an Eisenstein unit

$$u \in \{\pm 1, \pm\zeta_3, \pm(1 + \zeta_3)\}.$$

Since

$$p^n = |a + b\zeta_3| = p^{\alpha/2},$$

we have

$$a + b\zeta_3 = p^{\alpha/2}u \in \{\pm p^{\alpha/2}, \pm p^{\alpha/2}\zeta_3, \pm p^{\alpha/2}(1 + \zeta_3)\}.$$

The condition

$$b \equiv 0 \not\equiv \pm p^{\alpha/2} \pmod 3$$

requires that $u = \pm 1$ and thus $b = 0$. Moreover,

$$J_3(1, 1) = a = \pm p^{\alpha/2} \equiv 2 \equiv p \pmod 3,$$

and hence

$$J_3(1, 1) = -(-p)^{\alpha/2}.$$ □

As f is even, by Corollaries 3 and 5, for any $a, b, c \in \mathbb{Z}/3\mathbb{Z}$ we have

$$J_3(a, b, c) = J_3(c, b, a) = J_3(a, -a - b - c, c).$$

Along with Proposition 7, Corollary 8, and Lemma 9, we obtain:

$$\begin{aligned}
&J_3(0, 0, 0) = q - 3,\\
&J_3(2, 0, 1) = J_3(1, 0, 2) = J_3(0, 2, 0) = J_3(0, 1, 0) = -2,\\
&J_3(1, 2, 0) = J_3(0, 2, 1) = J_3(1, 0, 0) = J_3(0, 0, 1) = -1 - \zeta_3^g,\\
&J_3(2, 1, 0) = J_3(0, 1, 2) = J_3(2, 0, 0) = J_3(0, 0, 2) = -1 - \zeta_3^{2g},\\
&J_3(1, 1, 0) = J_3(0, 1, 1) = \frac{L + 3M}{2} + 3M\zeta_3 - \zeta_3^g,\\
&J_3(2, 2, 0) = J_3(0, 2, 2) = \frac{L + 3M}{2} + 3M\zeta_3^2 - \zeta_3^{2g},\\
&J_3(1, 1, 1) = J_3(1, 0, 1) = \zeta_3^{2g}\left(\frac{L + 3M}{2} + 3M\zeta_3\right) - 1,\\
&J_3(2, 2, 2) = J_3(2, 0, 2) = \zeta_3^{g}\left(\frac{L + 3M}{2} + 3M\zeta_3^2\right) - 1.
\end{aligned}$$

Next, we calculate

$$J_3(1, 2, 1) = \overline{J_3(2, 1, 2)},$$

following a similar approach to that for $J_2(1,1,1)$ in Section 3. Note that f is even and

$$\mathbb{F}_q^* = \{\gamma^m \mid 0 \leqslant m \leqslant 3f-1\}.$$

So

$$\begin{aligned} J_3(1,2,1) &= \sum_{v\in\mathbb{F}_q^*} \chi_3^2(v)\chi_3(v^2-1) = \sum_{m=0}^{3f-1} \chi_3(\gamma^{2m})\chi_3(\gamma^{2m}-1) \\ &= 2\sum_{m=0}^{\frac{3}{2}f-1} \chi_3(\gamma^{2m}-1)\chi_3(\gamma^{2m}). \end{aligned} \tag{4.2}$$

Also note that

$$\begin{aligned} J_3(1,1) &= \sum_{n=0}^{3f-1} \chi_3(\gamma^n-1)\chi_3(\gamma^n) \\ &= \sum_{m=0}^{\frac{3}{2}f-1} \chi_3(\gamma^{2m}-1)\chi_3(\gamma^{2m}) + \sum_{m=0}^{\frac{3}{2}f-1} \chi_3(\gamma^{2m+1}-1)\chi_3(\gamma^{2m+1}). \end{aligned} \tag{4.3}$$

Let us choose the primitive complex 6-th root of unity ζ_6 such that $\zeta_6^2 = \zeta_3$. As $\zeta_6^3 = -1$,

$$\zeta_6 = -\zeta_6^{-2} = -\zeta_3^{-1} = -\zeta_3^2 = 1+\zeta_3.$$

Write $J_6(i,j)$ $(i,j \in \mathbb{Z}/6\mathbb{Z})$ for the classical Jacobi sums of order 6 with respect to γ and ζ_6. Let χ_6 be the character of $\mathbb{F}_q$ defined by $\chi_6(0) = 0$ and

$$\chi_6(\gamma^m) = \zeta_6^m \quad \text{(for any } m \in \mathbb{Z}\text{)}.$$

Note that $\chi_6^2 = \chi_3$ on $\mathbb{F}_q$. By definition,

$$\begin{aligned} J_6(2,5) &= \sum_{n=0}^{3f-1} \chi_6^2(\gamma^n-1)\chi_6^5(\gamma^n) = \sum_{n=0}^{3f-1} \chi_3(\gamma^n-1)\chi_6^5(\gamma^n) \\ &= \sum_{m=0}^{\frac{3}{2}f-1} \chi_3(\gamma^{2m}-1)\chi_6^5(\gamma^{2m}) + \sum_{m=0}^{\frac{3}{2}f-1} \chi_3(\gamma^{2m+1}-1)\chi_6^5(\gamma^{2m+1}). \end{aligned}$$

Since

$$\begin{aligned} \chi_6^5(\gamma^{2m}) &= \chi_3(\gamma^{2m}), \\ \chi_6^5(\gamma^{2m+1}) &= \zeta_6^5\chi_3(\gamma^{2m}) = -\zeta_3\chi_3(\gamma^{2m}) = -\chi_3(\gamma^{2m+1}), \end{aligned}$$

we obtain

$$J_6(2,5) = \sum_{m=0}^{\frac{3}{2}f-1} \chi_3(\gamma^{2m}-1)\chi_3(\gamma^{2m}) - \sum_{m=0}^{\frac{3}{2}f-1} \chi_3(\gamma^{2m+1}-1)\chi_3(\gamma^{2m+1}). \tag{4.4}$$

Theorem 15. *Let $g = \mathrm{ind}_\gamma(2)$, and (L, M) be defined as in Lemma 14 for*

$$q = p^\alpha = 3f + 1$$

with p odd prime and $\alpha \geqslant 1$. Then

$$J_3(1,2,1) = J_3(1,1) + \overline{J_6(1,1)} = \begin{cases} L, & \text{if } g \equiv 0 \pmod 3, \\ \frac{-L+9M}{2}\zeta_3, & \text{if } g \equiv 1 \pmod 3, \\ \frac{L+9M}{2}(1+\zeta_3), & \text{if } g \equiv 2 \pmod 3. \end{cases}$$

Moreover, if $p \equiv 2 \pmod 3$, then $g \equiv 0 \pmod 3$ and

$$J_3(1,2,1) = L = -2(-p)^{\alpha/2}.$$

Proof. By Eqs (4.2)–(4.4), we have

$$J_3(1,2,1) = J_3(1,1) + J_6(2,5).$$

We know

$$J_3(1,1) = \frac{L+3M}{2} + 3M\zeta_3.$$

Also note that

$$J_6(2,5) = J_6(5,5) = \sigma_5(J_6(1,1)) = \overline{J_6(1,1)}.$$

To determine $J_6(1,1)$, we note that

$$J_6(1,1) \in \mathbb{Z}[\zeta_6] = \mathbb{Z}[\zeta_3]$$

by definition. Let

$$J_6(1,1) = \frac{E+F}{2} + F\zeta_3$$

for some $E, F \in \mathbb{Z}$. By finite Fourier series expansions, E and F are indeed $\mathbb{Z}$-linear combinations of classical cyclotomic numbers $A_{ij}^{(6)}$ (with $0 \leqslant i, j \leqslant 5$).

For $p \equiv 1 \pmod 3$, [14, Theorem 2] provides

$$J_6(1,1) = \frac{(-E+F)\zeta_3 - (E+F)\zeta_3^2}{2} = \frac{E+F}{2} + F\zeta_3,$$

where

$$(E,F) = \begin{cases} (L, 3M), & \text{if } g \equiv 0 \pmod 3, \\ (\frac{-L-9M}{2}, \frac{L-3M}{2}), & \text{if } g \equiv 1 \pmod 3, \\ (\frac{-L+9M}{2}, \frac{-L-3M}{2}), & \text{if } g \equiv 2 \pmod 3. \end{cases} \tag{4.5}$$

So we only need to show that Eq (4.5) also holds for $p \equiv 2 \pmod 3$.

In an earlier work, Dickson [7, §17–19] established Eq (4.5) in the setting of $q = p$, utilizing certain linear relations among cyclotomic numbers $A_{ij}^{(6)}$ (with $0 \leqslant i, j \leqslant 5$). These relations, in fact, are valid for $A_{ij}^{(6)}$ over any finite field $\mathbb{F}_q$ with $q \equiv 1 \pmod 6$. Thus, *Dickson's proof of Eq (4.5) is universally applicable to all fields $\mathbb{F}_q$ with $q \equiv 1 \pmod 6$.*

Note that the Jacobi sum $R(11)$ in [7, §17–19] corresponds to our $(-1)^f J_6(1,1)$. Consequently, the pair (E,F) in [7, §18] (with f even) matches our pair, while the pair in §19 (with f odd) is our $(-E,-F)$.

Using Eq (4.5), we obtain

$$\begin{aligned} J_3(1,2,1) &= J_3(1,1) + J_6(2,5) = J_3(1,1) + \overline{J_6(1,1)} \\ &= \frac{L+3M}{2} + 3M\zeta_3 + \frac{E+F}{2} + F\zeta_3^2 \\ &= \frac{L+3M+E-F}{2} + (3M-F)\zeta_3 \\ &= \begin{cases} L, & \text{if } g \equiv 0 \,(\mathrm{mod}\, 3), \\ \frac{-L+9M}{2}\zeta_3, & \text{if } g \equiv 1 \,(\mathrm{mod}\, 3), \\ \frac{L+9M}{2}(1+\zeta_3), & \text{if } g \equiv 2 \,(\mathrm{mod}\, 3). \end{cases} \end{aligned}$$

For the special case of $p \equiv 2 \,(\mathrm{mod}\, 3)$, we have

$$2 \equiv 2^{1+2(p-1)} \,(\mathrm{mod}\, p)$$

by Fermat's little theorem. As

$$1 + 2(p-1) \equiv 0 \,(\mathrm{mod}\, 3),$$

let

$$1 + 2(p-1) = 3t$$

with some $t \in \mathbb{Z}$. Then

$$g = \mathrm{ind}_\gamma(2) = \mathrm{ind}_\gamma(2^{3t}) \equiv 3tg \,(\mathrm{mod}\,(q-1)).$$

Since $3 \mid (q-1)$, we have $g \equiv 0 \,(\mathrm{mod}\, 3)$, and hence

$$J_3(1,2,1) = L = -2(-p)^{\alpha/2}.$$

This completes the proof. □

Remark 16. *For $p \equiv 1 \,(\mathrm{mod}\, 3)$ and $q = p^\alpha$, Acharya and Katre* [14, Theorem 2] *proved that (E,F) is the **unique** solution of the Diophantine system*

$$\begin{cases} 4q = E^2 + 3F^2, \\ E \equiv 1 \,(\mathrm{mod}\, 3), \quad p \nmid E, \quad F \equiv -g \,(\mathrm{mod}\, 3), \\ \gamma^{\frac{q-1}{3}} \equiv (-E+F)/(E+F) \,(\mathrm{mod}\, p). \end{cases}$$

The remaining issue now is to evaluate

$$J_3(1,1,2) = J_3(2,1,1) = J_3(2,2,1) = J_3(1,2,2).$$

Here, the second equality stems from Corollary 5, while the other two follow from Corollary 3. First, proving it to be an integer is straightforward.

Proposition 17. *$J_3(1,1,2)$ is an integer.*

Proof. By Corollaries 3, 5 and Lemma 9,

$$J_3(1,1,2) = J_3(2,1,1) = J_3(2,2,1) = \sigma_2(J_3(1,1,2)) = \overline{J_3(1,1,2)}.$$

So $J_3(1,1,2) \in \mathbb{R}$. By definition,

$$J_6(1,1) \in \mathbb{Z}[\zeta_6] = \mathbb{Z}[\zeta_3].$$

Let

$$J_3(1,1,2) = a + b\zeta_3$$

for some $a, b \in \mathbb{Z}$, whose imaginary part is 0 only if $b = 0$. So $J_3(1,1,2) = a \in \mathbb{Z}$. □

We have explored various approaches, but the exact value of $J_3(1,1,2)$ still eludes us. Finally, let us elaborate on two unsuccessful ideas regarding its calculation:

(1) Drawing from the prior computation of $J_3(1,2,1)$, we might guess: Can $J_3(1,1,2)$ be expressed as a linear combination of $J_6(i,j)$, with coefficients independent of $\mathbb{F}_q$? More precisely, let us consider 36 absolute constants $c_{ij} \in \mathbb{C}$ (for $0 \leqslant i, j \leqslant 5$) such that the equality

$$J_3(1,1,2) = \sum_{0 \leqslant i,j \leqslant 5} c_{ij} J_6(i,j)$$

holds for any finite field $\mathbb{F}_q$ with $q \equiv 1 \pmod 6$. For each q, this equality yields a linear relation among the coefficients c_{ij}. Unfortunately, computational solutions (by a computer program) to these linear equations (for a sufficient number of q) reveal that *such constants c_{ij} do not exist*.

(2) For $v = \gamma^n \in \mathbb{F}_q^*$, we note that

$$\sum_{i=0}^{2} \chi_3^i(v) = \sum_{i=0}^{2} \chi_3^i(\gamma^n) = \sum_{i=0}^{2} (\zeta_3^n)^i = \begin{cases} 3, & \text{if } 3 \mid n, \\ 0, & \text{otherwise.} \end{cases}$$

Also note that

$$\begin{aligned} &J(1,1,2) = J(2,1,1) = J(2,2,1), \\ &J(2,0,1) = -2. \end{aligned}$$

So

$$\begin{aligned} 2J(1,1,2) - 2 &= J(2,1,1) + J(2,2,1) + J(2,0,1) \\ &= \sum_{v \in \mathbb{F}_q^*} \chi_3^2(v-1)\Big(\sum_{i=0}^{2} \chi_3^i(v)\Big)\chi_3(v+1) = 3\sum_{m=0}^{f-1} \chi_3^2(\gamma^{3m}-1)\chi_3(\gamma^{3m}+1) \\ &= 3\sum_{m=1}^{f-1} \chi_3\Big(\frac{\gamma^{3m}+1}{\gamma^{3m}-1}\Big) = 3\sum_{m=1}^{f-1} \chi_3\Big(\frac{2}{\gamma^{3m}-1}+1\Big). \end{aligned}$$

Similar computations for $J(1,1,2) + J(0,1,2) + J(2,1,2)$ and $J(1,1,2) + J(1,1,0) + J(1,1,1)$ yields similar character sums involving cubic elements of $\mathbb{F}_q^*$. To evaluate $J_3(1,1,2)$, it suffices to evaluate any one of them. Currently, we have not found a good way to compute them in general.

5. Conclusions

In this paper, we introduce the trivariate counterparts of classical cyclotomic numbers and Jacobi sums, named "ternary cyclotomic numbers" and "ternary Jacobi sums". We present their basic properties that mirror those of the classical cyclotomic numbers and Jacobi sums. In Section 3 we provide explicit evaluations for all ternary Jacobi sums (Theorem 12) and ternary cyclotomic numbers (Theorem 13) of order $e = 2$. Section 4 delivers near-complete results for order $e = 3$, with the exception of the elusive integer $J_3(1, 1, 2)$ for us. To solve the cyclotomic problem for ternary cyclotomic numbers of order 3, one only needs to calculate $J_3(1, 1, 2)$. Determining the precise value of the integer $J_3(1, 1, 2)$ stands as our initial objective for upcoming endeavors. In the future, we will investigate more general methods for the ternary cyclotomic problem, as well as its potential applications in other fields.

Author contributions

Zhichao Tang: writing–original draft, conceptualization, investigation, software, validation; Xiang Fan: writing–review & editing, methodology, supervision, funding acquisition. All authors have read and agreed to the published version of the manuscript.

Acknowledgments

The authors gratefully acknowledge the editor and the anonymous reviewers for their insightful feedback, greatly enhancing the manuscript. This work is funded by Guangzhou Science and Technology Programme (No. 202102021218). The second author was also sponsored by the National Natural Science Foundation of China (No. 11801579) and Guangdong Basic and Applied Basic Research Foundation (No. 2020B1515310017).

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. C. F. Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, 1986. https://doi.org/10.1007/978-1-4939-7560-0
2. C. F. Gauss, *Werke, Band II*, Georg Olms Verlag, 1973.
3. Y. S. Kim, J. S. Chung, J. S. No, H. Chung, On the autocorrelation distributions of Sidel'nikov sequences, *IEEE Trans. Inf. Theory*, **51** (2005), 3303–3307. https://doi.org/10.1109/TIT.2005.853310
4. C. Ma, L. Zeng, Y. Liu, D. Feng, C. Ding, The weight enumerator of a class of cyclic codes, *IEEE Trans. Inf. Theory*, **57** (2011), 397–402. https://doi.org/10.1109/TIT.2010.2090272
5. C. Ding, Y. Liu, C. Ma, L. Zeng, The weight distributions of the duals of cyclic codes with two zeros, *IEEE Trans. Inf. Theory*, **57** (2011), 8000–8006. https://doi.org/10.1109/TIT.2011.2165314

6. Y. Liang, J. Cao, X. Chen, S. Cai, X. Fan, Linear complexity of Ding-Helleseth generalized cyclotomic sequences of order eight, *Cryptogr. Commun.*, **11** (2019), 1037–1056. https://doi.org/10.1007/s12095-018-0343-0
7. L. E. Dickson, Cyclotomy, higher congruences, and waring's problem, *Amer. J. Math.*, **57** (1935), 391–424. https://doi.org/10.2307/2371217
8. L. E. Dickson, Cyclotomy and trinomial congruences, *Trans. Amer. Math. Soc.*, **37** (1935), 363–380, 1935. https://doi.org/10.2307/1989714
9. L. E. Dickson, Cyclotomy when e is composite, *Trans. Amer. Math. Soc.*, **38** (1935), 187–200. https://doi.org/10.2307/1989680
10. M. H. Ahmed, J. Tanti, Cyclotomic numbers and Jacobi sums: a survey, In: *Class groups of number fields and related topics*, Springer-Verlag, 2020. https://doi.org/10.1007/978-981-15-1514-9_12
11. J. C. Parnami, M. K. Agrawal, A. R. Rajwade, Jacobi sums and cyclotomic numbers for a finite field, *Acta Arith.*, **41** (1982), 1–13. https://doi.org/10.4064/aa-41-1-1-13
12. S. A. Katre, A. R. Rajwade, Complete solution of the cyclotomic problem in $\mathbf{F}_q$ for any prime modulus l, $q = p^\alpha$, $p \equiv 1 \pmod{l}$, *Acta Arith.*, **45** (1985), 183–199. https://doi.org/10.4064/aa-45-3-183-199
13. L. L. Xia, J. Yang, Cyclotomic problem, Gauss sums and Legendre curve, *Sci. China Math.*, **56** (2013), 1485–1508. https://doi.org/10.1007/s11425-013-4653-6
14. V. V. Acharya, S. A. Katre, Cyclotomic numbers of orders $2l$, l an odd prime, *Acta Arith.*, **69** (1995), 51–74. https://doi.org/10.4064/aa-69-1-51-74
15. D. Shirolkar, S. A. Katre, Jacobi sums and cyclotomic numbers of order l^2, *Acta Arith.*, **147** (2011), 33–49. https://doi.org/10.4064/aa147-1-2
16. M. H. Ahmed, J. Tanti, A. Hoque, Complete solution to cyclotomy of order $2l^2$ with prime l, *Ramanujan J.*, **53** (2020), 529–550. https://doi.org/10.1007/s11139-019-00182-9
17. M. H. Ahmed, J. Tanti, Complete congruences of Jacobi sums of order $2l^2$ with prime l, *Ramanujan J.*, **59** (2022), 967–977. https://doi.org/10.1007/s11139-022-00592-2
18. A. Weil, Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.*, **55** (1949), 497–508. https://doi.org/10.1090/S0002-9904-1949-09219-4
19. L. M. Adleman, C. Pomerance, R. S. Rumely, On distinguishing prime numbers from composite numbers, *Ann. Math.*, **117** (1983), 173–206. https://doi.org/10.2307/2006975
20. P. van Wamelen, Jacobi sums over finite fields, *Acta Arith.*, **102** (2002), 1–20. https://doi.org/10.4064/aa102-1-1
21. M. H. Ahmed, J. Tanti, S. Pushp, Computation of Jacobi sums of orders l^2 and $2l^2$ with odd prime l, *Indian J. Pure Appl. Math.*, **54** (2023), 330–343. https://doi.org/10.1007/s13226-022-00256-3
22. K. H. Leung, S. L. Ma, B. Schmidt, New Hadamard matrices of order $4p^2$ obtained from Jacobi sums of order 16, *J. Combin. Theory*, **113** (2006), 822–838. https://doi.org/10.1016/j.jcta.2005.07.011

23. A. Rojas-León, On a generalization of Jacobi sums, *Finite Fields Appl.*, **77** (2022), 101944. https://doi.org/10.1016/j.ffa.2021.101944

24. S. A. Katre, A. R. Rajwade, Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum, *Math. Scand.*, **60** (1987), 52–62. https://doi.org/10.7146/math.scand.a-12171

25. T. Storer, On the unique determination of the cyclotomic numbers for Galois fields and Galois domains, *J. Comb. Theory*, **2** (1967), 296–300. http://doi.org/10.1016/S0021-9800(67)80031-0

26. B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi sums*, John Wiley & Sons, Inc., 1998.

AIMS Press