ACTA ARITHMETICA
LXXIII.4 (1995)

On Shioda's problem about Jacobi sums II

by

HIROO MIKI (Kyoto)

In the present paper, we will give a complete affirmative answer to the l-part of Shioda's problem ([5, Question 3.4]) on Jacobi sums $J_l^{(a)}(\mathfrak{p})$, and to the conjecture (F. Gouvêa and N. Yui [1, Conjecture (1.9)]) which comes from Shioda's problem and my congruences for Jacobi sums (see [3, Theorem 2]) (see Theorem 1 and its Corollary of the present paper).

We retain the notation of [4], but l is any odd prime number here. Furthermore, let n be any positive integer and let ζ_m be a primitive mth root of unity in $\mathbb{C}$ for any positive integer m. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. We fix an algebraic closure $\overline{\mathbb{Q}}_l$ of $\mathbb{Q}_l$, and by a fixed imbedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_l$ we consider $\overline{\mathbb{Q}}$ as a subfield of $\overline{\mathbb{Q}}_l$. Let M be any finite unramified extension of $\mathbb{Q}_l$ in $\overline{\mathbb{Q}}_l$, and put $M_n = M(\zeta_{l^n})$ and $\pi_n = \zeta_{l^n} - 1$. Then π_n is a prime element of M_n. Let $\sigma_{-1} \in G = \mathrm{Gal}(M_n/M)$ (the Galois group of M_n over M) be such that $\zeta_{l^n}^{\sigma_{-1}} = \zeta_{l^n}^{-1}$. Let ord_{M_n} denote the normalized additive valuation of M_n, and let $U_n = U(M_n)$ be the group of principal units in M_n:

$$U_n = U(M_n) = \{x \in M_n \mid \mathrm{ord}_{M_n}(x-1) \geq 1\}.$$

As is well known, U_n is a multiplicatively written $\mathbb{Z}_l$-module. In particular, $x^{1/2} \in U_n$ makes sense for $x \in U_n$.

LEMMA 1. *Let the notation and assumptions be as above. Furthermore, let $J \in U_n$ be such that $J \notin M$. Put $q' = J^{1+\sigma_{-1}}$, and assume $q' \in M$. Then* $\mathrm{ord}_{M_n}(1 - Jq'^{-1/2})$ *is odd. In particular*, $\mathrm{ord}_{M_n}(1-J)$ *is equal to* $\mathrm{ord}_{M_n}(1-q')$ *or odd.*

Proof. Put $e_- = (1-\sigma_{-1})/2$ and $e_+ = (1+\sigma_{-1})/2$. Note that $e_-, e_+ \in \mathbb{Z}_l[G]$ (the group ring of G over $\mathbb{Z}_l$), since $l \neq 2$ and $1/2 \in \mathbb{Z}_l$. Put $A = J^{e_-}$. Since $e_- + e_+ = 1$, we have

$$A = J^{1-e_+} = Jq'^{-1/2}. \tag{1}$$

On the other hand, the equality $e_-\sigma_{-1} = -e_-$ implies

$$A^{\sigma_{-1}} = A^{-1}. \tag{2}$$

If $A = 1$, then by (1) we have $J = q'^{1/2} \in M$; this contradicts the assumption. Hence $A \neq 1$, so we can write

$$A \equiv 1 + \lambda \pi_n^i \pmod{\pi_n^{i+1}}$$

with some unit λ in M and an integer $i \geq 1$. Since

$$\pi_n^{\sigma_{-1}} = \zeta_{l^n}^{-1} - 1 = (1 + \pi_n)^{-1} - 1 \equiv -\pi_n \pmod{\pi_n^2},$$

we have

$$(\pi_n^i)^{\sigma_{-1}} \equiv (-1)^i \pi_n^i \pmod{\pi_n^{i+1}}.$$

Hence

$$A^{\sigma_{-1}} \equiv 1 + (-1)^i \lambda \pi_n^i \pmod{\pi_n^{i+1}}. \tag{3}$$

On the other hand,

$$A^{-1} \equiv 1 - \lambda \pi_n^i \pmod{\pi_n^{i+1}}. \tag{4}$$

Since λ is a unit, by (2)–(4) we have $(-1)^i = -1$, so i is odd.

For any positive integer m and any $a \in \mathbb{Z}$ and for any prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\zeta_m)$ which is prime to m, let

$$g_m(\mathfrak{p}, a) = g_m(\mathfrak{p}, a; \zeta_p) = -\sum_{x \in \mathbb{F}_q} \chi_{\mathfrak{p}}^a(x) \psi_{\mathfrak{p}}(x) \in \mathbb{Z}[\zeta_{mp}]$$

be the *Gauss sum*, where $\mathbb{F}_q = \mathbb{Z}[\zeta_m]/\mathfrak{p}$, $q = N\mathfrak{p} = \#(\mathbb{F}_q)$, $\chi_{\mathfrak{p}}(x) = \left(\frac{x}{\mathfrak{p}}\right)_m$ is the mth power residue symbol in $\mathbb{Q}(\zeta_m)$, i.e., $\chi_{\mathfrak{p}}(x \bmod \mathfrak{p})$ is a unique mth root of unity in $\mathbb{C}$ such that

$$\chi_{\mathfrak{p}}(x \bmod \mathfrak{p}) \equiv x^{(N\mathfrak{p}-1)/m} \pmod{\mathfrak{p}}$$

for $x \in \mathbb{Z}[\zeta_m]$, $x \notin \mathfrak{p}$, $\chi_{\mathfrak{p}}(0) = 0$, and $\psi_{\mathfrak{p}}(x) = \zeta_p^{T(x)}$ (p is a prime number in $\mathfrak{p}$ and T is the trace from $\mathbb{F}_q$ to $\mathbb{Z}/p\mathbb{Z}$).

For arbitrary positive integers m, r and any $a = (a_1, \ldots, a_r) \in \mathbb{Z}^r$ (the direct product of r copies of $\mathbb{Z}$) and for any $\mathfrak{p}$ as above, let

$$J_m^{(a)}(\mathfrak{p}) = (-1)^{r+1} \sum_{\substack{x_1 + \ldots + x_r = -1 \\ x_1, \ldots, x_r \in \mathbb{F}_q}} \chi_{\mathfrak{p}}^{a_1}(x_1) \ldots \chi_{\mathfrak{p}}^{a_r}(x_r) \in \mathbb{Z}[\zeta_m]$$

be the *Jacobi sum*.

THEOREM 1. *Let the above notation and assumptions hold. Then*:

(i) *Assume that* $a \not\equiv 0 \pmod{l^n}$ *and that*

$$g_{l^n}(\mathfrak{p}, a) \neq q^{1/2}. \tag{$*$}$$

Then $\mathrm{ord}_{M_n}(1-g_{l^n}(\mathfrak{p},a)q^{-1/2})$ *is odd*, *where* $M=\mathbb{Q}_l(\zeta_p)$. *In particular*, $\mathrm{ord}_{M_n}(1-g_{l^n}(\mathfrak{p},a))$ *is equal to* $\mathrm{ord}_{M_n}(1-q)$ *or odd.*

(ii) *Assume that* $a=(a_1,\ldots,a_r)\not\equiv(0,\ldots,0) \pmod{l^n}$ *and that*

$$J_{l^n}^{(a)}(\mathfrak{p})\neq q^{(r'-2)/2}, \tag{$**$}$$

where $r'=\#\{0\le i\le r \mid a_i\equiv 0 \pmod{l^n}\}$ *and* $a_0=-\sum_{i=1}^r a_i$. *Then* $\mathrm{ord}_{M_n}(1-J_{l^n}^{(a)}(\mathfrak{p})q^{-(r'-2)/2})$ *is odd*, *where* $M=\mathbb{Q}_l$. *In particular*, $\mathrm{ord}_{M_n}(1-J_{l^n}^{(a)}(\mathfrak{p}))$ *is equal to* $\mathrm{ord}_{M_n}(1-q^{r'-2})$ *or odd.*

Proof. (i) Put $J=g_{l^n}(\mathfrak{p},a)$ and $\chi=\chi_{\mathfrak{p}}^a$. Since $a\not\equiv 0 \pmod{l^n}$, we have $\chi\neq 1$. Hence by [6, Lemma 6.1(b)], we have

$$J^{1+\sigma_{-1}}=\chi(-1)q=q, \tag{1}$$

since $(-1)^{l^n}=-1$ and $\chi(-1)=\chi(-1)^{l^n}=1$. If $J\in M$, then by (1) we have $J^2=q$, so $J=\pm q^{1/2}$. Since $J\equiv q\equiv 1 \pmod{\pi_n}$ and $l\neq 2$, this implies $J=q^{1/2}$; this contradicts our assumption $(*)$. Hence $J\notin M$. Thus the assertion follows from Lemma 1 for $q'=q$.

(ii) Put $J=J_{l^n}^{(a)}(\mathfrak{p})$. It is well known that

$$J=q^{-1}\prod_{i=0}^{r} g_{l^n}(\mathfrak{p},a_i)$$

if $a\not\equiv(0,\ldots,0) \pmod{l^n}$. By this equality and (1), we have

$$J^{1+\sigma_{-1}}=q^{r'-2}.$$

If $J\in M$, then $J^2=q^{r'-2}$, so $J=\pm q^{(r'-2)/2}$, hence $J=q^{(r'-2)/2}$, since $J\equiv q\equiv 1 \pmod{\pi_n}$ and $l\neq 2$. This contradicts the assumption $(**)$. Hence $J\notin M$. Using Lemma 1 for $q'=q^{r'-2}$, we have directly the assertion.

If $r\ge 3$ is odd (r is as in the definition of Jacobi sums) and if $a_i\not\equiv 0 \pmod{l}$ for all i $(0\le i\le r)$ $(a_0=-\sum_{i=1}^r a_i)$, then by Shioda [5, Corollary 3.3], we can write

$$N_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(1-J_l^{(a)}(\mathfrak{p})q^{-(r-1)/2})=Bl^3/q^w,$$

where B and w are non-negative integers, and w is defined by (2.8) of [5].

Shioda's problem (see [5, Question 3.4]). *Is B a square*?

By (ii) of the above Theorem 1, we have directly the following affirmative answer to the l-part of Shioda's problem.

Corollary. *Let the notation and assumptions be as above. Assume that* $B\neq 0$. *Then* $\mathrm{ord}_{\mathbb{Q}_l}(B)$ *is even.*

In the following, we will show that the case where $J\neq q'^{1/2}$ and $\mathrm{ord}_{M_n}(1-J)=\mathrm{ord}_{M_n}(1-q')$ actually happens in the above Theorem 1 when $n=1$, as an application of our congruences for Gauss sums and Jacobi sums previously obtained by the author ([3, Theorems 1 and 2]).

Assume $l\ge 5$. For any odd m $(3\le m\le l-2)$, put

$$\varepsilon_m=\prod_{d=1}^{l-1}(1-\zeta_l^d)^{m_d},$$

where $m_d\in\mathbb{Z}$ is such that $m_d\equiv d^{m-1} \pmod{l}$ and $\sum_{d=1}^{l-1}m_d=0$. Put $k=\mathbb{Q}(\zeta_l)$ and $K=k(\sqrt[l]{\varepsilon_m}\mid m \text{ odd}, 3\le m\le l-2)$.

THEOREM 2. *Let l, k, and K be as above and put $K'=K(\sqrt[l]{l})$. Then*:

(i) *If $a\not\equiv 0 \pmod{l}$ and $\deg\mathfrak{p}=1$, then the following* (a)–(c) *are equivalent*:

(a) $g_l(\mathfrak{p},a;\zeta_p)\equiv 1 \pmod{l}$ *for a suitable choice of ζ_p.*

(b) $g_l(\mathfrak{p},a;\zeta_p)\equiv 1+\frac{p-1}{2} \pmod{\pi_1^l}$ *for a suitable choice of ζ_p.*

(c) $\mathfrak{p}$ *is completely decomposed with respect to K'/k.*

(ii) (cf. [4, Theorem 3]). *The following* (d)–(f) *are equivalent*:

(d) $J_l^{(a)}(\mathfrak{p})\equiv 1 \pmod{l}$ *for any $a\in\mathbb{Z}^r$.*

(e) $J_l^{(a)}(\mathfrak{p})\equiv 1+\frac{r'-2}{2}(q-1) \pmod{\pi_1^l}$ *for any $a\in\mathbb{Z}^r$, where r' is as in* (ii) *of Theorem* 1.

(f) $\mathfrak{p}$ *is completely decomposed with respect to K/k.*

Proof. (i) If $r\not\equiv 0 \pmod{p}$, then

$$g_l(\mathfrak{p},a;\zeta_p^r)=\chi_{\mathfrak{p}}^{-a}(r)g_l(\mathfrak{p},a;\zeta_p).$$

Note that $\chi_{\mathfrak{p}}^{-a}(r)$ is a primitive lth root of unity if $r\notin(\mathbb{F}_p^\times)^l$. Hence by [3, Theorem 1] we see that $g_l(\mathfrak{p},a)\equiv 1 \pmod{\pi_1^2}$ for a suitable choice of ζ_p if and only if $\alpha_1\in\mathbb{F}_l$ (α_1 is as in [3, Theorem 1]). By [3, Theorem 7], this is equivalent to $\chi_{\mathfrak{p}}(l)=1$, i.e., $l \bmod p\in(\mathbb{F}_p^\times)^l$. Hence by [3, Theorem 1] we have the assertion.

(ii) See [4, Theorem 3].

LEMMA 2. *Let k and K' be as in Theorem* 2. *Then K' and $k(\sqrt[l]{\zeta_l})$ are linearly disjoint over k. In particular, there exist infinitely many prime ideals $\mathfrak{p}$ of k of degree* 1 *satisfying the condition* (c) *in Theorem* 2 *and $p-1\not\equiv 0 \pmod{l^2}$.*

Proof. The proof of the first part is similar to that of [4, Lemma 2]. The last part follows from the first part and Chebotarev's density theorem.

Concerning condition $J\ne q'^{1/2}$, the following theorem is known.

THEOREM 3. (i) ([2, (10)]). *Assume that $\deg\mathfrak{p}=1$ and $a\not\equiv 0 \pmod{l}$. Then $\mathbb{Q}(\zeta_p)(g_l(\mathfrak{p},a))=\mathbb{Q}(\zeta_{pl})$. In particular, $g_l(\mathfrak{p},a)\notin\mathbb{Q}_l(\zeta_p)$ and $g_l(\mathfrak{p},a)\ne q^{1/2}$.*

(ii) ([2, Theorem]). *Assume that* $l \nmid r$, $r \not\equiv 1 \pmod{p}$ *and* $\deg \mathfrak{p} = 1$. *Put* $a = (1, 1, \ldots, 1) \in \mathbb{Z}^r$. *Then* $\mathbb{Q}(J_l^{(a)}(\mathfrak{p})) = \mathbb{Q}(\zeta_l)$. *In particular*, $J_l^{(a)}(\mathfrak{p}) \notin \mathbb{Q}_l$ *and* $J_l^{(a)}(\mathfrak{p}) \neq q^{(r-1)/2}$.

(iii) ([5, Theorem 7.1]). *Let* $a = (a_1, a_2, a_3) \in \mathbb{Z}^3$ *be such that* $a_i \not\equiv 0 \pmod{l}$ *for all* i $(0 \le i \le 3)$ *and such that* $a_i + a_j \not\equiv 0 \pmod{l}$ *if* $i \neq j$, *where* $a_0 = -(a_1 + a_2 + a_3)$. *Then* $J_l^{(a)}(\mathfrak{p}) \neq q$ *if* $\deg \mathfrak{p} = 1$.

By Theorems 2 and 3, Lemma 2, Lemma 2 of [4], and Chebotarev's density theorem, there exist infinitely many prime ideals $\mathfrak{p}$ of k of degree 1 satisfying both $J \neq q'^{1/2}$ and $\mathrm{ord}_{M_n}(1 - J) = \mathrm{ord}_{M_n}(1 - q')$, where $J = g_l(\mathfrak{p}, a)$ or $J_l^{(a)}(\mathfrak{p})$ according to (i) or (ii) of Theorem 2.

I would like to thank Professors Don Zagier, Yuji Kida, and Masanobu Kaneko for supplying me further numerical data on Shioda's problem.

References

[1] F. Gouvêa and N. Yui, *Arithmetic of Diagonal Hypersurfaces over Finite Fields*, London Math. Soc. Lecture Note Ser. 200, Cambridge Univ. Press, 1995.

[2] M. Kida and T. Ono, *A note on Jacobi sums*, Proc. Japan Acad. 69 (1993), 32–34.

[3] H. Miki, *On the l-adic expansion of certain Gauss sums and its applications*, Adv. Stud. Pure Math. 12 (1987), 87–118.

[4] —, *On Shioda's problem about Jacobi sums*, Acta Arith. 69 (1995), 107–112.

[5] T. Shioda, *Some observations on Jacobi sums*, Adv. Stud. Pure Math. 12 (1987), 119–135.

[6] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer, New York, 1982.

DEPARTMENT OF LIBERAL ARTS AND SCIENCES
FACULTY OF ENGINEERING AND DESIGN
KYOTO INSTITUTE OF TECHNOLOGY
SAKYO-KU, KYOTO 606, JAPAN

Received on 24.10.1994 (2684)