On Shioda’s problem about Jacobi sums

by

HIROO MIKI (Bures-sur-Yvette and Kyoto)

In the present paper, we will give a positive result relating to the $l$-part of Shioda’s problem [2] on Jacobi sums $J_l^a(p)$ under a certain condition (see Corollary to Theorem 2 of the present paper), as an application of our congruence for Jacobi sums [1, Theorem 2] (see also Theorem 1 of the present paper).

Let $l$ be any prime number such that $l \geq 5$, and let $\zeta_l$ be a primitive $l$th root of unity in $\mathbb{C}$ (the field of complex numbers). Let $\mathbb{Q}$ be the field of rational numbers and let $\mathbb{Z}$ be the ring of rational integers. Put $k = \mathbb{Q}((\zeta_l))$.

For any integer $r \geq 1$ and any $a = (a_1, \ldots, a_r) \in \mathbb{Z}^r$ and for any prime ideal $p$ of $k$ which is prime to $l$, let

$$J_l^a(p) = (-1)^{r+1} \sum_{x_1, \ldots, x_r \in \mathbb{F}_q \atop x_1 + \cdots + x_r = -1} \chi_p^{a_1}(x_1) \ldots \chi_p^{a_r}(x_r) \in \mathbb{Z}[\zeta_l],$$

be the Jacobi sum, where $\mathbb{F}_q = \mathbb{Z}[\zeta_l]/p$, $q = Np = \#(\mathbb{F}_q)$, and $\chi_p(x) = \left(\frac{x}{p}\right)_l$ is the $l$th power residue symbol in $k$, i.e., $\chi_p(x \mod p)$ is a unique $l$th root of unity in $\mathbb{C}$ such that $\chi_p(x \mod p) \equiv x^{(Np-1)/l} \pmod{p}$ for $x \in \mathbb{Z}[\zeta_l]$, $x \not\equiv 0 \pmod{p}$, and $\chi_p(0) = 0$.

If $r \geq 3$ is odd and if $a_i \not\equiv 0 \pmod{l}$ for all $i$ ($0 \leq i \leq r$) (with $a_0 = -\sum_{i=1}^{r} a_i$), then by Shioda [2, Corollary 3.3] we can write

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

where $N_{k/\mathbb{Q}}$ is the norm mapping from $k$ to $\mathbb{Q}$, $B$ and $w$ are non-negative integers, and $w$ is defined by (2.8) of [2],

Shioda’s problem (see [2, Question 3.4]). Is $B$ a square if $B \neq 0$?

Zagier [4] (see [2, Example 3.5] and [3, Examples 5.15.1]) verified it by computer in the case where $l < 20$ and $p < 500$, $p \equiv 1 \pmod{l}$, where $p$ is a prime number in $p$. Shioda [2, Theorem 7.1] proved that $B$ is a square,
possibly multiplied by a divisor of \(2lp\) when \(r = 3\), and Suwa and Yui [3, Corollary 5.14.1] proved that \(B\) is divisible by \(p\) exactly even times under a certain condition when \(r = 3\).

Let \(\overline{\mathbb{Q}}\) be the algebraic closure of \(\mathbb{Q}\) in \(\mathbb{C}\) and let \(\overline{\mathbb{Q}}_l\) be a fixed algebraic closure of the field of \(l\)-adic numbers \(\mathbb{Q}_l\). By means of a fixed imbedding \(\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_l\), we consider \(\overline{\mathbb{Q}}\) as a subfield of \(\overline{\mathbb{Q}}_l\). We also consider that all algebraic extensions of \(\mathbb{Q}_l\) and all elements which are algebraic over \(\mathbb{Q}_l\) are contained in \(\overline{\mathbb{Q}}_l\). All congruences in the present paper are those in \(\overline{\mathbb{Q}}_l\).

For any odd \(m\) \((3 \leq m \leq l - 2)\), put

\[
E_m = \prod_{d=1}^{l-1} (1 - \zeta^d)^{m_d},
\]

where \(m_d \in \mathbb{Z}\) is such that \(m_d \equiv d^{m-1} \pmod{l}\) and \(\sum_{d=1}^{l-1} m_d = 0\). Let \(\beta_m(p) \in \mathbb{Z}\) be such that

\[
\left( \frac{E_m}{p} \right)_l = \zeta_l^{\beta_m(p)}.
\]

Then \(\beta_m(p)\) is uniquely determined \(\text{mod } l\) by \(l, m, \text{ and } p\).

**Theorem 1** ([1, Theorem 2]). If \(a = (a_1, \ldots, a_r) \neq (0, \ldots, 0) \pmod{l}\), then

\[
J_l^{(a)}(p) \equiv Np^{-1} \cdot \text{Exp} \left\{ \sum_{3 \leq m \leq l-2 \atop m \text{ odd}} \left( \sum_{j=0}^{r} a_j^m \right) \beta_m(p) \frac{\pi^m}{m!} \right. \\
- \frac{Np - 1}{2l} \left( \sum_{j=0}^{r} a_j^{l-1} \right) \pi^{l-1} \left\} \pmod{l} \right.,
\]

where \(a_0 = - \sum_{j=1}^{r} a_j\), \(\pi\) is a prime element of \(\mathbb{Q}_l(\zeta_l)\) such that

\[
\pi \equiv \log \zeta_l \pmod{(\zeta_l - 1)^l} \equiv \sum_{i=1}^{l-1} \frac{(-1)^{i+1} (\zeta_l - 1)^i}{i} \pmod{(\zeta_l - 1)^l}
\]

and

\[
\text{Exp } X = \sum_{i=0}^{l-1} \frac{X_i}{i!} \in \mathbb{Z}_l[X].
\]

**Remark.** The sign of the coefficient of \(\pi^{l-1}\) in the above formula is different from that of [1, Theorem 2], which was incorrect.
Lemma 1. For any odd \( m \) (\( 3 \leq m \leq l - 2 \)),

\[
E_m \equiv d_m \exp\left( -\frac{B_j}{j} \cdot \frac{\pi^j}{j!} \right) \pmod{\pi^{l-1}}
\]

\[
\equiv d_m \left( 1 - \frac{B_j}{j} \cdot \frac{\pi^j}{j!} \right) \pmod{\pi^{j+1}},
\]

where \( d_m = \prod_{d=1}^{l-1} (-d)^{m_d} \in \mathbb{Z}_l^\times \) (the group of units in \( \mathbb{Z}_l \)), \( j = l - m \), and \( B_j \) is the \( j \)-th Bernoulli number.

Proof. By definition,

\[
E_m = d_m \prod_{d=1}^{l-1} \left( \frac{1 - \zeta_l}{-d\pi} \right)^{m_d}
\]

and \( \zeta_l \equiv \exp \pi \pmod{\pi^l} \).

Easy computation shows that

\[
\log \frac{1 - e^t}{-t} = \frac{1}{2} t + \sum_{i=2}^{\infty} \frac{B_i}{i} \cdot \frac{t^i}{i!}.
\]

Hence

\[
\log \left( \frac{1 - \zeta_l}{-\pi} \right) = \frac{1}{2} \pi + \sum_{i=2}^{l-1} \frac{B_i}{i} \cdot \frac{\pi^i}{i!} \pmod{\pi^{l-1}},
\]

so

\[
\eta \log \left( \frac{1 - \zeta_l}{-\pi} \right) \equiv -\frac{B_j}{j} \cdot \frac{\pi^j}{j!} \pmod{\pi^{l-1}},
\]

where \( \eta = \sum_{d=1}^{l-1} m_d \sigma_d \in \mathbb{Z}_l[\text{Gal}(\mathbb{Q}_l(\zeta_l)/\mathbb{Q}_l)] \) (the group ring of the Galois group \( \text{Gal}(\mathbb{Q}_l(\zeta_l)/\mathbb{Q}_l) \) over \( \mathbb{Z}_l \)) and \( \sigma_d \in \text{Gal}(\mathbb{Q}_l(\zeta_l)/\mathbb{Q}_l) \) is such that \( \zeta_l^{\sigma_d} = \zeta_l^d \), since

\[
\eta \pi^i \equiv \begin{cases} 0 \pmod{\pi^j} & \text{if } i \neq j, \\ -\pi^i \pmod{\pi^j} & \text{if } i = j, \end{cases}
\]

for \( 1 \leq i \leq l - 1 \). Hence

\[
E_m \equiv d_m \left( \frac{1 - \zeta_l}{-\pi} \right)^\eta \pmod{\pi^{l-1}}
\]

\[
\equiv d_m \exp\left( -\frac{B_j}{j} \cdot \frac{\pi^j}{j!} \right) \pmod{\pi^{l-1}}.
\]

This completes the proof.

Put \( K = k(\sqrt{E_m} \mid m \text{ odd}, 3 \leq m \leq l - 2) \). We have \( K \neq k \), since \( B_2 = \frac{1}{6} \in \mathbb{Z}_l^\times \) implies \( E_{l-2} \notin k^l \) by Lemma 1. Since \( E_m \) is a unit of \( k \), \( K/k \) is a finite abelian extension which is unramified outside \( l \).
By Theorem 1 we have directly the following

**Theorem 2.** Let \( \sigma = (p, K/k) \) denote the Frobenius automorphism of \( p \) with respect to \( K/k \). Assume \( \sigma \neq 1 \). Then

\[
J^{(a)}_l(p) \equiv 1 + \left( \sum_{j=0}^{r} a_j^m \right) \beta_m(p) \frac{\pi^m}{m!} \quad (\text{mod } \pi^{m+1})
\]

and

\[
\beta_m(p) \not\equiv 0 \pmod{l},
\]

where \( m \) is the least odd \( m \) (3 \( \leq m \leq l - 2 \)) such that \((\sqrt[l]{E_m})^\sigma \neq \sqrt[l]{E_m}\).

**Corollary.** Let the notation and assumptions be as in Theorem 2 and let \( B \) be as in Shioda’s problem. Furthermore, assume that \( \sum_{j=0}^{r} a_j^m \not\equiv 0 \pmod{l} \). Then \( \text{ord}_l(B) = m - 3 \). In particular, \( \text{ord}_l(B) \) is even, where \( \text{ord}_l \) is the normalized additive valuation of \( \mathbb{Q}_l \).

The above corollary gives an affirmative answer to the \( l \)-part of Shioda’s problem when \( (p, K/k) \neq 1 \) and \( \sum_{j=0}^{r} a_j^m \not\equiv 0 \pmod{l} \).

**Lemma 2.** Let \( K \) be as just before Theorem 2. Then \( K \) and \( k(\sqrt[l]{\zeta_l}) \) are linearly disjoint over \( k \).

**Proof.** By Lemma 1,

\[
E_m \equiv d_m \pmod{\pi^2}.
\]

If the assertion is false, then \( k(\sqrt[l]{\zeta_l}) \subseteq K \), so by Kummer theory we can write

\[
\zeta_l = \prod_{3 \leq m \leq l-2 \atop m \text{ odd}} E_m^{\lambda_m} \cdot A^l
\]

with some \( \lambda_m \in \mathbb{Z} \) and some \( A \in k^\times \). Since \( \zeta_l \) and \( E_m \) are units of \( k \), \( A \equiv u \pmod{\pi} \) with some \( u \in \mathbb{Z}_l^\times \), so

\[
A^l \equiv u^l \pmod{\pi^l}.
\]

By (1)–(3),

\[
1 + \pi \equiv b \pmod{\pi^2},
\]

where \( b = \prod d_m^{\lambda_m} \cdot u^l \in \mathbb{Z}_l^\times \). Hence \( b \equiv 1 \pmod{\pi} \), so \( b \equiv 1 \pmod{\pi^{l-1}} \), since \( b \in \mathbb{Z}_l \). This contradicts (4) and completes the proof.

Put \( L = K(\sqrt[l]{\zeta_l}) = K(\zeta_{l^2}) \), where \( \zeta_{l^2} \) is a primitive \( l^2 \)-th root of unity. Then \( L/k \) is a finite abelian extension of \( k \) which is unramified outside \( l \). The next theorem and its corollary give a partial result toward Shioda’s problem when \( \sigma | K = 1 \).
THEOREM 3. Put \( \sigma = (p, L/k) \). Assume that \( \sigma|K = 1 \) and \( \zeta_{\sigma}^2 \neq \zeta_p \). Then

\[
J_l^{(a)}(p) \equiv 1 - \left( 1 - \frac{r'}{2} \right) (q - 1) \pmod{\pi^l}
\equiv 1 - \left( 1 - \frac{r'}{2} \right) \lambda l \pmod{\pi^l}
\]

and \( \lambda \not\equiv 0 \pmod{l} \), where \( \lambda = (q - 1)/l \in \mathbb{Z} \) and \( r' = \# \{ 0 \leq i \leq r \mid a_i \neq 0 \pmod{l} \} \).

Remark. By Lemma 2 and Chebotarev’s density theorem, there exist infinitely many prime ideals \( p \) of \( k \) of degree 1 satisfying the condition in Theorem 3.

Proof of Theorem 3. The condition \( \zeta_{\sigma}^2 \neq \zeta_p \) is equivalent to \( \lambda \not\equiv 0 \pmod{l} \), and the condition \( \sigma|K = 1 \) is equivalent to \( \beta_m(p) \equiv 0 \pmod{l} \) for all odd \( m \) (3 \( \leq m \leq \ell - 2 \)). Hence by Theorem 1,

\[
J_l^{(a)}(p) \equiv q^{-1} \left( 1 - \frac{q - 1}{l} \cdot \frac{r'}{2} \pi^{l-1} \right) \pmod{\pi^l}
\equiv (1 - \lambda l) \left( 1 + \lambda \cdot \frac{r'}{2} \cdot l \right) \pmod{\pi^l}
\equiv 1 - \left( 1 - \frac{r'}{2} \right) \lambda l \pmod{\pi^l}
\equiv 1 - \left( 1 - \frac{r'}{2} \right) (q - 1) \pmod{\pi^l},
\]

since \( \pi^{l-1} \equiv -l \pmod{\pi^l} \). This completes the proof.

Corollary. Assume that \( r \geq 3 \) is odd and that \( a_i \neq 0 \pmod{l} \) for all \( i \) (0 \( \leq i \leq r \)). Let \( p \) satisfy the condition in Theorem 3. Put

\[
S = 1 - J_l^{(a)}(p)q^{-(r-1)/2}.
\]

Then \( S \equiv 0 \pmod{\pi^l} \). In particular, \( \text{ord}_l(N_{k/Q}(S)) \geq l \).

Proof. By Theorem 3,

\[
J_l^{(a)}(p)q^{-(r-1)/2} \equiv \left( 1 - \left( 1 - \frac{r'}{2} \right) \lambda l \right) \left( 1 - \frac{r - 1}{2} \lambda l \right) \pmod{\pi^l}
\equiv 1 - \frac{1}{2} (r - r' + 1) \lambda l \pmod{\pi^l}.
\]

Hence \( S \equiv \frac{1}{2} (r - r' + 1) \lambda l \pmod{\pi^l} \). Since \( r' = r + 1 \) by assumption, this gives the assertion.

Remark. When \((p, L/k) = 1\), Shioda’s problem is still an open problem.
This paper has been written during my stay at the I.H.E.S. in 1991/92. I would like to thank the Institute for their hospitality and its financial support. I would also like to thank Professors Don Zagier, Yuji Kida, and Masanobu Kaneko for supplying me further numerical data on Shioda’s problem.

References