JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Vishal ARUL

On the ℓ-adic valuation of certain Jacobi sums

Tome 33, n° 2 (2021), p. 607-625.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2021__33_2_607_0>

Journal de Théorie des Nombres de Bordeaux **33** (2021), 607–625

On the ℓ-adic valuation of certain Jacobi sums

par Vishal ARUL

Résumé. Soient ℓ et f deux nombres premiers distincts. Soient $\mathbf{F}_q$ un corps fini tel que $q \equiv 1 \pmod{\ell f}$, $\chi_\ell, \chi_f \colon \mathbf{F}_q^\times \to \overline{\mathbf{Q}}^\times$ deux caractères multiplicatifs d'ordres respectifs ℓ et f et $J(\chi_\ell, \chi_f)$ la somme de Jacobi associée. Nous prouvons une nouvelle congruence pour $J(\chi_\ell, \chi_f)$. Plus précisément, nous montrons que $J(\chi_\ell, \chi_f) \equiv -1 \pmod{(1-\zeta_\ell)^i}$ avec $i \leq \ell$ si et seulement si certaines unités cyclotomiques de $\mathbf{F}_q^\times$ sont des puissances ℓ-ièmes.

Abstract. Fix distinct primes ℓ and f, a finite field $\mathbf{F}_q$ such that $q \equiv 1 \pmod{\ell f}$, multiplicative characters $\chi_\ell, \chi_f \colon \mathbf{F}_q^\times \to \overline{\mathbf{Q}}^\times$ of orders ℓ and f, and let $J(\chi_\ell, \chi_f)$ be the associated Jacobi sum. We prove new a ℓ-adic congruence for $J(\chi_\ell, \chi_f)$. More specifically, we give a necessary and sufficient condition for $J(\chi_\ell, \chi_f) \equiv -1 \pmod{(1-\zeta_\ell)^i}$ when $i \leq \ell$ in terms of certain cyclotomic units of $\mathbf{F}_q^\times$ being ℓth powers.

1. Introduction

We first recall the definition of Jacobi sum.

Definition 1.1. Fix a finite field $\mathbf{F}_q$, a field L, and two nontrivial multiplicative characters $\chi, \psi : \mathbf{F}_q^\times \to L^\times$. Then the Jacobi sum $J(\chi, \psi)$ is

$$J(\chi, \psi) := \sum_{x \in \mathbf{F}_q \setminus \{0,1\}} \chi(x)\psi(1-x) \in L.$$

Jacobi sums have various applications in number theory; see [2] for many examples. They appear as Frobenius eigenvalues for the Fermat curve in [9]. The Jacobi sums of the type studied in this paper are Frobenius eigenvalues of the diagonal curve $y^\ell = x^f + 1$, which are studied in [1, 7, 8].

For many applications it is helpful to know congruences for Jacobi sums. In [3], an application of Stickelberger's congruence is used to show the following result.

Theorem 1.2. *Fix a prime power $q = p^f$, where p is a prime. Suppose $\mathfrak{p}$ is a prime of $\mathbf{Q}(\zeta_{q-1})$ lying over p. Suppose $\omega_\mathfrak{p}$ is a Teichmüller character*

Manuscrit reçu le 21 juillet 2020, révisé le 17 janvier 2021, accepté le 19 avril 2021.

2010 *Mathematics Subject Classification.* 11L05, 11R18, 11R27.

Mots-clefs. Jacobi sums, finite fields, cyclotomic units, congruences.

This research was supported in part by grants from the Simons Foundation (#402472 to Bjorn Poonen, and #550033).

on $\mathbf{F}_q$*; i.e, for every* $\alpha \in \mathbf{Z}[\zeta_{q-1}]$ *we have* $\omega_{\mathfrak{p}}(\overline{\alpha}) \equiv \alpha \bmod \mathfrak{p}$*. Then for any integers* k_1, k_2 *in the range* $0 \leq k_1, k_2 < q-1$ *such that* k_1 *and* k_2 *are not both zero, we have*

$$J(\omega_{\mathfrak{p}}^{-k_1}, \omega_{\mathfrak{p}}^{-k_2}) \equiv \frac{(k_1+k_2)!}{k_1!k_2!} \bmod \mathfrak{p}.$$

Theorem 1.2 expands a Jacobi sum p-adically where p is the characteristic of $\mathbf{F}_q$. A variant of this question would be to ask to expand the Jacobi sum ℓ-adically, where ℓ is a prime such that $q \equiv 1 \bmod \ell$. In [4], Evans shows the following.

Theorem 1.3. *Let* $\mathbf{F}_q$ *be a finite field,* $k > 2$ *be an integer such that* $q = fk+1$ *for some integer* f*,* ζ *be a primitive* k*th root of unity, and* χ *a multiplicative character of order* k*. Given integers* a*,* b*, and* c *with* $c = -a-b$*,* $k \nmid a$*,* $k \nmid b$*,* $k \nmid c$*,* $\gcd(a,b,k) = 1$*, we have the following equation modulo* $(1-\zeta^a)(1-\zeta^b)(1-\zeta)$*:*

$$J(\chi^a, \chi^b) \equiv \begin{cases} 2-q & \text{if } k=3, \\ 1+i(q-1)/2 & \text{if } k=4, \\ \chi(-1) & \text{if } k>4. \end{cases}$$

In [10], Miki obtains an ℓ-adic congruence for generalized Jacobi sums $J(\chi^{a_1}, \chi^{a_2}, \ldots, \chi^{a_r})$ where $\chi : \mathbf{F}_q^\times \to \mathbf{C}^\times$ is a character of order $m = \ell^n$ (in particular, $q \equiv 1 \bmod \ell^n$). Miki's congruences generalize Iwasawa's ([6, Theorem 1]) and Ihara's congruences ([5, Corollary to Theorem 7]) for Jacobi sums.

In [11], Uehara establishes an ℓ-adic congruence for Jacobi sums of the form $J(\chi, \chi^{cf})$ where $\chi : \mathbf{F}_q^\times \to \mathbf{C}^\times$ is a character of order $f\ell$ and $q \equiv 1 \bmod f\ell$. Certain cyclotomic units of $\mathbf{Q}(\zeta_{f\ell})$ appear in Uehara's expansion.

Our setup will be very similar to that of Uehara's, and we will also find a connection with cyclotomic units. The main result of this paper is used in [1] to classify torsion points on the diagonal curve $y^n = x^d + 1$.

Let ℓ and f be distinct primes, let $\zeta_\ell, \zeta_f \in \overline{\mathbf{Q}}$ be primitive ℓth and fth roots of unity, let $L = \mathbf{Q}(\zeta_\ell, \zeta_f)$, and let $\pi_\ell = \zeta_\ell - 1$. Let $\mathbf{F}_q$ be a finite field such that $q \equiv 1 \pmod{\ell f}$, let $\chi_\ell, \chi_f \colon \mathbf{F}_q^\times \to L^\times$ be multiplicative characters of orders ℓ and f, and let $J(\chi_\ell, \chi_f)$ be the associated Jacobi sum. We give a necessary and sufficient condition for $J(\chi_\ell, \chi_f) \equiv -1 \pmod{(1-\zeta_\ell)^i}$ when $i \leq \ell$ in terms of certain cyclotomic units of $\mathbf{F}_q^\times$ being ℓth powers.

Uehara [11] establishes an ℓ-adic congruence for a specific linear combination of Jacobi sums of the form $J(\chi, \chi^{cf})$ where $\chi : \mathbf{F}_q^\times \to \mathbf{Q}^\times$ is a character of order ℓf, $q \equiv 1 \pmod{\ell f}$, and $c \not\equiv 0 \pmod{\ell}$. Certain cyclotomic units of $\mathbf{Q}(\zeta_\ell, \zeta_f)$ appear in Uehara's expansion. Since $J(\chi, \psi) = \psi(-1)J(\chi^{-1}\psi^{-1}, \psi)$ ([2, Theorem 2.1.5]), we see that if $cf \equiv -1 \pmod{\ell}$, then $J(\chi, \chi^{cf}) = \pm J(\chi^{-1-cf}, \chi^{cf}) = \pm J(\chi^{cf}, \chi^{-1-cf})$ is a Jacobi sum of

the type we consider since χ^{cf} is a character of order ℓ and χ^{-1-cf} is a character of order f. Therefore, our main result yields an ℓ-adic congruence for one specific Jacobi sum in Uehara's linear combination of Jacobi sums. Our congruence will also be stated in terms of cyclotomic units.

In [1], our congruence is used to determine explicit generators for torsion fields of the jacobian $\mathcal{J}$ of the curve $y^\ell = x^f + 1$. More specifically, the automorphism $\zeta_\ell : (x, y) \mapsto (x, \zeta_\ell y)$ of the curve induces an automorphism ζ_ℓ of $\mathcal{J}$, and $1-\zeta_\ell \in \mathrm{End}(\mathcal{J})$ has degree ℓ^{f-1}. Our Jacobi sum congruences provide a set of generators for the torsion field $L(\mathcal{J}[(1-\zeta_\ell)^i])$ when $i \leq \ell$ in terms of cyclotomic units. In particular, when $i = \ell - 1$, then $\mathcal{J}[(1-\zeta_\ell)^i] = \mathcal{J}[\ell]$, so we gain an explicit understanding of the ℓ-torsion of the jacobian.

Abuse notation to define $\zeta_\ell, \zeta_f \in \mathbf{F}_q$ to be primitive ℓth and fth roots of unity in $\mathbf{F}_q$. Our main theorem will give an ℓ-adic congruence for $J(\chi_\ell, \chi_f)$ in terms of the following cyclotomic units.

Definition 1.4. For $i \in \{0, 1, \ldots, \ell-1\}$ and $j \in \{1, 2, \ldots, f-1\}$, define $\eta_{i,j}$ to be the following cyclotomic unit:

$$\eta_{i,j} := \prod_{r=0}^{\ell-1} \left(1 - \zeta_\ell^r \zeta_f^j\right)^{\binom{r}{i}} \in \mathbf{F}_q^\times,$$

where we take the convention that $\binom{r}{i} = 0$ whenever $i \notin \{0, 1, \ldots, r\}$.

Our main result is the following.

Theorem 1.5. *For $k \in \{1, 2, \ldots, \ell-1\}$, the following are equivalent:*

(1) $J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell^k \mathcal{O}_L}$;
(2) $\eta_{i,j} \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in \{0, 1, \ldots, k-2\}$ *and* $j \in \{1, 2, \ldots, f-1\}$;
(3) $\eta_{i,j} \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in \{0, 1, \ldots, k-2\}$ *and* $j \in \{1, 2, \ldots, \lfloor f/2 \rfloor\}$.

In particular, $J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell \mathcal{O}_L}$ always holds. (Here, the set $\{0, 1, \ldots, k-2\}$ is the empty set if $k = 1$.)

Our methods allow us to even reach the case $k = \ell$, which we analyze in Section 8.

Theorem 1.6. *The following are equivalent:*

(1) $J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell^\ell \mathcal{O}_L}$;
(2) $q \equiv 1 \pmod{\ell^2 f}$ *and* $1 - \zeta_\ell^i \zeta_f^j \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in \{0, 1, \ldots, \ell-1\}$ *and* $j \in \{1, 2, \ldots, f-1\}$;
(3) $q \equiv 1 \pmod{\ell^2 f}$ *and* $1 - \zeta_\ell^i \zeta_f^j \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in \{0, 1, \ldots, \ell-1\}$ *and* $j \in \{1, 2, \ldots, \lfloor f/2 \rfloor\}$.

2. The index

Definition 2.1. Let g be a generator of $\mathbf{F}_q^\times$ such that $g^{(q-1)/\ell f} = \zeta_\ell \zeta_f$.

Definition 2.2. For $x \in \mathbf{F}_q^\times$, define $\operatorname{ind}(x) \in \{0, 1, \dots, q-2\}$ such that $x = g^{\operatorname{ind} x}$.

Lemma 2.3. *For $r \in \{0, 1, \dots, \ell-1\}$ and $j \in \{1, 2, \dots, f-1\}$,*

$$\sum_{\substack{a \in \{1,2,\dots,q-2\} \\ a \equiv j \pmod f \\ a \equiv r \pmod \ell}} \operatorname{ind}(1 - g^a) \equiv \operatorname{ind}\left(1 - \zeta_\ell^r \zeta_f^j\right) \pmod{q-1}.$$

Proof. Take the equality

$$\prod_{k=0}^{\frac{q-1}{\ell f}-1} (1 - g^{k\ell f} X) = 1 - X^{\frac{q-1}{\ell f}} \qquad \text{in } \mathbf{F}_q[X]$$

and substitute $X = g^a$ to obtain

$$\begin{aligned} \prod_{k=0}^{\frac{q-1}{\ell f}-1} (1 - g^{a+k\ell f}) &= 1 - g^{a\left(\frac{q-1}{\ell f}\right)} \\ &= 1 - \zeta_\ell^a \zeta_f^a \qquad (\text{since } g^{\frac{q-1}{\ell f}} = \zeta_\ell \zeta_f) \\ &= 1 - \zeta_\ell^r \zeta_f^j, \end{aligned}$$

so we are done by taking ind of both sides. □

Definition 2.4. For integers a and b, define the Kronecker delta

$$\delta_{a,b} = \begin{cases} 1 & \text{if } a = b \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 2.5.

(1) *For $m \in \{1, 2, \dots, f-1\}$,*

$$\eta_{0,m} = 1 - \zeta_f^{m\ell}.$$

(2) *We have*

$$\operatorname{ind} \zeta_f \equiv 0 \pmod \ell \tag{2.1}$$

$$\operatorname{ind} \zeta_\ell \equiv \frac{q-1}{\ell f} \pmod \ell. \tag{2.2}$$

(3) *For $i \in \{0, 1, \dots, \ell-1\}$ and $j \in \{1, 2, \dots, f-1\}$,*

$$\operatorname{ind} \eta_{i,j} \equiv \sum_{r=0}^{\ell-1} \binom{r}{i} \operatorname{ind}\left(1 - \zeta_\ell^r \zeta_f^j\right) \pmod{q-1}.$$

(4) *For* $i \in \{0, 1, \ldots, \ell-1\}$ *and* $j \in \{1, 2, \ldots, f-1\}$,

$$\operatorname{ind} \eta_{i,f-j} \equiv -\delta_{i,\ell-1}\left(\operatorname{ind}(-1) - \left(\frac{q-1}{\ell f}\right)\right) - \delta_{i,\ell-2}\left(\frac{q-1}{\ell f}\right) + (-1)^i \sum_{k=0}^{i} \binom{i-1}{i-k} \operatorname{ind} \eta_{k,j} \pmod{\ell}.$$

(5) *Suppose that* $i \in \{1, 2, \ldots, \ell-1\}$, $j \in \{1, 2, \ldots, f-1\}$, *and* $m \in \{1, 2, \ldots, f-1\}$ *are such that* $m\ell \equiv j \pmod{f}$. *Then*

$$\operatorname{ind}\left(1 - \zeta_\ell^i \zeta_f^j\right) \equiv \operatorname{ind} \eta_{0,m} - \sum_{s=\ell-1-i}^{\ell-2} \sum_{a=0}^{s} \binom{s}{a} \operatorname{ind} \eta_{\ell-2-a,j} \pmod{\ell}.$$

(6) *For* $i \in \{1, 2, \ldots, \ell-1\}$ *and* $j \in \{1, 2, \ldots, f-1\}$,

$$\operatorname{ind}\left(1 - \zeta_\ell^i \zeta_f^j\right) \equiv \operatorname{ind}(-1) + i\left(\frac{q-1}{\ell f}\right) + \operatorname{ind}\left(1 - \zeta_\ell^{\ell-i} \zeta_f^{f-j}\right) \pmod{\ell}.$$

Proof. (1). Take the equality

$$\prod_{r=0}^{\ell-1} (1 - \zeta_\ell^r X) = 1 - X^\ell \qquad \text{in } \mathbf{F}_q[X]$$

and substitute $X = \zeta_f^m$ to obtain

$$\begin{aligned} \eta_{0,m} &= \prod_{r=0}^{\ell-1} (1 - \zeta_\ell^r \zeta_f^m) \\ &= 1 - (\zeta_f^m)^\ell. \end{aligned}$$

(2). Since ζ_f is an fth root of unity and $\mathbf{F}_q$ contains a primitive ℓfth root of unity, $\zeta_f \in \mathbf{F}_q^{\times \ell}$; (2.1) follows.

Taking ind of both sides of Definition 2.1 yields $(q-1)/(\ell f) \equiv \operatorname{ind} \zeta_\ell + \operatorname{ind} \zeta_f \pmod{q-1}$, so (2.2) follows from Definition 2.1 and (2.1).

(3). Take ind of both sides of Definition 1.4.

(4). Modulo ℓ, we have

$$\begin{aligned} &\operatorname{ind} \eta_{i,f-j} \\ &\equiv \sum_{r=0}^{\ell-1} \binom{r}{i} \operatorname{ind}\left(1 - \zeta_\ell^r \zeta_f^{-j}\right) \\ &\qquad \text{(by Lemma 2.5 (3))} \\ &\equiv \sum_{r=0}^{\ell-1} \binom{r}{i} \left(\operatorname{ind}(-1) + r \operatorname{ind} \zeta_\ell - j \operatorname{ind} \zeta_f + \operatorname{ind}\left(1 - \zeta_\ell^{-r} \zeta_f^j\right)\right) \\ &\qquad \text{(since } \operatorname{ind}(yz) \equiv \operatorname{ind} y + \operatorname{ind} z \pmod{q-1}) \end{aligned}$$

$$\equiv \operatorname{ind}(-1)\left(\sum_{r=0}^{\ell-1}\binom{r}{i}\right)+\left(\frac{q-1}{\ell f}\right)\left(\sum_{r=0}^{\ell-1} r\binom{r}{i}\right) \tag{2.3}$$
$$+\sum_{r=0}^{\ell-1}\binom{r}{i}\operatorname{ind}\left(1-\zeta_\ell^{-r}\zeta_f^j\right)$$
(by Lemma 2.5(2))
$$\equiv \operatorname{ind}(-1)\binom{\ell}{i+1}+\left(\frac{q-1}{\ell f}\right)\left((\ell-1)\binom{\ell}{i+1}-\binom{\ell}{i+2}\right) \tag{2.4}$$
$$+\sum_{r=0}^{\ell-1}\binom{r}{i}\operatorname{ind}\left(1-\zeta_\ell^{-r}\zeta_f^j\right)$$
$$\equiv \delta_{i,\ell-1}\left(\operatorname{ind}(-1)-\left(\frac{q-1}{\ell f}\right)\right)-\delta_{i,\ell-2}\left(\frac{q-1}{\ell f}\right) \tag{2.5}$$
$$+\sum_{r=0}^{\ell-1}\binom{r}{i}\operatorname{ind}\left(1-\zeta_\ell^{-r}\zeta_f^j\right),$$

since $\binom{\ell}{k}$ is divisible by ℓ except when $k\in\{0,\ell\}$, in which case it equals 1 (and we assume that $i\in\{0,1,\dots,\ell-1\}$). Change variables in the last sum to $s\in\{0,1,\dots,\ell-1\}$ such that $s\equiv -r \pmod{\ell}$ (the values $\binom{r}{i}$ and ζ_ℓ^r only depend on $r \pmod{\ell}$ since $i\in\{0,1,\dots,\ell-1\}$). This yields

$$\sum_{r=0}^{\ell-1}\binom{r}{i}\operatorname{ind}\left(1-\zeta_\ell^{-r}\zeta_f^j\right)=\sum_{s=0}^{\ell-1}\binom{-s}{i}\operatorname{ind}\left(1-\zeta_\ell^{s}\zeta_f^j\right)$$
$$\equiv (-1)^i\sum_{s=0}^{\ell-1}\sum_{k=0}^{i}\binom{i-1}{i-k}\binom{s}{k}\operatorname{ind}\left(1-\zeta_\ell^{s}\zeta_f^j\right)$$
$$\equiv (-1)^i\sum_{k=0}^{i}\binom{i-1}{i-k}\operatorname{ind}\eta_{k,j} \tag{2.6}$$

by Lemma 2.5(3). We finish by combining (2.5) and (2.6).

(5). Modulo ℓ, we have

$$\sum_{s=\ell-1-i}^{\ell-2}\sum_{a=0}^{s}\binom{s}{a}\operatorname{ind}\eta_{\ell-2-a,j}$$
$$\equiv \sum_{s=\ell-1-i}^{\ell-2}\sum_{r=0}^{\ell-1}\sum_{a=0}^{s}\binom{s}{a}\binom{r}{\ell-2-a}\operatorname{ind}\left(1-\zeta_\ell^{r}\zeta_f^j\right)$$
(by Lemma 2.5(3))

$$
\begin{aligned}
&= \sum_{s=\ell-1-i}^{\ell-2} \sum_{r=0}^{\ell-1} \binom{r+s}{\ell-2} \operatorname{ind}\left(1-\zeta_\ell^r \zeta_f^j\right) \\
&\equiv \sum_{s=\ell-1-i}^{\ell-2} \left(\operatorname{ind}\left(1-\zeta_\ell^{\ell-2-s}\zeta_f^j\right) - \operatorname{ind}\left(1-\zeta_\ell^{\ell-1-s}\zeta_f^j\right)\right) \\
&\qquad \left(\text{since } \binom{r+s}{\ell-2} \equiv 0 \pmod{\ell} \text{ when } r+s \notin \{\ell-2, \ell-1\}\right) \\
&= \operatorname{ind}\left(1-\zeta_f^j\right) - \operatorname{ind}\left(1-\zeta_\ell^i\zeta_f^j\right) \\
&\qquad \text{(telescoping sum)} \\
&= \operatorname{ind}\eta_{0,m} - \operatorname{ind}\left(1-\zeta_\ell^i\zeta_f^j\right) \\
&\qquad \text{(by Lemma 2.5 (1))}.
\end{aligned}
$$

(6). Taking ind of both sides of $1-\zeta_\ell^i\zeta_f^j = -\zeta_\ell^i\zeta_f^j\left(1-\zeta_\ell^{\ell-i}\zeta_f^{f-j}\right)$ gives

$$
\begin{aligned}
&\operatorname{ind}\left(1-\zeta_\ell^i\zeta_f^j\right) \\
&\equiv \operatorname{ind}(-1) + i\operatorname{ind}\zeta_\ell + j\operatorname{ind}\zeta_f + \operatorname{ind}\left(1-\zeta_\ell^{\ell-i}\zeta_f^{f-j}\right) \pmod{\ell} \\
&\equiv \operatorname{ind}(-1) + i\left(\frac{q-1}{\ell f}\right) + \operatorname{ind}\left(1-\zeta_\ell^{\ell-i}\zeta_f^{f-j}\right) \pmod{\ell}
\end{aligned}
$$

by (2.2) and (2.1). □

3. Some rings

Definition 3.1. Without loss of generality and by abuse of notation, let $\zeta_\ell = \chi_\ell(g) \in L$, let $\zeta_f = \chi_f(g) \in L$, and let $\pi_\ell = \zeta_\ell - 1$. Let $M = \mathbf{Q}(\zeta_f)$.

Definition 3.2. Define $Q := \mathbf{Z}[t]/(t^f-1)$. Define ring homomorphisms $\alpha\colon Q \to \mathcal{O}_M$ and $\beta\colon Q \to \mathbf{Z}$ by $\alpha(t) = \zeta_f$ and $\beta(t) = 1$. Define

R	$:= Q/\ell Q = \mathbf{Z}[t]/(\ell, t^f-1)$
R'	:= the subring $\mathbf{Z}/\ell\mathbf{Z}$ of R
$\omega\colon R \to \mathcal{O}_M/\ell\mathcal{O}_M$	:= the ring homomorphism induced by α; $\omega(t) = [\zeta_f]$
$\tau\colon R \to \mathbf{Z}/\ell\mathbf{Z}$	:= the ring homomorphism induced by β; $\tau(t) = 1$.

Each $r \in R$ has a unique representation $r = a_0 + a_1 t + \cdots + a_{f-1}t^{f-1}$ for $a_0, a_1, \ldots, a_{f-1} \in \mathbf{Z}/\ell\mathbf{Z}$, so for $j \in \{0, 1, \ldots, f-1\}$, define

$$[t^j](r) := a_j$$

to be the jth coefficient of r.

Lemma 3.3. *The product homomorphism*

$$(\omega, \tau) : R \to (\mathcal{O}_M/\ell\mathcal{O}_M) \times (\mathbf{Z}/\ell\mathbf{Z})$$

is an isomorphism.

Proof. The ideals I_1, I_2 of R defined by

$$\begin{aligned} I_1 &:= (t^{f-1} + t^{f-2} + \cdots + 1) \\ I_2 &:= (t-1) \end{aligned}$$

are pairwise coprime because for

$$\begin{aligned} i_1 &:= t^{f-1} + t^{f-2} + \cdots + 1 && \in I_1, \\ i_2 &:= (t^{f-1} - 1) + (t^{f-2} - 1) + \cdots + (t-1) && \in I_2, \end{aligned}$$

the difference $i_1 - i_2 = f$ is a unit of R, so by the Chinese remainder theorem, the natural map

$$R \to (R/I_1) \times (R/I_2)$$

is an isomorphism. Since ω, τ are each surjective and their kernels are I_1, I_2 respectively, they induce the isomorphisms $R/I_1 \simeq \mathcal{O}_M/\ell\mathcal{O}_M$ and $R/I_2 \simeq \mathbf{Z}/\ell\mathbf{Z}$, so the lemma follows. □

Lemma 3.4. *For $r \in \ker\tau$, the following are equivalent.*

(1) $\omega(r) = 0$;
(2) $r = 0$;
(3) $r \in R'$.

Proof. The restriction $\tau|_{R'} : R' \to \mathbf{Z}/\ell\mathbf{Z}$ is an isomorphism, so $r \in R' \cap \ker\tau$ if and only if $r = 0$, giving the equivalence between Lemma 3.4(3) and Lemma 3.4(2). By Lemma 3.3, $r = 0$ if and only if $\tau(r) = 0$ and $\omega(r) = 0$, giving the equivalence between Lemma 3.4(1) and Lemma 3.4(2). □

Definition 3.5. For nonnegative integers u and v, define

$$\begin{aligned} S(u,v) &:= \sum_{x \in \mathbf{F}_q \setminus \{0,1\}} \binom{\operatorname{ind} x}{u} \binom{\operatorname{ind}(1-x)}{v} t^{\operatorname{ind} x} && \in R \\ T(u,v) &:= \tau(S(u,v)) && \in \mathbf{Z}/\ell\mathbf{Z} \\ W(u,v) &:= \omega(S(u,v)) && \in \mathcal{O}_M/\ell\mathcal{O}_M. \end{aligned}$$

Lemma 3.6. *For $i \in \{0, 1, \ldots, \ell-1\}$,*

$$T(0,i) = \begin{cases} -1 & \text{if } i = 0 \\ 0 & \text{if } i \in \{1, 2, \ldots, \ell-2\} \\ \frac{q-1}{\ell} & \text{if } i = \ell - 1. \end{cases}$$

Proof. We have

$$\begin{aligned} T(0,i) &= \tau(S(0,i)) \\ &= \tau\left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(1-x)}{i} t^{\operatorname{ind} x}\right) \\ &= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(1-x)}{i} \\ &= \sum_{k=1}^{q-2} \binom{k}{i} \\ &\qquad (\text{since } \{\operatorname{ind} x : x \in \mathbf{F}_q \setminus \{0,1\}\} = \{1,2,\dots,q-2\}) \\ &= \binom{q-1}{i+1} - \binom{0}{i}, \end{aligned}$$

and the rest follows from breaking into cases depending on the value of i; when $i = \ell - 1$, we use the fact that $\binom{a\ell}{b\ell} \equiv \binom{a}{b} \pmod{\ell}$. □

Lemma 3.7.

(1) *For $i \in \{1,2,\dots,\ell-2\}$, the following are equivalent:*
   (a) $S(0,i) \in R'$;
   (b) $W(0,i) = 0$.

(2) *The following are equivalent:*
   (a) $S(0,\ell-1) - \frac{q-1}{\ell f}(1+t+t^2+\cdots+t^{f-1}) \in R'$;
   (b) $W(0,\ell-1) = 0$.

Proof. Lemma 3.6 implies that

$$S(0,i) \in \ker\tau$$
$$S(0,\ell-1) - \frac{q-1}{\ell f}(1+t+t^2+\cdots+t^{f-1}) \in \ker\tau,$$

so we are done by applying the equivalence between Lemma 3.4(1) and Lemma 3.4(3) to $r = S(0,i)$ and to $r = S(0,\ell-1) - \frac{q-1}{\ell f}(1+t+t^2+\cdots+t^{f-1})$. □

4. ℓ-adic valuation of Jacobi sums

Lemma 4.1.

(1) *For $k \in \{1,2,\dots,\ell-1\}$, the following are equivalent:*
   (a) $J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell^k \mathcal{O}_L}$;
   (b) $S(0,1),\ S(0,2),\ \dots,\ S(0,k-1) \in R'$.

(2) *The following are equivalent:*
   (a) $J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell^\ell \mathcal{O}_L}$;
   (b) $S(0,1),\ S(0,2),\ \ldots,\ S(0,\ell-2) \in R'$, *and also* $S(0,\ell-1) - \frac{q-1}{\ell f}\left(1+t+\cdots+t^{f-1}\right) \in R'$.

Proof. Using $J(\chi,\psi) = J(\psi,\chi)$,

$$\begin{aligned}
J(\chi_\ell,\chi_f) &= J(\chi_f,\chi_\ell)\\
&= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \chi_f(x)\chi_\ell(1-x)\\
&= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \zeta_f^{\mathrm{ind}(x)}\zeta_\ell^{\mathrm{ind}(1-x)}\\
&= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \zeta_f^{\mathrm{ind}(x)}(1+\pi_\ell)^{\mathrm{ind}(1-x)}\\
&= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \zeta_f^{\mathrm{ind}(x)} \sum_{i=0}^{\mathrm{ind}(1-x)} \binom{\mathrm{ind}(1-x)}{i}\pi_\ell^i\\
&= \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \zeta_f^{\mathrm{ind}(x)} \sum_{i=0}^{q-1} \binom{\mathrm{ind}(1-x)}{i}\pi_\ell^i\\
&\qquad (\text{since } \mathrm{ind}(1-x) < q-1)\\
&= \sum_{i=0}^{q-1}\pi_\ell^i\left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}}\binom{\mathrm{ind}(1-x)}{i}\zeta_f^{\mathrm{ind}(x)}\right)\\
&\qquad \in \left(\sum_{i=0}^{\ell-1}\pi_\ell^i\left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}}\binom{\mathrm{ind}(1-x)}{i}\zeta_f^{\mathrm{ind}(x)}\right)\right) + \pi_\ell^\ell\mathcal{O}_L
\end{aligned}$$

Since $\{\mathrm{ind}\, x : x \in \mathbf{F}_q\setminus\{0,1\}\} = \{1,2,\ldots,q-2\}$, the $i=0$ term contributes $\zeta_f^1+\cdots+\zeta_f^{q-2} = (\zeta_f^{q-1}-\zeta_f)/(\zeta_f-1) = -1$ since $q \equiv 1 \pmod{\ell f}$, so

$$J(\chi_\ell,\chi_f) \in \left(-1+\sum_{i=1}^{\ell-1}\pi_\ell^i\left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}}\binom{\mathrm{ind}(1-x)}{i}\zeta_f^{\mathrm{ind}(x)}\right)\right)+\pi_\ell^\ell\mathcal{O}_L \tag{4.1}$$

Since $v_\ell(\pi_\ell) = \frac{1}{\ell-1}$, the term $\left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}}\binom{\mathrm{ind}(1-x)}{i}\zeta_f^{\mathrm{ind}(x)}\right)$ lies in $\mathcal{O}_M$, and M is unramified at ℓ, the ith term in the sum on the right hand side of (4.1) has ℓ-adic valuation $\frac{i}{\ell-1} \pmod 1$. In particular, all the valuations are distinct, so

$$J(\chi_\ell,\chi_f) \equiv -1 \pmod{\pi_\ell^k\mathcal{O}_L}$$

if and only if

$$\sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(1-x)}{i} \zeta_f^{\operatorname{ind}(x)} \in \ell\mathcal{O}_M \qquad \text{for } i\in\{1,2,\dots,k-1\},$$

which is the same as

$$W(0,1),\ W(0,2),\ \dots,\ W(0,k-1)=0,$$

so we are done by Lemma 3.7. □

5. The connection between $S(i,1)$ and cyclotomic units

Lemma 5.1. *For $i\in\{0,1,\dots,\ell-1\}$ and $j\in\{1,2,\dots,f-1\}$,*

$$[t^j]S(i,1)\equiv \operatorname{ind}\eta_{i,j} \pmod{\ell}.$$

Proof. By definition of $S(i,1)$,

$$\begin{aligned}
[t^j]S(i,1) &= \sum_{\substack{a\in\{1,2,\dots,q-2\}\\ a\equiv j \pmod f}} \binom{a}{i} \operatorname{ind}(1-g^a)\\
&= \sum_{r=0}^{\ell-1} \sum_{\substack{a\in\{1,2,\dots,q-2\}\\ a\equiv j \pmod f\\ a\equiv r \pmod \ell}} \binom{a}{i} \operatorname{ind}(1-g^a)\\
&\equiv \sum_{r=0}^{\ell-1} \binom{r}{i} \sum_{\substack{a\in\{1,2,\dots,q-2\}\\ a\equiv j \pmod f\\ a\equiv r \pmod \ell}} \operatorname{ind}(1-g^a) \pmod{\ell}\\
&\equiv \sum_{r=0}^{\ell-1} \binom{r}{i} \operatorname{ind}\left(1-\zeta_\ell^r\zeta_f^j\right) \pmod{\ell}\\
&\qquad \text{(by Lemma 2.3)}\\
&\equiv \operatorname{ind}\eta_{i,j} \pmod{\ell}\\
&\qquad \text{(by Lemma 2.5(3))}.
\end{aligned}$$

□

Lemma 5.2.

(1) *For $i\in\{0,1,\dots,\ell-3\}$, the following are equivalent:*
   (a) $S(i,1)\in R'$;
   (b) $\operatorname{ind}\eta_{i,j}\equiv 0 \pmod{\ell}$ *for* $j\in\{1,2,\dots,f-1\}$.

(2) *The following are equivalent:*
   (a) $S(\ell-2,1)+\frac{q-1}{\ell f}\left(1+t+\cdots+t^{f-1}\right)\in R'$;
   (b) $\operatorname{ind}(\eta_{\ell-2,j})+\frac{q-1}{\ell f}\equiv 0 \pmod{\ell}$ *for* $j\in\{1,2,\dots,f-1\}$.

Proof. For any $r \in R$, the condition $r \in R'$ is equivalent to $[t^j]r \equiv 0 \pmod{\ell}$ for $j \in \{1, 2, \ldots, f-1\}$. Apply this observation to $r = S(0,1), \ldots, r = S(\ell-3,1)$, and also to $r = S(\ell-2,1) + \frac{q-1}{\ell f}\left(1 + t + \cdots + t^{f-1}\right)$ and use Lemma 5.1 to finish. □

6. A recursion for $S(u, v)$

In this section, we will investigate the product of expressions of the form $S(u, v)$.

Lemma 6.1. *For $i \in \{1, 2, \ldots, \ell-2\}$ and $s \in \{1, 2, \ldots, i\}$,*

$$\begin{aligned}&(i-s+1)S(i-s+1,s) - (s+1)S(i-s,s+1)\\ &\equiv \left(\sum_{r=0}^{i-s} S(i-s-r,s)S(r,1)\right) - \left(\sum_{k=1}^{s} T(1,s-k)S(i-s,k)\right)\\ &\quad - (i-2s)S(i-s,s) \pmod{R'}.\end{aligned}$$

Proof. By definition of $S(u, v)$,

$$\begin{aligned}&\sum_{r=0}^{i-s} S(i-s-r,s)S(r,1)\\ &= \sum_{y,z\in\mathbf{F}_q\setminus\{0,1\}} \sum_{r=0}^{i-s} \binom{\operatorname{ind}(y)}{i-s-r}\binom{\operatorname{ind}(z)}{r}\binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(1-z)t^{\operatorname{ind} y}t^{\operatorname{ind} z}\\ &= \sum_{y,z\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(y)+\operatorname{ind}(z)}{i-s}\binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(1-z)t^{\operatorname{ind} y+\operatorname{ind} z}\\ &= \sum_{y,z\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(yz)}{i-s}\binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(1-z)t^{\operatorname{ind}(yz)}\\ &= \sum_{\substack{x\in\mathbf{F}_q\setminus\{0\}\\ y\in\mathbf{F}_q\setminus\{0,1,x\}}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}\left(1-\frac{x}{y}\right)\binom{\operatorname{ind} x}{i-s}t^{\operatorname{ind} x}\\ &\quad \text{(by setting } x := yz)\\ &= \sum_{\substack{x\in\mathbf{F}_q\setminus\{0\}\\ y\in\mathbf{F}_q\setminus\{0,1,x\}}} \binom{\operatorname{ind}(1-y)}{s} (\operatorname{ind}(y-x)-\operatorname{ind}(y))\binom{\operatorname{ind} x}{i-s}t^{\operatorname{ind} x}\\ &\quad \text{(since } \operatorname{ind}(1-x/y) \equiv \operatorname{ind}(y-x)-\operatorname{ind}(y) \pmod{q-1})\\ &\equiv \sum_{\substack{x\in\mathbf{F}_q\setminus\{0,1\}\\ y\in\mathbf{F}_q\setminus\{0,1,x\}}} \binom{\operatorname{ind}(1-y)}{s} (\operatorname{ind}(y-x)-\operatorname{ind}(y))\binom{\operatorname{ind} x}{i-s}t^{\operatorname{ind} x} \pmod{R'},\end{aligned}$$

so if we define

$$A := \sum_{\substack{x\in\mathbf{F}_q\setminus\{0,1\}\\ y\in\mathbf{F}_q\setminus\{0,1,x\}}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(y-x) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x},$$

$$B := \sum_{\substack{x\in\mathbf{F}_q\setminus\{0,1\}\\ y\in\mathbf{F}_q\setminus\{0,1,x\}}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(y) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x},$$

then

$$\sum_{r=0}^{i-s} S(i-s-r,s)S(r,1) \equiv A - B \pmod{R'}. \tag{6.1}$$

We have

$$\begin{aligned}
B &= \sum_{\substack{x\in\mathbf{F}_q\setminus\{0,1\}\\ y\in\mathbf{F}_q\setminus\{0,1\}}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(y) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\quad - \sum_{\substack{x\in\mathbf{F}_q\setminus\{0,1\}\\ y=x}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(y) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&= \left(\sum_{y\in\mathbf{F}_q\setminus\{0,1\}} \operatorname{ind}(y) \binom{\operatorname{ind}(1-y)}{s} \right) \left(\sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \right) \\
&\quad - \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(1-x)}{s} \operatorname{ind}(x) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&= T(1,s)S(i-s,0) - \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(1-x)}{s} \operatorname{ind}(x) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\qquad \text{(by definition of } T(1,s) \text{ and } S(i-s,0)) \\
&= T(1,s)S(i-s,0) \\
&\quad - \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(1-x)}{s} (i-s+1) \binom{\operatorname{ind} x}{i-s+1} t^{\operatorname{ind} x} \\
&\quad - \sum_{x\in\mathbf{F}_q\setminus\{0,1\}} \binom{\operatorname{ind}(1-x)}{s} (i-s) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&= T(1,s)S(i-s,0) - (i-s+1)S(i-s+1,s) - (i-s)S(i-s,s) \\
&\qquad \text{(by definition of } S(i-s+1,s) \text{ and } S(i-s,s))\,.
\end{aligned}$$

Since $s \geq 1$, the summand in A vanishes when $y = 0$, so we can put it back in to get

$$\begin{aligned}
A &= \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ y \in \mathbf{F}_q \setminus \{1,x\}}} \binom{\operatorname{ind}(1-y)}{s} \operatorname{ind}(y-x) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&= \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ w \in \mathbf{F}_q \setminus \{0,1\}}} \binom{\operatorname{ind}((1-x)(1-w))}{s} \operatorname{ind}((1-x)w) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\qquad \text{(by setting } w := (x-y)/(x-1)) \\
&= \sum_{k=0}^{s} \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ w \in \mathbf{F}_q \setminus \{0,1\}}} \binom{\operatorname{ind}(1-x)}{k} \binom{\operatorname{ind}(1-w)}{s-k} \operatorname{ind}(1-x) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\qquad + \sum_{k=0}^{s} \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ w \in \mathbf{F}_q \setminus \{0,1\}}} \binom{\operatorname{ind}(1-x)}{k} \binom{\operatorname{ind}(1-w)}{s-k} \operatorname{ind}(w) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&= \sum_{k=0}^{s} \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ w \in \mathbf{F}_q \setminus \{0,1\}}} (k+1) \binom{\operatorname{ind}(1-x)}{k+1} \binom{\operatorname{ind}(1-w)}{s-k} \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\qquad + \sum_{k=0}^{s} \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ w \in \mathbf{F}_q \setminus \{0,1\}}} k \binom{\operatorname{ind}(1-x)}{k} \binom{\operatorname{ind}(1-w)}{s-k} \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x} \\
&\qquad + \sum_{k=0}^{s} \sum_{\substack{x \in \mathbf{F}_q \setminus \{0,1\} \\ w \in \mathbf{F}_q \setminus \{0,1\}}} \binom{\operatorname{ind}(1-x)}{k} \binom{\operatorname{ind}(1-w)}{s-k} \operatorname{ind}(w) \binom{\operatorname{ind} x}{i-s} t^{\operatorname{ind} x},
\end{aligned}$$

which we rewrite using the definition of $S(u,v)$ and $T(u,v)$ as

$$\begin{aligned}
A &= \sum_{k=0}^{s} T(0, s-k)(k+1) S(i-s, k+1) \\
&\qquad + \sum_{k=0}^{s} T(0, s-k) k S(i-s, k) \\
&\qquad + \sum_{k=0}^{s} T(1, s-k) S(i-s, k) \\
&= -(s+1) S(i-s, s+1) - s S(i-s, s) + \sum_{k=0}^{s} T(1, s-k) S(i-s, k) \\
&\qquad \text{(by Lemma 3.6)}
\end{aligned}$$

$$= -(s+1)S(i-s,s+1) - sS(i-s,s) + T(1,s)S(i-s,0) + \sum_{k=1}^{s} T(1,s-k)S(i-s,k),$$

and we finish by substituting these expressions for A and B into (6.1). □

Corollary 6.2. *Suppose that $i \in \{1,2,\ldots,\ell-2\}$. Assume that $S(u,v) \in R'$ holds whenever $u+v \leq i$ and $v \geq 1$. Then for all $s \in \{1,2,\ldots,i\}$,*

$$(i-s+1)S(i-s+1,s) \equiv (s+1)S(i-s,s+1) \pmod{R'}.$$

Proof. The assumptions imply that all the terms on the right hand side of Lemma 6.1 lie in R', so Lemma 6.1 implies the corollary. □

Corollary 6.3. *Suppose that $i \in \{1,2,\ldots,\ell-2\}$. Assume that $S(u,v) \in R'$ holds whenever $u+v \leq i$ and $v \geq 1$. Then if one of*

$$S(i,1),\ S(i-1,2),\ \ldots,\ S(0,i+1)$$

is in R', then they must all be in R'.

Proof. For $s \in \{1,2,\ldots,i\}$, Corollary 6.2 implies

$$(i-s+1)S(i-s+1,s) \equiv (s+1)S(i-s,s+1) \pmod{R'},$$

so since $i-s+1$ and $s+1$ are invertible modulo ℓ (they lie in $[1,\ell-1]$),

$$S(i-s+1,s) \in R' \text{ if and only if } S(i-s,s+1) \in R'.$$

Since this holds for all $s \in \{1,2,\ldots,i\}$, we are done. □

7. Proof of main theorem

Now we combine all of our results from the previous sections in the following lemma.

Lemma 7.1. *For $k \in \{1,2,\ldots,\ell-1\}$, the following are equivalent:*

(1) *$S(0,1), S(1,1), \ldots, S(k-2,1)$ lie in R';*
(2) *$S(u,v)$ lies in R' for $u \geq 0$ and $v \geq 1$ satisfying $u+v \leq k-1$;*
(3) *$S(0,1), S(0,2), \ldots, S(0,k-1)$ lie in R';*
(4) *$J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell^k \mathcal{O}_L}$.*

Proof. Corollary 6.3 implies that the statements of Lemma 7.1 (1), Lemma 7.1 (2), Lemma 7.1 (3) are equivalent. By Lemma 4.1 (1), the statements of Lemma 7.1 (3), Lemma 7.1 (4) are equivalent. □

We now prove Theorem 1.5, which we restate in this section as Theorem 7.2.

Theorem 7.2. *For $k \in \{1,2,\ldots,\ell-1\}$, the following are equivalent:*

(1) *$J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell^k \mathcal{O}_L}$;*
(2) *$\eta_{i,j} \in \mathbf{F}_q^{\times \ell}$ for all $i \in \{0,1,\ldots,k-2\}$ and $j \in \{1,2,\ldots,f-1\}$;*

(3) $\eta_{i,j} \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in \{0, 1, \ldots, k-2\}$ *and* $j \in \{1, 2, \ldots, \lfloor f/2 \rfloor\}$.

In particular, $J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell \mathcal{O}_L}$ *always holds. (Here, the set* $\{0, 1, \ldots, k-2\}$ *is the empty set if* $k = 1$*.)*

Proof. Combine Lemma 5.2(1) and the equivalence between Lemma 7.1(1) and Lemma 7.1(4) to obtain that Theorem 7.2(1) and Theorem 7.2(2) are equivalent.

By Lemma 2.5(4), for $i \in \{0, 1, \ldots, \ell-3\}$ and $j \in \{1, 2, \ldots, \lfloor f/2 \rfloor\}$, $\operatorname{ind} \eta_{i,f-j}$ is a linear combination of $\operatorname{ind} \eta_{0,j}, \ldots, \operatorname{ind} \eta_{i,j}$ modulo ℓ, and this implies that Theorem 7.2(2) and Theorem 7.2(3) are equivalent. □

8. The case $k = \ell$

Lemma 8.1. *The following are equivalent.*

(1) $J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell^\ell \mathcal{O}_L}$;

(2) $S(0,1),\ S(1,1),\ \ldots,\ S(\ell-3,1),\ S(\ell-2,1) + \dfrac{q-1}{\ell f}(1 + t + t^2 + \cdots + t^{f-1}) \in R'$.

Proof. By Lemma 4.1(2),

- $J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell^\ell \mathcal{O}_L}$

is equivalent to

- $S(0,1)$, $S(0,2)$, …, $S(0,\ell-2)$ lie in R', and
- $S(0,\ell-1) - \frac{q-1}{\ell f}(1 + t + \cdots + t^{f-1})$ lies in R',

which by the equivalence between Lemma 7.1(3) and Lemma 7.1(2), is equivalent to

- for $u \geq 0$ and $v \geq 1$ satisfying $u + v \leq \ell - 2$, $S(u,v)$ lies in R', and
- $S(0,\ell-1) - \frac{q-1}{\ell f}(1 + t + \cdots + t^{f-1})$ lies in R',

which by Corollary 6.2, is equivalent to

- for $u \geq 0$ and $v \geq 1$ satisfying $u + v \leq \ell - 2$, $S(u,v)$ lies in R',
- $S(\ell-2,1) - (-1)^{\ell-2}\frac{q-1}{\ell f}(1 + t + \cdots + t^{f-1})$ lies in R',

which by the equivalence between Lemma 7.1(2) and Lemma 7.1(1), is equivalent to

- $S(0,1)$, $S(1,1)$, …, $S(\ell-3,1)$ lies in R',
- $S(\ell-2,1) - (-1)^{\ell-2}\frac{q-1}{\ell f}(1 + t + \cdots + t^{f-1})$ lies in R',

and we are done by observing that $(-1)^{\ell-2} \equiv -1 \pmod{\ell}$. □

Lemma 8.2. *The following are equivalent:*

(1) $J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell^\ell \mathcal{O}_L}$;

(2) *All the following are divisible by* ℓ*:*

$$\begin{array}{cccc} \operatorname{ind}(\eta_{0,1}) & \operatorname{ind}(\eta_{0,2}) & \dots & \operatorname{ind}(\eta_{0,f-1}) \\ \operatorname{ind}(\eta_{1,1}) & \operatorname{ind}(\eta_{1,2}) & \dots & \operatorname{ind}(\eta_{1,f-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \operatorname{ind}(\eta_{\ell-3,1}) & \operatorname{ind}(\eta_{\ell-3,2}) & \dots & \operatorname{ind}(\eta_{\ell-3,f-1}) \\ \operatorname{ind}(\eta_{\ell-2,1}) + \frac{q-1}{\ell f} & \operatorname{ind}(\eta_{\ell-2,2}) + \frac{q-1}{\ell f} & \dots & \operatorname{ind}(\eta_{\ell-2,f-1}) + \frac{q-1}{\ell f} \end{array}$$

Proof. Combine Lemma 5.2(2) and Lemma 8.1. □

Corollary 8.3. *The following are equivalent:*

(1) $J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell^\ell \mathcal{O}_L}$;

(2) $\frac{q-1}{\ell f} \equiv 0 \pmod{\ell}$ *and* $\operatorname{ind}(1-\zeta_\ell^i \zeta_f^j) \equiv 0 \pmod{\ell}$ *when* $i \in \{0, 1, \dots, \ell-1\}$ *and* $j \in \{1, 2, \dots, f-1\}$;

(3) $\frac{q-1}{\ell f} \equiv 0 \pmod{\ell}$ *and* $\operatorname{ind}(1-\zeta_\ell^i \zeta_f^j) \equiv 0 \pmod{\ell}$ *when* $i \in \{0, 1, \dots, \ell-1\}$ *and* $j \in \{1, 2, \dots, \lfloor f/2 \rfloor\}$.

Proof. We break the proof into four statements.

(1) That Corollary 8.3(2) implies Corollary 8.3(3).
This is obvious.

(2) That Corollary 8.3(2) implies Corollary 8.3(1).
This follows from Lemma 2.5(3) and that Lemma 8.2(2) implies Lemma 8.2(1).

(3) That Corollary 8.3(3) implies Corollary 8.3(2).
Suppose that $i \in \{0, 1, \dots, \ell-1\}$ and $j \in [f/2, f-1]$. Then

$$\operatorname{ind}\left(1-\zeta_\ell^i \zeta_f^j\right)$$

$$\equiv \operatorname{ind}(-1) + i\left(\frac{q-1}{\ell f}\right) + \operatorname{ind}\left(1-\zeta_\ell^{\ell-i}\zeta_f^{f-j}\right) \pmod{\ell} \tag{8.1}$$

(by Lemma 2.5(6))

$$\equiv \operatorname{ind}(-1) \tag{8.2}$$

$$\left(\text{since } \frac{q-1}{\ell f} \equiv 0 \pmod{\ell} \text{ and } f-j \in \{1, 2, \dots, \lfloor f/2 \rfloor\}\right).$$

If $\ell = 2$, then $\operatorname{ind}(-1) = (q-1)/2 = (q-1)/\ell \equiv 0 \pmod{\ell}$ since $q - 1 \equiv 0 \pmod{\ell^2 f}$ by assumption. If ℓ is odd, then $\operatorname{ind}(-1) = (q-1)/2 \equiv 0 \pmod{\ell}$ since $q - 1 \equiv 0 \pmod{\ell}$ and 2 is coprime to ℓ. In any case, $\operatorname{ind}(-1) \equiv 0 \pmod{\ell}$ so we are done by (8.2).

(4) That Corollary 8.3(1) implies Corollary 8.3(2).
Corollary 8.3(1) is Lemma 8.2(1), so Lemma 8.2 implies that Lemma 8.2(2) holds. Combining Lemma 8.2(2) with Lemma 2.5(4)

with $i = \ell - 2$ (and any value of j) yields

$$-\left(\frac{q-1}{\ell f}\right) \equiv -\left(\frac{q-1}{\ell f}\right) - (-1)^{\ell-2}\left(\frac{q-1}{\ell f}\right) \pmod{\ell},$$

which implies

$$\frac{q-1}{\ell f} \equiv 0 \pmod{\ell}.$$

Combining this with Lemma 8.2 (2) implies that $\operatorname{ind} \eta_{k,j} \equiv 0 \pmod{\ell}$ for all $k \in \{0, 1, \ldots, \ell-2\}$ and $j \in \{1, 2, \ldots, f-1\}$, so Lemma 2.5 (5) gives that $\operatorname{ind}\left(1 - \zeta_\ell^i \zeta_f^j\right) \equiv 0 \pmod{\ell}$ for all $i \in \{1, 2, \ldots, \ell-1\}$ and $j \in \{1, 2, \ldots, f-1\}$.

□

We now prove Theorem 1.6, which we restate in this section as Theorem 8.4.

Theorem 8.4. *The following are equivalent:*

(1) $J(\chi_\ell, \chi_f) \equiv -1 \pmod{\pi_\ell^\ell \mathcal{O}_L}$;
(2) $q \equiv 1 \pmod{\ell^2 f}$ *and* $1 - \zeta_\ell^i \zeta_f^j \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in \{0, 1, \ldots, \ell-1\}$ *and* $j \in \{1, 2, \ldots, f-1\}$;
(3) $q \equiv 1 \pmod{\ell^2 f}$ *and* $1 - \zeta_\ell^i \zeta_f^j \in \mathbf{F}_q^{\times \ell}$ *for all* $i \in \{0, 1, \ldots, \ell-1\}$ *and* $j \in \{1, 2, \ldots, \lfloor f/2 \rfloor\}$.

Proof. This is a restatement of Corollary 8.3. □

References

[1] V. Arul, "Torsion points on Fermat quotients of the form $y^n = x^d + 1$", `https://arxiv.org/abs/1910.14251`, 2020.

[2] B. C. Berndt, R. J. Evans & K. S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, 1998.

[3] K. Conrad, "Jacobi sums and Stickelberger's congruence", *Enseign. Math.* **41** (1995), no. 1-2, p. 141-141.

[4] R. J. Evans, "Congruences for Jacobi sums", *J. Number Theory* **71** (1998), no. 1, p. 109-120.

[5] Y. Ihara, "Profinite braid groups, Galois representations and complex multiplications", *Ann. Math.* **123** (1986), no. 1, p. 43-106.

[6] K. Iwasawa, "A note on Jacobi sums", *Symposia Math* **15** (1975), p. 447-459.

[7] T. Jędrzejak, "On the torsion of the jacobians of superelliptic curves $y^q = x^p + a$", *J. Number Theory* **145** (2014), p. 402-425.

[8] ———, "A note on the torsion of the jacobians of superelliptic curves $y^q = x^p + a$", in *Algebra, logic and number theory*, Banach Center Publications, vol. 108, Polish Academy of Sciences, 2016, p. 143-149.

[9] N. M. Katz, "Crystalline Cohomology, Dieudonné Modules, and Jacobi Sums", in *Automorphic forms, representation theory and arithmetic*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 10, Springer, 1981, p. 165-246.

[10] H. Miki, "On the ℓ-adic expansion of certain Gauss sums and its applications", in *Galois representations and arithmetic algebraic geometry*, Advanced Studies in Pure Mathematics, vol. 12, North-Holland, 1987, p. 87-118.

[11] T. Uehara, "On a congruence relation between Jacobi sums and cyclotomic units", *J. Reine Angew. Math.* **382** (1987), p. 199-214.

Vishal Arul
MIT Department of Mathematics
77 Massachusetts Ave., Bldg. 2-239A
Cambridge, MA 02139, USA
E-mail: varul.math@gmail.com