TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 351, Number 12, Pages 4769–4790
S 0002-9947(99)02223-0
Article electronically published on July 1, 1999

ON THE COEFFICIENTS OF JACOBI SUMS IN PRIME CYCLOTOMIC FIELDS

F. THAINE

Abstract. Let $p \geq 5$ and $q = pf + 1$ be prime numbers, and let s be a primitive root mod q. For $1 \leq n \leq p-2$, denote by J_n the Jacobi sum $-\sum_{k=2}^{q-1} \zeta_p^{\mathrm{ind}_s(k)+n\,\mathrm{ind}_s(1-k)}$. We study the integers $d_{n,k}$ such that $J_n = \sum_{k=0}^{p-1} d_{n,k}\zeta_p^k$ and $\sum_{k=0}^{p-1} d_{n,k} = 1$. We give a list of properties that characterize these coefficients. Then we show some of their applications to the study of the arithmetic of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$, in particular to the study of Vandiver's conjecture. For $m \in \mathbb{Z} - q\mathbb{Z}$, let $\rho_n(m)$ be the number of distinct roots of $X^{n+1} - X^n + m$ in $\mathbb{Z}/q\mathbb{Z}$. We show that $d_{n,k} = f - \sum_{a=0}^{f-1} \rho_n(s^{k+pa})$. We give closed formulas for the numbers $d_{1,k}$ and $d_{2,k}$ in terms of quadratic and cubic power residue symbols mod q.

Introduction

Let p and q be prime numbers such that $p \geq 5$ and $q \equiv 1 \bmod p$. Call $f = (q-1)/p$. Let ζ_p be a primitive p-th root of 1 and s a primitive root modulo q. For $1 \leq n \leq p-2$ we define the Jacobi sums J_n by

$$J_n = -\sum_{k=2}^{q-1} \zeta_p^{\mathrm{ind}_s(k)+n\,\mathrm{ind}_s(1-k)},$$

where $\mathrm{ind}_s(k)$ is the least nonnegative integer such that $s^{\mathrm{ind}_s(k)} \equiv k \bmod q$. Write

$$J_n = \sum_{k=0}^{p-1} d_{n,k}\zeta_p^k, \quad \text{with} \quad d_{n,k} \in \mathbb{Z} \quad \text{such that} \quad \sum_{k=0}^{p-1} d_{n,k} = 1.$$

This determines uniquely the integers $d_{n,k}$, $1 \leq n \leq p-2$, $0 \leq k \leq p-1$. If n and k are as above, and $i, j \in \mathbb{Z}$, define $d_{n+ip,k+jp} = d_{n,k}$. In this article we study the coefficients $d_{n,k}$, and some of their applications to the study of the arithmetic of $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$.

In Section 1 we show some basic properties of the Jacobi sums J_n and their coefficients, and their well-known relation with cyclotomic numbers of order p. Then we show a list of simple properties (Proposition 1) that turn out to characterize the J_n, or equivalently, the coefficients $d_{n,k}$ (Proposition 2). The proof of this fact depends on a characterization of the cyclotomic numbers given in [9]. It is interesting to see how properties of Jacobi sums are related with properties of

Received by the editors May 8, 1997 and, in revised form, August 29, 1997.
1991 *Mathematics Subject Classification.* Primary 11R18; Secondary 11T22.
This work was supported in part by grants from NSERC and FCAR.

©1999 American Mathematical Society

cyclotomic numbers, though the proof of one of these relations involves a long calculation.

Let Q be a prime ideal of $\mathbb{Z}[\zeta_p]$ above q. Choose the primitive root s modulo q such that $s^f \equiv \zeta_p \bmod Q$. We write $d_{n,l} = d_{n,l}(Q)$ when it is convenient to emphasize the dependency of the $d_{n,k}$ on Q. If $p \nmid a$, we denote by $\overline{a}$ the smallest positive integer such that $a\overline{a} \equiv 1 \bmod p$. For $1 \le n \le p-2$ and $1 \le l \le p-1$, let $\lambda_{n,l} = \lambda_{n,l}(Q)$ be the indices of the cyclotomic units

$$\varepsilon_{n,l} = \frac{(1-\zeta_p^l)(1-\zeta_p^{\overline{n}l})^n}{\left(1-\zeta_p^{(\overline{n+1})l}\right)^{n+1}}$$

with respect to Q and s, i.e. the integers $0 \le \lambda_{n,l} \le q-2$ such that

$$s^{\lambda_{n,l}} \equiv \varepsilon_{n,l} \quad \bmod Q.$$

In Section 2 we show (formula (24)) that

$$\text{(i)} \qquad \lambda_{n,l} \equiv \sum_{k=1}^{p-1} k d_{n,k} d_{n,k+l} \quad \bmod p.$$

This is just a reformulation of some of Kummer's complementary reciprocity laws stated in [3].

Let A be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$, Δ the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, $\mathbb{Z}_p$ the ring of p-adic integers, $\omega : \Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ the Teichmüller character, defined by $\omega(k) \equiv k \bmod p$, and e_k, $0 \le k \le p-2$, the idempotents $\frac{1}{p-1}\sum_{\sigma\in\Delta}\omega^k(\sigma)\sigma^{-1} \in \mathbb{Z}_p[\Delta]$. We use (i), and a result in [10], to give a criterion (Proposition 3) to recognize, in terms of the numbers $d_{n,k}$, whether or not the component $e_r(A)$ is trivial, for r even, $2 \le r \le p-3$. As is well-known, these $e_r(A)$ can be identified with the components of the p-part of the ideal class group of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Vandiver's conjecture is the statement that all such components are trivial. It is important to notice that, according to our criterion, for studying a given component $e_r(A)$ (r even, $2 \le r \le p-3$), we only need the numbers $d_{n,k}(Q)$, $0 \le k \le p-1$, for any fixed n such that $1 + n^{p-r} - (n+1)^{p-r} \not\equiv 0 \bmod p$. For example, if 2 is a primitive root modulo p, we only need the numbers $d_{1,k}(Q)$, $0 \le k \le p-1$, to study all even components of A.

In Section 3 we give formulas for the numbers $d_{n,k}$, $1 \le n \le p-2$, $0 \le k \le p-1$. If $p \nmid a$, let $\sigma_a \in \Delta$ be the automorphism such that $\sigma_a(\zeta_p) = \zeta_p^a$. If $k \in \mathbb{Z}$ and $m > 0$, we denote by $|k|_m$ the least **positive** integer such that $|k|_m \equiv k \bmod m$. It follows from a well-known result on Gauss sums ([4], Chapter 1, Theorem 2.1) that, for $1 \le n \le p-2$ and $1 \le k \le p-1$,

$$\sigma_k(\overline{J_n}) \equiv \binom{f|(n+1)k|_p}{fk} \quad \bmod Q,$$

where the bar denotes complex conjugation (formula (28)). Equivalently, we have that, for $1 \le n \le p-2$ and $0 \le k \le p-1$,

$$\text{(ii)} \qquad d_{n,k} \equiv \frac{1}{p}\sum_{l=0}^{p-1}\binom{f|(n+1)l|_p}{fl} s^{fkl} \quad \bmod q$$

(formula (29)). On the other hand, the fact that $|J_n| = \sqrt{q}$ implies that

$$\text{(iii)} \qquad |d_{n,k}| < \sqrt{q}.$$

Formulas (ii) and (iii) completely determine the coefficients $d_{n,k}$, since $\sqrt{q} < \frac{q-1}{2}$. This fact can be used to efficiently construct tables of the $d_{n,k}$ as the following.

Example. For $p = 7$, $q = 71$, and $s = 7$, the matrix $[d_{n,k}]_{\substack{1\le n\le p-2\\ 0\le k\le p-1}}$ is

$$\begin{bmatrix} -2 & 4 & -1 & -2 & -4 & 2 & 4 \\ 7 & 0 & 0 & -2 & 0 & -2 & -2 \\ -2 & 2 & -2 & 4 & 4 & -4 & -1 \\ 7 & 0 & 0 & -2 & 0 & -2 & -2 \\ -2 & 4 & -1 & -2 & -4 & 2 & 4 \end{bmatrix}.$$

Congruence (ii) can be written as

$$\text{(iv)} \qquad d_{n,k} \equiv \frac{1}{p} \sum_{l=0}^{p-1} \binom{|f(n+1)l|_{q-1}}{fl} s^{fkl} \mod q$$

(formula (31)). We will get our formulas for the numbers $d_{n,k}$ from (iii) and (iv).

For $0 \le n \le q-2$, define the functions $\rho_n : \mathbb{Z} - q\mathbb{Z} \to \mathbb{Z}$ by

$$\rho_n(m) = \text{number of distinct roots of } X^{n+1} - X^n + m \text{ in } \mathbb{Z}/q\mathbb{Z}.$$

By using an interesting property (Lemma 1) of the binomial coefficients $\binom{an}{ak}$ modulo q, where a is a divisor of $q-1$, we prove that

$$\sum_{l=0}^{q-2} \binom{|(n+1)l|_{q-1}}{l} m^l \equiv \rho_n(m) - 1 \mod q$$

(Proposition 4).

We give explicit formulas for the numbers $\rho_n(m)$, $m \in \mathbb{Z} - q\mathbb{Z}$, when $n = 1$ and $n = 2$ (Proposition 5). It follows from the formula for solving the quadratic congruence modulo q that

$$\rho_1(m) = 1 + \left(\frac{1-4m}{q}\right),$$

where $(\frac{\ }{q})$ is the Legendre symbol.

Define

$$e(q) = \begin{cases} 1 & \text{if } q \equiv 1 \mod 3, \\ -1 & \text{if } q \equiv -1 \mod 3. \end{cases}$$

We show that

$$\begin{aligned} \rho_2(m) \equiv 1 + \frac{1}{2} &\left(\left(\frac{1-(27/4)m)}{q} \right) + e(q) \left(\frac{-(27/4)m)}{q} \right) \right) \\ &\times \left(\left(\sqrt{1-(27/4)m} + \sqrt{-(27/4)m} \right)^{\frac{q-e(q)}{3}} \right. \\ &\left. + \left(\sqrt{1-(27/4)m} - \sqrt{-(27/4)m} \right)^{\frac{q-e(q)}{3}} \right) \mod q. \end{aligned}$$

This congruence has an interpretation, in terms of quadratic and cubic power residue symbols modulo q, that, together with the fact that $0 \le \rho_2(m) \le 3$, gives a closed formula for $\rho_2(m)$.

From the results mentioned above, we obtain formulas for the coefficients $d_{n,k}$ (Theorem 1):

For $1 \le n \le p-2$ and $0 \le k \le p-1$,

$$\text{(v)} \qquad \begin{aligned} d_{n,k} &= f - \sum_{a=0}^{f-1} \rho_n(s^{k+pa}) \\ &= f - \#\{u : 2 \le u \le q-1 \text{ and } (u^{n+1}-u^n)^f - s^{fk} \equiv 0 \mod q\}. \end{aligned}$$

For $0 \le k \le p-1$,

$$d_{1,k} = -\sum_{a=0}^{f-1} \left(\frac{1-4s^{k+pa}}{q} \right).$$

That is, $d_{1,k}$ = number of quadratic nonresidues mod q − number of quadratic residues mod q, in the set $\{1-4s^{k+pa} : 0 \le a \le f-1\}$ (do not count 0 as a quadratic residue mod q).

An explicit formula for $d_{2,k}$, $0 \le k \le p-1$, is given, which is similar to the one above, but a bit more complicated.

We want to point out that equalities (v) can also be obtained directly from the definitions of J_n and $d_{n,k}$. In any case, Proposition 4 is valuable in our study. In fact, we found the formulas for $\rho_n(m)$ and $d_{n,k}$, $n = 1, 2$, by observing first that $\sum_{l=0}^{q-2} \binom{|2l|_{q-1}}{l} m^l \equiv \sum_{l=0}^{q-2} \binom{2l}{l} m^l \equiv (1-4m)^{\frac{q-1}{2}} \equiv \left(\frac{1-4m}{q}\right) \mod q$, which gives the case $n = 1$, and then applying the theory of hypergeometric functions to the polynomials $\sum_{l=0}^{q-2} \binom{|3l|_{q-1}}{l} X^l$ to try and find a similar result for $n = 2$. We believe that other formulas for $\rho_n(m)$ and $d_{n,k}$, $n \ge 3$, can be obtained by using generalized hypergeometric functions (see, for example, [1] Chapter 15, and [6]).

Most of the results of this article can be generalized to propositions on Jacobi sums in arbitrary cyclotomic fields. By concentrating here on Jacobi sums in $\mathbb{Q}(\zeta_p)$ we expect to show some properties of these sums in their simplest, but perhaps not least interesting, forms.

1. Jacobi sums in $\mathbb{Q}(\zeta_p)$

Let $p \ge 5$ be a prime number, ζ_p a primitive p-th root of 1, $q \equiv 1 \bmod p$ a prime number, $f = (q-1)/p$, ζ_q a primitive q-th root of 1, and s a primitive root modulo q. Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, and if $p \nmid a$, let $\sigma_a \in \Delta$ be the automorphism such that $\sigma_a(\zeta_p) = \zeta_p^a$. If $k \in \mathbb{Z} - q\mathbb{Z}$, we call $\mathrm{ind}_s(k)$ the least nonnegative integer such that $s^{\mathrm{ind}_s(k)} \equiv k \bmod q$.

For $1 \le n \le p-2$, we define the Jacobi sums

$$J_n = -\sum_{k=2}^{q-1} \zeta_p^{\mathrm{ind}_s(k) + n\,\mathrm{ind}_s(1-k)}. \tag{1}$$

For n as above and $j \in \mathbb{Z}$ we define $J_{n+jp} = J_n$.

Call $G(X) = \sum_{k=0}^{q-2} X^k \zeta_q^{s^k}$, where X is an indeterminate. If $p \nmid a$, $G(\zeta_p^a) = \sum_{k=0}^{q-2} \zeta_p^{ka} \zeta_q^{s^k}$ is a Gauss sum, and we have

$$G(\zeta_p^a)\overline{G(\zeta_p^a)} = q, \tag{2}$$

where the bar denotes complex conjugation (see, for example, [11], Lemma 6.1). We have also, for $1 \le n \le p-2$,

$$J_n = -\frac{G(\zeta_p) G(\zeta_p^n)}{G(\zeta_p^{n+1})} \tag{3}$$

(see, for example, [11], Lemma 6.2).

For $1 \leq n \leq p-2$, write

$$J_n = \sum_{k=0}^{p-1} d_{n,k}\zeta_p^k \ , \quad \text{with} \quad d_{n,k} \in \mathbb{Z} \quad \text{such that} \quad \sum_{k=0}^{p-1} d_{n,k} = 1. \tag{4}$$

This determines uniquely the integers $d_{n,k}$, $1 \leq n \leq p-2$, $0 \leq k \leq p-1$. If n and k are as above, and $i, j \in \mathbb{Z}$, we define $d_{n+ip,k+jp} = d_{n,k}$.

Call $J_n(X) = \sum_{k=0}^{p-1} d_{n,k}X^k$ $(1 \leq n \leq p-2)$. So $J_n = J_n(\zeta_p)$ and $J_n(1) = 1$. From (4) we get

$$d_{n,k} = \frac{1}{p}\sum_{i=0}^{p-1} \zeta_p^{-ki} J_n(\zeta_p^i). \tag{5}$$

We will show later how to calculate the coefficients $d_{n,k}$, but first we want to show some properties that characterize these numbers, and their relation with the cyclotomic numbers of order p. Recall that, for $0 \leq i, j \leq p-1$, the cyclotomic number (i, j) is, by definition, the number of ordered pairs of integers $\langle k, l\rangle$, $0 \leq k, l \leq f-1$, such that $1 + s^{pk+i} \equiv s^{pl+j} \bmod q$. For $i,\ j$ as above and $a, b \in \mathbb{Z}$ we define $(i + ap, j + bp) = (i, j)$. (See, for example, [2] and [7].)

In what follows, if $a \in \mathbb{Z} - p\mathbb{Z}$, $\overline{a}$ will denote the least positive integer such that $a\overline{a} \equiv 1 \bmod p$; also, we use the following version of Kronecker's delta: for $k, l \in \mathbb{Z}$,

$$\delta_{k,l} = \begin{cases} 1 & \text{if } k \equiv l \bmod p, \\ 0 & \text{if } k \not\equiv l \bmod p. \end{cases}$$

We can express the cyclotomic numbers of order p in terms of Jacobi sums in $\mathbb{Q}(\zeta_p)$ and its coefficients, and vice versa, as follows:

$$(i, j) = -\frac{1}{p^2}\Big(p\delta_{0,i} + p\delta_{0,j} + p\delta_{i,j} - q - 1 + T_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}\big(\sum_{n=1}^{p-2} \zeta_p^{-i-jn} J_n\big)\Big), \tag{6}$$

where $T_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}$ is the trace from $\mathbb{Q}(\zeta_p)$ to $\mathbb{Q}$,

$$(i, j) = -\frac{1}{p}\big(\delta_{0,i} + \delta_{0,j} + \delta_{i,j} - f - 1 + \sum_{n=1}^{p-2} d_{n,i+jn}\big) \tag{7}$$

(see also [3], page 98), and

$$d_{n,k} = f - \sum_{i=0}^{p-1}(k - ni, i). \tag{8}$$

To prove (6) we can start from [2], formula (26), that in our particular case, and after using [2], formula (14), can be written as

$$J_n = -\sum_{k=0}^{p-1}\sum_{h=0}^{p-1} \zeta_p^{nk+h}(h, k). \tag{9}$$

So

$$\sum_{n=1}^{p-2}\zeta_p^{-i-jn}J_n=\sum_{k=0}^{p-1}\sum_{h=0}^{p-1}\zeta_p^{-(k-j)+(h-i)}(h,k)$$
$$-\sum_{k=0}^{p-1}\sum_{h=0}^{p-1}\sum_{n=1}^{p-1}\zeta_p^{n(k-j)+h-i}(h,k)$$
$$=\sum_{k=0}^{p-1}\sum_{h=0}^{p-1}\zeta_p^{-(k-j)+(h-i)}(h,k)-p\sum_{h=0}^{p-1}\zeta_p^{h-i}(h,j)+\sum_{k=0}^{p-1}\sum_{h=0}^{p-1}\zeta_p^{h-i}(h,k).$$

Therefore, using [2], formula (14), and formula (17) (with $e=p$ and $n_k=\delta_{0,k}$),

$$T_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{n=1}^{p-2}\zeta_p^{-i-jn}J_n)=p\sum_{k=0}^{p-1}\sum_{h=0}^{p-1}(h,k)\delta_{k+i-j,h}-\sum_{k=0}^{p-1}\sum_{h=0}^{p-1}(h,k)$$
$$-p\sum_{h=0}^{p-1}(h,j)(p\delta_{h,i}-1)+\sum_{k=0}^{p-1}\sum_{h=0}^{p-1}(h,k)(p\delta_{h,i}-1)$$
$$=p\sum_{k=0}^{p-1}(k,i-j)-\sum_{k=0}^{p-1}\sum_{h=0}^{p-1}(h,k)-p^2(i,j)+p\sum_{h=0}^{p-1}(h,j)+p\sum_{k=0}^{p-1}(i,k)-\sum_{k=0}^{p-1}\sum_{h=0}^{p-1}(h,k)$$
$$=p(f-\delta_{i,j})-p^2(i,j)+p(f-\delta_{0,j})+p(f-\delta_{0,i})$$
$$-2\sum_{k=0}^{p-1}(f-\delta_{0,k})=-p^2(i,j)-p\delta_{0,i}-p\delta_{0,j}-p\delta_{i,j}+q+1.$$

That is equivalent to (6).

Formula (7) follows easily from (4) and (6), and formula (8) from (5), (9), and the fact that $\sum_{h=0}^{p-1}(h,l)=f-\delta_{0,l}$ ([2], formula (17)). Furthermore we have:

Proposition 1. *The Jacobi sums J_n and its coefficients $d_{n,k}$ have the following properties:*

For $1\le n\le p-2$ and $0\le k\le p-1$,

a) $\sigma_n(J_{\overline{n}})=J_n$.
That is, $d_{n,k}=d_{\overline{n},\overline{n}k}$.

b) $J_n=J_{p-1-n}$.
That is, $d_{n,k}=d_{p-1-n,k}$.

c) $J_n\overline{J_n}=q$.
That is, $\sum_{j=0}^{p-1}d_{n,j}d_{n,j+k}=\delta_{0,k}q-f$.

d) *For $1\le n\le p-2$ and $1\le m\le p-2$ such that $n+m\ne p-1$: $\sigma_t(J_n\overline{J_m})=J_{nt}\overline{J_{mt}}$, where $t=-(\overline{n+m+1})$.*
That is, $\sum_{j=0}^{p-1}d_{n,j}d_{m,j+k}=\sum_{j=0}^{p-1}d_{nt,j}d_{mt,j+kt}$.

e) *The numbers $c_{i,j}=-\frac{1}{p^2}(qp\delta_{0,i}+p\delta_{0,j}+p\delta_{i,j}-q-1+T_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{n=1}^{p-2}\zeta_p^{-i-jn}J_n))$ $=-\frac{1}{p}(q\delta_{0,i}+\delta_{0,j}+\delta_{i,j}-f-1+\sum_{n=1}^{p-2}d_{n,i+jn})$ are integers. (In fact, by (6), the numbers $c_{i,j}+f\delta_{0,i}$ are the cyclotomic numbers (i,j) defined above.)*

f) *The characteristic polynomial of the matrix $[c_{i,j}]_{0\le i,j\le p-1}$ is irreducible over $\mathbb{Q}$. (In fact, that polynomial is the irreducible polynomial of the Gaussian periods of degree p corresponding to q.)*

Proof. a) Follows from (1).

b) Follows from (3) and from the fact that $G(\zeta_p^a)G(\zeta_p^{-a}) = q$ if $p \nmid a$ (see [11], Lemma 6.1 (b)).
c) Follows from (2) and (3).
d) We have that

$$\begin{aligned}\sigma_t^{-1}\big(J_{nt}\overline{J_{mt}}\big) &= \sigma_{\bar t}\bigg(\frac{G(\zeta_p)G(\zeta_p^{nt})}{G(\zeta_p^{1+nt})}\frac{G(\zeta_p^{-1})G(\zeta_p^{-mt})}{G(\zeta_p^{-1-mt})}\bigg) = q\frac{G(\zeta_p^{n})G(\zeta_p^{-m})}{G(\zeta_p^{\bar t+n})G(\zeta_p^{-\bar t-m})}\\ &= q\frac{G(\zeta_p^{n})G(\zeta_p^{-m})}{G(\zeta_p^{-m-1})G(\zeta_p^{n+1})}\\ &= \frac{G(\zeta_p)G(\zeta_p^{n})}{G(\zeta_p^{n+1})}\frac{G(\zeta_p^{-1})G(\zeta_p^{-m})}{G(\zeta_p^{-m-1})} = J_n\overline{J_m}\end{aligned}$$

(note that $G(\zeta_p^{-n}) = \overline{G(\zeta_p^n)}$ by [11], Lemma 6.1 (a)).
e) By (6) we have that $c_{i,j} = (i,j) - f\delta_{0,i} \in \mathbb{Z}$.
f) By (6), and [9], formula (4), the $c_{i,j}$ are the coefficients in the multiplication table of the Gaussian periods of degree p corresponding to q, defined by $\eta_i = \sum_{j=0}^{p-1}\zeta_q^{s^{i+pj}}$; that is, $\eta_0\eta_i = \sum_{j=0}^{p-1}c_{i,j}\eta_j$ (see [9], formula (1)). Now the result follows, for example, from [9], Theorem 1 (property (iv)), or [2], formula (9).

□

Properties (a)-(f) of Proposition 1 actually characterize the Jacobi sums J_n or, equivalently, the coefficients $d_{n,k}$, as is shown below.

Proposition 2. *Let J_n, $1 \le n \le p-2$, be elements of $\mathbb{Z}[\zeta_p]$ satisfying conditions (a)-(f) of Proposition 1. Then, for some primitive root s modulo q, the J_n are the Jacobi sums defined in (1).*

Observations. For primes q such that $p^{\frac{q-1}{p}} \not\equiv 1 \mod q$ (as the primes in $\mathcal{P}_m$, in Proposition 3 below), the irreducible polynomials of the Gaussian periods of degree p corresponding to q are irreducible modulo p. So, for those primes, condition (f) can be replaced by the condition: (f′) The characteristic polynomial of the matrix $[c_{i,j}]_{0\le i,j\le p-1}$ is irreducible modulo p. Notice also that (e) is just a condition modulo p on the numbers $d_{n,k}$.

Proof. Let J_n, $1 \le n \le p-2$, be elements of $\mathbb{Z}[\zeta_p]$ satisfying conditions (a)-(f) of Proposition 1. Write $J_n = \sum_{k=0}^{p-1} d_{n,k}\zeta_p^k$, with $d_{n,k} \in \mathbb{Z}$ such that $\sum_{k=0}^{p-1} d_{n,k} = 1$. The numbers $c_{i,j}$, $i,j \in \mathbb{Z}$, defined in Proposition 1 (e), are, by hypothesis, rational integers, and clearly $c_{i+p,j} = c_{i,j+p} = c_{i,j}$ for all $i,j \in \mathbb{Z}$. By (6), (9), and [9], formula (4), it is enough to prove that the $c_{i,j}$ are the coefficients in the multiplication table of the Gaussian periods of degree p (see [9], formula (1), or the proof of Proposition 1 (f)). In fact, if the $c_{i,j}$ are such coefficients, then $c_{i,j} + f\delta_{0,i}$ are the cyclotomic numbers (i,j), and, by (6) and (9), the J_n are the corresponding Jacobi sums. Now, Theorem 1 in [9] gives us a list of properties that characterize these coefficients, namely: For all integers i, j and l,
i) $\sum_{k=0}^{p-1} c_{i,k} = f - q\delta_{0,i}$,
ii) $\sum_{k=0}^{p-1} c_{k,j} = -\delta_{0,j}$,
iii) $\sum_{k=0}^{p-1} c_{i,k+i}c_{j-k,l-k} = \sum_{k=0}^{p-1} c_{j,k}c_{k+i,l+i}$,
iv) The characteristic polynomial of the matrix $[c_{i,j}]_{0\le i,j\le p-1}$ is irreducible over $\mathbb{Q}$.

Since condition (iv) is identical to condition (f) of Proposition 1, and since conditions (i) and (ii) follow immediately from the definition of the $c_{i,j}$ (condition (e)), the proposition will be proved if we show that the $c_{i,j}$ satisfy condition (iii). We affirm that

$$c_{i,j} + f\delta_{0,i} = c_{j,i} + f\delta_{0,j} \tag{10}$$

and

$$c_{i,j} = c_{-i,j-i}. \tag{11}$$

In fact, by property (a), we can write

$$\begin{aligned} c_{i,j} + f\delta_{0,i} &= -\frac{1}{p^2}(p\delta_{0,i} + p\delta_{0,j} + p\delta_{i,j} - q - 1 + \sum_{n=1}^{p-2} T_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{-i-jn}\sigma_n(J_{\overline{n}}))) \\ &= -\frac{1}{p^2}(p\delta_{0,i} + p\delta_{0,j} + p\delta_{i,j} - q - 1 + \sum_{n=1}^{p-2} T_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p^{-i\overline{n}-j}J_{\overline{n}})) \\ &= -\frac{1}{p^2}(p\delta_{0,i} + p\delta_{0,j} + p\delta_{i,j} - q - 1 + T_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{n=1}^{p-2} \zeta_p^{-in-j}J_n)) \\ &= c_{j,i} + f\delta_{0,j}. \end{aligned}$$

This proves (10). By property (b), we have

$$\begin{aligned} c_{i,j} + f\delta_{0,i} &= -\frac{1}{p^2}(p\delta_{0,i} + p\delta_{0,j} + p\delta_{i,j} - q - 1 + T_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{n=1}^{p-2} \zeta_p^{-i-jn}J_{p-1-n})) \\ &= -\frac{1}{p^2}(p\delta_{i-j,-j} + p\delta_{0,-j} + p\delta_{0,i-j} - q - 1 + T_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\sum_{n=1}^{p-2} \zeta_p^{-(i-j)+jn}J_n)) \\ &= c_{i-j,-j} + f\delta_{i,j}. \end{aligned}$$

Therefore, by (10), we have

$$\begin{aligned} c_{i,j} &= c_{j,i} + f\delta_{0,j} - f\delta_{0,i} = c_{j-i,-i} + f\delta_{i,j} - f\delta_{0,j} + f\delta_{0,j} - f\delta_{0,i} \\ &= c_{-i,j-i} + f\delta_{0,i} - f\delta_{i,j} + f\delta_{i,j} - f\delta_{0,i} = c_{-i,j-i}. \end{aligned}$$

This proves (11). Using (11) we can replace condition (iii) by the more symmetric condition iii′) $\sum_{k=0}^{p-1} c_{i,k}c_{k-j,l-j} = \sum_{k=0}^{p-1} c_{j,k}c_{k-i,l-i}$. Now, by (e),

$$\begin{aligned} p^2\sum_{k=0}^{p-1} c_{i,k}c_{k-j,l-j} = &\sum_{k=0}^{p-1}\Big(\big(q\delta_{0,i} + \delta_{0,k} + \delta_{i,k} - f - 1 + \sum_{m=1}^{p-2} d_{m,i+km}\big) \\ &\times \big(q\delta_{k,j} + \delta_{l,j} + \delta_{k,l} - f - 1 + \sum_{n=1}^{p-2} d_{n,(k-j)+(l-j)n}\big)\Big). \end{aligned} \tag{12}$$

To prove (iii′), and so end the proof of the proposition, it is enough to show that the expression at the right-hand side of (12) preserves its value if we interchange i and j. This requires a long calculation. To simplify things let us introduce some notation. We will say that two functions $f(i,j,l)$ and $g(i,j,l)$ are equivalent, and write $f \simeq g$, if $h = f - g$ is such that $h(i,j,l) = h(j,i,l)$. Also, call $[i,j] = c_{i,j} + f\delta_{0,i}$. By (10) and (11) we have that $[i,j] = [j,i]$ and $[i,j] = [-i,j-i]$.

By (12), and the fact that $\sum_{k=0}^{p-1} d_{n,k} = 1$, we have

$$\begin{aligned}
p^2 \sum_{k=0}^{p-1} c_{i,k}c_{k-j,l-j} &= q\delta_{0,j} + \delta_{0,l} + (1-q)\delta_{l,j} + q\delta_{i,j} + \delta_{i,l} + pq\delta_{l,j}\delta_{0,i} - (f+1)p \\
&+ q\sum_{n=1}^{p-2} d_{n,i+jn} + \sum_{n=1}^{p-2} d_{n,i+ln} + \sum_{n=1}^{p-2} d_{n,-j+(l-j)n} + \sum_{n=1}^{p-2} d_{n,(i-j)+(l-j)n} \\
&\quad + \sum_{m=1}^{p-2}\sum_{n=1}^{p-2}\sum_{k=0}^{p-1} d_{m,i+km}d_{n,(k-j)+(l-j)n} \\
&= q\delta_{0,j} + \delta_{0,l} + (1-q)\delta_{l,j} + q\delta_{i,j} + \delta_{i,l} + pq\delta_{l,j}\delta_{0,i} \\
&\quad - (f+1)p + q(-p[i,j] - \delta_{0,i} - \delta_{0,j} - \delta_{i,j} + (f+1)) \\
&\quad + (-p[i,l] - \delta_{0,i} - \delta_{0,l} - \delta_{i,l} + (f+1)) \\
&\quad + (-p[-j,l-j] - \delta_{0,j} - \delta_{l,j} - \delta_{0,l} + (f+1)) \\
&\quad + (-p[i-j,l-j] - \delta_{i,j} - \delta_{l,j} - \delta_{i,l} + (f+1)) \\
&\quad + \sum_{m=1}^{p-2}\sum_{n=1}^{p-2}\sum_{k=0}^{p-1} d_{m,i+km}d_{n,(k-j)+(l-j)n} \\
&= -(q+1)\delta_{0,i} - (q+1)\delta_{l,j} - \delta_{0,j} - \delta_{i,j} - \delta_{i,l} - \delta_{0,l} + pq\delta_{l,j}\delta_{0,i} \\
&\quad + (f+1)(q-p+3) - pq[i,j] - p[i,l] - p[j,l] \\
&\quad - p[i-l,j-l] + \sum_{m=1}^{p-2}\sum_{n=1}^{p-2}\sum_{k=0}^{p-1} d_{m,i+km}d_{n,(k-j)+(l-j)n} \\
&\simeq -q\delta_{0,i} - q\delta_{l,j} + pq\delta_{0,i}\delta_{l,j} + \sum_{m=1}^{p-2}\sum_{n=1}^{p-2}\sum_{k=0}^{p-1} d_{m,i+km}d_{n,(k-j)+(l-j)n}.
\end{aligned}$$

Using conditions (a) and (b), we see that the last expression is equal to $-q\delta_{0,i} - q\delta_{l,j} + pq\delta_{0,i}\delta_{l,j} + \sum_{m=1}^{p-2}\sum_{n=1}^{p-2}\sum_{k=0}^{p-1} d_{\overline{m},\overline{m}i+k}d_{p-1-n,-(1+n)j+nl+k} = -q\delta_{0,i} - q\delta_{l,j} + pq\delta_{0,i}\delta_{l,j} + \sum_{m=1}^{p-2}\sum_{n=1}^{p-2}\sum_{k=0}^{p-1} d_{m,mi+k}d_{n,nj-(1+n)l+k} = -q\delta_{0,i} - q\delta_{l,j} + pq\delta_{0,i}\delta_{l,j} + \sum_{m=1}^{p-2}\sum_{n=1}^{p-2}\sum_{k=0}^{p-1} d_{n,k}d_{m,mi-nj+(1+n)l+k}$. Therefore

$$\begin{aligned}
p^2 \sum_{k=0}^{p-1} c_{i,k}c_{k-j,l-j} &\simeq -q\delta_{0,i} - q\delta_{l,j} + pq\delta_{0,i}\delta_{l,j} \\
&+ \sum_{n=1}^{p-2}\sum_{k=0}^{p-1} d_{n,k}d_{n,ni+(1+n)j-nl+k} + \sum_{\substack{m,n=1 \\ m+n\neq p-1}}^{p-2}\ \sum_{k=0}^{p-1} d_{n,k}d_{m,mi-nj+(1+n)l+k}.
\end{aligned} \tag{13}$$

Now, by condition (c), we have

$$\begin{aligned}
&\sum_{n=1}^{p-2}\sum_{k=0}^{p-1} d_{n,k}d_{n,ni+(1+n)j-nl+k} \\
&\quad = \sum_{n=1}^{p-2}(q\delta_{0,ni+(1+n)j-nl} - f) = 1 + 2f - q\delta_{l,i} - q\delta_{0,j} - q\delta_{i+j,l} + pq\delta_{0,j}\delta_{l,i} \\
&\quad \simeq -q\delta_{0,j} - q\delta_{l,i} + pq\delta_{0,j}\delta_{l,i}.
\end{aligned}$$

Hence, by (13),

$$p^2\sum_{k=0}^{p-1}c_{i,k}c_{k-j,l-j} \simeq \sum_{\substack{m,n=1\\ m+n\neq p-1}}^{p-2}\sum_{k=0}^{p-1}d_{n,k}d_{m,mi-nj+(1+n)l+k}.$$

So, to finish the proof of the proposition, it is enough to show that

$$\sum_{\substack{m,n=1\\ m+n\neq p-1}}^{p-2}\sum_{k=0}^{p-1}d_{n,k}d_{m,mi-nj+(1+n)l+k} = \sum_{\substack{m,n=1\\ m+n\neq p-1}}^{p-2}\sum_{k=0}^{p-1}d_{n,k}d_{m,mj-ni+(1+n)l+k}.$$

Now, by condition (d), calling $t_{m,n} = -(\overline{m+n+1})$, we have

$$\begin{aligned}
&\sum_{\substack{m,n=1\\ m+n\neq p-1}}^{p-2}\sum_{k=0}^{p-1}d_{n,k}d_{m,mi-nj+(1+n)l+k}\\
&\quad= \sum_{\substack{m,n=1\\ m+n\neq p-1}}^{p-2}\sum_{k=0}^{p-1}d_{nt_{m,n},k}d_{mt_{m,n},t_{m,n}(mi-nj+(1+n)l)+k}\\
&\quad= \sum_{u=1}^{p-1}\sum_{\substack{n=1\\ n\not\equiv -u,-u-1}}^{p-2}\sum_{k=0}^{p-1}d_{\overline{u}n,k}d_{\overline{u}(-u-n-1),\overline{u}(-(u+n+1)i-nj+(1+n)l)+k}\\
&\quad= \sum_{u=1}^{p-1}\sum_{\substack{v=1\\ v\not\equiv -\overline{u},-\overline{u}-1}}^{p-2}\sum_{k=0}^{p-1}d_{v,k}d_{-1-v-\overline{u},-(1+v+\overline{u})i-vj+(\overline{u}+v)l+k}\\
&\quad= \sum_{v=1}^{p-2}\sum_{\substack{w=1\\ w\not\equiv -1-v}}^{p-2}\sum_{k=0}^{p-1}d_{v,k}d_{w,wi-vj-(1+w)l+k}\\
&\quad= \sum_{v=1}^{p-2}\sum_{\substack{w=1\\ w\not\equiv -1-v}}^{p-2}\sum_{k=0}^{p-1}d_{w,k}d_{v,-wi+vj+(1+w)l+k}\\
&\quad= \sum_{\substack{m,n=1\\ m+n\neq p-1}}^{p-2}\sum_{k=0}^{p-1}d_{n,k}d_{m,mj-ni+(1+n)l+k}
\end{aligned}$$

(the congruences on the summation indices are modulo p). This ends the proof of Proposition 2. □

2. Indices of cyclotomic units, Vandiver's conjecture and the coefficients of Jacobi sums in $\mathbb{Q}(\zeta_p)$

We preserve the notations of Section 1; $p \geq 5$ and $q = pf+1$ are prime numbers. Let Q be a prime ideal of $\mathbb{Z}[\zeta_p]$ above q. In this section, the primitive root s modulo q will be chosen so that $s^f \equiv \zeta_p \bmod Q$ (note that q splits completely in $\mathbb{Q}(\zeta_p)$). Recall that if $p \nmid a$, we denote by $\overline{a}$ the smallest positive integer such that $a\overline{a} \equiv 1 \bmod p$. Since the coefficients $d_{n,k}$ of the Jacobi sums defined in Section 1 depend on Q, we will write $d_{n,k} = d_{n,k}(Q)$ when it is convenient.

For $1 \leq n \leq p-2$ and $1 \leq l \leq p-1$, define the integers $\lambda_{n,l} = \lambda_{n,l}(Q)$, $0 \leq \lambda_{n,l} \leq q-2$, by

$$s^{\lambda_{n,l}} \equiv \frac{(1-\zeta_p^l)(1-\zeta_p^{\overline{n}l})^n}{\left(1-\zeta_p^{(\overline{n+1})l}\right)^{n+1}} \qquad \bmod Q. \tag{14}$$

We call $\lambda_{n,l}$ the index of the cyclotomic unit $\varepsilon_{n,l} = (1-\zeta_p^l)(1-\zeta_p^{\overline{n}l})^n/(1-\zeta_p^{(\overline{n+1})l})^{n+1}$ with respect to Q and s. It follows from formula (14) that $s^{\sum_{l=1}^{p-1}\lambda_{n,l}} \equiv pp^n/p^{n+1} = 1 \bmod q$. Therefore

$$\sum_{l=1}^{p-1} \lambda_{n,l} \equiv 0 \qquad \bmod q-1. \tag{15}$$

In this section we show that the indices $\lambda_{n,l}$ modulo p have simple expressions in terms of the coefficients $d_{n,k}$ (see formula (24)). This is just a restatement of a result of Kummer on complementary reciprocity laws ([3], pages 97 and 98). Then we use those expressions, and a result in [10], to give a criterion (Proposition 3) to recognize, in terms of the numbers $d_{n,k}$, whether or not a given even component of the p-part of the ideal class group of $\mathbb{Q}(\zeta_p)$ is trivial. Vandiver's conjecture is the statement that all those even components are trivial.

By our choice of s, we can write

$$s^{\lambda_{n,l}} \equiv \frac{(1-s^{fl})(1-s^{f\overline{n}l})^n}{\left(1-s^{f(\overline{n+1})l}\right)^{n+1}} \qquad \bmod q. \tag{16}$$

For $k \not\equiv 0 \bmod q-1$, let $\Phi(k)$ be the least positive integer such that $1-s^k \equiv s^{\Phi(k)} \bmod q$. By (16) we have

$$s^{\lambda_{n,l}} \equiv s^{\Phi(fl)+n\Phi(f\overline{n}l)-(n+1)\Phi(f(\overline{n+1})l)} \qquad \bmod q.$$

So, for $1 \leq n \leq p-2$ and $1 \leq l \leq p-1$,

$$\lambda_{n,l} \equiv \Phi(fl) + n\Phi(f\overline{n}l) - (n+1)\Phi(f(\overline{n+1})l) \qquad \bmod q-1. \tag{17}$$

For $1 \leq n \leq p-2$, define $\Psi_n(X) = G(X)G(X^n)/G(X^{n+1})$. By (3) we have that

$$\Psi_n(\zeta_p) = -J_n. \tag{18}$$

As a particular case of formula (1) of [8] we have

$$\zeta_p G'(\zeta_p)/G(\zeta_p) \equiv -\sum_{k=1}^{q-2} k\zeta_q^{s^k} + \sum_{l=1}^{f-1}\Phi(lp) + \sum_{i=1}^{p-1}\Phi(-if)\zeta_p^i \qquad \bmod \frac{q-1}{2}. \tag{19}$$

Therefore

$$\begin{aligned}
&\zeta_p\Psi_n'(\zeta_p)/\Psi_n(\zeta_p)\\
&\quad= \zeta_p G'(\zeta_p)/G(\zeta_p) + n\zeta_p^n G'(\zeta_p^n)/G(\zeta_p^n) - (n+1)\zeta_p^{n+1}G'(\zeta_p^{n+1})/G(\zeta_p^{n+1})\\
&\quad\equiv \sum_{l=1}^{p-1}\left(\Phi(-lf) + n\Phi(-l\overline{n}f) - (n+1)\Phi(-l(\overline{n+1})f)\right)\zeta_p^l \ \bmod (q-1)/2.
\end{aligned}$$

So, by (17), for $1 \leq n \leq p-2$,

$$\sum_{l=1}^{p-1} \lambda_{n,l}\zeta_p^{-l} \equiv \zeta_p \Psi_n'(\zeta_p)/\Psi_n(\zeta_p) \equiv \zeta_p \Psi_n'(\zeta_p)\overline{\Psi_n(\zeta_p)} \qquad \bmod \frac{q-1}{2} \tag{20}$$

(see also [8], page 133).

Since, by (4) and (18), the polynomials $J_n(X) = \sum_{k=0}^{p-1} d_{n,k}X^k$, $1 \le n \le p-2$, are such that $J_n(\zeta_p) = J_n = -\Psi_n(\zeta_p)$ and $J_n(1) = 1 = -\Psi_n(1)$, we have that

$$J_n(X) \equiv -\Psi_n(X) = -G(X)G(X^n)/G(X^{n+1}) \qquad \bmod (X^p - 1). \tag{21}$$

This implies that $XJ_n'(X)/J_n(X) \equiv XG'(X)/G(X) + nX^nG'(X^n)/G(X^n) - (n+1)X^{n+1}G'(X^{n+1})/G(X^{n+1}) \bmod (p, X^p - 1)$. On the other hand, by (4) and Proposition 1 (c), we have $J_n(X)J_n(X^{p-1}) \equiv q - f(1+X+\cdots+X^{p-1}) \bmod (X^p-1)$. So

$$\begin{aligned}
\sum_{l=0}^{p-1}\Big(\sum_{k=1}^{p-1} kd_{n,k}d_{n,k+l}\Big)X^{p-l} &\equiv XJ_n'(X)J_n(X^{p-1}) \equiv (q - f(1 + X + \cdots + X^{p-1})) \\
&\quad \times (XG'(X)/G(X) + nX^nG'(X^n)/G(X^n) - (n+1)X^{n+1}G'(X^{n+1})/G(X^{n+1})) \\
&\equiv XG'(X)/G(X) + nX^nG'(X^n)/G(X^n) \\
&\quad - (n+1)X^{n+1}G'(X^{n+1})/G(X^{n+1}) \bmod (p, X^p - 1),
\end{aligned}$$

since $G'(1)/G(1) + nG'(1)/G(1) - (n+1)G'(1)/G(1) = 0$. If we write

$$XG'(X)/G(X) \equiv \sum_{i=0}^{p-1} g_iX^i \bmod (X^p - 1),$$

with $g_i \in \mathbb{Z}$, then, by the congruence above, we have

$$\begin{aligned}
&\sum_{l=0}^{p-1}\Big(\sum_{k=1}^{p-1} kd_{n,k}d_{n,k+l}\Big)X^{p-l} \\
&\qquad \equiv \sum_{i=0}^{p-1} g_iX^i + n\sum_{i=0}^{p-1} g_iX^{|ni|} - (n+1)\sum_{i=0}^{p-1} g_iX^{|(n+1)i|} \bmod p,
\end{aligned}$$

where we denote by $|m|$ the least nonnegative integer such that $|m| \equiv m \bmod p$. This implies that

$$\sum_{k=1}^{p-1} kd_{n,k}^2 \equiv 0 \qquad \bmod p. \tag{22}$$

Taking logarithmic derivatives in (21), and using (20), we obtain the following version of a result of Kummer (see [3], pages 97 and 98): For $1 \le n \le p-2$,

$$\sum_{l=1}^{p-1} \lambda_{n,l}\zeta_p^{-l} \equiv \zeta_p J_n'(\zeta_p)J_n(\zeta_p^{-1}) \qquad \bmod p. \tag{23}$$

Equivalently, we have that, for $1 \le n \le p-2$ and $1 \le l \le p-1$,

$$\lambda_{n,l} \equiv \sum_{k=1}^{p-1} kd_{n,k}d_{n,k+l} \qquad \bmod p. \tag{24}$$

To prove that (23) and (24) are, in fact, equivalent, compare coefficients in (23), using (22). Note also that (4), (15), (22) and (24) imply that

$$\sum_{k=1}^{p-1} k d_{n,k} \equiv 0 \mod p.$$

Now, consider the numbers $\beta_r = \prod_{k=1}^{p-1}(1-\zeta_p^k)^{k^{p-1-r}}$, r even, $2 \le r \le p-3$. Let $i_r(Q)$ be the least nonnegative integer such that $s^{i_r(Q)} \equiv \beta_r \bmod Q$. Using (14) and (24) we easily get that, for $1 \le n \le p-2$, and r even, $2 \le r \le p-3$,

$$\begin{aligned}\big(1+n^{p-r}-(n+1)^{p-r}\big) i_r(Q) &\equiv \sum_{l=1}^{p-1} l^{p-1-r}\lambda_{n,l} \\ &\equiv \sum_{k=1}^{p-1}\sum_{l=1}^{p-1} k l^{p-1-r} d_{n,k} d_{n,k+l} \mod p\end{aligned} \tag{25}$$

(see also [3], pages 103 and 125, and [8], Theorem 1).

Let A be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$, $\mathbb{Z}_p$ the ring of p-adic integers, $\omega : \Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ the Teichmüller character, defined by $\omega(k) \equiv k \bmod p$, and e_k, $0 \le k \le p-2$, the idempotents $\frac{1}{p-1}\sum_{\sigma\in\Delta}\omega^k(\sigma)\sigma^{-1} \in \mathbb{Z}_p[\Delta]$. From (25), and [10], Theorem 1, we obtain the following criterion to recognize whether or not the components $e_r(A)$ of A, with r even and $2 \le r \le p-3$, are trivial.

Proposition 3. *Let r be even, $2 \le r \le p-3$, and let n be such that $1 \le n \le p-2$ and $1+n^{p-r}-(n+1)^{p-r} \not\equiv 0 \mod p$. If for some prime ideal Q of $\mathbb{Z}[\zeta_p]$, above a rational prime $q \equiv 1 \mod p$,*

$$\sum_{k=1}^{p-1}\sum_{l=1}^{p-1} k l^{p-1-r} d_{n,k}(Q) d_{n,k+l}(Q) \not\equiv 0 \mod p,$$

then $e_r(A)$ is trivial. Conversely, let $m \ge 1$, and let $\mathcal{P}_m$ be the set of all prime ideals Q of $\mathbb{Z}[\zeta_p]$ that are above rational primes q such that $q \equiv 1 \bmod p^m$ and $p^{\frac{q-1}{p}} \equiv \zeta_p \bmod Q$. If

$$\sum_{k=1}^{p-1}\sum_{l=1}^{p-1} k l^{p-1-r} d_{n,k}(Q) d_{n,k+l}(Q) \equiv 0 \mod p, \quad \textit{for all } Q \in \mathcal{P}_m,$$

then $e_r(A)$ is nontrivial. (Recall that for prime ideals Q, above rational primes $q \equiv 1 \mod p$, in the definition of the numbers $d_{n,l} = d_{n,l}(Q)$, we choose the primitive root $s = s_Q$ modulo q so that $s_Q^{\frac{q-1}{p}} \equiv \zeta_p \mod Q$.)

Example. For $p = 37$ all components $e_r(A)$ with r even, $2 \le r \le 34$, and $r \ne 32$ are trivial since 37 does not divide the Bernoulli numbers B_r. We can prove that $e_{32}(A)$ is also trivial as follows: We have $2^{37-32} = 32 \not\equiv 2 \bmod 37$, and for $q = 149$ and $s = 2$ the numbers $d_{1,k}$, $0 \le k \le 36$, are $[-2,-2,0,-2,0,-4,2,-2,2,0,2,0,-4,0,2,-2,0,0,2,-2,-4,0,0,2,4,-2,-2,2,0,0,2,0,2,2,2,1,2]$. So

$$\sum_{k=1}^{36}\sum_{l=1}^{36} k l^4 d_{n,k} d_{n,k+l} \equiv 34 \not\equiv 0 \mod 37.$$

Therefore, by Proposition 3, $e_{32}(A)$ is trivial.

3. Formulas for the coefficients $d_{n,k}$

We preserve the notations of Section 1. Let Q be a prime ideal of $\mathbb{Z}[\zeta_p]$ above $q = pf + 1$, and let B be the prime ideal of $\mathbb{Z}[\zeta_p, \zeta_q]$ above Q. The primitive root s modulo q will be chosen so that $s^f \equiv \zeta_p \bmod Q$. If $k \in \mathbb{Z}$ and $m > 0$, we denote by $|k|_m$ the least **positive** integer such that $|k|_m \equiv k \bmod m$. As before, if $p \nmid k$, $\overline{k}$ denotes the least positive integer such that $k\overline{k} \equiv 1 \bmod p$. We denote by $[x]$ the integral part of a real number x, and by $\mathbb{Z}_{(q)}$ the localization of $\mathbb{Z}$ at q. By [4], Chapter 1, Theorem 2.1, we have, for $1 \leq l \leq p-1$,

$$\frac{G(\zeta_p^{-l})}{(\zeta_q - 1)^{fl}} \equiv \frac{-1}{(fl)!} \quad \bmod B. \tag{26}$$

On one hand, this, and (2), give the prime ideal factorizations of the Gauss sum $G(\zeta_p)$ and of the Jacobi sums J_n (see [4], Chapter 1, Theorem 2.2, and FAC 3, page 13). Namely, for $1 \leq n \leq p-2$, we have, in $\mathbb{Z}[\zeta_p]$,

$$(\overline{J_n}) = Q^{\sum_{l=1}^{p-1}\left(\left[\frac{(n+1)l}{p}\right]-\left[\frac{nl}{p}\right]\right)\sigma_l^{-1}}, \tag{27}$$

where the bar denotes complex conjugation. On the other hand, for $1 \leq n \leq p-2$ and $1 \leq k \leq p-1$, we get from (26) that

$$\begin{aligned}
\sigma_k(\overline{J_n}) &= -\frac{G(\zeta_p^{-k})G(\zeta_p^{-|nk|_p})}{G(\zeta_p^{-|(n+1)k|_p})} \\
&= -\frac{\big(G(\zeta_p^{-k})/(\zeta_q-1)^{fk}\big)\big(G(\zeta_p^{-|nk|_p})/(\zeta_q-1)^{f|nk|_p}\big)}{\big(G(\zeta_p^{-|(n+1)k|_p})/(\zeta_q-1)^{f|(n+1)k|_p}\big)}(\zeta_q-1)^{f(k+|nk|_p-|(n+1)k|_p)} \\
&\equiv \frac{(f|(n+1)k|_p)!}{(fk)!(f|nk|_p)!}(\zeta_q-1)^{f(k+|nk|_p-|(n+1)k|_p)} \bmod B.
\end{aligned}$$

Therefore, for $1 \leq n \leq p-2$ and $1 \leq k \leq p-1$,

$$\sigma_k(\overline{J_n}) \equiv \binom{f|(n+1)k|_p}{fk} \quad \bmod Q. \tag{28}$$

Note that $\binom{f|(n+1)k|_p}{fk} \equiv 0 \bmod q$, if $k + |nk|_p - |(n+1)k|_p \neq 0$; in fact, in that case we have that $|(n+1)k|_p = k + |nk|_p - p < k$.

From (5) and (28) we get, for $1 \leq n \leq p-2$ and $0 \leq k \leq p-1$, $d_{n,k} = \frac{1}{p}(1 + \sum_{l=1}^{p-1} \zeta_p^{kl}\sigma_l(\overline{J_n})) \equiv \frac{1}{p}\sum_{l=0}^{p-1}\zeta_p^{kl}\binom{f|(n+1)l|_p}{fl} \bmod Q$. Therefore,

$$d_{n,k} \equiv \frac{1}{p}\sum_{l=0}^{p-1}\binom{f|(n+1)l|_p}{fl}s^{fkl} \quad \bmod q. \tag{29}$$

On the other hand, from (5) and Proposition 1 (c), we get

$$|d_{n,k}| \leq \frac{1}{p}(1 + \sum_{l=1}^{p-1}|\sigma_l(J_n)|) = \frac{1}{p}(1 + (p-1)\sqrt{q}).$$

Therefore, for $1 \leq n \leq p-2$ and $0 \leq k \leq p-1$,

$$|d_{n,k}| < \sqrt{q}. \tag{30}$$

Formulas (29) and (30) completely determine the coefficients $d_{n,k}$, since $\sqrt{q} < \frac{q-1}{2}$. (Proceeding in a similar way, we can obtain, from (6) and (28), V.A. Lebesgue's formulas for the cyclotomic numbers (i,j) modulo q, given in [5], Section III.)

Now observe that, for $n, l \in \mathbb{Z}$, $f|(n+1)l|_p = |f(n+1)l|_{q-1}$. So, we can write (29) as

$$d_{n,k} \equiv \frac{1}{p} \sum_{l=0}^{p-1} \binom{|f(n+1)l|_{q-1}}{fl} s^{fkl} \mod q. \tag{31}$$

For $1 \le n \le p-2$, call

$$h_n(X) = \sum_{l=0}^{q-2} \binom{|(n+1)l|_{q-1}}{l} X^l. \tag{32}$$

If ζ_f is a primitive f-th root of 1, then

$$\sum_{a=0}^{f-1} h_n(X\zeta_f^a) = \sum_{l=0}^{q-2} \binom{|(n+1)l|_{q-1}}{l} X^l \sum_{a=0}^{f-1} \zeta_f^{al} = f \sum_{l=0}^{p-1} \binom{|(n+1)fl|_{q-1}}{fl} X^{fl}.$$

Hence $\frac{1}{q-1} \sum_{a=0}^{f-1} h_n(X\zeta_f^a) = \frac{1}{p} \sum_{l=0}^{p-1} \binom{|(n+1)fl|_{q-1}}{fl} X^{fl}$. Since s^p is a primitive f-th root of 1 modulo q, we have similarly that

$$-\sum_{a=0}^{f-1} h_n(s^{k+pa}) \equiv \frac{1}{p} \sum_{l=0}^{p-1} \binom{|(n+1)fl|_{q-1}}{fl} s^{fkl} \mod q.$$

Therefore, by (31), for $1 \le n \le p-2$ and $0 \le k \le p-1$,

$$d_{n,k} \equiv -\sum_{a=0}^{f-1} h_n(s^{k+pa}) \mod q. \tag{33}$$

It turns out that the numbers $h_n(m)$, modulo q, with $m \in \mathbb{Z} - p\mathbb{Z}$, have an interesting interpretation, as we show below. We will use the following fact about binomial coefficients modulo q.

Lemma 1. *Let q be an odd prime number, and let a and b be positive integers such that $q - 1 = ab$. Then, for all $0 \le k, n \le b$,*

$$\binom{an}{ak} \equiv (-1)^{ak} \binom{a(b-n+k)}{ak} \equiv (-1)^{a(n+k)} \binom{a(b-k)}{a(b-n)} \mod q.$$

Proof. We have

$$\begin{aligned}\binom{a(b-n+k)}{ak} &= \frac{(q-1-a(n-k))(q-2-a(n-k))\dots(q-ak-a(n-k))}{(ak)!} \\ &\equiv (-1)^{ak} \frac{(an)(an-1)\dots(a(n-k)+1)}{(ak)!} = (-1)^{ak} \binom{an}{ak} \mod q.\end{aligned}$$

Therefore

$$\begin{aligned}\binom{an}{ak} &\equiv (-1)^{ak} \binom{a(b-n+k)}{ak} = (-1)^{ak} \binom{a(b-n+k)}{a(b-n)} \\ &\equiv (-1)^{ak}(-1)^{a(b-n)} \binom{a(n-k+b-n)}{a(b-n)} = (-1)^{a(n+k)} \binom{a(b-k)}{a(b-n)} \mod q.\end{aligned}$$

$\square$

Example. For $q=71$, $a=10$ and $b=7$, the matrix $\left[\binom{an}{ak}\right]_{0\le n,k\le b}$ modulo q is

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 1 & 14 & 1 & 0 & 0 & 0 & 0 & 0\\ 1 & 16 & 16 & 1 & 0 & 0 & 0 & 0\\ 1 & 48 & 65 & 48 & 1 & 0 & 0 & 0\\ 1 & 16 & 65 & 65 & 16 & 1 & 0 & 0\\ 1 & 14 & 16 & 48 & 16 & 14 & 1 & 0\\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

It can be shown that the symmetries we observe here correspond to properties of cyclotomic numbers.

Proposition 4. *For $0\le n\le q-2$, define the functions $\rho_n:\mathbb{Z}-q\mathbb{Z}\to\mathbb{Z}$ by*

$$\rho_n(m)=\#\{u:2\le u\le q-1 \quad \textit{and} \quad u^{n+1}-u^n+m\equiv 0 \mod q\}.$$

Then $\sum_{l=0}^{q-2}\binom{|(n+1)l|_{q-1}}{l}m^l\equiv\rho_n(m)-1 \mod q$.

Proof. (Compare with [4], page 9.) For $0\le n\le q-2$ and $1\le l\le q-2$,

$$\begin{aligned}\sum_{u=2}^{q-1}(1-u)^{-l}u^{-nl} &\equiv \sum_{u=1}^{q-1}(-1)^l(1-u^{-1})^{q-1-l}u^{-(n+1)l}\\ &= \sum_{u=1}^{q-1}(-1)^l u^{-(n+1)l}\sum_{i=0}^{q-2}(-1)^i\binom{q-1-l}{i}u^{-i}\\ &\equiv \sum_{i=0}^{q-2}(-1)^{l+i}\binom{q-1-l}{i}\sum_{u=1}^{q-1}u^{-i-|(n+1)l|_{q-1}}\\ &\equiv -(-1)^{nl}\binom{q-1-l}{q-1-|(n+1)l|_{q-1}}\equiv-\binom{|(n+1)l|_{q-1}}{l} \mod q.\end{aligned}$$

The last congruence holds by Lemma 1. Therefore, for $m\in\mathbb{Z}-q\mathbb{Z}$,

$$\begin{aligned}\sum_{l=0}^{q-2}\binom{|(n+1)l|_{q-1}}{l}m^l &\equiv 1-2-\sum_{u=2}^{q-1}\sum_{l=0}^{q-2}\left((1-u)^{-1}u^{-n}m\right)^l\\ &\equiv -1-(q-1)\#\{u:2\le u\le q-1 \text{ and } m\equiv(1-u)u^n \mod q\}\\ &\equiv -1+\rho_n(m) \mod q. \quad\square\end{aligned}$$

We have explicit formulas for $\rho_1(m)$ and $\rho_2(m)$. We will use the following lemma to prove the latter.

Lemma 2. *Define*

$$e(q)=\begin{cases}1 & \textit{if } q\equiv 1 \mod 3,\\ -1 & \textit{if } q\equiv -1 \mod 3.\end{cases} \tag{34}$$

For $0\le l\le q-2$,

$$\binom{|3l|_{q-1}}{l}\equiv(-27)^l e(q)\left(\binom{\frac{2q+e(q)}{3}+l}{2l+1}+\binom{\frac{q+2e(q)}{3}+l}{2l+1}\right) \mod q.$$

Proof. Call $e = e(q)$. Suppose first that $\frac{q-1}{2} \le l \le q-2$. Then (see [1], page 822)

$$\begin{aligned}
&(-27)^l e\left(\binom{\frac{2q+e}{3}+l}{2l+1} + \binom{\frac{q+2e}{3}+l}{2l+1}\right) \equiv (-27)^l e\left(\binom{\frac{2q+e}{3}+l-q}{2l+1-q}+0\right)\\
&\equiv \frac{(-27)^l e}{(2l+1)(2l)\dots(q+1)}\\
&\qquad \times [((e/3)+l)((e/3)+l-1)\dots((e/3)-(q+1)/2)]\\
&\qquad \times [((e/3)-l)((e/3)-(l-1))\dots((e/3)-(q+1)/2)]\\
&= (-27)^l e\frac{((1/3)^2-l^2)((1/3)^2-(l-1)^2)\dots((1/3)^2-((q+1)/2)^2)}{(2l+1)(2l)\dots(q+1)}\\
&\equiv 3^l e(-1)^{\frac{q-1}{2}}\frac{((3l)^2-1)((3(l-1))^2-1)\dots((3(q+1)/2)^2-1)}{(2l+1)(2l)\dots(q+1)}\\
&= \frac{(-3)^{\frac{q-1}{2}} e}{[(2l+1)(2l)\dots(q+1)][l(l-1)\dots((q+1)/2)]}\\
&\qquad \times [((3l)^2-1)((3(l-1))^2-1)\cdots((3(q+1)/2)^2-1)]\\
&\qquad \times [(3l)(3(l-1))\cdots(3(q+1)/2)]\\
&\equiv \left(\frac{-3}{q}\right) e\frac{(3l+1)!\,q!((q-1)/2)!}{(2l+1)!\,l!\,((3q-1)/2)!} = \binom{3l+1}{l} \Big/ \binom{(3q-1)/2}{(q-1)/2}\\
&\equiv \binom{3l+1}{l} \Big/ \binom{(q-1)/2}{(q-1)/2} = \binom{3l+1}{l} \equiv \binom{|3l|_{q-1}}{l} \bmod q\\
&\text{(note that if } \left[\frac{2(q-1)}{3}\right] < l \le q-2, \text{ then } \binom{3l+1}{l} \equiv \binom{|3l|_{q-1}}{l} = 0 \bmod q).
\end{aligned}$$

Suppose now that $0 \le l \le \frac{q-3}{2}$. Then

$$\begin{aligned}
&(-27)^l e\left(\binom{\frac{2q+e}{3}+l}{2l+1} + \binom{\frac{q+2e}{3}+l}{2l+1}\right)\\
&\quad \equiv (-27)^l e\left(\frac{((e/3)^2-l^2)((e/3)^2-(l-1)^2)\dots((e/3)^2-1)(e/3)}{(2l+1)!}\right.\\
&\qquad\quad \left.+\frac{((2e/3)^2-l^2)((2e/3)^2-(l-1)^2)\dots((2e/3)^2-1)(2e/3)}{(2l+1)!}\right)\\
&\quad = 3^{l-1}\left(\frac{((3l)^2-1)((3(l-1))^2-1)\dots(3^2-1)}{(2l+1)!}\right.\\
&\qquad\quad \left.+\frac{((3l)^2-2^2)((3(l-1))^2-2^2)\dots(3^2-2^2)2}{(2l+1)!}\right)\\
&\quad = \frac{1}{3}((3l+1)+(3l+2))\frac{(3l)!}{(2l+1)!l!} = \binom{3l}{l} \equiv \binom{|3l|_{q-1}}{l} \text{ mod } q
\end{aligned}$$

(note that if $\left[\frac{q-1}{3}\right] < l \le \frac{q-3}{2}$, then $\binom{3l}{l} \equiv \binom{|3l|_{q-1}}{l} = 0 \text{ mod } q$). ∎

Proposition 5. *Let ρ_n be as in Proposition 4. For $m \in \mathbb{Z} - q\mathbb{Z}$, we have*

$$\rho_1(m) = 1 + \left(\frac{1-4m}{q}\right), \tag{35}$$

where $\left(\frac{\ }{q}\right)$ is the Legendre symbol.

Let $e(q)$ be as in (34). For $m \in \mathbb{Z} - q\mathbb{Z}$, we have

$$\begin{aligned}\rho_2(m) &\equiv 1 + \frac{1}{2}\left(\left(\frac{1-(27/4)m}{q}\right) + e(q)\left(\frac{-(27/4)m}{q}\right)\right) \\ &\quad \times \left(\left(\sqrt{1-(27/4)m} + \sqrt{-(27/4)m}\right)^{\frac{q-e(q)}{3}} \right. \\ &\quad \left. + \left(\sqrt{1-(27/4)m} - \sqrt{-(27/4)m}\right)^{\frac{q-e(q)}{3}}\right) \bmod q. \end{aligned} \tag{36}$$

That is:

If $q \equiv 1 \bmod 3$, and we call $M = -(27/4)m$,

$$\begin{aligned}\rho_2(m) &= 1 + \frac{1}{2}\left(1 + \left(\frac{M^2+M}{q}\right)\right) \\ &\qquad \times \left(\left(\frac{M^2 + M\sqrt{M^2+M}}{q}\right)_3 + \left(\frac{M^2 - M\sqrt{M^2+M}}{q}\right)_3\right)\end{aligned}$$

$$= \begin{cases} 2 & \text{if } M \equiv -1 \mod q, \\ 1 & \text{if } \left(\frac{M^2+M}{q}\right) = -1, \\ 0 & \text{if } M^2 + M \equiv a^2 \not\equiv 0 \mod q \ (a \in \mathbb{Z}), \text{ and } \left(\frac{M^2+Ma}{q}\right)_3 \neq 1, \\ 3 & \text{if } M^2 + M \equiv a^2 \not\equiv 0 \mod q \ (a \in \mathbb{Z}), \text{ and } \left(\frac{M^2+Ma}{q}\right)_3 = 1. \end{cases} \tag{37}$$

Here $(\frac{b}{q})_3 = \zeta_3^k \equiv b^{\frac{q-1}{3}} \bmod q$, for $b \in \mathbb{Z}_{(q)} - q\mathbb{Z}_{(q)}$.

If $q \equiv -1 \bmod 3$, then $(\frac{-3}{q}) = -1$ and q is inert in $\mathbb{Q}(\sqrt{-3})$. Call $M = -(27/4)m$. We have four possibilities: If $M \equiv -1 \bmod q$, then $\rho_2(m) = 2$. If $(\frac{1+M}{q}) = (\frac{M}{q})$, then $\rho_2(m) = 1$. If $M \equiv -3a^2 \bmod q$ ($a \in \mathbb{Z} - q\mathbb{Z}$), and $1 + M \equiv b^2 \bmod q$ ($b \in \mathbb{Z} - q\mathbb{Z}$), then

$$\rho_2(m) = 1 + \left(\frac{b + a\sqrt{-3}}{q}\right)_3 + \left(\frac{b - a\sqrt{-3}}{q}\right)_3 = \begin{cases} 0 & \text{if } \left(\frac{b+a\sqrt{-3}}{q}\right)_3 \neq 1, \\ 3 & \text{if } \left(\frac{b+a\sqrt{-3}}{q}\right)_3 = 1. \end{cases} \tag{38}$$

Here $(\frac{\alpha}{q})_3 = \zeta_3^k \equiv \alpha^{\frac{q^2-1}{3}} \bmod q$, for $\alpha \in \mathbb{Z}_{(q)}\left[\sqrt{-3}\right] - q\mathbb{Z}_{(q)}\left[\sqrt{-3}\right]$. If $M \equiv a^2 \bmod q$ ($a \in \mathbb{Z} - q\mathbb{Z}$), and $1 + M \equiv -3b^2$ mod q ($b \in \mathbb{Z} - q\mathbb{Z}$), then

$$\rho_2(m) = 1 + \left(\frac{a + b\sqrt{-3}}{q}\right)_3 + \left(\frac{a - b\sqrt{-3}}{q}\right)_3 = \begin{cases} 0 & \text{if } \left(\frac{a+b\sqrt{-3}}{q}\right)_3 \neq 1, \\ 3 & \text{if } \left(\frac{a+b\sqrt{-3}}{q}\right)_3 = 1. \end{cases} \tag{39}$$

Proof. Formula (35) follows from the definition of $\rho_1(m)$ and from the formula for solving the quadratic congruence modulo q.

To prove congruence (36), call $e = e(q)$, $M = -(27/4)m$ and $u = \sqrt{1+M} + \sqrt{M}$. So $u^{-1} = \sqrt{1+M} - \sqrt{M}$. Call

$$S = \frac{1}{2}\left(\left(\frac{1+M}{q}\right) + e\left(\frac{M}{q}\right)\right)\left(\left(\sqrt{1+M} + \sqrt{M}\right)^{\frac{q-e}{3}} + \left(\sqrt{1+M} - \sqrt{M}\right)^{\frac{q-e}{3}}\right).$$

We have that

$$\begin{aligned}
S &\equiv \frac{1}{2}\left((\frac{u+u^{-1}}{2})^{q-1} + e(\frac{u-u^{-1}}{2})^{q-1}\right)(u^{\frac{q-e}{3}} + u^{-\frac{q-e}{3}}) \\
&\equiv \frac{1}{2}(\sum_{k=0}^{q-1}(-1)^k u^{q-1-k}u^{-k} + e\sum_{k=0}^{q-1} u^{q-1-k}u^{-k})(u^{\frac{q-e}{3}} + u^{-\frac{q-e}{3}}) \\
&= \sum_{k=0}^{q-1} \frac{(-1)^k + e}{2} u^{q-1-2k}(u^{\frac{q-e}{3}} + u^{-\frac{q-e}{3}}) \\
&= e\frac{u^{q+e} - u^{-(q+e)}}{u^2 - u^{-2}}(u^{\frac{q-e}{3}} + u^{-\frac{q-e}{3}}) \mod q.
\end{aligned}$$

That is,

$$\begin{aligned}
S \equiv \frac{e}{4\sqrt{M+M^2}}\Big((\sqrt{1+M}+\sqrt{M})^{\frac{4q+2e}{3}} - (\sqrt{1+M}-\sqrt{M})^{\frac{4q+2e}{3}} \\
+ (\sqrt{1+M}+\sqrt{M})^{\frac{2q+4e}{3}} - (\sqrt{1+M}-\sqrt{M})^{\frac{2q+4e}{3}}\Big) \mod q.
\end{aligned}$$

But for any positive integer n, we have

$$\begin{aligned}
&\frac{1}{2\sqrt{M+M^2}}\big((\sqrt{1+M}+\sqrt{M})^{2n} - (\sqrt{1+M}-\sqrt{M})^{2n}\big) \\
&\quad = \sum_{l=0}^{n-1} M^{n-1-l}\sum_{k=0}^{n-1}\binom{2n}{2k+1}\binom{k}{l} \\
&\quad = \sum_{l=0}^{n-1} 2^{2n-2l-1}\binom{2n-l-1}{l}M^{n-1-l} = \sum_{l=0}^{n-1} 2^{2l+1}\binom{n+l}{2l+1}M^l
\end{aligned}$$

(for the second identity see, if necessary, [12], Section 4.3 and formula (2.5.7)).

Hence

$$\begin{aligned}
S &\equiv e(\sum_{l=0}^{\frac{2q+e}{3}-1} 2^{2l}\binom{\frac{2q+e}{3}+l}{2l+1}M^l + \sum_{l=0}^{\frac{q+2e}{3}-1} 2^{2l}\binom{\frac{q+2e}{3}+l}{2l+1}M^l) \\
&= \sum_{l=0}^{q-2}(-27)^l e(\binom{\frac{2q+e}{3}+l}{2l+1} + \binom{\frac{q+2e}{3}+l}{2l+1})m^l \mod q.
\end{aligned}$$

Therefore, by Lemma 2 and Proposition 4, $S \equiv \sum_{l=0}^{q-2}\binom{|3l|_{q-1}}{l}m^l \equiv \rho_2(m) - 1 \mod q$. This proves congruence (36).

In order to prove the next equalities, suppose first that $q \equiv 1 \mod 3$. Then, by (36),

$$\begin{aligned}
\rho_2(m) &\equiv 1 + \frac{1}{2}\left(\left(\frac{1+M}{q}\right) + \left(\frac{M}{q}\right)\right) \\
&\qquad \times \left(\left(\sqrt{1+M}+\sqrt{M}\right)^{\frac{q-1}{3}} + \left(\sqrt{1+M}-\sqrt{M}\right)^{\frac{q-1}{3}}\right) \\
&\equiv 1 + \frac{1}{2}\left(1 + \left(\frac{M^2+M}{q}\right)\right)\left(\left(M^2 + M\sqrt{M^2+M}\right)^{\frac{q-1}{3}}\right. \\
&\qquad\qquad \left. + \left(M^2 - M\sqrt{M^2+M}\right)^{\frac{q-1}{3}}\right) \mod q.
\end{aligned}$$

This congruence must be interpreted as follows: If $M^2+M\equiv a^2 \bmod q$ for some $a\in\mathbb{Z}$, then $\sqrt{M^2+M}=a$ (or $-a$); otherwise $\left(1+(\frac{M^2+M}{q})\right)=0$, and so $\rho_2(m)\equiv 1 \bmod q$. Formula (37) follows from this and from the fact that $0\le\rho_2(m)\le 3$.

Suppose now that $q\equiv -1 \bmod 3$. We work in $\mathbb{Q}(\sqrt{-3})$. Note that $(\frac{-3}{q})=-1$, that q is inert, and that the Frobenius map for q is complex conjugation. By (36) we have

$$\begin{aligned}\rho_2(m)\equiv 1+\frac{1}{2}\left(\left(\frac{1+M}{q}\right)-\left(\frac{M}{q}\right)\right)\Bigg(&\left(\sqrt{1+M}+\sqrt{M}\right)^{\frac{q+1}{3}}\\ &+\left(\sqrt{1+M}-\sqrt{M}\right)^{\frac{q+1}{3}}\Bigg) \bmod q.\end{aligned}$$

Also $0\le\rho_2(m)\le 3$. If $M\equiv -1 \bmod q$, this gives $\rho_2(m)=2$. If $(\frac{1+M}{q})=(\frac{M}{q})$, this gives $\rho_2(m)=1$. If $M\equiv -3a^2 \bmod q$, and $1+M\equiv b^2 \bmod q$ for some $a,b\in\mathbb{Z}-q\mathbb{Z}$, then $(b+a\sqrt{-3})(b-a\sqrt{-3})\equiv 1 \bmod q$, and we can write

$$\begin{aligned}\rho_2(m)&\equiv 1+\left(\left(b+a\sqrt{-3}\right)^{\frac{q+1}{3}}+\left(b-a\sqrt{-3}\right)^{\frac{q+1}{3}}\right)\\ &\equiv 1+\left(\left(b+a\sqrt{-3}\right)^{\frac{q^2-1}{3}}+\left(b-a\sqrt{-3}\right)^{\frac{q^2-1}{3}}\right) \bmod q.\end{aligned}$$

Formula (38) follows from this congruence. The proof of formula (39) is similar. □

We can now show our formulas for the coefficients $d_{n,k}$.

Theorem 1. *Let ρ_n be as in Proposition 4. For $1\le n\le p-2$ and $0\le k\le p-1$,*

$$\begin{aligned}d_{n,k}=&f-\sum_{a=0}^{f-1}\rho_n(s^{k+pa})\\ =&f-\#\{u: 2\le u\le q-1 \text{ and } (u^{n+1}-u^n)^f-s^{fk}\equiv 0 \bmod q\}\end{aligned} \quad (40)$$

For $0\le k\le p-1$,

$$d_{1,k}=-\sum_{a=0}^{f-1}\left(\frac{1-4s^{k+pa}}{q}\right).$$

That is, $d_{1,k}$ = number of quadratic nonresidues $\bmod q$ *− number of quadratic residues* $\bmod q$*, in the set $\{1-4s^{k+pa}: 0\le a\le f-1\}$ (do not count 0 as a quadratic residue* $\bmod q$*).*

Let $e(q)$ be as in (34). Define the function $\lambda : \mathbb{Z} - q\mathbb{Z} \to \mathbb{Z}$ by $\lambda(m) =$

$$\begin{cases} 1 & \text{if } M \equiv -1 \bmod q, \\ 0 & \text{if } (\frac{1+M}{q}) = -e(q)(\frac{M}{q}), \\ -1 & \text{if } q \equiv 1 \bmod 3,\ M^2 + M \equiv a^2 \not\equiv 0 \bmod q\ (a \in \mathbb{Z}), \text{ and } (\frac{M^2+Ma}{q})_3 \neq 1, \text{ or} \\ & \text{if } q \equiv -1 \bmod 3,\ M \equiv -3a^2 \bmod q,\ 1+M \equiv b^2 \bmod q\ (a, b \in \mathbb{Z} - q\mathbb{Z}), \\ & \text{and } (\frac{b+a\sqrt{-3}}{q})_3 \neq 1, \text{ or if} \\ & q \equiv -1 \bmod 3,\ M \equiv a^2 \bmod q,\ 1+M \equiv -3b^2 \bmod q\ (a, b \in \mathbb{Z} - q\mathbb{Z}), \text{ and} \\ & (\frac{a+b\sqrt{-3}}{q})_3 \neq 1, \\ 2 & \text{if } q \equiv 1 \bmod 3,\ M^2 + M \equiv a^2 \not\equiv 0 \bmod q\ (a \in \mathbb{Z}), \text{ and } (\frac{M^2+Ma}{q})_3 = 1, \text{ or} \\ & \text{if } q \equiv -1 \bmod 3,\ M \equiv -3a^2 \bmod q,\ 1+M \equiv b^2 \bmod q\ (a, b \in \mathbb{Z} - q\mathbb{Z}), \\ & \text{and } (\frac{b+a\sqrt{-3}}{q})_3 = 1, \text{ or if} \\ & q \equiv -1 \bmod 3,\ M \equiv a^2 \bmod q,\ 1+M \equiv -3b^2 \bmod q\ (a, b \in \mathbb{Z} - q\mathbb{Z}), \text{ and} \\ & (\frac{a+b\sqrt{-3}}{q})_3 = 1, \end{cases}$$

where $M = -(27/4)m$. Then, for $0 \le k \le p-1$,

$$d_{2,k} = -\sum_{a=0}^{f-1} \lambda(s^{k+pa}).$$

Proof. Formula (40) can be obtained directly from (1) and (4). Alternatively: Let $1 \le n \le p-2$ and $0 \le k \le p-1$. It follows from (32), (33), and Proposition 4, that $f - d_{n,k} \equiv \sum_{a=0}^{f-1} \rho_n(s^{k+pa}) \bmod q$. On the other hand, since $0 \le \rho_n(m) \le n+1$, we have $0 \le \sum_{a=0}^{f-1} \rho_n(s^{k+pa}) \le (n+1)f < q$. By (8) and (30), we have that $0 \le f - d_{n,k} < f + \sqrt{q} < q$. Therefore $f - d_{n,k} = \sum_{a=0}^{f-1} \rho_n(s^{k+pa}) =$ number of roots, in $\mathbb{Z}/q\mathbb{Z}$, of $\prod_{a=0}^{f-1}(X^{n+1} - X^n + s^k s^{pa}) =$ number of roots, in $\mathbb{Z}/q\mathbb{Z}$, of $(X^{n+1} - X^n)^f - s^{kf}$. The other equalities follow from this and from Proposition 5. $\square$

Observation. By (3), we have that, for $2 \le k \le p-1$,

$$\prod_{i=1}^{k-1} J_i = (-1)^{k-1} G(\zeta_p)^k / G(\zeta_p^k).$$

Also, for $1 \le k \le p-1$,

$$\prod_{i=0}^{k-1} \sigma_{2^i}(J_1)^{2^{k-1-i}} = (-1)^k G(\zeta_p)^{2^k} / G(\zeta_p^{2^k}).$$

In particular

$$\prod_{i=0}^{p-2} \sigma_{2^i}(J_1)^{2^{p-2-i}} = (G(\zeta_p)^p)^{\frac{2^{p-1}-1}{p}}.$$

If 2 is a primitive root modulo p, using these relations, we can express all Jacobi sums J_n, $1 \le n \le p-2$, in terms of J_1 and $G(\zeta_p)^p$. If 2 is a primitive root modulo p^2, we can express all Jacobi sums J_n, up to p-th powers of elements in $\mathbb{Z}[\zeta_p]^\times$, in terms of J_1; so, by Theorem 1, in terms of the numbers of quadratic residues modulo q in the sets $\{1 - 4s^{k+pa} : 0 \le a \le f-1\}$, $0 \le k \le p-1$.

References

1. M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*, Dover Publications, New York, 1972.
2. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.
3. E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetsen*, J. Reine Angew. Math. **44** (1852), 93–146.
4. S. Lang, *Cyclotomic fields I and II (with an appendix by K. Rubin)*, Combined Second Edition, Graduate Texts in Mathematics, Springer-Verlag, New York, 1990. MR **91c:**11001
5. V. A. Lebesgue, *Recherches sur les nombres*, J. Math. Pures Appl. **2** (1837), 253–292.
6. L. J. Slater, *Generalized Hypergeometric Functions*, Cambridge University Press, 1966. MR **34:**1570
7. T. Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics, Markham Publishing Company, Chicago, 1967. MR **36:**128
8. F. Thaine, *On the relation between units and Jacobi sums in prime cyclotomic fields*, Manuscripta Math. **73** (1991), 127–151. MR **92m:**11122
9. F. Thaine, *Properties that characterize Gaussian periods and cyclotomic numbers*, Proc. Amer. Math. Soc. **124** (1996), 35–45. MR **96d:**11115
10. F. Thaine, *On the p-part of the ideal class group of* $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ *and Vandiver's conjecture*, Michigan Math. J. **42** (1995), 311–343. MR **96e:**11140
11. L. C. Washington, *Introduction to Cyclotomic Fields*, Second Edition, Graduate Texts in Mathematics, Springer-Verlag, New York, 1997. MR **97h:**11130
12. H. S. Wilf, *Generatingfunctionology*, Second Edition, Academic Press, San Diego, California, 1994. MR **95a:**05002

Department of Mathematics and Statistics - CICMA, Concordia University, 1455, de Maisonneuve Blvd. W., Montreal, Quebec, H3G 1M8, Canada

E-mail address: `ftha@vax2.concordia.ca`