ON THE COEFFICIENTS OF JACOBI SUMS 
IN PRIME CYCLOMATIC 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 \(-\sum_{k=2}^{q-1} \zeta_{q}^{\text{ind}_s(k)+n \text{ind}_s(1-k)}\). We study the integers \( d_{n,k} \) such that \( J_n = \sum_{k=0}^{p-1} d_{n,k} \zeta_{q}^{k} \) 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.

Introduction

Let \( p \) and \( q \) be prime numbers such that \( p \geq 5 \) and \( q \equiv 1 \mod p \). Call \( f = (q-1)/p \). Let \( \zeta_{p} \) 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

\[
J_n = -\sum_{k=2}^{q-1} \zeta_{q}^{\text{ind}_s(k)+n \text{ind}_s(1-k)},
\]

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

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

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
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 \( s^f \equiv \zeta_p \mod Q \). 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 \( \pi \) the smallest positive integer such that \( a\pi \equiv 1 \mod p \). For \( 1 \leq n \leq p - 2 \) and \( 1 \leq l \leq p - 1 \), let \( \lambda_{n,l} = \lambda_{n,l}(Q) \) be the indices of the cyclotomic units

\[
\varepsilon_{n,l} = \frac{(1 - \zeta_p^d)(1 - \zeta_p^{\pi})^n}{(1 - \zeta_p^{(p+1)f})^n+1}
\]

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

\[
s^{\lambda_{n,l}} \equiv \varepsilon_{n,l} \mod Q.
\]

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

(i) \[ \lambda_{n,l} \equiv \sum_{k=1}^{p-1} k d_{n,k} d_{n,k+l} \mod p. \]

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 \( \mathbb{Q}(\zeta_p) \), \( \Delta \) 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 \( \omega(k) \equiv k \mod p \), and \( \epsilon_k \), \( 0 \leq k \leq p - 2 \), the idempotents of \( \mathbb{Z}_p^{\text{even}} \). 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, \( 2 \leq r \leq p-3 \). 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, \( 2 \leq r \leq p-3 \)), we only need the numbers \( d_{n,k}(Q) \), \( 0 \leq k \leq p-1 \), for any fixed \( n \) such that \( 1 + n^{p-r} - (n+1)^{p-r} \neq 0 \mod p \). For example, if \( p \) is a primitive root modulo \( p \), we only need the numbers \( d_{1,k}(Q) \), \( 0 \leq k \leq p-1 \), to study all even components of \( A \).

In Section 3 we give formulas for the numbers \( d_{n,k} \), \( 1 \leq n \leq p-2, 0 \leq k \leq p-1 \). 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 \( |k|_m \equiv k \mod m \).

It follows from a well-known result on Gauss sums ([4], Chapter 1, Theorem 2.1) that, for \( 1 \leq n \leq p-2 \) and \( 1 \leq k \leq p-1 \),

\[
\sigma_k(\overline{J_n}) = \left( \frac{f|(n+1)k|_p}{f_k} \right) \mod Q,
\]

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

(ii) \[ d_{n,k} \equiv \frac{1}{p} \sum_{l=0}^{p-1} \left( \frac{f|(n+1)l|_p}{f_l} \right) s^{fk} \mod q \]

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

(iii) \[ |d_{n,k}| < \sqrt{q}. \]
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 $|d_{n,k}|_{0 \leq n \leq p-2, 0 \leq k \leq p-1}$ is

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

Congruence (ii) can be written as

$$(iv) \quad d_{n,k} \equiv \frac{1}{p} \sum_{l=0}^{p-1} (|f(n+1)|_{q-1} l^{k}) \mod q \quad (formula (31)).$$

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

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

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

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

$$\sum_{l=0}^{q-2} (\binom{n+1}{l}_{q-1} l^{m'}) \equiv \rho_n(m) - 1 \mod q \quad (Proposition 4).$$

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

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

where $\left(\frac{q}{7}\right)$ 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

$$\rho_2(m) \equiv 1 + \frac{1}{2} \left(\frac{1 - (27/4)m}{q} + e(q) \left(\frac{-(27/4)m}{q}\right)\right)$$

$$\times \left(\sqrt{1 - (27/4)m} + \sqrt{-(27/4)m}\right)^{\frac{q-1(q)}{3}}$$

$$+ \left(\sqrt{1 - (27/4)m} - \sqrt{-(27/4)m}\right)^{\frac{q-1(q)}{3}} \mod q.$$
For $1 \leq n \leq p - 2$ and $0 \leq k \leq p - 1$,

$$(v) \quad d_{n,k} = f - \sum_{a=0}^{f-1} \rho_n(s^{k+pa})$$

$$= f - \#\{u : 2 \leq u \leq q - 1 \text{ and } (u^{n+1} - u^f)^{s^{k+pa}} \equiv 0 \mod q\}.$$  

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

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

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

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 $\sum_{\ell=0}^{q-2} \frac{(2^{[\ell - 1]})}{\ell} m! \equiv \sum_{\ell=0}^{q-2} \frac{(2^{[\ell - 1]})}{\ell} m! \equiv (1 - 4m)^{\frac{q-1}{2}} \equiv \left(\frac{1 - 4m}{q}\right)$ mod $q$, which gives the case $n = 1$, and then applying the theory of hypergeometric functions to the polynomials $\sum_{\ell=0}^{q-2} \frac{(3^{[\ell - 1]})}{\ell} X^\ell$ to try and find a similar result for $n = 2$. We believe that other formulas for $\rho_n(m)$ and $d_{n,k}$, $n \geq 3$, 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 $p \geq 5$ be a prime number, $\zeta_p$ a primitive $p$-th root of 1, $q \equiv 1 \mod p$ a prime number, $f = (q - 1)/p$, $\zeta_q$ a primitive $q$-th root of 1, and $s$ a primitive root modulo $q$. Let $\Delta = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, 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 $\text{ind}_s(k)$ the least nonnegative integer such that $s^{\text{ind}_s(k)} \equiv k \mod q$.

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

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

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

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

$$(2) \quad G(\zeta_p^a)G(\zeta_p) = q,$$

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

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

(see, for example, [11], Lemma 6.2).
For $1 \leq n \leq p - 2$, write

$$J_n = \sum_{k=0}^{p-1} d_{n,k} \zeta_p^k,$$

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

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 $i, j \in \mathbb{Z}$, 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

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

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 $(k, l), 0 \leq k, l \leq f - 1$, such that $1 + s pk + i \equiv s pl + j \mod q$. 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 $a \in \mathbb{Z} - p\mathbb{Z}$, $\bar{a}$ will denote the least positive integer such that $a \bar{a} \equiv 1 \mod p$; also, we use the following version of Kronecker’s delta: for $k, l \in \mathbb{Z}$,

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

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:

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

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

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

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

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

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

$$J_n = -\sum_{k=0}^{p-1} \sum_{h=0}^{p-1} \zeta_p^{nk+h} (h, k).$$
Therefore, using (2), formula (14), and formula (17) (with \( e = p \) and \( n_k = \delta_{0,k} \)),

\[
T_{Q(\zeta_p)/Q}(\sum_{n=1}^{p-2} \zeta_p^{-in} J_n) = p \sum_{k=0}^{p-1} (h,k)\delta_{k+i,j} - \sum_{k=0}^{p-1} (h,k)
\]

\[
= p \sum_{h=0}^{p-1} (h,j)(p\delta_{h,i} - 1) + \sum_{k=0}^{p-1} (h,k)(p\delta_{h,i} - 1)
\]

\[
= p \sum_{h=0}^{p-1} (h,j) - \sum_{h=0}^{p-1} (h,k) - p^2(i,j) + p \sum_{h=0}^{p-1} (h,j) + p \sum_{h=0}^{p-1} (i,k) - \sum_{h=0}^{p-1} \sum_{h=0}^{p-1} (h,k)
\]

\[
= p(f - \delta_{i,j}) - p^2(i,j) + p(f - \delta_{0,j}) + p(f - \delta_{0,i})
\]

\[
- 2 \sum_{k=0}^{p-1} (f - \delta_{0,k}) = -p^2(i,j) - p\delta_{0,i} - p\delta_{0,j} - p\delta_{i,j} + q + 1.
\]

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 \( 1 \leq n \leq p - 2 \) and \( 0 \leq k \leq p - 1 \),
  a) \( \sigma_n(J_n) = J_n \).
  That is, \( d_{n,k} = d_{n,\pi k} \).
  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, \( \sum_{j=0}^{p-1} d_{n,j} d_{n,j+k} = \delta_{0,k}q - f \).

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

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

- The characteristic polynomial of the matrix \( [c_{i,j}]_{0 \leq i,j \leq p-1} \) 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 \( G(\zeta_p^n)G(\zeta_p^{-n}) = q \) if \( p \nmid a \) (see [11], Lemma 6.1 (b)).

c) Follows from (2) and (3).

d) We have that

\[
\sigma_t^{-1}(J_{nt}J_{mt}) = \sigma_t \left( \frac{G(\zeta_p^n)G(\zeta_p^{nt})G(\zeta_p^{-nt})}{G(\zeta_p^n+1)G(\zeta_p^{n+1})} \right) = q \frac{G(\zeta_p^n)G(\zeta_p^{-m})}{G(\zeta_p^n+1)G(\zeta_p^{n+1})} = J_nJ_m
\]

(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

\[
\eta_i = \sum_{j=0}^{p-1} \zeta_q^{i+j} \quad \text{; and, } \quad \eta_i\eta_j = \sum_{x=0}^{p-1} c_{i,j}\eta_x \quad \text{see [9], formula (1)).}
\]

Now the result follows, for example, from [9], Theorem 1 (property (iv)), or [2], formula (9).

\( \square \)

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

**Proposition 2.** Let \( J_n, 1 \leq n \leq p-2 \), 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 \( p^{n-1} \not\equiv 1 \mod q \) (as the primes in \( P_m \), 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 \( [c_{i,j}]_{0 \leq i,j \leq p-1} \) is irreducible modulo \( p \). Notice also that (e) is just a condition modulo \( p \) on the numbers \( d_{a,k} \).

**Proof.** Let \( J_n, 1 \leq n \leq p-2 \), 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 \( t \),

- \( \sum_{k=0}^{p-1} c_{i,k} = f - q\delta_{0,i} \)
- \( \sum_{k=0}^{p-1} c_{k,j} = -\delta_{0,j} \)
- \( \sum_{k=0}^{p-1} c_{i,k+j} = \sum_{k=0}^{p-1} c_{j,k+i} \)

iv) The characteristic polynomial of the matrix \( [c_{i,j}]_{0 \leq i,j \leq p-1} \) 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

\[
(10) \quad c_{i,j} + f \delta_{0,i} = c_{j,i} + f \delta_{0,j}
\]

and

\[
(11) \quad c_{i,j} = c_{-i,j-i}.
\]

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

\[
c_{i,j} + f \delta_{0,i} = -\frac{1}{p^2} (p\delta_{0,i} + p\delta_{0,j} + p\delta_{i,j} - q - 1 + \sum_{n=1}^{p-2} T_{Q(\zeta_p^n) / Q} (\zeta_p^{-ij} n \sigma_n (J_p)))
\]

\[
= -\frac{1}{p^2} (p\delta_{0,i} + p\delta_{0,j} + p\delta_{i,j} - q - 1 + \sum_{n=1}^{p-2} T_{Q(\zeta_p^n) / Q} (\zeta_p^{-ij} n J_p))
\]

\[
= -\frac{1}{p^2} (p\delta_{0,i} + p\delta_{0,j} + p\delta_{i,j} - q - 1 + T_{Q(\zeta_p^n) / Q} (\sum_{n=1}^{p-2} \zeta_p^{-ij} n J_n))
\]

\[
= c_{j,i} + f \delta_{0,j}.
\]

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

\[
c_{i,j} + f \delta_{0,i} = -\frac{1}{p^2} (p\delta_{0,i} + p\delta_{0,j} + p\delta_{i,j} - q - 1 + T_{Q(\zeta_p^n) / Q} (\sum_{n=1}^{p-2} \zeta_p^{-ij} n J_{p-1-n}))
\]

\[
= -\frac{1}{p^2} (p\delta_{i,j-i,j} + p\delta_{0,j} + p\delta_{0,i-j} - q - 1 + T_{Q(\zeta_p^n) / Q} (\sum_{n=1}^{p-2} \zeta_p^{-i-j} n J_n))
\]

\[
= c_{i-j,j} + f \delta_{i,j}.
\]

Therefore, by (10), we have

\[
c_{i,j} = c_{j,i} + f \delta_{0,j} - f \delta_{0,i} = c_{j-i,-i} + f \delta_{i,j} - f \delta_{0,j} + f \delta_{0,i} - f \delta_{0,i}
\]

\[
= c_{i-j,-i} + f \delta_{0,i} - f \delta_{i,j} + f \delta_{i,j} - f \delta_{0,i} = c_{i-j,-i}.
\]

This proves (11). Using (11) we can replace condition (iii) by the more symmetric condition \( iii' \): \( \sum_{k=0}^{p-1} c_{i,k} c_{k-j,i-j} = \sum_{k=0}^{p-1} c_{j,k} c_{k-i,t-i} \). Now, by (c),

\[
(12) \quad p^2 \sum_{k=0}^{p-1} c_{i,k} c_{k-j,i-j} = \sum_{k=0}^{p-1} \left( q \delta_{0,i} + \delta_{0,k} + \delta_{i,k} - f - 1 + \sum_{n=1}^{p-2} d_{m,i+km} \right)
\]

\[
\times \left( q \delta_{k,j} + \delta_{i,j} + \delta_{k,i} - f - 1 + \sum_{n=1}^{p-2} d_{n,(k-j)+(l-j)n} \right).
\]

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

\[
p^2 \sum_{k=0}^{p-1} c_{i,k} c_{k-j,l-j} = q\delta_{0,j} + \delta_{0,t} + (1 - q)\delta_{t,j} + q\delta_{t,i} + \delta_{i,t} + pq\delta_{t,j}\delta_{0,i} - (f + 1)p
\]

\[
+ q \sum_{n=1}^{p-2} d_{n,i+jn} + \sum_{n=1}^{p-2} d_{n,i+tn} + \sum_{n=1}^{p-2} d_{n,-j+(t-j)n} + \sum_{n=1}^{p-2} d_{n,(i+j)+(t-j)n}
\]

\[
+ \sum_{m=1}^{p-2} \sum_{n=1}^{p-2} \sum_{k=0}^{p-1} d_{m,i+nm} d_{n,(k-j)+(t-j)n}
\]

\[
= q\delta_{0,j} + \delta_{0,t} + (1 - q)\delta_{t,j} + q\delta_{t,i} + \delta_{i,t} + pq\delta_{t,j}\delta_{0,i}
\]

\[- (f + 1)p + q(-p[i,j] - \delta_{0,i} - \delta_{0,j} - \delta_{t,j} + (f + 1))
\]

\[+ (-p[i,l] - \delta_{0,i} - \delta_{0,t} + (f + 1))
\]

\[- (p[-j,l-j] - \delta_{0,j} - \delta_{t,j} - (f + 1))
\]

\[- (p[i-j,l-j] - \delta_{i,j} - \delta_{i,t} - (f + 1))
\]

\[+ \sum_{m=0}^{p-2} d_{m,i+nm} d_{n,(k-j)+(t-j)n}
\]

\[
= -(q + 1)\delta_{0,i} + (q + 1)\delta_{t,j} - \delta_{t,i} - \delta_{t,t} - \delta_{0,t} + pq\delta_{t,j}\delta_{0,i}
\]

\[- (f + 1)(q - p + 3) - pq[i,j] - p[i,l] - p[j,l]
\]

\[- p[i-l,j-l] + \sum_{m=1}^{p-2} \sum_{n=1}^{p-1} \sum_{k=0}^{p-1} d_{m,i+nm} d_{n,(k-j)+(t-j)n}
\]

\[
\leq -q\delta_{0,i} - q\delta_{t,j} + pq\delta_{t,j}\delta_{t,j} + \sum_{m=1}^{p-2} \sum_{n=1}^{p-1} \sum_{k=0}^{p-1} d_{m,i+km} d_{n,(k-j)+(t-j)n}.
\]

Using conditions (a) and (b), we see that the last expression is equal to

\[
-q\delta_{0,i} - q\delta_{t,j} + pq\delta_{t,j}\delta_{t,j} + \sum_{m=1}^{p-2} \sum_{n=1}^{p-2} \sum_{k=0}^{p-1} d_{m,i+km} d_{n,(k-j)+(t-j)n} = -q\delta_{0,i} - q\delta_{t,j} + \sum_{m=1}^{p-2} \sum_{n=1}^{p-2} \sum_{k=0}^{p-1} d_{m,i+km} d_{n,(k-j)+(t-j)n}.
\]

Therefore

\[
p^2 \sum_{k=0}^{p-1} c_{i,k} c_{k-j,l-j} \leq -q\delta_{0,i} - q\delta_{t,j} + pq\delta_{t,j}\delta_{t,j}
\]

\[
+ \sum_{n=1}^{p-1} \sum_{k=0}^{p-1} d_{n,k} d_{n,i+(1+n)j-nl+k} + \sum_{m,n=1}^{p-1} \sum_{k=0}^{p-1} d_{n,k} d_{m,i-(1+n)j+nk+k}.
\]

Now, by condition (c), we have

\[
\sum_{n=1}^{p-1} \sum_{k=0}^{p-1} d_{n,k} d_{n,i+(1+n)j-nl+k}
\]

\[
= \sum_{n=1}^{p-2} (q\delta_{0,i} + (1+n)j-nl - f) + 1 + 2f - q\delta_{0,i} - q\delta_{t,j} - q\delta_{i+j,t} + pq\delta_{0,j}\delta_{t,i}
\]

\[
\leq -q\delta_{0,j} - q\delta_{t,i} + pq\delta_{0,j}\delta_{t,i}.
\]
Hence, by \((13)\),

\[
p^2 \sum_{k=0}^{p-1} c_{i,k} c_{j-l,j} \sim \sum_{m,n=1}^{p-2} \sum_{k=0}^{p-1} d_{n,k} d_{m,mi-nj+(1+n)l+k}.
\]

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

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

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

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

We preserve the notations of Section 1; \(Z\) be a prime ideal of \(\mathbb{Z}\); 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 \(s^f \equiv \zeta_p \mod Q\) (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 \(a\overline{a} \equiv 1 \mod p\). 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.

### 2. Indices of cyclotomic units, Van der'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.

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
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

\begin{equation}
(14) \quad s^{\lambda_{n,l}} \equiv \frac{(1 - c_p^l)(1 - \zeta_p^{n+l})^n}{(1 - \zeta_p^{(n+1)l})^{n+1}} \mod Q.
\end{equation}

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

\begin{equation}
(15) \quad \sum_{l=1}^{q-1} \lambda_{n,l} \equiv 0 \mod q - 1.
\end{equation}

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

\begin{equation}
(16) \quad s^{\lambda_{n,l}} \equiv \frac{(1 - s^f l)(1 - s^f \zeta_p^{n+l})^n}{(1 - s^f \zeta_p^{(n+1)l})^{n+1}} \mod q.
\end{equation}

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

\begin{equation}
(17) \quad \lambda_{n,l} \equiv \Phi(f l) + n \Phi(f \zeta_p^{n+l}) - (n + 1) \Phi(f(\zeta_p^{n+1})l) \mod q - 1.
\end{equation}

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

\begin{equation}
(18) \quad \Psi_n(\zeta_p) = -J_n.
\end{equation}

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

\begin{equation}
(19) \quad \zeta_p G'(\zeta_p)/G(\zeta_p) \equiv - \sum_{k=1}^{q-2} k \zeta_q^k + \sum_{l=1}^{f-1} \Phi(l p) + \sum_{l=1}^{p-1} \Phi(-l f) \zeta_p^l \mod \frac{q - 1}{2}.
\end{equation}

Therefore

\begin{align*}
\zeta_p \Psi_n'(\zeta_p)/\Psi_n(\zeta_p) & = \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}) \\
& \equiv \sum_{l=1}^{p-1} \Phi(-l f) + n \Phi(-l \zeta_p f) - (n + 1) \Phi(-l(n + 1) f) \zeta_p^l \mod(q - 1)/2.
\end{align*}

So, by (17), for $1 \leq n \leq p - 2$,
\[ \sum_{l=1}^{p-1} \lambda_{n,l} \zeta_p^{-l} \equiv \zeta_p \Psi'_n(\zeta_p)/\Psi_n(\zeta_p) \equiv \zeta_p \Psi'_n(\zeta_p) \Psi_n(\zeta_p) \mod q - \frac{1}{2} \]  

(see also [8], page 133).

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

\[ J_n(X) \equiv -\Psi_n(X) = -G(X)G(X^n)/G(X^{n+1}) \mod (X^p - 1). \]  

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

\[
\sum_{l=0}^{p-1} k d_{n,k} d_{n,k+l} X^{p-l} \equiv XJ'_n(X)J_n(X^{p-1}) \equiv (q - f(1 + X + \ldots + X^{p-1})) \times (XG'(X)/G(X) + nX^nG'(X^n)/G(X^n) - (n + 1)X^{n+1}G'(X^{n+1})/G(X^{n+1})) \equiv XG'(X)/G(X) + nX^nG'(X^n)/G(X^n) - (n + 1)X^{n+1}G'(X^{n+1})/G(X^{n+1}) \mod (p, X^p - 1),
\]

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

\[ XG'(X)/G(X) \equiv \sum_{i=0}^{p-1} g_i X^i \mod (X^p - 1), \]

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

\[
\sum_{l=0}^{p-1} k d_{n,k} d_{n,k+l} X^{p-l} \equiv \sum_{i=0}^{p-1} g_i X^i + n \sum_{i=0}^{p-1} g_i X^{\lceil ni \rceil} - (n + 1) \sum_{i=0}^{p-1} g_i X^{\lceil (n+1)i \rceil} \mod p,
\]

where we denote by \( \lceil m \rceil \) the least nonnegative integer such that \( \lceil m \rceil \equiv m \mod p \). This implies that

\[ \sum_{k=1}^{p-1} k d_{n,k}^2 \equiv 0 \mod p. \]

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 \( 1 \leq n \leq p - 2 \),

\[ \sum_{l=1}^{p-1} \lambda_{n,l} \zeta_p^{-l} \equiv \zeta_p J'_n(\zeta_p)J_n(\zeta_p^{-1}) \mod p. \]  

Equivalently, we have that, for \( 1 \leq n \leq p - 2 \) and \( 1 \leq l \leq p - 1 \),

\[ \lambda_{n,l} \equiv \sum_{k=1}^{p-1} k d_{n,k} d_{n,k+l} \mod p. \]
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

\[ \sum_{k=1}^{p} kd_{n,k} \equiv 0 \quad \text{mod } p. \]

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

\[ (1 + n^{p-r} - (n + 1)^{p-r})i_r(Q) \equiv \sum_{l=1}^{p-1} l^{p-1-r} \lambda_{n,l} \]
\[ \equiv \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} kl^{p-1-r} d_{n,k} d_{n,k+l} \pmod{p} \]

(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, \( \omega: \Delta \cong (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{Z}_p^\times \) the Teichmüller character, defined by \( \omega(k) \equiv k \pmod{p} \) and \( e_k, \) \( 0 \leq k \leq p - 2, \) 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 \( 2 \leq r \leq p - 3, \) are trivial.

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

\[ \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} kl^{p-1-r} d_{n,k}(Q)d_{n,k+l}(Q) \not\equiv 0 \pmod{p}, \]

then \( e_r(A) \) is trivial. Conversely, let \( m \geq 1, \) and let \( P_m \) be the set of all prime ideals \( Q \) of \( \mathbb{Z}[\zeta_p] \) that are above rational primes \( q \) such that \( q \equiv 1 \pmod{p^m} \) and \( p \not\equiv r \pmod{p^m}. \) If

\[ \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} kl^{p-1-r} d_{n,k}(Q)d_{n,k+l}(Q) \equiv 0 \pmod{p}, \quad \text{for all } Q \in P_m, \]

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

**Example.** For \( p = 37 \) all components \( e_r(A) \) with \( r \) even, \( 2 \leq r \leq 34, \) and \( r \neq 32 \) 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 \( 37^{32} - 32 = 2 \not\equiv 2 \pmod{37}, \) and for \( q = 149 \) and \( s = 2 \) the numbers \( d_{1,k}, 0 \leq k \leq 36, \) are \([-2, -2, 0, -2, 0, -4, 2, -2, 0, 2, 0, -4, 0, 2, -2, 0, 0, -2, -4, 0, 0, 2, 4, -2, -2, 2, 0, 0, 2, 2, 2, 1, 2]. \) So

\[ \sum_{k=1}^{36} \sum_{l=1}^{36} kl^4 d_{n,k} d_{n,k+l} \equiv 34 \not\equiv 0 \pmod{37}. \]

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 $s^f \equiv \zeta_q \mod Q$. If $k \in \mathbb{Z}$ and $m > 0$, we denote by $|k|_m$ the least positive integer such that $|k|_m \equiv k \mod m$. As before, if $p \nmid k$, $\bar{k}$ denotes the least positive integer such that $k \bar{k} \equiv 1 \mod p$. 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 $1 \leq l \leq p - 1$,

$$\frac{G(\zeta_p^{-l})}{(\zeta_q - 1)^f} = \frac{-1}{(f!)^l} \mod B. \tag{26}$$

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 $\mathbb{Z}[\zeta_p]$,

$$\overline{(J_n)} = Q^{\sum_{i=1}^{p-1} ([\frac{(n+1)!}{2}] - [\frac{m!}{2}]) \sigma_i^{-1},} \tag{27}$$

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

$$\sigma_k(J_n) \equiv \frac{-G(\zeta_p^{-k})G(\zeta_p^{-|nk|_p})}{G(\zeta_p^{-((n+1)k)_p})} \mod Q. \tag{28}$$

Note that $\frac{f |(n+1)k|_p}{f} \equiv 0 \mod q$, 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 $0 \leq k \leq p - 1$, $d_{n,k} = \frac{1}{p} \left( 1 + \sum_{i=1}^{p-1} \zeta_p^i \sigma_i(J_n) \right) \equiv \frac{1}{p} \sum_{i=0}^{p-1} \zeta_p^i \left( \frac{1}{f} \sum_{l=0}^{f(k+((n+1)k)_p)} \right) \mod Q$. Therefore,

$$d_{n,k} \equiv \frac{1}{p} \left( \frac{1}{f} \sum_{l=0}^{p-1} \left( \frac{f |(n+1)l|_p}{f} \right) \right) \mod Q. \tag{29}$$

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

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

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 $\sqrt{q} < \frac{2 - \sqrt{2}}{2}$.

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

\[
\frac{1}{p} \sum_{l=0}^{n-1} \left( \frac{|f(n+1)l|_{q-1}}{f} \right) s^{fkl} \mod q.
\]

For \( 1 \leq n \leq p-2 \), call

\[
h_n(X) = \sum_{l=0}^{q-2} \left( \frac{|(n+1)l|_{q-1}}{l} \right) X^l.
\]

If \( \zeta_f \) is a primitive \( f \)-th root of 1, then

\[
\frac{1}{p} \sum_{a=0}^{f-1} h_n(X \zeta_f^a) = \sum_{l=0}^{q-2} \left( \frac{|(n+1)l|_{q-1}}{l} \right) X^l \sum_{a=0}^{f-1} \zeta_f^{al} = \frac{1}{p} \sum_{l=0}^{p-1} \left( \frac{|(n+1)fl|_{q-1}}{fl} \right) X^{fl}.
\]

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

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

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

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

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 \( 0 \leq k, n \leq b \),

\[
\left( \frac{an}{ak} \right) \equiv (-1)^{ak} \left( \frac{a(b - n + k)}{ak} \right) \equiv (-1)^{a(n+k)} \left( \frac{a(b - k)}{a(b - n)} \right) \mod q.
\]

**Proof.** We have

\[
\frac{a(b - n + k)}{ak} = \frac{(q-1 - a(n-k))(q-2 - a(n-k)) \ldots (q-ak - a(n-k))}{(ak)!} \equiv (-1)^{ak} \frac{(an)(an-1) \ldots (a(n-k) + 1)}{(ak)!} = (-1)^{ak} \left( \frac{an}{ak} \right) \mod q.
\]

Therefore

\[
\left( \frac{an}{ak} \right) \equiv (-1)^{ak} \left( \frac{a(b - n + k)}{ak} \right) = (-1)^{ak} \left( \frac{a(b - n + k)}{a(b - n)} \right)
\]

\[
\equiv (-1)^{ak} (-1)^{s(b-n)} \left( \frac{a(n - k + b - n)}{a(b - n)} \right) = (-1)^{a(n+k)} \left( \frac{a(b - k)}{a(b - n)} \right) \mod q.
\]

\[\square\]
Example. For $q = 71$, $a = 10$ and $b = 7$, the matrix \[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 14 & 1 & 0 & 0 & 0 & 0 \\
1 & 16 & 16 & 1 & 0 & 0 & 0 \\
1 & 48 & 65 & 48 & 1 & 0 & 0 \\
1 & 16 & 65 & 65 & 16 & 1 & 0 \\
1 & 14 & 16 & 48 & 16 & 14 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}
\] modulo $q$ is

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

Proposition 4. For $0 \leq n \leq q - 2$, define the functions $\rho_n : \mathbb{Z} \rightarrow \mathbb{Z}$ by
\[
\rho_n(m) = \# \{ u : 2 \leq u \leq q - 1 \text{ and } u^{n+1} - u^n + m \equiv 0 \mod q \}.
\]
Then \[
\sum_{l=0}^{q-2} \binom{(n+1)l - 1}{l} m^l \equiv \rho_n(m) - 1 \mod q.
\]
Proof. (Compare with [4], page 9.) For $0 \leq n \leq q - 2$ and $1 \leq l \leq q - 2$,
\[
\sum_{u=2}^{q-1} (1 - u)^{-l} u^{-n} m^l \equiv \sum_{u=1}^{q-1} (-1)^l (1 - u^{-1})^{q-1-i} u^{-(n+1)l}
\]
\[
= \sum_{u=1}^{q-1} (-1)^l u^{-(n+1)l} \sum_{i=0}^{q-2} (-1)^i \binom{q-1-l}{i} u^{-i}
\]
\[
= \sum_{i=0}^{q-2} (-1)^{l+i} \binom{q-1-l}{i} \sum_{u=1}^{q-1} u^{-i-(n+1)l} u^{-1}
\]
\[
= (-1)^n \left( \frac{q-1-l}{q-1-(n+1)l} \right) \equiv -\binom{(n+1)l - 1}{l} \mod q.
\]
The last congruence holds by Lemma 1. Therefore, for $m \in \mathbb{Z} - q\mathbb{Z}$,
\[
\sum_{l=0}^{q-2} \binom{(n+1)l - 1}{l} m^l \equiv 1 - 2 - \sum_{u=2}^{q-1} \sum_{l=0}^{q-2} (1 - u)^{-1} u^{-n} m^l
\]
\[
\equiv -1 - (q-1) \# \{ u : 2 \leq u \leq q - 1 \text{ and } m \equiv (1-u)u^n \mod q \}
\]
\[
\equiv -1 + \rho_n(m) \mod q. \quad \Box
\]

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
\[
e(q) = \begin{cases}
1 & \text{if } q \equiv 1 \mod 3, \\
-1 & \text{if } q \equiv -1 \mod 3.
\end{cases}
\]
For $0 \leq l \leq q - 2$,
\[
\binom{(q-1)l}{l} \equiv (-27)^l e(q) \left( \frac{2q + e(q)}{3} l + 1 \right) + \left( \frac{q + 2e(q)}{3} l + 1 \right) \mod q.
\]
Proof. Call \(e = e(q)\). Suppose first that \(q = \frac{2k-3}{2} \leq l \leq q-2\). Then (see [1], page 822)

\[
(-27)^l e \left( \frac{2q+e+1}{2l+1} + \frac{q+2e+1}{2l+1} \right) \equiv (-27)^l e \left( \frac{2q+e+1}{2l+1} - q \right) + 0
\]

\[
= \frac{(-27)^l e}{(2l+1)(2l) \ldots (q+1)} \times [(e/3) + l((e/3) + l - 1) \ldots ((e/3) - (q+1)/2)] \times ((e/3) - l)((e/3) - (l - 1)) \ldots ((e/3) - (q+1)/2)
\]

\[
= (-27)^l e \left( (1/3)^2 - l^2 \right)((1/3)^2 - (l - 1)^2) \ldots ((1/3)^2 - (q+1)/2)^2
\]

\[
(2l+1)(2l) \ldots (q+1)
\]

\[
= 3^l e(-1)^{\frac{q+1}{2}} \left( (3l)^2 - 1 \right)((3l - 1)^2 - 1) \ldots ((q+1)/2)^2 - 1
\]

\[
(2l+1)(2l) \ldots (q+1)
\]

\[
= \frac{(-3)^{\frac{q+1}{2}} e}{(2l+1)(2l) \ldots (q+1)} \times [(3l)^2 - 1]((3l - 1)^2 - 1) \ldots ((q+1)/2)^2 - 1
\]

\[
(3l)^2 - 1
\]

\[
\equiv (3l + 1)^l \mod q
\]

\[
(\text{note that if } \left[ \frac{2(q-1)}{3} \right] < l \leq q-2, \text{ then } \left( \frac{3l + 1}{l} \right) \equiv (3l^l^{-1}) = 0 \mod q).
\]

Suppose now that \(0 \leq l \leq \frac{q-3}{2}\). Then

\[
(-27)^l e \left( \frac{2q+e+1}{2l+1} + \frac{q+2e+1}{2l+1} \right)
\]

\[
= (-27)^l e \left( (e/3)^2 - l^2 \right)((e/3)^2 - (l - 1)^2) \ldots ((e/3)^2 - (q+1)/2)^2
\]

\[
(2l+1)!
\]

\[
+ (2e/3)^2 - l^2 \right)((2e/3)^2 - (l - 1)^2) \ldots ((2e/3)^2 - (q+1)/2)^2
\]

\[
(2l+1)!
\]

\[
= 3^{l-1} \left( (3l)^2 - 1 \right)((3l - 1)^2 - 1) \ldots (3^2 - 1)
\]

\[
(2l+1)!
\]

\[
+ (3l)^2 - 2^2 \right)((3l - 1)^2 - 2^2) \ldots (3^2 - 2^2)^2
\]

\[
(2l+1)!
\]

\[
= \frac{1}{3} \left( (3l + 1) + (3l + 2) \right) \left( \frac{3l!}{(2l+1)!!} \right) \equiv (3l^l^{-1}) \mod q
\]

\[
(\text{note that if } \left[ \frac{q+1}{2} \right] < l \leq q-2, \text{ then } \left( \frac{q}{l} \right) \equiv (3l^l^{-1}) = 0 \mod q).
\]

\[
\square
\]

Proposition 5. Let \(\rho_n\) be as in Proposition 4. For \(m \in \mathbb{Z} - q\mathbb{Z}\), we have

\[
(35) \quad \rho_1(m) = 1 + \left( \frac{1 - 4m}{q} \right),
\]

where \(\left( \frac{e}{q} \right)\) is the Legendre symbol.
Let $e(q)$ be as in (34). For $m \in \mathbb{Z} - q\mathbb{Z}$, we have

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

(36)

That is:

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

$$
\rho_2(m) = 1 + \frac{1}{2} \left( 1 + \left( \frac{M^2 + M}{q} \right) \right)
\times \left( \left( \frac{M^2 + M\sqrt{M^2 + M}}{q} \right)^3 + \left( \frac{M^2 - M\sqrt{M^2 + M}}{q} \right)^3 \right)
$$

(37)

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

Here $\left( \frac{b}{q} \right)_3 = \zeta_3^{k_b} \equiv b^{2^{\frac{q-1}{3}} \mod q}$, for $b \in \mathbb{Z}(q) - q\mathbb{Z}(q)$.

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

$$
\rho_2(m) = 1 + \left( \frac{b + a\sqrt{3}}{q} \right)^3 + \left( \frac{b - a\sqrt{3}}{q} \right)^3 = \begin{cases} 0 & \text{if } \left( \frac{b + a\sqrt{3}}{q} \right)^3 \not\equiv 1, \\
3 & \text{if } \left( \frac{b + a\sqrt{3}}{q} \right)^3 = 1. \end{cases}
$$

(38)

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

$$
\rho_2(m) = 1 + \left( \frac{a + b\sqrt{3}}{q} \right)^3 + \left( \frac{a - b\sqrt{3}}{q} \right)^3 = \begin{cases} 0 & \text{if } \left( \frac{a + b\sqrt{3}}{q} \right)^3 \not\equiv 1, \\
3 & \text{if } \left( \frac{a + b\sqrt{3}}{q} \right)^3 = 1. \end{cases}
$$

(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

$$
S = \frac{1}{2} \left( \left( \frac{1 + M}{q} \right) + e \left( \frac{M}{q} \right) \right) \left( (\sqrt{1 + M} + \sqrt{M})^{\frac{q}{2}} + (\sqrt{1 + M} - \sqrt{M})^{\frac{q}{2}} \right).
$$
We have that
\[
S = \frac{1}{2} \left( \frac{u + u^{-1}}{2} \right) ^{q - 1} + e \left( \frac{u - u^{-1}}{2} \right) ^{q - 1} \left( u \frac{q + e}{3} + u^{-\frac{q + e}{3}} \right)
\]
\[
\equiv \frac{1}{2} \left( \sum_{k=0}^{q-1} (-1)^k u^{q-1-k} u^{-k} + e \sum_{k=0}^{q-1} u^{q-1-k} u^{-k} \right) \left( u \frac{q + e}{3} + u^{-\frac{q + e}{3}} \right)
\]
\[
\equiv \sum_{k=0}^{q-1} \frac{(-1)^k}{2} u^{q-1-2k} \left( u \frac{q + e}{3} + u^{-\frac{q + e}{3}} \right)
\]
\[
= e \frac{u^{q+e} - u^{-(q+e)}}{u^2 - u^{-2}} \left( u \frac{q + e}{3} + u^{-\frac{q + e}{3}} \right) \mod q.
\]
That is,
\[
S \equiv \frac{e}{4 \sqrt{M+M^2}} \left( (\sqrt{1+M} + \sqrt{M})^{\frac{4q+2e}{3}} - (\sqrt{1+M} - \sqrt{M})^{\frac{4q+2e}{3}} \right)
\]
\[
+ (\sqrt{1+M} + \sqrt{M})^{\frac{2q+4e}{3}} - (\sqrt{1+M} - \sqrt{M})^{\frac{2q+4e}{3}} \right) \mod q.
\]
But for any positive integer \( n \), we have
\[
\frac{1}{2 \sqrt{M+M^2}} \left( (\sqrt{1+M} + \sqrt{M})^{2n} - (\sqrt{1+M} - \sqrt{M})^{2n} \right)
\]
\[
= \sum_{l=0}^{n-1} M^{n-1-l} \sum_{k=0}^{n-1} \binom{2n}{2k+1} \binom{k}{l}
\]
\[
= \sum_{l=0}^{n-1} 2^{2n-2l-1} \binom{2n-l-1}{l} M^{n-1-l} = \sum_{l=0}^{n-1} 2^{2l} \binom{n+l}{2l} M^l
\]
(for the second identity see, if necessary, [12], Section 4.3 and formula (2.5.7)).

Hence
\[
S \equiv \sum_{l=0}^{\frac{2q+2e-1}{3}} 2^{2l} \binom{\frac{2q+e}{3} + l}{2l+1} M^l + \sum_{l=0}^{\frac{q-2}{3}} 2^{2l} \binom{\frac{q+2e}{3} + l}{2l+1} M^l
\]
\[
= \sum_{l=0}^{q-1} (-27)^l \left( \frac{2q+e}{3} + l \right) + \binom{\frac{q+2e}{3} + l}{2l+1} M^l \mod q.
\]
Therefore, by Lemma 2 and Proposition 4, \( S \equiv \sum_{l=0}^{q-2} \binom{[3l]}{l} m^l \equiv \rho_2(m) - 1 \mod q \). This proves congruence (36).

In order to prove the next equalities, suppose first that \( q \equiv 1 \mod 3 \). Then, by (36),
\[
\rho_2(m) \equiv 1 + \frac{1}{2} \left( \left( \frac{1+M}{q} \right) + \left( \frac{M}{q} \right) \right)
\]
\[
\times \left( \left( \sqrt{1+M} + \sqrt{M} \right)^{\frac{q+1}{3}} + \left( \sqrt{1+M} - \sqrt{M} \right)^{\frac{q+1}{3}} \right)
\]
\[
\equiv 1 + \frac{1}{2} \left( 1 + \left( \frac{M^2+M}{q} \right) \right) \left( \left( M^2 + M \sqrt{M^2+M} \right)^{\frac{q+1}{3}} + \left( M^2 - M \sqrt{M^2+M} \right)^{\frac{q+1}{3}} \right) \mod q.
\]
This congruence must be interpreted as follows: If \( M^2 + M \equiv a^2 \mod q \) 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 \( \rho_2(m) \equiv 1 \mod q \). Formula (37) follows from this and from the fact that \( 0 \leq \rho_2(m) \leq 3 \).

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

\[
\rho_2(m) \equiv 1 + \frac{1}{2} \left( \left( \frac{1+M}{q} \right) - \left( \frac{M}{q} \right) \right) \left( \left( \sqrt{1+M} + \sqrt{M} \right)^{\frac{q+1}{2}} + \left( \sqrt{1+M} - \sqrt{M} \right)^{\frac{q+1}{2}} \right) \mod q.
\]

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

\[
\rho_2(m) \equiv 1 + \left( (b+a\sqrt{-3})^{\frac{q+1}{2}} + (b-a\sqrt{-3})^{\frac{q+1}{2}} \right) \equiv 1 + \left( (b+a\sqrt{-3})^{\frac{q-1}{2}} + (b-a\sqrt{-3})^{\frac{q-1}{2}} \right) \mod q.
\]

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

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

**Theorem 1.** Let \( \rho_n \) be as in Proposition 4. For \( 1 \leq n \leq p-2 \) and \( 0 \leq k \leq p-1 \),

\[
(40) \quad d_{n,k} = f - \sum_{a=0}^{f-1} \rho_n(s^{k+pa}) = f - \# \{ u : 2 \leq u \leq q-1 \ and \ (u^{n+1} - u^n)f - s/fk \equiv 0 \mod q \}.
\]

For \( 0 \leq k \leq p-1 \),

\[
(41) \quad d_{1,k} = - \sum_{a=0}^{f-1} \left( 1 - 4s^{k+pa} \right) \mod q.
\]

That is, \( d_{1,k} = \) number of quadratic nonresidues \( \mod q \) - number of quadratic residues \( \mod q \), in the set \( \{ 1 - 4s^{k+pa} : 0 \leq a \leq f-1 \} \) (do not count 0 as a quadratic residue \( \mod q \)).
Let $e(q)$ be as in (34). Define the function $\lambda : \mathbb{Z} - q\mathbb{Z} \rightarrow \mathbb{Z}$ by $\lambda(m) =$

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

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

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

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

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

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

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

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

In particular

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

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


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