Michigan Math. J. 50 (2002)

On Gaussian Periods That Are Rational Integers

F. Thaine

1. Preliminaries

Let $p \geq 3$ be a prime number, ζ_p a pth primitive root of 1, and Δ the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Let $q \neq p$ be a prime number, ζ_q a qth primitive root of 1, and n the order of q modulo p. Assume that $q \not\equiv 1 \bmod p$. Hence $n \geq 2$, $p(q-1) \mid q^n - 1$, and $n \mid p-1$. Set $f = (q^n - 1)/p$ and $e = (p-1)/n$. Let Q be a prime ideal of $\mathbb{Z}[\zeta_p]$ above q and let $\mathbb{F} = \mathbb{Z}[\zeta_p]/Q$. Thus $\mathbb{F} \simeq \mathbb{F}_{q^n}$, the finite field with q^n elements. Let $\alpha \in \mathbb{Z}[\zeta_p]$ be a generator of $\mathbb{F}^\times$ such that $\alpha^f \equiv \zeta_p \bmod Q$, and let T be the trace from $\mathbb{F}$ to $\mathbb{F}_q$. In this paper we study the Gaussian periods η_i $(0 \leq i \leq p-1)$ defined by

$$\eta_i = \sum_{j=0}^{f-1} \zeta_q^{T(\alpha^{i+pj})}, \tag{1}$$

as well as the Gauss sum

$$G = \sum_{i=0}^{q^n-2} \zeta_p^i \zeta_q^{T(\alpha^i)} = \sum_{i=0}^{p-1} \eta_i \zeta_p^i. \tag{2}$$

Some basic definitions and results are given in this section. A short review of the cyclotomic numbers of order e corresponding to p is given in Section 2. Those numbers will play an important role in Section 4. In Section 3 we show applications of the periods η_i to the study of indices of cyclotomic units in $\mathbb{Z}[\zeta_p]$ (with respect to Q and α) and of the orders of certain components of the ideal class group of $\mathbb{Q}(\zeta_p)$. More precisely, let A be the p-part of the ideal class group of $\mathbb{Q}(\zeta_p)$, $\mathbb{Z}_p$ the ring of p-adic integers, and $\omega\colon \Delta \to \mathbb{Z}_p^\times$ the Teichmüller character; in Section 3 we study the ω^{p-ln}-components of A for n and l odd, $1 \leq l \leq e-1$ (see the definitions in Section 3). In Section 4 we show an efficient method to calculate the periods η_i, based on the Gross–Koblitz formula and on properties of the cyclotomic numbers of order e corresponding to p; in Section 5 we give a MAPLE program to perform such calculations. I am grateful to Hershy Kisilevsky and John McKay for some valuable comments.

We start with a simple proof of the known result (see [6, Thm. 4]) that, under the stated hypothesis, the η_i are rational integers and so $G \in \mathbb{Z}[\zeta_p]$. In fact, G belongs to the only subfield of degree e of $\mathbb{Q}(\zeta_p)$ and is divisible by a (sometimes large) power of q.

Received March 15, 2001. Revision received December 17, 2001.
This work was supported in part by grants from NSERC and FCAR.

For $0 \leq i \leq p-1$ and $k \in \mathbb{Z}$, define $\eta_{i+kp} = \eta_i$. Let $s \in \mathbb{Z}$ be a primitive root modulo q such that $s \equiv \alpha^{(q^n-1)/(q-1)} \bmod Q$, and let τ be the automorphism of $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ such that $\tau(\zeta_q) = \zeta_q^s$. For any i, we have

$$\tau(\eta_i) = \sum_{j=0}^{f-1} \zeta_q^{sT(\alpha^{i+pj})} = \sum_{j=0}^{f-1} \zeta_q^{T(s\alpha^{i+pj})} = \sum_{j=0}^{f-1} \zeta_q^{T(\alpha^{p(q^n-1)/(p(q-1))+i+pj})} = \eta_i.$$

Since τ generates $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, this proves that $\eta_i \in \mathbb{Z}$. Note also that $\eta_{qi} = \sum_{j=0}^{f-1} \zeta_q^{T(\alpha^{qi+pj})} = \sum_{j=0}^{f-1} \zeta_q^{T(\alpha^{qi+pqj})}$. So, for $i \in \mathbb{Z}$, we have

$$\eta_{qi} = \eta_i. \tag{3}$$

Set $G(x) = \sum_{i=0}^{q^n-2} x^i \zeta_q^{T(\alpha^i)}$, where x is an indeterminate. Hence

$$G(x) \equiv \sum_{i=0}^{p-1} \eta_i x^i \mod (x^p - 1). \tag{4}$$

We have that $G = G(\zeta_p)$, and it is easy to see that

$$G(1) = \sum_{i=0}^{p-1} \eta_i = -1. \tag{5}$$

For $1 \leq i \leq p-1$, we have

$$G(\zeta_p^i) G(\zeta_p^{-i}) = q^n \tag{6}$$

(see [5, GS 2, p. 4] or [14, Lemma 6.1]).

If n is even then $G = q^{n/2}$. In fact, in this case we have by (3) that $\eta_{-i} = \eta_{q^{n/2}i} = \eta_i$. Therefore $G(\zeta_p^i) = G(\zeta_p^{-i})$ and, by (6), $G = \pm q^{n/2}$. The result now follows from (5) (work modulo $\zeta_p - 1$). We assume from now on that n is odd.

Let g be a primitive root modulo p and let $\sigma \in \Delta$ be the automorphism such that $\sigma(\zeta_p) = \zeta_p^g$. Thus σ is a generator of Δ. Note that $e = (p-1)/n$ is even. Define the numbers (also Gaussian periods) θ_i, $0 \leq i \leq e-1$, by

$$\theta_i = \sum_{l=0}^{n-1} \zeta_p^{g^{i+el}}. \tag{7}$$

We have that $\{\theta_0, \theta_1, \ldots, \theta_{e-1}\}$ is a normal integral basis over $\mathbb{Q}$ of $\mathbb{Q}(\theta_0)$, the subfield of $\mathbb{Q}(\zeta_p)$ of degree e. Clearly $\sum_{i=0}^{e-1} \theta_i = -1$. For $0 \leq i, j \leq e-1$, define the integers $c_{i,j}$ by

$$\theta_0 \theta_i = \sum_{j=0}^{e-1} c_{i,j} \theta_j; \tag{8}$$

for i, j as before and $k, l \in \mathbb{Z}$, define $\theta_{i+ke} = \theta_i$ and $c_{i+ke, j+le} = c_{i,j}$.

Since n is the order of q modulo p we have that $g^e \equiv q^t \bmod p$ for some integer t relatively prime to n. Hence, by (3),

$$\eta_{g^{i+e}} = \eta_{g^i} \tag{9}$$

for $i \geq 0$. We therefore have that

$$G(\zeta_p) = \eta_0 + \sum_{i=0}^{p-2} \eta_{g^i} \zeta_p^{g^i} = \eta_0 + \sum_{i=0}^{e-1} \eta_{g^i} \sum_{j=0}^{n-1} \zeta_p^{g^{i+ej}}.$$

That is,

$$G(\zeta_p) = \eta_0 + \sum_{i=0}^{e-1} \eta_{g^i} \theta_i. \tag{10}$$

In particular, we have

$$G(\zeta_p^{g^e}) = \sigma^e(G(\zeta_p)) = G(\zeta_p). \tag{11}$$

Given an integer a, denote by $|a|_p$ the smallest nonnegative residue of a modulo p. The prime ideal factorization of $(G(\zeta_p^{-1}))$ in $\mathbb{Z}[\zeta_p]$ is

$$(G(\zeta_p^{-1})) = \prod_{k=0}^{p-2} \sigma^{-k}(Q)^{|g^k|_p/p} = \prod_{k=0}^{e-1} \sigma^{-k}(Q)^{(1/p)\sum_{l=0}^{n-1}|g^{k+el}|_p} \tag{12}$$

(see [5, FAC 1, p. 12). Note that σ^e generates the decomposition group of Q over $\mathbb{Q}$; in particular, $\sigma^e(Q) = Q$. The numbers $\frac{1}{p}\sum_{l=0}^{n-1}|g^{k+el}|_p$ $(0 \leq k \leq e-1)$ are positive integers, as is easy to check. Let q^ν be the largest power of q dividing $G(\zeta_p)$. It follows from (12) that

$$\nu = \min_{0 \leq k \leq e-1} \frac{1}{p} \sum_{l=0}^{n-1} |g^{k+el}|_p. \tag{13}$$

Clearly $\nu \geq 1$.

By (10), $G(\zeta_p) = \sum_{i=0}^{e-1}(\eta_{g^i} - \eta_0)\theta_i$. Since $q^\nu \mid G(\zeta_p)$, it follows that $q^\nu \mid (\eta_{g^i} - \eta_0)$. Define

$$H = \frac{G(\zeta_p)}{q^\nu} \quad \text{and} \quad d_i = \frac{\eta_{g^i} - \eta_0}{q^\nu} \quad (0 \leq i \leq e-1). \tag{14}$$

Note that the d_i are integers. For $0 \leq i \leq e-1$ and $k \in \mathbb{Z}$, define $d_{i+ke} = d_i$. We have

$$H = \sum_{i=0}^{e-1} d_i \theta_i \quad \text{and} \quad H\bar{H} = q^{n-2\nu} \tag{15}$$

(by (6)), where the bar denotes complex conjugation. From (5) and (14) we obtain

$$\eta_0 = -\frac{1}{p}\left(1 + nq^\nu \sum_{j=0}^{e-1} d_j\right), \qquad \eta_{g^i} = q^\nu d_i + \eta_0 \quad \text{for } 0 \leq i \leq e-1. \tag{16}$$

In Section 4 we describe an efficient algorithm to calculate the integers d_i and therefore the periods η_i. The formula in the following proposition can be used to calculate the η_i for small values of p and q. We use the following version of Kronecker's delta:

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i \equiv j \bmod q, \\ 0 & \text{if } i \not\equiv j \bmod q. \end{cases}$$

PROPOSITION 1. *For* $0 \le i \le p-1$, *let* b_i *be the number of elements of trace* 0 *in the set* $\left\{\alpha^{i+pl} : 0 \le l \le \frac{q^n-1}{p(q-1)} - 1\right\} \subseteq \mathbb{F}^\times$; *then* $\eta_i = -\frac{q^n-1}{p(q-1)} + qb_i$. *Therefore*, $G = q\sum_{i=0}^{p-1} b_i \zeta_p^i$.

Proof. Let $w = \frac{q^n-1}{p(q-1)}$. From (1) we have

$$\begin{aligned}\eta_i &= \sum_{l=0}^{w-1}\sum_{j=0}^{q-2} \zeta_q^{T(\alpha^{i+p(l+jw)})} = \sum_{l=0}^{w-1}\sum_{j=0}^{q-2} \zeta_q^{T(s^j\alpha^{i+pl})} = \sum_{l=0}^{w-1}\sum_{j=0}^{q-2} \zeta_q^{s^jT(\alpha^{i+pl})} \\ &= \sum_{l=0}^{w-1}\sum_{j=0}^{q-2} \tau^j(\zeta_q^{T(\alpha^{i+pl})}) = \sum_{l=0}^{w-1} T_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(\zeta_q^{T(\alpha^{i+pl})}) = \sum_{l=0}^{w-1}(-1 + q\delta_{T(\alpha^{i+pl}),0}) \\ &= -w + q\sum_{l=0}^{w-1}\delta_{T(\alpha^{i+pl}),0} = -w + qb_i. \qquad \square\end{aligned}$$

Note that, by the additive form of Hilbert Theorem 90,

$$b_i = \left\{l : 0 \le l \le \tfrac{q^n-1}{p(q-1)} - 1 \text{ and } \alpha^{i+pl} = \alpha^m - \alpha^{qm} \text{ for some } m \in \mathbb{Z}\right\}.$$

COROLLARY. *Suppose that* q *divides* $p-1$. *Let* $w = \frac{q^n-1}{p(q-1)}$. *Then, for* $0 \le i \le p-1$, $\eta_i \equiv -w - q\sum_{l=0}^{w-1}\sum_{k=1}^{p-1} k^{((p-1)/q)T(\alpha^{i+pl})} \bmod p$.

Proof. By Proposition 1 we have $\eta_i = -w + q\sum_{l=0}^{w-1}\delta_{T(\alpha^{i+pl}),0}$. On the other hand, we have $\sum_{k=1}^{p-1} k^{((p-1)/q)T(\alpha^{i+pl})} \equiv -\delta_{T(\alpha^{i+pl}),0} \bmod p$. The corollary follows. $\square$

OBSERVATION. In order to actually calculate the periods η_i using Proposition 1, one needs to find traces (from $\mathbb{F}$ to $\mathbb{F}_q$) of powers of α. To calculate such traces, one can proceed as follows. Find an irreducible factor $f(x)$ of the cyclotomic polynomial $\Phi_{q^n-1}(x)$ modulo q. Regard $f(x)$ as the irreducible polynomial of α over $\mathbb{F}_q$. The trace of α^k is the remainder, modulo q, of the division of $\sum_{j=0}^{n-1} x^{kq^j}$ by $f(x)$.

By taking conjugates in (8), we obtain

$$\theta_i\theta_j = \sum_{k=0}^{e-1} c_{j-i,k-i}\theta_k. \tag{17}$$

By (15) and (17) we have

$$\begin{aligned}q^{n-2\nu} = H\bar{H} &= \sum_{i=0}^{e-1} d_i\theta_i \sum_{j=0}^{e-1} d_j\theta_{j+e/2} = \sum_{i=0}^{e-1}\sum_{j=0}^{e-1} d_i d_{j+e/2}\theta_i\theta_j \\ &= \sum_{i=0}^{e-1}\sum_{j=0}^{e-1} d_i d_{j+e/2}\sum_{k=0}^{e-1} c_{j-i,k-i}\theta_k = \sum_{k=0}^{e-1}\left(\sum_{i=0}^{e-1}\sum_{j=0}^{e-1} c_{j-i,k-i} d_i d_{j+e/2}\right)\theta_k.\end{aligned}$$

Hence, for $0 \le k \le e-1$,

$$q^{n-2\nu} = -\sum_{i=0}^{e-1}\sum_{j=0}^{e-1} c_{j+e/2-i,k-i} d_i d_j. \tag{18}$$

By (4) we have that, for $a \in \mathbb{Z}$, $\sum_{k=0}^{p-1} \zeta_p^{ak} G(\zeta_p^{-k}) = \sum_{i=0}^{p-1} \eta_i \sum_{k=0}^{p-1} \zeta_p^{(a-i)k} = p\eta_a$. Thus

$$\eta_a = \frac{1}{p}\sum_{k=0}^{p-1} \zeta_p^{ak} G(\zeta_p^{-k}). \tag{19}$$

By (6), (19), and the triangle inequality, if $p \nmid a$ then we have

$$\begin{aligned}
|\eta_a - \eta_0| &\le \frac{1}{p}\sum_{k=1}^{p-1} |\zeta_p^{ak} - 1||G(\zeta_p^{-k})| = \frac{q^{n/2}}{p}\sum_{k=1}^{p-1}|\zeta_p^k - 1| \\
&= \frac{q^{n/2} 2\sqrt{2}}{p}\sum_{k=1}^{(p-1)/2}\sqrt{1-\cos(2k\pi/p)} \\
&< q^{n/2}\left(\frac{2}{p} + 2\sqrt{2}\int_0^{1/2}\sqrt{1-\cos(2\pi x)}\,dx\right) = q^{n/2}\left(\frac{2}{p}+\frac{4}{\pi}\right).
\end{aligned}$$

We conclude that, for example,

$$|\eta_a - \eta_0| < 1.32 q^{n/2}$$

$\big($true for $p > 50$ by the preceding formula and true for $p < 50$ by direct calculation of $\frac{1}{p}\sum_{k=1}^{(p-1)/2}\sqrt{1-\cos(2k\pi/p)}\big)$. Consequently, for $0 \le i \le e-1$,

$$\begin{aligned}
|d_i| &= \frac{|\eta_{g^i} - \eta_0|}{q^\nu} < 1.32 q^{n/2-\nu} \\
&< \begin{cases} \frac{1}{2} q^{(n+1)/2+1-\nu} & \text{if } q = 2 \text{ or } q = 3 \text{ or } q = 5, \\ \frac{1}{2} q^{(n+1)/2-\nu} & \text{if } q \ge 7. \end{cases}
\end{aligned} \tag{20}$$

Observation. It is a simple calculus exercise to prove that, in fact,

$$\frac{1}{p}\sum_{k=1}^{(p-1)/2}\sqrt{1-\cos(2k\pi/p)} < \frac{\sqrt{2}}{\pi},$$

but we do not need this result.

Clearly, by (19) we also have that, for $a \in \mathbb{Z}$,

$$|\eta_a| \le \frac{1}{p}(1 + (p-1)q^{n/2}) < q^{n/2}.$$

By (5), (11), and (19) we have

$$\eta_a = \frac{1}{p}\left(-1+\sum_{j=0}^{p-2}\zeta_p^{ag^j}G(\zeta_p^{-g^j})\right)$$
$$= \frac{1}{p}\left(-1+\sum_{j=0}^{e-1}\sum_{k=0}^{n-1}\zeta_p^{ag^{j+ek}}G(\zeta_p^{-g^j})\right).$$

As a result,

$$\eta_0 = \frac{1}{p}\left(-1+\sum_{j=0}^{e-1} nG(\zeta_p^{-g^j})\right)$$

and, for $i \geq 0$,

$$\eta_{g^i} = \frac{1}{p}\left(-1+\sum_{j=0}^{e-1}\sum_{k=0}^{n-1}\zeta_p^{g^{i+j+ek}}G(\zeta_p^{-g^j})\right) = \frac{1}{p}\left(-1+\sum_{j=0}^{e-1}\theta_{i+j}G(\zeta_p^{-g^j})\right).$$

Hence, for $0 \leq i \leq e-1$,

$$d_i = \frac{\eta_{g^i}-\eta_0}{q^\nu} = \frac{1}{p}\sum_{k=0}^{e-1}(\theta_{i+k}-n)\frac{G(\zeta_p^{-g^k})}{q^\nu} = \frac{1}{p}\sum_{k=0}^{e-1}(\theta_{i+k}-n)\sigma^k(\bar{H}). \quad (21)$$

Finally, by (16) we have

$$\sum_{i=0}^{e-1} d_i = -\frac{1+p\eta_0}{nq^\nu} \equiv eq^{n-\nu} \mod p. \quad (22)$$

2. Cyclotomic Numbers of Order e Corresponding to p

In this section p is an odd prime number, n is an odd divisor of $p-1$ (here we allow $n=1$), $e=(p-1)/n$, g is a primitive root modulo p, and θ_i and $c_{i,j}$ are as in (7) and (8). We shall study the cyclotomic numbers (i, j) of order e corresponding to p and their relation with the numbers $c_{i,j}$. (A similar study for the cyclotomic numbers corresponding to the case n even can be found in [13, Sec. 2], though the notation in that article is different: we call there q, n, f, s, and η_i what we call here p, e, n, g, and θ_i, respectively. Note that in this article, where we are working with more objects, the symbols q, n, f, s, and η_i already have a meaning.) Let

$$C = [c_{i,j}]_{0\leq i,j\leq e-1}. \quad (23)$$

We will give a simple characterization of C that is, in fact, a variation of [11, Thm. 1], and we will show how to calculate C in an efficient way. This complements results in [13, Sec. 2].

For $0 \leq i, j \leq e-1$ we denote by (i, j) the cyclotomic number of order e, which is defined as the number of ordered pairs of integers $\langle k, l\rangle$ $(0 \leq k, l \leq n-1)$

such that $1+g^{ke+i} \equiv g^{le+j} \bmod p$. (See e.g. [1, Chap. 2, Sec. 2], [2], or [8].) Define $\theta_{i+ke} = \theta_i$, $c_{i+ke,j+le} = c_{i,j}$, and $(i+ke, j+le) = (i, j)$ for $0 \le i, j \le e-1$ and $k, l \in \mathbb{Z}$. We have $(i, j) = (j+e/2, i+e/2)$ and $(i, j) = (-i, j-i)$ (see [2, formula (15)]).

In this section we use the following version of Kronecker's delta:

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i \equiv j \bmod e, \\ 0 & \text{if } i \not\equiv j \bmod e. \end{cases}$$

By (8) and [2, formula (6)] we have, for $i, j \in \mathbb{Z}$,

$$c_{i,j} = (i, j) - n\delta_{e/2,i}. \tag{24}$$

Since $\theta_i\theta_j = \theta_j\theta_i$, it follows from (17) that $\theta_i\theta_j = \sum_{k=0}^{e-1} c_{j-i,k-i}\theta_k = \sum_{k=0}^{e-1} c_{i-j,k-j}\theta_k$. This proves that $c_{i,j} = c_{-i,j-i}$. Also from (17) we have

$$C\begin{bmatrix} \theta_j \\ \theta_{j+1} \\ \vdots \\ \theta_{j+e-1} \end{bmatrix} = \theta_j \begin{bmatrix} \theta_j \\ \theta_{j+1} \\ \vdots \\ \theta_{j+e-1} \end{bmatrix}. \tag{25}$$

Therefore the Gaussian periods $\theta_0, \ldots, \theta_{e-1}$ are exactly the eigenvalues of C, and $\det(xI - C)$ is the minimal polynomial of the periods (see also [2, formula (9)]). We have a field isomorphism

$$\mathbb{Q}(\theta_0) \simeq \mathbb{Q}(C), \quad \theta_0 \mapsto C.$$

Let

$$R = \begin{bmatrix} \theta_0 & \theta_{e-1} & \ldots & \theta_1 \\ \theta_1 & \theta_0 & \ldots & \theta_2 \\ \vdots & \vdots & \ddots & \vdots \\ \theta_{e-1} & \theta_{e-2} & \ldots & \theta_0 \end{bmatrix} \tag{26}$$

(a circulant matrix), and let K be the $e \times e$ matrix $[\delta_{i+1,j}]_{i,j}$; that is,

$$K = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix}. \tag{27}$$

It follows from (25) that

$$R^{-1}CR = \mathrm{diag}[\theta_0, \theta_{e-1}, \theta_{e-2}, \ldots, \theta_1]. \tag{28}$$

(We have that $R^{-1} = (1/p)(R^t - nE)K^{e/2}$, where E is the $e \times e$ matrix with all entries equal to 1.) Since circulant matrices commute with one another, we can conclude from (28) that $R^{-1}(K^{-i}CK^i)R = \mathrm{diag}[\theta_i, \theta_{i-1}, \ldots, \theta_{i-(e-1)}]$. Therefore, the matrices $K^{-i}CK^i$ $(0 \le i \le e-1)$ are simultaneously diagonalizable, and if we identify θ_0 with C as before then we must identify θ_i with $K^{-i}CK^i$. In particular, for all integers i we have

$$(K^{-i}CK^{i})C = C(K^{-i}CK^{i}). \tag{29}$$

Observe that the entry i, j of $K^{-l}CK^{l}$ is $c_{i-l,j-l}$.

In [11, Thm. 1] we give a list of properties that characterize the matrix C, which are equivalent to the following (see the observation at the end of [11]). Let K be as in (27). Denote by $[B]_i$ the ith row of a matrix B (starting from $i = 0$). Then C is a matrix with entries in $\mathbb{Z}$ such that:

(a) the sum of the elements of the ith row of C is $n - p\delta_{e/2,i}$;
(b) the sum of the elements of the jth column of C is $-\delta_{0,j}$;
(c) $[K^{-k}CK^{k}]_l = [K^{-l}CK^{l}]_k$ for $0 \le k, l \le e-1$;
(d) $[CK^{-k}CK^{k}]_l = [CK^{-l}CK^{l}]_k$ for $0 \le k, l \le e-1$; and
(e) $\det(xI - C)$ is irreducible over $\mathbb{Q}$.

These properties characterize C (up to some relabeling of the periods in formula (7), due to the choice of g), and property (c) together with formula (29) imply property (d) (since (c) implies that $[(K^{-k}CK^{k})C]_l = [(K^{-l}CK^{l})C]_k$). Also, (c) is equivalent to the equalities $c_{i,j} = c_{-i,j-i}$. We therefore have the following result.

PROPOSITION 2. *Let K be as in* (27). *The matrix $C = [c_{i,j}]_{0\le i,j\le e-1}$ is characterized* (*up to some relabeling of the periods in formula* (7), *due to the choice of g*) *by the following properties*: *it is a matrix with entries in $\mathbb{Z}$ such that, for all* $0 \le i, j \le e-1$,

(i) *the sum of the elements of its i*th *row is $n - p\delta_{e/2,i}$*,
(ii) *the sum of the elements of its j*th *column is $-\delta_{0,j}$*,
(iii) $c_{i,j} = c_{-i,j-i}$ (*indices modulo e*),
(iv) $C(K^{-i}CK^{i}) = (K^{-i}CK^{i})C$, *and*
(v) *the polynomial* $\det(xI - C)$ *is irreducible over $\mathbb{Q}$*.

The following proposition shows a congruence modulo p for the cyclotomic numbers (i, j)—which is a variation of a congruence first found by Lebesgue—and an inequality that together allow the efficient calculation of those numbers. The proof uses standard properties of Jacobi sums and a formula relating them to cyclotomic numbers, and it is similar to the proof of the corollary of Proposition 3 in [13, Sec. 2] (which corresponds to the case n even).

PROPOSITION 3. *For* $0 \le i, j \le e-1$,

$$(i, j) \equiv -\frac{1}{e^2}\sum_{k=0}^{e}\sum_{m=0}^{e-1}\binom{nk}{nm} g^{n(mi-kj)} \mod p.$$

Also,

$$|(i, j) - (p-1)/e^2| < \sqrt{p}$$

and so

$$0 \le (i, j) < \sqrt{p} + (p-1)/e^2 < p.$$

Proof. Let ζ_e be a primitive root modulo e. Let $\mathcal{P}$ be the prime in $\mathbb{Z}[\zeta_e]$ above p such that $g^n \equiv \zeta_e \mod \mathcal{P}$. For $a, b \in \mathbb{Z}$, define the Jacobi sum $J(a, b)$ by

$$J(a,b) = -\sum_{k=2}^{p-1} \zeta_e^{a\,\mathrm{ind}_g(k) + b\,\mathrm{ind}_g(1-k)},$$

where $\mathrm{ind}_g(k)$ is the least nonnegative integer such that $g^{\mathrm{ind}_g(k)} \equiv k \bmod p$. We have $J(a,b) = (-1)^{nb} J_{-a-b,b} = (-1)^b J_{-a-b,b}$ for $a, b \in \mathbb{Z}$ (to prove this, use the change of variable $k \mapsto \bar{k}$, where $\bar{k}$ is the inverse of k modulo p in $\{1, 2, \ldots, p-1\}$). Also, $J(a,b) = J(b,a)$ for $a, b \in \mathbb{Z}$; $J(a,b) = 1$ if $e \mid a$ and $e \nmid b$; $J(a,b) = (-1)^a$ if $e \mid (a+b)$ and $e \nmid a$; and $J(0,0) = -(p-2)$.

By [1, Thm. 2.5.1], since n is odd we have

$$(i,j) = -\frac{1}{e^2} \sum_{a=0}^{e-1} \sum_{b=0}^{e-1} (-1)^a \zeta_e^{ia+jb} \overline{J(a,b)},$$

where the bar denotes complex conjugation. By [13, formula (27)] (which holds regardless of the parity of n), if $a + b \not\equiv 0 \bmod e$ then

$$\overline{J(a,b)} \equiv \binom{n|a+b|_e}{na} \bmod \mathcal{P},$$

where $|k|_e$ denotes the least nonnegative residue of an integer k modulo e. Hence, for $0 \le i, j \le e-1$,

$$\begin{aligned}
(i,j) \equiv {} & -\left(\frac{1}{e^2}\right) \sum_{\substack{0 \le a,b \le e-1 \\ a+b \not\equiv 0 \bmod e}} (-1)^a g^{n(ia+jb)} \binom{n|a+b|_e}{na} \\
& - \left(\frac{1}{e^2}\right)\left(-(p-2) + \sum_{a=1}^{e-1} \zeta_e^{(i-j)a}\right) \\
\equiv {} & -\left(\frac{1}{e^2}\right)\left(e\delta_{i,j} + \sum_{a=0}^{e-1} \sum_{b=0}^{e-1} (-1)^a g^{n(ia+jb)} \binom{n|a+b|_e}{na}\right) \bmod \mathcal{P}.
\end{aligned}$$

By [2, formula (15)], we thus have

$$\begin{aligned}
(i,j) &= (j + e/2, i + e/2) = (-j - e/2, i - j) = (i + e/2 - j, -j) \\
&\equiv -\left(\frac{1}{e^2}\right)\left(e\delta_{e/2,i} + \sum_{a=0}^{n-1} \sum_{b=0}^{n-1} (-1)^a g^{n((i+e/2-j)a - jb)} \binom{n|a+b|_e}{na}\right) \\
&\equiv -\left(\frac{1}{e^2}\right)\left(e\delta_{e/2,i} + \sum_{a=0}^{e-1} \sum_{b=0}^{e-1} g^{n(ia-jb)} \binom{nb}{na}\right) \\
&\equiv -\left(\frac{1}{e^2}\right) \sum_{b=0}^{e} \sum_{a=0}^{e-1} g^{n(ia-jb)} \binom{nb}{na} \bmod p.
\end{aligned}$$

(Note that $\binom{p-1}{na} \equiv (-1)^{na} = (-1)^a \bmod p$.)

The inequality $|(i,j) - (p-1)/e^2| < \sqrt{p}$ follows from the triangle inequality and the preceding expression for (i,j) in terms of Jacobi sums, since $|J_{a,b}| = \sqrt{p}$ if $1 \le a, b \le n-1$ and $a + b \ne 0$. This ends the proof of Proposition 3. $\square$

The numbers $\binom{nk}{nm}$ are studied in [12, Lemma 1] and its subsequent example. Proposition 3 will be an important tool in Sections 3 and 4.

3. Indices of Cyclotomic Units and Orders of the ω^{p-ln}-Components of the p-Part of the Ideal Class Group of $\mathbb{Q}(\zeta_p)$ Modulo p

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, $\omega\colon \Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ the Teichmüller character defined by $\omega(k) \equiv k \bmod p$, and e_r $(0 \le r \le p-2)$ the idempotents $\frac{1}{p-1}\sum_{\lambda\in\Delta}\omega^r(\lambda)\lambda^{-1} \in \mathbb{Z}_p[\Delta]$. We have that $A = \bigoplus_{r=1}^{p-2} e_r(A)$. In this section we give a formula (modulo p) for the indices of the cyclotomic units of $\mathbb{Z}[\zeta_p]$, with respect to Q and α, in terms of the periods η_i; we use that formula to study the components $e_{p-ln}(A)$ of A for l odd, $1 \le l \le e-1$.

For $i \in \mathbb{Z}$ such that $i \not\equiv 0 \bmod q^n - 1$, define $\Phi(i)$ as the least positive integer such that

$$1 - \alpha^i = \alpha^{\Phi(i)} \tag{30}$$

in $\mathbb{F}$. Since $\alpha^f \equiv \zeta_p \bmod Q$, this implies that, for $1 \le i \le p-1$,

$$1 - \zeta_p^i \equiv \alpha^{\Phi(fi)} \mod Q. \tag{31}$$

Hence the numbers $\Phi(fi)$ are important in the calculation of indices of cyclotomic units modulo prime ideals in $\mathbb{Q}(\zeta_p)$. The following proposition, which can be regarded as one of Kummer's complementary reciprocity laws (see [4]), gives us the numbers $\Phi(fi)$ modulo p in terms of the Gaussian periods η_i (cf. [12, formulas (14) and (24)]). Note that this gives a formula, modulo p, for the indices of the cyclotomic units of $\mathbb{Z}[\zeta_p]$ (i.e., the units generated by $\pm\zeta_p$ and $1-\zeta_p^i$ for $1 \le i \le p-1$), since $\zeta_p^k \prod_{i=1}^{p-1}(1-\zeta_p^i)^{r_i} \equiv \alpha^{fk+\sum_{i=1}^{p-1} r_i\Phi(fi)} \bmod Q$.

PROPOSITION 4. *For* $1 \le i \le p-1$,

$$\Phi(fi) \equiv \sum_{j=1}^{p-1} j\eta_j\eta_{j+i} \mod p.$$

Proof. We have that

$$\zeta_p \frac{G'(\zeta_p)}{G(\zeta_p)} \equiv -\sum_{k=1}^{q^n-2} k\zeta_q^{T(\alpha^k)} + \sum_{l=1}^{f-1}\Phi(lp) + \sum_{i=1}^{p-1}\Phi(-if)\zeta_p^i \mod p$$

(see [9, formula (1)]). On the other hand, by taking logarithmic derivatives of both members of (4) and using (6), we obtain

$$\zeta_p \frac{G'(\zeta_p)}{G(\zeta_p)} \equiv \sum_{i=0}^{p-1}\left(\sum_{j=1}^{p-1} j\eta_j\eta_{j-i}\right)\zeta_p^i \mod p.$$

This shows that, for some integer c, we have $\Phi(fi) \equiv c + \sum_{j=1}^{p-1} j\eta_j\eta_{j+i} \bmod p$ for $1 \le i \le p-1$. Therefore, by (5),

$$c \equiv -(p-1)c \equiv -\sum_{i=1}^{p-1} \Phi(fi) + \sum_{j=1}^{p-1} j\eta_j \sum_{i=1}^{p-1} \eta_{j+i}$$

$$= -\sum_{i=1}^{p-1} \Phi(fi) + \sum_{j=1}^{p-1} j\eta_j(-\eta_j - 1)$$

$$= -\sum_{i=1}^{p-1} \Phi(fi) - \sum_{j=1}^{p-1} j\eta_j^2 - \sum_{j=1}^{p-1} j\eta_j \mod p.$$

But

$$\sum_{i=1}^{p-1} \Phi(fi) \equiv 0 \mod p,$$

since $\alpha^{\sum_{i=1}^{p-1}\Phi(fi)} \equiv \prod_{i=1}^{p-1}(1-\zeta_p^i) = p \mod Q$ and since p (in fact, any rational integer) is a pth power modulo Q (recall that $p(q-1) \mid (q^n - 1)$). Also, if $u \not\equiv 0 \mod n$ and $v \in \mathbb{Z}$ then, by (9), $\sum_{i=1}^{p-1} i^u \eta_i^v \equiv \sum_{j=0}^{p-2} g^{ju}\eta_{g^j}^v = \sum_{j=0}^{e-1}\left(\sum_{k=0}^{n-1} g^{eku}\right) g^{ju}\eta_{g^j}^v \equiv 0 \mod p$. In particular, $\sum_{j=1}^{p-1} j\eta_j \equiv 0 \mod p$ and $\sum_{j=1}^{p-1} j\eta_j^2 \equiv 0 \mod p$. Therefore $c \equiv 0 \mod p$. This ends the proof of Proposition 4. □

For r even, $2 \le r \le p-3$, let

$$\beta_r = \prod_{i=1}^{p-1}(1-\zeta_p^i)^{i^{p-1-r}} \tag{32}$$

and let $i_r(Q)$ be the least nonnegative integer such that

$$\beta_r \equiv \alpha^{i_r(Q)} \mod Q. \tag{33}$$

It is a well-known fact that $e_r(A)$ is trivial if and only if β_r is not the pth power of an element of $\mathbb{Z}[\zeta_p]$ (see e.g. [14, Thm. 15.7 and the discussion preceding Thm. 8.14]). In particular, we have the following.

Proposition 5. *For r even, $2 \le r \le p-3$, if $i_r(Q) \not\equiv 0 \mod p$ then $e_r(A)$ is trivial.*

The following numbers will prove useful in our study of the indices $i_r(Q)$ modulo p. For $k \in \mathbb{Z}$, we define

$$a_k = nq^v \sum_{i=0}^{e-1} g^{nki} d_i. \tag{34}$$

Note that $a_{k+e} \equiv a_k \mod p$. Also, by (22), $a_0 \equiv -1 \mod p$ and, by (9), for $1 \le k \le e-1$ we have $a_k = n\sum_{i=0}^{e-1} g^{nki}(\eta_{g^i} - \eta_0) \equiv \sum_{i=0}^{p-2} g^{nki}\eta_{g^i} \equiv \sum_{i=1}^{p-1} i^{nk}\eta_i$ mod p.

PROPOSITION 6. *Let r be an even integer, $2 \le r \le p-3$. Then*

$$i_r(Q) \equiv \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} i^{p-1-r} j \eta_j \eta_{j+i} \mod p.$$

If $n \nmid r-1$, then $i_r(Q) \equiv 0 \mod p$. If $n \mid r-1$, then

$$i_r(Q) \equiv -\sum_{l=1}^{(p-r)/n} (-1)^l \binom{p-1-r}{ln-1} a_{(p-r)/n-l} a_l \mod p.$$

In particular,

$$i_{p-n}(Q) \equiv -a_1 = -nq^{\nu} \sum_{j=0}^{e-1} g^{nj} d_j \mod p.$$

Proof. The first congruence follows directly from (31)–(33) and Proposition 4. Hence

$$\begin{aligned}
i_r(Q) & \\
&\equiv \sum_{i=0}^{p-1} \sum_{j=1}^{p-1} (i-j)^{p-1-r} j \eta_i \eta_j \\
&= \eta_0 \sum_{j=1}^{p-1} j^{p-r} \eta_j + \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \sum_{l=0}^{p-1-r} (-1)^l \binom{p-1-r}{l} i^{p-1-r-l} j^{l+1} \eta_i \eta_j \\
&= \eta_0 \sum_{j=1}^{p-1} j^{p-r} \eta_j + \sum_{l=0}^{p-1-r} (-1)^l \binom{p-1-r}{l} \sum_{i=1}^{p-1} i^{p-1-r-l} \eta_i \sum_{j=1}^{p-1} j^{l+1} \eta_j \\
&\equiv \eta_0 \sum_{j=0}^{p-2} g^{j(p-r)} \eta_{g^j} \\
&\quad + \sum_{l=0}^{p-1-r} (-1)^l \binom{p-1-r}{l} \sum_{i=0}^{p-2} g^{i(p-1-r-l)} \eta_{g^i} \sum_{j=0}^{p-2} g^{j(l+1)} \eta_{g^j} \\
&= \eta_0 \sum_{j=0}^{p-2} g^{j(p-r)} (q^{\nu} d_j + \eta_0) \\
&\quad + \sum_{l=0}^{p-1-r} (-1)^l \binom{p-1-r}{l} \sum_{i=0}^{p-2} g^{i(p-1-r-l)} (q^{\nu} d_i + \eta_0) \sum_{j=0}^{p-2} g^{j(l+1)} (q^{\nu} d_j + \eta_0) \\
&\equiv q^{\nu} \eta_0 \sum_{j=0}^{p-2} g^{j(p-r)} d_j \\
&\quad + q^{2\nu} \sum_{l=0}^{p-1-r} (-1)^l \binom{p-1-r}{l} \sum_{i=0}^{p-2} g^{i(p-1-r-l)} d_i \sum_{j=0}^{p-2} g^{j(l+1)} d_j \\
&\quad - q^{\nu} \eta_0 \sum_{j=0}^{p-2} g^{j(p-r)} d_j
\end{aligned}$$

$$
\begin{aligned}
&= q^{2\nu} \sum_{l=0}^{p-1-r} (-1)^l \binom{p-1-r}{l} \sum_{i=0}^{p-2} g^{i(p-1-r-l)} d_i \sum_{j=0}^{p-2} g^{j(l+1)} d_j \\
&= q^{2\nu} \sum_{l=0}^{p-1-r} (-1)^l \binom{p-1-r}{l} \sum_{i=0}^{e-1} \sum_{u=0}^{n-1} g^{(i+eu)(p-1-r-l)} d_i \sum_{j=0}^{e-1} \sum_{v=0}^{n-1} g^{(j+ev)(l+1)} d_j \\
&= q^{2\nu} \sum_{l=0}^{p-1-r} (-1)^l \binom{p-1-r}{l} \\
&\quad \times \sum_{i=0}^{e-1} g^{i(p-1-r-l)} d_i \sum_{u=0}^{n-1} g^{eu(p-1-r-l)} \sum_{j=0}^{e-1} g^{j(l+1)} d_j \sum_{v=0}^{n-1} g^{ev(l+1)} \mod p.
\end{aligned}
$$

If $n \nmid r-1$ then either $n \nmid p-1-r-l$ or $n \nmid l+1$; so, by the preceding congruence, $i_r(Q) \equiv 0 \bmod p$. If $n \mid r-1$ we obtain

$$
\begin{aligned}
i_r(Q) &\equiv -n^2 q^{2\nu} \sum_{l=1}^{(p-r)/n} (-1)^l \binom{p-1-r}{ln-1} \sum_{i=0}^{e-1} g^{i(p-r-ln)} d_i \sum_{j=0}^{e-1} g^{jln} d_j \\
&= -\sum_{l=1}^{(p-r)/n} (-1)^l \binom{p-1-r}{ln-1} a_{(p-r)/n-l} a_l \mod p.
\end{aligned}
$$

This proves the second congruence of the proposition. The last congruence follows from the second one and from the fact that $a_0 \equiv -1 \bmod p$. □

In the following theorem we summarize some properties of the numbers d_i and a_i that are useful in the study of certain components of the ideal class group of $\mathbb{Q}(\zeta_p)$. We believe that the theorem can be used to show that, with l odd ($1 \le l \le e-1$), some of the components $e_{p-ln}(A)$ of A are trivial. The idea is to show that if $e_{p-ln}(A)$ is nontrivial then *all* prime numbers q of order n modulo p must have a certain form; we hope this will contradict some version of Dirichlet's theorem on primes in arithmetic progressions.

THEOREM 1. (i) *We have*

$$
e^2 q^{n-2\nu} = \left(\sum_{i=0}^{e-1} d_i \right)^2 + p \left(e \sum_{i=0}^{e-1} d_i^2 - \left(\sum_{i=0}^{e-1} d_i \right)^2 \right)
$$

and

$$
\left(\sum_{i=0}^{e-1} d_i \right)^2 = \left(\frac{1 + p\eta_0}{nq^\nu} \right)^2 < e^2 q^{n-2\nu}.
$$

Also, for $0 \le k \le e-1$,

$$
q^{n-2\nu} = -\sum_{i=0}^{e-1} \sum_{j=0}^{e-1} c_{j+e/2-i,k-i} d_i d_j,
$$

where the integers $c_{i,j} = (i, j) - n\delta_{e/2,i}$ *are as in* (8) *and* (24).

(ii) *The numbers* $a_k = nq^\nu \sum_{i=0}^{e-1} g^{nki} d_i$ *satisfy the following congruences*: $a_0 \equiv -1 \bmod p$ *and, for* $1 \le l \le e-1$,

$$\sum_{m=0}^{l} (-1)^m \binom{ln}{mn} a_{l-m} a_m \equiv 0 \mod p.$$

Also,

$$\sum_{m=0}^{e-1} a_{e-m} a_m \equiv -nq^{2\nu} \sum_{i=0}^{e-1} d_i^2 \mod p$$

and, for l *odd* $(1 \le l \le e-1)$,

$$\sum_{m=1}^{l} (-1)^m m \binom{ln}{mn} a_{l-m} a_m \equiv -l i_{p-ln}(Q) \mod p.$$

(iii) *If, for* l *odd* $(1 \le l \le e-1)$, *the component* $e_{p-ln}(A)$ *of the* p*-part of the ideal class group of* $\mathbb{Q}(\zeta_p)$ *is nontrivial, then*

$$\sum_{m=1}^{l} (-1)^m m \binom{ln}{mn} a_{l-m} a_m \equiv 0 \mod p.$$

Proof. (i) Equation (18) and Proposition 2(i) yield

$$\begin{aligned} eq^{n-2\nu} &= -\sum_{i=0}^{e-1} \sum_{j=0}^{e-1} \left(\sum_{k=0}^{e-1} c_{j+e/2-i,k-i} \right) d_i d_j \\ &= -\sum_{i=0}^{e-1} \sum_{j=0}^{e-1} (n - p\delta_{i,j}) d_i d_j \\ &= -n \left(\sum_{i=0}^{e-1} d_i \right)^2 + p \sum_{i=0}^{e-1} d_i^2. \end{aligned}$$

Therefore, $e^2 q^{n-2\nu} = \left(\sum_{i=0}^{e-1} d_i\right)^2 + p\left(e \sum_{i=0}^{e-1} d_i^2 - \left(\sum_{i=0}^{e-1} d_i\right)^2\right)$. By (22) we have that $\left(\sum_{i=0}^{e-1} d_i\right)^2 = \left(\frac{1+p\eta_0}{nq^\nu}\right)^2$, and from (21) we obtain

$$\sum_{i=0}^{e-1} d_i = \frac{1}{pq^\nu} \sum_{k=0}^{e-1} (-1-en) G(\zeta_p^{-g^k}) = -\frac{1}{q^\nu} \sum_{k=0}^{e-1} G(\zeta_p^{-g^k}).$$

So, by (6) and the triangle inequality, $\left|\sum_{i=0}^{e-1} d_i\right| \le \frac{1}{q^\nu} \sum_{k=0}^{e-1} q^{n/2} = eq^{n/2-\nu}$. Since n is odd, this implies that $\left(\sum_{i=0}^{e-1} d_i\right)^2 < e^2 q^{n-2\nu}$. The last equality is just formula (18).

(ii) The congruence $a_0 \equiv -1 \bmod p$ follows from (22). By (18), (24), and Proposition 3 we have, for $0 \le k \le e-1$,

$$\begin{aligned}
1 \equiv q^n &= -q^{2\nu} \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} ((j + e/2 - i, k - i) - n\delta_{i,j}) d_i d_j \\
&= -q^{2\nu} \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} (j + e/2 - i, k - i) d_i d_j + nq^{2\nu} \sum_{i=0}^{e-1} d_i^2 \\
&\equiv q^{2\nu} \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} \frac{1}{e^2} \sum_{l=0}^{e} \sum_{m=0}^{e-1} \binom{nl}{nm} g^{n(m(j+e/2-i)-l(k-i))} d_i d_j + nq^{2\nu} \sum_{i=0}^{e-1} d_i^2 \\
&\equiv n^2 q^{2\nu} \sum_{l=0}^{e-1} \sum_{m=0}^{e-1} \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} (-1)^m \binom{nl}{nm} g^{n(m(j-i)-l(k-i))} d_i d_j;
\end{aligned}$$

this follows because

$$\begin{aligned}
n^2 q^{2\nu} \sum_{m=0}^{e-1} \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} (-1)^m \binom{p-1}{nm} g^{nm(j-i)} d_i d_j &\equiv n^2 q^{2\nu} \sum_{i=0}^{e-1} \sum_{j=0}^{e-1} e\delta_{i,j} d_i d_j \\
&\equiv -nq^{2\nu} \sum_{i=0}^{e-1} d_i^2 \mod p.
\end{aligned}$$

As a result, $1 \equiv \sum_{l=0}^{e-1} g^{-nkl} \sum_{m=0}^{e-1} (-1)^m \binom{nl}{nm} a_{l-m} a_m \mod p$ and hence, for $0 \leq t \leq e-1$,

$$\begin{aligned}
e\delta_{0,t} \equiv \sum_{k=0}^{e-1} g^{nkt} &\equiv \sum_{l=0}^{e-1} \sum_{k=0}^{e-1} g^{nk(t-l)} \sum_{m=0}^{e-1} (-1)^m \binom{nl}{nm} a_{l-m} a_m \\
&\equiv e \sum_{m=0}^{t} (-1)^m \binom{nt}{nm} a_{t-m} a_m \mod p.
\end{aligned}$$

That is, $a_0^2 \equiv 1 \mod p$, which we already know, and $\sum_{m=0}^{l} (-1)^m \binom{nl}{nm} a_{l-m} a_m \equiv 0 \mod p$ for $1 \leq l \leq e-1$. The congruence $\sum_{m=0}^{e-1} a_{e-m} a_m \equiv -nq^{2\nu} \sum_{i=0}^{e-1} d_i^2 \mod p$ can easily be obtained from (34), and the congruences

$$\sum_{m=1}^{l} (-1)^m m \binom{ln}{mn} a_{l-m} a_m \equiv -l i_{p-ln}(Q) \mod p$$

for l odd ($1 \leq l \leq e-1$) follow immediately from Proposition 6.

(iii) Follows from (ii) and Proposition 5. This ends the proof of the theorem. □

The following examples show how to use Theorem 1 to gain information about the components $e_{p-ln}(A)$ of the ideal class group of $\mathbb{Q}(\zeta_p)$ when e is small.

If $e = 2$, then $n = (p-1)/2$. Since we want n odd, we must have $p \equiv 3 \mod 4$. Suppose $i_{p-n}(Q) = i_{(p+1)/2}(Q) \equiv 0 \mod p$. Then, by Theorem 1(ii), we have that $a_1 \equiv 0 \mod p$ and so $d_1 \equiv d_0 \mod p$. On the other hand, by Theorem 1(i),

$$\begin{aligned}4q^{(p-1)/2-2\nu} &= (d_0+d_1)^2 + p(2(d_0^2+d_1^2)-(d_0+d_1)^2)\\ &= (d_0+d_1)^2 + p(d_0-d_1)^2.\end{aligned}$$

Therefore, $4q^{(p-1)/2-2\nu} \equiv (d_0+d_1)^2 \bmod p^2$.

OBSERVATION. It is well known that, when $p \equiv 3 \bmod 4$, the component $e_{p-(p-1)/2}(A) = e_{(p+1)/2}(A)$ is trivial. This follows from the reflexion theorem (see [14, Thm. 10.9]) and from the class number formula for the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$: If $e_{(p+1)/2}(A)$ is nontrivial then $e_{(p-1)/2}(A)$ is nontrivial and so $p \mid n-2\nu$; but $n-2\nu < p$, a contradiction. The preceding result, together with Proposition 5, could lead to an alternative proof of this fact. If $e_{(p+1)/2}(A)$ were nontrivial then, for each prime q of order $(p-1)/2 \bmod p$, if a and b are the integers such that $4q^{(p-1)/2-2\nu} = a^2+pb^2$ then we would have that $p \mid b$.

If $e=4$, then $n=(p-1)/4$. Since we want n odd, we must have $p \equiv 5 \bmod 8$. By Theorem 1(ii) we have $a_2 \equiv -\frac{1}{2}\binom{2n}{n}a_1^2 \bmod p$, and $16q^{-2\nu}(1+2a_1a_3+a_2^2) \equiv 4(d_0^2+d_1^2+d_2^2+d_3^2) \bmod p$. By Theorem 1(i),

$$\begin{aligned}16q^{(p-1)/4-2\nu} &= (d_0+d_1+d_2+d_3)^2\\ &\quad + p(4(d_0^2+d_1^2+d_2^2+d_3^2)-(d_0+d_1+d_2+d_3)^2).\end{aligned}$$

In particular, $(d_0+d_1+d_2+d_3)^2 \equiv 16q^{-2\nu} \bmod p$. Suppose first that $e_{p-n}(A) = e_{(3p+1)/4}(A)$ is nontrivial. Then, by Theorem 1(iii), $a_1 \equiv 0 \bmod p$, and so also $a_2 \equiv 0 \bmod p$. Hence $16q^{(p-1)/4-2\nu} \equiv (d_0+d_1+d_2+d_3)^2 \bmod p^2$. Suppose now that $e_{p-3n}(A) = e_{(p+3)/4}(A)$ is nontrivial. Then, by Theorem 1(iii), $a_3 \equiv -\frac{1}{3}\binom{3n}{n}a_1a_2 \bmod p$. Since $a_2 \equiv -\frac{1}{2}\binom{2n}{n}a_1^2 \bmod p$, we have $a_3 \equiv \frac{1}{6}\binom{2n}{n}\binom{3n}{n}a_1^3 = \frac{1}{6}\frac{(3n)!}{(n!)^3}a_1^3 \bmod p$. Therefore,

$$\begin{aligned}16q^{(p-1)/4-2\nu} &= (d_0+d_1+d_2+d_3)^2\\ &\quad + p(4(d_0^2+d_1^2+d_2^2+d_3^2)-(d_0+d_1+d_2+d_3)^2)\\ &\equiv (d_0+d_1+d_2+d_3)^2 + p(16q^{-2\nu}(1+2a_1a_3+a_2^2)-16q^{-2\nu})\\ &\equiv (d_0+d_1+d_2+d_3)^2 + 16pq^{-2\nu}\left(\frac{1}{3}\frac{(3n)!}{(n!)^3}+\frac{1}{4}\frac{((2n)!)^2}{(n!)^4}\right)a_1^4\\ &\equiv (d_0+d_1+d_2+d_3)^2 + \frac{4}{3}p\left(\left(\frac{p-1}{4}\right)!\right)^{-4}q^{-2\nu}a_1^4 \bmod p^2.\end{aligned}$$

If $e=6$, then $n=(p-1)/6$. Since we want n odd, we must have $p \equiv 7 \bmod 12$. By Theorem 1(ii) we have $a_2 \equiv -\frac{1}{2}\binom{2n}{n}a_1^2 \bmod p$ and $a_4 \equiv -\binom{4n}{n}a_1a_3 + \frac{1}{2}\binom{4n}{2n}a_2^2 \bmod p$, so $a_4 \equiv -\binom{4n}{n}a_1a_3 + \frac{1}{8}\frac{(4n)!}{(n!)^4}a_1^4 \bmod p$. Also $1+2a_1a_5+2a_2a_4+a_3^2 \equiv -nq^{2\nu}\sum_{i=0}^5 d_i^2 \bmod p$ and $\left(\sum_{i=0}^5 d_i\right)^2 \equiv 36q^{-2\nu} \bmod p$. Therefore,

$$6\sum_{i=0}^5 d_i^2 - \left(\sum_{i=0}^5 d_i\right)^2 \equiv 36q^{-2\nu}(2a_1a_5+2a_2a_4+a_3^2) \bmod p.$$

By Theorem 1(i), $36q^{(p-1)/6-2\nu} = \left(\sum_{i=0}^{5} d_i\right)^2 + p\left(6\sum_{i=0}^{5} d_i^2 - \left(\sum_{i=0}^{5} d_i\right)^2\right)$. Suppose that $e_{p-n}(A) = e_{(5p+1)/6}(A)$ is nontrivial. Then, by Theorem 1(iii), $a_1 \equiv 0 \bmod p$ and so also $a_2 \equiv 0 \bmod p$ and $a_4 \equiv 0 \bmod p$. Hence, $36q^{(p-1)/6-2\nu} \equiv \left(\sum_{i=0}^{5} d_i\right)^2 + 36pq^{-2\nu}a_3^2 \bmod p^2$.

4. Calculation of the Gaussian Periods η_i

We preserve the notation of Sections 1 and 2. As in Section 1, we assume that n, the order of q modulo p, is an odd integer ≥ 3. We have that $q \equiv g^{et} \bmod p$ for some integer t relatively prime to n. If $a \in \mathbb{Z}$, we denote by $|a|_p$ the smallest nonnegative residue of a modulo p. We denote by g_k the number $|g^k|_p$. Our calculation of the Gaussian periods η_i is based on the Gross–Koblitz formula, inequality (20), and Proposition 3, which gives us an easy way to find the cyclotomic numbers (i, j) of order e corresponding to p. Note that, by (9) and (16), in order to find the numbers η_i it is enough to calculate the numbers d_i.

By formulas (20) and (21) we have, for $0 \leq i \leq e-1$,

$$d_i = \frac{1}{p}\sum_{j=0}^{e-1}(\theta_{i+j} - n)\frac{G(\zeta_p^{-g^j})}{q^\nu};$$
$$|d_i| < \begin{cases} \frac{1}{2}q^{(n+1)/2+1-\nu} & \text{if } q = 2 \text{ or } 3 \text{ or } 5, \\ \frac{1}{2}q^{(n+1)/2-\nu} & \text{if } q \geq 7. \end{cases} \tag{35}$$

Set

$$m = m(q) = \begin{cases} \max\left\{3, \frac{n+1}{2} + 1 - \nu\right\} & \text{if } q = 2, \\ \frac{n+1}{2} + 1 - \nu & \text{if } q = 3 \text{ or } q = 5, \\ \frac{n+1}{2} - \nu & \text{if } q \geq 7. \end{cases} \tag{36}$$

Let $\mathcal{R} = \mathbb{Z}[\theta_0, \ldots, \theta_{e-1}]$ be the ring of integers of $\mathbb{Q}(\theta_0)$ and let $Q' = Q \cap \mathcal{R}$ be the prime ideal of $\mathcal{R}$ below Q. Note that $\mathbb{Q}(\theta_0)$ is the decomposition field of q. We can identify $\mathcal{R}/Q'$ with $\mathbb{Z}/q\mathbb{Z}$ and more generally $\mathcal{R}/Q'^l$ with $\mathbb{Z}/q^l\mathbb{Z}$ for $l \geq 1$. In particular, the periods θ_i are congruent to rational integers modulo Q'^l. In order to find the numbers d_i it is enough, by (35), to find their congruence classes modulo q^m, and for that it is enough to find the congruence classes modulo q^m of the numbers $G(\zeta_p^{-g^j})/q^\nu$ and the congruence classes modulo Q'^m of the periods θ_i.

Recall the Gross–Koblitz formula (see [3], [5, Chap. 15, Thm. 4.3], or [1, (11.2.12)], where one finds other references including one for Coleman's proof, which is valid also for $q = 2$). In our particular situation, and with our notation, it reads as follows. For $1 \leq k \leq p-1$, write $fk = \sum_{i=0}^{n-1} u_{k,i}q^i$, where $u_{k,i} \in \mathbb{Z}$ and $0 \leq u_{k,i} \leq q-1$. Since $f \equiv 0 \bmod q-1$, we have that $\sum_{i=0}^{n-1} u_{k,i} \equiv 0 \bmod q-1$. Define $v(k) = \frac{1}{q-1}\sum_{i=0}^{n-1} u_{k,i}$. Let $\mathbb{Z}_q$ be the ring of q-adic integers, let Γ_q be the q-adic Gamma function (see [5, Chap. 14]), and for $x \in \mathbb{Q}$ let $\langle x \rangle$ be the fractional part of x (i.e., $\langle x\rangle = x-[x]$, where $[x]$ is the integral part of x). Then, in $\mathbb{Z}_q$ we have that, for $1\le a\le p-1$,

$$G(\zeta_p^a) = q^n(-q)^{-v(a)}\prod_{i=0}^{n-1}\Gamma_q\left(1-\left\langle\frac{q^ifa}{q^n-1}\right\rangle\right). \tag{37}$$

By [5, Chap. 1, Sec. 2, Lemma 1] it follows that

$$v(g_k) = \sum_{i=0}^{n-1}\left\langle\frac{q^ifg_k}{q^n-1}\right\rangle = \sum_{i=0}^{n-1}\left\langle\frac{q^ig_k}{p}\right\rangle = \frac{1}{p}\sum_{i=0}^{n-1}|g_kg^{eti}|_p = \frac{1}{p}\sum_{i=0}^{n-1}g_{k+ei}.$$

For $0\le k\le p-2$, define

$$w(k) = \frac{1}{p}\sum_{i=0}^{n-1}g_{k+ei}. \tag{38}$$

Note that $\nu=\min_{0\le k\le e-1}w(k)$ (see (13)). By (6), (37), and (38), for $0\le k\le e-1$ we have

$$\frac{G(\zeta_p^{-g^k})}{q^\nu} = \frac{(-1)^{w(k)}q^{w(k)-\nu}}{\prod_{i=0}^{n-1}\Gamma_q\left(1-\left\langle\frac{q^ig_k}{p}\right\rangle\right)}.$$

But $\left\langle\frac{q^ig_k}{p}\right\rangle = \frac{1}{p}|q^ig_k|_p \equiv -f|g^{eti}g_k|_p = -fg_{k+eti} \bmod q^n$. Also, if $q^l\ne 4$ and if $\rho_1\equiv\rho_2 \bmod q^l$ in $\mathbb{Z}_q$, then $\Gamma_q(\rho_1)\equiv\Gamma_q(\rho_2)\bmod q^l$. Thus, for $0\le k\le e-1$,

$$\frac{G(\zeta_p^{-g^k})}{q^\nu} \equiv \frac{(-1)^{w(k)}q^{w(k)-\nu}}{\prod_{i=0}^{n-1}\Gamma_q(1+fg_{k+ei})} \mod q^n. \tag{39}$$

We have $\Gamma_q(0)=1$ and $\Gamma_q(1)=-1$; and if $a\in\mathbb{Z}$ and $a\ge 2$ then

$$\Gamma_q(a) = (-1)^a\prod_{\substack{j=1\\(j,q)=1}}^{a-1} j. \tag{40}$$

Since we only need an expression modulo q^m for $G(\zeta_p^{-g^k})/q^\nu$ and since m is often much smaller than n, we can improve congruence (39) as follows. For $a\in\mathbb{Z}$ let $|a|_{q^m}$ be the smallest nonnegative residue of a modulo q^m. For $1\le a\le p-1$, $0\le i\le n-1$, and $j\in\mathbb{Z}$, define $u_{a,i+nj}=u_{a,i}$. We have

$$\left\langle\frac{q^{n-i}a}{p}\right\rangle = \left\langle\frac{q^{n-i}fa}{q^n-1}\right\rangle = \frac{q^{n-i}fa-(q^n-1)\left[\frac{q^{n-i}fa}{q^n-1}\right]}{q^n-1}.$$

The numerator of this expression is less than q^n-1 and congruent to $q^{n-i}fa\equiv \sum_{l=0}^{n-1}u_{a,l+i}q^l \bmod q^n-1$. Hence

$$\left\langle \frac{q^{n-i}a}{p} \right\rangle = \frac{\sum_{l=0}^{n-1} u_{a,l+i} q^l}{q^n - 1} \equiv -\sum_{l=0}^{n-1} u_{a,l+i} q^l \mod q^n.$$

Therefore, since $fg_{k-eti} \equiv -\langle q^{n-i} g_k/p \rangle \mod q^n$, we have

$$|fg_{k-eti}|_{q^m} = \sum_{l=0}^{m-1} u_{g_k,l+i} q^l$$

and

$$\sum_{i=0}^{n-1} |fg_{k+ei}|_{q^m} = \sum_{i=0}^{n-1} \sum_{l=0}^{m-1} u_{g_k,l+i} q^l = \sum_{i=0}^{n-1} u_{g_k,i} \sum_{l=0}^{m-1} q^l = v(g_k)(q^m - 1).$$

In particular, $\sum_{i=0}^{n-1} |fg_{k+ei}|_{q^m} \equiv (q-1)\omega(k) \mod 2$. Thus, by (39) and (40), for $0 \le k \le e-1$ we have

$$\frac{G(\zeta_p^{-g^k})}{q^\nu} \equiv \frac{(-1)^{qw(k)-1} q^{w(k)-\nu}}{\prod_{i=0}^{n-1} \prod_{\substack{j=1 \\ (j,q)=1}}^{|fg_{k+ei}|_{q^m}} j} \mod q^m. \tag{41}$$

As before (see (23) and (24)), let

$$C = [c_{i,j}]_{0 \le i,j \le e-1} = [(i,j) - n\delta_{e/2,i}]_{0 \le i,j \le e-1}.$$

We can calculate C using Proposition 3. Let $F(x)$ be the characteristic polynomial of C. We showed in Section 2 that $F(x)$ is the minimal polynomial of the periods θ_i, so in $\mathcal{R}[x]$ it follows that

$$F(x) = \det(xI - C) = \prod_{i=0}^{e-1} (x - \theta_i). \tag{42}$$

Let $C_0 = [c_{i,j}]_{1 \le i,j \le e-1}$ and $F_0(x) = \det(xI - C_0)$ and let I_0 be the identity matrix of order $e-1$. By (25) with $j = 0$, we have

$$\begin{array}{ccccccccc}
(c_{1,1} - \theta_0)\theta_1 & + & c_{1,2}\theta_2 & + \cdots + & c_{1,e-1}\theta_{e-1} & = & -c_{1,0}\theta_0 \\
c_{2,1}\theta_1 & + & (c_{2,2} - \theta_0)\theta_2 & + \cdots + & c_{2,e-1}\theta_{e-1} & = & -c_{2,0}\theta_0 \\
\vdots & & \vdots & \ddots & \vdots & & \vdots \\
c_{e-1,1}\theta_1 & + & c_{e-1,2}\theta_2 & + \cdots + & (c_{e-1,e-1} - \theta_0)\theta_{e-1} & = & -c_{e-1,0}\theta_0.
\end{array}$$

Regard this as a system of $e-1$ equations with unknowns $\theta_1, \theta_2, \ldots, \theta_{e-1}$. The matrix of coefficients of this system is $M = C_0 - \theta_0 I_0$. We have that $\det(M) \neq 0$; otherwise, the degree of θ_0 would be smaller than e. Therefore

$$\begin{bmatrix} \theta_1 \\ \theta_2 \\ \vdots \\ \theta_{e-1} \end{bmatrix} = -\theta_0 M^{-1} \begin{bmatrix} c_{1,0} \\ c_{2,0} \\ \vdots \\ c_{e-1,0} \end{bmatrix}. \tag{43}$$

In order to use (35) and (41) to calculate the numbers d_i, we must find integers $t_0, t_1, \dots, t_{e-1}$, modulo q^m, such that $t_i \equiv \theta_i \bmod Q'^m$. Using the identification $\mathcal{R}/Q' \simeq \mathbb{Z}/q\mathbb{Z}$, we see that $F(x)$ splits in linear factors in $\mathbb{Z}/q\mathbb{Z}$. Moreover, every period θ_i can be identified with a q-adic integer. Recall what the q-adic expansion $\sum_{j=0}^{\infty} a_j q^j$ of θ_i is: a_0 is the integer $0 \le a_0 \le q-1$ such that $\theta_i \equiv a_0 \bmod Q'$. Since q is unramified in $\mathbb{Q}(\theta_0)$, we have that $(\theta_i - a_0)/q \in \mathcal{R}_{Q'}$, the localization of $\mathcal{R}$ in Q'. Then a_1 is the integer $0 \le a_1 \le q-1$ such that $(\theta_i - a_0)/q \equiv a_1 \bmod Q'$. We have that $\theta_i \equiv a_0 + a_1 q \bmod Q'^2$, so $(\theta_i - a_0 - a_1 q)/q^2 \in \mathcal{R}_{Q'}$, and so forth. This shows in particular that $F(x)$ has e roots in $\mathbb{Z}_q$. Of course these roots are distinct, but it can happen that two roots are congruent modulo a large power of q. It can also happen that some roots modulo a certain power of q do not lift to a q-adic root. Furthermore, even if we find the set of all t_i (as the set of roots of $F(x)$ modulo q^m that can be lifted to q-adic roots), there remains the problem of labeling its elements to make t_i correspond to θ_i. This shows that we must be careful in our search for the t_i. Let D be the discriminant of $F(x)$, D_0 the discriminant of $F_0(x)$, R the resultant of $F(x)$ and $F_0(x)$, and $q^\delta, q^{\delta_0}, q^\rho$ the largest powers of q that divide D, D_0, R (respectively). Note that $R \ne 0$ because $F(x)$, which is irreducible over $\mathbb{Q}$ of degree e, and $F_0(x)$, which is of degree $e-1$, cannot have a common root.

One way to proceed is as follows. Let $\mu' = \max\{\delta, \delta_0\} + m$. By [7, Thm. 2.24 and Thm. A.5], every root of $F(x)$ modulo $q^{\mu'}$ (actually every root of $F(x)$ modulo q^k with $k \ge \delta$) lifts to a unique root of $F(x)$ in $\mathbb{Z}_q$. So $F(x)$ has e distinct roots modulo $q^{\mu'}$. Among these roots there is (at least) one, which we call t_0, such that $F_0(t_0) \not\equiv 0 \bmod q^{\max\{\delta,\delta_0\}+1}$; otherwise (again by [7, Thm. 2.24 and Thm. A.5]), $F_0(x)$ would have e distinct roots in $\mathbb{Z}_q$, which is absurd since it is a polynomial of degree $e-1$. Let $M_0 = C_0 - t_0 I_0$ and define the integers $t_1, t_2, \dots, t_{e-1}$ by

$$\begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_{e-1} \end{bmatrix} = -t_0 M_0^{-1} \begin{bmatrix} c_{1,0} \\ c_{2,0} \\ \vdots \\ c_{e-1,0} \end{bmatrix} \tag{44}$$

(we are only interested in the classes modulo q^m of these numbers). For $0 \le i \le e-1$ and $j \in \mathbb{Z}$ define $t_{i+ej} = t_i$. Since $\det(M_0) = -F_0(t_0) \not\equiv 0 \bmod q^{\max\{\delta,\delta_0\}+1}$ it follows, by (43), that $t_i \equiv \theta_i \bmod Q'^m$ for $i \in \mathbb{Z}$ if we choose $Q = (t_0 - \theta_0, q)$ as the prime ideal of $\mathbb{Z}[\zeta_p]$ over q in the definition of the η_i (formula (1)).

Another way to find the integers t_i is the following. Let $\mu = \max\{\delta, \rho\} + m$ and let t_0 be any root of $F(x)$ modulo q^μ. By [7, Thm. 2.24 and Thm. A.5], t_0 can be lifted in a unique way to a root of $F(x)$ in $\mathbb{Z}_q$. We have that $F_0(t_0) \not\equiv 0 \bmod q^{\max\{\delta,\rho\}+1}$; otherwise, since $R = \Phi(x)F(x) + \Psi(x)F_0(x)$ for some $\Phi(x)$ and $\Psi(x) \in \mathbb{Z}[x]$, we would have $R = \Phi(t_0)F(t_0) + \Psi(t_0)F_0(t_0) \equiv 0 \bmod q^{\rho+1}$, an absurdity. Let $M_0 = C_0 - t_0 I_0$, define the integers $t_1, t_2, \dots, t_{e-1}$ as in (44), and define $t_{i+ej} = t_i$ for $0 \le i \le e-1$ and $j \in \mathbb{Z}$. Since $\det(M_0) = -F_0(t_0) \not\equiv 0 \bmod q^{\max\{\delta,\rho\}+1}$, we have by (43) that $t_i \equiv \theta_i \bmod Q'^m$ for $i \in \mathbb{Z}$ if $Q = (t_0 - \theta_0, q)$.

This is the method we shall use in the program described in Section 5. But consider also using the first method when μ happens to be too large—and larger than μ'.

Note that

$$t_i \equiv \theta_i = \sum_{j=0}^{n-1} \zeta_p^{g^{i+ej}} \equiv \sum_{j=0}^{n-1} \alpha^{fg^{i+ej}} \equiv \sum_{j=0}^{n-1} \alpha^{fg^i q^j} \equiv T(\alpha^{fg^i}) \mod Q.$$

Hence

$$t_i \equiv T(\alpha^{fg^i}) \mod q.$$

Observation. The exponent δ is seldom the smallest possible l that guarantees a unique lifting of a root modulo q^l of $F(x)$ to a q-adic root. It can be improved, by [7, Thm. 2.24], if we are able to choose a suitable root t_0.

We can now write our formula to calculate the coefficients d_i. In order to derive the Gaussian periods η_i from the numbers d_i, we use (16) and (9). By (35) and (41), we have

$$d_i \equiv \frac{1}{p} \sum_{k=0}^{e-1} (t_{i+k} - n) \frac{(-1)^{qw(k)-1} q^{w(k)-\nu}}{\displaystyle\prod_{l=0}^{n-1} \prod_{\substack{j=1 \\ (j,q)=1}}^{|fg_{k+le}|_{q^m}} j} \mod q^m \quad \text{and} \quad |d_i| < \frac{1}{2} q^m, \tag{45}$$

where m and $w(k)$ are as in (36) and (38).

5. A MAPLE Program to Calculate the Periods η_i

The following program calculates first the numbers d_i and $H = \sum_{i=0}^{e-1} d_i \theta_i$, using (45), and then the Gaussian periods η_i using (16) and (9). Notation is close to that used in the previous formula. Enter the numbers p an odd prime, q a prime distinct from p, and g a primitive root modulo p (the command `g:=primroot(p);` will assign to g the smallest positive primitive root modulo p). Check if the value of n (the order of q modulo p), calculated at the beginning, is odd and greater than 1.

There are a few pairs of primes (p, q), in a given range, for which the value of μ is too large (of course, the meaning of "too large" varies with time). This complicates the calculation and the labeling of the integers t_i, the roots of $F(x)$ modulo q^μ, using (44). In order to shorten such calculations one can try assigning smaller values to μ (take $\mu \geq m$). This is likely to work, because our estimate for a convenient value for this number (based on the largest powers of p dividing the discriminant D and the resultant R), though theoretically correct, is far from optimal. Recall that all we want to find are e roots modulo q^m of $F(x)$ which can be lifted to distinct q-adic roots and which are correctly labeled. Whether or not a value assigned to μ is good for calculations may depend on the choice of the root of $F(x)$ modulo q^μ, which we call t_0. We can change MAPLE's choice of such a root by giving another value to the variable a (change, in the first line of the program, the command `a:=1:` to `a:=k:` where k is a number between 1 and e). Choosing a different root modulo p^μ of $F(x)$ as a value for t_0 corresponds to changing H for one of its conjugates in $\mathbb{Q}(\theta_0)$, which corresponds to making a cyclic permutation of the values of the coefficients d_i.

For $p, q < 100$, most of the calculations (using a 400-MHz PC with 384 MB of RAM) take a few seconds; but for some values of p and q, they take much longer. This is the case, for example, when $p = 61$ and $q = 13$, where we have $n = 3$, $g = 2$, $e = 20$, $\nu = 1$, $m = 1$, $\delta = 26$, $\rho := 32$, $\mu = 33$ and

$$\begin{aligned}t_0 = 3 &+ 9\,13 + 7\,13^2 + 11\,13^3 + 2\,13^4 + 11\,13^5 + 11\,13^6 + 8\,13^7 + 12\,13^8 + 12\\ &13^9 + 11\,13^{10} + 13^{11} + 4\,13^{13} + 3\,13^{14} + 8\,13^{15} + 10\,13^{17} + 2\,13^{18} + 6\\ &13^{19} + 2\,13^{20} + 13^{21} + 5\,13^{22} + 11\,13^{23} + 3\,13^{24} + 11\,13^{25} + 9\,13^{26} + 8\\ &13^{27} + 13^{28} + 4\,13^{29} + 3\,13^{30} + 5\,13^{31};\end{aligned}$$

we obtain

$$\begin{aligned}H = &-2\theta_0 - 2\theta_1 - 2\theta_2 - 2\theta_3 - 2\theta_4 - 2\theta_5 - 2\theta_6 - 2\theta_7 - \theta_8 - 2\theta_9 - \theta_{10}\\ &- 2\theta_{11} - 2\theta_{12} - \theta_{13} - 2\theta_{14} - 2\theta_{15} - 2\theta_{16} - \theta_{17} - 2\theta_{18} - 2\theta_{19}.\end{aligned}$$

Other hard cases are $(p, q) = (71, 5)$ and $(p, q) = (97, 61)$. They all can be calculated by using smaller values of μ and by changing the values of a, as indicated in the previous paragraph.

Recall that, to see a given value that has been calculated by MAPLE, one ends the command with a semicolon; otherwise, one ends the command with a colon. For example, to see the matrix C, change the command

```
C:=evalm(C):
```

to

```
C:=evalm(C);
```

To see the (often large) values of the periods η_i, replace the command

```
eta[gexp[i16]]:=q∧nu∗d[i16]+eta[0]; od:
```

with

```
eta[gexp[i16]]:=q∧nu∗d[i16]+eta[0]; od;
```

The last part of the program is used to check that $G(1) = \sum_{i=0}^{e-1} \eta_i = -1$ and that $H\bar{H} = q^{n-2\nu}$.

I am grateful to Javier Thaine for an idea that improved the program by saving much computer memory.

```
with(numtheory): with(linalg): with(padic):
p:=89; q:=67; n:=order(q,p); g:=primroot(p); a:=1:
e:=(p-1)/n; f:=(q∧n-1)/p:
for i1 from 0 to p-2 do
gexp[i1]:=modp(g&∧i1,p); od:
for i2 from 0 to e-1 do
```

```
w[i2]:=(1/p)*sum(gexp[i2+e*j2],j2=0..n-1); od:
L1:=[seq(w[i3-1],i3=1..e)]:
L2:=sort(L1):
nu:=L2[1];
r:=floor(5/q):
m:=(n+1)/2+r-nu;
stored:=1: qm:=q^m:
indexes:=[seq(modp(f*i4,qm),i4=0..p-1)]:
for i5 from 0 to qm do
if modp(i5,q)<>0 then stored:=modp(stored*i5,qm); fi;
if member(i5,indexes) then Q[i5]:=stored; fi; od:
for i6 from 0 to p-2 do;
fgexp[i6]:=modp(f*gexp[i6],q^m); od:
for i7 from 0 to e-1 do
for j7 from 0 to n-1 do
Qf[i7,j7]:=Q[fgexp[i7+e*j7]]; od: od:
for i8 from 0 to e-1 do;
Hmod[i8]:=modp((-1)^(q*w[i8]-1)*q^(w[i8]-nu)/
  product(Qf[i8,j8],j8=0..n-1),q^m); od:
h:=gexp[n]:
Z:=(i9,j9)->modp((-1/(e^2))*sum(sum(binomial(n*k9,n*l9)
  *h^(l9*i9-k9*j9),l9=0..e-1),k9=0..e),p):
Id:=array(identity,1..e,1..e):
C:=array(1..e,1..e,[]):
for i10 from 1 to e do
for j10 from 1 to e do
C[i10,j10]:=Z(i10-1,j10-1)-n*Id[e/2+1,i10]: od: od:
C:=evalm(C):
F:=x->charpoly(C,x):
Dis:=discrim(F(x),x):
delta:=ordp(Dis,q);
C00:=delrows(C,1..1):
C0:=delcols(C00,1..1):
F0:=x->charpoly(C0,x):
R:=resultant(F(x),F0(x),x):
rho:=ordp(R,q);
mu:=max(delta,rho)+m;
L3:=rootp(F(x),q,mu):
l00:=L3[a]:
q_adic_t0:=l00;
l0:=ratvaluep(l00,mu):
E0:=delcols(C00,2..e):
Id0:=array(identity,1..e-1,1..e-1):
M0:=C0-l0*Id0:
T0:=evalm(-l0*M0^(-1)&*E0):
```

```
T1:=array(1..1,1..e):
T1[1,1]:=10 mod q^m:
for i11 from 2 to e do
T1[1,i11]:=modp(T0[i11-1,1],q^m); od:
T:=evalm(concat(T1,T1)):
for i12 from 0 to e-1 do;
d[i12]:=mods((1/p)*sum((T[1,i12+j12+1]-n)*Hmod[j12],
  j12=0..e-1),q^m); od;
H:=sum(d[i13]*theta[i13],i13=0..e-1);
for i14 from 0 to e-1 do
for j14 from 0 to n-1 do
d[i14+e*j14]:=d[i14]; od: od:
eta[0]:=-(1/p)*(1+n*q^nu*sum(d[i15],i15=0..e-1));
for i16 from 0 to p-2 do
eta[gexp[i16]]:=q^nu*d[i16]+eta[0]; od:
# check:
sum_of_eta_i:=sum(eta[i17],i17=0..p-1);
S:=normal((x^p-1)/(x-1)):
H0:=x->sum(d[i18]*sum(x^gexp[i18+e*j18],j18=0..n-1),
  i18=0..e-1):
H1:=sort(H0(x)):
H2:=y->sum(coeff(H1,x,i19)*y^i19,i19=0..p-1):
Hconj:=normal(x^p*H2(x^(-1))):
# check:
H_times_Hconj:=ifactor(rem((H2(x)*Hconj,S,x)));
ifactor(q^(n-2*nu));
```

References

[1] B. Berndt, R. Evans, and K. Williams, *Gauss and Jacobi sums,* Wiley, New York, 1998.

[2] L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem,* Amer. J. Math. 57 (1935), 391–424.

[3] B. H. Gross and N. Koblitz, *Gauss sums and the p-adic Γ-function,* Ann. of Math. (2) 109 (1979), 569–581.

[4] E. Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetsen,* J. Reine Angew. Math. 44 (1852), 93–146.

[5] S. Lang, *Cyclotomic fields I and II* (with an appendix by K. Rubin), combined 2nd ed., Grad. Texts in Math., 121, Springer-Verlag, New York, 1990.

[6] G. Myerson, *Period polynomials and Gauss sums for finite fields,* Acta Arith. 39 (1981) 251–264.

[7] I. Niven, H. Zuckerman, and H. Montgomery, *An introduction to the theory of numbers*, 5th ed., Wiley, New York, 1991.

[8] T. Storer, *Cyclotomy and difference sets,* Markham, Chicago, 1967.

[9] F. Thaine, *On the relation between units and Jacobi sums in prime cyclotomic fields,* Manuscripta Math. 73 (1991), 127–151.

[10] ———, *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.
[11] ———, *Properties that characterize Gaussian periods and cyclotomic numbers,* Proc. Amer. Math. Soc. 124 (1996), 35–45.
[12] ———, *On the coefficients of Jacobi sums in prime cyclotomic fields,* Trans. Amer. Math. Soc. 351 (1999), 4769–4790.
[13] ———, *Families of irreducible polynomials of Gaussian periods and matrices of cyclotomic numbers,* Math. Comp. 69 (2000), 1653–1666.
[14] L. C. Washington, *Introduction to cyclotomic fields,* 2nd ed., Grad. Texts in Math., 83, Springer-Verlag, New York, 1997.

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

ftha@vax2.concordia.ca