PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 124, Number 1, January 1996

PROPERTIES THAT CHARACTERIZE GAUSSIAN PERIODS AND CYCLOTOMIC NUMBERS

F. THAINE

(Communicated by William Adams)

ABSTRACT. Let $q = ef+1$ be a prime number, ζ_q a q-th primitive root of 1 and $\eta_0, \dots, \eta_{e-1}$ the periods of degree e of $\mathbb{Q}(\zeta_q)$. Write $\eta_0\eta_i = \sum_{j=0}^{e-1} a_{i,j}\eta_j$ with $a_{i,j} \in \mathbb{Z}$. Several characterizations of the numbers η_i and $a_{i,j}$ (or, equivalently, of the cyclotomic numbers (i,j) of order e) are given in terms of systems of equations they satisfy and a condition on the linear independence, over $\mathbb{Q}$, of the η_i or on the irreducibility, over $\mathbb{Q}$, of the characteristic polynomial of the matrix $[a_{i,j}]_{0\le i,j\le e-1}$.

Let q be an odd prime number, e and f positive integers such that $q = ef + 1$, s a primitive root modulo q, ζ_q a primitive q-th root of 1 and $\eta_0, \eta_1, \dots, \eta_{e-1}$ the Gaussian periods of degree e in $\mathbb{Q}(\zeta_q)$ defined by

$$\eta_i = \sum_{j=0}^{f-1} \zeta_q^{s^{i+ej}}.$$

Define $\eta_{i+je} = \eta_i$ for $0 \le i \le e-1$ and $j \in \mathbb{Z}$. Then $\mathbb{Q}(\eta_i) = \mathbb{Q}(\eta_0)$, for any i, and $\mathbb{Q}(\eta_0)$ is the only subfield of $\mathbb{Q}(\zeta_q)$ of degree e over $\mathbb{Q}$. The set $\{\eta_0, \eta_1, \dots, \eta_{e-1}\}$ is a normal basis of $\mathbb{Q}(\eta_0)/\mathbb{Q}$ and also an integral basis of $\mathbb{Q}(\eta_0)$. Let $a_{i,j}$, $0 \le i,\ j \le e-1$, be the rational integers such that

$$\eta_0\eta_i = \sum_{j=0}^{e-1} a_{i,j}\eta_j. \tag{1}$$

In this article we show several characterizations of the periods η_i, of the integers $a_{i,j}$ and (equivalently) of the cyclotomic numbers (i,j) related to them (see formula (4)). We state such characterizations in terms of some systems of equations satisfied by those numbers, in addition to a condition on the linear independence, over $\mathbb{Q}$, of the η_i, or on the irreducibility, over $\mathbb{Q}$, of the characteristic polynomial of the matrix $A = [a_{i,j}]_{0\le i,j\le e-1}$. The main result, Theorem 1, characterizes the numbers $a_{i,j}$ as the only integral solutions of a system of linear and quadratic equations (the latter corresponding essentially to the effect of the associative law in the multiplication

Received by the editors May 2, 1994 and, in revised form, August 1, 1994.
1991 *Mathematics Subject Classification.* Primary 11R18; Secondary 11T22.
This work was supported in part by grants from NSERC and FCAR.

table (3) of the periods), satisfying the condition that $\det(xI-A)$ is irreducible over $\mathbb{Q}$. The principal tool used in the proofs is the Kronecker-Weber Theorem.

One application of our results, in the case when p is an odd prime, n a positive integer and $e=p^n$, will be shown in [3], where we study the orders of the components of the p-Sylow subgroup of the ideal class group of the p-cyclotomic field and Vandiver's conjecture.

From the definition of the periods we get

$$\sum_{i=0}^{e-1}\eta_i=-1. \tag{2}$$

Define $a_{i+ke,j+le}=a_{i,j}$ for $0\le i,\ j\le e-1$ and $k,l\in\mathbb{Z}$. Since the permutation $\eta_i\mapsto\eta_{i+1}$ extends to an automorphism of $\mathbb{Q}(\eta_0)$, it follows from (1) that, for $i,j\in\mathbb{Z}$,

$$\eta_i\eta_j=\sum_{k=0}^{e-1}a_{j-i,k-i}\eta_k. \tag{3}$$

As is usual, for $0\le i,\ j\le e-1$, we denote by (i,j) the cyclotomic numbers of order e defined as the number of ordered pairs of integers (k,l), $0\le k,\ l\le f-1$, such that $1+s^{ek+i}\equiv s^{el+j}$ mod q ([1], formula (5) or [2], page 25). Define $(i+ek,j+el)=(i,j)$ for $0\le i,\ j\le e-1$ and $k,l\in\mathbb{Z}$.

We use the following variation 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 (1), (2) and by [1] formula (6) (or [2] Lemma 8, page 38) we have that

$$a_{i,j}=(i,j)-f\delta_i\ , \tag{4}$$

where

$$\delta_i=\begin{cases}\delta_{0,i}\ , & \text{if } f \text{ is even,}\\ \delta_{\frac{1}{2}e,i}\ , & \text{if } f \text{ is odd.}\end{cases} \tag{5}$$

We start by listing some well-known properties of Gaussian periods and cyclotomic numbers. Let ζ_e be a primitive e-th root of 1. For $1\le k\le e-1$, the numbers $G(\zeta_e^k)=\sum_{i=0}^{e-1}\zeta_e^{ki}\eta_i=\sum_{i=0}^{q-2}\zeta_e^{ki}\zeta_q^{s^i}$ are Gauss sums that satisfy $G(\zeta_e^k)G(\zeta_e^{-k})=(-1)^{fk}q$ (see, for example, [4] Lemma 6.1). This, together with (2), is equivalent to

$$\sum_{i=0}^{e-1}\eta_i\eta_{i+j}=q\delta_j-f\ , \tag{6}$$

for $0\le j\le e-1$ (see also [1] formula 20).

We have also, for all $i, j \in \mathbb{Z}$,

$$(i,j) = \begin{cases} (j,i) \ , & \text{if } f \text{ is even,} \\ (j+\tfrac{1}{2}e, i+\tfrac{1}{2}e) \ , & \text{if } f \text{ is odd ,} \end{cases} \tag{7}$$

$$(i,j) = (-i, j-i) \ , \tag{8}$$

$$\sum_{k=0}^{e-1} (i,k) = f - \delta_i \tag{9}$$

and

$$\sum_{k=0}^{e-1} (k,j) = f - \delta_{0,j} \tag{10}$$

(see [1] formulas 14, 15 and 17 or [2] page 25).

From (4) and formulas (7)–(10) we obtain the following properties of the numbers $a_{i,j}$:

$$a_{i,j} = \begin{cases} a_{j,i} + f(\delta_{0,j} - \delta_i) \ , & \text{if } f \text{ is even,} \\ a_{j+\frac{1}{2}e, i+\frac{1}{2}e} + f(\delta_{0,j} - \delta_i) \ , & \text{if } f \text{ is odd ,} \end{cases} \tag{11}$$

$$a_{i,j} = a_{-i,j-i} \ , \tag{12}$$

$$\sum_{k=0}^{e-1} a_{i,k} = f - q\delta_i \tag{13}$$

and

$$\sum_{k=0}^{e-1} a_{k,j} = -\delta_{0,j}, \tag{14}$$

for all $i, j \in \mathbb{Z}$. Observe that (12) follows from (3) since $\eta_i \eta_j = \eta_j \eta_i$, (13) follows from (1), (2) and (6), and (14) follows from (11) and (13).

By (1), $\eta_0 \eta_i \eta_j = \sum_{k=0}^{e-1} a_{i,k} \eta_k \eta_j$. Taking traces (from $\mathbb{Q}(\eta_0)$ to $\mathbb{Q}$) and using (6) and (13) we get

$$\begin{aligned} \sum_{l=0}^{e-1} \eta_l \eta_{l+i} \eta_{l+j} &= \sum_{k=0}^{e-1} a_{i,k} \sum_{l=0}^{e-1} \eta_{k+l} \eta_{j+l} = \sum_{k=0}^{e-1} a_{i,k} \sum_{l=0}^{e-1} \eta_l \eta_{j-k+l} \\ &= \sum_{k=0}^{e-1} a_{i,k} (q\delta_{j-k} - f) = q \sum_{k=0}^{e-1} a_{i,k} \delta_{j-k} + qf\delta_i - f^2. \end{aligned}$$

Therefore, by (5),

$$\frac{1}{q}\big(f^2 + \sum_{l=0}^{e-1} \eta_l \eta_{l+i} \eta_{l+j}\big) = \begin{cases} a_{i,j} + f\delta_i = (i,j) \ , & \text{if } f \text{ is even,} \\ a_{i,j+\frac{1}{2}e} + f\delta_i = (i, j+\tfrac{1}{2}e) \ , & \text{if } f \text{ is odd.} \end{cases} \tag{15}$$

The following proposition gives a characterization of the periods $\eta_0, \eta_1, \ldots, \eta_{e-1}$.

Proposition 1. *Let $\theta_0, \theta_1, \ldots, \theta_{e-1}$ be elements of a field K containing $\mathbb{Q}$. Define $\theta_{j+ke} = \theta_j$ for $0 \le j \le e-1$ and $k \in \mathbb{Z}$. Suppose that*

(i) *$\theta_0, \theta_1, \ldots, \theta_{e-1}$ are linearly independent over $\mathbb{Q}$,*

(ii) *$\sum_{i=0}^{e-1} \theta_i = -1$,*

(iii) *$\sum_{i=0}^{e-1} \theta_i\theta_{i+j} = q\delta_j - f$ for $0 \le j \le e-1$ (δ_j is defined in (5)),*

(iv) *the numbers $b_{i,j} = \frac{1}{q}(f^2 + \sum_{k=0}^{e-1} \theta_k\theta_{k+i}\theta_{k+j})$ are rational integers for $0 \le i,\ j \le e-1$.*

Then $\theta_0, \theta_1, \ldots, \theta_{e-1}$ are (in a certain order) the periods $\eta_0, \eta_1, \ldots, \eta_{e-1}$ of degree e in $\mathbb{Q}(\zeta_q)$ (ζ_q a primitive q-th root of 1 in the algebraic closure of K).

Conversely, if $\theta_0, \theta_1, \ldots, \theta_{e-1}$ are the periods $\eta_0, \eta_1, \ldots, \eta_{e-1}$, then the above conditions are satisfied.

Proof. We know, by (2), (6) and (15), that the periods η_i satisfy the conditions of the proposition.

Suppose that conditions (i)–(iv) hold. To prove that $\{\theta_0, \theta_1, \ldots, \theta_{e-1}\} = \{\eta_0, \eta_1, \ldots, \eta_{e-1}\}$ observe first that, by (iii), for $i, j \in \mathbb{Z}$

$$\sum_{k=0}^{e-1} \theta_{k+i}\theta_{k+j} = q\delta_{j-i} - f. \tag{16}$$

For $i, j \in \mathbb{Z}$ define the integers $c_{i,j}$ by

$$c_{i,j} = \begin{cases} b_{i,j} - f\delta_i\ , & \text{if } f \text{ is even,} \\ b_{i,j+\frac{1}{2}e} - f\delta_i\ , & \text{if } f \text{ is odd.} \end{cases} \tag{17}$$

Note that $c_{i,j} = c_{i+e,j} = c_{i,j+e}$.

If f is even we have $c_{i,k} = \frac{f^2}{q} - f\delta_i + \frac{1}{q}\sum_{l=0}^{e-1} \theta_l\theta_{l+i}\theta_{l+k}$ and, by (ii) and (16),

$$\begin{aligned} \sum_{k=0}^{e-1} c_{i,k}\theta_{j+k} &= -\frac{f^2}{q} + f\delta_i + \frac{1}{q}\sum_{l=0}^{e-1}\theta_l\theta_{l+i}\sum_{k=0}^{e-1}\theta_{l+k}\theta_{j+k} \\ &= -\frac{f^2}{q} + f\delta_i + \frac{1}{q}\sum_{l=0}^{e-1}\theta_l\theta_{l+i}(q\delta_{j,l} - f) \\ &= -\frac{f^2}{q} + f\delta_i + \theta_j\theta_{j+i} - \frac{1}{q}f(q\delta_i - f) = \theta_j\theta_{j+i}. \end{aligned}$$

If f is odd we have $c_{i,k} = \frac{f^2}{q} - f\delta_i + \frac{1}{q}\sum_{l=0}^{e-1} \theta_l\theta_{l+i}\theta_{l+k+\frac{1}{2}e}$ and, by (ii) and (16),

$$\begin{aligned} \sum_{k=0}^{e-1} c_{i,k}\theta_{j+k} &= -\frac{f^2}{q} + f\delta_i + \frac{1}{q}\sum_{l=0}^{e-1}\theta_l\theta_{l+i}\sum_{k=0}^{e-1}\theta_{l+k+\frac{1}{2}e}\theta_{j+k} \\ &= -\frac{f^2}{q} + f\delta_i + \frac{1}{q}\sum_{l=0}^{e-1}\theta_l\theta_{l+i}(q\delta_{j,l} - f) \\ &= -\frac{f^2}{q} + f\delta_i + \theta_j\theta_{j+i} - \frac{1}{q}f(q\delta_i - f) = \theta_j\theta_{j+i}. \end{aligned}$$

Therefore, in both cases, for $0 \leq i,\ j \leq e-1$,

$$\theta_i\theta_j = \sum_{k=0}^{e-1} c_{i-j,k-j}\theta_k = \sum_{k=0}^{e-1} c_{j-i,k-i}\theta_k. \tag{18}$$

That is, in matrix notation,

$$\begin{bmatrix} c_{0,0} & c_{0,1} & \dots & c_{0,e-1} \\ c_{1,0} & c_{1,1} & \dots & c_{1,e-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{e-1,0} & c_{e-1,1} & \dots & c_{e-1,e-1} \end{bmatrix} \begin{bmatrix} \theta_j \\ \theta_{j+1} \\ \vdots \\ \theta_{j+e-1} \end{bmatrix} = \theta_j \begin{bmatrix} \theta_j \\ \theta_{j+1} \\ \vdots \\ \theta_{j+e-1} \end{bmatrix}. \tag{19}$$

Call C the square matrix in the left-hand side of (19). That equality shows that the θ_j, $0 \leq j \leq e-1$, are eigenvalues of C with eigenvectors $[\theta_j, \theta_{j+1}, \dots, \theta_{j+e-1}]^t$. Let

$$P = \begin{bmatrix} \theta_0 & \theta_{e-1} & \dots & \theta_1 \\ \theta_1 & \theta_0 & \dots & \theta_2 \\ \vdots & \vdots & \ddots & \vdots \\ \theta_{e-1} & \theta_{e-2} & \dots & \theta_0 \end{bmatrix} \tag{20}$$

(a circulant matrix). Then $P^{-1}CP = \operatorname{diag}[\theta_0, \theta_{e-1}, \theta_{e-2}, \dots, \theta_1]$. Thus the characteristic polynomial of C factors as

$$\det(xI - C) = (x-\theta_0)(x-\theta_1)\dots(x-\theta_{e-1}).$$

This shows in particular that the θ_i are algebraic integers.

It follows from (i) and (18) that $\mathbb{Q}(\theta_0, \theta_1, \dots, \theta_{e-1})$ is a vector space of dimension e over $\mathbb{Q}$, with $B = \{\theta_0, \theta_1, \dots, \theta_{e-1}\}$ a basis. We affirm that it is a cyclic extension of $\mathbb{Q}$. In fact, the permutation of B defined by $\theta_i \mapsto \theta_{i+1}$ extends by linearity to an automorphism of $\mathbb{Q}(\theta_0, \theta_1, \dots, \theta_{e-1})$ of order e, as can be easily verified (use (18) to prove that it preserves multiplication). Therefore $\det(xI - C)$ is irreducible over $\mathbb{Q}$ (since all its roots are conjugate to θ_0 over $\mathbb{Q}$) and $\mathbb{Q}(\theta_0, \theta_1, \dots, \theta_{e-1}) = \mathbb{Q}(\theta_0)$.

Define the $e \times e$ matrices $R = [\delta_{i+1,j}]_{i,j}$ and $E = [1]_{i,j}$, that is,

$$R = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{bmatrix}, \qquad E = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \end{bmatrix}, \tag{21}$$

and define

$$e' = \begin{cases} 0\,, & \text{if } f \text{ is even,} \\ \frac{e}{2}\,, & \text{if } f \text{ is odd.} \end{cases} \tag{22}$$

A straightforward calculation shows that

$$P(P^t - fE) = qR^{e'}. \tag{23}$$

In fact, the equalities $PE = -E$ and (23) are equivalent to conditions (ii) and (iii). By (23) we have $\det(P)\det(P^t - fE) = \pm q^e$. Since the discriminant

$$D(\theta_0, \theta_1, \dots, \theta_{e-1}) = \det(P)^2$$

and since the numbers θ_i are algebraic integers, the absolute discriminant of $\mathbb{Q}(\theta_0)$ divides a power of q. Therefore, by Kronecker-Weber Theorem, $\mathbb{Q}(\theta_0) \subseteq \mathbb{Q}(\zeta_{q^k})$ for some integer k, which implies that $\mathbb{Q}(\theta_0) \subseteq \mathbb{Q}(\zeta_q)$ and that $\mathbb{Q}(\theta_0) = \mathbb{Q}(\eta_0)$, since $\mathbb{Q}(\eta_0)$ is the only subfield of $\mathbb{Q}(\zeta_{q^k})$ of degree e over $\mathbb{Q}$.

Rearrange the set $\{\theta_0, \theta_1, \dots, \theta_{e-1}\}$ in such a way that the automorphism $\eta_i \mapsto \eta_{i+1}$ of $\mathbb{Q}(\eta_0)$ sends θ_i to θ_{i+1}. Write $\theta_0 = \sum_{j=0}^{e-1} d_j \eta_j$, with $d_j \in \mathbb{Z}$. Since $\sum_{i=0}^{e-1} \theta_i = \sum_{i=0}^{e-1} \eta_i = -1$, we have that $\sum_{i=0}^{e-1} d_i = 1$. If we define the circulant matrices P' and D by

$$P' = \begin{bmatrix} \eta_0 & \eta_{e-1} & \dots & \eta_1 \\ \eta_1 & \eta_0 & \dots & \eta_2 \\ \vdots & \vdots & \ddots & \vdots \\ \eta_{e-1} & \eta_{e-2} & \dots & \eta_0 \end{bmatrix} \quad \text{and} \quad D = \begin{bmatrix} d_0 & d_1 & \dots & d_{e-1} \\ d_{e-1} & d_0 & \dots & d_{e-2} \\ \vdots & \vdots & \ddots & \vdots \\ d_1 & d_2 & \dots & d_0 \end{bmatrix},$$

then $P = DP'$. Since circulant matrices commute with each other we have, by (23), that $qR^{e'} - fE = PP^t = DP'P'^tD^t = DD^tP'P'^t = DD^t(qR^{e'} - fE)$. The matrix $qR^{e'} - fE$ is invertible (because PP^t is invertible); so $DD^t = I$. In particular $\sum_{i=0}^{e-1} d_i^2 = 1$. This, and the fact that the numbers d_i are integers such that $\sum_{i=0}^{e-1} d_i = 1$, imply that one of these numbers is 1 and the others are 0. Therefore D is a permutation matrix and $\{\theta_0, \theta_1, \dots, \theta_{e-1}\} = \{\eta_0, \eta_1, \dots, \eta_{e-1}\}$, as we wanted to prove.

Now we show characterizations of the periods η_i and of the integers $a_{i,j}$ (or, what is equivalent, of the cyclotomic numbers (i, j)) in which we gradually diminish the conditions on the η_i and increase the conditions on the $a_{i,j}$.

Proposition 2. *Let $c_{i,j}$, $i, j \in \mathbb{Z}$, be integers such that, for all i, j,*

(i) $c_{i,j} = c_{i+e,j} = c_{i,j+e}$,

(ii) $\sum_{k=0}^{e-1} c_{i,k} = f - q\delta_i$ *(δ_i is defined in (5)),*

(iii) $\sum_{k=0}^{e-1} c_{k,j} = -\delta_{0,j}$.

Let $\theta_0, \theta_1, \dots, \theta_{e-1}$ be elements in a field K containing $\mathbb{Q}$ such that

(iv) *$\theta_0, \theta_1, \dots, \theta_{e-1}$ are linearly independent over $\mathbb{Q}$,*

(v) $\theta_i\theta_j = \sum_{k=0}^{e-1} c_{j-i,k-i}\theta_k$ *for $0 \le i,\ j \le e-1$.*

Then $\theta_0, \theta_1, \dots, \theta_{e-1}$ are (in a certain order) the periods $\eta_0, \eta_1, \dots, \eta_{e-1}$ and $c_{i,j}$ are the corresponding numbers $a_{i,j} = (i, j) - f\delta_i$ defined in (1).

Conversely if $\theta_i = \eta_i$ and $c_{i,j} = a_{i,j}$ for $i, j \in \mathbb{Z}$, then the above conditions are satisfied.

Proof. It is clear, by (3), (13) and (14), that the periods η_i and the numbers $a_{i,j}$ satisfy the conditions of the proposition.

Suppose that conditions (i)–(v) are satisfied. Define $\theta_{i+ej} = \theta_i$ for $0 \le i \le e-1$

and $j \in \mathbb{Z}$. By (iii) and (v),

$$\begin{aligned}\theta_i \sum_{j=0}^{e-1} \theta_j &= \sum_{j=0}^{e-1} \sum_{k=0}^{e-1} c_{j-i,k-i}\theta_k \\ &= \sum_{k=0}^{e-1} (\sum_{j=0}^{e-1} c_{j-i,k-i})\theta_k = \sum_{k=0}^{e-1} (-\delta_{k,i})\theta_k = -\theta_i.\end{aligned}$$

Therefore

$$\sum_{j=0}^{e-1} \theta_j = -1. \tag{24}$$

By (v), $\theta_i\theta_{i+j} = \sum_{k=0}^{e-1} c_{j,k}\theta_{k+i}$. So, by (24),

$$\sum_{i=0}^{e-1} \theta_i\theta_{i+j} = \sum_{k=0}^{e-1} c_{j,k} \sum_{i=0}^{e-1} \theta_{k+i} = -\sum_{k=0}^{e-1} c_{j,k}$$

and, by (ii),

$$\sum_{i=0}^{e-1} \theta_i\theta_{i+j} = q\delta_j - f, \tag{25}$$

for $0 \leq j \leq e-1$.

By (v), $\theta_{k+i}\theta_{k+j} = \sum_{l=0}^{e-1} c_{j-i,l-i}\theta_{k+l}$. So, by (ii) and (25),

$$\begin{aligned}\sum_{k=0}^{e-1} \theta_k\theta_{k+i}\theta_{k+j} &= \sum_{l=0}^{e-1} c_{j-i,l-i} \sum_{k=0}^{e-1} \theta_k\theta_{k+l} \\ &= \sum_{l=0}^{e-1} c_{j-i,l-i}(q\delta_l - f) \\ &= \begin{cases} qc_{j-i,-i} - f(f - q\delta_{j-i}) \ , & \text{if } f \text{ is even,} \\ qc_{j-i,\frac{1}{2}e-i} - f(f - q\delta_{j-i}) \ , & \text{if } f \text{ is odd.} \end{cases}\end{aligned}$$

Therefore

$$\frac{1}{q}\left(f^2 + \sum_{k=0}^{e-1} \theta_k\theta_{k+i}\theta_{k+j}\right) = \begin{cases} c_{j-i,-i} + f\delta_{j-i} \ , & \text{if } f \text{ is even,} \\ c_{j-i,\frac{1}{2}e-i} + f\delta_{j-i} \ , & \text{if } f \text{ is odd ,} \end{cases} \tag{26}$$

for $0 \leq i, \ j \leq e-1$ (in particular, these numbers are integers).

By (iv), (24), (25), and (26) we see that all conditions of Proposition 1 are satisfied by the θ_i. Therefore $\{\theta_0, \theta_1, \ldots, \theta_{e-1}\} = \{\eta_0, \eta_1, \ldots, \eta_{e-1}\}$. Finally, by (v), after some reordering, $c_{i,j} = a_{i,j}$ for $0 \leq i, \ j \leq e-1$. This ends the proof of Proposition 2.

Let R be the matrix defined in (21) and T the matrix $[\eta_0, \eta_1, \ldots, \eta_{e-1}]^t$. We can write equality (3) as

$$(27) \qquad (A - \eta_k I)R^k T = 0 \ , \quad \text{where } A = [a_{i,j}]_{0 \le i,j \le e-1} \ ,$$

for $0 \le k \le e-1$ (see (19)). Since the minimal polynomial of η_0 over $\mathbb{Q}$ has degree e, if $e > 1$ any set of $e-1$ rows of $A - \eta_0 I$ is linearly independent over $\mathbb{C}$ (fix an embedding $\mathbb{Q}(\eta_0) \subseteq \mathbb{C}$). On the other hand, by (27), the rows of all matrices $(A - \eta_k I)R^k$, $0 \le k \le e-1$, are orthogonal to $\overline{T}^t$ (in the unitary space $\mathbb{C}^e$). Therefore, all these rows are linear combinations of any fixed set of $e-1$ rows of $A - \eta_0 I$. So, if for any r, k, l such that $0 \le r,\ k,\ l \le e-1$ we replace the r-th row of $A - \eta_0 I$ by the l-th row of $(A - \eta_k I)R^k$, we get a singular matrix, that is,

(28)

$$\det \begin{bmatrix} a_{0,0} - \eta_0 & \cdots & a_{0,r-1} & \cdots & a_{0,l+k} & \cdots & a_{0,e-1} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{r-1,0} & \cdots & a_{r-1,r-1} - \eta_0 & \cdots & \cdot & \cdots & a_{r-1,e-1} \\ a_{l,e-k} & \cdots & a_{l,e-k+r-1} & \cdots & a_{l,l} - \eta_k & \cdots & a_{l,e-k-1} \\ a_{r+1,0} & \cdots & a_{r+1,r-1} & \cdots & \cdot & \cdots & a_{r+1,e-1} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{e-1,0} & \cdots & a_{e-1,r-1} & \cdots & a_{e-1,l+k} & \cdots & a_{e-1,e-1} - \eta_0 \end{bmatrix} = 0$$

for $0 \le r,\ k,\ l \le e-1$.

Call $\alpha_{r,m}$ the cofactor of the r, m entry of $A - \eta_0 I$. That is,

$$(29) \quad \alpha_{r,m} = (-1)^{r+m} \det[a_{i,j} - \delta_{i,j}\eta_0]_{0 \le i,j \le e-1, i \ne r, j \ne m} \ , \qquad 0 \le r,\ m \le e-1.$$

Let $0 \le r,\ k,\ l \le e-1$ be arbitrary integers. By (28) we have

$$\sum_{j=0}^{e-1} a_{l,e-k+j}\alpha_{r,j} = \sum_{j=0}^{e-1} \delta_{l,j-k}\eta_k\alpha_{r,j} = \eta_k\alpha_{r,l+k}$$

(subindices modulo e). That is, $\eta_k\alpha_{r,l} = \sum_{j=0}^{e-1} a_{l-k,j-k}\alpha_{r,j}$. In particular, by (12),

$$\begin{aligned} \eta_k\alpha_{r,0} &= \sum_{j=0}^{e-1} a_{k,j}\alpha_{r,j} \\ &= \sum_{j=0}^{e-1} (a_{k,j} - \delta_{k,j}\eta_0)\alpha_{r,j} + \sum_{j=0}^{e-1} \delta_{k,j}\eta_0\alpha_{r,j} = \eta_0\alpha_{r,k}. \end{aligned}$$

Therefore, for $0 \le r,\ k,\ l \le e-1$,

$$(30) \qquad \eta_k = \frac{\eta_0}{\alpha_{r,0}}\alpha_{r,k} \quad \text{and} \quad \eta_0\alpha_{r,k}\alpha_{r,l} = \sum_{j=0}^{e-1} a_{l-k,j-k}\alpha_{r,0}\alpha_{r,j}$$

(note that $\alpha_{r,0} \ne 0$). In particular, the numbers $\alpha_{r,0}, \alpha_{r,1}, \ldots, \alpha_{r,e-1}$ are linearly independent over $\mathbb{Q}$.

The above properties allow us to give a characterization of the numbers $a_{i,j}$ that is more independent of conditions on the periods and brings us closer to our main result.

Proposition 3. *Let $c_{i,j}$, $i,j \in \mathbb{Z}$, be integers such that, for all i,j,*
(i) $c_{i,j} = c_{i+e,j} = c_{i,j+e}$,
(ii) $\sum_{k=0}^{e-1} c_{i,k} = f - q\delta_i$,
(iii) $\sum_{k=0}^{e-1} c_{k,j} = -\delta_{0,j}$.
Let C be the matrix $[c_{i,j}]_{0\le i,j\le e-1}$, θ_0 an eigenvalue of C, and r a fixed integer, $0 \le r \le e-1$. If $e > 1$ call $\gamma_{r,0}, \gamma_{r,1}, \dots, \gamma_{r,e-1}$ the cofactors of $C-\theta_0 I$ corresponding to the r-th row, that is,

$$\gamma_{r,m} = (-1)^{r+m} \det[c_{i,j} - \delta_{i,j}\theta_0]_{0\le i,j\le e-1, i\ne r, j\ne m}.$$

Suppose that
(iv) *The characteristic polynomial of C is irreducible over $\mathbb{Q}$,*
(v) $\theta_0\gamma_{r,k}\gamma_{r,l} = \sum_{j=0}^{e-1} c_{l-k,j-k}\gamma_{r,0}\gamma_{r,j}$ *for $0 \le k,\ l \le e-1$.*
Then, after some reordering of the columns of C, the numbers $c_{i,j}$ are the integers $a_{i,j} = (i,j) - f\delta_i$ defined in (1).

Conversely if $c_{i,j} = a_{i,j}$ for $i,j \in \mathbb{Z}$ (and, for example, $\theta_0 = \eta_0$), then the above conditions are satisfied.

Proof. We know, by (1), (13), (14), (29), (30) and the comment after (30), that the numbers $a_{i,j}$ and η_0 satisfy the conditions of the proposition.

Suppose that conditions (i)–(v) are satisfied. By (iv), $\gamma_{r,0} \ne 0$. Define $\theta_k = \frac{\theta_0}{\gamma_{r,0}}\gamma_{r,k}$ for $0 \le k \le e-1$. By (v), for $0 \le k,\ l \le e-1$,

$$\theta_k\theta_l = \sum_{j=0}^{e-1} c_{l-k,j-k}\theta_j. \tag{31}$$

By (iv) and (31), the field $\mathbb{Q}(\theta_0, \theta_1, \dots, \theta_{e-1})$ has dimension e over $\mathbb{Q}$. Therefore, by (31), $\theta_0, \theta_1, \dots, \theta_{e-1}$ are linearly independent over $\mathbb{Q}$. That shows that the numbers $c_{i,j}$ and θ_i satisfy all conditions of Proposition 2 and so, after some reordering, $\theta_i = \eta_i$ and $c_{i,j} = a_{i,j}$ for $0 \le i,\ j \le e-1$, as we wanted to prove.

By (3) we have, for $0 \le i,\ j \le e-1$,

$$\begin{aligned}\eta_0\eta_i\eta_j &= \sum_{k=0}^{e-1} a_{i,k}\eta_k\eta_j = \sum_{k=0}^{e-1} a_{i,k}\sum_{l=0}^{e-1} a_{j-k,l-k}\eta_l \\ &= \sum_{l=0}^{e-1}(\sum_{k=0}^{e-1} a_{i,k}a_{j-k,l-k})\eta_l.\end{aligned}$$

Therefore, using the equality $\eta_0\eta_i\eta_j = \eta_0\eta_j\eta_i$ and (12),

$$\sum_{k=0}^{e-1} a_{-i,k-i}a_{j-k,l-k} = \sum_{k=0}^{e-1} a_{i,k}a_{j-k,l-k} = \sum_{k=0}^{e-1} a_{j,k}a_{i-k,l-k} = \sum_{k=0}^{e-1} a_{j,k}a_{k-i,l-i} \tag{32}$$

for $0 \le i,\ j,\ l \le e-1$.

The following theorem characterizes the numbers $a_{i,j}$ as the integral solutions of a system of linear and quadratic equations such that the characteristic polynomial of the matrix $[a_{i,j}]_{0\le i,j\le e-1}$ is irreducible over $\mathbb{Q}$.

Theorem 1. *Let $C = [c_{i,j}]_{0\le i,j\le e-1}$ be a matrix with entries in $\mathbb{Z}$. Define $c_{i+ke,j+le} = c_{i,j}$ for $0 \le i,\ j \le e-1$ and $k,l \in \mathbb{Z}$. Suppose that for all integers i,j and l we have*

(i) $\sum_{k=0}^{e-1} c_{i,k} = f - q\delta_i$ *(δ_i is defined in (5)),*
(ii) $\sum_{k=0}^{e-1} c_{k,j} = -\delta_{0,j}$*,*
(iii) $\sum_{k=0}^{e-1} c_{i,k+i}c_{j-k,l-k} = \sum_{k=0}^{e-1} c_{j,k}c_{k+i,l+i}$*,*
(iv) $\det(xI - C)$ *is irreducible over $\mathbb{Q}$.*

Then (after some reordering due to our choice of the labeling of the periods $\eta_0,\eta_1,\dots,\eta_{e-1}$), $c_{i,j} = a_{i,j} = (i,j) - f\delta_i$, for $0 \le i,\ j \le e-1$, where $a_{i,j}$ are the numbers defined in (1) and (i,j) are the cyclotomic numbers of order e.

Conversely if $c_{i,j} = a_{i,j}$ for $0 \le i,\ j \le e-1$, then the above conditions are satisfied.

Proof. We know, by (13), (14) and (32), that the numbers $a_{i,j}$ satisfy the conditions of the theorem.

Let θ_0 be an eigenvalue of C in some extension of $\mathbb{Q}$. Let r be a fixed integer, $0 \le r \le e-1$. We can assume $e > 1$. Call $\gamma_{r,0}, \gamma_{r,1}, \dots, \gamma_{r,e-1}$ the cofactors of $C - \theta_0 I$ corresponding to the r-th row. That is

$$\gamma_{r,m} = (-1)^{r+m}\det[c_{i,j} - \delta_{i,j}\theta_0]_{0\le i,j\le e-1, i\ne r, j\ne m}\ , \tag{33}$$

for $0 \le m \le e-1$. Define $\gamma_{r,m+ke} = \gamma_{r,m}$ for $0 \le m \le e-1$ and $k \in \mathbb{Z}$. Call $\Gamma_r = [\gamma_{r,0}, \gamma_{r,1}, \dots, \gamma_{r,e-1}]^t$. By (iv), $\gamma_{r,0} \ne 0$.

Since $(C - \theta_0 I)\Gamma_r = 0$, we have

$$\sum_{l=0}^{e-1} c_{m,l}\gamma_{r,l} = \sum_{l=0}^{e-1} \delta_{m,l}\theta_0\gamma_{r,l} = \theta_0\gamma_{r,m}\ , \tag{34}$$

for $0 \le m \le e-1$. By (iii), for all $i,j \in \mathbb{Z}$,

$$\sum_{k=0}^{e-1} c_{i,k+i}\sum_{l=0}^{e-1} c_{j-k,l-k}\gamma_{r,l+i} = \sum_{k=0}^{e-1} c_{j,k}\sum_{l=0}^{e-1} c_{k+i,l+i}\gamma_{r,l+i} = \theta_0\sum_{k=0}^{e-1} c_{j,k}\gamma_{r,k+i}. \tag{35}$$

Define

$$\epsilon_{i,j} = \sum_{k=0}^{e-1} c_{j-i,k-i}\gamma_{r,k}, \qquad i,j \in \mathbb{Z}. \tag{36}$$

By (34), for all $j \in \mathbb{Z}$,

$$\epsilon_{0,j} = \theta_0\gamma_{r,j} \tag{37}$$

and, by (35), $\sum_{k=0}^{e-1} c_{i,k+i}\epsilon_{k+i,j+i} = \theta_0\epsilon_{i,j+i}$. Therefore, for all $i,j \in \mathbb{Z}$,

$$\sum_{k=0}^{e-1}(c_{i,k} - \delta_{i,k}\theta_0)\epsilon_{k,j} = 0.$$

Since, by (iv), $C - \theta_0 I$ has rank $e-1$ and since $(C-\theta_0 I)\Gamma_r = 0$, the equality above implies that for all $j \in \mathbb{Z}$ there is a number λ_j such that

$$[\epsilon_{0,j}, \epsilon_{1,j} \dots \epsilon_{e-1,j}] = [\gamma_{r,0}, \gamma_{r,1}, \dots, \gamma_{r,e-1}]\lambda_j. \tag{38}$$

By (37) and (38), $\lambda_j = \frac{\epsilon_{0,j}}{\gamma_{r,0}} = \frac{\theta_0}{\gamma_{r,0}}\gamma_{r,j}$. Therefore, by (38), $\epsilon_{i,j} = \frac{\theta_0}{\gamma_{r,0}}\gamma_{r,i}\gamma_{r,j}$ for all $i, j \in \mathbb{Z}$ and, by (36),

$$\theta_0 \gamma_{r,i}\gamma_{r,j} = \sum_{k=0}^{e-1} c_{j-i,k-i}\gamma_{r,0}\gamma_{r,k} \tag{39}$$

for $0 \le i,\ j \le e-1$. Properties (i), (ii), (iv) and (39) show that the integers $c_{i,j}$ satisfy all conditions of Proposition 3. Therefore, after some reordering, $c_{i,j} = a_{i,j}$ for $0 \le i,\ j \le e-1$, as we wanted to prove.

Observation. Let $A = [a_{i,j}]_{0\le i,j\le e-1}$, R be the matrix defined in (21) and denote the i-th row of a matrix B by $[B]_i$ (starting from $i=0$). From (13), (14), (12) and (32) we obtain the equivalent set of properties:

(a) The sum of the elements of the i-th row of A is $f - q\delta_i$.
(b) The sum of the elements of the j-th column of A is $-\delta_{0,j}$.
(c) $[R^{-k}AR^k]_l = [R^{-l}AR^l]_k$, for $0 \le k,\ l \le e-1$.
(d) $[AR^{-k}AR^k]_l = [AR^{-l}AR^l]_k$, for $0 \le k,\ l \le e-1$.

We also have

(e) $\det(xI - A)$ is irreducible over $\mathbb{Q}$.

By Theorem 1 we know that these properties characterize the numbers $a_{i,j}$.

References

1. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.
2. Thomas Storer, *Cyclotomy and difference sets*, Lectures in Adv. Math., Markham, Chicago, 1967. MR **36:**128
3. F. Thaine, *On the p-part of the ideal class group of* $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ *and Vandiver's Conjecture*, Michigan Math. J. (to appear).
4. L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math., Springer-Verlag, New York, 1982. MR **85g:**11001

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

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