FAMILIES OF IRREDUCIBLE POLYNOMIALS OF GAUSSIAN PERIODS AND MATRICES OF CYCLOTOMIC NUMBERS

F. THAINE

ABSTRACT. Given an odd prime p we show a way to construct large families of polynomials $P_q(x) \in \mathbb{Q}[x]$, $q \in \mathcal{C}$, where $\mathcal{C}$ is a set of primes of the form $q \equiv 1 \bmod p$ and $P_q(x)$ is the irreducible polynomial of the Gaussian periods of degree p in $\mathbb{Q}(\zeta_q)$. Examples of these families when $p = 7$ are worked in detail. We also show, given an integer $n \geq 2$ and a prime $q \equiv 1 \bmod 2n$, how to represent by matrices the Gaussian periods $\eta_0, \dots, \eta_{n-1}$ of degree n in $\mathbb{Q}(\zeta_q)$, and how to calculate in a simple way, with the help of a computer, irreducible polynomials for elements of $\mathbb{Q}(\eta_0)$.

INTRODUCTION

Let p be an odd prime number and ζ_p a p-th primitive root of 1. Let S be the set of all primes $q \equiv 1 \bmod p$. For each $q \in S$, choose a primitive root $s = s_q$ modulo q, and a q-th primitive root ζ_q of 1 (the choice of s_q will be made more precise later). For $q \in S$ and $0 \leq i \leq p - 1$, define the Gaussian periods of degree p in $\mathbb{Q}(\zeta_q)$ by $\eta_i = \eta_i(q) = \sum_{j=0}^{f-1} \zeta_q^{s^{i+pj}}$, where $f = f_q = (q - 1)/p$. In Section 1 we show a way to construct large families of polynomials $P_q(x) \in \mathbb{Q}[x]$, $q \in \mathcal{C}$, where $\mathcal{C} \subseteq S$ and $P_q(x)$ is the irreducible polynomial of the periods $\eta_i(q)$. When p is small, we could take $\mathcal{C} = S$. More precisely, for any p, the set of indices could, in principle, include all primes $q \in S$ such that the prime ideals over q in $\mathbb{Q}(\zeta_p)$ are principal. Of course, if we do not put some restrictions, the formulas describing these families will soon become enormously complicated. As examples we show, for $p = 7$, four two-parameter families of polynomials $P_q(x)$, whose indices put together include all the primes of the form $(a^7 + b^7)/(a + b)$ (see Proposition 1, and the MAPLE program, at the end of Section 1, to calculate the polynomials $P_q(x)$ for the four families). These results can be generalized to arbitrary positive integers in the place of the primes p.

For $p = 5$, H.W. Lloyd Tanner obtained, in [9], an expression for the family of polynomials $P_q(x)$, $q \in S$, in terms of coefficients of certain divisors of q in $\mathbb{Q}(\zeta_5)$. This result was used by Emma Lehmer, in [5], who gave a new expression for that family. In [6] Lehmer shows a family of polynomials of degree 5, which is obtained by a translation of a family of polynomials $P_q(x)$, and such that the roots of the polynomials in the family are units. This result has been used by Schoof and Washington in [7] to find some real cyclotomic fields with large class numbers.

We were not able to find, for $p = 7$, families of polynomials whose roots are units, which are translations of families of polynomials $P_q(x)$. This seems to be a feasible task though, and an interesting one in light of the results mentioned above. For particular primes q, polynomials with the desired properties can be easily obtained; for example:

$$P_{43}(x - 2) = x^7 - 13x^6 + 54x^5 - 75x^4 - 2x^3 + 44x^2 - 17x + 1$$

and

$$P_{127}(x + 2) = x^7 + 15x^6 + 42x^5 - 231x^4 - 1130x^3 - 836x^2 + 183x - 1.$$

In Section 2 we work with a fixed integer $n \geq 2$ and a fixed prime $q \equiv 1 \bmod 2n$. Let ζ_q be a q-th primitive root of unity, s a primitive root modulo q, and $f = (q - 1)/n$. For $0 \leq i, j \leq n - 1$, define the Gaussian periods of degree n of $\mathbb{Q}(\zeta_q)$ by $\eta_i = \sum_{k=0}^{f-1} \zeta_q^{s^{i+kn}}$, and the integers $c_{i,j}$ by $\eta_0 \eta_i = \sum_{k=0}^{n-1} c_{i,k} \eta_k$. (Recall that $\eta_0, \ldots, \eta_{n-1}$ is an integral basis of $\mathbb{Q}(\eta_0)$.) The numbers $c_{i,j}$ are closely related to the cyclotomic numbers (i, j) of order n (see formula (15)). In this section we show how to calculate the $c_{i,j}$, and how to use these numbers to find minimal polynomials of elements of $\mathbb{Q}(\eta_0)$.

Define the $n \times n$ matrices C and K by: $C = [c_{i,j}]_{0 \leq i,j \leq n-1}$, and

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

Using the facts that the conjugates $H_i = K^{-i} C K^i$, $0 \leq i \leq n - 1$, of C are simultaneously diagonalizable, and that the characteristic polynomial of C is the minimal polynomial of the periods η_i, we show that we can identify η_0 with C, η_i with H_i, and elements in $\mathbb{Q}(\eta_0)$ with linear combinations, over $\mathbb{Q}$, of the H_i. With this identification, characteristic polynomials of elements in $\mathbb{Q}(\eta_0)$ correspond to characteristic polynomials of the associated matrices. This reduces, in a way, the problem of calculating minimal polynomials of elements of $\mathbb{Q}(\eta_0)$ to the problem of calculating C. The properties that C is a matrix with entries in $\mathbb{Z}$, which commutes with its conjugates H_i (formula (21)), and whose characteristic polynomial is irreducible over $\mathbb{Q}$, together with some simple linear conditions on its entries $c_{i,j}$, actually characterize this matrix (Proposition 2).

To calculate C we use the fact that $0 \leq (i, j) \leq q - 1$, and a congruence modulo q first found by V.A. Lebesgue (see [4], Section III). We deduce both the inequality and the congruence from an expression of the cyclotomic numbers (i, j) in terms of Jacobi sums that is an immediate consequence of [1], formula (26) (see Proposition 3 and its corollary). We end Section 2 with a MAPLE program to carry out all calculations mentioned above. In particular this program is a tool to investigate whether a given linear combination of periods η_i is a unit of $\mathbb{Q}(\eta_0)$.

1. Families of irreducible polynomials of Gaussian periods of degree p, Jacobi sums and cyclotomic numbers

Let p be an odd prime, ζ_p a p-th primitive root of 1, and S_1 the set of all primes $q \equiv 1 \bmod p$ such that the prime ideals over q in $\mathbb{Q}(\zeta_p)$ are principal. For each $q \in S_1$, let $f = f_q = (q-1)/p$ and let ζ_q be a q-th primitive root of 1. Suppose that $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$, with $a_i \in \mathbb{Z}$, is such that its norm is a prime number $q \neq p$; that is, $N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha) = q \in S_1$. We begin by working in $\mathbb{Q}(\zeta_p)$, though here we are mainly interested in the subfield of degree p of $\mathbb{Q}(\zeta_q)$.

Choose a primitive root s modulo q such that $s^f \equiv \zeta_p \bmod \alpha$, and define the Gaussian periods $\eta_0, \ldots, \eta_{p-1}$ by

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

and the Jacobi sums $J_1, \ldots, J_{p-2}$ by

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

where $\operatorname{ind}_s(k)$ is the least nonnegative integer such that $s^{\operatorname{ind}_s(k)} \equiv k \bmod q$. We have that $J_n \equiv 1 \bmod (\zeta_p - 1)^2$, as is shown in [2], Theorem 1 (moreover, if $p > 3$, then $J_n \equiv 1 \bmod (\zeta_p - 1)^3$; see the Remark after Theorem 1 in [2]). Write

$$(3) \qquad J_n = \sum_{k=0}^{p-1} d_{n,k} \zeta_p^k, \quad \text{with} \quad d_{n,k} \in \mathbb{Z} \quad \text{such that} \quad \sum_{k=0}^{p-1} d_{n,k} = 1.$$

This uniquely determines 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 $d_{n+ip,k+jp} = d_{n,k}$. The numbers $d_{n,k}$ are studied in some detail in [11].

A summary of our simple method: By using Stickelberger's Theorem, write the coefficients $d_{n,k}$ of the Jacobi sums in terms of the coefficients a_i of α. Then write the cylotomic numbers (i, j) of order p corresponding to q (defined below) in terms of the $d_{n,k}$, and finally, by means of a well-known formula, write the irreducible polynomial $P_q(x)$ of the Gaussian periods η_i in terms of the (i, j). For small p, and suitable restrictions on the type of the prime q, we can obtain in that way a reasonably simple formula for $P_q(x)$ in terms of the a_i. A more detailed explanation of this construction follows.

If $p \nmid a$ let $\sigma_a \in \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ be the automorphism such that $\sigma_a(\zeta_p) = \zeta_p^a$. The ideals (J_n) factor in $\mathbb{Z}[\zeta_p]$ as follows:

$$(4) \qquad (J_n) = \left(\prod_{l=1}^{p-1} \sigma_l^{-1}(\overline{\alpha})^{\left[\frac{(n+1)l}{p}\right] - \left[\frac{nl}{p}\right]} \right),$$

where $[\rho]$ denotes the integral part of a real number ρ, and the bar denotes complex conjugation (see [3], FAC 3, page 13).

Let $\beta_n = \prod_{l=1}^{p-1} \sigma_l^{-1}(\overline{\alpha})^{\left[\frac{(n+1)l}{p}\right] - \left[\frac{nl}{p}\right]}$. Since $J_n \overline{J_n} = q$ and $\beta_n \overline{\beta_n} = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\alpha) = q$, it follows from (4) that $J_n = \pm \zeta_p^{k_n} \beta_n$, for some $k_n \in \mathbb{Z}$ (because all units of $\mathbb{Z}[\zeta_p]$

are products of real units with roots of 1). That is, for $1 \leq n \leq p - 2$,

$$(5) \qquad J_n = \pm \zeta_p^{k_n} \prod_{l=1}^{p-1} \sigma_l^{-1}(\overline{\alpha})^{\left[\frac{(n+1)l}{p}\right] - \left[\frac{nl}{p}\right]}.$$

The fact that $J_n \equiv 1 \bmod (\zeta_p - 1)^2$ allows us to determine the $\pm$ sign and the value of k_n in the above formula. This shows that we can express the numbers $d_{n,k}$ in terms of the coefficients a_i of α, when we can perform the indicated calculations.

For $0 \leq i, j \leq p - 1$, the cyclotomic number (i, j) of order p, corresponding to q, is defined as the number of ordered pairs of integers $\langle k, l \rangle$, $0 \leq k, l \leq f - 1$, such that $1 + s^{pk+i} \equiv s^{pl+j} \bmod q$. (See, for example, [1] and [8].) We can express the cyclotomic numbers of order p in terms of the coefficients $d_{n,k}$ as follows:

$$(6) \qquad (i, j) = -\frac{1}{p}\Big(\delta_{0,i} + \delta_{0,j} + \delta_{i,j} - f - 1 + \sum_{n=1}^{p-2} d_{n,i+jn}\Big)$$

(see, for example, [11], formula (7)).

The cyclotomic numbers (i, j) and the Gaussian periods η_i defined in (1) are connected by the multiplication table of the periods. For $k, l \in \mathbb{Z}$ define

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

We have, for $0 \leq i \leq p - 1$,

$$(7) \qquad \eta_0 \eta_i = \sum_{k=0}^{p-1} c_{i,k} \eta_k,$$

where $c_{i,j} = (i, j) - f \delta_{0,i}$ (see [1], formula (6)). That is (by (6))

$$(8) \qquad c_{i,j} = -\frac{1}{p}\Big(q\delta_{0,i} + \delta_{0,j} + \delta_{i,j} - f - 1 + \sum_{n=1}^{p-2} d_{n,i+jn}\Big).$$

Set $C = [c_{i,j}]_{0 \leq i,j \leq p-1}$. It follows easily from (7) that the irreducible polynomial $P_q(x)$ of the periods η_i is equal to the characteristic polynomial of the matrix C (see (16), or [1], formula (9)). That is,

$$(9) \qquad P_q(x) = \det(xI - C).$$

When we are able to do the calculations involved in formulas (3), (5), (8) and (9), we can express $P_q(x)$ in terms of the coefficients a_i of α.

As an example of the above construction, let $p = 7$ and let q be a prime of the form $(a^7 + b^7)/(a + b)$, with $a, b \in \mathbb{Z}$. Without loss of generality we can assume that $a + b$ is a quadratic residue modulo 7 (since we can replace a and b by $-a$ and $-b$). Let $\omega = \zeta_7$ be a 7-th primitive root of 1. Take $\alpha = a + b\omega$; so $N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\alpha) = q$.

Set $r = (1 - (a + b)^3)/7$; it is an integer by our choice of a, b. By (5) we have that, for $1 \leq n \leq 5$,

$$J_n = \pm \omega^{k_n} \prod_{l=1}^{6} (a + b\omega^{-l^5})^{\left[\frac{(n+1)l}{7}\right] - \left[\frac{nl}{7}\right]}.$$

The numbers $\pm \omega^{k_n}$ can be determined using the congruence $J_n \equiv 1 \bmod (\omega - 1)^2$ as follows: Put $\lambda = \omega - 1$. First, we have $1 \equiv J_n \equiv \pm (a + b)^3 \equiv \pm 1 \bmod \lambda$ (since $a + b$ is a quadratic residue modulo 7). This determines the $\pm$ sign. Therefore,

$1 \equiv J_n = \left(1+\lambda\right)^{k_n} \prod_{l=1}^{6} \left(a + b(1+\lambda)^{-l^5}\right)^{\left[\frac{(n+1)l}{7}\right] - \left[\frac{nl}{7}\right]} \bmod \lambda^2$. This determines k_n.
After some straightforward calculations we obtain:

(10)

$$J_1 = J_5 = \omega^{-3b(a+b)^2}(a + b\omega^5)(a + b\omega^4)(a + b\omega)$$

$$= \omega^{-3b(a+b)^2}\left((a^3 + r) + (a^2b + r)\omega + (ab^2 + r)\omega^2 + (b^3 + r)\omega^3\right.$$
$$\left. + (a^2b + r)\omega^4 + (a^2b + ab^2 + r)\omega^5 + (ab^2 + r)\omega^6\right),$$

$$J_2 = J_4 = (a + b\omega^2)(a + b\omega^4)(a + b\omega)$$

$$= (a^3 + b^3 + r) + (a^2b + r)\omega + (a^2b + r)\omega^2$$
$$+ (ab^2 + r)\omega^3 + (a^2b + r)\omega^4 + (ab^2 + r)\omega^5 + (ab^2 + r)\omega^6,$$

$$J_3 = \omega^{-2b(a+b)^2}(a + b\omega^3)(a + b\omega^5)(a + b\omega)$$

$$= \omega^{-2b(a+b)^2}\left((a^3 + r) + (a^2b + ab^2 + r)\omega\right.$$
$$\left. + (b^3 + r)\omega^2 + (a^2b + r)\omega^3 + (ab^2 + r)\omega^4 + (a^2b + r)\omega^5 + (ab^2 + r)\omega^6\right).$$

Notice that we added r to the coefficients of each Jacobi sum in (10) in order to have their sum equal to 1. So we have (by (3)) that $d_{n,k}$ is the coefficient of ω^k in the expression for J_n in (10) (after performing the multiplication by the indicated power of ω, that corresponds to a cyclic permutation of the coefficients).

For example let us find the family of polynomials $P_q(x)$, where q is of the form $(a^7 + b^7)/(a + b)$ and a, b are integers such that the class of (a, b) modulo 7 is in $\{(3,6), (5,3), (6,5)\}$. In this case $-3b(a+b)^2 \equiv 5 \bmod 7$ and $-2b(a+b)^2 \equiv 1 \bmod 7$, and the matrix $[d_{n,k}]_{\substack{1 \leq n \leq 5 \\ 0 \leq k \leq 6}}$ is

(11)

$$\begin{bmatrix} ab^2 + r & b^3 + r & a^2b + r & a^2b + ab^2 + r & ab^2 + r & a^3 + r & a^2b + r \\ a^3 + b^3 + r & a^2b + r & a^2b + r & ab^2 + r & a^2b + r & ab^2 + r & ab^2 + r \\ ab^2 + r & a^3 + r & a^2b + ab^2 + r & b^3 + r & a^2b + r & ab^2 + r & a^2b + r \\ a^3 + b^3 + r & a^2b + r & a^2b + r & ab^2 + r & a^2b + r & ab^2 + r & ab^2 + r \\ ab^2 + r & b^3 + r & a^2b + r & a^2b + ab^2 + r & ab^2 + r & a^3 + r & a^2b + r \end{bmatrix}$$

By using (8), (11), and a computer (as shown below), we find the matrix $C = [c_{i,j}]$:

(12) $$C = \begin{bmatrix} X_0 - f & X_1 - f & X_2 - f & X_3 - f & X_4 - f & X_5 - f & X_6 - f \\ X_1 & X_6 & X_7 & X_8 & X_9 & X_{10} & X_7 \\ X_2 & X_7 & X_5 & X_{10} & X_{11} & X_{11} & X_8 \\ X_3 & X_8 & X_{10} & X_4 & X_9 & X_{11} & X_9 \\ X_4 & X_9 & X_{11} & X_9 & X_3 & X_8 & X_{10} \\ X_5 & X_{10} & X_{11} & X_{11} & X_8 & X_2 & X_7 \\ X_6 & X_7 & X_8 & X_9 & X_{10} & X_7 & X_1 \end{bmatrix},$$

where $(q = (a^7 + b^7)/(a + b)$, $f = (q - 1)/7$, $r = (1 - (a + b)^3)/7$, and)

$X_0 = (1/7)(f - 5r - 2a^3 - 3ab^2 - 2b^3 - 2)$,

$X_1 = (1/7)(f - 5r - a^3 - 2a^2b - 2b^3)$,

$X_2 = (1/7)(f - 5r - 5a^2b - ab^2)$,

$X_3 = (1/7)(f - 5r - 2a^2b - 4ab^2 - b^3)$,

$X_4 = X_6 = (1/7)(f - 5r - 3a^2b - 2ab^2)$,

$X_5 = (1/7)(f - 5r - 2a^3 - 3ab^2)$,

$X_7 = (1/7)(f - 5r - 2a^2b - 4ab^2 + 1)$,

$$X_8 = (1/7)(f - 5r - a^3 - a^2b - 2ab^2 - 2b^3 + 1),$$
$$X_9 = (1/7)(f - 5r - a^3 - 2a^2b - 2ab^2 + 1),$$
$$X_{10} = (1/7)(f - 5r - 2a^3 - 3a^2b - ab^2 - b^3 + 1),$$
$$X_{11} = (1/7)(f - 5r - 2a^2b - 2ab^2 - b^3 + 1).$$

Observation. All the matrices $C = [c_{i,j}] = [(i,j) - f\delta_{0,i}]$ of order 7 have the form shown in (12), for some values of $X_0, \ldots, X_{11}$, since $(i,j) = (-i, j-i) = (j,i)$ (considering indices modulo 7); in our particular case we also have $X_4 = X_6$.

Using (9), we obtain the following proposition. We have similar results for the other families (see below).

Proposition 1. *Let q be a prime of the form $(a^7 + b^7)/(a+b)$, where the class of (a,b) modulo 7 is in $\{(3,6),(5,3),(6,5)\}$, and let C be as in (12) (with the given values for the X_i). Then the minimal polynomial of the Gaussian periods η_i that generate the subfield of degree 7 of $\mathbb{Q}(\zeta_q)$ is $P_q(x) = det(xI - C)$.*

The expanded expression of the polynomial $P_q(x)$ in Proposition 1 is large (as can be expected when one looks for large families of characteristic polynomials). For the complete expression use the program at the end of this section. We write the first few terms:

$$P_q(x) = x^7 + x^6 + (3/7)(-a^6 + a^5b - a^4b^2 + a^3b^3 - a^2b^4 + ab^5 - b^6 + 1)x^5 +$$
$$(1/49)(3a^9 - 8a^8b + 10a^7b^2 - 7a^6b^3 - 15a^6 + 7a^5b^4 + 15a^5b - 7a^4b^5 -$$
$$15a^4b^2 + 7a^3b^6 + 15a^3b^3 - 4a^2b^7 - 15a^2b^4 - ab^8 + 15ab^5 + 3b^9 - 15b^6 +$$
$$5)x^4 + \ldots$$

Recall that the coefficients above are integers, by the condition on the values of (a, b) modulo 7.

Example. Taking $a = -1$ and $b = -2 + 7t$ in Proposition 1, we obtain the following polynomial with large coefficients as the irreducible polynomial of the Gaussian periods of degree 7 in $\mathbb{Q}(\zeta_q)$, for a prime q of the form $\big((-2 + 7t)^7 - 1\big)/(-3 + 7t)$:

$$P_q(x) = x^7 + x^6 + (-50421t^6 + 79233t^5 - 52479t^4 + 18669t^3 -$$
$$3759t^2 + 405t - 18)x^5 + (2470629t^9 - 6235397t^8 + 6924484t^7 -$$
$$4489870t^6 + 1888558t^5 - 537922t^4 + 104230t^3 - 13285t^2 +$$
$$1011t - 35)x^4 + (524596891t^{12} - 1608379479t^{11} + 2272155137t^{10} -$$
$$1954032241t^9 + 1138001970t^8 - 472123036t^7 + 142808393t^6 -$$
$$31660762t^5 + 5091002t^4 - 576766t^3 + 43452t^2 - 1937t + 38)x^3 +$$
$$(-31637227888t^{15} + 124289109560t^{14} - 228522476441t^{13} +$$
$$261191603708t^{12} - 207749427809t^{11} + 121901187807t^{10} -$$
$$54540866296t^9 + 18953450782t^8 - 5158320062t^7 + 1099336168t^6 -$$
$$181908167t^5 + 22938966t^4 - 2132384t^3 + 137837t^2 - 5535t + 104)x^2 +$$
$$(-1162668124884t^{18} + 5674927752410t^{17} - 13032560563113t^{16} +$$
$$18688844949089t^{15} - 18732951441540t^{14} + 13923406791245t^{13} -$$
$$7943898248629t^{12} + 3552897680668t^{11} - 1260797979294t^{10} +$$
$$356918021103t^9 - 80566091109t^8 + 14407317610t^7 - 2013242231t^6 +$$
$$2146290001t^5 - 16758142t^4 + 889340t^3 - 27144t^2 + 232t + 7)x +$$
$$657876380663535t^{21} - 381161366941138t^{20} + 1048145314582926t^{19} -$$
$$1819367996135445t^{18} + 2236336773065570t^{17} - 2069846143780219t^{16} +$$
$$1497350005514503t^{15} - 867360288855690t^{14} + 408838734080749t^{13} -$$
$$158472686873837t^{12} + 50835524452986t^{11} - 13534904916484t^{10} +$$
$$2990348576089t^9 - 546389495813t^8 + 81999657615t^7 - 9995633361t^6 +$$
$$973145491t^5 - 73786003t^4 + 4191970t^3 - 167512t^2 + 4186t - 49.$$

Taking $t = 0$, we get

$$P_{43}(x) = x^7 + x^6 - 18x^5 - 35x^4 + 38x^3 + 104x^2 + 7x - 49.$$

We have in total seven families like the one above, one for each residue modulo 7 of $-3b(a + b)^2$, but we need to consider only four of them if we interchange the roles of a and b. Together these families contain, as indices, all the primes q of the form $(a^7 + b^7)/(a + b)$. The coefficient of x^5 of $P_q(x)$ is equal to $-(3/7)(q-1)$ for all of them; the coefficient of x^6 is of course 1. Now we show a program for MAPLE to calculate the matrices $A = [d_{n,k}]$ and $C = [c_{i,j}]$, and the polynomials $P_q(x)$ for all those families (and to experiment with them).

The fist line of the program is to write the value of l, a number $1 \le l \le 7$, that determines the family for which the calculations will be done, and the values of a and b. Write a:='a'; b:='b'; for general formulas (that erases the previous assignments for a and b). One can also give numerical values to a and b (to check if $(a^7 + b^7)/(a + b)$ is prime write: is prime((a^7+b^7)/(a+b));) or values like a:=6+7*s; b:=5+7*t; in those cases write l:=7+modp($-3*b*(a+b)^2,7$); and replace the last line by: Pq:=sort(collect(P(x),x),x);

For the general formulas write: l:=7; for the family such that the residue of (a,b) modulo 7 is in $\{(1,0),(2,0),(4,0)\}$; l:=1; if (a,b) mod 7 is in $\{(3,1),(5,4),(6,2)\}$; l:=2; if (a,b) mod 7 is in $\{(1,1),(2,2),(4,4)\}$; l:=3; if (a,b) mod 7 is in $\{(1,3),(2,6), (4,5)\}$; l:=4; if (a,b) mod 7 is in $\{(0,1),(0,2),(0,4)\}$; l:=5; if (a,b) mod 7 is in $\{(3,6),(5,3),(6,5)\}$; l:=6; if (a,b) mod 7 is in $\{(3,5),(5,6),(6,3)\}$.

To obtain expressions (sometimes shorter) in terms of a, b, f and r in which the actual values of f and r, as polynomials in a, b, are not used in the calculations, replace f:=normal((a^7+b^7)/(a+b)−1)/7); r:=normal(1−(a+b)^3)/7); by f:='f'; r:='r'; in the second line.

A MAPLE PROGRAM TO CALCULATE THE POLYNOMIALS $P_q(x)$
FOR THE DISTINCT FAMILIES

```
a:='a'; b:='b'; l:=5;
f:=normal(((a^7+b^7)/(a+b)−1)/7): r:=normal((1−(a+b)^3)/7):
with(numtheory): with(linalg):
t1:=normal(a^3+r): t2:=normal(a^2*b+r): t3:=normal(a*b^2+r):
t4:=normal(b^3+r): t5:=normal(a^2*b+r):
t6:=normal(a^2*b+a*b^2+r): t7:=normal(a*b^2+r):
u1:=normal(a^3+b^3+r): u2:=normal(a^2*b+r): u3:=normal(a*b^2+r):
Id:=array(1..7,1..7,identity):
K:=array(1..7,1..7):
for i1 from 1 to 6 do;
for j1 from 2 to 7 do;
K[i1,j1]:=Id[i1+1,j1];
K[i1,1]:=0; K[7,j1]:=0;
K[7,1]:=1; od: od:
K:=evalm(K);
V:=array(1..1,1..7):
for v from 1 to 7 do:
V[1,v]:=t.v: od:
H:=evalm(V&*K^l):
A:=array(1..5,1..7):
```

```
for i from 1 to 7 do:
A[1,i]:=H[1,i]:
A[5,i]:=H[1,i]: od:
A[3,1]:=A[1,1]: A[3,2]:=A[1,6]: A[3,3]:=A[1,4]: A[3,4]:=A[1,2]: A[3,5]:=A[1,7]:
A[3,6]:=A[1,5]: A[3,7]:=A[1,3]: A[2,1]:=u1: A[2,2]:=u2: A[2,3]:=u2: A[2,4]:=u3:
A[2,5]:=u2: A[2,6]:=u3: A[2,7]:=u3: A[4,1]:=u1: A[4,2]:=u2: A[4,3]:=u2:
A[4,4]:=u3: A[4,5]:=u2: A[4,6]:=u3: A[4,7]:=u3:
A:=evalm(A);
A1:=concat(A,A,A,A,A,A):
F:=(i,j)->expand((-1/7)*(Id[1,i]+Id[1,j]+ Id[i,j]-f-1
+sum(A1[n,1+(i-1+(j-1)*n)], n=1..5))-f*Id[1,i]):
C:=array(1..7,1..7):
for i2 from 1 to 7 do;
for j2 from 1 to 7 do;
C[i2,j2]:=F(i2,j2): od: od:
C:=evalm(C);
P:=x->charpoly(C,x);
Pq:=sort(sort(collect(P(x),x),a),x);
```


2. CYCLOTOMIC NUMBERS AND CHARACTERISTIC POLYNOMIALS OF LINEAR COMBINATIONS OF GAUSSIAN PERIODS OF DEGREE n

Let $n \geq 2$ be an integer, $q \equiv 1 \bmod 2n$ a prime number, and $f = (q-1)/n$. We are assuming that f is even for simplicity. Let ζ_q be a q-th primitive root of 1 and s a primitive root modulo q. Define the Gaussian periods $\eta_0, \ldots, \eta_{n-1}$ of degree n of $\mathbb{Q}(\zeta_q)$ by

$$(13) \qquad \eta_i = \sum_{k=0}^{f-1} \zeta_q^{s^{i+kn}}.$$

They form a normal integral basis of $\mathbb{Q}(\eta_0)$, the only subfield of $\mathbb{Q}(\zeta_q)$ of degree n over $\mathbb{Q}$. Define the integers $c_{i,j}$, $0 \leq i, j \leq n-1$, and the matrix C by

$$(14) \qquad \eta_0 \eta_i = \sum_{k=0}^{n-1} c_{i,k} \eta_k, \qquad C = [c_{i,j}]_{0 \leq i,j \leq n-1}.$$

In this section we show how the periods η_i can be identified with certain conjugates of C, and elements of $\mathbb{Q}(\eta_0)$ with linear combinations, over $\mathbb{Q}$, of such conjugates, in such a way that characteristic polynomials of elements in $\mathbb{Q}(\eta_0)$ correspond to characteristic polynomials of the associated matrices. We will give a simple characterization of C, actually a variation of Theorem 1 of [10], which is suitable for our purposes. Finally we will show how to calculate C, and hence also the other mentioned objects, in an efficient way.

As is usual, for $0 \leq i, j \leq n-1$, we denote by (i,j) the cyclotomic number of order n, defined as the number of ordered pairs of integers $\langle k, l \rangle$, $0 \leq k, l \leq f-1$, such that $1 + s^{kn+i} \equiv s^{ln+j} \bmod q$. (See, for example, [1] or [8].) Define $\eta_{i+kn} = \eta_i$, $c_{i+kn,j+ln} = c_{i,j}$, and $(i+kn, j+ln) = (i,j)$, for $0 \leq i, j \leq n-1$ and $k, l \in \mathbb{Z}$. We have $(i,j) = (j,i) = (-i, j-i)$ (see [1], formula (14)).

We use the following version of Kronecker's delta:

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

By [1], formula 6, we have

(15) $$c_{i,j} = (i,j) - f\delta_{0,i},$$

for $0 \le i, j \le n - 1$.

Since $\eta_i \eta_j = \eta_j \eta_i$, it follows from (14) that

$$\eta_i \eta_j = \sum_{k=0}^{n-1} c_{i-j,k-j}\eta_k = \sum_{k=0}^{n-1} c_{j-i,k-i}\eta_k.$$

This proves that $c_{i,j} = c_{-i,j-i}$ and that

(16) $$C \begin{bmatrix} \eta_j \\ \eta_{j+1} \\ \vdots \\ \eta_{j+n-1} \end{bmatrix} = \eta_j \begin{bmatrix} \eta_j \\ \eta_{j+1} \\ \vdots \\ \eta_{j+n-1} \end{bmatrix},$$

with C as in (14). In particular the Gaussian periods $\eta_0, \ldots, \eta_{n-1}$ are exactly the eigenvalues of C. So $\det(xI - C)$ is the minimal polynomial of the periods (see also [1], formula (9)), and we have a field isomorphism

(17) $$\mathbb{Q}(\eta_0) \simeq \mathbb{Q}(C), \qquad \eta_0 \mapsto C.$$

Let

(18) $$R = \begin{bmatrix} \eta_0 & \eta_{n-1} & \cdots & \eta_1 \\ \eta_1 & \eta_0 & \cdots & \eta_2 \\ \vdots & \vdots & \ddots & \vdots \\ \eta_{n-1} & \eta_{n-2} & \cdots & \eta_0 \end{bmatrix}$$

(a circulant matrix). It follows from (16) that

(19) $$R^{-1}CR = \text{diag}[\eta_0, \eta_{n-1}, \eta_{n-2}, \ldots, \eta_1].$$

(We have that $R^{-1} = (1/q)(R^t - fE)$, where E is the $n \times n$ matrix with all entries equal to 1.) Let K be the $n \times n$ matrix $[\delta_{i+1,j}]_{i,j}$; that is,

(20) $$K = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}$$

Since circulant matrices commute with one another, we can conclude from (19) that $R^{-1}(K^{-i}CK^i)R = \text{diag}[\eta_i, \eta_{i-1}, \ldots, \eta_{i-(n-1)}]$. Therefore the matrices $K^{-i}CK^i$, $0 \le i \le n - 1$, are simultaneously diagonalizable, and if we use (17) to identify η_0 with C, then we must identify η_i with $K^{-i}CK^i$. In particular we have, for all integers i,

(21) $$(K^{-i}CK^i)C = C(K^{-i}CK^i).$$

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

In [10], Theorem 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 [10]): Let K be as in (20). Denote by $[B]_i$ the i-th row of a matrix B. Then C is a matrix with entries in $\mathbb{Z}$ such that:

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

These properties characterize C (up to some relabeling of the periods in formula (13)), and property (c) together with formula (21) implies 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 $c_{i,j} = c_{-i,j-i}$. So we have the following more satisfactory result.

Proposition 2. *Let K be as in (20). The matrix $C = [c_{i,j}]_{0 \le i,j \le n-1}$ is characterized (up to some relabeling of the periods in formula (13), due to the choice of s) by the following properties: It is a matrix with entries in $\mathbb{Z}$ such that, for all $0 \le i, j \le n - 1$,*
i)   the sum of the elements of its i-th row is $f - q\delta_{0,i}$,
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 n),
iv) $C(K^{-i}CK^i) = (K^{-i}CK^i)C$,
v)   the polynomial $\det(xI - C)$ is irreducible over $\mathbb{Q}$.

Our next objective is to show a formula for cyclotomic numbers that will be used in the MAPLE program below. A variation of the formula was first found by V.A. Lebesgue (see [4], Section III); we obtain it as a corollary of the next proposition. For $0 \le a, b \le n - 1$, define the Jacobi sums $J_{a,b}$ by

$$(22) \qquad J_{a,b} = -\sum_{k=2}^{q-1} \zeta_n^{a\,\mathrm{ind}_s(k) + b\,\mathrm{ind}_s(1-k)},$$

where $\mathrm{ind}_s(k)$ is the least nonnegative integer such that $s^{\mathrm{ind}_s(k)} \equiv k \bmod q$, and ζ_n is an n-th primitive root of 1. Let $G(x) = \sum_{k=0}^{n-1} \eta_k x^k$, where x is an indeterminate. We have $G(1) = -1$ and $G(\zeta_n^a)\overline{G(\zeta_n^a)} = q$ if $n \nmid a$ ($G(\zeta_n^a)$ is a Gauss sum). Suppose that $0 \le a, b \le n - 1$. If $a + b \not\equiv 0 \bmod n$, we have

$$(23) \qquad J_{a,b} = -\frac{G(\zeta_n^a)G(\zeta_n^b)}{G(\zeta_n^{a+b})}.$$

Also

$$(24) \qquad J_{0,0} = -(q - 2), \quad \text{and} \quad J_{a,b} = 1 \text{ if } a + b \equiv 0 \mod n \text{ but } a \ne 0.$$

(See, for example, [12] Lemma 6.2, or [3] page 4.)

Proposition 3. *For $0 \le i, j \le n - 1$,*

$$(i,j) = -\frac{1}{n^2} \sum_{a=0}^{n-1} \sum_{b=0}^{n-1} \zeta_n^{-ia-jb} J_{a,b}$$

$$= -\frac{1}{n^2}\left(n\delta_{0,i} + n\delta_{0,j} + n\delta_{i,j} - q - 1 + \sum_{\substack{1 \le a,b \le n-1 \\ a+b \ne n}} \zeta_n^{-ia-jb} J_{a,b} \right).$$

Proof. For $0 \le a, b \le n - 1$, we have

$$(25) \qquad J_{a,b} = -\sum_{h=0}^{n-1}\sum_{k=0}^{n-1} \zeta_n^{bk-(a+b)h}(k, h).$$

In fact, when $ab(a + b) \not\equiv 0 \mod n$ this is just [1], formula (26); but this formula also holds when $ab(a + b) \equiv 0 \mod n$. In fact, let $S(a, b)$ be the sum in the right hand side of (25); we have

$$S(0, 0) = -\sum_{h=0}^{n-1}\sum_{k=0}^{n-1}(k, h) = -\sum_{k=0}^{n-1}(f - \delta_{0,k}) = -(nf - 1) = -(q - 2) = J_{0,0},$$

by [1], formula (17). Suppose $a + b \equiv 0 \mod n$ and $a \ne 0$; then

$$S(a, b) = -\sum_{h=0}^{n-1}\sum_{k=0}^{n-1}\zeta_n^{bk}(k, h) = -\sum_{k=0}^{n-1}\zeta_n^{bk}(f - \delta_{0,k}) = 1 = J_{a,b}.$$

Suppose $b = 0$ and $1 \le a \le n - 1$; then

$$S(a, b) = -\sum_{h=0}^{n-1}\sum_{k=0}^{n-1}\zeta_n^{-ah}(k, h) = -\sum_{h=0}^{n-1}\zeta_n^{-ah}(f - \delta_{0,h}) = 1 = J_{a,b}.$$

Finally suppose $a = 0$ and $1 \le b \le n - 1$; then

$$S(a, b) = -\sum_{h=0}^{n-1}\sum_{k=0}^{n-1}\zeta_n^{b(k-h)}(k, h)$$

$$= -\sum_{h=0}^{n-1}\sum_{k=0}^{n-1}\zeta_n^{bk}(k + h, h)$$

$$= -\sum_{h=0}^{n-1}\sum_{k=0}^{n-1}\zeta_n^{bk}(k, -h)$$

$$= -\sum_{k=0}^{n-1}\zeta_n^{bk}(f - \delta_{0,k})$$

$$= 1 = J_{a,b}.$$

Now using (25) we get

$$-(1/n^2)\sum_{a=0}^{n-1}\sum_{b=0}^{n-1}\zeta_n^{-ia-jb}J_{a,b}$$

$$= (1/n^2)\sum_{h=0}^{n-1}\sum_{k=0}^{n-1}(k, h)\sum_{a=0}^{n-1}\zeta_n^{(-i-h)a}\sum_{b=0}^{n-1}\zeta_n^{(-j+k-h)b}$$

$$= \sum_{h=0}^{n-1}\sum_{k=0}^{n-1}(k, h)\delta_{-i,h}\delta_{j+h,k}$$

$$= (j - i, -i) = (-i, j - i) = (i, j),$$

as we wanted to prove. The second equality follows from (23) and (24). $\qquad\square$

Corollary. *For $0 \leq i, j \leq n - 1$,*

$$(i, j) \equiv -\frac{1}{n^2} \sum_{k=0}^{n} \sum_{m=0}^{n-1} \binom{fk}{fm} s^{f(mi-kj)} \quad \mod q.$$

Also

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

and so

$$0 \leq (i, j) < \sqrt{q} + (q - 1)/n^2 < q.$$

For information about the numbers $\binom{fk}{fm}$ see [11] Lemma 1, and the example following it.

Proof. Let Q be the prime ideal of $\mathbb{Z}[\zeta_n]$ above q such that $s^f \equiv \zeta_n \mod Q$, and let B be the prime ideal of $\mathbb{Z}[\zeta_n, \zeta_q]$ above Q. If $k \in \mathbb{Z}$ and $m > 0$, we denote by $|k|_m$ the least nonnegative integer such that $|k|_m \equiv k \mod m$. By [3], Chapter 1, Theorem 2.1, we have, for $0 \leq l \leq n - 1$,

$$(26) \qquad \frac{G(\zeta_n^{-l})}{(\zeta_q - 1)^{fl}} \equiv \frac{-1}{(fl)!} \quad \mod B.$$

For $0 \leq a, b \leq n - 1$ such that $a + b \not\equiv 0 \mod n$ it follows from (23) and (26) that

$$\overline{J_{a,b}} = -\frac{G(\zeta_n^{-a})G(\zeta_n^{-b})}{G(\zeta_n^{-(a+b)})}$$

$$= -\frac{(G(\zeta_n^{-a})/(\zeta_q - 1)^{fa})(G(\zeta_n^{-b})/(\zeta_q - 1)^{fb})}{(G(\zeta_n^{-(a+b)})/(\zeta_q - 1)^{f|a+b|_n})}(\zeta_q - 1)^{f(a+b-|a+b|_n)}$$

$$\equiv \frac{(f|a+b|_n)!}{(fa)!(fb)!}(\zeta_q - 1)^{f(a+b-|a+b|_n)} \quad \mod B,$$

where the bar denotes complex conjugation. Therefore, for $0 \leq a, b \leq n - 1$ with $a + b \not\equiv 0 \mod n$,

$$(27) \qquad \overline{J_{a,b}} \equiv \binom{f|a+b|_n}{fa} \quad \mod Q.$$

Note that $\binom{f|a+b|_n}{fa} \equiv 0 \mod q$ if $a + b - |a + b|_n \neq 0$; in fact, in that case we have $|a + b|_n = a + b - n < a$.

From Proposition 3 and (27) we get

$$(i,j) = -(1/n^2) \sum_{a=0}^{n-1} \sum_{b=0}^{n-1} \zeta_n^{ia+jb} \overline{J_{a,b}}$$

$$\equiv -(1/n^2) \sum_{\substack{0 \le a,b \le n-1 \\ a+b \not\equiv 0 \mod n}} s^{f(ia+jb)} \binom{f|a+b|_n}{fa}$$

$$- (1/n^2)\left(-(q-2) + \sum_{a=1}^{n-1} \zeta_n^{(i-j)a}\right)$$

$$\equiv -(1/n^2)\left(n\delta_{i,j} + \sum_{a=0}^{n-1}\sum_{b=0}^{n-1} s^{f(ia+jb)} \binom{f|a+b|_n}{fa}\right) \mod Q.$$

Therefore

$$(i,j) = (i-j,-j)$$

$$\equiv -(1/n^2)\left(n\delta_{0,i} + \sum_{a=0}^{n-1}\sum_{b=0}^{n-1} s^{f((i-j)a-jb)} \binom{f|a+b|_n}{fa}\right)$$

$$\equiv -(1/n^2)\left(n\delta_{0,i} + \sum_{a=0}^{n-1}\sum_{b=0}^{n-1} s^{f(ia-jb)} \binom{fb}{fa}\right)$$

$$\equiv -(1/n^2) \sum_{b=0}^{n}\sum_{a=0}^{n-1} s^{f(ia-jb)} \binom{fb}{fa} \mod q,$$

as we wanted to prove (note that $\binom{q-1}{fa} \equiv (-1)^{fa} = 1 \mod q$).

The inequality $|(i,j) - (q-1)/n^2| < \sqrt{q}$ follows from Proposition 3 and the triangle inequality, since $|J_{a,b}| = \sqrt{q}$ if $1 \le a,b \le n-1$ and $a+b \neq 0$. $\qquad\square$

Now we exhibit a MAPLE program to find $C = [c_{i,j}]$ and $H(j) = K^{-j}CK^j$, $1 \le j \le n$, with K as in (20). In the first line write the values of n (an integer ≥ 2), q (a prime $\equiv 1 \mod 2n$) and s (a primitive root mod q). The command: s:=primroot(q); gives to s the value of the smallest positive primitive root mod q. The command: isprime(q); can be used to check if q is a prime number.

Think of C as η_0 and of $H(j)$ as η_j, and think of determinants as norms. So, for example,

$$P(x) = \det(xI - C)$$

is the irreducible polynomial of η_0;

$$\det\big(xI - (a_1 H(1) + \cdots + a_n H(n))\big)$$

is the characteristic polynomial of $a_1\eta_1 + \cdots + a_{n-1}\eta_{n-1} + a_n\eta_0$ (in MAPLE language this is: charpoly(a_1*H(1)+$\cdots$+a_n*H(n),x); where one writes all the terms). One can use the program to check the properties of Proposition 2; for example, given n, q and s, the command: evalm(H(2)&*C−C&*H(2)); should give the matrix 0.

Example. Let $n = 12$ and $q = 73$. Then $2 + \eta_0$ and $1 + \eta_0 - \eta_1$ are units of $\mathbb{Q}(\eta_0)$, since $\det(2I + C) = 1 = \det(I + C - H(1))$.

Warning: MAPLE regards K^0 as the number 1!! So, for example, $H(0)$ will not be calculated, but it will give correctly $H(n) = C$.

A MAPLE program to calculate C and $P_q(x)$ given n and $q \equiv 1 \mod 2n$

```
n:=12; q:=73; f:=(q−1)/n; s:=primroot(q);
with(numtheory): with(linalg):
h:=modp(sˆ f,q):
F:=(i,j)−>modp((−1/(nˆ 2))*sum(sum(binomial (f*k,f*m)*hˆ (m*i−k*j),
m=0..n−1), k=0..n),q);
Id:=array(identity,1..n,1..n):
C:=array(1..n,1..n):
for i from 1 to n do;
for j from 1 to n do;
C[i,j]:=F(i−1,j−1)−f*Id[1,i]: od: od:
C:=evalm(C);
P:=x−>charpoly(C,x);
Pq:=sort(P(x));
K:=array(1..n,1..n):
for i1 from 1 to n−1 do;
for j1 from 2 to n do;
K[i1,j1]:=Id[i1+1,j1];
K[i1,1]:=0; K[n,j1]:=0;
K[n,1]:=1; od: od:
K:=evalm(K);
H:=j−>evalm(Kˆ (−j)&*C&*Kˆ j);
det(Id+C−H(1));
```

REFERENCES

1. L.E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.
2. K. Iwasawa, *A note on Jacobi sums*, Symposia Mathematica **15** (1975), 447–459. MR **52**:5620
3. S. Lang, *Cyclotomic fields I and II (with an appendix by K. Rubin), Combined Second Edition*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1990. MR **91c**:11001
4. V. A. Lebesgue, *Recherches sur les nombres*, J. Math. Pures Appl. **2** (1837), 253–292.
5. E. Lehmer, *The quintic character of 2 and 3*, Duke Math. J. **18** (1951), 11–18. MR **12**:677a
6. E. Lehmer, *Connection between Gaussian periods and cyclic units*, Math. Comp. **50** (1988), 535–541. MR **89h**:10067a
7. R. Schoof and L. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), 543–556. MR **89h**:10067b
8. T. Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics, Markham Publishing Company, Chicago, 1967. MR **36**:128
9. H.W. Lloyd Tanner, *On the binomial equation $x^p − 1 = 0$: quinquisection*, Proc. London Math. Soc. **18** (1886/87), 214–234.
10. F. Thaine, *Properties that characterize Gaussian periods and cyclotomic numbers*, Proc. Amer. Math. Soc. **124** (1996), 35–45. MR **96d**:11115
11. F. Thaine, *On the coefficients of Jacobi sums in prime cyclotomic fields*, Transactions of the American Mathematical Society, to appear.
12. L. C. Washington, *Introduction to Cyclotomic Fields, Second Edition*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1996. MR **97h**:11130

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