JACOBI SUMS AND NEW FAMILIES OF IRREDUCIBLE POLYNOMIALS OF GAUSSIAN PERIODS

F. THAINE

ABSTRACT. Let \( m > 2 \), \( \zeta_m \) an \( m \)-th primitive root of 1, \( q \equiv 1 \mod 2m \) a prime number, \( s = s_q \) a \( q \)-th primitive root modulo \( q \) and \( f = f_q = (q - 1)/m \). We study the Jacobi sums \( J_{a,b} = -\sum_{k=2}^{q-1} \zeta_m^{a \text{ind}_s(k) + b \text{ind}_s(1-k)} \), \( 0 \leq a, b \leq m - 1 \), where \( \text{ind}_s(k) \) is the least nonnegative integer such that \( s^{\text{ind}_s(k)} \equiv k \mod q \). We exhibit a set of properties that characterize these sums, some congruences they satisfy, and a MAPLE program to calculate them. Then we use those results to show how one can construct families \( P_q(x), q \in \mathcal{P} \), of irreducible polynomials of Gaussian periods, \( \eta_i = \sum_{j=0}^{f-1} \zeta_q^{i + mj} \), of degree \( m \), where \( \mathcal{P} \) is a suitable set of primes \( \equiv 1 \mod 2m \). We exhibit examples of such families for several small values of \( m \), and give a MAPLE program to construct more of them.

INTRODUCTION

Let \( m > 2 \) be an integer and \( \zeta_m \) an \( m \)-th primitive root of 1. For each prime \( q \equiv 1 \mod 2m \) let \( \zeta_q \) be a \( q \)-th primitive root of 1, \( s = s_q \) a primitive root modulo \( q \) and \( f = f_q = (q - 1)/m \) (we will assume that \( f \) is even for simplicity). Let \( S \) be the set of all primes \( q \equiv 1 \mod 2m \). Given \( q \in S \), define the Jacobi sums \( J_{a,b} \), \( 0 \leq a, b \leq m - 1 \), and the Gaussian periods \( \eta_i \), \( 0 \leq i \leq m - 1 \), of degree \( m \) in \( \mathbb{Q}(\zeta_q) \), by

\[
J_{a,b} = -\sum_{k=2}^{q-1} \zeta_m^{a \text{ind}_s(k) + b \text{ind}_s(1-k)},
\]

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

\[
\eta_i = \sum_{j=0}^{f-1} \zeta_q^{i + mj}.
\]

Define \( P_q(x) = \prod_{i=0}^{m-1} (x - \eta_i) \), the irreducible polynomial, over \( \mathbb{Q} \), of the periods \( \eta_i \). In this article we study the numbers \( J_{a,b} \), and use them to construct large families of polynomials \( P_q(x), q \in \mathcal{P} \), where \( \mathcal{P} \) is a subset of \( S \). In principle the method shown here would allow us to construct a finite number of such families, whose indices put together include all the primes in \( S \).

This research originated from a problem indicated to me by René Schoof. The first part of the problem was to find, for \( m = 7 \), or \( m = 9 \), or \( m = 12 \), families of...
irreducible polynomials of real Gaussian periods of degree \( m \). The second part was to find families of irreducible polynomials of units of the number fields generated by those periods. I think we give here a complete answer to the first part (for arbitrary \( m \)). The second part seems to be an open problem, and a very interesting one in light of Schoof and Washington’s work in [7].

For an account of previous work in this and related subjects see [1], [6] and [7]. The path that leads directly to this article is the following. For \( m = 5 \), 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 exhibited 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. In [12], Section 1, we work with \( m = p \), an odd prime, and show how to construct certain families of irreducible polynomials of Gaussian periods of degree \( p \). In that article we were able to obtain, for general \( p \), only some of the families our present method allows us to construct. We could give all the families only when \( \mathbb{Z}[\zeta_p] \) was a principal ideal domain. In this article we work with general \( m > 2 \) and find all the families, thereby extending, in more than one way, the results of [12].

In Section 1 we use the well-known relations between Jacobi sums, Gauss sums, Gaussian periods and cyclotomic numbers to obtain a set of properties that characterize the numbers \( J_{a,b} \) (Propositions 2 and 3). We write these numbers in the form

\[
J_{a,b} = \sum_{k=0}^{m-1} d_{a,b,k} \zeta_m^k, \quad \text{with } d_{a,b,k} \in \mathbb{Z},
\]

in such a way that we can give natural formulas for the coefficients \( d_{a,b,k} \) (Propositions 1 and 4). This allows us to calculate Jacobi sums efficiently. We prove some congruences that the numbers \( d_{a,b,k} \) satisfy (formula (13)) which allow us to distinguish the Jacobi sums \( J_{a,b} \) among the other generators of the ideals \( (J_{a,b}) \) (a useful result when we apply the method of Section 2 to find families of polynomials \( P_q(x) \)). This generalizes some results of [11], where we considered only the case \( m = p \), an odd prime number. We end Section 1 with a MAPLE program to calculate the Jacobi sums \( J_{a,b} \).

In Section 2 we show how to construct families of irreducible polynomials of Gaussian periods in a very general situation. Let \( \mathcal{R} \) be an ideal of \( \mathbb{Z}[\zeta_m] \) relatively prime with \( m \). Suppose that we can calculate (for example using the MAPLE program of Section 1) the Jacobi sums corresponding to the prime ideals dividing \( \mathcal{R} \) (see formula (18)). Then we show a way to construct a family \( P_q(x), q \in \mathcal{P} \), of irreducible polynomials of Gaussian periods of degree \( m \), where the elements \( q \) of \( \mathcal{P} \) are such that \( q \in S \) and one of the prime ideals \( \mathcal{Q} \) of \( \mathbb{Z}[\zeta_m] \) above \( q \) is in the inverse of the ideal class of \( \mathcal{R} \). We give examples for \( m = 7, m = 9, m = 12 \) and (partially) \( m = 23 \); in them the sets \( \mathcal{P} \) of indices are chosen so that there are simple descriptions of the families of polynomials \( P_q(x) \). Examples 1-4 correspond to the case \( \mathcal{R} = (1) \) (for \( m = 7, m = 7, m = 9 \) and \( m = 12 \), respectively). Examples 5 and 6 illustrate the use of the method in a general situation. A MAPLE program to carry out the calculations for our examples, and to search for more examples, is given at the end of the section.
1. JACOBI SUMS IN $\mathbb{Q}(\zeta_m)$

Let $m > 2$ be an integer and $q = mf + 1$ a prime number. For simplicity we assume that $f$ is even. Let $s$ be a primitive root modulo $q$, $\zeta_q$ a $q$-th primitive root of 1, and $\eta_0, \ldots, \eta_{m-1}$ the Gaussian periods of degree $m$ in $\mathbb{Q}(\zeta_q)$ defined by

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

The set $\{\eta_0, \ldots, \eta_{m-1}\}$ is a normal integral basis of $\mathbb{Q}(\eta_0)/\mathbb{Q}$. Let $c_{i,j}$, $0 \leq i, j \leq m-1$, be the rational integers such that

$$\eta_0 \eta_i = \sum_{j=0}^{m-1} c_{i,j} \eta_j. \tag{2}$$

Define $C = [c_{i,j}]_{0 \leq i,j \leq m-1}$. It follows from (2) that the characteristic polynomial of the matrix $C$ is the irreducible polynomial $P_q(x)$ of the Gaussian periods $\eta_i$; that is,

$$P_q(x) = \prod_{i=0}^{m-1} (x - \eta_i) = \det(xI - C), \tag{3}$$

where $I$ is the $m \times m$ identity matrix (see [2], formula 9, or [10], formula 19).

For $0 \leq i, j \leq m - 1$, we denote by $(i, j)$ the cyclotomic numbers of order $m$. Recall that $(i, j)$ is defined as the number of ordered pairs of integers $(k, l)$, $0 \leq k, l \leq f - 1$, such that $1 + s^{km+i} \equiv s^{lm+j} \bmod q$ (see, for example, [1], §2.2, [2], or [8]). Define $\eta_{i+k} = \eta_i$, $c_{i+k,m,j+lm} = c_{i,j}$, and $(i + km, j + lm) = (i, j)$, for $0 \leq i, j \leq m - 1$ and $k, l \in \mathbb{Z}$.

We use the following version of Kronecker’s delta:

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i \equiv j \bmod m, \\ 0 & \text{if } i \not\equiv j \bmod m. \end{cases} \tag{4}$$

The cyclotomic numbers $(i, j)$ are very close to the numbers $c_{i,j}$; we have

$$c_{i,j} = (i, j) - f \delta_{0,i}, \tag{5}$$

for $i, j \in \mathbb{Z}$ (see [2], formula 6).

Let $G(x) = \sum_{k=0}^{q-2} x^k \zeta_q^k$, where $x$ is an indeterminate. We have that $G(x) \equiv \sum_{k=0}^{m-1} \eta_k x^k \bmod x^m - 1$ and that $G(1) = -1$. Let $\zeta_m$ be an $m$-th primitive root of 1. If $m \nmid k$, then $G(\zeta_m^k)$ is a Gauss sum which satisfies $G(\zeta_m^k)G(\zeta_m^{-k}) = q$ (recall that since $f$ is even the Gaussian periods $\eta_i$ are real numbers).

For $a, b \in \mathbb{Z}$, define the Jacobi sums $J_{a,b}$ by

$$J_{a,b} = -\sum_{k=2}^{q-1} \zeta_m^a \text{ind}_a(k) + b \text{ind}_a(1-k), \tag{6}$$

where $\text{ind}_a(k)$ is the least nonnegative integer such that $s^{\text{ind}_a(k)} \equiv k \bmod q$. It follows directly from the definition that, for all $a, b \in \mathbb{Z},$

$$J_{a+m,b} = J_{a,b+m} = J_{a,b}, \quad J_{a,b} = J_{b,a}, \quad \text{and} \quad J_{a,b} = J_{-a-b,b}. \tag{6}$$
For example,
\[
J_{-a-b, b} = \sum_{k=2}^{q-1} e^{(a-b) \text{ind}_s(k) + b \text{ind}_s(1-k)}
\]
\[
= \sum_{k=2}^{q-1} e^{-a \text{ind}_s(k) + b \text{ind}_s(k-1)}
\]
\[
= \sum_{k=2}^{q-1} e^{-a \text{ind}_s(k) + b \text{ind}_s(k-1)}
\]
\[
= \sum_{k=2}^{q-1} e^{-a \text{ind}_s(k) + b \text{ind}_s(1-k)} = J_{a, b},
\]

since \( f \) is even.

Suppose that \( 0 \leq a, b \leq m - 1 \). If \( a + b \not\equiv 0 \pmod{m} \), then

(7)
\[
J_{a, b} = -\frac{G(c_m^a)G(q_m^b)}{G(q_m^{a+b})}.
\]

also

(8) \( J_{0, 0} = -(q - 2) \), and \( J_{a, b} = 1 \) if \( a + b \equiv 0 \pmod{m} \) but \( a \not\equiv 0 \)

(see, for example, [13], Lemma 6.2, or [4], page 4).

We show now a way to represent Jacobi sums as linear combinations, over \( \mathbb{Z} \), of powers of \( \zeta_m \), which is very convenient for our purposes. For \( a \) and \( b \) nonnegative integers let \( f_{a, b}(x) \) be the polynomial

\[
f_{a, b}(x) = \sum_{k=2}^{q-1} x^{a \text{ind}_s(k) + b \text{ind}_s(1-k)} + \frac{x^{q-1} - 1}{x - 1}.
\]

Define \( J_{a, b}(x) = \sum_{j=0}^{m-1} d_{a, b, j} x^j \in \mathbb{Z}[x] \) as the remainder of the division of \( f_{a, b}(x) \) by \( x^m - 1 \); that is,

(9) \[ J_{a, b}(x) = \sum_{j=0}^{m-1} d_{a, b, j} x^j \equiv f_{a, b}(x) \pmod{x^m - 1}. \]

Clearly, for \( a, b \geq 0 \), we have

(10) \[ J_{a, b} = J_{a, b}(\zeta_m) = \sum_{j=0}^{m-1} d_{a, b, j} \zeta_m^j, \]

(11) \[ J_{a, b}(1) = \sum_{j=0}^{m-1} d_{a, b, j} = 1, \]

and, for \( k \geq 0 \) such that \( k \not\equiv 0 \pmod{m} \),

(12) \[ J_{a, b}(\zeta_m^k) = J_{ka, kb}(\zeta_m) = J_{ka, kb}. \]

We also have

(13) \[ J'_{a, b}(1) = \sum_{j=1}^{m-1} j d_{a, b, j} \equiv 0 \pmod{m}. \]
In fact, by (9),
\[ J_{a,b}(x) = -\sum_{k=2}^{q-1} x^{a \text{ind}_s(k) + b \text{ind}_s(1-k)} + (x^{q-1} - 1)/(x - 1) + (x^m - 1)g(x), \]
for some \( g(x) \in \mathbb{Z}[x] \). Taking derivatives, we get
\[ J'_{a,b}(x) = -\sum_{k=2}^{q-1} (a \text{ind}_s(k) + b \text{ind}_s(1-k))x^{a \text{ind}_s(k) + b \text{ind}_s(1-k)} - 1 \]
\[ + (1 + 2x + \cdots + (q - 2)x^{q-3}) + (x^m - 1)g'(x) + mx^{m-1}g(x). \]

Therefore
\[ J'_{a,b}(1) = -a \sum_{k=2}^{q-1} \text{ind}_s(k) - b \sum_{k=2}^{q-1} \text{ind}_s(1-k) + m(f/2)(q - 2) + mg(1) \equiv 0 \mod m. \]

The following result will be useful in calculating Jacobi sums. We denote by \( \overline{x} \) the complex conjugate of the number \( x \). Observe that, if we denote the Jacobi sums in (5) by \( J_{a,b,m} \) and \( c = \gcd(a, b, m) \), then \( J_{a,b,m} = J_{a/c,b/c,m/c} \) with \( \gcd(a/c, b/c, m/c) = 1 \) (assume \( c < m \) and choose \( \zeta_{m/c} = \zeta_m^c \)).

**Proposition 1.** Let \( a \) and \( b \) be integers, \( 1 \leq a, b \leq m-1 \), such that \( \gcd(a, b, m) = 1 \). Let \( v = \gcd(a + b, m) \) and \( u = m/v \). For \( l \in \mathbb{Z} \) let
\[ \varepsilon(l) = \begin{cases} 1 & \text{if } v \mid l, \\ 0 & \text{if } v \nmid l. \end{cases} \]

Then, for \( 0 \leq l \leq m-1 \), we have
\[ d_{a,b,l} = \frac{1}{m} \left( 1 + \sum_{k=1}^{m-1} \zeta_m^{-kl} J_{ka,kb} \right) = \frac{1}{m} \varepsilon(l) + \frac{1}{m} \sum_{i=1}^{u-1} \sum_{k=0}^{v-1} \zeta_m^{ukl} J_{(i+uk)a,(i+uk)b}. \]

**Proof.** Let \( d_1 = d_{a,b,l} \). For \( 0 \leq l \leq m-1 \), we have
\[ \sum_{k=0}^{m-1} \zeta_m^{-kl} J_{a,b}(\zeta_m^k) = \sum_{k=0}^{m-1} \zeta_m^{-kl} \sum_{j=0}^{m-1} d_j \zeta_m^{jk} = \sum_{j=0}^{m-1} d_j \sum_{k=0}^{m-1} \zeta_m^{(j-l)k} = md_1; \]
so
\[ d_1 = \frac{1}{m} \sum_{k=0}^{m-1} \zeta_m^{kl} J_{a,b}(\zeta_m^k) = \frac{1}{m} \left( 1 + \sum_{k=1}^{m-1} \zeta_m^{kl} J_{ka,kb} \right), \]
by (11) and (12). Therefore
\[ d_1 = \frac{1}{m} \left( 1 + \sum_{1 \leq k \leq m-1 \atop \text{gcd}(k,l) = 1} \zeta_m^{kl} J_{ka,kb} \right) = \frac{1}{m} \left( \sum_{1 \leq k \leq m-1 \atop \text{gcd}(k,l) = 1} \zeta_m^{kl} J_{ka,kb} \right) \]
\[ = \frac{1}{m} \left( 1 + \sum_{k=1}^{u-1} \zeta_m^{ukl} \right) + \frac{1}{m} \left( \sum_{i=1}^{u-1} \sum_{k=0}^{v-1} \zeta_m^{(i+uk)l} J_{(i+uk)a,(i+uk)b} \right) \]
\[ = \frac{1}{m} \varepsilon(l) + \frac{1}{m} \sum_{i=1}^{u-1} \sum_{k=0}^{v-1} \zeta_m^{ukl} J_{(i+uk)a,(i+uk)b}, \]
by (8), as we wanted to prove. \( \square \)
We can express the Jacobi sums $J_{a,b}$ in terms of the cyclotomic numbers $(i,j)$, and vice versa, as follows:

For $a, b \in \mathbb{Z}$,

$$J_{a,b} = - \sum_{h=0}^{m-1} \sum_{k=0}^{m-1} \zeta_m^{ah+bk}(h,k). \quad (14)$$

In fact, for example, by [2], formula 26 (for the case where $m \nmid a$, $m \nmid b$ and $m \nmid (a+b)$), and a straightforward calculation using [2], formulas 14 and 17 (when $m \mid a$ or $m \mid b$ or $m \mid (a+b)$), we have

$$J_{a,b} = - \sum_{h=0}^{m-1} \sum_{k=0}^{m-1} \zeta_m^{bk-(a+b)h}(k,h).$$

So, by (6), and [2], formula 14,

$$- \sum_{h=0}^{m-1} \sum_{k=0}^{m-1} \zeta_m^{ah+bk}(h,k) = - \sum_{h=0}^{m-1} \sum_{k=0}^{m-1} \zeta_m^{ah+bk}(k,h) = J_{-a-b,b} = J_{a,b}.$$

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

$$(i,j) = -\frac{1}{m^2} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \zeta_m^{-ia-jb} J_{a,b} \quad (15)$$

$$= -\frac{1}{m^2} \left( m \delta_{i,j} + m \delta_{i,-j} + m \delta_{i,j} - q - 1 + \sum_{1 \leq a,b \leq m-1 \atop a+b \neq m} \zeta_m^{-ia-jb} J_{a,b} \right)$$

(see, for example, [1], §2.5, or [12], Proposition 3, or formula (16) below).

Let $P$ be the matrix $[\zeta_m^{ij}]_{0 \leq i,j \leq m-1}$. We have that $P^{-1} = \overline{P}/m$, and (14) is equivalent to

$$[J_{-a,b}]_{0 \leq a,b \leq m-1} = -mP^{-1}[(i,j)]_{0 \leq i,j \leq m-1} P. \quad (16)$$

In the next proposition we give a list of properties of the Jacobi sums $J_{a,b}$ that actually characterize these numbers, as will be proved later (see Proposition 3).

**Proposition 2.** For $a, b \in \mathbb{Z}$, the Jacobi sums $J_{a,b}$ are elements of $\mathbb{Z}[\zeta_m]$ which satisfy the following conditions:

1. $J_{a+m,b} = J_{a,b+m} = J_{a,b}$.
2. $J_{a,b} = J_{b,a}$.
3. $J_{a,b} = J_{-a-b,b}$.
4. $J_{0,0} = - (q-2)$, and $J_{0,b} = 1$, if $m \nmid b$.
5. $J_{a,b}J_{-a,-b} = q$, if $m \mid a$, $m \mid b$ and $m \nmid (a+b)$.
6. $J_{a,b}J_{-a,-c} = J_{-(a+b+c),b}J_{a+b+c,-c}$, if $m \nmid (a+b)$, $m \nmid (a+c)$, $m \nmid a$ and $m \nmid (a+b+c)$. 
7. For \( i, j \in \mathbb{Z} \), the numbers
\[
h_{i,j} = -\frac{1}{m^2} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \zeta_m^{-ai-bj} (J_{a,b} + (q-1)\delta_{0,b})
\]
are rational integers. (Note that, by (4) and (15), the \( h_{i,j} \) are in fact the numbers \( c_{i,j} \).)

8. The characteristic polynomial of the matrix \([J_{a,b} + (q-1)\delta_{0,b}]_{0 \leq a,b \leq m-1}\) (which, by 7, is equal to the characteristic polynomial of \([-mh_{i,j}]_{0 \leq i,j \leq m-1}\)) is irreducible over \( \mathbb{Q} \).

**Proof.** Properties 1-3 were shown in (6). Property 4 follows from (7) and (8). Property 5 follows from (7) and from the fact that \( G(\zeta_m^k)G(\zeta_m^{-k}) = q \), if \( m \nmid k \).

Suppose that \( m \nmid (a + b), m \nmid (a + c), m \nmid a \) and \( m \nmid (a + b + c) \). Then, by (7),
\[
J_{a,b}J_{-a,-c} = (G(\zeta_m^a)G(\zeta_m^b)/G(\zeta_m^{a+b}))(G(\zeta_m^{-a})G(\zeta_m^{-c})/G(\zeta_m^{a-c}))
\]
\[
= (G(\zeta_m^{-a-b-c})G(\zeta_m^b)/G(\zeta_m^{a+b-c}))(G(\zeta_m^{a+b+c})G(\zeta_m^{-c})/G(\zeta_m^{a+b}))
\]
\[
= J_{-(a+b+c),b}J_{a+b+c,-c},
\]

since \( G(\zeta_m^a)G(\zeta_m^{-a}) = q = G(\zeta_m^{-a-b-c})G(\zeta_m^{a+b+c}) \). This proves property 6.

By (15) we have
\[
h_{i,j} + f\delta_{0,i} = -\frac{1}{m^2} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \zeta_m^{-ia-jb} J_{a,b} = (i,j).
\]

So, \( h_{i,j} = (i,j) - f\delta_{0,i} = c_{i,j} \in \mathbb{Z} \). This proves property 7.

To prove property 8, observe that, by (4), (16) and property 7, we have
\[
[J_{a,b} + (q-1)\delta_{0,b}]_{i,j} = P^{-1}[-mh_{i,j}]_{i,j}P = P^{-1}[-mc_{i,j}]_{i,j}P.
\]

So, the characteristic polynomial of the matrix \([J_{a,b} + (q-1)\delta_{0,b}]_{0 \leq a,b \leq m-1}\) is equal to the characteristic polynomial of the matrix \([-mc_{i,j}]_{0 \leq i,j \leq m-1}\), which is irreducible over \( \mathbb{Q} \) by (3).

**Proposition 3.** For \( a, b \in \mathbb{Z} \), let \( J_{a,b} \) be elements in \( \mathbb{Z}[\zeta_m] \) which satisfy conditions 1-8 of Proposition 2. Then, for some choice of the primitive root \( s \) modulo \( q \), the \( J_{a,b} \) are the Jacobi sums \( J_{a,b} \) defined in (5).

**Observation.** This proposition generalizes [11], Proposition 2, where we only considered the case \( m = p \), a prime, and denoted \( J_{1,n} \) by \( J_n \).

**Proof.** Let \( J_{a,b} \), \( a, b \in \mathbb{Z} \), be elements of \( \mathbb{Z}[\zeta_m] \) satisfying conditions 1-8 of Proposition 2. We will prove that the integers \( h_{i,j} \) of condition 7 are, for some choice of the primitive root \( s \) modulo \( q \), the numbers \( c_{i,j} = (i,j) - f\delta_{0,i} \). This will end the proof, since we can express the Jacobi sums \( J_{a,b} \) in terms of the \( c_{i,j} \) using (4) and (14), and, by condition 7, that expression must also give the numbers \( J_{a,b} \).
We showed in [10], Theorem 1 and the observation that follows it, that the numbers \( c_{i,j}, i, j \in \mathbb{Z} \), are characterized (up to some reordering due to the choice of \( s \)) by the following conditions: The \( c_{i,j} \) are integers such that

\[
\begin{align*}
\sum_{k=0}^{m-1} c_{i,k} &= f - q \delta_{0,i}, \\
\sum_{k=0}^{m-1} c_{k,j} &= -\delta_{0,j}, \\
\sum_{k=0}^{m-1} c_{i,k} c_{k,-i-j} &= \sum_{k=0}^{m-1} c_{j,k} c_{k,-i-l}, \\
\text{the characteristic polynomial of the matrix } [c_{i,j}]_{0 \leq i,j \leq m-1} \text{ is irreducible over } \mathbb{Q}.
\end{align*}
\]

(See also [12], Proposition 2.)

We are going to prove that the integers

\[
\begin{align*}
\begin{array}{c}
h_{i,j} = -f \delta_{0,i} - \frac{1}{m^2} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \zeta_{m}^{-ai-bj} J_{a,b}
\end{array}
\end{align*}
\]

satisfy the above conditions (with \( c_{i,j} \) replaced by \( h_{i,j} \)). Clearly \( h_{i+m,j} = h_{i,j} \), and condition 8 implies (v).

Define

\[
[i, j] = h_{i,j} + f \delta_{0,i} = -\frac{1}{m^2} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \zeta_{m}^{-ai-bj} J_{a,b}.
\]

By condition 2 we have \([i, j] = [j, i]\). By condition 4,

\[
\begin{align*}
\sum_{k=0}^{m-1} [i, k] &= -\frac{1}{m^2} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \zeta_{m}^{-ai} J_{a,b} \sum_{k=0}^{m-1} \zeta_{m}^{-bk} \\
&= -\frac{1}{m} \sum_{a=0}^{m-1} \zeta_{m}^{-ai} J_{a,0} \\
&= -\frac{1}{m} (-q - 2) + \sum_{a=1}^{m-1} \zeta_{m}^{-ai} = f - \delta_{0,i}.
\end{align*}
\]

Now (i) and (ii) follow at once.

By condition 3 we have

\[
\begin{align*}
[-i, j - i] &= -\frac{1}{m^2} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \zeta_{m}^{ai+b(i-j)} J_{a,b} \\
&= -\frac{1}{m^2} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \zeta_{m}^{(a+b)i-bj} J_{a,b} \\
&= -\frac{1}{m^2} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \zeta_{m}^{-ai-bj} J_{-a-b,b} \\
&= -\frac{1}{m^2} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \zeta_{m}^{-ai-bj} J_{a,b} = [i, j].
\end{align*}
\]

Therefore \( h_{-i,j-i} = [-i, j - i] - f \delta_{0,i} = [i, j] - f \delta_{0,i} = h_{i,j} \). This proves (iii).
Proof of (iv). It remains to prove that \( \sum_{k=0}^{m-1} h_{i,k} h_{k-j,1-j} = \sum_{k=0}^{m-1} h_{j,k} h_{k-i,1-i} \).
Since this proof requires a long calculation, to simplify matters we are going to use the following notation: If we have two expressions \( U(i,j,l) \) and \( V(i,j,l) \), we write \( U(i,j,l) \sim V(i,j,l) \) if the difference \( W(i,j,l) = U(i,j,l) - V(i,j,l) \) satisfies \( W(i,j,l) = W(j,i,l) \). Define \( H(i,j,l) = \sum_{k=0}^{m-1} h_{i,k} h_{k-j,1-j} \). We must prove that \( H(i,j,l) \sim 0 \).

We have

\[
H(i,j,l) = \sum_{k=0}^{m-1} ([i,k] - f \delta_{0,k}) ([k-j,1-j] - f \delta_{k,j})
\]

\[
= \sum_{k=0}^{m-1} [i,k][k-j,1-j] - f \delta_{0,i} \sum_{k=0}^{m-1} [k-j,1-j] - f \sum_{k=0}^{m-1} [i,k] \delta_{k,j} + f^2 \delta_{0,i} \sum_{k=0}^{m-1} \delta_{k,j}
\]

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

So,

\[
(*) \quad H(i,j,l) \sim f \delta_{0,i} \delta_{i,j} + \sum_{k=0}^{m-1} [i,k][k-j,1-j].
\]

Now, using conditions 2 and 3, we get

\[
\sum_{k=0}^{m-1} [i,k][k-j,1-j] = \frac{1}{m^4} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \sum_{t=0}^{m-1} \sum_{w=0}^{m-1} \zeta_m^{-ia - kb - (k-j)t - (1-j)w} \mathcal{J}_{a,b} \mathcal{J}_{t,w}
\]

\[
= \frac{1}{m^4} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \sum_{t=0}^{m-1} \sum_{w=0}^{m-1} \zeta_m^{-ia + jt - (1-j)w} \mathcal{J}_{a,b} \mathcal{J}_{t,w} \sum_{k=0}^{m-1} \zeta_m^{-k(b+t)}
\]

\[
= \frac{1}{m^3} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \sum_{t=0}^{m-1} \sum_{w=0}^{m-1} \zeta_m^{-ia - jb - (1-j)w} \mathcal{J}_{a,b} \mathcal{J}_{t,w}
\]

\[
= \frac{1}{m^3} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \sum_{w=0}^{m-1} \zeta_m^{-ia - j(b-w) - lw} \mathcal{J}_{a,b} \mathcal{J}_{b,w}
\]

\[
= \frac{1}{m^3} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \sum_{w=0}^{m-1} \zeta_m^{-ia - jw - l(b-w)} \mathcal{J}_{a,b} \mathcal{J}_{b,w}
\]

\[
= \frac{1}{m^3} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \sum_{w=0}^{m-1} \zeta_m^{-ia - jw - l(b-w)} \mathcal{J}_{a,b} \mathcal{J}_{b,w}
\]

\[
= \frac{1}{m^3} \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \sum_{w=0}^{m-1} \zeta_m^{-ia + jw - l(a+w)} \mathcal{J}_{a,b} \mathcal{J}_{a,-w}
\]
Now define

\[ F(i, j, l) = m^2(q - 1)\delta_{i,0}\delta_{l,j} \]
\[ + \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} \sum_{w=0}^{m-1} \zeta_m^{ib+jw-l(a+w)} J_{a,b} J_{-a,-w}. \]

By (\*), in order to prove (iv), it is enough to prove that \( F(i, j, l) = F(j, i, l) \), i.e. that \( F(i, j, l) \sim 0 \). Define

\[ A(i, j, l) = \sum_{0 \leq a, b, w \leq m-1 \atop m|a+b, (a+w), a, (a+b+w)} \zeta_m^{ib+jw-l(a+w)} J_{a,b} J_{-a,-w} \]

and

\[ B(i, j, l) = m^2(q - 1)\delta_{i,0}\delta_{l,j} \]
\[ + \sum_{0 \leq a, b, w \leq m-1 \atop m|a+b \text{ or } (a+w) \text{ or } a \text{ or } (a+b+w)} \zeta_m^{ib+jw-l(a+w)} J_{a,b} J_{-a,-w}. \]

Since \( F(i, j, l) = A(i, j, l) + B(i, j, l) \), it is enough to prove that \( A(i, j, l) \sim 0 \sim B(i, j, l) \). By condition 6, we have

\[ A(i, j, l) = \sum_{0 \leq a, b, w \leq m-1 \atop m|a+b, (a+w), a, (a+b+w)} \zeta_m^{ib+jw-l(a+w)} J_{-(a+b+w), b} J_{a+b+w,-w}. \]

Changing variables, \( a \rightarrow -(a+b+w) \), we get

\[ A(i, j, l) = \sum_{0 \leq a, b, w \leq m-1 \atop m|a+b, (a+w), a, (a+b+w)} \zeta_m^{-ib+jw+l(a+b)} J_{a,b} J_{-a,-w} \]
\[ = \sum_{0 \leq a, b, w \leq m-1 \atop m|a+b, (a+w), a, (a+b+w)} \zeta_m^{-jw+ib-l(a+b)} J_{a,w} J_{-a,-b} \]
\[ = \sum_{0 \leq a, b, w \leq m-1 \atop m|a+b, (a+w), a, (a+b+w)} \zeta_m^{-jw+ib-l(a+b)} J_{a,b} J_{-a,-w} \]
\[ = A(j, i, l). \]

So, \( A(i, j, l) \sim 0 \).
It remains to prove that $B(i, j, l) \sim 0$. Write

$$B(i, j, l) = m^2(q - 1)\delta_{0, i} \delta_{j, l} + C(i, j, l) + D(i, j, l),$$

where

$$C(i, j, l) = \sum_{b=0}^{m-1} \sum_{w=0}^{m-1} \zeta_m^{-ib+jw-lw} J_{0, b} J_{-w},$$

$$D(i, j, l) = \sum_{0 \leq a \leq m-1} \zeta_m^{-ib+jw-l(a+w)} J_{a, b} J_{-a-w} J_{-w}. $$

By condition 4,

$$C(i, j, l) = \sum_{b=0}^{m-1} \sum_{w=0}^{m-1} \zeta_m^{-ib+(j-l)w} \left(- (q - 1)\delta_{0, b} + 1 \right) \left(- (q - 1)\delta_{0, w} + 1 \right)$$

$$= (q - 1)^2 - (q - 1) \sum_{w=0}^{m-1} \zeta_m^{(j-l)w} - (q - 1) \sum_{b=0}^{m-1} \zeta_m^{-ib} + \sum_{b=0}^{m-1} \zeta_m^{-ib} \sum_{w=0}^{m-1} \zeta_m^{(j-l)w}$$

$$= (q - 1)^2 - m(q - 1)\delta_{j, l} - m(q - 1)\delta_{0, i} + m^2\delta_{0, i}\delta_{j, l}. $$

So,

$$C(i, j, l) \sim -m(q - 1)\delta_{j, l} - m(q - 1)\delta_{0, i} + m^2\delta_{0, i}\delta_{j, l}. $$

Finally, write $D(i, j, l) = X(i, j, l) + Y(i, j, l)$, where

$$X(i, j, l) = \sum_{a=1}^{m-1} \sum_{b=0}^{m-1} \zeta_m^{-ib-ja} J_{a, b} J_{-a, a},$$

$$Y(i, j, l) = \sum_{0 \leq a \leq m-1} \sum_{0 \leq b \leq m-1} \sum_{w \not\equiv -a \mod m} \sum_{0 \leq a \leq m-1} \sum_{0 \leq b \leq m-1} \sum_{w \not\equiv -a \mod m} \zeta_m^{-ib+jw-l(a+w)} J_{a, b} J_{-a-w}. $$

If $m \nmid a$, by conditions 3 and 4, we have $J_{-a, a} = J_{0, a} = 1$. Therefore, by condition 2,

$$X(i, j, l) = \sum_{a=1}^{m-1} \sum_{b=0}^{m-1} \zeta_m^{-ib-jb} J_{a, b} = - \sum_{b=0}^{m-1} \zeta_m^{-ib} J_{0, b} - m^2[i, j]$$

$$= (q - 2) - \sum_{b=1}^{m-1} \zeta_m^{-ib} - m^2[i, j] = (q - 1) - m\delta_{0, i} - m^2[i, j].$$
Therefore, $B(i, j, l) \sim 0$. This ends the proof of (iv), and of Proposition 3. 

Let $Q$ be the prime ideal of $\mathbb{Z}[\zeta_m]$ above $q$ such that $s^l \equiv \zeta_m \mod Q$. If $k \in \mathbb{Z}$ we denote by $|k|_m$ the least nonnegative integer such that $|k|_m \equiv k \mod m$. We showed in [12], formula (27), that, for $0 \leq a, b \leq m - 1$ with $a + b \neq 0 \mod m$,

\[
\mathcal{J}_{a, b} = \left( \frac{f|a + b|_m}{f_a} \right) \mod Q.
\]

This fact is a simple consequence of (7), and [13], Chapter 1, Theorem 2.1.
The MAPLE program to calculate Jacobi sums that ends this section is based on the following proposition.

**Proposition 4.** Let \( a, b \) be integers, \( 1 \leq a, b \leq m-1 \), such that \( \gcd(a, b, m) = 1 \), and let \( 0 \leq l \leq m-1 \). Let \( u, v \) and \( \varepsilon(l) \) be as in Proposition 1. Then

\[
\frac{1}{u} \varepsilon(l) + \frac{1}{m} \sum_{i=1}^{u-1} \sum_{k=0}^{v-1} s^{(i+uk)m} \left( \frac{f_l(a+b)}{f_l(1+uk)m} \right) \mod q,
\]

and \( |d_{a,b,l}| < \sqrt{q} < q/2 \).

**Proof.** The first assertion follows directly from Proposition 1 and (17). The second assertion follows from Proposition 1, the triangle inequality, and the fact that \( |J_{a,b}| = \sqrt{q} \) if \( m \nmid a, m \nmid b \) and \( m \nmid (a+b) \).

In the following program enter the values of \( m > 2, q \) a prime \( \equiv 1 \mod 2m \), \( s \) a primitive root modulo \( q \) (the command: \( s := \text{primroot}(q) \); will give to \( s \) the value of the smallest positive primitive root modulo \( q \)), \( a \) and \( b \) integers, \( 1 \leq a, b \leq m-1 \), such that \( m \nmid a+b \), and such that \( \gcd(a, b, m) = 1 \) (see the observation preceding Proposition 1). The resulting matrix \( A \) is the row matrix \([d_{a,b,0}, d_{a,b,1}, \ldots, d_{a,b,m-1}]\).

The expression \( F(x) \) is the Jacobi sum \( J_{a,b} = \sum_{j=0}^{m-1} d_{a,b,j} \zeta_m^j \), if one replaces \( x \) by \( \zeta_m \). The expression \( G(x) \), a polynomial of degree \( < \varphi(m) \), is also equal to the Jacobi sum \( J_{a,b} \), if one replaces \( x \) by \( \zeta_m \). The last two lines are to check that \( J_{a,b}(1) = 1 \) and that \( J_{a,b} \downarrow_{a,b} = q \).

**A MAPLE program to calculate the Jacobi sums \( J_{a,b} \) given \( m, q \) and \( s \)**

with(linalg): with(numtheory):

\( m := 12; q := 73; s := \text{primroot}(q); a := 2; b := 5; \)

\( f := (q-1)/m; v := \text{igcd}(a+b, m); u := m/v; \)

for \( i \) from 0 to \( m-1 \) do;
\( ep(i) := \text{floor}(1-i/v + \text{floor}(i/v)); \)
\( \text{od}; \)

\( C := \text{array}(1..u, 1..v); \)

for \( j1 \) from 1 to \( u \) do;
for \( k1 \) from 1 to \( v \) do;
\( C[j1, k1] := \text{modp}(\text{binomial}(f \modp((j1-1)+(a+b), m), f \modp(((j1-1)+u(k1-1))a, m)), q); \)
\( \text{od}; \)
\( \text{od}; \)

\( A := \text{array}(1..1, 1..m); \)

for \( l \) from 1 to \( m \) do;
\( A[1, l] := \text{modp}(\text{ep}(l-1)/u + (1/m)*\text{sum}(\text{sum}(s^((i+uk)m)/(f_l(i-1)+f_l(u*(k-1))))*C[j, k, j=2..u], k=1..v), q); \)
\( \text{od}; \)

\( \text{A} := \text{evalm}(A); \)

\( R := \text{cyclotomic}(m, x); \)

\( F := x -> \text{sum}(A[1, t]*x^{t-1} \mod p, t=1..m); \)

\( F(x) := F(x); G := \text{rem}(F(x), R,x); \)

\( \# \text{ check:} \)

\( F(1); \)

\( \text{rem}(F(x) + F(x^m - 1), R,x); \)

2. **Families of irreducible polynomials of Gaussian periods of degree \( m \)**

As in Section 1, let \( m > 2 \) be an integer and \( \zeta_m \) an \( m \)-th primitive root of 1. Let \( S \) be the set of all prime numbers \( q \equiv 1 \mod 2m \). If \( q \in S \), \( s \) is a primitive root modulo \( q \), and \( Q \) is the prime ideal of \( \mathbb{Z} \{\zeta_m\} \) above \( q \) such that \( s^{(q-1)/m} \equiv \zeta_m \mod Q \), we write \( J_{a,b} = J_{a,b}[Q] \) for the Jacobi sums defined in (5). In this section we
show how to construct families of irreducible polynomials of Gaussian periods of degree $m$. We first show how one can make this construction in a general situation, and then work out several examples with $m$ small.

The first step in our method is to construct families $(J_{a,b}[Q])$, $0 \leq a, b \leq m - 1$, $Q \in \mathcal{I}$, of sets of principal ideals generated by Jacobi sums of the type studied in Section 1, where $\mathcal{I}$ is a set of prime ideals of $\mathbb{Z}[\zeta_m]$ above rational primes in $S$.

Let $\nu$ be a positive integer and, for $1 \leq i \leq \nu$, let $r_i$ be prime numbers (not necessarily distinct) not dividing $m$. Let $f_i$ be the smallest positive integer such that $r_i^{f_i} \equiv 1 \mod m$, $R_i$ a prime ideal of $\mathbb{Z}[\zeta_m]$ above $r_i$, $s_i \in \mathbb{Z}[\zeta_m]$ a generator of $\mathbb{Z}[\zeta_m]/R_i \cong \mathbb{F}_{r_i^{f_i}}$ (the field with $r_i^{f_i}$ elements) such that $s_i^{(r_i^{f_i} - 1)/m} \equiv \zeta_m \mod R_i$.

For $1 \leq i \leq \nu$ and $0 \leq a, b \leq m - 1$, let $\mathfrak{J}_{i,a,b}$ be the Jacobi sum

\begin{equation}
\mathfrak{J}_{i,a,b} = - \sum_{\gamma \in \mathbb{Z}[\zeta_m]/R_i, \gamma \neq 0, 1} \zeta_m^{a \text{ind}_{i,s_i}(\gamma) + b \text{ind}_{i,s_i}(1 - \gamma)},
\end{equation}

where $\text{ind}_{i,s_i}(\gamma)$ is the least nonnegative integer such that $s_i^{\text{ind}_{i,s_i}(\gamma)} \equiv \gamma \mod R_i$. We assume that the numbers $\mathfrak{J}_{i,a,b}$ are known (i.e. that they have been calculated).

If $c$ is an integer relatively prime with $m$, denote by $\sigma_c$ the automorphism of $\mathbb{Q}(\zeta_m)$ such that $\sigma_c(\zeta_m) = \zeta_m^c$. If $a + b \not\equiv 0 \mod m$, the prime ideal factorization of the ideal $\mathfrak{J}_{i,a,b}$ of $\mathbb{Z}[\zeta_m]$ is given by

\begin{equation}
(\mathfrak{J}_{i,a,b}) = \prod_{1 \leq c \leq m - 1, \text{g.c.d.}(c,m) = 1} \sigma_c^{-1}(\mathcal{J}_c)[\frac{[\frac{a+b}{m}]}{[\frac{a}{m}]}]-[\frac{b}{m}],
\end{equation}

where the bar denotes complex conjugation, and $[\rho]$ denotes the integral part of a real number $\rho$ (see [4], page 13, Fac 3).

Define $r = \prod_{i=1}^\nu r_i$ and $r' = \prod_{i=1}^\nu r_i^{f_i}$. Let

\[ C = \{ \alpha \in \mathbb{Z}[\zeta_m] : (\alpha) = R_1 \ldots R_\nu Q, \text{ with } N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(Q) = q \in S \}, \]

$\mathcal{A}$ a nonempty subset of $C$, and $\mathcal{I} = \{ Q = (\alpha)(R_1 \ldots R_\nu)^{-1} : \alpha \in \mathcal{A} \}$ (a set of prime ideals of $\mathbb{Z}[\zeta_m]$ above primes in $S$). For $0 \leq a, b \leq m - 1$ such that $m \mid a + b$, set

\[ \mathfrak{R}_{a,b} = \prod_{i=1}^\nu \mathfrak{J}_{i,a,b}, \]

and for $\alpha \in \mathcal{A}$, set

\begin{equation}
\mathfrak{R}_{a,b}[\alpha] = \prod_{1 \leq c \leq m - 1, \text{g.c.d.}(c,m) = 1} \sigma_c^{-1}(\mathcal{R}_c)[\frac{[\frac{a+b+c}{m}]}{[\frac{a}{m}]}]-[\frac{b}{m}].
\end{equation}

Then, for $\alpha \in \mathcal{A}$, we have $(\mathfrak{R}_{a,b}[\alpha]/\mathfrak{J}_{a,b}) = (J_{a,b}[Q])$ (equality of ideals of $\mathbb{Z}[\zeta_m]$), with $J_{a,b} = J_{a,b}[Q]$ as in (5), where $Q \in \mathcal{I}$ is the prime ideal $(\alpha)(R_1 \ldots R_\nu)^{-1}$. To prove this equality just check, using (19), that both sides have the same prime ideal factorization.

The choice of the set $\mathcal{A}$ will determine whether our family of polynomials has a nice description. One way to make this choice is the following. Take $\alpha_0, \alpha_1 \in \mathbb{Z}[\zeta_m]$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
such that \((\alpha_0, \alpha_1) = R_1 \ldots R_\nu\) and define \(A = A_1\), where

\[
A_1 = \left\{ \alpha = \alpha_0 + \alpha_1 \beta : \beta = \sum_{i=0}^{\varphi(m)-1} b_i \zeta_m^i \in \mathbb{Z}[\zeta_m] \right\}
\]

and \(N_{Q(\zeta_m)}/Q(\alpha) = r'q\), with \(q \in S\).

The parameters of the family we construct will then be the coefficients \(b_i\) of \(\beta\). In the examples we work with the simpler sets

\[
A_2 = \{ \alpha = \alpha_0 + \alpha_1 n : n \in \mathbb{Z} \text{ and } N_{Q(\zeta_m)}/Q(\alpha) = r'q, \text{ with } q \in S \}.
\]

The second step is to identify the Jacobi sums \(J_{a,b}[Q], Q \in \mathbb{I}\), among the generators of the principal ideals \((J_{a,b}[Q])\). One way to do that is to start with a subset \(A\) of \(C\) such that if \(\alpha \in A\) the numbers \(\mathfrak{R}_{a,b}[\alpha]\) are products of Jacobi sums (as the ones defined in (18)). Then we know after Weil [14] that, using the notation above, for \(\alpha \in A\) and \(Q = (\alpha)(R_1 \ldots R_\nu)^{-1}\), \(J_{a,b}[Q] = \mathfrak{R}_{a,b}[\alpha]/\mathfrak{J}_{a,b}\). Also, by [14], we know that there is a divisor \(f\) of \(m^2\) such that any nonempty subset \(A\) of the set \(C = \{ \alpha \in C : \alpha \equiv 1 \text{ mod } f \}\) has the desired property. Another way to identify the \(J_{a,b}[Q]\) among the generators of the ideals \((J_{a,b}[Q])\), which works at least when \(m = p\) is a prime and was used in [12], relies on the fact that only one of the numbers \(\delta_{\zeta_m^k} \mathfrak{R}_{a,b}[\alpha]/\mathfrak{J}_{a,b}, \delta \in \{1, -1\}, 0 \leq k \leq m - 1\), satisfies congruence (13), and that number is \(J_{a,b}[Q]\).

From the family \(J_{a,b}[Q], Q \in \mathbb{I}\), of sets of Jacobi sums, we construct, using (4) and (15), a family \(C[Q], Q \in \mathbb{I}\), of matrices with entries \(c_{i,j} = c_{i,j}[Q]\), whose characteristic polynomials form, by (3), the desired family \(P_q(x), q \in \mathbb{P}\), of irreducible polynomials of Gaussian periods of degree \(m\). Here \(\mathbb{P} = \{ q = N_{Q(\zeta_m)}/Q(\mathbb{I}) : Q \in \mathbb{I} \}\) \(\subseteq S\). Note that ideals \(Q \in \mathbb{I}\) are in the inverse ideal class of the ideal \(\mathfrak{R} = \prod_{i=1}^\nu R_i\).

In what follows we give examples of this construction and a MAPLE program to search for more examples.

**Example 1.** For \(m = 7\), and primes of the form

\[
q = 49n^6 - 49n^3 + 49n^4 + 35n^3 + 21n^2 + 7n + 1,
\]

the irreducible polynomials of the Gaussian periods of degree \(m\) in \(\mathbb{Q}(\zeta_q)\) are

\[
P_q(x) = x^7 + x^6 + (-21n^6 + 21n^5 - 21n^4 - 15n^3 - 9n^2 - 3n)x^5
\]

\[
+ (-21n^9 + 28n^8 + 7n^7 - 48n^6 + 36n^5 + 20n^4 + 12n^3 + 3n^2)x^4
\]

\[
+ (91n^{12} - 147n^{11} + 252n^{10} - 85n^9 + 73n^8
\]

\[
+ 100n^7 + 21n^6 + 10n^5 - 2n^4 - n^3)x^3
\]

\[
+ (112n^{15} - 203n^{14} + 157n^{13} + 113n^{12} - 227n^{11}
\]

\[
+ 127n^{10} - 23n^9 - 45n^8 - 25n^7 - 14n^6 - 2n^5)x^2
\]

\[
+ (-84n^{18} + 238n^{17} - 518n^{16} + 629n^{15} - 442n^{14}
\]

\[
+ 196n^{13} - 8n^{12} - 22n^{10} - 26n^9 - 11n^8 - n^7)x
\]

\[
- 97n^{21} + 357n^{20} - 609n^{19} + 434n^{18} + 52n^{17} - 282n^{16} + 94n^{15}
\]

\[
+ 56n^{14} + 7n^{13} - 3n^{12} - 8n^{11} - 2n^{10}.
\]
To obtain this result we start with the elements $1 + n(\zeta_m - 1)^2$ in $\mathbb{Z}[\zeta_m]$, which have norms $q = q(n)$ and generate prime ideals $Q = (1 + n(\zeta_m - 1)^2)$. We calculate the Jacobi sums $J_{a,b}[Q]$ using Stickelberger’s theorem and the fact that if $m = p$ is a prime then $J_{a,b}[Q] \equiv 1 \mod (\zeta_m - 1)^2$. We use the values of the Jacobi sums found to calculate the matrices $C = C[Q]$. Finally we calculate the characteristic polynomials of the $C[Q]$, which are the irreducible polynomials we wanted to find. All these calculations are performed by the program at the end of the article, where we must enter only the values $m := 7$; and $F := z - 1 + n(z-1)^2$.

In general the “smallest” examples I found for $m$ prime start with the elements $\alpha = 1 + n(\zeta_m - 1)^3$ which have norms $q = q(n)$ that are polynomials in $n^2$. The coefficients of the resulting polynomials $P_q(x)$ are also polynomials in $n^2$. Something similar works for arbitrary $m$, where the right expression for $\alpha$ can be found by trial and error ($q(n)$ must be an irreducible polynomial in $\mathbb{Z}[n]$ and the matrix $C([\alpha])$ must have its entries in $\mathbb{Z}[n]$). This is illustrated in Examples 2, 3 and 4.

**Example 2.** For $m = 7$, and primes of the form

$$q = 343n^6 + 833n^4 + 70n^2 + 1,$$

the irreducible polynomials of the Gaussian periods of degree $m$ in $\mathbb{Q}(\zeta_q)$ are

$$P_q(x) = x^7 + x^6 + (-147n^6 - 357n^4 - 30n^2)x^5$$
$$+ (-294n^8 - 749n^6 - 145n^4 - 8n^2)x^4$$
$$+ (7203n^{12} + 30086n^{10} + 32403n^8 + 3436n^6 + 96n^4)x^3$$
$$+ (28812n^{14} + 128723n^{12} + 152306n^{10}$$
$$+ 21199n^8 + 1008n^6 + 16n^4)x^2$$
$$+ (-117649n^{18} - 617057n^{16} - 787577n^{14}$$
$$+ 47481n^{12} + 45234n^{10} + 3104n^8 + 32n^6)x$$
$$- 705894n^{20} - 3186127n^{18} - 3505999n^{16} + 213835n^{14}$$
$$+ 39841n^{12} + 904n^{10} + 16n^8.$$

To obtain this result we proceed in a similar way as in Example 1. Enter the values $m := 7$; and $F := z - 1 + n(z-1)^3$; in the program at the end of the article.

**Example 3.** For $m = 9$, and primes of the form

$$q = 2187n^6 + 729n^4 + 54n^2 + 1,$$
the irreducible polynomials of the Gaussian periods of degree $m$ in $\mathbb{Q}(\zeta_q)$ are

$$P_q(x) = x^9 + x^8 + (-972n^6 - 324n^4 - 24n^2)x^7 + (-3888n^8 - 1548n^6 - 180n^4 - 8n^2)x^6$$
$$+ (196830n^{12} + 148716n^{10} + 34830n^8 + 2856n^6 + 80n^4)x^5 + (62956n^{14} + 535086n^{12} + 148716n^{10} + 16830n^8 + 840n^6 + 16n^4)x^4$$
$$+ (-14880348n^{18} - 10786284n^{16} - 2259900n^{14} - 106164n^{12} + 7128n^{10} + 480n^8)x^3$$
$$+ (-25509168n^{20} - 18659484n^{18} - 6167340n^{16} - 1097388n^{14} - 95652n^{12} - 3480n^{10} - 32n^8)x^2$$
$$+ (387420489n^{24} + 70150212n^{22} - 29878794n^{20} - 7934436n^{18} - 489159n^{16} + 3672n^{14} + 720n^{12})x$$
$$- 29229255n^{24} - 1653372n^{22} + 2523798n^{20} + 384156n^{18} + 22761n^{16} + 792n^{14} + 16n^{12}.$$

To obtain this result we proceed in a similar way as in Example 1. This time enter the values $m=9$ and $F=z-1+3\pi n(z-z^{-1})$ in the program at the end of the article. Observe that the resulting matrix $C$ has entries in $\mathbb{Z}[n]$.

**Example 4.** For $m=12$, and primes of the form $q=1296n^4 + 72n^2 + 1$,

the irreducible polynomials of the Gaussian periods of degree $m$ in $\mathbb{Q}(\zeta_q)$ are

$$P_q(x) = x^{12} + x^{11} + (-594n^4 - 33n^2)x^{10} + (216n^6 - 153n^4 - 9n^2)x^9$$
$$+ (120771n^8 + 8937n^6 + 186n^4)x^8$$
$$+ (-116640n^{10} + 8586n^8 + 1044n^6 + 24n^4)x^7$$
$$+ (-9713196n^{12} - 858762n^{10} - 26784n^8 - 304n^6)x^6$$
$$+ (19840464n^{14} + 581742n^{12} - 28998n^{10} - 1368n^8 - 16n^6)x^5$$
$$+ (278337303n^{16} + 30561138n^{14} + 1165428n^{12} + 18144n^{10} + 96n^8)x^4$$
$$+ (-105500880n^{18} - 84367899n^{16} - 1851660n^{14} + 1512n^{12} + 288n^{10})x^3$$
$$+ (-806018850n^{20} - 210194757n^{18} - 14311728n^{16} - 377136n^{14} - 3456n^{12})x^2$$
$$+ (7971615000n^{22} + 1069672635n^{20} + 52743879n^{18} + 1137240n^{16} + 9072n^{14})x$$
$$- 8968066875n^{24} - 1102790075n^{22} - 5090530n^{20} - 1026432n^{18} - 7776n^{16}.$$

To obtain this result we proceed in a similar way as in Example 1. This time enter the values $m=12$ and $F=z-1+6\pi n(z-z^{-1})$ in the program at the end of the article. Observe that the resulting matrix $C$ has entries in $\mathbb{Z}[n]$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
The element \( s_1 = 1 + w^3 \) is too large for a complete example, in paper, of a family of irreducible polynomials such that \( s_1 = s_1^{(8-1)/7} \equiv w \mod R_1 \). Let

\[
A_3 = \{ \alpha = w^5 - 2w^4 + 3w^3 - w^2 + 2 + 2(w - 1)^2n \}
\]

\( n \in \mathbb{Z} \) and \( \mathcal{N}_{\mathbb{Q}(w)/\mathbb{Q}}(\alpha) = 8q, \) with \( q \in S \}, \)

and

\[
\mathcal{I} = \{ Q = (\alpha)R_1^{-1} : \alpha \in A_3 \}.
\]

Example 5. Let \( m = 7 \) and \( w = \zeta_7 \) a 7-th primitive root of 1. Take \( r_1 = 2 \). Set \( R_1 = (w^5 - 2w^4 + 3w^3 - w^2 + 2, 2(w - 1)^2) = (1 + w + w^3) \). We have \( (2) = R_1 R_1^\perp \). Since we really need to work with auxiliary Jacobi sums illustrate how the method works in the general situation. The first cases in which occur when \( m = 23 \), which is too large for a complete example, in paper, of a family of irreducible polynomials of Gaussian periods (but see Example 6).

If \( \alpha = w^5 - 2w^4 + 3w^3 - w^2 + 2 + 2(w - 1)^2n \in A_3 \), then

\[
\mathcal{N}_{\mathbb{Q}(w)/\mathbb{Q}}(\alpha) = 8(392n^6 + 98n^4 + 161n^3 + 14n^2 - 35n + 113).
\]

So we are searching for the irreducible polynomials of the Gaussian periods of degree 7 corresponding to the primes \( q \) of the form

\[
q = 392n^6 + 98n^4 + 161n^3 + 14n^2 - 35n + 113.
\]

Set \( \mathcal{J}_{a,b} = \mathcal{J}_{1,a,b} \), the Jacobi sums corresponding to \( s_1 \) and \( R_1 \). By (18) we have

\[
\mathcal{J}_{1,1} = \mathcal{J}_{1,5} = -2(w + w^2 + w^4),
\]

\[
\mathcal{J}_{1,2} = \mathcal{J}_{1,4} = -(3 + w^3 + w^5 + w^6),
\]

\[
\mathcal{J}_{1,3} = \mathcal{J}_{1,1} = -2(w^3 + w^5 + w^6).
\]

For \( Q \in \mathcal{I} \) and \( \alpha \in A_3 \) such that \( (\alpha) = R_1Q \), define \( \mathcal{R}_{a,b}[\alpha] \) as in (20). We have

\[
\mathcal{R}_{1,1}[\alpha] = (24n^2 - 12n - 6)w^5 + (-36n^2 - 18n - 6)w^4
\]

\[
+ (-56n^3 - 12n^2 + 32n - 4)w^3 + (12n^2 + 6n - 24)w^2
\]

\[
+ (-48n^2 - 18n + 12)w - 24n^2 + 24n + 6,
\]

\[
\mathcal{R}_{1,2}[\alpha] = (6n - 21)w^4 + (6n - 21)w^2 + (6n - 21)w - 56n^3 - 4n - 22,
\]

\[
\mathcal{R}_{1,3}[\alpha] = (-48n^2 - 24n + 18)w^5 + (-12n^2 - 6n + 24)w^4
\]

\[
+ (-60n^2 - 24n + 36)w^3 + (-56n^2 - 24n^2 + 26n + 20)w^2
\]

\[
+ (12n^2 - 18n + 18)w - 36n^2 + 18n + 30,
\]

\[
\mathcal{R}_{1,4}[\alpha] = (6n - 21)w^4 + (6n - 21)w^2 + (6n - 21)w - 56n^3 - 4n - 22,
\]

\[
\mathcal{R}_{1,5}[\alpha] = (24n^2 - 12n - 6)w^5 + (-36n^2 - 18n - 6)w^4
\]

\[
+ (-56n^3 - 12n^2 + 32n - 4)w^3 + (12n^2 + 6n - 24)w^2
\]

\[
+ (-48n^2 - 18n + 12)w - 24n^2 + 24n + 6.
\]
Using the formula \((J_{a,b}[Q]) = (R_{a,b}[\alpha]/J_{a,b})\), and the fact that \(J_{a,b}[Q] \equiv 1 \mod (w - 1)^2\), we get

\[
J_{1,1}(Q) = -w^3R_{1,1}[\alpha]/J_{1,1}
= (-14n^3 - 3n^2 + 5n - 1)w^5 + (-14n^3 + 15n^2 + 8n - 7)w^4
+ (-9n^2 - 6n - 3)w^3 + (-14n^3 - 12n^2 + 11n + 5)w^2
+ (6n^2 + 9n - 3)w + 3n^2 - 6n + 3,
\]

\[
J_{1,2}(Q) = -w^3R_{1,2}[\alpha]/J_{1,2}
= (-7n^3 + n - 8)w^4 + (-7n^3 + n - 8)w^2
+ (-7n^3 + n - 8)w - 21n^3 - 3n - 3,
\]

\[
J_{1,3}(Q) = -w^2R_{1,3}[\alpha]/J_{1,3}
= (27n^2 - 3n - 12)w^5 + (14n^3 + 12n^2 - 11n - 5)w^4
+ (14n^3 + 18n^2 - 2n - 8)w^3 + (14n^3 + 3n^2 - 17n - 8)w^2
+ (9n^2 - 6n - 6)w + 14n^3 + 15n^2 - 17n - 2,
\]

\[
J_{1,4}(Q) = -w^3R_{1,4}[\alpha]/J_{1,4}
= (-7n^3 + n - 8)w^4 + (-7n^3 + n - 8)w^2
+ (-7n^3 + n - 8)w - 21n^3 - 3n - 3,
\]

\[
J_{1,5}(Q) = -w^3R_{1,5}[\alpha]/J_{1,5}
= (-14n^3 - 3n^2 + 5n - 1)w^5 + (-14n^3 + 15n^2 + 8n - 7)w^4
+ (-9n^2 - 6n - 3)w^3 + (-14n^3 - 12n^2 + 11n + 5)w^2
- 6n + (6n^2 + 9n - 3)w + 3n^2 + 3.
\]

For \(1 \leq i \leq 5\) write

\[
J_u = J_{1,u}[Q] = \sum_{k=0}^{6} d_{u,k} \zeta_p^k, \quad \text{with} \quad d_{u,k} \in \mathbb{Z}[n] \quad \text{such that} \quad \sum_{k=0}^{6} d_{u,k} = 1.
\]

Denote by \(A\) the matrix \([d_{u,k}]_{0 \leq u \leq 5, 0 \leq k \leq 6}\). From the results above we obtain

\[
A^t = \begin{bmatrix}
4 - 9n + 3n^2 + 6n^3 & 1 - 3n - 15n^3 & 4 - 9n + 3n^2 + 6n^3 & 1 - 3n - 15n^3 & 4 - 9n + 3n^2 + 6n^3 \\
-2 + 6n + 6n^2 + 6n^3 & -4 + n - n^3 & 2n - 3n^2 - 8n^3 & -4 + n - n^3 & -2 + 6n + 6n^2 + 6n^3 \\
6 + 8n - 12n^2 - 8n^3 & -4 + n - n^3 & -2 - 9n - 9n^2 + 6n^3 & -4 + n - n^3 & 6 + 8n - 12n^2 - 8n^3 \\
-2 - 9n - 9n^2 + 6n^3 & 4 + 6n^3 & -2 + 6n + 6n^2 + 6n^3 & 4 + 6n^3 & -2 - 9n - 9n^2 + 6n^3 \\
-6 + 5n + 15n^2 - 8n^3 & -4 + n - n^3 & 1 - 3n + 6n^3 & -4 + n - n^3 & -6 + 5n + 15n^2 - 8n^3 \\
2n - 3n^2 - 8n^3 & 4 + 6n^3 & -6 + 5n + 15n^2 - 8n^3 & 4 + 6n^3 & 2n - 3n^2 - 8n^3 \\
1 - 3n + 6n^3 & 4 + 6n^3 & 6 + 8n - 12n^2 - 8n^3 & 4 + 6n^3 & 1 - 3n + 6n^3
\end{bmatrix}.
\]
Formula (15) is, in the case $m = p$ prime, equivalent to the following:

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

where $f = (q - 1)/p$ (see, for example, [11], formula 7). Using this and (4), we calculate the matrix $C = [c_{i,j}]$. We have

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

where $f = 56n^6 + 14n^4 + 23n^3 + 2n^2 - 5n + 16$ and

$$X_0 = 8n^6 + 2n^4 + 5n^3 - n^2 + 4n,$$

$$X_1 = 4 + 8n^6 + 2n^4 + 3n^3 - n^2 - 3n,$$

$$X_2 = 8n^6 + 2n^4 + 5n^3 + 5n^2 - 2n + 2,$$

$$X_3 = 8n^6 + 2n^4 - n^3 + 2n^2 + n + 2,$$

$$X_4 = 8n^6 + 2n^4 + 5n^3 - 4n^2 - 2n + 5,$$

$$X_5 = 8n^6 + 2n^4 + 5n^3 - n^2 + 2n + 2,$$

$$X_6 = 8n^6 + 2n^4 + n^3 + 2n^2 - n,$$

$$X_7 = 8n^6 + 2n^4 + 2n^3 - n^2 + n + 3,$$

$$X_8 = 8n^6 + 2n^4 + 6n^3 - n^2 - 3n + 2,$$

$$X_9 = 8n^6 + 2n^4 + 4n^3 + 2n^2 - n + 1,$$

$$X_{10} = 8n^6 + 2n^4 + 5n^3 + 2n^2 + n + 3,$$

$$X_{11} = 8n^6 + 2n^4 - n^2 + 2.$$

Therefore, by (3), for all primes of the form

$$q = 392n^6 + 98n^4 + 161n^3 + 14n^2 - 35n + 113,$$
the irreducible polynomials of the Gaussian periods of degree 7 in $\mathbb{Q}(\zeta_q)$ are

$$P_q(x) = \det(xI - C) = x^7 + x^6 + (-168n^6 - 42n^4 - 6n^2 + 15n - 48)x^5$$

$$+ (-224n^9 + 168n^8 + 672n^7 + 78n^6 - 93n^5$$

$$- 195n^4 + 49n^3 + 108n^2 - 189n + 37)x^4$$

$$+ (6608n^{12} + 2856n^{11} + 28n^{10} + 6140n^9$$

$$+ 1251n^8 + 1395n^7 + 3850n^6 + 1635n^5$$

$$+ 338n^4 + 1271n^3 - 57n^2 + 443n + 312)x^3$$

$$+ (14784n^{15} + 12768n^{14} + 23856n^{13} + 8184n^{12}$$

$$+ 8100n^{11} + 26226n^{10} + 4935n^9 + 4377n^8$$

$$+ 16176n^7 + 1200n^6 - 2373n^5$$

$$+ 6063n^4 + 792n^3 - 501n^2 + 573n - 12)x^2$$

$$+ (-36736n^{18} + 41664n^{17} + 64176n^{16} - 122352n^{15}$$

$$- 30492n^{14} + 16518n^{13} - 146848n^{12}$$

$$- 50097n^{11} + 22722n^{10} - 82665n^9 - 46842n^8$$

$$+ 3279n^7 - 29398n^6 - 16158n^5 + 1698n^4$$

$$- 4317n^3 - 4050n^2 - 894n - 49)x$$

$$- 33664n^{21} + 146496n^{20} + 24640n^{19} - 276528n^{18}$$

$$- 158904n^{17} - 275688n^{16} + 447508n^{15} - 216771n^{14}$$

$$- 185387n^{13} - 290411n^{12} - 179430n^{11} - 127792n^{10}$$

$$- 130448n^9 - 65166n^8 - 28901n^7 - 26116n^6$$

$$- 18399n^5 - 9110n^4 - 2993n^3 - 519n^2 - 39n - 1.$$

**Example 6.** Let $m = 23$, $r_1 = 47$ and $R_1 = (1 + \zeta_{23}^2 - \zeta_{23}^3, 47)$ (a nonprincipal prime ideal of $\mathbb{Z}[\zeta_{23}]$; see, for example, [3], page 104). Set

$$\mathcal{A}_1 = \{\alpha = 1 + \zeta_{23}^2 - \zeta_{23}^3 + 47n : n \in \mathbb{Z} \text{ and } N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}}(\alpha) = 47q, \text{ with } q \in S\},$$

and

$$\mathcal{I} = \{Q = (\alpha)R_1^{-1} : \alpha \in \mathcal{A}_1\}.$$

With notation as in (18), put $\mathfrak{J}_{a,b} = \mathfrak{J}_{1,a,b}$, and $s_1 = -2$, which is a primitive root modulo 47 such that $s_1^{(47-1)/23} = (-2)^2 \equiv \zeta_{23} \mod R_1$. Using the MAPLE program at the end of Section 1, with $m = 23$, $q = 47$ and $s = -2$, we find that

$$\mathfrak{J}_{1,1} = 2 - 2\zeta_{23}^2 + 2\zeta_{23}^8 - 2\zeta_{23}^9 + 2\zeta_{23}^{12} + 2\zeta_{23}^{13}$$

$$+ 2\zeta_{23}^{14} - 2\zeta_{23}^{15} + 2\zeta_{23}^{16} - 2\zeta_{23}^{18} - 2\zeta_{23}^{20} - \zeta_{23}^{21}.$$

For $\alpha \in \mathcal{A}_1$, let

$$\mathfrak{R}_{1,1}[\alpha] = \prod_{c=1}^{22} \sigma_c^{-1}(\alpha)[\zeta_{23}].$$
We can obtain the family of Jacobi sums $J_{1,1}[Q]$, $Q \in \mathcal{I}$, using the formula

$$J_{1,1}[Q] = \left( \frac{n+1}{23} \right)^{-k_1} \mathfrak{R}_{1,1}[\alpha]/J_{1,1,1} = \left( \frac{n+1}{23} \right)^{-k_1} \mathfrak{R}_{1,1}[\alpha]/J_{1,1,1}/47,$$

where $(\alpha) = R_1Q$, $\alpha \in A_4$, $\left( \frac{23}{n+1} \right)$ is the Legendre symbol, and

$$k \equiv 11 \left( \frac{n+1}{23} \right)(n+1)^{10} \mod 23.$$

To prove this equality, check that the numbers on both sides generate the same ideals in $\mathbb{Z}[\zeta_{23}]$, and that the right hand side is $\equiv 1 \mod (\zeta_{23} - 1)^2$. We do not write the expanded expression of $J_{1,1}[Q]$ in $\mathbb{Z}[\zeta_{23}, n]$, since it occupies more than one page.

Proceeding in a similar way we can find all the families of Jacobi sums $J_{1,1}[Q], \ldots, J_{1,21}[Q], Q \in \mathcal{I}$. With these families we can construct, using (3), (4), and (15) (or better [11], formulas (6) and (7), as in Example 4), the family of irreducible polynomials $P_Q(x) \in \mathbb{Z}[n, x]$, of Gaussian periods of degree 23, corresponding to the primes of the form

$$q = q(n) = 130033429462229783044185156533092847n^{22} + 60866711663171387807916456249532822n^{21} + 1359782392836161106023889162129673n^{20} + 19287776443739235611381403066850606n^{19} + 19492965554842845008641839505405n^{18} + 14930782127113668128321502600414n^{17} + 900082610499760135395267887259n^{16} + 43773014492389550657520626736n^{15} + 1746389479019419656026933311n^{14} + 5775967528053201788638220n^{13} + 1594119954503408569331187n^{12} + 36397389727152969816873n^{11} + 666486961951621859180n^{10} + 887425237258368851n^9 + 5433532966956750n^8 - 992442355341030n^7 - 37699732250660n^6 - 646801716550n^5 - 6475959625n^4 - 5641786n^3 + 1224820n^2 + 22033n + 139.$$

These primes are norms of the prime ideals in $\mathcal{I}$. Note that the prime ideals in $\mathbb{Q}[\zeta_{23}]$ above primes of the form $q(n)$ are not principal.

In the following program enter the values of $m$, an integer $> 2$, and $F$, a polynomial function in $z$, with coefficients depending on one or more parameters $n_1, \ldots, n_k$, which, when $z$ is replaced by $\zeta_m$ and the $n_i$ by integers, gives elements of $\mathbb{Z}[\zeta_m]$ that are either $\equiv 1 \mod m^2$, or $\equiv 1$ modulo a smaller divisor of $m^2$, provided that the resulting matrix $C$ still has its entries in $\mathbb{Z}[n_1, \ldots, n_k]$ (these entries are always in $\mathbb{Q}[n_1, \ldots, n_k]$). The smallest such divisor of $m^2$ for which the program works is, likely, the conductor of the Hecke character defined in Weil's article [14], which we called $f$ in the discussion above. The resulting value of $q$ must be irreducible in $\mathbb{Z}[n_1, \ldots, n_k]$. (With the help of a computer it is easy to check that in fact...
the matrix \( C = [c_{i,j}] \) satisfies the conditions of \[ \text{Proposition 2, or, equivalently,} \]
that the matrix \( H \), whose entry in row \( a \) and column \( b \) is equal to the Jacobi sum
\( J_{a,b} \) when \( m \nmid a + b \), satisfies the conditions of Propositions 2 and 3.\)
The resulting polynomial \( P \) gives, for all values of the parameters such that \( q = q(n_1, \ldots, n_k) \) is
a prime, the irreducible polynomials of the Gaussian periods of degree \( m \) in \( \mathbb{Q}(\zeta_q) \).

A MAPLE program to find families of irreducible polynomials of Gaussian periods of degree \( m \) for arbitrary \( m > 2 \)

```maple
with(numtheory): with(linalg):
m:=10; F:=z->z>1+n*10*(z-z^ (m-1));
R:=cyclotomic(m,z);
for i0 from 0 to m-1 do;
T[i0]:=modp(i0^ (phi(m)-1),m); od:
for i1 from 0 to m-1 do;
if igcd(i1,m)=1 then t[i1]:=1;
else t[i1]:=0; fi; od;
q:=rem(expand(product(F(z^ c)^ t[c],c=0..m-1)),R,z);
factor(q);
f:=(q-1)/m; A:=array(1..m-1,1..m-1,1..m):
for i2 from 1 to m-1 do;
for j2 from 1 to m-1 do;
for k2 from 1 to m do;
A[i2,j2,k2]:=((i2+j2-1)/(m-1)+m-1)/m;-
floor(floor((i2+j2-1)/(m-1)+m-1)/m)-
floor((i2+j2-1)/(m-1)+m-1)/m)*t[k2-1];
od: od: od:
B:=array(1..m-1,1..m-1):
for i3 from 1 to m-1 do;
for j3 from 1 to m-1 do;
B[i3,j3]:=expand(product(F(z^ (m-T[k3-1]))^ t[c],c=0..m-1),R,z));
H:=array(1..m-1,1..m-1):
for i4 from 1 to m-1 do;
for j4 from 1 to m-1 do;
H[i4,j4]:=sort(collect(rem(B[i4,j4],R,z),z)); od: od:
evalm(H);
C:=array(1..m-1,1..m):
for i5 from 1 to m do;
for j5 from 1 to m do;
C[i5,j5]:=rem(-F^ lId[i5]+(m^ lId[i5]+m^ lId[i5]+m^ lId[i5]+q-1+)
sum(sum(rem(z^ ((m-i5+1)*a+((m-i5+1)*b)+H[a,b],a=1..m-1, b=1..m-1)-
sum(z^ ((m-i5+1)*b)+H[l,m-l],l=1..m-1),R,z); od: od:
evalm(C);
P:=sort(collect(charpoly(C,x),x),x);
```

REFERENCES

1. B. Berndt, R. Evans and K. Williams, Gauss and Jacobi sums, John Wiley & Sons Inc., New
2. L.E. Dickson, Cyclotomy, higher congruences and Waring’s problem, Amer. J. Math. 57
(1935), 391–424.
3. H. Edwards, Fermat’s Last Theorem, a Genetic Introduction to Algebraic Number Theory,
83b:12001
4. S. Lang, Cyclotomic fields I and II (with an appendix by K. Rubin), Combined Second Edition,

**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