MATHEMATICS OF COMPUTATION
Volume 70, Number 236, Pages 1617–1640
S 0025-5718(01)01312-6
Article electronically published on May 11, 2001

JACOBI SUMS AND NEW FAMILIES OF IRREDUCIBLE POLYNOMIALS OF GAUSSIAN PERIODS

F. THAINE

ABSTRACT. Let $m > 2$, ζ_m an m-th primitive root of 1, $q \equiv 1 \bmod 2m$ a prime number, $s = s_q$ a primitive root modulo q and $f = f_q = (q-1)/m$. We study the Jacobi sums $J_{a,b} = -\sum_{k=2}^{q-1} \zeta_m^{a\,\mathrm{ind}_s(k)+b\,\mathrm{ind}_s(1-k)}$, $0 \le a, b \le m-1$, where $\mathrm{ind}_s(k)$ is the least nonnegative integer such that $s^{\mathrm{ind}_s(k)} \equiv k \bmod q$. 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, $\eta_i = \sum_{j=0}^{f-1} \zeta_q^{s^{i+mj}}$, of degree m, where $\mathcal{P}$ is a suitable set of primes $\equiv 1 \bmod 2m$. 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 ζ_m an m-th primitive root of 1. For each prime $q \equiv 1 \bmod 2m$ let ζ_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 $q \equiv 1 \bmod 2m$. Given $q \in S$, define the Jacobi sums $J_{a,b}$, $0 \le a, b \le m-1$, and the Gaussian periods η_i, $0 \le i \le m-1$, of degree m in $\mathbb{Q}(\zeta_q)$, by

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

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

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

Define $P_q(x) = \prod_{i=0}^{m-1}(x - \eta_i)$, the irreducible polynomial, over $\mathbb{Q}$, of the periods η_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

Received by the editor September 15, 1998 and, in revised form, January 19, 2000.
2000 *Mathematics Subject Classification.* Primary 11R18, 11R21, 11T22.
This work was supported in part by grants from NSERC and FCAR.

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

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

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 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, ζ_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

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

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 η_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 $\langle k, l \rangle$, $0 \leq k, l \leq f-1$, such that $1 + s^{km+i} \equiv s^{lm+j} \bmod q$ (see, for example, [1], §2.2, [2], or [8]). Define $\eta_{i+km} = \eta_i$, $c_{i+km,j+lm} = c_{i,j}$, 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:

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

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

$$c_{i,j} = (i, j) - f\delta_{0,i}, \tag{4}$$

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

Let $G(x) = \sum_{k=0}^{q-2} x^k \zeta_q^{s^k}$, 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 ζ_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 η_i are real numbers).

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

$$J_{a,b} = -\sum_{k=2}^{q-1} \zeta_m^{a \operatorname{ind}_s(k) + b \operatorname{ind}_s(1-k)}, \tag{5}$$

where $\operatorname{ind}_s(k)$ is the least nonnegative integer such that $s^{\operatorname{ind}_s(k)} \equiv k \bmod q$. 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,

$$\begin{aligned} J_{-a-b,b} &= -\sum_{k=2}^{q-1} \zeta_m^{(-a-b)\,\mathrm{ind}_s(k)+b\,\mathrm{ind}_s(1-k)} \\ &= -\sum_{k=2}^{q-1} \zeta_m^{-a\,\mathrm{ind}_s(k)+b\,\mathrm{ind}_s(k^{-1}-1)} \\ &= -\sum_{k=2}^{q-1} \zeta_m^{a\,\mathrm{ind}_s(k)+b\,\mathrm{ind}_s(k-1)} \\ &= -\sum_{k=2}^{q-1} \zeta_m^{a\,\mathrm{ind}_s(k)+b\,\mathrm{ind}_s(1-k)} = J_{a,b}, \end{aligned}$$

since f is even.

Suppose that $0 \le a, b \le m-1$. If $a+b \not\equiv 0 \bmod m$, then

$$J_{a,b} = -\frac{G(\zeta_m^a)G(\zeta_m^b)}{G(\zeta_m^{a+b})}; \tag{7}$$

also

$$J_{0,0} = -(q-2), \quad \text{and} \quad J_{a,b} = 1 \ \text{ if } \ a+b \equiv 0 \mod m \ \text{ but } \ a \neq 0 \tag{8}$$

(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 ζ_m, which is very convenient for our purposes. For a and b nonnegative integers let $f_{a,b}(x)$ be the polynomial

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

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,

$$J_{a,b}(x) = \sum_{j=0}^{m-1} d_{a,b,j}x^j \equiv f_{a,b}(x) \qquad \mod x^m - 1. \tag{9}$$

Clearly, for $a, b \ge 0$, we have

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

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

and, for $k \ge 0$ such that $k \not\equiv 0 \bmod m$,

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

We also have

$$J'_{a,b}(1) = \sum_{j=1}^{m-1} j d_{a,b,j} \equiv 0 \quad \mod m. \tag{13}$$

In fact, by (9),

$$J_{a,b}(x) = -\sum_{k=2}^{q-1} x^{a\,\mathrm{ind}_s(k)+b\,\mathrm{ind}_s(1-k)} + (x^{q-1}-1)/(x-1) + (x^m-1)g(x),$$

for some $g(x) \in \mathbb{Z}[x]$. Taking derivatives, we get

$$\begin{aligned} J'_{a,b}(x) = &-\sum_{k=2}^{q-1} (a\,\mathrm{ind}_s(k)+b\,\mathrm{ind}_s(1-k))x^{a\,\mathrm{ind}_s(k)+b\,\mathrm{ind}_s(1-k)-1} \\ &+ (1+2x+\cdots+(q-2)x^{q-3}) + (x^m-1)g'(x) + mx^{m-1}g(x). \end{aligned}$$

Therefore

$$J'_{a,b}(1) = -a\sum_{k=2}^{q-1}\mathrm{ind}_s(k) - b\sum_{k=2}^{q-1}\mathrm{ind}_s(1-k) + m(f/2)(q-2) + mg(1) \equiv 0 \bmod m.$$

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

Proposition 1. *Let a and b be integers, $1 \le a, b \le m-1$, such that* $\text{g.c.d.}(a,b,m) = 1$. *Let $v = \text{g.c.d.}(a+b,m)$ 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 $0 \le l \le m-1$, we have

$$d_{a,b,l} = \frac{1}{m}\Big(1 + \sum_{k=1}^{m-1}\zeta_m^{kl}\overline{J}_{ka,kb}\Big) = \frac{1}{u}\varepsilon(l) + \frac{1}{m}\sum_{i=1}^{u-1}\zeta_m^{il}\sum_{k=0}^{v-1}\zeta_m^{ukl}\overline{J}_{(i+uk)a,(i+uk)b}.$$

Proof. Let $d_l = d_{a,b,l}$. For $0 \le l \le m-1$, we have

$$\sum_{k=0}^{m-1}\zeta_m^{-kl}J_{a,b}(\zeta_m^k) = \sum_{k=0}^{m-1}\zeta_m^{-kl}\sum_{j=0}^{m-1}d_j\zeta_m^{kj} = \sum_{j=0}^{m-1}d_j\sum_{k=0}^{m-1}\zeta_m^{(j-l)k} = md_l;$$

so

$$d_l = \frac{1}{m}\sum_{k=0}^{m-1}\zeta_m^{kl}\overline{J_{a,b}(\zeta_m^k)} = \frac{1}{m}\big(1 + \sum_{k=1}^{m-1}\zeta_m^{kl}\overline{J}_{ka,kb}\big),$$

by (11) and (12). Therefore

$$\begin{aligned} d_l &= \frac{1}{m}\Big(1 + \sum_{\substack{1\le k\le m-1\\ u\mid k}}\zeta_m^{kl}\overline{J}_{ka,kb}\Big) + \frac{1}{m}\Big(\sum_{\substack{1\le k\le m-1\\ u\nmid k}}\zeta_m^{kl}\overline{J}_{ka,kb}\Big) \\ &= \frac{1}{m}\big(1 + \sum_{k=1}^{v-1}\zeta_m^{ukl}\big) + \frac{1}{m}\big(\sum_{i=1}^{u-1}\sum_{k=0}^{v-1}\zeta_m^{(i+uk)l}\overline{J}_{(i+uk)a,(i+uk)b}\big) \\ &= \frac{1}{u}\varepsilon(l) + \frac{1}{m}\big(\sum_{i=1}^{u-1}\zeta_m^{il}\sum_{k=0}^{v-1}\zeta_m^{ukl}\overline{J}_{(i+uk)a,(i+uk)b}\big), \end{aligned}$$

by (8), as we wanted to prove. □

We can express the Jacobi sums $J_{a,b}$ in terms of the cyclotomic numbers (i,j), and vice versa, as follows:

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

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

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

$$\begin{aligned}(i,j) &= -\frac{1}{m^2}\sum_{a=0}^{m-1}\sum_{b=0}^{m-1} \zeta_m^{-ia-jb}J_{a,b}\\ &= -\frac{1}{m^2}\Big(m\delta_{0,i} + m\delta_{0,j} + m\delta_{i,j} - q - 1 + \sum_{\substack{1\le a,b\le m-1\\ a+b\ne m}} \zeta_m^{-ia-jb}J_{a,b}\Big)\end{aligned} \tag{15}$$

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

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

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

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* $m \nmid a$, $m \nmid b$ *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*

$$h_{i,j} = -\frac{1}{m^2}\sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\zeta_m^{-ai-bj}\big(J_{a,b} + (q-1)\delta_{0,b}\big)$$
$$= -f\delta_{0,i} - \frac{1}{m^2}\sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\zeta_m^{-ai-bj}J_{a,b}$$

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 $[J_{-a,b} + (q-1)\delta_{0,b}]_{0\le a,b\le m-1}$ (which, by 7, is equal to the characteristic polynomial of $[-mh_{i,j}]_{0\le i,j\le m-1}$) 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),

$$\begin{aligned} J_{a,b}J_{-a,-c} &= \big(G(\zeta_m^a)G(\zeta_m^b)/G(\zeta_m^{a+b})\big)\big(G(\zeta_m^{-a})G(\zeta_m^{-c})/G(\zeta_m^{-a-c})\big)\\ &= \big(G(\zeta_m^{-a-b-c})G(\zeta_m^b)/G(\zeta_m^{-a-c})\big)\big(G(\zeta_m^{a+b+c})G(\zeta_m^{-c})/G(\zeta_m^{a+b})\big)\\ &= J_{-(a+b+c),b}J_{a+b+c,-c}, \end{aligned}$$

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

$$[J_{-a,b} + (q-1)\delta_{0,b}]_{a,b} = P^{-1}[-mh_{i,j}]_{i,j}P = P^{-1}[-mc_{i,j}]_{i,j}P.$$

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

Proposition 3. *For $a, b \in \mathbb{Z}$, let $\mathcal{J}_{a,b}$ 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 $\mathcal{J}_{a,b}$ 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 $\mathcal{J}_{a,b}$, $a, b \in \mathbb{Z}$, 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 $\mathcal{J}_{a,b}$.

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 $c_{i+m,j} = c_{i,j+m} = c_{i,j}$ and

i) $\sum_{k=0}^{m-1} c_{i,k} = f - q\delta_{0,i}$,
ii) $\sum_{k=0}^{m-1} c_{k,j} = -\delta_{0,j}$,
iii) $c_{i,j} = c_{-i,j-i}$,
iv) $\sum_{k=0}^{m-1} c_{i,k}c_{k-j,l-j} = \sum_{k=0}^{m-1} c_{j,k}c_{k-i,l-i}$,
v) the characteristic polynomial of the matrix $[c_{i,j}]_{0\le i,j\le m-1}$ is irreducible over $\mathbb{Q}$.

(See also [12], Proposition 2.)

We are going to prove that the integers

$$h_{i,j} = -f\delta_{0,i} - \frac{1}{m^2}\sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\zeta_m^{-ai-bj}\mathcal{J}_{a,b}$$

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

Define

$$[i,j] = h_{i,j} + f\delta_{0,i} = -\frac{1}{m^2}\sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\zeta_m^{-ai-bj}\mathcal{J}_{a,b}.$$

By condition 2 we have $[i,j] = [j,i]$. By condition 4,

$$\begin{aligned}\sum_{k=0}^{m-1}[i,k] &= -\frac{1}{m^2}\sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\zeta_m^{-ai}\mathcal{J}_{a,b}\sum_{k=0}^{m-1}\zeta_m^{-bk}\\ &= -\frac{1}{m}\sum_{a=0}^{m-1}\zeta_m^{-ai}\mathcal{J}_{a,0}\\ &= -\frac{1}{m}\Big(-(q-2)+\sum_{a=1}^{m-1}\zeta_m^{-ai}\Big) = f - \delta_{0,i}.\end{aligned}$$

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

By condition 3 we have

$$\begin{aligned}[-i,j-i] &= -\frac{1}{m^2}\sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\zeta_m^{ai+b(i-j)}\mathcal{J}_{a,b}\\ &= -\frac{1}{m^2}\sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\zeta_m^{(a+b)i-bj}\mathcal{J}_{a,b}\\ &= -\frac{1}{m^2}\sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\zeta_m^{-ai-bj}\mathcal{J}_{-a-b,b}\\ &= -\frac{1}{m^2}\sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\zeta_m^{-ai-bj}\mathcal{J}_{a,b} = [i,j].\end{aligned}$$

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 $\sum_{k=0}^{m-1} h_{i,k}h_{k-j,l-j} = \sum_{k=0}^{m-1} h_{j,k}h_{k-i,l-i}$. 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 $H(i,j,l) = \sum_{k=0}^{m-1} h_{i,k}h_{k-j,l-j}$. We must prove that $H(i,j,l) \sim 0$.

We have

$$\begin{aligned} H(i,j,l) &= \sum_{k=0}^{m-1} \big([i,k] - f\delta_{0,i}\big)\big([k-j,l-j] - f\delta_{k,j}\big) \\ &= \sum_{k=0}^{m-1} [i,k][k-j,l-j] - f\delta_{0,i} \sum_{k=0}^{m-1} [k-j,l-j] \\ &\qquad\qquad - f\sum_{k=0}^{m-1} [i,k]\delta_{k,j} + f^2\delta_{0,i}\sum_{k=0}^{m-1} \delta_{k,j} \\ &= \sum_{k=0}^{m-1} [i,k][k-j,l-j] - f\delta_{0,i}(f-\delta_{l,j}) - f[i,j] + f^2\delta_{0,i}. \end{aligned}$$

So,

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

Now, using conditions 2 and 3, we get

$$\begin{aligned} \sum_{k=0}^{m-1} [i,k][k-j,l-j] &= \frac{1}{m^4} \sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\sum_{t=0}^{m-1}\sum_{w=0}^{m-1}\sum_{k=0}^{m-1} \zeta_m^{-ia-kb-(k-j)t-(l-j)w} \mathcal{J}_{a,b}\mathcal{J}_{t,w} \\ &= \frac{1}{m^4} \sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\sum_{t=0}^{m-1}\sum_{w=0}^{m-1} \zeta_m^{-ia+jt-(l-j)w} \mathcal{J}_{a,b}\mathcal{J}_{t,w} \sum_{k=0}^{m-1} \zeta_m^{-k(b+t)} \\ &= \frac{1}{m^3} \sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\sum_{w=0}^{m-1} \zeta_m^{-ia-jb-(l-j)w} \mathcal{J}_{a,b}\mathcal{J}_{-b,w} \\ &= \frac{1}{m^3} \sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\sum_{w=0}^{m-1} \zeta_m^{-ia-j(b-w)-lw} \mathcal{J}_{a,b}\mathcal{J}_{-b,w} \\ &= \frac{1}{m^3} \sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\sum_{w=0}^{m-1} \zeta_m^{-ia-jw-l(b-w)} \mathcal{J}_{a,b}\mathcal{J}_{-b,b-w} \\ &= \frac{1}{m^3} \sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\sum_{w=0}^{m-1} \zeta_m^{-ia-jw-l(b-w)} \mathcal{J}_{a,b}\mathcal{J}_{-b,w} \\ &= \frac{1}{m^3} \sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\sum_{w=0}^{m-1} \zeta_m^{-ib+jw-l(a+w)} \mathcal{J}_{a,b}\mathcal{J}_{-a,-w}. \end{aligned}$$

Now define

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

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

$$A(i,j,l) = \sum_{\substack{0\le a,b,w\le m-1\\ m\nmid (a+b),(a+w),a,(a+b+w)}} \zeta_m^{-ib+jw-l(a+w)} \mathcal{J}_{a,b}\mathcal{J}_{-a,-w}$$

and

$$B(i,j,l) = m^2(q-1)\delta_{0,i}\delta_{l,j} + \sum_{\substack{0\le a,b,w\le m-1\\ m\mid (a+b) \text{ or } (a+w) \text{ or } a \text{ or } (a+b+w)}} \zeta_m^{-ib+jw-l(a+w)} \mathcal{J}_{a,b}\mathcal{J}_{-a,-w}.$$

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

$$A(i,j,l) = \sum_{\substack{0\le a,b,w\le m-1\\ m\nmid (a+b),(a+w),a,(a+b+w)}} \zeta_m^{-ib+jw-l(a+w)} \mathcal{J}_{-(a+b+w),b}\mathcal{J}_{a+b+w,-w}.$$

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

$$\begin{aligned}
A(i,j,l) &= \sum_{\substack{0\le a,b,w\le m-1\\ m\nmid (a+b),(a+w),a,(a+b+w)}} \zeta_m^{-ib+jw+l(a+b)} \mathcal{J}_{a,b}\mathcal{J}_{-a,-w}\\
&= \sum_{\substack{0\le a,b,w\le m-1\\ m\nmid (a+b),(a+w),a,(a+b+w)}} \zeta_m^{-jw+ib-l(a+b)} \mathcal{J}_{a,w}\mathcal{J}_{-a,-b}\\
&= \sum_{\substack{0\le a,b,w\le m-1\\ m\nmid (a+b),(a+w),a,(a+b+w)}} \zeta_m^{-jb+iw-l(a+w)} \mathcal{J}_{a,b}\mathcal{J}_{-a,-w}\\
&= A(j,i,l).
\end{aligned}$$

So, $A(i,j,l) \sim 0$.

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

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

where

$$\begin{aligned} C(i,j,l) &= \sum_{b=0}^{m-1}\sum_{w=0}^{m-1} \zeta_m^{-ib+jw-lw} \mathcal{J}_{0,b}\mathcal{J}_{0,-w}, \\ D(i,j,l) &= \sum_{\substack{1\le a\le m-1 \\ 0\le b,w\le m-1 \\ m\mid(a+b) \text{ or } (a+w) \text{ or } (a+b+w)}} \zeta_m^{-ib+jw-l(a+w)} \mathcal{J}_{a,b}\mathcal{J}_{-a,-w}. \end{aligned}$$

By condition 4,

$$\begin{aligned} C(i,j,l) &= \sum_{b=0}^{m-1}\sum_{w=0}^{m-1} \zeta_m^{-ib+(j-l)w}\big(-(q-1)\delta_{0,b}+1\big)\big(-(q-1)\delta_{0,w}+1\big) \\ &= (q-1)^2 - (q-1)\sum_{w=0}^{m-1}\zeta_m^{(j-l)w} - (q-1)\sum_{b=0}^{m-1}\zeta_m^{-ib} + \sum_{b=0}^{m-1}\zeta_m^{-ib}\sum_{w=0}^{m-1}\zeta_m^{(j-l)w} \\ &= (q-1)^2 - m(q-1)\delta_{j,l} - m(q-1)\delta_{0,i} + m^2\delta_{0,i}\delta_{j,l}. \end{aligned}$$

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

$$\begin{aligned} X(i,j,l) &= \sum_{a=1}^{m-1}\sum_{b=0}^{m-1} \zeta_m^{-ib-ja}\mathcal{J}_{a,b}\mathcal{J}_{-a,a}, \\ Y(i,j,l) &= \sum_{\substack{1\le a\le m-1 \\ 0\le b,w\le m-1 \\ w\not\equiv -a \bmod m \\ m\mid(a+b) \text{ or } (a+b+w)}} \zeta_m^{-ib+jw-l(a+w)} \mathcal{J}_{a,b}\mathcal{J}_{-a,-w}. \end{aligned}$$

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

$$\begin{aligned} X(i,j,l) &= \sum_{a=1}^{m-1}\sum_{b=0}^{m-1} \zeta_m^{-ib-ja}\mathcal{J}_{a,b} = -\sum_{b=0}^{m-1}\zeta_m^{-ib}\mathcal{J}_{0,b} - m^2[i,j] \\ &= (q-2) - \sum_{b=1}^{m-1}\zeta_m^{-ib} - m^2[i,j] = (q-1) - m\delta_{0,i} - m^2[i,j]. \end{aligned}$$

So, $X(i,j,l) \sim -m\delta_{0,i}$. Also, by conditions 2, 3 and 5,

$$\begin{aligned}
Y(i,j,l) &= \sum_{a=1}^{m-1} \sum_{\substack{0\le w\le m-1\\ w\not\equiv -a \bmod m}} \zeta_m^{ia+jw-l(a+w)} \mathcal{J}_{a,-a}\mathcal{J}_{-a,-w}\\
&\quad + \sum_{\substack{1\le a\le m-1\\ 0\le b,w\le m-1\\ b\not\equiv -a,\ w\not\equiv -a \bmod m\\ m\mid a+b+w}} \zeta_m^{-ib+jw-l(a+w)} \mathcal{J}_{a,b}\mathcal{J}_{-a,-w}\\
&= \sum_{a=1}^{m-1} \sum_{\substack{0\le w\le m-1\\ w\not\equiv -a \bmod m}} \zeta_m^{ia+jw-l(a+w)} \mathcal{J}_{-a,-w}\\
&\quad + \sum_{a=1}^{m-1} \sum_{\substack{1\le b\le m-1\\ b\not\equiv -a \bmod m}} \zeta_m^{-ib-j(a+b)+lb} \mathcal{J}_{a,b}\mathcal{J}_{-a,a+b}\\
&= \sum_{a=1}^{m-1} \sum_{\substack{0\le w\le m-1\\ w\not\equiv -a \bmod m}} \zeta_m^{-(i-l)a-(j-l)w} \mathcal{J}_{a,w}\\
&\quad + \sum_{a=1}^{m-1} \sum_{\substack{1\le b\le m-1\\ b\not\equiv -a \bmod m}} \zeta_m^{-ib-j(a+b)+lb} \mathcal{J}_{a,b}\mathcal{J}_{-a,-b}\\
&= -m^2[i-l,j-l] - \sum_{w=1}^{m-1} \zeta_m^{-(j-l)w}\mathcal{J}_{0,w} - \sum_{a=0}^{m-1} \zeta_m^{-(i-j)a}\mathcal{J}_{a,-a}\\
&\quad + q\sum_{a=1}^{m-1} \zeta_m^{-ja} \sum_{b=1}^{m-1} \zeta_m^{(l-i-j)b} - q\sum_{a=1}^{m-1} \zeta_m^{-ja-(l-i-j)a}\\
&= -m^2[i-l,j-l] - m\delta_{j,l} + 1 + 1 + (1-2) - (q-2) - m\delta_{i,j} + 1\\
&\quad + q(m\delta_{0,j}-1)(m\delta_{l,i+j}-1) - q(m\delta_{l,i}-1).
\end{aligned}$$

So, $Y(i,j,l) \sim -qm\delta_{0,j} - qm\delta_{l,i} - m\delta_{j,l} + qm^2\delta_{0,j}\delta_{l,i+j}$. Therefore,

$$\begin{aligned}
B(i,j,l) &= m^2(q-1)\delta_{0,i}\delta_{l,j} + C(i,j,l) + X(i,j,l) + Y(i,j,l)\\
&\sim m^2(q-1)\delta_{0,i}\delta_{l,j} - m(q-1)\delta_{j,l} - m(q-1)\delta_{0,i}\\
&\quad + m^2\delta_{0,i}\delta_{j,l} - m\delta_{0,i} - qm\delta_{0,j} - qm\delta_{l,i} - m\delta_{j,l} + qm^2\delta_{0,j}\delta_{l,i+j}\\
&= m^2q\delta_{0,i}\delta_{l,j} + m^2q\delta_{0,j}\delta_{l,i} - mq\delta_{l,i} - mq\delta_{l,j} - mq\delta_{0,i} - mq\delta_{0,j}.
\end{aligned}$$

Therefore $B(i,j,l) \sim 0$. This ends the proof of (iv), and of Proposition 3. $\square$

Let Q be the prime ideal of $\mathbb{Z}[\zeta_m]$ above q such that $s^f \equiv \zeta_m \bmod Q$. If $k \in \mathbb{Z}$ we denote by $|k|_m$ the least nonnegative integer such that $|k|_m \equiv k \bmod m$. We showed in [12], formula (27), that, for $0 \le a, b \le m-1$ with $a+b \not\equiv 0 \mod m$,

$$\overline{J}_{a,b} \equiv \binom{f|a+b|_m}{fa} \mod Q. \tag{17}$$

This fact is a simple consequence of (7), and [4], 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, $1 \le a, b \le m-1$, such that* g.c.d.$(a,b,m)=1$, *and let $0 \le l \le m-1$. Let u, v and $\varepsilon(l)$ be as in Proposition 1. Then*

$$d_{a,b,l} \equiv \frac{1}{u}\varepsilon(l) + \frac{1}{m}\sum_{i=1}^{u-1}\sum_{k=0}^{v-1} s^{f(i+uk)l}\binom{f|i(a+b)|_m}{f|(i+uk)a|_m} \qquad \bmod q,$$

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 $\equiv 1 \bmod 2m$, s a primitive root modulo q (the command: s :=primroot(q); will give to s the value of the smallest positive primitive root modulo q), a and b integers, $1 \le a, b \le m-1$, such that $m \nmid a+b$, and such that g.c.d.$(a,b,m)=1$ (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 ζ_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 ζ_m. The last two lines are to check that $J_{a,b}(1) = 1$ and that $J_{a,b}\overline{J}_{a,b} = q$.

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:=primroot(q); a:=2; b:=5;
f:=(q-1)/m: v:=igcd(a+b,m): u:=m/v:
for i from 0 to m-1 do;
ep(i):=floor(1-i/v+floor(i/v)); od:
C:=array(1..u,1..v):
for j1 from 1 to u do; for k1 from 1 to v do;
C[j1,k1]:=modp(binomial(f*modp((j1-1)*(a+b),m), f*modp(((j1-1)+u*(k1-1))*a,m)),q);
od: od:
A:=array(1..1,1..m):
for l from 1 to m do;
A[1,l]:=mods(ep(l-1)/u+(1/m)*sum(sum(s^ ((f*(j-1)+f* u*(k-1))*(l-1))*C[j,k],j=2..u),
k=1..v),q); od:
A:=evalm(A);
R:=cyclotomic(m,x);
F:=x->sum(A[1,t]*x^ (t-1),t=1..m):
F(x):=F(x); G:=rem(F(x),R,x);
# check:
F(1);
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 ζ_m an m-th primitive root of 1. Let S be the set of all prime numbers $q \equiv 1 \bmod 2m$. 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 $s^{(q-1)/m} \equiv \zeta_m \bmod Q$, 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 ν 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 $r_i^{f_i} \equiv 1 \bmod m$, 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 $s_i^{(r_i^{f_i}-1)/m} \equiv \zeta_m \bmod R_i$. For $1 \leq i \leq \nu$ and $0 \leq a, b \leq m-1$, let $\mathfrak{J}_{i,a,b}$ be the Jacobi sum

$$\mathfrak{J}_{i,a,b} = -\sum_{\substack{\gamma \in \mathbb{Z}[\zeta_m]/R_i \\ \gamma \neq 0,1}} \zeta_m^{a\,\mathrm{ind}_{s_i}(\gamma) + b\,\mathrm{ind}_{s_i}(1-\gamma)}, \tag{18}$$

where $\mathrm{ind}_{s_i}(\gamma)$ is the least nonnegative integer such that $s_i^{\mathrm{ind}_{s_i}(\gamma)} \equiv \gamma \bmod R_i$. 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 σ_c the automorphism of $\mathbb{Q}(\zeta_m)$ such that $\sigma_c(\zeta_m) = \zeta_m^c$. If $a + b \not\equiv 0 \bmod m$, the prime ideal factorization of the ideal $(\mathfrak{J}_{i,a,b})$ of $\mathbb{Z}[\zeta_m]$ is given by

$$(\mathfrak{J}_{i,a,b}) = \prod_{\substack{1 \leq c \leq m-1 \\ \text{g.c.d.}(c,m)=1}} \sigma_c^{-1}(\overline{R}_i)^{\left[\frac{(a+b)c}{m}\right] - \left[\frac{ac}{m}\right] - \left[\frac{bc}{m}\right]}, \tag{19}$$

where the bar denotes complex conjugation, and $[\rho]$ denotes the integral part of a real number ρ (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

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

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

$$\mathfrak{K}_{a,b}[\alpha] = \prod_{\substack{1 \leq c \leq m-1 \\ \text{g.c.d.}(c,m)=1}} \sigma_c^{-1}(\overline{\alpha})^{\left[\frac{(a+b)c}{m}\right] - \left[\frac{ac}{m}\right] - \left[\frac{bc}{m}\right]}. \tag{20}$$

Then, for $\alpha \in \mathcal{A}$, we have $(\mathfrak{K}_{a,b}[\alpha]/\mathfrak{J}_{a,b}) = (J_{a,b}[Q])$ (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 $(\alpha)(R_1 \dots R_\nu)^{-1}$. 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 $\alpha_0, \alpha_1 \in \mathbb{Z}[\zeta_m]$

such that $(\alpha_0, \alpha_1) = R_1 \dots R_\nu$ and define $\mathcal{A} = \mathcal{A}_1$, where

$$\mathcal{A}_1 = \left\{ \alpha = \alpha_0 + \alpha_1 \beta : \beta = \sum_{i=0}^{\varphi(m)-1} b_i \zeta_m^i \in \mathbb{Z}[\zeta_m] \right. \\ \left. \text{and } N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha) = r'q, \text{ with } q \in S \right\}.$$

The parameters of the family we construct will then be the coefficients b_i of β. In the examples we work with the simpler sets

$$\mathcal{A}_2 = \{\alpha = \alpha_0 + \alpha_1 n : n \in \mathbb{Z} \text{ and } N_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\alpha) = r'q, \text{ with } q \in S\}.$$

The second step is to identify the Jacobi sums $J_{a,b}[Q]$, $Q \in \mathcal{I}$, among the generators of the principal ideals $(J_{a,b}[Q])$. One way to do that is to start with a subset $\mathcal{A}$ of $\mathcal{C}$ such that if $\alpha \in \mathcal{A}$ the numbers $\mathfrak{K}_{a,b}[\alpha]$ are products of Jacobi sums (as the ones defined in (18)). Then we know after Weil [14] that, using the notation above, for $\alpha \in \mathcal{A}$ and $Q = (\alpha)(R_1 \dots R_\nu)^{-1}$, $J_{a,b}[Q] = \mathfrak{K}_{a,b}[\alpha]/\mathfrak{J}_{a,b}$. Also, by [14], we know that there is a divisor $\mathfrak{f}$ of m^2 such that any nonempty subset $\mathcal{A}$ of the set $\mathcal{C}_\mathfrak{f} = \{\alpha \in \mathcal{C} : \alpha \equiv 1 \bmod \mathfrak{f}\}$ 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 $\delta\zeta_m^k \mathfrak{K}_{a,b}[\alpha]/\mathfrak{J}_{a,b}$, $\delta \in \{1, -1\}$, $0 \le k \le m-1$, satisfies congruence (13), and that number is $J_{a,b}[Q]$.

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

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

$$q = 49n^6 - 49n^5 + 49n^4 + 35n^3 + 21n^2 + 7n + 1,$$

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

$$\begin{aligned} P_q(x) = {} & x^7 + x^6 + (-21n^6 + 21n^5 - 21n^4 - 15n^3 - 9n^2 - 3n)x^5 \\ & + (-21n^9 + 28n^8 + 7n^7 - 48n^6 + 36n^5 + 20n^4 + 12n^3 + 3n^2)x^4 \\ & + (91n^{12} - 147n^{11} + 252n^{10} - 85n^9 + 73n^8 \\ & \qquad + 100n^7 + 21n^6 + 10n^5 - 2n^4 - n^3)x^3 \\ & + (112n^{15} - 203n^{14} + 175n^{13} + 113n^{12} - 227n^{11} \\ & \qquad + 127n^{10} - 23n^9 - 45n^8 - 25n^7 - 14n^6 - 2n^5)x^2 \\ & + (-84n^{18} + 238n^{17} - 518n^{16} + 629n^{15} - 442n^{14} \\ & \qquad + 196n^{12} - 8n^{11} - 22n^{10} - 26n^9 - 11n^8 - n^7)x \\ & - 97n^{21} + 357n^{20} - 609n^{19} + 434n^{18} + 52n^{17} - 282n^{16} + 94n^{15} \\ & + 56n^{14} + 7n^{13} - 3n^{12} - 8n^{11} - 2n^{10}. \end{aligned}$$

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 $J_{a,b}[Q] \equiv 1 \bmod (\zeta_m - 1)^2$. 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)ˆ2;

In general the "smallest" examples I found for m prime start with the elements $\alpha = 1 + n(\zeta_m - \zeta_m^{-1})^3$ 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 α 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

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

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-zˆ(m-1))ˆ3; 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

$$\begin{aligned}P_q(x) = x^9 &+ x^8 + (-972n^6 - 324n^4 - 24n^2)x^7\\ &+ (-3888n^8 - 1548n^6 - 180n^4 - 8n^2)x^6\\ &+ (196830n^{12} + 148716n^{10} + 34830n^8 + 2856n^6 + 80n^4)x^5\\ &+ (629856n^{14} + 535086n^{12} + 148716n^{10} + 16830n^8 + 840n^6 + 16n^4)x^4\\ &+ (-14880348n^{18} - 10786284n^{16} - 2259900n^{14}\\ &\qquad - 106164n^{12} + 7128n^{10} + 480n^8)x^3\\ &+ (-25509168n^{20} - 18659484n^{18} - 6167340n^{16}\\ &\qquad - 1097388n^{14} - 95652n^{12} - 3480n^{10} - 32n^8)x^2\\ &+ (387420489n^{24} + 70150212n^{22} - 29878794n^{20}\\ &\qquad - 7934436n^{18} - 489159n^{16} + 3672n^{14} + 720n^{12})x\\ &- 29229255n^{24} - 1653372n^{22} + 2523798n^{20}\\ &+ 384156n^{18} + 22761n^{16} + 792n^{14} + 16n^{12}.\end{aligned}$$

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*n*(z-z^(m-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

$$\begin{aligned}P_q(x) = x^{12} &+ x^{11} + (-594n^4 - 33n^2)x^{10} + (216n^6 - 153n^4 - 9n^2)x^9\\ &+ (120771n^8 + 8937n^6 + 186n^4)x^8\\ &+ (-116640n^{10} + 8586n^8 + 1044n^6 + 24n^4)x^7\\ &+ (-9713196n^{12} - 858762n^{10} - 26784n^8 - 304n^6)x^6\\ &+ (19840464n^{14} + 581742n^{12} - 28998n^{10} - 1368n^8 - 16n^6)x^5\\ &+ (278337303n^{16} + 30561138n^{14} + 1165428n^{12} + 18144n^{10} + 96n^8)x^4\\ &+ (-1055008800n^{18} - 84367899n^{16}\\ &\qquad - 1851660n^{14} + 1512n^{12} + 288n^{10})x^3\\ &+ (-806018850n^{20} - 210194757n^{18}\\ &\qquad - 14311728n^{16} - 377136n^{14} - 3456n^{12})x^2\\ &+ (7971615000n^{22} + 1069672635n^{20}\\ &\qquad + 52743879n^{18} + 1137240n^{16} + 9072n^{14})x\\ &- 8968066875n^{24} - 1102740075n^{22}\\ &\qquad - 50585310n^{20} - 1026432n^{18} - 7776n^{16}.\end{aligned}$$

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*n*(z-z^(m-1)); in the program at the end of the article. Observe that the resulting matrix C has entries in $\mathbb{Z}[n]$.

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 $(2) = R_1\overline{R_1}$. The element $s_1 = 1 + w^3$ is a generator of $\mathbb{Z}[w]/R_1 \cong \mathbb{F}_8$ (the field with 8 elements), such that $s_1 = s_1^{(8-1)/7} \equiv w \bmod R_1$. Let

$$\mathcal{A}_3 = \{\alpha = w^5 - 2w^4 + 3w^3 - w^2 + 2 + 2(w-1)^2 n \\ n \in \mathbb{Z} \text{ and } N_{\mathbb{Q}(w)/\mathbb{Q}}(\alpha) = 8q, \text{ with } q \in S\},$$

and

$$\mathcal{I} = \{Q = (\alpha)R_1^{-1} : \alpha \in \mathcal{A}_3\}.$$

Observation. Since $\mathbb{Z}[w]$ is a principal ideal domain, we could simplify our example by dividing the elements of $\mathcal{A}_3$ by a generator of R_1. That, however, would not illustrate how the method works in the general situation. The first cases in which we really need to work with auxiliary Jacobi sums $\mathfrak{J}_{i,a,b}$ 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 $\alpha = w^5 - 2w^4 + 3w^3 - w^2 + 2 + 2(w-1)^2 n \in \mathcal{A}_3$, then

$$N_{\mathbb{Q}(w)/\mathbb{Q}}(\alpha) = 8(392n^6 + 98n^4 + 161n^3 + 14n^2 - 35n + 113).$$

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

$$\mathfrak{J}_{1,1} = \mathfrak{J}_{1,5} = -2(w + w^2 + w^4),$$
$$\mathfrak{J}_{1,2} = \mathfrak{J}_{1,4} = -(3 + w^3 + w^5 + w^6),$$
$$\mathfrak{J}_{1,3} = \overline{\mathfrak{J}}_{1,1} = -2(w^3 + w^5 + w^6).$$

For $Q \in \mathcal{I}$ and $\alpha \in \mathcal{A}_3$ such that $(\alpha) = R_1 Q$, define $\mathfrak{K}_{a,b}[\alpha]$ as in (20). We have

$$\begin{aligned}\mathfrak{K}_{1,1}[\alpha] = {} & (24n^2 - 12n - 6)w^5 + (-36n^2 - 18n - 6)w^4 \\ & + (-56n^3 - 12n^2 + 32n - 4)w^3 + (12n^2 + 6n - 24)w^2 \\ & + (-48n^2 - 18n + 12)w - 24n^2 + 24n + 6,\end{aligned}$$

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

$$\begin{aligned}\mathfrak{K}_{1,3}[\alpha] = {} & (-48n^2 - 24n + 18)w^5 + (-12n^2 - 6n + 24)w^4 \\ & + (-60n^2 - 24n + 36)w^3 + (-56n^3 - 24n^2 + 26n + 20)w^2 \\ & + (12n^2 - 18n + 18)w - 36n^2 + 18n + 30,\end{aligned}$$

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

$$\begin{aligned}\mathfrak{K}_{1,5}[\alpha] = {} & (24n^2 - 12n - 6)w^5 + (-36n^2 - 18n - 6)w^4 \\ & + (-56n^3 - 12n^2 + 32n - 4)w^3 + (12n^2 + 6n - 24)w^2 \\ & + (-48n^2 - 18n + 12)w - 24n^2 + 24n + 6.\end{aligned}$$

Using the formula $(J_{a,b}[Q]) = (\mathfrak{K}_{a,b}[\alpha]/\mathfrak{J}_{a,b})$, and the fact that $J_{a,b}[Q] \equiv 1 \bmod (w-1)^2$, we get

$$\begin{aligned} J_{1,1}[Q] &= -w^3\mathfrak{K}_{1,1}[\alpha]/\mathfrak{J}_{1,1} \\ &= (-14n^3 - 3n^2 + 5n - 1)w^5 + (-14n^3 + 15n^2 + 8n - 7)w^4 \\ &\quad + (-9n^2 - 6n - 3)w^3 + (-14n^3 - 12n^2 + 11n + 5)w^2 \\ &\quad + (6n^2 + 9n - 3)w + 3n^2 - 6n + 3, \end{aligned}$$

$$\begin{aligned} J_{1,2}[Q] &= -w^3\mathfrak{K}_{1,2}[\alpha]/\mathfrak{J}_{1,2} \\ &= (-7n^3 + n - 8)w^4 + (-7n^3 + n - 8)w^2 \\ &\quad + (-7n^3 + n - 8)w - 21n^3 - 3n - 3, \end{aligned}$$

$$\begin{aligned} J_{1,3}[Q] &= -w^2\mathfrak{K}_{1,3}[\alpha]/\mathfrak{J}_{1,3} \\ &= (27n^2 - 3n - 12)w^5 + (14n^3 + 12n^2 - 11n - 5)w^4 \\ &\quad + (14n^3 + 18n^2 - 2n - 8)w^3 + (14n^3 + 3n^2 - 17n - 8)w^2 \\ &\quad + (9n^2 - 6n - 6)w + 14n^3 + 15n^2 - 17n - 2, \end{aligned}$$

$$\begin{aligned} J_{1,4}[Q] &= -w^3\mathfrak{K}_{1,4}[\alpha]/\mathfrak{J}_{1,4} \\ &= (-7n^3 + n - 8)w^4 + (-7n^3 + n - 8)w^2 \\ &\quad + (-7n^3 + n - 8)w - 21n^3 - 3n - 3, \end{aligned}$$

$$\begin{aligned} J_{1,5}[Q] &= -w^3\mathfrak{K}_{1,5}[\alpha]/\mathfrak{J}_{1,5} \\ &= (-14n^3 - 3n^2 + 5n - 1)w^5 + (-14n^3 + 15n^2 + 8n - 7)w^4 \\ &\quad + (-9n^2 - 6n - 3)w^3 + (-14n^3 - 12n^2 + 11n + 5)w^2 \\ &\quad - 6n + (6n^2 + 9n - 3)w + 3n^2 + 3. \end{aligned}$$

For $1 \le i \le 5$ 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 $[d_{u,k}]_{\substack{1\le u\le 5\\ 0\le k\le 6}}$. 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:

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

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

$$\begin{aligned}
P_q(x) = \det(xI - C) = x^7 + x^6 &+ (-168n^6 - 42n^4 - 69n^3 - 6n^2 + 15n - 48)x^5 \\
&+ (-224n^9 + 168n^8 - 672n^7 + 78n^6 - 93n^5 \\
&\qquad - 195n^4 - 49n^3 + 108n^2 - 189n + 37)x^4 \\
&+ (6608n^{12} + 2856n^{11} + 28n^{10} + 6140n^9 \\
&\qquad + 1251n^8 + 1395n^7 + 3850n^6 + 1635n^5 \\
&\qquad + 338n^4 + 1271n^3 - 57n^2 + 443n + 312)x^3 \\
&+ (14784n^{15} + 12768n^{14} + 23856n^{13} + 8184n^{12} \\
&\qquad + 8100n^{11} + 26226n^{10} + 4935n^9 + 4377n^8 \\
&\qquad + 16176n^7 + 1200n^6 - 2373n^5 \\
&\qquad + 6063n^4 + 792n^3 - 501n^2 + 573n - 12)x^2 \\
&+ (-36736n^{18} + 41664n^{17} + 64176n^{16} - 122352n^{15} \\
&\qquad - 30492n^{14} + 16518n^{13} - 146848n^{12} \\
&\qquad - 50097n^{11} + 22722n^{10} - 82665n^9 - 46842n^8 \\
&\qquad + 3279n^7 - 29398n^6 - 16158n^5 + 1698n^4 \\
&\qquad - 4317n^3 - 4050n^2 - 894n - 49)x \\
&- 33664n^{21} + 146496n^{20} + 24640n^{19} - 276528n^{18} \\
&- 158904n^{17} - 275688n^{16} - 447508n^{15} - 216771n^{14} \\
&- 185387n^{13} - 290411n^{12} - 179430n^{11} - 127792n^{10} \\
&- 130448n^9 - 65166n^8 - 28901n^7 - 26116n^6 \\
&- 18399n^5 - 9110n^4 - 2993n^3 - 519n^2 - 39n - 1.
\end{aligned}$$

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

$$\mathcal{A}_4 = \{\alpha = 1 + \zeta_{23}^2 - \zeta_{23}^3 + 47n : n \in \mathbb{Z} \text{ and } N_{\mathbb{Q}(\zeta_{23})/\mathbb{Q}}(\alpha) = 47q, \text{ with } q \in S\},$$

and

$$\mathcal{I} = \{Q = (\alpha)R_1^{-1} : \alpha \in \mathcal{A}_4\}.$$

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 $s_1^{(47-1)/23} = (-2)^2 \equiv \zeta_{23} \bmod R_1$. Using the MAPLE program at the end of Section 1, with $m = 23$, $q = 47$ and $s = -2$, we find that

$$\begin{aligned}
\mathfrak{J}_{1,1} = 2 - 2\zeta_{23}^2 + 2\zeta_{23}^8 - 2\zeta_{23}^9 + 2\zeta_{23}^{12} + 2\zeta_{23}^{13} \\
+ 2\zeta_{23}^{14} - 2\zeta_{23}^{15} + 2\zeta_{23}^{16} - 2\zeta_{23}^{18} - 2\zeta_{23}^{20} - \zeta_{23}^{21}.
\end{aligned}$$

For $\alpha \in \mathcal{A}_4$, let

$$\mathfrak{K}_{1,1}[\alpha] = \prod_{c=1}^{22} \sigma_c^{-1}(\overline{\alpha})^{\left[\frac{2c}{23}\right]}.$$

We can obtain the family of Jacobi sums $J_{1,1}[Q]$, $Q \in \mathcal{I}$, using the formula

$$J_{1,1}[Q] = \left(\frac{n+1}{23}\right)\zeta_{23}^{-k}\mathfrak{K}_{1,1}[\alpha]/\mathfrak{J}_{1,1} = \left(\frac{n+1}{23}\right)\zeta_{23}^{-k}\mathfrak{K}_{1,1}[\alpha]\overline{\mathfrak{J}}_{1,1}/47,$$

where $(\alpha) = R_1 Q$, $\alpha \in \mathcal{A}_4$, $\left(\frac{\ }{23}\right)$ is the Legendre symbol, and

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

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 $\equiv 1 \bmod (\zeta_{23}-1)^2$. 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 $J_{1,1}[Q], \dots, J_{1,21}[Q]$, $Q \in \mathcal{I}$. 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

$$\begin{aligned} q = q(n) = {} & 13003342946222978304418515653309284 7n^{22} \\ & + 6086671166317138780791645624953282 2n^{21} \\ & + 1359788239283616110602388916212967 3n^{20} \\ & + 192877764437392356113814030668506 0n^{19} \\ & + 19492965554842844500864183950540 5n^{18} \\ & + 1493078212711366812832150260041 4n^{17} \\ & + 900082610499760135395267887259n^{16} \\ & + 43773014492389550657520626736n^{15} \\ & + 1746389479019419656026933311n^{14} \\ & + 57795967528053201788638220n^{13} + 1594119954503408569331187n^{12} \\ & + 36397389727152969816873n^{11} + 666486961951621859180n^{10} \\ & + 8874252237258368851n^{9} + 54335329669656750n^{8} \\ & - 992442355341030n^{7} - 37699732250660n^{6} - 646801716550n^{5} \\ & - 6475959625n^{4} - 5641786n^{3} + 1224820n^{2} + 22033n + 139. \end{aligned}$$

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 $n_1, \dots, n_k$, which, when z is replaced by ζ_m and the n_i by integers, gives elements of $\mathbb{Z}[\zeta_m]$ that are either $\equiv 1 \bmod m^2$, or $\equiv 1$ modulo a smaller divisor of m^2, provided that the resulting matrix C still has its entries in $\mathbb{Z}[n_1, \dots, n_k]$ (these entries are always in $\mathbb{Q}[n_1, \dots, n_k]$). 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 $\mathfrak{f}$ in the discussion above. The resulting value of q must be irreducible in $\mathbb{Z}[n_1, \dots, n_k]$. (With the help of a computer it is easy to check that in fact the matrix $C = [c_{i,j}]$ satisfies the conditions of [12], 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 $m > 2$

```
with(numtheory): with(linalg):
m:=10; F:=z−>1+n∗10∗(z-zˆ (m-1));
R:=cyclotomic(m,z);
for i0 from 0 to m-1 do;
T[i0]:=modp(i0ˆ (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(zˆ c)ˆ 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]:=(floor((i2+j2)∗(k2-1)/m)-floor(i2∗(k2-1)/m)- floor(j2∗(k2-1)/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(zˆ (m-T[k3-1]))ˆ A[i3,j3,k3], k3=1..m),z); od: od:
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);
Id:=array(identity,1..m,1..m):
C:=array(1..m,1..m):
for i5 from 1 to m do;
for j5 from 1 to m do;
C[i5,j5]:=rem(-f∗Id[1,i5]+(-1/mˆ 2)∗(m∗Id[1,i5]+m∗Id[1,j5]+m∗Id[i5,j5]-q-1+
sum(sum(zˆ ((m-i5+1)∗a+(m-j5+1)∗b)∗H[a,b],a=1..m-1), b=1..m-1)-
sum(zˆ ((m-i5+j5)∗l)∗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 York-Toronto, 1998. MR **99d:**11092
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*, Graduate Texts in Mathematics, Springer-Verlag, New York-Berlin-Heidelberg, 1977. MR **83b:**12001
4. 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

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:**11067a
7. R. Schoof and L. Washington, *Quintic polynomials and real cyclotomic fields with large class numbers*, Math. Comp. **50** (1988), 543–556. MR **89h:**11067b
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*, Trans. Amer. Math. Soc. **351** (1999), 4769–4790. MR **2000c:**11181
12. F. Thaine, *Families of irreducible polynomials of Gaussian periods and matrices of cyclotomic numbers*, Math. Comp. **69** (2000), 1653–1666. MR **2001a:**11179
13. L. C. Washington, *Introduction to Cyclotomic Fields, Second Edition*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1996. MR **97h:**11130
14. A. Weil, *Jacobi sums as "Grössencharaktere"*, Trans. Amer. Math. Soc. **73** (1952), 487–495. MR **14d:**452d

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`