On the Construction of Families of Cyclic Polynomials Whose Roots Are Units

F. Thaine

CONTENTS

For several values of m, we show ways to construct some families of cyclic monic polynomials of degree m with integer coefficients and constant terms ± 1, and to express their roots in terms of Gaussian periods. We give several examples illustrating those techniques. With the aim to find other methods to construct such families of polynomials, we consider the question whether one of them can be obtained by means of rational transformations of a given ordinary family $F(t, X) \in \mathbb{Z}[t][X]$ (at the parameter t) of cyclic monic polynomials of degree m (such families F are easy to find). We show a method, due to René Schoof, that allows us to answer at least the simpler question whether a family $G(t, X) \in \mathbb{Q}[t][X]$ of cyclic monic polynomials of degree m prime with constant term in $\mathbb{Q}^\times$ (independent of t) can be obtained from F by means of rational transformations.

1. INTRODUCTION

Let $m > 2$ be an integer, ζ_m an mth primitive root of 1, $\nu = \varphi(m)$, where φ is Euler's function, $t_0, t_1, \ldots, t_{\nu-1}$ parameters that are supposed to take integer values, $\alpha = t_0 + t_1\zeta_m + \cdots + t_{\nu-1}\zeta_m^{\nu-1}$, N the norm from $\mathbb{Q}[\zeta_m]$ to $\mathbb{Q}$, and $q = q(t_0, \ldots, t_{\nu-1}) = N(\alpha)$. We assume that the numbers t_i are such that q is a prime that does not divide m. (In our examples all the t_i will depend on a single parameter t.) We have that $q \equiv 1 \bmod m$. Let $f = (q-1)/m$, ζ_q a qth primitive root of 1, s a primitive root mod q, and $\eta_i = \sum_{j=0}^{f-1} \zeta_q^{s^{i+mj}}$, $i = 0, \ldots, m-1$, the Gaussian periods of degree m in $\mathbb{Q}[\zeta_q]$. They are real numbers if f is even and complex nonreal if f is odd. To simplify matters we assume that f is even. Let $\mathbb{L} = \mathbb{Q}[\eta_0] = \mathbb{Q}[\eta_0, \ldots, \eta_{m-1}]$, the cyclic subfield of degree m of $\mathbb{Q}[\zeta_q]$, and $D = D_q$ its ring of algebraic integers. We have that $\{\eta_0, \eta_1, \ldots, \eta_{m-1}\}$ is a normal integral basis for $\mathbb{L}$; in particular, $D = \mathbb{Z}[\eta_0, \ldots, \eta_{m-1}]$. Denote by τ the generator of $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ such that $\tau(\eta_i) = \eta_{i+1}$ (indices modulo m).

In this article we show some ways to construct, for several values of m, families of elements that are (nontrivial)

2000 AMS Subject Classification: Primary 11R09, 11R18, 11T22; Secondary 11R20, 12F10

Keywords: Cyclic polynomials, units, Gaussian periods

© A K Peters, Ltd.
1058-6458/2008 $0.50 per page

units of D_q for distinct primes $q = q(t_0, \ldots, t_{\nu-1})$ corresponding to special values of the parameters t_i. More generally, our techniques allow us to construct families of cyclic polynomials (that is, irreducible polynomials with cyclic Galois groups over $\mathbb{Q}$), monic of degree m, with coefficients in $\mathbb{Z}$ and constant terms ± 1, and to express their roots in terms of Gaussian periods.

We are mainly interested in families of polynomials, as above, such that their splitting fields have prime conductors of the form $q(t_0, \ldots, t_{\nu-1})$. Those families are, in general, difficult to find for arbitrary m.

Here are a few of the known examples:

- For $m = 3$,

$$F = x^3 - tx^2 - (t+3)x - 1,$$

with $q = t^2 + 3t + 9$, studied by D. Shanks (1974).

- For $m = 5$,

$$\begin{aligned} F = x^5 &+ t^2x^4 - (2t^3 + 6t^2 + 10t + 10)x^3 \\ &+ (t^4 + 5t^3 + 11t^2 + 15t + 5)x^2 \\ &+ (t^3 + 4t^2 + 10t + 10)x + 1, \end{aligned}$$

with $q = t^4 + 5t^3 + 15t^2 + 25t + 25$, due to Emma Lehmer [Lehmer 88].

This family was used in [Schoof and Washington 88] to construct a real p-cyclotomic field with class number divisible by a large prime. The authors showed that when for some integer t the number q is prime, then any set of four of the roots of F is a fundamental system of units of the ring of integers of the splitting field of F.

- For $m = 4$,

$$F = x^4 + tx^3 - 6x^2 - tx + 1,$$

with $q = t^2 + 16$, M-N. Gras (1977).

- For $m = 6$,

$$\begin{aligned} F = x^6 &+ 2tx^5 - (5t + 15)x^4 + 20x^3 + 5tx^2 \\ &- (2t + 6)x + 1, \end{aligned}$$

with $q = t^2 + 3t + 9$, M.-N. Gras (1987).

- For $m = 8$, families were found by Emma Lehmer [Lehmer 88] and by Y. Y. Shen (1988).

More examples and references can be found in [Washington 90].

- For $m = 7$ no such families are known, but Hashimoto and Hoshi [Hashimoto and Hoshi 05], using their geometric method to construct families of cyclic polynomials, have found a family

$$\begin{aligned} F = x^7 &- (t^3 + t^2 + 5t + 6)x^6 \\ &+ (9t^3 + 9t^2 + 24t + 12)x^5 \\ &+ (t^7 + t^6 + 9t^5 - 5t^4 - 15t^3 - 22t^2 - 36t - 8)x^4 \\ &- (t^8 + 5t^7 + 12t^6 + 24t^5 - 6t^4 + 2t^3 - 20t^2 - 16t)x^3 \\ &+ (2t^8 + 7t^7 + 19t^6 + 14t^5 + 2t^4 + 8t^3 - 8t^2)x^2 \\ &- (t^8 + 4t^7 + 8t^6 + 4t^4)x + t^7, \end{aligned}$$

with constant term t^7.

We will study these and other new examples in Section 4.

This work originated in a question posed to me by René Schoof regarding the possibility of generalizing the above family of cyclic quintic polynomials discovered by Emma Lehmer.

In Section 2, we recall some basic facts about the multiplication matrices C of Gaussian periods and the arithmetic of D, and show some polynomials $a_{i,j}$ of degree $\nu/2$ in the parameters t_i, with which we can construct q and C.

In Section 3, we show several ways to use those polynomials $a_{i,j}$ in the search for families of units of cyclic fields.

In Section 4, we apply the techniques of Section 3 to construct several families of cyclic polynomials of degrees 3, 4, 5, 6, 8, and 9 whose roots are algebraic units, and also other families, of degree 7, similar to Hashimoto and Hoshi's family of polynomials mentioned above, which have "small" constant terms.

In Section 5, we show a way to construct a family of cyclic polynomials of degree mn whose roots are algebraic units when m and n are relatively prime positive integers and we are given the multiplication matrices of the roots of two such families with degrees m and n. As examples, we calculate families of polynomials of degrees 10 and 12.

Since we have good methods to construct cyclic monic polynomials $F(t, X) \in \mathbb{Z}[t][X]$ of arbitrary degree $m > 2$ over $\mathbb{Q}(t)$, it would be interesting to have a way to know whether, by applying rational transformations on such a polynomial F, we can find a cyclic monic polynomial $G(t, X) \in \mathbb{Z}[t][X]$, of degree m, whose constant term is ± 1 (that is, a polynomial of the kind we consider in Sections 3 and 4).

Suppose that m is prime. In Section 6 we present a method, shown to us by René Schoof, that allows

us to know at least whether a cyclic monic polynomial $G(t,X) \in \mathbb{Q}[t][X]$ of degree m over $\mathbb{Q}(t)$ with constant term in $\mathbb{Q}^\times$ can be obtained by applying rational transformations on a given F. Some examples illustrating Schoof's method are given at the end of the section.

2. PRELIMINARIES

Let $c_{i,j}$, $0 \le i,j \le m-1$, be the integers such that

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

and let $C = [c_{i,j}]_{0\le i,j<m}$. We call C the multiplication matrix of the η_i. We use the following version of Kronecker's delta: for $i,j \in \mathbb{Z}$,

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

Let K be the $m \times m$ matrix $[\delta_{i+1,j}]_{i,j}$, that is,

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

We have that $K^m = I$, the identity matrix. The matrix C contains key information on the arithmetic of D.

Let $P(x) = (x-\eta_0)(x-\eta_1)\cdots(x-\eta_{m-1}) \in \mathbb{Z}[x]$, the minimal polynomial of the Gaussian periods η_i. Recall that $\eta_0+\eta_1+\cdots+\eta_{m-1} = -1$. We have that $P(x)$ is the characteristic polynomial of C. Also, for $l = 0,\dots,m-1$,

$$C(K^{-l}CK^l) = (K^{-l}CK^l)C, \tag{2–2}$$

and the field $\mathbb{Q}[C]$ is a decomposition field for $P(x)$. In $\mathbb{Q}[C]$ we have

$$P(x) = (x-C)\left(x-K^{-1}CK\right)\times\cdots \times\left(x-K^{-(m-1)}CK^{(m-1)}\right),$$

so we can identify, and we often do, the Gaussian periods η_i with the matrices $K^{-i}CK^i$ (for the proofs of these facts see, for example, [Thaine 01] or [Thaine 04]).

The elements $c_{i,j}$ can be regarded as polynomials over $\mathbb{Q}$ in the parameters $t_0,\dots,t_{m-1}$. We can calculate these elements by first expressing them in terms of some Jacobi sums $J_{a,b}$ and then constructing those Jacobi sums using Stickelberger's theorem and some roots of unity (see [Thaine 01]). More precisely, for $0 \le a,b \le m-1$, let

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

where $\mathrm{ind}_s(k)$ is the least nonnegative integer such that $s^{\,\mathrm{ind}_s(k)} \equiv k \bmod q$. We have [Thaine 01, (15) and (4)]

$$\begin{aligned} c_{i,j} &= -f\delta_{0,i} - \frac{1}{m^2}\sum_{a=0}^{m-1}\sum_{b=0}^{m-1}\zeta_m^{-ia-jb}J_{a,b} \\ &= -f\delta_{0,i} - \frac{1}{m^2}\Big(m\delta_{0,i}+m\delta_{0,j}+m\delta_{i,j}-q-1 \\ &\qquad + \sum_{\substack{1\le a,b<m \\ a+b\ne m}}\zeta_m^{-ia-jb}J_{a,b}\Big). \end{aligned} \tag{2–3}$$

If $c \in \mathbb{Z}$ and $\gcd(c,m) = 1$, we denote by σ_c the automorphism of $\mathbb{Q}[\zeta_m]$ such that $\sigma_c(\zeta_m) = \zeta_m^c$. Let Q be the prime ideal of $\mathbb{Z}[\zeta_m]$ over q such that $s^f \equiv \zeta_m \bmod Q$, and suppose that Q is a principal ideal: $Q = (\alpha) = (t_0 + t_1\zeta_m + \cdots + t_{\nu-1}\zeta_m^{\nu-1})$. Then by Stickelberger's theorem we have that for all a,b such that $a+b \not\equiv 0 \bmod m$,

$$(J_{a,b}) = \Big(\prod_{\substack{1\le c<m \\ (c,m)=1}} \sigma_c^{-1}(\overline{\alpha})^{\left[\frac{(a+b)c}{m}\right]-\left[\frac{ac}{m}\right]-\left[\frac{bc}{m}\right]}\Big) \tag{2–4}$$

(an equality of ideals), where the overbar denotes complex conjugation and $[\rho]$ is the integral part of the real number ρ.

To remove the parentheses in (2–4), we have to multiply by some suitable roots of unity; this can be tricky when m is not a prime number. More precisely, for $1 \le a,b \le m-1$ with $a+b \not\equiv 0 \bmod m$, there exist roots of unity $\varepsilon_{a,b} \in \mathbb{Z}[\zeta_m]$ such that

$$J_{a,b} = \varepsilon_{a,b}\prod_{\substack{1\le c<m \\ (c,m)=1}} \sigma_c^{-1}(\overline{\alpha})^{\left[\frac{(a+b)c}{m}\right]-\left[\frac{ac}{m}\right]-\left[\frac{bc}{m}\right]} \tag{2–5}$$

(see, for example, the comments preceding [Thaine 04, Proposition 11]).

When m is a prime number we have $J_{a,b} \equiv 1 \bmod (\zeta_m-1)^2$, for a,b as in (2–5), and these congruences are enough to determine the $\varepsilon_{a,b}$. One way to get the products in the right-hand side of (2–5) to be congruent to 1 mod $(\zeta_m-1)^2$ (when m is prime) is to choose α such that $\alpha \equiv c \bmod (\zeta_m-1)^2$ with $c \in \mathbb{Z} - p\mathbb{Z}$ and $\varepsilon_{a,b} = \varepsilon = \left(\frac{c}{m}\right)$ (Legendre symbol), since the products in (2–5) have $\varphi(m)/2$ terms. To simplify things, for general

m, in this article we are going to consider only the situation in which the Jacobi sums $J_{a,b}$ can be written, as in (2–5), with $\varepsilon_{a,b} = \varepsilon = \pm 1$ (independent of a, b) for some suitable $\alpha = t_0 + t_1\zeta_m + \cdots + t_{\nu-1}\zeta_m^{\nu-1}$.

So the theory above will hold only for values of the parameters t_i for which those conditions are satisfied. In particular, the entries of C are guaranteed to be integers only for those values of the parameters. But these considerations should not prevent us from performing the formal calculations with general $\alpha = t_0 + t_1\zeta_m + \cdots + t_{\nu-1}\zeta_m^{\nu-1}$ and $\varepsilon = \pm 1$ if this results at the end in nice cyclic monic polynomials in $\mathbb{Z}[t]$ with constant terms ± 1. (For a more elaborate account on the right choices of the roots of unity $\varepsilon_{a,b}$, in the general situation, see [Thaine 04, Proposition 11].)

We calculate the matrix C by replacing in (2–3) the values of $J_{a,b}$ obtained by the formulas in (2–5).

Remark 2.1. A program to calculate C can be found at the end of [Thaine 01]. There we take $\varepsilon = 1$; you can change it to $\varepsilon = -1$ by replacing the entry

```
H[i4,j4]:=sort(collect(rem(B[i4,j4],R,z),z));
```

by

```
H[i4,j4]:=sort(collect(-rem(B[i4,j4],R,z),z));
```

What one obtains from that program, after writing the value of m and F := $(t_0, t_1, \ldots, t_{\nu-1})$ -> $t_0 + t_1 z + \cdots + t_{\nu-1} z^{(\nu-1)}$ (write all the terms of the sum) in the first line, is an $m \times m$ matrix C with entries in $\mathbb{Q}[t_0, t_1, \ldots, t_{\nu-1}]$.[1]

The entries of the matrix C, as polynomials in the t_i, have degree $\nu = \varphi(m)$. This matrix is much too large for the information it contains, but it can be expressed in terms of a relatively small set of elements of degree $\nu/2$, as we are going to show.

For $0 \le i, j \le m-1$, define $c'_{i,j} = c_{i,j} + f\delta_{0,i}$. (The $c'_{i,j}$ are the so-called cyclotomic numbers of order m corresponding to q.) Regard indices modulo m. For all $i, j \in \mathbb{Z}$ we have that

$$c'_{i,j} = c'_{j,i}, \quad c'_{i,j} = c'_{-i,j-i}, \quad \sum_{k=0}^{m-1} c'_{i,k} = f - \delta_{0,i}. \quad (2\text{–}6)$$

[1]Alternatively, see the program at my web page (http://cicma.mathstat.concordia.ca/faculty/thaine/homepage.html).

It follows from (2–3) that

$$c'_{i,j} = -\frac{1}{m^2}\Big(m\delta_{0,i} + m\delta_{0,j} + m\delta_{i,j} - q - 1 + \sum_{\substack{1\le a,b<m \\ a+b\ne m}} \zeta_m^{-ia-jb} J_{a,b}\Big). \quad (2\text{–}7)$$

In particular (regarding the t_i and the $c'_{i,j}$ as integers), this implies, by the triangle inequality, that

$$\Big|c'_{i,j} - \frac{q}{m^2}\Big| \le \frac{3}{m} + \frac{1}{m^2} + \frac{(m-1)^2 - (m-1)}{m^2}\sqrt{q} < \sqrt{q},$$

since $|J_{a,b}| = \sqrt{q}$ when $1 \le a, b \le m-1$ and $a + b \ne m$.

For $i, j \in \mathbb{Z}$, regarding as always indices modulo m, define $a_{i,j} = m^2 c'_{i,j} - q$. These numbers are more convenient to work with than the $c_{i,j}$. Set $A = [a_{i,j}]_{0\le i,j<m}$. We have just proved that

$$|a_{i,j}| < m^2\sqrt{q}. \quad (2\text{–}8)$$

It follows from formulas (2–5) and (2–7) that the $a_{i,j}$ have degrees $\le \nu/2$ as polynomials in the parameters t_i. In fact, by (2–5), the Jacobi sums $J_{a,b}$ have degree $\nu/2$ in those parameters, since for fixed $1 \le a, b \le m-1$ such that $a+b \not\equiv 0 \bmod m$, the numbers $\left[\frac{(a+b)c}{m}\right] - \left[\frac{ac}{m}\right] - \left[\frac{bc}{m}\right]$ are equal to 1, $\nu/2$ times, and equal to 0, $\nu/2$ times, when $1 \le c \le m-1$ with $\gcd(c, m) = 1$. By (2–6) we also have that

$$a_{i,j} = a_{j,i}, \quad a_{i,j} = a_{-i,j-i}, \quad \sum_{k=0}^{m-1} a_{i,k} = -m - m^2\delta_{0,i}. \quad (2\text{–}9)$$

It follows from straightforward calculations (assuming (2–9)) that formula (2–2) is equivalent to the following equalities. For $0 \le i, j, l \le m-1$,

$$\sum_{k=0}^{m-1} a_{i,k}a_{k-j,l-j} - \sum_{k=0}^{m-1} a_{j,k}a_{k-i,l-i} = m^2 q(\delta_{0,i} - \delta_{0,j} - \delta_{l,i}\delta_{l,j}) - m^4 f(\delta_{0,i}\delta_{l,j} - \delta_{0,j} + \delta_{l,i}). \quad (2\text{–}10)$$

In particular, we can express q in terms of the $a_{i,j}$, for example by

$$q = \frac{1}{m^2}\Big(\sum_{k=0}^{m-1} a_{2,k}a_{k-1,0} - \sum_{k=0}^{m-1} a_{1,k}a_{k-2,-1}\Big), \quad (2\text{–}11)$$

and, of course, we can express $C = [c_{i,j}]$ in terms of the $a_{i,j}$ as

$$c_{i,j} = \frac{a_{i,j} + q}{m^2} - f\delta_{0,i}. \quad (2\text{–}12)$$

It can be shown that properties (2–9) through (2–12) characterize the integers $a_{i,j}$ and $c_{i,j}$ [Thaine 01]. We will show later how a few values of the elements $a_{i,j}$ give us all the information we need to construct $A = [a_{i,j}]$, and so also q and C.

We have $q = N_{\mathbb{Q}[\zeta_m]/\mathbb{Q}}(\alpha)$; this is the only prime that ramifies in $\mathbb{L}/\mathbb{Q}$, and $(q) = \mathcal{P}^m$, where $\mathcal{P}$ is a prime ideal of D. This ideal divides all elements $\mu = d_0\eta_0 + d_1\eta_1 + \cdots + d_{m-1}\eta_{m-1}$ with $d_i \in \mathbb{Z}$ and $d_0 + d_1 + \cdots + d_{m-1} \equiv 0 \bmod q$. So q divides the norms (from $\mathbb{L}$ to $\mathbb{Q}$) of such elements μ.

For example, we have that $\eta_i \equiv \eta_j \bmod \mathcal{P}$ for all i, j. So

$$m\eta_0 \equiv \eta_0 + \eta_1 + \cdots + \eta_{m-1} = -1 \equiv q - 1 \bmod \mathcal{P}.$$

Hence $\eta_i \equiv f \bmod \mathcal{P}$ for all i. Therefore for all $\lambda = z_0\eta_0 + \cdots + z_{m-1}\eta_{m-1} \in D$, with $z_0, \ldots, z_{m-1} \in \mathbb{Z}$, we have that

$$\lambda \equiv f \sum_{i=0}^{m-1} z_i \equiv \frac{-1}{m} \sum_{i=0}^{m-1} z_i \bmod \mathcal{P}.$$

Let

$$F(x) = (x - \lambda)(x - \tau(\lambda)) \cdots (x - \tau^{m-1}(\lambda))$$

be the characteristic polynomial of λ. Then we have that

$$F(x) \equiv \Big(x + \frac{1}{m} \sum_{i=0}^{m-1} z_i\Big)^m \bmod \mathcal{P}.$$

So

$$F(x) \equiv \Big(x + \frac{1}{m} \sum_{i=0}^{m-1} z_i\Big)^m \bmod q.$$

Now suppose that $\lambda \in D$ is an element of norm $N_{L/\mathbb{Q}}(\lambda) = q^k$, for some $k \geq 0$. Then $(\lambda) = \mathcal{P}^j$, for some $j \geq 0$, and since $\tau(\mathcal{P}) = \mathcal{P}$, we have that $\tau(\lambda)/\lambda$ is a unit of D. This shows that in order to find units of D, it is enough to look for elements of norm q^k.

2.1 Values of q and A for Small m

We end this section by showing the values of q and A for small m. Let $\varepsilon = \varepsilon_{a,b}$ be as in formula (2–5) (see the comments following that formula):

- For $m = 3$ we have $\alpha = t_0 + t_1\zeta_3$, $q = t_0^2 - t_0t_1 + t_1^2$, and
$$A = \begin{bmatrix} -12 - a - b & a & b \\ a & b & c \\ b & c & a \end{bmatrix},$$
where $a = -2 + \varepsilon(t_0 - 2t_1)$, $b = -2 + \varepsilon(t_0 + t_1)$, and $c = 1 - \varepsilon(2t_0 - t_1)$.

- For $m = 4$ we have $\alpha = t_0 + t_1\zeta_4$, $q = t_0^2 + t_1^2$, and
$$A = \begin{bmatrix} -20 - a - b - c & a & b & c \\ a & c & d & d \\ b & d & b & d \\ c & d & d & a \end{bmatrix},$$
where $a = -3 + \varepsilon(2t_0 - 4t_1)$, $b = -3 + 2\varepsilon t_0$, $c = -3 + \varepsilon(2t_0 + 4t_1)$, and $d = 1 - 2\varepsilon t_0$.

- For $m = 5$ we have $\alpha = t_0 + t_1\zeta_5 + t_2\zeta_5^2 + t_3\zeta_5^3$, $q = \frac{1}{25}(ac - ad - 2ae + bd - be + bf - ce + cf - 2de - 2ef - 30e)$, and
$$A = \begin{bmatrix} -30 - a - b - c - d & a & b & c & d \\ a & d & e & f & e \\ b & e & c & f & f \\ c & f & f & b & e \\ d & e & f & e & a \end{bmatrix},$$
where
$$\begin{aligned} a &= -4 + \varepsilon(3t_0^2 + 3t_1^2 - 2t_2^2 + 3t_3^2 - 9t_0t_1 - 4t_0t_2 + t_0t_3 \\ &\qquad + 6t_1t_2 - 4t_1t_3 - 4t_2t_3), \\ b &= -4 + \varepsilon(3t_0^2 + 3t_1^2 + 3t_2^2 - 7t_3^2 + t_0t_1 - 9t_0t_2 + 6t_0t_3 \\ &\qquad - 4t_1t_2 + t_1t_3 + t_2t_3), \\ c &= -4 + \varepsilon(3t_0^2 - 2t_1^2 - 7t_2^2 + 3t_3^2 - 4t_0t_1 + 6t_0t_2 - 9t_0t_3 \\ &\qquad + 6t_1t_2 + 6t_1t_3 + t_2t_3), \\ d &= -4 + \varepsilon(3t_0^2 - 7t_1^2 + 3t_2^2 - 2t_3^2 + 6t_0t_1 + t_0t_2 - 4t_0t_3 \\ &\qquad + t_1t_2 + 6t_1t_3 - 4t_2t_3), \\ e &= 1 - \varepsilon(2t_0^2 - 3t_1^2 + 2t_2^2 + 2t_3^2 - t_0t_1 - t_0t_2 - t_0t_3 \\ &\qquad + 4t_1t_2 - t_1t_3 - 6t_2t_3), \\ f &= 1 - \varepsilon(2t_0^2 + 2t_1^2 - 3t_2^2 - 3t_3^2 - t_0t_1 \\ &\qquad - t_0t_2 - t_0t_3 - t_1t_2 + 4t_1t_3 + 4t_2t_3). \end{aligned}$$

- For $m = 6$ we have $\alpha = t_0 + t_1\zeta_6$, $q = t_0^2 + t_0t_1 + t_1^2$ and
$$A = \begin{bmatrix} -42 - a - b - c - d - e & a & b & c & d & e \\ a & e & f & f & f & f \\ b & f & d & f & f & f \\ c & f & f & c & f & f \\ d & f & f & f & b & f \\ e & f & f & f & f & a \end{bmatrix},$$
where
$$\begin{aligned} a &= -5 + \varepsilon(4t_0 - 7t_1), \\ b &= -5 + \varepsilon(4t_0 - t_1), \\ c &= -5 + \varepsilon(4t_0 + 2t_1), \\ d &= -5 + \varepsilon(4t_0 + 5t_1), \\ e &= -5 + \varepsilon(4t_0 + 11t_1), \\ f &= 1 - \varepsilon(2t_0 + t_1). \end{aligned}$$

3. SEARCHING FOR THE FAMILIES OF UNITS

Suppose that $t_0, \dots, t_{\nu-1}$ depend on a single parameter t; then q and C are functions of t. We are looking for elements $z_0, \dots, z_{m-1} \in \mathbb{Z}[t]$ such that for suitable values of t, the numbers $\varepsilon_t = z_0\eta_0 + \cdots + z_{m-1}\eta_{m-1}$ are nontrivial units of D_q.

As we observed in Section 2, we can identify the Gaussian periods η_i with the conjugates $K^{-i}CK^i$ of C; so our problem can be restated as follows: Find $z_0, \dots, z_{m-1} \in \mathbb{Z}[t]$ such that for suitable values of t, the matrices $M = M_t = z_0C + z_1K^{-1}CK + \cdots + z_{m-1}K^{-(m-1)}CK^{(m-1)}$ have inverses in $\mathbb{Z}[t][C]$ (and are nontrivial). We can regard the parameter t as an indeterminate, the entries $c_{i,j}$ of C as polynomials in $\frac{1}{m^2}\mathbb{Z}[t]$ (by (2–3) and (2–5)), and the elements z_i as polynomials in $\mathbb{Z}[t]$.

We have that the minimal polynomial of ε_t over $\mathbb{Q}(t)$ is equal to the characteristic polynomial of M. (For a more formal approach to the construction and properties of the matrices of polynomials C and M see [Thaine 04].) So it is enough to look for matrices M, as above, with determinant ± 1; and in fact, by the observations in Section 2, it is also enough to find a matrix M such that

$$M = z_0C + z_1K^{-1}CK + \cdots + z_{m-1}K^{-(m-1)}CK^{(m-1)}, \tag{3–1}$$

with $\det(M) = \pm q^k$, for some $k \geq 0$.

For M as in (3–1), the matrices $K^{-j}MK^jM^{-1}$, $1 \leq j \leq m-1$, have characteristic polynomials in $\mathbb{Z}[t][x]$ and determinants equal to 1.

One way to search for matrices of one parameter satisfying (3–1) is to give a large number of distinct integer values to $z_0, \dots, z_{m-1}$ and to $t_1, \dots, t_{\nu-1}$, for example, leaving $t_0 = t$ as the parameter, and check whether for some of those values we get $\det(M) = \pm q^k$. We used variations of this straightforward method to find some of our examples. (However, giving polynomial values of degrees greater than 1 in some parameter t to all the z_i or t_i proved to need much computer memory.)

Another way is to give several integer values to $z_0, \dots, z_{m-1}$, satisfying $z_0 + \cdots + z_{m-1} = 0$, and take $t_2 = 0, \dots, t_{\nu-1} = 0$, for example, leaving $t_0 = u$ and $t_1 = v$ as parameters, searching for matrices M such that $\det(M)/q$ has small degree in u or v and then trying to write u and v as functions of some parameter t for which $\det(M)/q = \pm 1$. That works well, for example, when $m = 3$, 4, 6, or 8.

One can also regard all, or most, of the t_i and z_i as indeterminates, write $\det(M)$ as a polynomial in t_0, say, and factor the leading coefficient. One can then give the variables some values that annihilate this coefficient and start the process again with the new variables. Proceeding in this way, we end up with one free variable, say t, and $\det(M)$ with small degree in t. If we are lucky, we get this degree to be 0. Some of our examples were calculated using a variation of this idea, which we show next.

The problem of finding M as in (3–1) is included in the less-restrictive, but still difficult, problem of finding nontrivial solutions for the equation

$$\sum_{i=0}^{m-1} z_iK^{-i}CK^i \sum_{j=0}^{m-1} w_jK^{-j}CK^j = u, \tag{3–2}$$

with $z_0, \dots, z_{m-1}, w_0, \dots, w_{m-1} \in \mathbb{Q}[t_0, \dots, t_{\nu-1}]$, and $u \in q^k\mathbb{Q}^\times$ for some $k \geq 0$.

Let us use for the moment the simpler notation η_i for $K^{-i}CK^i$. By applying powers of τ to (2–1) we get, for all $i, j \in \mathbb{Z}$, $\eta_i\eta_j = \sum_{k=0}^{m-1} c_{j-i,k-i}\eta_k$. From (3–2) we get

$$\begin{aligned} u &= \sum_{i=0}^{m-1} z_i\eta_i \sum_{j=0}^{m-1} w_j\eta_j \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} z_iw_j\eta_i\eta_j \\ &= \sum_{k=0}^{m-1}\Big(\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} c_{j-i,k-i}z_iw_j\Big)\eta_k. \end{aligned}$$

That is, for $k = 0, \dots, m-1$,

$$-u = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} c_{j-i,k-i}z_iw_j.$$

Since $c_{i,j} = \frac{a_{i,j}+q}{m^2} - f\delta_{0,i}$, this gives

$$-u = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1}\Big(\frac{a_{j-i,k-i}+q}{m^2} - f\delta_{i,j}\Big)z_iw_j.$$

Therefore (3–2) is equivalent to

$$\begin{aligned} \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{j-i,k-i}z_iw_j = -m^2u - q\sum_{i=0}^{m-1} z_i\sum_{j=0}^{m-1} w_j \\ + m^2f\sum_{l=0}^{m-1} z_lw_l, \end{aligned} \tag{3–3}$$

for $k = 0, \dots, m-1$. Adding (3–3) for $k = 0, \dots, m-1$ and using (2–9), we get

$$mu = q\sum_{l=0}^{m-1} z_lw_l - f\sum_{i=0}^{m-1} z_i\sum_{j=0}^{m-1} w_j. \tag{3–4}$$

From (3–3) and (3–4) we get

$$\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{j-i,k-i}z_iw_j = -\sum_{i=0}^{m-1} z_i \sum_{j=0}^{m-1} w_j - m\sum_{l=0}^{m-1} z_lw_l. \tag{3–5}$$

Equalities (3–4) and (3–5) are equivalent to (3–2). If, for example, we stipulate that $\sum_{i=0}^{m-1} z_i = 0$, then, by (3–4), it is convenient to assume as well that $u = \pm q$ and $\sum_{l=0}^{m-1} z_lw_l = \pm m$. In that case we get the system of linear equations

$$\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{j-i,k-i}z_iw_j = \mp m^2$$

in the indeterminates $w_0, \dots, w_{m-1}$, and we can proceed (in the way we explained before) to look for values of $z_0, \dots, z_{m-1}$ and $t_1, \dots, t_{m-1}$ such that the determinant of the coefficients of this system has small degree in, say, $t_0 = t$, and then we can use, for example, Cramer's rule to find the w_i.

4. EXAMPLES

In the following examples we give, for several values of m, elements $\alpha(t) = t_0(t) + t_1(t)\zeta_m + \cdots + t_{\nu-1}(t)\zeta_m^{\nu-1} \in \mathbb{Z}[t][\zeta_m]$ such that their norms $q(t) = N(\alpha(t)) \in \mathbb{Z}[t]$ from $\mathbb{Q}(t)(\zeta_m)$ to $\mathbb{Q}(t)$ are irreducible, and matrices $M \in \mathbb{Q}(t)(C)$, where C is constructed from $\alpha(t)$ as in Section 2 and

$$M = \Big(\sum_i a_i(t)K^{-i}CK^i\Big)\Big(\sum_j b_j(t)K^{-j}CK^j\Big)^{-1}.$$

Each matrix M is chosen so that its characteristic polynomial $F(x)$ is irreducible over $\mathbb{Q}(t)$. Recall that then, for each value of the parameter t such that $q(t)$ is a prime number q, we have that $F(x)$ is the minimal polynomial of $\sum_i a_i(t)\eta_i / \sum_j b_j(t)\eta_j$, where the η_i are the Gaussian periods of degree m in $\mathbb{Q}[\zeta_q]$. So we are not only finding the cyclic polynomials $F(x)$ but also their roots in terms of Gaussian periods. If $F(x) \in \mathbb{Z}[x]$ and $F(0) = \pm 1$, then those roots are units of $\mathbb{Z}[\eta_0, \dots, \eta_{m-1}]$.

The examples in this and the next sections were calculated using the Maple system. Many of them were shown in [Thaine 05], but here we include some new ones. We calculated the matrices C using the value $\varepsilon = \varepsilon_{a,b} = 1$ in formula (2–5) (see Remark 2.1 following that formula). Similar examples can be calculated using $\varepsilon = -1$. For convenience, we name our parameters $n, t, u, v, \dots$ instead of $t_0, t_1, \dots$.

4.1 Degree $m = 3$

For $m = 3$, with $\alpha = n + t\zeta_3$, we get $q = n^2 - nt + t^2$. (The following are essentially cases of Shanks's simplest cubics, but the parameter is taken to be of a special form. This allows a factor to be removed from the conductor. See the comment below.)

Let $W = C - K^{-1}CK$. We have that $\det(W) = tq/3$. For $B = K^{-1}WKW^{-1}$, we have that

$$F = \det(xI - B) = x^3 + 3\frac{n}{t}x^2 + 3\frac{n-t}{t}x - 1.$$

Taking $t = 1$, we get $q = n^2 - n + 1$ and

$$F = x^3 + 3nx^2 + (3n-3)x - 1.$$

Taking $t = 3$, we get $q = n^2 - 3n + 9$ and

$$F = x^3 + nx^2 + (n-3)x - 1,$$

Shanks's polynomial.

Also we have, for example,

$$\det(W - K^{-1}WK) = (2n - t)q,$$
$$\det(W - 2K^{-1}WK - K^{-2}WK^2) = \left(6n + \frac{t}{3}\right)q,$$
$$\det(W - 2K^{-1}WK + 2K^{-2}WK^2) = \left(-12n - \frac{17t}{3}\right)q,$$
$$\det(W - 3K^{-1}WK + 2K^{-2}WK^2) = (-20n - 17t)q.$$

By finding values of n and t depending on one parameter such that those determinants equal $\pm q$, we can obtain more families of cyclic polynomials. For example, for $t = 2n + 1$, we have $q = 3n^2 + 3n + 1$, and for $U = W - K^{-1}WK$ and $B = K^{-1}UKU^{-1}$, we get

$$F = \det(xI - B) = x^3 + (9n+6)x^2 + (9n+3)x - 1.$$

In this and in the following examples, observe that F has the form $x^3 + ux^2 + (u-3)x - 1$ as before, but the conductor is distinct than that corresponding to Shanks's polynomial. In particular, when n runs through the integers, the sets of prime values taken by the conductors q are different.

For $t = -18n+3$, we have $q = 343n^2 - 111n + 9$, and for $U = W - 2K^{-1}WK - K^{-2}WK^2$ and $B = K^{-1}UKU^{-1}$, we get

$$F = \det(xI - B) = x^3 + (343n - 54)x^2 + (343n - 57)x - 1.$$

For $n = -17u + 7$ and $t = 36u - 15$, we have $q = 2197u^2 - 1825u + 379$, and for $U = W - 2K^{-1}WK + 2K^{-2}WK^2$ and $B = K^{-1}UKU^{-1}$, we get

$$F = \det(xI - B) = x^3 + (2197u - 911)x^2 + (2197u - 914)x - 1.$$

For $n = -17u - 6$ and $t = 20u + 7$, we have $q = 1029u^2 + 723u + 127$, and for $U = W - 3K^{-1}WK + 2K^{-2}WK^2$ and $B = K^{-1}UKU^{-1}$, we get

$$\begin{aligned} F &= \det(xI - B) \\ &= x^3 + (3087u + 1086)x^2 + (3087u + 1083)x - 1. \end{aligned}$$

4.2 Degree $m = 4$

For $m = 4$, with $\alpha = n + t\zeta_4$, we get $q = n^2 + t^2$.

Let $W = C - K^{-1}CK$. We have that $\det(W) = -t^2q/16$. For $B = K^{-1}WKW^{-1}$, we have that

$$F = \det(xI - B) = x^4 + 4\frac{n}{t}x^3 - 6x^2 - 4\frac{n}{t}x + 1.$$

Taking $t = 1$ and $t = 2$, we get some families.

Taking $t = 4$, we get $q = n^2 + 16$ and $F = x^4 + nx^3 - 6x^2 - nx + 1$, first found by M.-N. Gras.

For $B = K^{-2}WK^2W^{-1}$, we have that

$$\begin{aligned} F &= \det(xI - B) \\ &= x^4 + 4x^3 - \frac{16n^2 + 10t^2}{t^2}x^2 + 4x + 1. \end{aligned}$$

Taking $t = 1$, $t = 2$, and $t = 4$, we get more families.

Let $U = W - K^{-1}WK$. We have that $\det(U) = t^2q/4$. For $B = K^{-1}UKU^{-1}$, we have that

$$\begin{aligned} F &= \det(xI - B) \\ &= x^4 + \frac{8n^2 + 8t^2 + 4nt}{t^2}x^3 + \frac{20n^2 + 14t^2}{t^2}x^2 \\ &\quad + \frac{8n^2 + 8t^2 - 4nt}{t^2}x + 1. \end{aligned}$$

Taking $t = 1$ and $t = 2$, we get more families.

For $B = K^{-2}UK^2U^{-1}$, we have that

$$\begin{aligned} F &= \det(xI - B) \\ &= x^4 + \frac{-16n^2 - 12t^2}{t^2}x^3 + \frac{32n^2 + 38t^2}{t^2}x^2 \\ &\quad + \frac{-16n^2 - 12t^2}{t^2}x + 1. \end{aligned}$$

Taking $t = 1$, $t = 2$ and $t = 4$, we get more families.

Also we have, for example,

$$\det(W - 3K^{-2}WK^2 + 3K^{-3}WK^3) = -\frac{(24n + 7t)^2q}{16}.$$

If we take $n = -7u - 8$ and $t = 24u + 28$, then $q = 625u^2 + 1456u + 848$, and for $U = W - 3K^{-2}WK^2 + 3K^{-3}WK^3$ and $B = K^{-1}UKU^{-1}$, we get

$$\begin{aligned} F &= \det(xI - B) \\ &= x^4 - (625u + 728)x^3 - 6x^2 + (625u + 728)x + 1. \end{aligned}$$

4.3 Degree $m = 5$

For $m = 5$, with $\alpha = n + t\zeta_5 + u\zeta_5^2 + v\zeta_5^3$, we get

$$\begin{aligned} q &= 2v^2ut + 2vt^2n + 2vu^2n - 3v^2tn + 2v^2un + v^4 + 2u^2tn \\ &\quad + v^2n^2 + 2vtn^2 - u^3n - v^3t - vutn - u^3t + u^2n^2 - tn^3 \\ &\quad - un^3 - ut^3 + u^2t^2 - vn^3 - vt^3 - vu^3 + v^2t^2 + v^2u^2 \\ &\quad - v^3n - 3vun^2 - 3ut^2n + n^4 + 2vut^2 - 3vu^2t + 2utn^2 \\ &\quad + t^2n^2 + u^4 + t^4 - t^3n - v^3u. \end{aligned}$$

For $\alpha = n + 2 + \zeta_5 + 2\zeta_5^2$, we get $q = n^4 + 5n^3 + 15n^2 + 25n + 25$. Let $W = C - K^{-1}CK$. We have that $\det(W) = -q$.

For $B = -K^{-2}WK^2W^{-1}$, we have that

$$\begin{aligned} F &= \det(xI - B) \\ &= x^5 + n^2x^4 - (2n^3 + 6n^2 + 10n + 10)x^3 \\ &\quad + (n^4 + 5n^3 + 11n^2 + 15n + 5)x^2 \\ &\quad + (n^3 + 4n^2 + 10n + 10)x + 1, \end{aligned}$$

Lehmer's polynomial.

For $B = K^{-1}WKW^{-1}$, we have that

$$\begin{aligned} F &= \det(xI - B) \\ &= x^5 + (2n^2 + 5n + 10)x^4 \\ &\quad + (n^4 + 5n^3 + 17n^2 + 25n + 25)x^3 \\ &\quad + (n^4 + 3n^3 + 7n^2 + 5n + 5)x^2 \\ &\quad - (n^3 + 3n^2 + 5n + 5)x - 1. \end{aligned}$$

For $\alpha = n - \zeta_5 - (2 + 3n)\zeta_5^2 - (1 + 3n)\zeta_5^3$, we get $q = 25n^4 + 25n^3 + 15n^2 + 5n + 1$. Let $W = C - K^{-2}CK^2$. We have that $\det(W) = q/125$.

For $B = K^{-1}WKW^{-1}$, we have that

$$\begin{aligned} F &= \det(xI - B) \\ &= x^5 + (-125n^3 - 100n^2 - 50n - 10)x^4 \\ &\quad + (625n^4 + 625n^3 + 275n^2 + 75n + 5)x^3 \\ &\quad + (250n^3 + 150n^2 + 50n + 10)x^2 + 25n^2x - 1. \end{aligned}$$

For $B = K^{-2}WK^2W^{-1}$, we have that

$$\begin{aligned} F &= \det(xI - B) \\ &= x^5 + (50n^2 + 25n + 10)x^4 \\ &\quad + (625n^4 + 625n^3 + 425n^2 + 125n + 25)x^3 \\ &\quad + (625n^4 + 375n^3 + 175n^2 + 25n + 5)x^2 \\ &\quad + (-125n^3 - 75n^2 - 25n - 5)x - 1. \end{aligned}$$

This answers affirmatively a question of Emma Lehmer [Lehmer 88, comment at end of Section 5]:

"There may possibly be a second case for which $p = 25n^4 - 25n^3 + 15n^2 - 5n + 1$, but we have not been able to find the coefficients, which could be quite large in this case." Observe that the set

$$\{q = n^4 + 5n^3 + 15n^2 + 25n + 25 \mid n \in \mathbb{Z} \text{ and } q \text{ is prime}\}$$

is distinct from the set

$$\{q = 25n^4 + 25n^3 + 15n^2 + 5n + 1 \mid n \in \mathbb{Z} \text{ and } q \text{ is prime}\}.$$

4.4 Degree $m = 6$

For $m = 6$, with $\alpha = n + t\zeta_6$, we get $q = n^2 + nt + t^2$. Let $W = C - K^{-1}CK$. We have that $\det(W) = -t^4 q/5184$.

For $B = K^{-1}WKW^{-1}$, we have that

$$\begin{aligned} F &= \det(xI - B) \\ &= x^6 + 6\frac{n}{t}x^5 - 15\frac{n+t}{t}x^4 + 20x^3 + 15\frac{n}{t}x^2 \\ &\quad - 6\frac{n+t}{t}x + 1. \end{aligned}$$

Taking $t = 1$, we get $q = n^2 + n + 1$ and

$$\begin{aligned} F = x^6 + 6nx^5 - (15n + 15)x^4 + 20x^3 + 15nx^2 \\ - (6n + 6)x + 1. \end{aligned}$$

Taking $t = 3$, we get $q = n^2 + 3n + 9$ and

$$\begin{aligned} F = x^6 + 2nx^5 - (5n + 15)x^4 + 20x^3 + 5nx^2 \\ - (2n + 6)x + 1, \end{aligned}$$

first found by M.-N. Gras.

For $B = K^{-2}WK^2W^{-1}$, we have that

$$\begin{aligned} F &= \det(xI - B) \\ &= x^6 + 6\frac{n+t}{t}x^5 - 3\frac{24n^2 + 24t^2 + 19nt}{t^2}x^4 \\ &\quad + 20\frac{9n^2 + 8t^2 + 9nt}{t^2}x^3 - 3\frac{24n^2 + 29t^2 + 29nt}{t^2}x^2 \\ &\quad - 6\frac{n}{t}x + 1. \end{aligned}$$

Taking $t = 1$ and $t = 3$, we get more families.

For $B = K^{-3}WK^3W^{-1}$, we have that

$$\begin{aligned} F &= \det(xI - B) \\ &= x^6 + 6x^5 - 3\frac{48n^2 + 43t^2 + 48nt}{t^2}x^4 \\ &\quad + 4\frac{72n^2 + 77t^2 + 72nt}{t^2}x^3 - 3\frac{48n^2 + 43t^2 + 48nt}{t^2}x^2 \\ &\quad + 6x + 1. \end{aligned}$$

Taking $t = 1$, $t = 2$, $t = 3$, $t = 4$, $t = 6$, and $t = 12$, we get more families.

4.5 Degree $m = 7$

For $m = 7$, we could not find a family of cyclic polynomials in $\mathbb{Z}[x]$ whose roots are units, but the following family of cyclic polynomials, with constant term n^7, was found by Hashimoto and Hoshi using a different method [Hashimoto and Hoshi 05]:

$$\begin{aligned} F = x^7 &- (n^3 + n^2 + 5n + 6)x^6 + (9n^3 + 9n^2 + 24n + 12)x^5 \\ &+ (n^7 + n^6 + 9n^5 - 5n^4 - 15n^3 - 22n^2 - 36n - 8)x^4 \\ &- (n^8 + 5n^7 + 12n^6 + 24n^5 - 6n^4 + 2n^3 - 20n^2 - 16n)x^3 \\ &+ (2n^8 + 7n^7 + 19n^6 + 14n^5 + 2n^4 + 8n^3 - 8n^2)x^2 \\ &- (n^8 + 4n^7 + 8n^6 + 4n^4)x + n^7. \end{aligned}$$

This can be obtained using our method as follows: Take $\alpha = n - 2 + (1 - \zeta_7)(1 - \zeta_7^3)(1 + \zeta_7 + \zeta_7^3)$ and $U = C - K^{-2}CK^2$. We have that $\det(U) = -n^4 q$. With $B = -nK^{-2}UK^2U^{-1}$, we have that $F = \det(xI - B)$. Here

$$q = N(\alpha) = n^6 + 2n^5 + 11n^4 + n^3 + 16n^2 + 4n + 8.$$

If we take $B_1 = nK^{-6}UK^6U^{-1}$, we get another family

$$\begin{aligned} F_1 &= \det(xI - B_1) \\ &= x^7 - (n^5 + 2n^4 + 11n^3 + 2n^2 + 10n + 2)x^6 \\ &\quad + (n^9 + 4n^8 + 16n^7 + 26n^6 + 31n^5 + 45n^4 + 21n^3 \\ &\qquad + 12n^2 + 12n - 4)x^5 \\ &\quad + (n^{11} + 2n^{10} + 12n^9 + 7n^8 + 39n^7 + 58n^6 + 74n^5 \\ &\qquad + 68n^4 + 74n^3 + 24n^2 + 16n + 8)x^4 \\ &\quad - (n^{12} + 4n^{11} + 16n^{10} + 27n^9 + 33n^8 + 54n^7 + 19n^6 \\ &\qquad + 2n^5 - 9n^4 - 14n^3 - 20n^2)x^3 \\ &\quad - (2n^{11} + 7n^{10} + 30n^9 + 40n^8 + 56n^7 + 66n^6 + 46n^5 \\ &\qquad + 30n^4 + 20n^3 + 8n^2)x^2 \\ &\quad - (n^{10} + 3n^9 + 12n^8 + 10n^7 + 12n^6 + 10n^5 + 4n^4)x - n^7. \end{aligned}$$

Also, for $\alpha = n - 1 + (1 - \zeta_7)(1 - \zeta_7^3)$ and $U = C - K^{-2}CK^2$, we have that $\det(U) = n^4 q$. If we take $B_2 = -nK^{-1}UKU^{-1}$, we get

$$\begin{aligned} F_2 &= \det(xI - B_2) \\ &= x^7 + (n^3 + 4n^2 + 3n + 6)x^6 \\ &\quad + (3n^5 + 6n^4 + 15n^3 + 15n^2 + 12n + 12)x^5 \\ &\quad + (3n^7 + 4n^6 + 20n^5 + 11n^4 + 27n^3 + 6n^2 + 12n + 8)x^4 \\ &\quad + (n^9 + n^8 + 8n^7 + n^6 + 7n^5 - 17n^4 - 2n^3 - 20n^2)x^3 \\ &\quad - (n^8 + 7n^7 + 11n^6 + 19n^5 + 16n^4 + 8n^3 + 8n^2)x^2 \\ &\quad - (n^9 + 5n^7 - 4n^6 + 2n^5 - 4n^4)x + n^7. \end{aligned}$$

If we take $B_3 = nK^{-5}UK^5U^{-1}$, we get

$$\begin{aligned}F_3 &= \det(xI - B_3)\\ &= x^7 + (2n^3 + n^2 + 6n - 2)x^6\\ &\quad + (n^6 + n^5 + 5n^4 + n^3 - 2n^2 - 16n - 4)x^5\\ &\quad - (n^7 + 12n^5 + 13n^4 + 36n^3 + 16n^2 - 8)x^4\\ &\quad - (n^8 + 4n^7 + 6n^6 + 10n^5 - 26n^3 - 28n^2 - 16n)x^3\\ &\quad + (n^9 + 2n^8 + 9n^7 + 18n^6 + 38n^5 + 36n^4 + 28n^3\\ &\qquad + 8n^2)x^2\\ &\quad + (n^9 + 2n^8 + 5n^7 + 5n^6 + 4n^5 + 4n^4)x - n^7.\end{aligned}$$

Here $q = N(\alpha) = n^6 + n^5 + 8n^4 + n^3 + 22n^2 + 8n + 8$. Observe that if

$$q_1(n) = n^6 + 2n^5 + 11n^4 + n^3 + 16n^2 + 4n + 8$$

and

$$q_2(n) = n^6 + n^5 + 8n^4 + n^3 + 22n^2 + 8n + 8,$$

then

$$q_2(n) = \frac{1}{8}n^6 q_1(2n^{-1}) \quad \text{and} \quad q_1(n) = \frac{1}{8}n^6 q_2(2n^{-1}).$$

Similarly, for

$$\alpha = n - 2 - \zeta_7 - 2\zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5,$$

we get

$$q = n^6 - 12n^5 + 67n^4 - 153n^3 + 128n^2 + 144n + 64.$$

Let $W = C - K^{-1}CK$. We have that $\det(W) = -n^2(15n + 8)^2 q$. The characteristic polynomials of $n(15n + 8)K^{-i}WK^iW^{-1}$, $i = 1, \ldots, 6$, are all in $\mathbb{Z}[n][x]$ and have constant terms equal to $-n^7(15n + 8)^7$.

4.6 Degree $m = 8$

For $m = 8$, take, for example, $\alpha = n + t\zeta_8$. We get $q = n^4 + t^4$. Let $U = C - K^{-2}CK^2$. We have that $\det(U) = -t^{12}q/4096$.

Take $t = 1$. For $B = K^{-1}UKU^{-1}$, we have

$$\begin{aligned}F &= \det(xI - B)\\ &= x^8 + 8nx^7 + (-16n^4 + 28n^2 - 16)x^6\\ &\quad + (-64n^5 - 16n^4 + 56n^3 - 64n - 16)x^5\\ &\quad + (-64n^6 + 96n^4 - 64n^2 + 26)x^4\\ &\quad + (64n^6 + 128n^5 + 16n^4 + 64n^2 + 72n + 16)x^3\\ &\quad + (-32n^5 - 16n^4 - 28n^2 - 32n - 16)x^2 - 8n^3x + 1.\end{aligned}$$

For $B = K^{-2}UK^2U^{-1}$, we have

$$\begin{aligned}F &= \det(xI - B)\\ &= x^8 + (16n^4 - 8n^2 + 16)x^7 + (80n^4 + 52)x^6\\ &\quad + (-64n^6 + 64n^4 - 8n^2 + 64)x^5\\ &\quad + (-64n^6 - 48n^4 - 64n^2 + 22)x^4\\ &\quad + (-16n^4 - 56n^2 - 16)x^3 + (16n^4 - 12)x^2 + 8n^2x + 1.\end{aligned}$$

For $B = K^{-4}UK^4U^{-1}$, we have

$$\begin{aligned}F &= \det(xI - B)\\ &= x^8 + (-16n^4 - 8)x^7 + (64n^6 - 32n^4 + 64n^2 - 4)x^6\\ &\quad + (16n^4 + 72)x^5 + (-128n^6 - 192n^4 - 128n^2 - 122)x^4\\ &\quad + (16n^4 + 72)x^3 + (64n^6 - 32n^4 + 64n^2 - 4)x^2\\ &\quad + (-16n^4 - 8)x + 1.\end{aligned}$$

Take $t = 2$. For $B = K^{-1}UKU^{-1}$, we have

$$\begin{aligned}F &= \det(xI - B)\\ &= x^8 + 4nx^7 + (-n^4 + 7n^2 - 16)x^6\\ &\quad + (-2n^5 - n^4 + 7n^3 - 32n - 16)x^5\\ &\quad + (-n^6 + 6n^4 - 16n^2 + 26)x^4\\ &\quad + (n^6 + 4n^5 + n^4 + 16n^2 + 36n + 16)x^3\\ &\quad + (-n^5 - n^4 - 7n^2 - 16n - 16)x^2 - n^3x + 1.\end{aligned}$$

For $B = K^{-2}UK^2U^{-1}$, we have

$$\begin{aligned}F &= \det(xI - B)\\ &= x^8 + (n^4 - 2n^2 + 16)x^7 + (5n^4 + 52)x^6\\ &\quad + (-n^6 + 4n^4 - 2n^2 + 64)x^5\\ &\quad + (-n^6 - 3n^4 - 16n^2 + 22)x^4\\ &\quad + (-n^4 - 14n^2 - 16)x^3\\ &\quad + (n^4 - 12)x^2 + 2n^2x + 1,\end{aligned}$$

first found by Emma Lehmer [Lehmer 88].

For $B = K^{-4}UK^4U^{-1}$, we have

$$\begin{aligned}F &= \det(xI - B)\\ &= x^8 + (-n^4 - 8)x^7 + (n^6 - 2n^4 + 16n^2 - 4)x^6\\ &\quad + (n^4 + 72)x^5 + (-2n^6 - 12n^4 - 32n^2 - 122)x^4\\ &\quad + (n^4 + 72)x^3 + (n^6 - 2n^4 + 16n^2 - 4)x^2\\ &\quad + (-n^4 - 8)x + 1.\end{aligned}$$

4.7 Degree $m = 9$

For $m = 9$, take $\alpha = n + \zeta_9 - \zeta_9^4$. We get $q = n^6 + 9n^3 + 27$. Let

$$W = C - K^{-2}CK^2 - K^{-4}CK^4 + K^{-6}CK^6.$$

We have that $\det(W) = q$; therefore the characteristic polynomials F_i of $K^{-i}WK^iW^{-1}$, $i = 1, \dots, 4$, are cyclic of degree 9 in $\mathbb{Z}[n][x]$, with constant terms -1. For example,

$$\begin{aligned}F_2 = {} & x^9 + (-n^7 + n^6 + n^5 - 9n^4 + 9n^3 + 3n^2 - 27n + 27)x^8 \\ & + (-n^{10} + 2n^9 + 2n^8 - 19n^7 + 23n^6 + 18n^5 - 113n^4 \\ & \quad + 99n^3 + 54n^2 - 234n + 135)x^7 \\ & + (n^{11} - 4n^{10} + 2n^9 + 16n^8 - 47n^7 + 22n^6 + 90n^5 \\ & \quad - 207n^4 + 62n^3 + 189n^2 - 297n + 24)x^6 \\ & + (n^{11} - n^9 + 5n^8 + 8n^7 - 16n^6 + 5n^5 + 72n^4 - 90n^3 \\ & \quad - 24n^2 + 216n - 189)x^5 \\ & + (-n^{11} + 4n^{10} + n^9 - 17n^8 + 49n^7 + 6n^6 - 99n^5 \\ & \quad + 211n^4 - 216n^2 + 351n - 81)x^4 \\ & + (-n^{11} + n^{10} - 13n^8 + 12n^7 + 8n^6 - 63n^5 + 54n^4 \\ & \quad + 44n^3 - 108n^2 + 81n + 48)x^3 \\ & + (-n^8 - n^7 + n^6 - 9n^5 - 9n^4 + 9n^3 - 15n^2 \\ & \quad - 27n + 27)x^2 \\ & + (-2n^4 - 9n)x - 1\end{aligned}$$

and

$$\begin{aligned}F_4 = {} & x^9 + (n^7 + 8n^4 + 18n)x^8 \\ & + (n^{10} - n^8 + 13n^7 - 2n^6 - 5n^5 + 63n^4 - 18n^3 - 3n^2 \\ & \quad + 108n - 54)x^7 \\ & + (2n^{10} + 2n^8 + 24n^7 - 14n^6 + 18n^5 + 108n^4 - 98n^3 \\ & \quad + 54n^2 + 162n - 210)x^6 \\ & + (n^{10} - 2n^9 + 3n^8 + 14n^7 - 27n^6 + 27n^5 + 44n^4 \\ & \quad - 135n^3 + 81n^2 + 9n - 243)x^5 \\ & + (-2n^9 - 3n^7 - 20n^6 + 14n^5 - 27n^4 - 72n^3 + 42n^2 \\ & \quad - 81n - 54)x^4 \\ & + (n^8 - n^7 - n^6 + 9n^5 - 9n^4 + 19n^3 + 27n^2 \\ & \quad - 27n + 57)x^3 \\ & + (n^6 - 4n^4 + 9n^3 + 27)x^2 - 3n^2x - 1.\end{aligned}$$

5. A COMPOSITION OF MULTIPLICATION MATRICES

Let F be a cyclic monic polynomial with coefficients in a field $\mathbb{K}$. Let $\theta_0, \theta_1, \dots, \theta_{m-1}$ be the roots of F in an algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$, $L = \mathbb{K}[\theta_0] = \mathbb{K}[\theta_0, \dots, \theta_{m-1}]$, and τ a generator of $\mathrm{Gal}(L/\mathbb{K})$. Suppose that $\theta_0, \theta_1, \dots, \theta_{m-1}$ are linearly independent over $\mathbb{K}$ and that they are labeled such that $\tau(\theta_i) = \theta_{i+1}$ (indices modulo m).

For $0 \le i, j \le m-1$ define the elements $b_{i,j} \in \mathbb{K}$ by

$$\theta_0\theta_i = \sum_{j=0}^{m-1} b_{i,j}\theta_j. \tag{5–1}$$

Let $B = [b_{i,j}]_{0 \le i,j < m}$. We call B the multiplication matrix of the θ_i.

By applying powers of τ to (5–1), we get, for all i, j,

$$\theta_i\theta_j = \sum_{k=0}^{m-1} b_{i-j,k-j}\theta_k \tag{5–2}$$

(indices modulo m).

Let $K = [\delta_{i+1,j}]$, as in Section 2. It follows from formula (5–2) and a little linear algebra that F is the characteristic polynomial of B, that $\mathbb{K}[B]$ is a splitting field for F, and that the conjugates $K^{-i}BK^i$ of B ($i = 0, \dots, m-1$) belong to $\mathbb{K}[B]$.

It follows that F splits in $\mathbb{K}[B][x]$ as

$$F = (x - B)(x - K^{-1}BK)\cdots(x - K^{-(m-1)}BK^{m-1}).$$

Hence we can identify the conjugates $K^{-i}BK^i$ with the roots θ_i of F. (For proofs of these statements see [Thaine 04].)

By knowing the multiplication matrices of the roots of cyclic polynomials we get more information than by just knowing the polynomials. For example, suppose m and n are relatively prime integers ≥ 2. Suppose A and B are multiplication matrices of orders m and n respectively of the roots of cyclic polynomials F_i over $\mathbb{K}_i = \mathbb{Q}(t_i)$, $i = 1, 2$ respectively, which are monic and have coefficients in $\mathbb{Z}[t_i]$ and constant terms equal to ± 1. Then we can construct a cyclic monic polynomial F over $\mathbb{Z}[t_1, t_2]$, of degree mn, with constant term ± 1, by calculating first the multiplication matrix of its roots.

So, for example, since we can construct such polynomials for $m = 2, 4, 8, 3, 9, 5$, we can construct several families of cyclic polynomials at two parameters of degrees 10, 12, 15, 18, 20, 30, etc. (We can also construct, for example, families at three parameters of degree 360.)

In fact, let $A = [a_{i,j}]$ and $B = [b_{i,j}]$. Denote by θ_i the roots of $F_1 = \det(xI - A)$ and by η_i the roots of $F_2 = \det(xI - B)$. They are units in the integral closures of $\mathbb{Z}[t_1]$ and $\mathbb{Z}[t_2]$ in $\mathbb{K}_1[\theta_0]$ and $\mathbb{K}_2[\eta_0]$ respectively. Since $\gcd(m, n) = 1$ we have that the $\theta_i\eta_j$, $0 \le i \le m-1$, $0 \le j \le n-1$, are linearly independent (over $\mathbb{K}$) units in the composite field $\mathbb{K}[\theta_0, \eta_0]$.

If we arrange these elements as $\theta_0\eta_0, \theta_1\eta_1, \dots, \theta_{mn-1}\eta_{mn-1}$ (indices of θ modulo m and indices of η modulo n), then their multiplication matrix is the $mn \times mn$ matrix $E = [e_{i,j}]$ with $e_{i,j} = a_{|i|_m,|j|_m}b_{|i|_n,|j|_n}$, where $|i|_m$ is the integer such that $0 \le |i|_m < m-1$ and $|i|_m \equiv i \bmod m$. (This fact was also noticed by Professor Hashimoto, who pointed out that E is the tensor product of the matrices A and B.) Therefore, as

announced, $F = \det(xI - E)$ is a cyclic polynomial, over $\mathbb{Z}[t_1, t_2]$, of degree mn, with constant term equal to ± 1. As examples we construct families at two parameters of degrees 10 and 12.

Example 5.1. For $m = 2$, the matrix

$$A = \begin{bmatrix} n + 1/n & 1/n \\ -1/n & -1/n \end{bmatrix}$$

is the multiplication matrix of the roots of the polynomial

$$F_1 = \det(xI - A) = x^2 - nx - 1.$$

For $m = 5$, $\alpha = t - 1 - \zeta_5 - 2\zeta_5^2$ and $W = C - K^{-1}CK$, we have that $q = t^4 - t^3 + 6t^2 - 6t + 11$,

$$B = K^{-2}WK^2W^{-1} = \frac{1}{25}\begin{bmatrix} a & a & c & a-25 & a-25 \\ a & a & c-25 & a & a-25 \\ b & b-25 & d & f & f \\ a-25 & a & e & g & a \\ a-25 & a-25 & e & a & g+25 \end{bmatrix},$$

where

$$\begin{aligned} a &= -t^4 + t^3 - 4t^2 + 5t, \\ b &= 4t^4 - 4t^3 + 21t^2 - 10t + 50, \\ c &= -t^4 + t^3 - 9t^2 + 20t, \\ d &= 4t^4 - 4t^3 + 41t^2 - 20t + 50, \\ e &= -t^4 + t^3 - 9t^2 - 5t, \\ f &= 4t^4 - 4t^3 + 21t^2 - 35t + 50, \\ g &= -t^4 + t^3 - 4t^2 + 30t - 25, \end{aligned}$$

and

$$\begin{aligned} F_2 &= \det(xI - B) \\ &= x^5 + (-t^2 - 2t - 1)x^4 + (2t^3 + 4t - 4)x^3 \\ &\quad + (-t^4 + t^3 - 2t^2 + 4t + 3)x^2 \\ &\quad + (-t^3 + t^2 - 5t + 3)x - 1. \end{aligned}$$

Let E be the composite of A and B as defined before. Then we have the following family at two parameters of degree 10:

$$\begin{aligned} F &= \det(xI - E) \\ &= x^{10} - n(t^2 + 2t + 1)x^9 \\ &\quad + (2n^2t^3 + 4n^2t - 4n^2 - t^4 - 6t^2 + 4t - 9)x^8 \\ &\quad + n(-n^2t^4 + n^2t^3 - 2n^2t^2 + 4n^2t + 3n^2 + 2t^5 + t^4 + 9t^3 \\ &\qquad - 2t^2 + 8t + 5)x^7 \\ &\quad + (-n^4t^3 + n^4t^2 - 5n^4t - n^2t^6 - n^2t^5 - n^2t^4 - 3n^2t^3 \\ &\qquad + 13n^2t^2 - 10n^2t + 3n^4 + 15n^2 + 2t^6 - 2t^5 + 14t^4 \\ &\qquad - 16t^3 + 36t^2 - 22t + 28)x^6 \\ &\quad - n(n^2t^5 + n^2t^4 + 4n^2t^3 + 6n^2t^2 - n^2t + n^4 + 2n^2 \\ &\qquad + 2t^7 - 2t^6 + 11t^5 - 13t^4 + 18t^3 - 6t^2 + t + 8)x^5 \\ &\quad + (-n^4t^2 - 2n^4t - 2n^2t^6 + 2n^2t^5 - 14n^2t^4 + 14n^2t^3 \\ &\qquad - 28n^2t^2 + 24n^2t - n^4 - 16n^2 - t^8 + 2t^7 - 9t^6 + 16t^5 \\ &\qquad - 34t^4 + 38t^3 - 54t^2 + 36t - 35)x^4 \\ &\quad - n(2n^2t^3 + 4n^2t - 4n^2 + t^7 - 2t^6 + 8t^5 \\ &\qquad - 14t^4 + 20t^3 - 23t^2 + 9t - 3)x^3 \\ &\quad + (-n^2t^4 + n^2t^3 - 2n^2t^2 + 4n^2t + 3n^2 + t^6 - 2t^5 + 9t^4 \\ &\qquad - 14t^3 + 27t^2 - 22t + 15)x^2 \\ &\quad + n(t^3 - t^2 + 5t - 3)x - 1. \end{aligned}$$

Example 5.2. For $m = 3$, $\alpha = n + 3\zeta_3$ and $W = C - K^{-1}CK$, we have that $q = n^2 - 3n + 9$,

$$A = K^{-1}WKW^{-1} = \frac{1}{9}\begin{bmatrix} a & a & c \\ a & a-9 & c+9 \\ b & b+9 & d \end{bmatrix},$$

where $a = n^2 - 5n + 13$, $b = -2n^2 + 7n - 23$, $c = n^2 - 2n + 1$, $d = -2n^2 + n - 17$, and

$$F_1 = \det(xI - A) = x^3 + nx^2 + (n-3)x - 1.$$

For $m = 4$, $\alpha = t + 2\zeta_4$, and $W = C - K^{-1}CK$, we have that $q = t^2 + 4$,

$$B = K^{-1}WKW^{-1} = \frac{1}{8}\begin{bmatrix} a & a & c & a \\ a & a-8 & c+8 & a \\ b & b+8 & d & b-8 \\ a & a & c-8 & a+8 \end{bmatrix},$$

where $a = t^2 - 2t + 5$, $b = -3t^2 + 2t - 11$, $c = t^2 + 2t + 1$, $d = -3t^2 - 10t - 15$, and

$$F_2 = \det(xI - B) = x^4 + 2tx^3 - 6x^2 - 2tx + 1.$$

Let E be the composite of A and B as defined before. Then we have the following family at two parameters of degree 12:

$$\begin{aligned} F &= \det(xI - E) \\ &= x^{12} - 2ntx^{11} + (4nt^2 - 6n^2 + 12n - 12t^2 - 36)x^{10} \\ &\quad + (2n^3t + 6n^2t - 18nt + 8t^3 + 30t)x^9 \end{aligned}$$

$$
\begin{aligned}
&+(-4n^3t^2+20n^2t^2-28nt^2+n^4-4n^3+50n^2-160n\\
&\quad+72t^2+342)x^8\\
&+(-2n^4t-8n^2t^3+10n^2t+16nt^3+16nt-48t^3\\
&\quad-210t)x^7\\
&+(-36n^2t^2+108nt^2-6n^4+36n^3-138n^2+252n\\
&\quad-156t^2-522)x^6\\
&+(2n^4t-24n^3t+8n^2t^3+98n^2t-32nt^3-140nt\\
&\quad+72t^3+234t)x^5\\
&+(4n^3t^2-16n^2t^2+16nt^2+n^4-8n^3+68n^2\\
&\quad-140n+60t^2+285)x^4\\
&+(2n^3t-24n^2t+72nt-8t^3-84t)x^3\\
&+(-4nt^2-6n^2+24n-54)x^2+(-2nt+6t)x+1.
\end{aligned}
$$

6. SCHOOF'S CRITERION

Suppose now that m is an odd prime number. Let $D = \mathbb{Z}[t]$, where t is an indeterminate, and $\mathbb{K} = \mathbb{Q}(t)$. Let $\mathcal{C}$ be the curve $f(t,x) = 0$, where

$$f(t,X) = X^m + c_{m-1}(t)X^{m-1} + \cdots + c_0(t) \in D[X]$$

is a cyclic polynomial (over $\mathbb{K}$). Let $\mathbb{L} = \mathbb{K}(x) = \mathbb{Q}(t,x)$, $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, and τ a generator of G. Let R be the integral closure of D in $\mathbb{L}$.

Question: when is there a unit of R of degree m over $\mathbb{K}$? If ε_0 is such a unit, then the polynomial $g_0(t,X) = \prod_{i=0}^{m-1}(X - \tau^i(\varepsilon_0))$ belongs to $D[X]$, is cyclic over $\mathbb{K}$, and has a constant term equal to ± 1.

Such a polynomial can be regarded as one of the families (at the parameter t) considered in the previous sections of cyclic polynomials over $\mathbb{Q}$ whose roots are algebraic units. This seems a difficult question. Let us consider instead the following easier and, for our practical purposes equivalent, question, for which we do have a satisfactory answer thanks to some ideas of René Schoof.

Let $D' = \mathbb{Q}[t]$ and let R' be the integral closure of D' in $\mathbb{L}$. Question: when is there a unit of R' of degree m over $\mathbb{K}$ (that is, an element of $R'^{\times} - \mathbb{Q}^{\times}$)?

If ε is such a unit then the polynomial $g(t,X) = \prod_{i=0}^{m-1}(X - \tau^i(\varepsilon))$ belongs to $D'[X]$, is cyclic over $\mathbb{K}$, and has a constant term belonging to $\mathbb{Q}^{\times}$.

Let S be the set of prime divisors of $\mathbb{L}$ at infinity. The units ε we are searching for are precisely the nonconstant S-units of $\mathbb{L}$. In this section we show a way to find whether such units exist, given a curve $\mathcal{C}$ and $\mathbb{L}$ as above, and we give some examples (mostly negative) for $m = 5$ and $m = 7$.

Since the degree of the divisor (ε) is 0, when a nonconstant S-unit ε exists we must have $|S| > 1$; hence the prime divisor of $\mathbb{K}$ at infinity splits in $\mathbb{L}$ (recall that $\mathbb{L}/\mathbb{K}$ is cyclic of degree m). Denote by $\mathcal{J}$ the Jacobian of $\mathcal{C}$, that is,

$$\mathcal{J} = \frac{\{\text{divisors of } \mathbb{L} \text{ of degree zero}\}}{\{\text{principal divisors of } \mathbb{L}\}}.$$

Proposition 6.1. *Suppose that the prime divisor of $\mathbb{K}$ at infinity splits in $\mathbb{L}$. Let $S = \{P_0, P_1 = \tau(P_0), \ldots, P_{m-1} = \tau^{m-1}(P_0)\}$ be the set of prime divisors of $\mathbb{L}$ at infinity. Then $\mathbb{L}$ has nonconstant S-units if and only if the subgroup $\mathcal{I}$ of $\mathcal{J}$ generated by the classes of the divisors $P_i - P_j$, $0 \le i < j \le m-1$, is finite.*

Proof: Suppose that $\mathcal{I}$ is finite. Let k be a positive integer such that $k(P_0 - P_1) = (\beta)$ is a principal divisor; then β is a nonconstant S-unit of $\mathbb{L}$. Conversely, suppose that $\mathbb{L}$ has a nonconstant S-unit ε. We must prove that $\mathcal{I}$ is finite.

If $\mathcal{I} = \{0\}$ there is nothing to prove. Assume that $\mathcal{I} \neq \{0\}$. Observe first that $\mathcal{I}$ is a $\mathbb{Z}[G]$-module generated by the class of $P_0 - P_1 = (1-\tau)P_0$. Since $\tau^m = 1$, we have that $\mathcal{I}$ is a cyclic $\mathbb{Z}[G]/(1 + \tau + \cdots + \tau^{m-1})$-module; that is (since m is a prime number), a cyclic $\mathbb{Z}[\zeta_m]$-module, where ζ_m is a primitive mth root of 1 if we set $\zeta_m \cdot \alpha = \tau(\alpha)$ for all $\alpha \in \mathcal{I}$. Hence $\mathcal{I}$ is isomorphic, as a $\mathbb{Z}[\zeta_m]$-module, to a quotient ring of $\mathbb{Z}[\zeta_m]$.

Therefore, either $\mathcal{I}$ is finite or $\mathcal{I}$ is isomorphic to $\mathbb{Z}[\zeta_m]$ as a group. This proves that if $\mathcal{I}$ has a nonzero element of finite order, then it is finite. Since ε is a nonconstant S-unit, we have that $(\varepsilon) = (\sum_{i=0}^{m-2} k_i\tau^i)(P_0 - P_1)$, for some $k_i \in \mathbb{Z}$, not all zero.

But then, if $k = N_{\mathbb{Q}[\zeta_m]/\mathbb{Q}}(\sum_{i=0}^{m-1} k_i\zeta_m^i)$, we have that $k \neq 0$ annihilates the class of $P_0 - P_1$ in $\mathcal{J}$. Therefore, this class is a nonzero element of finite order in $\mathcal{I}$, and $\mathcal{I}$ is finite. □

Denote by g the genus of $\mathbb{L}/\mathbb{K}$. Suppose that $g > 0$ and that $\mathbb{L}$ contains nonconstant S-units. Then the prime divisor of $\mathbb{K}$ at infinity splits in $\mathbb{L}$. Let $S = \{P_0, P_1 = \tau(P_0), \ldots, P_{m-1} = \tau^{m-1}(P_0)\}$ be the set of prime divisors of $\mathbb{L}$ at infinity. We have that the divisor $P_0 - P_1$ is not principal [Stichtenoth 93, Theorem I.4.11], and by Proposition 6.1, its class in $\mathcal{J}$ has finite order. Therefore we have the following necessary condition for the existence of S-units.

Proposition 6.2. *If $\mathbb{L}$ has nonconstant S-units and $g > 0$, then $\mathcal{J}$ contains a nontrivial finite subgroup.*

Let p be a prime at which (the nonsingular model of) $\mathcal{C}$ has good reduction; then also $\mathcal{J}$ has good reduction at p. Denote by $\mathcal{J}_p$ the Jacobian $\mathcal{J}$ reduced modulo p, which is also the Jacobian of the reduced curve $\mathcal{C}_p$ over the residue field $\mathbb{F}_p$ (see, for example, [Mazur 86, pp. 237–238] and [Poonen 96, Section 5]). Denote by $h_p = |\mathcal{J}_p|$ the class number of the function field of $\mathcal{C}_p$ over $\mathbb{F}_p$. We have that if p is odd, then $\mathcal{J}_p$ has a subgroup isomorphic to the torsion group of $\mathcal{J}$, and if $p = 2$, then $\mathcal{J}_p$ has a subgroup isomorphic to the odd part of the torsion group of $\mathcal{J}$ (see, for example, [Poonen 96, Section 5] and [Katz 81, Appendix]). Therefore, we have the following result.

Proposition 6.3. *If $\mathbb{L}$ has nonconstant S-units and $g > 0$, then either there is an integer $r > 1$ such that $r \mid h_p$ for all primes p at which $\mathcal{C}$ has good reduction or h_p is even for all odd primes p at which $\mathcal{C}$ has good reduction.*

In order to use Proposition 6.3 in our search for families of units, we must calculate the class numbers h_p for function fields arising from the families of cyclic polynomials we studied in Section 2. (Here we name the parameter t instead of n.)

Let m be an odd prime, $\alpha = \beta + t\gamma$ with $\beta, \gamma \in \mathbb{Z}[\zeta_m] - \{0\}$ such that $q = N_{\mathbb{K}[\zeta_m]/\mathbb{K}}(\alpha)$ is irreducible in D', and $C = [c_{i,j}]$ the $m \times m$ matrix, with entries in D', defined in Section 2 by formulas (2–3) and (2–5) (which can be easily calculated using the program in [Thaine 01]). We have that $\mathbb{K}[C]/\mathbb{K}$ is a cyclic field extension.

Let $M \in \mathbb{K}[C] - \mathbb{K}$ and $f(t, X)$ the characteristic polynomial of M over $\mathbb{K}$. Then $f(t, X) \in D'[X]$ is a cyclic polynomial of degree m (we can easily find M such that $f(t, X) \in D[X]$). From now on we will consider only such polynomials $f(t, X)$ and the corresponding curves $\mathcal{C} : f(t, x) = 0$. Observe that $\mathbb{L}$ is $\mathbb{K}$-isomorphic to $\mathbb{K}[C]$.

We start by calculating the genus g of $\mathbb{L}/\mathbb{K}$. We have that q is the only prime of $\mathbb{K}$ that is ramified in $\mathbb{L}$, and its degree is $m - 1$ (since we are assuming that m is prime). By the formula in [Stichtenoth 93, Corollary III.5.6], we have that $2g - 2 = -2m + (m - 1)(m - 1)$. So $g = (m^2 - 4m + 3)/2$. This gives $g = 0$ for $m = 3$, $g = 4$ for $m = 5$, $g = 12$ for $m = 7$, and $g = 40$ for $m = 11$.

Let p be a prime at which $\mathcal{C}$ has good reduction; denote by $\mathbb{L}_p$ the function field of $\mathcal{C}_p$ over $\mathbb{F}_p$ and by $\mathbb{L}_{p^k}$ the constant field extension of $\mathbb{L}_p$ of degree k (i.e., $\mathbb{L}_{p^k} = \mathbb{L}_p\mathbb{F}_{p^k}$). Let $Z(t)$ be the zeta function of $\mathbb{L}_p/\mathbb{F}_p$ and $L(t) = (1 - t)(1 - pt)Z(t)$. We have that $h_p = L(1)$ [Stichtenoth 93, Theorem V.1.15], and that $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}$, where $a_0 = 1$, $a_{2g} = p^g$, $a_{2g-i} = p^{g-i} a_i$, for $0 \le i \le g$, and the a_i can be obtained by the recursive rule [Stichtenoth 93, Corollary V.1.17] $a_0 = 1$ and $i a_i = S_i a_0 + S_{i-1} a_1 + \cdots + S_1 a_{i-1}$ for $i = 1, \ldots, g$, where $S_k = N_k - p^k - 1$ and N_k is the number of places of degree 1 of $\mathbb{L}_{p^k}/\mathbb{F}_{p^k}$.

By the above formulas, to calculate h_p we have only to find the numbers N_k for $k = 1, \ldots, g$. We calculate these numbers by studying ramification of primes in $\mathbb{L}_{p^k}/\mathbb{F}_{p^k}(t)$ with the use of Kummer's theorem [Stichtenoth 93, Theorem III.3.7]. Recall that the extension $\mathbb{L}_{p^k}/\mathbb{F}_{p^k}(t)$ is cyclic of degree m.

For $a \in \mathbb{F}_{p^k}$ denote by P_a the place of $\mathbb{F}_{p^k}(t)$ that is the zero of $(t - a)$. The finite places of degree 1 in $\mathbb{L}_{p^k}$ are above the places P_a, $a \in \mathbb{F}_{p^k}$. To see how these places factor, we must look at the factorization of the polynomials $f(a, X) \in \mathbb{F}_{p^k}[X]$. If this factorization has two or more distinct factors, then we can be sure that P_a splits in $\mathbb{L}_{p^k}$. If the polynomial $f(a, X)$ is an mth power, then (very likely) P_a totally ramifies in $\mathbb{L}_{p^k}$. If $f(a, X)$ is irreducible, then P_a is inert in $\mathbb{L}_{p^k}$.

Let l be the degree of the polynomial $f(t, X) \in \mathbb{F}_{p^k}[t, X]$. Let $s = 1/t$ and $Y = X/t$. In order to see how the place of $\mathbb{F}_{p^k}(t)$ at infinity factors in $\mathbb{L}_{p^k}$, we look at the factorization of $s^l f(1/s, Y/s)$, when $s = 0$, in $\mathbb{F}_{p^k}[Y]$.

Let A_k be the number of places (finite and infinite) of degree 1 of $\mathbb{F}_{p^k}(t)$ totally ramified in $\mathbb{L}_{p^k}$, B_k the number of places (finite and infinite) of degree 1 of $\mathbb{F}_{p^k}(t)$ splitting in $\mathbb{L}_{p^k}$, and C_k the number of places of degree 1 of $\mathbb{F}_{p^k}(t)$ inert in $\mathbb{L}_{p^k}$. Then $N_k = A_k + mB_k$ and $A_k + B_k + C_k = p^k + 1$.

Schoof's result follows from Propositions 6.1 and 6.3 and can be stated as follows: If for two odd primes p_1 and p_2 at which $\mathcal{C}$ has good reduction we have $\gcd(h_{p_1}, h_{p_2}) = 1$, or if $\mathcal{C}$ has good reduction at 2 and at an odd prime p and we have $\gcd(h_2, h_p) = 1$ and h_p is odd, then $\mathbb{L}$ has no nonconstant S-units, and certainly we are not going to find families of units by using such a curve $\mathcal{C}$. On the other hand, if for several primes p where $\mathcal{C}$ has good reduction the numbers h_p are divisible by a number $r > 1$, then it is worth searching for families of units arising from $\mathcal{C}$ (I found no such curve $\mathcal{C}$, apart from Emma Lehmer's, in the few examples I was able to calculate).

The following examples were calculated using the Maple system.[2]

Example 6.4. Let us consider first Emma Lehmer's polynomial. Let $m = 5$ and $\alpha = t + 2 + \zeta_5 + 2\zeta_5^2$. We get $q = t^4 + 5t^3 + 15t^2 + 25t + 25$. The characteristic poly-

[2]The program is available online (http://cicma.mathstat.concordia.ca/faculty/thaine/homepage.html).

nomial of $C - K^{-1}CK$ is

$$f(t,X) = X^5 - qX^3 - (t+2)qX^2 - tqX + q.$$

(We know immediately that a family of units can be obtained using f because $f(t,0) = q$, but we want to show how Schoof's method works when such a family indeed exists.)

The Jacobian of $f(t,x) = 0$ has a subgroup of order 71. This is apparent when we consider the reduced curves modulo p for several primes p. We have $g = 4$.

For $p = 2$, we have $A_1 = 0$, $B_1 = 1$, $C_1 = 2$; $A_2 = 0$, $B_2 = 1$, $C_2 = 4$; $A_3 = 0$, $B_3 = 4$, $C_3 = 5$; $A_4 = 4$, $B_4 = 5$, $C_4 = 8$. Hence, $S_1 = 2$, $S_2 = 0$, $S_3 = 11$, $S_4 = 12$, and we get

$$L_2(t) = 1+2t+2t^2+5t^3+11t^4+10t^5+8t^6+16t^7+16t^8.$$

So $h_2 = L_2(1) = 71$.

For $p = 3$, we have $A_1 = 0$, $B_1 = 1$, $C_1 = 3$; $A_2 = 0$, $B_2 = 1$, $C_2 = 9$; $A_3 = 0$, $B_3 = 4$, $C_3 = 24$; $A_4 = 4$, $B_4 = 17$, $C_4 = 61$. Hence, $S_1 = 1$, $S_2 = -5$, $S_3 = -8$, $S_4 = 7$, and we get

$$L_3(t) = 1 + t - 2t^2 - 5t^3 + t^4 - 15t^5 - 18t^6 + 27t^7 + 81t^8.$$

So $h_3 = L_3(1) = 71$.

The curve $f(t,x) = 0$ has bad reduction at $p = 5$.

For $p = 7$, we have $A_1 = 0$, $B_1 = 2$, $C_1 = 6$; $A_2 = 0$, $B_2 = 20$, $C_2 = 30$; $A_3 = 0$, $B_3 = 62$, $C_3 = 282$; $A_4 = 4$, $B_4 = 432$, $C_4 = 1966$. Hence, $S_1 = 2$, $S_2 = 50$, $S_3 = -34$, $S_4 = -238$, and we get

$$L_7(t) = 1 + 2t + 27t^2 + 40t^3 + 281t^4 + 280t^5 + 1323t^6 + 686t^7 + 2401t^8.$$

So $h_7 = L_7(1) = 71^2$.

For $p = 11$, we have $A_1 = 4$, $B_1 = 2$, $C_1 = 6$; $A_2 = 4$, $B_2 = 28$, $C_2 = 90$; $A_3 = 4$, $B_3 = 272$, $C_3 = 1056$; $A_4 = 4$, $B_4 = 3024$, $C_4 = 11614$. Hence $S_1 = 2$, $S_2 = 22$, $S_3 = 32$, $S_4 = 482$, and we get

$$L_{11}(t) = 1 + 2t + 13t^2 + 34t^3 + 225t^4 + 374t^5 + 1573t^6 + 2662t^7 + 14641t^8.$$

So $h_{11} = L_{11}(1) = 5^2 \times 11 \times 71$. Likewise we get

$$h_{13} = 2^4 \times 11 \times 71,$$
$$h_{17} = 11 \times 61 \times 71,$$
$$h_{19} = 2^4 \times 5 \times 31 \times 71.$$

As we showed in Section 3, if $W = C - K^{-1}CK$, then the characteristic polynomial of $-K^{-2}WK^2W^{-1}$ is Lehmer's polynomial:

$$X^5 + t^2X^4 - (2t^3 + 6t^2 + 10t + 10)X^3 + (t^4 + 5t^3 + 11t^2 + 15t + 5)X^2 + (t^3 + 4t^2 + 10t + 10)X + 1.$$

I am grateful to the referee for pointing out that this is a modular curve of level 25, as in work of Darmon and Lecacheux.

Example 6.5. Let $m = 5$ and $\alpha = 1 + (\zeta_5 - \zeta_5^4)^3 t$. We get $q = 125t^4 + 50t^2 + 1$. The characteristic polynomial of C is

$$f(t,X) = X^5 + X^4 + (-50t^4 - 20t^2)X^3 + (-10t^4 - 4t^2)X^2 + (625t^8 + 300t^6 + 24t^4)X - 95t^8 - 36t^6.$$

The Jacobian of $f(t,x) = 0$ has no nontrivial finite subgroups, since the greatest common divisor of the distinct h_p is 1; this curve is birationally equivalent to

$$x^5 + (t^3 - 5t^2 + 35t + 25)x^4 + (-4t^5 + 16t^4 - 120t^3 + 240t^2 + 700t)x^3 + (-32t^6 - 128t^5 - 960t^4 - 1920t^3 + 5600t^2)x^2 + (-512t^6 - 2560t^5 - 17920t^4 + 12800t^3)x - (8t)^5 = 0.$$

We have $g = 4$.

For $p = 3$, we have $A_1 = 0$, $B_1 = 2$, $C_1 = 2$; $A_2 = 0$, $B_2 = 4$, $C_2 = 6$; $A_3 = 0$, $B_3 = 2$, $C_3 = 26$; $A_4 = 4$, $B_4 = 16$, $C_4 = 62$. Hence $S_1 = 6$, $S_2 = 10$, $S_3 = -18$, $S_4 = 2$, and we get

$$L_3(t) = 1 + 6t + 23t^2 + 60t^3 + 121t^4 + 180t^5 + 207t^6 + 162t^7 + 81t^8.$$

So $h_3 = L_3(1) = 29^2$.

For $p = 7$, we have $A_1 = 0$, $B_1 = 4$, $C_1 = 4$; $A_2 = 0$, $B_2 = 14$, $C_2 = 36$; $A_3 = 0$, $B_3 = 40$, $C_3 = 304$; $A_4 = 4$, $B_4 = 538$, $C_4 = 1860$. Hence $S_1 = 12$, $S_2 = 20$, $S_3 = -144$, $S_4 = 292$, and we get

$$L_7(t) = 1 + 12t + 82t^2 + 360t^3 + 1131t^4 + 2520t^5 + 4018t^6 + 4116t^7 + 2401t^8.$$

So $h_7 = L_7(1) = 11^4$.

Example 6.6. Let $m = 5$ and $\alpha = t + (1 - \zeta_5)^2\zeta_5$. We get $q = t^4 + 10t^2 + 25t + 25$. The characteristic polynomial

of $C - K^{-2}CK^2$ is

$$f(t,X) = X^5 - qX^3 + (2t+2)qX^2 + (-t^2-3t)qX + (t^2-t-1)q.$$

The Jacobian of $f(t,x) = 0$ has no nontrivial finite subgroups, since the greatest common divisor of the distinct h_p is 1, but this is not apparent for small values of p. We have $g = 4$.

The curve $f(t,x) = 0$ has bad reduction at $p = 5$ and at $p = 11$, and we have $h_2 = 11^2$, $h_3 = 2^4 \times 11$, and $h_7 = 11 \times 251$; but unfortunately, $h_{13} = 34141$, a prime number.

Example 6.7. Let $m = 7$ and $\alpha = t + (1-\zeta_7)^2$. We get

$$q = t^6 + 7t^5 + 21t^4 + 35t^3 + 49t^2 - 49t + 49.$$

The characteristic polynomial of $C - K^{-3}CK^3$ is

$$\begin{aligned} f(t,X) = {} & X^7 - qX^5 + (-t^2-4t+2)qX^4 \\ & + (-4t^3-2t^2+5t+8)qX^3 \\ & + (-5t^4+11t^3+34t-21)qX^2 \\ & + (-2t^5+16t^4-6t^3+44t^2-42t-7)qX \\ & + (6t^5-3t^4+19t^3-19t^2-35t+31)q. \end{aligned}$$

The Jacobian of $f(t,x) = 0$ has no nontrivial finite subgroups, since the greatest common divisor of the distinct h_p is 1. We have $g = 12$, $h_2 = 7 \times 11677$, and $h_3 = 2^9 \times 3137$.

Example 6.8. (Hashimoto and Hoshi's polynomial.) Let $m = 7$ and

$$\alpha = t - 2 + (1-\zeta_7)(1-\zeta_7^3)(1+\zeta_7+\zeta_7^3).$$

We get

$$q = t^6 + 2t^5 + 11t^4 + t^3 + 16t^2 + 4t + 8.$$

Let $W = C - K^{-2}CK^2$. The characteristic polynomial of $tK^{-2}WK^2W^{-1}$ is

$$\begin{aligned} f(t,X) = {} & X^7 + (t^3+t^2+5t+6)X^6 \\ & + (9t^3+9t^2+24t+12)X^5 \\ & + (-t^7-t^6-9t^5+5t^4+15t^3 \\ & + 22t^2+36t+8)X^4 \\ & + (-t^8-5t^7-12t^6-24t^5+6t^4-2t^3+20t^2 \\ & + 16t)X^3 \\ & + (-2t^8-7t^7-19t^6-14t^5-2t^4-8t^3+8t^2)X^2 \\ & + (-t^8-4t^7-8t^6-4t^4)X - t^7. \end{aligned}$$

The curve $f(t,x) = 0$ has bad reduction at $p = 2$. We have $g = 12$ and $h_3 = 17865037$, a prime number. We were not able to calculate h_5 in a reasonable amount of time, but it seems unlikely that all h_p have that large a common prime factor.

ACKNOWLEDGMENTS

Part of the research for this article was done during a sabbatical leave at the University of Rome "Tor Vergata," at Paderborn University, and at the Universidad del Pais Vasco. I am grateful to my colleagues in those universities for their hospitality and valuable comments, in particular to René Schoof, Preda Mihailescu, Jesús Gómez Ayala, and Rosario Clement. I also thank Masanari Kida for showing me some material that I used in the preparation of this article, and Javier Thaine for helping me to improve a Maple program to calculate some examples.

This work was supported in part by a grant from NSERC.

REFERENCES

[Hashimoto and Hoshi 05] K. Hashimoto and A. Hoshi. "Families of Cyclic Polynomials Obtained from Geometric Generalization of Gaussian Period Relations." *Math. Comp.* 74 (2005), 1519–1530.

[Katz 81] N. Katz. "Galois Properties of Torsion Points on Abelian Varieties." *Invent. math.* 62 (1981), 481–502.

[Lehmer 88] E. Lehmer. "Connection between Gaussian Periods and Cyclic Units." *Math. Comp.* 50 (1988), 535–541.

[Mazur 86] B. Mazur. "Arithmetic on Curves." *Bull. Amer. Math. Soc.* 14:2 (1986), 207–259.

[Poonen 96] B. Poonen. "Computational Aspects of Curves of Genus at Least 2." *ANTS-II, Talence, France, Lecture Notes in Computer Science* 1122 (1996), 283–306.

[Schoof and Washington 88] R. Schoof and L. Washington. "Quintic Polynomials and Real Cyclotomic Fields with Large Class Numbers." *Math. Comp.* 50 (1988), 543–556.

[Stichtenoth 93] H. Stichtenoth. *Algebraic Function Fields and Codes*. New York: Springer-Verlag, 1993.

[Thaine 01] F. Thaine. "Jacobi Sums and New Families of Irreducible Polynomials of Gaussian Periods." *Math. Comp.* 70:236 (2001), 1617–1640.

[Thaine 04] F. Thaine. "Cyclic Polynomials and the Multiplication Matrices of Their Roots." *J. Pure Appl. Algebra* 188 (2004), 247–286.

[Thaine 05] F. Thaine. "Finding Families of Units of Cyclic Fields." *Algebraic Number Theory and Related Topics, RIMS Kokyuroku* 1451 (2005), 207–215.

[Washington 90] "Abelian Number Fields of Small Degree." In *Proc. KAIST Math. Workshop, 5, Korea Adv. Sci. Tech., Taejon*, pp. 63–78, 1990.

Francisco Thaine, Department of Mathematics and Statistics–CICMA, Concordia University, 1455, de Maisonneuve Blvd. W., Montreal, Quebec, H3G 1M8, Canada (ftha@alcor.concordia.ca)

Received February 16, 2007; accepted in revised form January 23, 2008.