UNIMODULAR INTEGER CIRCULANTS

J. E. CREMONA

Dedicated to the memory of R.W.K.Odoni, 1947–2002

Abstract. We study families of integer circulant matrices, and methods for determining which are unimodular. This problem arises in the study of cyclically presented groups, and leads to the following problem concerning polynomials with integer coefficients: given a polynomial $f(x) \in \mathbb{Z}[x]$: determine all those $n \in \mathbb{N}$ such that $\mathrm{Res}(f(x), x^n - 1) = \pm 1$. In this paper we describe methods for resolving this problem, including a method based on the use of Strassman's Theorem on p-adic power series, which are effective in many cases. The methods are illustrated with examples arising in the study of cyclically presented groups and further examples which illustrate the strengths and weaknesses of the methods for polynomials of higher degree.

1. Statement of the problem and preliminary results

In the study of cyclically presented groups (see [8], [6], [7], [17], and [10, Chapter 16]), the following problem arises. Let $f = \sum_{i=0}^{d} a_i x^i$ be a polynomial of degree d with integer coefficients. Set $a_i = 0$ for $i > d$. For each $n > d$ we may form the circulant matrix $M_n(f)$ of size n whose first row is $(a_0, a_1, \ldots, a_{n-1})$.

Problem A. Given $f \in \mathbb{Z}[x]$, determine all $n > \deg(f)$ such that $\det M_n(f) = \pm 1$.

We see below that this is essentially equivalent to the following problem about integer polynomials.

Problem B. Given $f \in \mathbb{Z}[x]$, determine all $n \in \mathbb{N}$ such that $\mathrm{Res}(f(x), x^n - 1) = \pm 1$.

In this section we give some elementary preliminary results, most of which may be found in [10, Chapter 16] and [14], starting with the reduction of Problem A to Problem B in Lemma 1. In the subsequent sections we describe two methods for solving the problem: the first only requires the use of approximations to the complex roots of f, and is guaranteed to work provided that none of these roots lie on the unit circle; the second uses Strassman's Theorem on p-adic power series. The latter has been found to work in practice, at least for polynomials whose degree is small; further remarks on its general effectiveness will be made later. We also discuss the question of how to determine for a given integer polynomial, whether or not any of its complex roots do lie on the unit circle, and give a simple method for this.

Clearly, for there to exist any solutions to either problem, a necessary condition is that the a_i are coprime, *i.e.*, that f is primitive; we will therefore often assume this.

2000 *Mathematics Subject Classification.* 11C08,11C20,15A36.

Key words and phrases. unimodular matrices, circulants.

We also fix the following notation for the rest of the paper: $f(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ has degree $d \geq 1$ and leading coefficient a_d, with roots β_i for $1 \leq i \leq d$ (counted with multiplicity). Thus $f(x) = a_d \prod_{i=1}^{d}(x - \beta_i)$. The β_i will be taken to lie in $\mathbb{C}$ in Section 2, and in $\mathbb{Q}_p$ for a suitable prime p in Section 3; for now we do not need to be specific and can regard them as lying in some abstract splitting field for f.

The first result appears in Theorem 2 and equations (10) and (13) of [10, Chapter 16], and also in [14, Lemma 2.1].

Lemma 1. *Let $f(x) \in \mathbb{Z}[x]$ have degree d and leading coefficient a_d, with roots β_i for $1 \leq i \leq d$ (counted with multiplicity). Then*

$$\det M_n(f) = \mathrm{Res}(f, x^n - 1) = (-1)^{nd} a_d^n \prod_{i=1}^{d} (\beta_i^n - 1).$$

Proof. Well-known properties of circulants and resultants give that

$$\det M_n(f) = \prod_{\zeta:\zeta^n=1} f(\zeta) = \mathrm{Res}(f, x^n - 1) = (-1)^{nd} a_d^n \prod_{i=1}^{d} (\beta_i^n - 1).$$

□

We now define[1]

$$B(f, n) = a_d^n \prod_{i=1}^{d} (\beta_i^n - 1).$$

Then for $n > \deg(f)$ we have $B(f, n) = \pm \det M_n(f)$, but $B(f, n)$ is defined for all integers n, positive or negative (provided that $f(0) \neq 0$); Problem B is to determine all positive integers n such that $B(f, n) = \pm 1$, and a complete solution to Problem B for a given polynomial will also give a complete solution to Problem A. It will be necessary to consider negative n below when we apply p-adic methods.

Corollary. *If f has no cyclotomic factors then $B(f, n) \neq 0$ for all n.*

Corollary. *Let $m, n \in \mathbb{N}$. If $m \mid n$ then $B(f, m) \mid B(f, n)$. Hence, if n is a solution to Problem B then so is every positive divisor of n. In particular, if $f(1) \neq \pm 1$ then there are no solutions, since $B(f, 1) = \pm \mathrm{Res}(f(x), x - 1) = \pm f(1)$, and if $f(-1) \neq \pm 1$ then there are no even solutions, since $B(f, 2) = \pm \mathrm{Res}(f(x), x^2 - 1) = \pm f(1) f(-1)$.*

For $m \geq 1$ let $\Phi_m(x)$ denote the mth cyclotomic polynomial, which is a monic irreducible polynomial of degree $\varphi(m)$. For convenience, we will say that f is cyclotomic if $f = \pm\Phi_m$ for some $m \geq 1$. Clearly, if f is cyclotomic then $B(f, n)$ is periodic (of period dividing $\varphi(m)$). Algorithms exist (see [1]) to check whether an irreducible f is cyclotomic; a recursive test is given (for monic irreducible f) by

$$\begin{aligned} f \text{ is cyclotomic} \iff \quad & \text{either} \qquad f(x) = g(x^2) \quad \text{with } g \text{ cyclotomic}, \\ & \text{or} \qquad f(x) \mid f(x^2) f(-x^2). \end{aligned}$$

Alternatively, if f is monic and irreducible then it is cyclotomic if and only if all its roots lie on the unit circle, which may be tested using the methods of Section 2. This follows from Kronecker's Theorem that the only algebraic integers all of whose conjugates have modulus 1 are the roots of unity.

[1] In [14] the notation was $R_n(f)$.

Lemma 2. $B(fg,n) = B(f,n)B(g,n)$.

Proof. Clear from the definition. □

Corollary. *For $n \geq 1$, $B(f,n) = \pm 1$ if and only if $B(g,n) = \pm 1$ for all irreducible g dividing f.*

Proof. Clear from Lemma 2 and the fact that $B(f,n) \in \mathbb{Z}$ for $n \geq 1$. □

The factorization $x^n - 1 = \prod_{d|n} \Phi_d(x)$ implies the following.

Lemma 3. *For $n \geq 1$, $B(f,n) = \prod_{d|n} \mathrm{Res}(f, \Phi_d)$.*

Corollary. *For $f(x) \in \mathbb{Z}[x]$ and $n \geq 1$, the following are equivalent:*

1. $B(f,n) = \pm 1$;
2. $\mathrm{Res}(f, \Phi_d) = \pm 1$ *for all* $d \mid n$;
3. $f(\zeta_d)$ *is a unit in the ring* $\mathbb{Z}[\zeta_d]$ *for all* $d \mid n$, *where* ζ_d *denotes a primitive* d*th root of unity;*
4. $\mathrm{Res}(f, x^n - 1) = \pm 1$;
5. $f \pmod{x^n - 1}$ *is a unit in the ring* $\mathbb{Z}[x]/(x^n - 1)$.

Proof. (1) $\iff$ (2) follows from Lemma 3, and (1) $\iff$ (4) from Lemma 1. (2) $\iff$ (3) since $\mathrm{Res}(f, \Phi_d) = N_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(f(\zeta_d))$. (4) $\implies$ (5) since there exist polynomials $g, h \in \mathbb{Z}[x]$ such that $\mathrm{Res}(f, x^n - 1) = fg + (x^n - 1)h$, while (5) $\implies$ (3) is clear. □

The characterization (5) above was attributed in [10] to Dunwoody. Note that it is not quite obvious that (3) and (5) are equivalent, since the rings $\mathbb{Z}[x]/(x^n - 1)$ and $\oplus_{d|n}\mathbb{Z}[x]/(\Phi_d(x))$ are not isomorphic in general (though they certainly become so after inverting n).

The preceding Corollary and the Proposition below are also contained in [14, Theorem 1], as we now explain. Assume that $\deg(f) \geq 1$ and f is irreducible. Let ζ be the image of x in $\mathbb{Z}[x]/(x^n - 1)$, then Theorem 1(i) (op. cit.) states that $f(\zeta)$ is a zero-divisor if and only if $f = \pm\Phi_m$ for some divisor m of n, and Theorem 1(ii) states that the number of $n \geq 1$ such that $f(\zeta)$ is a unit (and hence such that $B(f,n) = \pm 1$) is finite unless $f(x) = \pm x$ or $f(x) = \pm\Phi_m(x)$ where $m > 1$ is not a prime power. We will return to the case of cyclotomic f in the last section of this paper.

From now on suppose that f is primitive and irreducible, and that $f \neq \pm x$, and we wish to determine the set of $n \in \mathbb{Z}$ such that $B(f,n) = \pm 1$. For any individual value of n the value of $B(f,n)$ may be easily computed, as for $n \geq 1$ we have $B(f,n) = \mathrm{Res}(f, x^n - 1)$, and $B(f,-n) = \pm(aa_0)^{-n}B(f,n)$. So in practice, when f is not cyclotomic, we can find small solutions to $B(f,n) = \pm 1$ by computation, and then try to prove that there are no more.

For each non-cyclotomic irreducible $f \neq \pm x$, the number of solutions to $B(f,n) = \pm 1$ is finite (and hence so is the number of solutions for any f with no cyclotomic factors). This is the content of the next result, which is however non-constructive and gives no bound on the number or size of solutions.

Proposition 1. *Let $f \in \mathbb{Z}[x]$ be irreducible, not equal to $\pm x$ and not cyclotomic. Then the set of integers n such that $B(f,n) = \pm 1$ is finite.*

Proof. Let β be a root of f and $K = \mathbb{Q}(\beta)$, which is a number field of degree $\deg(f)$. Let S be the finite set of primes of K dividing $a_0 a_d$ (recall that a_d is the leading coefficient of f and a_0 the constant coefficient). Then β is an S-unit; moreover the equation $B(f,n) = \pm 1$ implies that $N_{K/\mathbb{Q}}(\beta^n - 1) = \pm a_d^{-n}$, so that $\gamma = \beta^n - 1$ is also an S-unit. It is a classical result of Siegel that the equation $x + y = 1$ has only finitely many S-unit solutions, so there are only finitely many values in K that β^n may take. Since β is not a root of unity this implies that there are only finitely many possible values of n. □

Remark. Algorithms exist to find all solutions to S-unit equations; see, for example, [15]. In the case $S = \emptyset$ this is implemented in Magma[2], so when f is monic with $f(0) = \pm 1$ we may find all solutions this way. Note, however, that the algorithm requires us to find the unit group of the number field K, which can be time-consuming when K has large degree or discriminant. No implementations are known to the author for general S.

It should be possible, at least in principle, to use effective bounds on the number and height of solutions to S-unit equations to bound the solutions of our problem. We expect that these would not be practical except in small cases, and hence have developed alternative methods. To illustrate this approach, however, we present one example solved in this way. Let $f = x^6 + x^5 - x^4 - x^3 - x^2 + x + 1$, which is irreducible and not cyclotomic. Let $K = \mathbb{Q}(\beta)$ where β is a root of f; the unit group of K has rank 3. Using Magma's command `UnitEquation`, we find that the equation $x+y = 1$ has 126 solutions with x, y both units, and 8 of these have $x = \beta^n$ for some n. Specifically, for $n = \pm 1, \pm 3, \pm 13$ we have $B(f,n) = N_{K/\mathbb{Q}}(\beta^n - 1) = +1$ and for $n = \pm 2$ we have $B(f,n) = N_{K/\mathbb{Q}}(\beta^n - 1) = -1$.

We summaries this section in the following.

Theorem 1. *Let $f \in \mathbb{Z}[x]$ be non-constant, with no cyclotomic factors, and with $f(0) \neq 0$. Then the set of integers n such that $B(f,n) = \pm 1$ is finite, and hence the set of $n > \deg(f)$ for which $\det M_n(f) = \pm 1$ is also finite.*

The next two sections of the paper concern methods which may be applied, and have been found to be effective in most cases, to determine these finite sets for any given polynomial f. We also give examples, and will discuss the weaknesses of the methods.

We would like to thank Martin Edjvet for introducing the problem to us, and Sandro Mattarei and the anonymous referee for several helpful comments.

2. Method one: using complex roots

An elementary constructive method is possible when none of the complex roots of f lies on the unit circle, so we deal with this case first. Here our method is guaranteed to give the complete solution and hence may be termed an algorithm for the complete solution to the original problems.

We will assume that $f \in \mathbb{Z}[x]$ has no cyclotomic factors and that $f(0) \neq 0$. Below we will assume that f has no repeated roots, which is no loss since in practice we apply it to the irreducible non-cyclotomic factors of a given polynomial.

We first describe the method, and then discuss the question of how to decide whether a given polynomial satisfies this condition on its complex roots.

Proposition 2. *Let $f \in \mathbb{Z}[x]$ have leading coefficient $a = a_d > 0$, no repeated roots and no roots on the unit circle. Assume that $a_0 = f(0) \neq 0$. Set*

$$S = \{\beta \in \mathbb{C} \mid f(\beta) = 0, |\beta| < 1\}, s = \#S$$
$$R = \{\beta \in \mathbb{C} \mid f(\beta) = 0, |\beta| > 1\}, r = \#R.$$

Let n_0 be an integer such that

$$n_0 \geq \begin{cases} \max\left(\dfrac{s\log 2}{\log a}, \max\limits_{\beta\in S}\left\{\dfrac{\log 2}{-\log|\beta|}\right\}\right) & \text{if } r = 0 \\ \max\left(\max\limits_{\beta\in S}\left\{\dfrac{\log 2}{-\log|\beta|}\right\}, \max\limits_{\beta\in R}\left\{\dfrac{\log c}{\log|\beta|}\right\}\right) & \text{if } r > 0 \end{cases}$$

where $c = 2^{s/r} + 1$. Then $B(f, n) = \pm 1 \implies n \leq n_0$.

Proof. First note that if $r = 0$ then all roots have modulus less than one, so

$$a > a\prod|\beta| = |f(0)| \geq 1,$$

making the definition of n_0 valid since then $\log a \neq 0$.

Suppose that $r = 0$. Then for $n > n_0$ we have

$$n > s\log 2/\log a \implies a^n > 2^s;$$

also, for all roots β,

$$n \geq -\log 2/\log|\beta| \implies |\beta^n| \leq \frac{1}{2} \implies |\beta^n - 1| \geq \frac{1}{2}.$$

Hence for $n > n_0$ we have $\prod|\beta^n - 1| \geq 2^{-s} > a^{-n}$, so that $|B(f, n)| > 1$ as required.

Next suppose that $r > 0$ and let $n > n_0$. As before, we have $\prod_{\beta\in S}|\beta^n - 1| \geq 2^{-s}$. Now for $\beta \in R$ we have

$$|\beta^n| > |\beta|^{n_0} \geq c \geq 2^{s/r} + 1 \implies |\beta^n - 1| > 2^{s/r},$$

so that $\prod_{\beta\in R}|\beta^n - 1| > 2^s$. Hence $\prod_{\beta\in R\cup S}|\beta^n - 1| > 1 \geq a^{-n}$, so again we have $|B(f, n)| > 1$. □

Thus, for polynomials with no roots on the unit circle, we first compute n_0 as in the Proposition, using approximations to the roots of f, and then check the values of $B(f, n)$ for $0 < n \leq n_0$ to find all solutions $n \in \mathbb{N}$ to $B(f, n) = \pm 1$.

Detecting roots on the unit circle. In order to apply the preceding method, we need to have a reliable way to determine whether or not any of the complex roots of f lie on the unit circle, which does not rely on approximations. Clearly, numerical computation of approximations to the roots can establish that their moduli are not equal to 1, but cannot by itself prove that any root has modulus exactly 1.

We assume that f is primitive, irreducible, and that $\deg(f) \geq 2$; hence neither ± 1 is a root of f and also $f(0) \neq 0$. To any such polynomial f, we associate the "reverse" polynomial f^* defined by

$$f^*(x) = x^{\deg(f)} f(1/x)$$

whose coefficients are the same as those of f but in reverse order, and whose roots are the reciprocals of those of f. Our assumptions are satisfied by f^* if and only if they are satisfied by f. A polynomial satisfying $f = f^*$ is called *reciprocal*.

It has been observed elsewhere, for example in the study of Salem numbers (see [3, p. 316]) that if an irreducible integer polynomial has a root on the unit circle, then it must be reciprocal. For completeness we include one proof of this here.

Proposition 3. *Let $f \in \mathbb{Z}[x]$ be primitive, irreducible and of degree at least 2. If f has a root on the unit circle then $\deg(f)$ is even and f is reciprocal.*

Proof. Let $\alpha \in \mathbb{C}$ be a root of f with $|\alpha| = 1$. Then $\alpha^{-1} = \overline{\alpha}$ is also a root of f, so f and f^* are not coprime. Since f is irreducible, it follows that $f^* = cf$ for some constant c, and primitivity implies $c = \pm 1$. Now the roots of f come in reciprocal pairs (recall that ± 1 are not roots of f) so $\deg(f)$ is even, and consideration of the product of the roots shows that the leading and constant coefficients of f are equal, so $c = 1$ and f is reciprocal. □

Now let f be primitive, irreducible and reciprocal of even degree $2n$ and leading coefficient a. We may form[2] the so-called "trace polynomial" $R_f^0(t) \in \mathbb{Z}[t]$ of f, whose roots are of the form $\alpha + \alpha^{-1}$ for each pair of reciprocal roots $\{\alpha, \alpha^{-1}\}$ of f. To compute $R_f^0(t)$, first form the resultant

$$R_f(t) = \mathrm{Res}_x(f, x^2 - tx + 1) \in \mathbb{Z}[t],$$

which is a^2 times the product of $2n$ linear factors $t - (\alpha + \alpha^{-1})$, one for each root α of f; hence $R_f(t) = R_f^0(t)^2$ where the trace polynomial $R_f^0 \in \mathbb{Z}[t]$ has degree n and is a times the product of factors $t - (\alpha + \alpha^{-1})$, one for each reciprocal pair of roots $\{\alpha, \alpha^{-1}\}$ of f. Each pair of roots of f which are both conjugate and reciprocal, and hence which lie on the unit circle, corresponds to a unique real value of t in the open interval $(-2, 2)$ which is a root of R_f. The number of these can be obtained by the method of Sturm sequences.

Examples in low degree.

- $n = 1$, $f = a(x^2 + 1) + bx$: $R_f^0 = at + b$. This case is of course elementary, and the condition for the roots to be complex and hence both of modulus 1 is simply $b^2 < 4a^2$.
- $n = 2$, $f = a(x^4 + 1) + b(x^3 + x) + cx^2$: $R_f^0 = at^2 + bt + c - 2a$.
- $n = 3$, $f = a(x^6 + 1) + b(x^5 + x) + c(x^4 + x^2) + dx^3$:

$$R_f^0 = at^3 + bt^2 + ct + d - (3at + 2b).$$

Implementation.

(1) In `pari/gp` [18], if `f` is an integer reciprocal polynomial in the variable `x` then the command[3]

```
polsturm(factor(polresultant(f, x^2 - t*x + 1))[1,1], -2, 2)
```

returns the number of pairs of roots on the unit circle.

(2) In Maple™ [13] the syntax is

```
sturm(sturmseq(factors(resultant(f, x^2 - t*x + 1, x))[2][1][1], t), t, -2, 2);
```

Example: Let $f = 2x^6 - 3x^3 + 2$. Then $R_f^0(t) = 2t^3 - 6t - 3$, which has three real roots, all in the interval $(-2, 2)$; so the roots of f all have modulus 1.

[2]This terminology was introduced in [9], as was pointed out to us by the referee; but we have not seen the resultant formula for the trace polynomial elsewhere.

[3]It is more efficient to recover $R^0(t)$ from $R(t) = R^0(t)^2$ by computing $\gcd(R(t), R'(t))$, but this cannot be done in one line!

Further numerical examples. These examples come from [17]. In each case an irreducible reciprocal polynomial is given, followed by the number of conjugate pairs of roots on the unit circle.

f	#	f	#
$4x^2 - 7x + 4$	1	$3x^4 - 5x^2 + 3$	2
$3x^4 - x^3 - 3x^2 - x + 3$	2	$3x^4 - 2x^3 - x^2 - 2x + 3$	2
$3x^2 - 5x + 3$	1	$2x^4 + x^3 - 5x^2 + x + 2$	1
$2x^6 - 3x^3 + 2$	3	$2x^6 - x^4 - x^3 - x^2 + 2$	3
$2x^4 - 3x^2 + 2$	2	$2x^6 - x^5 - x^3 - x + 2$	3
$2x^4 - x^3 - x^2 - x + 2$	2	$2x^4 - x^3 - 3x^2 - x + 2$	1
$2x^4 - 2x^3 + x^2 - 2x + 2$	2	$2x^4 - 2x^3 - x^2 - 2x + 2$	1
$2x^2 - 3x + 2$	1	$2x^4 - 3x^3 + x^2 - 3x + 2$	1
$x^4 + 2x^3 - 5x^2 + 2x + 1$	1	$x^6 + x^5 - 3x^3 + x + 1$	1
$x^6 + x^5 - x^4 - x^3 - x^2 + x + 1$	2	$x^4 + x^3 - 3x^2 + x + 1$	1
$x^6 + x^4 - 3x^3 + x^2 + 1$	1	$x^6 - x^4 + x^3 - x^2 + 1$	2
$x^6 - x^4 - x^3 - x^2 + 1$	2	$x^6 - 2x^4 + x^3 - 2x^2 + 1$	1
$x^6 - x^5 - x^3 - x + 1$	2	$x^6 - x^5 - x^4 + x^3 - x^2 - x + 1$	2
$x^4 - x^3 - x^2 - x + 1$	1	$x^4 - 2x^3 + x^2 - 2x + 1$	1
$x^6 - 2x^5 + x^3 - 2x + 1$	2	$x^4 - 3x^3 + 3x^2 - 3x + 1$	1

3. Method two: using p-adic roots

We now describe a method which is applicable and works well in practice for any $f \neq \pm x$ with no cyclotomic factors, using p-adic analysis and p-adic approximations to the roots of f, instead of the complex roots. This method may be applied regardless of the size of the complex roots. The use of Strassman's Theorem (see [4, Theorem 4.1] or [15, Theorem II.5]) in this context was first suggested to us by Samir Siksek, though we later learnt that it had been proposed earlier as a general method by Odoni in [14]. In that paper, Odoni gives complete results for f of the form $x^n - x + 1$, but also proves finiteness results for the general case; he uses an alternative method from transcendence theory, but states clearly that for general f the so-called p-adic Skolem method is advantageous since Strassman's Theorem may be used to bound the solutions n. Here we follow this approach.

The strategy is as follows. Write $F^{\pm}(n) = B(f, n) \pm 1$. We deal with each sign separately. Suppose we have a small (finite) set of solutions n_i to $F^+(n) = 0$ and we wish to show that there are no more. We choose a prime number p satisfying a number of technical conditions (given below) and such that the n_i are in different residue classes modulo $p - 1$. We then try to use p-adic analysis to show first that for each i, the number of $n \in \mathbb{Z}_p$ satisfying $F^+(n) = 0$ and $n \equiv n_i \pmod{p-1}$ is exactly 1; and then, for all n_0 such that $n_0 \not\equiv n_i \pmod{p-1}$ for all i, that the number of $n \in \mathbb{Z}_p$ satisfying $n \equiv n_0 \pmod{p-1}$ is 0. Similarly for $F^-(n)$.

Let $f \in \mathbb{Z}[x]$ be as above, with degree d, leading coefficient $a = a_d$ and constant coefficient a_0. As usual we assume that $a_0 \neq 0$. Let $p \geq 5$ be a prime number not dividing aa_0, such that f splits into d linear factors modulo p. The existence of such a prime (and in fact infinitely many of them) is guaranteed by the Chebotarev Density theorem. Let β_i for $1 \leq i \leq d$ be the roots of f in $\mathbb{Q}_p$ (which exist by Hensel's Lemma); in fact each $\beta_i \in \mathbb{Z}_p^*$, since $p \nmid aa_0$. We will only need the values of β_i to a finite p-adic precision.

We now have $F^{\pm}(n) = a^n \prod(\beta_i^n - 1) \pm 1$. Let e be the least positive integer such that $a^e \equiv \beta_i^e \equiv 1 \pmod{p}$ for all i; by Fermat's Little Theorem, $e \mid p-1$. There are advantages in taking the smallest exponent rather than $p-1$ (see Example 2 below). The residues modulo p of a^n and each β_i^n, and hence of $F^{\pm}(n)$, only depend on $n \pmod{e}$; we will consider each residue class $n \equiv r \pmod{e}$ separately.

If $F^{\pm}(r) \not\equiv 0 \pmod{p}$ then certainly $F^{\pm}(n) \not\equiv 0$ for all $n \equiv r \pmod{e}$. So we may restrict our attention to one of the classes r modulo e (if any) for which $F^{\pm}(r) \equiv 0 \pmod{p}$. Fix such an r, and write $n = se + r$ with $s \in \mathbb{Z}$. The value of $G(s) = F^{\pm}(n) = a^{se+r} \prod(\beta_i^{se+r} - 1) \pm 1$ is given by a convergent p-adic power series in $\mathbb{Z}_p[s]$. Strassman's Theorem says that provided that this power series is not identically zero, $G(s)$ has only finitely many p-adic roots, with a simple bound for their number in terms of the p-adic valuations of the coefficients of the series. This often suffices in practice to show that the solutions we have are the only ones; but we emphasize that its efficacy relies both on first finding all the solutions, and also on finding a suitable prime; the latter is not trivial when f has large degree, as we will illustrate in Example 5 below.

For convenience we state Strassman's Theorem here in the form in which we will use it. We denote by v_p the additive valuation on $\mathbb{Q}_p$, normalised so that $v_p(p) = 1$, and put $v_p(0) = \infty$.

Theorem 2 (Strassman's Theorem)**.** *Let c_n for $n \geq 0$ be a sequence in $\mathbb{Q}_p$, not all zero, such that $c_n \to 0$ as $n \to \infty$. Then the power series $g(s) = \sum_{i=0}^{\infty} c_i s^i$, which converges for all $s \in \mathbb{Z}_p$, has at most N zeros in $\mathbb{Z}_p$, where*

$$v_p(c_N) = \min_i v_p(c_i) \quad \textit{and} \quad v_p(c_i) > v_p(c_N) \ \ (\forall i > N).$$

Note that since f has no cyclotomic factors, we have $\beta_i^r \neq 1$ for all r and $G(0) \neq \pm 1$. We set

$$c(r) = (a^e - 1) + \sum_{i=1}^{d} \frac{\beta_i^r(\beta_i^e - 1)}{(\beta_i^r - 1)}. \tag{1}$$

Proposition 4. *With notation as above, let $c = c(r)$. Then $G(s) = F^{\pm}(n) = \sum_{i=0}^{\infty} c_i s^i \in \mathbb{Z}_p[[s]]$ where*

$$\begin{aligned} c_0 &= G(0) = F^{\pm}(r); \\ c_1 &\equiv (c_0 \mp 1)c \pmod{p^2}; \\ c_i &\equiv 0 \pmod{p^2} \qquad \textit{for } i \geq 2. \end{aligned}$$

Proof. Since $F^{\pm}(r) \equiv 0 \pmod{p}$ we have $c_0 \equiv 0 \pmod{p}$.

By choice of e, we have $a^e = 1 + pb$ with $b \in \mathbb{Z}_p$, so

$$a^n = a^r(1+pb)^s = a^r \sum_{j=0}^{\infty} \binom{s}{j} p^j b^j,$$

where $\binom{s}{j} = s(s-1)\dots(s-j+1)/j!$. Now for $i \geq 2$ and $p \geq 5$ we have $i - v_p(i!) \geq 2$, hence

$$a^n \equiv a^r(1+pbs) \pmod{p^2}.$$

Similarly,

$$\beta_i^n \equiv \beta_i^r(1+p\delta_i s) \pmod{p^2}$$

where $\beta_i^e = 1 + p\delta_i$. It follows that, modulo p^2,

$$\begin{aligned} G(s) &\equiv a^n \prod_i (\beta_i^n - 1) \pm 1 \equiv a^r(1+pbs) \prod_i (\beta_i^r(1+p\delta_i s) - 1) \pm 1 \\ &\equiv a^r(1+pbs) \prod_i ((\beta_i^r - 1) + p\delta_i \beta_i^r s)) \pm 1 \\ &\equiv \pm 1 + a^r \prod_i (\beta_i^r - 1) + a^r ps \left[b \prod_i (\beta_i^r - 1) + \sum_i \beta_i^r \delta_i \prod_{j \neq i} (\beta_j^r - 1) \right] \\ &\equiv c_0 + (c_0 \mp 1)p \left[b + \sum_i \beta_i^r \delta_i / (\beta_i^r - 1) \right] s \\ &\equiv c_0 + (c_0 \mp 1) \left[(a^e - 1) + \sum_i \beta_i^r (\beta_i^e - 1)/(\beta_i^r - 1) \right] s \equiv c_0 + (c_0 \mp 1)cs. \end{aligned}$$

□

The following two special cases are of interest. In each case, we only need to know the roots of f modulo p^2, in order to determine the valuation of $c(r)$.

Firstly, suppose that we have a solution $n = r$ and wish to show that there are no more in its residue class modulo e.

Proposition 5. *Suppose that $F^{\pm}(r) = 0$ for some integer r. Let p be a prime satisfying the above hypotheses, let $\beta_i \in \mathbb{Z}_p^*$ for $1 \leq i \leq d$ be the roots of f and let $c = c(r)$. If $v_p(c) = 1$ then $F^{\pm}(n) \neq 0$ for all n such that $n \equiv r \pmod{e}$, $n \neq r$.*

Proof. Now $c_0 = 0$, so $G(s) = c_1 s + \sum_{j=2}^{\infty} c_j s^j$ where $v_p(c_j) \geq 2$ for $j \geq 2$ and $c_1 \equiv \mp c \pmod{p^2}$, so $v_p(c_1) = 1$. Strassman's Theorem implies that $s = 0$ is the only zero of $G(s)$ in $\mathbb{Z}_p$. □

Secondly, suppose that we wish to show that there are no solutions at all in some residue class r modulo e. This is clear when $F^{\pm}(r) \not\equiv 0 \pmod{p}$, so we may assume that $v_p(F^{\pm}(r)) \geq 1$; the following result applies when $v_p(F^{\pm}(r)) = 1$.

Proposition 6. *Suppose that for some integer r we have $v_p(F^{\pm}(r)) = 1$; that is, $F^{\pm}(r) \equiv 0 \pmod{p}$ but $F^{\pm}(r) \not\equiv 0 \pmod{p^2}$. Let p be a prime satisfying the above hypotheses, $\beta_i \in \mathbb{Z}_p^*$ for $1 \leq i \leq d$ the roots of f, and let $c = c(r)$. If $v_p(c) \geq 2$ then $F^{\pm}(n) \neq 0$ for all n such that $n \equiv r \pmod{e}$.*

Proof. Now we have $G(s) \equiv c_0 + c_1 s \pmod{p^2}$ in $\mathbb{Z}_p[[s]]$, where $c_0 = G(0) = F^{\pm}(r)$ has valuation 1 and $c_1 \equiv (c_0 \mp 1)c \pmod{p^2}$ with c as in the statement. Hence if $v_p(c) \geq 2$ then Strassman's Theorem implies that $G(s)$ has no zeroes in $\mathbb{Z}_p$. □

Example 1. Let $f = x^4 - 2x^3 + x^2 - 2x + 1$. Checking all n with $0 < |n| \leq 100$ we find that $B(f, n) = -1$ only for $n = \pm 1, \pm 7$ and $B(f, n) \neq 1$ for all n. (Note that $B(f, n)$ is an even function since f is reciprocal and monic).

Take $p = 23$; f has roots $5, 13, 14, 16 \pmod{23}$. The sequence $B(f, n) \pmod{23}$ is periodic with period 22, never equals $+1$ and equals -1 for $n \equiv \pm 1, \pm 7 \pmod{22}$ only. This already shows that $B(f, n) = +1$ has no solutions. We need to show that the only solutions with $n \equiv \pm 1 \pmod{22}$ are $n = \pm 1$, and that the only solutions with $n \equiv \pm 7 \pmod{22}$ are $n = \pm 7$.

By symmetry it suffices to consider $r = 1$ and $r = 7$; in each case we apply Strassman's Theorem to reach the desired conclusion. The roots of $f \pmod{23^2}$ are 97, 36, 60 and 338. When $r = 1$ we find that $c_0 = 0$ and $c_1 \equiv 23 \pmod{23^2}$ so $v_{23}(c_1) = 1$ are required. When $r = 7$ we again have $c_0 = 0$ and now $c_1 \equiv 207 \equiv 9{\cdot}23 \pmod{23^2}$, so again $v_{23}(c_1) = 1$.

Hence the only positive solutions are $n = 1$ and $n = 7$.

Example 2. Let $f = x^4 + x^3 - 3x^2 + x + 1$. Checking all n with $0 < |n| \le 100$ we find that $B(f, n) = +1$ only for $n = \pm 1$ and $B(f, n) \ne -1$ for all n. Working modulo $p = 67$, we may take $e = 33$ rather than 66, and our method shows that $B(f, n) \ne -1$ for all n, and $B(f, n) = +1$ only for $n \equiv \pm 1 \pmod{33}$. For $n \equiv \pm 1 \pmod{33}$ there is a unique p-adic solution, so $n = \pm 1$ are the only solutions in these residue classes, and it follows that $n = 1$ is the only positive solution to $B(f, n) = 1$.

Note that if we instead take $e = p - 1 = 66$, then we cannot show (using $p = 67$) that there are no solutions $n \equiv \pm 32 \pmod{66}$. Moreover, this particular polynomial f has the property that for *every* prime p such that f splits modulo p, its roots are always quadratic residues[4] and our method with $e = p - 1$ would not eliminate the residue classes $n \equiv \pm 1 + (p - 1)/2 \pmod{p - 1}$; hence the need to use the minimal exponent e as described above.

Example 3. Let $f = 2x^4 - x^3 - x^2 - x + 2$. Checking all n with $0 < |n| \le 100$ we find that $B(f, n) = +1$ for $n = 1$ only and $B(f, n) \ne -1$. We wish to show that $n = 1$ is the only (positive) solution to $B(f, n) = +1$. and that $B(f, n) = -1$ has no solutions. Note that $B(f, n)$ is no longer an even function since f is not monic.

Using $p = 59$ we can show that $B(f, n) \ne -1$ for all n, but cannot exclude the possibility of solutions to $B(f, n) = 1$ with $n \equiv 24, 36, 52 \pmod{58}$. Using $p = 139$ instead, we find that $n \equiv 1 \pmod{138}$ is the only solution to $B(f, n) \equiv 1 \pmod{139}$, and there is a unique solution in this residue class.

Examples 4 and 5. Let $f = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$. This is irreducible, not cyclotomic, and has four conjugate pairs of roots on the unit circle. Checking all n with $0 < |n| \le 200$ we find that $B(f, n) \ne +1$ and $B(f, n) = -1$ for $\pm n = 1, 2, 3, 5, 6, 7, 9, 10, 11, 13, 17, 18, 21, 23, 27, 29, 34, 37, 47, 63, 65, 74$. (This polynomial, famous for having the minimal known Mahler measure greater than 1, was found by D.H. Lehmer [11]: see [16] for more on this.)

The smallest prime modulo which f splits is $p = 11093$; using this, we can show that the above list is indeed the complete set of solutions. This computation took about 7 minutes with our `pari/gp` implementation of the p-adic method: of this, a few seconds was spent finding a suitable prime p, a few more on showing that the residue classes modulo $p-1$ containing known solutions contain no more solutions, and the remaining time showing that the other classes modulo $p-1$ do not contain any solutions.

At the referee's suggestion we also applied our method to the polynomial with second smallest known Mahler measure, namely $f(x) = x^{18}+x^{17}+x^{16}+x^{15}-x^{12}-x^{11}-x^{10}-x^9-x^8-x^7-x^6+x^3+x^2+x+1$. Checking $|n| < 1000$ reveals the following solutions: $B(f, n) = +1$ for $\pm n = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 23, 29, 37, 39, 45, 65, 91$, and $B(f, n) = -1$ for $\pm n = 2, 4, 6, 10, 14, 26, 28, 30, 34, 74$.

[4] One can show that each root β of f is a square in the splitting field of f (though not in $\mathbb{Q}(\beta)$), which explains this phenomenon.

The smallest prime p modulo which f splits is $p = 230186347$. Finding this prime took about six hours: we used a fairly naive search, testing all primes: to check that $x^p \equiv x \pmod{f, p}$ takes $O(\log(p))$ time.

Working modulo p we find that $B(f, n) \equiv 1 \pmod{p}$ if and only if n is in one of the 34 residue classes modulo $p - 1$ which contain known solutions, and using Proposition 5 we can then show quickly that there are no further solutions in these classes, thus solving the problem for sign $+1$. For sign -1, however, in addition to the 20 known residue classes of $n \pmod{p-1}$ such that $B(f, n) \equiv -1 \pmod{p}$, for which again we can prove that they contain no more solutions, there are four more residue classes giving solutions modulo p, namely $n \equiv \pm 11579318, \pm 57105438 \pmod{p-1}$; and these cannot be excluded by Proposition 6 since (in the notation used above) $v_p(c_1) = 1$. Hence Strassman's Theorem with this prime cannot exclude the possibility of their being more solutions to $B(f, n) = -1$, with n in these residue classes. This phenomenon is not rare, and occurred in many of our other examples, where we simply used another suitable prime where this problem did not arise.

In this example, finding a second candidate prime is quite time-consuming. However we were able to find a second prime modulo which f splits, namely $p = 1912762183$, and using this were able to verify that the lists of solutions to $B(f, n) = \pm 1$ are both complete with no further problems.

Note that the primes modulo which p splits are sparsely distributed: they have density $1/92897280$, or approximately 10^{-8}, see the next paragraph.

In order to handle polynomials of larger degree it would be desirable to extend the method in order to be able to make use of primes other than those modulo which $f(x)$ splits, since although the Chebotarev Density theorem guarantees that there infinitely many such, their density is small, namely $1/D$ where D is the degree of the splitting field of f (assuming f irreducible) which may therefore be as small as $1/d!$ where $d = \deg(f)$. In the degree 18 example of the previous paragraph, the Galois group of f has order $D = 92897280$ which is considerably smaller than $18! = 6402373705728000$. The 92897280th prime is 1886112211 which is about 8 times larger than the prime found.

Further numerical examples. In each case an irreducible reciprocal polynomial is given, followed by the complete list of solutions to $B(f, n) = +1$ and $B(f, n) = -1$. In each case, we give a prime such that the p-adic method is able to prove that the list of solutions given is complete.

f	$B(f,n)=+1$	p	$B(f,n)=-1$	p
$4x^2-7x+4$	1	17	–	19
$3x^4-x^3-3x^2-x+3$	1	31	–	31
$3x^2-5x+3$	1	23	–	5
$2x^6-3x^3+2$	$1,3$	67	–	487
$2x^4-3x^2+2$	$1,2$	11	–	11
$2x^4-x^3-x^2-x+2$	1	139	–	59
$2x^4-2x^3+x^2-2x+2$	$1,3$	37	–	29
$2x^2-3x+2$	1	11	–	113
$x^4+2x^3-5x^2+2x+1$	±1	23	–	23
$x^6+x^5-x^4-x^3-x^2+x+1$	$\pm1,\pm3,\pm13$	821	±2	1087
$x^6+x^4-3x^3+x^2+1$	±1	547	–	547
$x^6-x^4-x^3-x^2+1$	–	193	$\pm1,\pm2,\pm4,\pm7,\pm11,\pm37$	1303
$x^6-x^5-x^3-x+1$	–	941	$\pm1,\pm5,\pm13$	971
$x^4-x^3-x^2-x+1$	–	43	$\pm1,\pm3,\pm11$	43
$x^6-2x^5+x^3-2x+1$	–	239	$\pm1,\pm5,\pm7$	811
$3x^4-5x^2+3$	$1,2$	31	–	31
$3x^4-2x^3-x^2-2x+3$	1	59	–	59
$2x^4+x^3-5x^2+x+2$	$-3,1$	283	–	67
$2x^6-x^4-x^3-x^2+2$	$1,7$	1861	–	643
$2x^6-x^5-x^3-x+2$	$1,5$	107	–	107
$2x^4-x^3-3x^2-x+2$	–	199	$1,5$	43
$2x^4-2x^3-x^2-2x+2$	–	113	$1,3$	43
$2x^4-3x^3+x^2-3x+2$	–	433	1	331
$x^6+x^5-3x^3+x+1$	±1	607	–	607
$x^4+x^3-3x^2+x+1$	±1	67	–	67
$x^6-x^4+x^3-x^2+1$	$\pm1,\pm13,\pm17$	193	$\pm2,\pm4$	193
$x^6-2x^4+x^3-2x^2+1$	–	277	±1	523
$x^6-x^5-x^4+x^3-x^2-x+1$	–	643	$\pm1,\pm2,\pm5,\pm11$	643
$x^4-2x^3+x^2-2x+1$	–	23	$\pm1,\pm7$	23
$x^4-3x^3+3x^2-3x+1$	–	71	±1	71

4. The cyclotomic case

We now determine the value of $B(\Phi_m,n)=\mathrm{Res}(\Phi_m(x),x^n-1)$. In [14], Odoni already determines precisely those n for which $B(\pm\Phi_m,n)=\pm1$; here we determine all values of $B(\Phi_m,n)$. These can be determined using the known formula for $\mathrm{Res}(\Phi_m(x),\Phi_n(x))$ (see [12]): for $m>n$,

$$\mathrm{Res}(\Phi_m,\Phi_n)=\begin{cases}1 & \text{if } n\nmid m \text{ or } n\mid m \text{ and } m/n \text{ is not a prime power;}\\ p^{\phi(n)} & \text{if } m/n \text{ is a power of the prime } p.\end{cases}$$

Instead, we determine $B(\Phi_m,n)$ directly here. For fixed m, this is clearly periodic in n of period m. Note that for $m\ge3$ it is clear that $B(\Phi_m,n)=\prod(\beta^n-1)\ge0$, since the factors are in conjugate pairs, while $B(\Phi_1,n)=B(x-1,n)=0$ and $B(\Phi_2,n)=B(x+1,n)=1-(-1)^n$ for all $n\ge0$.

Theorem 3. *Let $m, n \geq 1$ and set $m = dm_1$ where $d = \gcd(m, n)$. Then*

$$B(\Phi_m, n) = \begin{cases} 0 & \text{if } m_1 = 1, \text{ i.e., if } m \mid n; \\ 1 & \text{if } m_1 > 1 \text{ and is not a prime power;} \\ p^{\phi(m)/\phi(m_1)} & \text{if } m_1 \text{ is a power of the prime } p. \end{cases}$$

The last exponent may also be written as $\phi(d)$ (when $p \nmid d$) or $\dfrac{p\phi(d)}{p-1}$ (when $p \mid d$).

Proof. Set $b(m, n) = B(\Phi_m, n)$. First we deal with the case $n = 1$:

$$b(m, 1) = \mathrm{Res}(\Phi_m(x), x - 1) = \Phi_m(1) = \begin{cases} 0 & \text{if } m = 1; \\ 1 & \text{if } m > 1 \text{ and is not a prime power;} \\ p & \text{if } m \text{ is a power of the prime } p. \end{cases}$$

This is well known in the theory of cyclotomic fields, and is a special case of the more general formula for $\mathrm{Res}(\Phi_m, \Phi_n)$ given above. The identity

$$\frac{x^m - 1}{x - 1} = \prod_{1 \neq d \mid m} \Phi_d(x),$$

when evaluated at $x = 1$, gives $m = \prod_{1 \neq d \mid m} b(d, 1)$, from which the result follows by induction.

Next observe that $b(m, n) = b(m, nn')$ when $\gcd(m, n') = 1$, since then as β runs through the primitive mth roots of unity, so does $\beta^{n'}$. This (together with periodicity) implies that $b(m, n) = b(m, d)$ where $d = \gcd(m, n)$.

Finally, if p is a prime dividing both m and n, we have

$$b(m, n) = \begin{cases} b(m/p, n/p)^p & \text{if } p^2 \mid m; \\ b(m/p, n/p)^{p-1} & \text{if } p^2 \nmid m. \end{cases}$$

This is because, as β runs over the primitive mth roots of unity, β^p runs over the primitive (m/p)th roots of unity either p or $p - 1$ times.

The given formula follows by repeated application of these. □

Corollary. *For $m \geq 2$ we have $\det M_n(\Phi_m) = B(\Phi_m, n) = +1$ if and only if $m/\gcd(m, n)$ is neither 1 nor a prime power, and $\det M_n(\Phi_m) \neq -1$ for all $n \geq 1$.*

Example. Let $m = 90$. Then $B(\Phi_{90}, n)$ is given by the following, in terms of $d = \gcd(90, n)$:

$$B(\Phi_{90}, n) = \begin{cases} 0 & \text{if } d = 90; \\ 1 & \text{if } d = 1, 2, 3, 5, 6, 9, 15; \\ 3^4 = 81 & \text{if } d = 10; \\ 5^6 = 15625 & \text{if } d = 18; \\ 3^{12} = 531441 & \text{if } d = 30; \\ 2^{24} = 16777216 & \text{if } d = 45. \end{cases}$$

Hence for $f = \Phi_{90}(x) = x^{24} + x^{21} - x^{15} - x^{12} - x^9 + x^3 + 1$, we have $\det M_n(f) = +1$ if and only if $\gcd(90, n) \in \{1, 2, 3, 5, 6, 9, 15\}$.

5. Further work

In [5] the Lehmer polynomial $f(x)$ of degree 10 used in Example 4 above was also studied, and a list was given of all the positive integers $m < 1000$ for which $\mathrm{Res}(f(x), \Phi_m(x)) = \pm 1$. The largest m listed is $m = 360$, and we have checked that there are no more solutions with $m < 10000$. It is natural to ask the following:

Problem C. Given $f(x) \in \mathbb{Z}[x]$, find all $m \in \mathbb{N}$ such that $\mathrm{Res}(f(x), \Phi_m(x)) = \pm 1$.

By Lemma 3 above it is clear that a solution to this problem would also provide a solution to both Problems A and B, but it is not immediately clear how to extend our methods to cover the problem. For example, applying the p-adic method would require treating $\Phi_m(\beta)$, for fixed $\beta \in \mathbb{Z}_p$, as a function of $m \in \mathbb{Z}_p$, which is certainly harder than the case $\beta^m - 1$ treated here.

References

[1] F. Beukers and C. J. Smyth. Cyclotomic points on curves. In *Number theory for the millennium, I (Urbana, IL, 2000)*, pages 67–85. A K Peters, Natick, MA, 2002.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] D. Boyd. Small salem numbers. *Duke Math. J.*, 44:315–328, 1977.

[4] J. W. S. Cassels. *Local fields*, volume 3 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1986.

[5] H. Cohen, L. Lewin, and D. Zagier. A sixteenth-order polylogarithm ladder. *Experiment. Math.*, 1(1):25–34, 1992.

[6] M. Edjvet. On irreducible cyclic presentations. *J. Group Theory*, 6(2):261–270, 2003.

[7] M. Edjvet and P. Hammond. On a class of cyclically presented groups. *Internat. J. Algebra Comput.*, 14(2):213–240, 2004.

[8] M. Edjvet, P. Hammond, and N. Thomas. Cyclic presentations of the trivial group. *Experiment. Math.*, 10(2):303–306, 2001.

[9] B. H. Gross and C. T. McMullen. Automorphisms of even unimodular lattices and unramified Salem numbers. *J. Algebra*, 257(2):265–290, 2002.

[10] D. L. Johnson. *Topics in the theory of group presentations*, volume 42 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1980.

[11] D. H. Lehmer. Factorization of certain cyclotomic functions. *Ann. of Math. (2)*, 34(3):461–479, 1933.

[12] S. Louboutin. Resultants of cyclotomic polynomials. *Publ. Math. Debrecen*, 50(1-2):75–77, 1997.

[13] M. B. Monagan, K. O. Geddes, K. M. Heal, G. Labahn, S. M. Vorkoetter, J. McCarron, and P. DeMarco. *Maple 10 Programming Guide*. Maplesoft, Waterloo ON, Canada, 2005.

[14] R. W. K. Odoni. Some Diophantine problems arising from the theory of cyclically-presented groups. *Glasg. Math. J.*, 41(2):157–165, 1999.

[15] N. P. Smart. *The algorithmic resolution of Diophantine equations: a computational cookbook*. Number 117 in London Mathematical Society Lecture Notes Series. Cambridge University Press, 1998.

[16] C. J. Smyth. The Mahler measure of algebraic numbers: a survey. In *Number theory and polynomials (University of Bristol, 3-7 April 2006), J. McKee and C.J. Smyth, eds.)* LMS Lecture notes (to appear).

[17] J. Swan. *Families of irreducible cyclically-presented groups*. PhD thesis, University of Nottingham, 2007.

[18] The PARI Group, Bordeaux. *PARI/GP, version* `2.4.1`, 2006. available from `http://pari.math.u-bordeaux.fr/`.

Mathematics Institute University of Warwick, Coventry, CV4 7AL, UK.
E-mail address: `J.E.Cremona@warwick.ac.uk`