Unimodular integer circulants associated with trinomials

Gerald Williams

May 8, 2009

Abstract

The $n \times n$ circulant matrix associated with the polynomial $f(t) = \sum_{i=0}^{d} a_i t^i$ (with $d < n$) is the one with first row $(a_0 \ldots a_d 0 \ldots 0)$. The problem as to when such circulants are unimodular arises in the theory of cyclically presented groups and leads to the following question, previously studied by Odoni and Cremona: when is $\text{Res}(f(t), t^{n-1}) = \pm 1$? We give a complete answer to this question for trinomials $f(t) = t^m \pm t^k \pm 1$. Our main result was conjectured by the author in an earlier paper and (with two exceptions) implies the classification of the finite Cavicchioli-Hegenbarth-Repovš generalized Fibonacci groups, thus giving an almost complete answer to a question of Bardakov and Vesnin.

1 Introduction

The $n \times n$ circulant matrix $M_n(f)$ associated with the polynomial $f(t) = \sum_{i=0}^{d} a_i t^i$ where $d < n$ and $a_i \in \mathbb{Z}$ is the one whose first row is $(a_0 \ldots a_d 0 \ldots 0)$. Well known properties of circulants and resultants give that $\det(M_n) = \text{Res}(f, t^{n-1})$. The question as to when $M_n$ is unimodular arises in the theory of cyclically presented groups and has been considered by Odoni [7] and Cremona [3].

For $n \geq 1$ define

$$R_n(f) = \prod_{\theta^n=1} f(\theta).$$

Our approach, as in [3],[7], is to work with $R_n(f)$ rather than with $M_n(f)$. It was shown in [3],[7] that, for $n > d$, $\det(M_n) = R_n(f)$ so it is enough to consider when $R_n(f) = \pm 1$. We note that $R_n(f)$ is defined for all $n \geq 1$ whereas $M_n(f)$ is only defined for $n > d$.

Briefly, the connection with cyclically presented groups is as follows. Fix a word $w(x_0, \ldots, x_{n-1})$ in generators $x_0, \ldots, x_{n-1}$ and let $\Gamma_n(w)$ be the group defined by the presentation with these $n$ generators and the $n$ relators

$$w(x_0, x_1, \ldots, x_{n-2}, x_{n-1}), w(x_1, x_2, \ldots, x_{n-1}, x_0), \ldots, w(x_{n-1}, x_0, \ldots, x_{n-3}, x_{n-2}).$$

If $a_i$ is the exponent sum of $x_i$ in $w(x_0, \ldots, x_{n-1})$ then $\Gamma_n(w)$ has infinite abelianization if and only if $R_n(f) = 0$ and is perfect if and only if $R_n(f) = \pm 1$ [5],[7]. Indeed $\Gamma_n(w)^{ab}$ has order $|R_n(f)|$ ([5, page 77]).
In this paper we consider trinomials \( f(t) = t^m \pm t^k \pm 1 \). When both signs are ‘+’ it is easy to deduce that \( R_n(f) \neq \pm 1 \). In the other three cases we can reduce to a polynomial of the form \( t^m - t^k + 1 \); moreover we may assume \( (n, m, k) = 1 \) (see Section 3). We note that Lemma 5 of [8] and Lemma 2.3 of [4] determine when \( R_n(t^m \pm tk \pm 1) = 0 \).

The Cavicchioli-Hegenbarth-Repovš generalized Fibonacci groups \( G_n(m, k) \) are the cyclically presented groups with generators \( x_1, \ldots, x_n \) and relators \( x_i x_{i+m} x_{i+k}^{-1} \) and these are our primary motivation for considering trinomials \( f(t) = t^m - t^k + 1 \).

Our main result is

**Main Theorem** Let \( n \geq 1 \) and \( f(t) = t^m - t^k + 1 \) where \( m, k \in \mathbb{Z} \) and \( (n, m, k) = 1 \). Then \( R_n(f) = \pm 1 \) if and only if \( (n, 6) = 1 \) and \( m = 2k \mod n \) or \( k = 0 \mod n \) or \( k = m \mod n \).

This was conjectured (in group theoretic terms) in [8] and is a natural generalization of a theorem of Odoni [7] which deals with the case \( k = 1 \). With the exception of two groups, the Main Theorem implies the classification of the finite groups \( G_n(m, k) \) (see [8]), thus giving an almost complete answer to a problem posed by Bardakov and Vesnin ([1, Question 1]).

**2 Preliminaries**

A number of equivalent characterizations of \( R_n(f) = \pm 1 \) were given in [3],[7]. We only need some of them:

**Lemma 2.1** ([3, 7]) For \( f \in \mathbb{Z}[t] \) and \( n \geq 1 \) the following are equivalent:

(a) \( R_n(f) = \pm 1 \);

(b) \( f(\zeta_d) \) is a unit in the ring \( \mathbb{Z}[\zeta_d] \) for all \( d|n \) where \( \zeta_d \) denotes a primitive \( d \)th root of unity;

(c) \( \text{Res}(f, t^n - 1) = \pm 1 \).

We record some properties of \( R_n \); those in Proposition 2.2 follow directly from its definition.

**Proposition 2.2** Let \( f, g \in \mathbb{Z}[t] \) and let \( n \geq 1 \). Then the following hold:

(a) \( R_n(fg) = R_n(f)R_n(g) \);

(b) \( R_n(t) = (-1)^{n+1} \);

(c) If \( m|n \) then \( R_m(f)|R_n(f) \).
Proposition 2.3 ([7]) Let \( f(t) = c \prod_{j=1}^{k} (t - \beta_j) \). Then

\[
R_n(f) = \left( (-1)^k c \right)^n \prod_{j=1}^{k} (\beta_j^n - 1).
\]

In [3] the expression \( c^n \prod_{j=1}^{k} (\beta_j^n - 1) \) was denoted \( B(f, n) \) and so \( R_n(f) = \pm B(f, n). \)

Proposition 2.4 Let \( f, F \in \mathbb{Z}[t] \) be polynomials such that \( f(t)^\alpha \). Then

\[
R_n(f) = \left( R_{n/(n,\alpha)}(F) \right)^{(n,\alpha)}.
\]

In particular \( R_n(t^m \pm t^k \pm 1) = (R_N(t^M \pm t^K \pm 1))^{(n,m,k)} \) where \( N = n/(n, m, k), M = m/(m, k), K = k/(m, k). \)

Proof
Let \( d = (n, \alpha) \). Then we have

\[
R_n(f) = \prod_{\theta^n=1} F(\theta^n) = \prod_{q=0}^{n-1} F(e^{2\pi i \alpha q/n}) = \prod_{q=0}^{n-1} F(e^{2\pi i \alpha q/(n/d)})
\]

which is equal to

\[
\left( \prod_{q=0}^{n/d-1} F(e^{2\pi i \alpha q/(n/d)}) \right)^d.
\]

so \( R_n(f) = (R_{n/d}(F))^d \). Now since \( (\alpha/d, n/d) = 1 \), for each \( q = 0, \ldots, (n/d - 1) \) there exists a unique \( Q = 0, \ldots, (n/d - 1) \) such that \( q(\alpha/d) = Q \mod n/d \). Hence

\[
\prod_{q=0}^{n/d-1} F(e^{2\pi i \alpha q/(n/d)}) = \prod_{Q=0}^{n/d-1} F(e^{2\pi i Q/(n/d)}) = \prod_{\phi^n=d=1} F(\phi) = R_{n/d}(F)
\]

so \( R_n(f) = (R_{n/d}(F))^d \).

To prove the last claim let \( f(t) = t^m \pm t^k \pm 1 \) and \( F(t) = t^M \pm t^K \pm 1 \). \( \square \)

Since \( (N, M, K) = 1 \), in considering when \( R_n(t^m \pm t^k \pm 1) = \pm 1 \) Proposition 2.4 allows us to assume that \( (n, m, k) = 1 \).

3 Properties of \( R_n(t^m \pm t^k \pm 1) \)

We have that \( R_1(t^m + t^k + 1) = 3 \) so by Proposition 2.2(c) \( R_n(t^m + t^k + 1) \neq \pm 1 \) for all \( n \). Thus we may assume that at least one of the signs is a ‘-’.

Proposition 3.1 (a) \( |R_n(t^m - t^k - 1)| = |R_n(t^k - t^m + 1)|; \)
(b) \(|R_n(t^m + t^k - 1)| = |R_n(t^{k-m} - t^k + 1)|\);

(c) \(|R_n(t^m - t^k + 1)| = |R_n(t^m - t^{m-k} + 1)|\).

**Proof**

(a) \(t^m - t^k - 1 = -(t^k - t^m + 1)\) so \(|R_n(t^m - t^k - 1)| = |R_n(t^k - t^m + 1)|\).

(b) \(t^m + t^k - 1 = t^k(t^{m-k} - t^{-k} + 1)\) so

\[
R_n(t^m + t^k - 1) = R_n(t^k)R_n(t^{m-k} - t^{-k} + 1) = (R_n(t))^k R_n(t^{k-m} - t^k + 1) = \pm R_n(t^{k-m} - t^k + 1).
\]

(c) \(t^m - t^k + 1 = t^m(t^{-m} - t^{k-m} + 1)\) so

\[
R_n(t^m - t^k + 1) = R_n(t^m)R_n(t^{-m} - t^{k-m} + 1) = (R_n(t))^m R_n(t^m - t^{m-k} + 1) = \pm R_n(t^m - t^{m-k} + 1).
\]

\[
\]

Other similar identities can be established. For example [2, Theorem 2] implies that if \(n, m, k, m', k'\) are integers such that \((n, m, k) = 1, (n, m', k') = 1, (n, k') = 1\) and \(m'(m-k) = mk'\mod n\) then \(R_n(t^m - t^k + 1) = \pm R_n(t^{m'} - t^{k'} + 1)\).

Parts (a) and (b) of Proposition 3.1 show that \(R_n(t^m - t^k - 1) = \pm R_n(t^{m'} - t^{k'} + 1)\) (for some \(m', k'\)) and \(R_n(t^m + t^k - 1) = \pm R_n(t^{m'} - t^{k'} + 1)\) (for some \(m', k'\)), so we only need consider \(R_n(f)\) for \(f(t) = t^m - t^k + 1\). Moreover, by Proposition 2.4 we may assume that \((n, m, k) = 1\). Proposition 3.1(c) shows that the roles of \(k\) and \((m-k)\) can be interchanged.

The next result was prompted by [1, Lemma 1.3].

**Proposition 3.2**

(a) If \((k, n) = 1\) then \(R_n(t^m - t^k + 1) = R_n(t^{m\ell} - t + 1)\) where \(\ell = k^{-1} \mod n;\)

(b) if \((m-k, n) = 1\) then \(R_n(t^m - t^k + 1) = R_n(t^{m\ell} - t + 1)\) where \(\ell = (m-k)^{-1} \mod n;\)

(c) if \((m, n) = 1\) then \(R_n(t^m - t^k + 1) = R_n(t - t^{k\ell} + 1)\) where \(\ell = m^{-1} \mod n.\)

**Proof**

(a) Let \(\phi = \theta^k\), then \(\theta = \phi^\ell\) so

\[
R_n(t^m - t^k + 1) = \prod_{\theta^n = 1} \theta^m - \theta^k + 1 = \prod_{\phi^n = 1} (\phi^k)^m - \phi + 1 = R_n(t^{m\ell} - t + 1).
\]
This follows from (a) by interchanging the roles of \( k \) and \((m - k)\).

Parts (a),(b) of Proposition 3.2 show that it is sometimes enough to consider the polynomials considered by Odoni [7] (that is, polynomials of the form \( t^m - t + 1 \)). When \( k = 0 \mod n \) or \( k = m \mod n \), it is clear that \( R_n(t^m - t^k + 1) = \pm 1 \). We can obtain the value of \( R_n \) in some other cases; for example, by Proposition 2.3 and Proposition 2.4 we have that \( R_n(t^0 - t^k + 1) = 2^{n/(n,k)} - 1 \). By [8, Lemma 3] we have

**Lemma 3.3** Suppose that \( n \) is even, \((m,k) = 1\) and either \( k = n/2 \mod n \) or \((m - k) = n/2 \mod n \). Then \( |R_n(t^m - t^k + 1)| = 2^{n/2} - (-1)^{m+n/2} \).

### 4 Proof of Main Theorem

Odoni proved the Main Theorem in the case \( k = 1 \): we summarize this result ([7, Theorem 2(ii),(iii)]) as

**Theorem 4.1 ([7])** Let \( n \geq 1 \) and \( f(t) = t^m - t + 1 \) where \( m \in \mathbb{Z} \). Then \( R_n(f) = \pm 1 \) if and only if \((n,6) = 1 \) and \( m = 2 \mod n \) or \( m = 1 \mod n \).

**Corollary 4.2** Let \( n \geq 1 \) and \( f(t) = t^m - t^k + 1 \) where \( m,k \in \mathbb{Z} \), \((n,m,k) = 1\) and suppose that either \((k,n) = 1\) or \((m - k,n) = 1\). Then \( R_n(f) = \pm 1 \) if and only if \((n,6) = 1 \) and \( m = 2k \mod n \) or \( k = 0 \mod n \) or \( k = m \mod n \).

**Proof**

By interchanging the roles of \( k \) and \((m - k)\) we may assume that \((k,n) = 1\). By Proposition 3.2(a) \( R_n(f) = R_n(t^{m \ell} - t + 1) \), where \( \ell = k^{-1} \mod n \). Now \( m \ell = 1, 2 \mod n \) if and only if \( m = k, 2k \mod n \), so the result follows from Theorem 4.1.

The following corollary generalizes [7, Lemma 3.2] to our setting.

**Corollary 4.3** Let \( n = p^u \) where \( p = 2 \) or \( 3 \), \( u \geq 1 \), and \( f(t) = t^m - t^k + 1 \) where \( m,k \in \mathbb{Z} \), \((n,m,k) = 1\). Then \( R_n(f) = \pm 1 \) if and only if \( k = 0 \mod n \) or \( k = m \mod n \).

**Proof**

The hypotheses imply that either \((k,n) = 1\) or \((m - k,n) = 1\) and so the result follows from Corollary 4.2.

The ‘if’ direction of the Main Theorem is straightforward to prove (see [8, Lemma 5]) so from now on we focus on the ‘only if’ direction.
Lemma 4.4 Let \( n = 2^r 3^s \geq 1 \) and \( f(t) = t^m - t^k + 1 \) where \( m, k \in \mathbb{Z} \), \((n, m, k) = 1\). If \( R_n(f) = \pm 1 \) then \( k = 0 \mod n \) or \( k = m \mod n \).

Proof
By Corollary 4.3 we may assume \( r \geq 1, s \geq 1 \). Now \( R_n(f) = \pm 1 \) implies \( R_{2^r}(f) = \pm 1 \) and so by Corollary 4.3 we have \( k = 0 \mod 2^r \) or \((m - k) = 0 \mod 2^r\). By interchanging the roles of \( k \) and \((m - k)\) we may assume that the first of these holds. We also have \( R_{3^s}(f) = \pm 1 \) so \( k = 0 \mod 3^s \) or \( k = m \mod 3^s \). In the first case we have \( k = 0 \mod n \), so assume the second.

Let \( d = 2 \cdot 3^s \). Now \( k \neq m \mod d \), for otherwise \( 2 \mid (n, m, k) = 1 \); thus \( k = m + d/2 \mod d \). It follows that \((m \mod d, k \mod d) = 1\) so Lemma 3.3 implies that \( R_d(f) \neq \pm 1 \) and hence \( R_n(f) \neq \pm 1 \).

Our next lemma generalizes \([7, \text{Lemma 3.3}]\) to our setting. We use ideas from the proof of that result.

Lemma 4.5 Let \( n = pq \) where \( q = 2 \) or \( 3 \) and \( p \geq 5 \) is prime, \( f(t) = t^m - t^k + 1 \) where \( m, k \in \mathbb{Z} \), \((n, m, k) = 1\). If \( R_n(f) = \pm 1 \) then \( k = 0 \mod n \) or \( k = m \mod n \).

Proof
By Corollary 4.2 we may assume \((k, n) > 1 \), \((m - k, n) > 1 \) so (since \((n, m, k) = 1\)) either \((q | k \text{ and } p | (m - k)) \) or \((p | k \text{ and } q | (m - k))\). By interchanging the roles of \( k \) and \((m - k)\) we may assume that the first case occurs, i.e. \( k = 0 \mod q \) and \((m - k) = 0 \mod p \). Moreover we may assume \( k \neq 0 \mod p \), \((m - k) \neq 0 \mod q \) for otherwise \( k = 0 \mod n \) or \((m - k) = 0 \mod n \).

If either \( p \) or \( q \) divides \( m \) then we get a contradiction to \((n, m, k) = 1\) so \((n, n) = 1\). Now by Proposition 3.2 \( R_n(f) = R_n(g) \) where \( g(t) = t^{m'} - t^{k'} + 1 \) where \( m' = 1 \), \( k' = km^{-1} \). The conditions on \( m, k \) imply \( k' = 0 \mod q \), \((m' - k') = 0 \mod p \), \((m' - k') \neq 0 \mod q \). When \( q = 2 \) we have that \((m' - k') = n/2 \mod n \) and since \((m', k') = 1 \) Lemma 3.3 implies \( R_n(g) \neq \pm 1 \).

Suppose then that \( q = 3 \) and \( R_n(g) = \pm 1 \). We have that \( k' = 1 \mod p \), \( k' = 0 \mod 3 \). Now \( R_{3p}(g) = \pm 1 \) so, writing \( \zeta_d \) for a primitive \( dt \)th root of unity, Lemma 2.1 implies that \( g(\theta) \) is a unit in \( \mathbb{Z}[\zeta_{3p}] \) whenever \( \theta \) is a primitive \((3p)\)th root of unity. In particular \( g(\zeta_p \zeta_d) = \zeta_p (\zeta_3 - 1) + 1 \) and \( g(\zeta_p \zeta_d^2) = \zeta_p (\zeta_3^2 - 1) + 1 \) are units in \( \mathbb{Z}[\zeta_p] \) and hence so is their product \( 3\zeta_p^2 - 3\zeta_p + 1 \), which must therefore also be a unit in \( \mathbb{Z}[\zeta_p] \). Let \( h(x) = 3x^2 - 3x + 1 \). Then \( h(1) = 1 \) and \( h(\zeta_p) \) are units in \( \mathbb{Z}[\zeta_p] \) so by Lemma 2.1 we have that \( R_p(h) = \pm 1 \). Now Proposition 2.3 implies that \( R_p(h) = 3^p(\beta_1^p - 1)(\beta_2^p - 1) \) where \( \beta_1, \beta_2 = 3^{-1/2} e^{\pm i\pi/6} \) are the roots of \( h \). But

\[ 3^p(\beta_1^p - 1)(\beta_2^p - 1) = 3^p + 1 \pm 3^{(p+1)/2} \neq \pm 1 \]

and we have a contradiction.
Our next result (Lemma 4.8) deals with the case \((n, 6) = 1\). It generalizes [7, Lemma 3.1] to our setting and its proof is essentially a re-run of the proof of that result. We will require the following theorem of Kronecker, a proof of which can be found on page 46 of [6].

**Lemma 4.6** Let \(\beta = \beta_1\) be a non-zero algebraic integer and let \(\beta_1, \ldots, \beta_k\) be the conjugates of \(\beta\) over \(\mathbb{Q}\). If \(\max_j |\beta_j| \leq 1\) then \(\beta\) is a root of unity.

We will also need the following:

**Lemma 4.7** If \(\sum_{i=1}^\ell w_i = \sum_{i=1}^\ell z_i^j\) for all \(j = 1, \ldots, \ell\) then the multisets \(\{w_1, \ldots, w_\ell\}\) and \(\{z_1, \ldots, z_\ell\}\) are equal.

The proof is a standard application of the Newton-Girard formula and so is omitted.

**Lemma 4.8** Let \(n \geq 1\) and \(f(t) = t^m - t^k + 1\) where \(m, k \in \mathbb{Z}\), \((n, m, k) = 1\) and suppose \((n, 6) = 1\). If \(R_n(f) = \pm 1\) then \(m = 2k \mod n\) or \(k = 0 \mod n\) or \(k = m \mod n\).

**Proof**

By Lemma 2.1 \(\lambda = f(\zeta)\) is a unit in the ring \(\mathbb{Z}[\zeta]\) for some primitive \(n\)th root of unity \(\zeta\), and therefore so is \(\sigma(\lambda)\) for any \(\sigma \in \Gamma = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})\). Let \(\mu = \overline{\lambda}^{-1}\).

Then, since \(\Gamma\) is abelian, we have

\[|\sigma(\mu)|^2 = \sigma(\mu)\overline{\sigma(\mu)} = \sigma(\mu\overline{\mu}) = \sigma(1) = 1.\]

Lemma 4.6 implies that \(\mu\) is a root of unity in \(\mathbb{Q}(\zeta)\), and thus \(\mu = s\zeta^j\) for some \(j \in \mathbb{Z}\), \(s = \pm 1\). Since \(\mu = \overline{\lambda}^{-1} = \overline{f(\zeta)}f(\zeta)^{-1} = f(\zeta^{-1})f(\zeta)^{-1}\) it follows that

\[s\zeta^j(\zeta^m - \zeta^k + 1) = \zeta^{-m} - \zeta^{-k} + 1.\]  \(4.1\)

**Case 1:** \(s = -1\). Let \(w_1 = \zeta^{-m}\), \(w_2 = 1\), \(w_3 = \zeta^{m+j}\), \(w_4 = \zeta^j\), \(z_1 = \zeta^{-k}\), \(z_2 = \zeta^{j+k}\), \(z_3 = z_4 = 0\). Then (4.1) is equivalent to

\[w_1 + w_2 + w_3 + w_4 = z_1 + z_2 + z_3 + z_4.\]  \(4.2\)

Since \((n, 6) = 1\) we have that \((r, n) = 1\) for \(r = 1, 2, 3, 4\). Thus the maps \(\zeta \mapsto \zeta^r\) \((r = 1, 2, 3, 4)\) are automorphisms of \(\mathbb{Q}(\zeta)\). Applying these to (4.2) we get

\[\sum_{i=1}^4 w_i^r = \sum_{i=1}^4 z_i^r \quad (r = 1, 2, 3, 4).\]  \(4.3\)

By Lemma 4.7 we have that \(\{w_1, w_2, w_3, w_4\} = \{z_1, z_2, z_3, z_4\}\), but \(z_3 = 0 \notin \{w_1, w_2, w_3, w_4\}\) which gives a contradiction.
**Case 2**: \( s = +1 \). Let \( w_1 = \zeta^{-m}, w_2 = 1, w_3 = \zeta^{k+j}, z_1 = \zeta^{-k}, z_2 = \zeta^{j+m}, z_3 = \zeta^j \). Then (4.1) is equivalent to
\[
 w_1 + w_2 + w_3 = z_1 + z_2 + z_3. \tag{4.4}
\]

As in Case 1, the maps \( \zeta \mapsto \zeta^r \) \((r = 1, 2, 3)\) are automorphisms of \( \mathbb{Q}(\zeta) \) and applying them to (4.4) gives \( \{w_1, w_2, w_3\} = \{z_1, z_2, z_3\} \). If \( (z_1, z_2, z_3) = (w_3, w_1, w_2) \) then \( \zeta^{2k} = \zeta^{2m} = 1 \) so \( k = 0 \) or \( n/2 \mod n \) and \( m = 0 \) or \( n/2 \mod n \) and so \( k = 0 \) or \( m \mod n \) or \( m = 2k \mod n \). If \( (z_1, z_2, z_3) = (w_1, w_2, w_3), (w_1, w_3, w_2), \) or \( (w_2, w_3, w_1) \) then \( \zeta^{m-k} = 1 \) and hence \( k = m \mod n \). If \( (z_1, z_2, z_3) = (w_3, w_2, w_1) \) then \( 2k = m \mod n \). If \( (z_1, z_2, z_3) = (w_2, w_1, w_3) \) then \( k = 0 \mod n \).

**Proof of Main Theorem**

The ‘if’ direction was proved in [8, Lemma 5] so suppose that \( R_n(f) = \pm 1 \). By Lemmas 4.4 and 4.8 we may assume \( n = ab \) where \( a = 2^r 3^s > 1, (b, 6) = 1, b > 1 \). Now \( R_a(f) = \pm 1 \) implies (by Lemma 4.4) that \( k = 0 \mod a \) or \( (m - k) = 0 \mod a \). By interchanging the roles of \( k \) and \( (m - k) \) we may assume that \( k = 0 \mod a \). Also, \( R_b(f) = \pm 1 \) implies (by Lemma 4.8) that \( k = 0 \mod b \) or \( m = 2k \mod b \) or \( k = m \mod b \). If \( k = 0 \mod b \) then \( k = 0 \mod n \) so assume otherwise.

Suppose \( m = 2k \mod b \). Then no prime divisor of \( n \) divides \( m - k \) for otherwise it would also divide \( (n, m, k) = 1 \). Therefore \( (m - k, n) = 1 \) and the result follows from Corollary 4.2. Suppose then that \( k = m \mod b \) and let \( p \geq 5 \) be a prime divisor of \( b \) and let \( q = 2 \) if \( r \geq 1 \) or \( q = 3 \) otherwise. Now \( k \neq m \mod pq \) and \( k \neq 0 \mod pq \) for otherwise \( q | (n, m, k) = 1 \) or \( p | (n, m, k) = 1 \) (respectively) and so Lemma 4.5 implies \( R_{pq}(f) \neq \pm 1 \) so \( R_n(f) \neq \pm 1 \).

**Acknowledgement**

I would like to thank the referee(s) of this paper and of an earlier version of it for the helpful comments.

**References**


[4] M. Edjvet and G. Williams. The cyclically presented groups with relators $x_i x_{i+k} x_{i+l}$. Preprint.


**Author’s address**

Gerald Williams  
Department of Mathematical Sciences  
University of Essex  
Wivenhoe Park  
Colchester  
Essex  
CO4 3SQ  
gwill@essex.ac.uk