*Glasgow Math. J.* **41** (1999) 157–165. © Glasgow Mathematical Journal Trust 1999. Printed in the United Kingdom

# SOME DIOPHANTINE PROBLEMS ARISING FROM THE THEORY OF CYCLICALLY-PRESENTED GROUPS

R. W. K. ODONI

*Department of Mathematics, University of Glasgow, Glasgow G12 8QW, UK*

(Received 30 March, 1995; revised 26 August, 1998)

**Abstract.** Let $n \in \mathbb{N}$ and let $F_n$ be the free group on $n$ generators. Let $w$ be an arbitrary word in $F_n$, and let $\sigma$ be an $n$-cycle in $S_n$. We consider groups of the type $\Gamma(n, w) = F_n/N$, where $N$ is the normal closure in $F_n$ of the "cycled words" $w$, $\sigma(w)$, $\sigma^2(w), \ldots, \sigma^{n-1}(w)$, and solve, by means of classical algebraic number theory, the following problems.

**A**. When is $\Gamma(n, w)^{ab}$ infinite?

**B**. When is $\Gamma(n, w)$ a perfect group?

**0. Introduction.** Let $n \in \mathbb{N}$ and let $F_n$ be the free group on the $n$ symbols $Y_1, \ldots, Y_n$. For later purposes it is convenient to introduce extra "dummy symbols" $Y_k$ ($k \in \mathbb{Z}$), such that $Y_k = Y_l$ wherever $k \equiv l (\mathrm{mod}\ n)$. Now let $\sigma$ be a permutation of $\{1, \ldots, n\}$.

The map $Y_i \mapsto Y_{\sigma(i)}$ ($1 \leq i \leq n$) extends uniquely to an automorphism of $F_n$, which we shall also denote by $\sigma$, so that $\sigma(Y_i) = Y_{\sigma(i)}$ ($1 \leq i \leq n$).

Now let $w \in F_n$, and let $\sigma_n$ be the $n$-cycle $(12 \ldots n)$. Groups of the type

$$\begin{aligned} \Gamma(n, w) &= < Y_1, \ldots, Y_n \mid \sigma_n(w), \ldots, \sigma_n^n(w) > \\ &= F_n/N, \end{aligned} \tag{0.1}$$

where $N$ is the normal closure in $F_n$ of $\sigma_n(w), \ldots, \sigma_n^n(w)$, are called *cyclically-presented*, and have been studied by various authors-see e.g. [**2**,**4**,**6**,**7**,**10**,**11**]. This paper addresses certain problems relating to the structure of the *abelianization* $\Gamma(n, w)^{ab}$ of the typical cyclically-presented $\Gamma(n, w)$. In particular we consider the following questions.

PROBLEM A. *When is $\Gamma(n, w)^{ab}$ infinite?*

PROBLEM B. *When is $\Gamma(n, w)$ a perfect group; i.e. when is $\Gamma(n, w)^{ab}$ trivial?*

There is a standard procedure (see e.g. [**7**,**8**]) which reduces these problems to questions about ideals in the (commutative) group ring $\mathbb{Z}C_n$, where $C_n$ is cyclic of order $n$. We now briefly describe this.

For $g \in F_n$ let $\bar{g}$ be the image of $g$ under the natural epimorphism $F_n \to F_n^{ab}$. If $\bar{w} = \bar{Y}_0^{c_c} \ldots \bar{Y}_{n-1}^{c_{n-1}}$, with the $c_i$ in $\mathbb{Z}$, we introduce the polynomial $f(x) = f_w(x) = \sum_{j<n} c_j x^j \in \mathbb{Z}[x]$.

The action of $C_n = < \sigma_n > \subseteq \mathrm{Aut}(F_n)$ on $F_n$ makes $F_n^{ab}$ into a left $\mathbb{Z}C_n$-module, and indeed $F_n^{ab} \cong \mathbb{Z}C_n$ as left $\mathbb{Z}C_n$-modules. Moreover $\Gamma(n, w)^{ab}$ is also a left $\mathbb{Z}C_n$-module, and we have an isomorphism

$$\Gamma(n, w)^{ab} \cong \mathbb{Z}C_n/f(\sigma_n)\mathbb{Z}C_n \tag{0.2}$$

both as left $\mathbb{Z}C_n$-modules, and as $\mathbb{Z}$-modules (if we use additive notation for the group law in $\Gamma(n, w)^{ab}$).

As we show in §1, $\Gamma(n, w)^{ab}$ is infinite if and only if $f(\sigma_n)$ is a zero-divisor in $\mathbb{Z}C_n$, and $\Gamma(n, w)^{ab}$ is trivial if and only if $f(\sigma_n)$ is a unit in $\mathbb{Z}C_n$. (In slightly disguised notation, these results appear in [**7**,**8**].)

Our first main result concerns the case where $f(x) \in \mathbb{Z}[x]$ is fixed and $n$ varies in $\mathbb{N}$. Since, for each $n$, we may find (several) $w \in F_n$ yielding our given $f$ via the above procedure, the following theorem yields some useful information about Problems A and B.

THEOREM 1. *Let* $f(x) \in \mathbb{Z}[x]$, $\deg f \geq 1$ *with* $f$ *irreducible. For* $n \in \mathbb{N}$ *let* $C_n =< \sigma_n >$ *be a cyclic group of order n. Then*

(i) $f(\sigma_n)$ *is a zero-divisor in* $\mathbb{Z}C_n$ *if and only if* $f(x) = \pm\Phi_m(x)$ *for some* $m|n$;

(ii) *there are infinitely many* $n \in \mathbb{N}$ *such that* $f(\sigma_n)$ *is a unit in* $\mathbb{Z}C_n$ *if and only if* $f(x) = \pm x$ *or* $\pm\Phi_m(x)$ *for some* $m > 1$ *not a prime-power. In the latter case,* $f(\sigma_n)$ *is a unit if and only if* $m|\gcd(m, n) > 1$ *and is not a prime-power.*

REMARKS. (i) In the above, for $m \in \mathbb{N}$, $\Phi_m(x)$ is the minimum polynomial for $\zeta_m = e^{2\pi i/m}$ over $\mathbb{Q}$; $\Phi_m(x)$ is monic in $\mathbb{Z}[x]$ of degree $\phi(m)$, where $\phi$ is Euler's totient function.

(ii) Since $\mathbb{Z}[x]$ is a unique factorisation domain, the results of Theorem 1 can be easily modified to cover the case where $f(x)$ is not irreducible. One simply notes that $f(\sigma_n)$ is a zero-divisor if and only if $g(\sigma_n)$ is a zero-divisor for *some* irreducible factor $g(x)$ of $f(x)$ in $\mathbb{Z}[x]$, while $f(\sigma_n)$ is a unit if and only if $g(\sigma_n)$ is a unit for *every* irreducible factor $g$ of $f$.

The remainder of the paper is devoted to the complete solution of Problems A and B for the case in which $f(x) = x^t - x + 1$, where $t \geq 2$ and $n \geq 1$ are arbitrary. We prove the following result.

THEOREM 2. *For* $t, n \in \mathbb{N}$, *with* $t \geq 2$,

(i) $\sigma_n^t - \sigma_n + 1$ *is a zero-divisor in* $\mathbb{Z}C_n$ *if and only if* $n \equiv 0 (\mathrm{mod}\ 6)$ *and* $t \equiv 2 (\mathrm{mod}\ 6)$;

(ii) *for* $\gcd(n, 6) = 1$, $\sigma_n^t - \sigma_n + 1$ *is a unit in* $\mathbb{Z}C_n$ *if and only if* $t \equiv 1$ *or* $2 (\mathrm{mod}\ n)$;

(iii) *for* $\gcd(n, 6) > 1$, $\sigma_n^t - \sigma_n + 1$ *is a unit in* $\mathbb{Z}C_n$ *if and only if* $t \equiv 1 (\mathrm{mod}\ n)$.

The principal ingredients in our proof of Theorem 2 are classical results on units in $\mathbb{Z}[\zeta_m]$, mostly due to Kronecker and Kummer.

I am indebted to Professor J. Howie (Heriot-Watt University) for drawing my attention to Problems A and B.

**1. Preliminary results.** We begin with some simple properties of $\mathbb{Q}C_n$ and $\mathbb{Z}C_n$ ($n \in \mathbb{N}$). We consider $\mathbb{Q}C_n$ as a $\mathbb{Q}$-algebra of dimension $n$.

For $\lambda \in \mathbb{Q}C_n$ let $L(\lambda)$ be the $\mathbb{Q}$-linear map $\alpha \mapsto \lambda\alpha$ on $\mathbb{Q}C_n$. The eigenvalues in $\mathbb{C}$ of $L(\sigma_n)$ are the $\theta$ with $\theta^n = 1$, and for $g(x) \in \mathbb{Q}[x]$, the eigenvalues of $L(g(\sigma_n))$ are the $g(\theta)$, ($\theta^n = 1$), so that

$$\det L(g(\sigma_n)) = \prod_{\theta^n=1} g(\theta) \in \mathbb{Q}.$$

Now let $f(x) \in \mathbb{Z}[x]$. Then $f(\sigma_n)$ is a zero-divisor in $\mathbb{Z}C_n$ if and only if it is a zero-divisor in $\mathbb{Q}C_n$, if and only if $\det L(f(\sigma_n)) = 0$, if and only if $\prod_{\theta^n=1} f(\theta) = 0$.

Now suppose that $f(x) \in \mathbb{Z}[x]$ but $\det L(f(\sigma_n)) \neq 0$.

Let $M = L(f(\sigma_n))$; it is a non-singular $\mathbb{Q}$-linear map on $\mathbb{Q}C_n$, while $M(\mathbb{Z}C_n)$ is a $\mathbb{Z}$-submodule of $\mathbb{Z}C_n$ of rank $n = \operatorname{rank} \mathbb{Z}C_n$. By "elementary divisor theory", $M(\mathbb{Z}C_n)$ has $\mathbb{Z}$-module index in $\mathbb{Z}C_n$ equal to $|\det M|$ or, equivalently,

$$\mathbb{Z}C_n/f(\sigma_n)\mathbb{Z}C_n = |\det M| = |\prod_{\theta^n=1} f(\theta)|. \tag{1.1}$$

We also see from the above that, for $f \in \mathbb{Z}[x]$, $\mathbb{Z}C_n/f(\sigma_n)\mathbb{Z}C_n$ is infinite if and only if $\prod_{\theta^n=1} f(\theta) = 0$, if and only if $f(\sigma_n)$ is a zero-divisor in $\mathbb{Z}C_n$. Also, by (1.1), $f(\sigma_n)$ is a unit in $\mathbb{Z}C_n$ if and only if $\prod_{\theta^n=1} f(\theta) = \pm 1$.

To summarise, we put

$$R_n(f) = \prod_{\theta^n=1} f(\theta) \in \mathbb{Z} \quad (f(x) \in \mathbb{Z}[x]). \tag{1.2}$$

Then we have proved the following result.

Lemma 1.1. *$\mathbb{Z}C_n/f(\sigma_n)\mathbb{Z}C_n$ is infinite if and only if $R_n(f) = 0$, and has order 1 if and only if $R_n(f) = \pm 1$.*

We now turn to standard classical results from algebraic number theory needed for the proofs of Theorems 1 and 2. Reference [**9**] is a convenient source for most of these.

Lemma 1.2. *(Kronecker). Let $\beta = \beta_1$ be an algebraic integer, and let $\beta_1, \ldots, \beta_k$ be the conjugates of $\beta$ over $\mathbb{Q}$. Suppose that $\max_j |\beta_j| \leq 1$. Then either $\beta_1 = \ldots = \beta_k = 0$ (and then $k = 1$), or $\beta$ is a root of unity.*

For a proof see [**9**, p.46]

Lemma 1.3. *Let $m \in \mathbb{N}$, $K = \mathbb{Q}(\zeta_m)$, where $\zeta_m = e^{2\pi i/m}$. The roots of unity in $K$ are precisely the $\pm\zeta_m^k (k \in \mathbb{Z})$.*

For a proof see [**9**, p. 170]

Lemma 1.4. *Let $t \in \mathbb{N}$, $t \geq 2$, and let $f(x) = x^t - x + 1 \in \mathbb{Z}[x]$. Then $f$ has a (complex) zero $\lambda$ of absolute value 1 if and only if $t \equiv 2 (\mathrm{mod}\ 6)$, in which case $\lambda = \pm\zeta_6$.*

*Proof.* Suppose that $f(\lambda) = 0$, where $\lambda \in \mathbb{C}$ has $|\lambda| = 1$. Then $f(\bar{\lambda}) = 0$ while $\bar{\lambda} = \lambda^{-1}$. Hence $\lambda^t = \lambda - 1$ and $\lambda^{-t} = \lambda^{-1} - 1$, so that $1 = \lambda^t\lambda^{-t} = (\lambda - 1)(\lambda^{-1} - 1) = 2 - \lambda - \lambda^{-1}$, and so $\lambda^2 - \lambda + 1 = 0$. Thus $\lambda = \pm\zeta_6$ while $0 \neq \lambda^t = \lambda - 1 = \lambda^2$. Hence $\lambda^{t-2} = 1$. Since $\pm\zeta_6$ has order 6 in $\mathbb{C}^*$ we see that $t \equiv 2 (\mathrm{mod}\ 6)$.

Conversely if $t \equiv 2 (\mathrm{mod}\ 6)$, then $\lambda = \pm\zeta_6$ satisfies $\lambda^t = \lambda^2$ and $\lambda^t - \lambda + 1 = \lambda^2 - \lambda + 1 = 0$, so that $f(x) = x^t - x + 1$ has $f(\lambda) = 0$ and $|\lambda| = 1$.

**2. Proof of Theorem 1.** We begin with an elementary calculation of $R_n(f)$.

LEMMA 2.1. *Let* $f(x) \in \mathbb{Z}[x]$, $\deg f = k \geq 1$, *and suppose that* $f(x) = c\prod_{j\leq k}(x-\beta_j)$ *in* $\mathbb{C}[x]$, *where* $0 \neq c \in \mathbb{Z}$. *Then* $R_n(f)$ of (1.2) *equals* $((-1)^k c)^n \prod_{j\leq k}(\beta_j^n - 1)$.

*Proof.*
$$\begin{aligned} R_n(f) &= \prod_{\theta^n=1}\left\{c\prod_{j\leq k}(\theta-\beta_j)\right\} \\ &= c^n\prod_{\theta}\prod_{j}(\theta-\beta_j) \\ &= c^n(-1)^{nk}\prod_{j}\prod_{\theta}(\beta_j-\theta) \\ &= c^n(-1)^{nk}\prod_{j\leq k}(\beta_j^n-1). \end{aligned}$$

Now suppose that $f(x)$ is irreducible in $\mathbb{Z}[x]$, of degree $k \geq 1$, and that $R_n(f) = \pm 1$, for all $n \in N_1$, an infinite subset of $\mathbb{N}$.

If $k = 1$ then it is clear from Lemma 2.1 that $c = \pm 1$ and that $f(x) = \pm(x - \beta_1)$ with $\beta \in \mathbb{Z}$, so that $\beta_1^n - 1 = \pm 1$, for all $n \in N_1$; i.e. $\beta_1^n = 0$ or $2$, for all $n \in N_1$. If $\beta_1 \neq 0$, then $\beta_1^n = 2$, for infinitely many $n$, which is impossible since $\beta_1 \in \mathbb{Z}$. Thus $\beta_1 = 0$, and so $f(x) = \pm x$ and $R_n(f) = \pm 1$, for all $n \in \mathbb{N}$.

We may now assume that $k \geq 2$. Put $a = |c| \geq 1$. Then there is an infinite subset $N_2$ of $N_1$ such that

$$a^n\prod_{j\leq k}(\beta_j^n - 1) = \zeta \quad (\forall n \in N_2), \tag{2.1}$$

where $\zeta$ is some *fixed* choice of $\pm 1$. We partition $\{1, \ldots k\}$ into three parts (some of them possible empty); thus let

$$A = \{j;\, |\beta_j| < 1\},\ \beta = \{j;\, |\beta_j| = 1\},\ C = \{j;\, |\beta_j| > 1\}.$$

We put $h = \prod_{j\in C}|\beta_j|$, with the convention that empty products equal 1. We shall first show that $C = \emptyset$. If this is false, then $h > 1$ and so $ah > 1$. We shall rule out the latter case.

Suppose, aiming for a contradiction, that $ah > 1$, given (2.1). Letting $n \to \infty$ through $N_2$ we have

$$\prod_{j\in A}(\beta_j^n - 1) \sim (-1)^A \ \text{ while } \ \prod_{j\in C}|\beta_j^n - 1| \sim h^n.$$

Applying (2.1), we have

$$\prod_{j\in B}|\beta_j^n - 1| \sim (ah)^{-n}, \tag{2.2}$$

https://doi.org/10.1017/S0017089599950383 Published online by Cambridge University Press

as $n \to \infty$ through $N_2$. As $ah > 1$ we immediately see that $B \neq \emptyset$. Then there is some $d > 0$ in $\mathbb{R}$ and an infinite subset $N_3$ of $N_2$ such that, for some $r \in B$, we have

$$|\beta_r^n - 1| \leq e^{-nd} \quad (\forall n \in N_3). \tag{2.3}$$

By Gel'fond's theorem [**5**, p. 28], (2.3) is impossible unless $\beta_r$ is a root of unity. (Recall that the $\beta_j$ are *algebraic numbers*.) Let $\beta_r$ be a primitive root of unity of order $m \in \mathbb{N}$. Then $\Phi_m(x) \mid f(x)$ in $\mathbb{Z}[x]$. As both are irreducible, we have $f(x) = \pm\Phi_m(x)$. Hence $a = |c| = 1$ and $|\beta_j| = 1$ for all $j \leq k = \phi(m)$. This forces $C = \emptyset$ and $h = 1$, so that $ah = 1$, a contradiction.

It follows that $ah \leq 1$ in (2.1). Since $a = |c| \geq 1$ we have $h \leq 1$. Hence (2.1) implies that $a = 1$, $h = 1$ and $C = \emptyset$, so that $\beta_1, \ldots, \beta_k$ are algebraic integers with $\max_{j \leq k} |\beta_j| \leq 1$, while the $\beta_j$ are the conjugates of $\beta_1$. Since $k \geq 2$ this forces $f(x) = \pm\Phi_m(x)$ with $\phi(m) = k \geq 2$ and so $m \geq 3$.

If $m \geq 3$ is a prime-power, then $\zeta_m - 1$ generates a maximal ideal $\mathbf{P}$ in $\mathbb{Z}[\zeta_m]$, and then Lemma 2.1 shows that $R_n(f) \in \mathbf{P}$, for all $n \in \mathbb{N}$, a contradiction.

Finally suppose that $m \geq 3$ is not a prime-power. Then $\zeta_m - 1$ is a unit in $\mathbb{Z}[\zeta_m]$, since $\Phi_m(1) = 1$, while

$$R_n(f) = \pm \prod_{r \in V} (\zeta_m^{rn} - 1), \tag{2.4}$$

where $V = \{r \in \mathbb{Z};\, 0 < r < m, \gcd(r, m) = 1\}$. But, for $r \in V$, $\zeta_m^{rn}$ is a primitive root of unity of order $m^* = m/\gcd(m, n)$, so that $\zeta_m^{rm} - 1$ is a non-unit in $\mathbb{Z}[\zeta_{m^*}]$ unless $m^* > 1$ is not a prime power. If the latter fails to hold, then $R_n(f)$ is a non-unit in $\mathbb{Z}[\zeta_{m^*}]$ and so cannot be $\pm 1$. To complete the proof of Theorem 1 we have

$$R_n(f) = \pm N_{K/\mathbb{Q}}(\zeta_m^n - 1), \tag{2.5}$$

where $N_{K/\mathbb{Q}}$ is the norm from $K = \mathbb{Q}(\zeta_m)$ to $\mathbb{Q}$, and so $R_n(f) = \pm\{N_{L/\mathbb{Q}}(\zeta_{m^*} - 1)\}^g$, where $g \in \mathbb{N}$ and $L = \mathbb{Q}(\zeta_{m^*})$.

(Here, as before, $m^* = m/\gcd(m, n)$.)

In particular $R_n(f) = \pm 1$ if and only if $\zeta_{m^*} - 1$ is a unit in $\mathbb{Z}[\zeta_{m^*}]$, and this certainly holds if $m^* > 1$ is not a prime-power.

**3. Proof of Theorem 2.** Let $t \in \mathbb{N}$, $t \geq 2$. Throughout this section $f(x)$ will be $x^t - x + 1 \in \mathbb{Z}[x]$.

We first dispose of the question of when $R_n(f) = \pm 1$; i.e. when $f(\sigma_n)$ is a unit in $\mathbb{Z}C_n$. The condition $R_n(f) = \pm 1$ is clearly equivalent to

$$f(\zeta_d) \text{ is a unit in } \mathbb{Z}[\zeta_d], (\forall d \mid n), \tag{3.1}$$

and this formulation turns out to be very fruitful.

LEMMA 3.1. *Let $n \in \mathbb{N}$,* $\gcd(n, 6) = 1$. *Then $f(\zeta_n)$ is a unit in $\mathbb{Z}[\zeta_n]$ if and only if $t \equiv 1$ or* $2 \pmod n$.

https://doi.org/10.1017/S0017089599950383 Published online by Cambridge University Press

*Proof*. The "if" part is easy. For $t \equiv 1 (\mathrm{mod}\ n)$ we have $f(\zeta_n) = \zeta_n^t - \zeta_n + 1 = 1$, while if $t \equiv 2 (\mathrm{mod}\ n)$ then $f(\zeta_n) = \zeta_n^2 - \zeta_n + 1$ and moreover $f(\theta) = \theta^2 - \theta + 1$ whenever $\theta^n = 1$, so that by Lemma 2.1 we have

$$R_n(f) = \pm \prod_{\lambda^2 = \lambda - 1} (\lambda^n - 1) = \pm 1 \text{ (since } \gcd(n, 6) = 1).$$

In particular $f(\zeta_n)$ is a unit in $\mathbb{Z}[\zeta_n]$ if $t \equiv 1$ or $2 (\mathrm{mod}\ n)$).

Suppose, conversely, that $\gcd(n, 6) = 1$, and that $f(\zeta_n)$ is a unit. The case $n = 1$ is trivial (since $f(1) = 1$ is a unit for any $t \geq 2$).

We may now suppose that $n \geq 5$. Let $\lambda = f(\zeta_n)$ be a unit in $\mathbb{Z}[\zeta_n]$. Then so is $\lambda^\sigma$ for all $\sigma \in G := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Let $\tau$ be complex-conjugation in $G$.

Since $G$ is abelian, we have

$$|\mu^\sigma|^2 = \mu^\sigma \mu^{\sigma\tau} = (\mu\mu^\tau)^\sigma = 1,$$

for all $\sigma \in G$, where $\mu = \lambda^\tau \lambda^{-1}$ is a unit in $\mathbb{Z}[\sigma_n]$.

By Lemma 1.2, $\mu$ is a root of unity in $\mathbb{Q}(\zeta_n)$, and thus has the form $\pm\zeta_n^k (k \in \mathbb{Z})$.

Since $\mu = \lambda^\tau \lambda^{-1}$ and $\lambda = f(\zeta_n)$, we have

$$\zeta^{-t} - \zeta^{-1} + 1 = s\zeta^k(\zeta^t - \zeta + 1), \tag{3.2}$$

where $\zeta = \zeta_n$ and $s = \pm 1$.

*Case 1:* $s = -1$. We shall rule this out, by the following argument. By (3.2) we have that

$$w_1 + w_2 + w_3 + w_4 = z_1 + z_2 + z_3 + z_4, \tag{3.3}$$

where $w_1 = \zeta^{-t}$, $w_2 = 1$, $w_3 = \zeta^{k+t}$, $w_t = \zeta^k$, $z_1 = \zeta^{-1}$, $z_2 = \zeta^{k+1}$, and $z_3 = z_4 = 0$.

Applying to (3.3) the elements $\zeta \mapsto \zeta^r$ of $G = \mathrm{Gal}\mathbb{Q}(\zeta)/\mathbb{Q}$ for $r = 1, 2, 3, 4$ (recalling that $\gcd(n, 6) = 1$), we see that

$$\sum_{j \leq 4} w_j^r = \sum_{j \leq 4} z_j^r \quad (1 \leq r \leq 4). \tag{3.4}$$

The classical Newton-Waring identities connecting symmetric power-sums and elementary symmetric functions yield from (3.4) that the sets $\{w_1, \ldots, w_4\}$ and $\{z_1, \ldots, z_4\}$ coincide. However $0 \in \{z_1, \ldots, z_4\}$ but $0 \notin \{w_1, \ldots, w_4\}$, a contradiction. Hence the case $s = -1$ cannot occur. We are left with Case 2.

*Case 2:* $s = 1$. Then we have

$$w_1 + w_2 + w_3 = z_1 + z_2 + z_3, \tag{3.5}$$

where $w_1 = \zeta^{-t}$, $w_2 = 1$, $w_3 = \zeta^{k+1}$, $z_1 = \zeta^{-1}$, $z_2 = \zeta^{k+2}$, $z_3 = \zeta^k$.

This time we apply to (3.5) the elements $\zeta \mapsto \zeta^r$ of $G$ $(r = 1, 2, 3)$ and find that

$$\left\{\zeta^{-t}, 1, \zeta^{k+1}\right\} = \left\{\zeta^{-1}, \zeta^{k+t}, \zeta^k\right\}.$$

https://doi.org/10.1017/S0017089599950383 Published online by Cambridge University Press

In particular $1 = \zeta^{k+t}$ or $\zeta^k$, the case $\zeta^{-1} = 1$ being ruled out since $\zeta = \zeta^n$ and $n \geq 5$. If $1 = \zeta^{k+t}$, then $\{\zeta^{-t}, \zeta^{k+1}\} = \{\zeta^{-1}, \zeta^k\}$ so that $\zeta^{k+2} = 1 = \zeta^{k+t}$, $\zeta^{t-2} = 1$ and $t \equiv 2(\text{mod } n)$. If $1 = \zeta^k$, then $\{\zeta^{-t}, \zeta\} = \{\zeta^{-1}, \zeta^t\}$, and so $\zeta^t \equiv \zeta^{-t}$ or $\zeta$.

If $\zeta^t = \zeta^{-t}$, then $\zeta_n^{2t} = 1$, and, as $n$ is odd, $\zeta^t = 1$, in which case $\{1, \zeta\} = \{\zeta^{-1}, 1\}$, clearly false. Hence we have $\zeta^t = \zeta$ and thus $t \equiv 1(\text{mod } n)$. This proves the lemma.

Before we proceed further we note a further property of $R_n(g)$ for $n \in \mathbb{N}$, $g \in \mathbb{Z}[x]$. It is clear from (1.2) that

$$R_n(g) \in R_d(g)\mathbb{Z}[\zeta_n] \tag{3.6}$$

whenever $d|n$. In particular if $R_n(g) \neq 0$, the $R_d(g) \neq 0$ and we have that $R_n(g)/\ R_d(g) \in \mathbb{Q}_\cap\mathbb{Z}[\zeta_n] = \mathbb{Z}$, so that $R_d(g)$ divides $R_n(g)$ in $\mathbb{Z}$.

Lemma 3.2. *Let $p = 2$ or $3$ and let $n$ be a power of $p$. Then $R_n(f) = \pm 1$ if and only if $t \equiv 1(\text{mod } n)$.*

*Proof.* (i) If $t \equiv 1(\text{mod } n)$ we have $\theta^t - \theta + 1 = 1$ whenever $\theta^n = 1$ and so $R_n(f) = \pm 1$.

(ii) We now prove by induction on $k \geq 0$ that if $n = p^k$ and $R_n(f) = \pm 1$ then $t \equiv 1(\text{mod } n)$. For $k = 0$ this is vacuously true. For $k = 1$ we have $R_p(f) = \prod_{\theta^p=1} f(\theta)$. If $p = 2$ we have $R_p(f) = R_2(f) = f(1)f(-1) = f(-1) = 2 + (-1)^t = \pm 1$ if and only if $t \equiv 1(\text{mod } 2)$; i.e. $t \equiv 1(\text{mod } n)$ as $n = 2$ here.

If $p = 3$ we have $R_p(f) = R_3(f) = f(1)f(\zeta_3)f(\zeta_3^2) = f(\zeta_3)f(\bar{\zeta}_3) = |f(\zeta_3)|^2 \geq 0$ and $R_3(f) = \pm 1$ if and only if $\zeta_3^t - \zeta_3 + 1$ is a unit in $\mathbb{Z}[\zeta_3]$. This happens if and only if $t \equiv 1(\text{mod } 3)$, since the units in $\mathbb{Z}[\zeta_3]$ are the powers of $\zeta_6$.

This covers the case $k = 1$. Now suppose that $k > 1$ and that $R_{p^s}(f) = \pm 1$ if and only if $t \equiv 1(\text{mod } p^s)$ holds whenever $0 \leq s \leq k$.

Suppose that $R_{p^{k+1}}(f) \pm 1$. Then by (3.1), we have $R_{p^k}(f) = \pm 1$, so that $t \equiv 1(\text{mod } p^k)$ and $t \equiv 1 + cp^k(\text{mod } p^{k+1})$, for some $c \in \mathbb{Z}$. We must show that $c \in p\mathbb{Z}$. We put $\zeta = \zeta_{p^{k+1}}$ and $\omega = \zeta_p$, and let $N(\ldots)$ be the norm map from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}(\omega)$.

We have $f(\zeta) = \zeta^{1+cp^k} - \zeta + 1 = \zeta(w^c - 1) + 1$, and, as $R_{p^{k+1}}(f) = \pm 1$, $f(\zeta)$ is a unit in $\mathbb{Z}[\zeta]$.

Since the characteristic polynomial for $\zeta$ over $\mathbb{Q}(\omega)$ is $X^{p^k} - \omega$ we see that $N(f(\zeta)) = 1 - \omega(1 - \omega^c)^{p^k}$ is a unit in $\mathbb{Z}[\omega]$. As $p = 2$ or $3$, $\mathbb{Q}(\omega)$ is $\mathbb{Q}$ or an imaginary quadratic field, and so Lemma 1.3 implies that

$$1 - \omega(1 - \omega^c)^{p^k} = s\omega^m (s = \pm 1, m \in \mathbb{Z}). \tag{3.7}$$

If $p = 2$, (3.7) gives

$$1 + (1 - (-1)^c)^{2^k} = s(-1)^m = \pm 1, \tag{3.8}$$

and if $c$ were odd, we would have $1 + 2^{2^k} = \pm 1$, which is impossible, so that $c$ is even and $t \equiv 1(\text{mod } 2^{k+1})$, as required., If $p = 3$, (3.8) gives

$$1 - s\zeta_3^m = \zeta_3(1 - \zeta_3^c)^{3^k}. \tag{3.9}$$

If $c \notin 3\mathbb{Z}$, then $\pi \parallel 1 - \zeta_3^c$ in $\mathbb{Z}[\zeta_3]$, where $\pi$ is the prime $1 - \zeta_3$, so that $\pi^{3^k} \parallel$ (right-hand side of (3.9)) But the left-hand side of (3.9) is one of $1 \pm 1$, $1 \pm \zeta_3$ or $1 \pm \zeta_3^2$, none of which is exactly divisible by $\pi^{3^k}$ (since $k \geq 1$). Hence $c \in 3\mathbb{Z}$ and so $t \equiv 1(\text{mod } 3^{k+1})$, as required.

https://doi.org/10.1017/S0017089599950383 Published online by Cambridge University Press

LEMMA 3.3. *Let $p \geq 5$ be prime. Then*

$$R_{2_p}(f) = \pm 1 \text{ if and only if } t \equiv 1 (\text{mod } 2p)$$

*and*

$$R_{3_p}(f) = \pm 1 \text{ if and only if } t \equiv 1 (\text{mod } 3p).$$

*Proof*. Let $q = 2$ or 3. If $R_{pq}(f) = \pm 1$, then $R_q(f) = \pm 1$, so that $t \equiv 1(\text{mod } q)$. Also $R_p(f) = \pm 1$, so that $t \equiv 1$ or $2(\text{mod } p)$. If $t \equiv 1(2\text{mod}p)$, then we have $t \equiv 1(\text{mod } pq)$, as required, and, conversely, if $t \equiv 1(\text{mod } pq)$, then $f(\theta) = 1$ whenever $\theta^{pq} = 1$, so that $R_{pq}(f) = \pm 1$. It remains to eliminate the possibility that $t \equiv 1(\text{mod } q)$ and $t \equiv 2(\text{mod } p)$. Suppose that these congruences hold, and the $R_{pq}(f) = \pm 1$; then $f(\theta)$ must be a unit in $\mathbb{Z}[\zeta_{pq}]$ whenever $\theta^{pq} = 1$. In particular, for every $b \in \mathbb{Z}$, $f(\zeta_p \zeta_q^b) = (\zeta_p^2 - \zeta_p)\zeta_q^b + 1$ must be a unit, and hence so is $\zeta_p^2 - \zeta_p + \zeta_q^{-b}$.

*Case* $q = 2$. We see that $\zeta_p^2 - \zeta_p - 1$ must be a unit in $\mathbb{Z}[\zeta_p]$. Let $g(X) = X^2 - X - 1$. Then $g(1) = -1$ and $g(\zeta_p)$ is a unit in $\mathbb{Z}[\zeta_p]$; hence so is $g(\zeta_p^\sigma)$, for all $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. In particular, by Lemma 2.1,

$$\prod_{\theta^p = 1} g(\theta) = \pm 1 = \pm(\lambda_1^p - 1)(\lambda_2^p - 1), \tag{3.10}$$

where $\lambda_1 > \lambda_2$ are the zeros $\frac{1}{2}(1 \pm \sqrt{5})$ of $g$.

Now $p \geq 5$ is odd and $\lambda_2 = -\lambda_1^{-1}$, so that $(\lambda_1^p - 1)(\lambda_2^p - 1)$ must be 1, by (3.10).

But $\lambda_1 > \frac{3}{2}$ and so

$$1 = (\lambda_1^p - 1)(\lambda_2^p - 1) = (\lambda_1^p - 1(1 + \lambda_1^{-p}) > \left(\tfrac{3}{2}\right)^5 - 1,$$

a contradiction. Hence if $q = 2$ we must have $t \equiv 1(\text{mod } pq)$ if $R_{pq}(f) = \pm 1$, as required.

*Case* $q = 3$. This time we have $\zeta_p^2 - \zeta_p + \zeta_3^{-b}$ is a unit, for all $b \in \mathbb{Z}$. Taking $b = 0, 1, 2$ and multiplying these units together we see that $1 + (\zeta_p^2 - \zeta_p)^3$ must be a unit in $\mathbb{Z}[\zeta_p]$. Let $\lambda = 1 - \zeta_p$. Then $\lambda\mathbb{Z}[\zeta_p]$ is a maximal ideal $\mathbf{P}$ in $\mathbb{Z}[\zeta_p]$, and $\mathbf{P}^{p-1} = p\mathbb{Z}[\zeta_p]$, while $N(\mathbf{P}) = \#\mathbb{Z}[\zeta_p]/\mathbf{P} = p$.

Now, by hypothesis $\delta = 1 + (\zeta_p^2 - \zeta_p)^3$ is a unit in $\mathbb{Z}[\zeta_p]$, while

$$\delta \equiv 1 - \lambda^3 (\text{mod } \mathbf{P}^4). \tag{3/11}$$

Let $\tau \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ be complex-conjugation. Then $\mathbf{P}^\tau = \mathbf{P}$ and $\lambda^\tau = 1 - \zeta_p^{-1} = -\zeta_p^{-1}\lambda$ so that

$$\delta^\tau \equiv (1 + \lambda^3)(\text{mod } \mathbf{P}^4). \tag{3.12}$$

However $\delta^\tau = s\zeta_p^k\delta$ $(s = \pm 1, k \in \mathbb{Z})$, by Lemmas 1.2 and 1.3, so that $s\zeta_p^k(1 - \lambda^3) \equiv 1 + \lambda^3(\text{mod } \mathbf{P}^4)$ and hence $s\zeta_p^k - 1 \in \mathbf{P}^3$. Since $\zeta_p \equiv 1(\text{mod } \mathbf{P})$ we have $s \equiv 1(\text{mod } \mathbf{P})$. As $2 \notin \mathbf{P}$ we have $s = 1$, and so $\delta^\tau = \zeta_p^k\delta$ and $\zeta_p^k - 1 \in \mathbf{P}^3$. If $k \notin p\mathbb{Z}$ we have $\mathbf{P} \parallel \zeta_p^k - 1$ and so $\delta^\tau = \delta$. But $\delta^\tau \equiv 1 + \lambda^3(\text{mod } \mathbf{P}^4)$ by (3.12) and (3.13). From $\delta^\tau = \delta$ we see that $2 \in \mathbf{P}$, a contradiction.

Thus there is no unit $\delta$ satisfying (3.12) and, in particular $1 + (\zeta_p^2 - \zeta_p)^3$ cannot be a unit in $\mathbb{Z}[\delta_p]$. Hence $R_{3p}(f)$ cannot be $\pm 1$ unless $t \equiv 1 (\text{mod } 3p)$, as required.

We can now complete the proof of Theorem 2.

Let $n \in \mathbb{N}$. If $n = 1$, we have $R_n(f) = R_1(f) = 1$, for all $t \geq 2$, and there is nothing more to prove. Now write $n = ab$, where $a = 2^r 3^s (r, s \geq 0)$ and $\gcd(6, b) = 1$. We may assume that $n = ab > 1$.

If $a = 1$ we use Lemma 3.1. If $b = 1$ and $a > 1$ we have from $R_n(f) = \pm 1$ that $R_{2^r}(f) = \pm 1$, so that $t \equiv 1 (\text{mod} 2^r)$, and also $R_{3^s}(f) = \pm 1$, so that $t \equiv 1 (\text{mod } 3^s)$. Hence $t \equiv 1 (\text{mod } a)$; i.e. $t \equiv 1 (\text{mod } n)$.

Finally, suppose that $a, b > 1$. From $R_n(f) = \pm 1$, we have $R_a(f) = \pm 1$, so that $t \equiv (\text{mod } a)$, by the above. Also $R_b(f)$ must be $\pm 1$, so that $t \equiv 1$ or $2 (\text{mod } b)$.

We rule out the case $t \equiv 2 (\text{mod } b)$ as follows. Since $a > 1$ and $b > 1$, $n$ has a divisor of the type $pq$, where $q = 2$ or $3$ and $p \geq 5$ is a prime divisor of $b$.

We must have $R_{pq}(f) = \pm 1$; hence $t \equiv 1 (\text{mod } p)$, by Lemma 3.3. Certainly $t \not\equiv 2 (\text{mod } b)$.

Since for every $n \in \mathbb{N}$ we certainly have $R_n(f) = \pm 1$ whenever $t \equiv 1 (\text{mod } n)$, the proof of Theorem 2 is completed.

**4. Concluding remarks.** (a) In place of the Gel'fond-Baker results, one may use "Skolem's $p$-adic method" [**3**, p. 67, 228] to obtain Theorem 1. For general $f$ the latter approach has various advantages, since explicit $p$-adic bounds for the $n$ with $R_n(f) = \pm 1$ can be obtained from Strassmann's theorem [**3**, p. 62].

(b) The polynomial $f(X) = X^t - X + 1$ was chosen in Theorem 2 since the corresponding groups $\Gamma(n, w)$ have attracted a good deal of attention (see the references in §0). However it is clear that the methods used in proving Theorem 2 will give useful information for more general $f$, particularly if $f$ has small height. (If $f(X) = \Sigma c_j X^j$, the *height* of $f$ is $\deg(f) + \Sigma |c_j|$.)

## REFERENCES


**1.** A. Baker, *Transcendental number theory* (Cambridge University Press, 1975).

**2.** C. M. Campbell and E. T. Robertson, The order of certain metacyclic groups. *Bull. London Math. Soc.* **6** (1974), 312–314.

**3.** J. W. S. Cassels, *Local fields*, London Math. Soc. Student Text No. 3 (Cambridge University Press, 1986).

**4.** J. H. Conway, Solution to Advanced Problem 5327, *American Math. Monthly* **74** (1967), 91–93.

**5.** A. O. Gel'fond, *Transcendental and algebraic numbers* (Dover, New York, 1960).

**6.** D. L. Johnson, A note on the Fibonacci groups, *Israel J. Math.* **17** (1974), 277–282.

**7.** D. L. Johnson, Presentations of groups London Math. Soc. Student Text No. 15 (Cambridge University Press, 1990).

**8.** D. L. Johnson and R. W. K. Odoni, Some results on symmetrically-presented groups, *Proc. Edinburgh Math. Soc.* **37** (1994), 227–237.

**9.** W. Narkiewicz, *Elementary and analytic theory of algebraic numbers* (2nd ed., Springer Verlag, 1990).

**10.** R. M. Thomas, The Fibonacci groups revisited, in *Groups, St. Andrews, 1989* (Cambridge University Press, 1994), 445–454.

**11.** R. M. Thomas, On a question of Kim concerning certain group presentations, *Bull. Korean Math. Soc.* **28** (1991), 219–224.


https://doi.org/10.1017/S0017089599950383 Published online by Cambridge University Press