

## ROOTS OF UNITY AS QUOTIENTS OF TWO ROOTS OF A POLYNOMIAL

ARTŪRAS DUBICKAS

(Received 1 March 2011; accepted 1 February 2012)

Communicated by I. E. Shparlinski

Dedicated to the memory of Alf van der Poorten

### Abstract

Let  $K$  be a number field. For  $f \in K[x]$ , we give an upper bound on the least positive integer  $T = T(f)$  such that no quotient of two distinct  $T$ th powers of roots of  $f$  is a root of unity. For each  $\varepsilon > 0$  and each  $f \in \mathbb{Q}[x]$  of degree  $d \geq d(\varepsilon)$  we prove that  $\log T(f) < (2 + \varepsilon)\sqrt{d \log d}$ . In the opposite direction, we show that the constant 2 cannot be replaced by a number smaller than 1. These estimates are useful in the study of degenerate and nondegenerate linear recurrence sequences over a number field  $K$ .

2010 *Mathematics subject classification*: primary 11R04; secondary 11R18, 11B37.

*Keywords and phrases*: root of unity, number field, linear recurrence sequence.

### 1. Introduction

Let  $K$  be a number field, that is, a finite extension of the field of rational numbers  $\mathbb{Q}$ , and let

$$f(x) := x^d + a_{d-1}x^{d-1} + \cdots + a_0 = \prod_{i=1}^d (x - \alpha_i) \in K[x]$$

be a monic polynomial of degree  $d \geq 2$ . It may happen that the quotient of two distinct roots of  $f$ , say,  $\alpha_i/\alpha_j$ ,  $1 \leq i < j \leq d$ , is a root of unity (for example, for  $f(x) = x^d - 2 \in \mathbb{Q}[x]$ ). We say that the polynomial  $f$  is *torsion-free* if no quotient of two distinct roots of  $f$  is a root of unity. In the case where  $f(x) = \prod_{i=1}^d (x - \alpha_i)$  is not torsion-free, the polynomial  $f_T(x) := \prod_{i=1}^d (x - \alpha_i^T)$  is torsion-free for some  $T \in \mathbb{N}$ . The smallest positive integer  $T = T(f)$  with this property is called the *torsion order* of  $f$ , so that torsion-free polynomials have torsion order one. For example, for the polynomial  $x^d - 2$ , we have  $T(x^d - 2) = d$ . The torsion order of a polynomial can be greater than its degree, for example,  $T(\Phi_d) = d$ , where  $\Phi_d$  is the  $d$ th cyclotomic polynomial of degree  $\varphi(d)$ . Note that the torsion order  $T(f)$  is independent of the field  $K$ . If  $f \in K[x]$

is not monic and has a leading coefficient  $a \in K \setminus \{0\}$  then the torsion order of  $f$  is defined as  $T(f/a)$ .

Here is the main result of this paper.

**THEOREM 1.** *Let  $K$  be a number field with  $k := [K : \mathbb{Q}]$ . For every  $f \in K[x]$  of degree  $d \geq 2$ ,*

$$\log T(f) < (1.053\,14 + \sqrt{6k})\sqrt{d \log(kd)}. \tag{1}$$

Furthermore, if  $\varepsilon > 0$  then

$$\log T(f) < (1 + \varepsilon)(1 + \sqrt{k})\sqrt{d \log d} \tag{2}$$

provided that  $d$  is large enough. On the other hand, for all  $\varepsilon > 0$  there exists  $d_0(\varepsilon)$  such that for each positive integer  $d \geq d_0(\varepsilon)$  there is a monic polynomial  $\Phi \in \mathbb{Z}[x] \subset K[x]$  of degree  $d$  for which

$$\log T(\Phi) > (1 - \varepsilon)\sqrt{d \log d}. \tag{3}$$

On replacing  $\varepsilon$  by  $\varepsilon/2$  in (2) and selecting  $K := \mathbb{Q}$ , we find that

$$\exp((1 - \varepsilon)\sqrt{d \log d}) < \max_{f \in \mathbb{Q}[x], \deg f = d} T(f) < \exp((2 + \varepsilon)\sqrt{d \log d}) \tag{4}$$

for each  $\varepsilon > 0$  and each sufficiently large  $d$ . Note that the difference between the upper and lower bounds in (4) is only in the constants 1 and 2.

The torsion order  $T$  of the polynomial  $f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0$  is related to the properties of the linear recurrence sequence

$$x_{n+d} = -a_{d-1}x_{n+d-1} - \dots - a_0x_n,$$

where  $n = 1, 2, \dots$ . Such a sequence is called *degenerate* if its characteristic polynomial  $f$  has a pair of distinct roots whose ratio is a root of unity and *nondegenerate* otherwise. On replacing  $f$  by  $f_T$ , where  $T$  is the torsion order of  $f$ , one reduces the study of arbitrary linear recurrence sequences to the study of nondegenerate sequences. Theorem 1.2 in [4] asserts that, for some  $t \leq T(f)$ , each subsequence  $x_{m+s}$ , where  $n = 1, 2, \dots$ , is either identically zero or nondegenerate. Other applications of the torsion order to the Skolem–Mahler–Lech theorem were mentioned by Berstel and Mignotte [2] (see also [4, Ch. 2]). Schinzel [11] used  $T(f)$  to treat an old problem of Pólya [9] on the description of rational functions  $\sum_{n=0}^{\infty} u_n x^n \in \mathbb{Q}(x)$  whose numerators are divisible by only finitely many primes. In this sense the bound in (4) gives the best possible (up to a constant) estimate in [11, Theorem 2]. See also [14], where the case  $K = \mathbb{Q}$  was considered. Robba [10] investigated the case of a number field, but his upper bound  $T(f) \leq 2^{kd+1}$  is weaker than that given in (1).

It seems likely that if  $f \in \mathbb{Q}[x]$  is irreducible over the field  $\mathbb{Q}$  then the upper bound for  $T(f)$  should be given by the inequality

$$\varphi(T(f)) \leq d, \tag{5}$$

where  $\varphi$  is Euler’s function. Note that equality holds in (5) for cyclotomic polynomials  $f = \Phi_d$ . Since  $\liminf_{n \rightarrow \infty} (\varphi(n) \log \log n)/n = e^{-\gamma}$ , where  $\gamma = 0.577\,21\dots$  is Euler’s

constant (see, for example, [5, Theorem 324]), the upper bound (5) via [11, Lemma 3] would imply the inequality

$$T(f) < e^\gamma d(\log \log d + 4) \tag{6}$$

for every  $d \geq 2$ . Unfortunately, the proof of Corollary 2.1 (which is equivalent to (5)) in our paper [3] contains an error. The best known bound in this direction is due to Schinzel [11] who showed that

$$T(f) < e^{3\gamma/2} d^{3/2} (\log \log d + 4)^{3/2}$$

for every irreducible polynomial  $f \in \mathbb{Q}[x]$  of degree  $d \geq 2$  (which is short of the conjectured bound (6)). In [1, 3, 6, 14], one can find different proofs of the inequality

$$[K(\zeta) : K] \leq d = [K(\alpha) : K]$$

when  $\alpha, \alpha'$  are two algebraic numbers conjugate over  $K$  and  $\zeta := \alpha/\alpha'$  is a root of unity. This shows that one can get rid of at least one root of unity among the ratios of roots of an irreducible polynomial  $f \in K[x]$  of degree  $d$  by taking some power  $t$  for which  $\varphi(t) \leq d$ .

In the next section we shall prove (3) and give another example which shows that for some  $f \in K[x]$  the torsion degree  $T(f)$  may tend to infinity as  $k \rightarrow \infty$  for cyclotomic extensions  $K$  of  $\mathbb{Q}$ . In Section 3 we state two results on the least common multiple of positive integers  $b_1, b_2, \dots, b_m$ , whose sum (or the sum of the values of Euler's function  $\varphi(b_1), \varphi(b_2), \dots, \varphi(b_m)$ ) does not exceed some fixed integer  $n$ . We give two more lemmas in Section 4, and then complete the proofs of (1) and (2) in Section 5.

## 2. Examples

Let  $X(d)$  be the largest integer for which

$$\sum_{p \leq X(d)} (p - 1) \leq d, \tag{7}$$

where the sum is taken over prime numbers  $p$ . Set

$$\Phi(x) := g(x) \prod_{p \leq X(d)} (x^{p-1} + \dots + x + 1), \tag{8}$$

where  $g(x) := \prod_{i=1}^e (x - i) \in \mathbb{Z}[x]$  is a polynomial of degree

$$e := d - \sum_{p \leq X(d)} (p - 1).$$

Then  $\Phi(x) \in \mathbb{Z}[x]$  is a monic polynomial of degree  $d$ . (Note that  $\Phi(x) \in \mathbb{Z}[x] \subset K[x]$  for every number field  $K$ .) Put

$$Y(d) := \prod_{p \leq X(d)} p, \tag{9}$$

where the product is taken over primes  $p$ . Clearly,  $\Phi_T$  is a torsion-free polynomial for  $T = Y(d)$ , since the  $T$ th powers of the roots of  $\Phi$  are  $i^T$ , where  $i = 1, \dots, e$ , and 1, because  $\zeta_p^{jY(d)} = 1$  whenever  $p \leq X(d)$  and  $j = 1, \dots, p - 1$ . (Throughout,  $\zeta_r := e^{2\pi i/r}$  is the primitive  $r$ th root of unity.) On the other hand, if some prime  $p \leq X(d)$  does not divide  $T$  then  $\Phi_T$  is not torsion-free, because the quotient of two distinct roots of  $\Phi_T$ , say  $\zeta_p^{2T}$  and  $\zeta_p^T$ , is a root of unity. Consequently, for the polynomial defined in (8),

$$T(\Phi) = Y(d).$$

Now, using the prime number theorem  $p_i \sim i \log i$  as  $i \rightarrow \infty$ , from (7) and (9) one can easily derive that

$$X(d) \sim \sqrt{d \log d} \quad \text{and} \quad \log Y(d) \sim X(d)$$

as  $d \rightarrow \infty$ . Hence the inequality  $\log T(\Phi) = \log Y(d) > (1 - \varepsilon)\sqrt{d \log d}$  holds for every  $d \geq d_0(\varepsilon)$  and every  $\varepsilon > 0$ . This proves (3).

Suppose next that  $K = \mathbb{Q}(\zeta_m)$ , where  $\varphi(m) = k$ , so that  $k = [K : \mathbb{Q}]$ . Let us take

$$G(x) := g_1(x) \prod_{m < p \leq X_1(d)} (x^p - \zeta_m),$$

where the product is taken over primes  $p$ , the number  $X_1(d)$  is the largest integer for which  $\sum_{m < p \leq X_1(d)} p \leq d$ , and  $g_1(x) := \prod_{i=1}^{e_1} (x - i)$  with  $e_1 := d - \sum_{m < p \leq X_1(d)} p$ . By the same argument as above, we see that  $G \in K[x]$  is a monic polynomial of degree  $d$  whose torsion order is

$$T(G) = m \prod_{m < p \leq X_1(d)} p > m \exp((1 - \varepsilon)\sqrt{d \log d})$$

for each  $\varepsilon > 0$  and each sufficiently large  $d$ . Since  $m > k$ , it follows that

$$\log T(G) > \log k + (1 - \varepsilon)\sqrt{d \log d}$$

for each  $\varepsilon > 0$  and each sufficiently large  $d$ .

### 3. Two results for the least common multiple

**LEMMA 2.** *Let  $b_1, \dots, b_m$  be some positive integers satisfying  $b_1 + \dots + b_m \leq n$ , where  $n \geq 2$ . Then*

$$\text{lcm}(b_1, \dots, b_m) < \exp(1.053 \, 14 \sqrt{n \log n}),$$

where lcm stands for the least common multiple. Furthermore, for each  $\varepsilon > 0$  there is an integer  $n_0(\varepsilon)$  such that, for every  $n \geq n_0(\varepsilon)$ ,

$$\text{lcm}(b_1, \dots, b_m) < \exp((1 + \varepsilon)\sqrt{n \log n}).$$

The first part of Lemma 2 was proved by Massias [7]. In fact,  $\text{lcm}(b_1, \dots, b_m)$  is the order of an element consisting of  $m$  disjoint cycles of lengths  $b_1, \dots, b_m$  in the

full symmetric group on  $n$  elements  $S_n$ . Let  $M(n)$  be the maximal order of an element in  $S_n$ . Landau proved that  $\log M(n) \sim \sqrt{n \log n}$  as  $n \rightarrow \infty$  and Shah [12] gave a more precise asymptotic formula

$$\log M(n) = \sqrt{n \log n} (1 + \log \log n / (2 \log n) + O(1/\log n)).$$

This implies the second part of Lemma 2. See also [8, 13] for further work on this problem. It is interesting to note that the upper bound  $1.053\ 13 \dots$  is attained for the symmetric group  $S_{1\ 319\ 766}$ .

The following lemma was proved by Berstel and Mignotte [2].

**LEMMA 3.** *Let  $b_1, \dots, b_m$  be positive integers satisfying  $\varphi(b_1) + \dots + \varphi(b_m) \leq n$ , where  $n \geq 2$ . Then*

$$\text{lcm}(b_1, \dots, b_m) < \exp(\sqrt{6n \log n}).$$

*Furthermore, the constant  $\sqrt{6}$  can be replaced by any constant strictly greater than 1 if  $n$  is sufficiently large.*

#### 4. Some divisibility results for the torsion order of a polynomial

Let  $f \in K[x]$  be a separable polynomial of degree  $d \geq 2$ . We say that two of its roots  $\alpha$  and  $\alpha'$  belong to the same equivalence class if their quotient is a root of unity. Suppose that there are  $s := s(f)$  distinct equivalence classes. It is easy to see that each equivalence class contains the same number of elements, say,  $\ell := \ell(f)$  roots of  $f$ , so

$$d = s\ell = s(f)\ell(f). \tag{10}$$

Now, let  $f \in K[x]$  be an irreducible polynomial of degree  $d \geq 2$ , and let  $\alpha$  be one of its roots. Suppose that  $r$  is the largest positive integer for which

$$\mathbb{Q}(\zeta_r) \subseteq K(\alpha). \tag{11}$$

Then  $K(\zeta_r) \subseteq K(\alpha)$ . Since  $K(\zeta_r)$  is a normal extension of  $K$ , the field  $K(\zeta_r)$  is contained in the field  $K(\alpha')$  for any conjugate  $\alpha'$  of  $\alpha$  over  $K$ . Hence  $\mathbb{Q}(\zeta_r)$  is contained in every field  $K(\alpha')$  too. Thus  $r := r(f, K)$  is independent of the choice of  $\alpha$  and depends only on the polynomial  $f$  and the field  $K$ . Of course,

$$r(f, K) = w(K(\alpha)), \tag{12}$$

where  $w(F)$  stands for the number of distinct roots of unity lying in the field  $F$ .

We claim that if  $\alpha \neq \alpha'$  and  $\alpha/\alpha'$  is a root of unity (so that  $\ell \geq 2$ ) then

$$\alpha^{\ell r} = (\alpha')^{\ell r}. \tag{13}$$

Indeed, write  $\gamma(C)$  for the product of conjugates of  $\alpha$  belonging to the equivalence class  $C$ . From  $\alpha, \alpha' \in C$  we obtain  $\alpha^\ell = \zeta\gamma(C)$  and  $(\alpha')^\ell = \zeta'\gamma(C)$  for some roots of unity  $\zeta, \zeta'$ . It is clear that  $s = s(f)$  equivalence classes are blocks of imprimitivity of the Galois group  $\text{Gal}(K(\alpha)/K)$ . Hence every automorphism  $\sigma \in \text{Gal}(K(\alpha)/K)$  satisfying  $\sigma(\alpha) = \alpha$  is a permutation of the set  $C$ , so it maps  $\gamma(C)$  to  $\gamma(C)$ . Thus  $\gamma(C) \in K(\alpha)$ .

This yields  $\zeta = \alpha^\ell / \gamma(C) \in K(\alpha)$ , so that  $\zeta \in \mathbb{Q}(\zeta_r)$ , by (11). Hence  $\zeta^r = 1$ . By the same argument,  $(\zeta')^r = 1$ . Therefore,

$$\left(\frac{\alpha}{\alpha'}\right)^{\ell r} = \left(\frac{\zeta\gamma(C)}{\zeta'\gamma(C)}\right)^r = \frac{\zeta^r}{(\zeta')^r} = 1.$$

This proves (13) and so implies the following result.

**LEMMA 4.** *The torsion order of an irreducible polynomial  $f \in K[x]$  satisfies*

$$T(f) \mid \ell(f)r,$$

where  $r := r(f, K)$  is defined in (11) and (12).

Next we extend this result to the product of two irreducible polynomials.

**LEMMA 5.** *Let  $f_1, f_2 \in K[x]$  be two distinct irreducible polynomials having  $\ell_1 := \ell(f_1)$  and  $\ell_2 := \ell(f_2)$  elements in their equivalence classes and with  $r_1 := r(f_1, K)$  and  $r_2 := r(f_2, K)$  defined as in (11) and (12). Then*

$$T(f_1 f_2) \mid \text{lcm}(\ell_1 \text{lcm}(r_1, r_2), \ell_2 \text{lcm}(r_1, r_2)).$$

**PROOF.** In view of Lemma 4 it suffices to prove that if  $\alpha$  is a root of  $f_1$  and  $\beta$  is a root of  $f_2$  such that  $\alpha/\beta$  is a root of unity then

$$\alpha^L = \beta^L,$$

where  $L := \text{lcm}(\ell_1 r, \ell_2 r)$  and  $r := \text{lcm}(r_1, r_2)$ . Suppose that  $\alpha$  and  $\beta$  belong to the equivalence classes  $C_1$  and  $C_2$ . As above, let  $\gamma(C_1)$  and  $\gamma(C_2)$  be the product of conjugates of  $\alpha$  from  $C_1$  and the product of conjugates of  $\beta$  from  $C_2$ . Then

$$\alpha^{\ell_1} = \xi_1 \gamma(C_1) \quad \text{and} \quad \beta^{\ell_2} = \xi_2 \gamma(C_2) \tag{14}$$

with some roots of unity  $\xi_1, \xi_2$ .

Let  $S$  be the set of  $\deg f_1 + \deg f_2$  roots of the polynomial  $f_1 f_2$ . The equivalence class of  $S$  containing  $\alpha$  consists of  $C_1 \cup C_2$ . Consider the Galois group  $\text{Gal}(K(\alpha, \beta)/K)$  as permutations of the set  $S$ . Each element  $\sigma \in \text{Gal}(K(\alpha, \beta)/K)$  that fixes  $\alpha$  (or  $\beta$ ) permutes the class  $C_1$  and the class  $C_2$ . Hence the products  $\gamma(C_1)$  and  $\gamma(C_2)$  both lie in the intersection  $K(\alpha) \cap K(\beta)$ . Thus  $\xi_1 \in K(\alpha)$  and  $\xi_2 \in K(\beta)$ , by (14). From (14), the quotient  $\zeta := \gamma(C_1)^{L/\ell_1 r} / \gamma(C_2)^{L/\ell_2 r}$  is a root of unity, because  $\alpha/\beta$  is a root of unity. Note that  $\zeta, \xi_1 \in K(\alpha)$  yields  $\zeta, \xi_1 \in \mathbb{Q}(\zeta_{r_1})$ , by the definition of  $r_1$ . Similarly,  $\zeta, \xi_2 \in K(\beta)$  yields  $\zeta, \xi_2 \in \mathbb{Q}(\zeta_{r_2})$ . It follows that  $\zeta, \xi_1, \xi_2$  lie in the compositum

$$\mathbb{Q}(\zeta_{r_1})\mathbb{Q}(\zeta_{r_2}) = \mathbb{Q}(\zeta_{r_1, r_2}) = \mathbb{Q}(\zeta_{\text{lcm}(r_1, r_2)}) = \mathbb{Q}(\zeta_r).$$

Now, using the fact that the root of unity  $\zeta \xi_1^{L/\ell_1 r} \xi_2^{-L/\ell_2 r}$  belongs to the field  $\mathbb{Q}(\zeta_r)$  (so that its  $r$ th power is 1), we obtain

$$\frac{\alpha^L}{\beta^L} = \frac{\xi_1^{L/\ell_1} \gamma(C_1)^{L/\ell_1}}{\xi_2^{L/\ell_2} \gamma(C_2)^{L/\ell_2}} = \left(\frac{\xi_1^{L/\ell_1} \zeta}{\xi_2^{L/\ell_2}}\right)^r = 1,$$

which completes the proof of the lemma. □

### 5. Proof of the upper bound for torsion order

Without loss of generality, we may assume that  $f \in K[x]$  is monic. Let us write  $f$  in the form

$$f(x) = f_1(x)^{k_1} f_2(x)^{k_2} \cdots f_m(x)^{k_m}$$

for distinct irreducible monic polynomials  $f_1, \dots, f_m \in K[x]$  and  $k_1, \dots, k_m \in \mathbb{N}$ . Obviously,  $T(f) = T(f_1 \cdots f_m)$  and the degree of the polynomial  $f_1 \cdots f_m$  is smaller than  $\deg f$  provided that at least one  $k_i$  is greater than 1. So we may assume that  $k_1 = \cdots = k_m = 1$ . Then, by Lemmas 4 and 5, for  $f = f_1 \cdots f_m$ ,

$$T(f) \mid \text{lcm}(\ell_1, \dots, \ell_m) \text{lcm}(r_1, \dots, r_m) \tag{15}$$

with  $r_i := r(f_i, K)$  defined in (11) and (12), because  $\text{lcm}(\ell_i \text{lcm}(r_i, r_j), \ell_j \text{lcm}(r_i, r_j))$  divides  $\text{lcm}(\ell_i, \ell_j) \text{lcm}(r_i, r_j)$  for all indices  $i, j$  in the range  $1 \leq i, j \leq m$ . From (10) we see that  $\ell_i \mid d_i$ , where  $d_i = \deg f_i$ . Thus  $\text{lcm}(\ell_1, \dots, \ell_m)$  divides  $\text{lcm}(d_1, \dots, d_m)$ . Using the equality  $\sum_{i=1}^m d_i = d = \deg f$  from Lemma 2 we deduce that

$$\text{lcm}(\ell_1, \dots, \ell_m) \leq \text{lcm}(d_1, \dots, d_m) < \exp(1.053 \, 14 \sqrt{d \log d}). \tag{16}$$

Suppose that  $\alpha_i$  is a root of  $f_i$  for  $i = 1, \dots, m$ . Then we see that  $\mathbb{Q}(\zeta_{r_i}) \subseteq K(\alpha_i)$  from (11). Hence  $[\mathbb{Q}(\zeta_{r_i}) : \mathbb{Q}] = \varphi(r_i)$  divides

$$[K(\alpha_i) : \mathbb{Q}] = [K : \mathbb{Q}] \cdot [K(\alpha_i) : K] = kd_i.$$

In particular,  $\varphi(r_i) \leq kd_i$  for each  $i = 1, \dots, m$  and thus

$$\sum_{i=1}^m \varphi(r_i) \leq k \sum_{i=1}^m d_i = kd.$$

Therefore, Lemma 3 implies that

$$\text{lcm}(r_1, \dots, r_m) < \exp(\sqrt{6kd \log(kd)}). \tag{17}$$

Now, from (15), multiplying (16) and (17) we derive (1).

Next, suppose that  $\varepsilon > 0$  and that  $d$  is large enough. Then, by Lemmas 2 and 3, inequality (16) becomes

$$\text{lcm}(\ell_1, \dots, \ell_m) \leq \text{lcm}(d_1, \dots, d_m) < \exp((1 + \varepsilon)\sqrt{d \log d}),$$

whereas (17) is replaced by

$$\text{lcm}(r_1, \dots, r_m) < \exp((1 + \varepsilon/2)\sqrt{kd \log(kd)}) < \exp((1 + \varepsilon)\sqrt{kd \log d}).$$

Multiplying these two inequalities, we derive (2) in view of (15).

## References

- [1] M. G. Aschbacher and R. M. Guralnick, ‘On Abelian quotients of primitive groups’, *Proc. Amer. Math. Soc.* **107** (1989), 89–95.
- [2] J. Berstel and M. Mignotte, ‘Deux propriétés décidables des suites récurrentes linéaires’, *Bull. Soc. Math. France* **104** (1976), 175–194.
- [3] P. Drungilas and A. Dubickas, ‘On subfields of a field generated by two conjugate algebraic numbers’, *Proc. Edinb. Math. Soc.* **47** (2004), 119–123.
- [4] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs, 104 (American Mathematical Society, Providence, RI, 2003).
- [5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (Oxford University Press, Oxford, 1979).
- [6] I. M. Isaacs, ‘Quotients which are roots of unity (solution of problem 6523)’, *Amer. Math. Monthly* **95** (1988), 561–562.
- [7] J.-P. Massias, ‘Majoration explicite de l’ordre maximum d’un élément du groupe symétrique’, *Ann. Fac. Sci. Toulouse Math.* **6** (1984), 269–281.
- [8] J.-P. Massias, J.-L. Nicolas and G. Robin, ‘Evaluation asymptotique de l’ordre maximum d’un élément du groupe symétrique’, *Acta Arith.* **104** (1988), 221–242.
- [9] G. Pólya, ‘Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen’, *J. reine angew. Math.* **151** (1921), 1–31.
- [10] Ph. Robba, ‘Zéros de suites récurrentes linéaires’, *Groupe Étude Anal. Ultramétrique*, 5 (1977/78), Exposé No. 13, 1978, 5 pp.
- [11] A. Schinzel, ‘Around Pólya’s theorem on the set of prime divisors of a linear recurrence’, in: *Diophantine Equations. Papers from the international conference held in honor of T. N. Shorey’s 60th birthday*, Mumbai, 16–20 December 2005, (ed. N. Saradha) (Narosa Publishing House, New Delhi, 2008), pp. 225–233.
- [12] S. Shah, ‘An inequality for the arithmetical function  $g(x)$ ’, *J. Indian Math. Soc.* **3** (1939), 316–318.
- [13] M. Szalay, ‘On the maximal order in  $S_n$  and  $S_n^{**}$ ’, *Acta Arith.* **37** (1980), 321–331.
- [14] K. Yokoyama, Z. Li and I. Nemes, ‘Finding roots of unity among quotients of the roots of an integral polynomial’, in: *Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation, ISSAC’95*, Montreal, 10–12 July 1995, (ed. A. H. M. Levelt) (ACM Press, New York, 1995), pp. 85–89.

ARTŪRAS DUBICKAS, Department of Mathematics and Informatics,  
 Vilnius University, Naugarduko 24, Vilnius LT-03225, Lithuania  
 e-mail: [arturas.dubickas@mif.vu.lt](mailto:arturas.dubickas@mif.vu.lt)