GLASNIK MATEMATIČKI
Vol. 52(72)(2017), 235 – 240

ROOTS OF UNITY AS QUOTIENTS OF TWO CONJUGATE ALGEBRAIC NUMBERS

Artūras Dubickas
Vilnius University, Lithuania

Abstract. Let α be an algebraic number of degree $d \geqslant 2$ over $\mathbb{Q}$. Suppose for some pairwise coprime positive integers $n_1, \dots, n_r$ we have $\deg(\alpha^{n_j}) < d$ for $j = 1, \dots, r$, where $\deg(\alpha^n) = d$ for each positive proper divisor n of n_j. We prove that then $\varphi(n_1 \dots n_r) \leqslant d$, where φ stands for the Euler totient function. In particular, if $n_j = p_j$, $j = 1, \dots, r$, are any r distinct primes satisfying $\deg(\alpha^{p_j}) < d$, then the inequality $(p_1 - 1) \cdots (p_r - 1) \leqslant d$ holds, and therefore $r \ll \log d / \log \log d$ for $d \geqslant 3$. This bound on r improves that of Dobrowolski $r \leqslant \log d / \log 2$ proved in 1979 and is best possible.

1. Introduction

Let α be an algebraic number of degree d with conjugates $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_d$ over $\mathbb{Q}$, and let n be a positive integer. If $D = \deg(\alpha^n)$ then the list $\alpha_1^n, \alpha_2^n, \dots, \alpha_d^n$ contains each of D conjugates of α^n exactly d/D times. In particular, $D = \deg(\alpha^n) < d$ if and only if $\mathbb{Q}(\alpha^n)$ is a proper subfield of $\mathbb{Q}(\alpha)$. For $n \geqslant 2$ and $d \geqslant 2$ this happens precisely when $\alpha^n = \alpha_j^n$ for some j in the range $2 \leqslant j \leqslant d$, so the quotient of two distinct conjugates of α is a root of unity.

Put

$$U(\alpha) := \{n \in \mathbb{N} \, : \, \deg(\alpha^n) < d\}.$$

Clearly, the set $U(\alpha)$ is either empty or infinite, since $n \in U(\alpha)$ implies $n\ell \in U(\alpha)$ for each $\ell \in \mathbb{N}$. Let $F(\alpha)$ be a subset of $U(\alpha)$ which is defined as

2010 *Mathematics Subject Classification.* 11R04, 11R18.

Key words and phrases. Root of unity, conjugate algebraic numbers, degenerate linear recurrence sequence.

follows:

$$F(\alpha) := \{n \in \mathbb{N} : \deg(\alpha^n) < d \quad \text{and} \quad \deg(\alpha^q) = d \\ \text{for each} \quad q \in \mathbb{N} \quad \text{satisfying} \quad q < n \quad \text{and} \quad q|n\}.$$

As we already observed above, $m \in F(\alpha)$ yields $\alpha^m = \alpha_j^m$ for some $j > 1$, so that $\alpha/\alpha_j = \exp(2\pi i u/m)$ with $u \in \mathbb{N}$ satisfying $1 \leqslant u < m$ and, by the definition of F, $\gcd(u, m) = 1$. In particular, $\deg(\exp(2\pi i u/m)) = \varphi(m)$ does not exceed the number of roots of unity in the field $\mathbb{Q}(\alpha_1, \ldots, \alpha_d)$, so that the set $F(\alpha)$ is finite. (Throughout, φ stands for Euler's totient function.) Moreover, writing

$$F(\alpha) = \{m_1, \ldots, m_k\},$$

where, by the definition of F, m_i does not divide m_j for $i \neq j$, we have

$$\varphi(m_1) + \cdots + \varphi(m_k) \leqslant d(d-1),$$

since there are $d(d-1)$ quotients of two distinct conjugates of α and the degree of each quotient which is a root of unity must be $\varphi(m_j)$ for some $j = 1, \ldots, k$. By the above, it is easy to see that the set $U(\alpha)$ can be also given in the form

$$U(\alpha) = \{\ell m : \ell \in \mathbb{N}, m \in F(\alpha)\}. \tag{1.1}$$

Various aspects of the sets $U(\alpha), F(\alpha)$ themselves and their complements $\mathbb{N} \setminus U(\alpha)$, $\mathbb{N} \setminus F(\alpha)$, the smallest positive integer t for which the sets $F(\alpha^t), U(\alpha^t)$ are empty, etc. with their applications to linear recurrence sequences and to other problems of number theory have been investigated in [1–6], [7, Chapter 2], [8, 11–13]. The relation of the problem to linear recurrence sequences rests on the fact that the sets $F(\alpha), U(\alpha)$ are empty iff the linear recurrence whose characteristic polynomial is the minimal polynomial of α over $\mathbb{Q}$ is nondegenerate.

In particular, one of the results of Dobrowolski in his famous paper [3], where a so far unbeaten estimate for the Mahler measure $M(\alpha)$ of an algebraic integer α which is not a root of unity was obtained, is the following:

THEOREM 1.1 (Lemma 3 in [3]). *For each α of degree $d \geqslant 2$ the set $U(\alpha)$ contains at most $\log d/\log 2$ prime numbers.*

Note that, by (1.1), the prime number p belongs to $U(\alpha)$ if and only if it belongs to $F(\alpha)$. So the same upper bound $\log d/\log 2$ also holds for the number of primes lying in $F(\alpha)$.

Although it is known that the main result of [3] can be obtained without the use of Theorem 1.1, this theorem is of interest itself. A stronger version of Theorem 1.1, although not best possible, was obtained by Matveev (see Lemma 6 and a subsequent remark in [10]). A slightly different proof of Theorem 1.1 is also given in the recent book of Masser [9, Lemma 16.3, p. 204].

[9, Exercise 16.6, p. 209] asks whether for $p_1, \dots, p_r \in U(\alpha)$, where $p_1, \dots, p_r$ are distinct primes, the bound

$$(p_1 - 1) \dots (p_r - 1) \leqslant d \tag{1.2}$$

is true.

The aim of this note is the next theorem which implies that the inequality (1.2) indeed holds.

THEOREM 1.2. *Let α be an algebraic number is of degree $d \geqslant 2$. Suppose that the set $F(\alpha)$ contains some pairwise coprime integers $n_1, \dots, n_r$. Then,*

$$\varphi(n_1 \dots n_r) \leqslant d.$$

In particular, if each $n_j = p_j$, $j = 1, \dots, r$, is a prime number, then (1.2) holds, since $\varphi(p_1 \dots p_r) = (p_1 - 1) \dots (p_r - 1)$. To show that the inequality (1.2) is best possible we can consider the number

$$\beta := \exp\Big(2\pi i\Big(\frac{1}{p_1} + \dots + \frac{1}{p_r}\Big)\Big). \tag{1.3}$$

Then, β is a root of unity, $\beta^{p_1 \dots p_r} = 1$ and $p_1 \dots p_r$ is the smallest positive integer q for which $\beta^q = 1$. Hence,

$$d = \deg(\beta) = \varphi(p_1 \dots p_r) = (p_1 - 1) \dots (p_r - 1).$$

The conjugates of β can be written in the form $\exp(2\pi i(k_1/p_1 + \dots + k_r/p_r))$, where $1 \leqslant k_j < p_j$ for $j = 1, \dots, r$. Thus, for β defined in (1.3), we have $p_j \in F(\beta)$ for $j = 1, \dots, r$ (in fact, $F(\beta) = \{p_1, \dots, p_k\}$). Hence, we for this β we have equality in (1.2).

Note that the left hand side of (1.2) is at least

$$(2-1) \cdot (3-1) \cdot (5-1) \cdot \dots \cdot (p_r - 1),$$

where p_r is the rth prime. By the prime number theorem, for this r one has the bound

$$r \leqslant c \frac{\log d}{\log \log d}, \tag{1.4}$$

where $d \geqslant 3$ and c is an absolute positive constant independent of α (and so independent of d). Here, we can take any c greater than 1 for d large enough. The bound (1.4) improves that of Theorem 1.1 and is best possible in the sense that there is an infinite sequence algebraic numbers α_k, $k = 1, 2, \dots$, such that $\deg \alpha_k = d_k \to \infty$ as $k \to \infty$ for which the number of primes in the set $U(\alpha_k)$ is asymptotic to

$$\frac{\log d_k}{\log \log d_k}$$

as $k \to \infty$.

In the proof of Theorem 1.2 we shall use the following:

LEMMA 1.3. *If α and α' are two conjugate algebraic numbers of degree $d \geqslant 2$ and $\zeta := \alpha/\alpha'$ is a root of unity, then* $\deg(\zeta) \leqslant d$.

Various proofs of Lemma 1.3 are given in [1, 4, 8, 13]. In the next section we shall prove Theorem 1.2.

2. Proof of Theorem 1.2

Let $\mathbb{L}$ be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ and $G := \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Assume that $n_1, \dots, n_r$ are pairwise coprime positive integers lying in $F(\alpha)$. Here, $n_1, \dots, n_r > 1$, since $1 \notin F(\alpha)$. Note that $n_j \in F(\alpha)$ yields $\alpha^{n_j} = \alpha_j^{n_j}$, where $\alpha_j \neq \alpha$ is a conjugate of α over $\mathbb{Q}$. Furthermore, by the definition of $F(\alpha)$, we have $\alpha^q \neq \alpha_j^q$ for any positive proper divisor q of n_j. Thus, $\zeta_j := \alpha/\alpha_j$ is a root of unity of the form $\zeta_j = \exp(2\pi i u_j/n_j)$, where $u_j \in \mathbb{N}$, $1 \leqslant u_j < n_j$ and $\gcd(u_j, n_j) = 1$.

Starting with $\zeta_1 = \alpha/\alpha_1$, we select an automorphism $\sigma_2 \in G$ which maps $\alpha \mapsto \alpha_1$. Applying it to $\zeta_2 = \alpha/\alpha_2$, we find that $\sigma_2(\zeta_2) = \alpha_1/\sigma_2(\alpha_2)$. Multiplying these equalities cancels α_1, so we obtain

$$\zeta_1\sigma_2(\zeta_2) = \frac{\alpha}{\alpha_1} \cdot \frac{\alpha_1}{\sigma_2(\alpha_2)} = \frac{\alpha}{\sigma_2(\alpha_2)}. \tag{2.1}$$

Next, we select $\sigma_3 \in G$ which maps $\alpha \mapsto \sigma_2(\alpha_2)$ and apply it to $\zeta_3 = \alpha/\alpha_3$. Multiplying (2.1) and $\sigma_3(\zeta_3) = \sigma_2(\alpha_2)/\sigma_3(\alpha_3)$ we further obtain

$$\zeta_1\sigma_2(\zeta_2)\sigma_3(\zeta_3) = \frac{\alpha}{\sigma_3(\alpha_3)}.$$

Continuing in this way with the next equality $\zeta_4 = \alpha/\alpha_4$, etc. up to $\zeta_r = \alpha/\alpha_r$ we derive that

$$\zeta_1\sigma_2(\zeta_2)\sigma_3(\zeta_3)\dots\sigma_r(\zeta_r) = \frac{\alpha}{\sigma_r(\alpha_r)}. \tag{2.2}$$

Since $\zeta_j \in \mathbb{L}$ for each $j = 2, \dots, r$, the number $\sigma_j(\zeta_j)$ is conjugate to ζ_j for $j = 2, \dots, r$. Hence, $\sigma_j(\zeta_j) = \exp(2\pi i w_j/n_j)$ for some $w_j \in \mathbb{N}$ satisfying $1 \leqslant w_j < n_j$, $\gcd(w_j, n_j) = 1$. Setting, for simplicity of notation, $w_1 := u_1$ we find that the left hand side of (2.2) is equal to

$$\zeta = \exp\Big(\frac{2\pi i w_1}{n_1}\Big)\prod_{j=2}^{r}\exp\Big(\frac{2\pi i w_j}{n_j}\Big) = \exp\Big(2\pi i\Big(\frac{w_1}{n_1} + \dots + \frac{w_r}{n_r}\Big)\Big). \tag{2.3}$$

Since ζ is a root of unity and, by (2.2) and (2.3), equals the quotient $\alpha/\sigma_r(\alpha_r)$ of two conjugates of α of degree d, from Lemma 1.3 we deduce that

$$\deg(\zeta) \leqslant d. \tag{2.4}$$

Consider the number

$$\frac{w_1}{n_1} + \dots + \frac{w_r}{n_r} = \frac{w}{n_1 \dots n_r}, \tag{2.5}$$

where $w := \sum_{i=1}^{r} w_i k_i$ and $k_i := \prod_{j \neq i} n_j$. We claim that $\gcd(w, n_1 \dots n_r) = 1$. Indeed, for a contradiction suppose that there is a prime number p which divides $n_1 \dots n_r$ and w. Without restriction of generality we can assume that $p|n_1$. Then, using $p|k_i$ for $i = 2, \dots, r$ and $p|w$, we deduce that $p|w_1 k_1$. However, in view of $\gcd(w_1, n_1) = 1$ and $p|n_1$ the number p does not divide w_1. Similarly, p does not divide $k_1 = n_2 \dots n_r$, since for each $j \geqslant 2$ the numbers n_j and n_1 are coprime.

Now, from (2.3) and (2.5), it follows that

$$\zeta = \exp(2\pi i w/(n_1 \dots n_r)),$$

where $w \in \mathbb{N}$ and $\gcd(w, n_1 \dots n_r) = 1$. Consequently, $\zeta^{n_1 \cdots n_r} = 1$, where $n_1 \dots n_r$ is the smallest positive integer with this property. Hence, $\deg(\zeta) = \varphi(n_1 \dots n_r)$ and so (2.4) implies the required inequality $\varphi(n_1 \dots n_r) \leqslant d$.

Acknowledgements.

I thank the referees for suggesting some simplifications and other useful remarks and corrections.

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 recurrentes linéaires,* Bull. Soc. Math. France **104** (1976), 175–194.

[3] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial,* Acta Arith. **34** (1979) 391–401.

[4] P. Drungilas and A. Dubickas, *On subfields of a field generated by two conjugate algebraic numbers,* Proc. Edinburgh Math. Soc. **47** (2004), 119–123.

[5] A. Dubickas, *Roots of unity as quotients of two roots of a polynomial,* J. Austral. Math. Soc. **92** (2012), 137–144.

[6] A. Dubickas and M. Sha, *Counting degenerate polynomials of fixed degree and bounded height,* Monatsh. Math. **177** (2015), 517–537.

[7] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, Recurrence sequences, Mathematical Surveys and Monographs 104, American Mathematical Society, Providence, RI, 2003.

[8] I. M. Isaacs, *Quotients which are roots of unity (solution of problem* 6523*),* Amer. Math. Monthly **95** (1988), 561–562.

[9] D. Masser, Auxiliary polynomials in number theory, Cambridge Tracts in Mathematics 207, Cambridge University Press, Cambridge, 2016.

[10] E. M. Matveev, *On a connection between the Mahler measure and the discriminant of algebraic numbers,* Math. Notes **59** (1996), 293–297.

[11] P. Robba, *Zéros de suites récurrentes linéaires,* Groupe Étude Anal. Ultramétrique, 5e Année (1977/78), Exposé No. 13, Paris, 1978, 5 p.

[12] A. Schinzel, *Around Pólya's theorem on the set of prime divisors of a linear recurrence,* in: Diophantine equations. Tata Inst. Fund. Res. Stud. Math., 20, Tata Inst. Fund. Res., Mumbai, 2008, pp. 225–233.

[13] 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 (ed. A.H.M. Levelt), ISSAC'95, Montreal, Canada, July 10–12, 1995, New York, NY: ACM Press, 1995, pp. 85–89.

A. Dubickas
Department of Mathematics and Informatics
Vilnius University
Naugarduko 24, Vilnius LT-03225
Lithuania
E-mail: `arturas.dubickas@mif.vu.lt`

Received: 13.4.2017.
Revised: 29.5.2017.