ROOTS OF UNITY AS QUOTIENTS OF TWO CONJUGATE ALGEBRAIC NUMBERS

Artūras Dubickas
Vilnius University, Lithuania

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

1. Introduction

Let \( \alpha \) be an algebraic number of degree \( d \) with conjugates \( \alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d \) over \( \mathbb{Q} \), and let \( n \) be a positive integer. If \( D = \deg(\alpha^n) \) then the list \( \alpha_1^n, \alpha_2^n, \ldots, \alpha_d^n \) contains each of \( D \) conjugates of \( \alpha^n \) 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 \( n \geq 2 \) and \( d \geq 2 \) this happens precisely when \( \alpha^n = \alpha_j^n \) for some \( j \) in the range \( 2 \leq j \leq d \), so the quotient of two distinct conjugates of \( \alpha \) 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.

235
follows:

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

As we already observed above, \( m \in F(\alpha) \) yields \( \alpha^m = \alpha_j^n \) for some \( j > 1 \), so that \( \alpha/\alpha_j = \exp(2\pi i u / m) \) with \( u \in \mathbb{N} \) satisfying \( 1 \leq u < m \) 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, \( \varphi \) 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

\[ \varphi(m_1) + \cdots + \varphi(m_k) \leq d(d - 1), \]

since there are \( d(d-1) \) quotients of two distinct conjugates of \( \alpha \) 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

\[ (1.1) \quad U(\alpha) = \{ \ell m : \ell \in \mathbb{N}, m \in F(\alpha) \} . \]

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 \( \alpha \) 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 \( \alpha \) which is not a root of unity was obtained, is the following:

**Theorem 1.1 (Lemma 3 in [3]).** For each \( \alpha \) of degree \( d \geq 2 \) 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 \( p_1, \ldots, p_r \in U(\alpha) \), where \( p_1, \ldots, p_r \) are distinct primes, the bound
\begin{equation}
(p_1 - 1) \cdots (p_r - 1) \leq d
\end{equation}
is true.

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

**Theorem 1.2.** Let \( \alpha \) be an algebraic number of degree \( d \geq 2 \). Suppose that the set \( F(\alpha) \) contains some pairwise coprime integers \( n_1, \ldots, n_r \). Then,
\[ \varphi(n_1 \cdots n_r) \leq d. \]

In particular, if each \( n_j = p_j \), \( j = 1, \ldots, r \), is a prime number, then (1.2) holds, since \( \varphi(p_1 \cdots p_r) = (p_1 - 1) \cdots (p_r - 1) \). To show that the inequality (1.2) is best possible we can consider the number
\begin{equation}
\beta := \exp \left( 2\pi i \left( \frac{1}{p_1} + \cdots + \frac{1}{p_r} \right) \right).
\end{equation}
Then, \( \beta \) is a root of unity, \( \beta^{p_1 \cdots p_r} = 1 \) and \( p_1 \cdots p_r \) is the smallest positive integer \( q \) for which \( \beta^q = 1 \). Hence,
\[ d = \deg(\beta) = \varphi(p_1 \cdots p_r) = (p_1 - 1) \cdots (p_r - 1). \]

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

Note that the left hand side of (1.2) is at least
\[ (2 - 1) \cdot (3 - 1) \cdot (5 - 1) \cdots (p_r - 1), \]
where \( p_r \) is the \( r \)th prime. By the prime number theorem, for this \( r \) one has the bound
\begin{equation}
r \leq c \frac{\log d}{\log \log d},
\end{equation}
where \( d \geq 3 \) and \( c \) is an absolute positive constant independent of \( \alpha \) (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 \( \alpha_k, k = 1, 2, \ldots \), 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 \( \alpha \) and \( \alpha' \) are two conjugate algebraic numbers of degree \( d \geq 2 \) and \( \zeta := \alpha/\alpha' \) is a root of unity, then \( \deg(\zeta) \leq d \).

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 \( L \) be the Galois closure of \( \mathbb{Q}(\alpha) \) over \( \mathbb{Q} \) and \( G := \text{Gal}(L/\mathbb{Q}) \). Assume that \( n_1, \ldots, n_r \) are pairwise coprime positive integers lying in \( F(\alpha) \). Here, \( n_1, \ldots, n_r > 1 \), 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 \( \alpha \) 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 and, by (2.2) and (2.3), equals the quotient \( \frac{\alpha}{\sigma_j(\alpha_j)} \). Hence, \( \sigma_j(\zeta_j) = \zeta_j \) for any positive proper divisor \( q \) of \( n_j \). Setting, for simplicity of notation, \( w_j := n_j \) for each \( j = 2, \ldots, r \) and \( \sigma_j(\zeta_j) = \zeta_j \).

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

(2.2) \[ \zeta_1 \sigma_2(\zeta_2) \sigma_3(\zeta_3) \cdots \sigma_r(\zeta_r) = \frac{\alpha}{\sigma_r(\alpha_r)}. \]

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

(2.3) \[ \zeta = \exp \left( \frac{2\pi i w_1}{n_1} \prod_{j=2}^r \frac{2\pi i w_j}{n_j} \right) = \exp \left( 2\pi i \left( \frac{w_1}{n_1} + \cdots + \frac{w_r}{n_r} \right) \right). \]

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

(2.4) \[ \deg(\zeta) \leq d. \]

Consider the number

(2.5) \[ \frac{w_1}{n_1} + \cdots + \frac{w_r}{n_r} = \frac{w}{n_1 \cdots n_r}. \]
where \( w := \sum_{i=1}^{r} w_i k_i \) and \( k_i := \prod_{j \neq i} n_j \). We claim that \( \gcd(w, n_1 \ldots n_r) = 1 \). Indeed, for a contradiction suppose that there is a prime number \( p \) which divides \( n_1 \ldots n_r \) and \( w \). Without restriction of generality we can assume that \( p \mid n_1 \). Then, using \( p \mid k_i \) for \( i = 2, \ldots, r \) and \( p \mid w \), we deduce that \( p \mid w_1 k_1 \).

However, in view of \( \gcd(w_1, n_1) = 1 \) and \( p \mid n_1 \) the number \( p \) does not divide \( w_1 \). Similarly, \( p \) does not divide \( k_1 = n_2 \ldots n_r \), since for each \( j \geq 2 \) the numbers \( n_j \) and \( n_1 \) are coprime.

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

\[
\zeta = \exp\left(\frac{2\pi i w}{n_1 \ldots n_r}\right),
\]

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

Acknowledgements.

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

References
