ALGEBRAIC INTEGERS WITH SMALL ABSOLUTE SIZE

ARTŪRAS DUBICKAS

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-03225 Vilnius, Lithuania.
E-Mail arturas.dubickas@mif.vu.lt

Abstract. In this paper we show that for each $k \geq 2$ there are infinitely many algebraic integers with norm $k$ and absolute normalized size smaller than 1. We also show that the lower bound $(n + s \log 2)/2$ on the square of the absolute size $\|\alpha\|$ of an algebraic integer $\alpha$ of degree $n$ with exactly $s$ real conjugates over $\mathbb{Q}$ is best possible for each even $s \geq 2$. For this, for each pair $s, k \geq 2$, where $s$ is even, we construct algebraic integers $\alpha$ with exactly $s$ real conjugates and norm of modulus $k$ satisfying $\deg \alpha = n$ and $\|\alpha\|^2 = (n + s \log 2)/2 + \log k + O(n^{-1})$ as $n \to \infty$. Finally, using the third smallest Pisot number $\theta_3$, which is the root of the polynomial $x^5 - x^4 - x^3 + x^2 - 1$, we construct algebraic integers $\alpha$ of degree $n$ that have exactly one real conjugate and satisfy $\|\alpha\|^2 \leq n/2 + 0.346981 \ldots$ (which is quite close to the above lower bound $(n + \log 2)/2 = n/2 + 0.346573 \ldots$ for $s = 1$). In the proofs we use some irreducibility theorems for lacunary polynomials and the Erdős and Turán bound on the number of roots of a polynomial in a sector.

Mathematics Subject Classification (2010): 11R06, 11R09, 11H06.

Key words: Lattice, the shortest vector, algebraic number field, absolute size, absolute normalised size.

1. Introduction. Let $\alpha$ be an algebraic number of degree $n$ over $\mathbb{Q}$ with $2t$ complex (nonreal) conjugates $\alpha_1, \ldots, \alpha_{2t}$, $\alpha_{t+1} = \overline{\alpha_1}, \ldots, \alpha_{2t} = \overline{\alpha_t}$ and $s$ real conjugates $\alpha_{2t+1}, \ldots, \alpha_{2t+s}$. We say that $(s, t)$ is the signature of $\alpha$. Recently, in [6] we studied the absolute size of $\alpha$ defined by

$$
\|\alpha\| := \left( \sum_{j=1}^{t} |\alpha_j|^2 + \sum_{i=1}^{s} \alpha_{2t+i}^2 \right)^{1/2},
$$

and the absolute normalised size of $\alpha$ defined by $\sqrt{m(\alpha)}$, where

$$
m(\alpha) := \frac{\|\alpha\|^2}{s + t}.
$$

A motivation for this study was some earlier work on certain lattices defined by number fields, when in the ring of integers $\mathcal{O}_K$ of a number field $K$ with $s$ real embeddings $\sigma_i$, $i = 1, \ldots, s$, and $2t$ complex embeddings $\tau_j, \tau_j^*$, $j = 1, \ldots, t$, one considers the vectors

$$(\sigma_1(\alpha), \ldots, \sigma_s(\alpha), \Re(\tau_1(\alpha)), \Im(\tau_1(\alpha)), \ldots, \Re(\tau_t(\alpha)), \Im(\tau_t(\alpha))) \in \mathbb{R}^n$$
defined for $\alpha \in \mathcal{O}_K$ (see [1, Chapter 8, Section 7]). This can be applied to show that the class number of a number field is finite [11]. A different but at the same time quite similar to (1) norm related to certain number field codes has been considered in [9]; see also [2].

As for absolute size $\|\alpha\|$ defined in (1), Tsfasman [20, Lemma 1.1(ii)] has shown that the minimal value of $\|\alpha\|$, when $\alpha$ runs through all nonzero algebraic integers with signature $(s, t)$, is between $(t + s)^{1/2}$ and $(t + s/2)^{1/2} = (n/2)^{1/2}$. Then, the latter lower bound has been improved in [17, Theorem 5.11] to $(n/2)^{1/2}2^{s/(2n)}$. To state this result in a slightly more general form, for a monic polynomial $f \in \mathbb{R}[x]$ of degree $n = 2t + s$ with $2t$ nonreal roots $\alpha_1, \ldots, \alpha_t, \bar{\alpha}_1, \ldots, \bar{\alpha}_t$ and $s$ real roots $\alpha_{2t+1}, \ldots, \alpha_n$, we define

$$
(2) \quad \|f\| := \left(\sum_{j=1}^{t} |\alpha_j|^2 + \sum_{i=1}^{s} \alpha_{2t+i}^2\right)^{1/2}.
$$

Note that, by (2), for any monic polynomials $f_1, \ldots, f_m \in \mathbb{R}[x]$ we have

$$
(3) \quad \|f_1 \cdots f_m\|^2 = \sum_{j=1}^{m} \|f_j\|^2.
$$

In case $f$ is a monic irreducible polynomial in $\mathbb{Z}[x]$, by (1) and (2), for any of its roots $\alpha$ we clearly have $\|f\| = \|\alpha\|$.

Now, by the same simple argument as in [6], let us show that the inequality

$$
(4) \quad \|f\|^2 \geq n2^{s/n-1}|f(0)|^{2/n}
$$

holds for any monic polynomial $f \in \mathbb{R}[x]$ of degree $n$ with $s$ real roots and $2t = n - s$ nonreal roots. Indeed, put $Y := \prod_{j=1}^{t} |\alpha_j|$ and $X := \prod_{i=1}^{s} |\alpha_{2t+i}|$. For $s = 0$, by (2) and AM-GM inequality, we have $\|f\|^2 \geq tY^2/t = t|f(0)|^{1/t} = (n/2)|f(0)|^{2/n}$, which is (4). Similarly, one obtains (4) for $s = n$. Assume that $st > 0$ and $|f(0)| > 0$ (which can be assumed without restriction of generality). Then, by AM-GM and $XY^2 = |f(0)|$, we find that

$$
\|f\|^2 \geq s|X|^{2/s} + t|Y|^{2/t} = s|X|^{2/s} + t|f(0)|^{1/t}|X|^{-1/t}.
$$

The minimum of the function $\varphi(x) := sx^{2/s} + t|f(0)|^{1/t}x^{-1/t}$ on the half line $x > 0$ is attained for $x_0 = 2^{-st/(s+2t)}|f(0)|^{s/(s+2t)}$, which is the root of the equation $2x^{2/s-1} = |f(0)|^{1/t}x^{-1/t-1}$. A simple calculation shows that $\varphi(x_0) = n2^{s/n-1}|f(0)|^{2/n}$, which implies (4). In particular, equality in (4) is attained for the monic polynomial

$$
f(x) = (x + 2^{-t/n}k^{1/n})^s(x^{2t} + 2^{st/n}k^{2t/n}) \in \mathbb{R}[x],
$$

where $f(0) = k > 0$.

Note that (4) implies

$$
\|f\|^2 \geq \frac{n}{2} + \frac{s \log 2}{2} + \log k
$$
for every monic \( f \in \mathbb{R}[x] \) with exactly \( s > 0 \) real roots and \( |f(0)| = k \geq 1 \). In particular, restricting \( f \) to monic irreducible polynomials in \( \mathbb{Z}[x] \) we deduce the following: if \( \alpha \) is a nonzero algebraic integer of degree \( n \) with signature \( (s, (n-s)/2) \), \( s > 0 \), and norm satisfying \( |\text{Norm}(\alpha)| = k \) then for the square of absolute size \( \|\alpha\|^2 \) the inequality

\[
\|\alpha\|^2 > \frac{n}{2} + \frac{s \log 2}{2} + \log k
\]

holds. (Recall that the \textit{norm} of \( \alpha \in \mathbb{Q} \), \( \text{Norm}(\alpha) \), is the product of its conjugates over the field \( \mathbb{Q} \).)

In the opposite direction, in [6], for each sufficiently large \( n \) of the form \( 4r + 2 \), \( r \in \mathbb{N} \), we gave an example of an algebraic unit \( \alpha \) of degree \( n \) with \( s = 2 \) real conjugates for which

\[
\|\alpha\|^2 = \frac{n}{2} + \log 2 + O(n^{-1/4}).
\]

This shows that the inequality (5) is best possible for \( s = 2 \) and \( k = 1 \) (in the sense that one cannot add to the right hand side of (5) a positive constant independent of \( n \)).

The next theorem shows that for each even \( s \geq 2 \) and each \( k \in \mathbb{N} \) the bound (5) is best possible and so it implies the answer to Question 5.3 raised in [6]:

**Theorem 1.** Let \( s \geq 2 \) be a fixed even integer, and let \( k \in \mathbb{N} \). Then, there is a sequence of positive integers \( n \) such that for each such \( n \) there is an algebraic integer \( \alpha \) of degree \( n \) with exactly \( s \) real conjugates and norm of modulus \( k \) satisfying

\[
\|\alpha\|^2 = \frac{n}{2} + \frac{s \log 2}{2} + \log k + O(n^{-1}),
\]

where the constant implied in \( O \) depends on \( s \) and \( k \) only.

In [6] we also asked whether the inequality \( m(\alpha) < 1 \) can only hold for an algebraic integer \( \alpha \neq 0 \) when \( \alpha \) is a unit (Question 5.1). Using (4) with a monic irreducible \( f \in \mathbb{Z}[x] \), it was shown that a possible such algebraic integer \( \alpha \) that is not a unit and satisfies \( m(\alpha) < 1 \) (if it exists) should be of degree at least 24.

The next result contains a negative answer to Question 5.1 in [6].

**Theorem 2.** For each \( k \in \mathbb{N} \) there are infinitely many algebraic integers \( \alpha \) satisfying \( |\text{Norm}(\alpha)| = k \) and \( m(\alpha) < 1 - 1/n \), where \( n \) is the degree of \( \alpha \).

Theorem 2 immediately follows from Theorem 1. Indeed, for each \( k \geq 1 \) select an even \( s \geq 2 \) satisfying

\[
4 + 2 \log k < s(1 - \log 2).
\]

(If, for instance, \( k = 2 \) we can take \( s = 18 \).) Then, as \( n = 2t + s \), by the inequality (7), we obtain

\[
\frac{n}{2} + \frac{s \log 2}{2} + \log k < t + s - 2.
\]
Hence, by Theorem 1, there exist infinitely many \( n \in \mathbb{N} \) with the property that for each such \( n \) there are algebraic integers \( \alpha \) with degree \( n \), signature \( (s, (n - s)/2) \) and norm of modulus \( k \) satisfying \( \|\alpha\|^2 < t + s - 1 \) (see (6)). Consequently,

\[
m(\alpha) = \frac{\|\alpha\|^2}{s + t} < \frac{s + t - 1}{s + t} = 1 - \frac{1}{s + t} < 1 - \frac{1}{n}
\]

for each such \( \alpha \). This completes the proof of Theorem 2. (In particular, \( \alpha \) is not a unit whenever \( k \geq 2 \).)

In [6], we showed that the smallest value of the square of normalized size, i.e. the quantity \( m(\alpha) \), where \( \alpha \) runs through all nonzero algebraic integers, should be greater than \( (e \log 2)/2 = 0.942084 \ldots \) and asked to find it explicitly. It was shown there that the smallest corresponding value among algebraic integers of degree at most 6 is

\[
m(\zeta) = \frac{\zeta^2 + \zeta^{-1}}{2} = 0.946467 \ldots,
\]

where \( \zeta = 0.826031 \ldots \) is the root of \( x^6 + x^2 - 1 = 0 \).

Theorem 1 itself follows from the following explicit construction, which is the main result of this paper:

**Theorem 3.** Let \( s \geq 2 \) be an even integer, and let \( k \in \mathbb{N} \). Suppose \( \gamma = \gamma_1 > 0 \) is a totally positive algebraic integer of degree \( m = s/2 \geq 1 \) over \( \mathbb{Q} \) with conjugates \( \gamma_1 < \gamma_2 < \cdots < \gamma_m \) and norm

\[
\text{Norm}(\gamma) = \gamma_1 \ldots \gamma_m = k
\]

satisfying, in addition, \( \sqrt{\gamma} \notin \mathbb{Q}(\gamma) \) for \( m = \deg \gamma \geq 2 \). Then, there is an even positive integer \( M_0 \) depending on \( \gamma \) only such that for each integer \( N = 2(rM_0 + m_0) \), where \( r, m_0 \in \mathbb{N} \), \( m_0 < M_0 \) and \( \gcd(M_0, m_0) = 1 \), the polynomial

\[
f_{\gamma}(x) := \prod_{\ell=1}^{m} (x^N + 2\gamma_\ell x^2 - \gamma_\ell)
\]

(a) has degree \( n = mN \),

(b) satisfies \( |f_{\gamma}(0)| = k \),

(c) is a monic irreducible polynomial in \( \mathbb{Z}[x] \),

(d) has exactly \( s \) real roots,

and satisfies

\[
\|f_{\gamma}\|^2 = \frac{n}{2} + \frac{s \log 2}{2} + \log k + O(n^{-1}),
\]

where the constant implied in \( O \) depends only on \( \gamma \).
To finalize the result of Theorem 3 we need to show that the algebraic integer \( \gamma \) as described in the statement of the theorem exists. For \( m = 1 \) we can simply take \( \gamma = k \) of degree \( m = 1 \). It is a totally positive algebraic integer with norm \( k \).

For \( m \geq 2 \) and \( k \in \mathbb{N} \), by the lemma below, there are infinitely many totally positive algebraic integers \( \gamma \) of degree \( m \) and norm \( k \) satisfying the additional condition \( \sqrt{\gamma} \notin \mathbb{Q}(\gamma) \).

**Lemma 4.** Given positive integers \( m \geq 2 \) and \( k \), and a positive number \( \delta \), there are infinitely many positive integers \( T \) for which the polynomial

\[
g(x) := x(x-1) \ldots (x-m+2)(x-T) + (-1)^m k \in \mathbb{Z}[x]
\]

is irreducible over \( \mathbb{Q} \) and its smallest root \( \gamma \) is a totally positive algebraic integer of degree \( m \) and norm \( k \) satisfying \( 0 < \gamma < \delta \) and \( \sqrt{\gamma} \notin \mathbb{Q}(\gamma) \).

Intervals of the real axis containing full sets of conjugates of an algebraic unit (this corresponds to the case \( k = 1 \)) have been investigated by Robinson in [12].

In the next theorem we give an example of the polynomial with one real root and small absolute size.

**Theorem 5.** For each \( n = 6r + 1 \), where \( r \) is a sufficiently large positive integer, the monic polynomial

\[
-1 + x^2 + \sum_{j=5}^{n} x^j
\]

is irreducible over \( \mathbb{Q} \). Moreover, it has a unique real root \( \alpha \) satisfying

\[
\|\alpha\|^2 \leq \frac{n-1}{2} + \theta_3^{-2} + \log \theta_3 + O(n^{-1/4}) = \frac{n}{2} + 0.346981 \ldots + O(n^{-1/4}),
\]

where \( \theta_3 = 1.443268 \ldots \) is the real root of the polynomial

\[
x^5 - x^4 - x^3 + x^2 - 1.
\]

This can be compared to the lower bound (5), which for \( s = k = 1 \) gives

\[
\|\alpha\|^2 > (n + \log 2)/2 = n/2 + 0.346573 \ldots
\]

with numerical constant quite close to the one of Theorem 5. In fact, the root \( \theta_3 \) of the polynomial (10) is the third smallest Pisot number (see [4], [5]). The first two have been found by Siegel [18].

One of the key results in the proof of Theorem 5 is the following lemma of independent interest. Recall that the Mahler measure of a polynomial

\[
g(x) := a_r(x - \alpha_1) \ldots (x - \alpha_r) \in \mathbb{C}[x], \quad a_r \neq 0,
\]

is \( M(g) := |a_r| \prod_{j=1}^{r} \max\{1, |\alpha_j|\} \).

**Lemma 6.** Let \( g(x) := a_r x^r + \cdots + a_1 x + a_0 \in \mathbb{R}[x] \), where \( a_r a_0 \neq 0 \), be a polynomial which has no roots on the unit circle \(|z| = 1\), and let \( q > 0 \) be a fixed constant.
Then, there is an integer \( n_0 \) which depends on \( g \) and \( q \) only such that for each integer \( n \geq n_0 \) we have

\[
\sum_{j=1}^{t} |\beta_j|^q \leq t + \frac{q}{2} \log M(g) + O(n^{-1/4}),
\]

where \( \beta_1, \ldots, \beta_t, \overline{\beta_1}, \ldots, \overline{\beta_t} \) are all \( 2t \) nonreal roots of the shifted polynomial \( x^n + g(x) \) (counted with multiplicities) and \( M(g) \) is the Mahler measure of the polynomial \( g \). Furthermore, we have equality in (11) if for some fixed constant \( c_0 \) the inequality \( |\beta_j| > 1 - c_0/\sqrt{n} \) holds for each \( j = 1, \ldots, t \).

We remark that, in principle, the condition on \( g \) to have no roots of modulus 1 can be removed at the expense of a slightly worse error term in (11). However, since this involves some further complications and mainly because Lemma 6 is later only used for the polynomial (10) when this condition on \( g \) holds, we prefer to give the proof only in the case as it is stated.

In the proof of Theorem 3 instead of Lemma 6 we shall use the next simple result:

**Lemma 7.** Let \( c_1, c_2, q \) be three positive constants, and \( \beta_1, \ldots, \beta_t \) be some complex numbers satisfying \( 1 - c_1/t < |\beta_j| < 1 + c_2/t \) for \( j = 1, \ldots, t \). Then, for \( t \) large enough we have

\[
\sum_{j=1}^{t} |\beta_j|^q = t + q \log \left( \prod_{j=1}^{t} |\beta_j| \right) + O(t^{-1}),
\]

where the constant implied in \( O \) depends on \( c_1, c_2 \) and \( q \) only.

**Proof.** Since \(|q \log |\beta_j|| = O(t^{-1})\), we can write

\[
|\beta_j|^q = e^{q \log |\beta_j|} = 1 + q \log |\beta_j| + O(t^{-2}).
\]

Thus, adding over \( j = 1, \ldots, t \) we obtain (12). \( \Box \)

In the next section we will state some earlier results which will be used in our proofs later on. Then, in Section 3, we will give some irreducibility results and also prove Lemma 4. Section 4 contains the proof of Lemma 6. Finally, in Section 5 we will complete the proofs of Theorems 3 and 5.

### 2. Some earlier results.

The next lemma is due to Erdős and Turán [7].

**Lemma 8.** Let \( N_P(\phi, \varphi) \) be the number of roots of a complex polynomial \( P(x) := a_d x^d + \cdots + a_0 \in \mathbb{C}[x] \), where \( a_d a_0 \neq 0 \), whose arguments belong to the interval \([\phi, \varphi) \subseteq [0, 2\pi)\). Then,

\[
\left| N_P(\phi, \varphi) - \frac{\varphi - \phi}{2\pi} d \right| \leq 16 \sqrt{d \log(L(P)/\sqrt{|a_d a_0|})},
\]

where \( L(P) := \sum_{j=0}^{d} |a_j| \).
In [8], Ganelius replaced the constant 16 by the smaller constant \( \sqrt{2\pi/G} = 2.61 \ldots \), where \( G = \sum_{j=1}^{\infty} (-1)^{j+1}/(2j - 1)^2 \) is Catalan’s constant. Lemma 8 will be one of the key ingredients in the proof of our Lemma 6 in Section 4.

Recall that a number field \( \mathbb{K} \) is called Kroneckerian if it is totally real, namely, its all embeddings are real, or \( \mathbb{K} \) is a totally complex quadratic extension of a totally real field. For a number field \( \mathbb{K} \) write a monic polynomial \( f \in \mathbb{K}[x] \) as the product \( f(x) = \prod f_i(x) \) with monic factors \( f_i \in \mathbb{K}[x] \) irreducible over \( \mathbb{K} \). Then, the noncycloptomic part of \( f \) is the product of its noncycloptomic factors \( f_i \). For instance, for \( \mathbb{K} = \mathbb{Q} \), the noncycloptomic part of the polynomial
\[
x^9 - x^8 - x^6 + 3x^5 - x^4 - x^3 - 2x^2 + x + 1 = (x - 1)^2(x^2 + x + 1)(x^5 + 2x + 1)
\]
is \( x^5 + 2x + 1 \). The next lemma follows from Corollary 1 on p. 440 in [15] (see also Convention 3 on p. 435 and the formulas (30) and (33) on p. 441 in [15]).

**Lemma 9.** Let \( \mathbb{K} \) be a Kroneckerian field, and let \( g(x) := a_rx^r + \cdots + a_0 \) be a polynomial with algebraic coefficients, where \( a_0 \) is not zero or a root of unity. Then, there exist two positive integers \( n_0 \) and \( N_0 \) such that for each integer \( n \) satisfying \( n > n_0 \) and \( \gcd(n, N_0) = 1 \) the noncycloptomic part of the polynomial \( x^n + g(x) \) is irreducible over the field \( \mathbb{K}(a_r, \ldots, a_0) \).

See also [13] and [14] for some earlier results on irreducibility of polynomials of the form \( x^n + g(x) \) and their relation with covering systems of integers. The next result follows from Theorems 1.1, 1.2 and Corollary 1.3 in [3].

**Lemma 10.** Let \( g \in \mathbb{Z}[x] \) be a polynomial satisfying \( g(0) \neq 0 \). Then, there is an integer \( n_0 \) depending on \( g \) only such that for each \( n > n_0 \) the noncycloptomic part of the polynomial \( x^n + g(x) \) is either irreducible over \( \mathbb{Q} \) or identically 1, unless one of the following holds:

(i) \( g(x) = -h(x)^p \) for some \( h \in \mathbb{Z}[x] \) and some prime \( p \) dividing \( n \);

(ii) \( g(x) = 4h(x)^4 \) for some \( h \in \mathbb{Z}[x] \) and \( 4|n \).

We conclude this section with the next simple form of Hilbert’s irreducibility theorem (which follows, e. g., from [15, Theorem 46]).

**Lemma 11.** Let \( h_1(x, y), h_2(x, y) \in \mathbb{Z}[x, y] \) be two polynomials irreducible in \( \mathbb{Q}[x, y] \). Then, for infinitely many positive integers \( y = T \) the polynomials \( h_1(x, T), h_2(x, T) \in \mathbb{Z}[x] \) are both irreducible over \( \mathbb{Q} \).

### 3. Irreducibility results

This section contains several irreducibility results. Lemma 14 proves parts (a) – (d) of Theorem 3, whereas Lemmas 15 and 16 will be used in the proof of Theorem 5.

**Lemma 12.** Let \( \gamma \geq 1 \) be a real number. Then, for any \( n, \ell \in \mathbb{N} \) the polynomial \( x^{n\ell} + 2\gamma x^\ell - \gamma \) has no zeros on the circle \( |z| = 1 \).
Proof. Assume that for some \( n, \ell \in \mathbb{N} \) there is some \( \eta \in \mathbb{C} \) of modulus 1 for which 
\[ \eta^n + 2\gamma \eta^\ell - \gamma = 0. \]
Then, for \( \zeta := \eta^\ell \) of modulus 1 we obtain 
\[ 2 = \zeta^{-1} - \zeta^{n-1} \gamma^{-1}. \]
Here, the modulus of the right hand side does not exceed \( 1 + \gamma^{-1} \leq 2 \), so equality can hold only when \( \gamma = 1, \zeta^{-1} = 1 \) and \( \zeta^{n-1} = -1 \), which is impossible. \( \square \)

Lemma 13. Let \( \gamma \) be a totally positive algebraic integer over \( \mathbb{Q} \). Then, there is an 
even positive integer \( M_0 \) depending on \( \gamma \) only such that for each \( n = rM_0 + m_0 \), 
where \( r, m_0 \in \mathbb{N}, m_0 < M_0 \) and \( \gcd(M_0, m_0) = 1 \), the polynomial 
\[ x^n + 2\gamma x - \gamma \] 
is irreducible over the field \( \mathbb{Q}(\gamma) \).

Proof. We first to prove the lemma for \( \gamma \geq 1 \). By Lemma 12 with \( \ell = 1 \), for each 
\( n \in \mathbb{N} \) the polynomial \( x^n + 2\gamma x - \gamma \) has no roots on the unit circle \(|z| = 1\), so, in particular, it has no cyclotomic factors.

Next, by Lemma 9, where \( K = \mathbb{Q}(\gamma) \) is Kroneckerian and \( g(x) = 2\gamma x - \gamma \) (so that 
\( K(\gamma) = K \)), there are \( n_0, N_0 \in \mathbb{N} \) such that for each \( n \in \mathbb{N} \) satisfying \( n > n_0 \) and 
\( \gcd(n, N_0) = 1 \) the noncyclotomic part of the polynomial \( x^n + 2\gamma x - \gamma \) is irreducible over 
\( \mathbb{Q}(\gamma) \). However, by the above, the noncyclotomic part of \( x^n + 2\gamma x - \gamma \) is equal to 
the polynomial \( x^n + 2\gamma x - \gamma \) itself for every \( n \in \mathbb{N} \). Thus, to ensure that each 
\( n = rM_0 + m_0 \) would be greater than \( n_0 \), coprime to \( N_0 \), and \( M_0 \) would be even, 
one can take, for instance, \( M_0 = 2n_0N_0 \). This completes the proof of the lemma when 
\( \gamma \geq 1 \).

Let \( \gamma' \) be any conjugate of \( \gamma \) over \( \mathbb{Q} \). Since \( \gamma \) is a totally positive algebraic 
integer, its all conjugates over \( \mathbb{Q} \) cannot lie in \((0, 1)\), so \( \gamma \) must have a conjugate 
\( \gamma' \geq 1 \). The above implies that the polynomial \( x^n + 2\gamma' x - \gamma' \) is irreducible over 
\( \mathbb{Q}(\gamma') \) for each \( n = rM_0 + m_0 \). Now, if \( x^n + 2\gamma x - \gamma \), where \( 0 < \gamma < 1 \), were reducible over \( \mathbb{Q}(\gamma) \), then \( x^n + 2\gamma' x - \gamma' \) must be reducible over the field \( \mathbb{Q}(\gamma') \), 
which is not the case. This completes the proof of the lemma. \( \square \)

Lemma 14. With the conditions of Theorem 3, the polynomial \( f_\gamma \) defined in (8) 
satisfies (a), (b), (c), (d) of Theorem 3.

Proof. The claims (a), (b) are immediate. By (8), \( f_\gamma \in \mathbb{Z}[x] \), since \( \gamma \) is an algebraic 
integer over \( \mathbb{Q} \).

We now show (c) (irreducibility) and (d) for \( m = 1 \). Then, \( \gamma = k \) and we have 
\[ f_\gamma(x) = x^N + 2kx^2 - k \in \mathbb{Z}[x], \]
where \( k \in \mathbb{N} \) and \( N \) is even. By Lemma 12 with \( \ell = 2 \), the polynomial \( f_\gamma \) has 
no cyclotomic factors. Hence, by Lemma 10, \( f_\gamma \) is irreducible over \( \mathbb{Q} \) for each 
sufficiently large \( N \). Thus, the claim (c) follows for each \( M_0 = 2p \), where \( p \) is 
sufficiently large prime number. Since \( N = 2(rM_0 + m_0) \) and \( N/2 \) is odd, the polynomial 
\( x^{N/2} + 2kx - k \) is negative at \( x \leq 0 \) and increasing for \( x > 0 \). So it has 
a unique real positive root. Consequently, \( f_\gamma(x) = x^N + 2kx^2 - k \) has exactly two 
real roots. This proves (d) for \( m = s/2 = 1 \).
In order to prove the irreducibility in (c) for \( m \geq 2 \), let us take \( N = 2n \), where \( n \) is described in Lemma 13, so that

\[
N = 2(rM_0 + m_0)
\]

with \( M_0 \) even, \( r, m_0 \in \mathbb{N}, m_0 < M_0 \) and \( \gcd(M_0, m_0) = 1 \). We first show that the polynomial \( x^{2n} + 2\gamma x^2 - \gamma \), where \( n \) is odd, is irreducible over the field \( \mathbb{K} := \mathbb{Q}(\gamma) \). (Of course, this implies that the polynomial \( x^{2n} + 2\gamma \ell x^2 - \gamma \ell \) is irreducible over \( \mathbb{Q}(\gamma_\ell) \) for each \( \ell = 1, \ldots, m \).)

Let \( \beta \) be one of the roots of \( x^{2n} + 2\gamma x^2 - \gamma \). By Lemma 13, \( x^n + 2\gamma x - \gamma \) is irreducible over \( \mathbb{K} \). Clearly, \( \beta^2 \) is one of its roots. Consequently, \( [\mathbb{K}(\beta^2) : \mathbb{K}] = n \). Since \( [\mathbb{K}(\beta) : \mathbb{K}] \leq 2n \) and \( [\mathbb{K}(\beta) : \mathbb{K}] \) contains \( \mathbb{K}(\beta^2) \), we have either \( [\mathbb{K}(\beta) : \mathbb{K}] = 2n \) (in which case \( x^{2n} + 2\gamma x^2 - \gamma \) is irreducible over \( \mathbb{K} \)) or \( [\mathbb{K}(\beta) : \mathbb{K}] = n \) in which case \( \beta \) is a root of some monic irreducible polynomial \( g \in \mathbb{K}[x] \) of degree \( n \). Since \( \beta \) is a root of \( x^{2n} + 2\gamma x^2 - \gamma = 0 \) we can write

\[
x^{2n} + 2\gamma x^2 - \gamma = g(x)g_1(x)
\]

with some monic \( g_1 \in \mathbb{K}[x] \) of degree \( n \). In case \(-\beta \) is the root of \( g \) as well, we have \( g(x) = h(2x^2) \) with \( h \in \mathbb{K}[x] \) of degree \( n/2 \). This is impossible, since \( n \) is odd. Thus, \(-\beta \) must be a root of \( g_1 \), and hence \( g_1(x) = (-1)^ng(-x) \). In particular, \( g_1(0) = -g(0) \), since \( n \) is odd. Now, inserting \( x = 0 \) into (13) we obtain \( \gamma = g(0)^2 \). Hence, \( \sqrt{\gamma} = \pm g(0) \in \mathbb{K} = \mathbb{Q}(\gamma) \), which is impossible, by the condition of Theorem 3 on \( \gamma \) of degree \( m \geq 2 \).

Now, to prove (c) it remains to show that the product of polynomials

\[
f_\gamma(x) = \prod_{\ell=1}^{m}(x^N + 2\gamma \ell x^2 - \gamma \ell)
\]

is irreducible over \( \mathbb{Q} \). Let \( A_\ell \) be the set of all \( N \) roots of the factor \( x^N + 2\gamma \ell x^2 - \gamma \ell \) for \( \ell = 1, \ldots, m \). Firstly, observe that

\[
A_\ell \cap A_{\ell'} = \emptyset \quad \text{for} \quad \ell \neq \ell'.
\]

Indeed, if \( \alpha \in A_\ell \cap A_{\ell'} \) then \( \alpha^2 \neq 1/2 \) and

\[
\gamma \ell = \frac{\alpha^N}{1 - 2\alpha^2} = \gamma_{\ell'};
\]

which is not the case. Secondly, as we already showed that \( x^N + 2\gamma \ell x^2 - \gamma \ell \) is irreducible over \( \mathbb{Q}(\gamma \ell) \), the numbers in \( A_\ell \) are conjugate over the field \( \mathbb{Q}(\gamma \ell) \), and hence they are conjugate over its subfield \( \mathbb{Q} \). Consequently, the set \( \bigcup_{\ell=1}^{m} A_\ell \) consists of \( mN \) distinct algebraic numbers conjugate over \( \mathbb{Q} \). Therefore, \( f_\gamma \in \mathbb{Z}[x] \) of degree \( mN \) is irreducible over \( \mathbb{Q} \). This completes the proof of (c) for each \( m \geq 2 \).

In order to prove (d) for \( m \geq 2 \), observe that each factor of \( f_\gamma \), \( x^N + 2\gamma \ell x^2 - \gamma \ell \), has exactly two real roots, since \( rM_0 + m_0 = N/2 \) is odd and \( \gamma \ell \) is positive, and so \( x^{N/2} + 2\gamma \ell x - \gamma \ell \) has a unique real root, which is positive. Hence, the polynomial \( f_\gamma \) consisting of \( m \) such factors \( x^N + 2\gamma \ell x^2 - \gamma \ell, \ell = 1, \ldots, m \), has precisely \( 2m = s \) real roots. This completes the proof of the lemma. \( \square \)
Lemma 15. The cyclotomic part of the polynomial
\[ x^{n+1} - x^5 + x^3 - x^2 - x + 1, \]
where \( n = 6r \pm 1, r \in \mathbb{N} \), is \( x - 1 \).

Proof. Clearly, the polynomial \( F(x) := x^{n+1} - x^5 + x^3 - x^2 - x + 1 \) is divisible by \( x - 1 \), but not by \((x - 1)^2\), since \( F(1) = 1 \) and \( F'(1) = n - 4 > 0 \).

For a contradiction, assume there is a root of unity \( \zeta \neq 1 \) for which \( F(\zeta) = 0 \). Then, multiplying
\[ \zeta^5 - \zeta^3 + \zeta^2 + \zeta - 1 = \zeta^{n+1} \]
and
\[ \zeta^{-5} - \zeta^{-3} + \zeta^{-2} + \zeta^{-1} - 1 = \overline{\zeta^5} - \overline{\zeta^3} + \overline{\zeta^2} + \overline{\zeta} - 1 = \overline{\zeta^{n+1}} = \zeta^{-n-1}, \]
we obtain
\[ 5 - \zeta - \zeta^{-1} - 3(\zeta^2 + \zeta^{-2}) + 2(\zeta^3 + \zeta^{-3}) + \zeta^4 + \zeta^{-4} - \zeta^5 - \zeta^{-5} = 1. \]
Hence, \( \zeta \) must be a root of the polynomial
\[ G(x) := x^{10} - x^9 - 2x^8 + 3x^7 + x^6 - 4x^5 + x^4 + 3x^3 - 2x^2 - x + 1 \]
\[ = (x^2 - x + 1)(x^4 - x^2 + 1)(x - 1)^2(x + 1)^2. \]
Since \( \zeta \neq 1 \), we deduce that \( \zeta = -1 \) or \( \zeta \) is a root of \( \Phi_6(x) = x^2 - x + 1 \) or \( \Phi_{12}(x) = x^4 - x^2 + 1 \).

It remains to check that \( F(\zeta) \neq 0 \) in each of those three cases. In the first case, \( \zeta = -1 \), we clearly have \( F(-1) = 2 \neq 0 \).

In the second case, \( \Phi_6(\zeta) = \zeta^2 - \zeta + 1 = 0 \), using the identity
\[ x^5 - x^3 + x^2 + x - 1 = (x^3 + x^2 - x - 1)(x^2 - x + 1) + x \]
we find that
\[ F(\zeta) = \zeta^{n+1} - \zeta^5 + \zeta^3 - \zeta^2 - \zeta + 1 = \zeta^{n+1} - \zeta = \zeta(\zeta^n - 1). \]
Hence, \( F(\zeta) = 0 \) implies \( \zeta^n = 1 \). Combining with \( \zeta^6 = 1 \), we find that 6 divides \( n \), which is not the case, by the choice of \( n \). Thus, \( F(\zeta) \neq 0 \).

Finally, in the third case, \( \Phi_{12}(\zeta) = \zeta^4 - \zeta^2 + 1 = 0 \), using
\[ x^5 - x^3 + x^2 + x - 1 = x(x^4 - x^2 + 1) + x^2 - 1 \]
we derive that
\[ F(\zeta) = \zeta^{n+1} - \zeta^5 + \zeta^3 - \zeta^2 - \zeta + 1 = \zeta^{n+1} - \zeta^2 + 1 = \zeta^{n+1} - \zeta^4. \]
Now, \( F(\zeta) = 0 \) implies \( \zeta^{n-3} = 1 \). This time \( \Phi_{12}(\zeta) = 0 \), so combining \( \zeta^{n-3} = 1 \) with \( \zeta^{12} = 1 \), we obtain \( 12|n-3 \). Hence, \( 3|n \), which is not the case again. Consequently, \( F(\zeta) \neq 0 \). \( \square \)
Lemma 16. The polynomial
\[
f_n(x) := \frac{x^{n+1} - x^5 + x^3 - x^2 - x + 1}{x - 1} = x^n + \cdots + x^5 + x^2 - 1,
\]
where \( n \geq 5 \) is odd, has a unique real root \( \beta_n \) which belongs to the interval \((\xi_0, \xi_0 + O(1/n))\), where \( \xi_0 = 0.692871 \ldots \) is the real root of the polynomial \( x^5 - x^3 + x^2 + x - 1 \).

**Proof.** Clearly, \( f_n(x) > 0 \) for \( x \geq 1 \). For \( x \leq -1 \) we obtain
\[
f_n(x) = (x^n + x^{n-1}) + \cdots + (x^7 + x^6) + x^5 + x^2 - 1 \leq x^5 + x^2 - 1 \leq -1.
\]
Similarly, in the interval \((-1, 0]\) we have
\[
(x - 1)f_n(x) = (1 - x)^2(1 + x) - x^5(1 - x^{n-4}) > 0.
\]
Hence, \( f_n \) has no roots in \((-\infty, 0] \cup [1, +\infty)\).

Evidently, in the interval \((0, 1)\) the polynomial \( f_n \) is increasing from \( f_n(0) = -1 \) to \( f_n(1) = n - 4 > 0 \), so \( f_n \) has a unique real root \( \beta_n \) in \((0, 1)\). Finally, note that
\[
f_n(\xi_0)(\xi_0 - 1) = \xi_0^{n+1} > 0.
\]
Selecting \( \xi_n := \xi_0 + 1/n \) and using \( \xi_0^5 - \xi_0^3 + \xi_0^2 + \xi_0 - 1 = 0 \) we see that
\[
f_n(\xi_n)(\xi_n - 1) = f_n\left(\xi_0 + \frac{1}{n}\right)\left(\xi_0 + \frac{1}{n} - 1\right)
= \left(\xi_0 + \frac{1}{n}\right)^{n+1} - \frac{5\xi_0^4 - 3\xi_0^2 + 2\xi_0 + 1}{n} + O\left(\frac{1}{n^2}\right)
< 0.7^{n+1} - \frac{2}{n} < 0
\]
for \( n \) sufficiently large. Hence, this real root \( \beta_n \) belongs to the interval \((\xi_0, \xi_n) = (\xi_0, \xi_0 + 1/n)\) for \( n \) large enough, which implies the last assertion of the lemma. \( \square \)

Proof of Lemma 4. Consider the polynomials
\[
h_1(x, y) := x(x - 1)\ldots(x - m + 2)(y - x) + (-1)^m k \in \mathbb{Z}[x, y]
\]
and \( h_2(x, y) := h_1(x^2, y) \). They are both linear in \( y \). Writing
\[
h_1(x, y) = -yg_1(x) + xg_1(x) + (-1)^m k
\]
with \( g_1(x) := x(x - 1)\ldots(x - m + 2) \), we see that the polynomials \( g_1(x) \) and \( xg_1(x) + (-1)^m k \) are relatively prime, so \( h_1(x, y) \) is irreducible in \( \mathbb{Z}[x, y] \). By the same argument, \( h_2(x, y) \) is irreducible in \( \mathbb{Z}[x, y] \). Thus, by Lemma 11, the polynomials \( g(x) = h_1(x, T) \) and \( g(x^2) = h_1(x^2, T) \) are irreducible over \( \mathbb{Q} \) for infinitely many positive integers \( T \).

Fix \( \delta < 1/3 \) and take one of those \( T \) which is large enough. Clearly, the sign of \( g(x) \) is \((-1)^m \) for \( x \leq 0 \), so \( g \) has no real negative roots (and \( g(0) \neq 0 \)). The value of \( g(x) \) at \( x = \delta \) is
\[
g(\delta) = (-1)^m\delta(1 - \delta)\ldots(m - 2 - \delta)(T - \delta) + (-1)^m k,
\]
which has the sign \((-1)^{m-1}\) for \(T\) large enough. So, \(g\) has a root \(\gamma\) in the interval 
\((0, \delta)\). Furthermore, \(g(j) = (-1)^m k\) for each \(j \in \{0, 1, \ldots, m - 2\}\), so, by the same argument, \(g\) must have roots in each of the intervals 
\((2q, 2q + \delta)\), where 
\(0 \leq q \leq \frac{(m - 2)}{2}\), and also in \((2q + 1 - \delta, 2q + 1)\), where 
\(0 \leq q \leq \frac{(m - 3)}{2}\) and 
\(m \geq 3\). Also, in view of \(g(T) = (-1)^m k\) the polynomial \(g\) has a root in 
\((T - \delta, T)\) when \(m\) is even and a root in 
\((T, T + \delta)\) when \(m\) is odd. Consequently, for \(m = 2\) the polynomials \(g\) has \(1 + 1 = 2\) roots. For \(m \geq 3\) it has
\[
\left\lfloor \frac{m - 2}{2} \right\rfloor + 1 + \left\lfloor \frac{m - 3}{2} \right\rfloor + 1 + 1 \\
= \left\lfloor \frac{m - 2}{2} \right\rfloor + \left\lfloor \frac{m - 3}{2} \right\rfloor + 3 \\
= \frac{m - 2}{2} + \frac{m - 3}{2} - \frac{1}{2} + 3 = m
\]
roots. Thus, \(\gamma < \delta\) is a totally positive algebraic integer of degree \(m\) and norm \(k\).

Finally, assume that \(\sqrt{\gamma} \in \mathbb{Q}(\gamma)\). Then, \(\sqrt{\gamma}\) is of degree at most \(m\) over \(\mathbb{Q}\). Also, it is the root of the polynomial \(g(x^2) \in \mathbb{Z}[x]\) of degree \(2m\). Hence, the polynomial \(g(x^2)\) must be reducible over \(\mathbb{Q}\). This is a contradiction, since we have chosen \(T\) so that \(g(x)\) and \(g(x^2)\) are both irreducible over \(\mathbb{Q}\). \(\square\)

4. Proof of Lemma 6. Throughout the proof we assume that \(n > r\). We label 
the roots of \(f(x) := x^n + g(x)\) by \(\beta_1, \ldots, \beta_n\), where \(\beta_1, \ldots, \beta_t\) are nonreal roots with 
positive complex parts, \(\beta_{t+j} = \overline{\beta_j}\) for \(j = 1, \ldots, t\), and \(\beta_{2t+1}, \ldots, \beta_n\) are \(s = n - 2t\) 
real roots of \(f\) (if any). Fix some positive number \(c_0\) and assume that among the 
first \(t\) roots the roots \(\beta_1, \ldots, \beta_{t_1}\) are of moduli greater than \(1 - c_0/\sqrt{n}\), whereas 
\(t_2 = t - t_1\) roots \(\beta_{t_1+1}, \ldots, \beta_t\) have moduli smaller than or equal to \(1 - c_0/\sqrt{n}\).

Recall that the Mahler measure of \(f\) (which is monic, since \(n > r\)) is given by
\[
M(f) = \prod_{j=1}^{n} \max\{1, |\beta_j|\}.
\]
In general, the Mahler measure \(M(P)\) of a polynomial \(P \in \mathbb{C}[x]\) can be found by 
Jensen’s formula
\[
\log M(P) = \frac{1}{2\pi} \int_{0}^{2\pi} \log |P(e^{ix})| dx,
\]
where (throughout the proof of this lemma) \(i = \sqrt{-1}\). In particular, for \(P \in \mathbb{R}[x]\) 
we have \(|P(e^{ix})| = |P(e^{i(2\pi - x)})|\), so that
\[
\frac{1}{2\pi} \int_{0}^{2\pi} \log |P(e^{ix})| dx = \frac{1}{\pi} \int_{0}^{\pi} \log |P(e^{ix})| dx = \int_{0}^{1} \log |P(e^{\pi ix})| dx.
\]
Hence, \(\log M(P) = \int_{0}^{1} \log |P(e^{\pi ix})| dx\). In particular, \(g \in \mathbb{R}[x]\), so
\[
(14) \quad \log M(g) = \int_{0}^{1} \log |g(e^{\pi ix})| dx.
\]
We first show that all $n$ roots of $f$ lie in the disc
\begin{equation}
|z| < 1 + c/n,
\end{equation}
where $c > 0$ is some constant depending on $g$ only. Indeed, suppose $\beta$ is a root of $f$ satisfying $|\beta| > 1$. Then, $\beta^n + g(\beta) = 0$ implies that $|\beta|^n = |g(\beta)| \leq (r + 1)H|\beta|^r$, where
\[ H = H(g) := \max_{0 \leq j \leq r} |a_j|. \]
In case $n > 2r$ this yields $|\beta|^n < ((r + 1)H)^2$. This proves (15), since $r$ and $H$ depend on $g$ only.

Now, let us estimate the number of nonreal roots of $f$ lying in the disc $|z| \leq 1 - c_0/\sqrt{n}$. By the above, we have $2t_2$ of such roots of $f$. Thus, the moduli of at least $2t_2$ roots of the reciprocal polynomial $f^*(x) = x^n f(1/x)$ are greater than or equal to $1/(1 - c_0/\sqrt{n}) > 1 + c_0/\sqrt{n}$. Hence,
\begin{equation}
M(f) = M(f^*) \geq |a_0| \left(1 + \frac{c_0}{\sqrt{n}}\right)^{2t_2}.
\end{equation}
By the inequality of Landau [10], we have
\[ M(f^*) = M(f) \leq \left(1 + \sum_{j=0}^r |a_j|^2\right)^{1/2} \leq \left(1 + (r + 1)H^2\right)^{1/2} \ll 1. \]
Clearly, the last inequality combined with (16) yields $2t_2 \ll \sqrt{n}$.

Also, by Lemma 8, the number of real roots $s$ of $f$ does not exceed $\sqrt{n}$ times a constant depending only on $g$. (In fact, this was obtained earlier with the better and best possible constant 2; see the papers of Schur [16] and Szegö [19].) Therefore,
\begin{equation}
n - 2t_1 = 2t_2 + s = O(\sqrt{n}).
\end{equation}
Furthermore, the annulus
\[ S = \left\{ z \in \mathbb{C} : 1 - \frac{c_0}{\sqrt{n}} < |z| < 1 + \frac{c}{n} \right\} \]
contains exactly $2t_1$ nonreal roots of $f$, with the remaining $2t_2$ nonreal roots lying in $|z| \leq 1 - c_0/\sqrt{n}$. Consequently,
\begin{equation}
C_q(f) := \sum_{j=1}^t |\beta_j|^q \leq \sum_{j=1}^{t_1} |\beta_j|^q + t_2 = \sum_{j=1}^{t_1} |\beta_j|^q + t - t_1.
\end{equation}
Of course, in case $t_2 = 0$ we have $t = t_1$ and equality in (18).

To estimate the remaining sum in (18) we will consider the following $K$ sectors with arguments in the intervals $[\pi j/K, \pi (j + 1)/K)$ for $j = 0, 1, \ldots, K - 1$:
\[ S_j = \left\{ z \in \mathbb{C} : 1 - \frac{c_0}{\sqrt{n}} < |z| < 1 + \frac{c}{n}, \quad \frac{\pi j}{K} \leq \arg z < \frac{\pi (j + 1)}{K} \right\}. \]
By our definitions, \( \beta_1, \ldots, \beta_{t_1} \) all lie in the union of those \( K \) sectors \( \cup_{j=0}^{K-1} S_j \). Furthermore, except for these roots, this union (more precisely, the sector \( S_0 \)) can contain at most \( O(\sqrt{n}) \) of real positive roots. Thus, applying Lemma 8 to the polynomial \( x^n + g(x) \), we find that the number of its nonreal roots \( N_j \) in \( S_j \) (in fact, all roots in \( S_j \) are nonreal when \( j > 0 \)) satisfies

\[
|N_j - n/(2K)| < 16 \sqrt{n} \log \left( (1 + (r + 1)H)|a_0|^{-1/2} \right)
\]

plus the term \( s = O(\sqrt{n}) \) on the right hand side for \( j = 0 \). Consequently, selecting

(19) \[ K := \lceil n^{1/4} \rceil \]

and using (17), we find that

(20) \[ N_j = t_1/K + O(\sqrt{n}) \]

for each \( j = 0, 1, \ldots, K - 1 \). Here,

(21) \[ N_0 + N_1 + \cdots + N_{K-1} = t_1. \]

It is easy to see that the diameter \( \delta \) of the sector \( S_j \) does not exceed

\[
2 \left( 1 + \frac{c}{n} \right) \sin \left( \frac{\pi}{2K} \right) + \frac{c}{n} + \frac{c_0}{\sqrt{n}} \ll \frac{1}{K}.
\]

For any root \( \beta \in S_j \) we have \( |\beta|^n = |g(\beta)| \). Since the distance from \( \beta \) to the point \( e^{\pi ij/K} \in S_j \) is less than or equal to \( \delta \ll 1/K \) and \( |g'(z)| \ll 1 \) for \( |z| \leq 1 + c/n \), we obtain

\[
|g(\beta) - g(e^{\pi ij/K})| \leq \delta \max_{|z| \leq 1 + c/n} |g'(z)| \ll K^{-1}.
\]

Hence, using the condition of the lemma \( \min_{|z|=1} |g(z)| \gg 1 \), we deduce that

\[
|\beta|^q = |g(\beta)|^{q/n} = (|g(e^{\pi ij/K})| + O(K^{-1}))^{q/n}
\]

\[
= 1 + \frac{q \log(|g(e^{\pi ij/K})| + O(K^{-1}))}{n} + O\left( \frac{1}{n^2} \right)
\]

\[
= 1 + \frac{q \log |g(e^{\pi ij/K})|}{n} + O\left( \frac{1}{Kn} \right).
\]

Combining this with (17), (19), (20) and \( t_1 \leq n/2 \), we derive that the total contribution of \( q \)th powers of \( N_j \) nonreal roots lying in the \( j \)th sector \( S_j \) into the sum \( C_q(f) \) is

\[
N_j \left( 1 + \frac{q \log |g(e^{\pi ij/K})|}{n} + O\left( \frac{1}{Kn} \right) \right) = N_j + \frac{q \log |g(e^{\pi ij/K})|}{2K} + O\left( \frac{1}{\sqrt{n}} \right).
\]

Next, summing over \( j \), \( 0 \leq j \leq K - 1 \), and using (19), (21), we further deduce that

(22) \[ \sum_{j=1}^{t_1} |\beta_j|^q = t_1 + \frac{q}{2K} \sum_{j=0}^{K-1} \log |g(e^{\pi ij/K})| + O(n^{-1/4}). \]
Now, replacing the sum $K^{-1} \sum_{j=0}^{K-1} \log |g(e^{\pi ij/K})|$ by a corresponding integral (which introduces the error of size $O(1/K)$), in view of (14) and (19), we obtain

$$
\frac{1}{K} \sum_{j=0}^{K-1} \log |g(e^{\pi ij/K})| = \int_0^1 \log |g(e^{\pi ix})|dx + O(K^{-1})
= \log M(g) + O(n^{-1/4}).
$$

Hence, by (22),

$$
\sum_{j=1}^{t_1} |\beta_j|^q = t_1 + \frac{q}{2} \log M(g) + O(n^{-1/4}).
$$

Inserting this into (18) we get the required bound (11) on $C_q(f)$. In case $t_2 = 0$ (which, as we already showed earlier, necessarily occurs when the bound $|\beta_j| > 1 - c_0/\sqrt{n}$ holds for $j = 1, \ldots, t$) we have equality in (18), and so equality in (11) too.

5. Proofs of Theorems 3 and 5. We begin with the following (final) preparation for the proof of Theorem 3.

**Lemma 17.** For each $\gamma > 0$ and each sufficiently large odd $n$ we have

$$
\|x^{2n} + 2\gamma x^2 - \gamma\|^2 = n + \log(2\gamma) + O(n^{-1}),
$$

where the constant implied in $O$ depends on $\gamma$ only.

**Proof.** Note that the polynomial $f(x) := x^n + 2\gamma x - \gamma$ is negative at $x \leq 0$ and increasing at $x > 0$. Thus, it has a unique real positive root $\beta_n$ satisfying

$$
\frac{1}{2} - \frac{1}{n} < \beta_n < \frac{1}{2}.
$$

The remaining $n - 1$ roots of $f$ are nonreal. We will show that they all lie in the annulus

$$
1 - \frac{c_1}{n} < |z| < 1 + \frac{c_2}{n},
$$

where $c_1, c_2 > 0$ depend on $\gamma$ only.

Indeed, if $f(z) = z^n + 2\gamma z - \gamma = 0$ with $|z| \geq 1$ then

$$
|z|^{n-1} = |-2\gamma + z^{-1}\gamma| \leq 3\gamma,
$$

which implies the upper bound in (24). For a lower bound, it suffices to show that the reciprocal polynomial $x^n - 2x^{n-1} - \gamma^{-1}$ of $f(x)$ has exactly $n - 1$ roots in the disc $|z| < R := 1 + c_1/n$ (which is less than $1/(1 - c_1/n)$). This is indeed the case, by Rouché’s theorem, since the polynomial $-2x^{n-1}$ has $n - 1$ roots in the disc $|z| < R$ and on the boundary, namely, on the circle $|x| = R$ we have

$$
|x^n - \gamma^{-1}| \leq R^n + \gamma^{-1} < 2R^{n-1} = | - 2x^{n-1} |$$
whenever $R^{n-1}(2 - R) > \gamma^{-1}$. Here, the left hand side tends to $e^{c_1}$ as $n \to \infty$, so this inequality is true for $n$ large enough with the choice, e. g., $c_1 := 1 + \max\{0, -\log \gamma\}$.

Now, by (23) and (24), we deduce that the polynomial $f(x^2)$ has two real roots in the intervals $(-1/\sqrt{2}, -1/\sqrt{2} + 1/n)$ and $(1/\sqrt{2} - 1/n, 1/\sqrt{2})$ and $2n - 2$ nonreal roots in the annulus $1 - c_1/n < |z| < 1 + c_2/(2n)$. Setting $t = n - 1$ and assuming that $\alpha_1, \ldots, \alpha_t$ are the nonreal roots of $f(x^2)$ with positive complex parts, by (2), we find that

$$\|x^{2n} + 2\gamma x^2 - \gamma\|^2 = \|f(x^2)\|^2 = \sum_{j=1}^t |\alpha_j|^2 + 1 + O(n^{-1}).$$

Using Lemma 7 with $q = 2$ and equality $\prod_{j=1}^t |\alpha_j|^2 = \gamma\beta_n^{-1}$, where $-\beta_n$ is the product of two real roots of $f(x^2)$ and satisfies (23), we find that

$$\sum_{j=1}^t |\alpha_j|^2 = t + 2 \log \left( \prod_{j=1}^t |\alpha_j| \right) + O(n^{-1}) = t + \log(\gamma\beta_n^{-1}) + O(n^{-1}) = t + \log(2\gamma) + O(n^{-1}).$$

Inserting this into (25) (and using $t + 1 = n$) we obtain the required result. \hfill \square

**Proof of Theorem 3.** In view of Lemma 14 it suffices to prove (9) for the polynomial $f_\gamma$ defined in (8). Since all $\gamma_\ell$, $\ell = 1, \ldots, m$, are real, using (3) and (8), we deduce that

$$\|f_\gamma\|^2 = \sum_{\ell=1}^m \|x^N + 2\gamma_\ell x^2 - \gamma_\ell\|^2,$$

where $N = 2(rM_0 + m_0)$. Now, since $N$ is twice an odd integer and $\gamma_\ell > 0$, by Lemma 17, we find that

$$\|x^N + 2\gamma_\ell x^2 - \gamma_\ell\|^2 = \frac{N}{2} + \log(2\gamma_\ell) + O(N^{-1}).$$

Hence, summing over $1 \leq \ell \leq m$ and using $\text{Norm}(\gamma) = k$, $n = mN$, $s = 2m$, by (26), we deduce that

$$\|f_\gamma\|^2 = \frac{mN}{2} + m \log 2 + \log \text{Norm}(\gamma) + mO(N^{-1}) = \frac{n}{2} + m \log 2 + \log k + O(n^{-1}) = \frac{n}{2} + \frac{s \log 2}{2} + \log k + O(n^{-1}),$$

where the constant implied in $O$ depends only on $m = s/2$ and $\gamma_1, \ldots, \gamma_m$. This proves (9) and so completes the proof of the theorem. \hfill \square
Proof of Theorem 5. Consider the polynomial
\[ f_n(x) = -1 + x^2 + \sum_{j=5}^{n} x^j, \]
where \( n = 6r \pm 1 \). By Lemma 15, \( f_n \) is the noncyclotomic part of the polynomial
\[ F_n(x) = (x - 1)f_n(x) = x^{n+1} - x^5 + x^3 - x^2 - x + 1. \]
Hence, by Lemma 10, \( f_n \) is irreducible over \( \mathbb{Q} \) for each sufficiently large \( k \).

Next, by Lemma 16, \( f_n \) has a unique real root \( \beta_n \in (\xi_0, \xi_0 + O(1/n)) \) and \( 2t = n-1 \) nonreal roots \( \beta_1, \ldots, \beta_t, \overline{\beta_1}, \ldots, \overline{\beta_t} \). By Lemma 6 with \( q = 2 \) applied to \( F_n \) with two real roots \( \beta_n, 1 \) and \( 2t \) nonreal roots, using (3) and \( M(-x^5 + x^3 - x^2 - x + 1) = \theta_3 \), where \( \theta_3 = \xi_0^{-1} = 1.443268 \ldots \) is the real root of the polynomial (10), we find that
\[
\|f_n\|^2 = \|F_n\|^2 - 1 = |\beta_1|^2 + \cdots + |\beta_t|^2 + |\beta_n|^2 \\
\leq t + \log \theta_3 + O(n^{-1/4}) + \xi_0^2 + O(n^{-1}) \\
= \frac{n - 1}{2} + \theta_3^{-2} + \log \theta_3 + O(n^{-1/4}) \\
= \frac{n}{2} + 0.346981 \ldots + O(n^{-1/4}),
\]
which finishes the proof. \( \square \)

Acknowledgements. I thank the referees for pointing out several misprints in the first version of the paper.

References


Received 29 June, 2016 and in revised form 3 October, 2016.