

LOWER BOUNDS FOR HEIGHTS IN CYCLOTOMIC EXTENSIONS

M. I. M. ISHAK, MICHAEL J. MOSSINGHOFF, CHRISTOPHER PINNER,
AND BENJAMIN WILES

ABSTRACT. We show that the height of a nonzero algebraic number α that lies in an abelian extension of the rationals and is not a root of unity must satisfy $h(\alpha) > 0.154997$.

1. INTRODUCTION

Recall that if $\alpha \neq 0$ is a root of an irreducible integer polynomial $f(x) = a \prod_{i=1}^d (x - \alpha_i)$, then the *absolute logarithmic height* $h(\alpha)$ of α is defined by

$$h(\alpha) = \frac{\log M(f)}{d},$$

where $M(f) = |a| \prod_{i=1}^d \max\{1, |\alpha_i|\}$ is the *Mahler measure* of f . *Lehmer's problem* asks if there exists a positive constant $c > 0$ such that $h(\alpha) > c/d$ as long as α is not zero or a root of unity. In certain cases one can do significantly better than this. For example, if α lies in a kroneckerian field (a totally real number field, or a totally quadratic extension of such a field) and $|\alpha| \neq 1$, then Schinzel [10, Corollary 1'] showed that

$$h(\alpha) \geq \frac{1}{2} \log \left(\frac{1 + \sqrt{5}}{2} \right) = 0.240605\dots \quad (1.1)$$

See Garza [7] for a generalization of this. When α lies in an abelian extension of the rationals (i.e., by the Kronecker-Weber theorem, α lies in some cyclotomic field), Amoroso & Dvornicich [1] proved the bound

$$h(\alpha) \geq \frac{\log 5}{12} = 0.134119\dots \quad (1.2)$$

Recently Amoroso & Zannier [2] have shown more generally that if k is a number field, $k(\alpha)$ is an abelian extension of k , and $m = [k : \mathbb{Q}]$, then

$$h(\alpha) \geq 3^{-m^2 - 2m - 6}.$$

In particular, if $\alpha \neq 0$ lies in a dihedral extension of the rationals, then using $m = 2$ we see that

$$h(\alpha) \geq 3^{-14}.$$

Garza [8] had previously obtained the bound $h(\alpha) \geq \frac{1}{d} \log M(x^3 - x - 1)$ in this situation, which is optimal with respect to Lehmer's problem.

Date: January 23, 2009.

2000 Mathematics Subject Classification. Primary: 11R18; Secondary: 11C08, 11R09.

Key words and phrases. Heights, Mahler measure, Lehmer's problem.

The research of the second author was supported in part by NSA grant H98230-08-1-0052.

Here we establish an improvement to (1.2). We shall assume throughout that α lies in a cyclotomic extension $\mathbb{Q}(\zeta_m)$, where ζ_m is a primitive m th root of unity, and that $\alpha \neq 0$ is not a root of unity. As observed by Amoroso & Dvornicich, such a lower bound cannot be replaced by anything larger than

$$h(\alpha_0) = \frac{\log 7}{12} = 0.162159\dots,$$

which is achieved for example when α_0 is a root of $7x^{12} - 13x^6 + 7$. Explicitly writing one of the roots of this polynomial in the form

$$\alpha_0 := \frac{(3u^2 - 5)}{\sqrt{7}i(1 + \lambda_0)}, \quad u := 2 \cos(2\pi/7), \quad (1.3)$$

where

$$\lambda_0 := \frac{1}{14}(2 - 9u - 3u^2) + \frac{1}{14}(5u^2 + u - 8)\sqrt{3}i \quad (1.4)$$

is a zero of $x^6 + \frac{13}{7}x^3 + 1$, the roots $\pm \alpha_0^\varepsilon \zeta_3^j$, $\varepsilon = \pm 1$, $j = 0, 1, 2$, of $7x^{12} - 13x^6 + 7$ plainly lie in $\mathbb{Q}(\zeta_{21})$.

When $2 \mid m$ and $\alpha \zeta_m^u \notin \mathbb{Q}(\zeta_{m/2})$ for any u , Amoroso & Dvornicich also obtained the stronger bound

$$h(\alpha) \geq \frac{\log 2}{4} = 0.173286\dots \quad (1.5)$$

This is sharp, as one may verify for example by using

$$\alpha_1 := \frac{1}{4}(1 + i)(1 + \sqrt{-7}) \in \mathbb{Q}(\zeta_{28}), \quad (1.6)$$

which has minimal polynomial $x^4 - x^3 + \frac{1}{2}x^2 - x + 1$, or by using

$$\alpha_2 := \frac{1}{4}(1 + i)(\sqrt{5} + \sqrt{-3}) \in \mathbb{Q}(\zeta_{60}), \quad (1.7)$$

which has minimal polynomial $x^8 - \frac{7}{4}x^4 + 1$. (Notice that $\sqrt{5} + \sqrt{-3} \in \mathbb{Q}(\zeta_{15})$, and also that $\alpha_2 = \zeta_8 \beta_2$ where $\beta_2 = \frac{1}{4}(\sqrt{10} + \sqrt{-6}) \in \mathbb{Q}(\zeta_{120})$ has lower degree with minimal polynomial $x^4 - \frac{1}{2}x^2 + 1$, but of course the same height.) We report here a similarly sharp bound when $3 \mid m$, as well as some restrictions on the form of α with low height when 2 or 3 divides m . For this we shall also need the value

$$\alpha_3 := \sqrt{\frac{5 + \sqrt{5}}{10}} + \sqrt{\frac{5 - \sqrt{5}}{10}}i \in \mathbb{Q}(\zeta_{20}), \quad (1.8)$$

which has minimal polynomial $x^8 + \frac{6}{5}x^4 + 1$ and $h(\alpha_3) = \frac{1}{8} \log 5$.

Theorem 1. *Suppose that $\alpha \in \mathbb{Q}(\zeta_m)$, $\alpha \neq 0$, and α is not a root of unity.*

(i) *Suppose that $3 \mid m$ and that $\alpha \zeta_m^u \notin \mathbb{Q}(\zeta_{m/3})$ for any u . Then*

$$h(\alpha) \geq \frac{\log 7}{12} = 0.162159\dots \quad (1.9)$$

If $7 \nmid m$, or $m = 21l$ with $3 \nmid l$ and $\alpha/\alpha_0^\varepsilon \zeta_3^j \notin \mathbb{Q}(\zeta_{7l})$ for any $\varepsilon = \pm 1$, $j = 0, 1$, or 2, then

$$h(\alpha) \geq \frac{\log 2}{4} = 0.173286\dots \quad (1.10)$$

If further $5 \nmid m$ or $m = 15l$ with $3 \nmid l$ and $\alpha/(\sqrt{5} + \sqrt{-3})^\varepsilon \zeta_3^j \notin \mathbb{Q}(\zeta_{5l})$ for any $\varepsilon = \pm 1$, $j = 0, 1$, or 2, or if $9 \mid m$, then

$$h(\alpha) \geq 0.174878. \quad (1.11)$$

(ii) Suppose that $2 \mid m$ and that $\alpha \zeta_m^u \notin \mathbb{Q}(\zeta_{m/2})$ for any u . Then

$$h(\alpha) \geq \frac{\log 2}{4} = 0.173286\dots$$

If $m = 4l$ with l odd, and $(1 \pm i)\alpha \notin \mathbb{Q}(\zeta_l)$ then

$$h(\alpha) \geq \frac{\log 5}{8} = 0.201179\dots \quad (1.12)$$

If further $5 \nmid m$, or $m = 20l$ with l odd, and $\alpha/\alpha_3^{\varepsilon j} \notin \mathbb{Q}(\zeta_{5l})$ for any $\varepsilon = \pm 1$, $0 \leq j \leq 3$, or if $8 \mid m$, then

$$h(\alpha) \geq 0.210291. \quad (1.13)$$

The bounds (1.11) and (1.13) can probably be improved, but the examples α_i with $0 \leq i \leq 3$ show that the other bounds are sharp, as well as the necessity of the restrictions on the form of any α having smaller height.

From Theorem 1, plainly any abelian α of height below $\frac{1}{12} \log 7$ must (if it exists, and after dividing by a root of unity as necessary) have $\gcd(6, m) = 1$. Amoroso & Dvornicich also obtained the bounds

$$h(\alpha) \geq \begin{cases} \frac{1}{6} \log(5/2) = 0.152715\dots & \text{if } 5 \nmid m, \\ \frac{1}{8} \log(7/2) = 0.156595\dots & \text{if } 7 \nmid m, \\ \frac{1}{12} \log(11/2) = 0.1420662\dots & \text{if } 11 \nmid m. \end{cases}$$

We improve these enough to deduce that an abelian α with height below $\frac{1}{12} \log 7$ must in fact have $35 \mid m$.

Theorem 2. Suppose that $\alpha \in \mathbb{Q}(\zeta_m)$, $\alpha \neq 0$, and α is not a root of unity.

(i) If $3 \nmid m$ then

$$h(\alpha) \geq 0.154997\dots \quad (1.14)$$

(ii) If $5 \nmid m$ then

$$h(\alpha) \geq 0.166968\dots, \quad (1.15)$$

unless $\alpha = \alpha_0^\varepsilon \zeta$ with $\varepsilon = \pm 1$ and ζ a root of unity, whence $h(\alpha) = \frac{1}{12} \log 7 = 0.162159\dots$

(iii) If $7 \nmid m$ then

$$h(\alpha) \geq 0.162368\dots \quad (1.16)$$

In a subsequent paper, we will show how the approach employed here can also be used to improve bounds of Borwein, Dobrowolski & Mossinghoff [3] and Dubickas & Mossinghoff [6] for the heights of roots of polynomials with all odd coefficients.

2. PRELIMINARIES & LEMMAS

Suppose that α lies in an algebraic number field k , V_k is a complete set of absolute values on k , normalised so that $|x|_v = \|x\|_v^{d_v/d}$ for $v \in V_k$, where $d = [k : \mathbb{Q}]$, $d_v = [k_v : \mathbb{Q}_v]$, and $\|x\|_v$ coincides with the usual absolute value or p -adic absolute value on \mathbb{Q} . Then

$$H(\alpha) = \prod_{v \in V_k} \max\{1, |\alpha|_v\},$$

and

$$h(\alpha) = \log H(\alpha).$$

The normalisations ensure that these values do not depend upon the choice of k .

In view of Schinzel's bound (1.1), we can assume that $|\alpha|_v = 1$ for all $v \mid \infty$.

Suppose that p is a prime. If $p \nmid m$, define $\sigma_p \in \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ by $\sigma_p(\zeta_m) = \zeta_m^p$. If $p \mid m$, define σ_p to be the generator for $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_{m/p}))$, so that $\sigma_p(\zeta_m) = \zeta_p \zeta_m$ for an appropriate primitive p th root of unity ζ_p .

Lemma 2.1. *Suppose that α is a nonzero element in an algebraic number field k and S a finite set of finite places on k . Then there exists an algebraic integer β in k such that $\alpha\beta$ is an algebraic integer and*

$$|\beta|_v = \frac{1}{\max\{1, |\alpha|_v\}}$$

for each $v \in S$.

Proof. Let P denote the set of primes p such that either $v \mid p$ for some v in S , or $v \mid p$ and $|\alpha|_v > 1$, and let S_0 denote the set of places w on k with $w \mid p$ for some $p \in P$ (in particular $S \subseteq S_0$ and $|\alpha|_v \leq 1$ for all $v \notin S_0$). By the Weak Approximation Theorem (e.g., [4, Theorem 3.1]), there exists $\beta_0 \in k$ with

$$|\beta_0 - \alpha^{-1}|_w < |\alpha|_w^{-1} \text{ if } |\alpha|_w > 1$$

and

$$|\beta_0 - 1|_w < 1 \text{ if } |\alpha|_w \leq 1$$

for all w in S_0 . Notice that $|\beta_0|_w = \frac{1}{\max\{1, |\alpha|_w\}}$ and $|\alpha\beta_0|_w \leq 1$ for all $w \in S_0$. Let Q denote the primes q such that $|\beta_0|_w > 1$ for some $w \mid q$ (note $Q \cap S_0 = \emptyset$). By the Chinese Remainder Theorem, there is an integer n such that $n \equiv 0 \pmod{q^{\alpha_q}}$ for $q \in Q$ and $n \equiv 1 \pmod{q^{\alpha_q}}$ for $q \in P$, with the α_q chosen large enough so that $|q|_w^{\alpha_q} |\beta_0|_w < 1$ for all $w \mid q$ and $q \in Q$, and $|q|_w^{\alpha_q} |\beta_0|_w < \frac{1}{\max\{1, |\alpha|_w\}}$ for all $w \mid q$ and $q \in P$. Thus $\beta = n\beta_0$ will satisfy $|\beta|_w = |n|_w |\beta_0|_w \leq 1$ for $w \mid q$, $q \in Q$, $|\beta|_w \leq |\beta_0|_w \leq 1$ for $w \mid q$, $q \notin Q \cup S_0$, and $|\beta|_w = |(n-1)\beta_0 + \beta_0|_w = |\beta_0|_w = \frac{1}{\max\{1, |\alpha|_w\}}$ for $w \mid q$, $q \in S_0$. Thus $|\beta|_v \leq 1$ and $|\alpha\beta|_v \leq 1$ for all $v \nmid \infty$, and β and $\alpha\beta$ are algebraic integers, as claimed. \square

Lemma 2.2. *Suppose that γ is an algebraic integer in $\mathbb{Q}(\zeta_m)$, $\alpha \in \mathbb{Q}(\zeta_m)$, and $v \nmid \infty$.*

- (i) *If $p \nmid m$ then $p \mid (\gamma^p - \sigma_p(\gamma))$.*
- (ii) *If $p \mid m$ then $(1 - \zeta_p)^p \mid (\gamma^p - \sigma_p(\gamma)^p)$.*
- (iii) *If $p \nmid m$ then $|\alpha^p - \sigma_p(\alpha)|_v \leq |p|_v \max\{1, |\alpha|_v\}^p \max\{1, |\sigma_p(\alpha)|_v\}$.*
- (iv) *If $p \mid m$ then $|\alpha^p - \sigma_p(\alpha)^p|_v \leq |p|_v^{\frac{p}{p-1}} \max\{1, |\alpha|_v\}^p \max\{1, |\sigma_p(\alpha)|_v\}^p$.*

Proof. Statement (i) is from Amoroso & Dvornicich [1, Lemma 2]. For (ii), write

$$\gamma = \sum_{i=0}^{p-1} \left(\sum_{j \equiv i \pmod{p}} a_j \zeta_m^j \right) = \sum_{i=0}^{p-1} A_i \zeta_m^i, \quad A_i \in \mathbb{Q}(\zeta_{m/p}).$$

Hence $\sigma_p(\gamma) = \sum_{i=0}^{p-1} A_i \zeta_m^i \zeta_p^i$, and for each $k = 0, \dots, p-1$, we have that $\sigma_p(\gamma) - \zeta_p^k \gamma = \sum_{i=0}^{p-1} A_i \zeta_m^i (\zeta_p^i - \zeta_p^k)$ is divisible by $(1 - \zeta_p)$.

For $v \nmid p$, statements (iii) and (iv) are trivial. From Lemma 2.1, there must exist an algebraic integer β such that $\alpha\beta$ is an algebraic integer, but $|\beta|_v = 1/\max\{1, |\alpha|_v\}$ for all places $v \mid p$. Hence when $p \nmid m$ and $v \mid p$ by (i) we have

$$\max\{ |(\alpha\beta)^p - \sigma_p(\alpha\beta)|_v, |\beta^p - \sigma_p(\beta)|_v \} \leq |p|_v,$$

and

$$\begin{aligned} |\alpha^p - \sigma_p(\alpha)|_v &= \max\{1, |\alpha|_v\}^p |(\alpha\beta)^p - \sigma_p(\alpha\beta) + \sigma_p(\alpha)(\sigma_p(\beta) - \beta^p)|_v \\ &\leq |p|_v \max\{1, |\alpha|_v\}^p \max\{1, |\sigma_p(\alpha)|_v\}. \end{aligned}$$

Similarly, when $p \mid m$ and $v \mid p$, by (ii) we have

$$\max\{ |(\alpha\beta)^p - \sigma_p(\alpha\beta)^p|_v, |\beta^p - \sigma_p(\beta)^p|_v \} \leq |p|_v^{\frac{p}{p-1}}$$

and

$$\begin{aligned} |\alpha^p - \sigma_p(\alpha)^p|_v &= \max\{1, |\alpha|_v\}^p |(\alpha\beta)^p - \sigma_p(\alpha\beta)^p + \sigma_p(\alpha)^p(\sigma_p(\beta)^p - \beta^p)|_v \\ &\leq |p|_v^{\frac{p}{p-1}} \max\{1, |\alpha|_v\}^p \max\{1, |\sigma_p(\alpha)|_v\}^p. \quad \square \end{aligned}$$

Lemma 2.3. *Suppose that $\alpha \in \mathbb{Q}(\zeta_m)$ and $\alpha \neq 0$.*

- (i) *If $\sigma_p(\alpha) = \alpha^p$ then α is a root of unity.*
- (ii) *If $p \mid m$ and $\alpha^p = \sigma_p(\alpha)^p$ then $\alpha/\zeta_m^u \in \mathbb{Q}(\zeta_{m/p})$ for some integer u .*
- (iii) *Suppose that $2 \mid m$ and $\sigma_2(\alpha) = \lambda\alpha$. If $\lambda = \pm i$ then $m = 4l$ with l odd, and $\alpha(1 + \lambda) \in \mathbb{Q}(\zeta_l)$. If $5\lambda^4 + 6\lambda^2 + 5 = 0$ then $m = 20l$ with l odd, $\lambda = -\alpha_3^{-2\varepsilon}(-1)^j$ for some $\varepsilon = \pm 1$, $j = 0$ or 1 , and $\alpha/\alpha_3^\varepsilon i^j \in \mathbb{Q}(\zeta_{5l})$.*
- (iv) *Suppose that $3 \mid m$ and $\sigma_3(\alpha) = \lambda\alpha$. If $7\lambda^6 + 13\lambda^3 + 7 = 0$ then $m = 21l$ with $3 \nmid l$, $\lambda = -\alpha_0^{-2\varepsilon} \zeta_3^j$ for some $\varepsilon = \pm 1$, $0 \leq j \leq 2$, and $\alpha/\alpha_0^\varepsilon \zeta_3^j \in \mathbb{Q}(\zeta_{7l})$. If $8\lambda^6 + 11\lambda^3 + 8 = 0$ then $m = 15l$, $3 \nmid l$, with $\lambda = \left(\frac{1-\sqrt{-15}}{4}\right)^\varepsilon \zeta_3^j$ for some $\varepsilon = \pm 1$, $0 \leq j \leq 2$, and $\alpha/(\sqrt{5} + \sqrt{-3})^\varepsilon \zeta_3^j \in \mathbb{Q}(\zeta_{5l})$.*

Proof. Statement (i) can be found in [5, Lemma 2.1], and (ii) is from [1, Lemma 2]. For (iii), suppose that $p = 2$, $4 \mid m$, and $\alpha \neq 0$ and $\sigma_2(\alpha) = \lambda\alpha$ with $\lambda = \pm i$ or a root of $5x^4 + 6x^2 + 5$ (so that $\lambda = -\alpha_3^{-2\varepsilon}(-1)^j$ for some $\varepsilon = \pm 1$, $j = 0$ or 1). Since $\alpha_3^2 = (1 + 2i)/\sqrt{5}$, in this latter case we must have $5 \mid m$. Writing $\alpha = A_0 + \zeta_m A_1$, with $A_i \in \mathbb{Q}(\zeta_{m/2})$, then $\sigma_2(\zeta_m) = -\zeta_m$ and $\sigma_2(\alpha) = A_0 - A_1 \zeta_m = \lambda A_0 + \lambda A_1 \zeta_m$. If $8 \mid m$, then $\lambda \in \mathbb{Q}(\zeta_{m/2})$ with $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_{m/2})] = 2$, forcing $A_0 = \lambda A_0$, $-A_1 = \lambda A_1$, and $\alpha = 0$. Thus $m = 4l$ with l odd and $A_i \in \mathbb{Q}(\zeta_l)$. If $\lambda = \pm i$, then $\zeta_m = i \zeta_l$, and $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_l)] = 2$ produces $\zeta_m A_1 = \mp i A_0$ and $\alpha = (1 \mp i) A_0$, with $A_0 \in \mathbb{Q}(\zeta_l)$. If $\lambda = -\alpha_3^{-2\varepsilon}(-1)^j$, then by observing that $\sigma_2(\alpha_3) = -1/\alpha_3$ and $\sigma(i) = -i$, we see that $\alpha/\alpha_3^\varepsilon i^j$ is fixed by σ_2 and hence lies in $\mathbb{Q}(\zeta_l)$.

For (iv), suppose that $3 \mid m$ and $\sigma_3(\alpha) = \lambda\alpha$, where λ^3 is a root of $7x^2 + 13x + 7$, so that $\lambda = -\alpha_0^{-2\varepsilon} \zeta_3^j$ for some $\varepsilon = \pm 1$ and $0 \leq j \leq 2$, or λ is a zero of $8x^2 + 11x + 8$, so that $\lambda = \left(\frac{1-\sqrt{-15}}{4}\right)^\varepsilon \zeta_3^j$ for some $\varepsilon = \pm 1$ and $0 \leq j \leq 2$. Since $\lambda \in \mathbb{Q}(\cos(2\pi/7), \zeta_3) \setminus \mathbb{Q}(\zeta_3)$ or $\mathbb{Q}(\sqrt{5}, \zeta_3) \setminus \mathbb{Q}(\zeta_3)$, we must have $7 \mid m$ or $5 \mid m$, respectively.

Write $\sigma_3(\zeta_m) = \zeta_m w$ for an appropriate primitive cube root of unity w . If $3^2 \mid m$, then λ and w are in $\mathbb{Q}(\zeta_{m/3})$ and $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_{m/3})] = 3$. Hence, writing $\alpha = A_0 + A_1 \zeta_m + A_2 \zeta_m^2$, where $A_i = \sum_{j \equiv i \pmod{3}} a_j \zeta_m^{j-i} \in \mathbb{Q}(\zeta_{m/3})$, we have $\sigma_3(\alpha) = A_0 + A_1 w \zeta_m + A_2 w^2 \zeta_m^2$, and $\sigma(\alpha) = \lambda\alpha$ forces $A_0 = \lambda A_0$, $A_1 w = \lambda A_1$, and $A_2 w^2 = \lambda A_2$, which cannot occur for $\alpha \neq 0$. So $3^2 \nmid m$.

For $m = 21l$ with $3 \nmid l$, we have $\sigma_3(\alpha_0) = -1/\alpha_0$ and $\sigma_3(\zeta_3) = \zeta_3^{-1}$. Hence $\alpha/\alpha_0^\varepsilon \zeta_3^j$ is fixed by σ_3 , so it is in $\mathbb{Q}(\zeta_{7l})$. Similarly, in the second case, when $m = 15l$ and $3 \nmid l$, we have $\sigma_3(\sqrt{5} + \sqrt{-3}) = \sqrt{5} - \sqrt{-3} = \left(\frac{1-\sqrt{-15}}{4}\right) (\sqrt{5} + \sqrt{-3})$, and $\alpha/(\sqrt{5} + \sqrt{-3})^\varepsilon \zeta_3^j$ is fixed by σ_3 . \square

Lemma 2.4. *Suppose that $\alpha \in \mathbb{Q}(\zeta_m)$, $\alpha \neq 0$, $p \nmid m$, and $\sigma_p(\alpha) = \lambda\alpha^p$.*

- (i) *If $p = 3$ and $11\lambda^4 + 19\lambda^3 + 21\lambda^2 + 19\lambda + 11 = 0$ then $h(\alpha) = \frac{1}{10} \log 11 = 0.239789\dots$*
- (ii) *If $p = 5$ and $7\lambda^2 + 11\lambda + 7 = 0$ then $\alpha = \alpha_0^\varepsilon \zeta$ for some root of unity ζ , $\varepsilon = \pm 1$, and $h(\alpha) = \frac{1}{12} \log 7 = 0.162159\dots$*
- (iii) *If $p = 5$ and $8\lambda^2 + 9\lambda + 8 = 0$ then $\alpha = \alpha_1^\varepsilon \zeta$ for some root of unity ζ , $\varepsilon = \pm 1$, and $h(\alpha) = \frac{1}{4} \log 2 = 0.173286\dots$*
- (iv) *If $p = 5$ and $61\lambda^4 + 156\lambda^3 + 191\lambda^2 + 156\lambda + 61 = 0$ then $h(\alpha) = \frac{1}{16} \log 61 = 0.256929\dots$*
- (v) *If $p = 7$ and $13\lambda^2 + 23\lambda + 13 = 0$ then $h(\alpha) = \frac{1}{12} \log 13 = 0.213745\dots$*

Proof. For (i), observe that the roots of $11x^4 + 19x^3 + 21x^2 + 19x + 11$ are in $\mathbb{Q}(\zeta_5)$ and take the form $\lambda_0 = -\frac{19}{44} + \frac{9}{44}\sqrt{5} + \frac{3}{11}\sin(\frac{4\pi}{5})(4 + \sqrt{5})i$, $\lambda_1 = \sigma_3(\lambda_0) = -\frac{19}{44} - \frac{9}{44}\sqrt{5} + \frac{3}{11}\sin(\frac{2\pi}{5})(4 - \sqrt{5})i$, $\sigma_3^2(\lambda_0) = 1/\lambda_0$, and $\sigma_3^3(\lambda_0) = 1/\lambda_1$. Hence if σ_3 has order $k = 4d$ and $\sigma_3(\alpha) = \lambda\alpha^3$, then

$$\begin{aligned} \alpha &= \sigma_3^k(\alpha) = \lambda^{3^{k-1}} \sigma_3(\lambda^{3^{k-2}}) \sigma_3^2(\lambda^{3^{k-3}}) \dots \sigma_3^{k-1}(\lambda) \alpha^{3^k} \\ &= \lambda^{3^{k-1} - 3^{k-3} + 3^{k-5} - \dots - 3} \sigma_3(\lambda)^{3^{k-2} - 3^{k-4} + 3^{k-6} - \dots - 1} \alpha^{3^k} \\ &= (\lambda^3 \sigma(\lambda))^{(3^k - 1)/10} \alpha^{3^k}, \end{aligned}$$

where $\lambda^3 \sigma(\lambda)$ has minimal polynomial $11^4 x^4 - 44209 x^3 + 59541 x^2 - 44209 x + 11^4$. Thus $h(\alpha) = \frac{1}{10} h((\lambda^3 \sigma(\lambda))^{-1}) = \frac{1}{10} \log 11$.

For (ii) and (iii), observe that if $\lambda = \frac{1}{14}(-11 \pm 5\sqrt{3}i) = (\zeta_3 \alpha_0^6)^{\pm 1}$, $\zeta_3 = \frac{1}{2}(-1 + \sqrt{3}i)$, or $\frac{1}{16}(-9 \mp 5\sqrt{7}i) = (-i\alpha_1^6)^{\pm 1}$, then $\sigma_5(\lambda) = \lambda^{-1}$. Hence if σ_5 has order $2d$ and $\sigma_5(\alpha) = \lambda\alpha^5$ then $\alpha = \sigma^{2d}(\alpha) = \lambda^{-1+5-5^2+\dots+5^{2d-1}} \alpha^{5^{2d}}$, producing $\alpha^{6(5^{2d}-1)} = (\lambda^{-1})^{5^{2d}-1}$, and $h(\alpha) = \frac{1}{6} h(\lambda^{-1}) = \frac{1}{12} \log 7$ or $\frac{1}{12} \log 8$, and $\alpha = \alpha_0^{\pm 1} \zeta$ or $\alpha_1^{\pm 1} \zeta$ for some root of unity ζ .

For (iv), observe that the zeros of $61x^4 + 156x^3 + 191x^2 + 156x + 61$ take the form $\lambda_0 = \frac{1}{122}(-78 + 25\sqrt{3} + 5(13 + 6\sqrt{3})i)$, $\sigma_5(\lambda_0) = \frac{1}{122}(-78 - 25\sqrt{3} + 5(13 - 6\sqrt{3})i)$, λ_0^{-1} and $\sigma_5(\lambda_0)^{-1}$. Hence if σ_5 has order $2d$ and $\sigma_5(\alpha) = \lambda\alpha^5$, then $\alpha = \sigma_5^{2d}(\alpha) = \sigma_5(\lambda)^{1+5^2+\dots+5^{2d-2}} \lambda^{5+5^3+\dots+5^{2d-1}} \alpha^{5^{2d}}$, yielding $\alpha^{24(5^{2d}-1)} = ((\lambda^5 \sigma_5(\lambda))^{-1})^{5^{2d}-1}$, where $(\lambda^5 \sigma_5(\lambda))^{-1}$ has minimal polynomial

$$61^6 x^4 - 74995263794 x^3 + 54052054491 x^2 - 74995263794 x + 61^6,$$

and $h(\alpha) = \frac{1}{24} (\frac{1}{4} \log 61^6)$.

For (v), if $p = 7$ and $\lambda = (-23 \pm 7\sqrt{3}i)/26$ then $\sigma_7(\lambda) = \lambda$. Hence if $\sigma_7(\alpha) = \lambda\alpha^7$ and σ_7 has order d , then $\alpha = \lambda^{1+7+\dots+7^{d-1}} \alpha^{7^d}$ and $h(\alpha) = \frac{1}{6} h(\lambda^{-1}) = \frac{1}{12} \log 13$. \square

Lemma 2.5. *If $t = 1$ or $t > 1$ and $k \leq 4t/(t-1)^2$, then*

$$\sup_{|z|=1} |(z-1)^k (z+t)| = \frac{(t+1)^{k+1}}{(k+1)^{\frac{1}{2}(k+1)}} \left(\frac{k}{t}\right)^{\frac{1}{2}k},$$

achieved at $z = -\frac{((t^2+1)k-2t)}{2t(k+1)} \pm \frac{(t+1)\sqrt{k(4t-(t-1)^2k)}}{2t(k+1)}i$. If $t > 1$ and $k \geq 4t/(t-1)^2$, the supremum is $2^k(t-1)$, achieved at $z = -1$.

Proof. Writing $z = e^{i\theta}$, $u = \cos \theta$, it is readily checked that

$$|(z-1)^k (z+t)|^2 = 2^k (1-u)^k ((t^2+1) + 2tu)$$

is maximised for $-1 \leq u \leq 1$ at $u = -\frac{((t^2+1)k-2t)}{2t(k+1)}$ provided $k \leq 4t/(t-1)^2$, and at $u = -1$ when $k \geq 4t/(t-1)^2$. \square

3. PROOF OF THEOREM 1

Suppose that $3 \mid m$. From Lemma 2.2 we have

$$|\alpha^3 - \sigma_3(\alpha)^3|_v \leq |3|_v^{3/2} \max\{1, |\alpha|_v\}^3 \max\{1, |\sigma_3(\alpha)|_v\}^3.$$

Similarly,

$$\begin{aligned} |\alpha^3 + 2\sigma_3(\alpha)^3|_v &= |\alpha^3 - \sigma_3(\alpha)^3 + 3\sigma_3(\alpha)^3|_v \\ &\leq |3|_v \max\{1, |\alpha|_v\}^3 \max\{1, |\sigma_3(\alpha)|_v\}^3, \end{aligned}$$

$$\begin{aligned} |7\alpha^6 + 13\alpha^3\sigma_3(\alpha)^3 + 7\sigma_3(\alpha)^6|_v &= \left| 7(\alpha^3 - \sigma_3(\alpha)^3)^2 + 27\alpha^3\sigma_3(\alpha)^3 \right|_v \\ &\leq |3|_v^3 \max\{1, |\alpha|_v\}^6 \max\{1, |\sigma_3(\alpha)|_v\}^6, \end{aligned}$$

and

$$\begin{aligned} |8\alpha^6 + 11\alpha^3\sigma_3(\alpha)^3 + 8\sigma_3(\alpha)^6|_v &= \left| 8(\alpha^3 - \sigma_3(\alpha)^3)^2 + 27\alpha^3\sigma_3(\alpha)^3 \right|_v \\ &\leq |3|_v^3 \max\{1, |\alpha|_v\}^6 \max\{1, |\sigma_3(\alpha)|_v\}^6 \end{aligned}$$

for the finite places v .

We consider the quantity

$$\begin{aligned} A &= (\alpha^3 - \sigma_3(\alpha)^3)^k (\alpha^3 + 2\sigma_3(\alpha)^3)^l (7\alpha^6 + 13\alpha^3\sigma_3(\alpha)^3 + 7\sigma_3(\alpha)^6)^t \\ &\quad \cdot (8\alpha^6 + 11\alpha^3\sigma_3(\alpha)^3 + 8\sigma_3(\alpha)^6)^s. \end{aligned}$$

Setting $\beta = \alpha^3/\sigma_3(\alpha)^3$, then as long as $\beta \neq 1$ when $k > 0$, β is not a zero of $7x^2 + 13x + 7$ when $t > 0$, and β is not a zero of $8x^2 + 11x + 8$ when $s > 0$, we have $A \neq 0$. Thus, writing $h(\alpha) = \log H(\alpha)$, where $H(\alpha) = \prod_{v \nmid \infty} \max\{1, |\alpha|_v\}$, the product formula produces

$$1 = \prod_{v \nmid \infty} |A|_v \prod_{v \mid \infty} |A|_v.$$

Since $|\alpha|_v = 1$ for all $v \mid \infty$, we have

$$\begin{aligned} \prod_{v \nmid \infty} |A|_v &\leq \prod_{v \mid 3} |3|_v^{3k/2+l+3t+3s} \left(\prod_{v \nmid \infty} \max\{1, |\alpha|_v\} \max\{1, |\sigma_3(\alpha)|_v\} \right)^{3k+3l+6t+6s} \\ &= 3^{-(1.5k+l+3t+3s)} H(\alpha)^{6(k+l+2t+2s)}, \end{aligned}$$

and

$$\begin{aligned} \prod_{v \mid \infty} |A|_v &= \prod_{v \mid \infty} \left| (\beta - 1)^k (\beta + 2)^l (7\beta^2 + 13\beta + 7)^t (8\beta^2 + 11\beta + 8)^s \right|_v \\ &\leq \prod_{v \mid \infty} \sup_{|z|=1} |(z-1)^k (z+2)^l (7z^2 + 13z + 7)^t (8z^2 + 11z + 8)^s|^{d_v/d} \\ &= \sqrt{M}, \end{aligned}$$

where

$$\begin{aligned} M &= \sup_{|z|=1} |(z-1)^k(z+2)^l(7z^2+13z+7)^t(8z^2+11z+8)^s|^2 \\ &= \sup_{-1 \leq u \leq 1} 2^k(1-u)^k(5+4u)^l(14u+13)^{2t}(16u+11)^{2s}. \end{aligned}$$

Hence

$$h(\alpha) \geq \frac{\log\left(3^{1.5k+l+3t+3s}/\sqrt{M}\right)}{6(k+l+2t+2s)}.$$

When $\beta \neq 1$, by taking $s = t = 0$, $k = 6$, and $l = 1$, we have $M = 3^{20}/7^7$, achieved at $u = -13/14$, producing $h(\alpha) \geq \frac{1}{12} \log 7$. When $\beta \neq 1$ and β is not a zero of $7x^2 + 13x + 7$, taking $s = 0$, $k = 14$, $l = 0$, and $t = 1$, we have $M = (3/2)^{48}$, achieved at $u = -11/16$, giving $h(\alpha) \geq \frac{1}{4} \log 2$. When $\beta \neq 1$ and β is not a zero of $7x^2 + 13x + 7$ or $8x^2 + 11x + 8$, then choosing $k = 303$, $l = 0$, $t = 37$, and $s = 17$ yields $h(\alpha) \geq 0.174878$. The restrictions on α (corresponding to the restrictions on β) needed for these bounds follow from Lemma 2.3, parts (ii) and (iv).

For $2 \mid m$, we assume $\beta = \alpha^2/\sigma_2(\alpha)^2 \neq 1$, and take

$$A = (\alpha^2 - \sigma_2(\alpha)^2)^k (\alpha^2 + \sigma_2(\alpha)^2)^l (5\alpha^4 + 6\alpha^2\sigma_2(\alpha)^2 + 5\sigma_2(\alpha)^4)^t,$$

where for $v \nmid \infty$

$$\begin{aligned} |\alpha^2 - \sigma_2(\alpha)^2|_v &\leq |2|_v^2 \max\{1, |\alpha|_v\}^2 \max\{1, |\sigma_2(\alpha)|_v\}^2, \\ |\alpha^2 + \sigma_2(\alpha)^2|_v &= |(\alpha^2 - \sigma_2(\alpha)^2) + 2\sigma_2(\alpha)^2| \\ &\leq |2|_v \max\{1, |\alpha|_v\}^2 \max\{1, |\sigma_2(\alpha)|_v\}^2, \end{aligned}$$

and

$$\begin{aligned} |5\alpha^4 + 6\alpha^2\sigma_2(\alpha)^2 + 5\sigma_2(\alpha)^4|_v &= |5(\alpha^2 - \sigma_2(\alpha)^2)^2 + 2^4\alpha^2\sigma_2(\alpha)^2|_v \\ &\leq |2|_v^4 \max\{1, |\alpha|_v\}^4 \max\{1, |\sigma_2(\alpha)|_v\}^4. \end{aligned}$$

Hence, as long as $A \neq 0$, we have

$$h(\alpha) \geq \frac{\log(2^{2k+l+4t}/\sqrt{M})}{4(k+l+2t)},$$

where

$$\begin{aligned} M &= \sup_{|z|=1} |(z-1)^k(z+1)^l(5z^2+6z+5)^t|^2 \\ &= \sup_{-1 \leq u \leq 1} 2^{k+l+2t}(1-u)^k(1+u)^l(5u+3)^{2t}. \end{aligned}$$

If $k = 1$ and $l = t = 0$, then we have $M = 4$, achieved at $u = -1$, which yields the Amoroso & Dvornicich bound, $h(\alpha) \geq \frac{1}{4} \log 2$. If $\beta \neq -1$, then choosing $k = 4$ and $l = 1$ produces $M = 2^{18}/5^5$, achieved at $u = -3/5$, from which one calculates $h(\alpha) \geq \frac{1}{8} \log 5$. Finally, when $\beta \neq -1$ and β is not a zero of $5x^2 + 6x + 5$, taking $k = 181$, $l = 37$, and $t = 17$, and calculating M numerically, we find the bound $h(\alpha) \geq 0.210291$. The conditions on α (for the various restrictions on β) follow from Lemma 2.3, parts (ii) and (iii). \square

4. PROOF OF THEOREM 2

The proof is similar to the proof of Theorem 1. When $p \nmid m$ (we will take $p = 3, 5, \text{ or } 7$), we consider

$$A = A_1^k A_2^l \prod_{i=1}^I A_{3,i}^{t_i} \prod_{j=1}^J A_{4,j}^{s_j},$$

where

$$\begin{aligned} A_1 &= \alpha^p - \sigma_p(\alpha), \\ A_2 &= \frac{1}{2}(p-1)\alpha^p + \frac{1}{2}(p+1)\sigma_p(\alpha), \end{aligned}$$

and for each i and j ,

$$\begin{aligned} A_{3,i} &= D_i(\alpha^p - \sigma_p(\alpha))^2 + p^2 \alpha^p \sigma_p(\alpha), \\ A_{4,j} &= C_j(\alpha^p - \sigma_p(\alpha))^4 + B_j p^2 \alpha^p \sigma_p(\alpha)(\alpha^p - \sigma_p(\alpha))^2 + p^4 \alpha^{2p} \sigma_p(\alpha)^2 \end{aligned}$$

for integers B_j, C_j , and D_i , with $D_1 = (p^2 + 3)/4$.

From Lemma 2.2 for $v \nmid \infty$, we have

$$\begin{aligned} |A_1|_v &\leq |p|_v \max\{1, |\alpha|_v\}^p \max\{1, |\sigma_p(\alpha)|_v\}, \\ |A_2|_v &= \left| \frac{1}{2}(p-1)(\alpha^p - \sigma_p(\alpha)) + p\sigma_p(\alpha) \right|_v \\ &\leq |p|_v \max\{1, |\alpha|_v\}^p \max\{1, |\sigma_p(\alpha)|_v\}, \\ |A_{3,i}|_v &\leq |p|_v^2 \max\{1, |\alpha|_v\}^{2p} \max\{1, |\sigma_p(\alpha)|_v\}^2 \end{aligned}$$

for each i , and

$$|A_{4,j}|_v \leq |p|_v^4 \max\{1, |\alpha|_v\}^{4p} \max\{1, |\sigma_p(\alpha)|_v\}^4$$

for each j . Hence, as long as $A \neq 0$, we find

$$1 \leq p^{-(k+l+2\sum_i t_i + 4\sum_j s_j)} H(\alpha)^{(p+1)(k+l+2\sum_i t_i + 4\sum_j s_j)} M^{\frac{1}{2}},$$

where

$$\begin{aligned} M &= \sup_{|z|=1} \left| (1-z)^k \left(\frac{1}{2}(p-1)z + \frac{1}{2}(p+1) \right)^l \prod_{i=1}^I (D_i(z-1)^2 + p^2 z)^{t_i} \right. \\ &\quad \left. \cdot \prod_{j=1}^J (C_j(z-1)^4 + B_j p^2 z(z-1)^2 + p^4 z^2)^{s_j} \right|^2 \\ &= \sup_{u \in [-1,1]} 2^k (1-u)^k \left(\frac{1}{2}(p^2+1) + \frac{1}{2}(p^2-1)u \right)^l \prod_{i=1}^I (2D_i(u-1) + p^2)^{2t_i} \\ &\quad \cdot \prod_{j=1}^J (4C_j(u-1)^2 + 2B_j p^2(u-1) + p^4)^{2s_j}. \end{aligned}$$

Since $\lambda = \sigma_p(\alpha)/\alpha^p$ is not 1 (as α is not a root of unity) or $-(p-1)/(p+1)$ (as $|\lambda| = 1$), we know that $A_1 A_2 \neq 0$. For $l = 1$, and all the $t_i, s_j = 0$, the optimal k is readily determined: By Lemma 2.5, with $t = (p+1)/(p-1)$, the maximum for

$k \leq p^2 - 1$ occurs at $u = -((p^2 + 1)k - (p^2 - 1)) / (p^2 - 1)(k + 1)$, leading to the bound

$$h(\alpha) \geq \frac{\log \left(\left(\frac{p^2-1}{4k} \right)^{\frac{1}{2}k} (k+1)^{\frac{1}{2}(k+1)} \right)}{(p+1)(k+1)}.$$

This is readily seen to be maximized by taking $k = \frac{1}{4}(p^2 - 1)$, with corresponding value of $u = -(p^2 - 3)/(p^2 + 3)$, producing the lower bound

$$h(\alpha) \geq \frac{\log \left(\frac{p^2+3}{4} \right)}{2(p+1)}. \tag{4.1}$$

In particular, with $p = 5$ we recover the bound $\frac{1}{12} \log 7$ when $5 \nmid m$, with equality only possible when $7\lambda^2 + 11\lambda + 7 = 0$.

When $p = 3$, we clearly have $\lambda \neq -\frac{p^2-3}{p^2+3} \pm \frac{2p}{p^2+3}\sqrt{3}i$ and $A_{3,1} \neq 0$. From Lemma 2.4, parts (ii) and (v), we may assume this also for $p = 5$ and 7 . For $p = 7$, the choice $k = 218$, $l = 14$, $t_1 = 7$, and $J = 0$ yields the lower bound $\log H(\alpha) \geq 0.1623680562\dots$. For $p = 5$, we take $D_1 = 7$, $D_2 = 8$ and $(C_1, B_1) = (61, 16)$. From Lemma 2.4, parts (iii) and (iv), we may assume that $A_{3,2}A_{4,1} \neq 0$. Taking $k = 149$, $l = 12$, $t_1 = 15$, $t_2 = 1$, and $s_1 = 3$, we obtain $\log H(\alpha) \geq 0.1669681194\dots$

For $p = 3$, we take $(C_1, B_1) = (11, 7)$ and $(C_2, B_2) = (13, 8)$. From Lemma 2.4, part (i), we can assume that $A_{4,1} \neq 0$, and since the zeros of $13x^4 + 20x^3 + 15x^2 + 20x + 13$ are $(-\frac{5}{26}(2 - 3i) \pm \frac{3}{26}\sqrt{3}(3 + 2i))^{\pm 1}$ and we are assuming that $3 \nmid m$, we may also assume that $A_{4,2} \neq 0$. Using a hill-climbing strategy, we find that the choice $k = 731428$, $l = 230997$, $t_1 = 139130$, $s_1 = 49072$, and $s_2 = 26663$ produces the bound $h(\alpha) \geq 0.1549971452\dots$ of (1.14). \square

Note that when $2 \nmid m$, taking $A = (\alpha^4 - \sigma_2(\alpha)^2)^4(\alpha^4 + \sigma_2(\alpha)^2)$ yields

$$1 \leq 2^{-9}H(\alpha)^{30}2^9/5^{5/2},$$

recovering the Amoroso & Dvornicich bound $H(\alpha) \geq 5^{1/12}$ without the need for their Lemma 4 inequality, similar to the simplification in [9] of the proof of Schinzel's theorem (1.1). Constructing additional auxiliary polynomials as in [6] would produce something marginally better and could be used in a similar way to improve (1.14) slightly.

REFERENCES

- [1] F. Amoroso & R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory **80** (2000), 260–262.
- [2] F. Amoroso & U. Zannier, *A uniform relative Dobrowolski's lower bound over abelian extensions*, preprint.
- [3] P. Borwein, E. Dobrowolski & M.J. Mossinghoff, *Lehmer's problem for polynomials with odd coefficients*, Ann. of Math. (2) **166** (2007), no. 2, 347–366.
- [4] J.W.S. Cassels, *Local Fields*, Cambridge Univ. Press, 1986.
- [5] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.
- [6] A. Dubickas & M.J. Mossinghoff, *Auxiliary polynomials for some problems regarding Mahler's measure*. Acta Arith. **119** (2005), no. 1, 65–79.
- [7] J. Garza, *On the height of algebraic numbers with real conjugates*, Acta Arith. **128** (2007), 385–389.
- [8] J. Garza, *The Mahler measure of dihedral extensions*, Acta Arith. **131** (2008), no. 3, 201–215.

- [9] G. Höhn & N.-P. Skoruppa, *Un résultat de Schinzel*, J. Théor. Nombres Bordeaux **5** (1993), 185.
- [10] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. **24** (1973), 385–399; Addendum *ibid.* 26 (1973), 329–361.

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: `mimishak@math.ksu.edu`

DEPARTMENT OF MATHEMATICS, DAVIDSON COLLEGE, DAVIDSON, NC 28035-6996
E-mail address: `mimossinghoff@davidson.edu`
Current address: Department of Mathematics, University of South Carolina, Columbia, SC 29208

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: `pinner@math.ksu.edu`

DEPARTMENT OF MATHEMATICS, KANSAS STATE UNIVERSITY, MANHATTAN, KS 66506
E-mail address: `wilesb@math.ksu.edu`