ACTA ARITHMETICA
151.1 (2012)

Multiplicative independence and bounded height

by

JOHN GARZA (Brownsville, TX)

1. Introduction. Amongst the absolute values in a place v of an algebraic number field $\mathbb{K}$, two play a role in this article. If v is archimedean, let $\|\cdot\|_v$ denote the unique absolute value in v that restricts to the usual archimedean absolute value on $\mathbb{Q}$. If v is non-archimedean and $v \mid p$, let $\|\cdot\|_v$ denote the unique absolute value in v that restricts to the usual p-adic absolute value on $\mathbb{Q}$. For each place v of $\mathbb{K}$, let $\mathbb{K}_v$ and $\mathbb{Q}_v$ be the completions of $\mathbb{K}$ and $\mathbb{Q}$ with respect to v and define the local degree of v as $d_v = [\mathbb{K}_v : \mathbb{Q}_v]$. For all places v let $|\cdot|_v = \|\cdot\|_v^{d_v/d}$.

The absolute values $|\cdot|_v$ satisfy the product rule: if $\alpha \in \mathbb{K}^\times$, then $\prod_v |\alpha|_v = 1$. The *absolute* (*logarithmic*) *Weil height* of α is defined as $h(\alpha) = \sum_v \log^+ |\alpha|_v$ where the sum is over all places v of $\mathbb{K}$. Because of the way in which the absolute values $|\cdot|_v$ are normalized, $h(\alpha)$ does not depend on the field $\mathbb{K}$ in which α is contained.

By Kronecker's theorem $h(\alpha) = 0$ if and only if $\alpha = 0$ or $\alpha \in \mathrm{Tor}(\overline{\mathbb{Q}}^\times)$. In 1933, Lehmer [L] asked whether or not there exists a constant $\varrho > 1$ such that

$$\deg(\alpha)h(\alpha) \geq \log \varrho \tag{1.1}$$

in all other cases. Lehmer's question remains unresolved to this day. For algebraic numbers α the *Mahler measure* $M(\alpha)$ is defined by $\log M(\alpha) = \deg(\alpha)h(\alpha)$. If $m_{\alpha,\mathbb{Z}} = a_0 \prod_{i=1}^d (x - \alpha_i) \in \mathbb{Z}[x]$ is the minimal polynomial of α in $\mathbb{Z}[x]$, it is known that

$$M(\alpha) = |a_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}. \tag{1.2}$$

The smallest non-zero Mahler measure known is that of the roots of $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$ and it is thought by many that if the

2010 *Mathematics Subject Classification*: Primary 11R09; Secondary 11G50.
Key words and phrases: Mahler measure, Weil height.

DOI: 10.4064/aa151-1-1

answer to Lehmer's question is yes then the minimum possible ϱ is the log of the Mahler measure of this polynomial.

If $\alpha \in \overline{\mathbb{Q}}^{\times}$ is not an algebraic integer, then the $|a_0|$ of equation (1.2) is at least 2. It follows that $M(\alpha) \geq 2$ so that Lehmer's question restricts to algebraic integers. For an algebraic number field $\mathbb{K}$, we let $\mathcal{O}_{\mathbb{K}}$ be the set of algebraic integers in $\mathbb{K}$. Also, if $\alpha \in \overline{\mathbb{Q}}^{\times}$ is an algebraic integer that is not a unit then

$$\mathrm{Norm}_{\mathbb{Q}(\alpha)/\mathbb{Q}} \geq 2. \tag{1.3}$$

It follows from (1.2) that (1.3) implies $M(\alpha) \geq 2$ and that Lehmer's problem restricts to consideration of algebraic units. We will let $\mathcal{O}_{\mathbb{K}}^{\times}$ denote the multiplicative group of algebraic units in $\mathbb{K}$.

Extending earlier work done by Schinzel [Sch], Beukers and Zagier [BZ], Samuels [Sa] and Garza [G1], Garza, Ishak and Pinner [GIP] established the following inequality involving the sum of logarithmic heights. Let $\alpha_1, \ldots, \alpha_r \in \overline{\mathbb{Q}}^{\times}$ be such that $\alpha_1 + \cdots + \alpha_r \neq \alpha_1^{-1} + \cdots + \alpha_r^{-1}$. Let $\mathcal{R}_{\mathcal{S}}$ be the proportion of the conjugates of $\mathcal{S} = \alpha_1 + \cdots + \alpha_r$ that are real. Then

$$\sum_{i=1}^{r} h(\alpha_i) \geq \frac{\mathcal{R}_{\mathcal{S}}}{2} \log\left(\frac{(2r)^{1-1/\mathcal{R}_{\mathcal{S}}} + \sqrt{(2r)^{2(1-1/\mathcal{R}_{\mathcal{S}})} + 4}}{2}\right). \tag{1.4}$$

From the arithmetic-geometric mean inequality, inequality (1.4) implies a lower bound for the average of $e^{h(\alpha_i)}$. In this article we derive a lower bound for $h(\alpha_1) + \cdots + h(\alpha_r)$ where $\alpha_1, \ldots, \alpha_r$ are multiplicatively independent algebraic integers. This can be applied to the non-torsion units in a generating set for $\mathcal{O}_{\mathbb{K}}^{\times}$ by using Dirichlet's unit theorem. It is noteworthy that Cohen and Zannier [CZ] established the upper bound $h(\alpha) + h(1-\alpha) \leq \log 2$ where $\alpha \in \overline{\mathbb{Q}}^{\times}$ and $\{\alpha, 1-\alpha\}$ is multiplicatively dependent.

2. Main results. A set $\{\alpha_1, \ldots, \alpha_r\} \subseteq \overline{\mathbb{Q}}^{\times}$ is said to be *multiplicatively independent* if the only solution to the equation $\alpha_1^{m_1} \cdots \alpha_r^{m_r} = 1$ with $m_1, \ldots, m_r \in \mathbb{Z}$ is $m_1 = \cdots = m_r = 0$. It follows that if $\{\alpha_1, \ldots, \alpha_r\}$ is multiplicatively independent then $\{\alpha_1, \ldots, \alpha_r\} \cap \mathrm{Tor}(\overline{\mathbb{Q}}^{\times}) = \emptyset$. We will say that $\{\alpha_1, \ldots, \alpha_r\} \subset \overline{\mathbb{Q}}^{\times}$ is *multiplicatively independent up to exponent n* if the inclusion $\alpha_1^{m_1} \cdots \alpha_r^{m_r} \in \mathrm{Tor}(\overline{\mathbb{Q}}^{\times})$ for $0 \leq |m_i| \leq n$ implies that $m_1 = \cdots = m_n = 0$. In this article we establish the following lower bound for $h(\alpha_1) + \cdots + h(\alpha_r)$ under the hypothesis of multiplicative independence up to exponent n.

THEOREM 2.1. *Let $\alpha_1, \ldots, \alpha_r \in \overline{\mathbb{Q}}^{\times}$, let $d = [\mathbb{Q}(\alpha_1, \ldots, \alpha_r) : \mathbb{Q}]$, and let $s \in \mathbb{N}$ be minimal such that $s > 2^{d/r}$. If $\alpha_1, \ldots, \alpha_r$ are multiplicatively* *independent up to exponent* $s-1$ *then*

$$\sum_{i=1}^{r} h(\alpha_i) \geq \frac{\log 2}{2(s-1)}. \tag{2.1}$$

It follows from the arithmetic-geometric mean inequality that Theorem 2.1 and equation (2.1) imply

$$\frac{e^{h(\alpha_1)} + \cdots + e^{h(\alpha_r)}}{r} \geq \big(\sqrt{2}\big)^{1/r(s-1)}.$$

Furthermore, Theorem 2.1, applied to the units in Dirichlet's theorem, results in the following.

THEOREM 2.2. *Let* $\mathbb{K}$ *be an algebraic number field of degree* $d \geq 8$. *Let* $\mathcal{O}_{\mathbb{K}}^{\times} = \langle \zeta, \alpha_1, \ldots, \alpha_t \rangle$ *where* $\{\alpha_1, \ldots, \alpha_t\} \cap \mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times}) = \emptyset$ *and* $\langle \zeta \rangle = \mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times})$. *Then*

$$\sum_{i=1}^{t} h(\alpha_i) \geq \frac{\log 2}{8}.$$

Although these theorems do not answer Lehmer's question, they tell us that, within a fixed algebraic number field, a large set of units of low height satisfy a multiplicative relation with small exponents. A generalization of this fact is used in Garza [G2].

3. Preliminary lemmas. In this section we present three lemmas used in the proof of Theorem 2.1. Lemma 3 will be used to establish the inclusion $0 \neq \gamma^2 - \beta^2 \in 4\mathcal{O}_{\mathbb{K}}$ where γ and β are algebraic numbers to be defined in Section 4. Lemma 1 with $p = 2$ will then be used to establish that $\prod_{v|4} |\gamma^2 - \beta^2|_v \leq 1/4$. This last inequality will be used in the application of Lemma 2 to $\gamma^2 - \beta^2$.

LEMMA 1. *Let* $\mathbb{K}/\mathbb{Q}$ *be a finite Galois extension and let* $p \in \mathbb{N}$ *be a prime with ramification index* e *in* $\mathbb{K}$. *Let* $\mathcal{A}_p = \{v_1, \ldots, v_t\}$ *be the set of places of* $\mathbb{K}$ *extending the* p*-adic place of* $\mathbb{Q}$. *For* $v_i \in \mathcal{A}_p$ *let* $\mathcal{M}_{v_i} = \{\alpha \in \mathbb{K} : |\alpha|_{v_i} < 1\}$. *Let* $s \in \mathbb{N}$, $s \leq t$, *and let* $\beta \in \mathbb{K}^{\times}$. *If* $\beta \in \mathcal{M}_{v_1}^{a_1} \cdots \mathcal{M}_{v_s}^{a_s}$ *for* $a_1, \ldots, a_s \in \mathbb{N} \cup \{0\}$, *then*

$$\sum_{\mathcal{A}_p} \log |\beta|_{v_i} \leq (-\log p) \cdot \left(\frac{1}{e \cdot t}\right) \cdot \Big(\sum_{j=1}^{s} a_j\Big).$$

Proof. Let $\mathfrak{B}_i = \mathcal{M}_{v_i} \cap \mathcal{O}_{\mathbb{K}}$ and let $\nu_{\mathfrak{B}_i} : \mathcal{O}_{\mathbb{K}} \to \mathbb{N} \cup \{0\}$ be the associated valuation. Given $\phi \in v_i$ there exists $\rho \in (0, \infty)$ such that for all $\gamma \in \mathbb{K}^{\times}$, $\phi(\gamma) = \rho^{-\nu_{\mathfrak{B}_i}(\gamma)}$. Since $\nu_{\mathfrak{B}_i}(p) = e$ and $\|p\|_{v_i} = p^{-1}$, the ρ associated to $\|\cdot\|_{v_i}$ is $p^{-1/e}$. Since $\mathbb{K}/\mathbb{Q}$ is Galois, the local degrees d_{v_i} of each place in $\mathcal{A}_p$ are equal. Their sum is $[\mathbb{K} : \mathbb{Q}]$ so the ρ associated to $|\cdot|_{v_i}$ is $p^{-1/et}$. Let π_i be a uniformizing parameter for $|\cdot|_{v_i}$. Then $\nu_{\mathfrak{B}_i}(\pi_i) = 1$ and $|\pi_i|_{v_i} = p^{-1/et}$. The lemma follows from this last equality. ∎

Lemma 2. *Let* $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^\times$, *let* $\mathbb{K}$ *be the Galois closure of* $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ *and let* $d = [\mathbb{K} : \mathbb{Q}]$. *For* $1 \leq j \leq n$ *and* $1 \leq k \leq m$ *let* $b_{j,k} \in \mathbb{N} \cup \{0\}$ *be such that* $\sum b_{j,k} \geq 1$ *and let* $c_k \in \mathbb{Z} - \{0\}$. *Define*

$$\delta = \sum_{k=1}^{m} c_k \prod_{j=1}^{n} \alpha_j^{b_{j,k}}, \qquad M_j = \max\{b_{j,k} : 1 \leq k \leq m\},$$

$$L = \sum_k |c_k|, \qquad w = \prod_{s \nmid \infty} |\delta|_v.$$

For each place $v \mid \infty$, *let* $a_v \in \mathbb{R}^+$ *be defined via*

$$\|\delta\|_v = a_v \prod_{j=1}^{n} \max\{1, \|\alpha_j^{M_j}\|_v\}$$

and let

$$A = \prod_{v \mid \infty} (a_v)^{d_v/d}.$$

If $\delta \neq 0$, *then*

$$wA \leq 1, \quad A \leq L \quad \text{and} \quad \sum_{j=1}^{n} M_j \cdot h(\alpha_j) \geq \log(1/wA).$$

Proof. By the triangle inequality, $a_v \leq L$ for all $v \mid \infty$, from which we obtain $A \leq L$. By the product rule, $\sum_v \log |\delta|_v = 0$. By definition, $\sum_{v \nmid \infty} \log |\delta|_v = \log w$ so that $\sum_{v \mid \infty} |\delta|_v = -\log w$. At this point we recall that $\| \cdot \|_v^{d_v/d} = | \cdot |_v$.

Fix $v \mid \infty$. Then

$$\|\delta\|_v = |\delta|_v^{d/d_v} = a_v \prod_{j=1}^{n} \max\{1, \|\alpha_j^{M_j}\|_v\}.$$

Consequently,

$$\log |\delta|_v = \left(\frac{d_v}{d}\right) \cdot \left(\log a_v + \sum_{j=1}^{n} M_j \log^+ \|\alpha_j\|_v\right).$$

Summing over all the archimedean places, we obtain

$$\sum_{v \mid \infty} \log |\delta|_v = \sum_{v \mid \infty} \log a_v^{d_v/d} + \sum_{v \mid \infty} \sum_{j=1}^{n} M_j \log^+ |\alpha_j|_v.$$

This leads to

$$\log(1/wA) = \sum_{j=1}^{n} M_j \sum_{v \mid \infty} \log^+ |\alpha_j|_v.$$

Since $\sum_{v|\infty} \log^+ |\alpha_j|_v \leq h(\alpha_j)$ the last equation implies

$$\log(1/wA) \leq \sum_{j=1}^{n} M_j \cdot h(\alpha_j). \blacksquare$$

LEMMA 3. *Let $\mathbb{K}$ be an algebraic number field of degree d over $\mathbb{Q}$. Let $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_{\mathbb{K}} - \{0\}$. Let $s \in \mathbb{N}$ be minimal such that $s^r > 2^d$. Define*

$$\mathcal{A} = \{\alpha_1^{\delta_1} \cdots \alpha_r^{\delta_r} : 0 \leq \delta_i \leq s-1,\ i = 1, \ldots, r\}.$$

If $\{\alpha_1, \ldots, \alpha_r\}$ is multiplicatively independent of exponent $s-1$ then there exist distinct elements γ and β of $\mathcal{A}$ such that

$$0 \neq \gamma^2 - \beta^2 \in 4\mathcal{O}_{\mathbb{K}}.$$

Proof. $(\mathcal{O}_{\mathbb{K}}, +)$ is a free abelian group of rank d. Let $\omega_1, \ldots, \omega_d \in \mathcal{O}_{\mathbb{K}}$ be such that $(\mathcal{O}_{\mathbb{K}}, +) = \langle \omega_1, \ldots, \omega_d \rangle$. Now, $2\mathcal{O}_{\mathbb{K}} \triangleleft \mathcal{O}_{\mathbb{K}}$ and $\mathcal{O}_{\mathbb{K}}/2\mathcal{O}_{\mathbb{K}}$ is an elementary abelian 2-group. Let $\Psi : \mathcal{O}_{\mathbb{K}} \to \mathcal{O}_{\mathbb{K}}/2\mathcal{O}_{\mathbb{K}}$ be the natural projection homomorphism. Then $\mathcal{O}_{\mathbb{K}}/2\mathcal{O}_{\mathbb{K}} = \langle \Psi(\omega_1), \ldots, \Psi(\omega_d) \rangle$. If there exists $1 \leq i < j \leq d$ such that $\Psi(\omega_i) = \Psi(\omega_j)$ then $\omega_i - \omega_j \in 2\mathcal{O}_{\mathbb{K}}$. So there exists $\tau \in \mathcal{O}_{\mathbb{K}}$ such that $\omega_i - \omega_j = 2\tau$. This last equation together with the fact that τ is an element of the free abelian group $\langle \omega_1, \ldots, \omega_d \rangle$ results in a non-trivial $\mathbb{Z}$-linear dependence equation amongst $\omega_1, \ldots, \omega_d$. This is a contradiction. Thus $|\mathcal{O}_{\mathbb{K}} : 2\mathcal{O}_{\mathbb{K}}| = 2^d$.

Since $\{\alpha_1, \ldots, \alpha_r\}$ is multiplicatively independent of exponent $s-1$ it follows from the counting principle that $\big|\mathcal{A}\big| = s^r$. There thus exist distinct γ and β in $\mathcal{A}$ such that $\Psi(\gamma) = \Psi(\beta)$ or equivalently $\Psi(\gamma) - \Psi(\beta) = \Psi(\gamma - \beta)$ $= 0$. It follows that $\gamma - \beta \in \ker \Psi = 2\mathcal{O}_{\mathbb{K}}$. Since $2\beta \in 2\mathcal{O}_{\mathbb{K}}$, $(\alpha - \beta) + 2\beta = \alpha + \beta \in 2\mathcal{O}_{\mathbb{K}}$. From this, $(\alpha - \beta)(\alpha + \beta) = \alpha^2 - \beta^2 \in 4\mathcal{O}_{\mathbb{K}}$. Since $\{\alpha_1, \ldots, \alpha_r\}$ is multiplicatively independent of exponent $s-1$, we have $0 \neq \gamma - \beta$ and $0 \neq \gamma + \beta$. It follows that $0 \neq (\gamma + \beta)(\gamma - \beta) = \gamma^2 - \beta^2$. $\blacksquare$

4. Proof of the main results

Proof of Theorem 2.1. Define

$$\mathcal{A} = \{\alpha_1^{\delta_1} \cdots \alpha_r^{\delta_r} : 0 \leq \delta_i \leq s-1,\ i = 1, \ldots, r\}.$$

Since $\{\alpha_1, \ldots, \alpha_r\}$ is multiplicatively independent of exponent $s-1$, we see that $|\mathcal{A}| > 2^d$. By Lemma 3, there exist γ and β in $\mathcal{A}$ such that $0 \neq \gamma^2 - \beta^2 \in 4\mathcal{O}_{\mathbb{K}}$. By Lemma 1 with $p = 2$,

$$\prod_{v \nmid \infty} |\gamma^2 - \beta^2|_v \leq \frac{1}{4}.$$

In this case, the notation of Lemma 2 corresponds with $w \leq 1/4$, $L = 2$, $M_j \leq 2(s-1)$, and $\log 2 \leq 2(s-1) \sum_{i=1}^{r} h(\alpha_i)$. $\blacksquare$

Proof of Theorem 2.2. Let r_1 be the number of isomorphisms of $\mathbb{K}$ into $\mathbb{R}$, let r_2 be the number of complex conjugation pairs of isomorphisms of $\mathbb{K}$ into $\mathbb{C}$ and not into $\mathbb{R}$ and let $r = r_1 + r_2$. By Dirichlet's unit theorem, there exist $\zeta \in \mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times})$ and $\omega_1, \ldots, \omega_{r-1} \in \mathcal{O}_{\mathbb{K}}^{\times} - \mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times})$ such that every $\epsilon \in \mathcal{O}_{\mathbb{K}}^{\times}$ can be uniquely represented as $\epsilon = \zeta^k \prod_{i=1}^{r-1} \omega_i^{m_i}$ where $m_i \in \mathbb{Z}$ for $i = 1, \ldots, r-1$ and $k = 0, \ldots, |\mathrm{Tor}(\mathcal{O}_{\mathbb{K}}^{\times})|$. By definition, $r \geq d/2$, so that $r - 1 \geq (d-2)/2$. Since $\langle \zeta, \alpha_1, \ldots, \alpha_t \rangle = \mathcal{O}_{\mathbb{K}}^{\times}$, we see that $\{\alpha_1, \ldots, \alpha_t\}$ contains a set of $r-1$ multiplicatively independent algebraic units. If $d \geq 8$ then $5^{r-1} > 2^d$. By Theorem 2.1,

$$\sum_{i=1}^{t} h(\alpha_i) \geq \frac{\log 2}{8}. \quad \blacksquare$$

References

[BZ] F. Beukers and D. Zagier, *Lower bounds of heights of points on hypersurfaces*, Acta Arith. 79 (1997), 103–111.

[CZ] P. B. Cohen and U. Zannier, *Multiplicative dependence and bounded height, an example*, in: Algebraic Number Theory and Diophantine Approximation (Graz, 1998), de Gruyter, 2000, 93–101.

[G1] J. Garza, *On the height of algebraic numbers with real conjugates*, Acta Arith. 128 (2007), 385–389.

[G2] —, *Polynomial relations amongst algebraic units of low measure*, preprint.

[GIP] J. Garza, M. I. M. Ishak and C. Pinner, *On the product of heights of algebraic numbers summing to real numbers*, Acta Arith. 142 (2010), 51–58.

[L] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. 34 (1933), 461–479.

[Sa] C. L. Samuels, *Lower bounds on the projective heights of algebraic points*, Acta Arith. 125 (2006), 41–50.

[Sch] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, ibid. 24 (1973), 385–399; Addendum, ibid. 26 (1975), 329–331.

John Garza
Department of Mathematics
The University of Texas at Brownsville
80 Fort Brown
Brownsville, TX 78520, U.S.A.
E-mail: John.Garza@utb.edu

Received on 21.3.2010
and in revised form on 29.1.2011 (6339)