ACTA ARITHMETICA
137.2 (2009)

The Lehmer strength bounds for total ramification

by

John Garza (Manhattan, KS)

1. Introduction. Mahler's measure of a polynomial f, denoted by $\mathrm{M}(f)$, is defined as the product of the absolute values of those roots of f that lie outside the unit disk, multiplied by the absolute value of the leading coefficient. If $f(x) = b\prod_{i=1}^{d}(x-\alpha_i)$, then

$$\mathrm{M}(f) = |b|\prod_{i=1}^{d}\max\{1,|\alpha_i|\}.$$

If $f \in \mathbb{Z}[x]$, then $\mathrm{M}(f) \geq 1$ and it is a result of Kronecker that for $f \in \mathbb{Z}[x]$, $\mathrm{M}(f) = 1$ if and only if f is a product of a power of x and cyclotomic polynomials. In 1933, D. H. Lehmer [1] asked if for every $\varepsilon > 0$ there exists $f_\varepsilon \in \mathbb{Z}[x]$ such that $1 < \mathrm{M}(f_\varepsilon) < 1+\varepsilon$. This is known as *Lehmer's question* and remains an open problem. For an algebraic number α, we let $m_{\alpha,\mathbb{Z}}$ be the minimal polynomial of α over $\mathbb{Z}$ and define $\mathrm{M}(\alpha) \equiv \mathrm{M}(m_{\alpha,\mathbb{Z}})$. It follows that for an algebraic number α that is not an integer, $\mathrm{M}(\alpha) \geq 2$.

Lehmer identified $l(x) = x^{10}+x^9-x^7-x^6-x^5-x^4-x^3+x+1$ as having lowest known Mahler measure and to this day l has the lowest known Mahler measure (other than 1) amongst polynomials in $\mathbb{Z}[x]$, $\mathrm{M}(l) \approx 1.176$. If a lower bound for the Mahler measure of a polynomial in $\mathbb{Z}[x]$ is greater than $\mathrm{M}(l)$ then we say that the lower bound is *of Lehmer strength*. Mossinghoff, Rhin and Wu [3] have determined that for algebraic numbers different from zero and the roots of unity and of degree ≤ 54, $\mathrm{M}(\alpha) \geq \mathrm{M}(l)$. An algebraic integer, $\alpha \notin \mathbb{Z}$, is said to be *reciprocal* if $1/\alpha$ is a Galois conjugate of α. C. Smyth [5] proved that amongst all nonreciprocal, nonzero algebraic integers the smallest Mahler measure is attained by the roots of x^3-x-1. Schinzel [4] has proven that if f is monic of degree d satisfying $f(0) = \pm 1$, $f(\pm 1) \neq 0$, and all roots of f real, then $\mathrm{M}(f) \geq ((1+\sqrt{5})/2)^{d/2}$.

For a rational prime p, an algebraic number α is said to be *totally p-adic* if the Galois closure of $\mathbb{Q}(\alpha)$ can be embedded into $\mathbb{Q}_p$. This is equivalent to

2000 *Mathematics Subject Classification*: Primary 11R09; Secondary 11G50.
Key words and phrases: Mahler measure, Weil height, ramification.

DOI: 10.4064/aa137-2-5

saying that the rational prime p splits completely in $\mathbb{Q}(\alpha)$ or that p is unramified in $\mathbb{Q}(\alpha)$ and that all the prime ideal divisors of $p\mathcal{O}_{\mathbb{Q}(\alpha)}$ have residue class degree 1. Mignotte [2] has proven that given an algebraic number α of degree d such that there exists a rational prime $p \leq d \log d$ that splits completely in $\mathbb{Q}(\alpha)$, $\mathrm{M}(\alpha) > \mathrm{M}(l)$. This result was quoted by Smyth [6] in a recent survey article.

The purpose of this article is to identify the corresponding lower bounds of Lehmer strength for the case of total ramification. We establish the following companions to the results of Mignotte and Schinzel.

THEOREM 1. *Let α be an algebraic number different from zero and the roots of unity. Let $p > [\mathbb{Q}(\alpha) : \mathbb{Q}]$ be a prime that ramifies completely in $\mathbb{Q}(\alpha)$. Then $\mathrm{M}(\alpha) \geq \sqrt{5} - 1 > \mathrm{M}(l)$.*

THEOREM 2. *Let α be an algebraic number different from zero and the roots of unity. If 2 ramifies completely in $\mathbb{Q}(\alpha)$ then $\mathrm{M}(\alpha) \geq \sqrt[4]{2} > \mathrm{M}(l)$.*

2. The absolute Weil height. Amongst the absolute values in a place v of an algebraic number field, $\mathbb{K}$, two will play a role in the development of Theorems 1 and 2. If v is Archimedean, let $\|\cdot\|_v$ denote the unique absolute value in v which 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 restricting to the usual p-adic absolute value on $\mathbb{Q}$. For each place v of $\mathbb{K}$, let $\mathbb{K}_v$ and $\mathbb{Q}_v$ denote the completions of $\mathbb{K}$ and $\mathbb{Q}$ with respect to v and define the local degree as $d_v \equiv [\mathbb{K}_v : \mathbb{Q}_v]$. Let $|\cdot|_v = \|\cdot\|_v^{d_v/d}$.

The absolute values $|\cdot|_v$ satisfy the product formula: 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 normalised, the absolute Weil height of α does not depend on the field $\mathbb{K}$ in which α is contained. If α_i and α_j are algebraic numbers, $h(\alpha_i \cdot \alpha_j) \leq h(\alpha_i) + h(\alpha_j)$ and if α_i and α_j are Galois conjugates then $h(\alpha_i) = h(\alpha_j)$. For a root of unity ζ and an algebraic number α, $h(\zeta \cdot \alpha) = h(\alpha)$. For an algebraic number α, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \cdot h(\alpha) = \mathrm{M}(\alpha)$.

An algebraic integer α is a unit if and only if $\mathrm{Norm}_{\mathbb{Q}}(\alpha) = 1$. Since we are considering Lehmer's question, it follows that we may restrict to consideration of units. In this case, $\sum_{v \nmid \infty} \log^+ |\alpha|_v = 0$ and $h(\alpha) = \sum_{v \mid \infty} \log^+ |\alpha|_v$. It follows from the product formula that for an algebraic number α,

$$\sum_{v \mid \infty} \log^+ |\alpha|_v \geq - \sum_{v \nmid \infty} \log |\alpha|_v.$$

3. Preliminary lemmas. This section establishes Lemmas 1 and 2 which are used in the proofs of Theorems 1 and 2.

LEMMA 1. *Let $\alpha \neq 1$ be an algebraic number whose trace is greater than or equal to its degree. Then* $\mathrm{M}(\alpha) \geq \sqrt{5} - 1 > \mathrm{M}(l)$.

Proof. Suppose that $\mathrm{M}(\alpha) < \sqrt{5} - 1$. Let $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Let $\mathcal{A} = \{\alpha_1, \ldots, \alpha_d\}$ be the set of Galois conjugates of α and let $\mathbb{K}$ be the Galois closure of $\mathbb{Q}(\alpha)$. Fix an embedding $\eta : \mathbb{K} \hookrightarrow \mathbb{C}$ and let $\| \cdot \|_\infty$ be the usual Archimedean absolute value on $\mathbb{C}$. Since

$$\mathrm{M}(\alpha) \geq \prod_{\mathcal{A}} \max\{1, \|\mathrm{Re}\,\eta(\omega)\|_\infty\} \geq 1 + \sum_{\mathcal{A}} \max\{0, \mathrm{Re}\,\eta(\omega) - 1\}$$

and $\sum_{\mathcal{A}} \mathrm{Re}\,\eta(\omega) \geq d$ it follows that for all $\omega \in \mathcal{A}$, $3 - \sqrt{5} < \mathrm{Re}\,\eta(\omega) < \sqrt{5} - 1$. Consequently,

$$\begin{aligned}
\|\mathrm{Im}\,\eta(\omega) - 1\|_\infty^2 &= \|\mathrm{Im}\,\eta(\omega)\|_\infty^2 = \|\eta(\omega)\|_\infty^2 - \|\mathrm{Re}\,\eta(\omega)\|_\infty^2 \\
&< (\sqrt{5} - 1)^2 - (3 - \sqrt{5})^2, \\
\|\mathrm{Re}\,\eta(\omega) - 1\|_\infty^2 &\leq (\sqrt{5} - 2)^2, \\
\|\eta(\omega) - 1\|_\infty^2 &= \|\mathrm{Re}\,\eta(\omega) - 1\|_\infty^2 + \|\mathrm{Im}\,\eta(\omega) - 1\|_\infty^2 \\
&\leq (\sqrt{5} - 2)^2 + (\sqrt{5} - 1)^2 - (3 - \sqrt{5})^2 \\
&< 1.
\end{aligned}$$

As a result, the rational integer $\prod_{\mathcal{A}} \|\eta(\omega) - 1\|_\infty$ lies strictly between 0 and 1. This contradicts the Fundamental Principle of Number Theory. ∎

LEMMA 2. *Let α be an algebraic number. Let p be a rational prime that ramifies completely in $\mathbb{Q}(\alpha)$. Let $\mathbb{K}$ be the Galois closure of $\mathbb{Q}(\alpha)$, let $\mathfrak{B}$ be a prime ideal divisor of $p\mathcal{O}_{\mathbb{K}}$, let $\mathrm{H}_{\mathbb{Q}(\alpha)}$ be the subgroup of* $\mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ *fixing the field $\mathbb{Q}(\alpha)$ and let G_0 be the ramification group of $\mathfrak{B}$. Then* $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \mathrm{G}_0\mathrm{H}_{\mathbb{Q}(\alpha)}$.

Proof. Let $\mathrm{G}_{\mathfrak{B}}$ be the decomposition group of $\mathfrak{B}$. Let $\mathcal{R}_\alpha = \{g_1, \ldots, g_t\}$ be a set of representatives for the double cosets of $\mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ with respect to $\mathrm{H}_{\mathbb{Q}(\alpha)}$ and G_0. Then

$$\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \bigcup_{i=1}^{t} \mathrm{H}_{\mathbb{Q}(\alpha)} g_i \mathrm{G}_{\mathfrak{B}}.$$

The distinct prime ideal divisors of $p\mathcal{O}_{\mathbb{Q}(\alpha)}$ are given by

$$g_i\mathfrak{B} \cap \mathcal{O}_{\mathbb{Q}(\alpha)}.$$

The ramification index e_i' of $g_i\mathfrak{B} \cap \mathcal{O}_{\mathbb{Q}(\alpha)}$ is given by

$$e_i' = \frac{|\mathrm{G}_0|}{|g_i \mathrm{G}_0 g_i^{-1} \cap \mathrm{H}_{\mathbb{Q}(\alpha)}|}.$$

Since p is completely ramified in $\mathbb{Q}(\alpha)$ there exists a unique prime ideal divisor $\mathfrak{B} \cap \mathcal{O}_{\mathbb{Q}(\alpha)}$ of $p\mathcal{O}_{\mathbb{Q}(\alpha)}$. As a result, $|\mathcal{R}_\alpha| = 1$ and we may suppose that

$\mathcal{R}_\alpha = \{1\}$. It thus follows that $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \mathrm{G}_{\mathfrak{B}}\mathrm{H}_{\mathbb{Q}(\alpha)}$. Furthermore, the ramification index e' of $\mathfrak{B} \cap \mathcal{O}_{\mathbb{Q}(\alpha)}$ is

$$e' = \frac{|\mathrm{G}_0|}{|\mathrm{G}_0 \cap \mathrm{H}_{\mathbb{Q}(\alpha)}|} = [\mathbb{Q}(\alpha) : \mathbb{Q}],$$

which implies that

$$|\mathrm{G}_0\mathrm{H}_{\mathbb{Q}(\alpha)}| = \frac{|\mathrm{G}_0| \cdot |\mathrm{H}_{\mathbb{Q}(\alpha)}|}{|\mathrm{G}_0 \cap \mathrm{H}_{\mathbb{Q}(\alpha)}|} = |\mathrm{H}_{\mathbb{Q}(\alpha)}| \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = |\mathrm{Aut}(\mathbb{K}/\mathbb{Q})|. \ \blacksquare$$

4. Proof of Theorem 1. By the result of Mossinghoff, Rhin and Wu [3], we may suppose that $p > [\mathbb{Q}(\alpha) : \mathbb{Q}] > 54$. Let $\mathbb{K}$ be the Galois closure of $\mathbb{Q}(\alpha)$, let $\alpha_1, \ldots, \alpha_d$ be the Galois conjugates of α and let $\mathrm{H}_{\mathbb{Q}(\alpha)}$ be the subgroup of $\mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ fixing the field $\mathbb{Q}(\alpha)$. Let $\mathfrak{B}$ be a prime ideal divisor of $p\mathcal{O}_{\mathbb{K}}$ and let G_0 be the ramification group of $\mathfrak{B}$. By the result of Smyth [5], we may suppose that there exists $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ such that $\sigma(\alpha) = 1/\alpha$. By Lemma 2, $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \mathrm{G}_0\mathrm{H}_{\mathbb{Q}(\alpha)}$. There thus exist $\tau \in \mathrm{H}_{\mathbb{Q}(\alpha)}$ and $\gamma \in \mathrm{G}_0$ such that $\sigma = \gamma\tau$. Since p ramifies completely in $\mathbb{Q}(\alpha)$, there exists a unique prime ideal divisor $\mathfrak{B}'$ of $p\mathcal{O}_{\mathbb{Q}(\alpha)}$ and $p\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathfrak{B}'^{[\mathbb{Q}(\alpha):\mathbb{Q}]}$. It follows that

$$\alpha - \sigma(\alpha) = \alpha - \gamma(\tau(\alpha)) = \alpha - \gamma(\alpha) \in \mathfrak{B}'.$$

As a result

$$\alpha - \sigma(\alpha) \in \mathfrak{B}', \quad \alpha - 1/\alpha \in \mathfrak{B}'.$$

Since α is a unit and by the difference of squares formula,

$$\alpha^2 - 1 \in \mathfrak{B}', \quad (\alpha + 1)(\alpha - 1) \in \mathfrak{B}'.$$

Since $\mathfrak{B}'$ is a prime ideal we may suppose that $\alpha - 1 \in \mathfrak{B}'$ or $\alpha + 1 \in \mathfrak{B}'$. In the following arguments it will not matter whether $\alpha - 1 \in \mathfrak{B}'$ or $\alpha + 1 \in \mathfrak{B}'$. We will thus suppose that $\alpha - 1 \in \mathfrak{B}'$.

Case 1: $p > 3 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Let $\mathfrak{B}_1, \ldots, \mathfrak{B}_t$ be the distinct prime ideal divisors of $p\mathcal{O}_{\mathbb{K}}$. It follows that for all conjugates α_i of α,

$$\alpha_i - 1 \in \prod_{j=1}^{t} \mathfrak{B}_j,$$

so that

$$\Big(\sum_{i=1}^{d} \alpha_i\Big) - [\mathbb{Q}(\alpha) : \mathbb{Q}] \in p\mathbb{Z}, \quad \mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) - [\mathbb{Q}(\alpha) : \mathbb{Q}] \in p\mathbb{Z}.$$

Since $3 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] < p$ we may suppose that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq |\mathrm{Tr}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha)|_\infty$. By Lemma 1 (considering $-\alpha$ if necessary), $\mathrm{M}(\alpha) \geq \sqrt{5} - 1$.

Case 2: $p < 3 \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]$. From the inclusion $\alpha - 1 \in \mathfrak{B}'$ and the Binomial Theorem it follows that $\alpha^p - 1 \in p\mathcal{O}_{\mathbb{Q}(\alpha)}$. Since $\alpha^p - 1 \in \mathcal{O}_{\mathbb{Q}(\alpha)}$ it

follows that

$$\sum_{v\nmid\infty} \log|\alpha^p - 1|_v < -\log p$$

and from the last paragraph of Section 2,

$$\sum_{v|\infty} \log|\alpha^p - 1|_v > \log p.$$

Since $[\mathbb{Q}(\alpha):\mathbb{Q}]\cdot h(\alpha) = \log \mathrm{M}(\alpha)$ and $59 < p < 3\cdot[\mathbb{Q}(\alpha):\mathbb{Q}]$ it follows from

$$\sum_{v|\infty} \log|\alpha^p - 1|_\infty \le \log 2 + p\cdot\sum_{v|\infty}\log^+|\alpha|_v$$

that

$$\frac{1}{p}\log\frac{p}{2} \le \sum_{v|\infty}\log^+|\alpha|_v = h(\alpha)$$

and

$$\sqrt{5} - 1 < \frac{1}{3}\log\frac{p}{2} \le \log \mathrm{M}(\alpha). \ \blacksquare$$

5. Proof of Theorem 2. Let $\mathbb{K}$ be the Galois closure of $\mathbb{Q}(\alpha)$ and let $\mathrm{H}_{\mathbb{Q}(\alpha)}$ be the subgroup of $\mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ fixing the field $\mathbb{Q}(\alpha)$. Let $\mathfrak{B}$ be a prime ideal divisor of $2\mathcal{O}_{\mathbb{K}}$ and let G_0 be the ramification group of $\mathfrak{B}$. By the result of Smyth we may suppose that there exists $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ such that $\sigma(\alpha) = 1/\alpha$. By Lemma 2, $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \mathrm{G}_0\mathrm{H}_{\mathbb{Q}(\alpha)}$. There thus exist $\tau \in \mathrm{H}_{\mathbb{Q}(\alpha)}$ and $\gamma \in \mathrm{G}_0$ such that $\sigma = \gamma\tau$. Since 2 ramifies completely in $\mathbb{Q}(\alpha)$ there exists a unique prime ideal divisor $\mathfrak{B}'$ of $2\mathcal{O}_{\mathbb{Q}(\alpha)}$ and $2\mathcal{O}_{\mathbb{Q}(\alpha)} = (\mathfrak{B}')^{[\mathbb{Q}(\alpha):\mathbb{Q}]}$. It follows from these remarks that $\alpha - \sigma(\alpha) = \alpha - \gamma(\tau(\alpha)) = \alpha - \gamma(\alpha) \in \mathfrak{B}'$. Since α is a unit, by the difference of squares formula and since $\mathfrak{B}'$ is a prime ideal $\alpha - \sigma(\alpha) \in \mathfrak{B}'$, $\alpha - 1/\alpha \in \mathfrak{B}'$, $\alpha^2 - 1 \in \mathfrak{B}'$, $(\alpha+1)(\alpha-1) \in \mathfrak{B}'$, $\alpha - 1 \in \mathfrak{B}'$. Let $r \in \mathbb{N}$ be minimal such that $2^r \ge [\mathbb{Q}(\alpha):\mathbb{Q}]$. Then $2^{r+1} < 4\cdot[\mathbb{Q}(\alpha):\mathbb{Q}]$. By the last inclusion, the difference of squares formula and the last paragraph of Section 2,

$$\alpha^{2^{r+1}} - 1 \in (\mathfrak{B}')^{2\cdot[\mathbb{Q}(\alpha):\mathbb{Q}]} = 4\mathcal{O}_{\mathbb{Q}(\alpha)},$$

$$\sum_{v\nmid\infty}\log|\alpha^{2^{r+1}} - 1|_v \le -\log 4,$$

$$\log 4 < \log 2 + 2^{r+1}\cdot\sum_{v|\infty}\log^+|\alpha|_v,$$

$$\frac{1}{2^{r+1}}\cdot\log 2 \le h(\alpha),$$

$$\mathrm{M}(l) < \sqrt[4]{2} \le \mathrm{M}(\alpha). \ \blacksquare$$

References

[1] D. H. Lehmer, *Factorizations of certain cyclotomic functions*, Ann. of Math. (2) 34 (1933), 461–479.

[2] M. Mignotte, *Entiers algébriques dont les conjugués sont proches du cercle unité*, in: Séminaire Delange–Pisot–Poitou, 19e année: 1977/78, Théorie des nombres, Fasc. 2, Exp. No. 39, Secrétariat Math., Paris, 1978, 6 pp.

[3] M. J. Mossinghoff, G. Rhin and Q. Wu, *Minimal Mahler measures*, Experiment. Math., to appear.

[4] 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), 329–331.

[5] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. 3 (1971), 169–175.

[6] —, *The Mahler measure of algebraic numbers*: *a survey*, arXiv:math.NT/0701397.

Department of Mathematics
Kansas State University
138 Cardwell Hall
Manhattan, KS 66506, U.S.A.
E-mail: johngarz@math.ksu.edu

Received on 26.3.2008
and in revised form on 28.8.2008 (5674)