ACTA ARITHMETICA
113.4 (2004)

On values of the Mahler measure in a quadratic field (solution of a problem of Dixon and Dubickas)

by

A. Schinzel (Warszawa)

To Robert Tijdeman on the occasion of his 60th birthday

For an algebraic number α, let $M(\alpha)$ be the Mahler measure of α and let $\mathcal{M} = \{M(\alpha) \mid \alpha \in \overline{\mathbb{Q}}\}$. No method is known to decide whether a given algebraic integer β is in $\mathcal{M}$. Partial results have been obtained by Adler and Marcus [1], Boyd [2]–[4], Dubickas [6]–[8] and Dixon and Dubickas [5], but the problem has not been solved even for β of degree two. The following theorem, similar to, but not identical with Theorem 9 of [5], is an easy consequence of [7].

Theorem 1. *A primitive real quadratic integer β is in $\mathcal{M}$ if and only if there exists a rational integer a such that $\beta > a > |\beta'|$ and $a \mid \beta\beta'$, where β' is the conjugate of β. If the condition is satisfied, then $\beta = M(\beta/a)$ and $a = N(a, \beta)$, where N denotes the absolute norm.*

There remain to be considered quadratic integers that are not primitive. The following theorem deals with the simplest class of such numbers.

Theorem 2. *Let K be a quadratic field with discriminant $\Delta > 0$, β, β' be conjugate primitive integers of K and p a prime. If*

$$p\beta \in \mathcal{M}, \tag{1}$$

then either there exists an integer r such that

$$p\beta > r > p|\beta'| \quad \text{and} \quad r \mid \beta\beta', \quad p \nmid r \tag{2}$$

or

$$\beta \in \mathcal{M} \quad \text{and} \quad p \text{ splits in } K. \tag{3}$$

2000 *Mathematics Subject Classification*: Primary 11R04.

Conversely, (2) *implies* (1), *while* (3) *implies* (1) *provided either*

$$\beta > \max\left\{-4\beta', \left(\frac{1+\sqrt{\Delta}}{4}\right)^2\right\} \tag{4}$$

or

$$p > \sqrt{\Delta}. \tag{5}$$

REMARK 1. (2) implies $\beta > p\beta|\beta'|/r \ge p$.

Theorem 2 answers two questions raised in [5].

COROLLARY 1. *For all primes* p *we have* $p\frac{3+\sqrt{5}}{2} \in \mathcal{M}$ *if and only if either* $p = 2$, *or* $p = 5$, *or* $p \equiv \pm 1 \pmod 5$.

COROLLARY 2. *For every real quadratic field* K *there is an irreducible polynomial* $f \in \mathbb{Z}[x]$, *basal in the sense of* [5], *such that* $M(f) \in K$, *but the zeros of* f *do not lie in* K.

COROLLARY 3. *In every real quadratic field* K *there are only finitely many integers* $p\beta$, *where* p *is prime*, *while* β *is primitive and totally positive*, *for which the condition* $p\beta \in \mathcal{M}$ *is not equivalent to the alternative of* (2) *and* (3).

Proof of Theorem 1. Necessity. Let $\beta = M(\alpha)$, let f be the minimal polynomial of α over $\mathbb{Z}$, $a > 0$ its leading coefficient, D its degree, and $\alpha_1, \ldots, \alpha_D$ all its zeros. By Lemma 2 of [7] applied with $d = 2$,

$$\beta\beta' = a^2 \prod_{i=1}^{D} \alpha_i = (-1)^D a f(0). \tag{6}$$

Moreover, by formula (3) of [7], $D = 2s$, where s is the number of $i \le D$ with $|\alpha_i| > 1$. Without loss of generality we may assume that $|\alpha_i| > 1$ precisely for $i \le s$. For some $\eta \in \{1, -1\}$ we have

$$\prod_{i=1}^{s} \alpha_i = \eta\beta/a, \tag{7}$$

hence, by (6),

$$\prod_{i=s+1}^{D} \alpha_i = \eta\beta'/a, \tag{8}$$

which gives

$$\beta > a > |\beta'|. \tag{9}$$

Also, by (6),

$$a \mid \beta\beta'. \tag{10}$$

Sufficiency. Assume the existence of an integer a satisfying (9) and (10) and consider the polynomial

$$g(x) = ax^2 - (\beta + \beta')x + \beta\beta'/a.$$

If g is not primitive, there exists a prime p such that $p \mid a$, $p \mid \beta + \beta'$ and $p \mid \beta\beta'/a$. However, then $p^2 \mid \beta\beta'$ and β/p is a zero of the polynomial $x^2 - \frac{\beta+\beta'}{p}x + \frac{\beta\beta'}{p^2} \in \mathbb{Z}[x]$, contrary to the assumption that β is primitive. Therefore, g is the minimal polynomial of β/a over $\mathbb{Z}$ and $\beta = M(\beta/a)$. Also, $(a) \mid (a^2, a\beta, a\beta', \beta\beta') \mid (a^2, a(\beta + \beta'), \beta\beta') = (a)$, hence

$$(a) = (a^2, a\beta, a\beta', \beta\beta') = (a, \beta)(a, \beta').$$

The proof of Theorem 2 is based on three lemmas.

Lemma 1. *If an integer β of K is the Mahler measure of an algebraic number whose minimal polynomial over $\mathbb{Z}$ has leading coefficient a, then a is the norm of an ideal of K.*

Proof. In the notation of the proof of Theorem 1 (necessity part) we have (7) and (8). Since $\eta\beta'/a$ is the only conjugate of $\eta\beta/a$, every automorphism of the splitting field of f that sends an α_i ($i \le s$) to an α_j ($j > s$) sends the set $\{\alpha_1, \ldots, \alpha_s\}$ onto $\{\alpha_{s+1}, \ldots, \alpha_D\}$ (compare the proof of Lemma 2 in [7]). Hence $\{\alpha_1, \ldots, \alpha_s\}$ and $\{\alpha_{s+1}, \ldots, \alpha_D\}$ are blocks of imprimitivity of the Galois group of f and the coefficients of the polynomials

$$P(x) = \prod_{i=1}^{s}(x - \alpha_i), \qquad P'(x) = \prod_{i=s+1}^{D}(x - \alpha_i)$$

belong to a quadratic field, which clearly is K. Let the contents of P and P' be $\mathfrak{a}^{-1}$ and $\mathfrak{a}'^{-1}$, where $\mathfrak{a}$ and $\mathfrak{a}'$ are conjugate ideals of K. Since f is primitive, we have

$$(1) = \operatorname{cont} f = \operatorname{cont}(aPP') = (a)/\mathfrak{a}\mathfrak{a}'$$

and, since $a > 0$, $a = N\mathfrak{a}$.

Lemma 2. *If the dash denotes conjugation in K, δ, ε are elements of K such that*

$$\delta > 1 > \delta' > -1/2, \tag{11}$$

$$(1, \delta) \mid \varepsilon, \qquad \varepsilon \ne \varepsilon', \tag{12}$$

$$|\varepsilon - \varepsilon'| + 1 < 4\sqrt{\delta}, \tag{13}$$

while $\mathfrak{p}$ is an ideal of K, then there exists $\gamma \in K$ such that

$$(1, \gamma, \delta) = \frac{(1, \delta)}{\mathfrak{p}}, \tag{14}$$

$$|\gamma| < 2\sqrt{\delta}, \qquad |\gamma'| < 1 + \delta'. \tag{15}$$

Proof. Take an integer α of K divisible by $\mathfrak{p}(1,\delta)^{-1}$. Applying Theorem 74 of [9] with

$$\mathfrak{a} = \frac{(\alpha)(1,\delta)}{\mathfrak{p}}, \qquad \mathfrak{b} = \frac{\mathfrak{p}}{(1,\delta)}$$

we find an integer ω of K such that $(\alpha,\omega) = \mathfrak{a}$, hence

$$\left(1, \frac{\omega}{\alpha}\right) = \frac{(1,\delta)}{\mathfrak{p}}. \tag{16}$$

Taking

$$b = \left\lfloor \left(\frac{\omega}{\alpha} - \frac{\omega'}{\alpha'}\right)/(\varepsilon - \varepsilon') + \frac{1}{2} \right\rfloor, \qquad a = \left\lfloor \frac{\omega'}{\alpha'} - b\varepsilon' + \frac{1}{2} \right\rfloor$$

we find

$$\left|\frac{\omega}{\alpha} - \frac{\omega'}{\alpha'} - b(\varepsilon - \varepsilon')\right| \le \frac{|\varepsilon - \varepsilon'|}{2}, \qquad \left|\frac{\omega'}{\alpha'} - a - b\varepsilon'\right| \le \frac{1}{2} < 1 + \delta', \tag{17}$$

hence on addition, by (13),

$$\left|\frac{\omega}{\alpha} - a - b\varepsilon\right| \le \frac{|\varepsilon - \varepsilon'|}{2} + \frac{1}{2} < 2\sqrt{\delta} \tag{18}$$

and for $\gamma = \omega/\alpha - a - b\varepsilon$, (14) follows from (16), while (15) from (17) and (18).

LEMMA 3. *If*, *in the notation of Lemma* 2, $\mathfrak{p}$ *is a prime ideal dividing a rational prime* p, *then the conclusion of the lemma holds*, *provided*

$$p > \frac{N(1,\delta)\sqrt{\Delta}}{\min\{N(1,\delta), 2\sqrt{\delta}(1+\delta')\}}. \tag{19}$$

Proof. Let the ideal $(1,\delta)$ considered as a module over $\mathbb{Z}$ have the basis $[\eta,\zeta]$. The system of inequalities

$$|c| < p, \quad \left|c\,\frac{\omega}{\alpha} - a\eta - b\zeta\right| < 2\sqrt{\delta}, \quad \left|c\,\frac{\omega'}{\alpha'} - a\eta' - b\zeta'\right| < \min\left\{\frac{N(1,\delta)}{2\sqrt{\delta}}, 1+\delta'\right\}$$

has a non-zero integer solution by Minkowski's theorem (Theorem 94 of [9]), since by Theorem 76 of [9], which applies also to fractional ideals (see §31, formula (47))

$$|\eta\zeta' - \eta'\zeta| = N(1,\delta)\sqrt{\Delta} < \min\{N(1,\delta),\, 2\sqrt{\delta}(1+\delta')\}p.$$

If in this solution we had $c = 0$ it would follow that $a\eta + b\zeta \ne 0$ and

$$N(1,\delta) \le |N(a\eta + b\zeta)| < 2\sqrt{\delta}\,\frac{N(1,\delta)}{2\sqrt{\delta}} = N(1,\delta),$$

a contradiction. Therefore $c \ne 0$, $c \not\equiv 0 \pmod{\mathfrak{p}}$ and $\gamma = c\frac{\omega}{\alpha} - a\eta - b\zeta$ has the required properties.

Proof of Theorem 2. Assume first that (1) holds and let f be the minimal polynomial of α over $\mathbb{Z}$, $a > 0$ its leading coefficient, and D its degree. By (6) and (7) with β replaced by $p\beta$, we have

$$p^2\beta\beta' = (-1)^D af(0), \tag{20}$$

$$p\beta > \max\{a, |f(0)|\} \ge \min\{a, |f(0)|\} > p|\beta'|. \tag{21}$$

Let $p^\mu \parallel a$, $p^\nu \parallel \beta\beta'$. If $\mu = 0$ or $\mu = \nu + 2$, then (2) follows with $r = a$ or $r = |f(0)|$, respectively. Therefore, assume

$$1 \le \mu \le \nu + 1. \tag{22}$$

Let $a = p^\mu b$. By (20) and (22),

$$p^{\mu-1} b \mid \beta\beta',$$

while by (21),

$$\beta > p^{\mu-1} b > |\beta'|.$$

By Theorem 1 we have $\beta \in \mathcal{M}$. If $\nu > 0$, then $p \mid \beta\beta'$ and since β is primitive, p splits in K. If $\nu = 0$ we have, by (22), $\mu = 1$ and since, by Lemma 1, a is the norm of an ideal of K, p splits in K. This proves (3).

In the opposite direction, (2) implies $p\beta = M(p\beta/r) \in \mathcal{M}$. Indeed, the minimal polynomial of $p\beta/r$ is $rx^2 - p(\beta+\beta')x + \beta\beta'/r$, where $(r, \beta+\beta', \beta\beta'/r) = 1$, since β is primitive (see the proof of Theorem 1). Assume now that (3) holds. By Theorem 1 we have $\beta = M(\beta/b)$, where

$$b \in \mathbb{N}, \qquad \beta > b > |\beta'|, \qquad b = N(b, \beta). \tag{23}$$

Replacing b by $\beta|\beta'|/b$ if necessary, we may assume

$$b \ge \sqrt{\beta|\beta'|}. \tag{24}$$

First, assume (4). Since β is primitive all prime ideal factors of (b, β) are of degree one and no two of them are conjugate. Hence there exists $c \in \mathbb{Z}$ such that

$$\omega := \frac{\Delta + \sqrt{\Delta}}{2} \equiv -c \pmod{(b, \beta)}. \tag{25}$$

We put $\delta = \beta/b$, $\varepsilon = (c+\omega)/b$. In order to apply Lemma 2 we have to check the assumptions. Now, (11) follows from (23), (24) and $\beta > -4\beta'$, (12) follows from (25), and (13) is equivalent to the inequality

$$\sqrt{\Delta}/\sqrt{b} + \sqrt{b} < 4\sqrt{\beta}.$$

The left-hand side considered as a function of b on the interval $[1, \beta]$ takes its maximum at an end of the interval. We have $\sqrt{\Delta} + 1 < 4\sqrt{\beta}$ by (4) and $\sqrt{\Delta}/\sqrt{\beta} + \sqrt{\beta} < 4\sqrt{\beta}$ since $\beta \ge (1+\sqrt{\Delta})/2$.

The assumptions of Lemma 2 being satisfied there exists $\gamma \in K$ such that

$$(1,\gamma,\delta) = \frac{(b,\beta)}{(b)\mathfrak{p}} = \frac{1}{(b,\beta')\mathfrak{p}}, \quad |\gamma| < 2\sqrt{\delta}, \quad |\gamma'| < 1+\delta'. \tag{26}$$

Let us consider the polynomial

$$P(x) = x^2 + \gamma x + \delta.$$

The discriminant of P, $\gamma^2 - 4\delta$, is negative, hence P is irreducible over the real field K, moreover its zeros are equal to $\sqrt{\delta} > 1$ in absolute value. On the other hand, the zeros of the polynomial

$$P'(x) = x^2 + \gamma' x + \delta'$$

are less than 1 in absolute value. This is clear if $\gamma'^2 - 4\delta' < 0$, since $|\delta'| < 1$, and if $\gamma'^2 - 4\delta' \ge 0$ the inequality

$$\frac{|\gamma'| + \sqrt{\gamma'^2 - 4\delta'}}{2} < 1$$

follows from the condition $|\gamma'| < 1 + \delta'$. Taking for α a zero of P we obtain, by (23) and (26),

$$M(\alpha) = \frac{M(PP')}{N \operatorname{cont} P} = \delta N(b,\beta') N\mathfrak{p} = \frac{\beta}{b}\cdot bp = p\beta.$$

Now, assume (5) and let again $\delta = \beta/b$. In order to apply Lemma 3 we have to check (19).

Consider first the case

$$\beta \notin \left\{\frac{1+\sqrt{4e+1}}{2} : \ e \in \mathbb{N}\right\}. \tag{27}$$

Then

$$\beta - |\beta'| \ge 2, \quad \beta \ge 1 + \sqrt{2} \tag{28}$$

and by (24),

$$R := \frac{2\sqrt{\delta}\,(1+\delta')}{N(1,\delta)} = 2\sqrt{\frac{\beta}{b}}\,(b+\beta') \ge 2\sqrt{\beta}(\sqrt[4]{\beta|\beta'|} + \operatorname{sgn}\beta' \sqrt[4]{|\beta'|^3/\beta}).$$

If $\beta' > 0$ we clearly have $R > 1$, while if $\beta' < 0$ we have, by (26),

$$R = 2\sqrt[4]{\beta|\beta'|}(\sqrt{\beta} - \sqrt{|\beta'|}) \ge 4\sqrt[4]{\beta|\beta'|}/(\sqrt{\beta} + \sqrt{|\beta'|}).$$

If $\sqrt{|\beta'|} \le \frac{1}{2}\sqrt{\beta}$, it follows that

$$R \ge \sqrt[4]{\beta|\beta'|}\sqrt{\beta} > 1,$$

while if $\sqrt{|\beta'|} > \frac{1}{2}\sqrt{\beta}$, it follows that

$$R > \frac{4}{\sqrt{2}}\,\frac{\sqrt{\beta}}{2\sqrt{\beta}} = \sqrt{2} > 1;$$

thus (27) implies

$$\min\{N(1,\delta),\, 2\sqrt{\delta}(1+\delta')\} = N(1,\delta)$$

and (19) follows from (5).

Consider now the case

$$\beta = \frac{1+\sqrt{4e+1}}{2}.$$

By (23), $b^2 + b > e > b^2 - b$, $b \mid e$, which implies $e = b^2$. On the other hand, $4e+1 = f^2\Delta$ for some $f \in \mathbb{N}$. The inequality

$$p > \sqrt{\Delta} = \frac{\sqrt{4b^2+1}}{f}$$

implies by a tedious computation

$$p \geq \frac{2b+1}{f} > \frac{\sqrt{\Delta}}{2\sqrt{\frac{\beta}{b}}\,(b+\beta')} = \frac{N(1,\delta)\sqrt{\Delta}}{\min\{N(1,\delta), 2\sqrt{\delta}\,(1+\delta')\}},$$

hence (19) holds.

The assumptions of Lemma 3 being satisfied there exists $\gamma \in K$ satisfying (26) and arguing as before we obtain

$$p\beta = M(\alpha),$$

where α is a zero of $x^2 + \gamma x + \delta$.

Proof of Corollary 1. For $\beta = (3+\sqrt{5})/2$ the condition (4) is satisfied. Now, (2) is fulfilled by $p = 2$ only, and (3) is fulfilled by $p = 5$ and by $p \equiv \pm 1 \pmod 5$ only.

Proof of Corollary 2. Take a totally positive unit $\varepsilon > 1$ of K and a prime $p > \varepsilon$ that splits in K. Then by Theorem 2, $p\varepsilon \in \mathcal{M}$. Assume that the basal irreducible polynomial f of $p\varepsilon$ has all its zeros in K. Hence

$$f(x) = a\left(x \pm \frac{p\varepsilon}{a}\right)\left(x \pm \frac{p\varepsilon'}{a}\right), \qquad p\varepsilon > a > p\varepsilon',\ a \in \mathbb{N}$$

and the condition $p^2/a \in \mathbb{Z}$ together with $p > \varepsilon$ implies $a = p$. However, for $a = p$, f is not primitive.

EXAMPLE 1. For $K = \mathbb{Q}(\sqrt{2})$ we can take

$$p\varepsilon = 21 + 14\sqrt{2} = M(7x^4 + 2x^3 + 41x^2 + 22x + 7).$$

Proof of Corollary 3. There are only finitely many totally positive integers β of K, which are Perron numbers, but do not satisfy (4).

Remark 2. By a more complicated argument one can show that for β totally positive, (3) implies (1) unless

$$\sqrt[4]{N\beta}+\frac{\sqrt{\Delta}}{\sqrt[4]{N\beta}}\ge 4\sqrt{\beta}\quad\text{and}\quad p<1+\frac{1}{2\sqrt{\beta}}\left(\sqrt[4]{N\beta}+\frac{\sqrt{\Delta}}{\sqrt[4]{N\beta}}\right).$$

Example 2. Theorem 2 does not allow us to decide whether $1+\sqrt{17}\in\mathcal{M}$. This question is open, as is a more general question, whether (3) implies (1).

References

[1] R. L. Adler and B. Marcus, *Topological entropy and equivalence of dynamical systems*, Mem. Amer. Math. Soc. 20 (1971), no. 219.
[2] D. W. Boyd, *Inverse problems for Mahler's measure*, in: Diophantine Analysis, J. Loxton and A. van der Poorten (eds.), London Math. Soc. Lecture Notes 109, Cambridge Univ. Press, 1986, 147–158.
[3] —, *Perron units which are not Mahler measures*, Ergodic Theory Dynam. Systems 6 (1986), 485–488.
[4] —, *Reciprocal algebraic integers whose Mahler measures are non-reciprocal*, Canad. Math. Bull. 30 (1987), 3–8.
[5] J. D. Dixon and A. Dubickas, *The values of Mahler measures*, Mathematika, to appear.
[6] A. Dubickas, *Mahler measures close to an integer*, Canad. Math. Bull. 45 (2002), 196–203.
[7] —, *On numbers which are Mahler measures*, Monatsh. Math. 141 (2004), 119–126.
[8] —, *Mahler measures generate the largest possible groups*, Math. Res. Lett., to appear.
[9] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer, 1981.

Institute of Mathematics
Polish Academy of Sciences
P.O. Box 21
00-956 Warszawa, Poland
E-mail: schinzel@impan.gov.pl

Received on 23.12.2003 (4684)