MATHEMATICS OF COMPUTATION
Volume 67, Number 222, April 1998, Pages 815–820
S 0025-5718(98)00963-6

ORBITS OF ALGEBRAIC NUMBERS WITH LOW HEIGHTS

GREGORY P. DRESDEN

ABSTRACT. We prove that the two smallest values of $h(\alpha)+h(\frac{1}{1-\alpha})+h(1-\frac{1}{\alpha})$ are 0 and $0.4218\ldots$, for α any algebraic integer.

INTRODUCTION

For K an algebraic number field, let K_v be the completion of K at the place v and let $|\ |_v$ be the absolute value associated with this completion K_v (more precise definitions are given below). For $\alpha \in K$, we define the (logarithmic) Weil height, $h(\alpha)$, as follows:

$$h(\alpha) = \sum_v \log\max(|\alpha|_v, 1). \tag{1}$$

In this paper, we will prove

Theorem 1. *Let α be an algebraic number, $\alpha \neq 0, 1$.*

(i) *For α a primitive sixth root of unity,*

$$h(\alpha) + h(\frac{1}{1-\alpha}) + h(1-\frac{1}{\alpha}) = 0.$$

(ii) *Otherwise,*

$$h(\alpha) + h(\frac{1}{1-\alpha}) + h(1-\frac{1}{\alpha}) \geq 0.4218\ldots,$$

with equality for α any root of the polynomial:

$$\begin{aligned} P_1(z) &= z^6 - 3z^5 + 5z^4 - 5z^3 + 5z^2 - 3z + 1 \\ &= (z^2 - z + 1)^3 - (z^2 - z)^2. \end{aligned} \tag{2}$$

The reader will note that this theorem is a specific case of the following general problem. We generalize the Weil height to $\mathbb{P}^1(\overline{\mathbb{Q}})$ in the obvious manner: for $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, we define

$$h(\mathbf{x}) = \sum_v \log\max(|x_1|_v, |x_2|_v).$$

Received by the editor September 30, 1996.
1991 *Mathematics Subject Classification.* Primary 11R04, 11R06; Secondary 12D10.
I am very grateful for the assistance and guidance of my advisor, Dr. Vaaler.

Then, for G a finite subgroup of $PGL_2(\overline{\mathbb{Q}})$, we extend the Weil height to orbits under the action of G, as follows:

$$h_G(\mathbf{x}) = \sum_{g \in G} h(g\mathbf{x}).$$

We now ask about the smallest values of $h_G(\mathbf{x})$ for $\mathbf{x} \in \mathbb{P}^1(\overline{\mathbb{Q}})$. We see that Theorem 1 answers this question for G the cyclic group

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix} \right\}.$$

At the end of this paper we mention further work that is being done on other subgroups G of $PGL_2(\overline{\mathbb{Q}})$.

The reader will also note that this theorem is related to a recent result by Zagier [7] in which he sharpens a result of Zhang [8] concerning a lower bound for $h(\alpha) + h(1-\alpha)$.

Let us now proceed to a proof of Theorem 1.

Definitions

For K_v the completion of the algebraic number field K at the place v, we will need two absolute values, $|\ |_v$ (mentioned above) and $\|\ \|_v$. We define $\|\ \|_v$ to be the absolute value which, when restricted to $\mathbb{Q}$, is the usual Euclidean or p-adic absolute value, and we define $|\ |_v$ as follows

$$|\ |_v = \|\ \|_v^{d_v/d}. \tag{3}$$

It follows that $|\ |_v$ satisfies the product formula on K: $\prod_v |\beta|_v = 1$ for all non-zero $\beta \in K$. (Our normalizations of the absolute values are exactly as in [1] or [5].) Let us also agree that single-bar absolute values, $|\ |$, without any subscript, will always refer to the usual Euclidean absolute value on $\mathbb{C}$. We will use the standard notation $\log^+(z)$ to refer to $\max(0, \log(z))$. Finally, we will need to define the following function for our proof:

(4)

$$E_v(z) = B \log \left\| \frac{(z^2 - z + 1)^3}{(z^2 - z)^2} \right\|_v - \log^+ \|z\|_v - \log^+ \left\| \frac{1}{1-z} \right\|_v - \log^+ \left\| 1 - \frac{1}{z} \right\|_v.$$

The constant B will be specified later; it is a positive real number, between 0 and 1/2. Notice that $E_v(z)$ is invariant under the transform $z \mapsto 1 - \frac{1}{z}$; this means that

$$E_v(z) = E_v(1 - \frac{1}{z}) = E_v(\frac{1}{1-z}). \tag{5}$$

In our proof of Theorem 1, we first establish some local estimates, and we then use these to establish a global result that will prove the theorem.

Local estimates

Lemma 1. *Let z be an algebraic number, $z \neq 0, 1$, or a primitive sixth root of unity.*

(i) $E_v(z) \leq 0$ *for v finite, with equality for z any root of P_1.*
(ii) $E_v(z) \leq -0.4218\ldots$ *for v infinite, with equality for z any root of P_1.*

Proof of Lemma 1. The two parts of this lemma will require entirely different techniques to prove. In (i), for v finite, we will rely on the triangle inequality property of $\| \|_v$, and in (ii), we will differentiate $E_v(z)$ and solve for z. (In both parts, we assume that z is neither 0 nor 1.)

Proof of part (i): v finite. Recall the ultrametric triangle inequality: $\|a+b\|_v \le \max(\|a\|_v, \|b\|_v)$, and if $\|a\|_v \ne \|b\|_v$, then $\|a+b\|_v = \max(\|a\|_v, \|b\|_v)$.

For $\Phi_6(z) = z^2 - z + 1$, we have the following interesting identity:

$$\Phi_6(z)\Phi_6(\frac{1}{1-z})\Phi_6(1-\frac{1}{z}) = \frac{(z^2-z+1)^3}{(z^2-z)^2}. \tag{6}$$

For finite v, then $\|\Phi_6(z)\|_v \le \max(1, \|z^2\|_v)$, and so $\log \|\Phi_6(z)\|_v \le 2\log^+ \|z\|_v$. Thus, if we apply $\| \|_v$ to both sides of (6) and then take the logarithm, we conclude:

$$2\log^+ \|z\|_v + 2\log^+ \left\| \frac{1}{1-z} \right\|_v + 2\log^+ \left\| 1 - \frac{1}{z} \right\|_v \ge \log \left\| \frac{(z^2-z+1)^3}{(z^2-z)^2} \right\|_v . \tag{7}$$

Since the constant B in equation (4) is less than 1/2, this implies that $E_v(z) \le 0$.

It remains to show that equality is achieved for z a root of the polynomial P_1. Let z_1 be such a root. It is easy to show that $1 - \frac{1}{z_1}$ and $\frac{1}{1-z_1}$ are also roots of P_1, and since P_1 is a monic polynomial with integer coefficients and a constant coefficient of 1, then all of its roots are algebraic units. This implies that all three of the $\log^+$ terms in $E_v(z_1)$ are zero; the first term is clearly zero as well, and thus $E_v(z_1) = 0$. □

Proof of part (ii): v infinite. We need to define a new constant, D, in terms of B:

$$D = \frac{1}{2}\left[(1+2B)\log(1+2B) - (6B)\log(6B) - (1-4B)\log(1-4B)\right]. \tag{8}$$

We now describe the method used to determine the value of B. This constant B is chosen so as to maximize the value of D; by differentiating (8) and solving, we find that B should be the single real root of the polynomial $184x^3 + 6x - 1$. That is, $B = 0.1172\ldots$, and subsequently, $D = 0.4218\ldots$. (Notice that $-D$ is the number appearing in the statement of Lemma 1, part (ii).)

Let us now show that $E_v(z) \le -D$ for all $z \in \mathbb{C}$. Recall that for v infinite, then $\| \|_v = | |$, the regular Euclidean absolute value on $\mathbb{C}$.

Since $E_v(z)$ goes to $-\infty$ for z near 0, 1, ∞, and the primitive sixth roots of unity, and since $E_v(z)$ is harmonic off the three curves $|z| = 1$, $\left|1 - \frac{1}{z}\right| = 1$, and $\left|\frac{1}{1-z}\right| = 1$, then (by the maximum principle) $E_v(z)$ achieves its maximum only on these three curves. By the invariance expressed in equation (5), we need only check one of these curves. We consider the straight line $\left|1 - \frac{1}{z}\right| = 1$, which is easily parametrized by $z = 1/2 + iy$. Since $E_v(z) = E_v(\bar{z})$, we need only consider $y \ge 0$. We substitute our parametrization into $E_v(z)$ and derive the following formula:

$$E_v(1/2+iy) = \begin{cases} 3B\log(\frac{3}{4} - y^2) + (\frac{1}{2} - 2B)\log(\frac{1}{4} + y^2) & \text{for } y \in (0, \frac{\sqrt{3}}{2}), \\ 3B\log(y^2 - \frac{3}{4}) - (\frac{1}{2} + 2B)\log(\frac{1}{4} + y^2) & \text{for } y \in (\frac{\sqrt{3}}{2}, \infty). \end{cases} \tag{9}$$

If we let $S = y^2 + 1/4$, then (9) becomes

$$E_v(z) = \begin{cases} 3B\log(1-S) + (\frac{1}{2} - 2B)\log(S) & \text{for } S \in (\frac{1}{4}, 1), \\ 3B\log(S-1) - (\frac{1}{2} + 2B)\log(S) & \text{for } S \in (1, \infty). \end{cases} \tag{10}$$

We now find the maximum of $E_v(z)$ by differentiating (10) with respect to S, setting the result equal to zero, and solving for S. We find that $E_v(z)$ has two maxima, at

$$S_1 = \frac{1-4B}{1+2B}, \qquad \text{and} \qquad S_2 = \frac{1+4B}{1-2B}. \tag{11}$$

Using our value of B we can compute that $S_1 \in (1/4, 1)$ and $S_2 \in (1, \infty)$. That both points are (local) maxima for $E_v(z)$ can easily be verified by the second derivative test.

We substitute S_1 and S_2 into E_v and find the following:

$$\begin{aligned} E_v(S_1) &= \frac{1}{2}\left[(6B)\log(6B) + (1-4B)\log(1-4B) - (1+2B)\log(1+2B)\right] \\ &= -D \end{aligned}$$

and,

$$\begin{aligned} E_v(S_2) &= \frac{1}{2}\left[(6B)\log(6B) - (1+4B)\log(1+4B) + (1-2B)\log(1-2B)\right] \\ &< -D. \end{aligned}$$

Thus, the maximum value for $E_v(z)$ is $-D$. This value is attained at $S_1 = (1-4B)(1+2B)^{-1}$, and since B is a root of $184x^3+6x-1$, we find that S_1 satisfies

$$S_1^3 - 2S_1^2 + 3S_1 - 1 = 0. \tag{12}$$

If we recall that $S_1 = y^2 + 1/4$, and $z = 1/2 + iy$, then we see that S_1 represents the algebraic number z that is a root of the polynomial

$$z^6 - 3z^5 + 5z^4 - 5z^3 + 5z^2 - 3z + 1 = 0.$$

This is exactly the polynomial $P_1(z)$ from equation (2). We have thus shown that $E_v(z) \leq -D$, and $E_v(z) = -D$ for z a root of $P_1(z)$. Of course, P_1 has five other roots; these are also maximums for $E_v(z)$ and reflect the invariance of E_v from equation (5) and the fact that $E_v(z) = E_v(\bar{z})$. □

Global estimates

We will now combine our local estimates to prove Theorem 1.

We first need to introduce a new constant, n_v, defined as $n_v = 0$ for v finite, and $n_v = d_v/d$ for v infinite. We now combine (i) and (ii) of Lemma 1 into a single statement:

$$d_v/d \; E_v(z) \leq -n_v \; D. \tag{13}$$

Proof of Theorem 1. In equation (13), we multiply each logarithm in $E_v(z)$ by the d_v/d term, and use the relation expressed in equation (3), to produce:

$$B \log\left|\frac{(z^2-z+1)^3}{(z^2-z)^2}\right|_v - \log^+|z|_v - \log^+\left|\frac{1}{1-z}\right|_v - \log^+\left|1-\frac{1}{z}\right|_v \leq -n_v \; D. \tag{14}$$

We now make use of the identities

$$\sum_v n_v = 1, \quad \sum_v \log|\beta|_v = 0, \quad \sum_v \log^+|\beta|_v = h(\beta). \tag{15}$$

(These last two formulas hold for all non-zero algebraic numbers, β). Then, for z not zero, 1, or a primitive sixth root of unity, we can sum (14) over all places v and apply (15) to get

$$-h(z) - h(\frac{1}{1-z}) - h(1 - \frac{1}{z}) \leq -D.$$

This implies

$$h(z) + h(\frac{1}{1-z}) + h(1 - \frac{1}{z}) \geq D = 0.4218\ldots, \tag{16}$$

and since equality holds in (13) for z any root of P_1, the same can be said of (16). This establishes part (ii) of Theorem 1; as for part (i), it follows easily from the fact that the minimal polynomial of the sixth roots of unity is $z^2 - z + 1$. □

Applications and generalizations

It is interesting to note that the Weil height h is related to the Mahler measure of a polynomial (as seen in [2] or [3]). Recall that for a polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, with zeroes at $\alpha_1, \ldots, \alpha_n$, we define the Mahler measure $M(f)$ to be

$$M(f) = |a_n| \prod_{i=1}^{n} \max(|\alpha_i|, 1).$$

D. Lehmer [4] asked if there exists a non-trivial lower bound to $M(f)$ for f not cyclotomic (it is conjectured that this lower bound is $1.17628\ldots$). The exact relationship between the Weil height and the Mahler measure is as follows [7]. For α_i a root of the polynomial $f(x)$, then

$$h(\alpha_i) = \frac{1}{\deg f} \log M(f).$$

Given this relation, one can establish an immediate corollary to Theorem 1. Let G be the cyclic group of order three, generated by $z \mapsto 1 - 1/z$. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n such that G is a subgroup of its Galois group. Then,

$$M(f) \geq e^{nk}$$

where k is $\frac{1}{3}(0.4218\ldots)$. One can compare this to the result of Dobrowolski [3], later improved by Rausch [6], that for $g(x) \in \mathbb{Z}[x]$ any non-cyclotomic polynomial of degree n, then

$$M(g) \geq 1 + b\left(\frac{\log\log n}{\log n}\right)^3$$

for b a small positive constant.

Let us now return to the generalization of Theorem 1, mentioned earlier in this paper. It is certainly possible to extend this result to other subgroups of $PGL_2(\overline{\mathbb{Q}})$; consider the subgroup K defined as

$$K = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \right\}.$$

Then, in a proof similar to the proof of Theorem 1, we can show that $h_K(\mathbf{x}) = 0$ for $x = \begin{bmatrix} i \\ 1 \end{bmatrix}$, $\begin{bmatrix} -i \\ 1 \end{bmatrix}$, or any element in the orbit of $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ under K; and that otherwise

$h_K(\mathbf{x}) \geq 0.732858\ldots$, with equality at $\mathbf{x}$ a root of the homogeneous polynomial $x_1^8 + 5x_1^6x_2^2 + 4x_1^4x_2^4 + 5x_1^2x_2^6 + x_2^8, = (x_1^2 + x_2^2)^4 + ((x_1x_2)(x_1 + x_2)(x_1 - x_2))^2$.

An interesting problem would be to specify for which other subgroups G of $PGL_2(\overline{\mathbb{Q}})$ one can find a similar statement.

It would also be interesting to determine if one can find other low values in the spectrum of h_G for a given group G, along with the exact algebraic numbers which achieve those values. For our original group G of order 3, after the first non-zero value of $0.4218\ldots$, the author conjectures that the next two values in the spectrum of h_G are $0.43359381\ldots$ and $0.43798825\ldots$.

I wish to thank Dr. Vaaler for his many helpful comments, and also for suggesting the identity in formula (6).

References

1. E. Bombieri, A van der Poorten, and J. Vaaler, *Effective measures of irrationality for cubic extensions of number fields*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **23** (1996), 211–248. CMP 97:08
2. D. Boyd, *Speculations concerning the range of Mahler's Measure*, Canad. Math. Bull. **24** (4) (1981), 453-469. MR **83h:**12002
3. E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arithmetica **34** (1979), 391-401. MR **80i:**10040
4. D. H. Lehmer, *Factorization of certain cyclotomic funcions*, Ann. of Math. **34** (1933), 461–479.
5. C. Pinner and J. Vaaler, *The number of irreducible factors of a polynomial, I*, Trans. Amer. Math. Soc. **339** (1993), 809–834. MR **93m:**11108
6. U. Rausch, *On a theorem of Dobrowolski about the product of conjugate numbers*, Colloquium Mathematicum **50** (1985), 137–142. MR **87i:**11144
7. D. Zagier, *Algebraic numbers close to both 0 and 1*, Mathematics of Computation **61** (203) (1993), 485–491. MR **94c:**11104
8. S. Zhang, *Positive line bundles on arithmetic surfaces*, Ann. of Math. (2) **136** (3) (1992), 569–587. MR **93j:**14024

Department of Mathematics, Washington & Lee University, Lexington, Virginia 24450
E-mail address: dresdeng@wlu.edu