ORBITS OF ALGEBRAIC NUMBERS WITH LOW HEIGHTS

GREGORY P. DRESDEN

Abstract. We prove that the two smallest values of $h(\alpha) + h\left(\frac{1}{1-\alpha}\right) + h\left(1 - \frac{1}{\alpha}\right)$ are 0 and 0.4218..., for $\alpha$ 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:

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

In this paper, we will prove

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

(i) For $\alpha$ a primitive sixth root of unity,

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

(ii) Otherwise,

$$h(\alpha) + h\left(\frac{1}{1-\alpha}\right) + h\left(1 - \frac{1}{\alpha}\right) \geq 0.4218..., \text{ with equality for } \alpha \text{ any root of the polynomial:}$$

$$P_1(z) = z^6 - 3z^5 + 5z^4 - 5z^3 + 5z^2 - 3z + 1 = (z^2 - z + 1)^3 - (z^2 - z)^2.$$  

(2)

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

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

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.

©1998 American Mathematical Society
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 $PGL_2(\mathbb{Q})$.

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, $| \cdot |_v$ (mentioned above) and $\| \cdot \|_v$. We define $\| \cdot \|_v$ to be the absolute value which, when restricted to $\mathbb{Q}$, is the usual Euclidean or $p$-adic absolute value, and we define $| \cdot |_v$ as follows

$$\| \cdot \|_v = \| d^{1/d} \cdot \|_v.$$  

It follows that $| \cdot |_v$ 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, $| \cdot |$, 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:

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

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

$$E_v(z) = E_v(1 - \frac{1}{z}) = E_v\left( \frac{1}{1 - z} \right).$$

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 $P_1$. 

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
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: \( \|a + b\|_v \leq \max(\|a\|_v, \|b\|_v) \), and if \( \|a\|_v \neq \|b\|_v \), then \( \|a + b\|_v = \max(\|a\|_v, \|b\|_v) \).

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

\[
\Phi_6(z)\Phi_6(\frac{1}{1 - z})\Phi_6(1 - \frac{1}{z}) = \frac{(z^2 - z + 1)^3}{(z^2 - z)^2}.
\]

For finite \( v \), then \( \|\Phi_6(z)\|_v \leq \max(1, \|z^2\|_v) \), and so \( \log \|\Phi_6(z)\|_v \leq 2 \log^+ \|z\|_v \).

Thus, if we apply \( \| \|_v \) to both sides of (6) and then take the logarithm, we conclude:

\[
2 \log^+ \|z\|_v + 2 \log^+ \left\| \frac{1}{1 - z} \right\|_v + 2 \log^+ \left\| 1 - \frac{1}{z} \right\|_v \geq \log \left( \frac{(z^2 - z + 1)^3}{(z^2 - z)^2} \right)_v.
\]

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

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 \( B \):

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

We now describe the method used to determine the value of \( D \). This constant \( B \) is chosen so as to maximize the value of \( D \) by differentiating (8) and solving, we find that \( B = \frac{1}{3} \), 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 \( E_v(z) \leq -D \) 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, \( \infty \), and the primitive sixth roots of unity, and since \( E_v(z) \) is harmonic off the three curves \( |z| = 1 \), \( |1 - \frac{1}{z}| = 1 \), 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 \( |1 - \frac{1}{z}| = 1 \), which is easily parametrized by \( z = 1/2 + iy \). Since \( E_v(z) = E_v(z) \), we need only consider \( y \geq 0 \). We substitute our parametrization into \( E_v(z) \) and derive the following formula:

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

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

\[
E_v(z) = \begin{cases} 
3B \log(1 - S) + (\frac{1}{2} - 2B) \log(S) & \text{for } S \in (\frac{1}{4}, 1), \\
3B \log(S - 1) - (\frac{1}{2} + 2B) \log(S) & \text{for } S \in (1, \infty).
\end{cases}
\]
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
\begin{equation}
S_1 = \frac{1 - 4B}{1 + 2B}, \quad \text{and} \quad S_2 = \frac{1 + 4B}{1 - 2B}.
\end{equation}

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{align*}
E_v(S_1) &= \frac{1}{2} \left[ (6B) \log(6B) + (1 - 4B) \log(1 - 4B) - (1 + 2B) \log(1 + 2B) \right] \\
&= -D
\end{align*}
and,
\begin{align*}
E_v(S_2) &= \frac{1}{2} \left[ (6B) \log(6B) - (1 + 4B) \log(1 + 4B) + (1 - 2B) \log(1 - 2B) \right] \\
&< -D.
\end{align*}

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
\begin{equation}
S_1^3 - 2S_1^2 + 3S_1 - 1 = 0.
\end{equation}
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
\begin{align*}
z^6 - 3z^5 + 5z^4 - 5z^3 + 5z^2 - 3z + 1 &= 0.
\end{align*}
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 maxima 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:
\begin{equation}
d_v/d \ E_v(z) \leq -n_v \ D.
\end{equation}

**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:
\begin{align*}
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( \frac{1 - 1}{z} \right)_v &\leq -n_v \ D.
\end{align*}

We now make use of the identities
\begin{equation}
\sum_v n_v = 1, \quad \sum_v \log |\beta|_v = 0, \quad \sum_v \log^+ |\beta|_v = h(\beta).
\end{equation}
(These last two formulas hold for all non-zero algebraic numbers, \( \beta \)). 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\left(\frac{1}{1 - z}\right) - h\left(1 - \frac{1}{z}\right) \leq -D.

This implies

\[h(z) + h\left(\frac{1}{1 - z}\right) + h\left(1 - \frac{1}{z}\right) \geq D = 0.4218\ldots,

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 \( f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \), 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 \( \alpha_i \) 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 \( z \mapsto 1 - \frac{1}{z} \). 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{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \right\}.

Then, in a proof similar to the proof of Theorem 1, we can show that \( h_K(x) = 0 \) for \( x = \begin{pmatrix} i \\ 1 \end{pmatrix}, \begin{pmatrix} -i \\ 1 \end{pmatrix} \), or any element in the orbit of \( \begin{pmatrix} 0 \\ 1 \end{pmatrix} \) under \( K \); and that otherwise
$h_K(x) \geq 0.732858 \ldots$, with equality at $x$ a root of the homogeneous polynomial
\[
x^8 + 5x^6 + 4x^4 + 5x^2 + x = (x^2 + x)^4 + ((x_1x_2)(x_1 + x_2)(x_1 - x_2))^2.
\]

An interesting problem would be to specify for which other subgroups $G$ of $PGL_2(\mathbb{Q})$ 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

7. D. Zagier, Algebraic numbers close to both 0 and 1, Mathematics of Computation 61 (203) (1993), 485–491. MR 94c:11104

DEPARTMENT OF MATHEMATICS, WASHINGTON & LEE UNIVERSITY, LEXINGTON, VIRGINIA 24450
E-mail address: dresdeng@wlu.edu