MATHEMATICS Proceedings A 91 (1), March 28, 1988

On the denominators of equivalent algebraic numbers

by K. Győry[1] and T.N. Shorey[2]

[1] *Kossuth Lajos University, Mathematical Institute, H-4010 Debrecen 10, Hungary*
[2] *School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Bombay 400005, India*

Communicated by Prof. R. Tijdeman at the meeting of September 28, 1987

1. INTRODUCTION

For an algebraic number α, we denote by $D^*(\alpha)$ the discriminant of the minimal defining polynomial of α over $\mathbf{Z}$ and we write d_α for the *denominator* of α. Thus, d_α is the least positive integer such that $d_\alpha \alpha$ is an algebraic integer. Two algebraic numbers α and β are called *equivalent* if

$$(1) \qquad \beta = \frac{a_1\alpha + a_2}{a_3\alpha + a_4}, \quad a_1, a_2, a_3, a_4 \in \mathbf{Z}, \ a_1a_4 - a_2a_3 = \pm 1$$

and *$\mathbf{Z}$-equivalent* if $\beta - \alpha \in \mathbf{Z}$ or $\beta + \alpha \in \mathbf{Z}$. We observe that $\mathbf{Z}$-equivalent numbers are equivalent and have the same denominator, but the converse does not hold in general. Further, we see from (1) that if α and β are equivalent, then

$$\deg(\beta) = \deg(\alpha), D^*(\beta) = D^*(\alpha), \mathbf{Q}(\beta) = \mathbf{Q}(\alpha).$$

The purpose of this paper is to study the denominators of equivalent algebraic numbers. Let $\mathscr{C}$ be an equivalence class of algebraic numbers of degree $n \geq 3$ and we fix a representative α of $\mathscr{C}$. In §2, we shall give effective and quantitative lower bounds, in terms of max $(|a_3|, |a_4|)$, for the denominator, the greatest prime factor and the greatest square free factor of the denominator of an arbitrary element β of $\mathscr{C}$ (cf. Theorems 1,3). Further, we shall derive

[1] Research supported in part by Hungarian National Foundation for Scientific Research grant 273.
[2] Research supported in part by NSF Grant # DMS-8610730(1) and by the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

effictive and quantitative lower bounds for d_β and for the greatest prime factor of d_β in terms of the height of an appropriate element of $\mathscr{C}$ which is $\mathbf{Z}$-equivalent to β (cf. Theorems 2,4). These bounds imply, in an effective way, that $\mathscr{C}$ contains only finitely many $\mathbf{Z}$-equivalence classes of algebraic numbers whose denominators are divisible only by finitely many fixed primes (cf. Corollary 2). We shall also obtain explicit upper bounds for the number of such $\mathbf{Z}$-equivalence classes of $\mathscr{C}$ (cf. Theorems 5,6). Further, our results will provide some information on the arithmetical structure of denominators of elements of $\mathscr{C}$ (cf. Corollary 1 and (15)). We shall point out an ineffective improvement of Corollary 2. Theorem 4, together with some results of Birch and Merriman [1] and Győry [5], implies that, for given $D^* \neq 0$, there are only finitely many $\mathbf{Z}$-equivalent classes of algebraic numbers β with $D^*(\beta) = D^*$ and with denominators divisible only by finitely many fixed primes. We note that $D^*(\beta)$ does not coincide, in general, (cf. (17)) with the discriminant $D(\beta)$ of β with respect to $\mathbf{Q}(\beta)/\mathbf{Q}$. This is the reason that our results cannot be deduced from effective finiteness theorems (cf. [5], [6], [8], [9]) concerning algebraic numbers of given discriminant. Next, we shall apply our results to derive lower bounds for the denominators of the complete quotients in the continued fraction expansions of algebraic numbers (cf. (19), (20), (21)).

Our results will be proved in §3. First, we shall reduce the investigation of denominators of elements of $\mathscr{C}$ to the study of Thue equations and Thue-Mahler equations. Then we shall apply certain finiteness theorems on Thue-equations and Thue-Mahler equations to establish our results. We shall also need an effective finiteness result of [6] on algebraic numbers of given degree, given discriminant and given denominator.

2. RESULTS

We shall keep the notation of §1. Further, K will denote the algebraic number field generated by the elements of the equivalence class $\mathscr{C}$. Denote by L the normal closure of $K/\mathbf{Q}$ and by l, R_L and h_L the degree, regulator and class number of L, respectively. Clearly $l \leq n!$. For an algebraic number β, let $H(\beta)$ denote the height of β, i.e. the maximum absolute value of the coefficients of the minimal defining polynomial of β over $\mathbf{Z}$. We recall that if β is of degree $n > 1$ then the discriminant of β with respect to $\mathbf{Q}(\beta)/\mathbf{Q}$ is defined by

$$D(\beta) = \prod_{1 \leq i < j \leq n} (\beta_i - \beta_j)^2$$

where $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ are the conjugates of β. Throughout the paper, $c_1, c_2, \ldots$ (resp. $C_1, C_2, \ldots$) denote positive numbers which are monotonically decreasing (resp. increasing) in each of their parameters.

THEOREM 1. *Let $\beta \in \mathscr{C}$ be given by* (1). *Then*

$$c_1(\max(|a_3|, |a_4|))^{c_2} \leq d_\beta \leq (n+1)H^2(\alpha)(\max(|a_3|, |a_4|))^n \tag{2}$$

where $c_1 > 0$ is an effectively computable number depending only on $H(\alpha)$, l, R_L and $c_2 > 0$ is an effectively computable number depending only on l, R_L.

The upper bound for d_β is easy to deduce. The proof of the lower bound for d_β is based on an effective result of Györy and Papp [10] on Thue equations which was proved by Baker's method concerning linear forms in logarithms of algebraic numbers. By using Roth's theorem on the approximations of algebraic numbers by rationals, the lower estimate can be improved (cf. §3) to

$$c_3(\max(|a_3|, |a_4|))^{1-2/n-\varepsilon} \le d_\beta \tag{3}$$

where $\varepsilon > 0$ and $c_3 = c_3(\varepsilon, n, H(\alpha)) > 0$. The constant c_3 is, however, not effective.

For every $\beta \in \mathscr{C}$, $D^*(\beta)$ has the same value which will be denoted by $D_{\mathscr{C}}$. Further, we put

$$d_{\mathscr{C}} = \min_{\beta \in \mathscr{C}} d_\beta .$$

Observe that $d_{\mathscr{C}} \ge 1$ and $d_{\mathscr{C}} = 1$ if and only if $\mathscr{C}$ contains algebraic integers. It is easy to see (cf. (22)) that

$$d_\beta \le H(\beta)$$

and that $H(\beta)$ can be arbitrarily large with respect to d_β. On the other hand, by a result of Györy ([6], Theorem 3; cf. Lemma 4 in the present paper), every $\beta \in \mathscr{C}$ is $\mathbf{Z}$-equivalent to a $\beta' \in \mathscr{C}$ such that

$$d_\beta > c_4(\log H)^{c_5}, \quad H = \max(H(\beta'), 4) \tag{4}$$

where $c_4 = c_4(n, |D_{\mathscr{C}}|) > 0$ and $c_5 = c_5(n) > 0$ are effectively computable numbers. Estimate (4) can be considerably improved in terms of H by using the lower estimate in (2) together with the above mentioned result of Györy [6].

THEOREM 2. *Every $\beta \in \mathscr{C}$ is $\mathbf{Z}$-equivalent to a $\beta' \in \mathscr{C}$ for which*

$$d_\beta > c_6(H(\beta'))^{c_7} \tag{5}$$

where $c_6 = c_6(|D_{\mathscr{C}}|, d_{\mathscr{C}}) > 0$ and $c_7 = c_7(|D_{\mathscr{C}}|) > 0$ are effectively computable numbers.

We note that (3) leads to

$$d_\beta > c_8(H(\beta'))^{1/n - 2/n^2 - \varepsilon} \tag{6}$$

instead of (5), where $c_8 = c_8(|D_{\mathscr{C}}|, d_{\mathscr{C}}, \varepsilon) > 0$ is, however, ineffective. This lower bound is not far from being best possible, as is shown by the example $\beta = \sqrt[n]{2}/d$, $d \in \mathbf{N}$ odd, where $d_\beta \le (H(\beta'))^{1/n}$ for every β' which is $\mathbf{Z}$-equivalent to β.

Unlike (4), the constants c_6 and c_8 in (5) and (6) depend also on $d_{\mathscr{C}}$. It follows from a theorem of Birch and Merriman [1] that, for given $n \ge 3$ and $D^* \in \mathbf{Z} \setminus \{0\}$, there are only finitely many equivalence classes $\mathscr{C}$ of algebraic numbers of degree n with $D_{\mathscr{C}} = D^*$. This implies that there is a $C_1(n, |D_{\mathscr{C}}|) > 0$ such that

$$d_{\mathscr{C}} < C_1(n, |D_{\mathscr{C}}|)$$

which, together with

$$(7) \qquad n \leq 3 + \frac{2}{\log 3} \log |D_{\mathscr{C}}|$$

(Györy ([5], Theorem 1)), implies that

$$(8) \qquad d_{\mathscr{C}} < C_2(|D_{\mathscr{C}}|).$$

The results in [1] are, however, ineffective and therefore, C_2 is ineffective. Thus, if we do not care for the effective nature of c_6, we see from (8) that Theorem 2 is valid with c_6 depending only on $|D_{\mathscr{C}}|$. We conjecture that $d_{\mathscr{C}}$ can be estimated from above by an effectively computable number depending only on $|D_{\mathscr{C}}|$. Further, together with (5), this conjecture would yield that every equivalence class $\mathscr{C}$ with given $D_{\mathscr{C}}$ would contain a representative with height bounded by an effectively computable number depending only on $|D_{\mathscr{C}}|$.

We denote by $P(d)$, $Q(d)$ and $\omega(d)$, respectively, the greatest prime factor, the greatest square free factor and the number of distinct prime factors of a non-zero rational integer d with $|d|>1$ and we put $P(\pm 1)=Q(\pm 1)=1$ and $\omega(\pm 1)=0$. Clearly $Q(d) \geq P(d)$. By applying a result of Györy [7] on Thue-Mahler equations, we shall prove the following result.

THEOREM 3. *Let $\beta \in \mathscr{C}$ with $d_\beta > 1$ be given by* (1). *Then*

$$(9) \qquad \log P(d_\beta) + \omega(d_\beta)\log(\omega(d_\beta)+1) > c_9 \log\log \max(|a_3|, |a_4|, 4),$$

$$(10) \qquad P(d_\beta) > c_{10} \log\log \max(|a_3|, |a_4|, 4)$$

and

$$(11) \qquad Q(d_\beta) > (\log \max(|a_3|, |a_4|, 4))^{c_{11}}$$

where c_9, c_{10} and c_{11} are effectively computable positive numbers depending only on $H(\alpha)$, l, R_L and h_L.

By (1) and (10), we observe that

$$(12) \qquad P(d_{1/\beta}) > c_{10} \log\log \max(|a_1|, |a_2|, 4).$$

Similarly, if $d_{1/\beta} > 1$, (1) and (11) give a lower bound for $Q(d_{1/\beta})$. We remark that $H(\beta)$ can be arbitrarily large compared to $P(d_\beta)$ and $Q(d_\beta)$. On the other hand, we derive from Theorem 3 and Györy [6], Theorem 3 the following result.

THEOREM 4. *Every $\beta \in \mathscr{C}$ is $\mathbb{Z}$-equivalent to a $\beta' \in \mathscr{C}$ such that*

$$P(d_\beta) > c_{12} \log\log H, \quad H = \max(H(\beta'), 4),$$

where $c_{12} > 0$ is an effectively computable number depending only on $|D_{\mathscr{C}}|$ and $d_{\mathscr{C}}$.

By (10), (12) and a result of Györy [6], we can deduce in a similar way that

$$(13) \qquad \max(P(d_\beta),\ P(d_{1/\beta})) > c_{13} \log\log H, \quad H = \max(H(\beta), 4),$$

where $c_{13}>0$ is an effectively computable number depending only on $|D_{\mathscr{C}}|$ and $d_{\mathscr{C}}$.

We observe that β' of Theorem 4 satisfies $d_{\beta'}=d_\beta$ and $d_{\beta'}\leq H(\beta')$. Hence, Theorem 4 yields the following interesting arithmetical property of denominators of elements of $\mathscr{C}$.

CORROLARY 1. *For every $\beta\in\mathscr{C}$, we have*

(14) $\quad P(d_\beta)>c_{12}\log\log d,\ d=\max(d_\beta,4).$

We can also deduce from (11) that if $d_\beta>1$ then

(15) $\quad Q(d_\beta)>(\log d)^{c_{14}},\ d=\max(d_\beta,4)$

with an effectively computable number $c_{14}>0$ depending only on $|D_{\mathscr{C}}|$ and $d_{\mathscr{C}}$. In view of (8), c_{12} and c_{14} can be replaced by ineffective constants depending only on $|D_{\mathscr{C}}|$.

Now, we turn to another consequence of Theorem 4. Let $\{p_1,\dots,p_s\}$ be a finite set of primes and we denote by S the set of all positive integers that are not divisible by primes different from $p_1,\dots,p_s$. We shall say that $\mathscr{C}$ is *effectively given* if a representative of $\mathscr{C}$ is given effectively in the usual sense (cf. [17], p. 243). If this is the case, then $D_{\mathscr{C}}$ is also effectively given.

COROLLARY 2. *There are only finitely many pairwise* **Z***-inequivalent $\beta\in\mathscr{C}$ with $d_\beta\in S$ and, if $\mathscr{C}$ is effectively given, a full set of representatives of such elements β can be effectively determined.*

It follows from (13) in a similar way that there are only finitely many $\beta\in\mathscr{C}$ with $d_\beta\in S$, $d_{1/\beta}\in S$ and, if $\mathscr{C}$ is effectively given, all these β's can be effectively found.

We remark that Theorem 4 and (8) imply that, for given $D^*\neq 0$, there are only finitely many pairwise **Z**-inequivalent algebraic numbers β with $D^*(\beta)=D^*$ and $d_\beta\in S$ (independently of the equivalence class $\mathscr{C}$). This finiteness assertion is, however, not effective. In the special case when both $D^*(\beta)$ and d_β are given, an effective version of this statement follows from (4) and (7).

Now, we shall derive an explicit upper bound for the maximal number of pairwise **Z**-inequivalent β considered in Corollary 2. Put

$$\omega_{\mathscr{C}}=\min_{\beta\in\mathscr{C}}\omega(d_\beta).$$

If $\mathscr{C}$ contains algebraic integers, then $\omega_{\mathscr{C}}=0$. By using a result of Evertse [2] on the number of solutions of Thue-Mahler equations, we shall establish the following result.

THEOREM 5. *There are at most*

(16) $\quad 2\times 7^{n^3(2\omega_{\mathscr{C}}+2s+3)}$

pairwise **Z***-inequivalent $\beta\in\mathscr{C}$ with $d_\beta\in S$.*

By means of a result of Evertse and Győry [3] on Thue-Mahler equations, we can also derive the bound

$$4 \times 7^{l(2\omega_{\mathscr{C}} + 2s + 3)}$$

instead of (16). We recall that here $n \leq l \leq n!$. One can see in a similar way that the number of $\beta \in \mathscr{C}$ with $d_\beta \in S$, $d_{1/\beta} \in S$ is at most

$$2 \times 7^{2n^3(2\omega_{\mathscr{C}} + 2s + 3)}.$$

Under certain restriction made on $D_{\mathscr{C}}$, we can considerably improve the bound (16) by using a recent result of Evertse and Győry [4] on Thue-Mahler equations. For a non-zero rational integer a, we denote by $[a]_S$ the S-free part of a, i.e. the largest positive divisor of a which is relatively prime to $p_1, \dots, p_{s-1}$ and p_s.

THEOREM 6. *There is a number $C_3 > 0$, depending only on K and S, such that if $[D_{\mathscr{C}}]_S > C_3$ then the number of pairwise $\mathbf{Z}$-inequivalent $\beta \in \mathscr{C}$ with $d_\beta \in S$ is at most* 2.

In particular, this implies that if $|D_{\mathscr{C}}|$ is large enough then $\mathscr{C}$ contains at most two $\mathbf{Z}$-inequivalent algebraic integers.

Next, we point out an interesting reformulation of Corollary 2, Theorem 5 and their consequences mentioned above. Let $\mathbf{Z}_S$ denote the ring of rational numbers whose denominators are contained in S, and let $\mathscr{Q}_S$ denote the set of all algebraic numbers β with $d_\beta \in S$. Then $\mathscr{Q}_S$ is an extension ring of $\mathbf{Z}_S$ and $\mathscr{Q}_S$ consists precisely of those algebraic numbers which are integral over $\mathbf{Z}_S$. Further, $d_\beta \in S$ and $d_{1/\beta} \in S$ if and only if $\beta \in \mathscr{Q}_S^*$ where $\mathscr{Q}_S^*$ is the unit group of $\mathscr{Q}_S$. In our statements above, the condition $\beta \in \mathscr{C}$ with $d_\beta \in S$ is equivalent to $\beta \in \mathscr{Q}_S \cap \mathscr{C}$, and $\beta \in \mathscr{C}$ with $d_\beta \in S$, $d_{1/\beta} \in S$ to $\beta \in \mathscr{Q}_S^* \cap \mathscr{C}$. Further, it follows that there are only finitely many pairwise $\mathbf{Z}$-inequivalent $\beta \in \mathscr{Q}_S$ with given non-zero $D^*(\beta)$. This assertion should be compared with an effective result of Győry ([9], Theorem 16) which asserts that up to the obvious translation by elements of $\mathbf{Z}_S$, there are only finitely many $\beta \in \mathscr{Q}_S$ with given degree and with given non-zero discriminant $D(\beta)$ (and a full set of representatives of such β can be effectively determined). These two last finiteness assertions are not contained in each other. The reason is that $D^*(\beta)$ and $D(\beta)$ are related by

$$(17) \qquad D^*(\beta) = b_0^{2(n-1)} D(\beta)$$

where $n = \deg(\beta)$, b_0 is the leading coefficient of the minimal defining polynomial of β over $\mathbf{Z}$ and $b_0 \mid d_\beta^n$ (cf. (22)). Consequently, the heights of $D^*(\beta)$ and $D(\beta)$ cannot be estimated from above by the other and $D^*(\beta)$ is not invariant under translation by elements of $\mathbf{Z}_S$.

Finally, we apply our results to denominators of complete quotients of the continued fraction expansion of an algebraic number. For an account on continued fractions, one may refer to Schmidt [13], Chapter 1. Let

$$\alpha = [a_0, a_1, \dots]$$

be the simple continued fraction expansion of a real algebraic number α of degree ≥ 3. We put $p_{-1}=1$ and $q_{-1}=0$. For $m\geq 0$, we write

$$\frac{p_m}{q_m}=[a_0, a_1, \ldots, a_m]$$

and

$$\alpha_m=[a_m, a_{m+1}, \ldots]$$

for the m-th convergent and the m-th complete quotient, respectively, in the continued fraction expansion of α. Observe that $\alpha=\alpha_0$. For $m\geq 0$, we have

$$\alpha=\frac{p_m\alpha_{m+1}+p_{m-1}}{q_m\alpha_{m+1}+q_{m-1}}$$

and

$$\alpha_{m+1}=\frac{q_{m-1}\alpha-p_{m-1}}{-q_m\alpha+p_m}. \tag{18}$$

Now, since

$$q_m p_{m-1}-p_m q_{m-1}=(-1)^m,$$

we see that the complete quotients of α are elements of $\mathscr{C}$, the equivalence class represented by α. For $m>1$, we derive from (2), (10), (11) and (18) that

$$d_{\alpha_m}\geq c_{15}C_4^m, \tag{19}$$

$$Q(d_{\alpha_m})\geq m^{c_{16}} \tag{20}$$

and

$$P(d_{\alpha_m})\geq c_{17}\log m \tag{21}$$

where c_{15}, c_{16}, c_{17} and $C_4>1$ are effectively computable positive numbers depending only on α.

3. PROOFS

Let α be an algebraic number of degree $n\geq 3$ with minimal defining polynomial $f(x)$ over $\mathbf{Z}$ and let a_0 be the leading coefficient of $f(x)$. It is important to note that

$$d_\alpha \mid a_0, \; a_0 \mid d_\alpha^n. \tag{22}$$

The first relation follows at once by observing that if $a_0=d_\alpha u+v$ with $u, v\in\mathbf{Z}$, $0\leq v<d_\alpha$, then $a_0\alpha$, $d_\alpha\alpha$ and hence $v\alpha$ are algebraic integers, i.e. $v=0$. The second relation follows from the fact that the polynomial $(d_\alpha^n/a_0)\,f(x)$ which has coefficients in $\mathbf{Z}$ has α as a root and therefore, it is divisible by $f(x)$ in $\mathbf{Z}[x]$.

Let $F(x, y)=y^n f(x/y)$. Then F is an irreducible binary form in $\mathbf{Z}[x, y]$ with degree n. Let $\mathscr{C}$ be the equivalence class of α. The following lemma makes it possible to reduce the investigation of denominators of elements of $\mathscr{C}$ to Thue equations and Thue-Mahler equations.

LEMMA 1. *Let $\beta \in \mathscr{C}$ be given by* (1). *Then*

(23) $$d_\beta \mid d_\alpha F(a_4, -a_3), \quad F(a_4, -a_3) \mid (d_\alpha d_\beta)^n.$$

PROOF. By (1), we obtain

(24) $$d_\alpha(a_3\alpha + a_4)\beta = (a_1(d_\alpha \alpha) + d_\alpha a_2).$$

It follows from a well-known lemma (see e.g. [17], Lemma 4.1.1.) that $F(a_4, -a_3)/(a_3\alpha + a_4)$ is an algebraic integer. Multiplying both sides of (24) by this integer, we deduce that $d_\alpha F(a_4, -a_3)\beta$ is an algebraic integer, i.e. $d_\beta \mid d_\alpha F(a_4, -a_3)$.

To prove the second assertion in (23), we observe that

$$\alpha = \frac{-a_4\beta + a_2}{a_3\beta - a_1}$$

whence, by (1),

$$(a_3\alpha + a_4)(a_3\beta - a_1) = 1 \text{ or } -1$$

i.e.

$$(a_3\alpha + a_4)(a_3(d_\beta\beta) - d_\beta a_1) = d_\beta \text{ or } -d_\beta.$$

By taking norms with respect to $\mathbf{Q}(\alpha)/\mathbf{Q}$ and multiplying by a_0, we see that $F(a_4, -a_3)$ divides $a_0 d_\beta^n$ in $\mathbf{Z}$. This, together with (22), proves the lemma. □

Let A be a non-zero rational integer. Denote by $H(F)$ the height of F, i.e. the maximum absolute value of the coefficients of F. We note that $H(F) = H(\alpha)$ and, by (22), $d_\alpha \le H(F)$. Let L, l, R_L and h_L be as in §2. Then L is the splitting field of F over $\mathbf{Q}$. Theorem 1 follows from Lemma 1 and the following lemma which depends on the theory of linear forms in logarithms of algebraic numbers.

LEMMA 2. *All solutions of the Thue equation*

$$F(x, y) = A \text{ in } x,\ y \in \mathbf{Z}$$

satisfy

$$\max(|x|, |y|) < C_5(|A| H(F))^{C_6}$$

where $C_5 > 0$ and $C_6 > 0$ are effectively computable numbers depending only on l and R_L.

This lemma is an immediate consequence of Corollary 1.1 of Győry and Papp [10]. Explicit values for C_5 and C_6 can be deduced from the result mentioned in [10].

PROOF *of Theorem* 1. For every $x, y \in \mathbf{Z}$, we have

$$|F(x, y)| \le (n+1)H(F)\ (\max(|x|, |y|))^n$$

which, together with (23), implies the upper bound for d_β in (2). The lower bound in (2) follows from Lemmas 1 and 2. □

The lower estimate (3) for d_β follows at once from Lemma 1 and the following lemma which is an immediate consequence of Roth's theorem on the approximations of algebraic numbers by rationals (cf. e.g. [12], p. III. 20, Corollary 1).

LEMMA 3. *For every $\varepsilon>0$, there exists a non-effective number $c_{18}=c_{18}(n, H(F), \varepsilon)>0$ such that*

$$|F(x, y)| \geq c_{18}(\max(|x|, |y|))^{n-2-\varepsilon}$$

for every $x, y \in \mathbf{Z}$ with $\max(|x|, |y|)>0$.

In the proof of Theorem 2, we shall need the following two lemmas.

LEMMA 4. *Let α be an algebraic number of degree $n \geq 3$ with discriminant satisfying $|D(\alpha)| \leq D$. Then α is $\mathbf{Z}$-equivalent to an α' for which*

$$H(\alpha')<\exp(C_7(d_\alpha^{n^3} D)^{5n^2})$$

where $C_7=C_7(n)>0$ is an effectively computable number.

This is Theorem 3 of Győry [6]. Its proof involves, among other things, Baker's method.

Denote by D_L the discriminant of L. We have

LEMMA 5(a). *There exists an effectively computable number $C_8=C_8(l)>0$ such that*

$$h_L R_L<C_8|D_L|^{1/2}(\log|D_L|)^{l-1}.$$

(b) $\qquad R_L \geq 0.056.$

The first inequality is due to Siegel [15] and the second inequality was proved by Zimmert [18].

We shall denote by $\overline{|\gamma|}$ the maximum absolute value of the conjugates of an algebraic number γ.

PROOF *of Theorem* 2. Let $\alpha \in \mathscr{C}$ with $d_\alpha=d_{\mathscr{C}}$. Then, by (17), $|D(\alpha)| \leq |D_{\mathscr{C}}|$ and, by Lemma 4 and (7), α can be chosen in $\mathscr{C}$ to satisfy

$$H(\alpha)<C_9(|D_{\mathscr{C}}|, d_{\mathscr{C}}) \tag{25}$$

with an effectively computable number $C_9(|D_{\mathscr{C}}|, d_{\mathscr{C}})$. Fix now such an α. Let β be an arbitrary element of $\mathscr{C}$ and consider the representation of the form (1) of β. Then, we have

$$a_1a_4-a_2a_3=1 \text{ or } -1.$$

There are rational integers a_1', a_2' such that

$$a_1'a_4-a_2'a_3=1 \text{ or } -1 \text{ as above,}$$

$$\max(|a_1'|, |a_2'|) \leq 2\max(|a_3|, |a_4|) \tag{26}$$

and

$$a_1=a_1'+a_3t,\ a_2=a_2'+a_4t,\ t \in \mathbf{Z}.$$

Put

$$(27) \qquad \beta' = \frac{a_1'\alpha + a_2'}{a_3\alpha + a_4}.$$

Then $\beta - \beta' = t$, that is β' is $\mathbf{Z}$-equivalent to β.

Denote by a_0 the leading coefficient of the minimal defining polynomial of α over $\mathbf{Z}$. Using (25), (26), (27), (7) and the properties of heights and sizes of algebraic numbers (see e.g. [8], §1.1), we have

$$(28) \qquad \begin{aligned} H(\beta') &\leq (\overline{|a_1'a_0\alpha + a_0a_2'|} + \overline{|a_3a_0\alpha + a_0a_4|})^n \\ &\leq (2H(\alpha)\max(|a_1'|, |a_2'|, |a_3|, |a_4|))^n \\ &\leq C_{10}(\max(|a_3|, |a_4|))^n \end{aligned}$$

where $C_{10} > 0$ is an effectively computable number depending only on $|D_{\mathscr{C}}|$ and $d_{\mathscr{C}}$. Now, we combine (2), (7), (28) and $l \leq n!$ to conclude that

$$d_\beta > c_{19}(H(\beta'))^{c_{20}}$$

where $c_{19} > 0$ and $c_{20} > 0$ are effectively computable numbers such that c_{19} depends only on $|D_{\mathscr{C}}|$, $d_{\mathscr{C}}$, R_L and c_{20} depends only on $|D_{\mathscr{C}}|$, R_L.

By Lemma 5 and $l \leq n!$, we see that R_L is bounded above by an effectively computable number depending only on n and $|D_L|$. If D_K denotes the discriminant of K, we refer to Stark [16] to obtain $D_L | D^l{}_K$ and furthermore, by a well-known theorem (see [11]), $D_K | D_{\mathscr{C}}$. Hence, by (7), we conclude that R_L is bounded by an effectively computable number depending only on $|D_{\mathscr{C}}|$. $\square$

Let $A \in \mathbf{Z} \setminus \{0\}$ and let $p_1, \ldots, p_s$ be distinct primes not exceeding P. Theorem 3 will be deduced from Lemma 1 and the next lemma.

LEMMA 6. *All solutions of the Thue-Mahler equation*

$$(29) \qquad F(x, y) = Ap_1^{z_1} \cdots p_s^{z_s} \textit{ in } x, y, z_1, \ldots, z_s \in \mathbf{Z} \textit{ with } (x, y) = 1,\ z_1 \geq 0, \ldots, z_s \geq 0,$$

satisfy

$$\max(|x|, |y|) \leq \exp(C_{11}(s+1)^{C_{12}(s+1)}P^{2l}(1 + \log(|A| H(F))))$$

where $C_{11} > 0$ and $C_{12} > 0$ are effectively computable numbers such that C_{11} depends only on l, h_L, R_L and C_{12} depends only on l.

This is a simplified form of a special case of Corollary 1 of Győry [7]. Its proof involves the theory of linear forms in logarithms and its p-adic analogue.

PROOF *of Theorem* 3. Let $p_1, \ldots, p_s$ denote the distinct prime factors of d_β. Suppose that $\max_i p_i = P$. By Lemma 1, we have

$$(30) \qquad F(a_4, -a_3) = Ap_1^{z_1} \cdots p_s^{z_s}$$

where $z_1, \ldots, z_s$ are non-negative integers and A is a nonzero integer which divides d_α^n. But $d_\alpha \leq H(F)$. Now, we apply Lemma 6 to (30) to obtain

$$(31) \qquad \max(|a_3|, |a_4|) < \exp((C_{13}(s+1))^{C_{12}(s+1)}P^{2l}(1 + \log H(F)))$$

with the C_{12} specified in Lemma 6 and with an effectively computable C_{13} depending only on l, h_L and R_L. Now, we observe that (31) with $H(F)=H(\alpha)$, $P=P(d_\beta)$ and $s=\omega(d_\beta)$ implies (9) which, by $s\le 2P/\log P$ (cf. [14], (3.6)) establishes (10). Further, we have $Q(d_\beta)=p_1\cdots p_s\ge P$. Hence (9), together with

$$\tfrac{1}{2}s\log(s+1)<s\text{th prime}<40\sum_{i=1}^{s}\log p_i$$

(cf. [14], (3.12), (3.16)), implies (11). □

PROOF *of Theorem* 4. As in the proof of Theorem 2, let $\alpha\in\mathscr{C}$ be chosen to satisfy (25). Let β be an arbitrary element of $\mathscr{C}$ represented in the form (1). As we have seen in the proof of Theorem 2, β is $\mathbf{Z}$-equivalent to an element β' of $\mathscr{C}$ satisfying (28) which, together with (25), (10), (7) and $l\le n!$, implies that

$$P(d_\beta)>c_{21}\log\log H,\ H=\max(H(\beta'),4),$$

where $c_{21}>0$ is an effectively computable number depending only on $|D_{\mathscr{C}}|$, $d_{\mathscr{C}}$, h_L and R_L. Now, we apply Lemma 5 and an argument of the proof of Theorem 2 to conclude that $\max(h_L, R_L)$ is bounded above by an effectively computable number depending only on $|D_{\mathscr{C}}|$. □

PROOF *of Corollary* 2. The finiteness assertion is an immediate consequence of Theorem 4. Further, if a representative, say α, of $\mathscr{C}$ is given effectively in the usual sense (cf. [17]), then $D_{\mathscr{C}}=D^*(\alpha)$ and $d_{\mathscr{C}}\le d_\alpha$, i.e. $|D_{\mathscr{C}}|$ and $d_{\mathscr{C}}$ can be effectively bounded above in terms of $n=\deg(\alpha)$ and $H(\alpha)$. Hence, it follows from Theorem 4 that if $\beta\in\mathscr{C}$ with $d_\beta\in S$ then there is a β' which is $\mathbf{Z}$-equivalent to β such that $H(\beta')\le C_{14}$ where $C_{14}>0$ is an effectively computable number depending only on n, $H(\alpha)$ and the maximum P of the primes $p_1,\dots,p_s$ involved. Since $d_{\beta'}\le H(\beta')$ and $d_{1/\beta'}\le H(1/\beta')=H(\beta')$, we see that $d_{\beta'}\le C_{14}$ and $d_{1/\beta'}\le C_{14}$. Consequently, representing β' and $1/\beta'$ in the form (1), we apply Theorem 1 to derive that $\max_{1\le i\le 4}|a_i|$ is bounded by an effectively computable number depending only on n, $H(\alpha)$, P, h_L and R_L. Now, as in the proof of Theorem 2, we see that $\max(h_L, R_L)$ is bounded above by an effectively computable number depending only on $|D_{\mathscr{C}}|$ and hence, $\max(h_L, R_L)$ is bounded above by an effectively computable number depending only on n and $H(\alpha)$. Thus

$$\max_{1\le i\le 4}|a_i|\le C_{15}(n, H(\alpha), P)$$

where $C_{15}(n, H(\alpha), P)>0$ is effectively computable. Finally, from among the algebraic numbers whose representations of the form (1) satisfy

$$\max_{1\le i\le 4}|a_i|\le C_{15}$$

and which are equivalent to α, we can select a full set of representatives of pairwise $\mathbf{Z}$-inequivalent elements in $\mathscr{C}$ with denominators contained in S. □

Theorem 5 will be proved by means of Lemma 1 and the following result which is an immediate consequence of Corollary 2 of Evertse [2].

LEMMA 7. *Equation* (29) *has at most*

$$2\times 7^{n^3(2s+2\omega(A)+3)}$$

Solutions

PROOF *of Theorem* 5. Choose $\alpha\in\mathscr{C}$ such that $\omega_{\mathscr{C}}=\omega(d_\alpha)$. Further, let $f(x)$ be the minimal defining polynomial of α over $\mathbf{Z}$ and let

$$F(x,y)=y^n f\left(\frac{x}{y}\right),\ n=\deg(f).$$

If $\beta\in\mathscr{C}$ and β is represented in the form (1) then, by Lemma 1, $F(a_4,-a_3)$ divides $(d_\alpha d_\beta)^n$. If $d_\beta\in S$, we apply Lemma 7 to derive that the number of pairs (a_4,a_3) under consideration is at most

$$2\times 7^{n^3(2s+2\omega_{\mathscr{C}}+3)}.$$

Fix now such a pair (a_4,a_3). If $\beta',\beta''\in\mathscr{C}$ have representations of the form

$$\beta'=\frac{a_1'\alpha+a_2'}{a_3\alpha+a_4},\ \beta''=\frac{a_1''\alpha+a_2''}{a_3\alpha+a_4}$$

with $a_1', a_2', a_1'', a_2''\in\mathbf{Z}$ and

$$|a_1'a_4-a_2'a_3|=|a_1''a_4-a_2''a_3|=1,$$

then

$$a_1'-a_1''=a_3t,\ a_2'-a_2''=a_4t$$

or

$$a_1'+a_1''=a_3t,\ a_2'+a_2''=a_4t$$

with some $t\in\mathbf{Z}$ and hence $\beta'-\beta''=t$ or $\beta'+\beta''=t$. □

Consider equation (29) for $A=1$, and denote by $D(F)$ the discriminant of the binary form F. Theorem 6 will be deduced form Lemma 1 and the next lemma which is an immediate consequence of Corollary 1 of Evertse and Győry [4].

LEMMA 8. *There exists a number* $C_{16}>0$ *which depends only on* K *and* S *such that if* $[D(F)]_S>C_{16}$ *then, for* $A=1$, *equation* (29) *has at most two solutions* (*with* (x,y) *and* $(-x,-y)$ *regarded as the same*).

PROOF *of Theorem* 6. Suppose that $\mathscr{C}$ has at least one element with denominator contained in S. Choose such an $\alpha\in\mathscr{C}$, and let $F(x,y)$ be as in the proof of Theorem 5. If $\beta\in\mathscr{C}$ with $d_\beta\in S$ and if β is represented in the form (1), then Lemma 1 implies that $F(a_4,-a_3)\in S$. Since

$$D(F)=D^*(\alpha)=D_{\mathscr{C}},$$

it follows from Lemma 8 that the number of pairs (a_4,a_3) under consideration (with (a_4,a_3) and $(-a_4,-a_3)$ regarded as the same) is at most 2. Following now the argument of the proof of Theorem 5 and observing that

$$\frac{a_1'\alpha + a_2'}{-a_3\alpha - a_4} = -\frac{a_1'\alpha + a_2'}{a_3\alpha + a_4},$$

the assertion follows. □

REFERENCES

1. Birch, B.J. and J.R. Merriman – Finiteness theorems for binary forms with given discriminant, Proc. London Math. Soc. **24**, 385-394 (1972).
2. Evertse, J.-H. – On equations in *S*-units and the Thue-Mahler equation, Invent. Math. **75**, 561-584 (1984).
3. Evertse, J.-H. and K. Győry – On unit equations and decomposable form equations, J. Reine Angew. Math. **358**, 6-19 (1985).
4. Evertse, J.-H. and K. Győry – Thue-Mahler equations with a small number of solutions, to appear.
5. Győry, K. – Sur les polynômes à coefficients entiers et de discriminant donné II, Publ. Math. Debrecen **21**, 125-144 (1974).
6. Győry, K. – Sur les polynômes à coefficients entiers et de discriminant donné III, Publ. Math. Debrecen **23**, 141-165 (1976).
7. Győry, K. – Explicit upper bounds for the solutions of some diophantine equations, Ann. Acad. Sci. Fenn., Ser. A, Math. **5**, 3-12 (1980).
8. Győry, K. – Résultats effectifs sur la représentation des entiers par des formes décomposables, Queen's Papers in Pure and Applied Math., **56**, Kingston, Canada (1980).
9. Győry, K. – Effective finiteness theorems for polynomials with given discriminant and integral elements with given discriminant over finitely generated domains, J. Reine Angew. Math. **346**, 54-100 (1984).
10. Győry, K. and Z.Z. Papp – Effective estimates for the integer solutions of norm form and discriminant form equations, Publ. Math. Debrecen **25**, 311-325 (1978).
11. Hilbert, D. – Über diophantische Gleichungen, Göttingen Nachr. 48-54 (1897).
12. Mignotte, M. – Approximation des nombres algébriques, Publications Mathématiques d'Orsay, 77-74, Département de Mathématique, Université de Paris-Sud, Orsay, pp. 136 (1977).
13. Schmidt, W.M. – Diophantine Approximation, Lecture Notes in Mathematics **785**, Springer-Verlag, Berlin (1980).
14. Barkley Rosser, J. and L. Schoenfeld – Approximate formulas for some functions of prime numbers, Illinois J. Math. **6**, 64-94 (1962).
15. Siegel, C.L. – Abschätzung von Einheiten, Nachr. Göttingen, 71-86 (1969).
16. Stark, H.M. – Some effective cases of Brauer-Siegel theorem, Invent. Math. **23**, 135-152 (1974).
17. Stolarsky, K.B. – Algebraic numbers and diophantine approximation, New York (1974).
18. Zimmert, R. – Ideale Kleiner Norm in Idealklassen und eine Regulatorabschätzung, Invent. Math. **62**, 367-380 (1981).