

HEIGHTS OF ALGEBRAIC POINTS LYING ON CURVES OR HYPERSURFACES

WOLFGANG M. SCHMIDT

(Communicated by William W. Adams)

ABSTRACT. Our first aim will be to give an explicit version of a generalization of the results of Zhang and Zagier on algebraic points (x, y) with $x + y + 1 = 0$. Secondly, we will show that distinct algebraic points lying on a given curve of certain type can be distinguished in terms of some height functions. Thirdly, we will derive a bound for the number of points on such a curve whose heights are under a given bound and whose coordinates lie in a multiplicative group of given rank.

0. INTRODUCTION

When K is a number field, let $V = V(K)$ be the set of its places, and for $v \in V$ let $|\cdot|_v$ be the absolute value belonging to v which extends the ordinary or a p -adic absolute value of \mathbb{Q} . Further set $\|x\|_v = |x|_v^{d_v/d}$ where d is the degree of K and d_v is the local degree associated with v . The additive version of the product formula is that

$$\sum_{v \in V} \log \|x\|_v = 0$$

for $x \in K^\times$. For such x set

$$h(x) = \sum_{v \in V} \max(0, \log \|x\|_v) = \frac{1}{2} \sum_{v \in V} |\log \|x\|_v|,$$

where the second equality follows from the product formula. Then $h(x)$ is the *absolute logarithmic height* of x ; it is independent of the number field K in which x is embedded.

It is an old conjecture of Lehmer [2] that when x is of degree d over \mathbb{Q} , and is not 0 or a root of 1, then

$$(0.1) \quad h(x) > c_1/d$$

with an absolute constant $c_1 > 0$. The best result in this direction is due to Dobrowolski [1] and says that $h(x) > (c_2/d)(\log \log d / \log d)^3$ if $d \geq 3$. The example $x = 2^{1/d}$ shows that (0.1) would be best possible. In contrast, there is the following

Received by the editors March 27, 1995.

1991 *Mathematics Subject Classification*. Primary 11G30.

The author was supported in part by NSF grant DMS-9401426.

result of Zhang [8]: Suppose x, y are algebraic but not 0 or cube roots of 1, and satisfy

$$x + y + 1 = 0.$$

Then

$$h(x) + h(y) \geq c_3 > 0$$

with an absolute constant c_3 . Zagier [7] gave a more natural proof and determined the best value of the constant: $c_3 = \frac{1}{2} \log((1 + \sqrt{5})/2)$. We will prove the following

Theorem 1. *Let $F(X_1, \dots, X_n)$ be a polynomial with rational coefficients. Let x_1, \dots, x_n be nonzero algebraic numbers with*

$$F(x_1, \dots, x_n) = 0, \quad F(1/x_1, \dots, 1/x_n) \neq 0.$$

Then

$$\sum_{i=1}^n h(x_i) \geq c_3(F) > 0.$$

When F has total degree f and coefficients in \mathbb{Z} of maximum modulus H , we may take

$$c_3(F) = 1/(2^{4f+2n}H).$$

S. Ahlgren pointed out to me that the theorem can be generalized to polynomials F with coefficients in a number field with at least one real embedding.

When $n = 2$ and $F(X, Y) = X + Y + 1$, then $F(x, y) = F(1/x, 1/y) = 0$ yields $x + y = -1$, $xy = 1$, so that x, y are the roots of $Z^2 + Z + 1$, hence are cube roots of 1. Therefore Theorem 1 contains Zhang's Theorem.

Instead of the sum

$$(0.2) \quad h_s(\underline{x}) = \sum_{i=1}^n h(x_i)$$

we could have taken a more "sophisticated" function, such as, e.g.,

$$h(x_1, \dots, x_n) = \sum_{v \in V} \max(0, \log \|x_1\|_v, \dots, \log \|x_n\|_v).$$

h can be interpreted as the height of the point $(1 : x_1 : \dots : x_n)$ in projective space \mathbb{P}^n , and one can formulate a result on heights of such points satisfying homogeneous polynomial equations. But the proofs are more conveniently done in the affine setting, and h has the disadvantage (crucial in (ii) below) that it is not invariant under replacing x_1, \dots, x_n by $1/x_1, \dots, 1/x_n$.

When A is a subgroup of $\bar{\mathbb{Q}}^\times$, where $\bar{\mathbb{Q}}$ is the algebraic closure of \mathbb{Q} , let A^n be the product group $A \times \dots \times A$. Suppose $\underline{x} = (x_1, \dots, x_n)$, $\underline{x}' = (x'_1, \dots, x'_n), \dots$ lie in $(\bar{\mathbb{Q}}^\times)^n$. In this group $\underline{x}/\underline{x}' = (x_1/x'_1, \dots, x_n/x'_n)$. We now set

$$\delta(\underline{x}, \underline{x}') = h_s(\underline{x}/\underline{x}') = \sum_{i=1}^n h(x_i/x'_i).$$

Since $h(1/x) = h(x)$ and $h(xy) \leq h(x) + h(y)$, we have

- (i) $\delta(\underline{x}, \underline{x}') \geq 0$, with equality precisely when $\underline{x}/\underline{x}' \in U^n$, where U is the group of roots of 1.
- (ii) $\delta(\underline{x}, \underline{x}') = \delta(\underline{x}', \underline{x})$.

$$(iii) \delta(\underline{x}, \underline{x}'') \leq \delta(\underline{x}, \underline{x}') + \delta(\underline{x}', \underline{x}'').$$

Thus δ induces a metric on the factor group $(\bar{\mathbb{Q}}^\times)^n/U^n$.

In what follows we will have $n = 2$ and we will have $\underline{x} = (x, y), \underline{x}' = (x', y'), \dots$ in $(\bar{\mathbb{Q}}^\times)^2$. Let $P \in \mathbb{C}[X, Y]$ be not divisible by X or Y . Let $\mathcal{M} = \mathcal{M}(P)$ be the set of monomials $X^i Y^j$ occurring in P with nonzero coefficients, so that $P = \sum_{M \in \mathcal{M}} u_M M$ with coefficients $u_M \neq 0$. Suppose P has respective degrees a, b in X, Y , and set

$$\tilde{P} = \sum_{M \in \mathcal{M}} u_M X^a Y^b M^{-1}.$$

It is easily seen that \tilde{P} (like P) is not divisible by X or Y and is again of respective degrees a, b . Thus $\tilde{\tilde{P}} = P$, and the relation between P and \tilde{P} is symmetric. Call P reflexive if $\mathcal{M}(P) = \mathcal{M}(\tilde{P})$. For example, $P = uX + vY + w$ with $uvw \neq 0$ is not reflexive, but $P = sXY + uX + vY + w$ with $suvw \neq 0$ is reflexive.

Theorem 2. *Suppose $P(X, Y)$ as above is irreducible and not reflexive. Let P, \tilde{P} be of respective total degrees p, \tilde{p} , and set $q = p\tilde{p}$. Suppose $\underline{x}_0, \underline{x}_1, \dots, \underline{x}_q$ are distinct zeros of P lying in $(\bar{\mathbb{Q}}^\times)^2$. Then*

$$\sum_{i=1}^q \delta(\underline{x}_0, \underline{x}_i) \geq c_4(P) > 0.$$

When $\mathcal{M}(P)$ has cardinality m , we may take

$$c_4(P) = 2^{-8pm}.$$

For a linear polynomial P , a related result had been proved by Schlickewei and Wirsing [5].

Finally we have

Theorem 3. *Let $P(X, Y)$ be as in Theorem 2, and Γ a subgroup of $(\bar{\mathbb{Q}}^\times)^2$ containing at most r multiplicatively independent elements. Then the number of zeros $\underline{x} \in \Gamma$ of P with $h(\underline{x}) \leq C$, where $C \geq 1$, is*

$$\leq c_5(P)^{r+1} C^r.$$

We may take

$$c_5(P) = 2^{9pm}.$$

In the case of a linear polynomial P , a bound with r^2 in the exponent is implicit in Schlickewei [3].

Added in proof. Since submission of this paper, further work was done by E. Bombieri and U. Zannier in *Algebraic Points on Subvarieties of \mathbb{G}_m^n* , which has already appeared in International Mathematical Research Notices **7** (1995), 333–347. See also W. Schmidt, *Heights of Points on Subvarieties of \mathbb{G}_m^n* (to appear in Proceedings Séminaire de Théorie des Nombres de Paris (1994/94)) and F. Beukers and D. Zagier, *Lower bounds of heights of points on hypersurfaces* (Preprint #943, Univ. Utrecht, 1996).

1. PROOF OF THEOREM 1

Lemma 1. *Let x_1, \dots, x_n be nonzero complex numbers, and set*

$$\rho = \max_i |1 - |x_i||.$$

Then when $\mu > 1$ we have

$$(1.1) \quad \log \rho + \log \mu \leq (e \log 2)^{-1} \mu \max_i |\log |x_i||.$$

Proof. Since we interpret $\log 0$ to be $-\infty$, we may suppose that $\rho \neq 0$. Set $\nu = \mu\rho$. We distinguish three cases.

(i) $0 < \nu \leq 1$. Here we observe that the left hand side of (1.1) is ≤ 0 .

(ii) $1 < \nu < \mu$. Pick i with $|1 - |x_i|| = \rho = \nu/\mu$. Then $|x_i| = 1 \pm \nu/\mu$, so that $|\log |x_i|| \geq (\nu/\mu) \log 2$. Now

$$\log \rho + \log \mu = \log \nu \leq \nu/e \leq (e \log 2)^{-1} \mu |\log |x_i||,$$

and (1.1) holds.

(iii) $\nu \geq \mu$. Then $\rho \geq 1$, so that $\rho = |x_i| - 1$ for some i , and the right hand side of (1.1) is $\geq (e \log 2)^{-1} \mu \log(\rho + 1)$. The desired assertion now follows from

$$(e \log 2)^{-1} \mu \log(\rho + 1) - \log \rho - \log \mu \geq (e \log 2)^{-1} \mu \log 2 - \log \mu \geq 0.$$

Now let $\underline{x} = (x_1, \dots, x_n)$ be as in Theorem 1, and set $K = \mathbb{Q}(x_1, \dots, x_n)$ and $V(K) = V = V_\infty \cup V_0$, where V_∞, V_0 consist of Archimedean and non-Archimedean places, respectively. For $v \in V$ set

$$B_v = \max(0, \log |x_1|_v, \dots, \log |x_n|_v),$$

so that

$$(1.2) \quad \max(1, |x_1|_v, \dots, |x_n|_v) = e^{B_v}$$

and

$$(1.3) \quad \begin{aligned} \sum_{v \in V} d_v B_v &= \sum_{v \in V} \max(0, d \log \|x_1\|_v, \dots, d \log \|x_n\|_v) \\ &\leq d \sum_{i=1}^n h(x_i) = dh_s(\underline{x}). \end{aligned}$$

Set

$$\rho_v = \max_i |1 - |x_i|_v| \quad (v \in V).$$

Write

$$(1.4) \quad \tilde{F}(X_1, \dots, X_n) = X_1^{r_1} \cdots X_n^{r_n} F(1/X_1, \dots, 1/X_n)$$

where r_1, \dots, r_n are the respective degrees of F in X_1, \dots, X_n . Then \tilde{F} is a polynomial of total degree $\tilde{f} \leq nf$. Our hypothesis implies that

$$(1.5) \quad \tilde{F}(\underline{x}) \neq 0.$$

Lemma 2.

$$\log |\tilde{F}(\underline{x})|_v \leq \begin{cases} nf B_v & \text{when } v \in V_0, \\ (n+1) f B_v + \log(2^{4f+2n-2} H) + \log \rho_v & \text{when } v \in V_\infty. \end{cases}$$

Proof. When $v \in V_0$, then

$$|\tilde{F}(\underline{x})|_v \leq e^{\tilde{f}B_v} \leq e^{nfB_v},$$

whence the assertion.

Suppose $v \in V_\infty$. We may assume that K is embedded in \mathbb{C} , and $|\cdot|_v$ is the ordinary absolute value. We denote the complex conjugate of a number z by \bar{z} . By the Taylor expansion about \underline{x} we have

$$F(1/\bar{x}_1, \dots, 1/\bar{x}_n) = \sum_{\underline{k}} c_{\underline{k}} ((1/\bar{x}_1) - x_1)^{k_1} \dots ((1/\bar{x}_n) - x_n)^{k_n}$$

where in view of $F(\underline{x}) = 0$ the sum is over n -tuples $\underline{k} = (k_1, \dots, k_n) \neq \underline{0}$ with $k_i \geq 0$ ($i = 1, \dots, n$), $k_1 + \dots + k_n \leq f$, and where $c_{\underline{k}} = F_{\underline{k}}(\underline{x})$ with

$$F_{\underline{k}} = \frac{1}{k_1! \dots k_n!} \frac{\partial^{k_1 + \dots + k_n}}{\partial X_1^{k_1} \dots \partial X_n^{k_n}} F.$$

The coefficients of $F_{\underline{k}}$ have modulus $\leq 2^f H$ (see, e.g., [6, Ch. V, Lemma 5A]). The number of monomials in $F_{\underline{k}}$ is $\leq \binom{f+n}{n} \leq 2^{f+n-1}$, so that by (1.2),

$$|c_{\underline{k}}| \leq 2^{2f+n-1} H e^{B(f-k_1-\dots-k_n)}$$

with $B = B_v$. After multiplication by $\bar{x}_1^{r_1} \dots \bar{x}_n^{r_n}$ we obtain

$$(1.6) \quad \tilde{F}(\underline{\bar{x}}) = \sum_{\underline{k}} c_{\underline{k}} \bar{x}_1^{r_1-k_1} (1 - |x_1|^2)^{k_1} \dots \bar{x}_n^{r_n-k_n} (1 - |x_n|^2)^{k_n}.$$

For $1 \leq i \leq n$,

$$|\bar{x}_i|^{r_i-k_i} (1 - |x_i|^2)^{k_i} \leq 2^{k_i} \max(1, |x_i|)^{r_i+k_i} \leq 2^{k_i} e^{(r_i+k_i)B}.$$

But when $k_i > 0$ we have with $\rho = \rho_v$ that

$$|\bar{x}_i|^{r_i-k_i} (1 - |x_i|^2)^{k_i} \leq 2^{k_i} \rho \max(1, |x_i|)^{r_i+k_i-1} \leq 2^{k_i} \rho e^{(r_i+k_i)B}.$$

Thus (since the sum in (1.6) is over $\underline{k} \neq \underline{0}$),

$$\begin{aligned} |\tilde{F}(\underline{\bar{x}})| &= |\tilde{F}(\underline{\bar{x}})| \leq \rho \cdot 2^f \sum_{\underline{k}} |c_{\underline{k}}| e^{(nf+k_1+\dots+k_n)B} \\ &\leq \rho \cdot 2^f \binom{f+n}{n} \cdot 2^{2f+n-1} H e^{(n+1)fB} \\ &\leq \rho \cdot 2^{4f+2n-2} H e^{(n+1)fB}. \end{aligned}$$

Therefore

$$\log |\tilde{F}(\underline{\bar{x}})| \leq \log \rho + \log(2^{4f+2n-2} H) + (n+1)fB,$$

and Lemma 2 is established.

We now multiply the inequality of the lemma by d_v and take the sum over $v \in V$. The left hand side will become zero by (1.5) and the product formula. In view of (1.3) we obtain

$$(1.7) \quad 0 \leq (n+1)fdh_s(\underline{x}) + d \log(2^{4f+2n-2} H) + \sum_{v \in V_\infty} d_v \log \rho_v.$$

When $\mu > 10$, Lemma 1 yields

$$\begin{aligned}
 \sum_{v \in V_\infty} d_v \log \rho_v &= -d \log \mu + \sum_{v \in V_\infty} d_v (\log \rho_v + \log \mu) \\
 (1.8) \quad &\leq -d \log \mu + (e \log 2)^{-1} \mu \sum_{v \in V_\infty} d_v \max_i |\log |x_i|_v| \\
 &= -d \log \mu + (e \log 2)^{-1} \mu d \sum_{v \in V_\infty} \max_i |\log \|x_i\|_v|.
 \end{aligned}$$

But

$$(1.9) \quad \sum_{v \in V_\infty} \max_i |\log \|x_i\|_v| \leq \sum_{i=1}^n \sum_{v \in V} |\log \|x_i\|_v| = 2h_s(\underline{x}).$$

If we substitute all this into (1.7) and divide by d , we get

$$(1.10) \quad 0 \leq -\log \mu + ((n + 1)f + (2/e \log 2)\mu)h_s(\underline{x}) + \log(2^{4f+2n-2}H).$$

We set

$$\mu = e \cdot 2^{4f+2n-2}H.$$

Since $f \geq 1$, the coefficient of $h_s(\underline{x})$ in (1.10) is

$$\begin{aligned}
 (n + 1)f + (2/e \log 2)\mu &\leq ((n + 1) \cdot 2^{-4} \cdot 2^{4f} + (1/\log 2) \cdot 2^{4f+2n-1})H \\
 &< 2^{4f+2n}H.
 \end{aligned}$$

Thus indeed $h_s(\underline{x}) > 1/(2^{4f+2n}H)$.

For later applications we will prove the following

Theorem 1a. *When $n = 4$ and*

$$F_0(X_1, X_2, X_3, X_4) = \begin{vmatrix} 1 & 1 & 1 \\ 1 & X_1 & X_2 \\ 1 & X_3 & X_4 \end{vmatrix},$$

we may take $c_3(F_0) = 1/52$.

We begin with

Lemma 2a. *In the situation of Theorem 1a,*

$$\log |\tilde{F}_0(\underline{x})|_v \leq \begin{cases} 3B_v & \text{when } v \in V_0, \\ 5B_v + 4 \log 2 + \log \rho_v & \text{when } v \in V_\infty. \end{cases}$$

Proof. Note that

$$\begin{aligned}
 \tilde{F}_0(X_1, X_2, X_3, X_4) &= X_2X_3 - X_1X_4 + X_1X_3X_4 + X_1X_2X_4 \\
 &\quad - X_2X_3X_4 - X_1X_2X_3.
 \end{aligned}$$

The assertion for $v \in V_0$ follows immediately. On the other hand, as a special case of (1.6),

$$\begin{aligned}
 \tilde{F}_0(\underline{x}) &= (x_4 - 1)(1 - |x_1|^2)\bar{x}_2\bar{x}_3\bar{x}_4 + (x_1 - 1)(1 - |x_4|^2)\bar{x}_1\bar{x}_2\bar{x}_3 \\
 &\quad - (x_3 - 1)(1 - |x_2|^2)\bar{x}_1\bar{x}_3\bar{x}_4 - (x_2 - 1)(1 - |x_3|^2)\bar{x}_1\bar{x}_2\bar{x}_4 \\
 &\quad + (1 - |x_1|^2)(1 - |x_4|^2)\bar{x}_2\bar{x}_3 - (1 - |x_2|^2)(1 - |x_3|^2)\bar{x}_1\bar{x}_4.
 \end{aligned}$$

The right hand side equals

$$(1 - |x_1|^2)\bar{x}_2\bar{x}_3 \left(\frac{1}{4}|x_4|^2 + \frac{1}{2} - \bar{x}_4 \right) + (1 - |x_4|^2)\bar{x}_2\bar{x}_3 \left(\frac{1}{2}|x_1|^2 + \frac{1}{2} - \bar{x}_1 \right) \\ - (1 - |x_2|^2)\bar{x}_1\bar{x}_4 \left(\frac{1}{2}|x_3|^2 + \frac{1}{2} - \bar{x}_3 \right) + (1 - |x_3|^2)\bar{x}_1\bar{x}_4 \left(\frac{1}{2}|x_2|^2 + \frac{1}{2} - \bar{x}_2 \right).$$

Now the sum of the moduli of the coefficients in $(1 + X) \left(\frac{1}{2}Y^2 + \frac{1}{2} - Y \right)$ is 4. Therefore we obtain

$$|\tilde{F}_0(\underline{x})| = |\tilde{F}_0(\underline{x})| \leq 4\rho \cdot 4e^{5B} = e^{5B} \cdot 2^4\rho,$$

and Lemma 2a follows.

If we take the inequalities of Lemma 2a, multiply by d_v , and take the sum over $v \in V$, we obtain

$$0 \leq 5dh_s(\underline{x}) + 4d \log 2 + \sum_{v \in V_\infty} d_v \log \rho_v.$$

In view of (1.8), (1.9) we obtain after division by d that

$$(1.10a) \quad 0 \leq -\log \mu + (5 + (2/e \log 2)\mu)h_s(\underline{x}) + 4 \log 2.$$

We now take $\mu = e \cdot 2^4$, so that

$$5 + (2/e \log 2)\mu = 5 + 2^5 / \log 2 < 52,$$

and (1.10a) gives $h_s(\underline{x}) > 1/52$.

2. PROOF OF THEOREM 2

Write

$$P = \sum_{k=1}^m u_k M_k$$

with distinct monomials M_k and nonzero coefficients u_k . Since P is nonreflexive, $\mathcal{M}(P) \not\subseteq \mathcal{M}(\tilde{P})$. By hypothesis, $P(\underline{x}_i) = 0$, i.e., $\sum_{k=1}^m u_k M_k(\underline{x}_i) = 0$ ($i = 0, \dots, q$), so that the matrix

$$(M_k(\underline{x}_i)) \quad (1 \leq k \leq m, 0 \leq i \leq q)$$

has rank $< m$. If we divide the k -th row by $M_k(\underline{x}_0)$ we obtain the matrix

$$(2.1) \quad (M_k(\underline{x}_i/\underline{x}_0)) \quad (1 \leq k \leq m, 0 \leq i \leq q),$$

which is also of rank $< m$.

Next, consider the matrix

$$(2.2) \quad (M_k(\underline{x}_0/\underline{x}_i)) \quad (1 \leq k \leq m, 0 \leq i \leq q).$$

Suppose this matrix also had rank $< m$. Then there are relations

$$\sum_{k=1}^m w_k M_k(\underline{x}_0/\underline{x}_i) = \sum_{k=1}^m w_k M_k(\underline{x}_0)/M_k(\underline{x}_i) = 0 \quad (0 \leq i \leq q)$$

where not all the coefficients w_k are zero. Thus the polynomial

$$\hat{P}(\underline{X}) = \sum_{k=1}^m w_k M_k(\underline{x}_0) X^a Y^b M_k(\underline{X})^{-1}$$

(where again a, b are the degrees of P in X, Y) vanishes at $\underline{x}_0, \dots, \underline{x}_q$. Clearly $\mathcal{M}(\widehat{P}) \subseteq \mathcal{M}(\widetilde{P})$, so that $\mathcal{M}(P) \not\subseteq \mathcal{M}(\widehat{P})$, and P, \widehat{P} are not constant multiples of each other. Since \widehat{P} has respective degrees $\leq a, b$ in X, Y , it is not a multiple of P . Since P is irreducible, P, \widehat{P} have no common factor. Their respective total degrees are p and $\leq \tilde{p}$, so that by Bezout's Theorem they have at most $q = p\tilde{p}$ common zeros, contradicting the fact that they have the zeros $\underline{x}_0, \underline{x}_1, \dots, \underline{x}_q$.

We may conclude that the matrix (2.2) has rank m . There are integers i_0, i_1, \dots, i_{m-1} such that the matrix

$$(M_k(\underline{x}_0/\underline{x}_{i_t})) \quad (1 \leq k \leq m, 0 \leq t < m)$$

is nonsingular. We clearly may pick i_0, \dots, i_{m-1} with $i_0 = 0$. Then the matrix with rows

$$(2.3) \quad (1, M_k(\underline{x}_0/\underline{x}_{i_1}), \dots, M_k(\underline{x}_0/\underline{x}_{i_{m-1}})) \quad (1 \leq k \leq m)$$

is nonsingular. Let $F(\underline{X}_1, \dots, \underline{X}_{m-1})$ with $\underline{X}_i = (X_i, Y_i)$ be the determinant with rows

$$(1, M_k(\underline{X}_1), \dots, M_k(\underline{X}_{m-1})) \quad (1 \leq k \leq m).$$

Then F is a polynomial in $n = 2(m - 1)$ variables of total degree $f \leq \deg M_1 + \dots + \deg M_m \leq mp$. By the nonsingularity of the matrix with rows (2.3),

$$F(\underline{x}_0/\underline{x}_{i_1}, \dots, \underline{x}_0/\underline{x}_{i_{m-1}}) \neq 0.$$

On the other hand, since (2.1) is of rank $< m$, the matrix with rows

$$(1, M_k(\underline{x}_{i_1}/\underline{x}_0), \dots, M_k(\underline{x}_{i_{m-1}}/\underline{x}_0)) \quad (1 \leq k \leq m)$$

is singular, so that

$$F(\underline{x}_{i_1}/\underline{x}_0, \dots, \underline{x}_{i_{m-1}}/\underline{x}_0) = 0.$$

By Theorem 1, the point $\mathfrak{r} = (x_{i_1}/x_0, y_{i_1}/y_0, \dots, x_{i_{m-1}}/x_0, y_{i_{m-1}}/y_0)$ has $h_s(\mathfrak{r}) \geq c_3(F)$. Then

$$\sum_{i=1}^q \delta(\underline{x}_0, \underline{x}_i) = \sum_{i=1}^q (h(x_i/x_0) + h(y_i/y_0)) \geq h_s(\mathfrak{r}) \geq c_3(F).$$

Now $4f + 2n \leq 4mp + 2 \cdot 2(m - 1) \leq 8pm - 4$, so that we may take $c_3(F) = 2^{-8pm+4}$. Therefore Theorem 2 is true with $c_4(P) = 2^{-8pm+4} > 2^{-8pm}$.

Theorem 2a. *When $P_0 = uX + vY + w$ with nonzero coefficients, we may take*

$$c_4(P_0) = 1/52.$$

Proof. In this special case we have $m = 3, M_1 = 1, M_2 = X, M_3 = Y$. Further $F(\underline{X}_1, \underline{X}_2)$ becomes

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & X_1 & X_2 \\ 1 & Y_1 & Y_2 \end{vmatrix},$$

so that we may take $c_4(P) = c_3(F) = 1/52$.

3. PROOF OF THEOREM 3

Suppose initially that Γ is finitely generated and of rank r . There are $\underline{\alpha}_1 = (\alpha_1, \beta_1), \dots, \underline{\alpha}_r = (\alpha_r, \beta_r)$, so that the elements of Γ are

$$(3.1) \quad \underline{x} = (x, y) = \underline{\zeta} \underline{\alpha}_1^{u_1} \cdots \underline{\alpha}_r^{u_r} = (\xi \alpha_1^{u_1} \cdots \alpha_r^{u_r}, \eta \beta_1^{u_1} \cdots \beta_r^{u_r})$$

where $\underline{\zeta} = (\xi, \eta) \in U^2$, and $\underline{u} = (u_1, \dots, u_r)$ runs through \mathbb{Z}^r . Here Γ , hence the α_i, β_i lie in a number field K . For $v \in V = V(K)$ put

$$a_{iv} = \log \|\alpha_i\|_v, \quad b_{iv} = \log \|\beta_i\|_v \quad (i = 1, \dots, r),$$

$$a_v(\underline{\xi}) = \sum_{i=1}^r a_{iv} \xi_i, \quad b_v(\underline{\xi}) = \sum_{i=1}^r b_{iv} \xi_i$$

where $\underline{\xi} = (\xi_1, \dots, \xi_r) \in \mathbb{R}^r$. Set

$$\psi(\underline{\xi}) = \frac{1}{2} \sum_{v \in V} (|a_v(\underline{\xi})| + |b_v(\underline{\xi})|).$$

When $\underline{u} \in \mathbb{Z}^r$,

$$\psi(\underline{u}) = h(\alpha_1^{u_1} \cdots \alpha_r^{u_r}) + h(\beta_1^{u_1} \cdots \beta_r^{u_r}) = h(x) + h(y) = h_s(\underline{x})$$

where \underline{x} is given by (3.1). We have

- (a) $\psi(\underline{\xi}) \geq 0$,
- (b) $\psi(\alpha \underline{\xi}) = |\alpha| \psi(\underline{\xi})$ for $\alpha \in \mathbb{R}$,
- (c) $\psi(\underline{\xi} + \underline{\eta}) \leq \psi(\underline{\xi}) + \psi(\underline{\eta})$.

We may infer that ψ is continuous. The set Ψ consisting of points $\underline{\xi} \in \mathbb{R}^r$ with $\psi(\underline{\xi}) \leq 1$ is convex, symmetric (i.e., $\underline{\xi} \in \Psi$ yields $-\underline{\xi} \in \Psi$), closed, and contains $\underline{0}$ in its interior.

Lemma 3. *Suppose $\psi : \mathbb{R}^r \rightarrow \mathbb{R}$ with (a), (b), (c) has*

$$(3.2) \quad \psi(\underline{u}) \geq c > 0$$

for every $\underline{u} \in \mathbb{Z}^r \setminus \{\underline{0}\}$, and a fixed constant c . Then the set Ψ is compact.

Proof. Pick α in $0 < \alpha < c$. Then $\alpha\Psi$ contains no nonzero integer point, hence has finite volume by Minkowski's Theorem. Therefore Ψ has finite volume, and since it is convex and contains $\underline{0}$ in its interior, it is bounded, hence compact.

Lemma 4. *Suppose ψ satisfies (3.2). Let $\mathfrak{A} \subseteq \mathbb{R}^r$ be a set of points such that*

$$(3.3) \quad \psi(\underline{u} - \underline{v}) \geq \delta_0 > 0$$

for $\underline{u} \neq \underline{v}$ in \mathfrak{A} . Then the number of $\underline{u} \in \mathfrak{A}$ with

$$\psi(\underline{u}) \leq C$$

is

$$\leq ((2C/\delta_0) + 1)^r.$$

Proof. Let $\Psi(\underline{u})$ be the set $\frac{1}{2}\delta_0\Psi + \underline{u}$, i.e., the set $\frac{1}{2}\delta_0\Psi$ translated by \underline{u} . By our hypothesis, sets $\Psi(\underline{u}), \Psi(\underline{v})$ with $\underline{u} \neq \underline{v}$ in \mathfrak{U} have no interior points in common. On the other hand, when $\psi(\underline{u}) \leq C$, the set $\Psi(\underline{u}) \subseteq (C + \frac{1}{2}\delta_0)\Psi$. Comparing volumes (which are finite by the preceding lemma) we see that the number of points $\underline{u} \in \mathfrak{U}$ with $\psi(\underline{u}) \leq C$ is

$$\leq \left(C + \frac{1}{2}\delta_0\right)^r / \left(\frac{1}{2}\delta_0\right)^r = ((2C/\delta_0) + 1)^r.$$

The proof of Theorem 3 is now rapidly finished as follows. Let \mathfrak{S} be the set of points whose cardinality is to be estimated. Call $\underline{x}, \underline{x}'$ in \mathfrak{S} *neighbors* if $\underline{x} \neq \underline{x}'$ and

$$\delta(\underline{x}, \underline{x}') < c_4(P)/q.$$

In view of Theorem 2, an element $\underline{x} \in \mathfrak{S}$ has $\leq q - 1$ neighbors. Pick $\underline{x}_1 \in \mathfrak{S}$, and let \mathfrak{S}_1 be obtained from \mathfrak{S} by removing \underline{x}_1 and its neighbors. If \mathfrak{S}_1 is nonempty, pick $\underline{x}_2 \in \mathfrak{S}_1$ and let \mathfrak{S}_2 be obtained from \mathfrak{S}_1 by removing \underline{x}_2 and its neighbors, etc. This process will come to an end, and we obtain a “thinned out” set $\mathfrak{S}' = \{\underline{x}_1, \dots, \underline{x}_\ell\} \subseteq \mathfrak{S}$ no two of whose elements are neighbors, with $\text{card } \mathfrak{S}' \geq q^{-1} \text{card } \mathfrak{S}$. To \mathfrak{S}' corresponds a set \mathfrak{U} of points $\underline{u} \in \mathbb{Z}^r$ having (3.3) with $\delta_0 = c_4(P)/q$. By Lemma 4,

$$(3.4) \quad \text{card } \mathfrak{U} \leq ((2Cq/c_4(P)) + 1)^r \leq (3Cq/c_4(P))^r$$

when $C \geq 1$. Then

$$\text{card } \mathfrak{S} \leq q \text{card } \mathfrak{S}' = q \text{card } \mathfrak{U} \leq q(3Cq/c_4(P))^r.$$

Therefore when Γ is finitely generated, Theorem 3 holds with

$$c_5(P) = 3q/c_4(P) \leq 3p\tilde{p} \cdot 2^{8pm-4} \leq 6p^2 \cdot 2^{8pm-4} < 2^{9pm},$$

since (as is clear from the proof of Theorem 2) we may take $c_4(P) = 2^{4-8pm}$, and since $\tilde{p} \leq 2p$.

In general, Γ is a union of finitely generated groups $\Gamma_1 \subseteq \Gamma_2 \subseteq \dots$ of rank r . Our estimate holds for each Γ_i ($i = 1, 2, \dots$), hence also for Γ .

Theorem 3a. *When $P_0 = uX + vY + w$ with nonzero coefficients, the number of zeros \underline{x} of P_0 with $\underline{x} \in \Gamma$ and $h_s(\underline{x}) \leq C$, where $C \geq 1$, is*

$$\leq 2 \cdot (210C)^r.$$

Proof. Here $p = 1, \tilde{p} = 2$, and we may take $c_4(P) = 1/52$. Therefore (3.4) becomes

$$\text{card } \mathfrak{U} \leq (208C + 1)^r < (210C)^r,$$

and

$$\text{card } \mathfrak{S} \leq 2\text{card } \mathfrak{S}' \leq 2(210C)^r.$$

4. A FURTHER RESULT

For applications in subsequent work [4], it will be convenient to give the following easy

Theorem 4. *Let K be a number field of degree d , and $\Gamma \subseteq (K^\times)^n$ of rank r . Given $C \geq 1$, the number of $\underline{x} \in \Gamma$ with $h_s(\underline{x}) \leq C$ is*

$$\leq (2d^2)^n (43d^3 C)^r.$$

Proof. Call $\underline{x} \neq \underline{x}'$ in Γ neighbors if $\underline{x}/\underline{x}' \in U^n$. Now if the roots of 1 in K form a group of order k , we have $\Phi(k) \leq d$. Since $\Phi(k) \geq (k/2)^{1/2}$, we have $k \leq 2d^2$. Therefore \underline{x} has $< k^n \leq (2d^2)^n$ neighbors. When $\underline{x} \neq \underline{x}'$ are not neighbors, we have for $d > 1$,

$$\delta(\underline{x}, \underline{x}') = h(\underline{x}/\underline{x}') > \log \left(1 + \frac{\log d}{6d^2} \right)^{1/d} > \log \left(1 + \frac{1}{20d^3} \right) > \frac{1}{21d^3}$$

by a very generous minorization of an estimate of Dobrowolski [1]. Therefore setting $\delta_0 = 1/21d^3$ and proceeding as for Theorem 3, we obtain

$$\text{card } \mathfrak{S} \leq (2d^2)^n ((2C/\delta_0) + 1)^r = (2d^2)^n (42d^3 C + 1)^r.$$

REFERENCES

1. E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401. MR **80i**:10040
2. D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. Math. **34** (2) (1933), 461–479.
3. H. P. Schlickewei, *Equations $ax + by = 1$* , Annals of Math., (to appear).
4. H. P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, In preparation.
5. H. P. Schlickewei and E. Wirsing, *Lower bounds for the heights of solutions of linear equations*, Invent. Math, (to appear).
6. W. M. Schmidt, *Diophantine Approximation*, Springer Lecture Notes in Mathematics **785** (1980). MR **81j**:10038
7. D. Zagier, *Algebraic numbers close to both 0 and 1*, Math. Computation **61** (1993), 485–491. MR **94c**:11104
8. S. Zhang, *Positive line bundles on arithmetic surfaces*, Ann. of Math. **136** (1992), 569–587. MR **93j**:14024

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO, BOULDER, COLORADO 80309-0395
E-mail address: Schmidt@Euclid.colorado.edu