ACTA ARITHMETICA
LXVI.3 (1994)

The number of solutions to cubic Thue inequalities

by

JEFFREY LIN THUNDER (Boulder, Colo.)

Introduction. Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be a form of degree $d \geq 3$ which is irreducible over the rational numbers $\mathbb{Q}$. In 1909 A. Thue [T] showed that the number of integral solutions (x,y) to the equation $F(x,y) = m$ is finite. Equations of this form are now called *Thue equations*. Thue's result implies that the number of integral solutions (x,y) to the *Thue inequality*

$$|F(x,y)| \leq m$$

is also finite, since obviously such a form takes integral values at integral points.

Let $N_F(m)$ denote the number of integral solutions to the Thue inequality above and consider the region $R_F = \{(x,y) \in \mathbb{R}^2 : |F(x,y)| \leq 1\}$. Then the dilation of R_F by $m^{1/d}$ consists of all $(x,y) \in \mathbb{R}^2$ with $|F(x,y)| \leq m$, so that one would expect $m^{2/d}A_F$, where A_F is the area of R_F, to approximate $N_F(m)$. Indeed, Mahler [M1] showed that

$$|N_F(m) - m^{2/d}A_F| = O(m^{1/(d-1)}),$$

where the constant implicit in the O notation depends on the form F. More recently, W. Schmidt showed that

$$N_F(m) \ll m^{2/d}(d + \log m),$$

where the implied constant is absolute ([S], Chapter 3, Theorem 1C).

Together, Mahler's and Schmidt's results indicated that the area A_F might be bounded above by some absolute constant, or perhaps some constant depending only on the degree d. In fact, more is true. Suppose we look more generally at forms $G(X,Y) \in \mathbb{R}[X,Y]$ with discriminant $D(G) \neq 0$. For $T \in \mathrm{GL}(2,\mathbb{R})$ we get a form $G^T(X,Y) = G((X,Y)T)$, where $(X,Y)T$ is the matrix product. The crucial observation here is that the product $A_G|D(G)|^{1/d(d-1)}$ is invariant under such actions, i.e.,

$$A_{G^T}|D(G^T)|^{1/d(d-1)} = A_G|D(G)|^{1/d(d-1)}.$$

Let A_d denote the maximum of this product over all such forms of degree d. In [B1] M. Bean showed that

$$A_3 > A_4 > A_5 > \ldots \tag{1}$$

and also

$$A_3 = 3B(1/3, 1/3)\,, \tag{2}$$

where B is the usual beta function. Since $|D(F)| \geq 1$ for any form with integral coefficients (and nonzero discriminant), (1) and (2) together show that the area A_F is bounded above by an absolute constant.

In comparing his result with Mahler's, Schmidt conjectured that the logarithmic term in his bound was unnecessary. In fact, one might even hope that Mahler's result would hold with an implied constant depending only on d, or perhaps an error term $O(m^{\varepsilon+1/(d-1)})$ or $O(m^{2/d-\varepsilon})$ where the implied constant depends on d and $\varepsilon > 0$. In this paper we prove the following theorem which gives partial evidence for such a result.

THEOREM 1. *Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be a cubic form which is irreducible over $\mathbb{Q}$. With the notation above we have*

$$|N_F(m) - m^{2/3}A_F| = O(1 + m^{29/44}\log m)\,,$$

where the constant implicit in the O notation is absolute.

Using (2) and noting that $29/44 < 2/3$, we get the following.

COROLLARY. *Let F be as in Theorem 1. Then*

$$N_F(m) \ll m^{2/3},$$

where the implied constant is absolute.

Thus Schmidt's conjecture is true in the cubic case.

Bounds for the height. Let F be an integral form as in the introduction and write $F(X,Y) = \sum_{i=0}^{d} a_i X^i Y^{d-i}$. The dependency on the form F in the error term of Mahler's result is essentially a positive power of the *height*,

$$H(F) = \max_{0\leq i\leq d}\{|a_i|\}\,.$$

Now if $T \in \mathrm{SL}(2,\mathbb{Z})$, then $N_F(m) = N_{F^T}(m)$. We say two forms F and G are *equivalent* if $G = F^T$ for some $T \in \mathrm{SL}(2,\mathbb{Z})$. So a reasonable approach to our problem is to find an equivalent form G where $H(G)$ is small as possible, making the error term in Mahler's result small. A form F is called *minimal* if its height is smallest among all equivalent forms. It is not difficult to show that the height of a minimal form F is bounded below in terms of the discriminant of the form, $D(F)$. Specifically, one has (see [M2])

$$H(F)^{2(d-1)}d^{2d-1} \geq |D(F)| \tag{3}$$

for all forms F, and for $S \in \mathrm{GL}(2,\mathbb{R})$

$$|D(F^S)| = |D(F)||\det(S)|^{d(d-1)}\,. \tag{4}$$

Thus, there is no hope for finding an equivalent form of small height if the discriminant is large.

To prove his result, Schmidt reduces to considering the case when the discriminant is relatively large in terms of the parameter m, so that the height is large as well by (3). This is an approach exactly opposite of the one above. The purpose of this is to force all solutions to the Thue inequality to satisfy some type of "gap principle," and thus allow one to get upper bounds for the number of such solutions, as opposed to estimating the number of solutions by $m^{2/d}A_F$. If one knows that the discriminant is large to begin with, then the number of solutions to the Thue inequality can be shown to be relatively small.

The difficulty in getting upper bounds for $N_F(m)$ which do not depend on the coefficients of F lies with the forms of small discriminant. What is needed is some upper bound for the height of a minimal equivalent form in terms of the discriminant, so that one may assume the height is small if the discriminant is small, allowing one to use Mahler's result to bound $N_F(m)$. For this approach to work one would need some upper bound which is polynomial in the discriminant. J. H. Evertse has given such a polynomial bound in [E]. Unfortunately, his bound also contains an ineffective constant which depends both on the degree and the splitting field of the form. Worse yet, the ineffectivity comes from the infamous ineffectivity in Roth's theorem on approximation of algebraic numbers by rationals. This indicates that giving effective upper bounds for the height in terms of the discriminant is a deep and difficult problem. Evertse and Győry in [EG] give an effective bound using linear forms in logarithms, but it is not surprising that this bound is far larger than polynomial in the discriminant.

From the reduction theories of Lagrange and Hermite, one sees that an effective upper bound for the height in terms of the discriminant exists in the cubic case. Here, making explicit some arguments given by Evertse in [E], we give a short proof of a bound using geometry of numbers ([1]).

THEOREM 2. *Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be a cubic form which is irreducible over the rationals and write*

$$F(X,Y) = \prod_{i=1}^{3}(X\alpha_i + Y\beta_i)\,.$$

([1]) I thank W. Schmidt for pointing out a way to improve my original result.

There is a $T \in \mathrm{SL}(2,\mathbb{Z})$,

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

such that

$$H(F^T) \ll M(F^T) := \prod_{i=1}^{3} \max\{|a\alpha_i + b\beta_i|, |c\alpha_i + d\beta_i|\} \le 64|D(F)|^{1/2}.$$

The relationship between the height and the Mahler measure $M(F)$ defined above is well known. See [S], for example. Define

$$\Delta_1 = \alpha_2\beta_3 - \alpha_3\beta_2, \qquad \Delta_2 = \alpha_1\beta_3 - \alpha_3\beta_1, \qquad \Delta_3 = \alpha_1\beta_2 - \alpha_2\beta_1,$$

so that

$$|D(F)| = \prod_{i=1}^{3} |\Delta_i|^2.$$

Let

$$C = \{(x,y) \in \mathbb{R}^2 : |x\alpha_i + y\beta_i| \le |\Delta_i|^{-1} \text{ for } i = 1,2,3\}.$$

Then C is a convex body (closed, convex and symmetric about the origin). Let $\lambda_1 \le \lambda_2$ be the successive minima of C with respect to the integer lattice $\mathbb{Z}^2$. Then there are $(a,b) \in \lambda_1 C \cap \mathbb{Z}^2$ and $(c,d) \in \lambda_2 C \cap \mathbb{Z}^2$ with

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}).$$

We have

$$\prod_{i=1}^{3} \max\{|a\alpha_i + b\beta_i|, |c\alpha_i + d\beta_i|\} \le \prod_{i=1}^{3} \lambda_2 |\Delta_i|^{-1} \le \lambda_2^3 |D(F)|^{-1/2}. \tag{5}$$

Suppose that

$$\lambda_1\lambda_2 \le 4|D(F)|^{1/2}. \tag{6}$$

Now $\prod_{i=1}^{3}(a\alpha_i + b\beta_i)$ is the coefficient of X^3 in $F^T(X,Y)$, hence a nonzero integer (since F is irreducible over $\mathbb{Q}$). Using this gives

$$1 \le \prod_{i=1}^{3} |a\alpha_i + b\beta_i| \le \prod_{i=1}^{3} \lambda_1 |\Delta_i|^{-1} = \lambda_1^3 |D(F)|^{-1/2}. \tag{7}$$

Combining (6) and (7), we get $\lambda_2 \le 4|D(F)|^{1/3}$. This, together with (5), proves Theorem 2 once we have shown the validity of (6).

Lemma 1. *With the notation and hypotheses above*,

$$\lambda_1\lambda_2 \le 4|D(F)|^{1/2}.$$

P r o o f. By Minkowski's theorem

$$\lambda_1\lambda_2 \le 4/\mathrm{Vol}(C)\,. \tag{8}$$

Let $\alpha_i' = \alpha_i\Delta_i$ and $\beta_i' = \beta_i\Delta_i$ for $i = 1, 2, 3$. Then

$$C = \{(x, y) \in \mathbb{R}^2 : |x\alpha_i' + y\beta_i'| \le 1 \text{ for } i = 1, 2, 3\}\,.$$

One easily verifies that

$$(\alpha_3'x + \beta_3'y) = (\alpha_2'x + \beta_2'y) - (\alpha_1'x + \beta_1'y)\,,$$

so that $|\alpha_3'x + \beta_3'y| \le |\alpha_2'x + \beta_2'y| + |\alpha_1'x + \beta_1'y|$ and hence

$$C \supseteq C' = \{(x, y) \in \mathbb{R}^2 : |\alpha_i'x + \beta_i'y| \le 1/2 \text{ for } i = 1, 2\}\,.$$

If β_1'/α_1' is complex, we may assume without loss of generality that it is the complex conjugate of β_2'/α_2'. We then have

$$\mathrm{Vol}(C)^{-1} \le \mathrm{Vol}(C')^{-1} \le \left|\det\begin{pmatrix} \alpha_1' & \beta_1' \\ \alpha_2' & \beta_2' \end{pmatrix}\right| = |\Delta_1\Delta_2\Delta_3| = |D(F)|^{1/2}\,,$$

and the lemma follows from (8).

Proof of Theorem 1. Throughout this section, when we write $\ll$ the implied constant is absolute. We write F as in the statement of Theorem 2 and assume, as we may by Theorem 2, that

$$H(F) \ll |D(F)|^{1/2}\,.$$

Let

$$H'(F) = \max_{1\le i\le 3}\{1 + |\beta_i/\alpha_i|\}\,.$$

Since, as noted above, $\prod_{i=1}^3 |\alpha_i| \ge 1$, we also have

$$H'(F) \ll |D(F)|^{1/2}\,.$$

By the explicit version of Mahler's theorem in [B2],

$$|N_F(m) - m^{2/3}A_F| \ll m^{1/2}H'(F)^3H(F)^4 \ll m^{1/2}|D(F)|^{7/2}\,.$$

In particular, if $|D(F)| < m^{1/22}$ then

$$|N_F(m) - m^{2/3}A_F| \ll m^{1/2}m^{7/44} = m^{29/44}\,.$$

So Theorem 1 is correct if $|D(F)| < m^{1/22}$.

LEMMA 2. *Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a form of degree $d \ge 3$ which is irreducible over $\mathbb{Q}$. Then*

$$N_F(m) \ll d(1 + \log(m^{1/d}))(m^{1/d} + m^{2/d}|D(F)|^{-1/d(d-1)})\,,$$

where the implicit constant is absolute.

P r o o f. Let $P_F(m)$ and $P_F'(m)$ denote the number of primitive solutions to $|F(x, y)| \le m$ and $m/2^d < |F(x, y)| \le m$, respectively. Let p be the smallest prime satisfying $p \ge 2500m^{2/d}|D(F)|^{-1/d(d-1)}$. By Lemma 2C, Remark 2D and Proposition 2E of [S], Chapter 3, we have

$$\begin{aligned} P_F'(m) &\ll d(1+\log m^{1/d})(p+1) \\ &\ll d(1+\log m^{1/d})(1+m^{2/d}|D(F)|^{-1/d(d-1)}) . \end{aligned}$$

Let u satisfy $2^{du} \le m < 2^{d(u+1)}$. Then

$$P_F(m) \le P_F(2^{du}) + P_F'(m) .$$

Now

$$\begin{aligned} P_F(2^{du}) &= \sum_{i=0}^{u} P_F'(2^{di}) \\ &\ll \sum_{i=0}^{u} d(1+\log 2^i)(1+2^{2i}|D(F)|^{-1/d(d-1)}) \\ &\le d(1+\log 2^u)\sum_{i=0}^{u} 1 + 2^{2u}|D(F)|^{-1/d(d-1)}2^{2(i-u)} \\ &\ll d(1+\log 2^u)\Big(u + 2^{2u}|D(F)|^{-1/d(d-1)}\sum_{j=0}^{\infty} 2^{-2j}\Big) \\ &\ll d(1+\log m^{1/d})(\log m^{1/d} + m^{2/d}|D(F)|^{-1/d(d-1)}) . \end{aligned}$$

If $|F(tx,ty)| \le m$ where (x,y) is primitive, then $|F(x,y)| \le mt^{-d}$ since F is homogeneous of degree d. This yields

$$\begin{aligned} &N_F(m) \\ &\quad \le \sum_{t \le m^{1/d}} P_F(mt^{-d}) \\ &\quad \ll \sum_{t \le m^{1/d}} d(1+\log(m^{1/d}t^{-1}))(\log(m^{1/d}t^{-1}) + m^{2/d}t^{-2}|D(F)|^{-1/d(d-1)}) \\ &\quad \le d(1+\log m^{1/d}) \sum_{t \le m^{1/d}} \log(m^{1/d}t^{-1}) + t^{-2}m^{2/d}|D(F)|^{-1/d(d-1)} . \end{aligned}$$

Finally, we have

$$\sum_{t \le m^{1/d}} \log(m^{1/d}t^{-1}) \ll 1 + \int_1^{m^{1/d}} \log(m^{1/d}t^{-1})\, dt \ll m^{1/d}$$

and

$$\sum_{t \le m^{1/d}} t^{-2} \ll 1 .$$

This completes the proof of Lemma 2.

Using $d = 3$ and $|D(F)| \ge m^{1/22}$ in Lemma 2 gives

$$\begin{aligned} N_F(m) &\ll (1 + \log m)(m^{1/3} + m^{2/3} m^{-1/132}) \\ &\ll 1 + m^{2/3-1/132} \log m = 1 + m^{29/44} \log m \,. \end{aligned}$$

By (2) we also have

$$m^{2/3} A_F \ll m^{2/3} |D(F)|^{-1/6} \le m^{29/44} \,.$$

These last two inequalities complete the proof of Theorem 1.

References

[B1] M. Bean, *Areas of plane regions defined by binary forms*, Ph.D. thesis, University of Waterloo, 1992.

[B2] —, *Bounds for the number of solutions of the Thue equation*, M. thesis, University of Waterloo, 1988.

[E] J. H. Evertse, *Estimates for reduced binary forms*, J. Reine Angew. Math. 434 (1993), 159–190.

[EG] J. H. Evertse and K. Győry, *Effective finiteness results for binary forms*, Compositio Math. 79 (1991), 169–204.

[M1] K. Mahler, *Zur Approximation algebraischer Zahlen III*, Acta Math. 62 (1934), 91–166.

[M2] —, *An inequality for the discriminant of a polynomial*, Michigan Math. J. 11 (1969), 257–262.

[S] W. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lecture Notes in Math. 1467, Springer, New York, 1991.

[T] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. 135 (1909), 284–305.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF COLORADO
CAMPUS BOX 395
BOULDER, COLORADO 80309
U.S.A.
E-mail: JTHUNDER@BOULDER.COLORADO.EDU

Received on 26.6.1993 (2452)