Available online at www.sciencedirect.com

ScienceDirect

C. R. Acad. Sci. Paris, Ser. I 347 (2009) 715–718

COMPTES RENDUS MATHEMATIQUE

Number Theory

Integer points on cubic Thue equations ☆

Cameron L. Stewart

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

Received 3 February 2009; accepted after revision 20 April 2009

Available online 14 May 2009

Presented by Jean-Pierre Serre

Abstract

We prove that there are infinitely many inequivalent cubic binary forms F with content 1 for which the Thue equation $F(x, y) = m$ has $\gg (\log m)^{6/7}$ solutions in integers x and y for infinitely many integers m. ***To cite this article: C.L. Stewart, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***
© 2009 Published by Elsevier Masson SAS on behalf of Académie des sciences.

Résumé

Points entiers sur les équations cubiques de Thue. Nous démontrons qu'il existe une infinité de formes binaires cubiques F avec contenu 1 qui sont inéquivalentes et pour lesquelles l'équation de Thue $F(x, y) = m$ a $\gg (\log m)^{6/7}$ a des solutions entiers x et y pour une infinité d'entiers m. ***Pour citer cet article : C.L. Stewart, C. R. Acad. Sci. Paris, Ser. I 347 (2009).***
© 2009 Published by Elsevier Masson SAS on behalf of Académie des sciences.

Let $F(x, y) = a_n x^n + a_{n-1}x^{n-1}y + \cdots + a_0 y^n$ be a binary form with integer coefficients, $n \geqslant 3$ and non-zero discriminant. Let m be a non-zero integer. The equation

$$F(x, y) = m, \tag{1}$$

in integers x and y is known as a Thue equation and it has only finitely many solutions. This was first established by Thue [9] in 1909 in the case that F is irreducible over the rationals. Consider also the Thue inequality

$$\left|F(x, y)\right| \leqslant m, \tag{2}$$

for m a positive integer. Let A_F denote the area of the set of points (x, y) in $\mathbb{R}^2$ for which (2) holds when $m = 1$. In 1935 Mahler [3] proved that the number of solutions of (2) in integers x and y is asymptotic to $A_F m^{2/n}$ as m tends to infinity. Thus for most integers m, Eq. (1) has no solution.

☆ This research was supported in part by the Canada Research Chairs Program and by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

E-mail address: cstewart@uwaterloo.ca.

1631-073X/$ – see front matter © 2009 Published by Elsevier Masson SAS on behalf of Académie des sciences.
doi:10.1016/j.crma.2009.04.018

Let $N_F(m)$ denote the number of solutions of (1) in integers x and y. Chowla [1], in 1933, building on earlier work of Mordell and Pillai, proved that there is a positive number c_0 such that if k is a non-zero integer and $F(x,y) = x^3 - ky^3$ then

$$N_F(m) > c_0 \log\log m,$$

for infinitely many positive integers m. In 1935 Mahler [4] proved that for each cubic form F, with non-zero discriminant, there is a positive number c_1, which depends on F, such that

$$N_F(m) > c_1(\log m)^{1/4}, \tag{3}$$

for infinitely many positive integers m. In 1983 Silverman [7] replaced the exponent $1/4$ by $1/3$ in (3) and recently Stewart [8] showed one may replace the exponent $1/4$ in (3) by $1/2$. In addition, Silverman [7] showed that there are infinitely many cubic forms F with integer coefficients and non-zero discriminant for which (3) holds with an exponent of $2/3$ in place of $1/4$. He deduced both results from the following theorem:

Silverman's Theorem. *Let F be a cubic binary form with integer coefficients and non-zero discriminant. Let m_0 be a non-zero integer such that the curve $E: F(x,y) = m_0 z^3$ has a point defined over $\mathbb{Q}$. Using that point as origin, we give E the structure of an elliptic curve. Let r be the rank of the Mordell–Weil group of $E/\mathbb{Q}$. Then there is a positive number c_2, which depends on F, such that*

$$N_F(m) > c_2(\log m)^{r/(r+2)},$$

for infinitely many positive integers m.

With Liverance [2] we showed, by means of Silverman's Theorem, that there are cubic forms with non-zero discriminant for which (3) holds with $6/7$ in place of $1/4$. In this note we shall show that we may adapt our argument to prove that there are infinitely many inequivalent forms with this property. We shall now discuss the notion of equivalence of forms which is appropriate in this context.

Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, with a, b, c and d integers. Let F be a binary form with integer coefficients, degree $n (\geqslant 2)$ and non-zero discriminant $D(F)$. We define the binary form F_A by

$$F_A(x,y) = F(ax+by, cx+dy).$$

We remark that

$$D(F_A) = (\det A)^{n(n-1)} D(F). \tag{4}$$

Further, for any non-zero integer t we have

$$D(tF) = t^{2(n-1)} D(F). \tag{5}$$

Notice that if A is in $GL(2,\mathbb{Z})$, so that A has integer entries and determinant ± 1, and (x,y) is a solution of (1) in integers then $A(x,y) = (ax+by, cx+dy)$ is a solution of

$$F_{A^{-1}}(X,Y) = m$$

in integers X and Y. Further, if F has integer coefficients and a non-zero discriminant then $F_{A^{-1}}$ also has integer coefficients and a non-zero discriminant. In particular, by (4),

$$D(F) = D(F_{A^{-1}}). \tag{6}$$

For any A in $GL(2,\mathbb{Z})$ we say that F_A and $-F_A$ are equivalent to F. Observe that the number of solutions of (1) is unchanged if we replace F by F_A or by $-F_A$ when F has odd degree. Furthermore, by (4) and (5), equivalent forms have the same discriminant.

Suppose that F is a binary form with integer coefficients and non-zero discriminant and that k is a non-zero rational number for which kF has integer coefficients. If the discriminant of F is non-zero then so is the discriminant of kF. Furthermore the number of solutions of (1) in integers x and y is the same as the number of solutions of

$$kF(x,y) = km,$$

in integers x and y. Accordingly, when looking for forms F for which the Thue equation (1) has many solutions we may restrict our attention to binary forms F for which the greatest common divisor of the coefficients is 1 or, equivalently, for which the content is 1.

Theorem. *Let r be a positive integer which is the rank of the Mordell–Weil group of rational points of the elliptic curve $E : y^2 = x^3 + D$, with origin the point at infinity, for some non-zero integer D. There exist infinitely many inequivalent cubic binary forms F with integer coefficients, content 1 and non-zero discriminant for which there is a positive number c, which depends on F, such that*

$$N_F(m) > c(\log m)^{r/(r+2)},$$

for infinitely many positive integers m.

Proof. Let $P = (s,t)$ be a rational point on E with $st \neq 0$. We put

$$F(x,y) = x^3 - 3sx^2y - 4Dy^3.$$

Note that the discriminant $\Delta(F)$ of F is $-432Dt^2$. The curve $C : F(x,y) = 1/2t$ is a non-singular cubic curve since $st \neq 0$. Further $Q = (-s/t, -1/2t)$ is a point on C. With Q as the origin, C is an elliptic curve.

Let H and G be the quadratic and cubic covariants of F and recall, Theorem 1 of Chapter 24 of [5], that

$$G^2 = 4H^3 - 27\Delta(F)F^2. \tag{7}$$

In particular, we have

$$(4G)^2 = (4H)^3 + (432t)^2DF^2,$$

where

$$H(x,y) = 9\big(s^2x^2 + 4Dxy - 4sDy^2\big)$$

and

$$G(x,y) = 54\big(\big(s^3 + 2D\big)x^3 - 6sDx^2y + 12s^2Dxy^2 + 8D^2y^3\big).$$

We have $C : F(x,y) = z^3/2t$ and $E : zy^2 = x^3 + Dz^3$ in $\mathbb{P}^2$. Define

$$\lambda : C \to E$$

by

$$\lambda\big([x,y,z]\big) = \big[zH(x,y)/9, G(x,y)/54, z^3\big].$$

Notice that λ is regular at those points $[x,y,z]$ for which either $z \neq 0$ or $G(x,y) \neq 0$. If $z = 0$ and $G(x,y) = 0$ then $F(x,y) = 0$ and, by (7), $H(x,y) = 0$. But the resultant of the binary forms $H(X,Y)/9$ and $F(X,Y)$ is $256D^2(s^3 + D)^2 = 256D^2t^4$ which is non-zero. Therefore λ is a non-constant morphism and so is an isogeny from the elliptic curve C with origin Q to the elliptic curve E with origin $\lambda(Q)$ $(= [s, -t, 1])$. Further, the kernel of any non-zero isogeny between elliptic curves is a finite group. Since λ is defined over $\mathbb{Q}$ the rank of the Mordell–Weil group of rational points of C with origin Q is the same as that of E with origin $\lambda(Q)$. Furthermore, the rank r of the elliptic curve E over $\mathbb{Q}$ does not depend on the choice of rational point for the origin. Therefore the rank of the group of rational points of C with origin Q is r.

Let $s = s_1/s_2$ and $t = t_1/t_2$ with s_1 and s_2 coprime integers with $s_2 > 0$ and t_1 and t_2 defined similarly. Put $b = s_2/(3, s_2)$ and $\tilde{F}(x,y) = bF(x,y)$. Note that $\tilde{F}$ is a cubic binary form with integer coefficients and content 1. Furthermore, recall (5), the discriminant $\Delta(\tilde{F})$ of $\tilde{F}$ is $-432b^4t^2D$. Put $m_0 = (b/2t)(2t_1)^3$ and $C_1 : \tilde{F}(x,y) = m_0z^3$. Note that m_0 is a non-zero integer and C_1 with origin $(-s/t, -1/2t, 1/2t_1)$ is an elliptic curve whose group of rational points has rank r. Thus by Silverman's Theorem there is a positive number c_3, which depends on $\tilde{F}$, such that

$$N_{\tilde{F}}(m) > c_3(\log m)^{r/(r+2)}, \tag{8}$$

for infinitely many positive integers m.

To complete the proof of our theorem it suffices to show that we can find infinitely many inequivalent forms $\tilde{F}$ with content 1 for which (8) holds. To this end we note, by our earlier discussion, that it is enough to prove that we can find forms $\tilde{F}$ with content 1 associated with points on E and with discriminants of arbitrarily large absolute value. In particular it suffices to show that b^4t^2 is unbounded or, equivalently, $s_2^4(t_1/t_2)^2$ is unbounded as we run over rational points (s,t) on E with $s,t \neq 0$. Since $t^2 = s^3 + D$ we see that $s_2^3 = \pm t_2^2$. Thus

$$s_2^4(t_1/t_2)^2 = |s_2|t_1^2 = |t_2|^{2/3}t_1^2,$$

which is unbounded since r is positive and so there are rational points (s,t) on E with t of arbitrarily large height. □

In 1987 Quer [6] investigated quadratic number fields for which the 3-rank of the ideal class group is 6. In this context he found three elliptic curves of the form $y^2 = x^3 + D$ with rank 12 ($D = -6533891544658786928$, -49317122354452517296, -50586546986138596528). Therefore we deduce the following result as a consequence of our main theorem:

Corollary. *There exist infinitely many inequivalent cubic binary forms F with integer coefficients, content* 1 *and non-zero discriminant such that*

$$N_F(m) > c_4(\log m)^{6/7}, \tag{9}$$

for infinitely many positive integers m, where c_4 is a positive number which depends on F.

Since $P = (2109824, 1690470036)$ is a point on $y^2 = x^3 - 6533891544658786928$ we see from the proof of the main theorem that (9) holds with

$$F(x,y) = x^3 - 6329472x^2y + 26135566178635147712y^3.$$

References

[1] S.D. Chowla, Contributions to the analytic theory of numbers (II), J. Indian Math. Soc. 20 (1933) 121–128.

[2] E. Liverance (prepared in collaboration with Cameron Stewart), Binary cubic forms with many integral points, Surikaisekikenkyusho Kokyuroku 998 (1997) 93–101.

[3] K. Mahler, Zur Approximation algebraischer Zahlen III (Über die mittlere Anzahl der Darstellungen grosser Zahlen durch binäre Formen), Acta Math. 62 (1933) 91–166.

[4] K. Mahler, On the lattice points on curves of genus 1, Proc. London Math. Soc. 39 (2) (1935) 431–466.

[5] L.J. Mordell, Diophantine Equations, Academic Press, London and New York, 1969.

[6] J. Quer, Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12, C. R. Acad. Sci. Paris 305 (1987) 215–218.

[7] J.H. Silverman, Integer points on curves of genus 1, J. London Math. Soc. 28 (1983) 1–7.

[8] C.L. Stewart, Cubic Thue equations with many solutions, Internat. Math. Res. Notices (2008) 2008:rnn040-11.

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