Stewart, C. L. (2008) "Cubic Thue Equations with Many Solutions,"
International Mathematics Research Notices, Vol. 2008, Article ID rnn040, 11 pages.
doi:10.1093/imrn/rnn040

Cubic Thue Equations with Many Solutions

Cameron L. Stewart

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

Correspondence to be sent to: cstewart@uwaterloo.ca

We shall prove that if F is a cubic binary form with integer coefficients and nonzero discriminant then there is a positive number c, which depends on F, such that the Thue equation $F(x, y) = m$ has at least $c(\log m)^{1/2}$ solutions in integers x and y for infinitely many positive integers m.

1 Introduction

Let $F(x, y)$ be a binary form with integer coefficients, degree r ($\geq$3), and nonzero discriminant. Let m be a nonzero integer and consider the equation

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

in integers x and y. It has only finitely many solutions as was first established by Thue [18] in 1909 in the case that F is irreducible over $\mathbb{Q}$. There is an extensive literature dealing with the problem of estimating from above the number of solutions to equation (1); see e.g. [1, 11, 14], and [5]. By contrast there are only a few papers which treat the problem of estimating the number of solutions of equation (1) from below. The first substantial result in this context is due to Chowla [2].

Received October 29, 2007; Revised March 26, 2008; Accepted March 28, 2008
Communicated by Prof. Barry Mazur

See http://www.oxfordjournals.org/our_journals/imrp/for proper citation instructions.

In 1933, Chowla proved that there is a positive number c_0 such that if k is a nonzero integer then the number of solutions of $x^3 - ky^3 = m$ in integers x and y is at least $c_0 \log\log m$ for infinitely many positive integers m. This was refined by Mahler [6] in 1935. He proved that there is a positive number c_1, which depends on F, such that for infinitely many positive integers m, equation (1) has at least

$$c_1(\log m)^{1/4} \tag{2}$$

solutions. In 1983, Silverman [10] proved that the exponent of 1/4 in equation (2) can be improved to 1/3. The purpose of this paper is to show that the exponent 1/3 can be further improved to 1/2.

Theorem 1.1. Let F be a cubic binary form with integer coefficients and nonzero discriminant. There is a positive number c, which depends on F, such that the number of solutions of equation (1) in integers x and y is at least

$$c(\log m)^{1/2} \tag{3}$$

for infinitely many positive integers m. □

Theorem 1.1 as well as the estimates of Chowla, Mahler, and Silverman are obtained by viewing equation (1), when it has a rational point, as defining an elliptic curve E and then by constructing, from rational points on E, integers m' for which $F(x, y) = m'$ has many solutions in integers x and y. The solutions (x, y), so constructed, have very large common factors. Silverman formalized this approach by proving the following result.

Silverman's Theorem. Let F be a cubic binary form with nonzero discriminant. Let m_0 be an integer such that the curve E with homogeneous equation

$$E : F(x, y) = m_0 z^3 \tag{4}$$

has a point defined over $\mathbb{Q}$. Using that point as origin, we give E the structure of an elliptic curve. Let r denote the rank of the Mordell–Weil group of rational points of E. There exists a positive number c_2, which depends on F, such that there are infinitely many positive integers m for which the number of solutions of equation (1) in integers x and y is at least

$$c_2(\log m)^{r/(r+2)}.$$ □

Thus, to establish equation (3), it suffices to prove that for each cubic binary form F with integer coefficients and nonzero discriminant, there is an integer m_0 for which the rank of the group of rational points of the curve E, defined by equation (4), is at least 2.

For particular forms, one can often improve on equation (3). For example, Silverman deduced from his result that there is a positive constant c_3 such that for infinitely many positive integers m, the equation

$$x^3 + y^3 = m$$

has at least $c_3(\log m)^{3/5}$ solutions in integers x and y, by exhibiting a twist of $x^3 + y^3 = 1$ of rank at least 3. Stewart [15] found a twist of rank at least 6 and so replaced the exponent of 3/5 by 3/4. Elkies and Rogers [3] have found a twist of rank 11 and so 3/4 may now be improved to 11/13.

Silverman [10] proved that there exist cubic binary forms with integer coefficients and nonzero discriminant for which the number of solutions of equation (1) in integers x and y is at least $c_4(\log m)^{2/3}$ for infinitely many positive integers m. Liverance and Stewart [4] employed elliptic curves of rank 12 found by Quer [9] to show that the exponent of 2/3 can be improved to 6/7. Recently, Stewart [16] has shown that there are infinitely many cubic binary forms with integer coefficients, content 1, and nonzero discriminant which are inequivalent under the action of $GL(2, \mathbb{Z})$ and for which the above estimate applies.

2 Preliminary Results

The strategy which we shall employ to prove that we can find, for each cubic form F of nonzero discriminant, an integer m_0 for which the rank of equation (4) is at least 2 is the one employed by Stewart and Top in [17] to study ranks of twists of elliptic curves. We shall consider the nonsingular cubic curve E_D over $\mathbb{Q}(t)$ given by

$$E_D : F(x, y) = D(t),$$

where D is a polynomial in $\mathbb{Z}[t]$ of positive degree. For each F we shall show that there exists a polynomial D such that E_D together with a $\mathbb{Q}(t)$ point determines an elliptic curve defined over $\mathbb{Q}(t)$, which is not isomorphic over $\mathbb{Q}$ to an elliptic curve defined over $\mathbb{Q}$, and for which the rank of the group of $\mathbb{Q}(t)$ points of E_D is at least 2. We then specialize

t to a rational number t_0 in order to find an appropriate m_0 by means of the following lemma due to Silverman [12].

Lemma 2.1. Let E be an elliptic curve defined over $\mathbb{Q}(t)$ which is not isomorphic over $\mathbb{Q}(t)$ to an elliptic curve defined over $\mathbb{Q}$. Suppose that t_0 is a rational number for which E_{t_0} is an elliptic curve, where E_{t_0} is obtained from E by specializing t to t_0. Let

$$\rho_{t_0} : E(\mathbb{Q}(t)) \to E_{t_0}(\mathbb{Q})$$

be the specialization homomorphism from the group of $\mathbb{Q}(t)$ points of E to the group of rational points of E_{t_0}. ρ_{t_0} is an injective homomorphism for all but finitely many rational numbers t_0. □

Proof. This is a special caseof Theorem C of [12]. ■

Let $D(t)$ be a polynomial with integer coefficients and positive degree and suppose that D is not a perfect cube in $\mathbb{C}[t]$. Let C be a smooth, complete model of the curve given by $s^3 = D(t)$ and let $H^0(C, \Omega^1_{C/\mathbb{Q}})$ denote the vector space of holomorphic differentials on C. Let E be an elliptic curve. We denote the set of morphisms from C to E defined over $\mathbb{Q}$ by $\mathrm{Mor}_{\mathbb{Q}}(C, E)$. $\mathrm{Mor}_{\mathbb{Q}}(C, E)$ is an abelian group where the sum of two morphisms φ_1 and φ_2 is defined to be the morphism which takes x in C to $\varphi_1(x) + \varphi_2(x)$, where $+$ denotes addition in E.

Lemma 2.2. Let $E/\mathbb{Q}$ be an elliptic curve given by an equation $y^2 = x^3 + k$ with k a nonzero integer and let $D \in \mathbb{Z}[t]$ be a nonconstant polynomial which is not a perfect cube in $\mathbb{C}[t]$. Let $C/\mathbb{Q}$ be a smooth, complete model of the curve defined by $s^3 = D(t)$ and let $E_D/\mathbb{Q}(t)$ be defined by $y^2 = x^3 + k(D(t))^2$. For each point $P = (x(t), y(t))$ in $E_D(\mathbb{Q}(t))$, we define an element φ_P of $\mathrm{Mor}_{\mathbb{Q}}(C, E)$ by $\varphi_P(t, s) = (x(t)s^{-2}, y(t)s^{-3})$. The map

$$\lambda : E_D(\mathbb{Q}(t)) \to H^0\left(C, \Omega^1_{C/\mathbb{Q}}\right)$$

given by

$$\lambda(P) = \varphi_P^* \omega_E,$$

where $\varphi_P^* \omega_E$ denotes the pullback via φ_P of the invariant differential ω_E on E, is a homomorphism with a finite kernel. □

Proof. This is part 2 of Proposition 1 of [17]. ■

We shall make use of Lemma 2.2 to calculate lower bounds for the rank of $E_D(\mathbb{Q}(t))$ for various curves $E_D/\mathbb{Q}(t)$. We do so by calculating the rank of the image under λ in the vector space of holomorphic differentials on C of sets of points from $E_D(\mathbb{Q}(t))$.

3 An Initial Simplification

Suppose that $F(x, y) = a_3x^3 + a_2x^2y + a_1xy^2 + a_0y^3$ with a_0, a_1, a_2, a_3 integers and that the discriminant $\Delta(F)$ of F is nonzero. Notice that the set of values with multiplicities assumed by F at integer points (x, y) is unchanged when $F(x, y)$ is replaced by $F(ax + by, cx + dy)$ with a, b, c and d integers for which $ad - bc = 1$. Thus, it is no loss of generality to assume that $a_3 \neq 0$. Next observe that $27a_3^2F(x, y) = F_1(X, y)$, where $X = 3a_3x$ and $F_1(X, y) = X^3 + 3a_2X^2y + 9a_3a_1Xy^2 + 27a_3^2a_0y^3$. Further $F_1(X, y) = F_2(Z, y)$, where $Z = X - a_2y$ and $F_2(Z, y) = Z^3 + (-3a_2^2 + 9a_1a_3)Zy^2 + (2a_2^2 - 9a_1a_2a_3 + 27a_3^2a_0)y^3$. The discriminant of F_2 is $729a_3^2\Delta(F)$ and therefore to establish Theorem 1.1 it is sufficient, by Silverman's Theorem, to prove that whenever F is a cubic form

$$F(x, y) = x^3 + axy^2 + by^3$$

with a and b integers and $4a^3 + 27b^2 \neq 0$, that there is an integer m_0 for which the curve E_{m_0} with

$$E_{m_0} : F(x, y) = m_0$$

together with a specified rational point as the origin is an elliptic curve with rank at least 2. In fact, we shall give an estimate from below for the number of cube-free integers m_0 below a given bound for which E_{m_0} has rank at least 2.

Let U be a binary form with integer coefficients. We let $S(U, x)$ denote the number of cube-free integers t with $|t| \leq x$ for which there exist integers a, b, and z with $z \neq 0$ such that $U(a, b) = tz^3$. We shall make use of the following two results of Stewart and Top [17]. The first is a special case of Theorem 2 of [17] and the second is a consequence of Theorem 1 of [17].

Lemma 3.1. Let U be a binary form with integer coefficients and degree r which is not a constant multiple of a power of a linear form and which is not divisible over $\mathbb{Q}$ by the cube of a nonconstant binary form. There are positive numbers c_5 and c_6, which depend on U, such that if x exceeds c_5, then

$$S(U,x) > \frac{c_6 x^{2/r}}{(\log x)^2}. \tag{5}$$

□

We are able to remove the factor $(\log x)^{-2}$ from the right-hand side of inequality (5), provided that all the irreducible factors of F over $\mathbb{Q}$ have degree at most 7.

Lemma 3.2. Let U be a binary form with integer coefficients and degree r. Suppose that $r \geq 3$, U has a nonzero discriminant, and the largest degree of an irreducible factor of U over $\mathbb{Q}$ is at most 7. Then there are positive numbers c_7 and c_8, which depend on U such that if x exceeds c_7, then

$$S(U,x) > c_8 x^{2/r}.$$

□

4 Counting Twists of Rank at least 2

Let $F(x,y) = x^3 + axy^2 + by^3$ with a and b integers with $4a^3 + 27b^2 \neq 0$. The quadratic covariant $H(x,y)$ of F is

$$H(x,y) = -3ax^2 - 9bxy + a^2y^2$$

and the cubic covariant $G(x,y)$ of F is

$$G(x,y) = -27bx^3 + 18a^2x^2y + 27abxy^2 + (27b^2 + 2a^3)y^3.$$

Furthermore we have (see Chapter 24 of [8]),

$$(4G)^2 = (4H)^3 + 432(4a^3 + 27b^2)F^2. \tag{6}$$

Suppose that $D(t)$ is a polynomial with rational coefficients and let O be a $\mathbb{Q}(t)$ point on

$$E_D : x^3 + axy^2 + by^3 = D(t)z^3.$$

Then E_D together with O as origin is an elliptic curve over $\mathbb{Q}(t)$. Define E'_D by

$$E'_D : zy^2 = x^3 + 432(4a^3 + 27b^2)D(t)^2z^3.$$

Notice, by equation (6), that

$$\psi : E_D \to E'_D$$

when we put

$$\psi([x, y, z]) = [4zH, 4G, z^3]. \tag{7}$$

ψ is certainly regular if $z \neq 0$ or $G \neq 0$. If $z = 0$ and $G = 0$ then $F = 0$ and, by equation (6), $H = 0$. But the resultant of the binary forms H and F is $(4a^3 + 27b^2)^2$ which is nonzero. Therefore ψ is a nonconstant morphism, and so an isogeny from the elliptic curve E_D with origin O to the elliptic curve E'_D with origin $\psi(O)$. The kernel of ψ is a finite group by Corollary 4.9 on page 76 of [13]. Since ψ is defined over $\mathbb{Q}(t)$, the rank of the Mordell–Weil group of $\mathbb{Q}(t)$ points of E_D with origin O is the same as that of E'_D with origin $\psi(O)$. The rank r of E'_D does not depend on the choice of $\mathbb{Q}(t)$ point for the origin. In the proof of our next result, we shall determine a lower bound for the rank of $E_D(\mathbb{Q}(t))$ by determining a lower bound for the rank of $E'_D(\mathbb{Q}(t))$ by means of Lemma 2.2 for three different choices of polynomial $D(t)$.

Theorem 1.1 is a consequence of our next result.

Theorem 4.1. Let $F(xy) = x^3 + axy^2 + by^3$ with a and b integers and $4a^3 + 27b^2 \neq 0$. There exist positive numbers C_1, C_2, C_3, and C_4 such that if T is a real number larger than C_1, then the number of cube-free integers d with $|d| \leq T$ for which the curve given by

$$x^3 + axy^2 + by^3 = d,$$

together with a rational point, determines an elliptic curve of rank at least 2 is at least $C_2T^{1/6}/(\log T)^2$ if $ab \neq 0$, at least $C_3T^{1/6}$ if $a = 0$, and at least $C_4T^{2/9}$ if $b = 0$. □

5 The Proof of Theorem 4.1

For many of the calculations in the proof we have employed the symbolic computation package MAPLE.

We first consider the case when $ab \neq 0$. In this case, we may modify a construction used by Mestre [7] to prove that there are infinitely many elliptic curves over $\mathbb{Q}$ with given modular invariant and rank at least 2.

Put

$$D(t) = -b^3t^{12} - 3b^3t^{10} + (-6b^3 - a^3b)t^8 + (-7b^3 - 2a^3b)t^6 + (-6b^3 - a^3b)t^4 - 3b^3t^2 - b^3,$$

and

$$E_D : x^3 + axy^2 + by^3 = D(t).$$

Notice that

$$P_1 = (-b(t^4 + t^2 + 1), a(t^4 + t^2))$$

and

$$P_2 = (-b(t^4 + t^2 + 1), a(t^2 + 1))$$

are points on E_D. By equation (7), there is a morphism ψ defined over $\mathbb{Q}(t)$ from E_D to the curve E'_D where

$$E'_D : y^2 = x^3 + 432(4a^3 + 27b^2)(D(t))^2.$$

Put $P'_1 = \psi(P_1)$ and $P'_2 = \psi(P_2)$. The invariant differential $\omega_{E'}$ on $E' : y^2 = x^3 + 432(4a^3 + 27b^2)$ is $dx/(2y)$ and so, as in Lemma 2.2,

$$\varphi^*_{P'_1}\omega_{E'} = -\frac{1}{3}ab(2t^3 + t)\frac{dt}{s^2}$$

and

$$\varphi^*_{P'_2}\omega_{E'} = \frac{1}{3}ab(t^5 + 2t^3)\frac{dt}{s^2}.$$

Since $ab \neq 0$, by Lemma 2.2 the $\mathbb{Q}(t)$ rank of E'_D and so of E_D is at least 2. By Lemma 2.1, the rank of $E_{D(t_0)}$ is at least 2 for all but finitely many rationals t_0. Put $U(x, y) = y^{12}D(x/y)$. To determine the number of cube-free integers d with $|d| \leq T$ for which $x^3 + axy^2 + by^3 = d$ has a rational point and defines an elliptic curve whose group of rational points has rank at least 2, it is enough to estimate $S(U, T)$. Our result now follows from Lemma 3.1, since the discriminant of U is $2^{12}a^{24}b^{38}(4a^3 + 27b^2)^6$ which is nonzero.

Next, we consider the case when $b = 0$. Then

$$P_1 = (a(t^2 + a)), (t(t^2 + a) - 1)$$

and

$$P_2 = (a, (t^2 + a)^2 - t)$$

are points on

$$E_D : x^3 + axy^2 = D(t),$$

where

$$D(t) = a^2(t^2 + a)(t^6 + 3at^4 - 2t^3 + 3a^2t^2 - 2at + a^3 + 1).$$

Let E'_D be the curve given by

$$y^2 = x^3 + 1728a^3(D(t))^2.$$

The morphism from E_D to E'_D determined by equation (7) maps P_1 and P_2 to P'_1 and P'_2, respectively. The invariant differential $\omega_{E'}$ on $E' : y^2 = x^3 + 1728a^3$ is $dx/(2y)$, and so we may compute the pullbacks $\varphi^*_{P'_1}\omega_{E'}$ and $\varphi^*_{P'_2}\omega_{E'}$ as in Lemma 2.2. We obtain

$$\varphi^*_{P'_1}\omega_{E'} = \frac{1}{6}a(t^4 + 2at^2 + 2t + a^2)\frac{dt}{s^2}$$

and

$$\varphi^*_{P'_2}\omega_{E'} = \frac{1}{6}a(4t^3 + 4at - 1)\frac{dt}{s^2}.$$

Since $a \neq 0$, it follows from Lemma 2.2 that the $\mathbb{Q}(t)$ rank of E'_D and of E_D is at least 2. As before, we apply Lemma 2.1 to find that the rank of E_D is at least 2 for all but finitely many rationals t_0. Put $U(x, y) = y^9 D(x/y)$. Note that the discriminant of U is $2^8a^{36}(1024a^3 + 729)$ which is nonzero, since a is a nonzero integer. Further, the largest degree of an irreducible factor of U over $\mathbb{Q}$ is at most 6. By Lemma 3.2, $S(U, T) > C_3T^{2/9}$ and the result follows in this case.

Finally, we consider the case when $a = 0$. Put

$$P_1 = (bt^3 + 3bt^2 + 3bt + 9b - 1, bt^4 + 6bt^2 - t + 9b - 3)$$

and

$$P_2 = (bt^3 - 3bt^2 + 3bt - 9b - 1, bt^4 + 6bt^2 - t + 9b + 3).$$

Next, define $D(t)$ by

$$D(t) = (b^2t^6 + 9b^2t^4 - 2bt^3 + 27b^2t^2 + 18bt + 27b^2 + 1) \times (b^2t^6 + 9b^2t^4 + 27b^2t^2 + 27b^2 - 1).$$

Then P_1 and P_2 are points on

$$E_D : x^3 + by^3 = D(t).$$

As before we may map P_1 and P_2 to P_1' and P_2', respectively on E_D', as in equation (7), where

$$E_D' : y^2 = x^3 + 2^4 3^6 b^2 (D(t))^2.$$

Let $E' : y^2 = x^3 + 2^4 3^6 b^2$. The invariant differential $\omega_{E'}$ on E' is $dx/(2y)$. Then, as in Lemma 2.2,

$$\varphi^*_{P_1'}\omega_{E'} = \left(\frac{1}{6}b^2t^6 + b^2t^5 + \frac{1}{2}b^2t^4 + \left(6b^2 - \frac{1}{3}b\right)t^3 + \left(-\frac{3}{2}b^2 + 2b\right)t^2 + (9b^2 + b)t - \frac{9}{2}b^2 + \frac{1}{6}\right)\frac{dt}{s^2}$$

and

$$\varphi^*_{P_2'}\omega_{E'} = \left(\frac{1}{6}b^2t^6 - b^2t^5 + \frac{1}{2}b^2t^4 + \left(-6b^2 - \frac{1}{3}b\right)t^3 + \left(-\frac{3}{2}b^2 - 2b\right)t^2 + (-9b^2 + b)t - \frac{9}{2}b^2 + \frac{1}{6}\right)\frac{dt}{s^2}.$$

Since $b \neq 0$, it follows from Lemma 2.2 that the $\mathbb{Q}(t)$ rank of E_D' and of E_D is at least 2. We apply Lemma 2.1 to find that the rank of E_D is at least 2 for all but finitely many rationals t_0. Put $U(x, y) = y^{12}D(x/y)$. The discriminant of U is $2^{24}3^{39}b^{50}(27b^2 - 1)(8b - 1)^6(8b + 1)^6$ which is nonzero, since b is a nonzero integer. Again, the largest degree of an irreducible factor of U over $\mathbb{Q}$ is at most 6. By Lemma 3.2,

$$S(U, T) > C_4 T^{1/6}$$

and our result follows.

Acknowledgment

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.

References

[1] Bombieri, E., and W. M. Schmidt. "On Thue's equation." *Inventiones Mathematicae* 88 (1987): 69–81.

[2] Chowla, S. "Contributions to the analytic theory of numbers 2." *The Journal of the Indian Mathematical Society* 20 (1933): 120–8.

[3] Elkies, N., and N. F. Rogers. "Elliptic curves $x^3 + y^3 = k$ of high rank." In *Proceedings of ANTS-6*, edited by D. Buell, 184–93, Lecture Notes in Computer Science 3076. Berlin: Springer, 2004.

[4] Liverance, E. "Binary cubic forms with many integral points." *Surikaisekikenkyusho Kokyuroku* 998 (1997): 93–101.

[5] Lorenzini, D., and T. Tucker. "Thue equations and the method of Chabauty–Coleman." *Inventiones Mathematicae* 148 (2002): 47–77.

[6] Mahler, K. "On the lattice points on curves of genus 1." *Proceedings of the London Mathematical Society* 39 (1935): 431–66.

[7] Mestre, J. F. "Rang des courbes elliptiques d'invariante donné." *Comptes Rendus Mathematique Academie des Sciences* 314, no. 1 (1992): 919–22.

[8] Mordell, L. J. *Diophantine Equations.* London: Academic Press, 1969.

[9] Quer, J. "Corps quadratiques de 3-rang 6 et courbes elliptiques de rang 12." *Comptes Rendus Mathematique Academie des Sciences* 305, no. 1 (1987): 215–8.

[10] Silverman, J. H. "Integer points on curves of genus 1." *Journal of the London Mathematical Society.* 28 (1983): 1–7.

[11] Silverman, J. H. "Representation of integers by binary forms and the rank of the Mordell–Weil group." *Inventiones Mathematicae* 74 (1983): 281–92.

[12] Silverman, J. H. "Heights and the specialization map for abelian varieties." *Journal fur die Reine und Angewandte Mathematik* 342 (1983): 197–211.

[13] Silverman, J. H. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 106. New York: Springer, 1986.

[14] Stewart, C. L. "On the number of solutions of polynomial congruences and Thue equations." *Journal of the American Mathematical Society* 4 (1991): 793–835.

[15] Stewart, C. L. "Thue equations and elliptic curves." *Canadian Mathematical Society Conference Proceedings* 15 (1995): 375–86.

[16] Stewart, C. L. "Integer points on cubic Thue equations." (forthcoming).

[17] Stewart, C. L., and J. Top. "On ranks of twists of elliptic curves and power-free values of binary forms." *Journal of the American Mathematical Society* 8 (1995): 943–73.

[18] Thue, A. "Über Annäherungswerte algebraischer Zahlen." *Journal fur die Reine und Angewandte Mathematik* 135 (1909): 284–305.