THUE EQUATIONS AND ELLIPTIC CURVES

C. L. STEWART

Abstract. We discuss estimates for the number of solutions of Thue equations and for the number of twists of elliptic curves over the rationals with rank at least 2. We indicate some of the connections between these problems.

1. THUE EQUATIONS

Let F be a binary form with rational integer coefficients and with $r \geq 3$. Let h be a non-zero integer. In 1909, Thue [43] proved that if F is irreducible then the equation

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

has only finitely many solutions in integers x and y. Equation (1) is known as Thue's equation and the problem of estimating the number of solutions of (1) has a rich history, see for example Siegel [34], Mahler [20], Erdős and Mahler [8], Davenport and Roth [6] and Lewis and Mahler [19]. Let $N_F(h)$ denote the number of pairs of integers (x, y) for which (1) holds. Chowla [5], in 1933, refuted a conjecture of Siegel by proving that there is a positive number C_1 such that if k is a non-zero integer and $F(x, y) = x^3 - ky^3$ then equation (1) has at least $C_1 \log\log|h|$ solutions in integers x and y for infinitely many integers h. Mahler, in 1935 [22], strengthened Chowla's argument to show that if F is a cubic form with non-zero discriminant then there is a positive number C_2 such that equation (1) has at least $C_2(\log|h|)^{1/4}$ solutions for infinitely many integers h. In 1983, Silverman [36] was able to improve Mahler's estimate of $C_2(\log|h|)^{1/4}$ to $C_3(\log|h|)^{1/3}$. Silverman noted that if h_0 is a non-zero integer for which the curve E given by the equation $F(x, y) = h_0$ has a rational point then E may be given the structure of an elliptic curve. Let r be the rank of the Mordell-Weil group of E over $\mathbb{Q}$. Silverman [36], by exploiting the theory of height functions, was able to prove that

$$N_F(h) > C_4(\log|h|)^{r/r+2}\ , \tag{2}$$

for infinitely many integers h. In 1951, Selmer [32] proved that the rank over $\mathbb{Q}$ of the elliptic curve given by the equation $x^3 + y^3 = 657$ is 3. Using this fact, Silverman deduced from (2) that if $F(x, y) = x^3 + y^3$ then

$$N_F(h) > C_5(\log|h|)^{3/5}\ , tag3 \tag{1}$$

for infinitely many integers h. The constructions of Chowla, Mahler and Silverman produce solutions (x, y) of (1) for which the greatest common divisor of x and y is large. They do not yield primitive solutions, that is, solutions with x and y coprime.

1991 *Mathematics Subject Classification.* 1991 Mathematics Subject Classification. Primary 11D25, 11D41, 11G05; Secondary 11N36.

The author's research was supported in part by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

For any integer h let $\omega(h)$ denote the number of distinct prime factors of h. In 1933, Mahler [20] proved that if F is irreducible then (1) has at most $C_6^{1+\omega(h)}$ primitive solutions where C_6 depends on F only. A half-century later Evertse [10] proved that if F has non-zero discriminant D then the number of primitive solutions of (1) is at most

$$2 \cdot 7^{r^3} \ , \tag{4}$$

This resolved a conjecture of Siegel since the bound does not depend on the coefficients of F. In 1987 Bombieri and Schmidt [2] refined this result for F irreducible over $\mathbb{Q}$ when they replaced the upper bound (4) with

$$C_7 r^{1+w(h)} \ , \tag{5}$$

where C_7 is an absolute constant. They proved that C_7 may be taken to be 430 for r sufficiently large. Further, Bombieri and Schmidt showed that the Thue equation may have at least r distinct primitive solutions. They gave the example

$$F(x,y) = x^r + a(x-y)(2x-y)\cdots(rx-y) \ ,$$

where a is a non-zero integer. Then $(1,1),(1,2),\ldots,(1,r)$ are primitive solutions of
$F(x,y) = 1$. In 1991, [41], we proved that the number of primitive solutions of (1) is at most

$$4r^{\omega(h)} \ ,$$

for h sufficiently large. For the proof, we reduced the problem to the study of S-unit equations and then applied estimates of Evertse, Győry, Stewart and Tijdeman [12] on the number of solutions of such equations. Also [41], by means of an argument which depends on the Thue-Siegel principle, we recovered the estimate (5) of Bombieri and Schmidt for the number of solutions of (1) with $C_7 = 2800$ under the less restrictive assumption that F has a non-zero discriminant. This is a consequence of the following result.

For any non-zero integer n and prime number p let $\mathrm{ord}_p n$ denote the exact power of p that divides n. For any real number x let $[x]$ denote the greatest integer less than or equal to x. Let p be a prime number and let r, k and D be integers with $r \geq 2$ and $D \neq 0$. We define $T = T(r,k,p,D)$ by

$$T = \min\left(\left[\left(\frac{r-1}{r}\right)k\right], \min_{j=0,\ldots,r-2}\left(\left[\frac{\mathrm{ord}_p D}{(j+1)(j+2)} + \left(\frac{j}{j+2}\right)k\right]\right)\right)$$

and for any non-zero integer g we define $G(g,r,D)$ by

$$G(g,r,D) = \prod_{p|g} p^{T(r,\ \mathrm{ord}_p g, p, D)} \ .$$

Notice that if $\mathrm{ord}_p g = 1$ then $\left[\left(\frac{r-1}{r}\right)\right] = 0$. Therefore $G(g,r,D) = 1$ whenever g is squarefree. Similarly if $\mathrm{ord}_p D = 1$ then $\left[\frac{\mathrm{ord}_p D}{(r-1)r}\right] = 0$ and so $G(g,r,D) = 1$ whenever D is squarefree. Further $G(g,r,D) = 1$ whenever g and D are coprime.

Recall that the content of a binary form with integer coefficients is the greatest common divisor of the coefficients of F.

Theorem 1. *Let F be a binary form with integer coefficients of degree $r(\geq 3)$, content 1 and non-zero discriminant D. Let h be a non-zero integer and let ϵ be a positive real number. Let g be any divisor of h with*

$$\frac{g^{1+\epsilon}|D|^{1/r(r-1)}}{G(g,r,D)} \geq |h|^{2/r+\epsilon} \ . \tag{6}$$

The number of pairs of coprime integers (x,y) for which $F(x,y)=h$ is at most

$$2800\left(1+\frac{1}{8\epsilon r}\right)r^{1+\omega(g)} \ . \tag{7}$$

Since

$$T(r,k,p,D) \leq \left[\frac{\mathrm{ord}_p D}{(r-1)r}+\left(\frac{r-2}{r}\right)k\right] \ ,$$

we see that

$$G(|h|,r,D) \leq |h|^{(r-2)/r}|D|^{1/r(r-1)} \ .$$

Therefore (6) is satisfied with $g=|h|$ and ϵ any positive real number and so the number of primitive solutions of (1) is at most 2800 $r^{1+\omega(h)}$ whenever $D(F)$ is non-zero.

Several authors, for instance, Siegel [35], Domar [7] and Evertse and György [11], have given estimates for the number of solutions of Thue equations and Thue inequalities when the discriminant of F is large relative to $|h|$. On taking $g=1$ in Theorem 1 we obtain a result of this type since $G(1,r,D)=1$ and condition (6) becomes

$$|D|^{1/r(r-1)} \geq |h|^{2/r+\epsilon} \ . \tag{8}$$

Thus if (8) holds then the number of solutions of (1) in coprime integers x and y is at most

$$2800\left(1+\frac{1}{8\epsilon r}\right)r \ .$$

In general the optimal choice of g will be different from 1 and $|h|$. Let (D,g^2) denote the greatest common divisor of D and g^2. It is readily checked that

$$G(g,r,D) \leq (D,g^2)^{1/2} \ .$$

Let g be any divisor of h with

$$g \geq |h|^{2/r+\epsilon} \ . \tag{9}$$

Then, since $|D|$ is at least 1, whenever

$$|h| \geq (D,g^2)^{1/\epsilon} \ , \tag{10}$$

(6) holds with ϵ replaced by $\epsilon/2$. Therefore if F is a binary form, as in the statement of Theorem 1, and (9) and (10) hold, then the number of solutions of (1) in coprime integers x and y is at most

$$2800\left(1+\frac{1}{4\epsilon r}\right)r^{1+\omega(g)} \ . \tag{11}$$

This result sharpens a result of Erdős and Mahler. In 1938, they proved [8] that there exist positive numbers C_8 and C_9, which depend on F, such that if g is a divisor of h with $g > h^{6/7}$ and $h > C_8$ then the number of primitive solutions of (1) is at most $C_9^{1+w(g)}$. The most significant aspect of estimate (11) is the fact that the term $w(h)$ of previous estimates has been replaced with $w(g)$. Provided that

$\epsilon < (r-2)/r$ condition (9) is satisfied with g a prime for a positive proportion of the positive integers h and in this case the upper bound (11) has the form $C(\epsilon)r^2$. By contrast, for almost all integers h, in the sense of natural asymptotic density, and any $\delta > 0$, $w(h) = \log\log h + 0((\log\log h)^{1/2+\delta})$.

Let s be the number of non-zero coefficients of F. Mueller and Schmidt [28] and Schmidt [31] have given upper bounds for the number of primitive solutions of (1) that depend on s and h only. The special case when $s = 2$ has been intensively studied by Siegel [35], Evertse [9] and others. As a final remark, we note that Silverman [37] proved that the number of primitive solutions of (1) is at most

$$r^{2r^2}(8r^3)^{R_F(h)},$$

where $R_F(h)$ is the rank of the Mordell-Weil group of the Jacobian of the curve (1) over $\mathbb{Q}$, provided that the discriminant of F is non-zero and that h is r-powerfree and sufficiently large relative to F.

2. RANKS OF ELLIPTIC CURVES

Let E be an elliptic curve over $\mathbb{Q}$ with Weiertrass equation $y^2 = x^3 + ax + b$, with $a, b, \epsilon\, \mathbb{Q}$ and $4a^3 + 27b^2 \neq 0$. The set of rational points on E together with the point at infinity can be endowed with a group structure in a natural way by the chord and tangent process. This group, denoted $E(\mathbb{Q})$, is abelian and is isomorphic to the direct product of a finite group and r copies of $\mathbb{Z}$; r is known as the rank of E. By a result of Mazur [24], [25], all 15 possible torsion groups are known. The rank is less well understood. In 1954 Néron [29] proved that there are infinitely many elliptic curves over $\mathbb{Q}$ with rank at least 11. In 1991 Mestre [26] improved 11 to 12. Recently Fermigier [13] produced an example over $\mathbb{Q}$ with rank at least 19. It is not known if there is a curve of rank at least 20 but there is a widely held belief that there exist curves of arbitrarily large rank. Computational work suggests that curves of rank 0 and 1 predominate. Brumer [3] has recently proved, subject to the Birch and Swinnerton-Dyer conjecture, the Shimura-Taniyama-Weil conjecture and the Riemann hypothesis for the L-function of elliptic curve, that the average rank of an elliptic curve, ordered accordingly to its Faltings height, is at most 2.3.

How does the rank vary as we run over twists of a given elliptic curve E? That is, we restrict our attention to families of curves defined over $\mathbb{Q}$ which are isomorphic over $\mathbb{C}$. There are families of quadratic cubic, quartic and sextic twists, see Proposition 5.4 of [39]. Let d be a non-zero integer and let E_d denote the quadratic twist of E given by the equation $dy^2 = x^3 + ax + b$. Let $r(d)$ denote the rank of E_d. Goldfeld [14] conjectured in 1979 that the average value of $r(d)$ is $1/2$. In 1960 Honda [17] conjectured that the rank of any twist of a given elliptic curve E over $\mathbb{Q}$ is bounded by a constant which depends on E only.

Those twists with rank at least 2 are interesting and expected to be somewhat uncommon. Can one show that there are in fact quite a few of them? The first theoretical results in this context were due to Gouvêa and Mazur [15] in 1991. Let $\epsilon > 0$. Under the assumption of the parity conjecture, they proved that there are positive numbers C_{10} and C_{11}, which depend on ϵ and E, such that for any positive integer T larger that C_{10} the number of square-free integers d with $|d| \leq T$ for which the rank of E_d is at least 2 is at least $C_{11}T^{1/2-\epsilon}$. Mai [23] extended this work to cubic twists of $x^3 + y^3 = 1$. Let $\epsilon > 0$. He proved, subject to the parity conjecture for cubic twists (see §4), that there are positive numbers C_{12} and C_{13},

which depend on ϵ, such that for any T larger than C_{12} the number of cube-free d with $|d| \leq T$ for which the rank of $x^3 + y^3 = d$ is at least 2 is at least $C_{13}T^{2/3-\epsilon}$.

Recently [42], Top and I have given unconditional analogues of the above results. Let E denote the elliptic curve $y^2 = x^3 + ax + b$ with $ab \neq 0$. We proved that there exist positive numbers C_{14} and C_{15}, which depend on E, such that if T exceeds C_{14} then the number of square-free integers d with $|d| \leq T$ for which the rank of $dy^2 = x^3 + ax + b$ is at least 2 is at least $C_{15}T^{1/7}/(\log T)^2$. We also gave several families of curves for which stronger results applied. For example, let t be a rational number different from -1, 0 and 1 and put $u = ((t^2+1)/2t)^2$. We showed that there exist positive numbers C_{16} and C_{17}, which depend on t, such that if T is a real number larger than C_{16} then the number of square-free integers d with $|d| \leq T$ for which the curve given by

$$dy^2 = x(x-1)(x-a) \ ,$$

has rank at least 3 is at least $C_{17}T^{1/6}$. Furthermore we proved that there exist positive numbers C_{18} and C_{19} such that if T is a real number larger than C_{18} then the number of sixth power free integers d with $|d| \leq T$ for which the curve given by

$$y^2 = x^3 + d \ ,$$

has rank at least 6 is at least $C_{19}T^{1/27}/(\log T)^2$.

Let me outline our strategy for proving these results. We work over the function field $\mathbb{Q}(t)$ initially. We search for polynomials H in $\mathbb{Z}[t]$ with non-zero discriminant for which the rank of the group of $\mathbb{Q}(t)$ points of E_H is large where E_H is given by $H(t)y^2 = x^3 + ax + b$. To this end, for several of the families of curves we study, we make use of polynomials found in Mestre [26] Next we appeal to a specialization result of Silverman [38] which tells us that for all but finitely many rationals t_0 the map ρ_{t_0}, where $\rho_{t_0} : E_H(\mathbb{Q}(t)) \to E_{H(t_0)}(\mathbb{Q})$ by sending a point $(x(t), y(t))$ to $(x(t_0), y(t_0))$, is an injective homomorphism. Thus, if the rank over $\mathbb{Q}(t)$ is large then the rank of the specialization over $\mathbb{Q}$ is also large, for all but finitely many rationals t_0. We then need to establish how many different twists we get from this process. For the case of quadratic twists we have to determine how many different square-free integers d with $|d| \leq T$ have the property that $H(a/b) = dz^2$ for some non-zero integers a and b and some rational number z. Equivalently we consider the binary form H_0 with $H_0(a, b) = b^m H(a/b)$ where m is the smallest even integer greater than or equal to the degree of H. Since we assume that H is in $\mathbb{Z}[t]$ and that d is square-free, it suffices to estimate the number of square-free integers d of the form $H_0(a, b)$.

3. POWER-FREE VALUES OF BINARY FORMS

Let k be an integer with $k \geq 2$. We say that an integer n is k-free if it is not divisible by the k-th power of prime. Let f be a polynomial with integer coefficients and degree $r \geq 2$. Suppose that f is primitive and irreducible. In 1933, Ricci [30] proved that if $k \geq r$ then the number of positive integers n, with n at most x, for which $f(n)$ is k-free is asymptotic to $C_{20}x$, where C_{20} is a positive number which depends on f and k. In 1966 Hooley [18] obtained the analogue of Ricci's result when $k = r - 1$ subject to the additional necessary assumption that there is no prime p for which p^{r-1} divides $f(n)$ for all integers n. What happens in the situation when we replace the polynomial f by a binary form F?

Let F be a binary form of degree r with integer coefficients and non-zero discriminant D. We write

$$F(x,y) = a_r x^r + a_{r-1}x^{r-1}y + \cdots + a_0 y^r \ . \tag{12}$$

We shall introduce three counting functions associated with F for each integer k with $k \geq 2$. Let w be the largest positive integer such that w^k divides $F(a,b)$ for all integers a and b. For any real number x let $P_k(x)$ denote the number of pairs of integers (a,b) with $1 \leq a \leq x$ and $1 \leq b \leq x$ for which $F(a,b)/w^k$ is k-free. Further for any real number x, let $R_k(x)$ denote the number of k-free integers t with $|t| \leq x$ for which there are integers a and b with $F(a,b) = tw^k$ and let $S_k(x)$ denote the number of k-free integers t with $|t| \leq x$ for which there exist integers a, b and z with z non-zero and $F(a,b) = tz^k$. Notice that

$$S_k(x) \geq R_k(x) \ , \tag{13}$$

and that for our estimates for the number of twists we require a lower bound for $S_k(x)$.

Let m denote the largest degree of an irreducible factor of F over $\mathbb{Q}$. Suppose that $w = 1$ and that $m \leq 3$. Gouvêa and Mazur [15] were able to modify Hooley's sieving argument in order to prove that in this case $P_2(x)$ is asymptotic to $C_{21}x^2$, where C_{21} is a positive number which depends on F. One year later, Greaves [16] employed Selberg's sieve and Gallagher's larger sieve to prove that if $a_r a_0 \neq 0$ and $w = 1$ then $P_k(x)$ is asymptotic to $C_{22}x^2$, where C_{22} is a positive number which depends on F and k, provided that m is at most 6 when k is 2 and m is at most $2k+1$ otherwise. In [42], Top and I noted that a straightforward modification of the argument of Greaves allowed one to remove the restriction that $w = 1$. Combining this argument with our estimate (11) for the number of solutions of the Thue equation we proved the following result.

Theorem 2. *Let k be an integer with $k \geq 2$ Let F be a binary form with integer coefficients, non-zero discriminant and degree r with $r \geq 3$. Let m be the largest degree of an irreducible factor of F over $\mathbb{Q}$ and suppose that $m \leq 2k+1$ or that $k = 2$ and $m = 6$. There are positive numbers C_{23} and C_{24}, which depend on k and F, such that if x is a real number larger than C_{23} then*

$$R_k(x) > C_{24}x^{2/r} \ . \tag{13}$$

Up to the determination of C_{24}, estimate (14) is best possible by virtue of a result of Mahler [**?**]. Erdős and Mahler [8], in 1938, used estimates for the number of solutions of the Thue equation in a similar fashion. Let F be a binary form, as in (12), with integer coefficients, non-vanishing discriminant, degree $r \geq 3$ and with $a_r a_0 \neq 0$. They proved that the number of integers t with $|t| \leq x$ for which there exist integers a and b with $F(a,b) = t$ is at least $C_{25}x^{2/r}$ for x sufficiently large where C_{25} is a positive number which depends on F.

We remark that Gouvêa and Mazur made use of their estimate for $P_2(x)$ to deduce a lower bound for $R_2(x)$ in the special case where $F(x,y) = y(x^3 + axy^2 + by^3)$, with a and b integers for which $4a^3 + 27b^2 \neq 0$. Let $\epsilon > 0$. They proved that there exist positive numbers C_{26} and C_{27}, which depend on a, b and ϵ, such that if x exceeds C_{26} then

$$R_2(x) > C_{27}x^{1/2-\epsilon} \ .$$

In order to apply the parity conjecture for quadratic twists, Gouvêa and Mazur needed to estimate the number of square-free values assumed by $F(x,y)$ below a given bound with additional congruence restrictions on x and y. It is possible to impose such restrictions for all the estimates for $P_k(x), R_k(x)$ and $S_k(x)$ referred to in this section but we have not bothered to do so in order to simplify the exposition.

There are several instances in [42] where the restrictions on m in Theorem 2 are too severe for the theorem to be applicable to the problem of estimating the number of twists below a given bound. In these situations we appeal to the following estimate for $S_k(x)$ which is weaker than the estimate obtained from Theorem 2 and (13) but which applies more generally.

Theorem 3. *Let k be an integer with $k \geq 2$. Let F 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 k-th power of a non-constant binary form. There are positive numbers C_{28} and C_{29}, which depend on F, such that if x is a real number larger than C_{28} then*

$$S_k(x) > C_{29} x^{2/r}/(\log x)^2 \ .$$

A key feature of the proof of Theorem 3 is an appeal to the Chebotarev density theorem.

4. CUBIC TWISTS OF $x^3 + y^3 = 1$

The family of curves E_d

$$x^3 + y^3 = d \ ,$$

with d a cube-free positive integer, is the family of cubic twists of the elliptic curve $x^3 + y^3 = 1$ and it has been much studied. In 1951, Selmer [32] [33], building on work of Cassels [4], determined the rank and generators of the Mordell-Weil group of E_d for all d up to 500. These tables were extended by Stephens [40] in 1968. In 1987 Zagier and Kramaz [44] computed the values of $L_d(1)$ and $L_d^{'}(1)$ where $L_d(s)$ is the L-series of the curve E_d for d up to 20,000. They found that for 8,320 of the cube-free positive integers d, in this range $L_d(s)$ has a root number of -1, or equivalently a factor of -1 in its functional equation. Of these 8,320 integers d, 179 also have $L_d^{'}(1) = 0$ whence, by the Birch and Swinnerton-Dyer conjecture, the rank of E_d is odd and at least 3.

In [42] Top and I proved that there are positive numbers C_{30}, C_{31} and C_{32} such that if T is a real number larger than C_{30} then the number of cube-free integers d with $|d| \leq T$ for which E_d has rank at least 2 is at least $C_{31} T^{1/3}$ and for which E_d has rank at least 3 is at least $C_{32} T^{1/6}$.

In 1966 Birch and Stephens [1] gave the following explicit version of the parity conjecture for cubic twists.

Parity conjecture for cubic twists. *Let d be a cube-free integer and let E_d be the elliptic curve given by $x^3 + y^3 = d$. Let $r(d)$ denote the rank of E_d. We have*

$$(-1)^{r(d)} = -w_3 \prod_{p \neq 2} w_p \ ,$$

where

$$w_3 = -1 \ \textit{if} \ d \equiv \pm 1, \pm 3 \pmod 9, \ w_3 = 1 \ \textit{otherwise},$$

and

$$w_p = -1 \ if \ p|d \ and \ p \equiv 2 \pmod 3, w_p = 1 \ otherwise.$$

Recall that Mai [23] had assumed this conjecture in order to estimate the number of twists E_d of rank at least 2. If we assume the above parity conjecture we are able to show that there are positive numbers C_{33} and C_{34} such that if T exceeds C_{33} then the number of cube-free integers d with $|d| \leq T$ for which E_d has rank at least 4 is at least $C_{34}T^{1/6}$.

We shall now indicate briefly how we produce cubic twists of rank at least 3. It turns out to be more convenient to work with the family $E_d^{'}$ where $E_d^{'}$ is the curve given by the equation

$$xy(x+y) = d \ . \tag{14}$$

We remark that the rank of $E_d^{'}$ is the same as the rank of E_d. Of course we can also view (15) as a Thue equation and in [41] we proved that there are infinitely many integers d for which the Thue equation (15) has at least 18 solutions in coprime integers x and y. We established in [42] that the elliptic curve defined over the function field $\mathbb{Q}(t)$ by the equation

$$xy(x+y) = (t^6-1)(t^6-9) \tag{15}$$

has $\mathbb{Q}(t)$ rank at least 3. In particular, P_1, P_2 and P_3 are in dependent points on (16) where

$$P_1 = \left(-t^2(t^3-1), \frac{3+t^3}{t}\right) \ , P_2 = \left(\frac{t^3-3}{t}, \ t^2(1+t^3)\right) \text{ and}$$

$P_3 = \left(4, \frac{t^6-9}{2}\right)$. Putting $t = a/b$ and multiplying by b^{12} we see that it suffices to count the number of cube-free integers d with $|d| \leq T$ for which $F(a,b) = d$ where

$$F(X,Y) = (X^6 - Y^6)(X^6 - 9Y^6) \ .$$

We then apply Theorem 2 to obtain our result.

We claim that if we take $t = 11$ in (16) we obtain a twist of $xy(x+y) = 1$ of rank at least 6. We may transform (16) into the Weierstrass form

$$Y^2 = X^3 + 16d^2 \ ,$$

by putting $X = 4y(x+y)$ and $Y = 4y(x+y)(x+2y)$. For $t = 11$ we find that $d = (11^6-1)(11^6-9) = 2^8 \cdot 3^2 \cdot 5 \cdot 7 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 83$ and so it suffices to prove that the rank of

$$Y^2 = X^3 + (2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 83)^2 \tag{16}$$

is at least 6. Consider the points $P_1 = [286769980, 4856306226310]$, $P_2 = [91402920, 874200377610]$, $P_3 = [7628364, 32327735238]$, $P_4 = [-7971984, 9722830986]$, $P_5 = [142000965, 1692320167215]$ and $P_6 = [18190125, 81362973915]$ on (16). We used Apecs on Maple V to check that the Grammian height-pairing determinant for $P_1, \ldots, P_6$ is 22870.45105 ... and so the rank of (16) is at least 6. On combining this information with Silverman's result (2) we deduce the next result, which improves upon (3).

Theorem 4. *There exists a positive number C_{35} such that for infinitely many integers h the equation*

$$x^3 + y^3 = h \ ,$$

has at least

$$C_{35}(\log h)^{3/4}$$

solutions in integers x and y.

References

[1] B. J. Birch and N. Stephens, *The parity of the rank of Mordell-Weil group*, Topology, 5 (1966), pp. 295–299.

[2] E. Bombieri and W. M. Schmidt, *On Thue's equation*, Invent Math. 88 (1987), pp. 69–81.

[3] A. Brumer, *The average rank of elliptic curves I*, Invent. Math., 109 (1992), pp. 445–472.

[4] J. W. S. Cassels, *The rational solutions of the Diophantine equation $Y^2 = X^3 - D$*, Acta. Math. 82 (1950), pp. 244–273.

[5] S. D. Chowla, *Contributions to the analytic theory of numbers* (II), J. Indian Math. Soc., 20 (1933), pp. 120–128.

[6] H. Davenport and K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), pp. 160–167.

[7] Y. Domar, *On the diophantine equation $|Ax^n - By^n| = 1, n \geq 5$*, Math. Scand. 2 (1954), pp. 29–32.

[8] P. Erdős and K. Mahler, *On the number of integers which can be represented by a binary form*, J. London Math. Soc., 13 (1938), pp. 134–139.

[9] J. H. Evertse, *On the equation $ax^n - by^n = c$*, Compositio Math. 47 (1982), pp. 289–315.

[10] ———, *On equations in S-units and the Thue-Mahler equation* Invent. Math. 75 (1984), pp. 561–584.

[11] J. H. Evertse and K. Győry, *Thue inequalities with a small number of solutions*, in The Mathematical Heritage of C. F. Gauss, G. R. Rassias, ed. pp. 204–224. World Scientific Publ., Singapore, 1991.

[12] J. H. Evertse, K. Győry, C. L. Stewart and R. Tijdeman, *On S-unit equations in two unknowns*, Invent. Math. 92 (1988), pp. 461–477.

[13] S. Fermigier, *Un exemple de courbe elliptique définie sur $\mathbb{Q}$ de rang ≥ 19*, C.R. Acad. Sci. Paris Sér. I Math. 315 (1992), pp. 719–722.

[14] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory (Proc. Conf. in Carbondale, 1979) (M. B. Nathanson ed.), Lecture Notes in Math. 751 Springer-Verlag, Berlin, New York and Heidelberg, 1979, pp. 108–118.

[15] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc., 4 (1991), pp. 1-23.

[16] G. Greaves, *Power-free values of binary forms*, Quart. J. Math. Oxford (2), 43 (1992), pp. 45–65.

[17] T. Honda, *Isogenies, rational points and section points of group varieties*, Jap. J. Math. 30 (1960), pp. 84–101.

[18] C. Hooley, *On power-free values of polynomials*, Mathematika, 14 (1967), pp. 21–26.

[19] D. Lewis and K. Mahler, *Representations of integers by binary forms*, Acta. Arith. 6 (1961), pp. 333–363.

[20] K. Mahler, *Zur Approximation algebraischer Zahlen.* II *Über die Anzahl der Darstellungen ganzer Zahlen durch Binärformen*, Math. Ann. 108 (1933), pp. 37–55.

[21] ———, *Zur Approximation algebraischer, III (Über die mittlere Anzahl der Darstellungen groszer Zahlen durch binäre Formen),* Acta Math., 62 (1933), pp. 91–166.

[22] ———, *On the lattice points on curves of genus* 1, Proc. London Math. Soc. (2) 39 (1935), pp. 431–466.

[23] L. Mai, *The analytic rank of a family of elliptic curves*, Can. J. Math., 45 (1993), pp. 847–862.

[24] B. Mazur, *Modular curves and the Eisenstein ideal*, I.H.E.S. Publ. Math. 47 (1977), pp. 33–186.

[25] ———, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), pp. 129–162.

[26] J. -F. Mestre, *Courbes elliptiques de rang ≥ 12 sur $\mathbb{Q}(t)$*, C. R. Acad. Sci. Paris, t. 313, Série I (1991), pp. 171–174.

[27] ———, *Rang de courbes elliptiques d'invariant donné*, C. R. Acad. Sci. Paris, t. 314, Série I (1992), pp. 919–922.
[28] J. Mueller and W. M. Schmidt, *Thue's equation and a conjecture of Siegel*, Acta. Math. 160 (1988), pp. 207–247.
[29] A. Néron, *Propriétés arithmetiques de certaines familles de courbes algebriques*, Proc. Int. Cong. Amsterdam, 1954, vol. III, pp. 481–488.
[30] G. Ricci, *Ricerche aritmetiche sur polinome*, Rend. Circ. Mat. Palermo, 57 (1933), pp. 433–475.
[31] W. M. Schmidt, *Thue equations with few coefficients*, Trans. Amer. Math. Soc. 303 (1987), pp. 241–255.
[32] E. S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta. Math. 85 (1951), pp. 203–362.
[33] ———, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$. *Completion of the tables*, Acta. Math. 92 (1954), pp. 191–197.
[34] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. preuss. Akad. Wiss. Phys. Math. Kl. (1929) No. 1.
[35] ———, *Die Gleichung* $ax^n - by^n = c$, Math. Ann. 114 (1937), pp. 57–68.
[36] J. H. Silverman, *Integer points on curves of genus* 1, J. London Math. Soc. (2) 28 (1983), pp. 1–7.
[37] ———, *Representation of integers by binary forms and the rank of the Mordell-Weil group*, Invent. Math. 74 (1983), pp. 281–292.
[38] ———, *Heights and the specialization map for families of abelian varieties*, J. reine u. angew. Math., 342 (1983), pp. 197–211.
[39] ———, *The arithmetic of elliptic curves*. Springer-Verlag, Berlin, New York and Heidelberg, 1985. Graduate Texts in Math.
[40] N. M. Stephens, *The diophantine equation* $X^3 + Y^3 = DZ^3$ *and the conjectures of Birch and Swinnerton-Dyer*, J. reine u. angew. Math., 231 (1968), pp. 121–162.
[41] C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc., 4 (1991), pp. 793–835.
[42] C. L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc., to appear.
[43] A. Thue, *Über Annäherungswerte algebraischer Zahler*, J. reine angew. Math. 135 (1909), pp. 284–305.
[44] D. Zagier and G. Kramarz, *Numerical investigations related to the L-series of certain elliptic curves*, J. Indian Math. Soc., 52 (1987), pp. 51–69.

C. L. Stewart
Department of Pure Mathematics
The University of Waterloo
Waterloo, Ontario
Canada N2L 3G1
email address: cstewart@watserv1.uwaterloo.ca