H. SHABANI-SOLT AND A. S. JANFADA
KODAI MATH. J.
41 (2018), 160–166

A LOWER BOUND FOR THE NUMBER OF INTEGRAL SOLUTIONS OF MORDELL EQUATION

Hassan Shabani-Solt and Ali S. Janfada

Abstract

For a nonzero integer d, a celebrated Siegel Theorem says that the number $N(d)$ of integral solutions of Mordell equation $y^2 + x^3 = d$ is finite. We find a lower bound for $N(d)$, showing that the number of solutions of Mordell equation increases dramatically. We also prove that for any positive integer n, there is an integer square multiply represented by Mordell equations, i.e., $k^2 = y_1^2 + x_1^3 = y_2^2 + x_2^3 = \cdots = y_n^2 + x_n^3$.

1. Introduction

Given an integer d, if the Diophantine equation $d = f(x_1, x_2, \dots, x_n)$ has integral (resp. rational) solutions then d is said to have integral (resp. rational) representation of the form f. We are interested on the integral representation of the form $y^2 + x^3$. Equivalently, we study the integral solutions of the so-called Mordell equation $y^2 + x^3 = d$. A well known result of Siegel [5, Theorem 12.11.2] says that the number of solutions of Mordell equation is finite.

Today, computer packages find all the integral solutions of equations $y^2 + x^3 = d$ provided d lies within reasonable bounds. An important, simple, natural question still remains unsolved is: *What is the best theoretical bound* (*in terms of d*) *for the size of the largest integer x solving* $y^2 + x^3 = d$ *in integers*? The truth is that the best known bound is far from what seems likely to be true. What seems likely to be true is the subject of the following conjecture made by Hall [7].

Conjecture 1 (Hall). *Given* $\varepsilon > 0$, *there is a constant* $c = c(\varepsilon)$ *such that, for any nonzero* $d \in \mathbf{Z}$, *any integral solution of* $y^2 + x^3 = d$ *satisfies*

$$\log|x| < (2 + \varepsilon) \log|d| + c.$$

Bennett [1] found an upper bound using cubic forms.

2010 *Mathematics Subject Classification*. Primary 11D41; Secondary 11G05.
Key words and phrases. Diophantine equation, elliptic curve, Mordell equation, taxicab number.
Received February 27, 2017; revised April 6, 2017.

Proposition 2. *If d is a nonzero integer, then the equation*

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

has at most $10h_3(-108d)$ solutions in integers x and y, where $h_3(-108d)$ is the class number of binary cubic forms of discriminant d.

Define

$$N(d) = \#\{(x, y) \in \mathbf{Z} \times \mathbf{Z} : y^2 + x^3 = d\}.$$

Silverman [12, Exercise 9.3] shows that $N(d)$ can be arbitrarily large. More precisely, using height function and by a demonstration not so easy, he shows that there is an absolute constant $c > 0$ such that $N(d) > c(\log|d|)^{1/3}$. In the next main result, using binary forms, we find a lower bound for $N(d)$ showing that the number of solutions of Mordell equation increases dramatically.

Theorem 3. *Consider $y^2 + x^3 = d$. Then there is an absolute constant $c > 0$ such that*

$$N(d) > c(\log|d|)^{11/13}$$

for infinitely many integers d.

To prove this result we need to show that some integer squares are multiply represented by Mordell equations.

Theorem 4. *Given any positive integer n, there is an integer k such that k^2 has multiple integral representations in Mordell equations.*

$$k^2 = y_1^2 + x_1^3 = y_2^2 + x_2^3 = \cdots = y_n^2 + x_n^3.$$

The following corollary immediately follows.

Corollary 5. *For any positive integer n, the Diophantine equations*

$$k^2 = y_1^2 + x_1^3 = y_2^2 + x_2^3 = \cdots = y_n^2 + x_n^3$$

have infinitely many integral solutions.

Corollary 5 can also be proved by elliptic curve method.

2. Preliminaries

The so-called super-Fermat equation is the equation $\alpha x^p + \beta y^q + \gamma z^r = 0$ for given nonzero integers α, β, γ and integral exponents p, q and r, all greater than or equal to 2. The two cases $z^2 \pm y^2 = x^r$ with $\gcd(y, z) = 1$, called Dihedral cases, are studied in details in [5, Section 14.2]. A particular case is the following.

Proposition 6. *The parametric solutions of the equation $k^2 = y^2 + x^3$ are:*

$$(k, y, x) = (s(s^2 + 3t^2), t(t^2 + 3s^2), (s - t)(s + t)), \quad s \not\equiv t \bmod 2, \quad \textit{or}$$

$$(k, y, x) = (\pm(2s^3 + t^3), 2s^3 - t^3, 2ts), \quad \textit{where } 2|t.$$

In each case, s and t are coprime.

The problem of representing integral or rational numbers by sums of squares is completely understood [4, Section 5.4.4]. However, the same problem for cubes is complicated and far from being understood [4, Proposition 6.4.29] (originally proved in [8, Theorem 235]).

Proposition 7. *Up to permutation of the variables, the equation*

$$u^3 + v^3 = w^3 + z^3 \tag{1}$$

in **Q** *has the trivial parametrization $v = -u$, $z = -w$, and the parametrization*

$$\begin{aligned} u &= -d((a - 3b)(a^2 + 3b^2) + 1), \\ v &= d((a + 3b)(a^2 + 3b^2) + 1), \\ w &= d((a^2 + 3b^2)^2 + (a + 3b)), \\ z &= -d((a^2 + 3b^2)^2 + (a - 3b)), \end{aligned}$$

with a, b, and d in **Q** *and $d \neq 0$.*

Remark 1. Clearly, taking (1) in **Z** makes the parameters a, b, and d to be also in **Z**, and the equation (1) has infinitely many integral solutions.

An unsystematic question arisen from the Fermat's last theorem is about equal sums of like powers [9, 10] which study the equation

$$\sum_{i=1}^{m} u_i^k = \sum_{j=1}^{n} v_j^k, \quad m, k > 0.$$

A special case is to solve the Diophantine equations $u_1^r + v_1^r = u_2^r + v_2^r$, $r \geq 3$, the common form of the equation (1). More general question in this circumstance is that if the equations

$$u_1^r + v_1^r = u_2^r + v_2^r = \cdots = u_n^r + v_n^r$$

is soluble for given r, n both ≥ 2. The case $r = 2$ is straightforward. For $r = 3$ the answer is also affirmative [8, Theorem 412].

Theorem 8. *Whatever n, there are numbers which are representable as sums of positive cubes in at least n different ways, i.e.*

$$u_1^3 + v_1^3 = u_2^3 + v_2^3 = \cdots = u_n^3 + v_n^3, \quad u_i, v_i \in \mathbf{Q}. \tag{2}$$

Strategy of the proof. In the first step, in [8, Section 13.7], it is proved that the equation

$$u_1^3 + v_1^3 = u_2^3 + v_2^3,$$

has solutions. Then, in the second step, the proof is professionally continued by induction on n. We will apply this strategy in the proof of Proposition 11. □

Let $F(x, y) \in \mathbf{Z}[x, y]$ be a binary form of degree $r \geq 3$ with nonzero discriminant. For any nonzero integer d, the equation

$$F(x, y) = d \tag{3}$$

is known as Thue equation. The next result [5, Theorem 12.11.1] says that Thue equation has finite solutions.

Theorem 9. *Let F be an irreducible, homogeneous, binary integral form of degree $r \geq 3$, and let d be a nonzero integer. The the equation*

$$F(x, y) = d, \quad \text{with } x, y \in \mathbf{Z},$$

has only finitely many solutions, and all of them can be effectively determined.

Define

$$N_F(d, r) = \#\{(x, y) \in \mathbf{Z} \times \mathbf{Z} : F(x, y) = d\},$$

where $F(x, y) = d$ is Thue equation. Theorem 9 shows that $N_F(d, r)$ is finite. There is an extensive literature dealing with the problem of estimating upper bounds for $N_F(d, r)$, see e.g. [2, 14, 17].

By contrast there are only a few works which treat the problem of estimating the lower bounds for $N_F(d, r)$ [3, 11, 15]. The estimates in these references are obtained by viewing (3), when it has a rational point, as defining an elliptic curve E and then by constructing, from rational points on E, integers d' for which $F(x, y) = d'$ 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 [16].

Theorem 10. *Let F be a cubic binary form with non-zero discriminant. Let d_0 be an integer such that the curve E with homogeneous equation*

$$E : F(x, y) = d_0 z^3$$

has a point defined over $\mathbf{Q}$. Using that point as origin, we give E the structure of an elliptic curve. Let ρ denote the rank of the Mordell-Weil group of rational points of E. There exists a positive number c, depending on F, such that there are infinitely many positive integers d for which

$$N_F(d, 3) \geq c(\log d)^{\rho/(\rho+2)}.$$

3. Proof of the main results

We prove the main theorem 4 in the general case $n \geq 2$ by parametrization method.

Proof of Theorem 4. We need the next result.

Proposition 11. *For an even integer* ℓ *let*

$$\ell = 2k = u_1^3 + v_1^3 = u_2^3 + v_2^3 = \cdots = u_n^3 + v_n^3, \quad u_i, v_i \in \mathbf{Z}. \tag{4}$$

Then there are pairs of integers (x_i, y_i), *for* $1 \leq i \leq n$, *such that*

$$k^2 = y_1^2 + x_1^3 = y_2^2 + x_2^3 = \cdots = y_n^2 + x_n^3. \tag{5}$$

Proof. Put $u_i = s_i + t_i$ and $v_i = s_i - t_i$. This parametrization turns (4) to

$$k = s_1(s_1^2 + 3t_1^2) = s_2(s_2^2 + 3t_2^2) = \cdots = s_n(s_n^2 + 3t_n^2), \quad t_i, s_i \in \mathbf{Z}.$$

Appealing to Proposition 6 one sees that for any i with $1 \leq i \leq n$,

$$(k, y_i, x_i) = (s_i(s_i^2 + 3t_i^2), t_i(t_i^2 + 3s_i^2), (s_i - t_i)(s_i + t_i))$$

is a solution for $k^2 = y_i^2 + x_i^3$. This completes the proof. □

We continue the proof of Theorem 4. By Proposition 7 and Remark 1 the equation

$$u^3 + v^3 = w^3 + x^3$$

has infinitely many integral solutions. It follows that for infinitely many "suitable choices" of the parameters a, b, and d in Proposition 7, we may have infinitely many integral solutions for

$$\ell = 2k = u_1^3 + v_1^3 = u_2^3 + v_2^3.$$

By the second step of the quoted strategy of the proof of Theorem 8, such a solution induces a solution for the equations

$$\ell = 2k = u_1^3 + v_1^3 = u_2^3 + v_2^3 = \cdots = u_n^3 + v_n^3, \quad u_i, v_i \in \mathbf{Z}.$$

Now by Proposition 11 the result follows. □

Proof of Theorem 3. It suffices to prove the result for integer squares. Let $\ell = 2k$ be any even integer. Put $F(X, Y) = X^3 + Y^3$. Then, by Theorem 9, the number $q = N_F(\ell, 3)$ of solutions of the equation $F(X, Y) = \ell$ is finite. Suppose that the solutions are u_i, v_i, $1 \leq i \leq q$.

$$\ell = 2k = u_1^3 + v_1^3 = u_2^3 + v_2^3 = \cdots = u_q^3 + v_q^3. \tag{6}$$

By Proposition 11, it follows that k^2 has the following representations.

$$k^2 = y_1^2 + x_1^3 = y_2^2 + x_2^3 = \cdots = y_q^2 + x_q^3. \tag{7}$$

This shows that each solution of (6) gives a solution for (7). Hence

$$N(k^2) \geq N_F(\ell, 3) = N_F(2k, 3). \tag{8}$$

On the other hand, Elkies and Rogers [6] constructs an elliptic curve $F(X, Y) = X^3 + Y^3 = m$ of rank $\rho = 11$. Now apply Theorem 10 for $d_0 = m$, $z = 1$ to claim the existence of a positive number c_1, depending on F, such that there are infinitely many positive integers k (in practice $2k$) for which

$$N_F(2k, 3) \geq c_1(\log 2k)^{11/13} \tag{9}$$

The relations (8) and (9) together gives

$$N(k^2) > c_1(\log 2k)^{11/13} > c_1(\log k)^{11/13} = \frac{c_1}{2^{11/13}}(\log k^2)^{11/13}.$$

The result now follows if we put $d = k^2$ and $c = \dfrac{c_1}{2^{11/13}}$. □

4. Closing comment

We showed that the Diophantine equation

$$k^2 = y_1^2 + x_1^3 = y_2^2 + x_2^3 = \cdots = y_n^2 + x_n^3$$

has infinitely many integral solution. These equations correspond to the equations

$$2k = u_1^3 + v_1^3 = u_2^3 + v_2^3 = \cdots = u_q^3 + v_q^3.$$

A natural question posed is: *Among the solutions, is there any smallest one*? To explain the problem exactly, following [13] we recall the definition of taxicab and cabtaxi number.

Definition. The taxicab (resp. cabtaxi) number is the smallest positive number expressible as the sum of two positive (resp. nonzero) cubes in two different ways. More precisely, taxicab(n) (resp. cabtaxi(n)) is the smallest positive number expressible as the sum of two positive (resp. nonzero) cubes in n different ways. Note that taxicab(2) (resp. cabtaxi(2)) is nothing but the taxicab (resp. cabtaxi) number.

For example,

$$\text{taxicab}(2) = 1729 = 1^3 + 12^3 = 9^3 + 10^3,$$

$$\text{cabtaxi}(2) = 91 = 3^3 + 4^3 = 6^3 + (-5)^3.$$

Till 2011, taxicab(n) for $2 \leq n \leq 6$ and cabtaxi(n), for $2 \leq n \leq 10$ had been calculated and an upper bound for taxicab(n) for $7 \leq n \leq 22$ and cabtaxi(n), for $11 \leq n \leq 42$ had been found. For more details see "New Upper Bounds for Taxicab and Cabtaxi Numbers" in http://www.christianboyer.com/taxicab/.

PROBLEM 1. Given a positive integer n, find the smallest positive integer m such that the Diophantine equation $m = y_1^2 + x_1^3 = y_2^2 + x_2^3 = \cdots = y_n^2 + x_n^3$ has positive integral solutions.

REFERENCES

[1] M. A. BENNETT, On the representation of unity by binary cubic forms, Trans. Amer. Math. Soc. **353** (2000), 1507–1534.

[2] E. BOMBIERI, AND W. M. SCHMIDT, On Thue's equation, Invent. Math. **88** (1987), 69–81.

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

[4] H. COHEN, Number theory **1**: Tools and Diophantine equations, Springer, 2007.

[5] H. COHEN, Number theory **2**: Analytic and modern tools, Springer, 2007.

[6] N. D. ELKIES AND N. F. ROGERS, Elliptic curves $x^3 + y^3 = k$ of high rank, Algorithmic number theory, Lecture notes in computer science **3076**, 2004, 184–193.

[7] M. HALL JR., The Diophantine equation $x^3 - y^2 = k$, Computers in number theory, Proc. sci. res. council atlas sympos. No. 2, Oxford, 1969, Academic Press, London, 1971, 173–198.

[8] G. H. HARDY AND E. M. WRIGHT, An introduction to theory of numbers, 4th edition, Oxford university press, 1960.

[9] R. L. KEL, New results in equal sums of like powers, Math. Comp. **67** (1998), 1309–1315.

[10] L. J. LANDER, T. R. PARKIN, AND J. L. SELFRIDGE, A survey of equal sums of like powers, Math. Comp. **21** (1967), 446–459.

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

[12] J. H. SILVERMAN, The arithmetic of elliptic curves, Springer, 2009.

[13] J. H. SILVERMAN, Taxicabs and sums of two cubes, Expanded version of talks at M.I.T and Brown university, 1993, 331–340.

[14] J. H. SILVERMAN, Representation of integers by binary forms and the rank of the Mordell-Weil group, Invent. Math. **74** (1983) 281–292.

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

[16] C. L. STEWART, Cubic Thue Equations with Many Solutions, Int. Math. Res. Notices, (2008) doi:10.1093/imrn/rnn040.

[17] C. L. STEWART, On the number of solutions of polynomial congruences and Thue equations, J. Amer. Math. Soc. **4** (1991), 793–835.

Hassan Shabani-Solt
DEPARTMENT OF MATHEMATICS
URMIA UNIVERSITY
URMIA 57561-51818
IRAN
E-mail: h.shabani.solt@gmail.com

Ali S. Janfada
DEPARTMENT OF MATHEMATICS
URMIA UNIVERSITY
URMIA 57561-51818
IRAN
E-mail: asjanfada@gmail.com
a.sjanfada@urmia.ac.ir