Czechoslovak Mathematical Journal

Yanfeng He; Wenpeng Zhang

An elliptic curve having large integral points

Czechoslovak Mathematical Journal, Vol. 60 (2010), No. 4, 1101–1107

Persistent URL: http://dml.cz/dmlcz/140809

Terms of use:

© Institute of Mathematics AS CR, 2010

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

AN ELLIPTIC CURVE HAVING LARGE INTEGRAL POINTS

Yanfeng He, and Wenpeng Zhang, Xi'an

(Received July 6, 2009)

Abstract. The main purpose of this paper is to prove that the elliptic curve $E\colon\ y^2 = x^3 + 27x - 62$ has only the integral points $(x, y) = (2, 0)$ and $(28844402, \pm 154914585540)$, using elementary number theory methods and some known results on quadratic and quartic Diophantine equations.

Keywords: elliptic curve, integral point, Diophantine equation

MSC 2010: 11D25

1. Introduction

In recent years, the determination of integral points on elliptic curves is an interesting problem in number theory and arithmetic algebraic geometry. Many advanced methods have been developed to solve this problem (see [1]–[3]). In this paper, another approach to the subject is proposed.

In [4] D. Zagier proposed whether the largest integral point of the elliptic curve

$$E\colon\ y^2 = x^3 + 27x - 62 \tag{1}$$

is $(x, y) = (28844402, \pm 154914585540)$. In this paper, all the integral points of formula (1) are determined as following, using elementary number theory methods and some known results on quadratic and quartic Diophantine equations.

Theorem. *Equation* (1) *has only the integral points* $(x, y) = (2, 0)$ *and* $(28844402, \pm 154914585540)$.

This work is supported by the N.S.F. (10671155) of P. R. China

2. Some lemmas

Let $\mathbb{N}^+$ be the set of all positive integers. Let D be a nonsquare positive integer. It is a well known fact that the equation

$$u^2 - Dv^2 = 1, \quad u, v \in \mathbb{N}^+ \tag{2}$$

has solutions (u, v), and it has exactly one solution (u_1, v_1) such that $u_1 + v_1\sqrt{D} \leqslant u + v\sqrt{D}$, where (u, v) runs through all solutions of (2). Such (u_1, v_1) is called the least solution of (2).

Lemma 1. *Let D_1 and D_2 be coprime positive integers with $D_1 > 1$. If the equation*

$$D_1U^2 - D_2V^2 = 1, \quad U, V \in \mathbb{N}^+ \tag{3}$$

has solutions (U, V), then it has exactly one solution (U_1, V_1) with

$$U_1\sqrt{D_1} + V_1\sqrt{D_2} \leqslant U\sqrt{D_1} + V\sqrt{D_2},$$

where (U, V) runs through all solutions of (3). Such (U_1, V_1) is called the least solution of (3). Moreover, for any solution (U, V) of (3), we have $U_1 \mid U$ and $V_1 \mid V$.

Proof. See reference [5]. □

Lemma 2. *The equation*

$$X^2 - DY^4 = 1, \quad X, Y \in \mathbb{N}^+ \tag{4}$$

has at most two solutions (X, Y). Moreover, if (4) has exactly two solutions, then either $D \in \{1785, 28560\}$ or $2u_1$ and v_1 are both squares, where (u_1, v_1) is the least solution of (2).

Proof. See reference [6]. □

Obviously, the following lemma can be deduced immediately.

Lemma 3. *If $2 \mid D$ and $D \neq 28560$, then (4) has at most one solution (X, Y).*

3. Proof of the theorem

In this section, the theorem is proved.

Let (x, y) be an integral point of (1). Obviously, (1) has only the integral point $(x, y) = (2, 0)$ with $y = 0$. Henceforth, we may assume that $y \neq 0$. Let

$$z = x - 2. \tag{5}$$

Substituting (5) into (1), we get

$$y^2 = z(z^2 + 6z + 39). \tag{6}$$

Since $y^2 > 0$ and $z^2 + 6z + 39 = (z + 3)^2 + 30 > 0$, we have $z > 0$. Let $d = \gcd(z, z^2 + 6z + 39)$. Then we have $d \mid 39$, $d \in \{1, 3, 13, 39\}$ and

$$z = da^2, \quad z^2 + 6z + 39 = db^2, \quad y = \pm dab, \quad a, b \in \mathbb{N}^+, \quad \gcd(a, b) = 1 \tag{7}$$

acording to (6).

If $d = 1$, then according to (7), we obtain

$$a^4 + 6a^2 + 39 = b^2. \tag{8}$$

However, since

$$a^4 + 6a^2 + 39 \equiv \begin{cases} 7 \pmod 8 & \text{if } 2 \mid a, \\ 2 \pmod 4 & \text{if } 2 \nmid a, \end{cases} \tag{9}$$

and

$$b^2 \equiv \begin{cases} 1 \pmod 8 & \text{if } 2 \mid a, \\ 0 \pmod 4 & \text{if } 2 \nmid a, \end{cases} \tag{10}$$

(8) is impossible.

If $d = 3$, then we have

$$3a^4 + 6a^2 + 13 = b^2. \tag{11}$$

However, since

$$3a^4 + 6a^2 + 13 \equiv \begin{cases} 5 \pmod 8 & \text{if } 2 \mid a, \\ 2 \pmod 4 & \text{if } 2 \nmid a, \end{cases} \tag{12}$$

and

$$b^2 \equiv \begin{cases} 1 \pmod 8 & \text{if } 2 \mid a, \\ 0 \pmod 4 & \text{if } 2 \nmid a, \end{cases} \tag{13}$$

(11) is impossible.

If $d = 13$, then we have

$$13a^4 + 6a^2 + 3 = b^2. \tag{14}$$

However, since

$$13a^4 + 6a^2 + 3 \equiv \begin{cases} 3 \pmod 8 & \text{if } 2 \mid a, \\ 2 \pmod 4 & \text{if } 2 \nmid a, \end{cases} \tag{15}$$

and

$$b^2 \equiv \begin{cases} 1 \pmod 8 & \text{if } 2 \mid a, \\ 0 \pmod 4 & \text{if } 2 \nmid a, \end{cases} \tag{16}$$

(14) is impossible.

If $d = 39$, then we have

$$39a^4 + 6a^2 + 1 = b^2.$$

Hence,

$$(3a^2 + 1)^2 + 30a^4 = b^2. \tag{17}$$

Since $3 \nmid 3a^2 + 1$, we see that $3 \nmid b$ according to (17). Furthermore, since $b^2 - (3a^2 + 1)^2 \not\equiv 2 \pmod 4$, (17) is false when $2 \nmid a$. Therefore, we have

$$a = 2c, \quad c \in \mathbb{N}^+. \tag{18}$$

Substituting (18) into (17), we obtain

$$b^2 - (12c^2 + 1)^2 = 480c^4. \tag{19}$$

Furthermore, since $\gcd(2c, b) = 1$ according to (18), we have $\gcd(b + (12c^2 + 1), b - (12c^2 + 1)) = 2$. Therefore, from (19), we obtain

$$\begin{gathered} b + (12c^2 + 1) = 2rf^4, \quad b - (12c^2 + 1) = 2sg^4, \quad c = fg, \\ f, g, r, s \in \mathbb{N}^+, \quad \gcd(f, g) = \gcd(r, s) = 1, \quad rs = 120. \end{gathered} \tag{20}$$

Hence, we get

$$rf^4 - 12f^2g^2 - sg^4 = 1 \tag{21}$$

and

$$(r,s) = (120,1),\ (40,3),\ (24,5),\ (15,8),\ (8,15),\ (5,24),\ (3,40),\ \text{or } (1,120). \tag{22}$$

The eight cases in (22) are discussed separately as following.

Case 1. $(r,s) = (120,1)$

According to (21), we obtain $120f^4 - 12f^2g^2 - g^4 = 1$. However, it is impossible for $3 \nmid g^4 + 1$.

Case 2. $(r,s) = (40,3)$

According to (21), we have $52f^4 - 3(2f^2 + g^2)^2 = 1$. It obtains that the equation

$$13U^2 - 3V^2 = 1, \quad U, V \in \mathbb{N}^+ \tag{23}$$

has the solution $(U,V) = (2f^2, 2f^2 + g^2)$. However, since $2 \nmid g$ and the least solution of (23) is $(U_1, V_1) = (1,2)$, according to Lemma 1, we obtain $2 \mid 2f^2 + g^2$, a contradiction.

Case 3. $(r,s) = (24,5)$

According to (21), we have

$$24f^4 - 12f^2g^2 - 5g^4 = 1, \tag{24}$$

whence we obtain $2 \nmid g$ and

$$24f^4 - 12f^2g^2 \equiv 0 \pmod 4; \quad 5g^4 + 1 \equiv 2 \pmod 4, \tag{25}$$

which contradicts (24).

Case 4. $(r,s) = (15,8)$

According to (21), we have

$$15f^4 - 12f^2g^2 - 8g^4 = 1, \tag{26}$$

whence we obtain $2 \nmid f$ and

$$12f^2g^2 + 8g^4 \equiv 0 \pmod 4; \quad 15f^4 - 1 \equiv 2 \pmod 4, \tag{27}$$

which contradics (26).

Case 5. $(r,s)=(8,15)$

According to (21), we have

$$8f^4-12f^2g^2-15g^4=1, \tag{28}$$

whence we obtain $3\nmid f$ and

$$12f^2g^2+15g^4\equiv 0 \pmod 3; \quad 8f^4-1\equiv 1 \pmod 3, \tag{29}$$

which contradicts (28).

Case 6. $(r,s)=(5,24)$

According to (21),we have

$$5f^4-12f^2g^2-24g^4=1, \tag{30}$$

whence we obtain $3\nmid f$ and

$$12f^2g^2+24g^4\equiv 0 \pmod 3; \quad 5f^4-1\equiv 1 \pmod 3, \tag{31}$$

which contradicts (30).

Case 7. $(r,s)=(3,40)$

According to (21), we have

$$3f^4-12f^2g^2-40g^4=1, \tag{32}$$

whence we obtain $3\nmid g$ and

$$3f^4-12f^2g^2\equiv 0 \pmod 3); \quad 40g^4+1\equiv 2 \pmod 3, \tag{33}$$

which contradicts (32).

Case 8. $(r,s)=(1,120)$

According to (21), we have $f^4-12f^2g^2-120g^4=1$, whence we obtain

$$(f^2-6g^2)^2-156g^4=1, \tag{34}$$

that is the equation

$$X^2-156Y^4=1, \quad X,Y\in\mathbb{N}^+ \tag{35}$$

has the solution

$$(X,Y)=(|f^2-6g^2|,g). \tag{36}$$

On the other hand, since $1249^2 - 156 \cdot 10^4 = 1$, (35) has only the solution $(X, Y) = (1249, 10)$ according to Lemma 3. Therefore, $f = 43$ and $g = 10$ according to (36). Furthermore, it can be obtained that $(x, y) = (2884402, \pm 15491585540)$ according to (5), (7), (18), and (20). Hence, the theorem is proved that the elliptic curve E: $y^2 = x^3 + 27x - 62$ has only the integral points $(x, y) = (2, 0)$ and $(28844402, \pm 154914585540)$.

Acknowledgement. The authors express their gratitude to the referee for his very helpful and detailed comments improving this paper.

References

[1] *A. Baker*: The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$. J. Lond. Math. Soc. *43* (1968), 1–9.

[2] *R. J. Stroeker, N. Tzanakis*: On the elliptic logarithm method for elliptic Diophantine equations: reflections and an improvement. Exp. Math. *8* (1999), 135–149.

[3] *R. J. Stroeker, N. Tzanakis*: Computing all integer solutions of a genus 1 equation. Math. Comput. *72* (2003), 1917–1933.

[4] *D. Zagier*: Large integral points on elliptic curves. Math. Comput. *48* (1987), 425–436.

[5] *D. T. Walker*: On the Diophantine equation $mx^2 - ny^2 = \pm 1$. Am. Math. Mon. *74* (1967), 504–513.

[6] *G. Walsh*: A note on a theorem of Ljunggren and the Diophantine equations $x^2 - kxy^2 + y^4 = 1, 4$. Arch. Math. *73* (1999), 119–125.

Authors' addresses: Y. He, Department of Mathematics, Northwest University, Xi'an, Shaanxi, 710069, P. R. China, and College of Mathematics and Computer Science, Yan'an University, Yan'an, Shaanxi, 716000, P. R. China, e-mail: ydheyanfeng@gmail.com; Wenpeng Zhang, Department of Mathematics, Northwest University, Xi'an, Shaanxi, 710069, P. R. China, e-mail: wpzhang@nwu.edu.cn.