Hai Yang; Ruiqin Fu

The integral points on elliptic curves $y^2 = x^3 + (36n^2 - 9)x - 2(36n^2 - 5)$

Czechoslovak Mathematical Journal, Vol. 63 (2013), No. 2, 375–383

Persistent URL: http://dml.cz/dmlcz/143318

THE INTEGRAL POINTS ON ELLIPTIC CURVES $y^2 = x^3 + (36n^2 - 9)x - 2(36n^2 - 5)$

Hai Yang, Ruiqin Fu, Xi'an

(Received November 7, 2011)

Abstract. Let n be a positive odd integer. In this paper, combining some properties of quadratic and quartic diophantine equations with elementary analysis, we prove that if $n > 1$ and both $6n^2 - 1$ and $12n^2 + 1$ are odd primes, then the general elliptic curve $y^2 = x^3 + (36n^2 - 9)x - 2(36n^2 - 5)$ has only the integral point $(x, y) = (2, 0)$. By this result we can get that the above elliptic curve has only the trivial integral point for $n = 3, 13, 17$ etc. Thus it can be seen that the elliptic curve $y^2 = x^3 + 27x - 62$ really is an unusual elliptic curve which has large integral points.

Keywords: elliptic curve, integral point, quadratic diophantine equation

MSC 2010: 11D25, 14G05

§1. Introduction

In recent years, the determination of integral points on elliptic curves has been an interesting problem in number theory and arithmetic algebraic geometry, and many advanced methods have been used to solve this problem (see [1], [5], [6]).

In [10], D. Zagier asked whether the largest integral point on the elliptic curve

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

is

$$(x, y) = (28844402, \pm 154914585540). \tag{2}$$

This work is supported by N. S. F. (11226038, 11101323) of P. R. China, the Education Department Foundation of Shaanxi Province (11Jk0472, 11Jk0474) and Scientific Research Foundation for Doctor of Xi'an Polytechnic University (BS1016).

Recently, using a computational method related to algebraic number theory and p-adic analysis, H. L. Zhu and J. H. Chen [11] solved the above mentioned problem. They proved that (1) has only the integral points $(x, y) = (2, 0)$ and (2). Y. F. He and W. P. Zhang [2] proved the same result by an elementary approach.

Let n be a positive odd integer. In this paper we discuss a general elliptic curve

$$y^2 = x^3 + (36n^2 - 9)x - 2(36n^2 - 5). \tag{3}$$

Obviously, (1) is the special case of (3) for $n = 1$. Combining some properties of quadratic and quartic Diophantine equations with elementary analysis, we prove the following result:

Theorem. *If $n > 1$, and both $6n^2 - 1$ and $12n^2 + 1$ are odd primes, then* (3) *has only the integral point $(x, y) = (2, 0)$.*

By our result, (3) *has only the trivial integral point for $n = 3, 13, 17$ etc. Thus it can be seen that* (1) *really is an unusual elliptic curve which has large integral points.*

§2. Preliminaries

Let $\mathbb{N}$ be the set of all positive integers. Let D be a positive integer which is not a square.

Lemma 1 ([3, Section 8.1]). *The equation*

$$u^2 - Dv^2 = 1, \quad u, v \in \mathbb{N} \tag{4}$$

has solutions (u, v), and it has a unique solution (u_1, v_1) satisfying $u_1 + v_1\sqrt{D} \leqslant u + v\sqrt{D}$, where (u, v) through all solutions of (4)*. Such (u_1, v_1) is called the least solution of* (4)*. Further, for any positive integer k, let*

$$u_k + v_k\sqrt{D} = \left(u_1 + v_1\sqrt{D}\right)^k. \tag{5}$$

Then $(u, v) = (u_k, v_k)$ $(k = 1, 2, \ldots)$ are all solutions of (1).

Lemma 2. *For any positive integer n, the least solution of the equation*

$$u^2 - 12(12n^2+1)v^2 = 1, \quad u, v \in \mathbb{N} \tag{6}$$

is $(u_1, v_1) = (24n^2+1, 2n)$.

Proof. Since $(24n^2+1)^2 - 12(12n^2+1)(2n)^2 = 1$, (6) has the solution $(u, v) = (24n^2+1, 2n)$. By Lemma 1, if $(u_1, v_1) \neq (24n^2+1, 2n)$, then we have

$$\begin{aligned} 2(24n^2+1) > (24n^2+1) + 2n\sqrt{12(12n^2+1)} \geqslant \bigl(u_1 + v_1\sqrt{12(12n^2+1)}\bigr)^2 \\ > 12(12n^2+1)v_1^2 \geqslant 12(12n^2+1) > 2(24n^2+1), \end{aligned}$$

a contradiction. Thus, we get $(u_1, v_1) = (24n^2+1, 2n)$. Lemma 2 is proved. □

Lemma 3 ([9]). *The equation*

$$X^2 - DY^4 = 1, \quad X, Y \in \mathbb{N} \tag{7}$$

has at most two solutions (X, Y). *Moreover, if* (7) *has exactly two solutions* $(X, Y) = (X_1, Y_1)$ *and* (X_2, Y_2) *with* $X_1 < X_2$, *then we have:*

(i) $D = 1785 \cdot 2^{4r}$, *where* $r \in \{0, 1\}$, $(X_1, Y_1) = (169, 2^{1-r})$ *and* $(X_2, Y_2) = (6525617281, 6214 \cdot 2^{1-r})$.

(ii) $D \neq 1785 \cdot 2^{4r}$, $(X_1, Y_1^2) = (u_1, v_1)$ *and* $(X_2, Y_2^2) = (u_2, v_2)$, *where* (u_j, v_j) $(j = 1, 2)$ *are defined as in* (5).

Lemma 4. *The equation*

$$X^2 - 24Y^4 = 1, \quad X, Y \in \mathbb{N} \tag{8}$$

has only the solution $(X, Y) = (5, 1)$.

Proof. Since the least solution of the equation

$$u^2 - 24v^2 = 1, \quad u, v \in \mathbb{N}$$

is $(u_1, v_1) = (5, 1)$, by (5) we get $(u_2, v_2) = (49, 10)$. Thus, by Lemma 3, (8) has only the solution $(X, Y) = (5, 1)$. Lemma 4 is proved. □

Lemma 5 ([7]). *Let* (X, Y) *be a solution of* (7). *Then there exists a positive integer* k *such that* $(X, Y^2) = (u_k, v_k)$, *where* (u_k, v_k) *if defined as in* (5). *Moreover, if* $2 \mid k$, *then we have:*

(i) $D = 1785 \cdot 2^{4r}$, *where* $r \in \{0, 1\}$, $k = 4$.

(ii) $D \neq 1785 \cdot 2^{4r}$, $k = 2$.

Lemma 6. *If n is a positive odd integer with $n > 1$, then the equation*

$$X^2 - 12(12n^2 + 1)Y^4 = 1, \quad X, Y \in \mathbb{N} \tag{9}$$

has no solution (X, Y).

Proof. We now assume that (X, Y) is a solution of (9). By Lemma 2, $(u_1, v_1) = (24n^2 + 1, 2n)$ is the least solution of (6). Hence, using Lemma 1 and Lemma 5, we have

$$X + Y^2\sqrt{12(12n^2 + 1)} = \bigl((24n^2 + 1) + 2n\sqrt{12(12n^2 + 1)}\bigr)^k, \quad k \in \mathbb{N}. \tag{10}$$

Since $2 \nmid n$, we see from (10) that $2 \mid Y$, $4 \mid Y^2$ and $2 \mid k$. Therefore, since $12(12n^2 + 1) \neq 1785 \cdot 2^{4r}$, using Lemma 5 again, we get $k = 2$. Substituting it into (10), we have

$$Y^2 = 4n(24n^2 + 1). \tag{11}$$

Since $\gcd(4n, 24n^2 + 1) = 1$, we get from (11) that

$$n = a^2,\ 24n^2 + 1 = b^2,\ Y = 2ab, \quad \gcd(a, b) = 1,\ a, b \in \mathbb{N}. \tag{12}$$

By (11), we obtain

$$b^2 - 24a^4 = 1. \tag{13}$$

Since $n > 1$ and $a > 1$ by (12), it follows that (8) has a solution $(X, Y) = (b, a)$ with $Y > 1$. But, by Lemma 4, this is impossible. Thus, (9) has no solution. Lemma 6 is proved. □

Lemma 7 ([4]). *For any fixed D with $2 \nmid D$ there exists exactly one pair (D_1, D_2, θ) of positive integers such that*

$$D = D_1D_2,\ \gcd(D_1, D_2) = 1, \quad \theta \in \{1, 2\},\ (D_1, D_2, \theta) \neq (1, D, 1)$$

and the equation

$$D_1U^2 - D_2V^2 = \theta, \quad \gcd(U, V) = 1,\ U, V \in \mathbb{N}$$

has solutions (U, V).

Lemma 8. *For any positive odd integer n, the equations*

$$3U^2-(12n^2+1)V^2=2,\quad \gcd(U,V)=1,\ U,V\in\mathbb{N} \tag{14}$$

and

$$3(12n^2+1)U^2-V^2=2,\quad \gcd(U,V)=1,\ U,V\in\mathbb{N} \tag{15}$$

has no solution (U,V).

Proof. Notice that $2\nmid 3(12n^2+1)$, $\gcd(3,12n^2+1)=1$, $(12n^2+1)\cdot 1^2-3\cdot(2n)^2=1$ and the equation

$$(12n^2+1)U^2-3V^2=1,\quad \gcd(U,V)=1,\ U,V\in\mathbb{N} \tag{16}$$

has solutions (U,V). By Lemma 7, we obtain Lemma 8 immediately. □

Lemma 9 ([8])**.** *Let D_1, D_2 be coprime positive integers with $\min\{D_1,D_2\}>1$. If the equation*

$$D_1U^2-D_2V^2=1,\quad \gcd(U,V)=1,\ U,V\in\mathbb{N} \tag{17}$$

has solutions (U,V), then it has a unique solution (U_1,V_1) satisfying $U_1\sqrt{D_1}+V_1\sqrt{D_2}\leqslant U\sqrt{D_1}+V\sqrt{D_2}$, where (U,V) is any solution of (17). Such (U_1,V_1) is called the least solution of (17). Further, for any nonnegative integer s, let

$$U_{2s+1}\sqrt{D_1}+V_{2s+1}\sqrt{D_2}=\bigl(U_1\sqrt{D_1}+V_1\sqrt{D_2}\bigr)^{2s+1}.$$

Then $(U,V)=(U_{2s+1},V_{2s+1})$ $(s=0,1,2,\ldots)$ are all solutions of (17).

Lemma 10. *All solutions (U,V) of (16) satisfy $2\mid V$.*

Proof. Obviously, (16) has the solution $(U,V)=(1,2n)$. If $(U_1,V_1)\neq(1,2n)$, then by Lemma 9 we have

$$\begin{aligned}2\sqrt{12n^2+1}&>\sqrt{12n^2+1}+2n\sqrt{3}\geqslant\bigl(U_1\sqrt{12n^2+1}+V_1\sqrt{3}\bigr)^3\\&>(12n^2+1)^{\frac{3}{2}}U_1^3\geqslant(12n^2+1)^{\frac{3}{2}}>2\sqrt{12n^2+1},\end{aligned}$$

a contradiction. Hence, we get $(U_1,V_1)=(1,2n)$. Moreover, by Lemma 9 again, every solution (U,V) of (16) can be expressed as

$$U\sqrt{12n^2+1}+V\sqrt{3}=\bigl(\sqrt{12n^2+1}+2n\sqrt{3}\bigr)^{2s+1} \tag{18}$$

where s is a nonnegative integer. Thus, we see from (18) that $2n\mid V$. Lemma 10 is proved. □

§3. Proof of the theorem

Let n be a positive odd integer with $n > 1$, and let

$$m = 36n^2 - 5, \ p = 12n^2 + 1, \ q = 6n^2 - 1. \tag{19}$$

Under the hypothesis that p and q are odd primes, by (19) we have

$$m \equiv 7 \pmod 8), \ p \equiv 5 \pmod 8, \ q \equiv 5 \pmod 8. \tag{20}$$

By (3) and (19) we have

$$y^2 = (x-2)(x^2 + 2x + m). \tag{21}$$

Since $x^2 + 2x + m > 0$, we see from (21) that (3) has only the integral point $(x, y) = (2, 0)$ with $y = 0$.

We now assume that (x, y) is an integral point of (3) with $y \neq 0$. Since $y^2 > 0$ and $x^2 + 2x + m > 0$, by (21) we have $x - 2 > 0$. Let $d = \gcd(x-2, x^2 + 2x + m)$. Since $d \mid (m+8)$ and $m + 8 = 36n^2 + 3 = 3(12n^2 + 1) = 3p$, where p is an odd prime with $p \neq 3$, we get

$$d \in \{1, 3, p, 3p\}. \tag{22}$$

By (22) we will prove that the integral point (x, y) does not exist in the following four cases:

Case I: $d = 1$.
By (21) we get

$$x - 2 = a^2, \ x^2 + 2x + m = b^2, \ y = \pm ab, \quad \gcd(a, b) = 1, \ a, b \in \mathbb{N}. \tag{23}$$

By the second equality of (23), we have

$$b^2 - (x+1)^2 = m - 1 = 36n^2 - 6. \tag{24}$$

Since $2 \mid (36n^2 - 6)$, we see from (24) that b and $x+1$ have the same parity. Therefore, by (24), we get $2 \equiv 36n^2 - 6 \equiv b^2 - (x+1)^2 \equiv 0 \pmod 4$, a contradiction.

Case II: $d = 3$.
By (21) we have

$$x - 2 = 3a^2, \ x^2 + 2x + m = 3b^2, \ y = \pm 3ab, \quad \gcd(a, \ b) = 1, \ a, b \in \mathbb{N}. \tag{25}$$

By the first two equalities of (25), we get

$$3(a^2+1)^2+2q=b^2. \tag{26}$$

Since $2\nmid q$, we see from (26) that both a^2+1 and b are odd. Therefore, by (20) and (26), we get $2\equiv 2q\equiv b^2-3(a^2+1)^2\equiv 1-3\equiv 6 \pmod 8$, a contradiction.

Case III: $d=p$.

By (21) we get

$$x-2=pa^2,\ x^2+2x+m=pb^2,\ y=\pm pab,\quad \gcd(a,b)=1,\ a,b\in\mathbb{N}. \tag{27}$$

By (19) and (27) we get

$$3(a^2+1)^2+2qa^4=b^2. \tag{28}$$

If $2\mid a$, then we have $2\nmid(a^2+1)b$ and $0\equiv 2qa^4\equiv b^2-3(a^2+1)^2\equiv 1-3\equiv 6 \pmod 8$ by (28), a contradiction. If $2\nmid a$, then both a^2+1 and b are even, and $2\equiv 2qa^4\equiv b^2-3(a^2+1)^2\equiv 0 \pmod 4$, a contradiction.

Case IV: $d=3p$.

By (21) we have

$$x-2=3pa^2,\ x^2+2x+m=3pb^2,\ y=\pm 3pab,\quad \gcd(a,b)=1,\ a,b\in\mathbb{N}, \tag{29}$$

whence we get

$$b^2-(3a^2+1)^2=6qa^4. \tag{30}$$

If $2\nmid a$, then both $3a^2+1$ and b are even, and $2\equiv 6qa^4\equiv b^2-(3a^2+1)^2\equiv 0 \pmod 4$ by (30), a contradiction.

If $2\mid a$, then we have

$$a=2c,\quad c\in\mathbb{N}. \tag{31}$$

Substituing (31) into (30), we get

$$b^2-(12c^2+1)^2=96qc^4. \tag{32}$$

Since $\gcd(a,b)=\gcd(2c,b)=1$, we see from (32) that $\gcd(b+(12c^2+1),\ b-(12c^2+1))=2$. Hence, by (32), we obtain

$$\begin{gathered} b+\lambda(12c^2+1)=2e_1f^4,\quad b-\lambda(12c^2+1)=2e_2g^4\\ c=fg,\quad \lambda\in\{\pm1\},\ \gcd(f,g)=1,\ f,g\in\mathbb{N} \end{gathered} \tag{33}$$

where

$$e_1e_2 = 24q,\ 2 \nmid e_1, \quad \gcd(e_1, e_2) = 1,\ e_1, e_2 \in \mathbb{N}. \tag{34}$$

By (33), we get

$$e_1f^4 - 12\lambda f^2g^2 - e_2g^4 = \lambda. \tag{35}$$

Since q is an odd prime, by (34) we have

$$(e_1, e_2) = (1, 24q),\ (3, 8q),\ (q, 24),\ \text{or } (3q, 8). \tag{36}$$

When $(e_1, e_2) = (1, 24q)$, we get from (19) and (35) that

$$\begin{aligned} f^4 - 12\lambda f^2g^2 - 24qg^4 &= (f^2 - 6\lambda g^2)^2 - (24q + 36)g^4 \\ &= (f^2 - 6\lambda g^2)^2 - 12(12n^2 + 1)g^4 \\ &= \lambda. \end{aligned} \tag{37}$$

Further, since $\lambda \in \{\pm 1\}$, we see from (37) that $2 \nmid (f^2 - 6\lambda g^2)$, $\lambda = 1$ and

$$(f^2 - 6g^2)^2 - 12(12n^2 + 1)g^4 = 1. \tag{38}$$

It follows that (9) has the solution $(X, Y) = (|f^2 - 6g^2|, g)$. But, since $n > 1$, by Lemma 6 this is impossible.

When $(e_1, e_2) = (3, 8q)$, by (35) we have

$$3(f^2 - 2\lambda g^2)^2 - 4(12n^2 + 1)g^4 = \lambda. \tag{39}$$

Further, since $\lambda \in \{\pm 1\}$, we see from (39) that $2 \nmid (f^2 - 2\lambda g^2)$, $\lambda = -1$ and

$$(12n^2 + 1)(2g^2)^2 - 3(f^2 + 2g^2)^2 = 1. \tag{40}$$

It follows that (16) has the solution $(U, V) = (2g^2, f^2 + 2g^2)$ with $2 \nmid V$. But, by Lemma 10, this is impossible.

When $(e_1, e_2) = (q, 24)$, we have

$$3(\lambda f^2 + 4g^2)^2 - (12n^2 + 1)f^4 = -2\lambda, \tag{41}$$

whence we get $2 \nmid f$, $\lambda = -1$ and

$$3(-f^2 + 4g^2)^2 - (12n^2 + 1)(f^2)^2 = 2. \tag{42}$$

It follows that (14) has the solution $(U,V) = (|-f^2+4g^2|, f^2)$. But, by Lemma 8, this is impossible.

When $(e_1, e_2) = (3q, 8)$, we have

$$(3\lambda f^2+4g^2)^2 - 3(12n^2+1)f^4 = -2\lambda, \tag{43}$$

whence we get $\lambda = 1$ and

$$3(12n^2+1)(f^2)^2 - (3f^2+4g^2)^2 = 2. \tag{44}$$

It follows that (15) has the solution $(U,V) = (f^2, 3f^2+4g^2)$. But, by Lemma 8, this is impossible.

To sum up, we conclude that (3) has no integral point (x,y) with $y \neq 0$. Thus, the theorem is proved. □

Acknowledgement. The authors express their gratitude to the referee for his/her very helpful and detailed comments.

References

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

[2] *Y. He, W. Zhang*: An elliptic curve having large integral points. Czech. Math. J. *60* (2010), 1101–1107.

[3] *L. J. Mordell*: Diophantine Equations. Pure and Applied Mathematics 30., Academic Press, London, 1969.

[4] *K. Petr*: On Pell's equation. Čas. Mat. Fys. *56* (1927), 57–66. (In Czech, French abstract.)

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

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

[7] *A. Togbé, P. M. Voutier, P. G. Walsh*: Solving a family of Thue equations with an application to the equation $x^2 - Dy^4 = 1$. Acta Arith. *120* (2005), 39–58.

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

[9] *P. 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.

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

[11] *H. Zhu, J. Chen*: Integral points on $y^2 = x^3 + 27x - 62$. J. Math. Study *42* (2009), 117–125.

Authors' addresses: Hai Yang, School of Science, Xi'an Polytechnic University, Xi'an, Shaanxi, 710048, P. R. China, and College of Mathematics and Information Science, Shaanxi Normal University, Xi'an, Shaanxi, 710062, P. R. China, e-mail: `xpuyhai@163.com`; Ruiqin Fu, College of Mathematics and Information Science, Shaanxi Normal University, Xi'an, Shaanxi, 710062, P. R. China, and School of Science, Xi'an Shiyou University, Xi'an, Shaanxi, 710065, P. R. China, e-mail: `xsyfrq@163.com`.