Indian J. Pure Appl. Math., **50**(2): 343-352, June 2019

DOI: 10.1007/s13226-019-0329-4

INTEGRAL POINTS ON THE ELLIPTIC CURVE $E_{pq} : y^2 = x^3 + (pq - 12)x - 2(pq - 8)$[1]

Teng Cheng, Qingzhong Ji and Hourong Qin

Department of Mathematics, Nanjing University, Nanjing 210093, *P. R. China*
e-mails: mathcheng@126.com; qingzhji@nju.edu.cn; hrqin@nju.edu.cn

(*Received* 23 *September* 2017; *accepted* 1 *June* 2018)

Let $p = 8k + 5, q = 8k + 3$ be the twin prime pair for some nonnegative integer k. Assume that $\left(\frac{5}{p}\right) = -1$ or $\left(\frac{7}{q}\right) = -1$. In this paper, we prove that the elliptic curve $E_{pq} : y^2 = x^3 + (pq - 12)x - 2(pq - 8)$ has unique integral point (2, 0).

Key words : Elliptic curve; integral point; Fibonacci (Lucas) sequence.

1. INTRODUCTION

Throughout this paper, let $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{N}$ denote the field of rational numbers, the ring of rational integers and the set of nonnegative integers, respectively. Let $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

Let E be an elliptic curve defined over $\mathbb{Q}$. Siegel's theorem states that for a fixed Weierstrass equation defining E, the set of integral points on E is finite. However it is difficult to determine all integral points on elliptic curves. For example, the points $(x, y) = (28844402, \pm 154914585540)$ are the largest integral points on the elliptic curve

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

proposed by Don Zagier [14], in 1987. Then the same problem of integral points on the elliptic curve (1) was dealt with by some authors and by using different methods, we refer the reader to ([2, 3, 12, 13, 15]). In the literature, there are many results and advanced methods have been developed in studying integral points on elliptic curves (see [1, 10, 11]). In [13], Yang and Fu proved that if $n > 1$ and both $6n^2 - 1$ and $12n^2 + 1$ are odd primes, then the elliptic curve $y^2 = x^3 + (36n^2 - 9)x - 2(36n^2 - 5)$ has

[1]Supported by NSFC (Nos. 11471154, 11631009, 11571163).

only the integral point $(x, y) = (2, 0)$. In this paper, using elementary number theory methods and some properties of generalized Fibonacci and Lucas sequences, we obtain the the following results.

***Theorem* 1.1** — *Let $p = 8k + 5, q = 8k + 3$ be the twin prime pair for some nonnegative integer k. Assume that $\left(\frac{5}{p}\right) = -1$ or $\left(\frac{7}{q}\right) = -1$. Let E_{pq} be the elliptic curve given by the Weierstrass equation:*

$$E_{pq} : y^2 = x^3 + (pq - 12)x - 2(pq - 8).$$

Then E_{pq} has only the integral point $(x, y) = (2, 0)$, where $\left(\frac{*}{*}\right)$ denote Legendre symbol.

Let E be an elliptic curve defined over $\mathbb{Z}$ given by a Weierstrass equation

$$y^2 = x^3 + Ax + B,\ A, B \in \mathbb{Z}.$$

By [9], VIII Corollary 7.2, we have $E(\mathbb{Q})_{\mathrm{tors}} \subseteq E(\mathbb{Z})$, where $E(\mathbb{Q})_{\mathrm{tors}}$ denotes the torsion subgroup of $E(\mathbb{Q})$.

Corollary 1.2 — Let $p = 8k + 5, q = 8k + 3$ be the twin prime pair for some nonnegative integer k. Let E_{pq} be the elliptic curve given by the Weierstrass equation:

$$E_{pq} : y^2 = x^3 + (pq - 12)x - 2(pq - 8).$$

Then we have

$$E_{pq}(\mathbb{Q})_{\mathrm{tors}} = \{O, (2, 0)\}.$$

PROOF : In particular, if we assume that $\left(\frac{5}{p}\right) = -1$ or $\left(\frac{7}{q}\right) = -1$, it is trivial from $E_{pq}(\mathbb{Q})_{\mathrm{tors}} \subseteq E_{pq}(\mathbb{Z})$ and Theorem 1.1. Next, we shall give another proof by reduction properties for arbitrary twin prime pair $p = 8k + 5, q = 8k + 3$.

It is clear that $\{O, (2, 0)\} \subseteq E_{pq}(\mathbb{Q})_{\mathrm{tors}}$. If $k = 0$, *i.e.*, $p = 5, q = 3$, we have

$$E_{5\cdot 3} : y^2 = x^3 + 3x - 14$$

It has discriminant $\Delta = 2^7 3^3 5^2$, so $\widetilde{E}_{5\cdot 3}$ is nonsingular modulo p for every prime $p \geq 7$. Hence, we have

$$\widetilde{E}_{5\cdot 3}(\mathbb{F}_7) = \{O, (0, 0), (1, 2), (1, 5), (2, 0), (3, 1), (3, 6), (5, 0)\}$$

$$\widetilde{E}_{5\cdot 3}(\mathbb{F}_{11}) = \{O, (1, 1), (1, 10), (2, 0), (3, 0), (5, 4), (5, 7), (6, 0),$$

$$(7, 3), (7, 8), (8, 4), (8, 7), (9, 4), (9, 7), (10, 2), (10, 9)\}$$

Since $E_{5\cdot 3}(\mathbb{Q})_{\mathrm{tors}}$ injects into both of these groups, we see that $(2,0)$ is the only nonzero torsion point in $E_{5\cdot 3}(\mathbb{Q})$. Hence, $E_{5\cdot 3}(\mathbb{Q})_{\mathrm{tors}} = \{O, (2,0)\}$.

Assume $k \geq 1$. Then the elliptic curve E_{pq} has good reduction at 3 since the discriminant $\Delta = -64(pq)^3 + 576(pq)^2$ and $3 \nmid \Delta$. Since $p = 8k+5$, $q = 8k+3$ are the twin primes, we have $k = 3t+1$ for some positive integer t. Reducing modulo 3, we have

$$\widetilde{E}_{pq}: \quad y^2 = x^3 + 2x.$$

By a similar way as above, it's easy to calculate that $\sharp \widetilde{E}_{pq}(\mathbb{F}_3) = 2$. By Proposition 2.3, we obtain $E_{pq}(\mathbb{Q})_{\mathrm{tors}} = \{O, (2,0)\}$. □

Remark 1.3 : For the above elliptic curves E_{pq}, there exists k such that $\mathrm{rank}(E_{pq}) \geq 1$, *e.g.*, $k = 7, p = 61, q = 59, \mathrm{rank}(E_{3599}) = 1$.

This paper is organized as follows. In section 2, we will recall some concepts and fundamental results which will be used in the following sections. In section 3, we will prove our main results.

2. Preliminary

Let α and β be non-zero integers with $\alpha^2 + 4\beta \neq 0$. The generalized Fibonacci sequence $(U_n(\alpha,\beta))$ and the Lucas sequence $(V_n(\alpha,\beta))$ are defined by the following recurrence relations:

$$U_0(\alpha,\beta) = 0, \quad U_1(\alpha,\beta) = 1, \qquad U_{n+2}(\alpha,\beta) = \alpha U_{n+1}(\alpha,\beta) + \beta U_n(\alpha,\beta)$$

and

$$V_0(\alpha,\beta) = 2, \quad V_1(\alpha,\beta) = \alpha, \qquad V_{n+2}(\alpha,\beta) = \alpha V_{n+1}(\alpha,\beta) + \beta V_n(\alpha,\beta)$$

for $n \geq 0$.

We have the well-known expressions named Binet's formulas:

$$U_n(\alpha,\beta) = \frac{\eta^n - \theta^n}{\eta - \theta} \text{ and } V_n(\alpha,\beta) = \eta^n + \theta^n$$

where $\eta = \frac{\alpha + \sqrt{\alpha^2+4\beta}}{2}$, and $\theta = \frac{\alpha - \sqrt{\alpha^2+4\beta}}{2}$, $n \geq 1$.

If $\beta = -1$, we represent (U_n) and (V_n) by (u_n) and (v_n), respectively. Note that if $\alpha \geq 3$, then $u_n > 0$ for all $n \geq 1$.

Lemma 2.1 — [8]. Let $t \geq 1$ and $s \geq 1$, then $(u_t, u_s) = u_{(t,s)}$.

Let $(u_n(\alpha, -1))$ be the generalized Fibonacci sequence, we state the following theorem.

Lemma 2.2 — [5]. Let α be an integer with $\alpha > 2$. If $u_n(\alpha, -1) = cx^2$ with $x \in \mathbb{Z}$ and $c \in \{1, 2, 3, 6\}$ and $n > 3$, then $(n, \alpha, c) = (4, 338, 1)$ or $(6, 3, 1)$.

The following identities for (u_n) and (v_n) are well-known:

(A) $u_{2n} = u_n v_n$

(B) $v_n = u_{n+1} - u_{n-1}$

(C) $u_{2t+1} - 1 = u_t v_{t+1}$

Moreover, if α is even, then:

(D) u_n is even $\Leftrightarrow$ n is even.

(E) u_n is odd $\Leftrightarrow$ n is odd.

For more information about generalized Fibonacci and Lucas sequences, we refer the reader to [6, 8].

Proposition 2.3 — [4, Theorem 5.1]. Let E be an elliptic curve given by Weierstrass equation with coefficients in $\mathbb{Z}$. If p is an odd prime such that $p \nmid \Delta$, then the restriction to $E(\mathbb{Q})_{tors}$ of the reduction homomorphism $r_p : E(\mathbb{Q}) \to E_p(\mathbb{F}_p)$ is one-one.

Proposition 2.4 — [7, Theorem 104]. If D is a natural number which is not a perfect square, the equation

$$x^2 - Dy^2 = 1 \tag{2}$$

has infinitely many solutions $x+y\sqrt{D}$. All solutions with positive x and y are obtained by the formula

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n \tag{3}$$

where $x_1 + y_1\sqrt{D}$ is the fundamental solution of (2), where n runs through all natural numbers.

3. Proof of Theorem 1.1

We would like point out that the idea used here is similar to that in [3].

We assume that $k \geq 1$ in the following. By the equation of the elliptic curve E_{pq}, we have:

$$E_{pq} : y^2 = (x - 2)(x^2 + 2x + (pq - 8)). \tag{4}$$

Since $x^2 + 2x + pq - 8 > 0$, the elliptic curve E_{pq} has only the integral point $(x, y) = (2, 0)$ with $y = 0$.

We now assume that (x, y) is an integral point of (4) with $y \neq 0$. Since $y^2 > 0$ and $x^2 + 2x + pq - 8 > 0$, by (4), we have $x - 2 > 0$. Let $l = x - 2 > 0$. Substituting this value of l into (4), we obtain:

$$E_{pq} : y^2 = l(l^2 + 6l + pq). \tag{5}$$

Let $d = (l, l^2 + 6l + pq)$. It's clear that $d \in \{1, q, p, pq\}$. From (5), we obtain

$$l = da^2, \quad l^2 + 6l + pq = db^2, \quad y = \pm dab, \quad (a, b) = 1$$

for some positive integers a and b.

Case 1 : Assume $d = 1$. By (5), we obtain:

$$a^4 + 6a^2 + pq = b^2.$$

Hence a and b have different parity.

(i) If a is odd and b is even, then $b = 2m$ for some $m \in \mathbb{N}^*$ and

$$6 \equiv a^4 + 6a^2 + pq \equiv b^2 \equiv 4m^2 \pmod 8$$

i.e.,

$$6 \equiv 4m^2 \equiv 0 \pmod 4$$

a contradiction.

(ii) If a is even and b is odd, then

$$-1 \equiv a^4 + 6a^2 + pq \equiv b^2 \equiv 1 \pmod 8,$$

a contradiction.

Case 2 : Assume $d = p, q$. By (5), we obtain:

$$pa^4 + 6a^2 + q = b^2, \text{ or } qa^4 + 6a^2 + p = b^2.$$

It is an analogy to that of case 1. By using modulo 8, we shall reduce a contradiction.

Case 3 : Assume $d = pq$. By (5), we obtain:

$$(pqa^2 + 3)^2 + pq - 9 = pqb^2.$$

This equation is of the form:

$$u^2 - pqv^2 = -(pq - 9). \tag{6}$$

It is easy to see that the fundamental solution of $x^2 - pqy^2 = 1$ is $\eta = (p-1) + \sqrt{pq}$. Hence all positive solutions of $x^2 - pqy^2 = 1$ are of the form

$$x_n + y_n\sqrt{pq} = \eta^n, \quad n \in \mathbb{N},$$

and $x_n = \frac{\eta^n + \theta^n}{2}$ and $y_n = \frac{\eta^n - \theta^n}{2\sqrt{pq}}$, where $\theta = (p-1) - \sqrt{pq}$.

By Binet's formulas (6), and $\eta = \dfrac{\alpha + \sqrt{\alpha^2 + 4\beta}}{2}, \theta = \dfrac{\alpha - \sqrt{\alpha^2 + 4\beta}}{2}$, we have $\alpha = 2(p-1)$, $\beta = -1$, hence, $x_n = \dfrac{\eta^n + \theta^n}{2} = \dfrac{v_n(2(p-1), -1)}{2}$ and $y_n = \dfrac{\eta^n - \theta^n}{2\sqrt{pq}} = \dfrac{(\eta - \theta)(u_n(2(p-1), -1))}{2\sqrt{pq}}$ $= u_n(2(p-1), -1)$. Since the fundamental solutions of (6) are $3 + \sqrt{pq}$ and $3 - \sqrt{pq}$, by Proposition 2.4 and $P_{204-212}$ of [7], the equation (6) has exactly two solution classes given by:

$$a_n + b_n\sqrt{pq} = (3 - \sqrt{pq})(x_n + y_n\sqrt{pq}) = 3x_n - pqy_n + (3y_n - x_n)\sqrt{pq} \tag{7}$$

and

$$a_n + b_n\sqrt{pq} = (3 + \sqrt{pq})(x_n + y_n\sqrt{pq}) = 3x_n + pqy_n + (x_n + 3y_n)\sqrt{pq} \tag{8}$$

with $n \geq 1$. Since $(pqa^2 + 3, b)$ is a solution of (6), we have $(pqa^2 + 3, b) = (a_{n_0}, b_{n_0})$ for some $n_0 \in \mathbb{N}^*$. Hence

$$pqa^2 + 3 = 3x_{n_0} - pqy_{n_0}, \ \text{ or } \ 3x_{n_0} + pqy_{n_0}.$$

On the one hand, by $x_n = \frac{v_n}{2}$, $y_n = u_n$ and $v_n = u_{n+1} - u_{n-1}$, we have

$$3x_{n_0} - pqy_{n_0} = (-4p^2 + 11p - 3)u_{n_0} - 3u_{n_0 - 1}$$

and

$$3x_{n_0} + pqy_{n_0} = 3u_{n_0+1} + (4p^2 - 11p + 3)u_{n_0}.$$

Since $-4p^2 + 11p - 3 < 0$ and $u_{n_0} \geq 0$, we obtain

$$pqa^2 + 3 = 3u_{n_0+1} + (4p^2 - 11p + 3)u_{n_0}.$$

On the other hand, by induction on n, it is easy to show that:

$$u_n \equiv \begin{cases} -n \pmod{p}, & \text{if } n \text{ even}, \\ \ \ n \pmod{p}, & \text{if } n \text{ odd}, \end{cases} \tag{9}$$

and

$$u_n \equiv n \pmod{2p-4}. \tag{10}$$

If n_0 is odd, by using (9), we have

$$3 \equiv pqa^2 + 3 \equiv 3u_{n_0+1} + (4p^2 - 11p + 3)u_{n_0} \equiv -3(n_0 + 1) + (4p^2 - 11p + 3)n_0 \equiv -3 \pmod{p}.$$

This is a contradiction. Hence n_0 is even, *i.e.*, $n_0 = 2r$ for some $r > 0$.

(i) Assume a is odd. By (10), we have

$$pqa^2 + 3 \equiv 3u_{n_0+1} + (4p^2 - 11p + 3)u_{n_0} \equiv (p^2 - 5p)n_0 + 6n_0 + 3 \pmod{2p - 4}.$$

Hence

$$pqa^2 \equiv 0 \pmod{2}.$$

This is a contradiction since p, q and a are odd.

(ii) Assume a is even. Then we have

$$\begin{aligned} pqa^2 &= 3u_{n_0+1} + (4p^2 - 11p + 3)u_{n_0} - 3 \\ &= 3u_{2r+1} + (4p^2 - 11p + 3)u_{2r} - 3 \\ &= 3(u_r v_{r+1}) + (4p^2 - 11p + 3)u_r v_r \text{ (by (A) and (C))} \\ &= u_r[3v_{r+1} + (4p^2 - 11p + 3)v_r] \\ &= u_r[3u_{r+2} - 3u_r + (4p^2 - 11p + 3)u_{r+1} - (4p^2 - 11p + 3)u_{r-1}] \text{ (by (B))} \\ &= u_r[(2p^3 - 8p)u_r - (2p^2 - 4p)u_{r-1}] \\ &= u_r[2pq(p + 2)u_r - 2pqu_{r-1}]. \end{aligned}$$

Hence

$$a^2 = u_r[2(p + 2)u_r - 2u_{r-1}].$$

This is a contradiction by the following Lemma 3.1.

To sum up, we complete the proof of the Theorem 1.1. □

Lemma 3.1 — Let $a \in \mathbb{N}^*$ and $r \in \mathbb{N}^*$. If a and r are even, then

$$a^2 \neq u_r[2(p + 2)u_r - 2u_{r-1}].$$

PROOF : Assume there exist even integers $a > 0, r > 0$ such that

$$a^2 = u_r[2(p + 2)u_r - 2u_{r-1}]. \tag{11}$$

By (D), u_r is even, *i.e.*, $u_r = 2A_r$ for some integer A_r. Let $a = 2b$ for some $b \in \mathbb{N}^*$. Then the equality (11) is changed to

$$4b^2 = 2A_r[2(p + 2)u_r - 2u_{r-1}],$$

i.e.,

$$b^2 = A_r[(p+2)u_r - u_{r-1}]. \tag{12}$$

Hence b and A_r have the same parity.

(i) If b is even and A_r is even, *i.e.*, $b = 2c$ for some $c \in \mathbb{N}^*$, and $A_r = 2B_r$ for some $B_r \in \mathbb{N}$. Then the equality (12) is changed to

$$4c^2 = 2B_r[(p+2)u_r - u_{r-1}]. \tag{13}$$

i.e.,

$$2c^2 = B_r[(p+2)u_r - u_{r-1}]. \tag{14}$$

By Lemma 2.1, we have

$$(4B_r, u_{r-1}) = (u_r, u_{r-1}) = u_{(r,r-1)} = 1.$$

Hence

$$(B_r, (p+2)u_r - u_{r-1}) = (B_r, u_{r-1}) = 1.$$

By (15), we have

$$\begin{cases} c = ef, (e,f) = 1, \\ B_r = 2e^2, \\ (p+2)u_r - u_{r-1} = f^2. \end{cases}$$

Hence

$$u_r = 2(2e)^2$$

(ii) If b is odd and A_r is odd, then By Lemma 2.2, we have

$$(2A_r, u_{r-1}) = (u_r, u_{r-1}) = u_{(r,r-1)} = 1.$$

Hence

$$(A_r, (p+2)u_r - u_{r-1}) = (A_r, u_{r-1}) = 1.$$

By (11), we have

$$\begin{cases} b = ef, (e,f) = 1, \\ A_r = e^2, \\ (p+2)u_r - u_{r-1} = f^2. \end{cases}$$

Hence

$$u_r = (2e)^2$$

By the above, we have $u_r = 2(2e)^2$ or $u_r = (2e)^2$, since r is even and $\alpha = 2(p-1) > 2$, by Lemma 2.2, we have $r = 2$. By (11), we have

$$a^2 = u_2[2(p+2)u_2 - 2u_1] = 8p^3 - 28p + 20 = 8q^3 + 48q^2 + 68q + 28.$$

Hence

$$a^2 \equiv 20 \pmod{p} \text{ and } \mathrm{a}^2 \equiv 28 \pmod{\mathrm{q}}$$

i.e.,

$$b^2 \equiv 5 \pmod{p} \text{ and } \mathrm{b}^2 \equiv 7 \pmod{\mathrm{q}}$$

This is a contradiction, since

$$\left(\frac{5}{p}\right) = -1 \text{ or } \left(\frac{7}{\mathrm{q}}\right) = -1.$$

This completes the proof of the lemma. □

ACKNOWLEDGEMENT

We would like to thank the referee for reading the manuscript carefully and providing valuable comments and suggestions.

REFERENCES

1. A. Bake, The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$, *J. Lond. Math. Soc.*, **43** (1968), 1-9.
2. Y. He and W. Zhang, An elliptic curve having large integral points, *Czech. Math. J.*, **60** (2010), 1101-1107.
3. O. Karaatli and R. Keskin, Integral points on the elliptic curve $y^2 = x^3 + 27x - 62$, *J. Inequalities and Applications*, **1** (2013), 1-6.
4. A. W. Knapp, Elliptic curves, *Mathematical Notes*, **40** (1992), Princeton University Press, Princeton, NJ.
5. M. Migotte and A. Pethõ, Sur les carrés dans certainies suites de Lucas, *J. Théor. Nr. Bordx.*, **5**(2) (1993), 333-341.
6. J. B. Muskat, Genaralized Fibonacci and Lucas sequences and root finding methods, *Math. Comput.*, **61** (1993), 365-372.

7. T. Nagell, *Introduction to number theory*, Wiley, New York, 1951.
8. P. Ribenboim, An algorithm to determine the points with integral coordinates in certain elliptic curves, *J. Number. Theory*, **74** (1999), 19-38.
9. J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.
10. R. J. Stroeker and N. Tzanakis, On the elliptic logarithm method for elliptic Diophantine equations: Reflections and an improvement, *Exp. Math.*, **8** (1999), 135-149.
11. R. J. Stroeker and N. Tzanakis, Computing all integral solutions of a genus 1 equation, *Math. Comput.*, **72** (2003), 1971-1933.
12. H. Wu, Points on the elliptic curve $y^2 = x^3 + 27x - 62$, *Acta Math. Sin. Chin. Ser.*, **53**(1) (2010), 205-208.
13. H. Yang and R. Fu, The integral points on elliptic curves $y^2 = x^3 + (36n^2 - 9)x - 2(36n^2 - 5)$, *Czechoslovak Math. J.*, **63**(2) (2013), 375-383.
14. D. Zagier, Large integral points on elliptic curves, *Math. Comput.*, **48** (1987), 425-436.
15. H. Zhu and J. Chen, Integeral points on $y^2 = x^3 + 27x - 62$, *J. Math. Study*, **42** (2009), 117-125.