Karaatlı and Keskin *Journal of Inequalities and Applications* 2013, **2013**:221
http://www.journalofinequalitiesandapplications.com/content/2013/1/221

Journal of Inequalities and Applications
a SpringerOpen Journal

RESEARCH Open Access

Integral points on the elliptic curve $y^2 = x^3 + 27x - 62$

Olcay Karaatlı* and Refik Keskin

*Correspondence:
okaraatli@sakarya.edu.tr
Department of Mathematics, Sakarya University, Sakarya, 54187, Turkey

Abstract

We give a new proof that the elliptic curve $y^2 = x^3 + 27x - 62$ has only the integral points $(x, y) = (2, 0)$ and $(x, y) = (28{,}844{,}402, \pm 15{,}491{,}585{,}540)$ using elementary number theory methods and some properties of generalized Fibonacci and Lucas sequences.

MSC: 11B25; 11B37

Keywords: elliptic curves; integral point; generalized Fibonacci and Lucas sequences

1 Introduction

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

$$U_0(P,Q) = 0, \qquad U_1(P,Q) = 1, \qquad U_{n+2}(P,Q) = PU_{n+1}(P,Q) + QU_n(P,Q) \quad \text{for } n \geq 0$$

and

$$V_0(P,Q) = 2, \qquad V_1(P,Q) = P, \qquad V_{n+2}(P,Q) = PV_{n+1}(P,Q) + QV_n(P,Q) \quad \text{for } n \geq 0.$$

$U_n(P,Q)$ is called the nth generalized Fibonacci number and $V_n(P,Q)$ is called the nth generalized Lucas number. Also, generalized Fibonacci and Lucas numbers for negative subscripts are defined as

$$U_{-n}(P,Q) = \frac{-U_n(P,Q)}{(-Q)^n} \quad \text{and} \quad V_{-n} = \frac{V_n(P,Q)}{(-Q)^n} \quad \text{for } n \geq 1, \tag{1.1}$$

respectively. Taking $\alpha = (P + \sqrt{P^2 + 4Q})/2$ and $\beta = (P - \sqrt{P^2 + 4Q})/2$ to be the roots of the characteristic equation $x^2 - Px - Q = 0$, we have the well-known expressions named Binet's formulas

$$U_n(P,Q) = \left(\alpha^n - \beta^n\right)/(\alpha - \beta) \quad \text{and} \quad V_n(P,Q) = \alpha^n + \beta^n \tag{1.2}$$

for all $n \in \mathbb{Z}$. Instead of $U_n(P,Q)$ and $V_n(P,Q)$, we use U_n and V_n, respectively. For $P = Q = 1$, the sequence (U_n) is the familiar Fibonacci sequence (F_n) and the sequence (V_n) is the familiar Lucas sequence (L_n). If $P = 2$ and $Q = 1$, then we have the well-known Pell sequence (P_n) and Pell-Lucas sequence (Q_n). For $Q = -1$, we represent (U_n) and (V_n) by

Springer

(u_n) and (v_n), respectively. Thus $u_0 = 0$, $u_1 = P$ and $u_{n+1} = Pu_n - u_{n-1}$ and $v_0 = 2$, $v_1 = P$ and $v_{n+1} = Pv_n - v_{n-1}$ for all $n \geq 1$. Also, it is seen from Eq. (1.1) that

$$u_{-n} = -u_n(P,-1) \quad \text{and} \quad v_{-n} = v_n(P,-1)$$

for all $n \geq 1$. For more information about generalized Fibonacci and Lucas sequences, one can consult [1–5].

There has been much interest in determining the problem of the integral points on elliptic curves, and many advanced methods have been developed to solve such problems (see [6, 7] and [8]). In 1987, Don Zagier [9] proposed that the largest integral point on the elliptic curve

$$y^2 = x^3 + 27x - 62 \tag{1.3}$$

is $(x, y) = (28{,}844{,}402, \pm 154{,}914{,}585{,}540)$. Then the same problem was dealt with by some authors. In [10], Zhu and Chen found all integral points on (1.3) by using algebraic number theory and p-adic analysis. In [11], Wu proved that (1.3) has only the integral points $(x, y) = (2, 0)$ and $(28{,}844{,}402, \pm 154{,}914{,}585{,}540)$ using some results of quartic Diophantine equations with elementary number methods. After that, in [12], the authors found the integral points on (1.3) using similar methods to those given in [11]. In this paper, we determine that the largest integral point on the elliptic curve $y^2 = x^3 + 27x - 62$ is $(x, y) = (28{,}844{,}402, \pm 154{,}914{,}585{,}540)$ by using elementary number theory methods and some properties of generalized Fibonacci and Lucas sequences. Our proof is extremely different from the proofs of the others.

2 Preliminaries

In this section, we present two theorems and some well-known identities regarding the sequences (u_n) and (v_n), which will be useful during the proof of the main theorem.

We state the following theorem from [13].

Theorem 2.1 *Let* $P > 2$. *If* $u_n = cx^2$ *with* $c \in \{1, 2, 3, 6\}$ *and* $n > 3$, *then* $(n, P, c) = (4, 338, 1)$ *or* $(6, 3, 1)$.

The following theorem is a well-known theorem (see [14]).

Theorem 2.2 *Let* $m \geq 1$ *and* $n \geq 1$. *Then* $(u_m, u_n) = u_{(m,n)}$.

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

$$u_{2n} = u_n v_n, \tag{2.1}$$

$$v_n = u_{n+1} - u_{n-1}, \tag{2.2}$$

$$u_{2k+1} - 1 = u_k v_{k+1}. \tag{2.3}$$

Moreover, if P is even, then

$$u_n \text{ is even} \Leftrightarrow n \text{ is even}, \tag{2.4}$$

$$u_n \text{ is odd} \Leftrightarrow n \text{ is odd}. \tag{2.5}$$

3 Proof of the main theorem

The main theorem we deal with here is as follows.

Theorem 3.1 *The elliptic curve* $y^2 = x^3 + 27x - 62$ *has only the integral points* $(x, y) = (2, 0)$ *and* $(28{,}844{,}402, \pm 154{,}914{,}585{,}540)$.

Proof Assume that (x, y) is an integral point on the elliptic curve $y^2 = x^3 + 27x - 62$. It can be easily seen that $x > 0$. On the other hand, obviously, the elliptic curve $y^2 = x^3 + 27x - 62$ has only the integral point $(x, y) = (2, 0)$ with $y = 0$. Hence, we may assume that $y \neq 0$. Let $k = x - 2$. Substituting this value of k into $y^2 = x^3 + 27x - 62$, we get

$$y^2 = k(k^2 + 6k + 39). \tag{3.1}$$

Since $y \neq 0$, it is obvious that $y^2 > 0$. On the other hand, since $k^2 + 6k + 39 = (k + 3)^2 + 30 > 0$, we conclude that $k > 0$. Clearly, $d = (k, k^2 + 6k + 39) = 1, 3, 13$ or 39. So, we get from (3.1) that

$$k = da^2, \qquad k^2 + 6k + 39 = db^2, \qquad y = \pm dab \tag{3.2}$$

for some positive integers a and b.

If $d = 1$, then from (3.2) we get $a^4 + 6a^2 + 39 = b^2$. Completing the square gives $(a^2 + 3)^2 + 30 = b^2$. This implies that $[b - (a^2 + 3)][b + (a^2 + 3)] = 30$. It can be easily shown that there are no integers a and b satisfying the previous equation.

If $d = 3$, then from (3.2) we obtain $9a^4 + 18a^2 + 39 = 3b^2$. Completing the square gives

$$b^2 - 3(a^2 + 1)^2 = 10. \tag{3.3}$$

Working on modulo 8 shows that (3.3) is impossible.

If $d = 13$, then from (3.2) we immediately have $169a^4 + 78a^2 + 39 = 13b^2$. Completing the square gives

$$(13a^2 + 3)^2 - 13b^2 = -30. \tag{3.4}$$

Working on modulo 8 shows that (3.4) is impossible.

Lastly, we consider (1.3) for the case when $d = 39$. If $d = 39$, then from (3.2) we get $k = 39a^2$ and $k^2 + 6k + 39 = 39b^2$. Substituting $k = 39a^2$ into $k^2 + 6k + 39 = 39b^2$ and completing the square give

$$(39a^2 + 3)^2 + 30 = 39b^2. \tag{3.5}$$

This equation is of the form

$$u^2 - 39v^2 = -30. \tag{3.6}$$

Let $x_n + y_n\sqrt{39}$ be a solution of the equation $x^2 - 39y^2 = 1$. Since the fundamental solution of this equation is $\alpha = 25 + 4\sqrt{39}$, we get $x_n + y_n\sqrt{39} = \alpha^n$, and therefore $x_n = (\alpha^n + \beta^n)/2$

and $y_n = (\alpha^n - \beta^n)/2\sqrt{39}$, where $\beta = 25 - 4\sqrt{39}$. It can be easily seen that $x_n = v_n(50, -1)/2$ and $y_n = 4u_n(50, -1)$. Equation (3.6) has exactly two solution classes and the fundamental solutions are $3 + \sqrt{39}$ and $3 - \sqrt{39}$. So, the general solution of (3.6) is given by

$$a_n + b_n\sqrt{39} = (3 - \sqrt{39})(x_n + y_n\sqrt{39}), \tag{3.7}$$

$$a_n + b_n\sqrt{39} = (3 + \sqrt{39})(x_n + y_n\sqrt{39}), \tag{3.8}$$

with $n \geq 1$, respectively [15]. Considering first Eq. (3.7), we readily obtain $a_n = 3x_n - 39y_n$. Since $x_n = v_n/2$ and $y_n = 4u_n$, it follows that

$$a_n = (3v_n - 312u_n)/2.$$

From (2.2), if we write $u_{n+1} - u_{n-1}$ instead of v_n and rearrange the above equation, then we get $a_n = -81u_n - 3u_{n-1}$. This means that $39a^2 + 3 = -81u_n - 3u_{n-1}$ by (3.5). Dividing both sides of the equation by 3 gives $13a^2 + 1 = -27u_n - u_{n-1}$. However, this is impossible for $13a^2 + 1 > 0$ and $n \geq 1$. Another possibility is that $-39a^2 - 3 = -81u_n - 3u_{n-1}$, implying that

$$13a^2 + 1 = 27u_n + u_{n-1}. \tag{3.9}$$

It can be shown by the induction method that

$$u_n \equiv \begin{cases} -n \pmod{13} & \text{if } n \text{ is even,} \\ n \pmod{13} & \text{if } n \text{ is odd} \end{cases} \tag{3.10}$$

and

$$u_n \equiv n \pmod 8. \tag{3.11}$$

So, working on modulo 8 and using (3.11) in Eq. (3.9) lead to a contradiction.

Now, we consider Eq. (3.8). Then we immediately have $a_n = 3x_n + 39y_n$. Since $x_n = v_n/2$ and $y_n = 4u_n$, it follows that $a_n = (3v_n + 312u_n)/2$. In view of (2.2), we readily obtain $a_n = 3u_{n+1} + 81u_n$. By (3.5), we get $39a^2 + 3 = 3u_{n+1} + 81u_n$, implying that

$$13a^2 + 1 = u_{n+1} + 27u_n. \tag{3.12}$$

Assume that n is odd. By using (3.10), we get

$$u_{n+1} + 27u_n \equiv -n - 1 + 27n \equiv -1 \pmod{13},$$

a contradiction by (3.12). So, n is even. Now, let us assume that a is odd in Eq. (3.12). Then using (3.11) gives

$$u_{n+1} + 27u_n \equiv n + 1 + 3n \equiv 4n + 1 \equiv 6 \pmod 8,$$

i.e.,

$$4n \equiv 5 \pmod 8,$$

which is impossible. So, a is even, and therefore $a = 2m$ for some positive integer m. Substituting $a = 2m$ into (3.12), we get

$$52m^2 + 1 = u_{n+1} + 27u_n. \tag{3.13}$$

In the above equation, if m is odd, then from (3.11) we get

$$u_{n+1} + 27u_n \equiv n + 1 + 3n \equiv 4n + 1 \equiv 5 (\bmod 8),$$

which implies that

$$n \equiv 1 (\bmod 2).$$

But this is impossible since n is even. As a consequence, m is even and therefore we conclude that $4|a$. We now return to (3.12). Since n is even, $n = 2r$ for some $r > 0$. Then (3.12) becomes

$$13a^2 = u_{2r+1} - 1 + 27u_{2r}.$$

By (2.3) and (2.1), it can be seen that $u_{2r+1} - 1 + 27u_{2r} = u_r v_{r+1} + 27u_r v_r = u_r(v_{r+1} + 27v_r)$ and therefore

$$13a^2 = u_r(v_{r+1} + 27v_r).$$

By using (2.2), we get $13a^2 = u_r(u_{r+2} - u_r + 27u_{r+1} - 27u_{r-1})$. In view of the recurrence relation of the sequence u_r, we immediately have

$$13a^2 = u_r(3{,}848u_r - 104u_{r-1}).$$

Dividing both sides of the above equation by 13 and rearranging the equation gives

$$a^2 = 8u_r(37u_r - u_{r-1}).$$

Since $4|a$, it follows that

$$2(a/4)^2 = u_r(37u_r - u_{r-1}).$$

By Theorem 2.2, since $(u_r, u_{r-1}) = 1$, clearly, $(u_r, 37u_r - u_{r-1}) = 1$. This implies that either

$$37u_r - u_{r-1} = 2c^2 \tag{3.14}$$

or

$$u_r = 2c^2 \tag{3.15}$$

for some positive integer c, where $u_r = u_r(50, -1)$. By (2.4) and (2.5), it can be seen that $37u_r - u_{r-1}$ is always odd. Therefore (3.14) is impossible. By Theorem 2.1, (3.15) is impossible for the case when $r > 3$. Hence, we have $r \leq 3$. On the other hand, since $u_r = 2c^2$ is even, from (2.4), it follows that r is even. Since r is even and $n = 2r$, we get $n = 4$. Substituting this value of n into (3.12), we obtain

$$13a^2 + 1 = u_5 + 27u_4.$$

Since $u_5 = 6{,}242{,}501$ and $u_4 = 124{,}900$, a simple computation shows that $a = 860$. Moreover, since $k = 39a^2$ and $x = k + 2$, we get $k = 28{,}844{,}400$ and therefore $x = 28{,}844{,}402$. Substituting $x = 28{,}844{,}402$ into $y^2 = x^3 + 27x - 62$ gives $y = \pm 15{,}491{,}585{,}540$. Hence, the theorem is proved, the elliptic curve $y^2 = x^3 + 27x - 62$ has only the integral points $(x, y) = (2, 0)$ and $(x, y) = (28{,}844{,}402, \pm 15{,}491{,}585{,}540)$, which is the largest integral point on it. This completes the proof of the main theorem. □

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
Both authors contributed equally in the preparation of this article. Both authors read and approved the final manuscript.

Acknowledgements
Dedicated to Professor Hari M Srivastava.

Received: 9 January 2013 Accepted: 6 March 2013 Published: 2 May 2013

References

1. Kalman, D, Mena, R: The Fibonacci numbers-exposed. Math. Mag. **76**, 167-181 (2003)
2. Karaatlı, O, Keskin, R: On some diophantine equations related to square triangular and balancing numbers. J. Algebra, Number Theory: Adv. Appl. **4**(2), 71-89 (2010)
3. Muskat, JB: Generalized Fibonacci and Lucas sequences and rootfinding methods. Math. Comput. **61**, 365-372 (1993)
4. Rabinowitz, S: Algorithmic manipulation of Fibonacci identities. In: Application of Fibonacci Numbers, vol. 6, pp. 389-408. Kluwer Academic, Dordrecht (1996)
5. Ribenboim, P: My Numbers, My Friends. Springer, New York (2000)
6. Baker, A: The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$. J. Lond. Math. Soc. **43**, 1-9 (1968)
7. Stroeker, RJ, Tzanakis, N: On the elliptic logarithm method for elliptic Diophantine equations: reflections and an improvement. Exp. Math. **8**, 135-149 (1999)
8. Stroeker, RJ, Tzanakis, N: Computing all integer solutions of a genus 1 equation. Math. Comput. **72**, 1917-1933 (2003)
9. Zagier, D: Large integral points on elliptic curves. Math. Comput. **48**, 425-436 (1987)
10. Zhu, H, Chen, J: Integral points on $y^2 = x^3 + 27x - 62$. J. Math. Study **42**(2), 117-125 (2009)
11. Wu, H: Points on the elliptic curve $y^2 = x^3 + 27x - 62$. Acta Math. Sin., Chin. Ser. **53**(1), 205-208 (2010)
12. He, Y, Zhang, W: An elliptic curve having large integral points. Czechoslov. Math. J. **60**(135), 1101-1107 (2010)
13. Mignotte, M, Pethő, A: Sur les carrés dans certanies suites de Lucas. J. Théor. Nr. Bordx. **5**(2), 333-341 (1993)
14. Ribenboim, P: An algorithm to determine the points with integral coordinates in certain elliptic curves. J. Number Theory **74**, 19-38 (1999)
15. Nagell, T: Introduction to Number Theory. Wiley, New York (1981)

doi:10.1186/1029-242X-2013-221
Cite this article as: Karaatlı and Keskin: **Integral points on the elliptic curve** $y^2 = x^3 + 27x - 62$. *Journal of Inequalities and Applications* 2013 **2013**:221.