Integer points on a family of elliptic curves

ANDREJ DUJELLA (Zagreb) and ATTILA PETHŐ*(Debrecen)

Dedicated to Professor Kálmán Győry on the occasion of his 60th birthday.

Abstract Let the sequence (c_k) be given by the recursion

$$c_0 = 0, \quad c_1 = 8, \quad c_{k+2} = 14c_{k+1} - c_k + 8, \quad k \geq 0.$$

Let the elliptic curve E_k be defined by the equation $y^2 = (x+1)(3x+1)(c_k x + 1)$. We prove in this paper that if the rank of $E_k(\mathbb{Q})$ is equal to two, or $k \leq 40$, with the possible exceptions $k = 23$ and $k = 37$, then all integer points on E_k are given by

$$(x, y) \in \{(-1, 0),\ (0, \pm 1),\ (c_{k-1}, \pm s_{k-1}t_{k-1}(2c_k - s_k t_k)),\ (c_{k+1}, \pm s_{k+1}t_{k+1}(2c_k + s_k t_k))\}.$$

1 Introduction

A set D of m positive integers is called a *Diophantine m-tuple* if the product of any two distinct elements of D increased by 1 is a perfect square. The first example of a Diophantine quadruple - $\{1, 3, 8, 120\}$ - was found by Fermat (see [6, p. 517]). In 1969, Baker and Davenport [2] proved that if d is a positive integer such that $\{1, 3, 8, d\}$ is a Diophantine quadruple, then d has to be 120.

Recently, in [9], we generalized this result to all Diophantine triples of the form $\{1, 3, c\}$. The fact that $\{1, 3, c\}$ is a Diophantine triple implies that $c = c_k$ for some positive integer k, where the sequence (c_k) is given by

$$c_0 = 0, \quad c_1 = 8, \quad c_{k+2} = 14c_{k+1} - c_k + 8, \quad k \geq 0.$$

Let $c_k + 1 = s_k^2$, $3c_k + 1 = t_k^2$ with positive integers s_k, t_k. It is easy to check that

$$c_{k\pm1}c_k + 1 = (2c_k \pm s_k t_k)^2.$$

The main result of [9] is the following theorem.

[1]Research partially supported by Hungarian National Foundation for Scientific Research Grants No. 25157 and 29330.

THEOREM 1 *Let k be a positive integer. If d is an integer which satisfies the system of equations*

$$d+1=x_1^2, \quad 3d+1=x_2^2, \quad c_kd+1=x_3^2, \tag{1}$$

then $d \in \{0, c_{k-1}, c_{k+1}\}$.

Eliminating d from the system (1) we obtain the following system of Pellian equations

$$x_3^2 - c_kx_1^2 = 1 - c_k \tag{2}$$
$$3x_3^2 - c_kx_2^2 = 3 - c_k. \tag{3}$$

We used the theory of Pellian equations and some congruence relations to reformulate the system (2) and (3) to four equations of the form $v_m = w_n$, where (v_m) and (w_n) are binary recursive sequences. After that, a comparison of the upper bound for the solutions obtained from the theorem of Baker and Wüstholz [3] with the lower bound obtained from the congruence condition modulo c_k^2 finished the proof for $k \geq 76$. The statement for $1 \leq k \leq 75$ was proved by a variant of the reduction procedure due to Baker and Davenport [2].

Similar results are proved in [7] and [8] for Diophantine triples of the form $\{k-1, k+1, 4k\}$ and $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$. In the second triple F_n denotes the n-th Fibonacci number.

It is clear that every solution $(d, x_1, x_2, x_3) \in \mathbb{Z}^4$ of (1) induce an integer point on the elliptic curve

$$E_k: \qquad y^2 = (x+1)(3x+1)(c_kx+1), \tag{4}$$

with $y = x_1x_2x_3$ and $x = d$. The purpose of the present paper is to prove that the converse of this statement is true, provided the rank of $E_k(\mathbb{Q})$ is equal to 2. As we will see in Proposition 2, for all $k \geq 2$ the rank of $E_k(\mathbb{Q})$ is always ≥ 2. Our main result is

THEOREM 2 *Let k be a positive integer. If* $\operatorname{rank}(E_k(\mathbb{Q})) = 2$ *or $k \leq 40$, with the possible exceptions $k = 23$ and $k = 37$, then all integer points on E_k are given by*

$$(x,y) \in \{(-1,0),\ (0,\pm 1),\ (c_{k-1}, \pm s_{k-1}t_{k-1}(2c_k - s_kt_k)),\ (c_{k+1}, \pm s_{k+1}t_{k+1}(2c_k + s_kt_k))\}.$$

2 Torsion group

Under the substitution $x \leftrightarrow 3c_kx$, $y \leftrightarrow 3c_ky$ the curve E_k is transformed into the following Weierstraß form

$$\begin{aligned} E_k': \qquad y^2 &= x^3 + (4c_k+3)x^2 + (3c_k^2 + 12c_k)x + 9c_k^2 \\ &= (x+3c_k)(x+c_k)(x+3). \end{aligned}$$

There are three rational points on E'_k of order 2, namely

$$A_k = (-3c_k, 0), \quad B_k = (-c_k, 0), \quad C_k = (-3, 0),$$

and also other two, more or less obvious, rational points on E'_k, namely

$$P_k = (0, 3c_k), \quad R_k = (s_k t_k + 2s_k + 2t_k + 1, (s_k + t_k)(s_k + 2)(t_k + 2)).$$

Note that if $k = 1$, then $R_1 = C_1 - P_1$.

Lemma 1 $E'_k(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. From [17, Main Theorem 1] it follows immediately that $E'_k(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $E'_k(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, and the later is possible iff there exist integers α and β such that $\frac{\alpha}{\beta} \notin \{-2, -1, -\frac{1}{2}, 0, 1\}$ and

$$c_k - 3 = \alpha^4 + 2\alpha^3\beta, \quad 3c_k - 3 = 2\alpha\beta^3 + \beta^4.$$

Now, we have

$$4c_k - 6 = (\alpha^2 + \alpha\beta + \beta^2)^2 - 3\alpha^2\beta^2. \tag{5}$$

Since c_k is even, the left hand side of (5) is $\equiv 2 \pmod 8$. If α and β are both even then the right hand side of (5) is is divisible by 8, and if α and β are both odd then the right hand side of (5) is $\equiv 6 \pmod 8$, a contradiction. Hence, $E'_k(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. ■

3 The independence of P_k and R_k

In this section we will often use the following 2-descent Proposition (see [12, 4.1, p.37]).

Proposition 1 *Let $P = (x', y')$ be a $\mathbb{Q}$-rational point on E, an elliptic curve over $\mathbb{Q}$ given by the equation*

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma),$$

where $\alpha, \beta, \gamma \in \mathbb{Q}$. Then there exists a $\mathbb{Q}$-rational point $Q = (x, y)$ on E such that $2Q = P$ iff $x' - \alpha$, $x' - \beta$, $x' - \gamma$ are all $\mathbb{Q}$-rational squares.

Lemma 2 $P_k, P_k + A_k, P_k + B_k, P_k + C_k \notin 2E'_k(\mathbb{Q})$.

Proof. We have:

$$\begin{aligned} P_k + A_k &= (-c_k - 2, -2c_k + 2), \\ P_k + B_k &= (-3c_k + 6, 6c_k - 18), \\ P_k + C_k &= (c_k^2 - 4c_k, -c_k^3 + 4c_k^2 - 3c_k). \end{aligned}$$

It follows immediately from Proposition 1 that $P_k, P_k + A_k, P_k + B_k \notin 2E'_k(\mathbb{Q})$. If $P_k + C_k \in 2E'_k(\mathbb{Q})$, then $c_k^2 - c_k = \square$, which is impossible. ■

LEMMA 3 $R_k, R_k+A_k, R_k+B_k, R_k+C_k \notin 2E'_k(\mathbb{Q})$.

Proof. We have:

$$\begin{aligned}
R_k &= (s_kt_k+2s_k+2t_k+1,(t_k+s_k)(s_k+2)(t_k+2)),\\
R_k+A_k &= (2s_k-2t_k-s_kt_k+1,(s_k-t_k)(s_k+2)(t_k-2)),\\
R_k+B_k &= (2t_k-2s_k-s_kt_k+1,(t_k-s_k)(s_k-2)(t_k+2)),\\
R_k+C_k &= (s_kt_k-2s_k-2t_k+1,(t_k+s_k)(2-s_k)(t_k-2)).
\end{aligned}$$

Since $2s_k-2t_k-s_kt_k+4=(s_k+2)(2-t_k)<0$ and $2t_k-2s_k-s_kt_k+4=(t_k+2)(2-s_k)<0$, we have $R_k+A_k, R_k+B_k \notin 2E'_k(\mathbb{Q})$.

If $R_k \in 2E'_k(\mathbb{Q})$, then $(t_k+s_k)(t_k+2)=\square$ and $(t_k+s_k)(s_k+2)=\square$. Let $d=\gcd(t_k+s_k,t_k+2,s_k+2)$. Then d divides $(t_k+2)+(s_k+2)-(t_k+s_k)=4$, and since s_k and t_k are odd, we conclude that $d=1$. Hence, we have

$$t_k+s_k=\square,\quad t_k+2=\square,\quad s_k+2=\square. \tag{6}$$

Consider the sequence $(t_k+s_k)_{k\in\mathbb{N}}$. It follows easily by induction that $t_k+s_k=2a_{k+1}$, where

$$a_0=0,\quad a_1=1,\quad a_{k+2}=4a_{k+1}-a_k,\quad k\geq 0. \tag{7}$$

Thus, (6) implies $a_{k+1}=2\square$, and this is impossible by a theorem of Mignotte and Pethő [14] (see also [16]) which says that $a_k=\square, 2\square, 3\square$ or $6\square$ implies $k\leq 3$.

If $R_k+C_k \in 2E'_k(\mathbb{Q})$, then $(t_k+s_k)(t_k-2)=\square$ and $(t_k+s_k)(s_k-2)=\square$. This implies $t_k+s_k=\square$ and we obtain a contradiction as above. ∎

LEMMA 4 *If $k\geq 2$, then* $R_k+P_k, R_k+P_k+A_k, R_k+P_k+B_k, R_k+P_k+C_k \notin 2E'_k(\mathbb{Q})$.

Proof. As in the proof of Lemmas 2 and 3, we use Proposition 1.

If $R_k+P_k+A_k \in 2E'_k(\mathbb{Q})$ then $0>c_k(s_k+2)(s_k-t_k)=\square$, and if $R_k+P_k+B_k \in 2E'_k(\mathbb{Q})$ then $0>c_k(s_k-2)(s_k-t_k)=\square$. Hence, $R_k+P_k+A_k$, $R_k+P_k+B_k \notin 2E'_k(\mathbb{Q})$.

If $R_k+P_k \in 2E'_k(\mathbb{Q})$ then

$$3c_k(t_k+s_k)(t_k+2)=\square,\quad c_k(t_k+s_k)(s_k+2)=\square,\quad 3(s_k+2)(t_k+2)=\square. \tag{8}$$

Substituing $2c_k=(t_k+s_k)(t_k-s_k)$ in (8) we obtain

$$(t_k-s_k)(t_k+2)=6\square,\quad (t_k-s_k)(s_k+2)=2\square,\quad (s_k+2)(t_k+2)=3\square.$$

Let $d=\gcd(s_k+2,t_k+2)$. Then the relation $t_k^2-3s_k^2=-2$ implies $d|6$. Since t_k+2 is odd, we have $d\in\{1,3\}$. Hence we obtain

$$t_k-s_k=6\square \quad\text{or}\quad t_k-s_k=2\square. \tag{9}$$

But $t_k - s_k = 2a_k$, where (a_k) is defined by (7). Thus (9) implies $a_k = \Box$ or $3\Box$. According to [14], this is possible only if $k = 2$. But $(s_2, t_2) = (11, 19)$ and $(s_2 + 2)(t_2 + 2) \neq 3\Box$.

If $R_k + P_k + C_k \in 2E'_k(\mathbb{Q})$ then

$$3c_k(t_k + s_k)(t_k - 2) = \Box, \quad c_k(t_k + s_k)(s_k - 2) = \Box, \quad 3(s_k - 2)(t_k - 2) = \Box.$$

Arguing as before, we obtain

$$(t_k - s_k)(t_k - 2) = 6\Box, \quad (t_k - s_k)(s_k - 2) = 2\Box, \quad (s_k - 2)(t_k - 2) = 3\Box,$$

and conclude that

$$t_k - s_k = 6\Box \quad \text{or} \quad t_k - s_k = 2\Box. \tag{10}$$

As we have already seen, it is possible only for $(s_2, t_2) = (11, 19)$, but then $(s_2 - 2)(t_2 - 2) \neq 3\Box$. ■

Proposition 2 *If $k \geq 2$, then the points P_k and R_k generate a subgroup of rank 2 in $E'_k(\mathbb{Q})/E'_k(\mathbb{Q})_{\text{tors}}$.*

Proof. We have to prove that $mP_k + nR_k \in E'_k(\mathbb{Q})_{\text{tors}}$, $m, n \in \mathbb{Z}$, implies $m = n = 0$.

Assume $mP_k + nR_k = T \in E'_k(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, A_k, B_k, C_k\}$ with $(m, n) \neq (0, 0)$. If m and n are not both even, then $T \equiv P_k, R_k$ or $P_k + R_k \pmod{2E'_k(\mathbb{Q})}$, which is impossible by Lemmas 2, 3 and 4. Hence, m and n are even, say $m = 2m_1$, $n = 2n_1$, and since by Lemma 1 $A_k, B_k, C_k \notin 2E'_k(\mathbb{Q})$,

$$2m_1 P_k + 2n_1 P_k = \mathcal{O}.$$

Thus we obtain $m_1 P_k + n_1 R_k \in E'_k(\mathbb{Q})_{\text{tors}}$. Arguing as above, we obtain that m_1 and n_1 are even, and continuing this process we finally conclude that $m = n = 0$. ■

4 Proof of Theorem 2 $(\text{rank}\,(E_k(\mathbb{Q})) = 2)$

Let $E'_k(\mathbb{Q})/E'_k(\mathbb{Q})_{\text{tors}} = \langle U, V \rangle$ and $X \in E'_k(\mathbb{Q})$. Then there exist integers m, n and a torsion point T such that $X = mU + nV + T$. Also $P_k = m_P U + n_P V + T_P$, $R_k = m_R U + n_R V + T_R$ with integers m_P, n_P, m_R, n_R and with $T_P, T_R \in E'_k(\mathbb{Q})_{\text{tors}}$. Let $\mathcal{U} = \{\mathcal{O}, U, V, U + V\}$. There exist $U_1, U_2 \in \mathcal{U}$, $T_1, T_2 \in E'_k(\mathbb{Q})_{\text{tors}}$ such that $P_k \equiv U_1 + T_1 \pmod{2E'_k(\mathbb{Q})}$, $R_k \equiv U_2 + T_2 \pmod{2E'_k(\mathbb{Q})}$. Let $U_3 \in \mathcal{U}$ such that $U_3 \equiv U_1 + U_2 \pmod{2E'_k(\mathbb{Q})}$. Then $P_k + R_k \equiv U_3 + (T_1 + T_2) \pmod{2E'_k(\mathbb{Q})}$. Now Lemmas 2, 3 and 4 imply that $U_1, U_2, U_3 \neq \mathcal{O}$ and accordingly $\{U_1, U_2, U_3\} = \{U, V, U + V\}$. Therefore $X \equiv X_1 \pmod{2E'_k(\mathbb{Q})}$, where

$$X_1 \in \mathcal{S} = \{\mathcal{O}, A_k, B_k, C_k, P_k, P_k + A_k, P_k + B_k, P_k + C_k, R_k, R_k + A_k, R_k + B_k,$$
$$R_k + C_k, R_k + P_k, R_k + P_k + A_k, R_k + P_k + B_k, R_k + P_k + C_k\}.$$

Let $\{a,b,c\} = \{3, c_k, 3c_k\}$. By [13, 4.6, p.89], the function $\varphi : E'_k(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ defined by

$$\varphi(X) = \begin{cases} (x+a)\mathbb{Q}^{*2}, & \text{if } X = (x,y) \neq \mathcal{O}, (-a,0), \\ (b-a)(c-a)\mathbb{Q}^{*2}, & \text{if } X = (-a,0), \\ \mathbb{Q}^{*2}, & \text{if } X = \mathcal{O} \end{cases}$$

is a group homomorphism.

This fact and Theorem 1 imply that it is sufficient to prove that for all $X_1 \in \mathcal{S} \setminus P_k$, $X_1 = (3c_k u, 3c_k v)$, the system

$$x+1 = \alpha\Box, \quad 3x+1 = \beta\Box, \quad c_k x + 1 = \gamma\Box \tag{11}$$

has no integer solution, where $\Box$ denotes a square of a rational number, and α, β, γ are defined by $u+1 = \alpha$, $3u+1 = \beta$, $c_k u + 1 = \gamma$ if all those numbers are $\neq 0$, and if e.g. $u+1 = 0$ then we choose $\alpha = \beta\gamma$ (so that $\alpha\beta\gamma = \Box$). Note that for $X_1 = P_k$ we obtain the system $x+1 = \Box$, $3x+1 = \Box$, $c_k x + 1 = \Box$, which is completely solved in Theorem 1.

For $X_1 \in \{A_k, B_k, P_k + A_k, P_k + B_k, R_k + A_k, R_k + B_k, R_k + P_k + A_k, R_k + P_k + B_k\}$ exactly two of the numbers α, β, γ are negative and thus the system (11) has no integer solution.

The rest of the proof falls naturally into 7 parts. By a' we will denote the square free part of an integer a.

1) $X_1 = \mathcal{O}$:
We have

$$x+1 = 3c_k\Box, \quad 3x+1 = c_k\Box, \quad c_k x + 1 = 3\Box. \tag{12}$$

From the second equation in (12) we see that $3 \not| c'_k$ and thus the first and second equations imply that c'_k divides $3x+1$ and $x+1$. Accordingly, $c'_k | 3(x+1) - (3x+1) = 2$ and we conclude that $c'_k = 1$ or 2. Hence,

$$c_k = \Box, \quad \text{or} \quad c_k = 2\Box.$$

However, $c_k = s_k^2 - 1 = \Box$ is obviously impossible, while $c_k = 2w^2$ leads to the system of Pellian equations

$$s_k^2 - 2w^2 = 1, \quad t_k^2 - 6w^2 = 1.$$

This system is solved by Anglin [1], and the only positive solution is $(s_k, t_k, w) = (3, 5, 2)$ which corresponds to $c_k = c_1 = 8$, contradicting our assumption that $k \geq 2$. (Note that for $c_1 = 8$ there is also no solution because in this case the first and the third equations in (12) imply $3|7$.)

2) $X_1 = C_k$:
We have

$$x+1 = c_k(c_k-1)\square, \quad 3x+1 = c_k(c_k-3)\square, \quad c_kx+1 = (c_k-1)(c_k-3)\square.$$

If $3 \not| c_k$ then, as in **1)**, we obtain $c_k' = 1$ or 2, and $c_k = \square$ or $2\square$, which is impossible.

If $c_k = 3e_k$ then e_k' divides $3x+1$ and $3x+3$ and thus $e_k' = 1$ or 2. Hence,

$$c_k = 3\square, \quad \text{or} \quad c_k = 6\square.$$

The relation $c_k = 3\square$ is impossible since it implies $t_k^2 - 1 = 9\square$, while $c_k = 6w^2$ leads to the system of Pellian equations

$$s_k^2 - 6w^2 = 1, \quad t_k^2 - 18w^2 = 1$$

which has no positive solution according to [1].

3) $X_1 = P_k + C_k$:
We have

$$x+1 = 3(c_k-1)\square, \quad 3x+1 = (c_k-3)\square, \quad c_kx+1 = 3(c_k-1)(c_k-3)\square.$$

Since $c_k = s_k^2 - 1$, we see that $c_k \not\equiv 1 \pmod 3$, and thus $x \equiv -1 \pmod 3$. From the second equation we have that $(c_k-3)'$ is not divisible by 3, and then the third equation gives $c_kx+1 \equiv 0 \pmod 3$. This implies $c_k \equiv 1 \pmod 3$, a contradiction.

4) $X_1 = R_k$:
We have

$$x+1 = 6(t_k-s_k)(t_k+2)\square, \quad 3x+1 = 2(t_k-s_k)(s_k+2)\square,$$
$$c_kx+1 = 3(s_k+2)(t_k+2)\square.$$

From the relation $t_k^2 - 3s_k^2 = -2$ it follows that $\gcd(t_k-s_k, s_k+2) = \gcd(t_k-s_k, t_k+2) = 1$ or 3.

If $3 \not| t_k - s_k$ then $[2(t_k-s_k)]'$ divides $x+1$ and $3x+1$, and thus $[2(t_k-s_k)]' = 1$ or 2. Accordingly,

$$t_k - s_k = 2\square \quad \text{or} \quad t_k - s_k = \square.$$

As we have already seen in the proof of Lemma 4, this implies

$$a_k = \square \quad \text{or} \quad a_k = 2\square,$$

and [14] implies again that $k = 2$. Now we obtain $120x + 1 = 91\square$, which is impossible modulo 4.

If $t_k - s_k = 3z_k$ then $(2z_k)'$ divides $x+1$ and $9x+3$. Hence $(2z_k)'$ divides 6, which implies $a_k = \square, 2\square, 3\square$ or $6\square$, and this is possible only if $k=2$. But for $k=2$, $t_k - s_k = 8 \not\equiv 0 \pmod 3$.

5) $X_1 = R_k + C_k$:
We have

$$x+1 = 6(t_k - s_k)(t_k - 2)\square, \quad 3x+1 = 2(t_k - s_k)(s_k - 2)\square,$$
$$c_k x + 1 = 3(s_k - 2)(t_k - 2)\square.$$

This case is completely analogous to the case **4)**.

6) $X_1 = R_k + P_k$:
We have

$$x+1 = (t_k + s_k)(t_k + 2)\square, \quad 3x+1 = (t_k + s_k)(s_k + 2)\square,$$
$$c_k x + 1 = (s_k + 2)(t_k + 2)\square.$$

As in **4)**, we obtain that if $3 \not| t_k + s_k$ then $(t_k + s_k)'$ divides 2, and if $t_k + s_k = 3z_k$ then z_k' divides 6. Hence, we have $a_{k+1} = \square, 2\square, 3\square$ or $6\square$, which is impossible for $k \geq 2$.

7) $X_1 = R_k + P_k + C_k$:
We have

$$x+1 = (t_k + s_k)(t_k - 2)\square, \quad 3x+1 = (t_k + s_k)(s_k - 2)\square,$$
$$c_k x + 1 = (s_k - 2)(t_k - 2)\square.$$

This case is completely analogous to the case **6)**. ∎

Remark 1 It is easy to check that rank $(E_1(\mathbb{Q})) = 1$, and from the proof of the first statement of Theorem 2 (parts **1)**, **2)** and **3)**) it is clear that all integer points on E_1 are given by $(x,y) \in \{(-1,0),\ (0,\pm 1),\ (120,\pm 6479)\}$. Hence Theorem 2 is true for $k=1$.

Remark 2 As the coefficients of E_k grow exponentially, the computation of the rank of E_k for large k is difficult. The following values of rank $(E_k(\mathbb{Q}))$ were computed using the programs SIMATH ([18]) and *mwrank* ([5]):

k	1	2	3	4	5	7	8^*	9	10^*
rank $(E_k(\mathbb{Q}))$	1	2	3	3	2	4	4	3	3

In the cases $k = 8, 10$, the rank is computed assuming the Parity Conjecture. For $k = 6, 11, 12$, under the same conjecture, we obtained that rank $(E_k(\mathbb{Q}))$ is equal to 2 or 4. We also verified by SIMATH that for $k=3$ and $k=4$ (when rank $(E_k(\mathbb{Q})) > 2$) all integer points on E_k are given by the values from Theorem 2.

REMARK 3 Let us mention that Bremner, Stroeker and Tzanakis [4] proved recently a similar result as the first statement of our Theorem 2 for the family of elliptic curves

$$C_k: \quad y^2 = \frac{1}{3}x^3 + (k - \frac{1}{2})x^2 + (k^2 - k + \frac{1}{6})x,$$

under the assumptions rank $(C_k(\mathbb{Q})) = 1$ and $C_k(\mathbb{Q})/C_k(\mathbb{Q})_{\text{tors}} = <(1,k)>$.

5 Proof of Theorem 2 $(3 \leq k \leq 40)$

We pointed out in Remark 2 that the coefficients of E_k are growing very fast. Therefore, using SIMATH[2] we were able to compute the integer points of $E_k(\mathbb{Q})$ only for $k \leq 4$. However, the following elementary argument gives us the proof of the second statement of Theorem 2.

Notice the following relations

$$\begin{aligned}
c_0 = 0, \quad c_1 = 8, \quad c_{k+2} &= 14c_{k+1} - c_k + 8, \quad \text{if } k \geq 0, && (13)\\
t_0 = 1, \quad t_1 = 5, \quad t_{k+2} &= 4t_{k+1} - t_k, \quad \text{if } k \geq 0, && (14)\\
s_0 = 1, \quad s_1 = 3, \quad s_{k+2} &= 4s_{k+1} - s_k, \quad \text{if } k \geq 0, && (15)\\
c_k + 1 = s_k^2 \quad \Longrightarrow \quad c_k &= (s_k+1)(s_k-1), && (16)\\
3c_k + 1 = t_k^2 \quad \Longrightarrow \quad 3c_k &= (t_k+1)(t_k-1), && (17)\\
3(c_k - 1) &= (t_k+2)(t_k-2), && (18)\\
c_k - 3 &= (s_k+2)(s_k-2). && (19)
\end{aligned}$$

We have $8|c_k$ for any $k \geq 0$ by (13). Hence s_k and t_k are odd. We have further $3 \not| c_k - 1$ by (16).

Assume that $(x, y) \in \mathbf{Z}^2$ is a solution of (4). Put $D_1 = \gcd(x+1, 3x+1)$, $D_2 = \gcd(x+1, c_kx+1)$ and $D_3 = \gcd(3x+1, c_kx+1)$. As $D_1 = \gcd(x+1, 3x+1) = \gcd(x+1, 2)$, we have $D_1 = 1$ if $x+1$ is odd, and $D_1 = 2$ if $x+1$ is even. We have further $D_2 = \gcd(x+1, c_kx+1) = \gcd(x+1, c_k-1)$ and $D_3 = \gcd(3x+1, c_kx+1) = \gcd(3x+1, c_k-3)$. Hence D_1, D_2 and D_3 are pairwise relatively prime.

Assume first $D_1 = 1$. Then there exist $x_1, x_2, x_3 \in \mathbf{Z}$ such that

$$\begin{aligned}
x + 1 &= D_2 x_1^2\\
3x + 1 &= D_3 x_2^2\\
c_k x + 1 &= D_2 D_3 x_3^2.
\end{aligned}$$

[2]SIMATH is presently the only available computer algebra system which is capable to compute all integer points of elliptic curves. There is implemented the algorithm of Gebel, Pethő and Zimmer [10].

Eliminating x we obtain the following system of equations

$$\begin{aligned} 3D_2x_1^2 - D_3x_2^2 &= 2 \\ c_kx_1^2 - D_3x_3^2 &= \frac{c_k - 1}{D_2}. \end{aligned}$$

Similarly, if $D_1 = 2$, then (4) implies

$$\begin{aligned} x + 1 &= 2D_2x_1^2 \\ 3x + 1 &= 2D_3x_2^2 \\ c_kx + 1 &= D_2D_3x_3^2, \end{aligned}$$

from which we obtain

$$\begin{aligned} 3D_2x_1^2 - D_3x_2^2 &= 1 \\ 2c_kx_1^2 - D_3x_3^2 &= \frac{c_k - 1}{D_2}. \end{aligned}$$

Hence, to find all integer solutions of (4), it is enough to find all integer solutions of the systems of equations

$$\begin{aligned} d_1x_1^2 - d_2x_2^2 &= j_1, & (20) \\ d_3x_1^2 - d_2x_3^2 &= j_2, & (21) \end{aligned}$$

where

- $d_1 = 3D_2$, D_2 is a square-free divisor of $c_k - 1 = (t_k + 2)(t_k - 2)/3$,
- $d_2 = D_3$, D_3 is a square-free divisor of $c_k - 3 = (s_k + 2)(s_k - 2)$, which is not divisible by 3,
- $(d_3, j_1, j_2) = (c_k, 2, \frac{c_k-1}{D_2})$ or $(d_3, j_1, j_2) = (2c_k, 1, \frac{c_k-1}{D_2})$.

We expect that most of the systems (20)–(21) are not solvable. To exclude as early as possible the unsolvable systems we considered the equations (20) and (21) separately modulo appropriate prime powers.

As $8|c_k$ and $c_k|d_3$, and d_2 and j_2 are odd, the equation (21) is solvable modulo 8 only if $-d_2j_2 \equiv 1 \pmod 8$.

Assume that equation (20) is solvable. Let p be an odd prime divisor of d_2. Then (20) implies

$$d_1x_1^2 \equiv j_1 \pmod p,$$

hence

$$(d_1x_1)^2 \equiv j_1d_1 \pmod p,$$

i.e. $\left(\frac{j_1d_1}{p}\right) = 1$, where $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol. Similarly, (21) implies $\left(\frac{j_2d_3}{p}\right) = 1$. If q and r are odd prime divisors of d_1 and d_3 respectively, then we obtain the following conditions for the solvability of (20) and (21): $\left(\frac{-j_1d_2}{q}\right) = 1$ and $\left(\frac{-j_2d_2}{r}\right) = 1$.

Let finally p_1 be an odd prime divisor of j_2, such that $\mathrm{ord}_{p_1}(j_2)$ is odd. Then a necessary condition for solvability of equation (21) is: $\left(\frac{d_2d_3}{p_1}\right) = 1$.

We performed this test for $3 \leq k \leq 40$ and we found that, apart from the systems listed in the following table, all are unsolvable except those of the form

$$\begin{aligned} 3x_1^2 - x_2^2 &= 2, \\ c_kx_1^2 - x_3^2 &= c_k - 1, \end{aligned}$$

and this system is equivalent to the system (2) and (3) which is completely solved by Theorem 1.

k	d_1, d_2, d_3, j_1, j_2
19	251210975091, 44809, 3371344269872647091408, 2, 40261110431
23/1	380631510488414383527682077, 11263976658479, 253754340325609589018454720, 1, 1
23/2	19509779867757, 11263976658479, 25375430325609589018454720, 1, 19509779867761
23/3	58529339603283, 1, 126877170162804794509227360, 2, 6503259955919
35	20288310329233162249058888791445649852717, 2254256703248129138784320976827294428079, 13525540219488774832705925860963766568480, 1, 1
37	187060083, 1489467623820555129, 1311942540724389723505929002667880175005208, 2, 21040446251556347115048521645334887

We considered in the case $k = 19$ equations (20) and (21), with the values of

d_1, d_2, d_3, j_1, j_2 given in the table, modulo 5. We obtained

$$\begin{aligned} x_1^2 - 4x_2^2 &\equiv 2 \pmod 5, \\ 3x_1^2 - 4x_3^2 &\equiv 1 \pmod 5. \end{aligned}$$

The first congruence implies $x_1^2 \equiv 1$, 2 or 3 $\pmod 5$, and the second congrunce implies $x_1^2 \equiv 0$, 2 or 4 $\pmod 5$. Hence, $x_1^2 \equiv 2 \pmod 5$, which is a contradiction.

In the cases $k = 23/3$ and $k = 35$ we used arithmetical properties of some real quadratic number fields.

In the case $k = 23/3$ we have $d_3 = 126877170162804794509227360$. The fundamental unit of the order $\mathbb{Z}[\sqrt{d_3}] = \mathbb{Z}[\sqrt{d_2 d_3}]$ is $\varepsilon = 11263976658481 + \sqrt{d_3}$. By a theorem of Nagell [15, Theorem 108a] the base solution of the equation

$$x_3^2 - 126877170126280479450922736 0 x_1^2 = -6503259955919$$

satisfies $0 < x_1^{(0)} < 1$, which is impossible.

In the case $k = 35$ the fundamental unit of the order $\mathbb{Z}[\sqrt{d_1 d_2}]$ is $u + \sqrt{d_1 d_2}$, where $u = 6762770109744387416352962930481883284238$. A necessary condition for the solvability of the equation $d_1 x_1^2 - d_2 x_2^2 = 1$ is that $2d_1 | (u+1)$ (see [11]). But $\frac{u+1}{2d_1} = \frac{1}{6}$, and hence the last equation has no solution. ■

In the remaining three cases $k = 23/1$, $23/2$ and 37 all our methods fail to work.

References

[1] W. A. Anglin, 'Simultaneous Pell equations', *Math. Comp.* 65 (1996), 355–359.

[2] A. Baker and H. Davenport, 'The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$', *Quart. J. Math. Oxford Ser. (2)* 20 (1969), 129–137.

[3] A. Baker and G. Wüstholz, 'Logarithmic forms and group varieties', *J. Reine Angew. Math.* 442 (1993), 19–62.

[4] A. Bremner, R. J. Stroeker and N. Tzanakis, 'On sums of consecutive squares', *J. Number Theory* 62 (1997), 39–70.

[5] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 1997.

[6] L. E. Dickson, *History of the Theory of Numbers, Vol. 2*, Chelsea, New York, 1992.

[7] A. Dujella, 'The problem of the extension of a parametric family of Diophantine triples', *Publ. Math. Debrecen* 51 (1997), 311–322.

[8] A. Dujella, 'A proof of the Hoggatt-Bergum conjecture', *Proc. Amer. Math. Soc.*, 127 (1999), 1999–2005.

[9] A. Dujella and A. Pethő, 'A generalization of a theorem of Baker and Davenport', *Quart. J. Math. Oxford Ser. (2)* 49 (1998), 291–306.

[10] J. Gebel, A. Pethő and H. G. Zimmer, 'Computing integral points on elliptic curve', *Acta Arith.* 68 (1994), 171–192.

[11] A. Grelak, A. Grytczuk, 'On the diophantine equation $ax^2 - by^2 = c$', *Publ. Math. Debrecen* 44 (1994), 291–299.

[12] D. Husemöller, *Elliptic Curves*, Springer-Verlag, New York, 1987.

[13] A. Knapp, *Elliptic Curves*, Princeton Univ. Press, 1992.

[14] M. Mignotte and A. Pethő, 'Sur les carres dans certaines suites de Lucas', *J. Théor. Nombres Bordeaux* 5 (1993), 333–341.

[15] T. Nagell, *Introduction to Number Theory*, Almqvist, Stockholm; Wiley, New York, 1951.

[16] K. Nakamula, A. Pethő, 'Squares in binary recurrence sequences', in: *Number Theory, Diophantine, Computational and Algebraic Aspects* (K. Győry, A. Pethő, V. T. Sós, eds.), Walter de Gruyter, Berlin, 1998, pp. 409–421.

[17] K. Ono, 'Euler's concordant forms', *Acta Arith.* 78 (1996), 101–123.

[18] SIMATH manual, Saarbrücken, 1997.

Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb
Croatia
E-mail: duje@math.hr

Institute of Mathematics
and Computer Science
Lajos Kossuth University
H-4010 Debrecen P.O. Box 12
Hungary
E-mail: pethoe@math.klte.hu