A parametric family of elliptic curves

ANDREJ DUJELLA (Zagreb)

(extended version)

Abstract

Let $k \geq 3$ be an integer and let E_k be the elliptic curve given by

$$E_k: \qquad y^2 = ((k-1)x+1)((k+1)x+1)(4kx+1).$$

It is proven that if $\operatorname{rank}(E_k(\mathbf{Q})) = 1$ or $k \leq 1000$, then all integer points on E_k are given by

$$(x, y) \in \{(0, \pm 1),\ (16k^3 - 4k, \pm(128k^6 - 112k^4 + 20k^2 - 1))\}.$$

The same result is also proven for two subfamilies with rank equal 2 and for one subfamily with rank equal 3.

1 Introduction

A set of positive integers $\{a_1, a_2, \ldots, a_m\}$ is called *a Diophantine m-tuple* if $a_i a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$. The problem of construction of Diophantine m-tuples has a long history (see [6]). Diophantus found a set of four positive rationals with the above property. However, the first Diophantine quadruple was found by Fermat, and it was the set $\{1, 3, 8, 120\}$.

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, the theorem of Baker and Davenport has been generalized to some parametric families of Diophantine triples ([7, 8, 10]). The main result of [7] is the following theorem.

Theorem 1 *Let $k \geq 2$ be an integer. If the set $\{k-1, k+1, 4k, d\}$ is a Diophantine quadruple, then d has to be $16k^3 - 4k$.*

---

[0]1991 *Mathematics Subject Classification:* 11G05, 11D09, 11Y50.

Eliminating d from the system

$$(k-1)d+1=x_1^2, \quad (k+1)d+1=x_2^2, \quad 4kd+1=x_3^2, \tag{1}$$

we obtain the system

$$(k+1)x_1^2-(k-1)x_2^2 = 2, \tag{2}$$
$$4kx_1^2-(k-1)x_3^2 = 3k+1, \tag{3}$$

and then we can reformulate this system into the equation $v_m=w_n$, where (v_m) and (w_n) are binary recursive sequences defined by

$$\begin{aligned} v_0=1, \quad v_1=2k-1, \quad v_{m+2} &= 2kv_{m+1}-v_m, \quad m\geq 0, \\ w_0=1, \quad w_1=3k-2, \quad w_{n+2} &= (4k-2)w_{n+1}-w_n, \quad n\in \mathbf{Z}. \end{aligned}$$

In order to prove Theorem 1, it suffices to prove that all solutions of the equation $v_m=w_n$ are given by $v_0=w_0=1$ and $v_2=w_{-2}=4k^2-2k-1$, which correspond to $d=0$ and $d=16k^3-4k$. A comparison of the upper bound for solutions, obtained from the theorem of Rickert [23] on simultaneous rational approximations to the numbers $\sqrt{(k-1)/k}$ and $\sqrt{(k+1)/k}$, with the lower bound, obtained from the congruence condition modulo $4k(k-1)$, finishes the proof for $k\geq 29$. In the proof of Theorem 1 for $k\leq 28$ we used Grinstead's method [15].

It is clear that every solution of the system (1) induces an integer point on the elliptic curve

$$E_k: \qquad y^2=((k-1)x+1)((k+1)x+1)(4kx+1).$$

Our conjecture is that the converse of this statement is also true.

Conjecture 1 *Let $k\geq 3$ be an integer. All integer points on E_k are given by*

$$(x,y)\in\{(0,\pm 1),\,(16k^3-4k,\pm(128k^6-112k^4-20k^2-1))\}.$$

In this paper we will prove Conjecture 1 under assumption that rank $(E_k(\mathbf{Q}))=1$. This condition is not unrealistic since "the generic rank" of the corresponding elliptic surface is equal 1. We will also prove Conjecture 1 for two subfamilies of curves with rank equal 2 and for one subfamily with rank equal 3. Finally, using properties of Pellian equations, we will prove Conjecture 1 for all k in the range $3\leq k\leq 1000$.

Let us note that in [11] the family of elliptic curves

$$C_l: \qquad y^2 = (x+1)(3x+1)(c_l x+1),$$

where $c_1 = 8$, $c_2 = 120$, $c_{l+2} = 14c_{l+1} - c_l + 8$ for $l \geq 1$, was considered. It is proven that if $\operatorname{rank}(C_l(\mathbf{Q})) = 2$ or $l \leq 40$, with possible exceptions $l = 23$ and $l = 37$, then all integer points on C_l are given by

$$x \in \{-1, 0, c_{l-1}, c_{l+1}\}.$$

In particular, for $l = 1$ it follows that all integer points on E_2 are given by

$$(x,y) \in \{(-1,0),\ (0,\pm 1),\ (120, \pm 6479)\}.$$

2 Torsion group

The coordinate transformation

$$x \mapsto \frac{x}{4k(k-1)(k+1)}, \quad y \mapsto \frac{y}{4k(k-1)(k+1)}$$

applied on the curve E_k leads to the elliptic curve

$$\begin{aligned} E'_k: \qquad y^2 &= (x+4k^2+4k)(x+4k^2-4k)(x+k^2-1) \\ &= x^3 + (9k^2-1)x^2 + 24k^2(k^2-1)x + 16k^2(k^2-1)^2. \end{aligned}$$

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

$$A_k = (-4k^2-4k, 0), \quad B_k = (-4k^2+4k, 0), \quad C_k = (-k^2+1, 0),$$

and also another obvious rational point on E'_k, namely

$$P_k = (0, 4k^3 - 4k).$$

We will show that the point P_k cannot be of finite order.

Theorem 2 $E'_k(\mathbf{Q})_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$

Proof. Assume that $E'_k(\mathbf{Q})_{\text{tors}}$ contains a subgroup isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$. Then a theorem of Ono [22, Main Theorem 1] implies that $3k^2+4k+1$ and $3k^2-4k+1$ are perfect squares. Since $\gcd(3k+1, k+1) = \gcd(3k-1, k-1) \in \{1,2\}$, we have

$$3k+1 = \alpha^2, \quad k+1 = \beta^2, \quad 3k-1 = 2\gamma^2, \quad k-1 = 2\delta^2 \tag{4}$$

or

$$3k+1=2\alpha^2, \quad k+1=2\beta^2, \quad 3k-1=\gamma^2, \quad k-1=\delta^2. \tag{5}$$

From $k=2\delta^2+1$ it follows that k is odd. On the other hand, from $\alpha^2-\beta^2=2k$ it follows that k is even, a contradiction. Similarly, relation (5) implies $k=2\beta^2-1$ and $\gamma^2-\delta^2=2k$, which again leads to a contradiction.

Hence, $E'_k(\mathbf{Q})_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ or $E'_k(\mathbf{Q})_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$, and according to the theorem of Ono the latter is possible iff there exist integers α and β such that $\frac{\alpha}{\beta} \notin \{-2,-1,-\frac{1}{2},0,1\}$ and

$$3k^2+4k+1=\alpha^4+2\alpha^3\beta, \quad 3k^2-4k+1=2\alpha\beta^3+\beta^4.$$

Now we have

$$(\alpha^2+\alpha\beta+\beta^2)^2-3\alpha^2\beta^2=6k^2+2 \tag{6}$$

which is impossible since left hand side of (6) is $\equiv 0$ or $1 \pmod 3$, and the right hand side of (6) is $\equiv 2 \pmod 3$. ■

Corollary 1 $\operatorname{rank}(E'_k(\mathbf{Q})) \geq 1$

PROOF. By Theorem 2, the point $P_k=(0,4k^3-4k)$ on E'_k is not of finite order, which shows that $\operatorname{rank}(E'_k(\mathbf{Q})) \geq 1$. ■

3 Case $\operatorname{rank}(E_k(\mathbf{Q}))=1$

In the rest of the paper we will often use the following 2-descent Proposition (see [16, 4.1, p.37], [18, 4.2, p.85]).

Proposition 1 *Let E be an elliptic curve over a field k of characteristic not equal to 2 or 3. Suppose E is given by*

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

with $\alpha,\beta,\gamma \in k$. For $P=(x',y') \in E(k)$, there exists $Q=(x,y) \in E(k)$ such that $2Q=P$ iff $x'-\alpha$, $x'-\beta$, $x'-\gamma$ are squares in k.

Lemma 1 $P_k, P_k+A_k, P_k+B_k, P_k+C_k \notin 2E'_k(\mathbf{Q})$

PROOF. We have

$$\begin{aligned} P_k + A_k &= (-4k^2 + 2k + 2, -6k^2 + 4k + 2), \\ P_k + B_k &= (-4k^2 - 2k + 2, 6k^2 + 4k - 2), \\ P_k + C_k &= (8k^2, -36k^3 + 4k). \end{aligned}$$

Since none of the numbers $k^2 - 1$, $-3k^2 + 2k + 1$, $-3k^2 - 2k + 1$ and $9k^2 - 1$ is a perfect square (for $k \geq 2$), Proposition 1 implies that $P_k, P_k + A_k, P_k + B_k, P_k + C_k \notin 2E'_k(\mathbf{Q})$. ∎

Theorem 3 *Let $k \geq 3$ be an integer. If the rank of the elliptic curve*

$$E_k: \qquad y^2 = ((k-1)x + 1)((k+1)x + 1)(4kx + 1)$$

is equal 1, then all integer points on E_k are given by

$$(x, y) \in \{(0, \pm 1), (16k^3 - 4k, \pm(128k^6 - 112k^4 + 20k^2 - 1))\}. \tag{7}$$

PROOF. Let $E'_k(\mathbf{Q})/E'_k(\mathbf{Q})_{\text{tors}} =< U >$ and $X \in E'_k(\mathbf{Q})$. Then we can represent X in the form $X = mU + T$, where m is an integer and T is a torsion point, i.e. $T \in \{\mathcal{O}, A_k, B_k, C_k\}$. Similarly, $P_k = m_P U + T_P$ for an integer m_P and a torsion point T_P. By Lemma 1 we have that m_P is odd. Hence, $U \equiv P + T_P \pmod{2E'_k(\mathbf{Q})}$. Therefore we have $X \equiv X_1 \pmod{2E'_k(\mathbf{Q})}$, where

$$X_1 \in \mathcal{S} = \{\mathcal{O}, A_k, B_k, C_k, P_k, P_k + A_k, P_k + B_k, P_k + C_k\}. \tag{8}$$

Let $\{a, b, c\} = \{4k^2 + 4k, 4k^2 - 4k, k^2 - 1\}$. By [18, 4.6, p.89], the function $\varphi : E'_k(\mathbf{Q}) \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ defined by

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

is a group homomorphism.

Therefore, in order to find all integer points on E_k, it suffices to solve in integers all systems of the form

$$(k-1)x + 1 = \alpha\square, \quad (k+1)x + 1 = \beta\square, \quad 4kx + 1 = \gamma\square \tag{9}$$

where for $X_1 = (4k(k^2 - 1)u, 4k(k^2 - 1)v) \in \mathcal{S}$, numbers α, β, γ are defined by $\alpha = (k-1)u + 1$, $\beta = (k+1)u + 1$, $\gamma = 4ku + 1$ if all of these three expressions are nonzero, and if e.g. $(k-1)u+1=0$ then we define $\alpha=\beta\gamma$. Here $\square$ denotes a square of a rational number.

Observe that for $X_1=P_k$ the system (9) becomes

$$(k-1)x+1=\square, \quad (k+1)x+1=\square, \quad 4kx+1=\square.$$

As we said in the introduction, this system is completely solved in [7], and its solutions correspond to the integers points on E_k listed in Theorem 3.

Hence, we have to prove that for $X_1 \in \mathcal{S} \setminus \{P_k\}$, the system (9) has no integer solution.

For $X_1 \in \{A_k, B_k, P_k+A_k, P_k+B_k\}$ exactly two of the numbers α, β, γ are negative and accordingly the system (9) has no integer solution. Let us consider three remaining cases. In the rest of the paper by e' we will denote the square-free part of an integer e.

1) $X_1=\mathcal{O}$
The system (9) becomes

$$(k-1)x+1 = k(k+1)\square, \tag{10}$$
$$(k+1)x+1 = k(k-1)\square, \tag{11}$$
$$4kx+1 = (k-1)(k+1)\square. \tag{12}$$

Since k' divides $(k-1)x+1$ and $(k+1)x+1$, we have $k'=1$ or 2, and it means that $k=\square$ or $2\square$. In the same way we obtain that $k-1=\square$ or $2\square$, and $k+1=\square$ or $2\square$. Thus, between three successive numbers $k-1$, k, $k+1$ we have two squares or two double-squares, a contradiction.

2) $X_1=C_k$
Now the system (9) becomes

$$(k-1)x+1 = k(3k+1)\square,$$
$$(k+1)x+1 = k(3k-1)\square,$$
$$4kx+1 = (3k-1)(3k+1)\square.$$

If k is even, then $(3k-1)(3k+1)\equiv -1 \pmod 4$ and thus the equation $4kx+1=(3k-1)(3k+1)\square$ is impossible modulo 4.

If $k\equiv 1 \pmod 4$, then $(k+1)x+1$ is odd. But $k(3k-1)\equiv 2 \pmod 4$ implies that $k(3k-1)\square$ is even, a contradiction.

If $k\equiv -1 \pmod 4$, then $(k-1)x+1$ is odd, but $k(3k+1)\equiv 2 \pmod 4$ and we have again a contradiction.

3) $X_1 = P_k + C_k$
We have to solve the system

$$\begin{aligned}(k-1)x+1 &= (k+1)(3k+1)\Box,\\ (k+1)x+1 &= (k-1)(3k-1)\Box,\\ 4kx+1 &= (k-1)(k+1)(3k-1)(3k+1)\Box.\end{aligned}$$

Assume that k is even. Since $(k+1)'$ divides $(k-1)x+1$ and $4kx+1$ we have that $(k+1)'|(3k+1)$, and it implies $(k+1)'=1$ and $k+1=\Box$. In the same way we obtain that $k-1=\Box$, and this is impossible.

Assume now that k is odd. Then $(k-1)x+1$ and $(k+1)x+1$ are odd. Furthermore, $(k+1)(3k+1) \equiv 0 \pmod 8$ and since the number $(k+1)(3k+1)\Box = (k-1)x+1$ is odd we should have $(k+1)(3k+1) \equiv 0 \pmod{16}$. It implies $k \equiv 5$ or $7 \pmod 8$.

Similarly, since $(k-1)(3k-1) \equiv 0 \pmod 8$ and $(k-1)(3k-1)\Box = (k+1)x+1$ is odd, we conclude that $(k-1)(3k-1) \equiv 0 \pmod{16}$. It implies $k \equiv 1$ or $3 \pmod 8$ and we get a contradiction. ■

Remark 1 Bremner, Stroeker and Tzanakis [3] proved recently a similar result to our Theorem 3 for the family of elliptic curves

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

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

We come to the following natural question: How realistic is the condition $\operatorname{rank}(E_k(\mathbf{Q})) = 1$? We calculated the rank for $2 \le k \le 100$ using the programs Simath [25] and Mwrank [5]. The rank values are listed in Table 1.

rank $(E_k(\mathbf{Q})) = 1$	$k =$ 2, 3, 5, 7, 8, 9, 12, 13, 17, 18, 24, 26, 29, 33, 35, 36, 41, 44, 51, 55, 57, 58, 61, 64, 66, 67, 70, 73, 75, 78, 79, 82, 85, 86, 87, 89, 92, 96, 98, 100
rank $(E_k(\mathbf{Q})) = 2$	$k =$ 4, 6, 10, 11, 15, 16, 19, 20, 21, 22, 23, 25, 27, 30, 32, 37, 38, 39, 40, 42, 43, 45, 46, 47, 48, 49, 50, 53, 54, 59, 62, 65, 68, 69, 71, 72, 74, 81, 83, 84, 88, 90, 91, 93, 94*, 95, 97, 99
rank $(E_k(\mathbf{Q})) = 3$	$k =$ 14, 31, 34, 52, 56, 60, 63, 76, 80

Table 1:

The rank has been determined unconditionally for k in the range $2 \leq k \leq 100$ except for $k = 94$, when it is computed assuming the Birch and Swinnerton-Dyer Conjecture (Manin's conditional algorithm). We obtained the following distribution of ranks: 41 cases of rank 1, 49 cases of rank 2 and 9 cases of rank 3.

In the range $101 \leq k \leq 200$ we determined the rank unconditionally for all k except for $k = 118$, when we used the Birch and Swinnerton-Dyer Conjecture, and for $k = 122$, when we were able only to conclude that $2 \leq \operatorname{rank}(E_{122}(\mathbf{Q})) \leq 4$. The rank values are listed in Table 2.

rank $(E_k(\mathbf{Q})) = 1$	$k =$ 104, 109, 110, 120, 126, 128, 134, 136, 137, 139, 141, 143, 147, 148, 149, 151, 156, 158, 165, 169, 171, 173, 177, 182, 185, 188, 191, 192, 193, 194, 196,
rank $(E_k(\mathbf{Q})) = 2$	$k =$ 102, 103, 105, 106, 107, 108, 111, 112, 113, 114, 115, 116, 117, 118*, 119, 121, 123, 124, 125, 130, 132, 135, 138, 140, 142, 144, 145, 146, 150, 152, 153, 157, 159, 160, 161, 162, 163, 164, 167, 168, 170, 172, 176, 178, 179, 181, 187, 190, 195, 198, 199, 200
rank $(E_k(\mathbf{Q})) = 3$	$k =$ 101, 127, 129, 131, 133, 154, 155, 166, 174, 175, 180, 183, 186, 189, 197
rank $(E_k(\mathbf{Q})) = 4$	$k =$ 184

Table 2:

In the range $101 \leq k \leq 200$ we obtained the following distribution of ranks: 31 cases of rank 1, 52 cases of rank 2, 15 cases of rank 3 and 1 case of rank 4.

The data from Tables 1 and 2 suggest that the generic rank of the elliptic curve E' over $\mathbf{Q}(k)$ is equal 1, and we will prove this statement in the following theorem.

Theorem 4 $\operatorname{rank} E'(\mathbf{Q}(k)) = 1$

Proof. Let $(x(k), y(k)) \in E'(\mathbf{Q}(k))$ and $x(k) = \frac{p(k)}{q^2(k)}$, where $p(k), q(k)$ are polynomials with integer coefficients. We have

$$p(k) + (k^2 - 1)q^2(k) \;=\; \mu_1(k)\mu_2(k)\square,$$

$$p(k) + (4k^2 - 4k)q^2(k) = \mu_1(k)\mu_3(k)\Box,$$
$$p(k) + (4k^2 + 4k)q^2(k) = \mu_2(k)\mu_3(k)\Box,$$

where $\Box$ denotes a square of a polynomial in $\mathbf{Z}[k]$, and $\mu_1(k), \mu_2(k), \mu_3(k)$ are square-free polynomials in $\mathbf{Z}[k]$. We may also choose that the leading coefficient of $\mu_1(k)$ is positive. After this choice, the triple $(\mu_1(k), \mu_2(k), \mu_3(k))$ is uniquely determined by $x(k)$.

Furthermore, we have $\mu_1(k) | (k-1)(3k-1)$, $\mu_2(k) | (k+1)(3k+1)$ and $\mu_3(k) | 8k$. Hence, $\mu_1(k) \in \{1,\ k-1,\ 3k-1,\ (k-1)(3k-1)\}$, $\mu_2(k) \in \{\pm 1,\ \pm(k-1),\ \pm(3k-1),\ \pm(k-1)(3k-1)\}$, $\mu_3(k) \in \{\pm 1,\ \pm 2,\ \pm k,\ \pm 2k\}$.

We claim that there are exactly eight triples $(\mu_1(k), \mu_2(k), \mu_3(k))$ which may appear, namely the triples

$$\begin{gathered}
(k(k+1),\ k(k-1),\ (k-1)(k+1)), \\
(2(3k+1),\ -2(k-1),\ -(k-1)(3k+1)), \\
(2(k+1),\ -2(3k+1),\ -(k+1)(3k-1)), \\
(k(3k+1),\ k(3k-1),\ (3k-1)(3k+1)),\ \ (1,\ 1,\ 1), \\
(2k(k+1)(3k+1),\ -2k,\ -(k+1)(3k+1)), \\
(2k,\ -2k(k-1)(3k-1),\ -(k-1)(3k-1)), \\
((k+1)(3k+1),\ (k-1)(3k-1),\ (k-1)(k+1)(3k-1)(3k+1)),
\end{gathered} \tag{13}$$

which correspond to the points $\mathcal{O}$, $A(k) = A_k$, $B(k) = B_k$, $C(k) = C_k$, $P(k) = P_k$, $P(k) + A(k)$, $P(k) + B(k)$ and $P(k) + C(k)$.

Let us consider now the specialization $k = 12$. We choose $k = 12$ because $\operatorname{rank}(E'_{12}(\mathbf{Q})) = 1$, $E'_{12}(\mathbf{Q})/E'_{12}(\mathbf{Q})_{\rm tors} = < P_{12} >$ and furthermore square-free parts of all polynomial factors of $(k-1)(3k-1)$, $(k+1)(3k+1)$ and $8k$ respectively, evaluated at $k = 12$, are distinct. Thus, if there are more that 8 choices for $(\mu_1(k), \mu_2(k), \mu_3(k))$ on $E'(\mathbf{Q}(k))$, there will be more than 8 choices on $E'_{12}(\mathbf{Q})$. Since this is not the case, we conclude that all possibilities for $(\mu_1(k), \mu_2(k), \mu_3(k))$ are indeed given by (13).

Let V be an arbitrary point on $E(\mathbf{Q}(k))$. Consider nine points

$$\mathcal{O},\ A(k),\ B(k),\ C(k),\ P(k),\ P(k) + A(k),\ P(k) + B(k),\ P(k) + C(k),\ V.$$

Two of them have equal corresponding triples. By [16, 4.3, p.125], these two points are congruent modulo $2E'(\mathbf{Q}(k))$. We have already proved in Theorem 2 and Lemma 1 that the first eight points are incongruent modulo

$2E'(\mathbf{Q}(k))$ (since the specialization map is a homomorphism). Hence we have two possibilities:

1) $V \equiv T_1 \pmod{2E'(\mathbf{Q}(k))}$,

2) $V \equiv P(k) + T_2 \pmod{2E'(\mathbf{Q}(k))}$,

where $T_i \in \{\mathcal{O}, A(k), B(k), C(k)\}$.

Let $\{D_1, \dots, D_r\}$ be the Mordell-Weil base for $E'(\mathbf{Q}(k))$ and assume that $r \geq 2$. Let $P(k) = \sum_{i=1}^{r} \alpha_i D_i + T$, where T is a torsion point. Consider the point D_r. According to the above discussion, we have two possibilities:

1) $D_r \equiv T_1 \pmod{2E'(\mathbf{Q}(k))}$

It implies $D_r = T_1 + 2F_r$, where $F_r = \sum_{i=1}^{r} \beta_i D_i + T'$, and we obtain $1 = 2\beta_r$, a contradiction.

2) $D_r \equiv P(k) + T_2 \pmod{2E'(\mathbf{Q}(k))}$

Now we have

$$\alpha_1 D_1 + \cdots + \alpha_{r-1} D_{r-1} + (\alpha_r - 1) D_r + T_2 + T \in 2E'(\mathbf{Q}(k)).$$

Hence, α_{r-1} is even and α_r is odd. Analogously, considering the point D_{r-1}, we conclude that α_{r-1} is odd and α_r is even, which leads to a contradiction.

■

If we define the average rank of $E'(\mathbf{Q}(k))$ to be

$$\text{Avg.rank}\, E'(\mathbf{Q}(k)) = \lim_{N \to \infty} \frac{1}{N} \sum_{k=1}^{N} \text{rank}\,(E'_k(\mathbf{Q})),$$

then the Katz-Sarnak Conjecture (see [24]) states that

$$\text{Avg.rank}\, E'(\mathbf{Q}(k)) = \text{rank}\, E'(\mathbf{Q}(k)) + \frac{1}{2} = 1.5\,.$$

This means that at least 50% of curves E_k should have the rank equal 1. As explained in [24], the Katz-Sarnak Conjecture is not in complete agreement with experimental results of Fermigier [12]. Examining an extensive collection of data (66918 curves in 93 families) Fermigier found that $\text{rank}\,(E_t(\mathbf{Q})) = \text{rank}\, E(\mathbf{Q}(t))$ in 32% of cases. Perhaps it can be compared with our situation where we found that in the range $2 \leq k \leq 200$ we have $\text{rank}\,(E'_k(\mathbf{Q})) = \text{rank}\, E'(\mathbf{Q}(k))$ in 36% of cases.

Thus we have reasons to believe that Theorem 3 shows that Conjecture 1 is valid for a large class of positive integers k.

4 The first family with rank ≥ 2

The Katz-Sarnak Conjecture implies, and Tables 1 and 2 confirm, that there are many curves in the family E_k with rank ≥ 2. Therefore, we may try to find an explanation for these additional rational points on E_k. We succeeded in two special cases. Namely, we used SIMATH[1] to find all integer points on E'_k in some cases with rank $(E'_k(\mathbf{Q})) > 1$. Then we transformed these integer points on E'_k to rational points on E_k. After doing it, we noticed some regularities in the appearance of these points. Namely, there were several curves with rational point with x-coordinate equal to $\frac{3}{4}$, and also several curves with two rational points with x-coordinates very close to 6. Analyzing these phenomena, we find two subfamilies of (E_k) which consist of elliptic curves with rank ≥ 2.

More precisely, these families are $E_{k_1(n)}$ and $E_{k_2(m)}$, where $k_1(n) = 3n^2 + 2n - 2$ and $k_2(m) = \frac{1}{2}(3m^2 + 5m)$ for integers $n \neq -1, 0, 1$ and $m \neq -2, -1, 0$.

Let us first consider the family $E_{k_1(n)}$. For the sake of simplicity we denote $E'_{k_1(n)}$ by E^*_n. It is easy to verify that the point

$$\begin{aligned} R_n &= (3(n+1)(3n-1)(3n^2+2n-3)(3n^2+2n-2), \\ &\quad (n+1)(3n-1)(3n+1)(3n^2+2n-3)(3n^2+2n-2)(9n^2+6n-5)) \end{aligned}$$

is a point on E^*_n. Note that x-coordinate of R_n is equal to

$$\frac{3}{4} \cdot 4k_1(n)(k_1(n)-1)(k_1(n)+1).$$

Let $A_n = A_{k_1(n)}$, $B_n = B_{k_1(n)}$, $C_n = C_{k_1(n)}$ and $P_n = P_{k_1(n)}$. Then we have

$$\begin{aligned} R_n + A_n &= (-4n(3n+2)(3n^2+2n-3), \\ &\quad -8(3n+1)(3n^2+2n-3)), \\ R_n + B_n &= \Big(-\tfrac{4(n+1)^2(3n-2)(3n-1)^2(3n+4)}{(3n+1)^2}, \\ &\quad \tfrac{8(n+1)(3n-1)(9n^2+6n-7)(9n^2+6n-5)}{(3n+1)^3} \Big), \\ R_n + C_n &= (-(n-1)(3n+5)(3n^2+2n-2), \\ &\quad -(3n+1)(3n^2+2n-2)(9n^2+6n-7)), \\ R_n + P_n &= (-8(3n^3-3n+1), \\ &\quad 4n(n-1)(n+1)(3n-2)(9n^2+6n-5)), \end{aligned}$$

[1]In SIMATH there is implemented the algorithm of Gebel, Pethő and Zimmer [13] for computing all integer points of the elliptic curve.

$$\begin{aligned}
R_n+P_n+A_n &= \Big(-\tfrac{2(n+1)(3n-1)(2n^2-1)(3n^2+2n-2)}{n^2},\\
&\quad -\tfrac{-2(n-1)(n+1)^2(3n-2)(3n-1)(3n^2+2n-2)}{n^3}\Big),\\
R_n+P_n+B_n &= \Big(-\tfrac{2(3n+1)(3n^2+2n-3)(3n^2+2n-2)(6n^3+2n^2-5n+1)}{(3n-2)^2(n+1)^2},\\
&\quad \tfrac{2n(n-1)(3n^2+2n-3)(3n^2+2n-2)(9n^2+6n-7)(9n^2+6n-5)}{(3n-2)^3(n+1)^3}\Big),\\
R_n+P_n+C_n &= \Big(\tfrac{8(n+1)(3n-1)(n^2+n-1)(3n^2+2n-3)}{(n-1)^2},\\
&\quad -\tfrac{4n(n+1)^2(3n-2)(3n-1)(3n^2+2n-3)(9n^2+6n-7)}{(n-1)^3}\Big).
\end{aligned}$$

Lemma 2 *If* $n \neq -1, 0, 1$, *then* R_n, R_n+A_n, R_n+B_n, R_n+C_n, R_n+P_n, $R_n+P_n+A_n$, $R_n+P_n+B_n$, $R_n+P_n+C_n \notin 2E_n^*(\mathbf{Q})$.

Proof. As in the proof of Lemma 1, we use Proposition 1. For the points R_n+A_n, R_n+B_n, $R_n+P_n+A_n$ and $R_n+P_n+B_n$ the conditions from Proposition 1 are obviously not satisfied, because two of these conditions give $\square < 0$.

If $R_n = (x, y) \in 2E_n^*(\mathbf{Q})$, then we have

$$x + 4k_1^2(n) - 4k_1(n) = (3n^2+2n-3)(3n^2+3n-2)(3n+1)^2 = \square,$$

a contradiction.

If $R_n + C_n = (x, y) \in 2E_n^*(\mathbf{Q})$, then we have

$$x + k_1^2(n) - 1 = 9n^2 + 6n - 7 = (3n+1)^2 - 8 = \square,$$

which implies $3n + 1 = \pm 3$, a contradiction.

If $R_n + P_n = (x, y) \in 2E_n^*(\mathbf{Q})$, then we have

$$x + 4k_1^2(n) + 4k_1(n) = 4n^2(9n^2+6n-5) = \square,$$

which implies $6 = (3n+1)^2 - \square$, a contradiction.

If $R_n + P_n + C_n = (x, y) \in 2E_n^*(\mathbf{Q})$, then we have

$$x + 4k_1^2(n) - 4k_1(n) = \frac{4n^2(3n^2+2n-3)(9n^2+6n-7)}{(n-1)^2} = \square.$$

Since $\gcd(3n^2+2n-3, 9n^2+6n-7) = 1$ or 2, and we have already seen that $9n^2+6n-7 = \square$ is impossible, this implies that

$$3n^2+2n-3 = 2\alpha^2 \quad \text{and} \quad 9n^2+6n-7 = 2\beta^2. \tag{14}$$

The condition $x + k_1^2(n) - 1 = \square$ gives

$$3n^2 + 2n - 1 = \gamma^2. \tag{15}$$

Combining (14) and (15) we obtain the following system of Pellian equations

$$\begin{aligned} \gamma^2 - 2\alpha^2 &= 2, \\ 2\beta^2 - 3\gamma^2 &= -4. \end{aligned}$$

These two equations imply that γ and β are even, say $\gamma = 2\delta$, $\beta = 2\varepsilon$. Define the integer s by $s = \frac{\varepsilon^2-1}{3}$. Then we have: $3s+1 = \varepsilon^2$, $2s+1 = \delta^2$, $4s+1 = \alpha^2$. Hence, s satisfies the equation

$$t^2 = (2s+1)(3s+1)(4s+1), \tag{16}$$

which under substitution $t_1 = 24t$, $s_1 = 24s$ becomes

$$t_1^2 = s_1^3 + 26s_1^2 + 216s_1 + 576. \tag{17}$$

Using SIMATH we find that all integer points on (17) are $(-6,0)$, $(-8,0)$, $(-12,0)$, $(-10,\pm 4)$, $(-9,\pm 3)$, $(-4,\pm 8)$, $(0,\pm 24)$, $(42,\pm 360)$. Hence, the only integer solution of (16) is $s = 0$, which implies $\alpha^2 = 1$ and $n = 1$. ■

Corollary 2 *If* $n \neq -1, 0, 1$, *then* $\operatorname{rank}(E_n^*(\mathbf{Q})) \geq 2$.

PROOF. We claim that the points P_n and R_n generate a subgroup of rank 2 in $E_n^*(\mathbf{Q})/E_n^*(\mathbf{Q})_{\text{tors}}$. We have to prove that $p_1P_n + r_1R_n \in E_n^*(\mathbf{Q})_{\text{tors}}$, $p_1, r_1 \in \mathbf{Z}$, implies $p_1 = r_1 = 0$.

Assume that $p_1P_n + r_1R_n = T \in E_n^*(\mathbf{Q})_{\text{tors}} = \{\mathcal{O}, A_n, B_n, C_n\}$. If p_1 and r_1 are not both even, then $T + P_n \in 2E_n^*(\mathbf{Q})$ or $T + R_n \in 2E_n^*(\mathbf{Q})$ or $T + P_n + R_n \in 2E_n^*(\mathbf{Q})$. But this is impossible by Lemmas 1 and 2. Hence, p_1 and r_1 are even, say $p_1 = 2p_2$, $r_1 = 2r_2$. Since, by Theorem 2, $A_n, B_n, C_n \notin 2E_n^*(\mathbf{Q})$, we have $T = \mathcal{O}$. Hence,

$$2p_2P_n + 2r_2R_n = \mathcal{O}.$$

Thus we obtain $p_2P_n + r_2R_n \in E_n^*(\mathbf{Q})_{\text{tors}}$ and we can continue with the same argumentation to conclude that p_2 and r_2 are even. Continuing this process, we finally conclude that $p_1 = r_1 = 0$. ■

Theorem 5 *If* $\operatorname{rank}(E_n^*(\mathbf{Q})) = 2$, *then all integer points on* E_k, *where* $k = k_1(n)$, *are given by (7).*

Proof. We follow the strategy from the proof of Theorem 3. Let $E_n^*(\mathbf{Q})/E_n^*(\mathbf{Q})_{\rm tors} = <U,V>$ and $X \in E_n^*(\mathbf{Q})$. Let $P_n = m_P U + n_P V + T_P$, $R_n = m_R U + n_R V + T_R$, where $T_P, T_R \in \{\mathcal{O}, A_n, B_n, C_n\}$. Let $\mathcal{U} = \{\mathcal{O}, U, V, U+V\}$. There exist $U_1, U_2 \in \mathcal{U}$, $T_1, T_2 \in E_n^*(\mathbf{Q})_{\rm tors}$ such that $P_n \equiv U_1 + T_1 \pmod{2E_n^*(\mathbf{Q})}$, $R_n \equiv U_2 + T_2 \pmod{2E_n^*(\mathbf{Q})}$. Let $U_3 \in \mathcal{U}$ such that $U_3 \equiv U_1 + U_2 \pmod{2E_n^*(\mathbf{Q})}$ and $T_3 = T_1 + T_2$. Then $P_n + R_n \equiv U_3 + T_3 \pmod{2E_n^*(\mathbf{Q})}$. Now Lemmas 1, 2 imply that $U_1, U_2, U_3 \neq \mathcal{O}$. Hence $\{U_1, U_2, U_3\} = \{U, V, U+V\}$ and $X \equiv X_1 \pmod{2E_n^*(\mathbf{Q})}$, $X_1 \in \mathcal{S} \cup \mathcal{S}_1$, where $\mathcal{S}$ is defined by (8) and

$$\begin{aligned}\mathcal{S}_1 \;=\; \{&R_n,\, R_n + A_n,\, R_n + B_n,\, R_n + C_n,\, R_n + P_n,\, R_n + P_n + A_n,\\ &R_n + P_n + B_n,\, R_n + P_n + C_n\}.\end{aligned}$$

Therefore, we have to solve the systems (9), with numbers α, β, γ defined in the proof of Theorem 3, for $X_1 \in \mathcal{S}_1$. However, for $X_1 \in \{R_n + A_n,\, R_n + B_n,\, R_n + P_n + A_n, R_n + P_n + B_n\}$ the system (9) has no integer solution since exactly two of the numbers α, β, γ are negative. Let us consider four remaining cases.

For the sake of simplicity, in the rest of the proof we will denote $k_1(n)$ by k. Note that from $k = 3n^2 + 2n - 2$ it follows $k \equiv 2$ or $3 \pmod 4$.

1) $X_1 = R_n$
The system (9) becomes

$$(k-1)x + 1 = (3k+1)\Box, \quad (k+1)x + 1 = \Box, \quad 4kx + 1 = (3k+1)\Box.$$

The third equation implies $k \equiv 0$ or $1 \pmod 4$, a contradiction.

2) $X_1 = R_n + C_n$
We have

$$\begin{aligned}(k-1)x + 1 &= (k+1)\Box,\\ (k+1)x + 1 &= (k-1)(3k-1)\Box,\\ 4kx + 1 &= (k-1)(k+1)(3k-1)\Box.\end{aligned}$$

Since $\gcd(k+1, (k-1)(3k-1)) | 8$, we conclude that at least one of the numbers $(k+1)'$ and $[2(k+1)]'$ divides $3k+1$ and accordingly this number divides 2. Hence, $k+1 = \Box$ or $2\Box$. In the same manner we conclude that $k-1 = \Box$ or $2\Box$. We have two possibilities:

$$k + 1 = \Box \quad \text{and} \quad k - 1 = 2\Box, \tag{18}$$

or

$$k+1=2\square \quad \text{and} \quad k-1=\square. \tag{19}$$

The system (18) leads to

$$(3n-1)(n+1)=u^2, \quad 3n^2+2n-3=2v^2. \tag{20}$$

The second equation implies $n \equiv 1 \pmod 4$, and then the first equation implies that there exist integers w and z such that

$$n+1=2w^2, \quad 3n-1=2z^2.$$

Let $s=(wz)^2$. Then we have: $3s+1=(z^2+1)^2$, $2s-1=v^2$. Hence, s satisfies the equation

$$t^2=s(3s+1)(2s-1). \tag{21}$$

By substitution $t_1=6t$, $s_1=6s$, we obtain the elliptic curve

$$t_1^2=s_1^3-s_1^2-6s_1, \tag{22}$$

and using Simath we find that all integer points on (22) are given by $(0,0)$, $(3,0)$, $(-2,0)$, $(-1,\pm 2)$, $(6,\pm 12)$, $(8,\pm 20)$, $(243,\pm 3780)$. Hence, the only integer solution of (21) is $s=1$, which implies $n=1$.

The second equation in (19) implies $(3n+1)^2-10=3\square$, and this is impossible modulo 8.

3) $X_1=R_n+P_n$
We have

$$\begin{aligned}(k-1)x+1 &= k(k+1)(3k+1)\square,\\ (k+1)x+1 &= k(k-1)\square,\\ 4kx+1 &= (k-1)(k+1)(3k+1)\square.\end{aligned}$$

As in **2)**, we obtain that $k-1=\square$ or $2\square$, $k=\square$ or $2\square$, $k+1=\square$ or $2\square$, in this leads to a contradiction.

4) $X_1=R_n+P_n+C_n$
Now the system (9) becomes

$$(k-1)x+1=k\square, \quad (k+1)x+1=k(3k-1)\square, \quad 4kx+1=(3k-1)\square.$$

The first two equations imply $k=\square$ or $2\square$. Since $k \equiv 2$ or $3 \pmod 4$, it has to hold $k=2\square$ and $k \equiv 2 \pmod 8$. Now the third equation gives $5\square \equiv 1 \pmod 8$, a contradiction. ■

In Table 3 we list the rank values of $E_n^*(\mathbf{Q})$ in the range $2 \le |n| \le 21$, which we were able to compute using Simath and Mwrank.

$\text{rank}\,(E_n^*(\mathbf{Q})) = 2$	$n =$ 4, 5, 6*, 7, 12, 21, −2, −3, −4, −6*, −11, −17, −19
$\text{rank}\,(E_n^*(\mathbf{Q})) = 3$	$n =$ 2, 3, 8, 9, 10, 13, 17, −5, −7, −8, −9, −10, −12, −14, −15, −16, −18, −20
$\text{rank}\,(E_n^*(\mathbf{Q})) = 4$	$n =$ 11, 14, 16, 18 −21

Table 3:

Theorem 6 *The rank of the elliptic curve*

$$E^*: \quad y^2 = [(k_1(n)-1)x+1][(k_1(n)+1)x+1][4k_1(n)x+1]$$

over $\mathbf{Q}(n)$ *is equal* 2.

Proof. As in the proof of Theorem 4, we consider the triples $(\mu_1(n), \mu_2(n), \mu_3(n))$. Now we have:

$$\begin{aligned} \mu_1(n) &\mid (3n^2+2n-3)(9n^2+6n-7), \\ \mu_2(n) &\mid (n+1)(3n-1)(9n^2+6n-5), \\ \mu_3(n) &\mid 8(3n^2+2n-2). \end{aligned}$$

We want to choose an integer n such that $\text{rank}\,(E_n^*(\mathbf{Q})) = 2$, $E_n^*(\mathbf{Q})/E_n^*(\mathbf{Q})_{\text{tors}} = <P_n, R_n>$ and square-free parts of the polynomial factors of $(3n^2+2n-2)(9n^2+6n-7)$, $(n+1)(3n-1)(9n^2+6n-5)$ and $8(3n^2+2n-2)$, evaluated at n, are distinct. We may choose $n = 4$ (then $k_1(n) = 54$).

Since for $n = 4$ we have exactly 16 choices of (μ_1, μ_2, μ_3) on $E_4^*(\mathbf{Q})$, we conclude that there are also exactly 16 choices of $(\mu_1(n), \mu_2(n), \mu_3(n))$ on $E^*(\mathbf{Q}(n))$, which correspond to the points $\mathcal{O}$, $A(n) = A_n$, $B(n) = B_n$, $C(n) = C_n$, $P(n) = P_n$, $P(n)+A(n)$, $P(n)+B(n)$, $P(n)+C(n)$, $R(n) = R_n$,

$R(n)+A(n)$, $R(n)+B(n)$, $R(n)+C(n)$, $R(n)+P(n)$, $R(n)+P(n)+A(n)$, $R(n)+P(n)+B(n)$, $R(n)+P(n)+C(n)$.

Let $V \in E^*(\mathbf{Q}(n)$. Together with the previous 16 points, it makes 17 points on $E^*(\mathbf{Q}(n))$. Two of them have equal corresponding triples $(\mu_1(n), \mu_2(n), \mu_3(n))$. Therefore, these two points are congruent modulo $2E^*(\mathbf{Q}(n))$. We have already proved that the first sixteen points are incongruent modulo $2E^*(\mathbf{Q}(n))$. Hence we have four possibilities:

1) $V \equiv T_1 \pmod{2E^*(\mathbf{Q}(n))}$,
2) $V \equiv P(n)+T_2 \pmod{2E^*(\mathbf{Q}(n))}$,
3) $V \equiv R(n)+T_3 \pmod{2E^*(\mathbf{Q}(n))}$,
4) $V \equiv P(n)+R(n)+T_4 \pmod{2E^*(\mathbf{Q}(n))}$,

where $T_i \in \{\mathcal{O}, A(n), B(n), C(n)\}$.

Let $\{D_1, \ldots, D_r\}$ be the Mordell-Weil base for $E^*(\mathbf{Q}(n))$ and assume that $r \geq 3$. Let $P(n) = \sum_{i=1}^r \alpha_i D_i + T_P$, $R(n) = \sum_{i=1}^r \beta_i D_i + T_R$, $P(n) + R(n) = \sum_{i=1}^r \gamma_i D_i + T_S$. As we have already seen in the proof of Theorem 4, the points D_i cannot satisfy the condition **1)**. Hence, $D_r \equiv P(n)+T_2 \pmod{2E^*(\mathbf{Q}(n))}$ or $D_r \equiv R(n)+T_3 \pmod{2E^*(\mathbf{Q}(n))}$ or $D_r \equiv P(n)+R(n)+T_4 \pmod{2E^*(\mathbf{Q}(n))}$. It implies that α_r is odd and $\alpha_1, \ldots, \alpha_{r-1}$ are even, or β_r is odd and $\beta_1, \ldots, \beta_{r-1}$ are even, or γ_r is odd and $\gamma_1, \ldots, \gamma_{r-1}$ are even. The same possibilities we have also for the points D_{r-1} and D_{r-2}. Therefore, for these three points all of the possibilities **2)**, **3)** and **4)** appear exactly once. Thus, we may assume that α_r is odd, β_{r-1} is odd and γ_{r-2} is odd. But then $\gamma_{r-2} = \alpha_{r-2} + \beta_{r-2}$ is even, a contradiction. ■

5 The second family with rank ≥ 2

Let us now consider the family $E_{k_2(m)}$, where $k_2(m) = \frac{1}{2}(3m^2+5m)$ for $m \in \mathbf{Z}$. For the sake of simplicity we denote $E'_{k_2(m)} = E^\circ_m$. We have the following rational point on E°_m:

$$Q_m = \Big(3m(m+1)(m+2)(27m^3+54m^2+9m-1,$$
$$\frac{1}{2}m(m+1)(m+2)(3m+2)(6m+1)(9m^2+15-2)(9m^2+18m+2)\Big).$$

Let $A_m = A_{k_2(m)}$, $B_m = B_{k_2(m)}$, $C_m = C_{k_2(m)}$ and $P_m = P_{k_2(m)}$. Then we have

$$Q_m + A_m = \Big(-\tfrac{(m+2)(3m+1)(3m+2)(3m+5)(27m^4+72m^3+42m^2-2m-1)}{(9m^2+18m+2)^2},$$

$$
\begin{aligned}
& -\frac{(m+2)(3m+2)^2(3m+5)(6m+1)(9m^2+15m-2)(9m^2+15m+2)}{2(9m^2+18m+2)^3}\Big),\\
Q_m+B_m &= \Big(-\frac{(m+1)(3m-1)(3m+5)(9m^3+21m^2+7m+1)}{(3m+2)^2},\\
& \frac{(m+1)(3m-2)(3m+5)(6m+1)(9m^2+18m+2)}{2(3m+2)^3}\Big),\\
Q_m+C_m &= \Big(-\frac{m(3m-1)(3m+2)(9m^3+30m^2+25m+3)}{(6m+1)^2},\\
& -\frac{m(3m-1)(3m+2)^2(9m^2+15m+2)(9m^2+18m+2)}{2(6m+1)^3}\Big),\\
Q_m+P_m &= (-\frac{1}{9}(3m-1)(3m+2)(3m+5),\\
& \frac{1}{54}(3m-1)(3m+1)(3m+2)(3m+5)(9m^2+15m-2)),\\
Q_m+P_m+A_m &= \Big(-\frac{m(m+1)(3m-1)(3m+4)(9m^2+18m+2)}{(3m+1)^2},\\
& -\frac{3m(m+1)(3m-1)(9m^2+15m-2)(9m^2+15m+2)}{2(3m+1)^3}\Big),\\
Q_m+P_m+B_m &= \Big(-m(m+2)(3m+2)^2,\\
& \frac{3}{2}m(m+2)(3m+1)(3m+2)\Big),\\
Q_m+P_m+C_m &= \Big((m+1)(m+2)(3m+5)(6m+1),\\
& -\frac{3}{2}(m+1)(m+2)(3m+1)(3m+5)(9m^2+15m+2)\Big).
\end{aligned}
$$

Lemma 3 *If* $m \neq -2,-1,0,$ *then* Q_m, Q_m+A_m, Q_m+B_m, Q_m+C_m, Q_m+P_m, $Q_m+P_m+A_m$, $Q_m+P_m+B_m$, $Q_m+P_m+C_m \notin 2E_m^{\circ}(\mathbf{Q})$.

Proof. As in the proof of Lemma 2, we conclude that Q_m+A_m, Q_m+B_m, $Q_m+P_m+A_m$, $Q_m+P_m+B_m \notin 2E_m^{\circ}(\mathbf{Q})$.

Furthermore, $Q_m \in 2E_m^{\circ}(\mathbf{Q})$ is impossible since it implies $m(m+1)=\square$, and $Q_m+P_m \in 2E_m^{\circ}(\mathbf{Q})$ is impossible since it implies $(3m+2)(3m+5)=(6m+7)^2-9=\square$.

If $Q_m+C_m=(x,y)\in 2E_m^{\circ}(\mathbf{Q})$, then we have

$$m=\alpha^2, \quad 3m-1=\beta^2, \quad 3m+2=2\gamma^2, \quad 9m^2+15m+2=2\delta^2.$$

It implies $\beta^2-2\gamma^2=-3$, which is impossible modulo 8.

If $Q_m+P_m+C_m=(x,y)\in 2E_m^{\circ}(\mathbf{Q})$, then we have

$$m+2=\alpha^2, \quad 3m+5=\beta^2, \quad m+1=2\gamma^2, \quad 9m^2+15m+2=2\delta^2.$$

It implies $\beta^2-6\gamma^2=2$. Hence β is even, say $\beta=2\varepsilon$, and we obtain $2\varepsilon^2-3\gamma^2=1$, which is impossible modulo 8. ■

Corollary 3 *If* $m \neq -2, -1, 0$, *then* $\operatorname{rank} E_m^\circ(\mathbf{Q}) \geq 2$.

Proof. As in the proof of Corollary 2, using Lemmas 1 and 3, we can check that P_m and Q_m generate a subgroup of rank 2 in $E_m^\circ(\mathbf{Q})/E_m^\circ(\mathbf{Q})_{\mathrm{tors}}$. ■

Theorem 7 *If* $\operatorname{rank}(E_m^\circ(\mathbf{Q})) = 2$, *then all integer points on* E_k, *where* $k = k_2(m)$, *are given by (7).*

Proof. As in the proof of Theorem 5, it suffices to prove that the systems (9), with numbers α, β, γ defined in the proof of Theorem 3, for $X_1 \in \mathcal{S}_2$, where

$$\begin{aligned}\mathcal{S}_2 = \{&Q_m, Q_m + A_m, Q_m + B_m, Q_m + C_m, Q_m + P_m, Q_m + P_m + A_m,\\ &Q_m + P_m + B_m, Q_m + P_m + C_m\},\end{aligned}$$

have no solutions in integers. Note that for $X_1 \in \{Q_m + A_m, Q_m + B_m, Q_m + P_m + A_m, Q_m + P_m + B_m\}$ exactly two of the numbers α, β, γ are negative. Let us consider four remaining cases. We will denote $k_2(m)$ by k. Note that $k + 1 = \frac{1}{2}(3m + 2)(m + 1)$ and $k - 1 = \frac{1}{2}(3m - 1)(m + 2)$.

1) $X_1 = Q_m$

The system (9) becomes

$$\begin{aligned}(k-1)x + 1 &= (3m+2)(3m+5)\square,\\ (k+1)x + 1 &= (3m-1)(3m+5)(6k-2)\square,\\ 4kx + 1 &= (3m-1)(3m+2)(6k-2)\square.\end{aligned}$$

It implies that $3m - 1 = \square$ or $2\square$, $3m + 2 = \square$ or $2\square$ and $3m + 5 = \square$ or $2\square$, a contradiction.

2) $X_1 = Q_m + C_m$

Now the system (9) becomes

$$\begin{aligned}(k-1)x + 1 &= (m+1)(3m+5)(6k+2)\square,\\ (k+1)x + 1 &= (m+2)(3m+5)\square,\\ 4kx + 1 &= (m+1)(m+2)(6k+2)\square,\end{aligned}$$

and this implies $m + 1 = \square$ or $2\square$, $m + 2 = \square$ or $2\square$ and $3m + 5 = \square$ or $2\square$. We have three possibilities:

(a) $m + 1 = \alpha^2$, $m + 2 = 2\beta^2$, $3m + 5 = \gamma^2$

It gives $\gamma^2 - 6\beta^2 = -1$, a contradiction.

(b) $m+1 = 2\alpha^2, \quad m+2 = \beta^2, \quad 3m+5 = \gamma^2$

It gives $\gamma^2 - 3\beta^2 = -1$, a contradiction.

(c) $m+1 = 2\alpha^2, \quad m+2 = 2\beta^2, \quad 3m+5 = 2\gamma^2$

This yields to the system of Pell equations

$$\begin{aligned} \beta^2 - 2\alpha^2 &= 1, \\ \gamma^2 - 3\alpha^2 &= 1. \end{aligned}$$

In [1] it is proved that this system has only the trivial solution. Hence, $\alpha = 0$ and $m = -1$.

3) $X_1 = Q_m + P_m$
We have

$$\begin{aligned} (k-1)x + 1 &= m(m+1)\Box, \\ (k+1)x + 1 &= m(m+2)(6k-2)\Box, \\ 4kx + 1 &= (m+1)(m+2)(6k-2)\Box. \end{aligned}$$

which implies that $m = \Box$ or $2\Box$, $m+1 = \Box$ or $2\Box$ and $m+2 = \Box$ or $2\Box$, a contradiction.

4) $X_1 = Q_m + P_m + C_m$
We have

$$\begin{aligned} (k-1)x + 1 &= m(3m+2)(6k+2)\Box, \\ (k+1)x + 1 &= m(3m-1)\Box, \\ 4kx + 1 &= (3m-1)(3m+2)(6k+2)\Box, \end{aligned}$$

which implies that $m = \Box$ or $2\Box$, $3m-1 = \Box$ or $2\Box$ and $3m+2 = \Box$ or $2\Box$. We have three possibilities:

(a) $m = \alpha^2, \quad 3m-1 = \beta^2, \quad 3m+2 = 2\gamma^2$

It implies $\beta^2 - 3\alpha^2 = -1$, a contradiction.

(b) $m = \alpha^2, \quad 3m-1 = 2\beta^2, \quad 3m+2 = \gamma^2$

It implies $\gamma^2 - 3\beta^2 = 2$, which is impossible modulo 8.

(c) $m = 2\alpha^2, \quad 3m-1 = \beta^2, \quad 3m+2 = 2\gamma^2$

It gives $\beta^2 - 6\alpha^2 = -1$, a contradiction. ∎

In Table 4 we list the rank values of $E_m^\circ(\mathbf{Q})$ in the ranges $1 \le m \le 20$ and $-22 \le m \le -3$, which we were able to compute.

$\mathrm{rank}\,(E_m^\circ(\mathbf{Q})) = 2$	$n =$ 1, 2, 3, 5, 6, 7, 8, 9, 12, 14, 15 −3, −5, −6, −9, −10, −16*, −18, −20, −22
$\mathrm{rank}\,(E_m^\circ(\mathbf{Q})) = 3$	$n =$ 4, 10, 11, 16, 17, 18, 19, 20 −4, −7, −8, −11, −12, −13, −14, −15, −17, −19, −21

Table 4:

Theorem 8 *The rank of elliptic curve*

$$E^\circ : \qquad y^2 = [(k_2(m) - 1)x + 1][(k_2(m) + 1)x + 1][4k_2(m)x + 1]$$

over $\mathbf{Q}(m)$ *is equal* 2.

Proof. The proof is completely analogous to the proof of Theorem 6. This time we choose $m = 12$ (and $k = 246$) because $\mathrm{rank}\,(E_{12}^\circ(\mathbf{Q})) = 2$, $E_{12}^\circ(\mathbf{Q})/E_{12}^\circ(\mathbf{Q})_{\mathrm{tors}} =< P_{12}, Q_{12} >$ and square-free parts of the polynomial factors of $(m+2)(3m-1)(9m^2+15m-1)$, $(m+1)(3m+2)(9m^2+15m+2)$ and $4m(3m+5)$, evaluated at $m = 12$, are distinct. ■

Assuming the Katz-Sarnak Conjecture, Theorems 5–8 imply that Conjecture 1 is valid for infinitely many curves of rank 2.

6 A family with rank ≥ 3

We will now consider the intersection of families $E_{k_1(n)}$ and $E_{k_2(m)}$. From $3n^2 + 2n - 2 = \frac{1}{2}(3m^2 + 5m)$ it follows

$$(6m + 5)^2 - 2(6n + 2)^2 = -31. \qquad (23)$$

Define the sequences $(r_i)_{i\in\mathbf{Z}}$ and $(s_i)_{i\in\mathbf{Z}}$ by

$$r_0 = 1, \quad r_1 = 19, \quad r_{i+2} = 6r_{i+1} - r_i, \quad i \in \mathbf{Z}; \tag{24}$$
$$s_0 = 1, \quad s_1 = 14, \quad s_{i+2} = 6s_{i+1} - s_i, \quad i \in \mathbf{Z}. \tag{25}$$

Let $6m + 5 = r$ and $6n + 2 = s$. Then there exists an integer i such that $r = \pm r_i$ and $s = \pm s_i$.

We have

$$k_2(m) = \frac{1}{24}(r^2 - 25), \quad k_2(m) - 1 = \frac{1}{24}(r^2 - 49), \quad k_2(m) + 1 = \frac{1}{24}(r^2 - 1),$$

$$3k_2(m) - 1 = \frac{1}{8}(r^2 - 33), \quad 3k_2(m) + 1 = \frac{1}{8}(r^2 - 17).$$

For the sake of simplicity, denote $E'_{(r^2-25)/24}$ by $E_i^\diamond$ and $A_{(r^2-25)/24} = A_i$, $B_{(r^2-25)/24} = B_i$, $C_{(r^2-25)/24} = C_i$, $P_{(r^2-25)/24} = P_i$, $Q_{(r-5)/6} = Q_i$, $R_{(s-2)/6} = R_i$, $\frac{1}{24}(r^2 - 25) = k$.

We will need some properties of the sequence (r_i) which are stated in the following three lemmas.

Lemma 4 *Let the sequence (r_i) be defined by (24). Then the equations $r_i^2 - 33 = \Box, 2\Box, 3\Box, 6\Box$ and $r_i^2 - 17 = \Box, 2\Box, 3\Box, 6\Box$ have no solutions.*

Proof. The equation $r_i^2 - 33 = \Box$ implies $r_i = \pm 7$ or ± 17, a contradiction. The equation $r_i^2 - 33 = 2\Box$ is impossible modulo 3, and the equations $r_i^2 - 33 = 3\Box$ and $r_i^2 - 33 = 6\Box$ imply $3|r_i$, a contradiction.

The equation $r_i^2 - 33 = \Box$ implies $r_i = \pm 9$, a contradiction. The equations $r_i^2 - 33 = 3\Box$ and $r_i^2 - 17 = 6\Box$ are impossible modulo 3. Let $r_i^2 - 17 = 2t^2$. Then from $r_i^2 - 2s_i^2 = -31$ we obtain $s_i = \pm 5$ or ± 7, a contradiction. ∎

Lemma 5 *Let the sequence (r_i) be defined by (24). Then the equations*

$$|r_i| + 7 = \Box, 3\Box;$$
$$|r_i| - 7 = \Box, 2\Box, 3\Box, 6\Box;$$
$$|r_i| + 5 = 3\Box;$$
$$|r_i| - 5 = \Box, 3\Box, 6\Box$$

have no solutions with $|i| \geq 3$.

Proof. In [17], Kedlaya presented a systematic procedure, using the method of Cohn introduced in [4], for solving certain systems of Diophantine equations of the form

$$x^2 - ay^2 = b, \quad P(x,y) = z^2.$$

Using Kedlaya's program genpellsquare, we obtain that all solutions of the equations from the lemma are given by

$$r_1 - 7 = 3 \cdot 2^2, \quad |r_{-1}| - 7 = 6 \cdot 1^2, \quad |r_{-2}| - 7 = 2 \cdot 6^2, \quad r_2 - 5 = 3 \cdot 6^2.$$

■

Lemma 6 $r \equiv 1, 6 \pmod 7$ *or* $r \equiv 19, 30 \pmod{49}$.

Proof. Considering the sequence (r_i mod 49) one can easily deduce that $r_i \equiv 1 \pmod 7$ or $r_i \equiv 19 \pmod{49}$. ■

Lemma 7 *If* $i \neq -1, 0$*, then* Q_i+R_i, $Q_i+R_i+A_i$, $Q_i+R_i+B_i$, $Q_i+R_i+C_i$, $Q_i+R_i+P_i$, $Q_i+R_i+P_i+A_i$, $Q_i+R_i+P_i+B_i$, $Q_i+R_i+P_i+C_i \notin 2E_i^{\diamond}(\mathbf{Q})$.

Proof. **1)**

$$\begin{aligned} x(Q_i + R_i) + k^2 - 1 &= 2(r-1)(r-7)(r^2-17)(r^2-33)\Box, \\ x(Q_i + R_i) + 4k(k-1) &= (r+5)(r-7)(r^2-33)\Box, \\ x(Q_i + R_i) + 4k(k+1) &= 2(r-1)(r+5)(r^2-17)\Box, \end{aligned}$$

where $\Box$ denotes a square of a rational number. If $Q_i + R_i \in 2E_i^{\diamond}(\mathbf{Q})$, then Proposition 1 implies $r^2 - 33 = \Box$, $2\Box$, $3\Box$ or $6\Box$, and this is impossible by Lemma 4.

2)

$$\begin{aligned} x(Q_i + R_i + A_i) + k^2 - 1 &= -6(r+1)(r-7)(r^2-33)\Box, \\ x(Q_i + R_i + A_i) + 4k(k-1) &= -3(r-5)(r-7)(r^2-33)\Box, \\ x(Q_i + R_i + A_i) + 4k(k+1) &= 2(r+1)(r-5)\Box. \end{aligned}$$

Since $-3(r-5)(r-7)(r^2-33) < 0$, we conclude that $Q_i+R_i+A_i \notin 2E_i^{\diamond}(\mathbf{Q})$.

3)

$$\begin{aligned} x(Q_i + R_i + B_i) + k^2 - 1 &= -6(r-1)(r+7)(r^2-17)\Box, \\ x(Q_i + R_i + B_i) + 4k(k-1) &= -(r-5)(r+7)\Box, \\ x(Q_i + R_i + B_i) + 4k(k+1) &= 6(r-1)(r-5)(r^2-17)\Box. \end{aligned}$$

Since $-(r-5)(r+7)<0$, we conclude that $Q_i+R_i+B_i \notin 2E_i^{\diamond}(\mathbf{Q})$.

4)

$$\begin{aligned} x(Q_i+R_i+C_i)+k^2-1 &= 2(r+1)(r+7)\Box, \\ x(Q_i+R_i+C_i)+4k(k-1) &= 3(r+5)(r+7)\Box, \\ x(Q_i+R_i+C_i)+4k(k+1) &= 6(r+1)(r+5)\Box. \end{aligned}$$

By Lemma 5 we have $r+7=2\Box$ or $6\Box$ if r is positive, and $r=-19$ or -79 if r is negative. However, if $r=-19$ or -79, then $2(r+1)(r+7)$ is not a perfect square. Hence we have two possibilities:

$$r+7=2\alpha^2, \quad r+1=\beta^2, \quad r+5=6\gamma^2;$$

or

$$r+7=6\alpha^2, \quad r+1=3\beta^2, \quad r+5=2\gamma^2;$$

but both systems are impossible modulo 3.

5)

$$\begin{aligned} x(Q_i+R_i+P_i)+k^2-1 &= 2(r+1)(r+7)(r^2-17)(r^2-33)\Box, \\ x(Q_i+R_i+P_i)+4k(k-1) &= (r-5)(r+7)(r^2-33)\Box, \\ x(Q_i+R_i+P_i)+4k(k+1) &= 2(r+1)(r-5)(r^2-17)\Box. \end{aligned}$$

Since $r^2-33 \neq \Box, 2\Box, 3\Box, 6\Box$ by Lemma 5, Proposition 1 implies $Q_i+R_i+P_i \notin 2E_i^{\diamond}(\mathbf{Q})$.

6)

$$\begin{aligned} x(Q_i+R_i+P_i+A_i)+k^2-1 &= -6(r-1)(r+7)(r^2-33)\Box, \\ x(Q_i+R_i+P_i+A_i)+4k(k-1) &= -3(r+5)(r+7)(r^2-33)\Box, \\ x(Q_i+R_i+P_i+A_i)+4k(k+1) &= 2(r-1)(r+5)\Box. \end{aligned}$$

Since $-3(r+5)(r+7)(r^2-33)<0$, we have $Q_i+R_i+P_i+A_i \notin 2E_i^{\diamond}(\mathbf{Q})$.

7)

$$\begin{aligned} x(Q_i+R_i+P_i+B_i)+k^2-1 &= -6(r+1)(r-7)(r^2-17)\Box, \\ x(Q_i+R_i+P_i+B_i)+4k(k-1) &= -(r+5)(r-7)\Box, \\ x(Q_i+R_i+P_i+B_i)+4k(k+1) &= 6(r+1)(r+5)(r^2-17)\Box. \end{aligned}$$

Since $-(r+5)(r-7)<0$, we have $Q_i+R_i+P_i+B_i \notin 2E_i^{\diamond}(\mathbf{Q})$.

8)

$$\begin{aligned} x(Q_i+R_i+P_i+C_i)+k^2-1 &= 2(r-1)(r-7)\Box, \\ x(Q_i+R_i+P_i+C_i)+4k(k-1) &= 3(r-5)(r-7)\Box, \\ x(Q_i+R_i+P_i+C_i)+4k(k+1) &= 6(r-1)(r-5)\Box. \end{aligned}$$

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

Corollary 4 *If* $i \neq -1, 0$, *then* $\mathrm{rank}\,(E_i^{\diamond}(\mathbf{Q})) \geq 3$.

PROOF. As in the proof of Corollary 2, using Lemmas 1–3 and 7, we can prove that P_i, Q_i and R_i generate a subgroup of rank 3 in $E_i^{\diamond}(\mathbf{Q})/E_i^{\diamond}(\mathbf{Q})_{\mathrm{tors}}$. ■

Theorem 9 *If* $\mathrm{rank}\,(E_i^{\diamond}(\mathbf{Q})) = 3$, *then all integer points on* E_k, *where* $k = \frac{1}{24}(r_i^2 - 25)$, *are given by (7).*

PROOF. As in the proofs of Theorems 5 and 7, it suffices to prove that the systems (9), with the numbers α, β, γ defined in the proof of Theorem 3 for $X_1 \in \mathcal{S}_3$, where

$$\begin{aligned} \mathcal{S}_3 \;=\; \{ & Q_i+R_i,\, Q_i+R_i+A_i,\, Q_i+R_i+B_i,\, Q_i+R_i+C_i,\, Q_i+R_i+P_i, \\ & Q_i+R_i+P_i+A_i,\, Q_i+R_i+P_i+B_i,\, Q_i+R_i+P_i+C_i\}, \end{aligned}$$

have no solutions in integers.

As we have already seen in the proof of Lemma 7, for $X_i \in \{Q_i+R_i+A_i, Q_i+R_i+B_i, Q_i+R_i+P_i+A_i, Q_i+R_i+P_i+B_i\}$ exactly two of the numbers α, β, γ are negative and accordingly the corresponding systems have no integer solutions. Let us consider four remaining cases. We will use the following notation: $e'' = \min\{|e|', |2e|', |3e|', |6e|'\}$ for an integer e.

1) $X_1 = Q_i + R_i$
The system (9) becomes

$$\begin{aligned} (k-1)x+1 &= 2(r+1)(r-5)(r^2-17)\Box, \\ (k+1)x+1 &= (r-5)(r+7)(r^2-33)\Box, \\ 4kx+1 &= 2(r+1)(r+7)(r^2-17)(r^2-33)\Box. \end{aligned}$$

From the first two equations of this system we have that $(r-5)''$ divides $(k-1)x+1$ and $(k+1)x+1$. Therefore, $(r-5)'' \in \{1,2\}$ which implies

$$r-5 = \pm\Box,\ \pm2\Box,\ \pm3\Box,\ \pm6\Box. \tag{26}$$

Similarly we obtain

$$r+1=\pm\square,\ \pm2\square,\ \pm3\square,\ \pm6\square \tag{27}$$

and

$$r+7=\pm\square,\ \pm2\square,\ \pm3\square,\ \pm6\square. \tag{28}$$

Assume that r is positive. Since $r=113$ does not satisfy the conditions (27) and (28), Lemma 5 implies

$$r-5=2\square,\quad r+7=2\square \text{ or } 6\square.$$

Hence, $r-5=2\alpha^2$, $r+7=6\beta^2$. Then $\alpha=3\delta$ and we have $\beta^2-3\delta^2=2$, which is impossible modulo 3.

Assume now that r is negative. Then Lemma 5 implies that $r=-19$ or -79, but $r=-79$ does not satisfy the condition (27), and for $r=-19$ we have $15x+1=41\square$ which is impossible modulo 3.

2) $X_1=Q_i+R_i+C_i$
We have

$$\begin{aligned}(k-1)x+1 &= 6(r-1)(r-5)\square,\\ (k+1)x+1 &= 3(r-5)(r-7)\square,\\ 4kx+1 &= 2(r-1)(r-7)\square.\end{aligned}$$

As in **1)** we obtain that

$$r-1=\pm\square,\ \pm2\square,\ \pm3\square,\ \pm6\square, \tag{29}$$

$$r-5=\pm\square,\ \pm2\square,\ \pm3\square,\ \pm6\square \tag{30}$$

and

$$r-7=\pm\square,\ \pm2\square,\ \pm3\square,\ \pm6\square. \tag{31}$$

If r is positive, then Lemma 5 implies that $r=19$ or $r=79$, which both contradict the condition (30).

Assume that r negative. Then Lemma 5 implies

$$r-7=-2\square \text{ or } -6\square,\quad r-5=-\square,\ -2\square \text{ or } -6\square.$$

Consideration modulo 3 rules out all but three possibilities: $r-7=-2\square$ and $r-5=-\square$; $r-7=-2\square$ and $r-5=-6\square$; $r-7=-6\square$ and $r-5=-\square$.

a) $r-7=-2\alpha^2, \quad r-5=-\beta^2$
By Lemma 6, the first equation implies $r \equiv 5,6 \pmod 7$ and the second implies $r \equiv 1 \pmod 7$, a contradiction.
b) $r-7=-2\alpha^2, \quad r-5=-6\beta^2, \quad r-1=-4\gamma$
It implies $\alpha^2-2\gamma^2=3$, which is impossible modulo 3.
c1) $r-7=-6\alpha^2, \quad r-5=-4\beta^2, \quad r-1=-72\gamma^2$
We obtain the system of Pell equations

$$\begin{aligned} \alpha^2-12\gamma^2 &= 1, \\ \beta^2-18\gamma^2 &= 1, \end{aligned}$$

and by [1] this system has no non-trivial solution. It means that $r=-1$, contradicting the assumption that $i \neq 0$.
c2) $r-7=-6\alpha^2, \quad r-5=-4\beta^2, \quad r-1=-12\gamma^2$
This leads to the system

$$\begin{aligned} \alpha^2-2\gamma^2 &= 1, \\ \beta^2-3\gamma^2 &= 1, \end{aligned}$$

which has no non-trivial solution by [1].

3) $X_1=Q_i+R_i+P_i$
We have

$$\begin{aligned} (k-1)x+1 &= 2(r-1)(r+5)(r^2-17)\square, \\ (k+1)x+1 &= (r+5)(r-7)(r^2-33)\square, \\ 4kx+1 &= 2(r-1)(r-7)(r^2-17)(r^2-33)\square. \end{aligned}$$

Therefore, this case is completely analogous to the case **1)**.

4) $X_1=Q_i+R_i+P_i+C_i$
We have

$$\begin{aligned} (k-1)x+1 &= 6(r+1)(r+5)\square, \\ (k+1)x+1 &= 3(r+5)(r+7)\square, \\ 4kx+1 &= 2(r+1)(r+7)\square, \end{aligned}$$

and this case is completely analogous to the case **2)**. ■

In Table 5 we list a few rank values of $E_i^{\diamond}(\mathbf{Q})$.

We have not enough data to support any conjecture about distribution of rank $(E_i^{\diamond}(\mathbf{Q}))$. However, from Theorem 9 and Table 5 we obtain immediately

i	r	m	s	n	k	rank $(E_i^\diamond(\mathbf{Q}))$
1	−19	−4	14	2	14	3
2	113	18	80	13	531	3
3	659	109	−466	−78	18094	5
−2	−79	−14	56	9	259	3

Table 5:

Corollary 5

$$\begin{aligned} \limsup \{\text{rank}\,(E_k(\mathbf{Q}))\,:\, k \geq 2\} \;&\geq\; 3 \\ \sup \{\text{rank}\,(E_k(\mathbf{Q}))\,:\, k \geq 2\} \;&\geq\; 5 \end{aligned}$$

Let us note that in [9] an example is constructed which shows that $\sup\{\text{rank}\,(E(\mathbf{Q}))\,:\, E(\mathbf{Q})_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}\} \geq 7$.

7 Case $k \leq 1000$

In this section we will check Conjecture 1 for $k \leq 1000$ using the approach introduced in [11]. Assume that (x, y) is a solution of

$$y^2 = ((k-1)x+1)((k+1)x+1)(4kx+1). \tag{32}$$

Then there exist integers x_1, x_2, x_3 such that

$$\begin{aligned} (k-1)x+1 &= \mu_2\mu_3x_1^2 \\ (k+1)x+1 &= \mu_1\mu_3x_2^2 \\ 4kx+1 &= \mu_1\mu_2x_3^2, \end{aligned}$$

where $\mu_1|3k-1$, $\mu_2|3k+1$, $\mu_3|2$.

If $\mu_3 = 1$, eliminating x we obtain the system

$$\begin{aligned} (k+1)\mu_2x_1^2 - (k-1)\mu_1x_2^2 &= 2 \\ 4kx_1^2 - (k-1)\mu_1x_3^2 &= \frac{3k+1}{\mu_2}, \end{aligned}$$

and if $\mu_3 = 2$, we obtain the system

$$\begin{aligned} (k+1)\mu_2 x_1^2 - (k-1)\mu_1 x_2^2 &= 1 \\ 8kx_1^2 - (k-1)\mu_1 x_3^2 &= \frac{3k+1}{\mu_2}. \end{aligned}$$

Hence, to find all integer solutions of (32), it is enough to find all integer solutions of the systems of equations

$$d_1 x_1^2 - d_2 x_2^2 = j_1, \tag{33}$$
$$d_3 x_1^2 - d_2 x_3^2 = j_2, \tag{34}$$

where
$d_1 = (k+1)\mu_2$, μ_2 is a square-free factor of $3k+1$,
$d_2 = (k-1)\mu_1$, μ_1 is a square-free factor of $3k-1$,
$(d_3, j_1, j_2) = (4k, 2, \frac{3k+1}{\mu_2})$ or $(8k, 1, \frac{3k+1}{\mu_2})$.
Note that the system

$$\begin{aligned} (k+1)x_1^2 - (k-1)x_2^2 &= 2 \\ 4kx_1^2 - (k-1)x_3^2 &= 3k+1 \end{aligned}$$

is completely solved in [7]. Hence we may assume that $(d_1, d_2, d_3, j_1, j_2) \neq (k+1, k-1, 4k, 2, 3k+1)$.

From (33) and (34) we obtain

$$d_1 x_3^2 - d_3 x_2^2 = j_3, \tag{35}$$

where $j_3 = \frac{j_1 d_3 - j_2 d_1}{d_2}$.

We first consider the equations (33), (34) and (35) separately modulo appropriate prime powers. More precisely, assume that p_1 is an odd prime divisor of d_1, p_2 is an odd prime divisor of d_2, p_3 is an odd prime divisor of d_3, p_4 is an odd prime divisor of j_2 such that $\mathrm{ord}_{p_4}(j_2)$ is odd, p_5 is an odd prime divisor of j_3 such that $\mathrm{ord}_{p_5}(j_3)$ is odd. Then necessary conditions for solvability of (33), (34) and (35) are:

$$\left(\frac{-j_1 d_2}{p_1}\right) = 1, \quad \left(\frac{j_1 d_1}{p_2}\right) = 1, \quad \left(\frac{j_2 d_3}{p_2}\right) = 1,$$

$$\left(\frac{-j_2 d_2}{p_3}\right) = 1, \quad \left(\frac{d_2 d_3}{p_4}\right) = 1, \quad \left(\frac{d_1 d_3}{p_5}\right) = 1,$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol.

Furthermore, if k is even, we have also the conditions

$$j_1 \equiv d_1 - d_2 \pmod 8 \text{ or } j_1 \equiv d_1 \pmod 4 \text{ or } j_1 \equiv -d_2 \pmod 4;$$

$$j_2 \equiv 0 \pmod 4 \text{ or } j_2 \equiv -d_2 \pmod 8;$$

$$j_3 \equiv 0 \pmod 4 \text{ or } j_3 \equiv d_1 \pmod 8.$$

If k is odd, then $j_1 = 2$ and j_2, j_3 are even, say $j_2 = 2i_2$, $j_3 = 2i_3$. We have the following solvability conditions:

$$1 \equiv \frac{d_1}{2} - \frac{d_2}{2} \pmod 8 \quad \text{or} \quad \Big(d_1 \equiv 0 \pmod 4 \text{ and } d_2 \equiv -2 \pmod{16}\Big)$$
$$\text{or} \quad \Big(d_1 \equiv 2 \pmod{16} \text{ and } d_2 \equiv 0 \pmod 4\Big);$$

$$i_2 \equiv \frac{d_3}{2} - \frac{d_2}{2},\ -\frac{d_2}{2},\ \frac{d_3}{2},\ \text{or}\ \frac{d_3}{2} - 2d_2 \pmod 8;$$

$$i_3 \equiv \frac{d_1}{2} - \frac{d_3}{2},\ -\frac{d_3}{2},\ \frac{d_1}{2},\ \text{or}\ -\frac{d_3}{2} + 2d_1 \pmod 8.$$

We performed these tests for $2 \le k \le 1000$ using A. Pethő's program developed for the purposes of our joint paper [11]. We found that all systems are unsolvable apart from 106 systems on which we apply the further tests based on the properties of Pellian equations.

Lemma 8 a) *Let $a > 1$, $b > 0$ be integers such that $\gcd(a,b) = 1$ and $d = ab$ is not a perfect square, and let (u_0, v_0) be the minimal solution of Pell equation $u^2 - dv^2 = 1$. Then the equation*

$$ax^2 - by^2 = 1$$

has a solution if and only if $2a | u_0 + 1$ and $2b | u_0 - 1$.

b) *Let a, b be positive integers such that $\gcd(a,b) = \gcd(a,2) = \gcd(b,2) = 1$ and $d = ab$ is not a perfect square, and let (u_0, v_0) be the minimal solution of Pell equation $u^2 - dv^2 = 1$. Then the equation*

$$ax^2 - by^2 = 2$$

has a solution if and only if $a | u_0 + 1$ and $b | u_0 - 1$.

Proof. See [14, Criteria 1 and 2]. ■

Corollary 6 *Let $k \geq 2$ be an integer. The equations*

$$\begin{aligned} 4kx^2 - (k-1)y^2 &= 1, \\ (k+1)x^2 - (k-1)y^2 &= 1, \\ 4kx^2 - (k-1)y^2 &= 2, \\ 4kx^2 - (k+1)y^2 &= 1 \end{aligned}$$

have no integer solutions.

PROOF. Consider first the equation $4kx^2-(k-1)y^2 = 1$. In the notation of Lemma 8, we have $a = 4k$, $b = k-1$, $u_0 = 2k-1$, $v_0 = 1$ and $\frac{u_0+1}{2a} = \frac{1}{4} \notin \mathbf{Z}$.

For the equation $(k+1)x^2 - (k-1)y^2 = 1$ we have $a = k+1$, $b = k-1$, $u_0 = k$, $v_0 = 1$ and $\frac{u_0+1}{2a} = \frac{1}{2} \notin \mathbf{Z}$.

For the equation $4kx^2 - (k-1)y^2 = 2$ we have $a = 4k$, $b = k-1$, $u_0 = 2k-1$, $v_0 = 1$ and $\frac{u_0+1}{a} = \frac{1}{2} \notin \mathbf{Z}$.

For the equation $4kx^2 - (k+1)y^2 = 2$ we have $a = 4k$, $b = k+1$, $u_0 = 2k+1$, $v_0 = 1$ and $\frac{u_0+1}{a} = \frac{k+1}{2k} \notin \mathbf{Z}$. ■

Corollary 6 rules out 46+4+4+4 = 58 cases from the list of the remaining 106 cases. Lemma 8 can be also applied to the equation $123x^2 - 8833y^2 = 2$ when we have $a = 123$, $b = 8833$, $u_0 = 9778130$, $v_0 = 9381$ and $\frac{u_0-1}{b} \notin \mathbf{Z}$, and to the equation $14065x^2 - 24y^2 = 1$ when we have $a = 14065$, $b = 24$, $u_0 = 581$, $v_0 = 1$ and $\frac{u_0+1}{2a} \notin \mathbf{Z}$. Hence, after the application of Lemma 8, our list of remaining cases is reduced to 46 cases.

Lemma 9 *Let $a > 1$ and $b > 0$ be square-free integers. If (x_1, y_1) is the minimal solution of the equation*

$$ax^2 - by^2 = 1, \tag{36}$$

then all solutions of (36) in positive integers are given by

$$x\sqrt{a} + y\sqrt{b} = (x_1\sqrt{a} + y_1\sqrt{b})^n,$$

where n is a positive odd integer.

In particular, $x_1|x$ and $y_1|y$.

PROOF. See [20, Theorem 11.1]. ■

Corollary 7 *Let $k \equiv 1 \pmod 4$ be a square-free positive integer. Then the system of equations*

$$\begin{aligned} 4kx^2 - (k-1)z^2 &= 4, & (37) \\ \frac{1}{8}(3k+1)(k+1)z^2 - 2ky^2 &= -\frac{1}{2}(3k-1) & (38) \end{aligned}$$

has no solutions in integers.

Proof. Let $k-1 = 4l^2(k-1)'$. We will apply Lemma 9 to the equation

$$kx^2 - (k-1)'v^2 = 1.$$

We have $x_1 = 1$, $v_1 = 2l$ and Lemma 9 implies that $2l|v$. From (37) it follows that $2l|lz$. Hence, z is even and we obtain a contradiction since left hand side of (38) even, while the right hand side is odd. ∎

Corollary 7 rules out 7 cases from our list of remaining cases. The similar even-odd type of the argumentation can be applied to some other cases.

Consider the system

$$\begin{aligned} 969x^2 - 50y^2 &= 1, \\ 101x^2 - 25z^2 &= 4. \end{aligned}$$

All solutions of $v^2 - 101x^2 = -4$ are given by $\frac{v+x\sqrt{101}}{2} = (10+\sqrt{101})^{2n+1}$. Hence, x is even, contradicting the first equation of the system.

Consider the system

$$\begin{aligned} 801x^2 - 200z^2 &= 1, \\ 241001z^2 - 1602y^2 &= -1201. \end{aligned}$$

Applying Lemma 9 to the equation $89u^2 - 2v^2 = 1$, we obtain $u_1 = 3$, $v_1 = 20$. It implies that z is even, a contradiction.

Next system in our consideration is

$$\begin{aligned} 869x^2 - 217z^2 &= 4, \\ 70905z^2 - 1738y^2 &= -1303. \end{aligned}$$

The first equation implies $(217z^2+2)^2 - 869\cdot 217(xz)^2 = 4$ and since all solutions of $a^2 - 869\cdot 217b^2 = 4$ are given by $\frac{a+b\sqrt{869\cdot 217}}{2} = (1737+4\sqrt{869\cdot 217})^n$, we conclude that z is even, a contradiction.

Completely the same argumentation shows that the system

$$\begin{aligned} 229x^2 - 57z^2 &= 4, \\ 4945z^2 - 458y^2 &= -343 \end{aligned}$$

has no integer solution.

At this point we are left with 35 cases in our list of remaining cases.

Lemma 10 *Let $C \neq 0$ and $d \neq \square$ be integers and let (u_0, v_0) be the minimal solution of Pell equation $u^2 - dv^2 = 1$. If the Pellian equation*

$$x^2 - dy^2 = C \tag{39}$$

has a solution, then there exists a solution of (39) such that

$$0 < x \leq \sqrt{\frac{(u_0+1)C}{2}}, \quad 0 \leq y \leq \frac{v_0\sqrt{C}}{\sqrt{2(u_0+1)}} \quad \text{if } C > 0,$$

$$0 \leq x \leq \sqrt{\frac{(u_0-1)(-C)}{2}}, \quad 0 < y \leq \frac{v_0\sqrt{-C}}{\sqrt{2(u_0-1)}} \quad \text{if } C < 0,$$

Proof. See [19, Theorems 108 and 108a]. ■

Using Lemma 10 it is easy to verify that the following equations have no integer solutions:

$$\begin{aligned} x^2 - 163 \cdot 648y^2 &= -5 \cdot 163, \\ x^2 - 191 \cdot 766y^2 &= -25 \cdot 191, \\ x^2 - 523 \cdot 2088y^2 &= -5 \cdot 523, \\ x^2 - 563 \cdot 2248y^2 &= -5 \cdot 563, \\ x^2 - 2432 \cdot 607y^2 &= -25 \cdot 607, \\ x^2 - 1286 \cdot 321y^2 &= -5 \cdot 321, \\ x^2 - 162 \cdot 647y^2 &= -5 \cdot 162, \\ x^2 - 5392 \cdot 21y^2 &= -43 \cdot 21, \\ x^2 - 339 \cdot 1354y^2 &= -7 \cdot 339, \\ x^2 - 709 \cdot 177y^2 &= -28 \cdot 177, \\ x^2 - 1442 \cdot 361y^2 &= -47 \cdot 361, \\ x^2 - 3048 \cdot 763y^2 &= -5 \cdot 763, \end{aligned}$$

$$\begin{aligned}
x^2 - 3232 \cdot 807y^2 &= -25 \cdot 807, \\
x^2 - 823 \cdot 3288y^2 &= -17 \cdot 823, \\
x^2 - 843 \cdot 3368y^2 &= -5 \cdot 843, \\
x^2 - 853 \cdot 3408y^2 &= -35 \cdot 853, \\
x^2 - 953 \cdot 3816y^2 &= -7 \cdot 953.
\end{aligned}$$

Note that in all 17 cases we have $v_0 \leq 4$ and by Lemma 10 it suffices to check that the above equations have no solutions with $1 \leq y \leq 5$.

Two cases can be excluded by reduction modulo 5. These systems are

$$\begin{aligned}
25123x^2 - 258y^2 &= 1, && (40) \\
517x^2 - 129z^2 &= 4 && (41)
\end{aligned}$$

and

$$\begin{aligned}
317x^2 - 23068y^2 &= 1, && (42) \\
633x^2 - 11534z^2 &= 475. && (43)
\end{aligned}$$

Namely, (40) implies $x^2 \equiv 1, 2, 3 \pmod 5$ and (41) implies $x^2 \equiv 0, 2, 4 \pmod 5$. Hence, $x^2 \equiv 2 \pmod 5$, a contradiction. Furthermore, (43) implies $x \equiv z \equiv 0 \pmod 5$ and then (42) implies $y^2 \equiv 3 \pmod 5$, a contradiction.

Hence, it remains to consider 16 systems listed in Table 6.

Lemma 11 *Let d be a positive integer which is not a perfect square. If d is not square-free, then there is at most one square-free integer C which divides $2d$, such that $C \neq 1, -d$ and that the equation*

$$x^2 - dy^2 = C \qquad (44)$$

is solvable.

If d is square-free, then there are exactly two square-free integers C which divide $2d$, such that $C \neq 1, -d$ and that the equation (44) is solvable. The product of these two values of C is equal $-4d$ when d is odd and C is even; in all other cases the product is equal $-d$.

Proof. See [20, Theorems 11.2 and 11.3]. ■

k	d_1, d_2, d_3, j_1, j_2
108	7085, 1819, 864, 1, 5
192	111361, 191, 1536, 1, 1
312	293281, 311, 2496, 1, 1
405	7714, 404, 1620, 2, 64
432	561601, 431, 3456, 1, 1
513	197891, 393728, 2052, 2, 4
548	2745, 28991, 4384, 1, 329
600	1082401, 599, 4800, 1, 1
602	1089621, 57095, 4816, 1, 1
673	340370, 678048, 2692, 2, 4
675	684788, 15502, 2700, 2, 2
698	1464405, 16031, 5584, 1, 1
720	1558081, 719, 5760, 1, 1
744	1663585, 72071, 5952, 1, 1
801	482002, 960800, 3204, 2, 4
838	422017, 5859, 6704, 1, 5

Table 6:

Lemma 12 *Let d and n be integers such that $d > 0$, d is not a perfect square, and $|n| < \sqrt{d}$. If $x^2 - dy^2 = n$, then $\frac{x}{y}$ is a convergent of the simple continued fraction of $\sqrt{d}$.*

PROOF. See [21, Theorem 7.24] ■

$$\boxed{k = 108}$$

We have the system

$$7085x^2 - 1819y^2 = 1, \quad (45)$$
$$864x^2 - 1819z^2 = 5. \quad (46)$$

By Lemma 12 we have that $\frac{1819y}{x}$ is a convergent of the simple continued fraction of $\sqrt{1819 \cdot 7085}$. Using MATHEMATICA, we find that the minimal solution of (45) is

$$x_1 = 5 \cdot 31 \cdot 3336834223313386522939860860860 8237,$$
$$y_1 = 2 \cdot 7 \cdot 11 \cdot 19 \cdot 73 \cdot 97 \cdot 191 \cdot 257939363360940170442 3241.$$

Since $5|x_1$, Lemma 9 implies $5|x$ which contradicts the equation (46).

$$\boxed{k = 192}$$

Using continued fraction algorithm we find that the equation $a^2 - 111361 \cdot 191b^2 = 193$ is solvable. Note that $111361 = 193 \cdot 577$. Hence, Lemma 11 implies that the equation $a^2 - 111361 \cdot 191b^2 = -191$ is not solvable and accordingly the equation $111361x^2 - 191y^2 = 1$ has no integer solution.

$$\boxed{k = 312}$$

As in the case $k = 192$, since the equation $a^2 - 311 \cdot 293281b^2 = 626$ is solvable and $293281 = 313 \cdot 937$, we conclude that the equation $293281x^2 - 311y^2 = 1$ is not solvable.

$$\boxed{k = 405}$$

From [19, Theorem 108] if follows that the fundamental solutions of the equation $u^2 - 405 \cdot 101v^2 = 16 \cdot 405$ are $(u_0, v_0) = (\pm 1620, 8)$. Hence, from

$405x^2 - 101z^2 = 16$ it follows that x is even, and this is in a contradiction with $3875x^2 - 202y^2 = 1$.

$$\boxed{k = 432}$$

Using continued fraction algorithm we conclude from Lemma 12 that the equation $a^2 - 3456 \cdot 431b^2 = -431$ is not solvable, and therefore the equation $3456x^2 - 431y^2 = 1$ is not solvable too.

$$\boxed{k = 513}$$

Since the equation $a^2 - 57 \cdot 1538b^2 = -2$ has a solution, Lemma 11 implies that the equation $57 \cdot (3x)^2 - 1538(8y)^2 = 1$ has no solution.

$$\boxed{k = 548}$$

As in the case $k = 108$, we find that the minimal solution of the equation $2745x^2 - 28991y^2 = 1$ is $x_1 = 293 \cdot 760351607 \cdot 305381425231$, $y_1 = 2^6 \cdot 7^3 \cdot 1823 \cdot 523122644602993$. Hence $523122644602993 | y$, but then $2745z^2 - 4384y^2 = -31$ is impossible since $\left(\frac{-2745 \cdot 31}{523122644602993} \right) = -1$.

$$\boxed{k = 600}$$

Since the equation $a^2 - 1082401 \cdot 599b^2 = 3602$ has a solution and $1082401 = 601 \cdot 1801$, we conclude that the equation $1082401x^2 - 599y^2 = 1$ is not solvable.

$$\boxed{k = 602}$$

Solvability of the equation $a^2 - 301 \cdot 57095b^2 = -1634$ implies unsolvability of the equation $301 \cdot (4x)^2 - 57095y^2 = 1$.

$$\boxed{k = 673}$$

As in the previous two cases, solvability of the equation $a^2 - 170185 \cdot 21189b^2 = -1011$ implies, by Lemma 11, unsolvability of the equation $170185x^2 - 339024y^2 = 1$.

$$\boxed{k = 675}$$

The minimal solution of the equation $150u^2 - 7751z^2 = 1$ is $u_1 = 2 \cdot 343488449$, $z_1 = 19 \cdot 71 \cdot 70843$. Hence by Lemma 9 we have $71|z$. But then $171197z^2 - 675y^2 = -22$ is impossible since $\left(\frac{675 \cdot 22}{71}\right) = -1$.

$$\boxed{k = 698}$$

As in the previous case, from the minimal solution of the equation $1464405x^2 - 16031y^2 = 1$ we conclude that $3|x$. Furthermore, in the same way, from the equation $5584x^2 - 16031z^2 = 1$ we obtain that $3|z$ and this is an obvious contradiction.

$$\boxed{k = 720}$$

Since the equation $a^2 - 1558081 \cdot 719b^2 = -1438$ has a solution, we conclude that the equation $155808x^2 - 719y^2 = 1$ has no solution.

$$\boxed{k = 744}$$

Since the equation $a^2 - 5952 \cdot 72071b^2 = 97$ has a solution, the equation $5952x^2 - 72071y^2 = 1$ has no solution.

$$\boxed{k = 801}$$

The solvability of the equation $a^2 - 1201 \cdot 241001b^2 = 401$ implies unsolvability ot the equation $241001x^2 - 1201 \cdot (20y)^2 = 1$.

$$\boxed{k = 838}$$

The minimal solution of the equation $422017x^2 - 5859y^2 = 1$ satisfies $5|x_1$. It implies that $5|x$. But then $6704x^2 - 5859z^2 = 5$ is clearly impossible.

Therefore, we eliminated all cases and we proved the following theorem.

Theorem 10 *If* $3 \leq k \leq 1000$*, then all integer points on* E_k *are given by (7).*

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

[4] J. H. E. Cohn, *Lucas and Fibonacci numbers and some Diophantine equations*, Proc. Glasgow Math. Assoc. **7** (1965), 24–28.

[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, 1966, pp. 513–520.

[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, *Diophantine triples and construction of high-rank elliptic curves over* $\mathbf{Q}$ *with three non-trivial* 2*-torsion points*, Rocky Mountain J. Math., to appear.

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

[11] A. Dujella and A. Pethő, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen, to appear.

[12] S. Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur* $\mathbf{Q}$, Experimental Math. **5** (1996), 119-130.

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

[14] A. Grelak and A. Grytczuk, *On the diophantine equation* $ax^2 - by^2 = c$, Publ. Math. Debrecen **44** (1994), 191–199.

[15] C. M. Grinstead, *On a method of solving a class od Diophantine equations*, Math. Comp. **32** (1978), 936–940.

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

[17] K. S. Kedlaya, *Solving constrained Pell equations*, Math. Comp. **67** (1998), 833–842.

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

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

[20] T. Nagell, *Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns*, Nova Acta Soc. Sci. Upsal. **16** (1954), 1–38.

[21] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, Wesley, New York, 1991.

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

[23] J. H. Rickert, *Simultaneous rational approximations and related diophantine equations*, Math. Proc. Cambridge Philos. Soc. **113** (1993), 461–472.

[24] J. H. Silverman, *Rational points on elliptic surfaces*, preprint.

[25] SIMATH manual, Saarbrücken, 1997.

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

E-mail address: duje@math.hr