ACTA ARITHMETICA
XCIV.1 (2000)

A parametric family of elliptic curves

by

Andrej Dujella (Zagreb)

1. Introduction. A set of positive integers $\{a_1, \ldots, a_m\}$ is called a *Diophantine m-tuple* if $a_i a_j + 1$ is a perfect square for all $1 \le i < j \le m$. The problem of construction of Diophantine m-tuples has a long history (see [4]). 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 [1] 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 ([5, 6, 8]). The main result of [5] is the following theorem.

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

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

$$v_0 = 1, \quad v_1 = 2k - 1, \quad v_{m+2} = 2kv_{m+1} - v_m, \quad m \ge 0,$$
$$w_0 = 1, \quad w_1 = 3k - 2, \quad w_{n+2} = (4k-2)w_{n+1} - w_n, \quad n \in \mathbb{Z}.$$

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

2000 *Mathematics Subject Classification*: 11G05, 11D09, 11Y50.

the upper bound for solutions, obtained from the theorem of Rickert [20] 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 [13].

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

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

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 the assumption that $\operatorname{rank}(E_k(\mathbb{Q}))=1$. 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 2 and for one subfamily with rank 3. Finally, using the 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 [9] the family of elliptic curves

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

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 $\operatorname{rank}(C_l(\mathbb{Q})) = 2$ or $l \leq 40$, with possible exceptions $l = 23$ and $l = 37$, then all integer points on C_l are

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

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

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

2. Torsion group. The coordinate transformation

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

applied on the curve E_k leads to the elliptic curve

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

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. $E'_k(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Proof. Assume that $E'_k(\mathbb{Q})_{\mathrm{tors}}$ contains a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Then a theorem of Ono [19, 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, $E'_k(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $E'_k(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, and according to the theorem of Ono the latter is possible iff there exist integers α and β such that $\alpha/\beta \notin \{-2, -1, -1/2, 0, 1\}$ and

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

Now we have

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

which is impossible since the 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. $\mathrm{rank}(E'_k(\mathbb{Q})) \geq 1$.

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

3. Case $\mathrm{rank}(E_k(\mathbb{Q})) = 1$

LEMMA 1. $P_k, P_k + A_k, P_k + B_k, P_k + C_k \notin 2E'_k(\mathbb{Q})$.

Proof. We have

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

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 $k \geq 2$), by [15, 4.2, p. 85] we conclude that $P_k, P_k + A_k, P_k + B_k, P_k + C_k \notin 2E'_k(\mathbb{Q})$. ∎

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

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

is 1, *then all integer points on E_k are*

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

Proof. Let $E_k'(\mathbb{Q})/E_k'(\mathbb{Q})_{\text{tors}} = \langle U \rangle$ and $X \in E_k'(\mathbb{Q})$. 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, m_P is odd. Hence, $U \equiv P + T_P \pmod{2E_k'(\mathbb{Q})}$. Therefore we have $X \equiv X_1 \pmod{2E_k'(\mathbb{Q})}$, where

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

Let $\{a,b,c\} = \{4k^2+4k, 4k^2-4k, k^2-1\}$. By [15, 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.

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 $X_1 = (4k(k^2-1)u, 4k(k^2-1)v) \in \mathcal{S}$, the 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 [5], and its solutions correspond to the integer 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 find 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

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

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 again have a contradiction.

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

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

Assume that k is even. Since $(k+1)'$ divides $(k-1)x+1$ and $4kx+1$ we have $(k+1)' \mid (3k+1)$, which implies $(k+1)'=1$ and $k+1=\square$. In the same way we obtain $k-1=\square$, which 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 as the number $(k+1)(3k+1)\square = (k-1)x+1$ is odd we should have $(k+1)(3k+1)\equiv 0 \pmod{16}$. This implies $k\equiv 5$ or $7 \pmod 8$.

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

Remark 1. Bremner, Stroeker and Tzanakis [2] recently proved a result similar to our Theorem 3 for the family of elliptic curves

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

under the assumptions that $\operatorname{rank}(C_k(\mathbb{Q}))=1$ and that $C_k(\mathbb{Q})/C_k(\mathbb{Q})_{\mathrm{tors}} = \langle (1,k)\rangle$.

We come to the following natural question: How realistic is the condition $\mathrm{rank}(E_k(\mathbb{Q})) = 1$? We calculated the rank for $2 \le k \le 100$ using the programs SIMATH [22] and MWRANK [3]. The rank values are listed in Table 1.

Table 1

$\mathrm{rank}(E_k(\mathbb{Q})) = 1$	$k = 2, 3, 5, 7, 8, 9, 12, 13, 17, 18, 24, 26, 28, 29, 33, 35, 36, 41, 44, 51, 55, 57, 58, 61, 64, 66, 67, 70, 73, 75, 78, 79, 82, 85, 86, 87, 89, 92, 96, 98, 100$
$\mathrm{rank}(E_k(\mathbb{Q})) = 2$	$k = 4, 6, 10, 11, 15, 16, 19, 20, 21, 22, 23, 25, 27, 30, 32, 37, 38, 39, 40, 42, 43, 45, 46, 47, 48, 49, 50, 53, 54, 59, 62, 65, 68, 69, 71, 72, 74, 77, 81, 83, 84, 88, 90, 91, 93, 94^*, 95, 97, 99$
$\mathrm{rank}(E_k(\mathbb{Q})) = 3$	$k = 14, 31, 34, 52, 56, 60, 63, 76, 80$

The rank has been determined unconditionally for k in the range $2 \le k \le 100$ 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.

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

THEOREM 4. $\mathrm{rank}\, E'(\mathbb{Q}(k)) = 1$.

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

$$\begin{aligned} p(k) + (k^2-1)q^2(k) &= \mu_1(k)\mu_2(k)\square, \\ p(k) + (4k^2-4k)q^2(k) &= \mu_1(k)\mu_3(k)\square, \\ p(k) + (4k^2+4k)q^2(k) &= \mu_2(k)\mu_3(k)\square, \end{aligned}$$

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

Furthermore, we have $\mu_1(k) \mid (k-1)(3k-1)$, $\mu_2(k) | (k+1)(3k+1)$ and $\mu_3(k) \mid 8k$. Hence,

$$\begin{aligned} &\mu_1(k) \in \{1, k-1, 3k-1, (k-1)(3k-1)\}, \\ &\mu_2(k) \in \{\pm 1, \pm(k-1), \pm(3k-1), \pm(k-1)(3k-1)\}, \\ &\mu_3(k) \in \{\pm 1, \pm 2, \pm k, \pm 2k\}. \end{aligned}$$

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

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

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 now consider the specialization $k = 12$. We choose $k = 12$ because $\operatorname{rank}(E'_{12}(\mathbb{Q})) = 1$, $E'_{12}(\mathbb{Q})/E'_{12}(\mathbb{Q})_{\text{tors}} = \langle P_{12} \rangle$ and furthermore the 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 than 8 choices for $(\mu_1(k), \mu_2(k), \mu_3(k))$ on $E'(\mathbb{Q}(k))$, there will be more than 8 choices on $E'_{12}(\mathbb{Q})$. 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 $E(\mathbb{Q}(k))$. Consider the 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 [14, 4.3, p. 125], these two points are congruent modulo $2E'(\mathbb{Q}(k))$. We have already proved in Theorem 2 and Lemma 1 that the first eight points are incongruent modulo $2E'(\mathbb{Q}(k))$ (since the specialization map is a homomorphism). Hence we have two possibilities:

(1) $V \equiv T_1 \pmod{2E'(\mathbb{Q}(k))}$,
(2) $V \equiv P(k) + T_2 \pmod{2E'(\mathbb{Q}(k))}$,

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

Let $\{D_1, \ldots, D_r\}$ be the Mordell–Weil base for $E'(\mathbb{Q}(k))$ 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) $D_r \equiv T_1 \pmod{2E'(\mathbb{Q}(k))}$. This 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) $D_r \equiv P(k) + T_2 \pmod{2E'(\mathbb{Q}(k))}$. Now we have

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

Hence, α_{r-1} is even and α_r is odd. Analogously, considering 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 $E'(\mathbb{Q}(k))$ to be

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

then the Katz–Sarnak Conjecture (see [21]) states that

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

This means that at least 50% of curves E_k should have rank 1. As explained in [21], the Katz–Sarnak Conjecture is not in complete agreement with experimental results of Fermigier [10]. Examining an extensive collection of data (66918 curves in 93 families) Fermigier found that $\text{rank}(E_t(\mathbb{Q})) = \text{rank}\, E(\mathbb{Q}(t))$ in 32% of cases. Perhaps it can be compared with our situation where we found that in the range $2 \le k \le 200$ we have $\text{rank}(E'_k(\mathbb{Q})) = \text{rank}\, E'(\mathbb{Q}(k))$ 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. Families with rank equal 2 and 3. The Katz–Sarnak Conjecture implies, and Table 1 confirms, 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 $\text{rank}(E'_k(\mathbb{Q})) > 1$. 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 $3/4$, 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 $k_2(m) = \frac{1}{2}(3m^2 + 5m)$.

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

$$R_n = (3(n+1)(3n-1)(3n^2+2n-3)(3n^2+2n-2),\\ (n+1)(3n-1)(3n+1)(3n^2+2n-3)(3n^2+2n-2)(9n^2+6n-5))$$

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

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

([1]) In SIMATH there is implemented the algorithm of Gebel, Pethő and Zimmer [11] for computing all integer points of the elliptic curve.

Using similar arguments to those in the previous section, we can prove that $\operatorname{rank}(E_n^*(\mathbb{Q})) \geq 2$ for $n \neq -1, 0, 1$ and that the generic rank of E^* over $\mathbb{Q}(n)$ is 2.

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

We omit the proof of Theorem 5 since it differs from the proof of Theorem 3 only in technical details. An interested reader may find the complete proof in the extended version of this paper which can be obtained from: http://www.math.hr/~duje/papers.html.

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

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

We can prove that $\operatorname{rank}(E_m^\circ(\mathbb{Q})) \geq 2$ for $m \neq -2, -1, 0$ and that the generic rank of E° over $\mathbb{Q}(m)$ is equal 2.

THEOREM 6. *If* $\operatorname{rank}(E_m^\circ(\mathbb{Q})) = 2$, *then all integer points on* E_k, *where* $k = k_2(m)$, *are given by* (7).

Again, we omit the proof and we refer an interested reader to the extended version of the paper.

Assuming the Katz–Sarnak Conjecture, Theorems 5 and 6 imply that Conjecture 1 is valid for infinitely many curves of rank 2.

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

$$(6m+5)^2 - 2(6n+2)^2 = -31. \tag{14}$$

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

$$r_0 = 1, \quad r_1 = 19, \quad r_{i+2} = 6r_{i+1} - r_i, \quad i \in \mathbb{Z}; \tag{15}$$

$$s_0 = 1, \quad s_1 = 14, \quad s_{i+2} = 6s_{i+1} - s_i, \quad i \in \mathbb{Z}. \tag{16}$$

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

$$k_2(m) = \frac{1}{24}(r^2 - 25).$$

For the sake of simplicity, denote $E'_{(r^2-25)/24}$ by $E_i^\diamond$.

Using the properties of the recursive sequence (r_i) it is not hard to check that $\operatorname{rank}(E_i^\diamond(\mathbb{Q})) \geq 3$ for $i \neq -1, 0$, and to prove the following theorem.

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

In Table 2 we list a few rank values of $E_i^\diamond(\mathbb{Q})$.

Table 2

i	r	m	s	n	k	$\operatorname{rank}(E_i^\diamond(\mathbb{Q}))$
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

We do not have enough data to support any conjecture about the distribution of $\operatorname{rank}(E_i^\diamond(\mathbb{Q}))$. However, from Theorem 7 and Table 2 we obtain immediately

COROLLARY 2.

$$\limsup\{\operatorname{rank}(E_k(\mathbb{Q})) : k \geq 2\} \geq 3,$$
$$\sup\{\operatorname{rank}(E_k(\mathbb{Q})) : k \geq 2\} \geq 5.$$

Let us note that in [7] an example is constructed which shows that

$$\sup\{\operatorname{rank}(E(\mathbb{Q})) : E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\} \geq 7.$$

5. Case $k \leq 1000$. In this section we check Conjecture 1 for $k \leq 1000$ using the approach introduced in [9]. Assume that (x, y) is a solution of

$$y^2 = ((k-1)x + 1)((k+1)x + 1)(4kx + 1). \tag{17}$$

Then there exist integers x_1, x_2, x_3 such that

$$(k-1)x + 1 = \mu_2\mu_3 x_1^2,$$
$$(k+1)x + 1 = \mu_1\mu_3 x_2^2,$$
$$4kx + 1 = \mu_1\mu_2 x_3^2,$$

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

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

$$(k+1)\mu_2 x_1^2 - (k-1)\mu_1 x_2^2 = 2,$$
$$4kx_1^2 - (k-1)\mu_1 x_3^2 = (3k+1)/\mu_2,$$

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

$$(k+1)\mu_2 x_1^2 - (k-1)\mu_1 x_2^2 = 1,$$
$$8kx_1^2 - (k-1)\mu_1 x_3^2 = (3k+1)/\mu_2.$$

Hence, to find all integer solutions of (17), it is enough to find all integer solutions of the systems of equations

$$d_1 x_1^2 - d_2 x_2^2 = j_1, \tag{18}$$

$$d_3x_1^2 - d_2x_3^2 = j_2, \tag{19}$$

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 $3k-1$,
- $(d_3, j_1, j_2) = (4k, 2, (3k+1)/\mu_2)$ or $(8k, 1, (3k+1)/\mu_2)$.

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 [5]. 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 (18) and (19) we obtain

$$d_1x_3^2 - d_3x_2^2 = j_3, \tag{20}$$

where $j_3 = (j_1d_3 - j_2d_1)/d_2$.

We first consider the equations (18), (19) and (20) 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 $\operatorname{ord}_{p_4}(j_2)$ is odd, p_5 is an odd prime divisor of j_3 such that $\operatorname{ord}_{p_5}(j_3)$ is odd. Then necessary conditions for solvability of (18), (19) and (20) are:

$$\left(\frac{-j_1d_2}{p_1}\right) = 1, \quad \left(\frac{j_1d_1}{p_2}\right) = 1, \quad \left(\frac{j_2d_3}{p_2}\right) = 1,$$
$$\left(\frac{-j_2d_2}{p_3}\right) = 1, \quad \left(\frac{d_2d_3}{p_4}\right) = 1, \quad \left(\frac{d_1d_3}{p_5}\right) = 1,$$

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

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

$$\begin{gathered}j_1 \equiv d_1 - d_2 \pmod 8 \quad \text{or} \quad j_1 \equiv d_1 \pmod 4 \quad \text{or} \quad j_1 \equiv -d_2 \pmod 4;\\ j_2 \equiv 0 \pmod 4 \quad \text{or} \quad j_2 \equiv -d_2 \pmod 8;\\ j_3 \equiv 0 \pmod 4 \quad \text{or} \quad j_3 \equiv d_1 \pmod 8.\end{gathered}$$

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:

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

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

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

We performed these tests for $2 \le k \le 1000$ using A. Pethő's program developed for the purposes of our joint paper [9]. We found that all systems are unsolvable apart from 106 systems on which we apply further tests based on the properties of Pellian equations. These properties are contained in the following five lemmas.

LEMMA 2. (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 the Pell equation $u^2 - dv^2 = 1$. Then the equation*

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

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

(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 the Pell equation $u^2 - dv^2 = 1$. Then the equation*

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

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

Proof. See [12, Criteria 1 and 2]. ∎

LEMMA 3. *Let $a > 1$ and $b > 0$ be square-free integers. If (x_1, y_1) is the minimal solution of the equation*

$$ax^2 - by^2 = 1, \tag{21}$$

then all solutions of (21) 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, $x_1 \mid x$ and $y_1 \mid y$.

Proof. See [17, Theorem 11.1]. ∎

LEMMA 4. *Let $C \ne 0$ and $d \ne \square$ be integers and let (u_0, v_0) be the minimal solution of the Pell equation $u^2 - dv^2 = 1$. If the Pellian equation*

$$x^2 - dy^2 = C \tag{22}$$

has a solution, then there exists a solution of (22) such that

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

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

P r o o f. See [16, Theorems 108 and 108a]. ∎

LEMMA 5. *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*

$$x^2 - dy^2 = C \tag{23}$$

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 (23) is solvable. The product of these two values of C is $-4d$ when d is odd and C is even; in all other cases the product is $-d$.

P r o o f. See [17, Theorems 11.2 and 11.3]. ∎

LEMMA 6. *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 x/y is a convergent of the simple continued fraction of $\sqrt{d}$.*

P r o o f. See [18, Theorem 7.24]. ∎

Using Lemmas 2–6 we were able to eliminate all remaining 106 systems, and therefore we proved the following theorem.

THEOREM 8. *If $3 \leq k \leq 1000$, then all integer points on E_k are given by (7).*

All details are contained in the extended version of the paper, and here we present only four typical examples.

EXAMPLE 1. Let $k \geq 2$ be an integer. The equation

$$4kx^2 - (k-1)y^2 = 1$$

has no integer solution.

Indeed, in the notation of Lemma 2, we have $a = 4k$, $b = k - 1$, $u_0 = 2k - 1$, $v_0 = 1$ and $(u_0 + 1)/(2a) = 1/4 \notin \mathbb{Z}$.

This result eliminates 46 cases from the list of the remaining 106 cases.

EXAMPLE 2. Let $k = 162$ and consider the equation

$$163x^2 - 648y^2 = -5. \tag{24}$$

Assume that (24) has a solution. Then, by Lemma 4, the equation

$$X^2 - 163 \cdot 648Y^2 = -5 \cdot 163$$

has a solution (X, Y) which satisfies $0 < Y \leq 1 \cdot \sqrt{5 \cdot 163}/\sqrt{2(325 - 1)}$ < 1.12, a contradiction. Therefore, equation (24) has no integer solution.

EXAMPLE 3. Let $k = 108$ and consider the system

$$7085x^2 - 1819y^2 = 1, \tag{25}$$

$$864x^2 - 1819z^2 = 5. \tag{26}$$

By Lemma 6 we deduce that $1819y/x$ is a convergent of the simple continued fraction of $\sqrt{1819 \cdot 7085}$. Using MATHEMATICA, we find that the minimal solution of (25) is

$$x_1 = 5 \cdot 31 \cdot 33368342233133865229398608608608237,$$
$$y_1 = 2 \cdot 7 \cdot 11 \cdot 19 \cdot 73 \cdot 97 \cdot 191 \cdot 257939363360940170442324 1.$$

Since $5 \mid x_1$, Lemma 3 implies $5 \mid x$, which contradicts the equation (26).

EXAMPLE 4. Let $k = 192$ and consider the equation

$$111361x^2 - 191y^2 = 1. \tag{27}$$

The continued fraction algorithm shows that the equation $a^2 - 111361 \cdot 191b^2 = 193$ is solvable. Note that $111361 = 193 \cdot 577$. Hence, Lemma 5 implies that the equation $a^2 - 111361 \cdot 191b^2 = -191$ is not solvable and accordingly equation (27) has no integer solution.

Acknowledgements. The author would like to thank the referee for many helpful suggestions.

References

[1] 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.

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

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

[4] L. E. Dickson, *History of the Theory of Numbers*, Vol. 2, Chelsea, New York, 1966, pp. 513–520.

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

[6] —, *A proof of the Hoggatt–Bergum conjecture*, Proc. Amer. Math. Soc. 127 (1999), 1999–2005.

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

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

[9] —, —, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen, to appear.

[10] S. Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur* $\mathbb{Q}$, Experiment. Math. 5 (1996), 119–130.

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

[12] A. Grelak and A. Grytczuk, *On the diophantine equation* $ax^2 - by^2 = c$, Publ. Math. Debrecen 44 (1994), 191–199.
[13] C. M. Grinstead, *On a method of solving a class of Diophantine equations*, Math. Comp. 32 (1978), 936–940.
[14] D. Husemöller, *Elliptic Curves*, Springer, New York, 1987.
[15] A. Knapp, *Elliptic Curves*, Princeton Univ. Press, 1992.
[16] T. Nagell, *Introduction to Number Theory*, Almqvist, Stockholm; Wiley, New York, 1951.
[17] —, *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.
[18] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, Wiley, New York, 1991.
[19] K. Ono, *Euler's concordant forms*, Acta Arith. 78 (1996), 101–123.
[20] J. H. Rickert, *Simultaneous rational approximations and related diophantine equations*, Math. Proc. Cambridge Philos. Soc. 113 (1993), 461–472.
[21] J. H. Silverman, *Rational points on elliptic surfaces*, preprint.
[22] SIMATH manual, Universität des Saarlandes, Saarbrücken, 1997.

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

Received on 6.4.1999
and in revised form on 21.12.1999 (3583)