Publ. Math. Debrecen
75/3-4 (2009), 401–418

Integer points on two families of elliptic curves

By FILIP NAJMAN (Zagreb)

Abstract. In this paper we find all the integer points on elliptic curves induced by the Diophantine triples $\{k-1, k+1, 16k^3-4k\}$ and $\{k-1, k+1, 64k^5-48k^3+8k\}$ that have either rank two or $2 \leq k \leq 10000$ (with one possible exception).

1. Introduction

It is expected that the number of integer points on an elliptic curve E in Weierstrass form depends on the rank of $E(\mathbb{Q})$. More precisely, Lang conjectured that it grows exponentially with the rank (see [23]). Since not much is known on the distribution of ranks in parametric families of elliptic curves, it is hard to expect to find (or even predict) all integer points on a family of elliptic curves in Weierstrass form. However, for some families of elliptic curves not in Weierstrass form, there are results which give evidence that the number of integer points might not depend on rank, and that actually the number of points can be the same for all curves in a family. Several such results involve so called $D(n)-m$-tuples.

A set of positive integers $\{a_1, a_2, \ldots, a_m\}$ is called a *Diophantine* $D(n)-m$-*tuple* if a_ia_j+n is a perfect square for all $1 \leq i < j \leq m$. We define for $k \geq 0$, $c_l = ((k+\sqrt{k^2-1}\,)^{2l+1} + (k-\sqrt{k^2-1}\,)^{2l+1} - 2k)/(2(k^2-1))$. A parametric family induced by the Diophantine $D(1)$-triples $\{k-1, k+1, c_1\}$ has been examined in [6] and all the integer points have been determined under the assumption that the rank of the elliptic curve is 1. This is a consequence of the fact that the

Mathematics Subject Classification: 11G05, 11Y50.
Key words and phrases: family of elliptic curves, integer points, Diophantine m-tuple.
The author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, Grant 037-0372781-2821.

Diophantine $D(1)$-triple $\{k-1, k+1, c_1\}$ can be uniquely extended to a quadruple with the same property by c_2 (proven in [5]).

Let us mention the articles [12], [13], [7] and [9] in which are examined families of elliptic curves induced by the $D(-1)$-triples $\{F_{2k+1}, F_{2k+3}, F_{2k+5}\}$, the $D(-1)$-triples $\{1, 2, \frac{1}{8}((1+\sqrt{2})^{4k} + (1-\sqrt{2})^{4k} + 6)\}$ and the $D(1)$-triples $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$ and $\{1, 3, c_l(2)\}$ respectively, where $c_l(2)$ denotes the c_l with $k = 2$.

In all these families, except [12], the integer points come from the possible extensions of the triple.

It has been recently proven (see [11] and [2]) that the Diophantine $D(1)$-triple $\{k-1, k+1, c_l\}$ can be extended to a quadruple with the same property only by either c_{l-1} or c_{l+1}.

Although it has been conjectured by Dujella that all the integer points can be determined (and arise from the possible extensions) on all families of elliptic curves induced by the triple $\{k-1, k+1, c_l\}$, there are no general results so far. As the next logical step, we examine the families induced by the triples $\{k-1, k+1, c_2\}$ and $\{k-1, k+1, c_3\}$.

2. The family generated by c_2

We examine the elliptic curve

$$E_k : y^2 = ((k-1)x+1)((k+1)x+1)((16k^3-4k)x+1). \tag{1}$$

We use the variable change

$$y \mapsto \frac{y}{(k-1)(k+1)(16k^3-4k)}, \quad x \mapsto \frac{x}{(k-1)(k+1)(16k^3-4k)},$$

and obtain the curve

$$E_k' : y^2 = (x+k^2-1)(x+16k^4-16k^3-4k^2+4k)(x+16k^4+16k^3-4k^2-4k). \tag{2}$$

We have three obvious points

$$A = (1-k^2, 0),\ B = (-16k^4+16k^3+4k^2-4k, 0),\ C = (-16k^4-16k^3+4k^2+4k, 0)$$

of order two. We will prove these are the only points of finite order.

Lemma 1. $E_k(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Proof. As $\{k-1, k+1, 16k^3-4k\}$ is a Diophantine triple, by ([7], Theorem 2) there are no points of order 4.

Suppose $E_k(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 + \mathbb{Z}_6$ for $l \geq 2$. By a theorem of Ono ([21], Main Theorem 1), this implies there exist integers a, b such that

$$32k^3 - 8k = a^4 + 2a^3b \quad \text{and} \quad -16k^4 + 16k^3 + 5k^2 - 4k - 1 = b^4 + 2ab^3.$$

From the first equation we see that a has to be even, so the right side is divisible by 16, which implies k is even. Adding these equations we obtain

$$-16k^4 + 48k^3 + 5k^2 - 12k - 1 = (a^2 + ab + b^2)^2 - 3a^2b^2,$$

which is impossible since the left side is congruent to 3 or 7 modulo 8, while the right side is congruent to 1 or 6 modulo 8. By Mazur's theorem, this proves the lemma. $\square$

We define

$$P = (0, (k^2-1)(16k^3-4k)),\ R = (-16(-k^2+k^4), 4k(1+3k-4k^2)(-1+3k+4k^2)).$$

It is easy to see that both points lie on the curve $E_k(\mathbb{Q})$.

Lemma 2. *$R, R+A, R+B, R+C \notin 2E'_k(\mathbb{Q})$.*

Proof. The 2-descent proposition (see [16], Theorem 4.2, p. 85) implies that $R \in 2E'_k(\mathbb{Q})$ iff $x(R) + k^2 - 1$, $x(R) + 16k^4 - 16k^3 - 4k^2 + 4k$ and $x(R) + 16k^4 + 16k^3 - 4k^2 - 4k$ are squares. For the rest of the article we will use this argument without mentioning it.

For $k \geq 2$, $x(R) + k^2 - 1 < 0$, and thus can not be a square, which proves $R \notin 2E'_k(\mathbb{Q})$. $x(R + A) = -16k^4 + 8k^2$, so for $k \geq 2$, $x(R + A) + k^2 - 1 < 0$ and thus it can not be a square, which proves $R + A \notin 2E'_k(\mathbb{Q})$.

Suppose $R + B \in 2E'_k(\mathbb{Q})$. $x(R + B) = 16k^4 + 8k^3 - 12k^2 - 2k + 2$, so $16k^4+8k^3-11k^2-2k+1$ is a square, but $(4k^2+k-2)^2 < 16k^4+8k^3-11k^2-2k+1 < (4k^2 + k - 1)^2$ for $k \geq 2$. $R + C \notin 2E'_k(\mathbb{Q})$ is proved in the same way. $\square$

Lemma 3. *$P, P + A, P + B, P + C \notin 2E'_k(\mathbb{Q})$.*

Proof. P is obviously not in $2\ E'_k(\mathbb{Q})$ since $k^2 - 1$ can not be a square.

Suppose $P + A \in 2E'_k(\mathbb{Q})$. Then $x(P + A) = 256k^6 - 160k^4 + 24k^2$, so $256k^6 - 160k^4 + 25k^2 - 1 = (16k^3 - 5k)^2 - 1$ is a square, which is impossible.

Suppose $P + B \in 2E'_k(\mathbb{Q})$. $x(P + B) = -16k^4 - 16k^3 + 4k^2 + 6k + 2$, so $x(P+B)+k^2-1 = 1+6k+5k^2-16k^3-16k^4 < 0$ for $k \geq 2$. The same argument works for $P + C$. $\square$

Lemma 4. $R+P, R+P+A, R+P+B, R+P+C \notin 2E'_k(\mathbb{Q})$.

Proof. $x(R+P) = \frac{-64k^6+64k^4-16k^2+1}{4k^2}$, so $x(R+P)+k^2-1<0$ for $k \geq 2$, and hence can not be a square, which implies $R+P \notin 2E'_k(\mathbb{Q})$.

$x(R+P+A) = \frac{-64k^8+96k^6-32k^4-k^2+1}{4k^4-4k^2+1}$, so $x(R+P)+k^2-1<0$ for $k \geq 2$, and hence can not be a square, which implies $R+P+A \notin 2E'_k(\mathbb{Q})$.

$x(R+P+B) = \frac{64k^6-32k^5-64k^4+16k^3+20k^2-4k}{4k^2-4k+1}$. Suppose $R+P+B \in 2E'_k(\mathbb{Q})$. This implies $x(R+P+B)-4k-4k^2+16k^3+16k^4$ is a rational square. Hence $8k(-1+4k)(1-2k^2)^2$ is a square, which implies that $8k(-1+4k)$ is a square. But $8k$ and $4k-1$ are coprime, and $4k-1$ can not be a square, since it is congruent to 3 modulo 4.

Suppose $R+P+C \in 2E'_k(\mathbb{Q})$. Then $x(R+P+C)+k^2-1$ is a square, which implies $-1-4k+5k^2+24k^3+16k^4$ is a square, but $(4k^2+3k-1)^2 < -1-4k+5k^2+24k^3+16k^4 < (4k^2+3k)^2$. □

Proposition 5. *The rank of E'_k over $\mathbb{Q}$ is greater than or equal to two.*

Proof. We claim that R and P generate a subgroup of rank 2 in $E'_k(\mathbb{Q}) / E'_k(\mathbb{Q})_{\mathrm{tors}}$. We will prove $aP+bR \in E'_k(\mathbb{Q})_{\mathrm{tors}}$ implies $a=b=0$.

Suppose $aP+bR = T \in E'_k(\mathbb{Q})_{\mathrm{tors}}$. If a and b are not both even, then one of the following is true: $P+T \in 2E'_k(\mathbb{Q})$, $R+T \in 2E'_k(\mathbb{Q})$, $P+R+T \in 2E'_k(\mathbb{Q})$. This gives a contradiction with Lemmas 2, 3 and 4. We conclude that $a=2a_1$ and $b=2b_1$. We have $2a_1P+2b_1R \in E'_k(\mathbb{Q})_{\mathrm{tors}}$, so $a_1P+b_1R \in E'_k(\mathbb{Q})_{\mathrm{tors}}$. We can again conclude that a_1 and b_1 are both even and continuing this process we get $a=b=0$. □

Theorem 6. *If* $\operatorname{rank}(E_k(\mathbb{Q})) = 2$ *or* $2 \leq k \leq 10000$ *and* $k \neq 6300$*, then all integer points on* E_k *are given by*

$$(x,y) \in \{(0,\pm 1),\ (4k, \pm(1-12k^2+32k^4)),$$
$$(64k^5-48k^3+8k, \pm(1-40k^2+496k^4-2112k^6+3584k^8-2048k^{10}))\}. \quad (3)$$

The x-coordinates of the non trivial integer points correspond to c_1 and c_3.

Proof. *Case* $\operatorname{rank}(E_k)=2$

Let $\delta = (k-1)(k+1)(16k^3-4k)$. If $X_0 = (u,v)$ is an integer point on E_k, then $X = (\delta u, \delta v)$ is an integer point on E'_k. Let $E'_k(\mathbb{Q})/E'_k(\mathbb{Q})_{\mathrm{tors}} = \langle U, V\rangle$. Then $P \equiv U_1+T_1 \pmod{2E'_k(\mathbb{Q})}$, $R = U_2+T_2 \pmod{2E'_k(\mathbb{Q})}$ and $P+R \equiv U_3+(T_1+T_2) \pmod{2E'_k(\mathbb{Q})}$, where T_i are torsion points and U_i are elements of $\langle U,V\rangle$. From Lemmas 2, 3 and 4 we have $\{U_1,U_2,U_3\} = \{U,V,U+V\}$. Now we have $X \equiv X_1 \pmod{2E'_k(\mathbb{Q})}$, where

$$X_1 \in S = \{O, A, B, C, P, P+A, P+B, P+C, R, R+A, R+B, R+C,\\ P+R, P+R+A, P+R+B, P+R+C\}.$$

Let $\{a,b,c\} = \{(k-1)(k+1), (k-1)(16k^3-4k), (k+1)(16k^3-4k)\}$. By [16], Proposition 4.6, p. 89, the function $\phi : E'_k(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ defined by

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

is a group homomorphism.

This implies that to find integer points on E, all we have to do is find integer solutions to all systems of the form

$$(k-1)x+1 = \alpha\square, \quad (k+1)x+1 = \beta\square, \quad (16k^3-4k)x+1 = \gamma\square,$$

where for $X_1 = (\delta u, \delta v)$, α, β, γ are defined by $\alpha = (k-1)u+1$, $\beta = (k+1)u+1$, $\gamma = (16k^3-4k)u+1$ if all these are nonzero, and if one is zero then that one is defined as the product of the other two. $\square$ denotes a rational square, and we will use this notation in the rest of the paper.

1) $X_1 = P$

This case is completely solved in [2] and corresponds to the integer points whose x-coordinates are $4k$ and $64k^5 - 48k^3 + 8k$.

2) $X_1 \in \{B, C, P+B, P+C, R, R+A, R+P, R+P+A\}$

In these cases, exactly two of the numbers from the set $\{\alpha, \beta, \gamma\}$ are negative, so the system has no solutions.

3) $X_1 = O$

This induces the system

$$(k-1)x+1 = k(k+1)(4k^2-1)\square, \qquad (k+1)x+1 = k(k-1)(4k^2-1)\square,$$
$$(16k^3-4k)x+1 = (k-1)(k+1)\square.$$

Let X' be the square-free part of X. We will use this notation in the rest of the paper. We note that $\gcd((4k^2-1)', (k+1)') = 1$ or 3 and $\gcd((4k^2-1)', (k-1)') = 1$ or 3 (obviously $(k-1)'$ and $(k+1)'$ can not be both divisible by 3). If $3|(k+1)'$ or

$3|(k-1)'$, this implies that in the last equation the right side is divisible by 3 an odd number of times, while the left side is congruent to 1 modulo 3. We conclude that $\gcd((4k^2-1)',(k+1)') = \gcd((4k^2-1)',(k-1)') = 1$. By subtracting the first equation from the second we see that $(4k^2-1)' > 1$ divides x, which makes the first equation impossible since $(4k^2-1)'$ divides the right side, but not the left.

4) $X_1 = R + B$

This induces the system

$$(k-1)x+1 = 2k(4k-1)\square, \qquad (k+1)x+1 = 2k(4k^2-k-1)(k-1)\square,$$
$$(16k^3-4k)x+1 = (k-1)(4k-1)(4k^2-k-1)\square.$$

If k is even, then $(k-1)(4k-1)(4k^2-k-1) \equiv 3 \pmod 4$, while the left side in the third equation is congruent to 1 modulo 4, which is a contradiction.

If k is odd, then $2k(4k-1) \equiv 2 \pmod 4$, which implies $2k(4k-1)\square$ is even, while the left side of the first equation is odd, a contradiction.

5) $X_1 = R + C$

This induces the system

$$(k-1)x+1 = 2k(k+1)(4k^2+k-1)\square, \qquad (k+1)x+1 = 2k(4k+1)\square,$$
$$(16k^3-4k)x+1 = (k+1)(1+4k)(-1+k+4k^2)\square.$$

If k is even, then $(k+1)(1+4k)(-1+k+4k^2) \equiv 3 \pmod 4$, while the left side in the third equation is congruent to 1 modulo 4, which is a contradiction.

If k is odd, the left side of the second equation is odd, while $2k(4k+1) \equiv 2 \pmod 4$, which implies the right side is even, a contradiction.

6) $X_1 = A$

This induces the system

$$(k-1)x+1 = k(-1+4k^2)(-1+4k)(-1+k+4k^2)\square,$$
$$(k+1)x+1 = k(-1+4k^2)(1+4k)(-1-k+4k^2)\square,$$
$$(16k^3-4k)x+1 = (-1+4k)(1+4k)(-1-k+4k^2)(-1+k+4k^2)\square.$$

If k is even, then $(-1+4k)(1+4k)(-1-k+4k^2)(-1+k+4k^2) \equiv 3 \pmod 4$, while the left side in the third equation is congruent to 1 modulo 4, which is a contradiction.

If $k \equiv 1 \pmod 4$, as in the above cases, we conclude that the right side of the second equation is even, while the left is odd.

If $k \equiv 3 \pmod 4$, as in the above cases, we conclude that the right side of the first equation is even, while the left is odd.

7) $X_1 = R + P + B$

This induces the system

$$(k-1)x + 1 = 2(-1+2k)(-1+4k)(2k+1)(k+1)\square,$$
$$(k+1)x + 1 = 2(1+2k)(-1-k+4k^2)(2k-1)\square,$$
$$(16k^3-4k)x + 1 = (k+1)(-1-k+4k^2)(4k-1)\square.$$

We note that $\gcd(((-1+4k)(k+1))', 4k^2-1) = 1$ or 3. If the result is 3, this gives a contradiction with the last equation, since the right side is divisible by 3 while the left is congruent to 1 modulo 3.

By subtracting the first equation from the second we obtain that $(2k+1)'$ and $(2k-1)'$ divide x. If $(2k+1)' > 1$ or $(2k-1)' > 1$ the first equation is impossible. So $2k+1 = \square$ and $2k-1 = \square$, which is impossible.

8) $X_1 = R + P + C$

This induces the system

$$(k-1)x + 1 = 2(-1+2k)(1+2k)(-1+k+4k^2)\square,$$
$$(k+1)x + 1 = 2(1+2k)(1+4k)(2k-1)(k-1)\square,$$
$$(16k^3-4k)x + 1 = (-1+k)(4k+1)(4k^2+k-1)\square.$$

Again, by subtracting the first equation from the second we obtain that $(2k+1)'$ and $(2k-1)'$ divide x. This implies that $2k+1$ and $2k-1$ are both squares, which is impossible.

9) $X_1 = P + A$

This induces the system

$$(k-1)x + 1 = (1+k)(4k-1)(4k^2+k-1)\square,$$
$$(k+1)x + 1 = (-1+k)(4k+1)(4k^2-k-1)\square,$$
$$(16k^3-4k)x + 1 = (-1+k^2)(-1+k+4k^2)(4k^2-k-1)(4k+1)(4k-1)\square.$$

First suppose $\gcd(((1+k)(4k-1)(4k^2+k-1))', ((-1+k)(4k+1)(4k^2-k-1))') = 1$. This implies, by subtracting the second equation from the third, that $((-1+k)(4k+1)(4k^2-k-1))' | (4k+1)(4k^2-k-1)x$. Since $(k-1)' | x$ would lead to a contradiction, we conclude $(k-1)' | (4k+1)(4k^2-k-1)$. But from

$(4k+1)(4k^2-k-1) = (11+16k+16k^2)(k-1)+10$, it follows that $(k-1)'|10$, i.e. $(k-1)' = 1, 2, 5$ or 10. In the same way as above we obtain $(k+1)' = 1, 2, 5$ or 10.

Examining the possibilities (modulo 5 and eliminating the trivial ones), we see that the only possible ones are that either $(k-1)' = 2$ or $(k+1)' = 2$. We conclude that k is odd. We can write k as $k = 2t-1$ or $k = 2t+1$, where t is an odd integer.

Suppose $k = 2t+1$. The right side of the second equation is then equal to $2t(8t+5)(4(2t+1)^2-2(t+1))\square$. This expression is divisible by 2 an odd number of times, giving a contradiction because the left side is odd, unless $ord_2(t+1) = 1$. Suppose $ord_2(t+1) = 1$. But now the right side of the first equation is divisible by 2 an odd number of times, while the left is odd, which is a contradiction.

Assume $k = 2t-1$. The right side of the first equation is then equal to $2t(8t-5)(4(2t-1)^2+2(t-1))\square$. In the same way as above, we will arrive at a contradiction.

Suppose $\gcd(((1+k)(4k-1)(4k^2+k-1))', ((-1+k)(4k+1)(4k^2-k-1))') = d_7 > 1$. This implies that $d_7|(k-1)x+1$ and $d_7|(k+1)x+1$, which implies $d_7|2x$. Since $d_7|x$ would lead to a contradiction, we conclude $d_7 = 2$, meaning that the right sides of the first and second equation will be divisible by 2 a odd number of times. On the other hand, $d_7 = 2$ implies that k has to be odd, making the left sides of the fist two equations odd, giving a contradiction.

Case $2 \le k \le 10000$

We now prove that the mentioned integer points are the only ones without any conditions on the rank, for $2 \le k \le 10000$ with one possible exceptional case. Assume (x, y) is an integer point on the elliptic curve E_k. This implies

$$(k-1)x+1 = \mu_2\mu_3x_1^2, \qquad (k+1)x+1 = \mu_1\mu_3x_2^2,$$
$$(16k^3-4k)x+1 = \mu_1\mu_2x_3^2,$$

where $\mu_1|16k^3-5k-1$, $\mu_2|16k^3-5k+1$, $\mu_3|2$. By eliminating x we obtain

$$d_1x_1^2 - d_2x_2^2 = j_1, \qquad d_3x_1^2 - d_2x_3^2 = j_2, \qquad d_1x_3^2 - d_3x_2^2 = j_3, \tag{4}$$

where $d_1 = (k+1)\mu_2$, μ_2 is a square-free factor of $16k^3-5k+1$, $d_2 = (k-1)\mu_1$, μ_1 is a square-free factor of $16k^3-5k-1$, $(d_3, j_1, j_2) = \left(16k^3-4k, 2, \frac{16k^3-5k+1}{\mu_2}\right)$ or $\left(32k^3-8k, 1, \frac{16k^3-5k+1}{\mu_2}\right)$ and $j_3 = \frac{j_1d_3-j_2d_1}{d_2}$ if d_2 divides $j_1d_3-j_2d_1$. If $j_1d_3-j_2d_1$ is not divisible by d_2, we can eliminate the case. Now we test whether the system has a solution modulo various primes. If the system passes all these local tests, we test whether each equation independently has a global solution, i.e. test whether a Pellian equation is solvable. Since the coefficients (and with them the fundamental solutions) in these equations become large, we can not use standard methods (using continued fractions) to check this. By using *compact representations* of quadratic integers, we are able to store the large fundamental solutions of the Pell equation. Compact representations were used for solving systems of Pellian equations for the first time in [15]. These methods and all the tests for determining the local solvability are explained in detail in [20].

We obtain that for $2 \le k \le 10000$ the above system is insoluble except for the case

$$k = 6300, \quad d_1 = 591594589, \quad d_2 = 13556071355339,$$
$$d_3 = 1000187993700, \quad j_1 = 2,\ j_2 = 42611509,\ j_3 = -1859.$$

This case passed all the congruence tests, every equation individually has a solution, but the coefficients are too large to try to get a solution by continued fractions and the regulators of the induced quadratic fields are too large to give any usable bound on the solution. Also, as the right side is not 1 in all three equations it is possible that the equations have more than one class of solutions, which further complicates matters. □

Let us also mention that for the cases $k = 3072$, 3294, 3428, 4176 and 9552, there exist systems that pass all congruence tests, but one of the equations is globally insoluble.

One example of this is the case

$$k = 9552, \quad d_1 = 133211801105681857, \quad d_2 = 9551, \quad d_3 = 6972249617760,$$
$$j_1 = 1, \quad j_2 = 1, \quad j_3 = -13946689232129.$$

We examine the equation $d_3'x^2 - d_2y^2 = 1$, where $d_3' = 435765601110$ is the squarefree part of d_3, and compute a compact representation of the fundamental solution $x_1 + y_1\sqrt{d_3'd_2}$ of the Pell equation $x^2 - d_2d_3'y^2 = 1$. Applying the algorithm from [20] we obtain that $x_1 \equiv 40771521982 \pmod{2d_3'}$, and by [14], Criterion 1, this implies that $d_3'x^2 - d_2y^2 = 1$ has no solutions.

Rank distribution. We used the mwrank ([4]) program to compute the rank and in most cases this was sufficient to find the rank exactly and unconditionally. In the cases where the rank was not computed exactly, the ellrootno() function from PARI/GP ([1]) was also used to determine whether the rank is even or odd. ellrootno() gives a correct output if the Parity conjecture holds (a consequence of the Birch–Swinnerton–Dyer conjecture). Also, the Mestre() function from APECS ([3]) was used to (conditionally) find the upper bound on the rank.

We obtained the following results:

rank	k
2	2,3,6,9,13,15,17*,20*,25,26,27*,28,34,36,42,52,57,59,60,61,62, 63,71,75,79,85,89,97,98
3	4,5,7,10,12,18,19,21,23,24,31,32,35,37,38,39,42,43,45,46,47,49,50,54, 56,58,67,68*,69,70,73,74,76,77,78,83,86,87,92,93,94,95,99,100,101
4	8,11,14,16,23,29,30,41,44*,51,55,65,81,82,90,91,96*
5	33,48,53,72
2 or 4*	40,64,66,80,88
3 or 5*	84

*assuming the Parity conjecture.

It is most likely that the cases where the rank is possibly either 2 or 4 have rank 2 and where the rank is possibly either 3 or 5 have rank 3.

So for the first 100 cases we get (assuming B-S-D) 29–34 curves with rank 2 (the result is most likely 34), 44–45 curves with rank 3 (most likely 45), 17–22 curves of rank 4 (most likely 17) and 4–5 curves of rank 5 (most likely 4).

It is a natural question how often $\mathrm{rank}(E_k(\mathbb{Q})) = 2$. Although we were unable to prove this, we expect $\mathrm{rank}(E_k(\mathbb{Q}(k))) = 2$ and the results for $2 \leq k \leq 101$ also suggest this. If this is true, the Katz–Sarnak conjecture (see [22]) would imply that 50% of the curves have rank 2. Our results on the rank distribution are closer to the experimental results obtained by FERMIGIER ([10]), where 32% of the curves satisfied $\mathrm{rank}(E_k(\mathbb{Q})) = \mathrm{rank}(E(\mathbb{Q}(k)))$.

If k is allowed to be a rational number, then there exists an elliptic curve from this family with rank 9 (see [8]).

3. The family generated by c_3

We examine the elliptic curve

$$E_k : y^2 = ((k-1)x+1)((k+1)x+1)((64k^5 - 48k^3 + 8k)x + 1). \tag{5}$$

We use the variable change

$$y \mapsto \frac{y}{(k-1)(k+1)(64k^5 - 48k^3 + 8k)}, \quad x \mapsto \frac{x}{(k-1)(k+1)(64k^5 - 48k^3 + 8k)},$$

and obtain the curve

$$\begin{aligned} E_k' : y^2 = (x + k^2 - 1)(x + (k-1)(64k^5 - 48k^3 + 8k)) \\ \times (x + (k+1)(64k^5 - 48k^3 + 8k)). \end{aligned} \tag{6}$$

We have three obvious points

$$A = (1 - k^2, 0), \qquad B = (-(k-1)(64k^5 - 48k^3 + 8k), 0),$$
$$C = (-(k+1)(64k^5 - 48k^3 + 8k), 0)$$

of order two. We will prove these are the only points of finite order.

Lemma 7. *$E_k(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_6$.*

Proof. As $\{k-1, k+1, 64k^5 - 48k^3 + 8k\}$ is a Diophantine triple, by ([7], Theorem 2) there are no points of order 4. □

We define

$$P = (0, (k^2 - 1)(64k^5 - 48k^3 + 8k)),$$

$$R = (16(k^2 - 4k^4 + 4k^6), 8k(-1 + 2k^2)(1 - 3k - 4k^2 + 8k^3)(-1 - 3k + 4k^2 + 8k^3))$$

Lemma 8. *$P, P + A, P + B, P + C \notin 2E_k'(\mathbb{Q})$.*

Proof. $x(P) + k^2 - 1 = k^2 - 1$ obviously can not be a square. $(64k^5 - 48k^3 + 7k - 1)^2 < x(P + A) + k^2 - 1 < (64k^5 - 48k^3 + 7k)^2$, so this can not be a square. $x(P + B) + k^2 - 1 < 0$ and $x(P + C) + k^2 - 1 < 0$, so these can not be squares. □

Lemma 9. *$R, R + A, R + B, R + C \notin 2E_k'(\mathbb{Q})$.*

Proof. $(8k^3 - 6k - 1)^2 < x(R + A) + k^2 - 1 < (8k^3 - 6k)^2$ and $(8k^3 - 4k - 1)^2 < x(R) + k^2 - 1 < (8k^3 - 4k)^2$, so can not be squares. $x(R + B) + k^2 - 1 < 0$ and $x(R + C) + k^2 - 1 < 0$, so these can not be squares. □

Lemma 10. *$R + P, R + P + A, R + P + B, R + P + C \notin 2E_k'(\mathbb{Q})$.*

Proof. $\left(\frac{(8k^4 - 8k^2 + 1)}{k}\right)^2 < x(R + P) + k^2 - 1 < \left(\frac{(8k^4 - 8k^2 + 2)}{k}\right)^2$, so this can not be a square. $(8k^3 - 2k - 1)^2 < x(R + P + A) + k^2 - 1 = k^2 - 32k^4 + 64k^6 < (8k^3 - 2k)^2$. $x(R + P + B) + k^2 - 1 < 0$ and $x(R + P + C) + k^2 - 1 < 0$ so $x(R + P + A)$, $x(R + P + B)$ and $x(R + P + C)$ can not be squares. □

Proposition 11. *The rank of E_k' over $\mathbb{Q}$ is greater or equal to two.*

Proof. We note that if $E'_k(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6$, a torsion point T satisfies $T \equiv O, A, B$ or $C \pmod{2E'_k(\mathbb{Q})}$. Having this in mind, using Lemmas 8 to 10, one can prove this proposition along the same lines as Proposition 5. $\square$

Theorem 12. *If* $\operatorname{rank}(E_k(\mathbb{Q})) = 2$ *or* $2 \leq k \leq 10000$, *then all integer points on* E_k *are given by*

$$(x,y) \in \{(0,\pm 1),\ (-4k+16k^3, \pm(-1-2k+4k^2)(-1+2k+4k^2)(1-16k^2+32k^4)),$$

$$(-8k+112k^3-320k^5+256k^7,$$

$$\pm(-1+2k)(1+2k)(-1-6k+8k^3)(1-6k+8k^3)(-1+32k^2-128k^4+128k^6))\}.$$

The x*-coordinates of the non trivial integer points correspond to* c_2 *and* c_4.

Proof. *Case* $\operatorname{rank}(E_k) = 2$

Let $\delta = (k-1)(k+1)(64k^5 - 48k^3 + 8k)$. We follow the proof of Theorem 6. To find integer points on E, all we have to do is find integer solutions to all systems of the form

$$(k-1)x + 1 = \alpha\square,\ (k+1)x + 1 = \beta\square,\ (64k^5 - 48k^3 + 8k)x + 1 = \gamma\square,$$

where for $X_1 = (\delta u, \delta v)$, α, β, γ are defined by $\alpha = (k-1)u+1$, $\beta = (k+1)u+1$, $\gamma = (8k - 48k^3 + 64k^5)u + 1$ if all these are nonzero, and if one is zero then that one is defined as the product of the other two.

So we have to check, as in Theorem 6, the cases

$$X_1 \in S = \{O, A, B, C, P, P+A, P+B, P+C, R, R+A, R+B, R+C,$$
$$P+R, P+R+A, P+R+B, P+R+C\}.$$

1) $X_1 = P$

This case is completely solved in [11] and corresponds to the integer points whose x-coordinates are $-4k+16k^3$ and $-8k+112k^3-320k^5+256k^7$.

2) $X_1 \in \{B, C, P+B, P+C, R+B, R+C, R+P+B, R+P+C\}$.

In these cases, exactly two of the numbers α, β, γ are negative, so the system does not have a solution.

3) $X_1 = P + A$

$$(k-1)x + 1 = (-1-4k+8k^2)(-1-3k+4k^2+8k^3)(1+k)\square,$$

$$(k+1)x + 1 = (-1+4k+8k^2)(1-3k-4k^2+8k^3)(-1+k)\square,$$

$$(64k^5 - 48k^3 + 8k)x + 1 = (-1-4k+8k^2)(-1+4k+8k^2)$$
$$\times (1-3k-4k^2+8k^3)(-1-3k+4k^2+8k^3)(-1+k)(1+k)\square.$$

Suppose $\gcd(((-1-4k+8k^2)(-1-3k+4k^2+8k^3)(1+k))', ((-1+4k+8k^2)(1-3k-4k^2+8k^3)(-1+k))') = d_1 > 1$. This implies that $d_1|(k-1)x+1$ and $d_1|(k+1)x+1$, which implies $d_1|2x$. Since $d_1|x$ would lead to a contradiction, we conclude $d_1 = 2$, meaning that the right sides of the first two equations will be divisible by 2 a odd number of times. On the other hand, $d_1 = 2$ implies that k is odd. But now the left side of the first and second equation are odd, giving a contradiction. So, $d_1 = 1$.

By subtracting the first equation from the third we get $((-1-4k+8k^2)(-1-3k+4k^2+8k^3)(1+k))'$ divides $(-1-4k+8k^2)(-1-3k+4k^2+8k^3)x$. Since $(k+1)'$ would lead to a contradiction, this implies $(k+1)'|(-1-4k+8k^2)(-1-3k+4k^2+8k^3)$. Since $(-1-4k+8k^2)(-1-3k+4k^2+8k^3) = (23-16k+16k^2-64k^3+64k^4)(k+1)-22$, we conclude that $(k+1)' = 1, 2, 11$ or 22.

In the same way we conclude $\gcd(((-1+4k+8k^2)(1-3k-4k^2+8k^3))', (k-1)') = d_3 = (k-1)'$. From $(-1+4k+8k^2)(1-3k-4k^2+8k^3) = (23+16k+16k^2+64k^3+64k^4)(k-1)'+22$, we conclude $(k-1)' = 1, 2, 11$, or 22.

First suppose k is even. $(k-1)' = (k+1)' = 11$ is impossible modulo 11. $(k+1)' = (k-1)' = 1$ is impossible since this would imply that both $k+1$ and $k-1$ are squares. $(k-1)' = 11$, $(k+1)' = 1$ is impossible, since this would imply $\square \equiv 2 \pmod{11}$. So, we conclude $(k-1)' = 1$, $(k+1)' = 11$.

Let $k-1 = x_1^2$, $k+1 = 11x_2^2$. We obtain the equation $x_1^2 - 11x_2^2 = -2$. By [19], Theorem 108, all the solutions of this equation are $x_1 + x_2\sqrt{11} = (3+\sqrt{11})(10+3\sqrt{11})^n$, $n \geq 0$. Let $u_n + v_n\sqrt{11} = (10+3\sqrt{11})^n$. By [18], Theorem 11.1, we have $3|v_n$. Now we have $x_1 + x_2\sqrt{11} = (3+\sqrt{11})(u_n + v_n\sqrt{11}) = 3u_n + 11v_n + \sqrt{11}(u_n + 3v_n)$. We conclude $3|x_1$, which further implies $k \equiv 1 \pmod 9$. From the first equation of the system, we get $1 \equiv 3\square \pmod 9$, a contradiction.

Now suppose k is odd. We note that when k is odd $\gcd((-1+4k+8k^2)(1-3k-4k^2+8k^3), (k-1)) = \gcd(((-1-4k+8k^2)(-1-3k+4k^2+8k^3), (1+k))$ is either 2 or 22. This means that either $(-1+4k+8k^2)(1-3k-4k^2+8k^3)$ or $k-1$ is divisible by 2 once. But examining the second equation, we conclude that the other expression is divisible by 2 an odd number of times (otherwise the left side is odd and the right is even). From this we obtain that $(k-1)'$ has to be even. In the same way we deduce that $(k+1)'$ is even.

$(k-1)' = (k+1)' = 2$ is impossible since it would imply that 2 consecutive squares exist. $(k-1)' = (k+1)' = 22$ is impossible modulo 22. $(k-1)' = 2$, $(k+1)' = 22$ is impossible, since this would imply $\square \equiv 10 \pmod{11}$. We are left with the case $(k-1)'=22$, $(k+1)'=2$. This case leads to the equation $(k-1)^2-11(k+1)^2=-1$, which is not solvable modulo 4.

4) $X_1=R$

$$(k-1)x+1=(-1-3k+4k^2+8k^3)(1+k)(-1+2k)(1+2k)\square,$$

$$(k+1)x+1=(1-3k-4k^2+8k^3)(-1+k)(-1+2k)(1+2k)\square,$$

$$(64k^5-48k^3+8k)x+1=(1-3k-4k^2+8k^3)(-1-3k+4k^2+8k^3)\times(-1+k)(1+k)\square.$$

We first note that $\gcd(4k^2-1,-1-3k+4k^2+8k^3)=\gcd(4k^2-1,1-3k-4k^2+8k^3)=1$. Next we note that $\gcd((4k^2-1)',(k+1)')=1$ or 3 and $\gcd((4k^2-1)',(k-1)')=1$ or 3 (obviously $(k-1)'$ and $(k+1)'$ can not be both divisible by 3). If $3|(k+1)'$ or $3|(k-1)'$, this implies that in the last equation the right side is divisible by 3 an odd number of times, while the right side is congruent to 1 modulo 3 (since 3 does not divide $1-3k-4k^2+8k^3$ and $1-3k-4k^2+8k^3$, while $64k^5-48k^3+8k$ is always divisible by 3). We conclude $\gcd((4k^2-1)',(k+1)')=\gcd((4k^2-1)',(k-1)')=1$.

By subtracting the first equation from the second, we get $(2k+1)'$ divides x, which gives a contradiction if $(2k+1)'>1$. In the same way we get that $(2k-1)'=1$. This implies that $2k+1$ and $2k-1$ are squares, which is impossible.

5) $X_1=R+A$

$$(k-1)x+1=(-1-4k+8k^2)(-1+2k)(1+2k)\square,$$

$$(k+1)x+1=(-1+4k+8k^2)(-1+2k)(1+2k)\square,$$

$$(64k^5-48k^3+8k)x+1=(-1-4k+8k^2)(-1+4k+8k^2)\square.$$

We first note that $\gcd((4k^2-1)',(-1-4k+8k^2)')=1$ or 3 and $\gcd((4k^2-1)',(-1+4k+8k^2)')=1$ or 3 and that both $(-1-4k+8k^2)'$ and $(-1+4k+8k^2)'$ can not be divisible by 3. If one of the above is 3, this implies that the right side of the last equation is divisible by 3 an odd number of times, while the right is to 1 modulo 3. We conclude $\gcd((4k^2-1)',(-1-4k+8k^2)')=\gcd((4k^2-1)',(-1+4k+8k^2)')=1$.

By subtracting the first equation from the second, we get $(2k+1)'$ divides x, which gives a contradiction if $(2k+1)'>1$. In the same way we get that $(2k-1)'=1$. This implies that $2k+1$ and $2k-1$ are both squares, which is impossible.

6) $X_1=R+P$

$$(k-1)x+1=2k(-1-3k+4k^2+8k^3)(-1+2k^2)\square,$$

$$(k+1)x+1=2k(1-3k-4k^2+8k^3)(-1+2k^2)\square,$$

$$(64k^5-48k^3+8k)x+1=(1-3k-4k^2+8k^3)(-1-3k+4k^2+8k^3)\square.$$

If k is even, we get that the right side of the third equation is congruent to 0 or 3 modulo 4, while the left side is congruent to 1 modulo 4.

If k is odd, we note that $\gcd(k', ((-1-3k+4k^2+8k^3)(-1+2k^2))') = \gcd(k', ((1-3k-4k^2+8k^3)(-1+2k^2))') = 1$, so we conclude that $k'|x$, which is a contradiction, unless $k'=1$. We conclude that k is a square. Let $k=y^2$. In the same way we conclude that $2k^2-1$ is a square. We now have the Diophantine equation $2y^4-1=z^2$. The only positive solutions to this equation are $y=1$ and 13 (see [17]). So we have $k=1$ or 169. Since our assumption is $k \geq 2$, we only consider the case $k=169$ and easily see it has no solutions (the right side of the first equation is even, while the left is odd).

7) $X_1 = R+P+A$

$$(k-1)x+1 = 2k(1+k)(-1+2k^2)(-1-4k+8k^2)\square,$$

$$(k+1)x+1 = 2k(-1+4k+8k^2)(-1+k)(-1+2k^2)\square,$$

$$(64k^5-48k^3+8k)x+1 = (-1-4k+8k^2)(-1+4k+8k^2)(-1+k)(1+k)\square.$$

By the same method as in the previous case, we get that k and $2k^2-1$ are both squares, which leads to the equation $2y^4-1=z^2$. Again, we conclude $k=169$. We get that $3|168x+1$, which is impossible.

8) $X_1 = A$

$$\begin{aligned}(k-1)x+1 &= 2k(-1-4k+8k^2)(-1-3k+4k^2+8k^3)(-1+2k)(1+2k)\\ &\quad\times(-1+2k^2)\square,\\ (k+1)x+1 &= 2k(-1+4k+8k^2)(1-3k-4k^2+8k^3)(-1+2k)(1+2k)\\ &\quad\times(-1+2k^2)\square,\\ (64k^5-48k^3+8k)x+1 &= (-1-4k+8k^2)(-1+4k+8k^2)\\ &\quad\times(1-3k-4k^2+8k^3)(-1-3k+4k^2+8k^3)\square.\end{aligned}$$

This case is analogous to the previous. We conclude that $k=169$, implying $3|168x+1$, a contradiction.

9) $X_1 = O$

$$(k-1)x+1 = 2k(k+1)(-1+2k)(1+2k)(-1+2k^2)\square,$$

$$(k+1)x+1 = 2k(k-1)(-1+2k)(1+2k)(-1+2k^2)\square,$$

$$(64k^5-48k^3+8k)x+1 = (k+1)(k-1)\square.$$

This case is analogous to the previous three.

Case $2 \leq k \leq 10000$

We will prove that the mentioned integer points are the only ones without any conditions on the rank, for $2 \leq k \leq 10000$. Assume (x,y) is an integer point on the elliptic curve E_k. This implies

$$(k-1)x+1=\mu_2\mu_3x_1^2, \qquad (k+1)x+1=\mu_1\mu_3x_2^2,$$
$$(64k^5-48k^3+8k)x+1=\mu_1\mu_2x_3^2,$$

where $\mu_1|64k^5-48k^3+7k-1$, $\mu_2|64k^5-48k^3+7k+1$, $\mu_3|2$. By eliminating x we obtain

$$d_1x_1^2-d_2x_2^2=j_1, \qquad d_3x_1^2-d_2x_3^2=j_2, \qquad d_1x_3^2-d_3x_2^2=j_3, \tag{7}$$

where $d_1=(k+1)\mu_2$, μ_2 is a square-free factor of $64k^5-48k^3+7k+1$, $d_2=(k-1)\mu_1$, μ_1 is a square-free factor of $64k^5-48k^3+7k-1$, $(d_3,j_1,j_2)=\big(64k^5-48k^3+8k, 2, \frac{64k^5-48k^3+7k+1}{\mu_2}\big)$ or $\big(2(64k^5-48k^3+8k), 1, \frac{64k^5-48k^3+7k+1}{\mu_2}\big)$ and $j_3=\frac{j_1d_3-j_2d_1}{d_2}$ if d_2 divides $j_1d_3-j_2d_1$. If $j_1d_3-j_2d_1$ is not divisible by d_2, we can eliminate the case. Again, using tests described in [20] we obtain that for $2\le k\le 10000$ the above system is insoluble. All the systems were locally unsolvable, so there was no need to test for global solutions. □

Rank distribution. We used the mwrank ([4]) program to compute the rank and in most cases this was sufficient to find the rank exactly and unconditionally. In the cases where the rank was not computed exactly, the ellrootno() function from PARI/GP ([1]) was also used to determine whether the rank is even or odd. ellrootno() gives a correct output if the Parity conjecture holds (a consequence of the Birch-Swinnerton-Dyer conjecture).
Also, the Mestre() function from APECS ([3]) was used to (conditionally) find the upper bound on the rank.

rank	k
2	4,6,8,9,15,25,27,46
3	2,3,5,13,14,16,19,21,28*, 32*, 34*, 35, 36, 37, 39*, 42, 43*44, 47, 50
4	10,29,30,31,33,41,
5	7,11,12,23,38
2 or 4*	17,18,24,40,45,48,49
3 or 5*	20,22,26,51

*assuming the Parity conjecture

We were only able to efficiently compute the rank up to $k\le 50$, since for larger k, mwrank could in most cases only compute bounds on the rank. We obtained less curves of rank 2 for this family or curves than for the previous one, 8–15 of them (again the actual number is likely to be closer to 15). Again the results are closer to the experimental results of Fermigier, than to those predicted by the Katz-Sarnak conjecture.

ACKNOWLEDGEMENT. We would like to thank Professor ANDREJ DUJELLA for many valuable suggestions and his generous help with the preparation of this manuscript. We would also like to thank the referees for very detailed comments and many helpful suggestions.

References

[1] C. BATUT, D. BERNARDI, H. COHEN and M. OLIVIER, GP/PARI, 1994.

[2] Y. BUGEAUD, A. DUJELLA and M. MIGNOTTE, On the family of Diophantine triples $\{k-1, k+1, 16k^3-4k\}$, *Glasgow Math. J.* **49** (2007), 333–344.

[3] I. CONELL, APECS, `ftp://ftp.math.mcgill.ca/pub/apecs/`.

[4] J. CREMONA, Algorithms for Modular Elliptic Curves, *Cambridge University Press Cambridge*, 1997.

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

[6] A. DUJELLA, A parametric family of elliptic curves, *Acta Arith.* **94** (2000), 87–101.

[7] A. DUJELLA, Diophantine m-tuples and elliptic curves, *J. Theor. Nombres Bordeaux* **13** (2001), 111–124.

[8] A. DUJELLA, On Mordell-Weil groups of elliptic curves induced by Diophantine triples, *Glas. Mat. Ser. III* **42** (2007), 3–18.

[9] A. DUJELLA and A. PETHŐ, Integer points on a family of elliptic curves, *Publ. Math. Debrecen* **56** (2000), 321–335.

[10] S. FERMIGIER, Etude experimentale du rang de familles de courbes elliptiques sur $\mathbb{Q}$, *Experimental Math.* **5** (1996), 119–130.

[11] Y. FUJITA, The extensibility of Diophantine pairs $\{k-1, k+1\}$, *J. Number Theory* **128** (2008), 322–353.

[12] Y. FUJITA, The $D(1)$-extensions of $D(-1)$-triples $\{1, 2, c\}$ and integer points on the attached elliptic curves, *Acta Arith.* **128** (2007), 349–375.

[13] Y. FUJITA, The Hoggatt-Bergum conjecture on $D(-1)$-triples $\{F_{2k+1}, F_{2k+3}, F_{2k+5}\}$ and integer points on the attached elliptic curves (*to appear in* Rocky Mountain J. Math.).

[14] A. GRELAK and A. GRYTZCUK, On the Diophantine equation $ax^2 - by^2 = c$, *Publ. Math. Debrecen* **44** (1994), 291–299.

[15] M. J. JACOBSON, JR. and H. C. WILLIAMS, Modular arithmetic on elements of small norm in quadratic fields, *Designs, Codes and Cryptography* **27** (2002), 93–110.

[16] A. KNAPP, Elliptic Curves, *Princeton Univ. Press*, 1992.

[17] W. LJUNGGREN, Zur Theorie der Gleichung $x^2 + 1 = Dy^4$, *Avh. Norsk. Vid. Akad. Oslo* (1942), 1–27.

[18] 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).

[19] T. NAGELL, Introduction on Number Theory, *Wiley*, 1951.

[20] F. Najman, Compact representation of quadratic integers and integer points on some elliptic curves (*to appear in* Rocky Mountain J. Math.).

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

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

[23] J. H. Silverman, The Arithmetic of Elliptic Curves, *Springer-Verlag*, 1986.

FILIP NAJMAN
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ZAGREB
BIJENIČKA CESTA 30
10000 ZAGREB
CROATIA

E-mail: fnajman@math.hr

(Received September 26, 2008; revised March 9, 2009)