Journal de Théorie des Nombres
de Bordeaux **13** (2001), 111–124

Diophantine m-tuples and elliptic curves

par Andrej DUJELLA

Résumé. Un m-uplet diophantien est un ensemble de m entiers naturels non nuls tel que le produit quelconque de deux d'entre eux augmenté de 1 est un carré parfait. Dans cet article, nous nous intéressons à certaines propriétés de courbes elliptiques d'équation du type $y^2 = (ax+1)(bx+1)(cx+1)$, où $\{a,b,c\}$ est un triplet diophantien.

Nous considérons en particulier la courbe elliptique E_k définie par l'équation $y^2 = (F_{2k}x+1)(F_{2k+2}x+1)(F_{2k+4}x+1)$, où $k \geq 2$ et F_n désigne le n-ème nombre de Fibonacci. Nous montrons que si le rang de E_k est égal à 1, ou si $k \leq 50$, alors les points entiers sur E_k sont donnés par

$$(x,y) \in \big\{(0,\pm 1),\ (4F_{2k+1}F_{2k+2}F_{2k+3}, \pm(2F_{2k+1}F_{2k+2}-1) \times (2F_{2k+2}^2+1)(2F_{2k+2}F_{2k+3}+1))\big\}.$$

Abstract. A Diophantine m-tuple is a set of m positive integers such that the product of any two of them is one less than a perfect square. In this paper we study some properties of elliptic curves of the form $y^2 = (ax+1)(bx+1)(cx+1)$, where $\{a,b,c\}$ is a Diophantine triple.

In particular, we consider the elliptic curve E_k defined by the equation $y^2 = (F_{2k}x+1)(F_{2k+2}x+1)(F_{2k+4}x+1)$, where $k \geq 2$ and F_n denotes the n-th Fibonacci number. We prove that if the rank of $E_k(\mathbf{Q})$ is equal to one, or $k \leq 50$, then all integer points on E_k are given by

$$(x,y) \in \big\{(0,\pm 1),\ (4F_{2k+1}F_{2k+2}F_{2k+3}, \pm(2F_{2k+1}F_{2k+2}-1) \times (2F_{2k+2}^2+1)(2F_{2k+2}F_{2k+3}+1))\big\}.$$

1. Introduction

Diophantus found four positive rational numbers $\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}$ with the property that the product of any two of them increased by 1 is a perfect square. The first set of four positive integers with the above property was

Manuscrit reçu le 8 octobre 1999.

found by Fermat and that set was $\{1,3,8,120\}$ (see [6, 7]). These two examples motivate the following definition.

Definition 1. A set $\{a_1, a_2, \ldots, a_m\}$ of m positive integers (rationals) is called *a (rational) Diophantine m-tuple* if $a_i \cdot a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$.

The famous conjecture is that there does not exist a Diophantine quintuple. There is a stronger version of this conjecture. Let $\{a,b,c\}$ be a Diophantine triple, *i.e.*

$$ab+1=r^2, \quad ac+1=s^2, \quad bc+1=t^2, \quad r,\, s,\, t \in \mathbf{N}.$$

Define

$$d_+ = a+b+c+2abc+2rst, \qquad d_- = a+b+c+2abc-2rst. \tag{1}$$

Then it is easy to verify (see [1]) that $\{a,b,c,d_+\}$ and $\{a,b,c,d_-\}$ are Diophantine quadruples.

Conjecture 1. *If $\{a,b,c,d\}$ is a Diophantine quadruple, then $d=d_+$ or $d=d_-$.*

Remark 1. We have

$$\begin{aligned} d_+ \cdot d_- &= (a+b+c+2abc)^2 - 4(ab+1)(ac+1)(bc+1) \\ &= a^2+b^2+c^2-2ab-2ac-2bc-4. \end{aligned} \tag{2}$$

Assume that $a<b<c$. Then (2) implies $d_+d_- < c^2$ and $d_- < c$. Therefore the validity of Conjecture 1 would imply that there does not exist a Diophantine quintuple.

Remark 2. It is possible that $d_- = 0$. By (2), this is equivalent to

$$(c-a-b)^2 = 4ab+4 = 4r^2.$$

Hence we proved that $d_- = 0$ iff $c = a+b+2r$. According to [18], we may say that $d_- = 0$ iff c is the smallest positive integer greater than b such that $\{a,b,c\}$ is a Diophantine triple.

Conjecture 1 was verified for the triple $\{1,3,8\}$ by Baker and Davenport [2], for the triple $\{2,4,12\}$ by Veluppillai [27] and for the triples $\{1,3,120\}$, $\{1,8,120\}$, $\{1,8,15\}$, $\{1,15,35\}$ and $\{1,24,35\}$ by Kedlaya [19]. We verified Conjecture 1 for the parametric families of triples $\{k-1,k+1,4k\}$, $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$ and $\{1,3,c_k\}$ (see [9, 10] and a joint paper with Attila Pethő [13]). Here F_n denotes n^{th} Fibonacci number, and the sequence (c_k) is defined by $c_1=8$, $c_2=120$, $c_{k+2}=14c_{k+1}-c_k+8$, $k \in \mathbf{N}$.

However, Conjecture 1 is still unproved and as far as we know the best general result is our recent result that there does not exist a Diophantine 9-tuple [12].

Let $\{a, b, c\}$ be a (rational) Diophantine triple. In order to extend this triple to a quadruple, we have to solve the system

$$ax + 1 = \square, \qquad bx + 1 = \square, \qquad cx + 1 = \square. \tag{3}$$

It is natural idea to assign to the system (3) the elliptic curve

$$E: \qquad y^2 = (ax + 1)(bx + 1)(cx + 1). \tag{4}$$

The purpose of this paper is to study properties of elliptic curves obtained in this manner and to study connections between solutions of the system (3) and the equation (4).

Let us mention that the system (3) where a, b, c are arbitrary integers (rationals) is called *Fermat's triple equation*, and in that general case some connections between (3) and (4) were studied in [15, 25, 28].

2. Obvious points on E

The coordinate transformation

$$x \mapsto \frac{x}{abc}, \quad y \mapsto \frac{y}{abc}$$

applied on the curve E leads to the elliptic curve

$$E': \qquad y^2 = (x + bc)(x + ac)(x + ab).$$

There are three rational points on E of order 2:

$$A = (-\frac{1}{a}, 0), \quad B = (-\frac{1}{b}, 0), \quad C = (-\frac{1}{c}, 0),$$

and also other obvious rational points

$$P = (0, 1), \quad S = \Big(\frac{1}{abc}, \frac{rst}{abc}\Big).$$

It is not so obvious, but it is easy to verify that $S \in 2E(\mathbf{Q})$. Namely, $S = 2R$, where

$$R = \Big(\frac{rs + rt + st + 1}{abc}, \frac{(r + s)(r + t)(s + t)}{abc}\Big) \in E(\mathbf{Q}).$$

It is clear that every rational point on (3) induce a rational point on E. Thus, the question is which rational points on E induce a rational solution of (3). The answer is given in the following proposition.

Proposition 1. *The x-coordinate of the point $T \in E(\mathbf{Q})$ satisfies (3) iff $T - P \in 2E(\mathbf{Q})$.*

Proof. For $X = (x, y) \in E(\mathbf{Q})$ we denote by $X' = (xabc, yabc) \in E'(\mathbf{Q})$. By [20, 4.6, p.89], the function $\varphi_a : E'(\mathbf{Q}) \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ defined by

$$\varphi_a(X') = \begin{cases} (x + bc)\mathbf{Q}^{*2} & \text{if } X' = (x, y) \neq \mathcal{O}, A' \\ (ac - bc)(ab - bc)\mathbf{Q}^{*2} & \text{if } X = A' \\ \mathbf{Q}^{*2} & \text{if } X = \mathcal{O} \end{cases}$$

is a group homomorphism. The same is also valid for the analogously defined functions φ_b and φ_c. We have $\varphi_a(P') = bc\mathbf{Q}^{*2}$, $\varphi_b(P') = ac\mathbf{Q}^{*2}$, $\varphi_c(P') = ab\mathbf{Q}^{*2}$. Now, $x(T)$ satisfies (3) iff

$$\varphi_a(T') = \varphi_a(P'), \quad \varphi_b(T') = \varphi_b(P'), \quad \varphi_c(T') = \varphi_c(P'),$$

and this is equivalent to

$$\varphi_a(T' - P') = \varphi_b(T' - P') = \varphi_c(T' - P') = \mathbf{Q}^{*2}.$$

By the 2-descent Proposition (see [17, 4.1, p.37], [20, 4.2, p.85]), this is equivalent to $T' - P' \in 2E'(\mathbf{Q})$. □

By Proposition 1 and the relation $S = 2R$ it follows that the numbers $x(P + S)$ and $x(P - S)$ satisfy the system (3). It is easy to check that $x(P + S) = d_-$ and $x(P - S) = d_+$, where d_+ and d_- are defined by (1).

The addition and subtraction of point S has another interesting property.

Theorem 1. *If x-coordinate of the point $T = (x, y) \in E(\mathbf{Q})$ satisfies (3), then for the points $T \pm S = (u, v)$ it holds that $x \cdot u + 1$ is a square.*

Proof. Direct computation shows that $x(T \pm S)$ are exactly the numbers x_5^- and x_5^+, obtained from [8, Theorem 1] applied to $(x_1, x_2, x_3, x_4) = (a, b, c, x)$. Since $x_4x_5^+ + 1$ and $x_4x_5^- + 1$ are perfect squares, the proof is finished. □

Corollary 1. *Every Diophantine quadruple $\{a, b, c, d\}$ can be extended to a* rational *Diophantine quintuple $\{a, b, c, d, e\}$.*

Note that by [8, Corollary 1], if e in Corollary 1 is obtained by construction from Theorem 1, then $e < 1$, and therefore e is not a positive integer.

3. Torsion group and rank of E

In this section we assume that a, b, c are positive integers and $a < b < c$.

Lemma 1. A', B', $C' \notin 2E'(\mathbf{Q})$

Proof. If $A' \in 2E'(\mathbf{Q})$, then 2-descent Proposition implies that $c(a - b)$ is a square. But $c(a - b) < 0$, a contradiction. Similarly $B' \notin 2E'(\mathbf{Q})$.

If $C' \in 2E'(\mathbf{Q})$, then

$$a(c - b) = \square, \qquad b(c - a) = \square. \tag{5}$$

Let

$$\begin{aligned} ac - ab &= s^2 - r^2 = (s - \alpha)^2, \\ bc - ab &= t^2 - r^2 = (t - \beta)^2, \end{aligned}$$

where $0 < \alpha < s$, $0 < \beta < t$. Then we have

$$r^2 = 2s\alpha - \alpha^2 = 2t\beta - \beta^2. \tag{6}$$

From (6) we have

$$4(bc+1)\beta^2 = (ab+1+\beta^2)$$

and

$$(\beta^2-1)^2 = b[4c - a^2b - 2a(1+\beta^2)]. \tag{7}$$

From (7) we conclude that $c > \frac{a^2b}{4}$ and furthermore either $\beta = 1$ or $\beta^2 - 1 \geq \sqrt{b}$.

If $\beta^2 - 1 \geq \sqrt{b}$, then $\beta > \sqrt[4]{b}$, and if we put this in (6), we obtain

$$\begin{aligned} ab = t^2 - (t-\beta)^2 - 1 > 2t\sqrt[4]{b} - \sqrt{b} - 1 > 2\sqrt{bc}\sqrt[4]{b} - \sqrt{b} - 1 \\ > ab\sqrt[4]{b} - \sqrt{b} - 1, \end{aligned}$$

which implies $ab < \sqrt[4]{b} + 1$, a contradiction.

If $\beta = 1$, then from (7) we find that

$$c = \frac{a^2b + 4a}{4}. \tag{8}$$

Now we have

$$s^2 = ac + 1 = \frac{1}{4}(a^3b + 4a^2 + 4) = \frac{1}{4}(a^2r^2 + 3a^2 + 4).$$

Hence $s^2 > \left(\frac{ar}{2}\right)^2$ and $s^2 < \left(\frac{ar+2}{2}\right)^2$. Therefore $s^2 = \left(\frac{ar+1}{2}\right)^2$ which is equivalent to

$$2ar = 3a^2 + 3. \tag{9}$$

It is obvious that (9) implies $a \in \{1, 3\}$. For $a = 1$ we find from (9) and (8) that $b = 8$ and $c = 3 < b$. For $a = 3$ we find $b = 8$ and $c = 21$, and this does not satisfy the first equation in (5). □

Theorem 2. $E'(\mathbf{Q})_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ *or* $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$

Proof. The statement follows directly from Lemma 1 and the theorem of Mazur [21]. □

Remark 3. In [11] it is proved that for the triples of the form $\{k-1, k+1, 4k\}$ it holds $E'(\mathbf{Q})_{\text{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. In [14] the same result is proved for the triples $\{1, 3, c_k\}$, where c_k is defined in the introduction.

Theorem 3. $\operatorname{rank} E(\mathbf{Q}) \geq 1$

Proof. It suffices to prove that the point S' on $E'(\mathbf{Q})$ has an infinite order. Assume that S' has finite order. Then $S'+A'$ has finite order too, and by Lutz-Nagell Theorem [20, 1.6, p.15], the coordinates of $S'+A'$ are integers. The first coordinate of $S'+A'$ is

$$\left(\frac{rst}{t^2}\right)^2 - ab - ac + 1.$$

If this number is an integer, then

$$\frac{r^2s^2}{t^2} = \frac{a^2bc+ab+ac+1}{bc+1} = a^2 + \frac{ab+ac+1-a^2}{bc+1}$$

is also an integer, and hence $ab+ac+1-a^2 \geq bc+1$. But this implies $(b-a)(c-a) \leq 0$, a contradiction. $\square$

Remark 4. In general, we may expect that the points P and S are two independent points of infinite orders, and therefore that $\operatorname{rank} E(\mathbf{Q}) \geq 2$. This is checked for the triples $\{1,3,c_k\}$, $k \geq 2$, in [14]. However, if c is smallest possible, *i.e.* $c = a+b+2r$, then the direct computation shows that $2P = -S$.

4. Integer points on E

Let $\{a,b,c\}$ be a Diophantine triple. We would like to find all integer points on the elliptic curve

$$E: \quad y^2 = (ax+1)(bx+1)(cx+1).$$

We have always the following integer points:

$$(0,\pm 1), \quad (d_+, \pm(at+rs)(bs+rt)(cr+st)),$$
$$(d_-, \pm(at-rs)(bs-rt)(cr-st)),$$

and also $(-1,0)$ if $1 \in \{a,b,c\}$. The question is whether there is any other integer point on E. We don't know any counterexample to the conjecture that there are no other points on E. However, we can prove this conjecture only in very special cases. First of all, in these cases we have to prove Conjecture 1.

If we can prove Conjecture 1 for the triple $\{a,b,c\}$, then we may try to prove that in that case there are no other integer points on E apart from seven points listed above. However, we are able to do this only under the assumption that the rank is "the smallest possible".

More precisely, we proved in [11] that if $\operatorname{rank} E_k(\mathbf{Q}) = 1$, where

$$E_k: \quad y^2 = ((k-1)x+1)((k+1)x+1)(4kx+1), \tag{10}$$

then all integer points on E_k are given by

$$(x,y) \in \{(0,\pm 1),\ (16k^3-4k, \pm(128k^6-112k^4-20k^2-1))\}. \tag{11}$$

We also verified this statement for all $3 \le k \le 1000$. The condition $\operatorname{rank} E_k(\mathbf{Q}) = 1$ is not unrealistic since the generic rank of (10), *i.e.* $\operatorname{rank} E(\mathbf{Q}(k))$, is equal to 1. In the range $2 \le k \le 100$ we obtained (using MWRANK [5] and SIMATH [26]) the following distribution of ranks: 41 cases of rank 1, 49 cases of rank 2 and 9 cases of rank 3.

If $k = k_1(n) = 3n^2 + 2n - 2$, $n \in \mathbf{Z} \setminus \{-1, 0, 1\}$, or $k = k_2(m) = \frac{1}{2}(3m^2 + 5m)$, $m \in \mathbf{Z} \setminus \{-2, -1, 0\}$, then $\operatorname{rank} E_k(\mathbf{Q}) \ge 2$ and we proved that if in these cases $\operatorname{rank} E_k(\mathbf{Q}) = 2$, then all integer points on E_k are given by (11). Here for the generic ranks it holds $\operatorname{rank} E(\mathbf{Q}(n)) = \operatorname{rank} E(\mathbf{Q}(m)) = 2$. Finally, we considered the intersection of the families $E_{k_1(n)}$ and $E_{k_2(m)}$. We proved that if $k = \frac{1}{24}(t_i^2 - 25)$, where

$$t_0 = 1, \ t_1 = 19, \quad t_{i+2} = 6t_{i+1} - t_i, \quad i \in \mathbf{Z},$$

then $\operatorname{rank} E_k(\mathbf{Q}) \ge 3$ for $i \ne -1, 0$, and if $\operatorname{rank} E_k(\mathbf{Q}) = 3$, then again all integer points on E_k are given by (11).

In the joint paper with Attila Pethő [14] we considered the family

$$C_k : \quad y^2 = (x+1)(3x+1)(c_k x + 1),$$

where c_k is defined in the introduction. Here $\operatorname{rank} C_k(\mathbf{Q}) \ge 2$ for $k \ge 2$. Let $c_k + 1 = s_k^2$ and $3c_k + 1 = t_k^2$. We proved that if $\operatorname{rank} C_k(\mathbf{Q}) = 2$, then all integer points on C_k are given by

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

We also verified this statement for $k \le 40$, with possible exceptions $k = 23$ and $k = 37$.

Lemma 2. *Let $\{a,b,c\}$, $a < b < c$, be a Diophantine triple. Then P, $P + A$, $P + B \notin 2E(\mathbf{Q})$. Furthermore, $P + C \notin 2E(\mathbf{Q})$ unless $c = a + b + 2r$ and c, $c - a$ and $c - b$ are all twice a square.*

Proof. If $P \in 2E(\mathbf{Q})$, then the 2-descent Proposition implies that ab is a square, which is in a contradiction with $ab + 1 = r^2$. Since $a(a-b) < 0$ and $b(b-c) < 0$, the 2-descent Proposition implies $P + A$, $P + B \notin 2E(\mathbf{Q})$.

Assume that $P + C \in 2E(\mathbf{Q})$. Then by the 2-descent Proposition we have

$$c(c-a) = \square, \qquad c(c-b) = \square. \tag{12}$$

Let $c^2 - ac = (c-e)^2$, where $0 < e < c$. From $e^2 = c(2e - a)$ we conclude that $e \ge \sqrt{c}$. This implies $2\sqrt{c} \le a + 1$ and $c \le a^2 < ab$. By [18], $c < 4ab$ implies $c = a + b + 2r$. Then $t = b + r$ and $a = b + c - 2t$. Now system (12) becomes

$$c(2t - b) = \square, \qquad c(c-b) = \square.$$

Assume c, $2t-b$ and $c-b$ are all a square multiplied by δ. Then $c \equiv b \equiv 2t \equiv 0 \pmod{\delta}$ and from $2bc+2=2t^2$ we find that $\delta=1$ or $\delta=2$.

Assume that $\delta=1$. Then $c=\alpha^2$, $c-b=\beta^2$, $2t-b=\gamma^2$. If α is even and β is odd, then we have $c \equiv 0 \pmod 4$, $b \equiv 3 \pmod 4$ and $\gamma^2 \equiv 3 \pmod 4$, a contradiction. If α is odd and β is even, then we have $b \equiv c \equiv 1 \pmod 4$ and $t^2 \equiv 2 \pmod 4$, a contradiction. Finally, if α and β are odd, then we have $c \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$ and $\gamma^2 \equiv 2 \pmod 4$, a contradiction.

Therefore $\delta=2$ and c, $c-a$ and $c-b$ are all twice a square. $\square$

Theorem 4. *Let $ab+1=r^2$ and $c=a+b+2r$. Assume that among the numbers a, $2a$, b, $2b$, c, $2c$ there are no perfect squares. If* $\operatorname{rank} E(\mathbf{Q})=1$, *then all integer points (x,y) on E satisfy the system*

$$ax+1=\square, \quad bx+1=\square, \quad cx+1=\square.$$

Proof. Let $E'(\mathbf{Q})/E'(\mathbf{Q})_{\mathrm{tors}} = <U>$. If $X \in E'(\mathbf{Q})$, then we can represent X in the form $X=mU+T$, where $m \in \mathbf{Z}$ and $T \in E'(\mathbf{Q})_{\mathrm{tors}}$. We have also $P'=nU+T_1$ for an integer m_P and a torsion point T_1. Since $E'(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$, we have $T_1 \equiv \mathcal{O}$, A', B' or C' $(\bmod\ 2E'(\mathbf{Q}))$. Now Lemma 2 implies that n is odd. Therefore we have $X \equiv X_1 \,(\bmod\ 2E'(\mathbf{Q}))$, where

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

Since the functions φ_a, φ_b, φ_c defined in the proof of Proposition 1 are homomorphisms, in order to find all integer points on E, it suffices to solve in integers all systems of the form

$$ax+1=\alpha\square, \quad bx+1=\beta\square, \quad cx+1=\gamma\square \tag{13}$$

where for $X_1=(abcu, abcv) \in \mathcal{S}$, the numbers α,β,γ are defined by $\alpha=au+1$, $\beta=bu+1$, $\gamma=cu+1$ if all of these three expressions are nonzero, and if e.g. $au+1=0$ then we define $\alpha=\beta\gamma$. Here $\square$ denotes a square of a rational number.

Since for $X_1=P'$ the system (13) is equivalent to system (3), we have to prove that for $X_1 \in \mathcal{S} \setminus \{P'\}$, the system (13) has no integer solutions.

For $X_1 \in \{A',\, B',\, P'+A',\, P'+B'\}$ exactly two among the numbers α,β,γ are negative and therefore the system (13) has no integer solution. Let e' denote the square-free part of an integer e and let $e''=\min\{|e'|, |2e|'\}$.

If $X_1=\mathcal{O}$, then the system (13) becomes

$$ax+1=bc\square, \quad bx+1=ac\square, \quad cx+1=ab\square.$$

First we will prove that $\gcd(a',b')=1$ or 2. Assume that a prime p divides a' and b'. Then from $ax+1=bc\square$ we conclude that $p|c'$, and from $c=a+b+2r$ that $p|2r$. Now from $2ab+2=2r^2$ it follows that $p=2$. Analogously we can prove that $\gcd(a',c')=1$ or 2 and $\gcd(b',c')=1$ or 2.

Since a'' divides $bx+1$ and $cx+1$, we conclude that a'' divides $c-b = a+2r$. Therefore $a''|2r$. Analogously we find that $b''|2r$ and $c''|2s$. But now the relations $2ab+2 = 2r^2$ and $2ac+2 = 2s^2$ imply $a'', b'', c'' \in \{1,2\}$. Thus at least one of the numbers ab, ac and bc is a perfect square, a contradiction.

If $X_1 = C'$, then the system (13) becomes

$$ax+1 = c(c-a)\Box, \quad bx+1 = c(c-b)\Box, \quad cx+1 = (c-a)(c-b)\Box.$$

Assume that $p|c'$ and $p|(c-a)'$. Then from $cx+1 = (c-a)(c-b)\Box$ we conclude that $p|(c-b)'$. Hence we have $p|a,b,c$ and therefore $p|2r$ and we obtain that $p=2$, as before. Hence we proved that $\gcd(c',(c-a)') = 1$ or 2, and in the same manner we can prove that $\gcd(c'(c-b)') = 1$ or 2 and $\gcd((c-a)',(c-b)') = 1$ or 2. Since c'' divides $b-a = c-2s$ we find as above that c is either a square or twice a square.

If $X_1 = P' + C'$, then the system (13) becomes

$$ax+1 = b(c-a)\Box, \quad bx+1 = a(c-b)\Box, \quad cx+1 = ab(c-a)(c-b)\Box.$$

As before we can prove that $\gcd(a',(c-b)')$, $\gcd(a',(c-a)')$, $\gcd(a',b') = 1$ or 2, and since a'' divides $c-b$ we conclude that a is either a square or twice a square. Similarly we can prove that b is either a square or twice a square. $\Box$

5. On the Hoggatt-Bergum conjecture

In 1977, Hoggatt and Begum [16] proved that for $k \geq 1$ the set

$$\{F_{2k},\, F_{2k+2},\, F_{2k+4},\, 4F_{2k+1}F_{2k+2}F_{2k+3}\}$$

is a Diophantine quadruple. They conjectured that the fourth number $4F_{2k+1}F_{2k+2}F_{2k+3}$ with the above property is unique. This is a special case of Conjecture 1. We proved the Hoggatt-Bergum conjecture in [10]. We will give a sketch of the proof.

Eliminating d from the system

$$F_{2k}d+1 = x_1^2, \quad F_{2k+2}d+1 = x_2^2, \quad F_{2k+4}d+1 = x_3^2 \tag{14}$$

we obtain the system of Pellian equations

$$\begin{aligned} F_{2k}x_2^2 - F_{2k+2}x_1^2 &= -F_{2k+1}\,, \\ F_{2k}x_3^2 - F_{2k+4}x_1^2 &= F_{2k} - F_{2k+4}\,. \end{aligned}$$

We reformulate our problem to the problem of finding the intersection of two binary recurrence sequences. We then transform the exponential equation into an inequality for linear forms in three logarithms of algebraic numbers. A comparison of the theorem of Baker and Wüstholz [3] with the lower bound for the solutions obtained for the congruence condition modulo $2F_{2k}F_{2k+2}$ finishes the proof for $k \geq 49$. We prove the statement for $k \leq 48$ by a version of the reduction procedure due to Baker and Davenport [2].

Since we can solve the system (14) completely, we may try to find all integer points on the elliptic curve

$$(15) \qquad E_k: \quad y^2 = (F_{2k}x+1)(F_{2k+2}x+1)(F_{2k+4}x+1).$$

Theorem 5. $E_k(\mathbf{Q})_{\rm tors} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Proof. By Theorem 2, it suffices to prove $E_k(\mathbf{Q})_{\rm tors} \not\simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$. Assume $E_k(\mathbf{Q})_{\rm tors} \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$. By a theorem of Ono [24], this implies that there exist integers α and β such that $\frac{\alpha}{\beta} \notin \{-2,-1,-\frac{1}{2},0,1\}$ and

$$(16)\, F_{2k}F_{2k+3} = \alpha^4 + 2\alpha^3\beta, \qquad F_{2k+2}(F_{2k+4}-F_{2k}) = 2\alpha\beta^3+\beta^4.$$

Adding the two expressions in (16) we obtain

$$(17) \qquad F_{2k+2}F_{2k+4} + F_{2k}F_{2k+1} = (\alpha^2+\alpha\beta+\beta^2)^2 - 3\alpha^2\beta^2.$$

The sequence $(F_{2k+2}F_{2k+4} + F_{2k}F_{2k+1})_{k\geq 1}$ is periodic with period equal 3: $(2,7,3,2,7,3,\dots)$. Therefore, the left hand side of (17) is congruent to 2, 3 or 7 modulo 8. Since the right hand side of (17) is congruent to 0, 1, 5 or 6 modulo 8, we obtain a contradiction. □

Theorem 6. *Let $k \geq 2$ be an integer. If* $\operatorname{rank} E_k(\mathbf{Q}) = 1$, *then all integer points on E_k are given by*

$$(18) \quad (x,y) \in \Big\{(0,\pm 1),\, \big(4F_{2k+1}F_{2k+2}F_{2k+3}, \pm(2F_{2k+1}F_{2k+2}-1) \\ \times (2F_{2k+2}^2+1)(2F_{2k+2}F_{2k+3}+1)\big)\Big\}.$$

Proof. The statement follows directly from [10, Theorem 2] and Theorem 4, unless at least one of the numbers F_{2k}, F_{2k+2}, F_{2k+4} is a square or twice a square. By [4], this is the case iff $2 \leq k \leq 6$.

However, from the proof of Theorem 4 it follows that if F_{2k+4} is neither a square nor twice a square, then we should have that F_{2k} and F_{2k+2} are both either a square or twice a square. This observation eliminates all cases except $k=4$.

If $k=4$, we have to solve the system (13) for $X_1 = C'$. In this case the system (13) becomes

$$(19) \qquad 21x+1 = 123\square, \quad 55x+1 = 89\square, \quad 144x+1 = 123\cdot 89\square,$$

where $\square$ denotes a square of a rational number. But the first equation in (19) is clearly impossible modulo 3. □

In the following table we list the values of rank $(E_k(\mathbf{Q}))$ which we were able to compute using John Cremona's program MWRANK [5]:

k	1	2	3	4	5	6	7	8	9	12	16	17
rank $(E_k(\mathbf{Q}))$	1	1	2	2	3	1	3	2	3	1	1	2

Theorem 7. *If $2 \le k \le 50$, then all integer points on E_k are given by (18).*

Proof. We will use the approach introduced in our joint paper with Attila Pethő [14].

Assume that (x, y) is an integer solution of (15). Then there exist integers x_1, x_2, x_3 such that

$$\begin{aligned} F_{2k}x + 1 &= D_2 D_3 x_1^2 \\ F_{2k+2}x + 1 &= D_1 D_3 x_2^2 \\ F_{2k+4}x + 1 &= D_1 D_2 x_3^2, \end{aligned}$$

where $D_1 | F_{2k+3}$, $D_2 | F_{2k+4} - F_{2k}$ and $D_3 | F_{2k+1}$. This leads to the system

$$\begin{aligned} F_{2k+2}D_2D_3x_1^2 - F_{2k}D_1D_3x_2^2 &= F_{2k+1} \\ F_{2k+4}D_2D_3x_1^2 - F_{2k}D_1D_2x_3^2 &= F_{2k+4} - F_{2k}. \end{aligned}$$

Hence, to find all integer solutions of (15), it is enough to find all integer solutions to the systems of equations

$$d_1x_1^2 - d_2x_2^2 = j_1, \tag{20}$$

$$d_3x_1^2 - d_2x_3^2 = j_2, \tag{21}$$

where

- $d_1 = F_{2k+2}D_2$, D_2 is a square-free factor of $F_{2k+4} - F_{2k}$,
- $d_2 = F_{2k}D_1$, D_1 is a square-free factor of F_{2k+4},
- $d_3 = F_{2k+4}D_3$, D_3 is a square-free factor of F_{2k+1},
- $j_1 = \frac{F_{2k+1}}{D_3}$,
- $j_2 = \frac{F_{2k+4} - F_{2k}}{D_2}$.

By [10, Theorem 2], we may assume $(D_1, D_2, D_3) \neq (1, 1, 1)$.

We first considered the equations (20) and (21) separately modulo appropriate prime powers (see [14] and [11] for details). We tested all possible systems for $2 \le k \le 50$ using A. Pethő's program developed for the purposes of our joint paper [14]. We found that all systems are unsolvable apart from three systems listed in the following table.

k	$d_1,\ d_2,\ d_3,\ j_1,\ j_2$
10	233802911, 193864605, 46368, 10946, 3
11	192736, 17711, 121393, 28567, 51841
40	61305790721611591, 23416728348467685, 5263301804126784110390702740 32, 11554, 137083915467899403

Remaining three cases we consider separately.

$\boxed{k=10}$

Assume that the equation $46368x_1^2 - 193864605x_3^2 = 3$ has an integer solution. Then there is an integer solution of the equation

$$x^2 - 15456 \cdot 64621535y^2 = 15456. \tag{22}$$

Note that $15456 = 2 \cdot 3 \cdot 7 \cdot 23 \cdot 4^2 = 966 \cdot 4^2$ and $64621535 = 5 \cdot 11 \cdot 41 \cdot 28657$. Since the equation $a^2 - 966 \cdot 64621535b^2 = 6601 = 7 \cdot 23 \cdot 41$ has an integer solution ($(a, b) = (p_{854}, q_{854})$, where $\frac{p_n}{q_n}$ is the n^{th} convergent in the continued fraction expansion of $\sqrt{966 \cdot 64621535}$), by a theorem of Nagell [23, Theorem 11], equation (22) has no integer solution.

$\boxed{k=11}$

We have the system

$$\begin{aligned} 92736x_1^2 - 17711x_2^2 &= 28657, \\ 121393x_1^2 - 17711x_3^2 &= 51841, \\ 121393x_2^2 - 92736x_3^2 &= 75025. \end{aligned}$$

Let consider this system modulo 5. The third equation implies $x_2 \equiv x_3 \equiv 0 \pmod{5}$. Now the first equation implies $x_1^2 \equiv 2 \pmod{5}$, a contradiction.

$\boxed{k=40}$

Assume that the equation $d_1x_1^2 - d_2x_2^2 = j_1$ has an integer solution. Then the equation

$$x^2 - d_1d_2y^2 = -d_2j_1 \tag{23}$$

also has an integer solution. The fundamental solution of the equation $u^2 - d_1d_2v^2 = 1$ is $(u_0, v_0) = (37889062373143906, 1)$. By a theorem of

Nagell [22, Theorem 108], it follows that if (23) has an integer solution, then there is a solution of (23) such that

$$0 < y \leq \frac{\sqrt{d_2 j_1}}{\sqrt{2(u_0 - 1)}} < 60.$$

It is easy to check that there are no solutions of (23) with $1 \leq y \leq 59$, and therefore there are no solutions of the original equation $d_1 x_1^2 - d_2 x_2^2 = j_1$. □

References

[1] J. Arkin, V.E. Hoggatt, E.G. Strauss, *On Euler's solution of a problem of Diophantus.* Fibonacci Quart. **17** (1979), 333–339.

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

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

[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] Diophantus of Alexandria, *Arithmetics and the Book of Polygonal Numbers.* (I.G. Bashmakova, Ed.), Nauka, Moscow, 1974 (in Russian), pp. 103–104, 232.

[8] A. Dujella, *On Diophantine quintuples.* Acta Arith. **81** (1997), 69–79.

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

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

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

[12] A. Dujella, *Absolute bound for the size of Diophantine m-tuples.* J. Number Theory, to appear.

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

[14] A. Dujella, A. Pethő, *Integer points on a family of elliptic curves.* Publ. Math. Debrecen **56** (2000), 321–335.

[15] E. Herrmann, A. Pethő, H.G. Zimmer, *On Fermat's quadruple equations.* Abh. Math. Sem. Univ. Hamburg **69** (1999), 283–291.

[16] V.E. Hoggatt, G.E. Bergum, *A problem of Fermat and the Fibonacci sequence.* Fibonacci Quart. **15**(1977), 323–330.

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

[18] B.W. Jones, *A second variation on a problem of Diophantus and Davenport.* Fibonacci Quart. **16** (1978), 155–165.

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

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

[21] B. Mazur, *Rational isogenies of prime degree.* Invent. Math. **44** (1978), 129–162.

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

[23] 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.

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

[25] A. Pethő, E. Herrmann, H.G. Zimmer, *S-integral points on elliptic curves and Fermat's triple equations.* In: Algorithmic Number Theory, (J. P. Buhler, ed.), Lecture Notes in Comput. Sci. **1423** (1998), 528–540.

[26] SIMATH manual, Universität des Saarlandes, Saarbrücken, 1997.
[27] M. Vellupillai, *The equations* $z^2 - 3y^2 = -2$ *and* $z^2 - 6x^2 = -5$*, in: A Collection of Manuscripts Related to the Fibonacci Sequence.* (V. E. Hoggatt, M. Bicknell-Johnson, eds.), The Fibonacci Association, Santa Clara, 1980, pp. 71–75.
[28] D. Zagier, *Elliptische Kurven: Fortschritte und Anwendungen.* Jahresber. Deutsch. Math.-Verein **92** (1990), 58–76.

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