ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 39, Number 6, 2009

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

YASUTSUGU FUJITA

ABSTRACT. Denote by F_n the nth Fibonacci number. We show that if a positive integer d satisfies the property that for an integer $k \geq 0$ each of $F_{2k+1}d+1$, $F_{2k+3}d+1$ and $F_{2k+5}d+1$ is a perfect square, then d must be $4F_{2k+2}F_{2k+3}F_{2k+4}$. Using this result, we further show that if for an integer $k \geq 1$ the rank of the attached elliptic curve

$$E_k : y^2 = (F_{2k+1}x + 1)(F_{2k+3}x + 1)(F_{2k+5}x + 1)$$

over $\mathbf{Q}$ equals one, then the integer points on E_k are given by

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

1. Introduction. Diophantus found that the rational numbers $1/16$, $33/16$, $68/16$, $105/16$ have the property that the product of any two of them increased by one is a square of a rational number. The first example of four positive integers with such a property was found by Fermat, which was the set $\{1, 3, 8, 120\}$. Replacing "one" by "n" leads to the following definition.

Definition 1. Let n be a nonzero integer. A set $\{a_1, \dots, a_m\}$ of m distinct positive integers is called a Diophantine m-tuple with the property $D(n)$ (or a $D(n)$-m-tuple) if $a_i a_j + n$ is a perfect square for all i, j with $1 \leq i < j \leq m$.

In case $n = 1$, a folklore conjecture says that a $D(1)$-quintuple does not exist. This is an immediate consequence of the following:

Received by the editors on November 27, 2006, and in revised form on May 26, 2007.

DOI:10.1216/RMJ-2009-39-6-1907

Conjecture 1 (cf. [**1**]). *If* $\{a, b, c, d\}$ *is a* $D(1)$*-quadruple with* $a < b < c < d$*, then* $d = d_+$*, where*

$$d_+ = 2abc + a + b + c + 2\sqrt{(ab+1)(ac+1)(bc+1)}.$$

The first result supporting the validity of Conjecture 1 was shown by Baker and Davenport [**2**], which states that if $\{1, 3, 8, d\}$ is a $D(1)$-quadruple, then $d = 120 (= d_+)$. This result has been generalized in three directions. First, Dujella [**8**] showed that if $\{k-1, k+1, 4k, d\}$ with $k \geq 2$ is a $D(1)$-quadruple, then $d = 4k(4k^2 - 1)(= d_+)$; secondly, Dujella and Pethő [**18**] showed that if $\{1, 3, c, d\}$ with $c < d$ is a $D(1)$-quadruple, then $d = c_{\nu+1}(= d_+)$, where

$$c = c_\nu = \frac{1}{6}\left\{(2+\sqrt{3})^{2\nu+1} + (2-\sqrt{3})^{2\nu+1} - 4\right\}, \quad \nu = 1, 2, \dots ;$$

and thirdly, Dujella [**10**] showed that if $\{F_{2k}, F_{2k+2}, F_{2k+4}, d\}$, where $k \geq 1$ and F_ν denotes the νth Fibonacci number, is a $D(1)$-quadruple, then $d = 4F_{2k+1}F_{2k+2}F_{2k+3}(= d_+)$ (this is called the Hoggatt-Bergum conjecture, see [**24**]). The first two results have been generalized, and it is known that if $\{k-1, k+1, c, d\}$ is a $D(1)$-quadruple with $c < d$, then $c = c_{\nu+1}(= d_+)$, where

$$c = c_\nu = \frac{1}{2(k^2-1)}\left\{(k+\sqrt{k^2-1})^{2\nu+1} + (k-\sqrt{k^2-1})^{2\nu+1} - 2k\right\}, \quad \nu = 1, 2, \dots ,$$

cf. [**4, 22**]. In general, it has been shown by Dujella [**15**] that there does not exist a $D(1)$-sextuple and there exist only finitely many $D(1)$-quintuples.

For $n = -1$, Dujella [**9**] showed that the pair $\{1, 2\}$ cannot be extended to a $D(-1)$-quadruple. Moreover, Dujella and Fuchs showed that any $D(-1)$-triple $\{a, b, c\}$ with $2 \leq a < b < c$ cannot be extended to a $D(-1)$-quadruple. This immediately implies that there does not exist a $D(-1)$-quintuple. (For results in the cases of $a = 1$ and $b \geq 5$, see [**20, 21, 32**].) Recently, Dujella, Filipin and Fuchs [**16**] showed that there exist only finitely many $D(-1)$-quadruples.

Whereas any $D(-1)$-triple $\{a,b,c\}$ with $a < b < c$ cannot be conjecturally extended to a $D(-1)$-quadruple, there exists a positive integer d such that each of $ad+1$, $bd+1$ and $cd+1$ is a perfect square. In fact, $d = d^+$ has such a property, where

$$d^+ = 2abc - (a+b+c) + 2\sqrt{(ab-1)(ac-1)(bc-1)},$$

cf. [**14**, Lemma 3]. This leads to the following definition.

Definition 2. A set $\{a,b,c;d\}$ of positive integers is said to have the property $D(-1;1)$ if $\{a,b,c\}$ is a $D(-1)$-triple and each of $ad+1$, $bd+1$ and $cd+1$ is a perfect square.

It is to be noted that a $D(-1)$-triple $\{a,b,c\}$ can be extended to a $D(-1)$-quadruple $\{a,b,c,-d\}$ in the ring $\mathbf{Z}[i]$ of Gaussian integers, cf. [**7**, Example 1], which corresponds to our quadruple $\{a,b,c;d\}$ having the property $D(-1;1)$. In this paper, we first show that if $a = F_{2k+1}$, $b = F_{2k+3}$ and $c = F_{2k+5}$, then such a d is unique, which is another conjecture of Hoggatt and Bergum [**24**]:

Theorem 1. *Let $k \geq 0$ be an integer. If the set $\{F_{2k+1}, F_{2k+3}, F_{2k+5}\}$ has the property $D(-1;1)$, then d must be $4F_{2k+2}F_{2k+3}F_{2k+4}$.*

Note that $4F_{2k+2}F_{2k+3}F_{2k+4} = d^+$.

We next examine integer points on the attached elliptic curves. Let C_k be the elliptic curve defined by

$$C_k : y^2 = (F_{2k}x+1)(F_{2k+2}x+1)(F_{2k+4}x+1).$$

Then, using the result obtained in [**10**], Dujella [**13**] showed that if the rank of C_k over $\mathbf{Q}$ equals one, then the integer points on C_k are given by

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

(For similar results on the $D(1)$-triples $\{k-1, k+1, 4k\}$, $k \geq 3$, and $\{1,3,c_\nu\}$, $\nu \geq 1$, see [**11, 19**].) Analogously, let E_k be the elliptic curve defined by

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

Then, using Theorem 1 we show the following.

Theorem 2. *Let $k \geq 1$ be an integer and E_k the elliptic curve given by* (1)*. If the rank of E_k over $\mathbf{Q}$ equals one, then the integer points on E_k are given by*

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

Note that without the assumption on the rank of E_k, one can show that the integer points on E_k are given by (2) for $4 \leq k \leq 50$ with $k \notin \{9, 20, 24, 25, 32, 43\}$, see Remark 2, while the same is not true for $k \in \{0, 2, 3\}$, see Remark 1.

We prove Theorem 1 in Section 2 and Theorem 2 in Section 3 along the same lines as in [**10, 13**], respectively.

2. The proof of Theorem 1.

2.1. A lower bound for solutions. Let $\{a, b, c\}$ be a $D(-1)$-triple with $a < b < c$. Let r, s, t be positive integers with

$$ab - 1 = r^2, \qquad ac - 1 = s^2, \qquad bc - 1 = t^2.$$

The latter two relations lead to the Diophantine equation

$$(3)\qquad at^2 - bs^2 = b - a.$$

Lemma 1. *Let (t, s) be a positive solution of* (3)*. Then there exists a solution (t_0, s_0) of* (3) *satisfying the following:*

(i) $|s_0| < \sqrt{a(b-a)}$, $0 < t_0 \leq \sqrt{b(b-a)}$;

(ii) *There exists an integer $j \geq 0$ such that*

$$(4)\qquad t\sqrt{a} + s\sqrt{b} = (t_0\sqrt{a} + s_0\sqrt{b})(2ab - 1 + 2r\sqrt{ab})^j.$$

Proof. We apply [**33**, Theorem II.9, Section 4], which is analogous to [**29**, Theorems 108, 108a], to the equation $bs^2 - at^2 = a - b$. Then we see that there exists a solution (t_0, s_0) of (3) with

$$|s_0| \le \frac{r\sqrt{b-a}}{\sqrt{b}} < \sqrt{a(b-a)}, \qquad 0 < t_0 \le \sqrt{b(b-a)}$$

and an integer $j \ge 0$ such that

$$t\sqrt{a} + s\sqrt{b} = \pm(t_0\sqrt{a} + s_0\sqrt{b})(2ab - 1 \pm 2r\sqrt{ab})^j, \tag{5}$$

where the $\pm$ signs may be taken independently. Suppose that the first sign is minus. Since

$$(t_0\sqrt{a} + s_0\sqrt{b})(t_0\sqrt{a} - s_0\sqrt{b}) = b - a > 0$$

and $t_0 > 0$ together imply that $t_0\sqrt{a} + s_0\sqrt{b} > 0$, the righthand side of (5) is negative, which is a contradiction. Hence, the first sign must be plus. If the second sign is minus and $j > 0$, then

$$\begin{aligned} t\sqrt{a} + s\sqrt{b} &= (t_0\sqrt{a} + s_0\sqrt{b})(2ab - 1 - 2r\sqrt{ab})^j \\ &\le \frac{t_0\sqrt{a} + s_0\sqrt{b}}{2ab - 1 + 2r\sqrt{ab}} < \frac{b\sqrt{a} + r\sqrt{b}}{4ab - 3} < 1, \end{aligned}$$

which is a contradiction. Hence, the second sign must be plus, too. This completes the proof of Lemma 1. $\square$

By (4), we may write $s = \sigma_j$, where

$$\sigma_0 = s_0, \qquad \sigma_1 = (2ab-1)s_0 + 2art_0, \qquad \sigma_{j+2} = 2(2ab-1)\sigma_{j+1} - \sigma_j.$$

It is easy to see by induction that

$$\sigma_j \equiv (-1)^j s_0 \pmod{a}.$$

Hence, if $(s^2+1)/a$ is an integer (this is the case in our situation), then so is $(s_0^2+1)/a$.

Lemma 2. *Let (t, s) be a positive solution of* (3). *Assume that $(s^2+1)/a$ is an integer and $b < 3a$. If (t_0, s_0) is a solution of* (3) *satisfying* (i) *and* (ii) *in Lemma* 1, *then we have*

$$(t_0, s_0) = (b - r, \pm(r - a)).$$

Proof. If $a = 1$ and $b = 2$, then equation (3) becomes $t^2 - 2s^2 = 1$, and its positive solutions are given by $t + s\sqrt{2} = (3 + 2\sqrt{2})^j$. Hence, Lemma 2 holds. We may assume that $(a, b) \neq (1, 2)$. Put $c_0 = (s_0^2 + 1)/a$. Then, as we mentioned above, c_0 is an integer and it is clear that $\{a, b, c_0\}$ is a $D(-1)$-triple with

$$c_0 < \frac{1}{a}(r^2 + 1) = b.$$

Applying Lemma 7 in [**17**] to this triple, we see from $b < 3a \leq 3ac_0$ that

$$b = a + c_0 + 2\sqrt{ac_0 - 1},$$

that is, $c_0 = a + b - 2r$. It follows that

$$\begin{aligned} s_0 &= \pm\sqrt{a^2 + ab - 2ar - 1} = \pm(r - a), \\ t_0 &= \sqrt{ab + b^2 - 2br - 1} = b - r. \end{aligned}$$

This completes the proof of Lemma 2. $\square$

We now assume that $\{a, b, c; d\}$ has the property $D(-1; 1)$. Then, there exist positive integers x, y and z such that

$$ad + 1 = x^2, \qquad bd + 1 = y^2, \qquad cd + 1 = z^2. \tag{6}$$

Eliminating d, we obtain the system of Diophantine equations:

$$\begin{cases} ay^2 - bx^2 = a - b, \\ az^2 - cx^2 = a - c, \\ bz^2 - cy^2 = b - c \end{cases} \tag{7}$$

Lemma 3. *Let (y, x), (z, x) and (z, y) be positive solutions of* (7), (8) *and* (9), *respectively. Then there exist solutions (y_0, x_0), (z_1, x_1) and (z_2, x_2) of* (7), *satisfying the following*:

$$\text{(i) } 0 < x_0 \le \sqrt{a(b-a)}, \qquad |y_0| < \sqrt{b(b-a)},$$

$$0 < x_1 \le \sqrt{a(c-a)}, \qquad |z_1| < \sqrt{c(c-a)}, \tag{8}$$

$$0 < y_2 \le \sqrt{b(c-b)}, \qquad |z_2| < \sqrt{c(c-b)}; \tag{9}$$

(ii) *There exist integers m, n and $l \ge 0$ such that*

$$y\sqrt{a} + x\sqrt{b} = (y_0\sqrt{a} + x_0\sqrt{b})(2ab - 1 + 2r\sqrt{ab})^m, \tag{10}$$

$$z\sqrt{a} + x\sqrt{c} = (z_1\sqrt{a} + x_1\sqrt{c})(2ac - 1 + 2s\sqrt{ac})^n, \tag{11}$$

$$z\sqrt{b} + y\sqrt{c} = (z_2\sqrt{b} + y_2\sqrt{c})(2bc - 1 + 2t\sqrt{bc})^l. \tag{12}$$

Proof. Since one may prove this lemma in exactly the same way as Lemma 1, we omit the proof. □

In what follows, let (y_0, x_0), (z_1, x_1) and (z_2, y_2) be the ones in Lemma 3. In the same way as was mentioned just before Lemma 2, we easily see that if $(x^2 - 1)/a$ is an integer (this is the case in our situation), then so is $(x_0^2 - 1)/a$.

Lemma 4. *Let (y, x) be a positive solution of* (7)*. If $(x^2 - 1)/a$ is an integer and $b < 3a$, then we have*

$$(y_0, x_0) = (\pm 1, 1).$$

Proof. If $a = 1$ and $b = 2$, then equation (7) becomes $y^2 - 2x^2 = -1$, and its positive solutions are given by $y + x\sqrt{2} = (1 + \sqrt{2})(3 + 2\sqrt{2})^m$. Hence, Lemma 4 holds. We may assume that $(a, b) \ne (1, 2)$.

Put $d_0 = (x_0^2 - 1)/a$ and

$$c' = a + b + (2ab - 1)d_0 + 2rx_0|y_0|.$$

Then, as we mentioned above, d_0 is an integer. From

$$ac' - 1 = (rx_0 + a|y_0|)^2 \text{ and } bc' - 1 = (bx_0 + r|y_0|)^2,$$

we see that $\{a, b, c'\}$ is a $D(-1)$-triple. Suppose now that $d_0 > 0$. Since $c' > a + b + 2r$, by Lemma 7 in [**17**] we have

$$c' > 3ab. \tag{13}$$

Since $d_0 \leq (a(b-a)-1)/a < b - a$, we also have

$$\begin{aligned} c' &< a + b + (2ab-1)(b-a) + 2r(b-a)\sqrt{ab} \\ &< (4ab-1)(b-a) + a + b \\ &< 4ab^2. \end{aligned} \tag{14}$$

On the other hand, when we number the c's satisfying the property that $\{a, b, c\}$ is a $D(-1)$-triple by $c_0 < c_1 < \cdots$, Lemmas 1 and 2 imply that

$$\begin{aligned} c_0 &= a + b - 2r, \\ c_1 &= a + b + 2r < 3ab, \\ c_2 &= \frac{\{4ab(r-a) + 3a - r\}^2 + 1}{a} > 4ab^2, \end{aligned}$$

where the last inequality follows from $(a, b) \neq (1, 2)$. This contradicts (13) and (14). Hence, we obtain $d_0 = 0$ and $x_0 = 1$, $y_0 = \pm 1$. $\square$

In what follows, assume that $k \geq 0$ is an integer and that

$$a = F_{2k+1}, \qquad b = F_{2k+3}, \qquad c = F_{2k+5}.$$

Then we have $(2a \leq) b < 3a$ and

$$c = 3b - a, \qquad r = b - a, \qquad s = b, \qquad t = 2b - a.$$

Lemma 5. *Let (x, y, z) be a positive solution of the system of equations* (6). *Then we have*

$$(z_2, y_2) = (\pm 1, 1) \quad \textit{and} \quad (z_1, x_1) = (\pm 1, 1).$$

Proof. By (10) and (12) we may write $y = \alpha_m = \beta_l$, where

(15)
$$\alpha_0 = y_0,\ \alpha_1 = (2ab-1)y_0 + 2brx_0,\ \alpha_{m+2} = 2(2ab-1)\alpha_{m+1} - \alpha_m,$$
(16)
$$\beta_0 = y_2,\ \beta_1 = (2bc-1)y_2 + 2btz_2,\ \beta_{l+2} = 2(2bc-1)\beta_{l+1} - \beta_l.$$

By induction, it is easy to see from (15) and (16) that

$$\alpha_m \equiv (-1)^m y_0 \pmod{2b} \quad \text{and} \quad \beta_l \equiv (-1)^l y_2 \pmod{2b}.$$

We know from Lemma 4 that $y_0 = \pm 1$, and we see from (9), with $c = 3b - a$, that

$$0 < y_2 \le \sqrt{b(2b-a)} < 2b - 1.$$

It follows from $\alpha_m = \beta_l$ that $y_2 = 1$ and $z_2 = \pm 1$.

Similarly, by (11) and (12) we may write $z = p_n = q_l$, where

$$p_0 = z_1, \quad p_1 = (2ac-1)z_1 + 2csx_1, \quad p_{n+2} = 2(2ac-1)p_{n+1} - p_n,$$
$$q_0 = z_2, \quad q_1 = (2bc-1)z_2 + 2cty_2, \quad q_{l+2} = 2(2bc-1)q_{l+1} - q_l,$$

and we obtain

$$p_n \equiv (-1)^n z_1 \pmod{2c} \quad \text{and} \quad q_l \equiv (-1)^l z_2 \pmod{2c}.$$

We know from the above that $z_2 = \pm 1$, and we see from (8) that

$$|z_1| < \sqrt{c(c-a)} < c.$$

It follows from $p_n = q_l$ that $z_1 = \pm 1$ and $x_1 = 1$. $\square$

Lemma 6. *Let (x, y, z) be a positive solution of the system of equations (6). Then, there exist integers m and n such that*

$$x = v_m = w_n,$$

where v_m and w_n are the two-sided sequences, respectively, given by the following:

(17)
$$v_0 = 1, \quad v_1 = 2a(2b-a) - 1, \quad v_{m+2} = 2(2ab-1)v_{m+1} - v_m;$$
(18)
$$w_0 = 1, \quad w_1 = 2a(4b-a) - 1, \quad w_{n+2} = 2(6ab - 2a^2 - 1)w_{n+1} - w_n.$$

Proof. If we note that $c = 3b - a$, $r = b - a$ and $s = b$, Lemmas 4, 5 and equations (10) and (11) together allow us to write $x = v_m = w_n$ with $m, n \geq 0$, where

(19)
$$v_0 = 1,\ v_1 = 2ab - 1 \pm 2a(b-a),\ v_{m+2} = 2(2ab-1)v_{m+1} - v_m,$$
(20)
$$w_0 = 1,\ w_1 = 6ab - 2a^2 - 1 \pm 2ab,\ w_{n+2} = 2(6a^2 - 2a^2 - 1)w_{n+1} - w_n.$$

If we define

$$v_{-1} = 2ab - 1 - 2a(b-a) = 2a^2 - 1,$$
$$w_{-1} = 6ab - 2a^2 - 1 - 2ab = 4ab - 2a^2 - 1,$$

and choose the plus signs in the expressions of v_1 and w_1, we can replace (19) and (20) with $m, n \geq 0$ by (17) and (18) with arbitrary m, n. $\square$

Lemma 7. *Assume that $a \neq 1$, i.e., $k \neq 0$. If $|m| \geq 2$, then we have*

$$|m| \geq 2b - 1 \geq 5a - 1.$$

Proof. By induction, we easily see from (17) that

$$v_m \equiv (-1)^m(2ma^2 + 1) \pmod{4ab}.$$

Since

$$a^2 + 1 = b(3a - b) \equiv 0 \pmod{b}, \tag{21}$$

from (18) it follows that

$$w_n \equiv \begin{cases} 1 & \pmod{4ab} \text{ if } n \text{ is even;} \\ -(2a^2+1) & \pmod{4ab} \text{ if } n \text{ is odd.} \end{cases}$$

(i) If both m and n are even, then we have $2ma^2 \equiv 0 \pmod{4ab}$, that is, $ma/2 \equiv 0 \pmod{b}$. Since $\gcd(a, b) = 1$, we obtain $m/2 \equiv 0 \pmod{b}$.

(ii) If m is even and n is odd, then we have $2ma^2+1 \equiv -(2a^2+1) \pmod{4ab}$, that is, $(m+1)a^2 \equiv -1 \pmod{2ab}$, which contradicts $a \neq 1$.

(iii) If m is odd and n is even, then we have $-(2ma^2+1) \equiv 1 \pmod{4ab}$, that is, $ma^2 \equiv -1 \pmod{2ab}$, which contradicts $a \neq 1$.

(iv) If both m and n are odd, then we have $-(2ma^2+1) \equiv -(2a^2+1) \pmod{4ab}$, that is, $(m-1)a/2 \equiv 0 \pmod{b}$. Since $\gcd(a,b)=1$, we obtain $(m-1)/2 \equiv 0 \pmod{b}$.

By (i), (ii), (iii) and (iv), if $m \geq 2$, then we have $m/2 \geq b$; if $m \leq -2$, then we have $(m-1)/2 \leq -b$. Hence, we obtain $|m| \geq 2b-1$. This completes the proof of Lemma 7. □

2.2. Linear forms in three logarithms and the reduction method. In this section, we apply Baker's theory to linear forms in three logarithms arising from the sequences $\{v_m\}$ and $\{w_n\}$, and complete the proof of Theorem 1 using the reduction method due to Dujella and Pethő, cf. [**18**], based on the Baker-Davenport lemma, cf. [**2**].

Lemma 8. *If $v_m = w_n$ for some m and n with $|m| \geq 2$, then we have*

$$0 < \Lambda := |m|\log\alpha_1 - |n|\log\alpha_2 + \log\alpha_3 < 6\alpha_1^{-2|m|}, \tag{22}$$

where

$$\alpha_1 = 2ab-1+2(b-a)\sqrt{ab},\ \alpha_2 = 2ac-1+2b\sqrt{ac},\ \alpha_3 = \frac{\sqrt{c}(\sqrt{b}\pm\sqrt{a})}{\sqrt{b}(\sqrt{c}\pm\sqrt{a})}.$$

(*Here, the $\pm$ signs in α_3 are taken independently.*)

Proof. By (17) and (18), we have

$$\begin{aligned} v_m = \frac{1}{2\sqrt{b}}\Big\{&(\sqrt{b}\pm\sqrt{a})(2ab-1+2(b-a)\sqrt{ab})^{|m|} \\ &+(\sqrt{b}\mp\sqrt{a})(2ab-1-2(b-a)\sqrt{ab})^{|m|}\Big\}, \\ w_n = \frac{1}{2\sqrt{c}}\Big\{&(\sqrt{c}\pm\sqrt{a})(2ac-1+2(c-a)\sqrt{ac})^{|n|} \\ &+(\sqrt{c}\mp\sqrt{a})(2ac-1-2(c-a)\sqrt{ac})^{|n|}\Big\}. \end{aligned}$$

Put

$$
\begin{aligned}
P &= \frac{\sqrt{b} \pm \sqrt{a}}{\sqrt{b}}(2ab - 1 + 2(b-a)\sqrt{ab})^{|m|}, \\
Q &= \frac{\sqrt{c} \pm \sqrt{a}}{\sqrt{c}}(2ac - 1 + 2b\sqrt{ac})^{|n|}.
\end{aligned}
$$

Then, $v_m = w_n$ implies that

$$
P + \frac{b-a}{b}P^{-1} = Q + \frac{c-a}{c}Q^{-1}.
$$

The assumption $|m| \geq 2$ immediately implies that $n \neq 0$ and that $P > 1$, $Q > 1$. Since

$$
\begin{aligned}
P - Q &= \frac{c-a}{c}Q^{-1} - \frac{b-a}{b}P^{-1} > \frac{c-a}{c}(Q^{-1} - P^{-1}) \\
&= \frac{c-a}{c}(P-Q)P^{-1}Q^{-1},
\end{aligned}
$$

we have $P > Q$. $|m| \geq 2$ further implies that $P > 2a^2b^2$. Since $(c-a)/a = (3b-2a)/a < (9a-2a)/a = 7$, we have $P - (c-a)/a > 0$, which together with $Q > P - (c-a)Q^{-1}/c > P - (c-a)/c$ implies that

$$
\begin{aligned}
P - Q &= \frac{c-a}{c}Q^{-1} - \frac{b-a}{b}P^{-1} \\
&< \frac{c-a}{c}\left(P - \frac{c-a}{c}\right)^{-1} - \frac{b-a}{b}P^{-1} \\
&< P^{-1} - \frac{b-a}{b}P^{-1} = \frac{a}{b}P^{-1}.
\end{aligned}
$$

Noting that $aP^{-2}/b < 1/(4a^3b^5) < 1/2$, we obtain

$$
\begin{aligned}
0 < \log\frac{P}{Q} &= -\log\left(1-\frac{P-Q}{P}\right) \\
&< -\log\left(1-\frac{a}{b}P^{-2}\right) < \left(1+\frac{a}{b}P^{-2}\right)\cdot\frac{a}{b}P^{-2} \\
&< \left(1+\frac{1}{4a^3b^5}\right)\cdot\frac{a}{b}\cdot\frac{b}{(\sqrt{b}-\sqrt{a})^2}(2ab-1+2(b-a)\sqrt{ab})^{-2|m|} \\
&\le \frac{129}{128}(\sqrt{2}+1)^2(2ab-1+2(b-a)\sqrt{ab})^{-2|m|} \\
&< 6(2ab-1+2(b-a)\sqrt{ab})^{-2|m|}.
\end{aligned}
$$

From this inequality, Lemma 8 immediately follows. □

It is easy to see from Lemma 8 that if $v_m = w_n$ with $|m| \ge 2$, then

$$|m| \ge |n|.$$

For, if $|m| \le |n| - 1$, then we have

$$
\begin{aligned}
\Lambda &\le |n|\log\left(\frac{\alpha_1}{\alpha_2}\right) + \log\left(\frac{\alpha_3}{\alpha_1}\right) \\
&< \log\left(\frac{\sqrt{c}(\sqrt{b}+\sqrt{a})}{\sqrt{b}(\sqrt{c}+\sqrt{a})}\cdot\frac{1}{4(b-a)^2}\right) \\
&< \log\frac{1}{\sqrt{c}+\sqrt{a}} < 0,
\end{aligned}
$$

which contradicts (22).

Applying now Matveev's theorem to (22), we obtain upper bounds for $|m|$ and k.

Theorem 3 (cf. [**27**]). *Let Λ be a linear form in logarithms of l multiplicatively independent totally real algebraic numbers $\alpha_1, \dots, \alpha_l$ with rational integer coefficients $b_1, \dots, b_l$, $b_l \ne 0$. Let $h(\alpha_j)$ denote the absolute logarithmic height of α_j for $1 \le j \le l$. Define the numbers D, A_j, $1 \le j \le l$, and B by $D = [\mathbf{Q}(\alpha_1, \dots, \alpha_l) : \mathbf{Q}]$, $A_j = \max\{Dh(\alpha_j), |\log\alpha_j|\}$, $B = \max\{1, \max\{|b_j|A_j/A_l;\ 1 \le j \le l\}\}$. Then,*

$$\log|\Lambda| > -C(l)C_0W_0D^2\Omega,$$

where

$$C(l) = \frac{8}{(l-1)!}(l+2)(2l+3)(4\mathrm{e}(l+1))^{l+1},$$
$$C_0 = \log(\mathrm{e}^{4.4l+7} l^{5.5} D^2 \log(\mathrm{e}D)),$$
$$W_0 = \log(1.5\mathrm{e}BD\log(\mathrm{e}D)), \quad \Omega = A_1 \cdots A_l.$$

Proposition 1. *Let $k \geq 0$ be an integer, and let $a = F_{2k+1}$, $b = F_{2k+3}$, $c = F_{2k+5}$. Assume that the set $\{a, b, c; d\}$ has the property $D(-1; 1)$ with $d \neq 4F_{2k+2}F_{2k+3}F_{2k+4}$. If $k \geq 1$, then $|m| < 2 \cdot 10^{18}$ and $k \leq 42$; if $k = 0$, then $2 \leq m < 10^{15}$.*

Proof. If $m = 0$, then $x = 1$ and $d = 0$; if $m = 1$, then $x = 2a(2b-a) - 1$ and

$$\begin{aligned} d &= 4(2b-a)(a(2b-a)-1) \\ &= 4b(b-a)(2b-a) = 4F_{2k+2}F_{2k+3}F_{2k+4}. \end{aligned}$$

Hence, we have $m \neq 0, 1$. Moreover, if $k \geq 1$, then

$$v_0 = w_0 = 1 < v_{-1} = 2a^2 - 1 < v_1 = w_{-1} = 2a(2b-a) - 1 < w_1 < \cdots,$$

whence we have $|m| \geq 2$ and we may apply Lemma 7.

We now apply Theorem 3 with

$$l = 3, \qquad b_1 = |m|, \qquad b_2 = -|n|, \qquad b_3 = 1, \qquad D = 4,$$

and α_1, α_2 and α_3 defined by Lemma 8. We have

$$h(\alpha_1) = \frac{1}{2}\log\alpha_1 < \frac{1}{2}\log(4ab-1) < \log(4a),$$
$$h(\alpha_2) = \frac{1}{2}\log\alpha_2 < \frac{1}{2}\log(4ac-1) < \log(6a).$$

α_3 satisfies the following relation:

$$\begin{aligned} b^2(c-a)^2\alpha_3^4 - 4b^2c(c-a)\alpha_3^3 + 2bc(3bc - (a+b+c)a)\alpha_3^2 \\ - 4bc^2(b-a)\alpha_3 + c^2(b-a)^2 = 0. \end{aligned}$$

Since $\gcd(a,b) = \gcd(a,c) = \gcd(b,c) = 1$, we have $\gcd(b(c-a), c(b-a)) = 1$. Hence, the leading coefficient of the minimal polynomial of α_3 is $b^2(c-a)^2$. Since the conjugates of α_3 which are greater than one are

$$\frac{\sqrt{c}(\sqrt{b}+\sqrt{a})}{\sqrt{b}(\sqrt{c}\pm\sqrt{a})},$$

we have

$$\begin{aligned} h(\alpha_3) &= \frac{1}{4}\log\left\{b^2(c-a)^2 \cdot \frac{\sqrt{c}(\sqrt{b}+\sqrt{a})}{\sqrt{b}(\sqrt{c}+\sqrt{a})} \cdot \frac{\sqrt{c}(\sqrt{b}+\sqrt{a})}{\sqrt{b}(\sqrt{c}-\sqrt{a})}\right\} \\ &= \frac{1}{4}\log\left\{bc(c-a)(\sqrt{b}+\sqrt{a})^2\right\}. \end{aligned}$$

Since

$$\begin{aligned} bc(c-a)(\sqrt{b}+\sqrt{a})^2 &< 3a\cdot 8a\cdot 7a(\sqrt{3a}+\sqrt{a})^2 \\ &= 168(\sqrt{3}+1)^2a^4 < (6a)^4, \end{aligned}$$

$$\begin{aligned} bc(c-a)(\sqrt{b}+\sqrt{a})^2 &> 2a\cdot 5a\cdot 4a(\sqrt{2a}+\sqrt{a})^2 \\ &= 40(\sqrt{2}+1)^2a^4 > (3a)^4, \end{aligned}$$

we have

$$\log(3a) < h(\alpha_3) < \log(6a).$$

Hence, we obtain the following:

$$\begin{aligned} A_1 &< 4\log(4a); \quad A_2 < 4\log(6a); \quad 4\log(3a) < A_3 < 4\log(6a); \\ B &\le \max\left\{\frac{|m|\cdot\log(4a)}{\log(3a)}, \frac{|n|\cdot\log(6a)}{\log(3a)}, 1\right\} \\ &< \frac{|m|\log(6a)}{\log(3a)} \le \frac{(\log 6)|m|}{\log 3} < 1.64|m|; \\ C(3) &= \frac{8}{2!}\cdot 5\cdot 9\cdot(16\mathrm{e})^4 < 6.45\cdot 10^8; \\ C_0 &= \log\left(\mathrm{e}^{4.4\cdot 3+7}\cdot 3^{5.5}\cdot 16\cdot\log(4\mathrm{e})\right) < 29.9; \\ W_0 &= \log\left(1.5\mathrm{e}\cdot B\cdot 4\log(4\mathrm{e})\right) < \log(64|m|); \\ \Omega &= A_1A_2A_3 < 64(\log(4a))^2\cdot\log(6a) < 82.8(\log(4a))^3. \end{aligned}$$

It follows from Theorem 3 that

$$\log \Lambda > -2.6 \cdot 10^{13} (\log(4a))^3 \log(64|m|),$$

which together with Lemma 8 implies that

$$-2.6\cdot 10^{13} (\log(4a))^3 \log(64|m|) < \log\left(6(2ab-1+2(b-a)\sqrt{ab})^{-2|m|}\right).$$

Since

$$\begin{aligned}\log\left(6(2ab-1+2(b-a)\sqrt{ab})^{-2|m|}\right) &< \log\left(6(4a^2)^{-2|m|}\right)\\ &< -(2|m|-1)\log(4a^2),\end{aligned}$$

we have

$$\frac{2|m|-1}{\log(64|m|)} < (\log(4a))^2 \cdot 2.6 \cdot 10^{13}.$$

If $k \geq 1$, then Lemma 7 implies that $|m| > 4a$; hence, we have

$$\phi(m) := \frac{2|m|-1}{\log(64|m|)(\log|m|)^2} < 2.6 \cdot 10^{13}.$$

Since the function $\phi(m)$ is increasing and $\phi(2\cdot 10^{18}) > 4.8 \cdot 10^{13}$, we obtain $|m| < 2 \cdot 10^{18}$. Hence, we have

$$F_{2k+1} = a < \frac{|m|}{4} < 5 \cdot 10^{17},$$

which together with $F_{2\cdot 43+1} > 6.7 \cdot 10^{17}$ implies that $k \leq 42$.

If $k = 0$, then since $|m| = m$ (see the beginning of the proof of Lemma 4) we have

$$\psi(m) := \frac{2m-1}{\log(64m)} < (\log 4)^2 \cdot 2.6 \cdot 10^{13} < 5 \cdot 10^{13}.$$

Since the function $\psi(m)$ is increasing and $\psi(10^{15}) > 5.1\cdot 10^{13}$, we obtain $m < 10^{15}$. This completes the proof of Proposition 1. □

Proof of Theorem 1. Dividing (22) by $\log \alpha_2$, we have

$$0 < |m|\kappa - |n| + \mu < AB^{-|m|}, \tag{23}$$

where

$$\kappa = \frac{\log \alpha_1}{\log \alpha_2}, \qquad \mu = \frac{\log \alpha_3}{\log \alpha_2}, \qquad A = \frac{6}{\log \alpha_2}, \qquad B = \alpha_1^2.$$

Note that if $k \geq 1$, respectively $k = 0$, then there are four, respectively two, possibilities for μ because of the $\pm$ sign(s) in α_3. The following lemma is a variant of the Baker-Davenport lemma, cf. [**2**].

Lemma 9 (cf. [**10, 18**]). *Let M be a positive integer and p/q a convergent of the continued fraction expansion of κ such that $q > 6M$. Put $\varepsilon = ||\mu q|| - M||\kappa q||$ and $r = [\mu q + 1/2]$, where $||\cdot||$ denotes the distance from the nearest integer and $[x]$ denotes the greatest integer less than or equal to x.*

(1) *If $\varepsilon > 0$, then the inequality* (23) *has no solution in the range*

$$\frac{\log(Aq/\varepsilon)}{\log B} \leq |m| \leq M.$$

(2) *If $p - q + r = 0$, then the inequality* (23) *has no solution in the range*

$$\max\left\{\frac{\log(3Aq)}{\log B}, 1\right\} < |m| \leq M.$$

(3) *If $p - q - 2r = 0$, then the inequality* (23) *has no solution in the range*

$$\frac{\log(3Aq)}{\log B} \leq |m| \leq M.$$

Proof of Lemma 9. (1), (2). These are exactly Lemma 5 a), b) in [**18**].

(3) One may prove this along the same lines as Lemma 5 b) in [**18**]. Indeed, assume that the inequality (23) with $|m| \leq M$ has a solution. Since

$$0 < |m|(\kappa q - p) + (|m|p - |n|q + r) + (\mu q - r) < qAB^{-|m|},$$

we have

$$\begin{aligned}||m|p-|n|q+r| &< qAB^{-|m|}+|\mu q-r|+|m||\kappa q-p| \\ &< qAB^{-|m|}+\frac{2}{3}.\end{aligned}$$

If $qAB^{-|m|} \leq 1/3$, then $|m|p-|n|q+r=0$, which together with $p-q-2r=0$ implies that

$$(2|m|+1)p=(2|n|+1)q.$$

Since $\gcd(p,q)=1$, we have $2|m|+1 \equiv 0 \pmod{q}$. On the other hand, we know that

$$2|m|+1 \leq 2M+1 < \frac{q}{3}+1 < q;$$

thus, we have $2|m|+1=0$, which is a contradiction. Hence, we obtain $qAB^{-|m|} > 1/3$, that is,

$$|m| < \frac{\log(3Aq)}{\log B}.$$

This completes the proof of Lemma 9. $\square$

We apply Lemma 9 with $M=2\cdot 10^{18}$ for $1 \leq k \leq 42$ and with $M=10^{15}$ for $k=0$. We have to consider $4\cdot 42+2=170$ cases. In case $k \geq 1$, the second convergent is needed only in 11 cases; in any case, the first step of reduction gives $|m| \leq 6$, which contradicts Lemma 7 (note that $m \notin \{0, \pm 1\}$; see the beginning of the proof of Proposition 1). In case $k=0$, the first step of reduction gives $m \leq 10$, the second step gives $m \leq 2$, and the third step gives $m \leq 1$, which is a contradiction. This completes of the proof of Theorem 1. $\square$

3. Integer points on the attached elliptic curves. In this section, we prove Theorem 2.

For an integer $k \geq 0$ and $a=F_{2k+1}$, $b=F_{2k+3}$, $c=F_{2k+5}$, the elliptic curve $E=E_k$ is given by

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

The coordinate transformation

$$x \longmapsto \frac{x}{abc}, \qquad y \longmapsto \frac{y}{abc}$$

leads to the elliptic curve

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

E' has the following trivial $\mathbf{Q}$-rational points besides the identical element O:

$$A = (-bc, 0), \qquad B = (-ac, 0), \qquad C = (-ab, 0), \qquad P = (0, abc).$$

In order to determine the torsion group $E'(\mathbf{Q})_{\rm tors}$ over $\mathbf{Q}$ of E', we need the following two lemmas.

Lemma 10 (cf. [**26**, Theorem 4.2, page 85]). *Let $\mathcal{C}$ be an elliptic curve over $\mathbf{Q}$ given by*

$$\mathcal{C} : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

with α, β, γ in $\mathbf{Q}$. For $S = (x, y) \in \mathcal{C}(\mathbf{Q})$, there exists a $\mathbf{Q}$-rational point $T = (x', y')$ on $\mathcal{C}$ such that $[2]T = S$ if and only if $x - \alpha$, $x - \beta$ and $x - \gamma$ are all squares in $\mathbf{Q}$.

Lemma 11 (cf. [**5**]). (1) *If F_n is a perfect square, then $n = 1$, 2, or* 12.

(2) *If F_n is twice a perfect square, then $n = 3$ or 6.*

Lemma 12. *The torsion group $E'(\mathbf{Q})_{\rm tors}$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.*

Proof. By Lemma 10, if $A \in 2E'(\mathbf{Q})$, then $b(a-c)$ is a perfect square; if $B \in 2E'(\mathbf{Q})$, then $a(b-c)$ is a perfect square. Since $a < b < c$, these do not occur. Suppose that $C \in 2E'(\mathbf{Q})$. Since $c = 3b - a$, Lemma 10 implies that both $a(2b-a)$ and $b(3b-2a)$ must be perfect squares. Let's denote by N' the square-free part of an integer N. Then, a'

and b' divide $2b$ and $2a$, respectively. Since $\gcd(a,b)=1$, we have $a',b'\in\{1,2\}$. By Lemma 11, we have $a=1$ and $b=2$. However, $a(2b-a)=3$ is not a perfect square. Hence, we obtain $E'(\mathbf{Q})\not\supset \mathbf{Z}/4\mathbf{Z}$.

Suppose that $E'(\mathbf{Q})_{\mathrm{tors}}\simeq \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/6\mathbf{Z}$. We know from $\gcd(a,b)=\gcd(a,c)=\gcd(b,c)=1$ that $\gcd(c(b-a),b(c-a))=1$. It follows from [**30**, Main Theorem 1] that there exist integers α and β with $\alpha/\beta\notin\{-2,-1,-1/2,0,1\}$ and $\gcd(\alpha,\beta)=1$ such that

$$c(a-b)=\alpha^4+2\alpha^3\beta,\qquad b(a-c)=\beta^4+2\beta^3\alpha.$$

Adding both sides respectively, we have

$$a(b+c)-2bc=(\alpha^2+\alpha\beta+\beta^2)^2-3\alpha^2\beta^2. \tag{24}$$

While the lefthand side of (24) satisfies

$$\begin{aligned} a(b+c)-2bc&=F_{2k+1}(F_{2k+3}+F_{2k+5})-2F_{2k+3}F_{2k+5}\\ &=F_{2k+1}F_{2k+3}-F_{2k+4}F_{2k+5}\end{aligned}$$

and

$$(F_{2k+1}F_{2k+3}-F_{2k+4}F_{2k+5})_{k\geq 0}\equiv(3,2,7,3,2,7,\dots)\pmod 8,$$

the righthand side of (24) satisfies

$$(\alpha^2+\alpha\beta+\beta^2)^2-3\alpha^2\beta^2\equiv 0,\ 1,\ 5\text{ or }6\pmod 8,$$

which is a contradiction. Hence, we obtain $E'(\mathbf{Q})_{\mathrm{tors}}\not\simeq\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/6\mathbf{Z}$. It follows from Mazur's theorem, cf. [**28**], that $E'(\mathbf{Q})_{\mathrm{tors}}\simeq\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}$. □

Corollary 1. *The rank of $E'(\mathbf{Q})$ is greater than or equal to one.*

Proof. By Lemma 12, $P=(0,abc)$ is not a torsion point, from which the corollary immediately follows. □

Lemma 13. $P, P+A, P+B, P+C\notin 2E'(\mathbf{Q})$.

Proof. Denote by $x(S)$ the x-coordinate of a point S on E'. We have

$$x(P+A) = a(a-b-c), \quad x(P+B) = b(b-a-c), \quad x(P+C) = c(c-a-b).$$

By Lemma 10, if $P \in 2E'(\mathbf{Q})$, then both bc and ca are perfect squares. Since $\gcd(a,b) = 1$, both a and b are perfect squares, which contradicts Lemma 11. If $P + A \in 2E'(\mathbf{Q})$ or $P + B \in 2E'(\mathbf{Q})$, then $a(a-b)$ or $b(b-c)$ is a perfect square, which is impossible. If $P+C \in 2E'(\mathbf{Q})$, then $c(c-b) = F_{2k+4}F_{2k+5}$ is a perfect square. Since $\gcd(F_{2k+4}, F_{2k+5}) = 1$, both F_{2k+4} and F_{2k+5} are perfect squares, which contradicts Lemma 11. This completes the proof of Lemma 13. $\square$

Lemma 14 (cf. [**26**, Proposition 4.6, page 89]). *The function* $\varphi_a : E'(\mathbf{Q}) \to \mathbf{Q}^\times/(\mathbf{Q}^\times)^2$ *defined by*

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

is a group homomorphism. (*The functions* φ_b *and* φ_c *can be defined analogously and are group homomorphisms.*)

Proof of Theorem 2. Let (x,y) be an integer point on E, and let $X = (abcx, abcy) \in E'(\mathbf{Q})$. Let $E'(\mathbf{Q})/E'(\mathbf{Q})_{\text{tors}} = \langle U \rangle$. Then there exist an integer $m \geq 0$ and a point $T \in E'(\mathbf{Q})_{\text{tors}}$ such that

$$X = mU + T.$$

When we write

$$P = nU + T_1$$

for some integer $n \geq 0$ and some point $T_1 \in E'(\mathbf{Q})_{\text{tors}}$, we see from Lemma 12 that

$$T_1 \in \{O, A, B, C\}$$

and from Lemma 13 that n is odd. Hence, we have

$$X \equiv X_1 \pmod{2E'(\mathbf{Q})},$$

where

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

Since the functions φ_a, φ_b and φ_c in Lemma 14 are homomorphisms, the integer points (x, y) on E satisfy the following system:

$$ax + 1 = \alpha\Box, \qquad bx + 1 = \beta\Box, \qquad cx + 1 = \gamma\Box, \tag{25}$$

where $\Box$ denotes a square of a rational number and

(i) if $X_1 = O$, put $\alpha = bc$, $\beta = ac$, $\gamma = ab$;

(ii) if $X_1 = (abcu, abcv) \in \mathcal{S}\setminus\{O, A, B, C\}$, put $\alpha = au+1$, $\beta = bu+1$, $\gamma = cu + 1$;

otherwise, e.g., if $au + 1 = 0$, put $\alpha = \beta\gamma$, $\beta = bu + 1$, $\gamma = cu + 1$.

If $X_1 = P = (0, abc)$, then (25) means that

$$ax + 1 = \Box, \qquad bx + 1 = \Box, \qquad cx + 1 = \Box.$$

By Theorem 1 this system has the only solution $x = 4F_{2k+2}F_{2k+3}F_{2k+4}$ other than the trivial one $x = 0$. These solutions correspond to the integer points (2).

If $X_1 \in \{A, B, P+A, P+B\}$, then exactly two of α, β, γ are negative, and (25) has no solution. Hence, it suffices to consider the cases where

$$X_1 \in \{O, C, P + C\}.$$

Note that by Lemma 11 and the assumption $k \geq 1$, none of b, $2b$, c, $2c$ is a perfect square.

If $X_1 = O$, then (25) means that

$$ax + 1 = bc\Box, \qquad bx + 1 = ac\Box, \qquad cx + 1 = ab\Box.$$

Since $\gcd(a, b) = \gcd(b, c) = 1$, both of $ax + 1$ and $cx + 1$ are divisible by b' (the square-free part of b), and so is $c - a = 3b - 2a$. Hence, we have $b' \in \{1, 2\}$, which is impossible.

If $X_1 = C$, then we have $u = -1/c$, and (25) means that

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

Since $\gcd(c, c - a) = \gcd(c, c - b) = 1$, $b - a = c - 2b$ is divisible by c'. Hence, we have $c' \in \{1, 2\}$, which is impossible.

If $X_1 = P + C$, then we have $u = (c-a-b)/(ab)$, and (25) means that

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

For a positive integer N, let $N'' = \min\{N', (2N)'\}$. Since $\gcd(a,b) = \gcd(b, c-b) = 1$ and $\gcd(b, c-a) = \gcd(b, 3b-2a) = 1$ or 2, both of $ax+1$ and $cx+1$ are divisible by b'', and so is $c-a = 3b-2a$. Hence, we have $b' \in \{1,2\}$, which is impossible. This completes the proof of Theorem 2. $\Box$

Remark 1. We calculated, using MWRANK [**6**], the values of the ranks $\mathrm{rk}\,(E_k(\mathbf{Q}))$ of E_k over $\mathbf{Q}$ for $0 \le k \le 10$:

k	0	1	2	3	4	5	6	7	8	9	10
$\mathrm{rk}\,(E_k(\mathbf{Q}))$	1	1	3	2	2	2	1	2	1	4	2

Since $\mathrm{rk}\,(E_1(\mathbf{Q})) = 1$, the integer points on E_1 are given by (2) with $k = 1$. However, in each case of $k = 0$, 2 and 3, the same is not true. In fact,

$$(-1,0),\ (1,\pm 6) \in E_0,\ (23, \pm 5220) \in E_2,\ (1, \pm 210) \in E_3 \tag{26}$$

are integer points other than (2). In order to confirm that the integer points on E_0, E_2 and E_3 other than (2) are given by (26), we used the function "faintp" of SIMATH ([**31**], version 2.4). Note that the algorithm finding integer points on elliptic curves in SIMATH is based on [**23**].

Remark 2. Let (x,y) be an integer point on E_k. There exist positive integers x_1, x_2 and x_3 such that

$$\begin{cases} ax+1 = D_2 D_3 x_1^2, \\ bx+1 = D_1 D_3 x_2^2, \\ cx+1 = D_1 D_2 x_3^2, \end{cases} \tag{27}$$

where D_1, D_2 and D_3 are square-free integers dividing $c-b$, $c-a$ and $b-a$, respectively. Then, using the method due to Dujella and Pethő

([**19**]; see also [**11, 13, 25**]), we found that if $(D_1, D_2, D_3) \neq (1,1,1)$, then system (27) is unsolvable for all k with $4 \leq k \leq 50$ except the six cases listed in the following table:

TABLE 1. The exceptional six cases.

k	(D_1, D_2, D_3)
9	$(89, 29, 2255)$
20	$(1174889, 144481, 5473)$
24	$(1563, 2, 503450761)$
25	$(98209, 1, 47140601)$
32	$(303955413, 4021, 1762289)$
43	$(3932105689, 22235502640988369, 153088726119)$

It follows that Theorem 2 holds for all k with $4 \leq k \leq 50$ except $k \in \{9, 20, 24, 25, 32, 43\}$ without the assumption on the rank of E_k. The reason why we could not examine the above six cases is that the fundamental solutions of the Pell equations attached to the Diophantine equations given by eliminating x from (27) are too large.

Acknowledgments. We would like to thank Professor Andrej Dujella for his helpful comments. Thanks also go to the referee for valuable suggestions.

REFERENCES

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

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

3. M.A. Bennett, *On the number of solutions of simultaneous Pell equations*, J. Reine angew. Math. **498** (1998), 173–199.

4. 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.

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

6. J.E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1997.

7. A. Dujella, *The problem of Diophantus and Davenport for Gaussian integers*, Glasgow Math. **32** (1997), 1–10.

8. ———, *The problem of the extension of a parametric family of Diophantine triples*, Publ. Math. Debrecen **51** (1997), 311–322.

9. ———, *Complete solution of a family of simultaneous Pellian equations*, Acta Math. Inform. Univ. Ostraviensis **6** (1998), 59–67.

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

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

12. ———, *An absolute bound for the size of Diophantine m-tuples*, J. Number Theory **89** (2001), 126–150.

13. ———, *Diophantine m-tuples and elliptic curves*, J. Theor. Nombres Bordeaux **13** (2001), 111–124.

14. ———, *On the size of Diophantine m-tuples*, Math. Proc. Cambridge Philos. Soc. **132** (2002), 23–33.

15. ———, *There are only finitely many Diophantine quintuples*, J. reine Angew. Math. **566** (2004), 183–214.

16. A. Dujella, A. Filipin and C. Fuchs, *Effective solution of the $D(-1)$-quadruple conjecture*, Acta Arith. **128** (2007), 319–338.

17. A. Dujella and C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. **71** (2005), 33–52.

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

19. ———, *Integer points on a family of elliptic curves*, Publ. Math. Debrecen **56** (2000), 321–335.

20. A. Filipin, *Non-extendibility of $D(-1)$-triples of the form* $\{1, 10, c\}$, Internat. J. Math. Math. Sci. **35** (2005), 2217–2226.

21. Y. Fujita, *The extensibility of $D(-1)$-triples* $\{1, b, c\}$, Publ. Math. Debrecen **70** (2007), 103–117.

22. ———, *The extensibility of Diophantine pairs* $\{k-1, k+1\}$, J. Number Theory **128** (2008), 322–353.

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

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

24. M.J. Jacobson, Jr. and H.C. Williams, *Modular arithmetic on elements of small norm in quadratic fields*, Designs, Codes, Cryptography **27** (2002), 93–110.

25. A.W. Knapp, *Elliptic curves*, Princeton University Press, Princeton, 1992.

26. E.M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers.* II, Izv. Math. **64** (2000), 1217–1269.

27. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.

28. T. Nagell, *Introduction to number theory*, Wiley, New York, 1951.

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

30. SIMATH *manual*, Universität des Saarlandes, Saarbrücken, 1997.

31. R. Tamura, *Non-extendibility of* $D(-1)$*-triples* $\{1, b, c\}$, preprint.

32. G. Walsh, *The Pell equation and powerful numbers*, Master's thesis, The University of Calgary, Calgary, 1988.

Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan
Email address: fujita.yasutsugu@nihon-u.ac.jp