ACTA ARITHMETICA
128.4 (2007)

The $D(1)$-extensions of $D(-1)$-triples $\{1,2,c\}$ and integer points on the attached elliptic curves

by

YASUTSUGU FUJITA (Sendai)

1. Introduction. Diophantus noted 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. Fermat first found four positive integers with this property, which were $1,3,8,120$. Let n be a non-zero 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_ia_j+n is a perfect square for all i,j with $1\le i<j\le m$. Recently, Gibbs ([22]) found several examples of $D(n)$-sextuples.

In case $n=1$, Baker and Davenport ([2]) showed that if $\{1,3,8,d\}$ is a $D(1)$-quadruple, then $d=120$. This result has been generalized in three directions. First, Dujella ([7]) showed that if $\{k-1,k+1,4k,d\}$ with $k\ge 2$ is a $D(1)$-quadruple, then $d=4k(4k^2-1)$; secondly, Dujella and Pethő ([16]) showed that if $\{1,3,c,d\}$ is a $D(1)$-quadruple, then $d=c_{\nu-1}$ or $c_{\nu+1}$, where

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

and thirdly, Dujella ([9]) showed that if $\{F_{2k},F_{2k+2},F_{2k+4},d\}$, where $k\ge 1$ and F_ν denotes the νth Fibonacci number, is a $D(1)$-quadruple, then $d=4F_{2k+1}F_{2k+2}F_{2k+3}$ (this is called the Hoggatt–Bergum conjecture; see [24]). The first two results have been generalized to show that if $\{k-1,k+1,c,d\}$ is a $D(1)$-quadruple, then $c=c_{\nu-1}$ or $c_{\nu+1}$, where

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

(cf. [4] and [20]). In general, Dujella ([13]) showed that there does not exist a $D(1)$-sextuple and there exist only finitely many $D(1)$-quintuples. According

2000 *Mathematics Subject Classification*: Primary 11D09, 11G05; Secondary 11B37, 11J68, 11J86, 11Y50.

to the last results, it seems that one needs only a step to settle the long-standing conjecture which says that there does not exist a $D(1)$-quintuple. This conjecture is an immediate consequence of the following:

Conjecture 1.1 (cf. [1]). *If $\{a,b,c,d\}$ is a $D(1)$-quadruple, then $d = d_-$ or d_+, where*

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

The $D(1)$-quadruples $\{a,b,c,d_{\pm}\}$ are called *regular*. All the above $D(1)$-quadruples are regular.

In case $n = -1$, Dujella ([8]) showed that the pair $\{1,2\}$ cannot be extended to a $D(-1)$-quadruple. Moreover, Dujella and Fuchs ([15]) showed that no $D(-1)$-triple $\{a,b,c\}$ with $2 \le a < b < c$ can be extended to a $D(-1)$-quadruple. This immediately implies that there does not exist a $D(-1)$-quintuple. (For the results in the cases of $a = 1$ and $b \ge 5$, see [18], [19] and [34].) Recently, Dujella, Filipin and Fuchs ([14]) 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

(1.1) each of $ad+1$, $bd+1$ and $cd+1$ is a perfect square.

In fact, $d = d^-$ and d^+ have the property (1.1), where

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

(cf. [12, Lemma 3]; note that $d^- > 0$ if and only if $c > a + b + 2\sqrt{ab-1}$). This leads to the following definition:

Definition 1.2. Let $\{a,b,c\}$ be a $D(-1)$-triple. A set $\{a,b,c;d\}$ of positive integers is said to have the *property* $D(-1;1)$ (or to be a $D(1)$-*extension* of $\{a,b,c\}$) if each of $ad+1$, $bd+1$ and $cd+1$ is a perfect square.

Note that a $D(-1)$-triple $\{a,b,c\}$ can be extended to a $D(-1)$-quadruple $\{a,b,c,-d\}$ in the ring $\mathbb{Z}[i]$ of Gaussian integers (cf. [6, Example 1]), which corresponds to our quadruple $\{a,b,c;d\}$ having the property $D(-1;1)$. In a similar manner to the above-mentioned result (the Hoggatt–Bergum conjecture) on $D(1)$-triples $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$, we showed ([21]) that if $\{F_{2k+1}, F_{2k+3}, F_{2k+5}; d\}$ with $k \ge 0$ has the property $D(-1;1)$, then $D = 4F_{2k+2}F_{2k+3}F_{2k+4}$, which is another conjecture of Hoggatt and Bergum (cf. [24]).

In this paper, we show the following:

Theorem 1.3. *If the set $\{1,2,c;d\}$ has the property $D(-1;1)$, then d must be either of $s(3s \pm 2t)$, where $s = \sqrt{c-1}$ and $t = \sqrt{2c-1}$.*

In our notation, $s(3s \pm 2t) = d^{\pm}$, respectively. Our strategies are based on the ones in [16] and [8], except that we need to treat the cases $c < d$ and $c > d$ separately and apply a theorem of Rickert in each case (see Sections 2 and 3).

We next examine integer points on the attached elliptic curves. Let C_k $(k \geq 1)$ be the elliptic curve defined by

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

Along the same lines as in [11], we showed ([21]) that if the rank of C_k over $\mathbb{Q}$ equals one, then the integer points on C_k are

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

Similarly, let $\{1, 2, c\}$ be a $D(-1)$-triple and E the elliptic curve defined by

$$E_k : \quad y^2 = (x + 1)(2x + 1)(cx + 1). \tag{1.2}$$

Then, using Theorem 1.3 we show the following:

THEOREM 1.4. *Let $\{1, 2, c\}$ be a $D(-1)$-triple and E the elliptic curve given by* (1.2). *Assume that $c - 2$ is square-free and that the rank of E over $\mathbb{Q}$ equals two. Then the integer points on E are*

$$\begin{aligned} &(-1, 0), (0, \pm 1), \left(\frac{c-3}{2}, \pm s(c-2)\right), \\ &(s(3s - 2t), \pm(t - s)(2s - t)(st - c)), \\ &(s(3s + 2t), \pm(t + s)(2s + t)(st + c)), \end{aligned} \tag{1.3}$$

where $s = \sqrt{c-1}$ and $t = \sqrt{2c-1}$.

It is worthy of remark that E has the integer points $((c-3)/2, \pm s(c-2))$, neither trivial nor coming from $d^{\pm}$. This is a crucial difference from the result in [17], [10], [11] and [21]. The proof of Theorem 1.4 proceeds along the same lines as in [17]. On the way, we encounter a system (4.4) of equations, which has non-trivial solutions corresponding to $x = (c-3)/2$. We then prove that they are the only solutions of (4.4) in case $c - 2$ is square-free (see Proposition 4.9).

2. The case of $c < d$. Assume that $\{1, 2, c; d\}$ has the property $D(-1; 1)$. In this section, we will prove Theorem 1.3 for a certain c with $c < d$ (see Assumption 2.3). The assumption on c enables us to narrow the possibilities for fundamental solutions of the Diophantine equations (2.4) and (2.5) attached to $\{1, 2, c; d\}$.

2.1. *A lower bound for solutions.* Let s, t be positive integers such that

$$c - 1 = s^2, \qquad 2c - 1 = t^2.$$

Eliminating c, we obtain the Pell equation

$$t^2 - 2s^2 = 1. \tag{2.1}$$

Then we may write $s = \sigma_k$, where

$$\sigma_0 = 0, \quad \sigma_1 = 2, \quad \sigma_{k+2} = 6\sigma_{k+1} - \sigma_k; \tag{2.2}$$

hence we have

$$c = c_k = \frac{1}{8}\{(1+\sqrt{2})^{4k} + (1-\sqrt{2})^{4k} + 6\}. \tag{2.3}$$

Since [21, Theorem 1.3] contains the case $c = c_1 = 5$ of Theorem 1.3, we may assume that $c \geq c_2 = 145$. Let x, y, z be positive integers such that

$$d + 1 = x^2, \quad 2d + 1 = y^2, \quad cd + 1 = z^2.$$

Eliminating d, we obtain the system of simultaneous Diophantine equations

$$\begin{cases} z^2 - cx^2 = 1 - c, & (2.4) \\ 2z^2 - cy^2 = 2 - c. & (2.5) \end{cases}$$

LEMMA 2.1. *Let* (z, x), (z, y) *be positive solutions of* (2.4), (2.5), *respectively. Then there exist solutions* (z_0, x_0) *of* (2.4) *and* (z_1, y_1) *of* (2.5) *satisfying the following*:

$$0 < x_0 \leq \sqrt{c-1}, \qquad |z_0| \leq c - 1, \tag{2.6}$$

$$0 < y_1 \leq \sqrt{2(c-2)}, \qquad |z_1| \leq \sqrt{(c-1/2)(c-2)} < c - 1, \tag{2.7}$$

$$z + x\sqrt{c} = (z_0 + x_0\sqrt{c})(2c - 1 + 2s\sqrt{c})^m, \tag{2.8}$$

$$z\sqrt{2} + y\sqrt{c} = (z_1\sqrt{2} + y_1\sqrt{c})(4c - 1 + 2t\sqrt{2c})^n, \tag{2.9}$$

for some integers $m, n \geq 0$.

Proof. This lemma follows from [29, Theorem 108a]. ■

By (2.8) we may write $z = v_m$, where

$$v_0 = z_0, \quad v_1 = (2c-1)z_0 + 2scx_0, \quad v_{m+2} = 2(2c-1)v_{m+1} - v_m, \tag{2.10}$$

and by (2.9) we may write $z = w_n$, where

$$w_0 = z_1, \quad w_1 = (4c-1)z_1 + 2tcy_1, \quad w_{n+2} = 2(4c-1)w_{n+1} - w_n. \tag{2.11}$$

Hence, it is easy to verify by induction the following:

LEMMA 2.2 (cf. [8, Lemma 2]).

$$v_m \equiv (-1)^m(z_0 - 2cm^2z_0 - 2scmx_0) \pmod{8c^2},$$
$$w_n \equiv (-1)^n(z_1 - 4cn^2z_1 - 2tcny_1) \pmod{8c^2}.$$

In particular, we have

$$v_m \equiv (-1)^m z_0 \pmod{2c} \quad \text{and} \quad w_n \equiv (-1)^n z_1 \pmod{2c}.$$

Hence, $v_m = w_n$ together with (2.6) and (2.7) implies that

$$z_0 = z_1 \quad \text{and} \quad m \equiv n \pmod 2.$$

Suppose now the following:

ASSUMPTION 2.3. There exists an integer c' satisfying the following:

(2.12) If $\{1,2,c';d\}$ has the property $D(-1;1)$ with $d \neq d^- = s(3s-2t)$, then $c' < d$.

In what follows, let c' be an integer satisfying (2.12), and assume that $\{1,2,c';d\}$ has the property $D(-1;1)$ with $d \notin \{d^-, d^+\}$. We define $d_0 = (z_0^2-1)/c'$. Then $d_0 = x_0^2 - 1 \in \mathbb{Z}$ and $d_0 < ((c')^2-1)/c' < c'$. Furthermore, since $d_0+1 = x_0^2$, $2d_0+1 = y_1^2$ and $cd_0+1 = z_0^2$, the property (2.12) implies that $d_0 = 0$ or d^-. Hence we obtain

LEMMA 2.4. *If $v_m = w_n$ has a solution, then*

$$z_0 = z_1 = \pm 1 \ \text{or} \ \pm (s't' - c'),$$

where $s' = \sqrt{c'-1}$ and $t' = \sqrt{2c'-1}$.

LEMMA 2.5. *If $v_m = w_n$ has a solution, then $m \ge n$.*

Proof. One can prove this lemma in the same way as [13, Lemma 3]. ∎

LEMMA 2.6. *Assume that $c' \ge c_2 = 145$ and that either* (i) $v_{2m} = w_{2n}$ *or* (ii) $v_{2m+1} = w_{2n+1}$ *with $m \ge 1$ has a solution. Then*

$$0 < \Lambda := m_i \log\alpha_1 - n_i \log\alpha_2 + \log\alpha_3 < 1.1\alpha_1^{-2m_i} \tag{2.13}$$

for $i = 1$ (resp. 2) in the case of (i) *(resp.* (ii)), *where*

$$m_1 = 2m, \quad n_1 = 2n, \quad m_2 = 2m+1, \quad n_2 = 2n+1,$$

$$\alpha_1 = 2c' - 1 + 2s'\sqrt{c'}, \quad \alpha_2 = 4c' - 1 + 2t'\sqrt{2c'}, \quad \alpha_3 = \frac{(z_0 + x_0\sqrt{c'})\sqrt{2}}{z_1\sqrt{2} + y_1\sqrt{c'}}.$$

Proof. By (2.10) and (2.11), we have

$$v_m = \frac{1}{2}\{(z_0 + x_0\sqrt{c'})(2c'-1+2s'\sqrt{c'})^m + (z_0 - x_0\sqrt{c'})(2c'-1-2s'\sqrt{c'})^m\},$$

$$w_n = \frac{1}{2\sqrt{2}}\{(z_1\sqrt{2} + y_1\sqrt{c'})(4c'-1+2t'\sqrt{2c'})^n + (z_1\sqrt{2} - y_1\sqrt{c'})(4c'-1-2t'\sqrt{2c'})^n\}.$$

Since the exponential equations can be transformed to a logarithmic inequality in the standard way (see, e.g., [16, Lemma 3]), we omit the proof. ∎

It is not difficult to deduce from the inequality (2.13) the following:

$$m_i \log\alpha_1 - n_i \log\alpha_2 < 0 \quad (i = 1,2).$$

This implies that

$$\frac{m_i}{n_i} < \frac{\log \alpha_2}{\log \alpha_1} = \frac{\log(\sqrt{2c'-1}+\sqrt{2c'})}{\log(\sqrt{c'-1}+\sqrt{c'})} =: \xi(c').$$

Since $\xi(c')$ is decreasing and $\xi(c') \le \xi(145) < 1.11$, we conclude that

$$m_i < 1.11 n_i \quad (i = 1, 2) \tag{2.14}$$

whenever $m \ge n \ge 1$ and $c' \ge c_2 = 145$.

Lemma 2.7. *On the assumptions of Lemma* 2.6, *the following hold for* $i = 1, 2$:

(i) *If* $z_0 = z_1 = \pm 1$, *then* $m_i \ge n_i \ge 0.1518\sqrt{c'}$.
(ii) *If* $z_0 = z_1 = \pm(s't' - c')$, *then* $m_i \ge n_i \ge 0.4675\sqrt[4]{c'}$.

Proof. (i) By Lemma 2.2, we have

$$\pm m_i^2 + m_i s' \equiv \pm 2n_i^2 + n_i t' \pmod{4c'}. \tag{2.15}$$

Suppose that $n_i < 0.1518\sqrt{c'}$. Then by (2.14) we have

$$|\pm m_i^2 + m_i s'| < 1.11 \cdot 0.1518 c' \left(1.11 \cdot 0.1518 + \sqrt{1 - \frac{1}{c'}}\right) < 2c',$$

$$|\pm 2n_i^2 + n_i t'| < 0.1518 c' \left(2 \cdot 0.1518 + \sqrt{2 - \frac{1}{c'}}\right) < 2c'.$$

It follows from (2.15) that

$$\pm m_i^2 + m_i s' = \pm 2n_i^2 + n_i t'. \tag{2.16}$$

We now have

$$\pm m_i^2 + m_i s' < \left(1.11 \cdot 0.1518\sqrt{\frac{c'}{c'-1}} + 1\right) m_i s' < 1.1691 m_i s',$$

$$\pm 2n_i^2 + n_i t' > \left(1 - 0.3036\sqrt{\frac{c'}{2c'-1}}\right) n_i t' > 0.7849 n_i t'.$$

If (2.16) holds with the plus signs, then

$$\frac{m_i}{n_i} > \frac{t'}{1.1691 s'} > \frac{\sqrt{2}}{1.1691} > 1.2,$$

which contradicts (2.14). If (2.16) holds with the minus signs, then

$$\frac{m_i}{n_i} > \frac{0.7849 t'}{s'} > 0.7849\sqrt{2} > 1.11,$$

which is also a contradiction. Therefore, $n_i \ge 0.1518\sqrt{c'}$.

(ii) By Lemma 2.2,

$$(\pm(m_i^2 - 2n_i^2) + m_i - 2n_i)s't' \equiv -(m_i - n_i) \pmod{c'}. \tag{2.17}$$

Multiplying (2.17) by s', we have

$$(\pm(m_i^2 - 2n_i^2) + m_i - 2n_i)t' \equiv (m_i - n_i)s' \pmod{c'}; \tag{2.18}$$

multiplying (2.17) by t', we obtain

$$(\pm(m_i^2 - 2n_i^2) + m_i - 2n_i)s' \equiv (m_i - n_i)t' \pmod{c'}. \tag{2.19}$$

Suppose now that $n_i < 0.4675\sqrt[4]{c'}$. Then

$$\begin{aligned} |(\pm(m_i^2 - 2n_i^2) + m_i - 2n_i)t'| &< n_i(n_i+1)\sqrt{2c'} \\ &< 0.4675\sqrt{2}\Big(0.4675 + \frac{1}{\sqrt[4]{c'}}\Big)c' < \frac{c'}{2}, \\ |(m_i - n_i)t'| < 0.11 n_i t' &< 0.11 \cdot 0.4675\sqrt{2}c' < \frac{c'}{2}. \end{aligned}$$

It follows from (2.18) and (2.19) that

$$(\pm(m_i^2 - 2n_i^2) + m_i - 2n_i)t' = (m_i - n_i)s', \tag{2.20}$$

$$(\pm(m_i^2 - 2n_i^2) + m_i - 2n_i)s' = (m_i - n_i)t'. \tag{2.21}$$

(2.20) and (2.21) together imply that $(m_i - n_i)((s')^2 - (t')^2) = 0$. It follows from $s' \neq \pm t'$ that $m_i = n_i$. Substituting this into (2.20), we conclude that $(\pm n_i + 1)n_i t' = 0$, which is a contradiction. ∎

2.2. *Application of a theorem of Rickert and the reduction method.* In this section, applying a theorem of Rickert we will prove that $c' \leq c_3 = 4901$ (see Proposition 2.11) and then, using the reduction method based on the Baker–Davenport lemma (cf. [2]) we will complete the disproof of Assumption 2.3.

LEMMA 2.8. *Let*

$$\theta_1 = \sqrt{1 - 1/N}, \qquad \theta_2 = \sqrt{1 + 1/N}, \qquad N = (t')^2.$$

The positive solutions (x, y, z) of the system of equations (2.4) *and* (2.5) *satisfy*

$$\max\bigg\{\bigg|\theta_1 - \frac{2s'x}{t'y}\bigg|, \bigg|\theta_2 - \frac{2z}{t'y}\bigg|\bigg\} < y^{-2}.$$

Proof. This is exactly [8, Lemma 6]. ∎

THEOREM 2.9 (cf. [32], [33]). *Let $N \geq 26$ be an integer. Then*

$$\theta_1 = \sqrt{1 - 1/N} \quad \textit{and} \quad \theta_2 = \sqrt{1 + 1/N}$$

satisfy

$$\max\{|\theta_1 - p_1/q|, |\theta_2 - p_2/q|\} > cq^{-1-\lambda} \tag{2.22}$$

for all integers p_1, p_2, q with $q > 0$, where $c = (181N)^{-1}$ and

$$\lambda = \frac{\log(12\sqrt{3}\,N + 24)}{\log(27(N^2 - 1)/32)} \; (< 1).$$

Proof. This is a slight modification of [32, Theorem] following immediately from the remark in [3, p. 186], which says that one can replace the term $m+1$ by m in the expression

$$c^{-1} = 2(m+1)pdVC^{\lambda}f^{-1}$$

in [32, Lemma 2.1]. Since

$$m=2, \quad p=11/4, \quad d=1, \quad V \le 12N(\sqrt{3}+1), \quad C=1, \quad f=2,$$

we obtain

$$c = \frac{1}{2pV} \ge \frac{1}{66N(1+\sqrt{3})} > \frac{1}{181N}. \ \blacksquare$$

LEMMA 2.10. *On the assumptions of Lemma* 2.6, *the following hold*:

(i) *If* $z_0 = z_1 = \pm 1$, *then* $\log y > (0.1518\sqrt{c'}-1)\log(4c'-3)$.
(ii) *If* $z_0 = z_1 = \pm(s't'-c')$, *then* $\log y > (0.4675\sqrt[4]{c'}-1)\log(4c'-3)$.

Proof. By (2.8), we may write $x = u_m$, where

$$u_0 = x_0, \quad u_1 = (2c'-1)x_0 + 2s'z_0, \quad u_{m+2} = 2(2c'-1)u_{m+1} - u_m;$$

hence for some $m_i \ge 2$ with $i \in \{1,2\}$, we have

$$x = \frac{1}{2\sqrt{c'}}\{(z_0 + x_0\sqrt{c'})(2c'-1+2s'\sqrt{c'})^{m_i} - (z_0 - x_0\sqrt{c'})(2c'-1-2s'\sqrt{c'})^{m_i}\}.$$

(i) In this case, we have

$$\begin{aligned} y &\ge x \\ &= \frac{1}{2\sqrt{c'}}\{(\sqrt{c'}\pm 1)(2c'-1+2s'\sqrt{c'})^{m_i} + (\sqrt{c'}\mp 1)(2c'-1-2s'\sqrt{c'})^{m_i}\} \\ &> \frac{(\sqrt{c'}-1)(4c'-3)^{m_i}}{2\sqrt{c'}} > (4c'-3)^{m_i-1}. \end{aligned}$$

It follows from Lemma 2.7 that

$$\log y > (m_i - 1)\log(4c'-3) > (0.1518\sqrt{c'}-1)\log(4c'-3).$$

(ii) In the same way as in (i), we see that $y > (4c'-3)^{m_i-1}$, and from Lemma 2.7 that

$$\log y > (0.4675\sqrt[4]{c'}-1)\log(4c'-3). \ \blacksquare$$

We are now ready to bound c'.

PROPOSITION 2.11. *Let* c' *be an integer satisfying* (2.12). *Assume that* $\{1,2,c';d\}$ *has the property* $D(-1;1)$ *with* $d \ne s'(3s' \pm 2t')$ $(= d^{\pm})$.

(i) *If* $z_0 = z_1 = \pm 1$, *then* $c' = 145$.
(ii) *If* $z_0 = z_1 = \pm(s't'-c')$, *then* $c' = 145$ *or* 4901.

Proof. As mentioned just after (2.3), we may assume that $c' \geq c_2$. In case $m_1 = 0$, we have $z = 1$ or $s't' - c'$, that is, $d = 0$ or $s'(3s' - 2t')$ $(= d^-)$. In case $m_2 = 1$, if $z_0 = z_1 = -(s't' - c')$, then $z = s't' + c'$, that is, $d = s'(3s' + 2t')$ $(= d^+)$; otherwise,

$$\begin{aligned}(v_0 =)\ w_0 = z_0 < v_1 = (2c' - 1)z_0 + 2s'c'x_0 \\ < w_1 = (4c' - 1)z_0 + 2t'c'y_1 < w_2 < \cdots .\end{aligned}$$

Hence $m_i \geq 2$ for $i = 1, 2$ and we may apply Lemma 2.10.

Letting

$$N = (t')^2 = 2c' - 1, \quad p_1 = 2s'x, \quad p_2 = 2z, \quad q = t'y,$$

we see from Lemma 2.8 and Theorem 2.9 that $(181(t')^2)^{-1}(t'y)^{-1-\lambda} < y^{-2}$, that is,

$$y^{1-\lambda} < 181(t')^{3+\lambda} < (26.91c')^2.$$

Since

$$\frac{1}{1-\lambda} = \frac{\log \frac{27((t')^2-1)}{32}}{\log \frac{27((t')^2-1)}{32(12\sqrt{3}(t')^2+24)}} < \frac{2\log(1.838c')}{\log(0.08118c')},$$

we have

$$\log y < \frac{4\log(1.838c')\log(26.91c')}{\log(0.08118c')}.$$

(i) Suppose that $c' \geq c_3 = 4901$. Lemma 2.10 implies that

$$0.1518\sqrt{c'} - 1 < \frac{4\log(1.838c')\log(26.91c')}{\log(4c'-3)\log(0.08118c')} =: f(c').$$

Since f is decreasing, we have $f(c') \leq f(c_3) < 8$. On the other hand,

$$0.1518\sqrt{c'} - 1 \geq 0.1518\sqrt{c_3} - 1 > 9,$$

which is a contradiction. Hence we obtain $c' = c_2$.

(ii) Suppose that $c' \geq c_4 = 166465$. In the same way as in (i), we would have

$$8 < 0.4675\sqrt[4]{c'} - 1 < f(c') < 7,$$

which is a contradiction. Hence we obtain $c' = c_2$ or c_3. ∎

In order to bound m_i, we need the following theorem due to Matveev:

THEOREM 2.12 (cf. [27]). *Let Λ be a linear form in logarithms of l multiplicatively independent totally real algebraic numbers $\alpha_1, \ldots, \alpha_l$ with rational integer coefficients $b_1, \ldots, b_l$ $(b_l \neq 0)$. Let $h(\alpha_j)$ denote the absolute logarithmic height of α_j for $1 \leq j \leq l$. Define the numbers D, A_j $(1 \leq j \leq l)$ and B by $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_l) : \mathbb{Q}]$, $A_j = \max\{Dh(\alpha_j), |\log \alpha_j|\}$, $B = \max\{1, \max\{|b_j|A_j/A_l;\ 1 \leq j \leq l\}\}$. Then*

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

where

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

We apply Theorem 2.12 with

$$l = 3, \quad D = 4, \quad b_1 = m_i, \quad b_2 = -n_i, \quad b_3 = 1,$$

and the same symbols α_1, α_2, α_3. We have

$$h(\alpha_1) = \frac{1}{2}\log\alpha_1 < \frac{1}{2}\log(4c'),$$
$$h(\alpha_2) = \frac{1}{2}\log\alpha_2 < \frac{1}{2}\log(8c'),$$
$$h(\alpha_3) = \frac{1}{4}\log(c'-2)^2\,\frac{(x_0\sqrt{c'}+z_0)\sqrt{2}}{y_1\sqrt{c'}+z_1\sqrt{2}} \cdot \frac{(x_0\sqrt{c'}-z_0)\sqrt{2}}{y_1\sqrt{c'}-z_1\sqrt{2}}$$
$$= \frac{1}{4}\log(2(c'-1)(c'-2)).$$

Hence we obtain the following:

$$A_1 < 2.56\log c', \quad A_2 < 2.84\log c', \quad 2\log c' < A_3 < 2.14\log c';$$
$$B \le \max\left\{\frac{m_i \cdot 2.56}{2}, \frac{n_i \cdot 2.84}{2}, 1\right\} \le 1.42 m_i;$$
$$C(3) = \frac{8}{2!}\cdot 5 \cdot 9(16e)^4 < 6.45 \cdot 10^8;$$
$$C_0 = \log(e^{4.4\cdot 3+7} \cdot 3^{5.5} \cdot 16\log(4e)) < 29.9;$$
$$W_0 = \log(1.5eB \cdot 4\log(4e)) < \log(56 m_i);$$
$$\Omega = A_1A_2A_3 < 2.56 \cdot 2.84 \cdot 2.14(\log c')^3 < 15.6(\log c')^3.$$

It follows from Theorem 2.12 that

$$\log\Lambda > -4.9 \cdot 10^{12}\log(56m_i)(\log c')^2. \tag{2.23}$$

The inequalities (2.13) and (2.23) together imply that

$$\psi(m_i) := \frac{2m_i - 1}{\log(56m_i)} < 4.9 \cdot 10^{12}(\log c')^2.$$

Since $c' \le c_3 = 4901$ in any case, we have $\psi(m_i) < 3.6 \cdot 10^{14}$. It follows from $\psi(8\cdot 10^{15}) > 3.9 \cdot 10^{14}$ that $m_i < 8 \cdot 10^{15}$ for $i = 1, 2$.

Dividing the inequality (2.13) by $\log\alpha_2$, we have

$$0 < m_i\kappa - n_i + \mu < AB^{-m_i} \quad (i = 1, 2), \tag{2.24}$$

where

$$\kappa = \frac{\log \alpha_1}{\log \alpha_2}, \qquad \mu = \frac{\log \alpha_3}{\log \alpha_2}, \qquad A = \frac{1.1}{\log \alpha_2}, \qquad B = \alpha_1^2.$$

The following is a variant of the Baker–Davenport lemma:

LEMMA 2.13 ([16, Lemma 5]). *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* (2.24) *has no solution in the range*

$$\frac{\log(Aq/\varepsilon)}{\log B} \le |m_i| \le M.$$

(2) *If $p - q + r = 0$, then* (2.24) *has no solution in the range*

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

We apply Lemma 2.13 with $M = 8 \cdot 10^{15}$. Note that $m_i \ge 2$. We have to examine $2 \cdot 2 + 2 = 6$ cases. In each case of $c' = c_2 = 145$, the first step of reduction gives $m_i \le 3$, and the second step gives $m_i \le 1$, which is a contradiction. In each case of $c' = c_3 = 4901$, the first step of reduction gives $m_i \le 1$, which is a contradiction. This completes the disproof of Assumption 2.3.

3. The case of $c > d$. In this section, we will complete the proof of Theorem 1.3. Suppose that $\{1, 2, c; d\}$ has the property $D(-1; 1)$ with $d \notin \{d^-, d^+\}$. In view of Section 2, there exists an integer $d_1 < c$ with $d_1 \ne d^-$ such that $\{1, 2, c; d_1\}$ has the property $D(-1; 1)$. Throughout this section,

> let d' be the minimal integer among the d's such that $\{1, 2, c; d\}$ has the property $D(-1; 1)$ with $d \notin \{d^-, d^+\}$ for some c.

Then we have $d' < c$. The minimality of d' enables us to narrow the possibilities for fundamental solutions of the Diophantine equations (3.1) and (3.2) attached to $\{1, 2, c; d\}$.

3.1. *Lower bounds for solutions.* Let x' and y' be positive integers such that

$$d' + 1 = (x')^2 \quad \text{and} \quad 2d' + 1 = (y')^2.$$

Eliminating d', we have

$$(y')^2 - 2(x')^2 = -1.$$

Then we may write $x' = u'_k$, where

$$u'_0 = 1, \quad u'_1 = 5, \quad u'_{k+2} = 6u'_{k+1} - u'_k;$$

hence we have

$$d' = d_k = \tfrac{1}{8}\{(1+\sqrt{2})^{4k+2} + (1-\sqrt{2})^{4k+2} - 6\}.$$

Note that $d' \geq d_1 = 24$. Let s, t, z be positive integers such that

$$c - 1 = s^2, \quad 2c - 1 = t^2, \quad cd' + 1 = z^2.$$

Eliminating c, we obtain the system of simultaneous Diophantine equations

$$\begin{cases} z^2 - d's^2 = 1 + d', & (3.1)\\ 2z^2 - d't^2 = 2 + d'. & (3.2) \end{cases}$$

Lemma 3.1. *Let* (z,s), (z,t) *be positive solutions of* (3.1), (3.2), *respectively. Then, there exist solutions* (z'_0, s_0) *of* (3.1) *and* (z'_1, t_1) *of* (3.2) *satisfying the following*:

$$|s_0| \leq \frac{x'}{\sqrt{2(x'+1)}} < \sqrt[4]{d'}, \qquad 0 < z'_0 \leq x'\sqrt{\frac{x'+1}{2}} < d', \tag{3.3}$$

$$|t_1| \leq \sqrt{\frac{d'+2}{y'+1}} < \sqrt[4]{d'}, \qquad 0 < z'_1 \leq \frac{\sqrt{(y'+1)(d'+2)}}{2} < d', \tag{3.4}$$

$$z + s\sqrt{d'} = (z'_0 + s_0\sqrt{d'})(x' + \sqrt{d'})^m, \tag{3.5}$$

$$z\sqrt{2} + t\sqrt{d'} = (z'_1\sqrt{2} + t_1\sqrt{d'})(y' + \sqrt{2d'})^n \tag{3.6}$$

for some integers $m, n \geq 0$.

Proof. This follows from [29, Theorem 108]. ■

By (3.5) we may write $z = p_m$, where

$$p_0 = z'_0, \quad p_1 = x'z'_0 + d's_0, \quad p_{m+2} = 2x'p_{m+1} - p_m, \tag{3.7}$$

and by (3.6) we may write $z = q_n$, where

$$q_0 = z'_1, \quad q_1 = y'z'_1 + d't_1, \quad q_{n+2} = 2y'q_{n+1} - q_n. \tag{3.8}$$

Lemma 3.2.

(1) $p_{2m} \equiv z'_0 + 2d'(m^2 z'_0 + mx's_0) \pmod{8(d')^2}$.
(2) $p_{2m+1} \equiv x'z'_0 + d'\{2m(m+1)x'z'_0 + (2m+1)s_0\} \pmod{4(d')^2}$.
(3) $q_{2n} \equiv z'_1 + 2d'(2n^2 z'_1 + ny't_1) \pmod{8(d')^2}$.
(4) $q_{2n+1} \equiv y'z'_1 + d'\{4n(n+1)y'z'_1 + (2n+1)t_1\} \pmod{4(d')^2}$.

Proof. One can prove this lemma in the same way as [16, Lemma 2]. ■

Lemma 3.3. *The equations* $p_{2m+1} = q_{2n}$ *and* $p_{2m} = q_{2n+1}$ *have no solutions. Moreover, we have the following*:

(i) *If* $p_{2m} = q_{2n}$ *has a solution, then* $z'_0 = z'_1 = x'$.
(ii) *If* $p_{2m+1} = q_{2n+1}$ *has a solution, then* $z'_0 = y'$ *and* $z'_1 = x'$.

Proof. In the case of $d' = d_2 = 24$, the positive solutions of (3.1) and (3.2) are given by

$$z + 2s\sqrt{6} = 5(5+2\sqrt{6})^m \text{ or } (7 \pm 2\sqrt{6})(5+2\sqrt{6})^m,$$
$$z + 2t\sqrt{3} = (5 \pm 2\sqrt{3})(7+4\sqrt{3})^n.$$

Considering the sequences (p_m) and (q_n) modulo 8, one can easily see that the assertions hold with

$$\text{(i) } z_0' = z_1' = 5\ (= x'), \qquad \text{(ii) } z_0' = 7\ (= y'),\ z_1' = 5\ (= x').$$

In the following, assume that $d' \geq d_3 = 840$.

Suppose first that $p_{2m+1} = q_{2n}$ has a solution. Since (z_0', s_0) is a solution of (3.1) and $z_0' > 0$, we have $z_0' \geq x'$. Suppose that $z_0' > x'$. Then a similar argument to the proof of [16, Lemma 1(2)] will lead us to a contradiction. Hence $z_0' = x'$. Then we see that $s_0 = 0$ and from Lemma 3.2 that

$$z_1' \equiv (x')^2 = d' + 1 \pmod{2d'},$$

which contradicts (3.4). Therefore, $p_{2m+1} = q_{2n}$ has no solution.

Secondly, suppose that $p_{2m} = q_{2n+1}$ has a solution. Since (z_1', t_1) is a solution of (3.2), and $z_1' > 0$ and $t_1 \neq 0$, we have $z_1' \geq x'$. Suppose that $z_1' > x'$. Then a similar argument to the proof of [16, Lemma 1(3)] will lead us to a contradiction. Hence $z_1' = x'$. Then we see that $t_1 = \pm 1$ and from Lemma 3.2 that

$$z_0' \equiv y' z_1' \pmod{d'},$$

and using (3.3) we arrive at a contradiction. Therefore, $p_{2m} = q_{2n+1}$ has no solution.

(i) Assume that $p_{2m} = q_{2n}$ has a solution. By Lemma 3.2 we have $z_0' \equiv z_1' \pmod{2d'}$, which together with (3.3) and (3.4) implies that $z_0' = z_1'$. Put $c_0' = ((z_0')^2 - 1)/d'$. Then either $c_0' = 1$ or $\{1, 2, c_0'; d'\}$ has the property $D(-1;1)$. If the latter holds, then we arrive at a contradiction. Therefore, $c_0' = 1$ and $z_0' = z_1' = x'$.

(ii) Assume that $p_{2m+1} = q_{2n+1}$ has a solution. By Lemma 3.2 we have $x'z_0' \equiv y'z_1' \pmod{d'}$, which together with (3.3) and (3.4) implies that

$$x'z_0' - d'|s_0| = y'z_1' - d'|t_1|. \tag{3.9}$$

Put $c_0'' = ((x'z_0' - d'|s_0|)^2 - 1)/d'$. Then $\{1, 2, c_0''; d'\}$ has the property $D(-1;1)$. If $d' \neq d^+$, then we arrive at a contradiction. Hence $d' = d^+$ and $c_0'' = x'(3x' - 2y')$. Then $c_0''d' + 1 = (x'z_0' - d'|s_0|)^2$ implies that

$$x'y' - d' = x'z_0' - d'|s_0|, \tag{3.10}$$

that is, $d'(|s_0| - 1) = x'(z_0' - y')$. Since $\gcd(d', x') = 1$, we have $|s_0| \equiv 1 \pmod{x'}$. It follows from (3.3) that $|s_0| = 1$ and $z_0' = y'$. By (3.9) and (3.10) we also have $d'(|t_1| - 1) = y'(z_1' - x')$. Since $\gcd(d', y') = 1$, we have $|t_1| \equiv 1$

$(\mathrm{mod}\, y')$. It follows from (3.4) that $|t_1| = 1$ and $z_1 = x'$. This completes the proof of Lemma 3.3. ∎

LEMMA 3.4. *If $p_m = q_n$ has a solution, then $n \le m \le 2n$.*

Proof. One can prove this lemma in the same way as [13, Lemma 3]. ∎

LEMMA 3.5.
(i) *If $p_{2m} = q_{2n}$ has a solution with $m \ge n \ge 1$, then $n > 0.418\sqrt[4]{d'}$.*
(ii) *If $p_{2m+1} = q_{2n+1}$ has a solution with $m \ge n \ge 1$, then $n > 0.413\sqrt[4]{d'}$.*

Proof. One can prove this lemma in the same way as [8, Lemma 5] for (i) and as [16, Lemma 4(2)] for (ii). ∎

3.2. *Application of a theorem of Rickert and the reduction method.* In this section, applying a theorem of Rickert we will prove that $d' \le d'_4 = 28560$ (see Proposition 3.8), and then using the reduction method we will complete the proof of Theorem 1.3.

LEMMA 3.6. *Let*

$$\theta_1 = \sqrt{1 - 1/N}, \qquad \theta_2 = \sqrt{1 + 1/N}, \qquad N = (y')^2.$$

The positive solutions (s, t, z) of the system of equations (3.1) and (3.2) satisfy

$$\max\left\{\left|\theta_1 - \frac{2z}{y't}\right|, \left|\theta_2 - \frac{2x's}{y't}\right|\right\} < t^{-2}.$$

Proof. One can prove this lemma in the same way as [8, Lemma 6]. ∎

LEMMA 3.7.
(i) *If $p_{2m} = q_{2n}$ has a solution with $m \ge n \ge 1$, then*

$$\log t > (0.418\sqrt[4]{d'} - 1/2)\log(4d').$$

(ii) *If $p_{2m+1} = q_{2n+1}$ has a solution with $m \ge n \ge 1$, then*

$$\log t > 0.413\sqrt[4]{d'}\log(4d').$$

Proof. By (3.5) we may write $s = p'_m$, where

$$p'_m = \frac{1}{2\sqrt{d'}}\{(z'_0 + s_0\sqrt{d'})(x' + \sqrt{d'})^m - (z'_0 - s_0\sqrt{d'})(x' - \sqrt{d'})^m\};$$

hence we see that $t > s\sqrt{2} > (x' + \sqrt{d'})^m$. The lemma follows from this inequality and Lemma 3.5. ∎

We are now ready to bound d'.

PROPOSITION 3.8. *Suppose that d' is the minimal positive integer among the d's such that $\{1, 2, c; d\}$ has the property $D(-1; 1)$ with $d \notin \{d^-, d^+\}$ for some c. Then*

$$d' = 24,\ 840 \ \text{or}\ 28560.$$

Proof. In case $n = 0$, we have $z = x'$, that is, $c = 1$. In case $n = 1$, we have $z = x'y' \pm d'$, that is, $c = x'(3x' \pm 2y')$ and $d' = s(3s \mp 2t)$, which are d^- and d^+, respectively. Hence $n \geq 2$ and we may apply Lemma 3.7.

Letting

$$N = (y')^2 = 2d' + 1, \quad p_1 = 2z, \quad p_2 = 2x's, \quad q = y't,$$

we see from Lemma 3.6 and Theorem 2.9 that

$$t^{1-\lambda} < 181(y')^{3+\lambda} < (27.47d')^2.$$

Hence

$$\log t < \frac{4\log(1.875d')\log(27.47d')}{\log(0.08091d')}.$$

Suppose that $d' \geq d_4 = 970224$.

(i) Lemma 3.7 implies that

$$0.418\sqrt[4]{d'} - \frac{1}{2} < \frac{4\log(1.875d')\log(27.47d')}{\log(4d')\log(0.08091d')} =: f(d').$$

Since f is decreasing, we have $f(d') \leq f(d_4) < 6$. On the other hand,

$$0.418\sqrt[4]{d'} - 1/2 \geq 0.418\sqrt[4]{d_4} - 1/2 > 12,$$

which is a contradiction.

(ii) In the same way as in (i), we would have

$$12 < 0.413\sqrt[4]{d'} < f(d') < 6,$$

which is a contradiction. In any case, we obtain $d' \leq d_3 = 28560$. ∎

LEMMA 3.9. *Assume that either* (i) $p_{2m} = q_{2n}$ *or* (ii) $p_{2m+1} = q_{2n+1}$ *with* $m \geq n \geq 1$ *has a solution. Then*

$$0 < \Lambda' := n_i \log\alpha_1' - m_i \log\alpha_2' + \log\alpha_3' < 0.7(\alpha_1')^{-n_i} \tag{3.11}$$

for $i = 1$ (*resp.* 2) *in the case of* (i) (*resp.* (ii)), *where*

$$m_1 = 2m, \quad n_1 = 2n, \quad m_2 = 2m+1, \quad n_2 = 2n+1,$$

$$\alpha_1' = y' + \sqrt{2d'}, \quad \alpha_2' = x' + \sqrt{d'}, \quad \alpha_3' = \frac{z_1'\sqrt{2} + t_1\sqrt{d'}}{(z_0' + s_0\sqrt{d'})\sqrt{2}}.$$

Proof. One can prove this lemma in the standard way. ∎

We apply Theorem 2.12 with

$$l = 3, \quad D = 4, \quad b_1 = n_i, \quad b_2 = -m_i, \quad b_3 = 1,$$

and $\alpha_1 = \alpha_1'$, $\alpha_2 = \alpha_2'$, $\alpha_3 = \alpha_3'$. Then we obtain the following:

$$A_1 < 1.17\log d', \quad A_2 < 1.12\log d', \quad 2\log d' < A_3 < 2.37\log d',$$

$$B \leq 1.12n_i, \quad C(3) < 6.45\cdot 10^8, \quad C_0 < 29.9,$$

$$W_0 < \log(44n_i), \quad \Omega < 3.11(\log d')^3.$$

It follows from Theorem 2.12 that

$$\log \Lambda' > -9.6 \cdot 10^{11} \log(44n_i)(\log d')^3. \tag{3.12}$$

The inequalities (3.11) and (3.12) together imply that

$$\psi(n_i) := \frac{n_i - 1}{\log(44n_i)} < 2 \cdot 10^{12} (\log d')^2.$$

Since $d' \le d_3 = 28560$, we have $\psi(n_i) < 2.2 \cdot 10^{14}$. It follows from $\psi(9 \cdot 10^{15}) > 2.2 \cdot 10^{14}$ that $n_i < 9 \cdot 10^{15}$ for $i = 1, 2$.

Dividing the inequality (3.11) by $\log \alpha_2'$, we obtain

$$0 < n_i \kappa' - m_i + \mu' < A'(B')^{-n_i} \qquad (i = 1, 2), \tag{3.13}$$

where

$$\kappa' = \frac{\log \alpha_1'}{\log \alpha_2'}, \qquad \mu' = \frac{\log \alpha_3'}{\log \alpha_2'}, \qquad A' = \frac{0.7}{\log \alpha_2'}, \qquad B' = \alpha_1'.$$

We apply Lemma 2.13 with $M = 9 \cdot 10^{15}$ for m_i and n_i interchanged. We have to examine $2 \cdot 3 + 4 \cdot 3 = 18$ cases (note that in the case of $(z_0', z_1') = (y', x')$, the signs of $s_0 = \pm 1$ and $t_1 = \pm 1$ are taken independently; hence there are four cases for each d'). The second convergent is needed in only one case. In each case of $d' = 24$, the second or third step of reduction gives $n_i \le 1$, which is a contradiction; in each case of $d' = 840$, the second step gives $n_i \le 1$, which is a contradiction; and in each case of $d' = 28560$, the first step gives $n_i \le 6$, which contradicts Lemma 3.5. This completes the proof of Theorem 1.3.

4. Integer points on the attached elliptic curves.

4. Integer points on the attached elliptic curves. In this section, we prove Theorem 1.4.

Let $\{1, 2, c\}$ $(c = c_k)$ be a $D(-1)$-triple and E the elliptic curve given by

$$E = E_k : \quad y^2 = (x + 1)(2x + 1)(cx + 1).$$

The coordinate transformation

$$x \mapsto \frac{x}{2c}, \qquad y \mapsto \frac{y}{2c}$$

leads to the elliptic curve

$$E' = E_k' : \quad y^2 = (x + 2c)(x + c)(x + 2).$$

E' has the following trivial $\mathbb{Q}$-rational points besides the point at infinity O:

$$A = (-2c, 0), \qquad B = (-c, 0), \qquad C = (-2, 0),$$
$$P = (0, 2c), \qquad R = (st + s + t - 1, (s + t)(s + 1)(t + 1)).$$

Note that if $k = 1$, then $P + R = C$. The following lemma is useful for examining whether a point in $E'(\mathbb{Q})$ is divisible by 2 in $E'(\mathbb{Q})$.

LEMMA 4.1 (cf. [26, Theorem 4.2, p. 85]). *Let C be an elliptic curve over $\mathbb{Q}$ given by*

$$C: \quad y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

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

LEMMA 4.2. *The torsion group $E'(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

Proof. If $E'(\mathbb{Q}) \supset \mathbb{Z}/4\mathbb{Z}$, then Lemma 4.1 implies that $2(c-1)$ must be a perfect square, which contradicts $c - 1 = s^2$. Hence, $E'(\mathbb{Q}) \not\supset \mathbb{Z}/4\mathbb{Z}$. Suppose that $E'(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. [31, Main Theorem 1] implies that there exist integers α, β with $\alpha/\beta \notin \{-2, -1, -1/2, 0, 1\}$ and $\gcd(\alpha, \beta) = 1$ such that

$$c - 2 = \alpha^4 + 2\alpha^3\beta, \qquad 2(c-1) = \beta^4 + 2\alpha\beta^3.$$

Adding these two equalities, we have

$$3c - 4 = (\alpha^2 + \alpha\beta + \beta^2)^2 - 3\alpha^2\beta^2. \tag{4.1}$$

While the left-hand side is congruent to 3 or 7 modulo 8 (since $s \equiv 0 \pmod 2$ and $c \equiv 1$ or $5 \pmod 8$), the right-hand side is congruent to $0, 1, 5$ or 6 modulo 8, which is a contradiction. It follows from Mazur's theorem (cf. [28]) that $E'(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. ∎

LEMMA 4.3. *$P, P + A, P + B, P + C \notin 2E'(\mathbb{Q})$.*

Proof. We have

$$\begin{aligned} P + A &= (-c-1, -c+1), \\ P + B &= (-2c+2, 2c-4), \\ P + C &= (c^2 - 3c, -c^3 + 3c^2 - 2c). \end{aligned}$$

By Lemma 4.1, if Lemma 4.3 is not valid, then at least one of the following must be a perfect square:

$$2, \quad -c+1, \quad -2(c-2), \quad c(c-1),$$

which is impossible. ∎

LEMMA 4.4. *$R, R + A, R + B, R + C \notin 2E'(\mathbb{Q})$.*

Proof. We have

$$\begin{aligned} R + A &= (-(st - s + t + 1), -(t-s)(s+1)(t-1)), \\ R + B &= (-(st + s - t + 1), (t-s)(s-1)(t+1)), \\ R + C &= (st - s - t - 1, -(t+s)(s-1)(t-1)). \end{aligned}$$

By Lemma 4.1, if $R + A \in 2E'(\mathbb{Q})$, then

$$-(st - s + t + 1) + 2 = -(s+1)(t-1)$$

must be a perfect square, and if $R+B \in 2E'(\mathbb{Q})$, then

$$-(st+s-t+1)+2=-(s-1)(t+1)$$

must be a perfect square; both are impossible.

Suppose that $R \in 2E'(\mathbb{Q})$. Then both $(s+t)(s+1)$ and $(s+t)(t+1)$ are perfect squares. Since s is even and t is odd, we have $\gcd(s+t, s+1, t+1)=1$. Hence, $s+t$, $s+1$ and $t+1$ are perfect squares. Since we may write $t=\tau_k$, where

$$\tau_0=1, \quad \tau_1=3, \quad \tau_{k+2}=6\tau_{k+1}-\tau_k,$$

it follows from (2.2) that we may write $s+t=a_k$ for some $k \geq 1$, where

$$a_0=1, \quad a_1=5, \quad a_{k+2}=6a_{k+1}-a_k. \tag{4.2}$$

However, letting $\{u_n\}_{n\geq 0}$ be the sequence given by

$$u_0=0, \quad u_1=1, \quad u_{n+2}=2u_{n+1}+u_n,$$

we see that $a_k=u_{2k+1}$ and from [30, Theorem 1] that u_n is not a perfect square for all $n>3$ with $n \neq 7$. Hence, we have $s+t=a_3=169$ and $s+1=71$, which is a contradiction.

Suppose that $R+C \in 2E'(\mathbb{Q})$. Then in the same way as above, we see that $s+t$ and $s-1$ must be perfect squares and that this cannot happen. ∎

Lemma 4.5. *If $k \geq 2$, then $P+R, P+R+A, P+R+B, P+R+C \notin 2E'(\mathbb{Q})$.*

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

$$x(P+R+A)+2=-\left(\frac{t-1}{t+1}\right)^2(s+1)(t+1),$$

$$x(P+R+B)+2=-\left(\frac{t+1}{t-1}\right)^2(s-1)(t-1),$$

Lemma 4.1 implies that $P+R+A, P+R+B \notin 2E'(\mathbb{Q})$.

Suppose that $P+R \in 2E'(\mathbb{Q})$. Since

$$x(P+R)+2c=\left(\frac{s}{2s-t+1}\right)^2\cdot 2(t-s)(t+1),$$

$$x(P+R)+c=\left(\frac{t-1}{2s-t+1}\right)^2(t-s)(s+1),$$

$$x(P+R)+2=\left(\frac{s(2s-t-1)}{(t+1)(2s-t+1)}\right)^2\cdot 2(s+1)(t+1),$$

Lemma 4.1 implies that both $2(t-s)(t+1)$ and $(t-s)(s+1)$ are perfect squares, and hence so are $t-s$, $2(t+1)$ and $s+1$. However, since we may write $t-s=a_{k-1}$ for some $k \geq 2$, where a_k is defined by (4.2), it follows from [30, Theorem 1] that $t - s = a_3 = 169$ and $s + 1 = 409$, which is a contradiction.

Suppose that $P + R + C \in 2E'(\mathbb{Q})$. Then in the same way as above, we see that $t - s$ and $s - 1$ must be perfect squares and that this cannot happen. ∎

PROPOSITION 4.6. *If $k \geq 2$, then the rank of $E' = E'_k$ over $\mathbb{Q}$ is greater than or equal to two.*

Proof. Put together Lemmas 4.3, 4.4 and 4.5 (see the proof of [17, Proposition 2]). ∎

Let $\{\delta_1, \delta_2, \delta_3\} = \{2, c, 2c\}$. In order to prove Theorem 1.4, we need the following lemmas:

LEMMA 4.7 (cf. [26, Proposition 4.6, p. 89]). *The function $\varphi : E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ defined by*

$$\varphi(X) = \begin{cases} (x + \delta_1)(\mathbb{Q}^\times)^2 & \text{if } X = (x, y) \neq O, (-\delta_1, 0), \\ (\delta_2 - \delta_1)(\delta_3 - \delta_1)(\mathbb{Q}^\times)^2 & \text{if } X = (-\delta_1, 0), \\ (\mathbb{Q}^\times)^2 & \text{if } X = O, \end{cases}$$

is a group homomorphism.

LEMMA 4.8 (cf. [23, Criterion 1]). *Let $a > 1$ and $b > 0$ be relatively prime integers such that $d = ab$ is not a perfect square. Let (u_0, v_0) be the fundamental solution of the Pell equation $u^2 - dv^2 = 1$. Then the equation*

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

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

Proof of Theorem 1.4. The proof follows the same strategy as [17, Theorem 2]. Since the rank of E_1 over $\mathbb{Q}$ equals one (see Remark 4.10(2) below), the assumption implies $k \geq 2$, and we may apply Lemmas 4.3–4.5.

Let (x, y) be an integer point on E and let $X = (2cx, 2cy) \in E'(\mathbb{Q})$. Let $E'(\mathbb{Q})/E'(\mathbb{Q})_{\text{tors}} = \langle U, V\rangle$. Then there exist integers $m, n \geq 0$ and a point $T \in E'(\mathbb{Q})_{\text{tors}}$ such that

$$X = mU + nV + T.$$

We also write

$$P = m_P U + n_P V + T_P, \qquad R = m_R U + n_R V + T_R$$

for some integers $m_P, n_P, m_R, n_R \geq 0$ and some points $T_P, T_R \in E'(\mathbb{Q})_{\text{tors}}$. Put $\mathcal{U} = \{O, U, V, U + V\}$. There exist $U_1, U_2 \in \mathcal{U}$ and $T_1, T_2 \in E'(\mathbb{Q})_{\text{tors}}$ such that

$$P \equiv U_1 + T_1,\ R \equiv U_2 + T_2 \pmod{2E'(\mathbb{Q})}.$$

Choosing $U_3 \in \mathcal{U}$ satisfying $U_3 \equiv U_1 + U_2 \pmod{2E'(\mathbb{Q})}$, we have

$$P + R \equiv U_3 + (T_1 + T_2) \pmod{2E'(\mathbb{Q})}.$$

It follows from Lemmas 4.3–4.5 that

$$\{U_1, U_2, U_3\} = \{U, V, U + V\}.$$

Hence, $X \equiv X_1 \pmod{2E'(\mathbb{Q})}$, where

$$\begin{aligned} X_1 \in \mathcal{S} := \{&O, A, B, C, P, P + A, P + B, P + C, R, R + A, R + B, R + C, \\ &P + R, P + R + A, P + R + B, P + R + C\}. \end{aligned}$$

In view of Lemma 4.7, the integer points (x, y) on E satisfy the following system:

$$x + 1 = \alpha\Box, \qquad 2x + 1 = \beta\Box, \qquad cx + 1 = \gamma\Box, \tag{4.3}$$

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

- if $X_1 = O$, put $\alpha = 2c$, $\beta = c$, $\gamma = 2$;
- if $X_1 = (2cu, 2cv) \in \mathcal{S} \setminus \{O, A, B, C\}$, put $\alpha = u + 1$, $\beta = 2u + 1$, $\gamma = cu + 1$;
- otherwise, e.g., if $u + 1 = 0$, put $\alpha = \beta\gamma$, $\beta = 2u + 1$, $\gamma = cu + 1$.

If $X_1 = P = (0, 2c)$, then (4.3) means that

$$x + 1 = \Box, \qquad 2x + 1 = \Box, \qquad cx + 1 = \Box;$$

by Theorem 1.3 the solutions of this system are $x = 0, s(3s \pm 2t)$, which appear as the x-coordinates of integer points (1.3).

If $X_1 = A = (-1, 0)$, then (4.3) means that

$$x + 1 = \Box, \qquad 2x + 1 = -\Box, \qquad cx + 1 = -\Box;$$

this immediately implies that $x = -1$, which corresponds to the integer point $(-1, 0)$.

If $X_1 \in \{B, P + A, P + B, R + A, R + B, P + R + A, P + R + B\}$, then $\alpha > 0$, $\beta < 0$ and $\gamma < 0$, from which it follows that (4.3) has no solution. Hence, it suffices to consider the cases where

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

Denote by a' the square-free part of an integer a.

(I) $X_1 = O$. In this case, (4.3) means that

$$x + 1 = 2c\Box, \qquad 2x + 1 = c\Box, \qquad cx + 1 = 2\Box.$$

Since c is odd, c' divides both $x + 1$ and $2x + 1$; hence $c' = 1$, that is, c is a perfect square, which contradicts $c = s^2 + 1 > 1$.

(II) $X_1 = C$. In this case, (4.3) means that

$$x + 1 = c(c - 1)\Box, \qquad 2x + 1 = c(c - 2)\Box, \qquad cx + 1 = (c - 1)(c - 2)\Box.$$

In the same way as in (I), we see that c is a perfect square, which is a contradiction.

(III) $X_1 = P + C$. In this case, (4.3) means that

$$x+1 = 2\square, \qquad 2x+1 = (c-2)\square, \qquad cx+1 = 2(c-2)\square. \tag{4.4}$$

This system has a solution $x = (c-3)/2$, which corresponds to the integer points $((c-3)/2, \pm s(c-2))$. We will show later that if $c-2$ is square-free, then the system (4.4) has only the solution $x = (c-3)/2$ (see Proposition 4.9).

(IV) $X_1 = R$. In this case, (4.3) means that

$$\begin{aligned} x+1 &= 2(t-s)(t+1)\square, \\ 2x+1 &= (t-s)(s+1)\square, \\ cx+1 &= 2(s+1)(t+1)\square. \end{aligned}$$

Since $t-s$ is odd and

$$(t+s)(t-s) = s^2+1 \equiv 2 \pmod{(s+1)},$$

we have $\gcd(t-s, s+1) = \gcd(t-s, t+1) = 1$. Hence, $(t-s)'$ divides both $x+1$ and $2x+1$, that is, $t-s$ is a perfect square. It follows from [30, Theorem 1] that $t-s = a_3 = 169$, and we obtain the following system:

$$x+1 = X^2, \qquad 2x+1 = 409Y^2, \qquad 166465x+1 = 409Z^2.$$

The first two equations imply that

$$2X^2 - 409Y^2 = 1. \tag{4.5}$$

Since the fundamental solution of $u^2 - 2\cdot 409v^2 = 1$ is given by

$$u_0 + v_0\sqrt{409} = 40899 + 1430\sqrt{2\cdot 409},$$

and $2\cdot 409$ does not divide $u_0 - 1 = 40898$, if follows from Lemma 4.8 that (4.5) has no solution.

(V) $X_1 = R + C$. In this case, (4.3) means that

$$\begin{aligned} x+1 &= 2(t-s)(t-1)\square, \\ 2x+1 &= (t-s)(s-1)\square, \\ cx+1 &= 2(s-1)(t-1)\square. \end{aligned}$$

In the same way as in (IV), we see that $t-s = 169$, and obtain the system

$$x+1 = 2X^2, \qquad 2x+1 = 407Y^2, \qquad 166465x+1 = 2\cdot 407Z^2.$$

The first two equations imply that

$$4X^2 - 407Y^2 = 1. \tag{4.6}$$

Since the fundamental solution of $u^2 - 4\cdot 407Y^2 = 1$ is given by

$$u_0 + v_0\sqrt{4\cdot 407} = 2663 + 66\sqrt{4\cdot 407}$$

and $2\cdot 407$ does not divide $u_0 - 1 = 2662$, it follows from Lemma 4.8 that (4.6) has no solution.

(VI) $X_1 = P + R$. In this case, (4.3) means that

$$x + 1 = (s + t)(t + 1)\square,$$
$$2x + 1 = (s + t)(s + 1)\square,$$
$$cx + 1 = (s + 1)(t + 1)\square.$$

In the same way as in (IV), we see that $s + t = 169$, and obtain the system

$$x + 1 = X^2, \quad 2x + 1 = 71Y^2, \quad 4901x + 1 = 71Z^2.$$

The last two equations imply that

$$2Z^2 - 4901Y^2 = -69. \tag{4.7}$$

Since the fundamental solution of $u^2 - 2 \cdot 4901v^2 = 1$ is given by

$$u_0 + v_0\sqrt{2 \cdot 4901} = 19603 + 198\sqrt{2 \cdot 4901},$$

[29, Theorem 108a] implies that if (4.7) has a solution, then there exists a solution (Z_0, Y_0) of (4.7) such that

$$0 < Y_0 \le \frac{v_0\sqrt{2 \cdot 69}}{\sqrt{2(u_0 - 1)}} < 12.$$

It is easy to check that (4.7) has no solution in this range. Hence (4.7) has no solution.

(VII) $X_1 = P + R + C$. In this case, (4.3) means that

$$x + 1 = (s + t)(t - 1)\square,$$
$$2x + 1 = (s + t)(s - 1)\square,$$
$$cx + 1 = (s - 1)(t - 1)\square.$$

In the same way as in (IV), we see that $s + t = 169$, and obtain the system

$$x + 1 = 2X^2, \quad 2x + 1 = 69Y^2, \quad 4901x + 1 = 2 \cdot 69Z^2.$$

The first two equations imply that

$$4X^2 - 69Y^2 = 1. \tag{4.8}$$

Since the fundamental solution of $u^2 - 4 \cdot 69v^2 = 1$ is given by

$$u_0 + v_0\sqrt{4 \cdot 69} = 7775 + 468\sqrt{4 \cdot 69},$$

and $2 \cdot 69$ does not divide $u_0 - 1 = 7774$, it follows from Lemma 4.8 that (4.8) has no solution. ∎

The following proposition will complete the proof of Theorem 1.4.

Proposition 4.9. *Let $\{1, 2, c\}$ be a $D(-1)$-triple with $c \ge 145$ such that $c-2$ is square-free. Then the system* (4.4) *has only the solution $x = (c-3)/2$.*

Proof. Since $c - 2$ is square-free, it suffices to find the (positive) integer solutions of the system

$$x + 1 = 2X^2, \quad 2x + 1 = (c - 2)Y^2, \quad cx + 1 = 2(c - 2)Z^2.$$

Eliminating x and replacing $2X$, $2Z$ by X, Z respectively, we obtain the system of Diophantine equations

$$\left\{\begin{array}{l} X^2-(c-2)Y^2=1, \qquad (4.9)\\ Z^2-cY^2=-1. \qquad (4.10)\end{array}\right.$$

The positive solutions of (4.9) and (4.10) are given by

$$X+Y\sqrt{c-2}=(s+\sqrt{c-2})^{m+1} \qquad (m\geq 0),$$
$$Z+Y\sqrt{c}=(s+\sqrt{c})^{2n+1} \qquad (n\geq 0),$$

respectively. Hence we may write $Y=V_m$, where

$$V_0=1, \quad V_1=2s, \quad V_{m+2}=2sV_{m+1}-V_m, \tag{4.11}$$

and $Y=W_n$, where

$$W_0=1, \quad W_1=4c-3, \quad W_{n+2}=2(2c-1)W_{n+1}-W_n. \tag{4.12}$$

Since

$$(V_m \bmod s)_{m\geq 0}=(1,0,-1,0,1,0,\dots),$$
$$(W_n \bmod s)_{n\geq 0}=(1,1,1,1,1,1,\dots),$$

we have $m\equiv 0 \pmod 4$. Letting $b_m=V_{4m}$, we have

$$b_{m+2}\equiv -2(8s^2-1)b_{m+1}-b_m \pmod{16s^4}.$$

Since we see by induction that

$$V_{4m}=b_m\equiv -4m(2m+1)s^2+1 \pmod{16s^4},$$
$$W_n\equiv 2n(n+1)s^2+1 \pmod{16s^4},$$

it follows from $V_{4m}=W_n$ that

$$2m(2m+1)\equiv -n(n+1) \pmod{8s^2}. \tag{4.13}$$

Suppose now that $(m+1/4)^2\leq 2s^2/5$. Then we have

$$2m(2m+1)<4\left(m+\frac{1}{4}\right)^2\leq \frac{8}{5}\,s^2,$$

and since one may easily verify that $V_l\leq W_l$ $(l\geq 0)$, that is, $4m\geq n$, we have

$$n(n+1)\leq 4m(4m+1)<16(m+1/4)^2\leq \frac{32}{5}\,s^2.$$

Hence $2m(2m+1)+n(n+1)<8s^2$, which together with (4.13) implies that $2m(2m+1)+n(n+1)=0$, that is, $m=n=0$. Hence, if $m\geq 1$, then

$$m>\sqrt{\frac{2(c-1)}{5}}-\frac{1}{4}>0.6\sqrt{c},$$

which yields

$$c<(1.67m)^2. \tag{4.14}$$

In the standard way we see from (4.11) and (4.12) that

$$0 < \Lambda'' := 4m \log \alpha_1'' - n \log \alpha_2'' + \log \alpha_3'' < 0.02c(\alpha_2'')^{-2n-1}, \tag{4.15}$$

where

$$\alpha_1'' = s + \sqrt{c-2}, \quad \alpha_2'' = 2c - 1 + 2s\sqrt{c}, \quad \alpha_3'' = \frac{(s+\sqrt{c-2})\sqrt{c}}{(s+\sqrt{c})\sqrt{c-2}}.$$

Since we easily deduce from (4.15) that $4m \log \alpha_1'' < n \log \alpha_2''$, we have

$$m < 0.51n. \tag{4.16}$$

We now apply Theorem 2.12 with

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

and $\alpha_1 = \alpha_1''$, $\alpha_2 = \alpha_2''$, $\alpha_3 = \alpha_3''$. Then we obtain the following:

$$A_1 < 1.279 \log c, \quad A_2 < 2.558 \log c, \quad 1.494 \log c < A_3 < 1.5 \log c,$$

$$B < 6.85m, \quad C(3) < 6.45 \cdot 10^8, \quad C_0 < 29.9,$$

$$W_0 < \log(267m), \quad \Omega < 4.91(\log c)^3.$$

It follows from Theorem 2.12 that

$$\log \Lambda'' > -1.6 \cdot 10^{12} (\log c)^3 \log(267m),$$

which together with (4.15) implies that

$$-1.6 \cdot 10^{12} (\log c)^3 \log(267m) < -2n \log c.$$

Hence by (4.14) and (4.16) we obtain

$$\varrho(n) := \frac{n}{\log(140n)(\log(0.86n))^2} < 3.2 \cdot 10^{12}.$$

It follows from $\varrho(3 \cdot 10^{17}) > 4.1 \cdot 10^{12}$ and (4.16) that $m < 1.6 \cdot 10^{17}$, and from (4.14) that $c < 6.6 \cdot 10^{34}$. Since $c_{24} > 6.9 \cdot 10^{35}$, we obtain $c \le c_{23}$, that is, $k \le 23$.

Dividing (4.15) by $\log \alpha_2''$, we have

$$0 < m\kappa'' - n + \mu'' < A''(B'')^{-n}, \tag{4.17}$$

where

$$\kappa'' = \frac{\log \alpha_1''}{\log \alpha_2''}, \quad \mu'' = \frac{\log \alpha_3''}{\log \alpha_2''}, \quad A'' = \frac{0.02c}{\alpha_2'' \log \alpha_2''}, \quad B'' = (\alpha_2'')^2.$$

We apply this lemma with $M = 1.6 \cdot 10^{17}$. We have to examine 22 cases. The second convergent is needed only in three cases. In all cases, the first steps of reduction give $m \le 2$, which contradicts (4.14) and $c \ge 145$. This completes the proof of Proposition 4.9. ■

REMARK 4.10.

(1) We checked that $c_k - 2$ is square-free for all k with $1 \le k \le 50$ except $k \in \{26, 40\}$.

(2) Denote by E_k the elliptic curve E corresponding to $\{1, 2, c_k\}$. We calculated, using MWRANK ([5]), the values of the ranks $\mathrm{rk}(E_k(\mathbb{Q}))$ of E_k over $\mathbb{Q}$ for $1 \le k \le 6$:

k	1	2	3	4	5	6
$\mathrm{rk}(E_k(\mathbb{Q}))$	1	2	2	4	2	2

(3) Let (x, y) be an integer point on E. There exist positive integers x_1, x_2, x_3 such that

$$\begin{cases} x + 1 = D_2 x_1^2, \\ 2x + 1 = D_1 x_2^2, \\ cx + 1 = D_1 D_2 x_3^2, \end{cases} \tag{4.18}$$

where D_1 and D_2 are square-free integers dividing $c-2$ and $c-1$, respectively. Then, by examining the system (4.18) modulo appropriate prime powers (cf. [16], [10], [11], [25]), one can find that if $(D_1, D_2) \notin \{(1, 1), ((c-2)', 2)\}$ (where $(c-2)'$ denotes the square-free part of $c-2$), then (4.18) is unsolvable for all k with $2 \le k \le 40$ except possibly in the following 13 cases:

$$k \in \{4, 7, 8, 11, 12, 15, 20, 24, 25, 27, 30, 36, 39\}. \tag{4.19}$$

It follows that Theorem 1.4 holds for all k with $2 \le k \le 40$ except (4.19) without the assumptions on $c - 2$ and the rank of E.

Acknowledgments. We would like to thank Professor Andrej Dujella and Professor Gary Walsh for their valuable comments. Thanks also go to the referee for careful reading and detailed 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 Ser. (2) 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., to appear.

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

[6] A. Dujella, *The problem of Diophantus and Davenport for Gaussian integers*, Glas. Mat. Ser. III 32 (1997), 1–10.

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

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

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

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

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

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

[13] —, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. 566 (2004), 183–214.

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

[15] A. Dujella and C. Fuchs, *Complete solution of a problem of Diophantus and Euler*, J. London Math. Soc. (2) 71 (2005), 33–52.

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

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

[18] A. Filipin, *Non-extendibility of* $D(-1)$*-triples of the form* $\{1, 10, c\}$, Int. J. Math. Math. Sci. 2005, no. 14, 2217–2226.

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

[20] —, *The extensibility of Diophantine pairs* $\{k-1, k+1\}$, J. Number Theory, to appear.

[21] —, *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*, preprint.

[22] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III 41 (2006), 195–203.

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

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

[25] M. J. Jacobson, Jr. and H. C. Williams, *Modular arithmetic on elements of small norm in quadratic fields*, Des. Codes Cryptogr. 27 (2002), 93–110.

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

[27] 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.

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

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

[30] K. Nakamula and A. Pethő, *Squares in binary recurrence sequences*, in: Number Theory, Diophantine, Computational and Algebraic Aspects, K. Győry, A. Pethő and V. T. Sós (eds.), de Gruyter, Berlin, 1998, 409–421.

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

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

[33] M. Sudo, *Rickert's methods on simultaneous Pell equations*, Technical Reports of Seikei Univ. 38 (2001), 41–50 (in Japanese).

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

Mathematical Institute
Tohoku University
Sendai 980-8578, Japan
E-mail: fyasut@yahoo.co.jp

Received on 30.10.2006
and in revised form on 21.2.2007 (5308)