Publ. Math. Debrecen
82/2 (2013), 293–308
DOI: 10.5486/PMD.2013.5200

The number of Diophantine quintuples II

By ALAN FILIPIN (Zagreb) and YASUTSUGU FUJITA (Narashino)

Abstract. A set of m distinct positive integers is called a Diophantine m-tuple if the product of any two of its distinct elements increased by 1 is a perfect square. It is known that there does not exist a Diophantine sextuple and that there are only finitely many Diophantine quintuples. In this paper, we prove that there are at most 10^{96} Diophantine quintuples, which improves the known bounds.

1. Introduction

A set $\{a_1, \dots, a_m\}$ of m distinct positive integers is called *a Diophantine m-tuple* if $a_i a_j + 1$ is a perfect square for any i, j with $1 \leq i < j \leq m$. This area of research has been studied through the ages.

Diophantus of Alexandria was the first who studied the existence of such sets. However, the first example $\{1, 3, 8, 120\}$ of a Diophantine quadruple was found by Fermat. In 1969, Baker and Davenport [1] proved that $\{1, 3, 8\}$ cannot be extended to a Diophantine quintuple. Recently, this result was generalized by Dujella [5], who proved that the Diophantine triple $\{k-1, k+1, 4k\}$ cannot be extended to a Diophantine quintuple for integer $k > 1$, and by Dujella and Pethő [10] who proved that the Diophantine pair $\{1, 3\}$ cannot be extended to a Diophantine quintuple. One generalization of it was given by the second author ([12]; see also [4]) who proved that the Diophantine pair $\{k-1, k+1\}$ cannot be extended to a Diophantine quintuple for integer $k > 1$. Other generalizations can be found in [6], [15], [16]. All those results support a folklore conjecture, which states that there does not exist a Diophantine quintuple. Actually, there is even

---

Mathematics Subject Classification: Primary: 11D09; Secondary: 11J86.
Key words and phrases: Diophantine tuples, system of Diophantine equations.

stronger version of this conjecture, that a Diophantine triple can be extended to a quadruple with a larger element in the unique way. In 2004, Dujella [8] proved that there does not exist a Diophantine sextuple and that there exist only finitely many Diophantine quintuples, and he furthermore proved that the number of Diophantine quintuples is bounded by 10^{1930} (see [9]). This bound was recently reduced by the second author in [14] where he proved that there are at most 10^{276} Diophantine quintuples.

In this paper we furthermore improve this bound and prove the following theorem.

Theorem 1.1. *The number of Diophantine quintuples is less than* 10^{96}.

To prove this, we use the already known methods and results mostly from [14], but significantly improve some of them. We first recall some useful results on extending Diophantine triples. We transform that problem to the system of simultaneous Diophantine equations which induces binary recurrence sequences. Then, we improve some congruence relations which give us the better lower bounds for the solutions. After that, using the improvement of Rickert's theorem in our special case, which is the important part here, we get an upper bound for the solutions. Combining this with the results from [14], we get the upper bounds for b and d in a Diophantine quintuple $\{a, b, c, d, e\}$ where $a < b < c < d < e$. After we get those upper bounds we prove Theorem 1.1 along the same lines as Theorem 4 in [9] and Theorem 1.3 in [14].

It is to be noted that our idea on the improvement of Rickert's theorem can be applicable to the $D(-1)$-quadruple $\{1, b, c, d\}$ $(1 < b < c < d)$, which means that b, c, d are integers such that the product of any two of 1, b, c, d decreased by 1 is a perfect square. In [11], we improve the known upper bounds for c in terms of b to $9.5b^4$ by improving Rickert's theorem. This bound is smaller than the result $c < \min\{2.5b^6, 10^{146}\}$ obtained recently in [3] for $b < 10^{36}$.

2. Preliminaries

Our first goal is to prove the following theorem.

Theorem 2.1. *Suppose that* $\{a, b, c, d, e\}$ *is a Diophantine quintuple with* $a < b < c < d < e$. *Then,* $b < 5 \cdot 10^{49}$ *and* $d \leq 10^{100}$.

So, in this section we will give some necessary preliminaries here. Let $\{a, b, c\}$ be a Diophantine triple with $a < b < c$ such that $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$, where r, s, t are positive integers. Assume that $\{a, b, c, d\}$ is a

Diophantine quadruple. Then, there exist positive integers x, y, z satisfying $ad+1=x^2$, $bd+1=y^2$, $cd+1=z^2$. Eliminating d from these equations, we obtain the system of simultaneous Diophantine equations

$$az^2 - cx^2 = a - c, \tag{2.1}$$

$$bz^2 - cy^2 = b - c. \tag{2.2}$$

The solutions of equations (2.1) and (2.2) are respectively given by $z = v_m$ and $z = w_n$ with positive integers m and n, where

$$v_0 = z_0, \quad v_1 = sz_0 + cx_0, \quad v_{m+2} = 2sv_{m+1} - v_m,$$
$$w_0 = z_1, \quad w_1 = tz_1 + cy_1, \quad w_{n+2} = 2tw_{n+1} - w_n$$

with some integers z_0, z_1, x_0, y_1 (cf. [7, Section 2]). We first find the bounds for b and c on the following assumption.

Assumption 2.2. *$v_{2m} = w_{2n}$ has a solution with $m \geq 3$, $n \geq 2$ and $|z_0| = 1$, and $c > b^5$.*

Note that Assumption 2.2 together with Lemma 3 1) in [7] implies $z_0 = z_1 = \pm 1$ and $x_0 = y_1 = 1$.

Firstly, we find connection between indices m and n.

Lemma 2.3. *On Assumption 2.2, we have $m \leq 1.2n$.*

Proof. The proof proceeds along the same lines as Lemma 3 in [8]. Since $|z_0| = |z_1| = x_0 = y_1 = 1$ and $c > b^5 \geq 8^5$, we have

$$\begin{aligned} v_{2m} &> v_1(2s-1)^{2m-1} = (c \pm s)(2s-1)^{2m-1} \\ &\geq \left(1 - \frac{\sqrt{ac+1}}{c}\right) c(2s-1)^{2m-1} > 0.984c(2s-1)^{2m-1} \end{aligned}$$

and

$$w_{2n} < w_1(2t)^{2n-1} = (c \pm t)(2t)^{2n-1} \leq \left(1 + \frac{\sqrt{bc+1}}{c}\right) c(2t)^{2n-1} < 1.016c(2t)^{2n-1}.$$

Hence, we see from $v_{2m} = w_{2n}$ that $(2s-1)^{2m-1} < 1.033(2t)^{2n-1}$. Since

$$(2s-1)^{2m-1} > 1.994^{2m-1}(ac)^{(2m-1)/2}$$

and

$$1.033(2t)^{2n-1} < 1.033 \cdot 2^{2n-1}(bc+1)^{(2n-1)/2} < 2.001^{2n} b^{(2n-1)/2} c^{(2n-1)/2},$$

we obtain $1.994^{2m-1} a^{(2m-1)/2} c^m < 2.001^{2n} b^{(2n-1)/2} c^n$, which yields

$$1.994^{2m-1} c^m < 2.001^{2n} c^{(12n-1)/10}.$$

Therefore, either $m < (12n-1)/10$ or $2m-1 < 2.02n$ holds. If the former holds, then $m < 1.2n - 0.1$ and if the latter holds, then $m < 1.01n + 0.5$. If $n = 2$, then $m < \max\{1.2n - 0.1, 1.01n + 0.5\} \leq 2.52$, which contradicts the assumption $m \geq 3$. Hence, $n \geq 3$ and we obtain $m < 1.2n$. $\square$

Now we are ready to find lower bounds for n in terms of a, b and c, using congruence relations.

Lemma 2.4. *On Assumption 2.2, the following hold.*

(i) *If $b \geq 2a$, then $n > 0.178a^{1/2}b^{-1}c^{1/2}$.*

(ii) *If $b \geq 1.45a$, then $n > 0.0033a^{1/2}b^{-1}c^{1/2}$.*

(iii) *If $b < 2a$, then $n > a^{-1/2}c^{1/8}$.*

Proof. The proof proceeds along the same lines as the one of Lemma 20 (i) (I) in [13]. By Lemma 4 in [7] with $|z_0| = |z_1| = x_0 = y_1 = 1$, we have

$$\pm am^2 + sm \equiv \pm bn^2 + tn \pmod{4c}. \tag{2.3}$$

(i) Suppose that $n \leq 0.178a^{1/2}b^{-1}c^{1/2}$. Lemma 2.3 and $c > b^5 \geq 8^5$ together imply that

$$am^2 \leq 1.2^2 \cdot 0.178^2 a^2 b^{-2} c < c, \quad sm \leq 1.2 \cdot 0.178\sqrt{ac+1}\,a^{1/2}b^{-1}c^{1/2} < c,$$

$$bn^2 \leq 0.178^2 ab^{-1}c < c, \quad tn \leq 0.178\sqrt{bc+1}\,a^{1/2}b^{-1}c^{1/2} < c.$$

Thus we have an equality in (2.3):

$$\pm am^2 + sm = \pm bn^2 + tn. \tag{2.4}$$

If $z_0 = 1$, then $am^2 + sm = bn^2 + tn$. We see from $b \geq 2a$ that $bn^2 + tn > 2an^2 + 1.414sn$ and from $m \leq 1.2n$ that $am^2 + sm < 1.44an^2 + 1.2sn$, which are contradictions. If $z_1 = -1$, then $bn/m - am/n = t/m - s/n$. We know by Lemma 3 in [8] that $n \leq m$ and $bn/m - am/n < b$. On the other hand,

$$\frac{t}{m} - \frac{s}{n} \geq \left(\frac{1}{1.2} \cdot \frac{t}{s} - 1\right)\frac{s}{n} > (0.833 \cdot 1.414 - 1)\frac{b}{0.178} > b,$$

which is a contradiction. Therefore, we obtain $n > 0.178a^{1/2}b^{-1}c^{1/2}$.

(ii) Suppose that $n \leq 0.0033a^{1/2}b^{-1}c^{1/2}$. Then, equation (2.4) holds. If $z_0 = 1$, then $bn^2 + tn > 1.45an^2 + 1.204sn$ and $am^2 + sm < 1.44an^2 + 1.2sn$, which are contradictions. If $z_0 = -1$, then $bn/m - am/n < b$ and

$$\frac{t}{m} - \frac{s}{n} > \left(\frac{1}{1.2} \cdot 1.204 - 1\right) \frac{b}{0.0033} > b,$$

which are also contradictions. Therefore, we obtain $n > 0.0033a^{1/2}b^{-1}c^{1/2}$.

(iii) Suppose that $n \leq a^{-1/2}c^{1/8}$. Squaring both sides of congruence (2.3) yields

$$\left\{(am^2 - bn^2)^2 - (m^2 + n^2)\right\}^2 \equiv 4m^2n^2 \pmod{c}. \tag{2.5}$$

Since it is easy to check that both sides of (2.5) are less than c, (2.5) is an equation, that is,

$$\mp(am^2 - bn^2) = m + n, \tag{2.6}$$

We also easily see that equation (2.4) holds, where the signs in (2.4) and (2.6) are taken simultaneously. Hence, we have $m(s-1) = n(t+1)$, which together with (2.4) implies

$$\left| a\left(\frac{t+1}{s-1}\right)^2 - b \right| n = \frac{s+t}{s-1}.$$

This shows that

$$n = \frac{(s+t)(s-1)}{|a(t+1)^2 - b(s-1)^2|} = \frac{(s+t)(s-1)}{2(at+bs+a-b)} > \frac{s-1}{2b} > \frac{s-1}{4a} > a^{-1/2}c^{1/8},$$

which contradicts the assumption. Therefore, we obtain $n > a^{-1/2}c^{1/8}$. □

Now, we will improve Rickert's theorem in our special case which plays an important role here.

Theorem 2.5. *Let a, b and N be integers with $0 < a \leq b - 5$, $b \geq 8$ and $N \geq 9.5a'b^2(b-a)^2$, where $a' = \max\{b-a, a\}$. Assume that N is divisible by ab. Then the numbers $\theta_1 = \sqrt{1 + b/N}$ and $\theta_2 = \sqrt{1 + a/N}$ satisfy*

$$\max\left\{\left|\theta_1 - \frac{p_1}{q}\right|, \left|\theta_2 - \frac{p_2}{q}\right|\right\} > \left(\frac{32.01a'bN}{a}\right)^{-1} q^{-\lambda}$$

for all integers p_1, p_2, q with $q > 0$, where

$$\lambda = 1 + \frac{\log(16.01a^{-1}a'bN)}{\log(1.687a^{-1}b^{-1}(b-a)^{-2}N^2)} < 2.$$

Remark 2.6. The essential difference from the provious result ([13, Theorem 21] or [2, Theorem 3.2]) is in λ. Since λ in Theorem 2.5 is smaller than others, we can get the weaker condition $N \geq 9.5a'b^2(b-a)^2$ for $\lambda < 2$ and apply Theorem 2.5 with $N = abc$ on Assumption 2.2.

We need the following lemma.

Lemma 2.7 ([13, Lemma 22]; see also [17, Lemma 3.1], [2, Lemma 2.1])**.** *Let $\theta_1, \dots, \theta_m$ be arbitrary real numbers and $\theta_0 = 1$. Assume that there exist positive real numbers l, p, L, P and positive integers D, f with f dividing D and with $L > D$, having the following property. For each positive integer k, we can find rational numbers p_{ijk} $(0 \leq i, j \leq m)$ with nonzero determinant such that $f^{-1}D^k p_{ijk}$ $(0 \leq i, j \leq m)$ are integers and*

$$|p_{ijk}| \leq pP^k \ \ (0 \leq i, j \leq m), \qquad \left| \sum_{j=0}^{m} p_{ijk}\theta_j \right| \leq lL^{-k} \ \ (0 \leq i \leq m).$$

Then

$$\max\left\{ \left|\theta_1 - \frac{p_1}{q}\right|, \dots, \left|\theta_m - \frac{p_m}{q}\right| \right\} > cq^{-\lambda}$$

holds for all integers $p_1, \dots, p_m, q$ with $q > 0$, where

$$\lambda = 1 + \frac{\log(DP)}{\log(L/D)} \quad \textit{and} \quad c^{-1} = 2mf^{-1}pDP\left(\max\{1, 2f^{-1}l\}\right)^{\lambda}.$$

Proof of Theorem 2.5. In our situation, we take $m = 2$ and θ_1, θ_2 as in Theorem 2.5. The only difference from the proof of Theorem 21 in [13] is the way to take D. We here show that we may take $D = 4ab(b-a)^2N$ (whereas $D = 2a^2b^2(b-a)^2N$ is taken in [13]).

For $1 \leq i, j \leq 2$, let $p_{ij}(x)$ be the polynomial defined by

$$p_{ij}(x) = \sum_{ij} \binom{k+\frac{1}{2}}{h_j} (1 + a_j x)^{k-h_j} x^{h_j} \prod_{l \neq j} \binom{-k_{il}}{h_l} (a_j - a_l)^{-k_{il}-h_l},$$

where $k_{il} = k + \delta_{il}$ with δ_{il} the Kronecker delta, $\sum_{ij}$ denotes the sum over all non-negative integers h_0, h_1, h_2 satisfying $h_0 + h_1 + h_2 = k_{ij} - 1$, and $\prod_{l \neq j}$ denotes the product from $l = 0$ to $l = 2$ omitting $l = j$ (which is the expression (3.7) in [17] with $\nu = 1/2$). Substituting $x = 1/N$, we have

$$(p_{ijk} =)\, p_{ij}\left(\frac{1}{N}\right) = \sum_{ij} \binom{k+\frac{1}{2}}{h_j} C_{ij}^{-1} \prod_{l \neq j} \binom{-k_{il}}{h_l}, \tag{2.7}$$

where

$$C_{ij} = \frac{N^k}{(N + a_j)^{k-h_j}} \prod_{l \neq j} (a_j - a_l)^{k_{il}+h_l}.$$

Now we take $a_0 = 0$, $a_1 = a$, $a_2 = b$ and $N = abN_0$ for some integer N_0. If $j = 0$, then

$$|C_{i0}| = N^{h_0} a^{k_{i1}+h_1} b^{k_{i2}+h_2} = \frac{a^{k_{i1}+h_0+h_1-k} b^{k_{i2}+h_0+h_2-k} N^k}{N_0^{k-h_0}}.$$

Since $k_{il} + h_j + h_l - k \leq k_{il} + k_{ij} - 1 - k \leq k$, we have $a^k b^k N^k C_{i0}^{-1} \in \mathbb{Z}$ for all i. If $j = 1$, then

$$|C_{i1}| = \frac{a^{h_1} b^k N_0^k}{(bN_0 + 1)^{k-h_1}} \cdot a^{k_{i0}+h_0} (b - a)^{k_{i2}+h_2} = \frac{a^{k_{i0}+h_0+h_1-k} (b - a)^{k_{i2}+h_2} N^k}{(bN_0 + 1)^{k-h_1}}.$$

Since $k_{il} + h_l \leq k_{il} + k_{ij} - 1 \leq 2k$, we have $a^k (b - a)^{2k} N^k C_{i1}^{-1} \in \mathbb{Z}$ for all i. If $j = 2$, then $|C_{i2}| = b^{k_{i0}+h_0+h_2-k} (b - a)^{k_{i1}+h_1} N^k/(aN_0 + 1)^{k-h_2}$ and we have $b^k (b - a)^{2k} N^k C_{i2}^{-1} \in \mathbb{Z}$ for all i. It follows that $a^k b^k (b - a)^{2k} N^k C_{ij}^{-1} \in \mathbb{Z}$ for all i, j. Since

$$2^{h_j+h'_j} \binom{k + \frac{1}{2}}{h_j} \in \mathbb{Z}$$

for all j (see the proof of Lemma 4.3 in [17]), we obtain
$2^{-1}\{4ab(b-a)^2 N\}^k p_{ij}(1/N) \in \mathbb{Z}$ for all i, j, which means that we may take $f = 2$ and $D = 4ab(b - a)^2 N$.

As in the proof of Theorem 21 in [13], we may take

$$l = \frac{27}{64} \left(1 - \frac{b}{N}\right)^{-1}, \qquad L = \frac{27}{4} \left(1 - \frac{b}{N}\right)^2 N^3,$$

$$p = \left(1 + \frac{a'}{2N}\right)^{1/2}, \qquad P = \frac{8\left(1 + \frac{3b-a}{2N}\right)}{\zeta},$$

where

$$\zeta = \begin{cases} a^2(2b - a) & \text{if } b - a \geq a, \\ (b - a)^2(a + b) & \text{if } b - a < a. \end{cases} \tag{2.8}$$

Hence, we easily see from the assumptions that

$$DP < \frac{16.01a'bN}{a}, \qquad \frac{L}{D} > \frac{1.687N^2}{ab(b - a)^2}, \qquad c^{-1} < \frac{32.01a'bN}{a}.$$

Therefore, the assertion follows from Lemma 2.7. □

We are now ready to give an upper bounds for b and c first.

Lemma 2.8 (cf. [7, Lemma 12])**.** *Let $N = abc$ and let θ_1, θ_2 be as in Theorem 2.5. Then all positive solutions of the system of Diophantine equations* (2.1) *and* (2.2) *satisfy*

$$\max\left\{\left|\theta_1 - \frac{sbx}{abz}\right|, \left|\theta_2 - \frac{tay}{abz}\right|\right\} < \frac{c}{2a} z^{-2}.$$

Lemma 2.9. *Let $\{a, b, c, d\}$ be a Diophantine quadruple with $a < b < c < d$. Assume that $c > 9.5a'b(b-a)^2/a$. Then,*

$$\log z < \frac{4\log(4.001a^{1/2}(a')^{1/2}b^2c)\log(1.299a^{1/2}b^{1/2}(b-a)^{-1}c)}{\log(0.1053a(a')^{-1}b^{-1}(b-a)^{-2}c)}.$$

Proof. Putting $q = abz$, $p_1 = sbx$ and $p_2 = tay$, we see from Theorem 2.5 and Lemma 2.8 that

$$z^{2-\lambda} < 16.005aa'b^4c^2 < \left(4.001a^{1/2}(a')^{1/2}b^2c\right)^2.$$

Since

$$\frac{1}{2-\lambda} = \frac{\log(1.687ab(b-a)^{-2}c^2)}{\log\frac{1.687a(b-a)^{-2}c}{16.01a'b}} < \frac{2\log(1.299a^{1/2}b^{1/2}(b-a)^{-1}c)}{\log(0.1053a(a')^{-1}b^{-1}(b-a)^{-2}c)},$$

we obtain the assertion. □

Lemma 2.10. *On Assumption 2.2, we have*

$$\log z > n\log(4bc).$$

Proof. The proof proceeds along the same lines as the one of Lemma 25 in [13]. Indeed, the assertion immediately follows from the following inequalities:

$$w_{2n} > \frac{1}{2\sqrt{b}}\left(z_1\sqrt{b} + y_1\sqrt{c}\right)\left(t + \sqrt{bc}\right)^{2n} > \left(t + \sqrt{bc}\right)^{2n} > (4bc)^n. \qquad \square$$

Proposition 2.11. *On Assumption 2.2, the following hold.*

(1) $b < 10^{10}$.

(2) $c < b^9$.

PROOF. Note that $c > b^5$ implies $c > 9.5a'b(b-a)^2/a$. For, if $b \geq 10$, then $b^5 > 9.5a'b(b-a)^2/a$; otherwise, $b = 8$ and the same inequality clearly holds. By Lemmas 2.9 and 2.10 we have

$$\frac{n}{4} < \frac{\log(4.001a^{1/2}(a')^{1/2}b^2c)\log(1.299a^{1/2}b^{1/2}(b-a)^{-1}c)}{\log(4bc)\log(0.1053a(a')^{-1}b^{-1}(b-a)^{-2}c)}. \tag{2.9}$$

(1) Suppose first that $b \geq 2a$. Then by (2.9) we have

$$\frac{n}{4} < \frac{\log(2.83b^3c)\log(1.299b^{1/2}c)}{\log(4bc)\log(0.1053b^{-4}c)}. \tag{2.10}$$

Since the right-hand side of this inequality is a decreasing function with respect to c, we obtain

$$\frac{n}{4} < \frac{\log(2.83b^8)\log(1.299b^{5.5})}{\log(4b^6)\log(0.1053b)} < \frac{8\cdot 5.5}{6}f_1(b) = \frac{22}{3}f_1(b),$$

where

$$f_1(b) = \frac{\log(1.139b)\log(1.049b)}{\log(1.259b)\log(0.1053b)}.$$

Combining this inequality with Lemma 2.4 implies that

$$\frac{0.178}{4}a^{1/2}b^{-1}c^{1/2} < \frac{22}{3}f_1(b),$$

which yields $b^{2/3} < 165f_1(b)$. Since $f_1(b)$ is a decreasing function for $b \geq 10$, if $b \geq 53$, then $165f_1(b) \leq 165f_1(53) < 377$, which contradicts $b^{3/2} \geq 53^{3/2} > 385$. Therefore, we obtain $b \leq 52$.

Secondly, suppose that $b < 2a$. Then by (2.9) we have

$$\frac{n}{4} < \frac{\log(4.001b^3c)\log(0.1856bc)}{\log(4bc)\log(0.4212b^{-3}c)},$$

where we used the fact that $b-a \geq 7$, which is attained by the pair $\{a,b\} = \{8,15\}$, and we obtain

$$\frac{n}{4} < \frac{8\cdot 6}{6\cdot 2}f_2(b) = 4f_2(b),$$

where

$$f_2(b) = \frac{\log(1.19b)\log(0.7553b)}{\log(1.259b)\log(0.6489b)}.$$

It follows from Lemma 2.4 that

$$\frac{a^{-1/2}c^{1/8}}{4} < 4f_2(b),$$

which yields $b^{1/8} < 16f_2(b)$. Since $f_2(b)$ is decreasing for $b \geq 2$, if $b \geq 17^8$, then $16f_2(b) \leq 16f_2(17^8) < 17$, which contradicts $b^{1/8} \geq 17$. Therefore, we obtain $b < 10^{10}$, which gives an upper bound in all the cases.

(2) Suppose that $c > b^9$. We also have inequality (2.9). The proof is divided into three cases.

Suppose first that $b \geq 2a$. Then, we have inequality (2.10). By $c > b^9$, we have

$$\frac{n}{4} < \frac{\log(2.83b^{12})\log(1.299b^{9.5})}{\log(4b^{10})\log(0.1053b^5)} < \frac{12\cdot 9.5}{10\cdot 5}g_1(b) = \frac{57}{25}g_1(b),$$

where

$$g_1(b) = \frac{\log(1.091b)\log(1.028b)}{\log(1.148b)\log(0.6375b)}.$$

Lemma 2.4 now shows that

$$\frac{0.178}{4}a^{1/2}b^{-1}c^{1/2} < \frac{57}{25}g_1(b),$$

that is, $b^{7/2} < 52g_1(b)$. Since $g_1(b)$ is decreasing for $b \geq 2$, we have $52g_1(b) \leq 52g_1(8) < 66$, which contradicts $b^{7/2} \geq 8^{7/2} > 1100$.

Suppose secondly that $1.45a \leq b < 2a$. We see from (2.9) that

$$\frac{n}{4} < \frac{\log(2.76b^3c)\log(4.083c)}{\log(4bc)\log(0.4212b^{-3}c)} < \frac{\log(2.76b^{12})\log(4.083b^9)}{\log(4b^{10})\log(0.4212b^6)} < \frac{12\cdot 9}{10\cdot 6}g_2(b) = \frac{9}{5}g_2(b),$$

where

$$g_2(b) = \frac{\log(1.089b)\log(1.17b)}{\log(1.148b)\log(0.8657b)}.$$

By Lemma 2.4 we have

$$\frac{0.0033}{4}a^{1/2}b^{-1}c^{1/2} < \frac{9}{5}g_2(b),$$

yielding $b^4 < 2182g_2(b)$. Since $b \geq 15$ holds for $b < 2a$ and $g_2(b)$ is decreasing for $b \geq 2$, we see that $2182g_2(b) \leq 2182g_2(15) < 2400$, which contradicts $b^4 \geq 15^4 > 50000$.

Finally, suppose that $b < 1.45a$. By (2.9) we have

$$\frac{n}{4} < \frac{\log(4.001b^3c)\log(0.1856bc)}{\log(4bc)\log(1.093b^{-3}c)} < \frac{\log(4.001b^{12})\log(0.1856b^{10})}{\log(4b^{10})\log(1.093b^6)} < 2g_3(b) < 2,$$

where

$$g_3(b) = \frac{\log(1.123b)\log(0.8451b)}{\log(1.148b)\log(1.014b)}.$$

Thus we have $n < 8$, which together with Lemma 2.4 implies that $a^{-1/2}c^{1/8} < 8$, and hence $b \leq 27$. In this range, there does not exist a Diophantine pair satisfying $a + 2 < b < 1.45a$. This completes the proof of Proposition 2.11. $\square$

3. Proof of Theorem 2.1

In this section we find the upper bounds for b and d. We first review some results on Diophantine quintuples from Sections 2 and 3 in [14]. Suppose that $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$. Then, there exist integers α, β, γ, δ such that

$$ae + 1 = \alpha^2, \quad be + 1 = \beta^2, \quad ce + 1 = \gamma^2, \quad de + 1 = \delta^2,$$

from which we obtain the system of Diophantine equations.

$$a\delta^2 - d\alpha^2 = a - d, \tag{3.1}$$

$$b\delta^2 - d\beta^2 = b - d, \tag{3.2}$$

$$c\delta^2 - d\gamma^2 = c - d. \tag{3.3}$$

The solutions of equations (3.1), (3.2) and (3.3) respectively are given by $\delta = U_i$, $\delta = V_j$ and $\delta = W_k$ with positive integers i, j and k, where

$$\begin{aligned} U_0 &= \pm 1, & U_1 &= \pm x + d, & U_{i+2} &= 2xU_{i+1} - U_i, \\ V_0 &= \pm 1, & V_1 &= \pm y + d, & V_{j+2} &= 2yV_{j+1} - V_j, \\ W_0 &= \pm 1, & W_1 &= \pm z + d, & W_{k+2} &= 2zW_{k+1} - W_k. \end{aligned}$$

The indices satisfy $4 \le i \le j \le k \le 2i$ and $j \ge 6$ and all of i, j and k are even. Moreover, $\{a, b, c, d\}$ contains a standard triple $\{A, B, C\}$ with $A < B < C = d$. Hence, the quadruple $\{A, B, d, e\}$ is considered as the one in Section 2, v_m and w_n in Section 2 correspond to two of U_i, V_j and W_k, and Assumption 2.2 holds if $C = d > B^5 \ge b^5$, which is exactly the case where $\{A, B, C\}$ is a standard triple of the first kind in the sense of Definition 3.1 in [14].

Proof of Theorem 2.1. Suppose that $d > 10^{100}$. Then, Proposition 4.3 in [14] enables us to assume that $\{a, b, c, d\}$ contains a standard triple of the first kind. Hence, $d > b^5$ and Proposition 2.11 (1) implies that $b < 10^{10}$. It follows from Proposition 2.11 (2) that $d < b^9 < 10^{90}$, which contradicts $d > 10^{100}$. Hence, $d \le 10^{100}$. Since $d > 4abc > 4b^2$, we conclude that $b < 0.5 \cdot 10^{50} = 5 \cdot 10^{49}$. $\square$

4. The number of Diophantine quintuples

We are now left to prove our main theorem.

Proof of Theorem 1.1. Assume that $\{a,b,c,d,e\}$ is a Diophantine quintuple such that $a<b<c<d<e$. We consider the cases $d<b^5$ and $d>b^5$ separately.

Suppose first that $d<b^5$. Theorem 2.1 implies $b<5\cdot 10^{49}$ and $d<10^{100}$. We first bound the number of pairs $\{a,b\}$. If $b\le 10^{31}$, then the number of pairs is at most 10^{62}. And if $10^{31}<b<5\cdot 10^{49}$, by (8) in [9] we have

$$\log b > \frac{1}{2}\omega(b)\log\omega(b),$$

where $\omega(b)$ denotes the number of distinct prime factors of b. Now, if $2^{\omega(b)}\ge b^{0.38}$, then by the displayed inequality above we have $\omega(b)<38.41$ which yields $b<3\cdot 10^{30}$, a contradiction. Hence, $2^{\omega(b)}<b^{0.38}$, and the number of pairs $\{a,b\}$ is less than (see the proof of Theorem 1 in [9]):

$$\sum_{b=10^{31}+1}^{5\cdot 10^{49}-1} 2^{\omega(b)+1} < 2\sum_{b=10^{31}+1}^{5\cdot 10^{49}-1} b^{0.38} < 2\int_{10^{31}}^{5\cdot 10^{49}} b^{0.38}db < 6\cdot 10^{68}.$$

Therefore, the number of pairs $\{a,b\}$ is less than $6\cdot 10^{68}$.

For a fixed pair $\{a,b\}$ the number c such that $\{a,b,c\}$ is a Diophantine triple belongs to the union of finitely many binary recurrent sequences, and the number of those sequences is less than or equal to the number of solutions of the congruence $t_0^2\equiv 1 \pmod{b}$ such that $-0.71b^{0.75}<t_0<0.71b^{0.75}$ (cf. [7, Lemma 1]). This congruence comes from $bc+1=t^2$ and $t^2=t_n^2\equiv t_0^2 \pmod{b}$. If $b\le 10^{34}$, then the number of the sequences is less than or equal to $2\cdot 0.71\cdot 10^{34\cdot 0.75}<4.5\cdot 10^{25}$. And assuming $10^{34}<b<5\cdot 10^{49}$, we conclude as above $2^{\omega(b)}<b^{0.51}$. Hence, the number of sequences is less than $2\cdot 2^{\omega(b)+1}<4\cdot b^{0.51}<9\cdot 10^{25}$ (cf. [9, Lemma 1]). Moreover, each sequence $t=t_\nu$ satisfies $(2r-1)^{\nu-1}<t_\nu=\sqrt{bc+1}$. Since we know by the assumption that $bc<d/4<b^5/4$, we obtain $(1.64\sqrt{b})^{\nu-1}<0.51b^{5/2}$ and $\nu\le 3$. Hence, the number of elements contained in each of the sequences is less than or equal to 3. Furthermore, the second author proved in [13] and [14] that for a fixed Diophantine triple $\{a,b,c\}$ there are at most four ways for it to be extended to a quintuple. Consequently, we see that the number of Diophantine quintuples is less than

$$6\cdot 10^{68}\cdot 9\cdot 10^{25}\cdot 3\cdot 4 < 7\cdot 10^{95}.$$

Suppose secondly that $d > b^5$. Then, $b < d^{1/5} < 10^{20}$ and the number of the pairs $\{a, b\}$ is less than 10^{40}. For a fixed pair $\{a, b\}$ the number of sequences attached to the third element c is less than $2 \cdot 0.71 \cdot 10^{20 \cdot 0.75} < 2 \cdot 10^{15}$ and the number of elements contained in each of the sequences is less than or equal to $\nu \le 6$ (note that by Proposition 2.11 $bc < b^9/4$ and $(1.64\sqrt{b}\,)^{\nu-1} < 0.51 b^{9/2}$). It follows that the number of Diophantine quintuples is less than

$$10^{40} \cdot 2 \cdot 10^{15} \cdot 6 \cdot 4 < 10^{57}.$$

To sum up, we obtain the bound 10^{96} as in the assertion. □

5. Concluding remarks

In this section, we explain that the upper bound 10^{96} is (more or less) best possible when we use Rickert's theorem.

We first consider whether one can further improve Theorem 2.5, that is, whether one can take better quantities in Lemma 2.7. In order to do it (essentially), we have to reduce "λ", that is, make L larger or D, P smaller.

For L, following [2, p. 186] one can see that

$$\left| I_i \left(\frac{1}{N} \right) \right| > \frac{1}{\pi N^{3k}} \int_0^\infty \frac{x^{k+1/2}}{(x+\alpha)^{3k+1}} dx = \frac{1}{\alpha^{2k-1/2} N^{3k}} \cdot \frac{2k+1}{4k-1} \binom{4k}{k} 2^{-6k},$$

where $\alpha = 1 + b/N$. By Stirling's formula

$$n! = \sqrt{2\pi} n^{n-1/2} e^{\mu_n - n} \quad \text{with } 0 < \mu_n < \frac{1}{12n},$$

we have

$$\left| I_i \left(\frac{1}{N} \right) \right| > 0.8 \cdot \frac{2k+1}{4k+1} \sqrt{\frac{2\alpha}{3\pi k}} \left(\frac{27}{4\alpha^2} N^3 \right)^{-k}.$$

Hence, the value L one could take is at most $27(1 + b/N)^2 N^3$, which is merely 1.1 times larger than our choice $L = 27(1 - b/N)^2 N^3$ in our situation $N = abc$.

For P, we have to estimate $|A(z)| = |z(z-a)(z-b)|$. Let Γ_j be the contour defined by $|z - a_j| = \min_{i \ne j} \{|a_j - a_i|/2\}$. Then, we have $|A(z)| \le 3a^2(a+2b)/8$ on Γ_0 and $|A(z)| \le 3(3b-a)(b-a)^2/8$ on Γ_2. On Γ_1, we have $|A(z)| \le 3\zeta/8$, where ζ is defined in (2.8). Since

$$\begin{aligned} \left| p_{ii} \left(\frac{1}{N} \right) \right| \left(1 + \frac{a_i}{N} \right)^{1/2} &= \frac{1}{2\pi} \left| \int_{\Gamma_i} \frac{(1 + z/N)}{(z - a_i)(A(z))^k} dz \right| \\ &\ge \frac{r_i (1 - a/(2N))}{\max_{z \in \Gamma_i} |A(z)|^k}, \quad \text{where } r_i \text{ is the radius of } \Gamma_i, \end{aligned}$$

and p, P satisfy $|p_{ijk}| = |p_{ij}(1/N)| \le pP^k$ for all i, j, k, we see that the lower bound for P is $8/(3\zeta)$. This value $8/(3\zeta)$ is less than one third of our choice $P = 8(1 + (3b - a)/(2N))/\zeta$.

For D, we show that in our situation $N = abc$, if $D^k p_{ijk} \in \mathbb{Z}$ for all i, j, k, then $D \equiv 0 \pmod{ab(b-a)^2N}$. It suffices to prove this for $k = 1$ and $i \ne j$. Then, since $h_0 = h_1 = h_2 = 0$, we see from (2.7) that

$$p_{ijk} = C_{ij}^{-1} = \frac{N + a_j}{N(a_j - a_i)^2(a_j - a_l)} \quad \text{with } l \notin \{i, j\}.$$

Considering the cases $(i, j) = (0, 1)$, $(0, 2)$, $(1, 2)$, one can find that if

$$\begin{aligned} \gcd(a, b) &= \gcd(a, bc + 1) = \gcd(b, ac + 1) = \gcd(b - a, ac + 1) \\ &= \gcd(b - a, bc + 1) = 1, \end{aligned} \tag{5.1}$$

then $Dp_{ijk} \in \mathbb{Z}$ implies $D \equiv 0 \pmod{ab(b-a)^2N}$. It is easy to check that there exist (infinitely) many Diophantine triples $\{a, b, c\}$ satisfying (5.1) (for example, the triple $\{K - 1, 4K, 144K^3 - 192K^2 + 76K - 8\}$ satisfies (5.1) if $K \equiv 0 \pmod 2$ and $K \equiv 2 \pmod 3$). Hence, the value D one could take is at least $ab(b - a)^2N$, which is one fourth of our choice $D = 4ab(b - a)^2N$.

To sum up, the lower bound for N such that $\lambda < 2$ can be improved only by a constant multiple (for example, if $b \ge 2a$ and $N > 0.05b^2(b - a)^3$, then $\lambda < 2$). Therefore, Theorem 2.5 even with the improved assumption on N cannot be applied to a Diophantine quadruple containing a standard triple of the second or the third kind in general.

Secondly, we consider whether the bound $d \le 10^{100}$ can be reduced. In Theorem 2.1, we proved $d \le 10^{100}$ by using Proposition 4.3 in [14], which states that if $d > 10^{100}$, then a Diophantine quadruple $\{a, b, c, d\}$ contains a standard triple of the first kind, to which Theorem 2.5 can be applied. In the proof of the proposition, it is shown that if $d > 10^{100}$ and if $\{a, b, c, d\}$ contains a standard triple of the second or the third kind, then $d^{0.19} < 7.2 \cdot 10^{18}$. This does not lead to a contradiction if $d > 10^{99}$. Hence, in order to ensure that $\{a, b, c, d\}$ contains a triple of the first kind, we have to assume that $d > 10^{100}$.

Also we cannot significantly reduce the bound for b by this method. We got the bound $b < 10^{10}$ only on the assumption 2.2 and in our proof we use the fact that our quadruple $\{a, b, c, d\}$ contains the triple of the first kind.

Consequently, it is deduced that we cannot essentially improve the bound 10^{96} using Rickert's theorem. In order to do that or to settle the conjecture on Diophantine quintuples, either another tool or a significant advance in computer technology would be necessary.

Acknowlegements. The authors would like to thank the referees for their helpful comments and suggestions, especially for suggesting to consider whether our bound is best possible or not.

References

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

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

[3] N. C. Bonciocat, M. Cipu and M. Mignotte, On $D(-1)$-quadruples, preprint.

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

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

[7] A. Dujella, An absolute bound for the size of Diophantine m-tuples, *J. Number Theory* **89** (2001), 126–150.

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

[9] A. Dujella, On the number of Diophantine m-tuples, *Ramanujan J.* **15** (2008), 37–46.

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

[11] A. Filipin and Y. Fujita, The relative upper bound for the third element in a $D(-1)$-quadruple, *Math. Commun.* (*to appear*).

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

[13] Y. Fujita, Any Diophantine quintuple contains a regular Diophantine quadruple, *J. Number Theory* **129** (2009), 1678–1697.

[14] Y. Fujita, The number of Diophantine quintuples, *Glas. Mat. Ser.* III **45** (2010), 15–29.

[15] B. He and A. Togbé, On a family of Diophantine triples $\{k, A^2k+2A, (A+1)^2k+2(A+1)\}$ with two parameters, *Acta Math. Hungar.* **124** (1–2) (2009), 99–113.

[16] B. He and A. Togbé, On a family of Diophantine triples $\{k, A^2k+2A, (A+1)^2k+2(A+1)\}$ with two parameters II, *Periodica Math. Hungar.* (*to appear*).

[17] J. H. Rickert, Simultaneous rational approximation and related Diophantine equations, *Math. Proc. Cambridge Philos. Soc.* **11** (1993), 461–472.

ALAN FILIPIN
FACULTY OF CIVIL ENGINEERING
UNIVERSITY OF ZAGREB
FRA ANDRIJE KAČIĆA-MIOŠIĆA 26
10000 ZAGREB
CROATIA

E-mail: filipin@grad.hr

YASUTSUGU FUJITA
DEPARTMENT OF MATHEMATICS
COLLEGE OF INDUSTRIAL TECHNOLOGY
NIHON UNIVERSITY
2-11-1 SHIN-EI, NARASHINO, CHIBA
JAPAN

E-mail: fujita.yasutsugu@nihon-u.ac.jp

(Received April 4, 2011, revised December 24, 2011)