# THE NUMBER OF DIOPHANTINE QUINTUPLES

Yasutsugu Fujita

College of Industrial Technology, Nihon University, Japan

ABSTRACT. A set $\{a_1, \ldots, a_m\}$ of $m$ distinct positive integers is called a Diophantine $m$-tuple if $a_i a_j + 1$ is a perfect square for all $i$, $j$ with $1 \leq i < j \leq m$. It is known that there does not exist a Diophantine sextuple and that there exist only finitely many Diophantine quintuples. In this paper, we first show that for a fixed Diophantine triple $\{a, b, c\}$ with $a < b < c$, the number of Diophantine quintuples $\{a, b, c, d, e\}$ with $c < d < e$ is at most four. Using this result, we further show that the number of Diophantine quintuples is less than $10^{276}$, which improves the bound $10^{1930}$ due to Dujella.

## 1. INTRODUCTION

Diophantus posed the problem of finding a set of four (positive rational) numbers which has the property that the product of any two numbers in the set increased by one is a square, and found such a set $\{1/16, 33/16, 68/16, 105/16\}$. A set $\{a_1, \ldots, a_m\}$ of $m$ distinct positive integers is called *a Diophantine m-tuple* if $a_i a_j + 1$ is a perfect square for all $i$, $j$ with $1 \leq i < j \leq m$. Fermat found the first example of a Diophantine quadruple, which was the set $\{1, 3, 8, 120\}$.

Euler found that for any Diophantine pair $\{a, b\}$ the set $\{a, b, a+b+2r\}$ is a Diophantine triple, where $r = \sqrt{ab + 1}$. We call such a triple *regular*. In 1979, Arkin-Hoggatt-Strauss ([1]) found that for any Diophantine triple $\{a, b, c\}$ the set $\{a, b, c, d_+\}$ is a Diophantine quadruple, where $d_+ = a+b+c+2abc+2rst$ and $r = \sqrt{ab + 1}$, $s = \sqrt{ac + 1}$, $t = \sqrt{bc + 1}$, and conjectured the following.

CONJECTURE 1.1. *If $\{a, b, c, d\}$ is a Diophantine quadruple with $a < b < c < d$, then $d = d_+$.*

We say that a Diophantine quadruple $\{a, b, c, d\}$ with $a < b < c < d$ is *regular* if $d = d_+$. Conjecture 1.1 immediately implies a folklore conjecture, which says that there does not exist a Diophantine quintuple. It is known that there does not exist a Diophantine sextuple and that there does not exist only finitely many Diophantine quintuples ([8]). Recently, we ([12]) showed that if $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$, then $d = d_+$ (note that all the quadruples contained in the quintuple, other than $\{a, b, c, d\}$, are irregular; see Section 1 in [12]).

The first result supporting Conjecture 1.1 is due to Baker and Davenport ([2]), which asserts that if $\{1, 3, 8, d\}$ is a Diophantine quadruple, then $d = 120$. This result has been generalized and it is known that the Diophantine quadruples containing the pairs $\{k - 1, k + 1\}$ with $k \geq 2$ (cf. [4, 5, 10, 11]) or the triples $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$ with $k \geq 1$ (cf. [6]), where $F_\nu$ is the $\nu$-th Fibonacci number, are always regular. Besides them, the Diophantine quadruples containing the following triples are regular:

$\{1, 8, 15\}$, $\{1, 8, 120\}$, $\{1, 15, 24\}$, $\{1, 24, 35\}$, $\{2, 12, 24\}$   (by Kedlaya [13]),

$\{4, 12, 30\}$   (by Dujella [8, p. 213]).

Thus, one may easily check that if $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$, then $b \geq 8$, $d \geq 6440$ and

$$ad \geq 6888 \qquad \text{(coming from } \{1, 35, 48, 6888\}),$$
$$bd \geq 16 \cdot 6440 \qquad \text{(coming from } \{3, 16, 33, 6440\}).$$

The last two lower bounds play important roles in proving Theorem 1.2.

We are interested in bounding the number of Diophantine quintuples. We first consider the number of Diophantine quintuples $\{a, b, c, d, e\}$ with $a < b < c < d < e$ for a fixed triple $\{a, b, c\}$. Since the above-mentioned result ([12]) implies that $d$ is unique, it suffices to bound the number of the $e$'s. The essential tool to do this is an exponential gap principle between the solutions due to Okazaki (cf. [3, Lemma 2.2]), which we may apply if there exist five such $e$'s. Thus, we obtain the following.

THEOREM 1.2. *Fix a Diophantine triple $\{a, b, c\}$ with $a < b < c$. Then the number of Diophantine quintuples $\{a, b, c, d, e\}$ with $c < d < e$ is at most four.*

Using Theorem 1.2, one may easily improve the bound $10^{1930}$ due to Dujella ([9]) for the number of Diophantine quintuples. In fact, we reduce it to about the one-seventh power further by improving the upper bounds for $b$ and $d$ (in particular, for $b$).

THEOREM 1.3. *The number of Diophantine quintuples is less than $10^{276}$.*

This paper is organized as follows. In Section 2, we rephrase the assumption that $\{a, b, c, d, e\}$ is a Diophantine quintuple in terms of a system of three

Diophantine equations, which induces binary recurrent sequences. Then, we completely determine the initial terms of the sequences. In Section 3, using some congruence relations we give lower bounds for the solutions. In Section 4, using Baker's theory we give upper bounds for the solutions and for $b$ and $d$. It is to be noted that its proof tells that any regular Diophantine triple $\{a, b, c\}$ with $c = a + b + 2r > 10^{50}$ cannot be extended to a Diophantine quintuple (cf. Corollary 4.5). In Section 5, we give an exponential gap principle between the solutions. Combining it with the upper bound for the solutions we prove Theorem 1.2. Finally, in Section 6 using the bounds for $b$ and $d$ and Theorem 1.2, we prove Theorem 1.3 along the same lines as Theorem 4 in [9].

## 2. The fundamental solutions of the system of Diophantine equations

In this section, we transform the problem into solving a system of three Diophantine equations, which induces binary recurrent sequences $\{u_l\}, \{v_m\}, \{w_n\}$. Then, we determine the initial terms of the sequences, which we call *the fundamental solutions* of the system. We also examine the relationship between $l$, $m$ and $n$ in the case of $u_l = v_m = w_n$.

Let $\{a, b, c\}$ be a Diophantine triple with $a < b < c$, and $r, s, t$ positive integers such that

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

Furthermore, suppose that $\{a, b, c, d, e\}$ is a Diophantine quintuple with $c < d < e$, and put

$$ad + 1 = x^2, \ bd + 1 = y^2, \ cd + 1 = z^2$$

with positive integers $x, y, z$. Then there exist integers $\alpha, \beta, \gamma, \delta$ such that

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

from which, by eliminating $e$, we obtain the system of Diophantine equations.

$$(2.1) \qquad\qquad a\delta^2 - d\alpha^2 = a - d,$$

$$(2.2) \qquad\qquad b\delta^2 - d\beta^2 = b - d,$$

$$(2.3) \qquad\qquad c\delta^2 - d\gamma^2 = c - d.$$

Note that by Theorem 2.1 in [12] we know that $d = d_+ = a + b + c + 2abc + 2rst$.

LEMMA 2.1. (cf. [8, Lemma 1],[12, Lemma 2.1]) *Let $(\delta, \alpha)$, $(\delta, \beta)$, $(\delta, \gamma)$ be positive solutions of* (2.1), (2.2), (2.3), *respectively. Then there exist solutions*

$(\delta_0, \alpha_0)$ *of* (2.1), $(\delta_1, \beta_1)$ *of* (2.2) *and* $(\delta_2, \gamma_2)$ *of* (2.3) *in the ranges*

$$1 \le \alpha_0 \le \sqrt{\frac{x+1}{2}} < 0.76\sqrt[4]{ad}, \qquad 1 \le |\delta_0| \le \sqrt{\frac{d\sqrt{d}}{2\sqrt{a}}} < 0.269d,$$

$$1 \le \beta_1 \le \sqrt{\frac{y+1}{2}} < 0.723\sqrt[4]{bd}, \qquad 1 \le |\delta_1| \le \sqrt{\frac{d\sqrt{d}}{2\sqrt{b}}} < 0.148d,$$

$$1 \le \gamma_2 \le \sqrt{\frac{z+1}{2}} < 0.723\sqrt[4]{cd}, \qquad 1 \le |\delta_2| \le \sqrt{\frac{d\sqrt{d}}{2\sqrt{c}}} < 0.148d$$

*such that*

$$(2.4) \qquad \delta\sqrt{a} + \alpha\sqrt{d} = (\delta_0\sqrt{a} + \alpha_0\sqrt{d})(x + \sqrt{ad})^l,$$

$$(2.5) \qquad \delta\sqrt{b} + \beta\sqrt{d} = (\delta_1\sqrt{b} + \beta_1\sqrt{d})(y + \sqrt{bd})^m,$$

$$(2.6) \qquad \delta\sqrt{c} + \gamma\sqrt{d} = (\delta_2\sqrt{c} + \gamma_2\sqrt{d})(z + \sqrt{cd})^n$$

*for some integers* $l, m, n \ge 0$.

PROOF. This immediately follows from Lemma 2.1 in [12].     □

By (2.4), (2.5) and (2.6), we may write $\delta$ as follows:

- $\delta = u_l$, where
  $u_0 = \delta_0$, $u_1 = x\delta_0 + d\alpha_0$, $u_{l+2} = 2xu_{l+1} - u_l$;
- $\delta = v_m$, where
  $v_0 = \delta_1$, $v_1 = y\delta_1 + d\beta_1$, $v_{m+2} = 2yv_{m+1} - v_m$;
- $\delta = w_n$, where
  $w_0 = \delta_2$, $w_1 = z\delta_2 + d\gamma_2$, $w_{n+2} = 2zw_{n+1} - w_n$.

LEMMA 2.2. *If* $\delta = u_l = v_m = w_n$, *then* $l \equiv m \equiv n \equiv 0 \pmod 2$ *and* $\delta_0 = \delta_1 = \delta_2 = \pm 1$.

PROOF. If $l$ is odd, then by Lemma 8 in [8] we have $|\delta_0| = y$ and $|\delta_0| = z$, which are contradictions. Similarly, if $m$ is odd, then $|\delta_1| = x$, $|\delta_1| = z$, and if $n$ is odd, then $|\delta_2| = x$, $|\delta_2| = y$; in any case, we arrive at contradictions. It follows that $l$, $m$, $n$ must be all even. Then Lemma 3 in [7] implies that $\delta_0 = \delta_1 = \delta_2$.

Put $e_0 = (\delta_0^2 - 1)/d$. Then

$$ae_0 + 1 = \alpha^2, \ be_0 + 1 = \beta^2, \ ce_0 + 1 = \gamma^2, \ de_0 + 1 = \delta_0^2.$$

If $\delta_0^2 \ne 1$, then $\{a, b, c, d, e_0\}$ is a Diophantine quintuple with $e_0 < d$, which contradicts $d = d_+$ (cf. Section 1). Therefore, we obtain $|\delta_0| = 1$.     □

LEMMA 2.3. *If* $\delta = u_l = v_m = w_n$, *then* $4 \le n \le m \le l \le 2n$.

PROOF. From Lemma 3 in [8] we see that

$$n - 1 \le m \le 2n + 1, \ n - 1 \le l \le 2n + 1 \ \text{ and } \ m - 1 \le l \le 2m + 1,$$

that is,

$$n - 1 \le m \le 2n + 1 \ \text{ and } \ m - 1 \le l \le 2n + 1,$$

which together with Lemma 2.2 imply that $n \le m \le l \le 2n$.

The first inequality $n \ge 4$ follows from Lemmas 2.4 to 2.7 in [12] (see also [12, p. 7]). □

We need the following lemma in order to prove Theorem 1.2.

LEMMA 2.4. *If $\delta = u_l = v_m = w_n$, then $m \ge 6$.*

PROOF. It suffices to show that $u_4 \ne v_4$ and $u_6 > v_4$. The latter immediately follows from Lemma 2.10 (1) in [12] and its proof, in view of $\delta_0 = \delta_1 = \pm 1$ and $d > 4abc > b^2$. Suppose that $u_4 = v_4$. By Lemma 2.2 we have

$$\pm 2a(ad + 1) + (2ad + 1)x = \pm 2b(bd + 1) + (2bd + 1)y.$$

Since $2(by - ax)d + y - x > 0$, we have

$$2(b - a)\left\{(b - a)d + 1\right\} = 2(by - ax)d + y - x.$$

However, $d > 4abc > b^2$ implies that $(b-a)d+1 < yd$ and $by - ax > (b-a)y$, which are contradictions. □

## 3. LOWER BOUNDS FOR SOLUTIONS

In this section, we first introduce the notion of "standard triples". Then, we give lower bounds for $m$ in terms of $d$.

DEFINITION 3.1. Let $\{a, b, c\}$ be a Diophantine triple with $a < b < c$. We call $\{a, b, c\}$ a Diophantine triple of

(i) *the first kind* if $c > b^5$;
(ii) *the second kind* if $b > 4a$ and $c \ge b^2$;
(iii) *the third kind* if $b > 12a$ and $b^{5/3} < c < b^2$.

A Diophantine triple is called *standard* if it is of the first, the second or the third kind.

REMARK 3.2. The definition of standard triples in [8] differs from the one above in the following:

- The condition for the first kind in [8] is $c > b^{4.5}$;
- The second and the fourth kind in [8] correspond to the second kind above.

We modified the first kind in order to get better upper bounds for $b$ and $d$, and combined the second and the fourth kind because dividing those cases does not affect the bounds (see the proof of Proposition 4.3).

LEMMA 3.3. *Any Diophantine quadruple contains a standard triple.*

PROOF. Let $\{a, b, c, d\}$ be a Diophantine quadruple. In view of the proof of Proposition 2 in [8], we may assume that $\{a, b, c, d\}$ is regular and $b < 4a$. If $c > b^3$, then $d > 4abc > b^5$, whence $\{a, b, d\}$ is of the first kind. Assume that $c \le b^3$. Then, from the same argument as in the proof of Proposition 2 in [8] we see that either

$$\text{(i) } c = a + b + 2r \quad \text{or} \quad \text{(ii) } c > 4ab + 2a + 2b,$$

and that in the case of (i), $\{a, c, d\}$ is of the second kind; in the case of (ii), $d < c^2$ and $d > 4abc > b^2 c \ge c^{5/2}$, whence $\{a, c, d\}$ is of the third kind. ☐

REMARK 3.4. It follows from the proof of Lemma 3.3 that any Diophantine quadruple $\{a, b, c, d\}$ with $a < b < c < d$ contains a standard triple $\{A, B, C\}$ with $A < B < C = d$.

LEMMA 3.5. *Suppose that $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$. Assume that $d > 10^{100}$.*
  (i) *If $\{a, b, c, d\}$ contains a triple of the first kind, then $m > d^{0.025}$.*
  (ii) *If $\{a, b, c, d\}$ contains a triple of the second kind, then $m > d^{0.24}$.*
  (iii) *If $\{a, b, c, d\}$ contains a triple of the third kind, then $m > d^{0.19}$.*

PROOF. Let $\{A, B, C\}$ be a standard triple with $A < B < C$ contained in $\{a, b, c, d\}$, and $\{V_j\}$ and $\{W_k\}$, which are two of $\{u_l\}$, $\{v_m\}$ and $\{w_n\}$, the attached sequences with $4 \le k \le j \le 2k$. Put $S = \sqrt{AC + 1}$ and $T = \sqrt{BC + 1}$. It suffices to show that

$$\text{(i) } k > C^{0.025}, \quad \text{(ii) } k > C^{0.24}, \quad \text{(iii) } k > C^{0.19}.$$

(i) Suppose that $k \le C^{0.025}$. By Lemma 9 in [8] and Lemma 2.2, we have

$$\pm Aj^2 + Sj \equiv \pm Bk^2 + Tk \pmod{4C}.$$

Since $Aj^2 < C^{0.2} \cdot 4C^{0.05} < C$, $Sj < \sqrt{C^{1.2} + 1} \cdot 2C^{0.025} < C$, $Bk^2 < C^{0.2}C^{0.05} < C$, $Tk < \sqrt{C^{1.2} + 1}\, C^{0.025} < C$, we have

$$(3.1) \qquad\qquad \pm Aj^2 + Sj = \pm Bk^2 + Tk.$$

Squaring (3.1) twice, we have

$$(3.2) \qquad \left\{ (Aj^2 - Bk^2)^2 - j^2 - k^2 \right\}^2 \equiv 4j^2 k^2 \pmod{C}.$$

Since $k \le C^{0.025}$ yields

$$\left\{ (Aj^2 - Bk^2)^2 - j^2 - k^2 \right\}^2 < (Bk^2)^4 < C^{0.8}C^{0.2} = C,$$
$$4j^2 k^2 \le 16k^4 \le 16C^{0.1} < C,$$

the congruence (3.2) is in fact an equation, that is,

$$(3.3) \qquad\qquad Aj^2 - Bk^2 = \mp(j + k).$$

By (3.1) and (3.3), we have $j(S \mp 1) = k(T \pm 1)$, which together with (3.1) implies that

$$\pm \left\{ A \left( \frac{T \pm 1}{S \mp 1} \right)^2 - B \right\} k = T - \frac{S(T \pm 1)}{S \mp 1}.$$

It follows from $C = d > 10^{100}$ that

$$k = \frac{(S+1)(T+S)}{2(AT + BS - A + B)} > \frac{AC}{B(2S+1)} > 0.49 C^{0.3} > C^{0.025},$$

which contradicts the assumption. Therefore, we obtain $k > C^{0.025}$.

(ii) Note that in this case Lemma 4 in [8] and $k \geq 4$ together imply that $j \leq 3k/2 + 1/2 \leq 1.625k$. Suppose that $k \leq C^{0.24}$. Since $Aj^2 < \frac{1}{4} C^{0.5} \left( 1.625 C^{0.24} \right)^2 < C$, $Sj < \sqrt{\frac{1}{4} C^{1.5} + 1} \cdot 1.625 C^{0.24} < C$, $Bk^2 < C^{0.5} \left( C^{0.24} \right)^2 < C$, $Tk < \sqrt{C^{1.5} + 1} \, C^{0.24} < C$, we have the equation (3.1). We now have

$$\frac{Aj}{S} < \frac{j\sqrt{A}}{\sqrt{C}} < \frac{1.625 C^{0.24} \cdot 0.5 C^{0.25}}{C^{0.5}} = 0.8125 C^{-0.01} < 0.08125,$$

$$\frac{Bk}{T} < \frac{k\sqrt{B}}{\sqrt{C}} < \frac{C^{0.24} C^{0.25}}{C^{0.5}} = C^{-0.01} < 0.1.$$

It follows from (3.1) that $1.08125 Sj > 0.9 Tk$, that is,

$$\frac{j}{k} > \frac{0.9}{1.08125} \cdot \frac{T}{S} > 0.832 \sqrt{\frac{B}{A}} > 1.664,$$

which contradicts $j \leq 1.625k$. Therefore, we obtain $k > C^{0.24}$.

(iii) Note that in this case Lemma 4 in [8] and $k \geq 4$ together imply that $j \leq 8k/5 + 3/5 \leq 1.75k$. Suppose that $k \leq C^{0.19}$. Since $Aj^2 < \frac{1}{12} C^{0.6} \left( 1.75 C^{0.19} \right)^2 < C$, $Sj < \sqrt{\frac{1}{12} C^{1.6} + 1} \cdot 1.75 C^{0.19} < C$, $Bk^2 < C^{0.6} \left( C^{0.19} \right)^2 < C$, $Tk < \sqrt{C^{1.6} + 1} \, C^{0.19} < C$, we have the equation (3.1). In the same way as (ii), we see that

$$\frac{Aj}{S} < 0.05052, \quad \frac{Bk}{T} < 0.1,$$

and that $1.05052 Sj > 0.9 Tk$, that is, $j/k > 2.965$, which contradicts $j \leq 1.75k$. Therefore, we obtain $k > C^{0.19}$. This completes the proof of Lemma 3.5. $\square$

## 4. Upper bounds for $b$ and $d$

In this section, combining Lemma 3.5 with a theorem of Matveev ([14]) we give upper bounds for $b$ and $d$. In its proof, it emerges that if $d > 10^{100}$, then $d > b^5$, which implies that any regular Diophantine triple $\{a, b, c\}$ with $c = a + b + 2r > 10^{50}$ cannot be extended to a Diophantine quintuple.

We begin by quoting the theorem of Matveev.

THEOREM 4.1 ([14]). *Let $\Lambda$ be a linear form in logarithms of $N$ multiplicatively independent totally real algebraic numbers $\alpha_1, \ldots, \alpha_N$ with rational integer coefficients $b_1, \ldots, b_N$ ($b_N \neq 0$). Let $h(\alpha_j)$ denote the absolute logarithmic height of $\alpha_j$ for $1 \leq j \leq N$. Define the numbers $D$, $A_j$ ($1 \leq j \leq N$) and $E$ by $D = [\mathbb{Q}(\alpha_1, \ldots, \alpha_N) : \mathbb{Q}]$, $A_j = \max\{Dh(\alpha_j), |\log \alpha_j|\}$, $E = \max\{1, \max\{|b_j|A_j/A_N; 1 \leq j \leq N\}\}$. Then,*

$$\log |\Lambda| > -C(N)C_0 W_0 D^2 \Omega,$$

*where*

$$C(N) = \frac{8}{(N-1)!}(N+2)(2N+3)(4e(N+1))^{N+1},$$

$$C_0 = \log(e^{4.4N+7} N^{5.5} D^2 \log(exD)),$$

$$W_0 = \log(1.5exED \log(exD)), \quad \Omega = A_1 \cdots A_N.$$

PROPOSITION 4.2. *Suppose that $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$. Then,*

$$\frac{m}{\log(351m)} < 2.786 \cdot 10^{12}(\log d)^2$$

*with $m$ as in the equation (2.5).*

PROOF. Let $A, B, C, S, T$ and $V_j, W_k$ be as in the proof of Lemma 3.5. We may assume that $C(= d) > B^{5/3}$ and $C \geq 6440 > 10^3$ (cf. Section 1). Put

$$\Lambda = j \log \xi - k \log \eta + \log \mu,$$

where

$$\xi = S + \sqrt{AC}, \quad \eta = T + \sqrt{BC}, \quad \mu = \frac{\sqrt{B}(\sqrt{C} \pm \sqrt{A})}{\sqrt{A}(\sqrt{C} \pm \sqrt{B})}.$$

Then, by (60) in [8] we know that

(4.1) $$0 < \Lambda < \frac{8}{3}AC\xi^{-2j}.$$

We apply Theorem 4.1 with $N = 3$, $D = 4$, $\alpha_1 = \xi$, $\alpha_2 = \eta$, $\alpha_3 = \mu$. We have

$$A_1 = 2\log \alpha_1 < 2\log(2\sqrt{AC+1}) < 2\log(2.0001C^{0.8}) < 1.8007 \log C,$$

$$A_2 = 2\log \alpha_2 < 2\log(2\sqrt{BC+1}) < 2\log(2.0001C^{0.8}) < 1.8007 \log C.$$

Since the minimal polynomial of $\mu$ is

$$A^2(C-B)^2 X^4 + 4A^2 B(C-B)X^3 + 2AB(3AB - AC - BC - C^2)X^2$$
$$+ 4AB^2(C-A)X + B^2(C-A)^2$$

up to a multiple of a constant, the leading coefficient $a_0$ of the minimal polynomial of $\mu$ satisfies

$$\frac{1}{4}\left(\frac{C}{B} - 1\right) \le a_0 \le A^2(C - B)^2.$$

Since

$$\sqrt{\frac{B}{A}} < \frac{\sqrt{B}(\sqrt{C} \pm \sqrt{A})}{\sqrt{A}(\sqrt{C} - \sqrt{B})} < \frac{\sqrt{B}(\sqrt{C} + \sqrt{B})^2}{\sqrt{A}(C - B)}$$

$$< \frac{\sqrt{B}(1 + \sqrt{B/C})^2}{\sqrt{A}(1 - B/C)} < 1.6709\sqrt{\frac{B}{A}},$$

$$\sqrt{\frac{B}{A}} > \frac{\sqrt{B}(\sqrt{C} \pm \sqrt{A})}{\sqrt{A}(\sqrt{C} + \sqrt{B})} > \frac{\sqrt{B}(\sqrt{C} - \sqrt{B})^2}{\sqrt{A}(C - B)}$$

$$> \left(1 - \sqrt{\frac{B}{C}}\right)^2 \sqrt{\frac{B}{A}} > 0.5607\sqrt{\frac{B}{A}},$$

we have

$$A_3 = 4h(\mu) < \log\left(1.6709^2 B^2(C - B)^2\right) < 3.3489\log C,$$

and noting that $\{A, B, C\}$ is a standard triple with $C > 10^3$ we have

$$A_3 > \log\left(0.5607^2\frac{B(C - B)}{4A^2}\right) > \log(C^{1/5}) = 0.2\log C.$$

Since $k \le j$, we have

$$E < \frac{jA_1}{A_3} < 9.0035j.$$

Hence we obtain the following:

$$C(3) = \frac{8}{2} \cdot 5 \cdot 9(16e)^4 < 6.4407 \cdot 10^8,$$

$$C_0 = \log\left(e^{20.2} \cdot 3^{5.5} \cdot 16\log(4e)\right) < 29.8847,$$

$$W_0 = \log\left(6exE\log(4e)\right) < \log(351j),$$

$$\Omega = A_1 A_2 A_3 < 10.8583(\log C)^3.$$

Since

$$\log\frac{8}{3}AC\xi^{-2j} < \log\frac{8}{3}C(4C)^{-j} < -1.2006j\log C,$$

Theorem 4.1 and (4.1) together yield

$$1.2006j\log C < 6.4407 \cdot 10^8 \cdot 29.8847 \cdot 16 \cdot 10.8583(\log C)^3\log(351j),$$

whence we obtain

$$\frac{j}{\log(351j)} < 2.786 \cdot 10^{12}(\log C)^2.$$

Proposition 4.2 now follows from $j \ge m$ and $C = d$. $\qquad\qquad \square$

PROPOSITION 4.3. *Suppose that $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$. Then, $d < 10^{830}$ and $b < 10^{166}$. Moreover, if $d > 10^{100}$, then $d > b^5$.*

PROOF. We may assume that $d > 10^{100}$. In case $\{a, b, c, d\}$ contains a triple of the first kind, by Lemma 3.5 we have $m > d^{0.025}$, which together with Proposition 4.2 implies that

$$f(m) := \frac{m}{\log(351m)(\log m)^2} < 4.458 \cdot 10^{15}.$$

Hence we have $m < 5.45 \cdot 10^{20}$. It follows that $d < m^{40} < 10^{830}$ and $b < d^{0.2} < m^8 < 10^{166}$.

In case $\{a, b, c, d\}$ contains a triple of the second or the third kind, $m > d^{0.19}$ and Proposition 4.2 together imply that $f(m) < 7.718 \cdot 10^{13}$, which yields $m < 7.2 \cdot 10^{18}$. On the other hand, the assumption $d > 10^{100}$ implies that $m > d^{0.19} > 10^{19}$, which is a contradiction. Therefore, we obtain $d < 10^{830}$ and $b < 10^{166}$. In addition, we have proved that $\{a, b, c, d\}$ cannot contain a triple of either the second or the third kind. Hence $\{a, b, c, d\}$ has to contain a triple of the first kind, which yields $d > b^5$. ∎

COROLLARY 4.4. *Suppose that $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$. Then, $l < 1.1 \cdot 10^{21}$.*

PROOF. If $l \geq 1.1 \cdot 10^{21}$, then by Lemma 2.3 we have $m \geq 5.5 \cdot 10^{20}$, and Proposition 4.2 implies that

$$d > \exp \sqrt{\frac{m}{2.786 \cdot 10^{12} \log(351m)}} > 2 \cdot 10^{833},$$

which contradicts Proposition 4.3. ∎

COROLLARY 4.5. *Let $\{a, b, c\}$ be a Diophantine triple with $c = a + b + 2r$, where $r = \sqrt{ab + 1}$. If $c > 10^{50}$, then $\{a, b, c\}$ cannot be extended to a Diophantine quintuple.*

PROOF. Suppose that $\{a, b, c, d, e\}$ is a Diophantine quintuple. We may assume that $c < d = d_+ < e$ by Theorem 1.2 in [12]. Since $c > 10^{50}$ means $d > c^2 > 10^{100}$, we see from Proposition 4.3 that $d > b^5$. On the other hand, since $d < 4b^2c$ and $b \geq 8$, we have $c > b^3/4 \geq 16b$, which contradicts $c = a + b + 2r < 4b$. ∎

## 5. PROOF OF THEOREM 1.2

Let $\{A, B, C\}$ be a Diophantine triple with $A < B < C$ and let $S = \sqrt{AC + 1}$, $T = \sqrt{BC + 1}$. In this section, we first give an exponential gap principle for the solutions of

(5.1)           $AZ^2 - CX^2 = A - C, \quad BZ^2 - CY^2 = B - C,$

using Okazaki's idea (cf. [3, Lemma 2.2]). Then we prove Theorem 1.2 combining the gap principle with Corollary 4.4. We may express the solutions of (5.1) as $Z = V_j = W_k$ ($j \geq 0$, $k \geq 0$) with some binary recurrent sequences $\{V_j\}$ and $\{W_k\}$ (cf. Section 2).

LEMMA 5.1. *Suppose that $V_0 = W_0 = \pm 1$ and that there exist three positive solutions $(X_i, Y_i, Z_i)$ ($1 \leq i \leq 3$) of (5.1) with $Z_1 < Z_2 < Z_3$ that come from the same fundamental solution $Z = V_0 = W_0$. Put $Z_i = V_{j_i} = W_{k_i}$ ($1 \leq i \leq 3$) with $j_1 < j_2 < j_3$. Then we have*

$$(5.2) \qquad j_3 - j_2 > \frac{3}{8AC} \Delta \xi^{2j_1} \log \eta,$$

*where*

$$\xi = S + \sqrt{AC}, \ \eta = T + \sqrt{BC}, \ \Delta = \begin{vmatrix} k_2 - k_1 & k_3 - k_2 \\ j_2 - j_1 & j_3 - j_2 \end{vmatrix} > 0.$$

PROOF. The proof proceeds along the same lines as that of Lemma 2.2 in [3]. Let $\epsilon = V_0 = W_0$. By $Z = V_j = W_k$, we have

$$Z = \frac{1}{2\sqrt{A}} \left\{ (\sqrt{C} + \epsilon \sqrt{A}) \xi^j - (\sqrt{C} - \epsilon \sqrt{A}) \xi^{-j} \right\}$$

$$= \frac{1}{2\sqrt{B}} \left\{ (\sqrt{C} + \epsilon \sqrt{B}) \eta^k - (\sqrt{C} - \epsilon \sqrt{B}) \eta^{-k} \right\},$$

whence we can find three points

$$(p_i, q_i) = (j_i \log \xi, k_i \log \eta) \quad (1 \leq i \leq 3)$$

on the curve

$$F(p, q) = (\sqrt{C} + \epsilon \sqrt{B}) e^q - (\sqrt{C} - \epsilon \sqrt{B}) e^{-q}$$

$$(5.3) \qquad - \sqrt{\frac{B}{A}} \left\{ (\sqrt{C} + \epsilon \sqrt{A}) e^p - (\sqrt{C} - \epsilon \sqrt{A}) e^{-p} \right\} = 0.$$

Since

$$F_q(p, q) = (\sqrt{C} + \epsilon \sqrt{B}) e^q + (\sqrt{C} - \epsilon \sqrt{B}) e^{-q} > 0$$

for all $p$ and $q$, we may implicitly differentiate (5.3) to obtain

$$\left\{ (\sqrt{C} + \epsilon \sqrt{B}) e^q + (\sqrt{C} - \epsilon \sqrt{B}) e^{-q} \right\} \frac{dq}{dp}$$

$$(5.4) \qquad = \sqrt{\frac{B}{A}} \left\{ (\sqrt{C} + \epsilon \sqrt{A}) e^p + (\sqrt{C} - \epsilon \sqrt{A}) e^{-p} \right\},$$

which yields

$$\frac{dq}{dp} = \sqrt{\frac{\left\{(\sqrt{C} + \epsilon\sqrt{A})e^p - (\sqrt{C} - \epsilon\sqrt{A})e^{-p}\right\}^2 + 4(C-A)}{A/B\left[\left\{(\sqrt{C} + \epsilon\sqrt{B})e^q - (\sqrt{C} - \epsilon\sqrt{B})e^{-q}\right\}^2 + 4(C-B)\right]}}$$

$$(5.5) \quad = \sqrt{\frac{\left\{(\sqrt{C} + \epsilon\sqrt{A})e^p - (\sqrt{C} - \epsilon\sqrt{A})e^{-p}\right\}^2 + 4(C-A)}{\left\{(\sqrt{C} + \epsilon\sqrt{A})e^p - (\sqrt{C} - \epsilon\sqrt{A})e^{-p}\right\}^2 + 4(AC/B - A)}} > 1.$$

Similarly, we may implicitly differentiate (5.4) to obtain

$$\left\{(\sqrt{C} + \epsilon\sqrt{B})e^q + (\sqrt{C} - \epsilon\sqrt{B})e^{-q}\right\}\frac{d^2q}{dp^2}$$

$$+ \left\{(\sqrt{C} + \epsilon\sqrt{B})e^q - (\sqrt{C} - \epsilon\sqrt{B})e^{-q}\right\}\left(\frac{dq}{dr}\right)^2$$

$$= (\sqrt{C} + \epsilon\sqrt{B})e^q - (\sqrt{C} - \epsilon\sqrt{B})e^{-q},$$

which yields

$$(5.6) \quad \frac{d^2q}{dp^2} = \left\{1 - \left(\frac{dq}{dp}\right)^2\right\}\frac{(\sqrt{C} + \epsilon\sqrt{B})e^q - (\sqrt{C} - \epsilon\sqrt{B})e^{-q}}{(\sqrt{C} + \epsilon\sqrt{B})e^q + (\sqrt{C} - \epsilon\sqrt{B})e^{-q}} < 0.$$

From (5.5) and (5.6) we see that

$$(5.7) \quad 0 < \frac{q_2 - q_1}{p_2 - p_1} - \frac{q_3 - q_2}{p_3 - p_2} < \frac{q_2 - q_1}{p_2 - p_1} - 1.$$

On the other hand, we may transform $V_{j_i} = W_{k_i}$ $(i = 1, 2)$ into inequalities for linear forms in three logarithms of algebraic numbers

$$0 < p_i - q_i + \log\mu < \frac{8}{3}AC\xi^{-2j_i} \quad (i = 1, 2),$$

where

$$\mu = \frac{\sqrt{B}(\sqrt{C} + \epsilon\sqrt{A})}{\sqrt{A}(\sqrt{C} + \epsilon\sqrt{B})}$$

(cf. (4.1)). Hence we have

$$0 < p_2 - q_2 + \log\mu < p_1 - q_1 + \log\mu < \frac{8}{3}AC\xi^{-2j_1},$$

which yields

$$(5.8) \quad 0 < (q_2 - q_1) - (p_2 - p_1) < \frac{8}{3}AC\xi^{-2j_1}.$$

It follows from (5.7) and (5.8) that

$$0 < \frac{q_2 - q_1}{p_2 - p_1} - \frac{q_3 - q_2}{p_3 - p_2} < \frac{(q_2 - q_1) - (p_2 - p_1)}{p_2 - p_1} < \frac{8AC}{3(p_2 - p_1)\xi^{2j_1}}.$$

Substituting $p_i = j_i \log \xi$ and $q_i = k_i \log \eta$, we have

$$0 < \frac{k_2 - k_1}{j_2 - j_1} - \frac{k_3 - k_2}{j_3 - j_2} < \frac{8AC}{3(j_2 - j_1)\xi^{2j_1} \log \eta}.$$

Therefore, we obtain

$$j_3 - j_2 > \frac{3}{8AC} \Delta \xi^{2j_1} \log \eta,$$

as desired. □

We are now ready to prove Theorem 1.2.

PROOF OF THEOREM 1.2. Suppose that there exist five Diophantine quintuples $\{a, b, c, d, e\}$ ($c < d < e$) containing the fixed triple $\{a, b, c\}$. Since $d = d_+$ by Theorem 1.2 in [12], we have five such $e$'s, which yield five positive solutions

$$\delta = u_{l_i} = v_{m_i} = w_{n_i} \quad (1 \le i \le 5)$$

with $l_1 < l_2 < l_3 < l_4 < l_5$ of the system of Diophantine equations (2.1), (2.2), (2.3). Let $\{A, B, C\}$ be a standard triple with $A < B < C$ contained in $\{a, b, c, d\}$ and $Z = V_j = W_k$ the solutions of (5.1). Then, $V_0 = W_0 = \pm 1$ by Lemma 2.2 and we have three positive solutions $(X_i, Y_i, Z_i)$ ($1 \le i \le 3$) of (5.1) that come from the same fundamental solution. Hence, putting $Z_i = V_{j_i} = W_{k_i}$, we have the gap principle (5.2). Since we may assume that $C = d$, we know that $AC \ge ad \ge 6888$ and $BC \ge bd \ge 16 \cdot 6440$ (cf. Section 1), which together with Lemma 2.4 imply that

$$\frac{\xi^{2j_1}}{AC} > \frac{(2\sqrt{ad})^{2m_1}}{ad} \ge 2^{12}(ad)^5 > 6.35 \cdot 10^{22},$$
$$\log \eta > \log(2\sqrt{bd}) > 6.46.$$

Moreover, since each of $l_i$, $m_i$ and $n_i$ is even by Lemma 2.2, we have $\Delta \equiv 0$ (mod 4), which yields $\Delta \ge 4$. It follows from (5.2) that

$$l_5 \ge j_3 > 1.5 \cdot 6.35 \cdot 10^{22} \cdot 6.46 > 6.15 \cdot 10^{23},$$

which contradicts Corollary 4.4. This completes the proof of Theorem 1.2. □

## 6. Proof of Theorem 1.3

In this section, we prove Theorem 1.3 along the same lines as Theorem 4 in [9].

Proof of Theorem 1.3. Suppose that $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$. We know by Proposition 4.3 that $d < 10^{830}$ and $b < 10^{166}$. We first bound the number of the $\{a, b\}$'s. If $b \leq 10^{102}$, then the number is at most $10^{204}$. Assume that $10^{102} < b < 10^{166}$. By (8) in [9] we have

$$(6.1) \qquad \log b > \frac{1}{2}\omega(b)\log\omega(b),$$

where $\omega(b)$ denotes the number of distinct prime factors of $b$. If $2^{\omega(b)} \geq b^{0.3}$, then (6.1) implies that $\omega(b) < 101.6$, which yields $b < 10^{102}$, a contradiction. Hence we have $2^{\omega(b)} < b^{0.3}$, and the number of corresponding $\{a, b\}$'s is less than the following (see the proof of Theorem 1 in [9]):

$$\sum_{b=10^{102}+1}^{10^{166}-1} 2^{\omega(b)+1} < 2 \sum_{b=10^{102}+1}^{10^{166}-1} b^{0.3} < 2 \int_{10^{102}}^{10^{166}} b^{0.3}\, db < 10^{216}.$$

Therefore, the number of the $\{a, b\}$'s is less than $10^{216}$.

Secondly, for a fixed $\{a, b\}$ 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 the sequences is less than or equal to the number of solutions of the congruence $z_0^2 \equiv 1 \pmod{b}$ with $-0.71b^{0.75} < z_0 < 0.71b^{0.75}$ (cf. [7, Lemma 1]). If $b \leq 10^{58}$, then the number of the sequences is $2 \cdot 0.71 \cdot 10^{58 \cdot 0.75} < 5 \cdot 10^{43}$. Assume that $10^{58} < b < 10^{166}$. We see from (6.1) that $2^{\omega(b)} < b^{1/3}$ in the same way as above. Hence, the number of the sequences is less than $2 \cdot 2^{\omega(b)+1} < 4b^{1/3} < 9 \cdot 10^{55}$ (cf. [9, Lemma 1]). Moreover, the number of elements contained in each of the sequences is less than $\log_{32}(10^{830}) < 600$ (see the proof of Theorem 4 in [9]). Therefore, the number of the $c$'s is less than $9 \cdot 10^{55} \cdot 600 < 6 \cdot 10^{58}$.

Consequently, we see from Theorem 1.2 that the number of Diophantine quintuples is less than $10^{216} \cdot 6 \cdot 10^{58} \cdot 4 < 10^{276}$, which completes the proof of Theorem 1.3. □

## 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, M. Cipu, M. Mignotte and R. Okazaki, *On the number of solutions of simultaneous Pell equations II,* Acta Arith. **122** (2006), 407–417.

[4] Y. Bugeaud, A. Dujella and M. Mignotte, *On the family of Diophantine triples $\{k - 1, k + 1, 16k^3 - 4k\}$,* Glasg. 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] Y. Fujita, *The extensibility of Diophantine pairs $\{k - 1, k + 1\}$,* J. Number Theory **128** (2008), 322–353.

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

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

[14] 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.

Y. 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`