OPEN ACCESS

University of
BRISTOL

Platt, D. J., & Trudgian, T. (2016). Diophantine quintuples containing triples of the first kind. Periodica Mathematica Hungarica, 72(2), 235-242. DOI: 10.1007/s10998-016-0127-2

Peer reviewed version

Link to published version (if available):
10.1007/s10998-016-0127-2

Link to publication record in Explore Bristol Research
PDF-document

University of Bristol - Explore Bristol Research
General rights

Diophantine quintuples containing triples of the first kind

D.J. Platt

Heilbronn Institute for Mathematical Research
University of Bristol, Bristol, UK
dave.platt@bris.ac.uk

and

T.S. Trudgian[*]

Mathematical Sciences Institute
The Australian National University, ACT 0200, Australia
timothy.trudgian@anu.edu.au

February 27, 2015

Abstract

We consider Diophantine quintuples $\{a, b, c, d, e\}$, sets of integers with $a < b < c < d < e$ the product of any two elements of which is one less than a perfect square. Triples of the first kind are sets $\{A, B, C\}$ with $C \geq B^5$. We show that there are no Diophantine quintuples $\{a, b, c, d, e\}$ such that $\{a, b, d\}$ is a triple of the first kind.

1 Introduction

Define a Diophantine m-tuple as a set of m distinct positive integers $a_1 < a_2 < \cdots < a_m$ such that $a_i a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$. For example, the set $\{1, 3, 8, 120\}$ is a Diophantine quadruple. Throughout the rest of this article we simply refer to m-tuples, and not to Diophantine m-tuples.

One may extend any triple $\{a, b, c\}$ to a quadruple $\{a, b, c, d_+\}$ where

$$d_+ = a + b + c + 2abc + 2rst, \quad r = \sqrt{ab + 1}, \quad s = \sqrt{ac + 1}, \quad t = \sqrt{bc + 1},$$

1

by appealing to a result by Arkin, Hoggatt and Straus [2]. Such a quadruple $\{a, b, c, d_+\}$ is called a *regular* quadruple. Arkin, Hoggatt and Straus conjectured that all quadruples are regular. Note that any possible quintuple $\{a, b, c, d, e\}$ contains the quadruples $\{a, b, c, d\}$ and $\{a, b, c, e\}$. If the conjecture by Arkin, Hoggatt and Straus were true then $d_+ = d = e$, whence d and e are not distinct. This implies that there are no quintuples. A partial result towards this is the following theorem, proved by Fujita [10].

Theorem 1 (Fujita). *If $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$, then $d = d_+$.*

When attempting to bound the number of possible quintuples $\{a, b, c, d, e\}$ it is useful to examine the relative size of b and d. To this end, Fujita [11] considered three classes of triples $\{A, B, C\}$, namely, triples of the *first kind* in which $C > B^5$; triples of the *second kind* in which $B > 4A$ and $B^2 \le C \le B^5$; and triples of the *third kind* in which $B > 12A$ and $B^{5/3} < C < B^2$.

Lemma 4.2 in [6] states that every quadruple contains a triple of the first, second, or third kind. Specifically, we have

Lemma 1 (Lemma 4.2 in [6]). *Let $\{a, b, c, d, e\}$ be a Diophantine quintuple with $a < b < c < d < e$. Then*

1. *$\{a, b, d\}$ is a triple of the first kind, or*

2.   *(i) $\{a, b, d\}$ is of the second kind, with $4ab + a + b \le c \le b^{3/2}$, or*

     (ii) $\{a, b, d\}$ is of the second kind, with $c = a + b + 2r$, or

     (iii) $\{a, b, d\}$ is of the second kind, with $c > b^{3/2}$, or

     (iv) $\{a, c, d\}$ is of the second kind, with $b < 4a$ and $c = a + b + 2r$, or

3. *$\{a, c, d\}$ is of the third kind, with $b < 4a$ and $c = (4ab + 2)(a + b - 2r) + 2(a + b)$.*

Lemma 1 allows us to take aim at various triples: to prove there are no quintuples one need only prove the nonexistence of quintuples containing each of the kinds of triples listed in Lemma 1. The aim of this paper is to show that there are no quintuples satisfying part 1 of Lemma 1.

The current best estimate[1], by Elsholtz, Filipin and Fujita [6], is that there are at most $6.8 \cdot 10^{32}$ quintuples comprising

- $5.05 \cdot 10^{15}$ possible quintuples derived from triples of the first kind,

- $6.72 \cdot 10^{32}$ possible quintuples derived from triples of the second kind, and

- $1.92 \cdot 10^{26}$ possible quintuples derived from triples of the third kind.

---

[1]The second author has announced [16] that there are at most $2.1 \cdot 10^{29}$ quintuples, and that there are no quintuples of the kind 3 in Lemma 1.

Attempts to bound the total number of quintuples have used a result by Matveev [14] on linear forms of logarithms. This is not required for triples of the first kind, which greatly simplifies the exposition. Rather, the bounds on b and d come from work of Filipin and Fujita [7] wherein so-called gap principles between solutions of Pell's equation are considered.

In §2 we improve Fujita and Filipin's proof slightly. This enables us to perform computations in §3 that prove:

Theorem 2. *There are no Diophantine quintuples $\{a, b, c, d, e\}$ such that $\{a, b, d\}$ is a Diophantine triple with $d > b^5$.*

Independently of this work, Cipu [5] has considered the same problem. Indeed, his Theorem 1.1 states that "the quadruple left after removing the largest entry of a Diophantine quintuple contains no standard triple of the first kind". This is somewhat stronger than our Theorem 2, though either result may be used to eliminate the triples in part 1 of Lemma 1. Moreover, Cipu shows [5, Thm. 1.1] that there are at most 10^{31} quintuples.

We were only made aware of this result when this paper was essentially completed. Elements of Cipu's paper, such as the reliance on inequalities of the form (2) and (7) are similar to ours. Our computational approach is different, and, in particular, our Algorithm 2 introduces some new ideas to the field.

Acknowledgements

2 Bounds considered by Filipin and Fujita

If a double or a triple cannot be extended to form a quintuple, we need not consider them in what follows. We call such doubles and triples *discards*. Many discards are known; we require only a few. The first, due to Fujita [9] (see also [3]), that shows that the double $\{k, k + 2\}$ is a discard. In addition, Filipin, Fujita and Togbé [8, Cor. 1.6, 1.9] proved that the following are discards for $k \geq 1$

$$\begin{aligned} &\{3k^2 - 2k, 3k^2 + 4k + 1\}, \qquad \{2(k + 1)^2 - 2(k + 1), 2(k + 1)^2 + 2(k + 1)\}, \\ &\{(k + 1)^2 - 1, (k + 1)^2 + 2(k + 1)\}, \qquad \{k, 4k + 4\}. \end{aligned} \quad (1)$$

For the following arguments we make frequent reference to Lemma 2.4 and (2.9) in [7]. These rely on a property denoted as 'Assumption 2.2' concerning the relations between the indexed solutions of the Pellian equations associated with the hypothetical quintuple. For ease of exposition, we do not write out the details of Assumption 2.2; we merely note that, for its application to quintuples containing triples of the kind in 1 in Lemma 1, it is satisfied as per [7, p. 303].

We also note, for the convenience of the reader, that a' in [7, (2.9)] is defined as $a' = \max\{b - a, a\}$. We assume that $\{a, b, d\}$ is a triple with $d > b^5$. We consider two cases according as $b \geq 2a$ or $b < 2a$.

2.1 When $b \geq 2a$

Combining (2.9) and Lemma 2.4(i) in [7] we have

$$\frac{0.178a^{1/2}d^{1/2}}{4b} < \frac{\log(4.001a^{1/2}(b-a)^{1/2}b^2d)\log(1.299a^{1/2}b^{1/2}(b-a)^{-1}d)}{\log(4bd)\log(0.1053ab^{-1}(b-a)^{-3}d)}. \tag{2}$$

It is easy to see that both factors of the numerator and the second factor of the denominator are increasing in a for $b \geq 2a$. Hence, given that $1 \leq a \leq b/2$, the right side of (2) is bounded above by

$$\frac{\log(2.0005b^3d)\log(1.8371d)}{\log(4bd)\log(0.1053b^{-4}d)}. \tag{3}$$

It is easy to see that $(\log A_1 x)(\log A_2 x)/((\log A_3 x)(\log A_4 x))$ is decreasing in x if $A_1 > A_3$ and $A_2 > A_4$. Since $b \geq 2$ it follows that (3) is decreasing in d, and since $d > b^5$, we have from (2) that

$$b^{3/2} < \frac{4}{0.178}\frac{\log(2.0005b^8)\log(1.8371b^5)}{\log(4b^6)\log(0.1053b)}. \tag{4}$$

We find that (4) holds provided that $b \leq 50$; in [7] the bound derived is $b \leq 52$. Thus we need only consider those pairs $\{a, b\}$ for which $1 \leq a \leq b/2 \leq 25$. We enumerate these pairs, and test them against the inequality in (2). After discarding pairs containing $\{k, k+2\}$ and those doubles in (1) we find that the only possibilities are

$$\{1, 15\}, \quad \{1, 24\}, \quad \{1, 35\}, \quad \{2, 24\}, \quad \{3, 21\}. \tag{5}$$

For each of these five doubles we insert values of a, b into (2), and solve for d. For example, with $\{1, 15\}$ we find that $d \leq 5.2 \cdot 10^6$. We now search for all those d with $15^5 < d \leq 5.2 \cdot 10^6$ such that $\{1, 15, d\}$ is a triple. We find only one such value of d, namely $d = 2030624$. We now search for all those $c \in (15, 2030624)$ such that $\{1, 15, c, 2030624\}$ is a quadruple. This yields exactly one value of c, namely $c = 32760$. Thus, one possible quadruple is $\{1, 15, 37260, 2030624\}$. We continue in this way with each of the doubles in (5). We find that the only possible quadruples are

$$\{1, 15, 37260, 2030624\}, \quad \{1, 24, 148995, 14600040\}, \quad \{1, 35, 494208, 70174128\}. \tag{6}$$

Note that each of the quadruples in (6) has $a = 1$. The proof of Lemma 2.4(i) in [7], that leads to the '0.178' on the right side of (2) can be improved significantly if it is known that $a = 1$. Indeed, if one there assumes $n \leq 0.45b^{-1}c^{1/2}$ one obtains (2.4) in [7] as well as the desired contradiction, as before. Thus, for $a = 1$ one may replace the '0.178' in (2) by '0.45'. It now follows that the double $\{1, 15\}$ when extended to a triple $\{1, 15, d\}$ must have $d < 2 \cdot 10^6$, whence we eliminate the first quadruple in (6). The other two quadruples are similarly eliminated. We conclude that there are no quintuples with $b \geq 2a$ for which $\{a, b, d\}$ is a triple of the first kind.

4

2.2   When $b < 2a$

In this case we combine (2.9) and Lemma 2.4(iii) in [7] and obtain

$$\frac{a^{-1/2}d^{1/8}}{4} < \frac{\log(4.001ab^2d)\log(1.299a^{1/2}b^{1/2}(b-a)^{-1}d)}{\log(4bd)\log(0.1053db^{-1}(b-a)^{-2})}. \tag{7}$$

We need a lower bound on $b - a$: given Fujita's result that $\{k, k+2\}$ cannot be extended to a quintuple, we can write $b - a \geq 3$. Since, again, the logarithms dependent upon a in (7) are increasing with a, and since $a + 3 \leq b < 2a$ we rewrite (7) as

$$b^{1/8} < 4\frac{\log(4.001b^8)\log(0.433b^6)}{\log(4b^6)\log(0.4212b^2)}. \tag{8}$$

We find that (8) is true provided that $b \leq 4.69 \cdot 10^9$. In fact, we can squeeze a little more out of the argument. Let $\alpha \in [1/2, 1)$ be a parameter to be chosen later. Then, for $a \leq \alpha b$ we have

$$b^{1/8} < 4\alpha^{1/2}\frac{\log(4.001\alpha b^8)\log(1.299\alpha^{1/2}b^6(1-\alpha)^{-1})}{\log(4b^6)\log(0.4212b^2)}, \tag{9}$$

whereas, for $a > \alpha b$ we have

$$b^{1/8} < 4\frac{\log(4.001b^8)\log(0.433b^5)}{\log(4b^6)\log(0.1053b^2(1-\alpha)^{-2})}. \tag{10}$$

Therefore $b^{1/8}$ is less than the maximum of the right sides in (9) and (10). We find that choosing $\alpha = 0.9862$ gives $b \leq 1.3 \cdot 10^9$. Filipin and Fujita [7] proved that $b < 10^{10}$: while our improvement is only slight, it makes the problem computationally tractable.

Filipin and Fujita proved also that $d < b^9$; this was improved in [6] to $d < b^{7.7}$. We use the weaker bound $d < b^8$ for computational convenience.

We hope now to search for possible quadruples $\{a, b, c, d\}$ with $\{a, b, d\}$ a triple of the first kind. We first enumerate all double $\{a, b\}$ with $a \geq 1$, $a + 2 < b < 2a$ and $b \leq 1.3 \cdot 10^9$. For each such doubles we enumerate all c where $c < b^8$ such that $\{a, b, c\}$ is a triple. We now appeal to Theorem 1 and compute $d = d_+$. If $b^5 < d < b^8$ and a, b and d satisfy inequality (7), then we add the quadruples to our *initial list*.

2.3   Specific bounds for d

There are a little under 11 million quadruples in our initial list (details are given in §3). We now propose a criterion against which to test these specimens.

Each quadruple $\{a, b, c, d\}$ gives rise to a system of Pellian equations the solutions to which are indexed by integers m and n — see [7, pp. 294-295]. One obtains tighter bounds by showing that m and n must be of roughly the same size. Implicit in the proof of Lemma 2.3 in [7] is the following problem. Given $\{a, b, d\}$ a triple of the first kind, and given m, n with $m \geq 3$ and $n \geq 2$ we want to find good bounds on

$$\frac{m}{n} < \frac{\log(2.001^2bd) + \frac{1}{n}\log(1.994a^{1/2}b^{-1/2})}{\log(1.994^2ad)} = w(a, b, d, n), \tag{11}$$

5

say. Note that w is decreasing with n. Let n_0 be the smallest value of n such that $(n_0 + 1)/n_0 < w(a, b, d, n_0) = \gamma_1$, say.

Now let γ_2 be any number satisfying $\gamma_2 > \gamma_1^2$, and let γ_3 be any number less than

$$\frac{1}{\gamma_1}\sqrt{1 + \frac{1}{ad}}\left(\sqrt{\frac{\gamma_2 ad + 1}{ad + 1}} - \gamma_1\right) = v(a, d, \gamma_1, \gamma_2). \tag{12}$$

Filipin and Fujita have $\gamma_1 = 1.2, \gamma_2 = 1.45, \gamma_3 = 0.0033$. This gives them a criterion against which to test quadruples provided that $b \geq 1.45a$. We should like to take γ_2 to be less than 1.45, so that we can test more quadruples. We do this in the following lemma.

Lemma 2. *Assume that $\gamma_2 a \leq b < 2a$, and that $\{a, b, d\}$ is a triple with $d > b^5$. Then*

$$\frac{\gamma_3 a^{1/2} b^{-1} d^{1/2}}{4} < \frac{\log(4.001 ab^2 d)\log(1.299 a^{1/2} b^{1/2}(b - a)^{-1} d)}{\log(4bd)\log(0.1053 db^{-1}(b - a)^{-2})}. \tag{13}$$

Proof. Using (12), and that fact that $\gamma_2 > \gamma_1^2$, the proof follows exactly the same lines as in the proof of Lemma 2.4(ii) in [7]. We complete the proof by combining the bound on n with (2.9) in [7]. $\square$

3 Computations

We first present a simple result on triples.

Lemma 3. *Let a, b, r be positive integers with $a < b$ such that $ab + 1 = r^2$. That is, $\{a, b\}$ is a double. Then all admissible c_n such that $\{a, b, c_n\}$ is a triple are of the form*

$$c_n = \frac{x_n^2 - 1}{a} = \frac{y_n^2 - 1}{b}$$

where c_n is an integer and the x_n, y_n are integer solutions to

$$bx^2 - ay^2 = b - a. \tag{14}$$

Proof. For c_n to be admissible, we have

$$ac_n = x^2 - 1$$

and

$$bc_n = y^2 - 1$$

for some integers x, y. We now simply eliminate c_n. $\square$

6

We now require an efficient algorithm to identify low-lying solutions to (14). We start by dividing throughout by $g = (a, b)$ to get

$$b^\dagger x^2 - a^\dagger y^2 = b^\dagger - a^\dagger$$

and then write $X = b^\dagger x$, $D = a^\dagger b^\dagger$ and $N = b^\dagger(b^\dagger - a^\dagger)$ to get

$$X^2 - Dy^2 = N. \tag{15}$$

Since D is not a square by construction, this is an example of Pell's equation which has been widely studied (see, for example, [13]). To find solutions, we first use Lagrange's PQa algorithm to find (u, v), the fundamental solution to

$$X^2 - Dy^2 = 1.$$

We then use brute force[2] to locate all the fundamental solutions to (15). Each such fundamental solution potentially gives rise to two infinite sequences of solutions, one generated by

$$X_{n+1} + y_{n+1}\sqrt{D} = (X_n + y_n\sqrt{D})(u + v\sqrt{D})$$

and the other by

$$X_{n+1} + y_{n+1}\sqrt{D} = (X_n + y_n\sqrt{D})(u - v\sqrt{D}).$$

Thus we have a series of recurrence relations, indexed by i that will generate all possible solutions, which we denote

$$x_{i,n+1} = fx_i(x_{i,n}, y_{i,n}) \quad \text{and} \quad y_{i,n+1} = fy_i(x_{i,n}, y_{i,n})$$

for $i \in [0, I - 1]$.

We can now proceed as described in Algorithm 1 to find all quadruples $\{a, b, c, d\}$ with $0 < a < b < c < d$, $a + 2 < b < 2a$, $b < 1.3 \cdot 10^9$ and $b^5 < d < b^8$ that satisfy inequality (7).

We note that iterating over the divisors of $r^2 - 1$ is more efficient than iterating over a and b and testing whether $ab + 1$ is a perfect square. When factoring $r^2 - 1$ for this purpose, we first factor $r \pm 1$ and merge the results.

We implemented Algorithm 1 in Pari [4] (for the factoring) and in 'C' using GMP [12] (for everything else). We ran it on 5 nodes of the University of Bristol Bluecrystal Phase III cluster [1] each of which comprises two 8 core Intel Xeon E5-2670 CPUs running at 2.60 GHz. The total time used across these nodes was about 40 hours.

There are $4,038,480,906$ pairs $\{a, b\}$ with $ab + 1$ a perfect square, $a + 2 < b < 2a$ and $b \leq 1.3 \cdot 10^9$. From these pairs, we obtained $12,115,454,363$ potential quadruples with $b < c < d$ and $b^5 < d < b^8$. Applying inequality (7) eliminated all but $10,811,817$ of these quadruples and these survivors formed our initial list.

---

[2]Theorem 6.2.5 of [15] gives upper bounds on such a brute force approach.

```
for r ← 2 to 1.3 · 10⁹ do
    w ← r² − 1;
    for a|w, a < r − 1 do
        b ← w/a;
        if b ≥ 2a or b > 1.3 · 10⁹ then continue Solve Pell's equation
        bx² − ay² = b − a to get I base solutions;
        for i ∈ [0, I − 1] do
            x ← x_{i,0};
            y ← y_{i,0};
            c ← x²−1 / a;
            while c ≤ b do
                t ← fx_i(x, y);
                y ← fy_i(x, y);
                x ← t;
                c ← x²−1 / a;
            end
            d ← a + b + c + 2abc + 2r√(ac + 1)√(bc + 1);
            while d ≤ b⁵ do
                t ← fx_i(x, y);
                y ← fy_i(x, y);
                x ← t;
                c ← x²−1 / a;
                d ← a + b + c + 2abc + 2r√(ac + 1)√(bc + 1);
            end
            while d < b⁸ do
                if c ∈ ℤ and a, b, d satisfy inequality (7) then
                    output {a, b, c, d}
                end
                t ← fx_i(x, y);
                y ← fy_i(x, y);
                x ← t;
                c ← x²−1 / a;
                d ← a + b + c + 2abc + 2r√(ac + 1)√(bc + 1)
            end
        end
    end
end
```

Algorithm 1: Producing the initial list.

We now apply Algorithm 2, based on inequalities (11), (12) and (13), to prune our initial list. To illustrate, consider the quadruple $\{a, b, c, d\} = \{8, 15, 21736, 10476753\}$ which survives Algorithm 1. We have

$$\frac{31}{30} > w(a, b, d, 30)$$

but

$$\frac{32}{31} < w(a, b, d, 31) = 1.0330\ldots = \gamma_1.$$

Now $b/a = 15/8 > \gamma_1^2$ so we will take $\gamma_2 = 15/8$. We now set

$$\gamma_3 = v(a, d, \gamma_1, \gamma_2) = 0.32555\ldots$$

and we find that the left hand side of (13) is $49.67\ldots$ and the right hand side is $2.852\ldots$ so the inequality fails and we have eliminated this quadruple.

When coded in Pari, Algorithm 2 takes less than 20 minutes on a single core to determine that none of the quadruples in our initial list is admissible. This proves Theorem 2.

---

for $\{a, b, c, d\} \in$ initial list **do**
  $n_0 \leftarrow$ smallest n such that $\frac{n+1}{n} < w(a, b, d, n)$;
  $\gamma_1 \leftarrow w(a, b, d, n_0)$;
  $\gamma_2 \leftarrow \max\left(\frac{b}{a}, \gamma_1^2\right)$;
  $\gamma_3 \leftarrow v(a, d, \gamma_1, \gamma_2)$;
  if a, b, d, γ_3 satisfy inequality (13) **then output** $\{a, b, c, d\}$
end

Algorithm 2: Pruning the initial list.

References

[1] ACRC. Bluecrystal phase 3 user guide, 2014.

[2] J. Arkin, Jr. Hoggatt, V. E., and E. G. Straus. On Euler's solution of a problem of Diophantus. *Fibonacci Quart.*, 17(4):333–339, 1979.

[3] Y. Bugeaud, A. Dujella, and M. Mignotte. On the family of Diophantine triples $\{k - 1, k + 1, 16k^3 - 4k\}$. *Glasg. Math. J.*, 49(2):333-344, 2007.

[4] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. User's Guide to PARI-GP, 2000.

[5] M. Cipu. Further remarks on Diophantine quintuples. *To appear in Acta Arith.*, 2015.

[6] C. Elsholtz, A. Filipin, and Y. Fujita. On Diophantine quintuples and $D(-1)$-quadruples. *Monatsh Math.*, 2013.

[7] A. Filipin and Y. Fujita. The number of Diophantine quintuples II. *Publ. Math. Debrecen*, 82:293–308, 2013.

[8] A. Filipin, Y. Fujita, and A Togbé. The extendibility of Diophantine pairs II: examples. *J. Number Theory*, 145:604–631, 2014.

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

[10] Y. Fujita. Any Diophantine quintuple contains a regular Diophantine quadruple. *J. Number Theory*, 129(7):1678–1697, 2009.

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

[12] Torbjörn Granlund. *The GNU Multiple Precision Arithmetic Library*, 5.1.1 edition, February 2013.

[13] William J. LeVeque. *Topics in Number Theory Vols. I and II*. Dover Books on Mathematics. Dover Publications, 2002.

[14] E. M. Matveev. An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II. *Izv. Math.*, 64(6):1217–1269, 2000.

[15] Richard A. Mollin. *Fundamental Number Theory with Applications*. CRC Press, 1997.

[16] T.S. Trudgian. Bounds on the number of Diophantine quintuples. 2015. Submitted. Preprint available at arXiv:1501.04401.