On Diophantine quintuples and $D(-1)$-quadruples

Christian Elsholtz, Alan Filipin and Yasutsugu Fujita

September 13, 2013

Abstract

In this paper the known upper bound 10^{96} for the number of Diophantine quintuples is reduced to $6.8\cdot 10^{32}$. The key ingredient for the improvement is that certain individual bounds on parameters are now combined with a more efficient counting of tuples, and estimated by sums over divisor functions. As a side effect, we also improve the known upper bound $4\cdot 10^{70}$ for the number of $D(-1)$-quadruples to $5\cdot 10^{60}$.

1 Introduction

Let $n \neq 0$ be an integer. A set of m positive integers is called a Diophantine m-tuple with the property $D(n)$, or simply a $D(n)$-m-tuple, if the product of any two of them increased by n is a perfect square. A $D(1)$-m-tuple is often called a Diophantine m-tuple, which is the most frequently studied case. Let us briefly review the history and some of the key results on this subject.

Diophantus of Alexandria was the first to look for such sets and it was in the case $n = 1$. He found a set of four positive rational numbers with the above property $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$. However, Fermat found a first Diophantine quadruple, the set $\{1, 3, 8, 120\}$. Euler was later able to add the fifth positive rational, $\frac{777480}{8288641}$, to Fermat's set. There is a folklore conjecture that Diophantine quintuples (i.e. five such positive integers) do not exist at all. Actually there is a stronger version of this conjecture.

Conjecture 1.1 (cf. [1, 5])**.** *Let $\{a, b, c, d\}$ be a Diophantine quadruple such that $a < b < c < d$, then*

$$d = d_+ = a + b + c + 2(abc + rst),$$

where r, s and t are positive integers given by $ab + 1 = r^2$, $ac + 1 = s^2$ and $bc + 1 = t^2$.

A Diophantine quadruple $\{a, b, c, d\}$, where $d > \max\{a, b, c\}$, is called a regular quadruple if $d = d_+$. So, it is conjectured that all Diophantine quadruples are regular. There have been a number of previous results on this problem. Dujella [4] first proved that there are no Diophantine 9-tuples, and at most finitely many 8-tuples, and later [5] significantly improved this proving there are no sextuples, and at most finitely many quintuples, giving an upper bound [6] of 10^{1930} for the number of conceivable quintuples. This upper bound was later reduced to 10^{276} by the third author [14], and to 10^{96} by the second and third authors [12].

A variety of different methods have been used to study this problem, including linear forms of logarithms, elliptic curves, theory around Pell's equation, elementary methods, separating the problem into several subproblems depending on the size of parameters etc. A detailed survey on the subject is the webpage [7] by Andrej Dujella.

The main result in the present paper is the following:

Theorem 1.2. *The number of Diophantine quintuples is less than* $6.8 \cdot 10^{32}$.

We remark that a complete computer search based on this bound is still out of reach of current computers, but that the new bound makes one much more optimistic about a complete solution. Is it possible that one or two further ideas can reduce the bound to the region where a complete computer search can finish the problem?

There are several sources where this improvement comes from. On the one hand side, the upper bounds on b and d have been reduced by a more careful study of all subcases that appear. The methods used for this are the same as the ones from [14] and [12], i.e. congruence method, linear forms in three logarithms and some improvement of the hypergeometric method: dividing the relevant case into subcases enables us for example to conclude $d > b^4$ in the worst case for the bound on d, which gives us a much better bound on b. However, the main new ingredient is a more efficient way of estimating upper bounds on the number of tuples, when bounds on individual parameters are known, by an averaging process. For this we have made use of explicit sum of divisor estimates. Similar ideas have already been used in Dujella [6] and Martin and Sitar [17] but it is not apparent how their result can be used for counting the number of quintuples.

There is a vast literature on the subject of counting $D(m)$-tuples, and it seems likely to us that divisor estimates of the type used in this paper can be frequently combined with the existing methods and results on $D(m)$-tuples. As a further example we show that a simple divisor estimate also gives an improvement on a very recent paper on $D(-1)$-quadruples. While it is conjectured that $D(-1)$-quadruples do not exist, it is known that no $D(-1)$-quintuple exists and that if $\{a, b, c, d\}$ is a $D(-1)$-quadruple with $a < b < c < d$, then $a = 1$ ([9]). Dujella, Filipin and Fuchs [8] proved that there are at most finitely many $D(-1)$-quadruples, by giving an upper bound of 10^{903} for the number. This bound was improved to 10^{356} by the second and third authors ([11]), and recently to $4 \cdot 10^{70}$ by Bonciocat, Cipu and Mignotte ([2]). Here we show that a simple divisor estimate improves this as follows:

Theorem 1.3. *The number of* $D(-1)$*-quadruples is less than* $5 \cdot 10^{60}$.

The organization of this paper is as follows: In section 2 we collect a number of known results on Diophantine tuples that we will use in our proofs. In secton 3 we collect some divisor estimates and prove some variants. Section 4 gives bounds on individual parameters, and section 5 combines the lemmas from sections 2-4 to prove the main theorem on Diophantine quintuples. Finally, section 6 gives a short proof of the result on $D(-1)$-quadruples.

2 Upper bounds for the number of extensions

Let us first recall two useful results from [13] and [14].

Lemma 2.1 ([13, Theorem 2]). *Let $\{a, b, c, d, e\}$ be a Diophantine quintuple with $a < b < c < d < e$. Then, $d = d_+$.*

Lemma 2.2 ([14, Theorem 1.2]). *Let $\{a, b, c\}$ be a Diophantine triple with $a < b < c$. Then there are at most four ways of extending this triple to a Diophantine quintuple $\{a, b, c, d, e\}$ with $a < b < c < d < e$.*

3 Explicit bounds on the divisor function

In this section we collect some explicit elementary bounds on the divisor function. Asymptotically, slightly stronger bounds are known in the literature, but almost all statements in the literature use inexplicit error estimates. Denote by $\omega(n)$ the number of distinct prime divisors of n.

Lemma 3.1.

$$\sum_{n=1}^{N} 2^{\omega(n)} < N(\log N + 1).$$

Proof. As in the proof of Lemma 2 in [6], we see that

$$\sum_{n=1}^{N} 2^{\omega(n)} = \sum_{n=1}^{N} \sum_{\substack{y|n \\ \mu^2(y)=1}} 1 = \sum_{\substack{y=1 \\ \mu^2(y)=1}}^{N} \left\lfloor \frac{N}{y} \right\rfloor \leq N \sum_{y=1}^{N} \frac{1}{y} < N(\log N + 1).$$

□

Observing that $k^{\omega(n)} \leq d_k(n)$, where $d_k(n)$ denotes the number of ways to write n as a product of k positive integers, we will make use of the following explicit bound:

Lemma 3.2 (Bordellès, [3, Theorem 2.1]). *Let $k \geq 3$ be an integer. For any real number $N \geq 13$, we have:*

$$\sum_{n \leq N} d_k(n) \leq \frac{N}{(n-1)!} (\log N + n - 2)^{n-1}.$$

By the above remarks the following is an immediate consequence:

Lemma 3.3.

$$\sum_{n=1}^{N} 4^{\omega(n)} \leq \sum_{n=1}^{N} d_4(n) \leq \frac{N}{6} (\log N + 2)^3.$$

Denote by $d(n)$ the number of positive divisors of n, which coincides with $d_2(n)$.

Lemma 3.4 (Consequence of Vinogradov [19, Chapter 5, §4 g]).
(1) *The number of solutions of $x^2 \equiv 1 \pmod{b}$ with $0 < x < b$ is at most $2^{\omega(b)+1}$.*
(2) *The number of solutions of $x^2 \equiv -1 \pmod{b}$ with $0 < x < b$ is at most $2^{\omega(b)}$.*

Lemma 3.5.

$$\sum_{n=2}^{N} d(n^2-1) < 2N\left((\log N)^2 + 4\log N + 2\right).$$

Proof. By elementary estimates and Lemma 3.4 (1) we have

$$\begin{aligned}\sum_{n=2}^{N} d(n^2-1) &\le 2\sum_{n=1}^{N}\sum_{\substack{y=1\\ y\mid n^2-1}}^{n} 1 = 2\sum_{y=1}^{N}\sum_{\substack{n=y\\ n^2\equiv 1 \pmod{y}}}^{N} 1\\ &\le 2\sum_{y=1}^{N}\frac{N}{y}2^{\omega(y)+1} = 4N\sum_{y=1}^{N}\frac{2^{\omega(y)}}{y}.\end{aligned}$$

Putting $A(N) = \sum_{y=1}^{N} 2^{\omega(y)}$, we know by Lemma 3.1 that $A(N) < N(\log N + 1)$, and we see that

$$\begin{aligned}\sum_{y=1}^{N}\frac{2^{\omega(y)}}{y} &= \sum_{y=1}^{N}\frac{A(y)-A(y-1)}{y} = \sum_{y=1}^{N-1}\frac{A(y)}{y(y+1)} + \frac{A(N)}{N}\\ &< \sum_{y=2}^{N}\frac{\log(y-1)+1}{y} + \log N + 1 < \sum_{y=2}^{N}\frac{\log y}{y} + 2\log N + 1\\ &= \sum_{y=2}^{N} f(y) + \int_1^N \frac{\log u}{u}du + 2\log N + 1,\end{aligned}$$

where

$$f(y) = \int_{y-1}^{y}\left(\frac{\log y}{y} - \frac{\log u}{u}\right)du.$$

Since $f(y)$ is increasing for $y \ge 5$, $\lim_{y\to\infty} f(y) = 0$ and $f(5) < 0$, we have $f(y) < 0$ for $y \ge 5$, from which one can easily check that $\sum_{y=2}^{N} f(y) < 0$ for $N \ge 21$. Therefore, we obtain

$$\begin{aligned}\sum_{n=2}^{N} d(n^2-1) &< 4N\left(\int_1^N \frac{\log u}{u}du + 2\log N + 1\right)\\ &= 2N\left((\log N)^2 + 4\log N + 2\right)\end{aligned}$$

for $N \ge 21$. It is also easy to check that the desired inequality holds for $2 \le N \le 20$. $\square$

We will use the last lemma in the cases when we get an upper bound N on r, because then it yields that the number of Diophantine pairs $\{a, b\}$ such that $a < b$ is less than $N\left((\log N)^2 + 4\log N + 2\right)$.

The same argument shows

Lemma 3.6.

$$\sum_{n=2}^{N} d'(n^2-1) < 2N\left((\log A)^2 + 4\log A + 2\right),$$

where $d'(n^2-1)$ only counts divisors $a \le A$.

The following is a key to prove Theorem 1.3.

Lemma 3.7. *For $N \geq 2$, we have*

$$\sum_{n=1}^{N} d(n^2+1) < N\left((\log N)^2 + 4\log N + 2\right).$$

Proof. One can easily prove this lemma in the same way as Lemma 3.5, noting Lemma 3.4 (2). $\square$

No attempt has been made of optimising this estimate. Asymptotically it is known that this case gives a better order of magnitude, namely $\sum_{n=1}^{N} d(n^2+1) \sim \frac{3}{\pi} N \log N$, see McKee [18], as n^2+1 is irreducible over $\mathbb{Z}$, whereas n^2-1 is not. For comparison, it is known (see Hooley [15]) that $\sum_{n=2}^{N} d(n^2-1) \sim CN(\log N)^2$, for some positive constant C.

4 Upper bounds for the second and the fourth elements

In this section our main goal is to improve the known bounds from [12] on elements b and d in Diophantine quintuple $\{a,b,c,d,e\}$ with $a<b<c<d<e$. First, we recall the definition of standard triples in [14].

Definition 4.1. 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 $c \geq b^2$;

(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.

Lemma 4.2. *Any Diophantine quadruple contains a standard triple. More precisely, if $\{a,b,c,d\}$ is a Diophantine quadruple with $a<b<c<d$, then one of the following holds*:

(i) $\{a,b,d\}$ *is of the first kind.*

(ii) $\{a,B,d\}$ *is of the second kind satisfying one of the following*:

- $B = b$ *with* $b > 4a$;
- $B = c$ *with* $b < 4a$ *and* $c = a+b+2r$;
- $B = c$ *such that* $\{a,b,c,d\}$ *is not a regular Diophantine quadruple.*

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

Proof. Let $\{a,b,c,d\}$ be a Diophantine quadruple with $a<b<c<d$. If it is irregular, then from [5, Lemma 6] we have $d>c^2$ and $c>4a$, so in this case $\{a,c,d\}$ is of the second kind. So, we can assume that $\{a,b,c,d\}$ is a regular quadruple. Then, it is easy to see that

$$c(4ab+1)<d<4c(ab+1).$$

If $b>4a$, then $d>b^2$ shows that $\{a,b,d\}$ is a triple of the second kind. Let us consider the case when $b<4a$. Then, by [16, Theorem 8] we have $c=c_k$, $k\geq 1$ or $c=\bar{c}_k$, $k\geq 2$, where (c_k) and $(\bar{c}_k)$ are defined by

$$c_0=0,\ c_1=a+b+2r,\ c_k=(4ab+2)c_{k-1}-c_{k-2}+2(a+b),$$

$$\bar{c}_0=0,\ \bar{c}_1=a+b-2r,\ \bar{c}_k=(4ab+2)\bar{c}_{k-1}-\bar{c}_{k-2}+2(a+b).$$

If $c>b^3$, then $d>4abc>b^5$ and we see that $\{a,b,d\}$ is a triple of the first kind. If $c\leq b^3$, since $c_2=4r(a+r)(b+r)>4ab^2>b^3$, we have $c=c_1$ or $c=\bar{c}_2$. If $c=c_1=a+b+2r$, we have $4a<c<4b$, which yields $d>4abc>c^2$, so in this case $\{a,c,d\}$ is a triple of the second kind. If $c=\bar{c}_2=(4ab+2)(a+b-2r)+2(a+b)$, then since we may assume $b>a+2$ (otherwise $\bar{c}_2=c_1$), we have $d=\bar{c}_3<c^2$ and $d>c^{5/3}$ in which case $\{a,c,d\}$ is a triple of the third kind. □

We now recall some useful results on extending a Diophantine triple. 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

$$az^2-cx^2=a-c, \tag{4.1}$$
$$bz^2-cy^2=b-c. \tag{4.2}$$

The solutions of equations (4.1) and (4.2) are respectively given by the following recursive definitions: $z=v_m$ and $z=w_n$ with positive integers m and n, where

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

with some integers z_0,z_1,x_0,y_1 (cf. [4, Section 2]).

Moreover, if $\{a,b,c,d,e\}$ is a Diophantine quintuple with $a<b<c<d<e$, 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 we obtain the system of Diophantine equations

$$a\delta^2-d\alpha^2=a-d, \tag{4.3}$$
$$b\delta^2-d\beta^2=b-d, \tag{4.4}$$
$$c\delta^2-d\gamma^2=c-d. \tag{4.5}$$

The solutions of equations (4.3), (4.4) and (4.5) respectively are given by $\delta = U_i$, $\delta = V_j$ and $\delta = W_k$ with positive integers i, j and k, where

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

The indices satisfy $4 \leq k \leq j \leq i \leq 2k$ and $j \geq 6$ and all of i, j and k are even. Moreover, by Lemma 4.2 $\{a, b, c, d\}$ contains a standard triple $\{A, B, C\}$ with $A < B < C = d$. Hence, considering $\{A, B, d, e\}$ as a quadruple we get from extending the triple $\{A, B, d\}$, that v_m and w_n correspond to two of U_i, V_j and W_k. We have the following lemma from [14], the only difference is that we now state it with three decimal places instead of two which gives us slight improvement.

Lemma 4.3. (cf. [14, Lemma 3.5]) *Let $\{a, b, c, d, e\}$ be a Diophantine quintuple with $a < b < c < d < e$. Assume $d \geq 4.2 \cdot 10^{76}$.*

(i) *If $\{a, b, c, d\}$ contains a triple of the first kind, then $j > d^{0.025}$.*

(ii) *If $\{a, b, c, d\}$ contains a triple of the second kind, then $j > d^{0.244}$.*

(iii) *If $\{a, b, c, d\}$ contains a triple of the third kind, then $j > d^{0.199}$.*

Furthermore, using this lemma and a result on linear forms in logarithms from [14, proposition 4.2.], where the third author proved (using $m \geq j$ and $C = d$)

$$\frac{m}{\log(351m)} < 2.786 \cdot 10^{12} (\log d)^2, \tag{4.6}$$

we can prove the following proposition. It is also good to remember that we usually get a better bound when using the hypergeometric method but to use that we need to have some gap between elements b and c in Diophantine triple $\{a, b, c\}$ with $a < b < c$, which is the case only in the standard triple of the first kind.

Proposition 4.4. *Let $\{a, b, c, d, e\}$ be a Diophantine quintuple with $a < b < c < d < e$. Then, $b < 1.03 \cdot 10^{38}$ and $d < 3.5 \cdot 10^{94}$. More precisely, the following estimates hold:*

(i) *If $\{a, b, d\}$ is of the first kind, then $b < 6.98 \cdot 10^9$ and $d < b^{7.7} < 6.28 \cdot 10^{75}$.*

(ii) *If either $\{a, b, d\}$ with $b > 4a$ or $\{a, c, d\}$ with $b < 4a$ and $c = a + b + 2r$ is of the second kind, then $b < 1.03 \cdot 10^{38}$ and $d < 4.2 \cdot 10^{76}$.*

(iii) *If $\{a, c, d\}$ is of the third kind with $b < 4a$ and $c = (4ab + 2)(a + b - 2r) + 2(a + b)$, then $b < 4.33 \cdot 10^{23}$ and $b^4 < d < 3.5 \cdot 10^{94}$.*

Proof. By Lemma 4.2, we may assume that one of the assumptions in (i), (ii) and (iii) holds.

(i) The proof is the same as the proof of [12, Proposition 2.11]. We combine the lower bounds for indices that we get from congruence relations together with the upper bound we get from the hypergeometric method to get a contradiction for large values of b and d. In [12] we did not have to prove this result as precise as now, because later in that paper we only needed that $d < 10^{100}$.

(ii) Lemma 4.3 together with (4.6) implies $d < 4.2 \cdot 10^{76}$. Since $d > 4abc > 4b^2$, we obtain $b < 1.03 \cdot 10^{38}$.

(iii) Lemma 4.3 together with (4.6) implies $d < 3.5 \cdot 10^{94}$. Since $b < 4a$ and $c > 4ab$, we obtain

$$d > 4abc > (4ab)^2 > (b^2)^2 = b^4.$$

□

5 Proof of Theorem 1.2

Proof of Theorem 1.2. Our strategy is to sum up the bounds computed in the cases of (i) to (iii) in Lemma 4.2 separately. The proof proceeds in order of (ii), (i), (iii).

Assume that $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$.

(ii) In this case, we know by Proposition 4.4 that $d < 4.2 \cdot 10^{76}$. We compute the number by dividing this case into the following subcases:

(ii-1) $b > 4a$ and $4ab + a + b \le c \le b^{1.5}$;

(ii-2) $b > 4a$ and $c = a + b + 2r$;

(ii-3) $b > 4a$ and $c > b^{1.5}$;

(ii-4) $b < 4a$ and $c = a + b + 2r$.

(ii-1) With $r = \sqrt{ab+1} \ge 3$ (see [10]) and $d = d_+ > 4abc$, it follows that $4.2 \cdot 10^{76} > d > 4abc > 16a^2b^2 > 12.64r^4$. This proves $r < 7.6 \cdot 10^{18} =: N_1$. By $r^2 - 1 = ab$ the number of pairs $\{a, b\}$ with $a < b$ is at most $\sum_{r=2}^{N_1} d(r^2-1)/2$. It follows from Lemma 3.5 that there are at most $1.58 \cdot 10^{22}$ pairs $\{a, b\}$.

For a fixed pair $\{a, b\}$, an integer 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 $t_0^2 \equiv 1 \pmod{b}$ with $-0.71b^{0.75} < t_0 < 0.71b^{0.75}$ (see [4, Lemma 1]). By Lemma 3.4 (1) this number is less than $2 \cdot 2^{\omega(b)+1}$. Since we now have $b < \sqrt{d/20} < 4.59 \cdot 10^{37}$ and the product of the first 26 primes exceeds $2 \cdot 10^{38}$, the number of such sequences is less than

$$2 \cdot 2^{\omega(b)+1} \le 2 \cdot 2^{26} < 1.35 \cdot 10^8.$$

Each sequence $t = t_\nu$ satisfies $\nu \le 3$, since if $\nu \ge 4$, then $(2r-1)^{\nu-1} < t_\nu = \sqrt{bc+1}$, which together with $c \le b^{1.5}$ implies $(\sqrt{b+1}-1)^3 < \sqrt{b^{2.5}+1}$, but this is impossible. To obtain the above inequality, we have used that if we want to extend the Diophantine pair $\{a, b\}$ to a triple $\{a, b, c\}$, there exist positive integers s and t satisfying $ac+1 = s^2$ and $bc+1 = t^2$. Eliminating c we get that t is a solution of Pellian equation $at^2 - bs^2 = a - b$. In our notation t_0 is a fundamental solution for which we have estimates, and the satisfying recurrence $t_{\nu+2} = 2rt_{\nu+1} - t_\nu$, which inductively gives us the lower bound $t_\nu > (2r-1)^{\nu-1}$.

Moreover, for a fixed Diophantine triple $\{a, b, c\}$, there are at most four ways for it to be extended to a quintuple by Lemma 2.2. Therefore, the number of Diophantine quintuples is less than

$$1.58 \cdot 10^{22} \cdot 1.35 \cdot 10^{8} \cdot 3 \cdot 4 < 2.56 \cdot 10^{31}. \tag{5.1}$$

(ii-2) Since $d > 4abc \geq 4(r^2 - 1)(3r + 2) > 12r^3$, we have $r < 1.52 \cdot 10^{25} =: N_2$. Lemma 3.5 implies that the number of pairs $\{a, b\}$ with $a < b$ is at most

$$\frac{1}{2} \sum_{r=2}^{N_2} d(r^2 - 1) < N_2 \left((\log N_2)^2 + 4 \log N_2 + 2 \right).$$

In this case, c is uniquely determined, and there are at most 4 possibilities to extend a triple to a quintuple. Hence the number of such quintuples is at most $2.19 \cdot 10^{29}$.

(ii-3) With the current bounds on the subcases this is the most relevant case. Therefore, we took care to treat the occurring factors of $2^{\omega(b)}$ in a more efficient way, by averaging over it. This estimate gives a number of Diophantine triples which is not too far off from the true number of Diophantine triples.

If $a \geq 5.16 \cdot 10^{11}$, then $d > 4 \cdot 5.16 \cdot 10^{11} b^{2.5}$ and $b < 5.29 \cdot 10^{25} =: N_3$.

For a fixed b, the number of Diophantine pairs $\{a, b\}$ with $a < b$ is less than $2^{\omega(b)+1}$ by Lemma 3.4 (1). Thus, the number of Diophantine pairs $\{a, b\}$ is less than $2 \sum_{b=1}^{N_3} 2^{\omega(b)}$. For a fixed $\{a, b\}$, the number of sequences $t = t_\nu$ corresponding to c is less than $2 \cdot 2^{\omega(b)+1}$ and each ν satisfies $\nu \leq 5$. It follows from Lemma 3.3 that the number of Diophantine quintuples is less than

$$8 \frac{N_3}{6} (\log(N_3) + 2)^3 \cdot 5 \cdot 4 < 3.24 \cdot 10^{32}. \tag{5.2}$$

If $a < 5.16 \cdot 10^{11} =: A_3$, then $b < (d/4)^{1/2.5} < 2.57 \cdot 10^{30}$ and $r < 1.001\sqrt{51.6} \cdot 10^5 \cdot \sqrt{b} < 1.153 \cdot 10^{21} =: N_3'$.

Lemma 3.6 implies that the number of Diophantine pairs $\{a, b\}$ is less than

$$2N_3' \left((\log A_3)^2 + 4 \log A_3 + 2 \right) < 1.931 \cdot 10^{24}.$$

Since the product of the first 22 primes exceeds $3 \cdot 10^{30}$, we have $\omega(b) \leq 21$. We also have $\nu \leq 5$. Hence, the number of Diophantine quintuples is less than

$$1.931 \cdot 10^{24} \cdot 4 \cdot 2^{21} \cdot 5 \cdot 4 < 3.24 \cdot 10^{32}. \tag{5.3}$$

(ii-4) We know by $d > 4abc > b^2(b/4 + b + b) = 9b^3/4$ that $b < 2.66 \cdot 10^{25} =: N_4$. Then, Lemma 3.1 shows that the number of Diophantine pairs is less than

$$2 \sum_{b=1}^{N_4} 2^{\omega(b)} < 2N_4(\log N_4 + 1).$$

Since c is unique, the number of Diophantine quintuples is less than

$$2N_4(\log N_4 + 1) \cdot 4 < 1.27 \cdot 10^{28}. \tag{5.4}$$

Summing up the right-hand sides of (5.1) to (5.4), we see that the number of Diophantine quintuples which contain $\{a, b, c, d\}$ satisfying (ii) in Lemma 4.2 is less than

$$2.56 \cdot 10^{31} + 2.19 \cdot 10^{29} + 3.24 \cdot 10^{32} + 3.24 \cdot 10^{32} + 1.27 \cdot 10^{28} < 6.74 \cdot 10^{32}. \tag{5.5}$$

(i) By Proposition 4.4 we have $b < 6.98 \cdot 10^9 =: N_5$. Then, the number of Diophantine pairs is less than $2\sum_{b=1}^{N_5} 2^{\omega(b)}$. For a fixed $\{a, b\}$, the number of sequences $t = t_\nu$ is less than $4 \cdot 2^{\omega(b)}$, and $\nu \le 9$. It follows from Lemma 3.3 that the number of Diophantine quintuples which contain $\{a, b, c, d\}$ satisfying (i) in Lemma 4.2 is less than

$$8 \cdot \frac{N_5}{6}(\log N_5 + 2)^3 \cdot 9 \cdot 4 < 5.03 \cdot 10^{15}. \tag{5.6}$$

(iii) By Proposition 4.4 we have $b < 4.33 \cdot 10^{23} =: N_6$. Since c is unique, we see from Lemma 3.1 that the number of Diophantine quintuples which contain $\{a, b, c, d\}$ satisfying (iii) in Lemma 4.2 is less than

$$2N_6(\log N_6 + 1) \cdot 4 < 1.92 \cdot 10^{26}. \tag{5.7}$$

Therefore, we conclude from (5.5), (5.6) and (5.7) that the number of Diophantine quintuples is less than

$$6.74 \cdot 10^{32} + 5.03 \cdot 10^{15} + 1.92 \cdot 10^{26} < 6.8 \cdot 10^{32}.$$

□

6 Proof of Theorem 1.3

Proof of Theorem 1.3. Assume that $\{1, b, c, d\}$ is a $D(-1)$-quadruple with $b < c < d$. By Proposition 4.1 in [2], we have $b < 2.69 \cdot 10^{110}$. Thus, the number of $D(-1)$-pairs $\{1, b\}$ is less than

$$r = \sqrt{b-1} < 1.641 \cdot 10^{55} =: N.$$

For each $D(-1)$-pair $\{1, b\}$, the number of sequences $t = t_m$ defining the third elements c with $b < c$ is at most the number of solutions of $t^2 \equiv -1 \pmod{b}$ with $0 < t < b$, which is less than $2^{\omega(b)}$ by Lemma 3.4 (2). Since the index m is at most 9 (see Section 5 in [2]) and the number of extensions of $\{1, b, c\}$ to $\{1, b, c, d\}$ with $c < d$ is at most 2 by Theorem 1.1 in [11], we see from Lemma 3.7 that the number of $D(-1)$-quadruples is less than

$$\begin{aligned} 2 \cdot 9 \sum_{r=1}^{N} 2^{\omega(r^2+1)} &\le 18 \sum_{r=1}^{N} d(r^2+1) \\ &< 18N\left((\log N)^2 + 4\log N + 2\right) \\ &< 4.93 \cdot 10^{60}, \end{aligned}$$

which completes the proof of Theorem 1.3. □

7 Acknowledgements

The authors would like to thank Andrej Dujella for discussions on the subject, and the referee for a careful reading of the manuscript. The first author was partially supported by the Austrian Science Fund (FWF): W1230, and the third author was partially supported by JSPS KAKENHI Grant Number 25400025.

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] N. C. Bonciocat, M. Cipu and M. Mignotte, *On* $D(-1)$*-quadruples*, Publ. Mat. **56** (2012), 279–304.

[3] O. Bordellès, *An inequality for the class number*, J. Ineq. Pure and Appl. Math. **7**, Article 87 (2006), 1–8.

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

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

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

[7] A. Dujella, webpage. http://web.math.pmf.unizg.hr/∼duje/dtuples.html

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

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

[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 number of* $D(-1)$*-quadruples*, Math. Commun. **15** (2010), 387–391.

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

[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] C. Hooley, *On the number of divisors of quadratic polynomials*, Acta Math. **110** (1963), 97–114.

[16] B. W. Jones, *A second variation on a problem of Diophantus and Davenport*, Fibonacci Quart. **16** (1978) 155–165.

[17] G. Martin and S. Sitar, *Erdős-Turán with a moving target, equidistribution of roots of reducible quadratics, and Diophantine quadruples*, Mathematika **57** (2011), 1–29.

[18] J. McKee, *On the average number of divisors of quadratic polynomials*, Math. Proc. Camb. Philos. Soc. **117** (1995), 389–392.

[19] I. M. Vinogradov, *Elements of number theory*, Dover, New York, 1954.

Institut für Mathematik A, Steyrergasse 30/II, Technische Universität Graz, A-8010 Graz, Austria
elsholtz@math.tugraz.at

Faculty of Civil Engineering, University of Zagreb, Fra Andrije Kačića-Miošića 26, 10000 Zagreb, Croatia
Email: filipin@grad.hr

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

MSC 2010:
11D45 Counting solutions of Diophantine equations
11D09 Quadratic and bilinear equations