On the size of Diophantine m-tuples

Andrej Dujella

Department of Mathematics, University of Zagreb
Bijenička cesta 30, 10000 Zagreb, Croatia
E-mail: duje@math.hr

1 Introduction

Let n be a nonzero integer. A set of m positive integers $\{a_1, a_2, \ldots, a_m\}$ is said to have the property $D(n)$ if $a_i a_j + n$ is a perfect square for all $1 \le i < j \le m$. Such a set is called a Diophantine m-tuple (with the property $D(n)$), or P_n-set of size m.

Diophantus found the quadruple $\{1, 33, 68, 105\}$ with the property $D(256)$. The first Diophantine quadruple with the property $D(1)$, the set $\{1, 3, 8, 120\}$, was found by Fermat (see [8, 9]). Baker and Davenport [3] proved that this Fermat's set cannot be extended to the Diophantine quintuple, and a famous conjecture is that there does not exist a Diophantine quintuple with the property $D(1)$. The theorem of Baker and Davenport has been recently generalized to several parametric families of quadruples [12, 14, 16], but the conjecture is still unproved.

On the other hand, there are examples of Diophantine quintuples and sextuples like $\{1, 33, 105, 320, 18240\}$ with the property $D(256)$ [11] and $\{99, 315, 9920, 32768, 44460, 19534284\}$ with the property $D(2985984)$ [19].

The purpose of this paper is to find some upper bounds for the numbers M_n defined by

$$M_n = \sup\{|S| \,:\, S \text{ has the property } D(n)\},$$

where $|S|$ denotes the number of elements in the set S.

Considering congruences modulo 4, it is easy to prove that $M_{4k+2} = 3$ for all integers k (see [6, 21, 29]). In [10] we proved that if $n \not\equiv 2 \pmod 4$ and $n \notin \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then $M_n \ge 4$. Recently, we were able to prove that $M_1 \le 8$ (see [15]). (As we said before, the conjecture is that

$M_1 = 4$.) Since a set with the property $D(4)$ may contain at most two odd elements, this result implies $M_4 \le 10$.

Since the number of integer points on the elliptic curve

$$y^2 = (a_1x + n)(a_2x + n)(a_3x + n) \tag{1}$$

is finite, we conclude that there does not exist an infinite set with the property $D(n)$. However, bounds for the size [2] and for the number [33] of solutions of (1) depend not only on n but also on a_1, a_2, a_3.

On the other hand, we may consider the hyperelliptic curve

$$y^2 = (a_1x + n)(a_2x + n)(a_3x + n)(a_4x + n)(a_5x + n) \tag{2}$$

of genus $g = 2$. Caporaso, Harris and Mazur [7] proved that the Lang conjecture on varieties of general type implies that for $g \ge 2$ the number $B(g, \mathbf{K}) = \max_C |C(\mathbf{K})|$ is finite. Here C runs over all curves of genus g over a number field $\mathbf{K}$, and $C(\mathbf{K})$ denotes the set of all $\mathbf{K}$-rational points on C. However, even the question whether $B(2, \mathbf{Q}) < \infty$ is still open. An example of Keller and Kulesz [26] shows that $B(2, \mathbf{Q}) \ge 588$ (see also [17, 34]). Since $M_n \le 5 + B(2, \mathbf{Q})$ (by [23] we have also $M_n \le 4 + B(4, \mathbf{Q})$), we see that the Lang conjecture implies that

$$M = \sup\{M_n \,:\, n \in \mathbf{Z} \setminus \{0\}\}$$

is finite.

At present we are able to prove only the weaker result that M_n is finite for all $n \in \mathbf{Z} \setminus \{0\}$. In the proof of this result we will try to estimate the number of "large" (greater than $|n|^3$), "small" (between n^2 and $|n|^3$) and "very small" (less that n^2) elements of a set with the property $D(n)$. Let us introduce the following notation:

$$\begin{aligned} A_n &= \sup\{|S \cap [|n|^3, +\infty\rangle| \,:\, S \text{ has the property } D(n)\}, \\ B_n &= \sup\{|S \cap \langle n^2, |n|^3\rangle| \,:\, S \text{ has the property } D(n)\}, \\ C_n &= \sup\{|S \cap [1, n^2]| \,:\, S \text{ has the property } D(n)\}. \end{aligned}$$

In estimating the number of "large" elements, we used a theorem of Bennett [4] on simultaneous approximations of algebraic numbers and a very useful gap principle. We proved

Theorem 1 $A_n \le 21$ *for all nonzero integers n.*

For the estimate of the number of "small" elements we used a "weak" variant of the gap principle and we proved

Theorem 2 $B_n < 0.65 \log|n| + 2.24$ *for all nonzero integers* n.

Finally, in the estimate of the number of "very small" elements we used a large sieve method due to Gallagher [18] and we proved

Theorem 3 $C_n < 265.55 \log|n| (\log\log|n|)^2 + 9.01 \log\log|n|$ *for* $|n| \geq 400$.

Since we checked that $C_n \leq 5$ for $|n| \leq 400$, we may combine Theorems 1, 2 and 3 to obtain

Theorem 4

$$
\begin{aligned}
M_n &\leq 32 \quad \textit{for } |n| \leq 400, \\
M_n &< 267.81 \log|n| (\log\log|n|)^2 \quad \textit{for } |n| > 400.
\end{aligned}
$$

2 Large elements

Assume that the set $\{a, b, c, d\}$ has the property $D(n)$. Let $ab + n = r^2$, $ac + n = s^2$, $bc + n = t^2$, where r, s, t are nonnegative integers. Eliminating d from the system

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

we obtain the following system of Pellian equations

$$
\begin{aligned}
az^2 - cx^2 &= n(a - c), & (3) \\
bz^2 - cy^2 &= n(b - c). & (4)
\end{aligned}
$$

We will apply the following theorem of Bennett [4] on simultaneous approximations of square roots of two rationals which are very close to 1.

Theorem 5 ([4]) *If* c_i*,* p_i*,* q *and* L *are integers for* $0 \leq i \leq 2$*, with* $c_0 < c_1 < c_2$*,* $c_j = 0$ *for some* $0 \leq j \leq 2$*,* q *nonzero and* $L > M^9$*, where*

$$M = \max\{|c_0|, |c_1|, |c_2|\},$$

then we have

$$\max_{0\le i\le 2}\Big\{\Big|\sqrt{1+\frac{c_i}{L}}-\frac{p_i}{q}\Big|\Big\} > (130L\gamma)^{-1}q^{-\lambda}$$

where

$$\lambda = 1+\frac{\log(33L\gamma)}{\log\Big(1.7L^2\prod_{0\le i<j\le 2}(c_i-c_j)^{-2}\Big)}$$

and

$$\gamma = \begin{cases} \frac{(c_2-c_0)^2(c_2-c_1)^2}{2c_2-c_0-c_1} & \text{if } c_2-c_1\ge c_1-c_0,\\ \frac{(c_2-c_0)^2(c_1-c_0)^2}{c_1+c_2-2c_0} & \text{if } c_2-c_1< c_1-c_0.\end{cases}$$

We will apply Theorem 5 to the numbers

$$\begin{aligned}\theta_1 &= \frac{s}{a}\sqrt{\frac{a}{c}}=\sqrt{\frac{ac+n}{ac}}=\sqrt{1+\frac{n}{ac}}=\sqrt{1+\frac{nb}{abc}},\\ \theta_2 &= \frac{t}{b}\sqrt{\frac{b}{c}}=\sqrt{\frac{bc+n}{bc}}=\sqrt{1+\frac{n}{bc}}=\sqrt{1+\frac{na}{abc}}.\end{aligned}$$

Lemma 1 *Assume that $a<b<c$ and $ac>n$. Then all positive integer solutions x,y,z of the system (3) and (4) satisfy*

$$\max\Big(|\theta_1-\frac{sbx}{abz}|,\,|\theta_2-\frac{zay}{abz}|\Big)<\frac{c\cdot|n|}{a}z^{-2}.$$

PROOF. We have

$$\Big|\frac{s}{a}\sqrt{\frac{a}{c}}-\frac{sbx}{abz}\Big| = \frac{s}{az\sqrt{c}}|z\sqrt{a}-x\sqrt{c}| = \frac{s}{az\sqrt{c}}\cdot\frac{|n(c-a)|}{z\sqrt{a}+x\sqrt{c}}.$$

If $n<0$, then $s=\sqrt{ac-|n|}<\sqrt{ac}$ and we obtain

$$|\theta_1-\frac{sbx}{abz}|<\frac{\sqrt{ac}\cdot|n|\cdot c}{a\sqrt{ac}z^2}=\frac{c|n|}{a}z^{-2}.$$

If $n>0$, then $x\sqrt{c}>z\sqrt{a}$ and we obtain

$$|\theta_1-\frac{sbx}{abz}|<\frac{\sqrt{ac+n}\cdot n\cdot c}{2a\sqrt{ac}z^2}=\sqrt{1+\frac{n}{ac}}\cdot\frac{cn}{2a}z^{-2}<\frac{cn}{a}z^{-2}.$$

In the same manner, we obtain $|\theta_2-\frac{tay}{abz}|<\frac{c|n|}{b}z^{-2}<\frac{c|n|}{a}z^{-2}$. ∎

Lemma 2 *Let $\{a,b,c,d\}$, $a<b<c<d$, be a Diophantine quadruple with the property $D(n)$. If $c>b^{11}|n|^{11}$, then $d\le c^{131}$.*

Proof. Let r,s,t,x,y,z be defined as in the beginning of this section. We will apply Theorem 5 with $\{c_0,c_1,c_2\}=\{0,na,nb\}$, $L=abc$, $M=|nb|$, $q=abz$, $p_1=sbx$, $p_2=tay$. Since $abc>|n|^9b^9$, the condition $L>M^9$ is satisfied. For the quantity γ from Theorem 5 we have $\gamma=\frac{b^2(b-a)^2}{2b-a}|n|^3$ if $b\ge 2a$ and $\gamma=\frac{a^2b^2}{a+b}|n|^3$ if $a<b\le 2a$. In both cases we have

$$\frac{b^3}{6}|n|^3\le\gamma<\frac{b^3}{2}|n|^3.$$

For the quantity λ from Theorem 5 we have

$$\lambda=1+\frac{\log(33abc\gamma)}{\log(1.7c^2(b-a)^{-2}n^{-6})}=2-\lambda_1\,,$$

where

$$\lambda_1=\frac{\log\frac{1.7c}{33ab(b-a)^2n^6\gamma}}{\log(1.7c^2(b-a)^{-2}n^{-6})}\,.$$

Theorem 5 and Lemma 1 imply

$$\frac{c|n|}{az^2}>(130abc\gamma)^{-1}(abz)^{\lambda_1-2}>(130abc\gamma)^{-1}a^{-2}b^{-2}z^{\lambda_1-2}.$$

This implies

$$z^{\lambda_1}<130a^2b^3c^2|n|\gamma$$

and

$$\log z<\frac{\log\left(130a^2b^3c^2|n|\gamma\right)\log\left(1.7c^2(b-a)^{-2}n^{-6}\right)}{\log(\frac{1.7c}{33ab(b-a)^2n^6\gamma})}\,. \tag{5}$$

Let us estimate the right hand side of (5). We have

$$130a^2b^3c^2|n|\gamma<65a^2b^6c^2n^4<c^3\cdot\frac{65a^2}{b^5|n|^7}<c^3,$$

unless $n=-1$, $a=1$, $b=2$. However, in [13] it was proved that the Diophantine pair $\{1,2\}$ with the property $D(-1)$ cannot be extended to a Diophantine quadruple.

The same result implies also that if $|n|=1$, then $b-a>1$. Therefore

$$1.7c^2(b-a)^{-2}n^{-6}<c^2.$$

Finally,

$$\frac{1.7c}{33ab(b-a)^2n^6\gamma} > 0.103a^{-1}b^{-6}cn^{-9} > c^{\frac{1}{11}} \cdot \frac{b^4|n|}{9.71a} > c^{\frac{1}{11}}\,.$$

The last estimate shows that $\lambda_1 > 0$, what we implicitly used in (5).

Putting these three estimates in (5), we obtain

$$\log z < \frac{3\log c \cdot 2\log c}{\frac{1}{11}\log c} = 66\log c\,.$$

Hence, $z < c^{66}$ and

$$d = \frac{z^2-n}{c} \le \frac{z^2+|n|}{c} < \frac{c^{132}+c^{\frac{1}{11}}}{c} < c^{131}+1.$$

∎

Now we will develop a very useful gap principle for the elements of a Diophantine m-tuple. The principle is based on the following construction which generalizes the constructions of Arkin, Hoggatt and Strauss [1] and Jones [25] for the case $n = 1$.

Lemma 3 *If $\{a,b,c\}$ is a Diophantine triple with the property $D(n)$ and $ab+n=r^2$, $ac+n=s^2$, $bc+n=t^2$, then there exist integers e,x,y,z such that*

$$ae+n^2 = x^2, \quad be+n^2 = y^2, \quad ce+n^2 = z^2$$

and

$$c = a+b+\frac{e}{n}+\frac{2}{n^2}(abe+rxy).$$

Proof. Define

$$e = n(a+b+c)+2abc-2rst.$$

Then

$$\begin{aligned}(ae+n^2)-(at-rs)^2 &= an(a+b+c)+2a^2bc-2arst+n^2\\ &\quad - a^2(bc+n)+2arst-(ab+n)(ac+n) = 0.\end{aligned}$$

Hence we may take $x = at-rs$, and analogously $y = bs-rt$, $z = cr-st$. We have

$$\begin{aligned}abe+rxy &= abn(a+b+c)+2a^2b^2c-2abrst\\ &+ abrst-a(ab+n)(bc+n)-b(ab+n)(ac+n)+rst(ab+n)\\ &= -abcn-n^2(a+b)+rstn,\end{aligned}$$

and finally

$$a+b+\frac{e}{n}+\frac{2}{n^2}(abe+rxy) = 2a+2b+c+\frac{2abc}{n}-\frac{2rst}{n}-\frac{2abc}{n}-2a-2b+\frac{2rst}{n} = c.$$

■

Lemma 4 *If $\{a,b,c,d\}$ is a Diophantine quadruple with the property $D(n)$ and $|n|^3 \le a < b < c < d$, then*

$$d > \frac{3.847\,bc}{n^2}\,.$$

Proof. We apply Lemma 3 to the triple $\{a,c,d\}$. Since $ce+n^2$ is a perfect square, we have that $ce+n^2 \ge 0$. On the other hand, the assumption is that $c > |n|^3$. Hence, if $e \le -1$, then $ce+n^2 < -|n|^3+n^2 < 0$, a contradiction. Since e is an integer, we have $e \ge 0$. If $e=0$, then $d = a+c+2s$. If $e \ge 1$, then

$$d > a+c+\frac{2ac}{n^2}+\frac{2s\sqrt{ac}}{n^2} > \frac{2ac}{n^2}\,. \tag{6}$$

(Note that if $n>0$ then $x<0$, $y<0$, and if $n<0$ and $b>|n|$ then $x>0$, $y>0$.)

Analogously, applying Lemma 3 to the triple $\{b,c,d\}$ we obtain that $d=b+c+2t$ or $d > b+c+\frac{2bc}{n^2}+\frac{2t\sqrt{bc}}{n^2}$. However, $d=b+c+2t$ is impossible since $b+c+2t > a+c+2s$ and

$$b+c+2t \le b+c+2\sqrt{c(c-1)+n} < 4c \le \frac{2ac}{n^2}\,,$$

unless $a < 2n^2$. But if $|n|^3 \le a < 2n^2$, then $|n|=1$, $a=1$, and in that case we have

$$a+c+\frac{2ac}{n^2}+\frac{2s\sqrt{ac}}{n^2} > 3c+2\sqrt{c(c-1)} > 4c.$$

Hence we proved that

$$d > b+c+\frac{2bc}{n^2}+\frac{2t\sqrt{bc}}{n^2}\,. \tag{7}$$

From [30] we know that the triples $\{1,2,3\}$ and $\{1,2,4\}$ cannot be extended to Diophantine quadruples. Thus $bc \ge 10$ and it implies

$$t^2 = bc+n \ge bc-|n| > bc-\sqrt[6]{bc} > 0.853\,bc.$$

If we put this in (7), we obtain $d > \frac{3.847\,bc}{n^2}$. ∎

Proof of Theorem 1. Assume that $\{a_1, a_2, \dots, a_{22}\}$ has the property $D(n)$ and $|n|^3 \le a_1 < a_2 < \cdots < a_{22}$. By Lemma 4 we find that

$$a_4 > \frac{a_2^2}{n^2}, \quad a_5 > \frac{a_2^3}{n^4}, \quad a_6 > \frac{a_2^5}{n^8}, \quad a_7 > \frac{a_2^8}{n^{14}},$$
$$a_8 > \frac{a_2^{13}}{n^{24}}, \quad a_9 > \frac{a_2^{21}}{n^{40}}, \quad a_{10} > \frac{a_2^{34}}{n^{66}}, \quad a_{11} > \frac{a_2^{55}}{n^{108}}.$$

Since $a_2 > |n|^3$, we have $\frac{a_2^{55}}{n^{108}} > a_2^{11}|n|^{11}$, and we may apply Lemma 2 with $a = a_1$, $b = a_2$, $c = a_{11}$. We conclude that $a_{22} \le a_{11}^{131}$. However, Lemma 4 implies

$$a_{12} > |n|a_{11}, \quad a_{13} > \frac{a_{11}^2}{|n|}, \quad a_{14} > \frac{a_{11}^3}{n^2}, \quad a_{15} > \frac{a_{11}^5}{|n|^5},$$
$$a_{16} > \frac{a_{11}^8}{|n|^9}, \quad a_{17} > \frac{a_{11}^{13}}{n^{16}}, \quad a_{18} > \frac{a_{11}^{21}}{|n|^{27}}, \quad a_{19} > \frac{a_{11}^{34}}{|n|^{45}},$$
$$a_{20} > \frac{a_{11}^{55}}{n^{74}}, \quad a_{21} > \frac{a_{11}^{89}}{|n|^{121}}, \quad a_{22} > \frac{a_{11}^{144}}{|n|^{197}}.$$

Since $a_{11} > a_2^{11}|n|^{11} > n^{44}$, we obtain

$$a_{22} > \frac{a_{11}^{144}}{|n|^{197}} \ge a_{11}^{144-\frac{197}{44}} > a_{11}^{139} > a_{11}^{131},$$

a contradiction. ∎

3 Small elements

Lemma 5 *If $\{a, b, c, d\}$ is a Diophantine quadruple with the property $D(n)$, $|n| \ne 1$, and $n^2 \le a < b < c < d$, then $c > 3.88\,a$ and $d > 4.89\,c$.*

Proof. We will apply Lemma 3. Since $b > n^2$, we have $e \ge 0$. Thus Lemma 3 implies that

$$c \ge a + b + 2r.$$

Since $|n| \ne 1$ we have $ab \ge 20$ and $r^2 \ge ab - \sqrt[4]{ab} > 0.89ab > 0.89a^2$. Hence, $c > 3.88\,a$.

Since $d \ge b + c + 2t > a + c + 2s$, from (6) we conclude that

$$d > a + c + \frac{2ac}{n^2} + \frac{2s\sqrt{ac}}{n^2}.$$

We have $ac \geq 24$ and $s^2 \geq ac - \sqrt[4]{ac} > 0.9\,ac$. Therefore

$$d > a + c + \frac{3.89\,ac}{n^2} > 4.89\,c\,.$$

■

PROOF OF THEOREM 2. We may assume that $|n| \geq 2$ since $B_1 = B_{-1} = 0$. Let $\{a_1, a_2, \dots, a_m\}$ be a Diophantine m-tuple with the property $D(n)$ and $n^2 < a_1 < a_2 < \cdots < |n|^3$. By Lemma 5 we have

$$a_3 > 3.88a_1, \quad a_4 > 3.88 \cdot 4.89a_1, \quad \dots, \quad a_m > 3.88 \cdot 4.89^{m-3}a_1.$$

Therefore

$$3.88 \cdot 4.89^{m-3} \cdot n^2 < |n|^3$$

and from $m - 3 < \frac{\log \frac{|n|}{3.88}}{\log 4.89}$ we obtain $m < 0.65 \log |n| + 2.24$. ■

4 Very small elements

We are left with the task to estimate the number of "very small" elements in a Diophantine m-tuple. Let $\{a_1, a_2, \dots, a_m\}$ be a Diophantine m-tuple with the property $D(n)$ and assume that $a_1 < a_2 < \cdots < a_m \leq N$, where N is a positive integer. Let $1 \leq k < m$. Then $x = a_{k+1}, \dots, x = a_m$ satisfy the system

$$a_1x + n = \square, \quad a_2x + n = \square, \quad \dots, \quad a_kx + n = \square, \tag{8}$$

where $\square$ denotes a square of an integer. Denote by $Z_k(N)$ the number of solutions of system (8) satisfying $1 \leq x \leq N$.

Motivated by the observations from the introduction of [5], we will apply a sieve method based on the following theorem of Gallagher [18] (see also [24, p.29]):

Theorem 6 ([18]) *If all but $g(q)$ residue classes* (mod q) *are removed for each prime power q in a finite set $\mathcal{S}$, then the number of integers which remain in any interval of length N is at most*

$$\Big(\sum_{q\in\mathcal{S}} \Lambda(q) - \log N\Big) \Big/ \Big(\sum_{q\in\mathcal{S}} \frac{\Lambda(q)}{g(q)} - \log N\Big)$$

provided the denominator is positive. Here $\Lambda(q) = \log p$ for $q = p^\alpha$.

We will use Theorem 6 to estimate the number $Z_k(N)$. For this purpose, we will take

$$\mathcal{S} = \{p \,:\, p \text{ is prime, } 83 \le p \le Q,\ \gcd(a_1a_2\cdots a_k, p) = 1\},$$

where Q is sufficiently large. For a prime $p \in \mathcal{S}$ we may remove all residue classes (mod p) such that $\left(\frac{a_ix+n}{p}\right) = -1$ for some $i \in \{1,\dots,k\}$. Here $(\frac{\cdot}{p})$ denotes the Legendre symbol.

Let $1 \le l \le k$. Then

$$\begin{aligned} g(p) &\le \left|\left\{x \in \mathbf{F}_p \,:\, \left(\frac{a_ix+n}{p}\right) = 0 \text{ or } 1, \text{ for } i = 1,\dots,l\right\}\right| \\ &\le l + \left|\left\{x \in \mathbf{F}_p \,:\, \left(\frac{x+n\overline{a_i}}{p}\right) = \left(\frac{\overline{a_i}}{p}\right), \text{ for } i = 1,\dots,l\right\}\right|. \end{aligned}$$

Here $a_i\overline{a_i} \equiv 1 \pmod{p}$. Using estimates for character sums (see [28, p.325]), we obtain

$$g(p) \le l + \frac{p}{2^l} + \Big(\frac{l-2}{l} + \frac{1}{2^l}\Big)\sqrt{p} + \frac{l}{2}\,.$$

Assume that $k = \lfloor \log_2 Q \rfloor$. We may take $l = \lfloor \log_2 p \rfloor$. Then we have

$$\frac{p}{2^l} + \frac{\sqrt{p}}{2^l} + \frac{3l}{2} < 2 + \frac{2}{\sqrt{p}} + \frac{3\log_2 p}{2} < \sqrt{p}$$

for $p \ge 179$. Hence

$$l + \frac{p}{2^l} + \Big(\frac{l-2}{2} + \frac{1}{2^l}\Big)\sqrt{p} + \frac{l}{2} < \frac{l}{2}\sqrt{p} < \frac{\log_2 p}{2}\sqrt{p} < 0.722\,\sqrt{p}\,\log p$$

for $p \ge 179$, and we may check directly that $l + \frac{p}{2^l} + \left(\frac{l-2}{2} + \frac{1}{2^l}\right) + \frac{l}{2} < 0.722\,\sqrt{p}\log p$ for $83 \le p \le 173$. Therefore we proved that

$$g(p) < 0.722\,\sqrt{p}\log p.$$

By Theorem 6, we have $Z_k(N) \le \frac{E}{F}$, where

$$E = \sum_{p\in\mathcal{S}} \log p - \log N, \quad F = \sum_{p\in\mathcal{S}} \frac{1}{0.722\,\sqrt{p}} - \log N.$$

By [32, Theorem 9], we have $E < \sum_{83\le p\le Q} \log p < \theta(Q) < 1.01624\,Q$.

Assume that at least $\frac{4}{5}\pi(Q)$ primes less than Q satisfy the condition $\gcd(a_1a_2\cdots a_k, p) = 1$. Then we have

$$\begin{aligned} F &\geq \frac{1}{0.722\sqrt{Q}}|\mathcal{S}| - \log N \geq \frac{1}{0.722\sqrt{Q}}\Big(\frac{4}{5}\pi(Q) - 23\Big) - \log N \\ &> 1.108\frac{\sqrt{Q}}{\log Q} - \frac{31.86}{\sqrt{Q}} - \log N\,. \end{aligned} \tag{9}$$

Since F must be positive in the applications of Theorem 6, we will choose Q of the following form

$$Q = c_1 \cdot \log^2 N \cdot (\log\log N)^2, \tag{10}$$

where c_1 is a constant.

We have to check whether our assumption is correct. Suppose that $a = a_1a_2\cdots a_k$ is divisible by at least one fifth of the primes $\leq Q$. Then $a \geq p_1p_2\cdots p_{\lceil\frac{1}{5}\pi(Q)\rceil}$, where p_i denotes the i^{th} prime. By [32, p.69], we have

$$p_{\lceil\frac{1}{5}\pi(Q)\rceil} > \frac{1}{5}\pi(Q)\log(\frac{1}{5}\pi(Q)) > \frac{1}{5}\frac{Q}{\log Q}\log\Big(\frac{1}{5}\frac{Q}{\log Q}\Big) := R.$$

Therefore, by [32, p.70],

$$\log a > \sum_{p\leq R}\log p > R\Big(1 - \frac{1}{\log R}\Big).$$

Assume that $Q \geq 2\cdot 10^4$. Then $\frac{1}{5}\frac{Q}{\log Q} > Q^{0.605}$ and $R > 0.128\,Q$. Furthermore, $\log R > 7.793$ and therefore

$$\log a > 0.105\,Q.$$

On the other hand, $a < N^k$ and $\log a < k\log N \leq \log_2 Q\log N$.

Assume that $N \geq 1.6\cdot 10^5$ and $c_1 \leq 80$. Then $Q \leq \log^{4.498} N$. In order to obtain a contradiction, it suffices to check that

$$0.105\,c_1\,\log^2 N\,(\log\log N)^2 > \frac{4.498}{\log 2}\log N\cdot\log\log N$$

or

$$c_1\,\log N\,\log\log N > 61.81,$$

and this is certainly true for $N \geq 1.6\cdot 10^5$ if we choose $c_1 \geq 2.08$.

Thus we may continue with estimating the quantity F. We are working under assumptions that (10) holds with $2.08 \le c_1 \le 80$, $Q \ge 2 \cdot 10^4$ and $N \ge 1.6 \cdot 10^5$. We would like to have the estimate of the form

$$F > \frac{\sqrt{Q}}{c_2 \log Q}\,. \tag{11}$$

This estimate will lead to

$$Z_k(N) < 1.01624\, c_2 \sqrt{Q} \log Q < 4.572\, c_2 \sqrt{c_1} \log N (\log\log N)^2. \tag{12}$$

In order to fulfill (11), it suffice to check

$$\frac{31.86}{\sqrt{Q}} + \log N < \frac{\sqrt{Q}}{\log Q}\Big(1.108 - \frac{1}{c_2}\Big).$$

Since $Q > 2 \cdot 10^4$ we have $\frac{31.86}{\sqrt{Q}} < 0.016\, \frac{\sqrt{Q}}{\log Q}$. Furthermore,

$$\frac{\log N \log Q}{\sqrt{Q}} < \frac{4.498\, \log N \log\log N}{\sqrt{c_1} \log N \log\log N} = \frac{4.498}{\sqrt{c_1}}\,.$$

Hence $c_2 > 1\Big/(1.092 - \frac{4.498}{\sqrt{c_1}})$. Thus if we choose $c_1 = 68$, then we may take $c_2 = 1.83$ and from (12) we obtain

$$Z_k(N) < 69\, \log N (\log\log N)^2. \tag{13}$$

Note that with this choice of c_1, $N \ge 1.6 \cdot 10^5$ implies $Q > 60222 > 2 \cdot 10^4$.

Proof of Theorem 3. Let $\{a_1, a_2, \dots, a_m\}$ be a Diophantine m-tuple with the property $D(n)$ and $a_1 < a_2 < \cdots < a_m \le n^2$. Then for any $k \in \{1, 2, \dots, m\}$ we have

$$m \le k + Z_k(n^2).$$

Let $k = \lfloor \log_2 Q \rfloor$, where $Q = 68 \log^2 n^2 (\log\log n^2)^2$. Since $|n| \ge 400$, we have $n^2 \ge 1.6 \cdot 10^5$ and we may apply formula (13) to obtain

$$Z_k(n^2) < 69\, \log n^2 (\log\log n^2)^2 < 265.55\, \log |n|\, (\log\log |n|)^2, \tag{14}$$

Furthermore,

$$k < \frac{1}{\log_2}\, \log(\log^{4.489} n^2) < 9.01\, \log\log |n|, \tag{15}$$

and combining (14) and (15) we finally obtain

$$m < 265.55\, \log |n| (\log\log |n|)^2 + 9.01\, \log\log |n|.$$

∎

Remark 1 In [22] Katalin Gyarmati recently considered the more general problem. She estimated $\min\{|\mathcal{A}|, |\mathcal{B}|\}$, where $\mathcal{A}, \mathcal{B} \subseteq \{1, 2, \ldots, N\}$ satisfy the condition that $ab + 1$ is a k^{th} power for all $a \in \mathcal{A}$, $b \in \mathcal{B}$. Using her approach, it can be deduced that if $\{a_1, a_2, \ldots, a_m\}$ has the property $D(n)$, where $n > 0$ and $a_1 < a_2 < \cdots < a_m \leq N$, then $m \leq 2n \log N$. This yields $C_n \leq 4n \log n$ for $n \geq 2$.

Remark 2 Let us mention that Rivat, Sárközy and Stewart [31] recently used Gallagher's "larger sieve" method in estimating the size of a set Z of integers such that $z + z'$ is a perfect square whenever z and z' are distinct elements of Z. They proved that if $Z \subset \{1, 2, \ldots, N\}$, where N is greater that an effectively computable constant, then $|Z| < 37 \log N$.

Largest known set with the above property is a set with six elements found by J. Lagrange [27]. Maybe this may be compared with our situation where the largest known Diophantine m-tuples are Diophantine sextuples found by Gibbs [19, 20].

Proof of Theorem 4. Since $M_n \leq A_n + B_n + C_n$, the second part of the theorem follows directly from Theorems 1, 2 and 3.

For $|n| \leq 400$, Theorem 2 gives $B_n \leq 6$. It is easy to verify with a computer that for $|n| \leq 400$ it holds $C_n \leq 5$. More precisely, $C_n = 5$ if and only if $n \in \{-299, -255, 256, 400\}$. These two estimates together with Theorem 1 imply $M_n \leq 32$. ∎

5 Concluding remarks

It is not surprising that in Theorem 4 the main contribution comes from C_n. Namely, if we define $C = \sup\{C_n : n \in \mathbf{Z} \setminus \{0\}\}$, then we have $M = C$. Indeed, if $\{a_1, a_2, \ldots, a_m\}$ is a Diophantine m-tuple with the property $D(n)$, then $\{a_1c, a_2c, \ldots, a_mc\}$ has the property $D(nc^2)$ and for sufficiently large c we have $a_ic \leq (nc^2)^2$, $i = 1, 2, \ldots, m$. It means that in order to prove $M < \infty$, it suffices to prove $C < \infty$. The above argumentation shows that it suffice to prove that for some $\varepsilon > 0$ it holds

$$\sup_{n \neq 0} \sup\{|S \cap [1, n^{0.5+\varepsilon}]| : S \text{ has the property } D(n)\} < \infty.$$

We may define also $A = \sup\{A_n : n \in \mathbf{Z} \setminus \{0\}\}$ and $B = \sup\{B_n : n \in \mathbf{Z} \setminus \{0\}\}$. Gibbs' example mentioned in introduction shows that $C \geq 6$ and

$M \geq 6$. If $n = a^2$, $a \geq 5$, then $B_n \geq 3$ since $\{a^2+1,\ a^2+2a+1,\ 4a^2+4a+4\}$ has the property $D(a^2)$. Hence $B \geq 3$. Finally, since $\{k,\ k+2,\ 4k+4,\ 16k^3+48k^2+44k+12\}$ has the property $D(1)$ we have $A \geq A_1 \geq 4$.

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. The diophantine equation $y^2 = ax^3 + bx^2 + cx + d$. *J. London Math. Soc.* **43** (1968), 1–9.

[3] 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.

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

[5] E. Bombieri, A. Granville and J. Pintz. Squares in arithmetic progressions. *Duke Math. J.* **66** (1992), 360–385.

[6] E. Brown. Sets in which $xy + k$ is always a square. *Math. Comp.* **45** (1985), 613–620.

[7] L. Caporaso, J. Harris and B. Mazur. Uniformity of rational points. *J. Amer. Math. Soc.* **10** (1997), 1–35.

[8] L. E. Dickson. *History of the Theory of Numbers, Vol. 2.* (Chelsea, 1966), pp. 513–520.

[9] Diophantus of Alexandria. *Arithmetics and the Book of Polygonal Numbers.* (I. G. Bashmakova, Ed.) (Nauka, 1974) (in Russian), pp. 103–104, 232.

[10] A. Dujella. Generalization of a problem of Diophantus. *Acta Arith.* **65** (1993), 15–27.

[11] A. Dujella. On Diophantine quintuples. *Acta Arith.* **81** (1997), 69–79.

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

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

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

[15] A. Dujella. An absolute bound for the size of Diophantine m-tuples. *J. Number Theory* (to appear).

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

[17] N. Elkies. Curves with many points. preprint.

[18] P. X. Gallagher. A larger sieve. *Acta Arith.* **18** (1971), 77–81.

[19] P. Gibbs. Some rational Diophantine sextuples. preprint, `math.NT/9902081`.

[20] P. Gibbs. A generalised Stern-Brocot tree from regular Diophantine quadruples. preprint, `math.NT/9903035`.

[21] H. Gupta and K. Singh. On k-triad sequences. *Internat. J. Math. Math. Sci.* **5** (1985), 799–804.

[22] K. Gyarmati. On a problem of Diophantus. preprint.

[23] E. Herrmann, A. Pethő and H. G. Zimmer. On Fermat's qudruple equations. *Abh. Math. Sem. Univ. Hamburg* **69** (1999), 283–291.

[24] C. Hooley. *Applications of Sieve Methods to the Theory of Numbers*. (Nauka, 1987) (in Russian).

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

[26] W. Keller and L. Kulesz. Courbes algébriques de genre 2 and 3 posśedant de nombreux points rationnels. *C. R. Acad. Sci. Paris Sér.* I **321** (1995), 1469–1472.

[27] J. Lagrange. Six entiers dont les sommes deux à deux sont des carrés. *Acta Arith.* **40** (1981), 91–96.

[28] R. Lidl and H. Niederreiter. *Finite Fields*. (Mir, 1988) (in Russian).

[29] S. P. Mohanty and A. M. S. Ramasamy. On $P_{r,k}$ sequences. *Fibonacci Quart.* **23** (1985), 36–44.

[30] V. K. Mootha and G. Berzsenyi. Characterization and extendibility of P_t-sets. *Fibonacci Quart.* **27** (1989), 287–288.

[31] J. Rivat, A. Sárközy and C. L. Stewart. Congruence properties of the Ω-function on sumsets. *Illinois J. Math.* **43** (1999), 1–18.

[32] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.* **6** (1962), 64–94.

[33] W. M. Schmidt. Integer points on curves of genus 1. *Compositio Math.* **81** (1992), 33–59.

[34] C. Stahlke. Algebraic curves over **Q** with many rational points and minimal automorphism group. *Inter. Math. Res. Not.* (1997), 1–4.