Bounds for the size of sets with the property $D(n)$

Andrej Dujella
University of Zagreb, Croatia

Abstract

Let n be a nonzero integer and $a_1 < a_2 < \cdots < a_m$ positive integers such that $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$. It is known that $m \leq 5$ for $n = 1$. In this paper we prove that $m \leq 31$ for $|n| \leq 400$ and $m < 15.476 \log |n|$ for $|n| > 400$.

1 Introduction

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

Diophantus himself found the $D(256)$-quadruple {1, 33, 68, 105}, while the first $D(1)$-quadruple, the set {1, 3, 8, 120}, was found by Fermat (see [4, 5]). In 1969, Baker and Davenport [1] proved that this Fermat's set cannot be extended to a $D(1)$-quintuple, and in 1998, Dujella and Pethő [10] proved that even the Diophantine pair $\{1, 3\}$ cannot be extended to a D(1)-quintuple. A famous conjecture is that there does not exist a $D(1)$-quintuple. We proved recently that there does not exist a $D(1)$-sextuple and that there are only finitely many, effectively computable, $D(1)$-quintuples (see [7, 9]).

The question is what can be said about the size of sets with the property $D(n)$ for $n \neq 1$. Let us mention that Gibbs [12] found several examples of Diophantine sextuples, e.g. {99, 315, 9920, 32768, 44460, 19534284} is a $D(2985984)$-sextuple.

Define

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

[0] *2000 Mathematics Subject Classification.* 11D45, 11D09, 11N36.
Key words and phrases. Diophantine m-tuples, property $D(n)$, large sieve.

Considering congruences modulo 4, it is easy to prove that $M_n = 3$ if $n \equiv 2 \pmod 4$ (see [3, 13, 15]). On the other hand, if $n \not\equiv 2 \pmod 4$ and $n \notin \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then $M_n \geq 4$ (see [6]).

In [8], we proved that $M_n \leq 32$ for $|n| \leq 400$ and

$$M_n < 267.81 \log|n| (\log\log|n|)^2 \quad \text{for } |n| > 400.$$

The purpose of the present paper is to improve this bound for M_n, specially in the case $|n| > 400$. We will remove the factor $(\log\log|n|)^2$, and also the constants will be considerably smaller.

The above mentioned bounds for M_n were obtained in [8] by considering separately three types (large, small and very small) of elements in a $D(n)$-m-tuple. More precisely, let

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

In [8], it was proved that $A_n \leq 21$ and $B_n < 0.65 \log|n| + 2.24$ for all nonzero integers n, while $C_n < 265.55 \log|n| (\log\log|n|)^2 + 9.01 \log\log|n|$ for $|n| > 400$ and $C_n \leq 5$ for $|n| \leq 400$. The combination of these estimates gave the bound for M_n.

In the estimate for A_n, a theorem of Bennett [2] on simultaneous approximations of algebraic numbers was used in combination with a gap principle, while a variant of the gap principle gave the estimate for B_n. The bound for C_n (number of "very small" elements) was obtained using the Gallagher's large sieve method [11] and an estimate for sums of characters.

In the present paper, we will significantly improve the bound for C_n using a result of Vinogradov on double sums of Legendre's symbols. Let us mention that Vinogradov's result, in a slightly weaker form, was used recently, in similar context, by Gyarmati [14] and Sárközy & Stewart [17]. We will prove the following estimates for C_n.

Proposition 1 *If $|n| > 400$, then $C_n < 11.006 \log|n|$. If $|n| \geq 10^{100}$, then $C_n < 8.37 \log|n|$.*

More detailed analysis of the gap principle used in [8] will lead us to the slightly improved bounds for B_n.

Proposition 2 *For all nonzero integers n it holds $B_n < 0.6114 \log|n| + 2.158$. If $|n| > 400$, then $B_n < 0.6071 \log|n| + 2.152$.*

By combining Propositions 1 and 2 with the above mentioned estimate for A_n, we obtain immediately the following estimates for M_n.

Theorem 1 *If* $|n| \leq 400$, *then* $M_n \leq 31$. *If* $|n| > 400$, *then* $M_n < 15.476, \log|n|$. *If* $|n| \geq 10^{100}$, *then* $M_n < 9.078 \log|n|$.

2 Three lemmas

Lemma 1 (Vinogradov) *Let* p *be an odd prime and* $\gcd(n,p) = 1$. *If* $A, B \subseteq \{0, 1, \dots, p-1\}$ *and*

$$T = \sum_{x \in A} \sum_{y \in B} \Big(\frac{xy+n}{p} \Big),$$

then $|T| < \sqrt{p|A| \cdot |B|}$.

PROOF. See [18, Problem V.8.c)]. ■

Lemma 2 (Gallagher) *If all but* $g(p)$ *residue classes* mod p *are removed for each prime* p *in a finite set* $\mathcal{S}$, *then the number of integers which remain in any interval of length* N *is at most*

$$\Big(\sum_{p \in \mathcal{S}} \log p - \log N \Big) \Big/ \Big(\sum_{p \in \mathcal{S}} \frac{\log p}{g(p)} - \log N \Big) \tag{1}$$

provided the denominator is positive.

PROOF. See [11]. ■

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. See [8, Lemma 3]. ■

3 Proof of Proposition 1

Let $N \geq n^2$ be a positive integer. Since $|n| > 400$, we have $N > 1.6 \cdot 10^5$. Let $D = \{a_1, a_2, \dots, a_m\} \subseteq \{1, 2, \dots, N\}$ be a Diophantine m-tuple with the property $D(n)$. We would like to find an upper bound for m in term of N. We will use the Gallagher's sieve (Lemma 2). Let

$$\mathcal{S} = \{p : p \text{ is prime, } \gcd(n,p) = 1 \text{ and } p \leq Q\},$$

where Q is sufficiently large. For a prime $p \in \mathcal{S}$, let C denotes the set of integers b such that $b \in \{0, 1, 2, \dots, p-1\}$ and there is at least one $a \in D$ such that $b \equiv a \pmod{p}$. Then $\left(\frac{xy+n}{p}\right) \in \{0, 1\}$ for all distinct $x, y \in C$. Here $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol. If $0 \in C$, then $\left(\frac{n}{p}\right) = 1$. For a given $x \in C \setminus \{0\}$, we have $\left(\frac{xy_0+n}{p}\right) = 0$ for at most one $y_0 \in C$. If $y \neq x, y_0$, then $\left(\frac{xy+n}{p}\right) = 1$. Therefore,

$$\begin{aligned} T &= \sum_{x,y \in C} \left(\frac{xy+n}{p}\right) = \sum_{x \in C} \Big(\sum_{y \in C} \left(\frac{xy+n}{p}\right) \Big) \\ &\geq \sum_{x \in C} (|C| - 3) \geq |C|(|C| - 3). \end{aligned}$$

On the other hand, Lemma 1 implies

$$T < |C| \cdot \sqrt{p}.$$

Thus, $|C| < \sqrt{p} + 3$ and we may apply Lemma 2 with

$$g(p) = \min\{\lfloor \sqrt{p} \rfloor + 3, p\}.$$

Let us denote the numerator and denominator from (1) by E and F, respectively. By [16, Theorem 9], we have

$$E = \sum_{p \in \mathcal{S}} \log p - \log N < \theta(Q) < 1.01624\, Q.$$

The function $f(x) = \frac{\log x}{\min\{\sqrt{x}+3, x\}}$ is strictly decreasing for $x > 25$. Also, if $Q \geq 118$, then $f(p) \geq f(Q)$ for all $p \leq Q$.

For $p \in \mathcal{S}$ it holds $\gcd(n,p) = 1$. This condition comes from the assumptions of Lemma 1. However, we will show later that n can be divisible only by a small proportion of the primes $\le Q$. Assume that n is divisible by at most 5% of primes $\le Q$. Then, for $Q \ge 118$, we have

$$\begin{aligned} F &\ge \sum_{p\in\mathcal{S}} f(p) - \log N \ge \frac{\log Q}{\sqrt{Q}+3}\cdot|\mathcal{S}| - \log N \\ &\ge \frac{\log Q}{\sqrt{Q}+3}\cdot\frac{19}{20}\pi(Q) - \log N > \frac{0.95\,Q}{\sqrt{Q}+3} - \log N. \end{aligned} \tag{2}$$

Since F has to be positive in the applications of Lemma 2, we will choose Q of the form

$$Q = c_1 \cdot \log^2 N.$$

We have to check whether our assumption on the proportion of primes which divide n is correct. Suppose that n is divisible by at least 5% of the primes $\le Q$. Then $|n| \ge p_1 p_2 \cdots p_{\lceil \pi(Q)/20\rceil}$, where p_i denotes the i-th prime. By [16, 3.5 and 3.12], we have $p_{\lceil \pi(Q)/20\rceil} > R$, where

$$R = \frac{1}{20}\frac{Q}{\log Q}\log\Big(\frac{1}{20}\frac{Q}{\log Q}\Big).$$

Assume that $c_1 \ge 6$. Then $Q > 860$ and $R > 11.77$. From [16, 3.16], it follows that

$$\log|n| > \sum_{p\le R}\log p > R\Big(1 - \frac{1.136}{\log R}\Big). \tag{3}$$

Furthermore, $\frac{1}{20}\frac{Q}{\log Q} > Q^{0.273}$ and $R > 0.0136\,Q$. Hence, (3) implies $\log R > 7.793$ and therefore

$$\log N \ge 2\log|n| > 0.01466\,Q \ge 0.08796\,\log^2 N,$$

contradicting the assumption that $N > 1.6\cdot 10^5$.

Therefore, we have that n is divisible by at most 5% of the primes $\le Q$, and hence we have justified the estimate (2).

Under the assumption that $c_1 \ge 6$, the inequality (2) implies

$$F > 0.861\sqrt{Q} - \log N = (0.861\sqrt{c_1} - 1)\log N$$

and

$$\frac{E}{F} < \frac{1.017\,c_1}{0.861\sqrt{c_1} - 1}\cdot\log N.$$

For $c_1 = 6$ we obtain

$$\frac{E}{F} < 5.503\,\log N. \tag{4}$$

Assume now that $N \geq 10^{200}$ and $c_1 \geq 4$. Then $Q > 848303$ and we can prove in the same manner as above that n is divisible by at most 1% of the primes $\leq Q$. This fact implies

$$\frac{E}{F} < \frac{1.017c_1}{0.986\sqrt{c_1} - 1} \cdot \log N.$$

For $c_1 = 4.11$ we obtain

$$\frac{E}{F} < 4.185 \log N. \tag{5}$$

Setting $N = n^2$ in (4) and (5), we obtain the statements of Proposition 1. ∎

4 Proof of Proposition 2

We may assume that $|n| > 1$. Let $\{a, b, c, d\}$ be a $D(n)$-quadruple such that $n^2 < a < b < c < d$. We apply Lemma 3 on the triple $\{b, c, d\}$. Since $b > n^2$ and $be + n^2 \geq 0$, we have that $e \geq 0$. If $e = 0$, then $d = b + c + 2\sqrt{bc + n} < 2c + 2\sqrt{c(c-1) + n} < 4c$, contradicting the fact that $d > 4.89\,c$ (see [8, Lemma 5]).

Hence $e \geq 1$ and

$$d > b + c + \frac{2bc}{n^2} + \frac{2t\sqrt{bc}}{n^2}. \tag{6}$$

Lemma 3 also implies

$$c \geq a + b + 2r. \tag{7}$$

From $r^2 \geq ab - \sqrt[4]{ab}$ and $ab \geq 30$ it follows that $r > 0.96\,a$, and (7) implies $c > 3.92\,a$. Similarly, $bc \geq 42$ implies $t > 0.969\sqrt{bc}$ and, by (6), $d > b + c + 3.938\,\frac{bc}{n^2} > 4.938\,c + b$.

Assume now that $\{a_1, a_2, \ldots, a_m\}$ is a $D(n)$-m-tuple and $n^2 < a_1 < a_2 < \cdots < a_m < |n|^3$. We have

$$a_3 > 3.92\,a_1, \quad a_i > 4.938\,a_{i-1} + a_{i-2}, \quad \text{for } i = 4, 5, \ldots, m.$$

Therefore, $a_m > \alpha_m a_1$, where the sequence (α_k) is defined by

$$\alpha_k = 4.938\alpha_{k-1} + \alpha_{k-2}, \quad \alpha_2 = 1, \ \alpha_3 = 3.92. \tag{8}$$

Solving the recurrence (8), we obtain $\alpha_k \approx \beta\gamma^{k-3}$, with $\beta \approx 3.964355$, $\gamma \approx 5.132825$. More precisely,

$$|\alpha_k - \beta\gamma^{k-3}| < \frac{1}{\beta\gamma^{k-3}}.$$

From $|n|^3 - 1 \geq a_m > \alpha_m a_1 \geq \alpha_m(n^2+1)$, it follows $\alpha_m \leq |n| - \frac{1}{|n|}$ and $\beta\gamma^{m-3} < |n|$. Hence,

$$m < \frac{1}{\log\gamma}\log|n| + 3 - \frac{\log\beta}{\log\gamma}. \tag{9}$$

For the above values of β and γ we obtain

$$m < 0.6114\,\log|n| + 2.158.$$

Assume now that $|n| > 400$. Then $bc > ab > 400^4$, which implies $c > 3.999999\,a$ and $d > 4.999999\,c + b$. Therefore, in this case the relation (9) holds with $\beta \approx 4.042648$, $\gamma \approx 5.192581$, and we obtain

$$m < 0.6071\,\log|n| + 2.152.$$

■

Remark 1 The constants in Theorem 1 can be improved, for large $|n|$, by using formula (2.26) from [16] in the estimate for the sum $\sum_{p\in\mathcal{S}} f(p)$. In that way, it can be proved that for every $\varepsilon > 0$, $F > (2-\varepsilon)\sqrt{Q} - \log N$ holds for sufficiently large Q.

Also, in the proof of Proposition 2, for sufficiently large $|n|$ we have $c > (4-\varepsilon)a$ and $d > (5-\varepsilon)c + b$, which leads to $B_n < \left(\frac{1}{\log(\frac{5+\sqrt{29}}{2})} + \varepsilon\right)\log|n|$.

These results imply that for every $\varepsilon > 0$ there exists $n(\varepsilon)$ such that for $|n| > n(\varepsilon)$ it holds

$$M_n < \left(2 + \frac{1}{\log(\frac{5+\sqrt{29}}{2})} + \varepsilon\right)\log|n|.$$

Acknowledgements. The author is grateful to the referees for valuable comments, and in particular for pointing out a gap in the proof of Proposition 1 in the first version of the manuscript.

References

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

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

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

[4] L. E. Dickson, History of the Theory of Numbers, Vol. 2, Chelsea, New York, 1966, pp. 513–520.

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

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

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

[8] A. Dujella, *On the size of Diophantine m-tuples*, Math. Proc. Cambridge Philos. Soc. **132** (2002), 23–33.

[9] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math., to appear.

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

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

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

[14] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. **97** (2001), 53–65.

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

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

[17] A. Sárközy and C. L. Stewart, *On prime factors of integers of the form $ab+1$*, Publ. Math. Debrecen **56** (2000), 559–573.

[18] I. M. Vinogradov, Elements of Number Theory, Nauka, Moscow, 1972 (in Russian).

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