Journal of Combinatorial Theory, Series A 170 (2020) 105155

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

The Paley graph conjecture and Diophantine m-tuples

Ahmet M. Güloğlu [a], M. Ram Murty [b,1]

[a] Department of Mathematics, Bilkent University, 06800 Bilkent, Ankara, Turkey
[b] Department of Mathematics and Statistics, Queen's University, Kingston, Ontario, K7L 3N6, Canada

ARTICLE INFO

Article history:
Received 28 January 2019
Received in revised form 23 July 2019
Accepted 29 September 2019
Available online xxxx

Keywords:
Diophantine m-tuples
Gallagher's sieve
Vinogradov's inequality
Paley graph conjecture

ABSTRACT

A Diophantine m-tuple with property $D(n)$, where n is a nonzero integer, is a set of m positive integers $\{a_1, ..., a_m\}$ such that $a_i a_j + n$ is a perfect square for all $1 \leqslant i < j \leqslant m$. It is known that $M_n = \sup\{|\mathcal{S}| : \mathcal{S} \text{ is a } D(n)\ m\text{-tuple}\}$ exists and is $O(\log |n|)$. In this paper, we show that the Paley graph conjecture implies that the upper bound can be improved to $\ll (\log |n|)^{\epsilon}$, for any $\epsilon > 0$.

1. Introduction

A Diophantine m-tuple with property $D(n)$, where n is a nonzero integer, is a set of m positive integers $\{a_1, a_2, \ldots, a_m\}$ such that $a_i a_j + n$ is a perfect square for all $1 \leqslant i < j \leqslant m$.

Diophantus found the quadruple $\{1, 33, 68, 105\}$ with property $D(256)$. The first $D(1)$-quadruple $\{1, 3, 8, 120\}$ was found by Fermat (cf. [9]). Baker and Davenport showed in 1969 (cf. [2]) that Fermat's set is the only extension of $\{1, 3, 8\}$ to a $D(1)$-quadruple,

E-mail addresses: guloglua@fen.bilkent.edu.tr (A.M. Güloğlu), murty@queensu.ca (M.R. Murty).
[1] Research of the second author was partially supported by an NSERC Discovery grant.

https://doi.org/10.1016/j.jcta.2019.105155

and thus it cannot be extended to a $D(1)$-quintuple. This result follows from a paper of Baker [1] published in 1968 on linear forms in logarithms of algebraic numbers, which is an effective version of Gelfond's theorem used for solutions of Diophantine equations in two unknowns and a reduction method introduced in [2].

Baker and Davenport's remarkable result was the first step towards the folklore conjecture which predicts that there are no $D(1)$-quintuples. In 2004, Dujella (cf. [13]) proved using similar methods to those of Baker and Davenport that there is no sextuple with property $D(1)$ and there are only finitely many effectively computable $D(1)$-quintuples. In 2018, in a very recent paper, He, Togbé and Ziegler (cf. [26]) have shown that there are no Diophantine quintuples, thereby settling this conjecture.

For $n \neq 1$, however, there are Diophantine quintuples and sextuples, such as the quintuple $\{1, 33, 105, 320, 18240\}$ with $n = 256$ (cf. [16]) and the sextuple $\{99, 315, 9920, 32768, 44460, 19534284\}$ with $n = 2985984$ (cf. [19]).

Thus, two related and important questions in the study of Diophantine m-tuples are (i) to determine, for a given n and m, the number of possible $D(n)$-m-tuples; and (ii) to estimate the quantity

$$M_n = \sup\{|\mathcal{S}| : \mathcal{S} \text{ is a } D(n)\ m\text{-tuple}\}.$$

The first observation is that there is no infinite Diophantine m-tuples, for any $n \neq 0$, since the number of integral points on the elliptic curve

$$y^2 = (a_1x + n)(a_2x + n)(a_3x + n)$$

is finite, which follows from a celebrated theorem of Siegel (see, for example, [31]). Unfortunately, known bounds (cf. [30]) for the number of integral solutions depend on n, a_1, a_2, and a_3. On the other hand, as a result of a conjecture of Caporaso, Harris, and Mazur [6], the hyperelliptic curve of genus 2 given by

$$y^2 = (a_1x + n)(a_2x + n)(a_3x + n)(a_4x + n)(a_5x + n)$$

has a bounded number of integral points, independent of n and the coefficients $a_1, \ldots, a_5$. This would imply that $\sup_n M_n$ is bounded. This observation has been made by Dujella in [12] and the first result in this direction is due to Dujella and Luca [11], who proved that M_n is bounded by an absolute constant whenever $|n|$ is prime, and that, for every $\varepsilon > 0$, the set of positive integers n for which a $D(n)$ or $D(-n)$ Diophantine m-tuple exists with $m > (1 + \varepsilon) \log \log n$ is of asymptotic density zero.

A related elementary observation made independently by Brown [4], Gupta and Singh [21], and Mohanty and Ramasamy [28] is that $M_n \leqslant 3$ if $n \equiv 2 \pmod 4$. Indeed, being a square, $a_ia_j + n \equiv 0, 1 \pmod 4$. It follows that $a_i \not\equiv a_j \pmod 4$ and that at most one a_i can be even. On the other hand, if $n \not\equiv 2 \pmod 4$ and $n \notin \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then $M_n \geqslant 4$ (cf. [15]).

More generally, Dujella proved in [14] that $M_n \leqslant 31$ for $|n| \leqslant 400$ and

$$M_n < C \log |n|,$$

where $C = 15.476$ if $|n| > 400$ and $C = 9.078$ if $n > 10^{100}$. This is done by estimating separately the quantities

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

He proved that $A_n \leqslant 21$, $B_n < 0.6071 \log |n| + 2.152$, and $C_n < 11.006 \log |n|$ for $|n| > 400$. If $|n| > 10^{100}$, he showed that $C_n < 8.37 \log |n|$ and the final result is derived by combining all of these estimates. The most significant contribution comes from C_n and is obtained by using Gallagher's sieve inequality together with an estimate on double Dirichlet character sums due to Vinogradov. Improving these results, Murty and Becker [3] have recently shown that for any n,

$$M_n \leqslant 2.6071 \log |n| + O\left(\frac{\log |n|}{(\log \log |n|)^2}\right).$$

Our purpose in this manuscript is to relate the estimate of M_n for all sufficiently large n to the Paley graph conjecture (stated below) and show how one can improve the known estimates. The basic idea is to use this conjecture together with Gallagher's sieve inequality to handle B_n and C_n simultaneously which will lead to Theorem 1. We first recall the Paley Graph Conjecture.

Conjecture 1 *(Paley graph conjecture). Let $\varepsilon > 0$ be a real number, $S, T \subseteq \mathbb{F}_p$ for an odd prime p with $|S|, |T| > p^{\varepsilon}$, and χ any nontrivial multiplicative character modulo p. Then, there is some number $\delta = \delta(\varepsilon)$ for which the inequality*

$$\left| \sum_{a \in S, b \in T} \chi(a+b) \right| \leqslant p^{-\delta} |S||T| \tag{1}$$

holds for primes larger than some constant $C(\varepsilon)$.

The related estimate from Murty and Becker [3] yields

$$\left| \sum_{a \in S, b \in T} \chi(ab+n) \right| \leqslant \sqrt{p|S||T|},$$

where $p \nmid n$ is an odd prime and not both sets S and T contain 0.

In general, a positive answer for this conjecture is known only in the case $|S| > p^{1/2+\varepsilon}$, and $|T| > p^{\varepsilon}$. However, if the sets S and T have a certain structure, there are nontrivial estimates that can be obtained under weaker constraints on their size (see [7,18,27,32,33]) using recent advances in additive combinatorics. We quote from [32] why this conjecture is called the Paley graph conjecture below.

> A Paley graph is a graph $G(V, E)$ with vertex set $V = \mathbb{F}_p$ and edge set E such that $(a, b) \in E$ if and only if $a - b$ is a quadratic residue modulo p. For this graph to be undirected, it is also necessary that $p \equiv 1 \bmod 4$. Under this assumption, setting $S = -T$ in the conjecture and taking the Legendre symbol for the multiplicative character χ, we obtain the following remarkable statement: the clique number of the Paley graph and its independence number increase slower than p^{ε} for any positive ε.

On the other hand, Graham and Ringrose [20] proved that for infinitely many primes p, the least quadratic non-residue q is at least $c(\log p)(\log\log\log p)$ for some constant $c > 0$. Obviously, for these primes, (1) does not hold for $S = T = \{1, 2, \dots, q/2\}$. See also [29] for a recent result of Mrazović relating Paley graphs to the result of Graham and Ringrose.

Our main theorem is:

Theorem 1. *If the Paley graph conjecture holds for some $\varepsilon \in (0, 1)$, then*

$$M_n \ll_{\varepsilon} (\log|n|)^{\frac{\varepsilon}{1-\varepsilon}} \left(1 + O\left(\frac{1}{(\log\log|n|)^2}\right)\right).$$

Remark 1. In particular, if for any $\varepsilon > 0$, the Paley graph conjecture holds, then

$$M_n \ll_{\varepsilon} (\log|n|)^{\varepsilon}.$$

We refer the reader to several other related papers that apply results from graph theory to certain problems concerning Diophantine m-tuples such as [23,24,5,10,25].

2. Preliminaries and proof of Theorem 1

We collect here some results needed to prove our main theorem.

Lemma 1 *(cf. [17, Thm 4.2]). For $x \geqslant 2$,*

$$|\theta(x) - x| < 3.965\frac{x}{\log^2 x},$$

where $\theta(x) = \sum_{p \leqslant x} \log p$. Also, for $x \geqslant 1$, $\theta(x) < 2x$.

Lemma 2. *For any* $\alpha \in (0,1)$,

$$\sum_{p \leqslant Q} \frac{\log p}{p^{\alpha}} = \frac{Q^{1-\alpha}}{1-\alpha}\left(1 + O\Big(\frac{1}{\log^2 Q}\Big)\right)$$

with an effectively computable implied constant. Furthermore,

$$\sum_{p \leqslant Q} \frac{\log p}{p^{\varepsilon}} < \frac{2Q^{1-\varepsilon}}{1-\varepsilon}. \tag{2}$$

Proof. Both results follow from Lemma 1 and partial integration. □

Lemma 3 *(cf. [17, Thm 5.1, Lemma 5.10]). For* $x > 1$,

$$\pi(x) \leqslant \frac{x}{\log x}\Big(1 + \frac{1}{\log x} + \frac{2}{\log^2 x} + \frac{7.59}{\log^3 x}\Big). \tag{3}$$

Furthermore, for $k \geqslant 4$,

$$p_k \leqslant k(\log k + \log\log k + 1) < 2k \log k, \tag{4}$$

where p_k *denotes the* k*th prime.*

Lemma 4 *(cf. [22, Thm 11]). For* $n \geqslant 3$,

$$\omega(n) \leqslant 1.38402 \frac{\log n}{\log\log n} \tag{5}$$

with equality for $n = p_1 p_2 \cdots p_9$, *where* $\omega(n)$ *is the number of distinct prime divisors of* n.

The following is an inequality which is a result of Gallagher's Sieve Inequality.

Lemma 5. *Let* $\mathcal{S}$ *be a subset of* $\{1, 2, \ldots, N\}$ *for some positive integer* N*. For any* $1 < Q \leqslant N$,

$$|\mathcal{S}| \leqslant \frac{\sum\limits_{p \leqslant Q} \log p - \log N}{\sum\limits_{p \leqslant Q} \frac{\log p}{|\mathcal{S}_p|} - \log N},$$

where $\mathcal{S}_p = \mathcal{S}$ *mod* p, *provided the denominator is positive.*

Proof of Theorem 1. As mentioned in the introduction, $A_n \leqslant 21$. Thus, it is enough to take a $D(n)$-m-tuple $\mathcal{S}$ lying inside $[1, N]$, where $N = |n|^3$.

Assume Conjecture 1 holds for some $\varepsilon > 0$ at least for the quadratic character given by the Legendre's symbol $\left(\frac{\cdot}{p}\right)$. Then, there exists some $\delta = \delta(\varepsilon) > 0$ such that (1) holds for $p > C(\varepsilon)$ for some constant $C(\varepsilon) > 0$. Increasing $C(\varepsilon)$ if necessary we can make sure that the inequality

$$p^{\varepsilon}(1 - p^{-\delta}) \geqslant 3 \tag{6}$$

also holds for $p > C(\varepsilon)$. Note that $p^{\varepsilon} > 3$ for these primes. If $N \leqslant C(\varepsilon)$, we get $|\mathcal{S}| \leqslant C(\varepsilon)$. Otherwise, assume that N is large enough so that we can take a prime $p \nmid n$ with $C(\varepsilon) < p \leqslant Q < N$, where Q is to be chosen later.

For $i = \pm 1$, let S_i denote the elements a of $\mathcal{S}_p$ for which $\left(\frac{a}{p}\right) = i$. Thus, we have

$$|\mathcal{S}_p| \leqslant |S_1| + |S_{-1}| + 1,$$

with equality when $0 \in \mathcal{S}_p$. Since $p \nmid n$, for each $a \in S_i$, there is at most one $b_0 \in S_i$ such that $p \mid ab_0 + n$, and for $b \in S_i \setminus \{b_0, a\}$, $\left(\frac{ab+1}{p}\right) = 1$. Finally, it may happen that $\left(\frac{a^2+1}{p}\right) = -1$. Thus, assuming $|S_i| > p^{\varepsilon}$ (so that $|S_i| > 3$ as well) would result in

$$\begin{aligned} 0 < |S_i|(|S_i| - 3) \leqslant \sum_{a,b \in S_i} \left(\frac{ab+n}{p}\right) &= \left| \sum_{a,b \in S_i} \left(\frac{b + na^{-1}}{p}\right) \right| \\ &= \left| \sum_{\substack{b \in S_i \\ a \in nS_i^{-1}}} \left(\frac{b+a}{p}\right) \right| \leqslant p^{-\delta(\varepsilon)} |S_i|^2, \end{aligned}$$

implying

$$p^{\varepsilon} < |S_i| \leqslant \frac{3}{1 - p^{-\delta}},$$

which contradicts (6). Thus, we must have $|S_i| \leqslant p^{\varepsilon}$ for $C(\varepsilon) < p \leqslant Q$ with $p \nmid n$.

We conclude that $|\mathcal{S}_p| \leqslant 1 + 2p^{\varepsilon}$. Take $\gamma = 2 + C(\varepsilon)^{-\varepsilon}$. Then, $|\mathcal{S}_p| < \gamma p^{\varepsilon}$ for the primes in question. Therefore,

$$\begin{aligned} \sum_{p \leqslant Q} \frac{\gamma \log p}{|\mathcal{S}_p|} &> \sum_{\substack{C(\varepsilon) < p \leqslant Q \\ p \nmid n}} \frac{\log p}{p^{\varepsilon}} \\ &\geqslant \sum_{p \leqslant Q} \frac{\log p}{p^{\varepsilon}} - \sum_{p \leqslant C(\varepsilon)} \frac{\log p}{p^{\varepsilon}} - \sum_{p \mid n} \frac{\log p}{p^{\varepsilon}}. \end{aligned}$$

If n has no prime divisor exceeding $e^{1/\varepsilon}$, which is the only critical point of $x^{-\varepsilon} \log x$ on $[2, \infty)$, then using the inequality (3) it follows that

$$\sum_{p|n} \frac{\log p}{p^{\varepsilon}} \leqslant \frac{\pi(e^{1/\varepsilon})}{e\varepsilon} \leqslant (1+11\varepsilon)e^{1/\varepsilon-1}.$$

Otherwise, using (2) we obtain

$$\sum_{p|n} \frac{\log p}{p^{\varepsilon}} \leqslant \sum_{p\leqslant p_{\omega(n)}} \frac{\log p}{p^{\varepsilon}} < \frac{2p_{\omega(n)}^{1-\varepsilon}}{1-\varepsilon}.$$

Using the inequalities (4) and (5) to estimate the last term, and combining this with the previous estimate above we derive that

$$\sum_{p|n} \frac{\log p}{p^{\varepsilon}} \ll_{\varepsilon} (\log|n|)^{1-\varepsilon}.$$

Using Lemma 2 again yields

$$\sum_{p\leqslant Q} \frac{\gamma \log p}{|\mathcal{S}_p|} > Q^{1-\varepsilon}\left(1-\frac{c_1}{\log^2 Q}\right) - c_2(\log N)^{1-\varepsilon}$$

for some positive constants c_1 and c_2 depending on ε. Since we need the sum on the left larger than $\gamma \log N$ to be able to use Lemma 5, we choose $Q = (\lambda^{-1}\log N)^{1/(1-\varepsilon)}$ for some $\lambda < 1$. Combining the estimates above and using Lemmas 2 and 5 we obtain

$$\begin{aligned} |\mathcal{S}| &\leqslant \gamma \frac{Q(1+O(1/\log^2 Q)) - \log N}{Q^{1-\varepsilon}\left(1-\frac{c_1}{\log^2 Q}\right) - c_2(\log N)^{1-\varepsilon} - \log N} \\ &\leqslant \frac{\gamma}{(1-\lambda)\lambda^{\frac{\varepsilon}{1-\varepsilon}}} \frac{(\log N)^{\frac{\varepsilon}{1-\varepsilon}}(1+O(1/(\log\log N)^2))}{1-\frac{c_4}{(\log\log N)^2}}. \end{aligned}$$

Choosing $\lambda = \varepsilon$ minimizes the coefficient above and we obtain

$$|\mathcal{S}| \leqslant \frac{2C(\varepsilon)^{\varepsilon}+1}{C(\varepsilon)^{\varepsilon}(1-\varepsilon)}\left(\frac{3}{\varepsilon}\right)^{\frac{\varepsilon}{1-\varepsilon}} (\log|n|)^{\frac{\varepsilon}{1-\varepsilon}}\left(1+O\Big(\frac{1}{(\log\log|n|)^2}\Big)\right). \quad \square$$

3. Concluding remarks

The Paley graph conjecture is not only important in graph theory but has important consequences in computer science as explained in [8]. There is some progress towards this conjecture in the emerging field of additive combinatorics as evident in the paper of [7]. However, here, one needs to have some information on the additive structure of our sets S and T. Our main idea in the paper is to demonstrate the intimate connection between this important conjecture and the problem of Diophantine m-tuples, which was hitherto unknown.

Acknowledgments

We would like to thank the referees for carefully reading this manuscript and their helpful comments/suggestions. This work has been completed in Queen's University during the sabbatical visit of the first author and he would like to thank both Queen's University for their hospitality and Bilkent University for their support.

References

[1] A. Baker, Linear forms in the logarithms of algebraic numbers. IV, Mathematika 15 (1968) 204–216.
[2] A. Baker, H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, Q. J. Math. Oxford Ser. (2) 20 (1969) 129–137.
[3] R. Becker, M.R. Murty, Diophantine m-tuples, Glas. Mat. Ser. III 54 (74) (2019) 65–75.
[4] E. Brown, Sets in which $xy + k$ is always a square, Math. Comp. 45 (172) (1985) 613–620.
[5] Y. Bugeaud, K. Gyarmati, On generalizations of a problem of Diophantus, Illinois J. Math. 48 (4) (2004) 1105–1115.
[6] L. Caporaso, J. Harris, B. Mazur, Uniformity of rational points, J. Amer. Math. Soc. 10 (1) (1997) 1–35.
[7] M. Chang, On a question of Davenport and Lewis and new character sum bounds in finite fields, Duke Math. J. 145 (3) (2008) 409–442.
[8] B. Chor, O. Goldreich, Unbiased bits from sources of weak randomness and probabilistic communication complexity, SIAM J. Comput. 17 (2) (1988) 230–261.
[9] L.E. Dickson, Recent publications: reviews: history of mathematics; vol. I, General survey of the history of elementary mathematics; vol. II, Special topics of elementary mathematics, Amer. Math. Monthly 32 (10) (1925) 511–512.
[10] R. Dietmann, C. Elsholtz, K. Gyarmati, M. Simonovits, Shifted products that are coprime pure powers, J. Combin. Theory Ser. A 111 (1) (2005) 24–36.
[11] A. Dujella, F. Luca, Diophantine m-tuples for primes, Int. Math. Res. Not. (47) (2005) 2913–2940.
[12] A. Dujella, On the size of Diophantine m-tuples, Math. Proc. Cambridge Philos. Soc. 132 (1) (2002) 23–33.
[13] A. Dujella, There are only finitely many Diophantine quintuples, J. Reine Angew. Math. 566 (2004) 183–214.
[14] A. Dujella, Bounds for the size of sets with the property $D(n)$, Glas. Mat. Ser. III 39 (59) (2) (2004) 199–205.
[15] A. Dujella, Generalization of a problem of Diophantus, Acta Arith. 65 (1) (1993) 15–27.
[16] A. Dujella, On Diophantine quintuples, Acta Arith. 81 (1997) 69–79.
[17] P. Dusart, Explicit estimates of some functions over primes, Ramanujan J. 45 (1) (2018) 227–251.
[18] J. Friedlander, H. Iwaniec, Estimates for character sums, Proc. Amer. Math. Soc. 119 (2) (1993) 365–372.
[19] P. Gibbs, Some rational Diophantine sextuples (English summary), Glas. Mat. Ser. III 41 (61) (2) (2006) 195–203.
[20] S.W. Graham, C.J. Ringrose, Lower bounds for least quadratic nonresidues, in: Analytic Number Theory, Allerton Park, IL, 1989, in: Progr. Math., vol. 85, Birkhäuser Boston, Boston, MA, 1990, pp. 269–309.
[21] H. Gupta, K. Singh, On k-triad sequences, Int. J. Math. Math. Sci. 8 (4) (1985) 799–804.
[22] R. Guy, Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n (in French) [Estimate of the Chebyshev function θ on the kth prime number and large values of the number of prime divisors function $\omega(n)$ of n], Acta Arith. 42 (4) (1983) 367–389.
[23] K. Gyarmati, On a problem of Diophantus, Acta Arith. 97 (1) (2001) 53–65.
[24] K. Gyarmati, A. Sárközy, C.L. Stewart, On shifted products which are powers, Mathematika 49 (1–2) (2002) 227–230, (2004).
[25] K. Gyarmati, C.L. Stewart, On powers in shifted products, Glas. Mat. Ser. III 42(62) (2) (2007) 273–279.
[26] B. He, A. Togbé, V. Ziegler, There is no Diophantine quintuple, Trans. Amer. Math. Soc. 371 (9) (2019) 6665–6709.

[27] A.A. Karatsuba, The distribution of values of Dirichlet characters on additive sequences, Dokl. Akad. Nauk SSSR 319 (3) (1991) 543–545, Sov. Math., Dokl. 44 (1) (1992) 145–148.
[28] S. Mohanty, A. Ramasamy, On $p_{r,k}$ sequences, Fibonacci Quart. 23 (1) (1985) 36–44.
[29] R. Mrazović, A random model for the Paley graph, Q. J. Math. 68 (1) (2017) 193–206.
[30] W.M. Schmidt, Integer points on curves of genus 1, Compos. Math. 81 (1) (1992) 33–59.
[31] On some applications of Diophantine approximations. A translation of Carl Ludwig Siegel's "Über einige Anwendungen diophantischer Approximationen" by Clemens Fuchs. With a commentary and the article "Integral points on curves: Siegel's theorem after Siegel's proof" by Fuchs and Umberto Zannier. Edited by Zannier. Quaderni/Monographs, 2. Edizioni della Normale, Pisa, 2014.
[32] A.S. Volostnov, On double sums with multiplicative characters (in Russian), Russian summary, Mat. Zametki 104 (2) (2018) 174–182.
[33] A.S. Volostnov, I.D. Shkredov, Sums of multiplicative characters with additive convolutions, in: Analytic and Combinatorial Number Theory, in: Trudy Mat. Inst. Steklova, vol. 296, MAIK Nauka/Interperiodica, Moscow, 2017, pp. 265–279, Proc. Steklov Inst. Math. 296 (2017) 256–269.