GENERALIZED DIOPHANTINE m-TUPLES

ANUP B. DIXIT, SEOYOUNG KIM, AND M. RAM MURTY

ABSTRACT. For non-zero integers n and $k \geq 2$, a generalized Diophantine m-tuple with property $D_k(n)$ is a set of m positive integers $\{a_1, a_2, \ldots, a_m\}$ such that $a_i a_j + n$ is a k-th power for $1 \leq i < j \leq m$. Define $M_k(n) := \sup\{|S| : S \text{ has property } D_k(n)\}$. In this paper, we study upper bounds on $M_k(n)$, as we vary n over positive integers. In particular, we show that for $k \geq 3$, $M_k(n)$ is $O(\log n)$ and further assuming the Paley graph conjecture, $M_k(n)$ is $O((\log n)^\epsilon)$. The problem for $k = 2$ was studied by a long list of authors that goes back to Diophantus.

1. Introduction

Given a non-zero integer n, we say a set of natural numbers $S = \{a_1, a_2, \ldots, a_m\}$ is a Diophantine m-tuple with property $D(n)$ if $a_i a_j + n$ is a perfect square for all $1 \leq i < j \leq m$. Diophantus first studied such sets of numbers and found the quadruple $\{1, 33, 68, 105\}$ with property $D(256)$. The first $D(1)$-quadruple $\{1, 3, 8, 120\}$ was discovered by Fermat, and this was later generalized by Euler, who found the following infinite family of quadruples with property $D(1)$, namely

$$\{a, b, a + b + 2r, 4r(r + a)(r + b)\},$$

where $ab + 1 = r^2$. In fact, it is known that any $D(1)$-triple can be extended to a Diophantine quadruple [1]. In 1969, using Baker's theory of linear forms in logarithms and a reduction method based on continued fractions, Baker and Davenport [2] proved that Fermat's example is the only extension of $\{1, 3, 8\}$ with property $D(1)$. In 2004, Dujella [9], using similar methods, proved that there are no $D(1)$-sextuples and there are only finitely many $D(1)$-quintuples, if any. The conjecture on the non-existence of $D(1)$-quintuples was finally settled in 2019 by He, Togbé, and Ziegler in [17].

However, in general, there are $D(n)$-quintuples for $n \neq 1$. For instance,

$$\{1, 33, 105, 320, 18240\} \quad \text{and} \quad \{5, 21, 64, 285, 6720\}$$

are Diophantine quintuples satisfying property $D(256)$. Also, we note that there are known examples of $D(n)$-sextuples, but no $D(n)$-septuple is known. So, it is natural to study the size of the largest tuple with property $D(n)$. Following [8], we define

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

Date: July 25, 2021.

2010 *Mathematics Subject Classification.* 11D45, 11D72, 11N36.

Key words and phrases. Diophantine m-tuples, Gallagher's sieve, Paley graph conjecture, abc conjecture.

The first two authors were supported by Coleman Postdoctoral Fellowships. The first author was also partially supported by the Inspire Faculty fellowship. Research of the third author was partially supported by an NSERC Discovery grant.

Note that if $S = \{a_1, a_2, \ldots\}$ satisfies property $D(n)$, then $x = a_i$ yields an integer point on the elliptic curve

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

for all $i > 3$. By Siegel's theorem (see for example, page 146 of [21]), the number of integer points on any elliptic curve is bounded. Hence, S cannot be an infinite set. But the known upper bounds for the number of integer points on (1) depend on the coefficients n, a_1, a_2, a_3 (see [19]). Therefore, Siegel's theorem does not give significant information about M_n. However, the same line of reasoning can produce conditional results. Caporaso, Harris, and Mazur [6] conjectured that the number of rational points on curves of genus $g \geq 2$ is bounded by a constant which only depends on g (which is implied by a more general conjecture of Lang). This conjecture implies that $\sup_n M_n$ is bounded.

Unconditionally, Dujella [8] showed that

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

where C is an absolute constant. He also showed that for $n > 10^{100}$, one can choose $C = 8.37$. This constant was improved by Becker and Murty [3], who showed that for any n,

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

More recently, Güloğlu and Murty [15] discovered a connection between the Paley graph conjecture (described below) and this problem. They showed that under this conjecture, for any $\epsilon > 0$,

$$M_n \ll (\log |n|)^{\epsilon},$$

where the implied constant depends only on ϵ.

In this paper, we focus on the following natural generalization of the concept of Diophantine m-tuples.

Definition 1 (generalized Diophantine m-tuples)**.** *Fix a natural number $k \geq 2$. A set of natural numbers $S = \{a_1, a_2, \ldots, a_m\}$ is said to satisfy property $D_k(n)$ if $a_ia_j + n$ is a k-th power for all $1 \leq i < j \leq m$.*

We analogously define the following quantity for each n,

$$M_k(n) := \sup\{|S| : S \text{ satisfies property } D_k(n)\}.$$

For $k \geq 3$ and $m \geq 3$, we can apply the celebrated theorem of Faltings [12] to deduce that a superelliptic curve of the form

$$y^k = f(x) = (a_1x + n)(a_2x + n)(a_3x + n)(a_4x + n) \cdots (a_mx + n)$$

has only finitely many rational points and a fortiori, finitely many integral points. Therefore, a set S satisfying property $D_k(n)$ must be finite. All known upper bounds for the number of such integral points depend on the coefficients of $f(x)$. In fact, one could produce upper bounds in terms of the number of prime divisors of the discriminant of $f(x)$ (see [11]). Thus, the question regarding the size of $M_k(n)$ remains unanswered. Again, the Caporaso-Harris-Mazur conjecture [6] implies that $M_k(n)$ is uniformly bounded, independent of n. The case $n = 1$ is better understood. Unconditionally, Bugeaud and Dujella [5] showed that

$$M_3(1) \leq 7, \quad M_4(1) \leq 5, \quad M_k(1) \leq 4 \text{ for } 5 \leq k \leq 176, \text{ and } M_k(1) \leq 3 \text{ for } k \geq 177.$$

In other words, the size of $D_k(1)$-tuples is bounded by 3 for large enough k. In the general case, for any $n \neq 0$ and $k \geq 3$, Bérczes, Dujella, Hajdu and Luca [4] obtained upper bounds for $M_k(n)$. In particular, they showed that for $k \geq 5$

$$M_k(n) \leq 2|n|^5 + 3. \tag{2}$$

The goal of this paper is to obtain better upper bounds on $M_k(n)$ and the set

$$M_k(n; L) := \sup\{|S \cap [n^L, \infty)| : S \text{ satisfies property } D_k(n)\}$$

as we vary n over positive integers. Henceforth, we assume that $n > 0$.

We produce sharper bounds on $M_k(n)$ under the Paley graph conjecture, namely,

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

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

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

The conjecture is known for the case $|S| > p^{1/2+\epsilon}$ and $|T| > p^\epsilon$. For more information about the conjecture and related recent progress, we refer the readers to [15] and [20, p. 305]. One can expect a similar conjecture to be valid in general for all finite fields, but we will not need such a generalization here.

Our main theorem is:

Theorem 1.1. *Let k be a positive integer ≥ 3. Then, the following holds as $n \to \infty$.*

(a) *For $L \geq 3$,*

$$M_k(n, L) \ll 1,$$

where the implied constant depends on k and L, but is independent of n.

(b) *Unconditionally,*

$$M_k(n) \ll_k \log n.$$

(c) *Assuming the Paley graph conjecture, for any $\epsilon > 0$,*

$$M_k(n) \ll_{k,\epsilon} (\log n)^\epsilon.$$

This improves the bound (2) obtained in [4] in the n-aspect for $n > 0$. The methods in this paper could be modified to address the case $n < 0$, but we do not do so here.

2. **Preliminaries**

In this section, we develop the necessary ingredients to prove our main theorem.

2.1. **Gallagher's large sieve.** In 1971, Gallagher [13] discovered an elementary sieve inequality which he called the larger sieve. We refer the reader to [7] for the general discussion but here record the result in a form applicable to our context.

Theorem 2.1. *Let N be a natural number and $\mathcal{S}$ a subset of $\{1, 2, \dots, N\}$. Let $\mathcal{P}$ be a set of primes. For each prime $p \in \mathcal{P}$, let $\mathcal{S}_p = \mathcal{S} \pmod p$. For any $1 < Q \leq N$, we have*

$$|\mathcal{S}| \leq \frac{\sum\limits_{p \leq Q, p \in \mathcal{P}} \log p - \log N}{\sum\limits_{p \leq Q, p \in \mathcal{P}} \frac{\log p}{|\mathcal{S}_p|} - \log N}, \tag{3}$$

where the summations are over primes $p \leq Q, p \in \mathcal{P}$ and the inequality holds provided the denominator is positive.

2.2. **A quantitative Roth's theorem.** Quantitative results related to counting exceptions in Roth's celebrated theorem on Diophantine approximations were established by a variety of authors. We will use the following result due to Evertse [10]. For an algebraic number ξ of degree r, we define the (absolute) height by

$$H(\xi) := \left(a \prod_{i=1}^{r} \max(1, |\xi^{(i)}|) \right)^{1/r},$$

where $\xi^{(i)}$ for $1 \leq i \leq r$ are the conjugates (over $\mathbb{Q}$) and a is the positive integer such that

$$a \prod_{i=1}^{r} (x - \xi^{(i)})$$

has rational integer coefficients with gcd 1.

Theorem 2.2. *Let α be a real algebraic number of degree r over $\mathbb{Q}$, and $0 < \kappa \leq 1$. The number of rational numbers p/q satisfying $\max(|p|, |q|) \geq \max(H(\alpha), 2)$,*

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{\max(|p|, |q|)^{2+\kappa}}$$

is at most

$$2^{25} \kappa^{-3} \log(2r) \log(\kappa^{-1} \log(2r)).$$

2.3. **Vinogradov's theorem.** The following bound on character sums was proved by Vinogradov (see [22]).

Lemma 2.3. *Let $\chi \pmod q$ be a non-trivial Dirichlet character and n be an integer such that $(n, q) = 1$. If $\mathcal{A} \subseteq (\mathbb{Z}/q\mathbb{Z})^*$ and $\mathcal{B} \subseteq (\mathbb{Z}/q\mathbb{Z})^* \cup \{0\}$, then*

$$\sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} \chi(ab + n) \leq \sqrt{q|\mathcal{A}||\mathcal{B}|}.$$

The original method of Vinogradov does not produce the bound above and instead gives the right hand side as $\sqrt{2q|\mathcal{A}||\mathcal{B}|}$. However, the above bound holds and a short proof of this can be found in [3, Proposition 2.5].

The next lemma is a variation of a gap principle of Gyarmati [14].

Lemma 2.4. *Let $k \geq 2$. Suppose that a, b, c, d are positive integers such that $a < b$ and $c < d$. Suppose further that*

$$ac + n, \quad bc + n, \quad ad + n, \quad bd + n$$

are perfect k-th powers. Then,

$$bd \geq k^k n^{-k} (ac)^{k-1}.$$

Proof. Since $(b - a)(d - c) > 0$, it is easily seen that

$$(ac + n)(bd + n) > (ad + n)(bc + n).$$

As $(ac + n)(bd + n)$ and $(ad + n)(bc + n)$ are both perfect k-th powers, we see that

$$\begin{aligned} (ac + n)(bd + n) &\geq [((ad + n)(bc + n))^{1/k} + 1]^k \\ &\geq (ad + n)(bc + n) + k((ad + n)(bc + n))^{(k-1)/k} \\ &\geq (ad + n)(bc + n) + k(abcd)^{(k-1)/k}. \end{aligned}$$

Thus,

$$n(ac + bd) \geq n(ad + bc) + k(abcd)^{(k-1)/k}.$$

As $ad + bc > ac$, we deduce

$$nbd > k(abcd)^{(k-1)/k}$$

so that

$$bd \geq k^k n^{-k} (ac)^{k-1},$$

as claimed. □

The following corollaries of the above lemma will be useful to keep in mind as we proceed with our proof of the main theorem. Loosely speaking, they show that "large" elements of any set with property $D_k(n)$ have "super-exponential growth."

Corollary 1. *Let $k \geq 3$. If $n^3 \leq a < b < c < d < e$ are natural numbers such that the set $\{a, b, c, d, e\}$ has property $D_k(n)$, then $e \geq b^{k-1}$.*

Proof. We have by Lemma 2.4,

$$ce \geq k^k n^{-k} (bd)^{k-1} \geq k^k n^{-k} (bc)^{k-1}.$$

Thus, $e \geq b^{k-1} c^{k-2} n^{-k} \geq b^{k-1} n^{2k-6} \geq b^{k-1}$, as claimed. □

An easy induction argument now shows the following.

Corollary 2. *Let $k \geq 3$ and $m \geq 5$. Suppose that $n^3 \leq a_1 < a_2 < \ldots < a_m$ and the set $\{a_1, a_2, ..., a_m\}$ has property $D_k(n)$. Then $a_{2+3j} \geq a_2^{(k-1)^j}$ provided $1 \leq j \leq (m - 2)/3$.*

3. **Proof of the main theorem**

3.1. **Proof of Theorem 1.1 (a).** If k is an even integer, then it reduces to the "square" case, which was treated by Dujella [8], who showed that $M_2(n; 3) \leq 21$. Hence, for any even k, we clearly obtain Theorem 1.1 (a).

Thus, we can assume $k \geq 3$ to be an odd integer. Let $m = M_k(n)$ and $S = \{a_1, a_2, a_3, \ldots, a_m\}$ be a generalized m-tuple with property $D_k(n)$. Suppose $n^L < a_1 < a_2 < \ldots < a_m$ for some $L \geq 3$. Consider the system of equations

$$\begin{cases} a_1 x + n = u^k \\ a_2 x + n = v^k. \end{cases} \tag{4}$$

Clearly, $x = a_i$ for $i \geq 3$ are solutions to this system. Moreover, we have

$$a_2 u^k - a_1 v^k = n(a_2 - a_1). \tag{5}$$

Let $\alpha := (a_1/a_2)^{1/k}$ and $\zeta_k := e^{2\pi i/k}$. Then, we prove the following lemma.

Lemma 3.1. *Let $k \geq 3$ be odd. Suppose u, v satisfy the system of equations (4). Let*

$$c(k) := \prod_{j=1}^{(k-1)/2} \left(\sin \frac{2\pi j}{k}\right)^2.$$

Then, for $n > 2^{1/(L-1)} c(k)^{-1/(L-1)}$,

$$\left|\frac{u}{v} - \alpha\right| \leq \frac{a_2}{2v^k}. \tag{6}$$

Proof. We can write

$$\begin{aligned} a_2 u^k - a_1 v^k = a_2 \left(u^k - (\alpha v)^k\right) &= a_2 \prod_{j=0}^{k-1} \left(u - \alpha \zeta_k^j v\right) \\ &= a_2 |u - \alpha v| \prod_{j=1}^{(k-1)/2} \left|u - \alpha \zeta_k^j v\right|^2, \end{aligned} \tag{7}$$

where the second equality can be obtained by separating the factor for $j = 0$ and pairing $u - \alpha\zeta_k^j v$ with its complex conjugate (which is distinct since k is odd). Observe that for a complex number $z = x + iy$, with x, y real, we have $|z|^2 \geq \max(x^2, y^2)$. Thus, for $1 \leq j \leq (k-1)/2$,

$$\left|u - \alpha \zeta_k^j v\right|^2 \geq |\alpha|^2 v^2 \left(\sin \frac{2\pi j}{k}\right)^2,$$

since α and v are real. Using this and (5) in (7), we deduce

$$n a_2 \geq n(a_2 - a_1) \geq a_2 |u - \alpha v|\, |\alpha|^{k-1} v^{k-1} c(k) \geq a_2 |u - \alpha v| |\alpha|^k v^{k-1} c(k),$$

since $|\alpha| < 1$. Therefore,

$$\left|\frac{u}{v} - \alpha\right| \leq \frac{n(a_2 - a_1)}{a_2\, c(k) v^k |\alpha|^k} \leq \frac{n a_2}{a_1\, c(k) v^k}.$$

Since $a_1 > n^L$, for $n^{L-1} > 2c(k)^{-1}$, we obtain

$$\left|\frac{u}{v} - \alpha\right| \leq \frac{a_2}{2v^k}$$

as claimed. □

Towards the proof of Theorem 1.1 (a), it suffices to show that there are finitely many solutions (u_i, v_i) for the system of equations (4) and to estimate this number. In this context, it is useful to keep in mind that the v_i have "super-exponential growth" by Corollary 2. An estimate for the system of equations (4) would follow from the fact that there are few rational approximations of α as in (6). In order to show this, we apply Theorem 2.2 to α, which is a real algebraic number of degree k. Moreover, $H(\alpha) \leq a_2^{1/k}$ with equality if $(a_1, a_2) = 1$. We first derive the following result based on a gap principle which is well-known in the theory of Diophantine approximation.

Lemma 3.2. *Let (u_i, v_i) denote distinct pairs that satisfy the system of equations (4) with $v_{i+1} > v_i$. For $n > 2^{1/(L-1)} c(k)^{-1/(L-1)}$, there is an absolute constant i_0, depending only on k, such that for $i \geq i_0$,*

$$\left| \frac{u_i}{v_i} - \alpha \right| < \frac{1}{v_i^{k-1/2}},$$

and $v_i > a_2^4$.

Proof. By Lemma 3.1, we have

$$\left| \frac{u_i}{v_i} - \alpha \right| < \frac{a_2}{2v_i^k}.$$

To prove the lemma, we need to show $a_2 < 2v_i^{1/2}$ for $i > i_0$. But this is now clear by a simple application of Corollary 2. Indeed, as $v_i^k = a_2 a_i + n$, we have $v_i \geq a_i^{1/k}$ and by Corollary 2,

$$a_{2+3j} \geq a_2^{(k-1)^j} \tag{8}$$

so that $v_{2+3j} \geq a_2^{(k-1)^j/k}$. Choose a positive integer j_0 satisfying $(k-1)^{j_0} > 4k$. Since $k \geq 3$, one can choose $j_0 = 4$. Setting $i_0 = 2 + 3j_0$, we have $v_i \geq v_{i_0} > a_2^4$ for all $i \geq i_0$. This completes the proof.

□

Now let $u_1/v_1, \ldots, u_m/v_m$ satisfy the system of equations (4) with $v_i > \max(a_2^{1/k}, 2) \geq \max(H(\alpha), 2)$. By Lemma 3.2, for $i_0 \leq i \leq m$,

$$\left| \frac{u_i}{v_i} - \alpha \right| \leq \frac{1}{v_i^{k-1/2}} \leq \frac{1}{v_i^{2.5}}, \tag{9}$$

because $k \geq 3$. Since $\alpha = (a_1/a_2)^{1/k} < 1$, $\max(u_i, v_i) = v_i$. Hence, an application of Theorem 2.2 shows that the number of such i's is $O((\log k)(\log\log k))$. This proves Theorem 1.1(a).

3.2. **Proof of Theorem 1.1 (b).** Let $S = \{a_1, a_2, \ldots, a_m\}$ be a generalized Diophantine m-tuple with property $D_k(n)$ and each $a_i \leq n^3$. Since $M_k(n; 3) \ll 1$, it is enough to show that $|S| \ll \log n$. We will apply the larger sieve with primes $p \leq Q$ satisfying $p \equiv 1 \pmod{k}$ because such primes have a non-trivial Dirichlet character χ of order k. For these primes p, we let S_p be the image of $S \pmod{p}$. Applying Lemma 2.3, with $\mathcal{A} = \mathcal{B} = S_p$ and a character $\chi \pmod{p}$ of order k, we obtain

$$|S_p|(|S_p| - 1) \leq \sum_{a \in S_p - \{0\}} \sum_{b \in S_p} \chi(ab + n) + |S_p| \leq \sqrt{p}|S_p| + |S_p|.$$

Hence,

$$|S_p| \ll \sqrt{p}.$$

Since $a_i \leq n^3$, we take $N = n^3$. Applying Theorem 2.1, we get

$$\Big|S\Big| \leq \frac{\displaystyle\sum_{p\leq Q, p\equiv 1(\mathrm{mod}\, k)} \log p - \log N}{\displaystyle\sum_{p\leq Q, p\equiv 1(\mathrm{mod}\, k)} \frac{\log p}{|S_p|} - \log N}.$$

By the prime number theorem for arithmetic progressions,

$$\sum_{p\leq Q, p\equiv 1(\mathrm{mod}\, k)} \log p \sim \frac{Q}{\varphi(k)},$$

and by a simple partial summation,

$$\sum_{p\leq Q, p\equiv 1(\mathrm{mod}\, k)} \frac{\log p}{\sqrt{p}} \sim \frac{2\sqrt{Q}}{\varphi(k)}.$$

Since $|S_p| \ll \sqrt{p}$, we deduce

$$|S| \ll_k \frac{Q - \varphi(k)\log N}{2\sqrt{Q} - \varphi(k)\log N}.$$

Choosing $Q = (\varphi(k)\log N)^2$, we conclude that $|S| \ll_k \log N \ll \log n$ as claimed.

3.3. **Proof of Theorem 1.1 (c).** From Theorem 1.1(a), $M_k(n;3)$ is bounded, and thus it is sufficient to consider an m-tuple with the property $D_k(n)$ which lies in $[1, N]$, where $N = n^3$. Assume Conjecture 1 holds for some $\epsilon > 0$. If necessary, we choose larger $C(\epsilon)$ so that the inequality

$$p^{\epsilon}(1 - p^{-\delta}) \geq 3 \tag{10}$$

also holds for $p > C(\epsilon)$. Without loss of generality, we assume that N is large enough so that we can take a prime $p \nmid n$ satisfying

$$C(\epsilon) < p \leq Q < N, \quad p \equiv 1(\mathrm{mod}\, k),$$

where Q will be chosen later in the proof. Let $S = \{a_1, a_2, \ldots, a_m\} \subset \mathbb{Z}$ be a Diophantine m-tuple with property $D_k(n)$ and let $S_p = S \pmod p$ for some prime p in $\mathbb{Z}$. We denote by ζ_k a primitive kth root of unity. Since $p \equiv 1(\mathrm{mod}\, k)$, there is a Dirichlet character $\chi(\mathrm{mod}\, p)$ of order k. For $i = 0, 1, \ldots, k-1$, define for each prime p,

$$T_i = \left\{ a \in S_p \;\middle|\; \chi(a) = \zeta_k^i \right\}.$$

Then we have

$$|S_p| \leq |T_0| + |T_1| + \cdots + |T_{k-1}| + 1, \tag{11}$$

with equality when $0 \in S_p$. Since $p \nmid n$, for each $a \in T_i$, there is at most one $b_0 \in T_i$ such that $ab_0 + n \equiv 0(\mathrm{mod}\, p)$. Moreover, for $b \in T_i \backslash \{a, b_0\}$, we have $\chi(ab+n) = 1$, since χ is a character of order k. Also, it is possible that $\chi(a^2 + n) = -1$. Hence, by the triangle inequality, under the Paley graph conjecture, the assumption $|T_i| > p^{\epsilon}$ (thus, $|T_i| > 3$) implies that

$$0 < |T_i|(|T_i| - 3) \leq \left| \sum_{a,b\in T_i} \chi(ab+n) \right| = \left| \sum_{a,b\in T_i} \chi(b + na^{-1}) \right| = \left| \sum_{\substack{a\in nT_i^{-1} \\ b\in T_i}} \chi(b+a) \right| \leq p^{-\delta}|T_i|^2,$$

where $\delta = \delta(\epsilon)$. Thus, we have

$$p^{\epsilon} < |T_i| \leq \frac{3}{1-p^{-\delta}},$$

which gives a contradiction to (10), and we must have $|T_i| \leq p^{\epsilon}$ for $C(\epsilon) < p \leq Q$ with $p \nmid n$ and $p \equiv 1 (\mathrm{mod}\, k)$. From (11), we get

$$|S_p| \leq 1 + kp^{\epsilon},$$

for $C(\epsilon) < p \leq Q$ with $p \nmid n$ and $p \equiv 1 (\mathrm{mod}\, k)$. Take $\gamma = k + C(\epsilon)^{-\epsilon}$, then $|S_p| < \gamma p^{\epsilon}$ for these primes, and we obtain

$$\begin{aligned}\sum_{p \leq Q, p \equiv 1 (\mathrm{mod}\, k)} \frac{\gamma \log p}{|S_p|} &> \sum_{\substack{C(\epsilon) < p \leq Q, p \equiv 1 (\mathrm{mod}\, k) \\ p \nmid n}} \frac{\log p}{p^{\epsilon}} \\ &\geq \sum_{p \leq Q, p \equiv 1 (\mathrm{mod}\, k)} \frac{\log p}{p^{\epsilon}} - \sum_{p \leq C(\epsilon)} \frac{\log p}{p^{\epsilon}} - \sum_{p \mid n} \frac{\log p}{p^{\epsilon}}.\end{aligned}$$

The rest of the proof can follow [15]. Alternatively, we present the following proof which is simpler. Note that we have

$$\sum_{p \mid n} \frac{\log p}{p^{\epsilon}} = \mathcal{O}_{\epsilon}\left(\frac{\log n}{\log \log n}\right)$$

since the fucntion $p \mapsto \log p / p^{\epsilon}$ has a maximal value depending on ϵ. Then the application of the prime number theorem for arithmetic progressions (as applied before) implies

$$\sum_{p \leq Q, p \equiv 1 (\mathrm{mod}\, k)} \frac{\log p}{p^{\epsilon}} \sim \frac{Q^{1-\epsilon}}{(1-\epsilon)\varphi(k)}. \tag{12}$$

Hence, we have the lower denominator of the expression from Gallagher's sieve

$$\sum_{p \leq Q, p \equiv 1 (\mathrm{mod}\, k)} \frac{\gamma \log p}{|S_p|} > \frac{Q^{1-\epsilon}}{(1-\epsilon)\varphi(k)} - \mathcal{O}_{\epsilon}\left(\frac{\log n}{\log \log n}\right).$$

Choosing $Q = (\gamma \varphi(k))^{1/(1-\epsilon)} (\log N)^{1/(1-\epsilon)}$, we obtain

$$\sum_{p \leq Q, p \equiv 1 (\mathrm{mod}\, k)} \frac{\log p}{|S_p|} - \log N > \frac{(1+o(1)) \log N}{(1-\epsilon)} - \mathcal{O}_{\epsilon}\left(\frac{\log n}{\log \log n}\right) - \log N \gg_{\epsilon} \log N, \tag{13}$$

and the numerator is bounded above by $\ll (\log N)^{1/(1-\epsilon)}$. Hence, we obtain

$$|S| \ll (\log N)^{1/(1-\epsilon)-1} < (\log N)^{O(\epsilon)},$$

and the theorem is proved.

4. **Concluding remarks**

The methods applied above are effective and one can obtain precise upper bounds for $M_k(n)$. The key point to note is that though Roth's theorem is not effective, the number of exceptions to Roth's theorem affords an effective estimate as was first noticed by Roth and Davenport shortly after Roth proved his celebrated theorem. This was subsequently exploited by a sequence of mathematicians such as Bombieri, Corvaja, Mignotte, van der Poorten, Schmidt, and finally Evertse whose theorem we have used in this paper.

Acknowledgements

We thank Andrej Dujella, Ahmet Güloğlu and Siddhi Pathak for helpful comments on an earlier version of this paper. We also thank the anonymous referees for their helpful suggestions.

References

[1] J. Arkin, V. E. Hoggatt, Jr., and E. G. Straus. On Euler's solution of a problem of Diophantus. *Fibonacci Quart.*, **17**, no. 4, (1979), 333-339.
[2] A. Baker and H. Davenport. The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$. *Quar. J. Math. Oxford Ser. (2)*, **20**, (1969).
[3] R. Becker and M. R. Murty. Diophantine m-tuples with the property $D(n)$. *Glas. Mat. Ser. III*, **54**, (2019), 65-75.
[4] A. Bérczes, A. Dujella, L. Hajdu and F. Luca. On the size of sets whose elements have perfect power n-shifted products. *Publ. Math. Debrecen*, **79**, no. 3-4, (2011), 325–339.
[5] Y. Bugeaud and A. Dujella. On a problem of Diophantus for higher powers. *Math. Proc. Cambridge Philos. Soc.*, **135**, (2003), 1-10.
[6] L. Caporaso, J. Harris and B. Mazur. Uniformity of rational points. *J. Amer. Math. Soc.*, **10**, (1997), 1-35.
[7] A. Cojocaru and M. Ram Murty, An introduction to sieve methods and their applications, London Mathematical Society Student Texts **66**, Cambridge University Press, 2005.
[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 finintely many Diophantine quintuples. *J. Reine Angew. Math.*, **566**, (2004), 183-214.
[10] J.-H. Evertse. On the quantitative subspace theorem, *Journal of Mathematical Sciences*, **171**, no. 6, (2010), 824-837.
[11] J.-H. Evertse and J. H. Silverman. Uniform bounds for the number of solutions to $Y^n = f(X)$. *Math. Proc. Cambridge Philos. Soc.*, **100**, no. 2, (1986), 237-248.
[12] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zählkorpern, *Inventiones Math.*, **73**, (1983), 349-366. Erratum: ibid., **75**, 381.
[13] P. X. Gallagher. A larger sieve. *Acta Arith.*, **18**, (1971), 77-81.
[14] K. Gyarmati, On a problem of Diophantus, *Acta Arith.,* **97**, (2001), 53-65.
[15] A. M. Güloğlu and M. R. Murty. The Paley graph conjecture and Diophantine m-tuples. *J. Combin. Theory Ser. A*, **170**, (2020), 105155.
[16] M. Hall Jr., The diophantine equation $x^3 - y^2 = k$, in Computers in Number Theory, edited by A.O.L. Atkin and B. Birch, Academic Press, London, (1971), 173-198.
[17] B. He, A. Togbé, V. Ziegler. There is no Diophantine quintuple. *Trans. Amer. Math. Soc.*, **371**, no. 9, (2019), 6665-6709.
[18] K. F. Ireland and M. I. Rosen. A classical introduction to modern number theory, vol. **84** of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, (1982).
[19] W. M. Schmidt. Integer points on curves of genus 1. *Compositio Math.*, **81**, (1992), 33-59.
[20] I. E. Shparlinski. Finite fields: theory and computation, vol. **477** of *Mathematics and its Applications*. Kluwer Academic Publishers, Dordrecht, (1999).
[21] J. Silverman and J. Tate, Rational Points on Elliptic Curves, Undergraduate Texts in Mathematics, Springer, New York, (1992).
[22] I. M. Vinogradov. Elements of number theory. Dover Publications, Inc., New York, (1954). Translated by S. Kravetz.
[23] P. Vojta, Diophantine Approximation and Value Distribution Theory, Lecture Notes in Mathematics, **1239**, Springer-Verlag, Berlin, (1987).

Institute of Mathematical Sciences, CIT Campus, Taramani, Chennai, Tamil Nadu, India 600113.
Email address: anupdixit@imsc.res.in

Department of Mathematics and Statistics, Jeffery Hall, Queen's University, Kingston, Canada, ON K7L 3N6.
Email address: sk206@queensu.ca

Department of Mathematics and Statistics, Jeffery Hall, Queen's University, Kingston, Canada, ON K7L 3N6.
Email address: murty@queensu.ca