Bull. Aust. Math. Soc. **109** (2024), 242–253
doi:10.1017/S0004972723001077

AN EFFECTIVE BOUND FOR GENERALISED DIOPHANTINE m-TUPLES

SAUNAK BHATTACHARJEE, ANUP B. DIXIT and DISHANT SAIKIA

(Received 10 April 2023; accepted 20 August 2023; first published online 6 November 2023)

Abstract

For $k \geq 2$ and a nonzero integer n, a generalised Diophantine m-tuple with property $D_k(n)$ is a set of m positive integers $S = \{a_1, a_2, \ldots, a_m\}$ such that $a_ia_j + n$ is a kth power for $1 \leq i < j \leq m$. Define $M_k(n) := \sup\{|S| : S \text{ having property } D_k(n)\}$. Dixit *et al.* ['Generalised Diophantine m-tuples', *Proc. Amer. Math. Soc.* **150**(4) (2022), 1455–1465] proved that $M_k(n) = O(\log n)$, for a fixed k, as n varies. In this paper, we obtain effective upper bounds on $M_k(n)$. In particular, we show that for $k \geq 2$, $M_k(n) \leq 3\,\phi(k)\log n$ if n is sufficiently large compared to k.

2020 *Mathematics subject classification*: primary 11D45; secondary 11D72, 11N36.

Keywords and phrases: Diophantine m-tuples, Gallagher's sieve, gap principle, quantitative Roth's theorem.

1. Introduction

Given a nonzero 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 $a_ia_j + n$ is a perfect square for $1 \leq i < j \leq m$. 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 generalised by Euler who found an 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, any $D(1)$-triple can be extended to a Diophantine quadruple [1]. In 1969, using Baker's theory of linear forms in the logarithms of algebraic numbers 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 [10], using similar methods, proved that there are no $D(1)$-sextuples and there are only finitely many $D(1)$-quintuples, if any. The nonexistence of $D(1)$-quintuples was finally settled in 2019 by He *et al.* in [15].

In general, there are $D(n)$-quintuples for $n \neq 1$. For example,

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

The research of the second author is partially supported by the Inspire Faculty Fellowship. The research of the first and third authors was supported by a summer research program in IMSc, Chennai.

are Diophantine quintuples satisfying property $D(256)$. There are also examples of $D(n)$-sextuples, but no $D(n)$-septuple is known. So, it is natural to study the size of the largest m-tuple with property $D(n)$. Define

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

In 2004, Dujella [9] 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,

$$M_n \leq 2.6071 \log |n| + O\left(\frac{\log |n|}{(\log \log |n|)^2}\right). \tag{1.1}$$

Our goal is to study this problem when squares are replaced by higher powers.

Definition 1.1 (Generalised Diophantine m-tuples). Fix a natural number $k \geq 2$. A set of natural numbers $S = \{a_1, a_2, \ldots, a_m\}$ satisfies property $D_k(n)$ if $a_i a_j + n$ is a kth power for $1 \leq i < j \leq m$.

For each nonzero integer n, define

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

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

$$y^k = f(x) = (a_1 x + n)(a_2 x + n)(a_3 x + n)(a_4 x + n) \cdots (a_m x + n)$$

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. When $n = 1$, Bugeaud and Dujella [6] showed that

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

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 *et al.* [5] obtained upper bounds for $M_k(n)$. In particular, they showed that for $k \geq 5$,

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

Dixit *et al.* [8] improved these bounds on $M_k(n)$ for large n and a fixed k. Define

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

Then, for $k \geq 3$, as $n \to \infty$,

$$M_k(n, L) \ll_{k,L} 1 \text{ for } L \geq 3 \quad \text{and} \quad M_k(n) \ll_k \log n. \tag{1.2}$$

The purpose of this paper is to make the implied constants in (1.2) explicit. In [8], the bounds for $M_k(n)$ were proved under the further assumption that $n > 0$. As remarked

https://doi.org/10.1017/S0004972723001077 Published online by Cambridge University Press

in [8], this assumption is not necessary, but an argument was not provided. We begin by proving the bounds (1.2) for all nonzero integers n.

THEOREM 1.2. *Let $k \geq 3$ be an integer. Then the following statements hold as $|n| \to \infty$.*

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

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

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

(2) *Moreover,*

$$M_k(n) \ll \log |n|,$$

where the implied constant depends on k.

We next state our main theorem, which is an effective version of Theorem 1.2.

THEOREM 1.3. *Let $k \geq 3$ be a positive integer. Then the following statements hold.*

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

$$M_k(n, L) \leq 2^{28} \log(2k) \log(2 \log(2k)) + 14. \tag{1.3}$$

(b) *Suppose n and k vary such that as $|n| \to \infty$ and $k = o(\log \log |n|)$, then*

$$M_k(n) \leq 3\,\phi(k)\, \log |n| + O\Big(\frac{(\phi(k))^2 \log |n|}{\log \log |n|}\Big),$$

where $\phi(n)$ denotes the Euler totient function.

REMARK 1.4. (a) It is possible to replace 14 on the right-hand side of (1.3) with a smaller positive integer for large values of k.

(b) For a fixed $k > 2$, Theorem 1.3(b) gives

$$M_k(n) \leq 3\,\phi(k)\, \log |n| + O\Big(\frac{\log |n|}{\log \log |n|}\Big) \quad \text{as } |n| \to \infty.$$

For $k = 2$, this upper bound is very close to the best known upper bound due to Becker and Murty which is given by (1.1).

(c) Theorem 1.3 holds in a slightly more general setting for Diophantine tuples with property $D_k(n)$ in the ring of integers of the kth cyclotomic field $\mathbb{Q}(\zeta_k)$. In that case, we replace the Legendre symbol by the power residue symbol and follow the same method as in the proof of Theorem 1.3.

2. Preliminaries

In this section, we develop the necessary tools to prove our main theorems.

2.1. Gallagher's larger 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 and record the result in a form applicable to our context.

https://doi.org/10.1017/S0004972723001077 Published online by Cambridge University Press

THEOREM 2.1. *Let N be a natural number and $\mathcal{S}$ a subset of $\{1, 2, \ldots, N\}$. Let $\mathcal{P}$ be a set of primes. For each prime $p \in \mathcal{P}$, let $\mathcal{S}_p = \mathcal{S} \pmod{p}$. For $1 < Q \le N$,*

$$|\mathcal{S}| \le \frac{\sum_{p \le Q, p \in \mathcal{P}} \log p - \log N}{\sum_{p \le Q, p \in \mathcal{P}} \frac{\log p}{|\mathcal{S}_p|} - \log N},$$

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

2.2. A quantitative Roth's theorem. There are several quantitative results counting exceptions in Roth's celebrated theorem on Diophantine approximations. We will use the following result due to Evertse [11]. 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 $1 \le i \le r$ are the conjugates of ξ (over $\mathbb{Q}$) and a is the positive integer such that

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

has rational integer coefficients with greatest common divisor equal to 1.

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

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

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 [16]).

LEMMA 2.3. *Let $\chi \pmod{q}$ be a nontrivial Dirichlet character and n 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*

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

The original method of Vinogradov gives the bound on the right-hand side of the inequality as $\sqrt{2q|\mathcal{A}||\mathcal{B}|}$. However, the above bound holds and a short proof can be found in [3, Proposition 2.5].

https://doi.org/10.1017/S0004972723001077 Published online by Cambridge University Press

2.4. Bounds for primes in arithmetic progression. Let Q, k, a be positive integers with $(a, k) = 1$. Denote by $\theta(Q; k, a)$ the sum of the logarithms of the primes $p \equiv a \pmod{k}$ with $p \leq Q$, that is,

$$\theta(Q; k, a) := \sum_{\substack{p \equiv a \bmod k \\ p \text{ prime} \leq Q}} \log p.$$

The following bound on $\theta(Q; k, a)$ was obtained by Bennet *et al.* in [4, Theorem 1.2].

THEOREM 2.4. *For $k \geq 3$ and $(a, k) = 1$,*

$$\left|\theta(Q; k, a) - \frac{Q}{\phi(k)}\right| < \frac{1}{160} \frac{Q}{\log Q}$$

for all $Q \geq Q_0(k)$, where

$$Q_0(k) = \begin{cases} 8 \cdot 10^9 & \text{if } 3 \leq k \leq 10^5, \\ \exp(0.03\sqrt{k} \log^3 k) & \text{if } k > 10^5. \end{cases}$$

2.5. Gap principle. The next two lemmas are variations of a gap principle of Gyarmati [14].

LEMMA 2.5 [8, 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 kth powers. Then,

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

An immediate corollary of this lemma shows that 'large' elements of any set with property $D_k(n)$ have 'super-exponential growth'.

COROLLARY 2.6 [8, Corollary 2]. *Let $k \geq 3$ and $m \geq 5$. Suppose that $n^3 \leq a_1 < a_2 < \cdots < a_m$ and the set $\{a_1, a_2, \ldots, a_m\}$ has property $D_k(n)$. Then $a_{2+3j} \geq a_2^{(k-1)^j}$ provided $1 \leq j \leq (m-2)/3$.*

A modification of the proof of Lemma 2.5 yields a gap principle for negative values of n.

LEMMA 2.7. *For $n > 0$ and natural numbers a, b, c, d such that $n^3 \leq a < b < c < d$,*

$$(ac - n)(bd - n) \geq \frac{abcd}{2}.$$

PROOF. Since $(ac - n)(bd - n) = abcd - n(ac + bd) + n^2$, it is enough to prove that

$$\frac{abcd}{2} \geq n(ac + bd) - n^2.$$

https://doi.org/10.1017/S0004972723001077 Published online by Cambridge University Press

Also, since $a \geq n^3$ and $c > n^3$, for all cases other than $n = 1, a = 1, b = 2, c = 3$,

$$\begin{aligned} abcd &\geq 4nbd \\ &\geq 2nbd + 2nac \\ &\geq 2nbd + 2nac - 2n^2, \end{aligned}$$

where the first inequality is obvious as $a \geq n^3$ and $c \geq n^3 + 2$. This gives the desired result. For the case $n = 1, a = 1, b = 2, c = 3$, since $d > c$, clearly

$$2n(ac + bd) - 2n^2 = 4 + 4d < 6d = abcd. \qquad \square$$

We are now ready to prove the following analogue of Lemma 2.5.

LEMMA 2.8. *Let $n > 0$ and $k \geq 2$. Suppose that a, b, c, d are positive integers such that $n^3 \leq a < b < c < d$. Suppose further that $ac - n, bc - n, ad - n, bd - n$ are perfect kth powers. Then,*

$$bd \geq k^k 2^{-k} n^{-k} (ac)^{k-1}.$$

PROOF. Since $(b - a)(d - c) > 0$, we have $bd + ac > ad + bc$ and it is easily seen that

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

As $(ac - n)(bd - n)$ and $(ad - n)(bc - n)$ are both perfect kth powers,

$$\begin{aligned} (ad - n)(bc - n) &\geq [((ac - n)(bd - n))^{1/k} + 1]^k \\ &\geq (ac - n)(bd - n) + k((ac - n)(bd - n))^{k-1/k} \\ &\geq (ac - n)(bd - n) + k\Big(\frac{abcd}{2}\Big)^{k-1/k}, \end{aligned}$$

where the last inequality follows from Lemma 2.7. Thus,

$$-n(ad + bc) \geq -n(ac + bd) + k\Big(\frac{abcd}{2}\Big)^{k-1/k}.$$

Since $bd > ad + bc - ac > 0$, we have $bd + ac - ad - bc < bd$ and hence,

$$nbd > k\Big(\frac{abcd}{2}\Big)^{k-1/k}.$$

Therefore,

$$bd \geq k^k 2^{1-k} n^{-k} (ac)^{k-1} \geq k^k 2^{-k} n^{-k} (ac)^{k-1},$$

which proves the lemma. $\square$

This enables us to prove super-exponential growth for large elements of a set with $D_k(n)$, when $n < 0$.

COROLLARY 2.9. *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 $e \geq b^{k-1}$.*

https://doi.org/10.1017/S0004972723001077 Published online by Cambridge University Press

PROOF. From Lemma 2.8,

$$ce \geq k^k 2^{-k} n^{-k} (bd)^{k-1} \geq k^k 2^{-k} n^{-k} (bc)^{k-1}.$$

Therefore,

$$e \geq b^{k-1} c^{k-2} n^{-k} 2^{-k} \geq b^{k-1} n^{2k-6} 2^{-k} \geq b^{k-1}. \qquad \square$$

Using induction on the previous corollary, we deduce the following corollary.

COROLLARY 2.10. *Let $k \geq 3$ and $m \geq 5$. Suppose that $n^3 \leq a_1 < a_2 < \cdots < a_m$ and the set $\{a_1, a_2, \ldots, a_m\}$ has property $D_k(-n)$. Then we have $a_{2+3j} \geq a_2^{(k-1)^j}$ provided $1 \leq j \leq (m-2)/3$.*

3. Proof of the main theorems

3.1. Proof of Theorem 1.2. We first prove Theorem 1.2. The proof follows a similar method to [8].

Let n be a positive integer, $m = M_k(-n)$ and $S = \{a_1, a_2, a_3, \ldots, a_m\}$ be a generalised m-tuple with the property $D_k(-n)$. Suppose $n^L < a_1 < a_2 < \cdots < a_m$ for some $L \geq 3$. Consider the system of equations

$$\begin{aligned} a_1 x - n &= u^k, \\ a_2 x - n &= v^k. \end{aligned} \tag{3.1}$$

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

$$|a_2 u^k - a_1 v^k| = n(a_2 - a_1).$$

Let $\alpha := (a_1/a_2)^{1/k}$ and $\zeta_k := e^{2\pi i/k}$. Then, we have the following two lemmas analogous to those proved in [8]. The proof of the first lemma is identical to the proof of [8, Lemma 3.1].

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

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

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

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

LEMMA 3.2. *Let (u_i, v_i) denote distinct pairs that satisfy the system of equations (3.1) with $v_{i+1} > v_i$. For $n > 2^{1/(L-1)} c(k)^{-1/(L-1)}$ and $i \geq 14$,*

$$\left|\frac{u}{v} - \alpha\right| < \frac{1}{v_i^{k-1/2}} \quad \textit{and} \quad v_i > a_2^4.$$

https://doi.org/10.1017/S0004972723001077 Published online by Cambridge University Press

PROOF. From Lemma 3.1, $|u_i/v_i - \alpha| < a_2/2v_i^k$. Thus, we need to show $a_2 < 2v_i^{1/2}$ for $i > 14$. Since $v_i^k = a_2a_i - n$, we have $v_i \geq a_i^{1/k}$. By Corollary 2.10, $a_{2+3j} \geq a_2^{(k-1)^j}$, so that $v_{2+3j} \geq a_2^{(k-1)^j/k}$. We choose a positive integer j_0 such that $(k-1)^{j_0} > 4k$. Since $k \geq 3$, we can take $j_0 = 4$. As $2 + 3j_0 = 14$, we have $v_i \geq v_{14} > a_2^4$ for all $i \geq 14$. This completes the proof. □

For larger values of k, the number 14 in the above lemma can be improved to $2 + 3j_0$, where j_0 satisfies the condition $(k-1)^{j_0} > 4k$.

PROOF OF THEOREM 1.2. Now, assume that $(u_1, v_1), (u_2, v_2), \dots, (u_m, v_m)$ satisfy the system of equations (3.1) with

$$v_i > \max(a_2^{1/k}, 2) \geq \max(H(\alpha), 2).$$

By Lemma 3.2, for $14 \leq i \leq m$,

$$\left|\frac{u}{v} - \alpha\right| < \frac{1}{v_i^{k-1/2}} \leq \frac{1}{v_i^{2.5}},$$

as $k \geq 3$. Since $\alpha = (a_1/a_2)^{1/k} < 1$ and $\max(u_i, v_i) = v_i$, from Theorem 2.2, the number of such v_i is $O(\log k \, \log\log k)$. This proves Theorem 1.2. □

3.2. Proof of Theorem 1.3. Let $m = M_k(n)$ and $S = \{a_1, a_2, a_3, \dots, a_m\}$ be a generalised m-tuple with the property $D_k(n)$. Suppose $|n|^L < a_1 < a_2 < \cdots < a_m$ for some $L \geq 3$. We consider the system of equations

$$\begin{aligned} a_1x + n &= u^k, \\ a_2x + n &= v^k. \end{aligned} \tag{3.2}$$

As before, $x = a_i$ for $i \geq 3$ are solutions to this system. The statements of Lemmas 3.1 and 3.2 hold for all nonzero integers n. For $n > 0$, this was proved in [8].

PROOF OF THEOREM 1.3(a). Let $(u_1, v_1), \dots, (u_m, v_m)$ satisfy the system of equations (3.2) with $v_i > \max(a_2^{1/k}, 2) \geq \max(H(\alpha), 2)$. By Lemma 3.2, for $14 \leq i \leq m$,

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

as $k \geq 3$. Since $\alpha = (a_1/a_2)^{1/k} < 1$ and $\max(u_i, v_i) = v_i$, applying Theorem 2.2 with $\kappa = 0.5$ shows that the number of v_i satisfying the above inequality is

$$2^{25}(0.5)^{-3}\log(2k)\log((0.5)^{-1}\log(2k)) = 2^{28}\log(2k)\log(2\log(2k)).$$

So, for $k \geq 3$, the total number of solutions is at most

$$2^{28}\log(2k)\log(2\log(2k)) + 14.$$ □

PROOF OF THEOREM 1.3(b). Let $S = \{a_1, a_2, \dots, a_m\}$ be a generalised Diophantine m-tuple with property $D_k(n)$ such that each $a_i \leq |n|^3$. Since $M_k(n; 3)$ has a finite bound depending on k, it is enough to prove the statement for $|S|$. We shall apply Gallagher's

https://doi.org/10.1017/S0004972723001077 Published online by Cambridge University Press

larger sieve with primes $p \leq Q$ satisfying $p \equiv 1 \pmod{k}$. Let $\mathcal{P}$ be the set of all primes $p \equiv 1 \pmod{k}$. For all such primes $p \in \mathcal{P}$, there exists a Dirichlet character $\chi \pmod{p}$ of order k.

Denote by S_p the image of $S \pmod{p}$ for a given prime p. For $p \in \mathcal{P}$, applying Lemma 2.3 with $\mathcal{A} = \mathcal{B} = S_p$ and $\chi \pmod{p}$ a character of order k,

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

Thus,

$$|S_p| \leq \sqrt{p} + 2.$$

Take $N = |n|^3$. Since $a_i \leq |n|^3$, applying Theorem 2.1 yields

$$|S| \leq \frac{\sum_{p \in \mathcal{P}, p \leq Q} \log p - \log N}{\sum_{p \in \mathcal{P}, p \leq Q} \dfrac{\log p}{|S_p|} - \log N}.$$

By Theorem 2.4,

$$\sum_{\substack{p \leq Q \\ p \equiv 1 \bmod k}} \log p = \frac{Q}{\phi(k)} + O\Big(\frac{Q}{\log Q}\Big),$$

when $Q > Q_0(k)$. As in Section 2.4, $\theta(Q; k, 1) = \sum_{p \leq Q, p \equiv 1 \bmod k} \log p$. We take $f(t) = 1/(\sqrt{t} + 2)$. By partial summation,

$$\sum_{\substack{p \leq Q \\ p \equiv 1 \bmod k}} f(p) \log p = \theta(Q; k, 1) f(Q) - \int_2^Q \theta(t; k, 1) f'(t)\, dt. \tag{3.3}$$

The right-hand side is equal to

$$\frac{Q}{\phi(k)(\sqrt{Q} + 2)} + O\Big(\frac{\sqrt{Q}}{\log Q}\Big) + \frac{1}{\phi(k)}\Big(\int_2^Q \frac{t}{2(\sqrt{t} + 2)^2 \sqrt{t}}\, dt\Big) + O\Big(\int_2^Q \frac{1}{\sqrt{t} \log t}\, dt\Big).$$

The three terms above can be estimated as

$$\begin{aligned} \frac{Q}{\phi(k)(\sqrt{Q} + 2)} &= \frac{\sqrt{Q}}{\phi(k)} + O(1), \\ \frac{1}{\phi(k)}\Big(\int_2^Q \frac{t}{2(\sqrt{t} + 2)^2 \sqrt{t}}\, dt\Big) &= \frac{\sqrt{Q}}{\phi(k)} + O(\log Q), \\ O\Big(\int_2^Q \frac{1}{\sqrt{t} \log t}\, dt\Big) &= O\Big(\frac{\sqrt{Q}}{\log Q}\Big). \end{aligned}$$

https://doi.org/10.1017/S0004972723001077 Published online by Cambridge University Press

Putting this together in (3.3) yields

$$\sum_{\substack{p\le Q\\ p\equiv 1 \bmod k}} \frac{\log p}{\sqrt{p}+2} = \frac{2\sqrt{Q}}{\phi(k)} + O\Big(\frac{\sqrt{Q}}{\log Q}\Big).$$

Thus,

$$|S| \le \frac{\dfrac{Q}{\phi(k)} + O\Big(\dfrac{Q}{\log Q}\Big) - \log N}{\dfrac{2\sqrt{Q}}{\phi(k)} + O\Big(\dfrac{\sqrt{Q}}{\log Q}\Big) - \log N}.$$

Choose $Q = (\phi(k)\log N)^2$. Note that the condition $Q > Q_0(k)$ is the same as

$$\log N > \frac{\exp(0.015\sqrt{k}(\log k)^3)}{\phi(k)}. \tag{3.4}$$

Since $k = o(\log\log|n|)$, (3.4) holds for N large enough. Now, for both the numerator and the denominator, divide by $\log N$ to get

$$|S| \le \frac{\phi(k)\log N - 1 + O\Big(\dfrac{Q}{\log N \log Q}\Big)}{1 + O\Big(\dfrac{\sqrt{Q}}{\log N\log Q}\Big)}. \tag{3.5}$$

Because $k = o(\log\log N)$, it is easy to see that

$$\frac{\sqrt{Q}}{\log N\log Q} = \frac{\phi(k)}{2\log\phi(k) + 2\log\log N} = o(1).$$

Hence, from (3.5),

$$|S| \le \frac{\phi(k)\log N + O\Big(\dfrac{(\phi(k))^2\log N}{\log\log N}\Big)}{1 + O\Big(\dfrac{\phi(k)}{\log\log N}\Big)}.$$

As $O(\phi(k)/\log\log N) = o(1)$, it follows that

$$\frac{1}{1 + O\Big(\dfrac{\phi(k)}{\log\log N}\Big)} = 1 + O\Big(\frac{\phi(k)}{\log\log N}\Big).$$

So, we obtain

$$|S| \le \phi(k)\log N + O\Big(\frac{(\phi(k))^2\log N}{\log\log N}\Big).$$

https://doi.org/10.1017/S0004972723001077 Published online by Cambridge University Press

Since $N = |n|^3$ and $M_k(n) := \sup\{|S|\}$, we conclude that

$$M_k(n) \leq 3\,\phi(k)\,\log|n| + O\Big(\frac{(\phi(k))^2\log|n|}{\log\log|n|}\Big)$$

as required. □

Acknowledgements

We thank Professor Alain Togbé for his question regarding effective versions of the bounds in [8] during the second author's talk in the Leuca 2022 conference, which motivated this paper. We are grateful to Professor Ram Murty and Dr. Seoyoung Kim for helpful comments on an earlier version of this paper. We also thank the referee for detailed and helpful comments on the paper.

References

[1] J. Arkin, V. E. Hoggatt Jr and E. G. Straus, 'On Euler's solution of a problem of Diophantus', *Fibonacci Quart.* **17**(4) (1979), 333–339.
[2] A. Baker and 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 and M. R. Murty, 'Diophantine m-tuples with the property $D(n)$', *Glas. Mat. Ser. III* **54** (2019), 65–75.
[4] M. A. Bennett, G. Martin, K. O'Bryant and A. Rechnitzer, 'Explicit bounds for primes in arithmetic progressions', *Illinois J. Math.* **62**(1–4) (2018), 427–532.
[5] 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**(3–4) (2011), 325–339.
[6] Y. Bugeaud and A. Dujella, 'On a problem of Diophantus for higher powers', *Math. Proc. Cambridge Philos. Soc.* **135** (2003), 1–10.
[7] A. Cojocaru and M. R. Murty, *An Introduction to Sieve Methods and Their Applications*, London Mathematical Society Student Texts, 66 (Cambridge University Press, Cambridge, 2005).
[8] A. B. Dixit, S. Kim and M. R. Murty, 'Generalised Diophantine m-tuples', *Proc. Amer. Math. Soc.* **150**(4) (2022), 1455–1465.
[9] A. Dujella, 'Bounds for the size of sets with the property $D(n)$', *Glas. Mat. Ser. III* **39**(2) (2004), 199–205.
[10] A. Dujella, 'There are only finitely many Diophantine quintuples', *J. reine angew. Math.* **566** (2004), 183–214.
[11] J.-H. Evertse, 'On the quantitative subspace theorem', *J. Math. Sci. (N.Y.)* **171**(6) (2010), 824–837.
[12] G. Faltings, 'Endlichkeitssätze für abelsche Varietäten über Zählkorpern', *Invent. Math.* **73** (1983), 349–366. Erratum: ibid., **75** (1984), 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] B. He, A. Togbé and V. Ziegler, 'There is no Diophantine quintuple', *Trans. Amer. Math. Soc.* **371**(9) (2019), 6665–6709.
[16] I. M. Vinogradov, *Elements of Number Theory* (Dover Publications, Inc., New York, 1954), translated by S. Kravetz.

SAUNAK BHATTACHARJEE, IISER Tirupati,
C/O Sree Rama Engineering College, (Transit Campus),
Tirupati, Andhra Pradesh 517507, India
e-mail: saunakbhattacharjee@students.iisertirupati.ac.in

ANUP B. DIXIT, Institute of Mathematical Sciences (HBNI),
CIT Campus, Taramani, Chennai, Tamil Nadu 600113, India
e-mail: anupdixit@imsc.res.in

DISHANT SAIKIA, Freie Universität Berlin,
Kaiserswerther Str. 16-18, Berlin 14195, Germany
e-mail: saikiadishant@gmail.com

https://doi.org/10.1017/S0004972723001077 Published online by Cambridge University Press