Publ. Math. Debrecen
Manuscript (July 23, 2011)

On the size of sets whose elements have perfect power n-shifted products

By Attila Bérczes, Andrej Dujella, Lajos Hajdu and Florian Luca

Dedicated to Professors K. Győry and A. Sárközy on their 70th birthdays and Professors A. Pethő and J. Pintz on their 60th birthdays

Abstract. We show that the size of sets $\mathcal{A}$ having the property that with some non-zero integer n, $a_1a_2 + n$ is a perfect power for any distinct $a_1, a_2 \in \mathcal{A}$, cannot be bounded by an absolute constant. We give a much more precise statement as well, showing that such a set $\mathcal{A}$ can be relatively large. We further prove that under the *abc*-conjecture a bound for the size of $\mathcal{A}$ depending on n can already be given. Extending a result of Bugeaud and Dujella, we also derive an explicit upper bound for the size of $\mathcal{A}$ when the shifted products $a_1a_2 + n$ are k-th powers with some fixed $k \geq 2$. The latter result plays an important role in some of our proofs, too.

1. Introduction

A set $\mathcal{A} = \{a_1, \ldots, a_m\}$ of positive integers is called a Diophantine m-tuple, if for any $1 \leq i < j \leq m$ we have $a_ia_j + 1 = x_{ij}^2$ for an integer x_{ij}. The

Mathematics Subject Classification: 11B75, 11D99.
Key words and phrases: shifted product, perfect power, *abc*-conjecture, Diophantine m-tuple.
The first three authors are supported by the Hungarian-Croatian bilateral project *Number theory and cryptography*. The first and third authors are supported in part by the OTKA grants K67580 and K75566, and by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, cofinanced by the European Social Fund and the European Regional Development Fund. The second author is supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 037-0372781-2821. The fourth author was supported in part by Grants SEP-CONACyT 79685 and PAPIIT 100508.

history and theory of Diophantine m-tuples is very rich. Diophantus found the set $\{1/16, 33/16, 17/4, 105/16\}$ of four positive rationals with the above property. However, the first Diophantine quadruple, $\{1, 3, 8, 120\}$, was found by Fermat (see [5]). A folklore conjecture is that there does not exist a Diophantine quintuple. The first important result concerning this conjecture was proved in 1969 by Baker and Davenport [1]. They proved that if d is a positive integer such that $\{1, 3, 8, d\}$ forms a Diophantine quadruple, then $d = 120$. Hence, the triple $\{1, 3, 8\}$ cannot be extended to a Diophantine quintuple. In 1998, Dujella and Pethő [13] proved that the pair $\{1, 3\}$ cannot be extended to a Diophantine quintuple. In 2004, Dujella [8] proved that there does not exist a Diophantine sextuple and there are only finitely many Diophantine quintuples (recently Fujita [15] showed that there are at most 10^{276} Diophantine quintuples). An overview of classical and recent results and the complete list of references on Diophantine m-tuples can be found on web page [10]. As a generalization of Diophantine m-tuples one can consider sets $\mathcal{A}$ of positive integers such that for any $a, b \in \mathcal{A}$ with $a \neq b$ we have $ab + n = x_{ab}^2$, where n is a fixed non-zero integer. Such sets are referred to as $D(n)$-m-tuples. E.g. the set $\{99, 315, 9920, 32768, 44460, 19534284\}$, found by Gibbs [17] is a $D(2985984)$-sextuple. Define

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

It is easy to prove that $M_n = 3$ for $n \equiv 2 \pmod 4$ (see e.g. [2]). By the Lang conjecture on varieties of general type, we expect that there exists an absolute constant C such that $M_n < C$ for all non-zero integers n. However, the best known general result of this shape is $M_n \leq 31$ for $|n| \leq 400$, $M_n < 15.476 \log |n|$ for $|n| > 400$ (see [7, 9]). Furthermore, Dujella and Luca [12] proved that $M_p < 3 \cdot 2^{168}$ holds for all primes p. It is known that $4 \leq M_1 \leq 5$ [8], $4 \leq M_4 \leq 5$ [16] and $3 \leq M_{-1} \leq 4$ [11].

As an alternative, but also natural generalization of Diophantine m-tuples, Bugeaud and Dujella [3] considered sets $\mathcal{A}$ of positive integers with the property that $ab + 1 = x_{ab}^k$ whenever a, b are distinct elements of $\mathcal{A}$ and k is an integer with $k \geq 2$. Such sets are called k-th power Diophantine tuples. Examples of such triples for $k = 3$ and $k = 4$ are given, respectively, by $\{2, 171, 25326\}$ and $\{1352, 8539880, 9768370\}$. Let

$$E_k = \sup\{|\mathcal{A}| : \mathcal{A} \text{ is a } k\text{-th power Diophantine tuple}\}.$$

In [3, Corollary 4] absolute upper bounds for the numbers E_k, $k \geq 3$ were obtained. More precisely, it was proved that $E_3 \leq 7$, $E_4 \leq 5$, $E_5 \leq 5$, $E_k \leq 4$ for $6 \leq k \leq 176$, and $E_k \leq 3$ for $k \geq 177$.

As a further generalization, in this paper we consider sets $\mathcal{A}$ of positive integers such that for any distinct elements a, b of $\mathcal{A}$, $ab + n$ is a perfect power, where n is some fixed non-zero integer. That is, writing $\mathcal{A} = \{a_1, a_2, \dots\}$ we have

$$a_i a_j + n = x_{ij}^{k_{ij}} \tag{1}$$

for some integers x_{ij} and k_{ij} with $k_{ij} \geq 2$, and here the exponents k_{ij} can of course be different. The case $n = 1$ of this problem has already been studied by several authors, see e.g. [19], [20], [4], [6], [22], [21]. The main direction of research concerns finding an upper bound for the size of sets $\mathcal{A} \subseteq \{1, 2, \dots, N\}$ such that $ab + 1$ is a perfect power for all $a \neq b$ in $\mathcal{A}$. The best known result of that type is due to Stewart [24], who proved that $|\mathcal{A}| \ll (\log N)^{2/3}(\log\log N)^{1/3}$. Further, Luca [22] proved that if $\mathcal{A}$ satisfies (1) with $n = 1$, then assuming the *abc*-conjecture the number of elements $|\mathcal{A}|$ of $\mathcal{A}$ can be bounded by an absolute constant.

We show that this is not true in case of arbitrary n (Theorem 1). We also give a much more precise statement (Theorem 2), which shows that such sets can be relatively large. Further, we prove that assuming the *abc*-conjecture we already have $|\mathcal{A}| < C(n)$, where $C(n)$ is a constant depending only on n. In view of our construction in the proof of Theorem 2, the dependence of $C(n)$ on n is necessary. To prove this result we extend a theorem of Bugeaud and Dujella [3] concerning shifted products which are k-th powers (Theorem 3). Assuming the *abc*-conjecture we obtain a bound in terms of n for all but one a_i, provided that the exponents k_{ij} in $a_i a_j + n = x_{ij}^{k_{ij}}$ are sufficiently large (Lemma 1). Then following the approach of Luca [22], we use Ramsey theory to prove the bound $|\mathcal{A}| < C(n)$ (Theorem 4). Finally, we note that our Theorems 3 and 4 are formulated for the more general case $\mathcal{A} \subseteq \mathbb{Z}$. Though this formulation qualitatively has no advantage (since one can bound the positive and negative parts of $\mathcal{A}$ separately and then just combine the bounds), quantitatively the statements are still more general in this way.

2. Main results

Our first theorem shows that the size of sets with the property (1) cannot be bounded by an absolute constant.

Theorem 1. *For any $K \in \mathbb{N}$ there exists an $n \in \mathbb{N}$ and a set $\mathcal{A} \subseteq \mathbb{N}$ such that $|\mathcal{A}| \geq K$ and $ab + n$ is a perfect power for any distinct $a, b \in \mathcal{A}$.*

As one can easily see, Theorem 1 is a simple and immediate consequence of the following, much more precise statement.

Theorem 2. *Let $x \geq e^{e^e}$, and take*

$$K := \left\lfloor \left(\frac{\log\log x}{2\log\log\log x} \right)^{1/3} \right\rfloor. \tag{2}$$

Then there exists a set $\mathcal{A}_K = \{a_1, \ldots, a_K\}$ with elements all in $[1, x]$, as well as an integer n_K also in $[1, x]$, such that $a_i a_j + n_K = x_{ij}^{k_{ij}}$ for $1 \leq i < j \leq K$ with some integers x_{ij}, where the exponents k_{ij} are the first $\binom{K}{2}$ primes.

Remark 1. The condition $x \geq e^{e^e} = 3814279.105\ldots$ is meant to insure that $\log\log\log x > 1$. If $x > e^{e^{68}}$, then the above number K is ≥ 2. For smaller values of x the statement is empty. However, obviously, $K \to \infty$ as $x \to \infty$.

Remark 2. Let $f(x)$ be the maximum K such that there exists $\mathcal{A}_K \subseteq [1, x] \cap \mathbb{N}$ with K elements and some $n \leq x$ such that $aa' + n$ is a perfect power for all $a \neq a'$ in $\mathcal{A}_K$. A natural question is to find sharp upper and lower bounds on $f(x)$. It is clear that $f(x)$ is at least as large as the bound shown at (2) and it is easy to see that $f(x) \leq x^{2/3+o(1)}$ as $x \to \infty$. Indeed, let $\mathcal{A}_K$ be a maximal example (with $K = f(x)$). Let $\mathcal{A}_1 = \{a \in \mathcal{A}_K : aa' + n \text{ is a square for all } a' \in \mathcal{A}_K \backslash \{a\}\}$. It is clear that elements in $\mathcal{A}_1$ participate in every maximal $D(n)$-tuple in $\mathcal{A}_K$, so the cardinality of $\mathcal{A}_1$ is $O(\log |n|) = O(\log x)$ (see [7, 9]). On the other hand, for each $a \in \mathcal{A}_K \backslash \mathcal{A}_1$ there is an a' in $\mathcal{A}_K$ such that $aa' + n$ is a perfect power u^k of exponent $k \geq 3$. Since $aa' + n = u^k \leq 2x^2$, the number of such perfect powers is $O(x^{2/3})$. Given one such perfect power u^k, a is a divisor of $u^k - n$, a positive integer $\leq x^2$, so which has at most $x^{o(1)}$ divisors as $x \to \infty$. This indeed shows that $f(x) \leq x^{2/3+o(1)}$ as $x \to \infty$, which is a nontrivial upper bound. To derive sharp upper and lower bounds for $f(x)$ we leave as an open problem.

The next result is an extension of a theorem of Bugeaud and Dujella [3].

Theorem 3. *Let k and n be integers with $k \geq 2$ and $n \neq 0$, and let $\mathcal{A} \subseteq \mathbb{Z}$ such that $ab + n$ is a k-th power for all distinct $a, b \in \mathcal{A}$. Then we have $|\mathcal{A}| \leq C_1(k, n)$, where $C_1(k, n)$ is a constant depending only on k and n. In particular, if $k = 2$ (or more generally, if k is even), we may take $C_1(k, n) = 31 + 15.476 \log |n|$, if $k = 3$, we may take $C_1(k, n) = 2|n|^{17} + 6$, while for $k \geq 5$ we may take $C_1(k, n) = 2|n|^5 + 3$.*

Corollary 1. *Let k and n be integers with $k \geq 2$ and $n \neq 0$, and let $\mathcal{A} \subseteq \mathbb{Z}$ such that $ab+n$ is a k-th power for all distinct $a, b \in \mathcal{A}$. Then we have $|\mathcal{A}| \leq C_2(n)$, where $C_2(n)$ is a constant depending only on n. We may take $C_2(n) = 2|n|^{17}+31$.*

Our next result proves that assuming the *abc*-conjecture, the size of the sets $\mathcal{A}$ considered in Theorem 1, i.e. with the property that the products of distinct elements of $\mathcal{A}$ shifted by some fixed nonzero integer n are perfect powers, can already be bounded in terms of n.

Theorem 4. *Let n be a non-zero integer, and suppose that the abc-conjecture is valid. Then there exists a constant $C_3(n)$ depending only on n with the following property. If $\mathcal{A} \subseteq \mathbb{Z}$ such that $ab+n$ is a perfect power for any distinct $a, b \in \mathcal{A}$, then $|\mathcal{A}| < C_3(n)$ holds.*

Remark 3. The above theorem extends Theorem 1.4 of Luca [22], where the case $n = 1$ is handled.

Remark 4. In view of the set $\mathcal{A} = \{2^\alpha \ : \ \alpha \geq 1\}$ it is necessary to assume that $n \neq 0$ in Theorem 4.

3. Lemmas and auxiliary results

We shall need the *abc*-conjecture. We use the same version of the conjecture as in [22]. For any positive integer t write $N(t)$ for the radical of t, i.e. $N(t) = \prod_{p|t} p$.

The *abc*-conjecture. Let $\varepsilon > 0$ and a, b, c be non-zero integers with $\gcd(a, b, c) = 1$ and $a + b = c$. Then

$$\max\{|a|, |b|, |c|\} \ll N(abc)^{1+\varepsilon}$$

where the implied constant depends only on ε.

The next lemma plays an important part in the proof of Theorem 4. It is in fact a simple extension of results of Luca [22] to the case where we shift our products by n, rather than just by 1.

Lemma 1. *Suppose that the set $\mathcal{A} = \{a_1, a_2, a_3, a_4, a_5\}$ has the following properties*

(1) *The elements of $\mathcal{A}$ are distinct non-zero integers with $|a_1| \leq |a_2| \leq |a_3| \leq |a_4| \leq |a_5|$,*
(2) *$a_i a_j + n = x_{ij}^{k_{ij}}$ with $k_{ij} \geq 3205$ for $1 \leq i < j \leq 5$.*

If the abc-conjecture holds, then we have

$$|a_2| \leq c_0 |n|^3,$$

where c_0 is an absolute constant.

Proof. In the proof below, the Vinogradov symbol always implies a constant depending only on ε. Since at the appropriate point of the proof we choose a concrete value for ε, in fact Vinogradov symbols imply an absolute constant. We shall follow the method in [22].

First put $u := x_{15}$, $v := x_{25}$, $k := k_{15}$ and $l := k_{25}$, and consider the identities

$$a_1a_5 + n = u^k, \quad a_2a_5 + n = v^l.$$

By eliminating the first terms of the above identities we get the equality

$$a_2u^k - a_1v^l = n(a_2 - a_1).$$

Putting $d := \gcd(a_2u^k, a_1v^l)$ we get

$$\frac{a_2u^k}{d} - \frac{a_1v^l}{d} = \frac{n(a_2 - a_1)}{d}. \tag{3}$$

By applying the *abc*-conjecture to equation (3) we obtain

$$\left|\frac{a_2u^k}{d}\right| \ll N(a_1a_2u^kv^l(a_2 - a_1)n)^{1+\varepsilon} \ll (2|a_2|^3 \cdot |n| \cdot |u| \cdot |v|)^{1+\varepsilon}. \tag{4}$$

However,

$$|u| \le (2|na_1a_5|)^{\frac{1}{k}}, \quad |v| \le (2|na_2a_5|)^{\frac{1}{l}}. \tag{5}$$

Thus combining (4), (5) and $|a_1| \le |a_2|$ we get

$$\left|\frac{a_2u^k}{d}\right| \ll \left((2|n|)^{1+\frac{1}{k}+\frac{1}{l}} \cdot |a_2|^{3+\frac{1}{k}+\frac{1}{l}} \cdot |a_5|^{\frac{1}{k}+\frac{1}{l}}\right)^{1+\varepsilon}. \tag{6}$$

Choosing $\varepsilon := 0.1$, by $k, l > 11$ we infer

$$\left(\frac{1}{k} + \frac{1}{l}\right) \cdot (1+\varepsilon) \le \frac{1}{5}, \quad \left(3 + \frac{1}{k} + \frac{1}{l}\right) \cdot (1+\varepsilon) \le 4. \tag{7}$$

Moreover, since $d \mid (a_2 - a_1)n$, we get $d \le 2|na_2|$. Hence, using

$$|a_5| \le |a_1a_5| = |u^k - n| \le 2|nu^k|$$

together with (6) and (7), we deduce

$$|a_5| \le 2|nu^k| = \left|\frac{a_2u^k}{d}\right| \cdot \left|\frac{2nd}{a_2}\right| \le \left|\frac{a_2u^k}{d}\right| \cdot 4n^2 \ll |na_2|^4 \cdot |a_5|^{1/5}.$$

This yields

$$|a_5|^{4/5} \ll |na_2|^4,$$

and we conclude

$$|a_5| \ll |na_2|^5. \tag{8}$$

In the sequel we consider the elements $0 < |a_1| \leq |a_2| \leq |a_3| \leq |a_4|$ and we use the following notations: $x_1 := x_{12}, x_2 := x_{23}, x_3 := x_{34}, x_4 := x_{41}$ and $k_1 := k_{12}, k_2 := k_{23}, k_3 := k_{34}, k_4 := k_{41}$. Further, suppose that $k > k_0$, where k_0 will be specified later. With these notations we have

$$\begin{aligned} a_1a_2 &= x_1^{k_1} - n, & a_3a_4 &= x_3^{k_3} - n, \\ a_2a_3 &= x_2^{k_2} - n, & a_4a_1 &= x_4^{k_4} - n. \end{aligned} \tag{9}$$

By (9) we clearly have

$$(x_1^{k_1} - n)(x_3^{k_3} - n) - (x_2^{k_2} - n)(x_4^{k_4} - n) = 0,$$

which yields

$$x_1^{k_1}x_3^{k_3} - x_2^{k_2}x_4^{k_4} = n(x_1^{k_1} + x_3^{k_3} - x_2^{k_2} - x_4^{k_4}). \tag{10}$$

In (10) neither the left nor the right hand side can be zero. Indeed, $x_1^{k_1} + x_3^{k_3} - x_2^{k_2} - x_4^{k_4} = 0$ would lead to $a_1a_2 + n + a_3a_4 + n - a_2a_3 - n - a_4a_1 - n = 0$, and this would mean $(a_1 - a_3)(a_2 - a_4) = 0$, which cannot happen since $\mathcal{A}$ contains distinct elements.

Put $D := \gcd(x_1^{k_1}x_3^{k_3}, x_2^{k_2}x_4^{k_4})$. Then by (10) we have

$$\frac{x_1^{k_1}x_3^{k_3}}{D} - \frac{x_2^{k_2}x_4^{k_4}}{D} = \frac{n(x_1^{k_1} + x_3^{k_3} - x_2^{k_2} - x_4^{k_4})}{D}. \tag{11}$$

Here we use again the *abc*-conjecture to infer

$$\left|\frac{x_1^{k_1}x_3^{k_3}}{D}\right| \ll \left|x_1x_2x_3x_4\frac{n(x_1^{k_1} + x_3^{k_3} - x_2^{k_2} - x_4^{k_4})}{D}\right|^{1+\varepsilon}. \tag{12}$$

For $i = 1, 2, 4$ with the appropriate j we clearly have

$$|x_i^{k_i}| = |a_ia_j + n| \leq 2|n| \cdot |a_ia_j| \leq 2|n| \cdot |a_3a_4| = 2|n| \cdot |x_3^{k_3} - n| \leq 4n^2|x_3|^{k_3}.$$

This together with (12) proves that

$$|x_1^{k_1}x_3^{k_3}| \ll \left|n^3x_1x_2x_3x_4x_3^{k_3}\right|^{1+\varepsilon}. \tag{13}$$

Similarly to (5), using (9) we get the estimates

$$\begin{aligned} |x_1| &\le (2|na_1a_2|)^{1/k_1} \qquad & |x_3| &\le (2|na_3a_4|)^{1/k_3} \\ |x_2| &\le (2|na_2a_3|)^{1/k_2} \qquad & |x_4| &\le (2|na_4a_1|)^{1/k_4} \end{aligned} \tag{14}$$

and combining these with (13) we have

$$|x_1^{k_1}x_3^{k_3}| \ll \left|n^3(na_1a_2)^{\frac{1}{k_1}}(na_2a_3)^{\frac{1}{k_2}}(na_3a_4)^{\frac{1}{k_3}}(na_4a_1)^{\frac{1}{k_4}}\right|^{1+\varepsilon}|x_3|^{k_3(1+\varepsilon)}. \tag{15}$$

Using that $k_i > k_0$ and $|a_1| \le |a_2| \le |a_3| \le |a_4|$, (13) leads to the estimate

$$|x_1^{k_1}| \ll \left(|n|^{3+4/k_0}|a_4|^{8/k_0}\right)^{1+\varepsilon}|x_3|^{k_3\varepsilon}. \tag{16}$$

Now using again (14) for $|x_3|$, we have

$$\begin{aligned} |a_1|^2 \le |a_1a_2| \le 2|n||x_1|^{k_1} &\ll |n|\left(|n|^{3+4/k_0}|a_4|^{8/k_0}\right)^{1+\varepsilon}|x_3|^{k_3\varepsilon} \\ &\ll |n|^{1+(3+\frac{4}{k_0})(1+\varepsilon)}|a_4|^{\frac{8}{k_0}(1+\varepsilon)}(|na_3a_4|)^{\varepsilon}. \end{aligned}$$

This yields

$$|a_1|^2 \ll |n|^{(4+\frac{4}{k_0})(1+\varepsilon)} \cdot |a_4|^{\frac{8}{k_0}+(2+\frac{8}{k_0})\varepsilon}. \tag{17}$$

Now choose $\varepsilon = \frac{1}{1000}$ and $k_0 := 2000$, so that $\frac{8}{k_0} + \left(2+\frac{8}{k_0}\right)\varepsilon < \frac{1}{100}$. Thus we get

$$|a_1|^2 \ll |n|^5 \cdot |a_4|^{\frac{1}{100}}, \tag{18}$$

i.e.

$$|a_1|^{200} \ll |n|^{500} \cdot |a_4|. \tag{19}$$

Since $0 < |a_1| \le |a_2| \le |a_3| \le |a_4| \le |a_5|$ we also have

$$|a_2|^{200} \ll |n|^{500} \cdot |a_5|. \tag{20}$$

Now (20) and (8) together show that

$$|a_2|^{200} \ll |n|^{500} \cdot |a_5| \ll |n|^{505}|a_2^5|,$$

which proves the estimate

$$|a_2| \ll |n|^3.$$

□

4. Proof of Theorem 2

Proof of Theorem 2. We construct inductively for every $K \geq 2$ a set $\mathcal{A}_K = \{a_1, \ldots, a_K\}$ with $a_1 < \cdots < a_K$ and a positive integer n_K such that

$$a_i a_j + n_K = x_{ij}^{k_{ij}}$$

for $1 \leq i < j \leq K$, where the exponents k_{ij} are the first $t(K) := \binom{K}{2}$ primes. When $K = 2$, we take $\mathcal{A}_2 = \{1, 3\}$ and $n_2 = 1$. Let $T_K = \max\{n_K, a_K^2\}$, and choose an integer a_{K+1} with $\sqrt{2T_K} > a_{K+1} > \sqrt{T_K}$. Observe that $a_{K+1} > a_K$. Let

$$m_K := \prod_{i=1}^{K} (a_i a_{K+1} + n_K).$$

Clearly,

$$m_K < ((\sqrt{2} + 1)T_K)^K < T_K^{2K}.$$

Let $\mathcal{P}_K$ be the set of prime factors of m_K. Let p_i be the ith prime. For a positive integer m and a prime q we write $\nu_q(m)$ for the exponent of q in the factorization of m. For each prime $p \in \mathcal{P}_K$, consider the following system of congruences

$$\begin{cases} \alpha_p \equiv 0 \pmod{p_i} & \text{for} \quad 1 \leq i \leq t(K), \\ \alpha_p \equiv -\nu_p(a_j a_{K+1} + n_K) \pmod{p_{t(K)+j}} & \text{for} \quad 1 \leq j \leq K. \end{cases} \tag{21}$$

Let α_p be the first positive integer in the above progression. Clearly,

$$\alpha_p \leq \prod_{i \leq t(K+1)} p_i < 4^{p_{t(K+1)}} < 4^{2K(K+1)\log K} < e^{3(K+1)^2 \log(K+1)}.$$

In the above inequalities, we used the Erdős lemma, i.e. the fact that $\prod_{p \leq x} p < 4^x$ holds for all $x \geq 1$, as well as the inequality $p_n < 2n \log n$ holding for all positive integers $n \geq 3$ (see estimate (3.13) in [23]), which we may apply with $n = t(K+1)$ since $t(K+1) \geq t(3) = 3$ for $K \geq 2$.

Put $\beta_p := \alpha_p/2$. Since α_p is even by the first of the above congruences (21), β_p is an integer. Put

$$u_K := \prod_{p \in \mathcal{P}_K} p^{\beta_p}.$$

A simple calculation gives

$$u_K < m_K^{\max\{\alpha_p : p \in \mathcal{P}_K\}} < T_K^{e^{4(K+1)^2 \log(K+1)}}. \tag{22}$$

Put $n_{K+1} := u_K^2 n_K$, and observe that $n_{K+1} \leq u_K^2 T_K$. Set $a_i^* := u_K a_i$ for $i = 1, \dots, K+1$. Then we obviously have $a_1^* < \dots < a_{K+1}^*$, and by the choice of a_{K+1}, also $(a_{K+1}^*)^2 < 2u_K^2 T_K$. Further, by the construction of our numbers, one can easily check that $a_i^* a_j^* + n_{K+1} = u_K^2(a_i a_j + n_K)$ is a perfect power of exponent k_{ij} for all $1 \leq i < j \leq K+1$, and moreover the exponents k_{ij} can be chosen to be exactly the $t(K+1)$ primes $p_1, \dots, p_{t(K+1)}$.

Let $T_{K+1} = \max\{n_{K+1}, (a_{K+1}^*)^2\}$. Then combining the above upper bounds for n_{K+1} and $(a_{K+1}^*)^2$ with (22), we obtain

$$T_{K+1} < 2u_K^2 T_K < T_K^{2+2e^{4(K+1)^2 \log(K+1)}} < T_K^{e^{5(K+1)^2 \log(K+1)}}$$

for all $K \geq 2$. Hence by induction, using that $T_2 = 9$, by a simple calculation we get that $T_K < e^{e^{6K^3 \log K}}$ holds for all $K \geq 2$. Now we would like to choose a positive integer x such that $\mathcal{A}_K$ and n_K are all contained in $[1, x]$. Then it suffices that

$$e^{e^{6K^3 \log K}} \leq x,$$

giving $6K^3 \log K \leq \log\log x$. This yields $K^3 \log(K^3) \leq (\log\log x)/2$. This is fulfilled with

$$K := \left\lfloor \left(\frac{\log\log x}{2 \log\log\log x} \right)^{1/3} \right\rfloor,$$

and the statement follows. □

5. Proofs of Theorems 3 and 4

In the proof of Theorem 3 we follow [3]. In particular, we use the following result of Evertse [14, Theorem 2.1].

Lemma 2. *If a, b and k are positive integers with $k \geq 3$ and c is a positive real number, then there is at most one positive integral solution (x, y) to the inequality*

$$|ax^k - by^k| \leq c$$

with $\gcd(x, y) = 1$ *and*

$$\max\{|ax^k|, |by^k|\} > \beta_k c^{\alpha_k},$$

where α_k and β_k are effectively computable positive constants satisfying

$$\alpha_3 = 9, \quad \alpha_k = \max\left\{ \frac{3k-2}{2(k-3)}, \frac{2(k-1)}{k-2} \right\} \qquad \text{for } k \geq 4$$

and

$$\beta_3 = 1152.2, \quad \beta_4 = 98.53, \quad \beta_k < k^2 \qquad \text{for } k \geq 5.$$

Note that in [3], in the application of Lemma 2, the condition $\gcd(x, y) = 1$ was omitted. However, all corresponding inequalities from the proofs in [3] hold with safe margins, except for $k = 4, 5$, so that this omission has not significant influence to validity of the final results. In particular, in the result from [3, Corollary 4] cited in the introduction, only $E_5 \leq 4$ should be replaced by $E_5 \leq 5$.

Proof of Theorem 3. By the results from [7, 9] cited in the introduction, we may assume that k is odd and $k \geq 3$.

Consider first the case $k \geq 5$. Let $\{a_1, a_2, \dots, a_m\}$ be a kth-power $D(n)$-m-tuple, and $0 < a_1 < a_2 < \cdots < a_m$. For $i \geq 3$ we have

$$a_1 a_i + n = x_i^k, \quad a_2 a_i + n = y_i^k,$$

i.e.

$$a_2 x_i^k - a_1 y_i^k = n(a_2 - a_1). \tag{23}$$

Let $d_i = \gcd(x_i, y_i)$ and write $x_i = d_i x_i'$. Note that $d_i^k \leq |n|(a_2 - a_1)$. We apply Lemma 2 to the Thue inequality

$$|a_2 x^k - a_1 y^k| \leq |n|(a_2 - a_1). \tag{24}$$

By Lemma 2, there is only one very large primitive solution to (24). It may correspond to a_m, but certainly not to a_i for $i < m$. Thus we have

$$a_1 a_{m-1} < 2|n| x_{m-1}^k = 2|n| x_{m-1}'^k d_{m-1}^k \leq 2n^2 a_2 x_{m-1}'^k < 2n^2 \cdot k^2 \cdot (|n| a_2)^{13/4},$$

i.e.

$$a_{m-1} < 2k^2 |n|^{21/4} a_2^{13/4}. \tag{25}$$

Assume now that at least four a_i's are larger than $2|n|^5$, i.e. $a_{m-3} > 2|n|^5$. In order to obtain a lower bound for a_{m-1}, we first consider the case $n > 0$. Then we have

$$(a_1 a_{m-2} + n)(a_2 a_{m-1} + n) > (a_2 a_{m-2} + n)(a_1 a_{m-1} + n),$$

which implies

$$(a_1 a_{m-2} + n)(a_2 a_{m-1} + n) \geq (((a_2 a_{m-2} + n)(a_1 a_{m-1} + n))^{1/k} + 1)^k,$$

$$na_2a_{m-1} \geq k(a_1a_2a_{m-2}a_{m-1})^{(k-1)/k},$$

and finally

$$a_{m-1} > k^k a_1^{k-1} a_{m-2}^{k-2} n^{-k}. \tag{26}$$

Assume now that $n < 0$. Then

$$(a_1a_{m-2}+n)(a_2a_{m-1}+n) < (a_2a_{m-2}+n)(a_1a_{m-1}+n),$$

which implies

$$(a_2a_{m-2}+n)(a_1a_{m-1}+n) \geq ((a_1a_{m-2}+n)(a_2a_{m-1}+n)^{1/k}+1)^k,$$

$$|n|a_2a_{m-1} \geq k(4a_1a_2a_{m-2}a_{m-1}/9)^{(k-1)/k}, \tag{27}$$

(here we use that $a_{m-2} \geq 2|n|^5+1 \geq 3|n|$) and finally

$$a_{m-1} > (9/4)^{1-k} k^k a_1^{k-1} a_{m-2}^{k-2} |n|^{-k}. \tag{28}$$

From (26) and (28) in both cases we get

$$a_{m-1} > 2k^2 a_{m-2}^{k-2} |n|^{-k}. \tag{29}$$

By the same arguments we get $a_{m-2} > 2k^2 a_{m-3}^{k-2}|n|^{-k}$. Therefore,

$$a_{m-1} > (2k^2)^{k-1} a_{m-2}^{(k-2)^2} |n|^{-k(k-1)}. \tag{30}$$

Comparing (25) with (30), we get $a_{m-3}^{(k-2)^2-13/4} < |n|^{k^2-k+21/4}$. Now we use the assumption that $a_{m-3} > 2|n|^5$. We get $4k^2-19k-3/2 < 0$, and $k < 5$, a contradiction. Hence, at most three a_i's are greater than $2|n|^5$, which shows that $m \leq 2|n|^5+3$, as claimed.

It remains to consider the case $k=3$. In that case the above approach needs some modifications because the exponent of a_{m-2} in (28), i.e. $k-2$, is not greater than 1. The bound for m will also be considerably weaker. Assume that at least seven a_i's are larger than $2|n|^{17}$, i.e. $a_{m-6} > 2|n|^{17}$. We take a closer look at (27), which for $k=3$ gives

$$a_2a_{m-1} > 5a_1^2 a_{m-2}^2 |n|^{-3} \tag{31}$$

and analogously

$$a_3a_{m-1} > 5a_2^2 a_{m-2}^2 |n|^{-3}. \tag{32}$$

We claim that

$$a_{m-1} > 5|n|^{-3} a_{m-2}^{5/3}. \tag{33}$$

Indeed, if $a_{m-1} \leq 5|n|^{-3} a_{m-2}^{5/3}$, then (31) and (32) imply $a_2 > a_1^2 a_{m-2}^{1/3}$ and $a_3 > a_2^2 a_{m-2}^{1/3}$. But this leads to $a_3 > a_1^4 a_{m-2} \geq a_{m-2}$, a contradiction. By iterating (33) five times, we obtain

$$a_{m-1} > (5|n|^{-3})^{1441/81} a_{m-6}^{3125/243}. \tag{34}$$

On the other hand, an application of Lemma 2 to (24) for $k = 3$ gives

$$a_{m-1} < 2305|n|^{11} a_2^9. \tag{35}$$

Comparing (35) with (34) we get

$$a_{m-6}^{938/243} < |n|^{1738/27}. \tag{36}$$

The assumption that $a_{m-6} > 2|n|^{17}$, combined with (36), leads to a contradiction. Hence, $m \leq 2|n|^{17} + 6$, as we claimed. □

Proof of Theorem 4. The proof goes along the same lines as the corresponding one in [22, Theorem 1.4]. However, for the convenience of the reader we give the details. We may assume that $\mathcal{A} \subseteq \mathbb{N}$, since the bound for subsets of $\mathbb{Z}$ can be obtained by doubling the bound for subsets of $\mathbb{N}$. Let $\mathcal{A}' = \{a \in \mathcal{A} : a > c_0|n|^3\}$, where c_0 is defined in Lemma 1. By Lemma 1, in the set $\mathcal{A}'$ there does not exist a subset of five elements such that $a_i a_j + n = x_{ij}^{k_{ij}}$ with $k_{ij} \geq 3205$ for all distinct i and j. Let $t = \pi(3205) = 453$ and let p_i be the ith prime. We let G be the graph whose vertices are the elements of $\mathcal{A}'$. We color the edges of G with the $t+1$ colors $p_1, \ldots, p_t, \infty$ in such a way that if $a, b \in \mathcal{A}'$, then we assign to the edge ab the color p_i, $i \in \{1, \ldots, t\}$ if p_i is the smallest prime for which there exist an integer x such that $ab + 1 = x^{p_i}$. If such p_i does not exist, we assign the color ∞ to the edge ab.

We finish the proof by using the existence of Ramsey numbers. The Ramsey number $R(n_1, \ldots, n_s)$ is the smallest positive integer R such that no matter how we color the edges of the complete graph with R vertices with the colors $1, 2, \ldots, s$, there exist a color i and a complete monochromatic subgraph with n_i vertices colored with color i (see e.g. [18]). For given non-zero integer n, consider the following well-defined positive integer

$$R(n) = R(C_1(2, n), C_1(3, n), C_1(5, n), \ldots, C_1(3203, n), 5),$$

where the quantities $C_1(k,n)$ are defined in Theorem 3. We claim that $|\mathcal{A}'| < R(n)$, and therefore $|\mathcal{A}| < c_0n^3 + R(n)$, which will complete the proof of Theorem 4. Indeed, if $|\mathcal{A}'| \geq R(n)$, then either there exist a prime number $p \leq 3203$ and at least $C_1(p,n)$ elements of $\mathcal{A}'$ such that the product of any two of them plus n is a pth power, contradicting Theorem 3, or there exist at least five elements of $\mathcal{A}'$ such that the product of any two of them plus n is a kth power with some $k \geq 3205$, contradicting Lemma 1. □

6. Acknowledgements

The authors are grateful to the referee for her/his helpful remarks and suggestions.

References

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

[3] Y. Bugeaud, A. Dujella, On a problem of Diophantus for higher powers, *Math. Proc. Cambridge Phil. Soc.* **135** (2003), 1–10.

[4] Y. Bugeaud, K. Gyarmati, On generalizations of a problem of Diophantus, *Illinois J. Math* **148** (2004), 1105–1115.

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

[6] R. Dietmann, C. Elsholtz, K. Gyarmati, M. Simonovits, Shifted products that are coprime pure powers, *J. Combin. Theory Ser. A* **111** (2005), 24–36.

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

[8] A. Dujella, There are only finitely many Diophantine quintuples, *J. Reine Angew. Math.* **566** (2004), 183–214.

[9] A. Dujella, Bounds for the size of sets with the property $D(n)$, *Glas. Mat. Ser. III* **39** (2004), 199–205.

[10] A. Dujella, Diophantine m-tuples, http://web.math.hr/˜duje/dtuples.html.

[11] A. Dujella, C. Fuchs, Complete solution of a problem of Diophantus and Euler, *J. London Math. Soc.* **71** (2005), 33–52.

[12] A. Dujella, F. Luca, Diophantine m-tuples for primes, *Intern. Math. Research Notices* **47** (2005), 2913–2940.

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

[14] J. H. Evertse, Upper Bounds for the Numbers of Solutions of Diophantine Equations, MCT 168, *Mathematisch Centrum*, *Amsterdam*, 1983.

[15] Y. Fujita, The number of Diophantine quintuples, *Glas. Mat. Ser. III* **45** (2010), 15–29.

[16] A. Filipin, There does not exist a $D(4)$-sextuple, *J. Number Theory* **128** (2008), 1555–1565.

[17] P. Gibbs, Some rational Diophantine sextuples, *Glas. Mat. Ser. III* **41** (2006), 195–203.

[18] R.L. Graham, B.L. Rothschild, J.H. Spencer, Ramsey Theory, *John Wiley & Sons, New York*, 1980.

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

[20] K. Gyarmati, A. Sárközy, C. L. Stewart, On shifted products which are powers, *Mathematika* **49** (2002), 227–230.

[21] K. Gyarmati, C. L. Stewart, On powers in shifted products, *Glas. Mat. Ser. III* **42** (2007), 273–279.

[22] F. Luca, On shifted products which are powers, *Glas. Mat. Ser. III* **40** (2005), 13–20.

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

[24] C. L. Stewart, On sets of integers whose shifted products are powers, *J. Combin. Theory Ser. A* **115** (2008), 662–673.

A. BÉRCZES
INSTITUTE OF MATHEMATICS, UNIVERSITY OF DEBRECEN
NUMBER THEORY RESEARCH GROUP, HUNGARIAN ACADEMY OF SCIENCES AND UNIVERSITY OF DEBRECEN
H-4010 DEBRECEN, P.O. BOX 12, HUNGARY

E-mail: berczesa@math.klte.hu

A. DUJELLA
UNIVERSITY OF ZAGREB,
DEPARTMENT OF MATHEMATICS,
BIJENIČKA CESTA 30,
10000 ZAGREB,
CROATIA

E-mail: duje@math.hr

L. HAJDU
INSTITUTE OF MATHEMATICS, UNIVERSITY OF DEBRECEN
NUMBER THEORY RESEARCH GROUP, HUNGARIAN ACADEMY OF SCIENCES AND UNIVERSITY OF DEBRECEN
H-4010 DEBRECEN, P.O. BOX 12, HUNGARY

E-mail: hajdul@math.klte.hu

F. LUCA
MATHEMATICAL INSTITUTE, UNAM
AP. POSTAL 61–3 (XANGARI), CP 58 089
MORELIA, MICHOACÁN
MEXICO

E-mail: fluca@matmor.unam.mx