Shifted products that are coprime pure powers

(Mathematics Subject classification: Primary 11B75, 11D99; Secondary 05D10, 05C38)

Rainer Dietmann*, Christian Elsholtz†, Katalin Gyarmati‡, Miklós Simonovits

September 17, 2004

Abstract

A set A of positive integers is called a coprime Diophantine powerset if the shifted product $ab+1$ of two different elements a and b of A is always a pure power, and the occuring pure powers are all coprime. We prove that each coprime Diophantine powerset $A \subset \{1,\dots,N\}$ has $|A| \leq 8000 \log N/\log\log N$ for sufficiently large N. The proof combines results from extremal graph theory with number theory. Assuming the famous *abc*-conjecture, we are able to both drop the coprimality condition and reduce the upper bound to $c\log\log N$ for a fixed constant c.

1. Introduction

A finite set A of integers is called a Diophantine n-tuple if $|A| = n$ and $ab+1$ is a perfect square for all elements a and b of A with $a \neq b$. Diophantus of Alexandria studied such sets and found the following examples of rational numbers: $A = \{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$. Fermat found the following set of integers: $\{1,3,8,120\}$. Euler found a parametric solution $\{a, b, a+b+2r, 4r(r+a)(r+b)\}$, where $ab+1 = r^2$. Baker and Davenport [1] proved that 120 is the only positive integer that extends the triple $\{1,3,8\}$ to a Diophantine quadruple. This implies that Fermat's example cannot be extended to a Diophantine quintuple. A well known folklore conjecture asserts that there are no Diophantine 5-tuples. In this

*corresponding author

†Research partially supported by the Technische Universität Clausthal, a travel grant by the DFG and a Fellowship by the centre for interdisciplinary research (ZIF), Bielefeld.

‡Research partially supported by Hungarian Scientific Research Grant OTKA T043631 and T043623

direction Dujella proved that there are no Diophantine 6-tuples and that there are at most finitely many Diophantine quintuples ([8], [9]). Dujella maintains an interesting web page (see [10]) on this and related problems, giving many further references.

Recently, Bugeaud and Dujella [6] obtained a uniform upper bound of 7 for the cardinality of the set A when the set of squares is replaced by the set of k-th powers of integers. A further generalization arises when, in addition, the exponent k is also allowed to vary. This leads to the following definition: We call a set A of positive integers a *Diophantine powerset* if $ab+1$ is always a pure power for different elements a and b of A. In view of the aforementioned results it is reasonable to conjecture that all Diophantine powersets are finite, their cardinality being bounded by an absolute constant. However, at present only the following weaker results are known. Gyarmati, Sárközy and Stewart ([18], see also [17], Theorem 6.4) showed that for sufficiently large N any Diophantine powerset $A \subset \{1, \dots, N\}$ has cardinality

$$|A| < 340 \frac{(\log N)^2}{\log \log N}, \tag{1}$$

so Diophantine powersets are very thin. More recently Bugeaud and Gyarmati [7] obtained a slight improvement of this result, namely they proved

$$|A| \leq 177000 (\log N / \log \log N)^2.$$

In their proof Gyarmati, Sárközy and Stewart defined for each k a graph where the vertices are the elements of A, and an edge connects the vertices a_i and a_j if and only if $a_i a_j + 1$ is a perfect k-th power. Using that these graphs do not contain a cycle of length 4 they obtained (1). One may wonder whether a stronger bound can be proved by imposing a further, not too restrictive, condition on the set A. The purpose of this paper is to show that this is indeed the case.

We call a set A of positive integers a *coprime Diophantine powerset* if $ab+1$ is always a pure power for different elements a and b of A where in addition all occurring powers are coprime in pairs. This condition is not too restrictive since it includes the following important case. If the elements are multiples of $P = \prod_{p<y} p$, where the product is taken over primes less than y, then the numbers $a_i a_j + 1$ do not have any small prime $p \leq y$ as a common factor and therefore many of these might be coprime. But it is known that for example the most difficult case for giving an upper bound for the number of squares in arithmetic progressions is when the common difference is the product of many small prime factors. (See page 371 of [3], or [4].) It is interesting to note that Stewart and Tijdeman [23] discussed a hypothesis (so called balanced sets) which is related to our coprime condition.

Theorem 1. *For every sufficiently large integer N and for every coprime Diophantine powerset $A \subset \{1, \ldots, N\}$ we have*

$$|A| \leq 8000 \frac{\log N}{\log \log N}.$$

For the experts it is perhaps not surprising that we reach an upper bound close to $\log N$ since we make heavy use of Ramsey type arguments. In fact, a weaker but more complicated condition instead of 'coprime' would have been sufficient to establish this result. It is easily seen that for example the following is enough to prove Lemma 6 and thus Theorem 1: For every shifted product $ab + 1$ there is a prime dividing $ab + 1$ but none of the other shifted products. However, we decided to state our theorem using the more natural notion of coprimality.
Moreover, we relate this problem to two of the standard conjectures in number theory. It is well known that the *abc*-conjecture due to Oesterlé and Masser (see Masser [20]) has applications to very different problems in number theory, see for example the results by Granville [12], Granville and Stark [13] or the survey by Granville and Tucker [14]. Let us state the *abc*-conjecture first:

Conjecture 1 (*abc*-conjecture, Oesterlé-Masser [20]). *For every $\epsilon > 0$ there exists a constant $C(\epsilon)$ with the following property: Let a, b, c be non-zero integers with $\gcd(a, b, c) = 1$ and $a + b + c = 0$, and put*

$$P = \prod_{p \,|\, abc} p.$$

Then

$$\max\{|a|, |b|, |c|\} < C(\epsilon) P^{1+\epsilon}.$$

Assuming the *abc*-conjecture we are able to give a significant improvement over (1) even without assuming coprimality of the occuring pure powers.

Theorem 2. *Assume that the abc-conjecture is true. Then there exists a constant $c > 0$ such that for every integer $N \geq 3$ and for every Diophantine powerset $A \subset \{1, \ldots, N\}$ we have*

$$|A| \leq c(\log \log N).$$

The following conjecture is also widely believed:

Conjecture 2. *Let $k \geq k_0$, where k and k_0 are positive integers and k_0 is sufficiently large. Then there are only finitely many positive integer solutions of*

$$x_1^k + x_2^k = y_1^k + y_2^k$$

where $x_i \notin \{y_1, y_2\}$ for $i \in \{1, 2\}$.

It is not known whether there are any solutions for $k \geq 5$ (see [15], chapter D1). Indeed this is a very special case of a much more general problem where all existing heuristics and experiments even suggest that for $k > 3$ the diophantine equation $x_1^k + \cdots + x_m^k = y_1^k + \cdots + y_n^k$ does not have any nontrivial positive integer solutions ($x_i \neq y_j$) for $m + n < k$, see Lander, Parkin and Selfridge [19].

In this situation one can prove

Theorem 3. *Let us assume conjecture 2. Further, let $A \in \{1, \ldots, N\}$ be a set of positive integers such that $a_i + a_j$ is always a k-th power of an integer for $a_i, a_j \in A$, $a_i \neq a_j$, and fixed $k \geq k_0$. Then $|A| \leq C(k)$ where $C(k)$ is a constant.*

Unconditionally it is known that $|A| \ll_k \log N$, see [21], Theorem 6 and [16], Theorem 9.

Theorem 3 possibly holds with $C(k) = 3$ for $k \geq k_0$. This could be proved by a stronger version of Conjecture 2, which replaces 'finitely many solutions' by 'no solutions'.

The authors would like to thank E. Bombieri, T. Browning, Y. Bugeaud, A. Dujella, D. R. Heath-Brown, A. Sárközy and G. Wüstholz for comments and discussions. We also thank the referees for their careful reading and suggesting a refinement of Theorem 1.

2. Results from graph theory

In this section we collect four useful lemmas from graph theory. The underlying philosophy is that a graph with sufficiently many edges must necessarily contain a prescribed substructure.

Lemma 1 (Ramsey Theorem for graphs). *For all positive integers m, n there is a positive integer $C_1(m, n)$ with the following property: if G is a complete graph on at least $C_1(m, n)$ vertices, whose edges are coloured by m colours, then G contains a complete monochromatic subgraph on n edges.*

Proof. See for example [2], p. 271, Theorem 6.2.

Our next lemma is related to a classical result by Bondy and Simonovits (see [5]).

Lemma 2. *If a graph G on n vertices has at least $n^{1+1/k} + n$ edges, then G contains a $2s$-cycle for some $s \in \{2, \ldots, k\}$.*

To prove this lemma we need the following auxiliary result. Here $e(G)$ denotes the number of the edges of G and $\underline{d}(G)$ denotes the minimum degree in G. By G^n and H^m we denote graphs on n and m vertices, respectively.

Lemma 3. *Every graph G^n contains a subgraph H^m such that $\underline{d}(H^m) \geq e(G^n)/n$.*

A proof of Lemma 3 can be found in [2] or [11].

Proof of Lemma 2. Suppose that, contrary to the statement of Lemma 2, G does not contain a $2s$-cycle for $2 \leq s \leq k$. By Lemma 3 we have a subgraph H^m such that

$$\underline{d}(H^m) \geq n^{1/k} + 1.$$

Note that $m \leq n$. Let u be an arbitrary vertex of the graph H^m, and $S_i \subseteq H^m$ be the set of vertices of distance i from u, $i = 0, 1, 2, \ldots, k$. (Two vertices are said to have distance i if the shortest path connecting them is of length i.) By assumption H^m does not contain any $2s$-cycle for $2 \leq s \leq k$; thus each vertex of S_{i+1} is joined only to one element of S_i. On the other hand $\underline{d}(H^m) \geq n^{1/k} + 1$; therefore $|S_{i+1}| \geq n^{1/k} |S_i|$. Thus

$$m > |S_k| \geq (n^{1/k})^k = n,$$

a contradiction. □

Our last lemma is a slightly weakened version of Turán's graph theorem:

Lemma 4 (Turán's graph theorem (see [24], [25] or [2])). *For every integer $r \geq 3$, if G is a graph on n vertices not containing a complete subgraph K_r, then*

$$e(G) \leq \left(1 - \frac{1}{r-1}\right) \binom{n}{2} + r^2$$

where $e(G)$ denotes the number of edges.

3. Results from number theory

3.1. The connection between number theory and graph theory

The purpose of this section is to state or prove some results from number theory which complement the above lemmas from graph theory. As mentioned in the introduction, we define a coloured graph where the numbers correspond to vertices and where the vertices are connected by an edge of colour $k \geq 2$ if and only if the property '$ab + 1$ is a k-th power, and k is minimal' holds. Using the number theoretic lemmas below we prove that certain substructures (namely certain complete graphs of size k, where k is fixed, and certain cycles) cannot occur in this graph. Using the graph theoretic lemmas we conclude that graphs without these substructures cannot be too large.

3.2. There are no Diophantine 6-tuples

Lemma 5. *There are no* 6 *distinct positive integers* $a_1, \ldots, a_6$ *such that* $a_i a_j + 1$ *is a square of an integer whenever* $i \neq j$.

Proof. This is Theorem 2 in [9]. □

3.3. A gap principle for coprime Diophantine $(2k, \ell)$-cycles

Let $x_1, \ldots, x_{2k}$ be positive integers. For $k \geq 2$ we call the $(2k)$-tuple $(x_1, \ldots, x_{2k})$ a coprime Diophantine $(2k, \ell)$-cycle if each of the shifted products $x_1x_2+1, x_2x_3+1, \ldots, x_{2k-1}x_{2k}+1, x_{2k}x_1+1$ is an ℓ-th power of an integer, and all occurring ℓ-th powers are coprime. The following gap principle for coprime Diophantine $(2k, \ell)$-cycles shows that not all x_i can be of the same order of magnitude.

Lemma 6. *Let* $(x_1, \ldots, x_{2k})$ *be a coprime Diophantine* $(2k, \ell)$*-cycle, and let*

$$M = \max\{x_1x_2,\ x_2x_3, \ldots, x_{2k}x_1\},\ m = \min\{x_1x_2,\ x_2x_3, \ldots, x_{2k}x_1\}.$$

Then

$$m^{\ell/k} \leq M.$$

Proof. If $\ell \leq k$, then the lemma is trivial, so let us suppose that $\ell > k$. Then $\ell \geq k+1 \geq 3$. Since $x_1x_2+1, x_2x_3+1, \ldots, x_{2k}x_1+1$ are perfect ℓ-th powers we have $m \geq 2^\ell - 1$. Moreover, since the shifted products $x_1x_2+1, \ldots, x_{2k}x_1+1$ are coprime, clearly

$$\begin{aligned} L &:= (x_1x_2+1)(x_3x_4+1)\cdot\ldots\cdot(x_{2k-1}x_{2k}+1) \\ &\neq (x_2x_3+1)(x_4x_5+1)\cdot\ldots\cdot(x_{2k}x_1+1) =: R. \end{aligned}$$

By symmetry we may suppose that $L > R$. Since both L and R are perfect ℓ-th powers we also have

$$L^{1/\ell} \geq R^{1/\ell} + 1.$$

From this we get

$$\begin{aligned} L &\geq R + \ell R^{(\ell-1)/\ell}, \\ L - R &\geq \ell R^{(\ell-1)/\ell} \geq \ell(x_1 \ldots x_{2k})^{(\ell-1)/\ell}. \end{aligned} \tag{2}$$

We further have the upper bound

$$\begin{aligned} L - R &\leq (x_1x_2+1)(x_3x_4+1)\cdot\ldots\cdot(x_{2k-1}x_{2k}+1) - x_1x_2\ldots x_{2k} \\ &\leq x_1x_2\ldots x_{2k}\left(\left(1+\frac{1}{x_1x_2}\right)\ldots\left(1+\frac{1}{x_{2k-1}x_{2k}}\right)-1\right) \\ &\leq x_1x_2\ldots x_{2k}\left(\left(1+\frac{1}{m}\right)^k - 1\right) \leq x_1x_2\ldots x_{2k}\frac{k}{m}\left(1+\frac{1}{m}\right)^{k-1}. \end{aligned} \tag{3}$$

Using (2) and (3) we obtain

$$\ell(x_1x_2\dots x_{2k})^{(\ell-1)/\ell} \le L - R \le \frac{k}{m}\left(1+\frac{1}{m}\right)^{k-1} x_1x_2\dots x_{2k},$$
$$\left(\frac{\ell}{k}\right)^{\ell} m^{\ell} \frac{1}{\left(1+\frac{1}{m}\right)^{(k-1)\ell}} \le x_1x_2\dots x_{2k} \le mM^{k-1}.$$

Since $\ell > k$ we conclude that

$$\frac{1}{\left(1+\frac{1}{m}\right)^{\ell}} m^{(\ell-1)/(k-1)} \le M. \tag{4}$$

Using $1+x \le e^x$, $m \ge 2^{\ell}-1$ and $\ell \ge k+1$ we find

$$\begin{aligned}\left(1+\frac{1}{m}\right)^{\ell} &\le e^{\ell/m} \le e^{\ell/(2^{\ell}-1)} \le \left(2^{\ell}-1\right)^{1/(\ell-1)(\ell-2)} \le m^{1/(\ell-1)(\ell-2)} \\ &\le m^{-\ell/k+(\ell-1)/(k-1)}. \end{aligned} \tag{5}$$

Now equations (4) and (5) yield

$$m^{\ell/k} \le M,$$

which proves the assertion. □

3.4. An explicit estimate from prime number theory

Let $\pi(x)$ denote the number of primes which do not exceed x. For the proof of Theorem 1 we also need the following simple lemma.

Lemma 7. *If n is sufficiently large and $K \le n^{1/4}$, then*

$$\sum_{\substack{3\le p\le K\\ p \text{ is a prime}}} n^{1/(p-1)} \le 2n^{1/2}.$$

Proof. By Corollary 2 of Rosser and Schoenfeld [22] we have $\pi(x) \le \frac{5x}{4\log x}$ for $x \ge 2$. Thus

$$\begin{aligned}\sum_{\substack{3\le p\le K\\ p \text{ is a prime}}} n^{1/(p-1)} &= n^{1/2} + \sum_{\substack{5\le p\le K\\ p \text{ is a prime}}} n^{1/4} \le n^{1/2} + \pi(K)n^{1/4} \\ &\le n^{1/2} + \frac{5K}{4\log K} n^{1/4} \le n^{1/2} + \frac{5n^{1/2}}{\log n} \le 2n^{1/2},\end{aligned}$$

which completes the proof of the lemma. □

4. Proof of Theorem 1

Let $K = 2\log\log N$. We cover the interval $[3, N]$ by t subintervals I_j of the form $[3^{(1+1/K)^j}, 3^{(1+1/K)^{j+1}}]$. For each subinterval $[z, z^{1+1/K}]$ we define a graph and use the previous graph theoretic lemmas to bound the number of vertices of the graph. The number t of subintervals of the prescribed form can be bounded as follows: a power series expansion shows that

$$\frac{1}{\log(1+\frac{1}{K})} = K + \frac{1}{2} + O(\frac{1}{K}) \leq K + 0.51,$$

providing that N and thus K is sufficiently large (we shall assume this for the whole proof). This implies that

$$\begin{aligned} 3^{(1+1/K)^{t+1}} &\leq N, \\ t &\leq \frac{1}{\log(1+1/K)}(\log\log N - \log\log 3), \\ t &\leq (K+0.51)(\log\log N - \log\log 3). \end{aligned}$$

Similarly, we have

$$t \geq (\log\log N)^2.$$

Moreover,

$$\frac{t}{K} \leq \frac{(K+0.51)(\log\log N - \log\log 3)}{K} \leq 0.17 + \log\log N.$$

In the following we will show that for sufficiently large N the bound

$$n = \left|A \cap [z, z^{1+1/K}]\right| \leq \max\left\{189\frac{\log z}{(\log\log z)^2}, 16(\log\log N)^4\right\}$$

holds true. In other words, we show that if $n \geq 16(\log\log N)^4$, then $n \leq 189\log z/(\log\log z)^2$. So suppose that $n \geq 16(\log\log N)^4$. Then $K \leq n^{1/4}$. Let $A \cap [z, z^{1+1/K}] = \{x_1, x_2, \ldots, x_n\}$ where $x_1 < x_2 < \cdots < x_n$. From (1) we know that $n = O(\frac{(\log z)^2}{\log\log z})$ which implies that

$$\log n \leq 2\log\log z - \log\log\log z + O(1) \leq 2\log\log N = K.$$

This implies that $n^{1/K} \leq e$ and so

$$n^{1+1/K} \leq en. \tag{6}$$

We colour the edges of the complete graph G on the vertices $x_1, \ldots, x_n$ as follows: The edge connecting x_i and x_j is coloured by the smallest integer $\ell \geq 2$ for which $x_i x_j + 1$ is a perfect ℓ-th power. Note that each edge coming from the interval

$[z, z^{1+1/K}]$ is coloured by a prime number less than $1.5 \log z$. For $i = 2, 3, \ldots$ let b_i denote the number of edges in G which are coloured with the integer i. By Lemma 4 and Lemma 5 we find that $b_2 \leq \frac{2}{5}n^2 + 36$. Let G_p be the subgraph of G whose vertices are those of G and whose edges are the edges of G coloured with the prime p. The graph G_p does not contain a $2k$-cycle for $2 \leq k \leq \min\{K, p-1\}$. Otherwise, this $2k$-cycle $(x_1, \ldots, x_{2k})$ defines a coprime Diophantine $(2k, p)$-cycle. Defining m and M as in Lemma 6 we have that $z^2 < m$ and $M < z^{2+2/K}$. By Lemma 6 we find that

$$\left(z^2\right)^{1+1/K} \leq \left(z^2\right)^{(k+1)/k} \leq \left(z^2\right)^{p/k} < m^{p/k} \leq M < z^{2+2/K},$$

which is a contradiction. Therefore, by Lemma 2,

$$b_p \leq n^{1+1/\min\{K, p-1\}} + n.$$

For large p this upper bound can be improved: Since the pth powers that occur are distinct integers by the coprimality condition, the number of such pth powers is bounded by the largest positive integer a satisfying $a^p \leq z^{2+2/K} \leq z^3$. Hence

$$b_p \leq \min\{n^{1+1/\min\{K, p-1\}} + n, z^{3/p}\}. \tag{7}$$

Now Lemma 7 and the upper bounds (6), (7), and $\pi(x) \leq 5x/(4 \log x)$ imply that

$$\begin{aligned}
\binom{n}{2} &= e(G) = b_2 + b_3 + \ldots \\
&\leq \frac{2}{5}n^2 + 36 + \sum_{\substack{3 \leq p \leq 1.5 \log z \\ p \text{ is a prime}}} \min\{n^{1+1/\min\{K,p-1\}} + n, z^{3/p}\} \\
&\leq \frac{2}{5}n^2 + 36 + \sum_{\substack{3 \leq p \leq \min\{K, 4 \log z/\log\log z\} \\ p \text{ is a prime}}} (n^{1+1/(p-1)} + n) \\
&+ \sum_{\substack{K < p \leq 4 \log z/\log\log z \\ p \text{ is a prime}}} (n^{1+1/K} + n) \\
&\quad \text{(where the latter sum is empty if } K \geq 4 \log z/\log\log z) \\
&+ \sum_{4 \log z/\log\log z < p \leq 1.5 \log z} z^{3/p} \\
&\leq \frac{2}{5}n^2 + 36 + n\left(2n^{1/2} + K + 5.01(e+1)\frac{\log z}{(\log\log z)^2}\right) + \frac{15}{8}(\log z)^{7/4} \\
&\leq 0.4005n^2 + n18.7\frac{\log z}{(\log\log z)^2} + 2(\log z)^{7/4}.
\end{aligned}$$

Now if $n \geq (\log z)^{9/10}$ then $2(\log z)^{7/4} \leq 2n^{35/18}$, so

$$\binom{n}{2} \leq 0.401n^2 + n18.7\frac{\log z}{(\log\log z)^2}$$

and consequently

$$n \le 189 \frac{\log z}{(\log\log z)^2}, \tag{8}$$

confirming our claim above. In case of $n < (\log z)^{9/10}$ the bound (8) is trivially true. This completes the verification of our claim. Thus

$$\begin{aligned} |A| &\le \sum_{i=1}^{t} \max\left\{ 189 \frac{\log\left(3^{(1+1/K)^{i+1}}\right)}{(\log\log(3^{(1+1/K)^{i+1}}))^2}, 16(\log\log N)^4 \right\} \\ &\le 16t(\log\log N)^4 + 189 \sum_{i=1}^{t} \frac{(\log 3)(1+1/K)^{i+1}}{(i+1)^2(\log(1+1/K))^2} \\ &\le 33(\log\log N)^6 + 208K^2 \sum_{i=1}^{t} \frac{(1+1/K)^{i+1}}{(i+1)^2}. \end{aligned}$$

Now

$$\begin{aligned} \sum_{i=1}^{t} \frac{(1+1/K)^{i+1}}{(i+1)^2} &\le \sum_{i=1}^{t} \frac{e^{(i+1)/K}}{(i+1)^2} \\ &\le \sum_{i\le t/2} \frac{e^{(i+1)/K}}{(i+1)^2} + 4 \sum_{t/2<i\le t} \frac{e^{(i+1)/K}}{(\log\log N)^4} \\ &\le \sum_{i\le t/2} e^{(i+1)/K} + \frac{4}{(\log\log N)^4} \sum_{i\le t} e^{(i+1)/K} \\ &\le e^{0.086} K (\log N)^{1/2} + 4e^{0.18} K \frac{\log N}{(\log\log N)^4}. \end{aligned}$$

Hence

$$\begin{aligned} |A| &\le 832 e^{0.181} K^3 \frac{\log N}{(\log\log N)^4} \\ &\le 8000 \frac{\log N}{\log\log N}, \end{aligned}$$

and the proof of the theorem is complete.

5. Conditional results

If we assume that the *abc*-conjecture (see Conjecture 1) holds, then we can prove a much stronger gap principle. No coprimality condition is necessary, and even the occuring powers are allowed to have different exponents. This leads to the much stronger bound in Theorem 2.

Lemma 8. *Suppose that the abc-conjecture is true. Let q, r, x, y be distinct positive integers such that $qx+1$, $qy+1$, $rx+1$, $ry+1$ are pure powers, none of them a square or a cube. Let*

$$M = \max\{q, r, x, y\}$$

and

$$m = \min\{q, r, x, y\}.$$

Then $M \gg_\epsilon m^{6/5-\epsilon}$.

Proof. Let

$$L = (qx+1)(ry+1) \quad \text{and} \quad R = (qy+1)(rx+1).$$

We first remark that clearly $L \neq R$, for otherwise we would have $q(x-y) = r(x-y)$, a contradiction since q, r, x, y were assumed to be distinct. Now

$$qx+1 = W^\alpha,\ ry+1 = X^\beta,\ qy+1 = Y^\gamma,\ rx+1 = Z^\delta$$

for suitable positive integers $W, X, Y, Z, \alpha, \beta, \gamma, \delta$ with $W, X, Y, Z \geq 2$ and $\alpha, \beta, \gamma, \delta \geq 5$. Let $\Delta = L - R$. Then as shown above, $\Delta \neq 0$. Let $D = \gcd(W^\alpha X^\beta, Y^\gamma Z^\delta, \Delta)$. We apply the *abc*-conjecture with $a = -W^\alpha X^\beta/D$, $b = Y^\gamma Z^\delta/D$, and $c = \Delta/D$. Now

$$P = \prod_{p \,|\, abc} p \leq |c| \prod_{p \,|\, ab} p \leq \frac{WXYZ|\Delta|}{D} \leq \frac{L^{1/5}R^{1/5}|\Delta|}{D}.$$

Since the *abc*-conjecture was assumed to be true, we have

$$|a| = \frac{W^\alpha X^\beta}{D} \ll_\epsilon P^{1+\frac{\epsilon}{2}}$$

and

$$b = \frac{Y^\gamma Z^\delta}{D} \ll_\epsilon P^{1+\frac{\epsilon}{2}}.$$

Hence

$$LR = W^\alpha X^\beta Y^\gamma Z^\delta \ll_\epsilon D^2 P^{2+\epsilon} \ll_\epsilon L^{2/5+\epsilon/5} R^{2/5+\epsilon/5} |\Delta|^{2+\epsilon}.$$

Consequently,

$$|\Delta| \gg_\epsilon L^{3/10-\epsilon/10} R^{3/10-\epsilon/10} \gg_\epsilon m^{12/5-\epsilon}. \tag{9}$$

On the other hand, we have

$$|\Delta| = |L - R| = |q(x-y) + r(y-x)| \ll M^2. \tag{10}$$

On comparing (9) and (10) we obtain $m^{6/5-\epsilon} \ll_\epsilon M$, and the proof of the lemma is finished. □

We need a further preliminary result for the proof of Theorem 2. A quantitative version of a more general result has been given in [7], Theorem 3, but let us give a short proof of what we need.

Lemma 9. *Let $x_1, \dots, x_n$ be positive integers such that for all $i, j \in \{1, \dots, n\}$ with $i \neq j$ the number $x_i x_j + 1$ is a square or a cube of an integer. Then $n \leq C_2$ for an absolute constant C_2.*

Proof. Our proof will be by contradiction. Let $(x_1, \dots, x_n)$ be a tuple having the property stated in the lemma, where n is sufficiently large. We consider the complete graph G with vertices $x_1, \dots, x_n$. We colour the edges of G in the following way: The edge connecting x_i and x_j is coloured red if $x_i x_j + 1$ is a square, otherwise it is coloured blue. By Lemma 1, as n was chosen large enough, there exists a complete monochromatic subgraph having at least 7 vertices. Hence there are 7 different integers such that the shifted product of two different of them is either always a square or always a cube. But this contradicts Lemma 5 or [6], Corollary 4. □

We are now in a position to prove Theorem 2.

Proof of Theorem 2. Our proof will be by contradiction. Let us suppose that

$$n = |A \cap [1, N]| \geq C_4(\log\log N)$$

where $N \geq 3$ and where C_4 is a sufficiently large positive constant. We now cover the interval $[3, N]$ by disjoint subintervals of the form $[z, z^{7/6}]$. Note that the number t of these subintervals can be bounded by

$$t \leq \log\log N / \log(7/6) \leq 7 \log\log N.$$

Thus by the pigeonhole principle there is an interval $[z, z^{7/6}]$ containing more than

$$n/(7 \log\log N) \geq C_4/7$$

elements of A. We may suppose that $z \geq C_5$ for some sufficiently large constant C_5. Let us denote these elements by $x_1, \dots, x_n$, and let G be the complete graph on $x_1, \dots, x_n$. We colour the edges of G red and blue in the following way: if $x_i x_j + 1$ is a square or a cube, then we colour the edge connecting x_i and x_j red, otherwise blue. Let r be the total number of red edges arising this way. Now by Turán's graph theorem (see Lemma 4) it is easily seen that there exists a number C_3 with $0 < C_3 < 1$ such that if

$$r > C_3 \binom{n}{2},$$

then G contains a complete red subgraph on C_2 edges. However, this contradicts Lemma 9. Hence the number s of blue edges satisfies the bound

$$s \geq (1 - C_3)\binom{n}{2} \geq n^{3/2} + n \tag{11}$$

for large enough C_4. Using Lemma 2 we conclude that there are $q, r, x, y \in [z, z^{7/6}]$ such that $qx+1$, $qy+1$, $rx+1$ and $ry+1$ are pure powers, none of them a square or a cube. But this contradicts Lemma 8, providing that C_5 was chosen large enough, proving the theorem. □

Proof of Theorem 3. Let a, b, c, d be four elements of A with $a < b < c < d$ and sufficiently large d. Then

$$a + b = x^k,\ a + c = y^k,\ b + d = z^k,\ c + d = w^k$$

for suitable integers x, y, z, w. Hence

$$x^k + w^k = y^k + z^k.$$

Since d was assumed to be sufficiently large, by Conjecture 2 we either have $x = y$ or $x = z$. In the first case we obtain $b = c$; in the second case, it follows that $a = d$. Both are impossible. So d must be bounded by a constant depending only on k, which proves the corollary. □

References

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

[2] B. Bollobás, *Extremal graph theory*, Academic Press, London-New York 1978.

[3] E. Bombieri, A. Granville and J. Pintz, Squares in arithmetic progressions, *Duke Math. J.* **66** (1992), 369–385.

[4] E. Bombieri and U. Zannier, A note on squares in arithmetic progressions II, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. **13** (2002), no. 2, 69–75.

[5] J. A. Bondy and M. Simonovits, Cycles of even length in graphs, *J. Combinatorial Theory Ser. B.* **16** (1974), 97–105.

[6] Y. Bugeaud and A. Dujella, On a problem of Diophantus for higher powers, *Math. Proc. Cambr. Philos. Soc.* **135** (2003), 1–10.

[7] Y. Bugeaud and K. Gyarmati, On generalizations of a problem of Diophantus, preprint.

[8] A. Dujella, An absolute bound for the size of Diophantine m-tuples, *J. Number Theory* **89** (2001), no. 1, 126–150.

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

[10] A. Dujella, Web page: http://www.math.hr/∼duje/dtuples.html

[11] R. J. Faudree and M. Simonovits, On a class of degenerate extremal graph problems, *Combinatorica* **3** (1983) no. 1, 83–93.

[12] A. Granville, *ABC* allows us to count squarefrees, Internat. Math. Res. Notices 1998, no. 19, 991–1009.

[13] A. Granville and H. M. Stark, *abc* implies no "Siegel zeros" for L-functions of characters with negative discriminant, Invent. Math. **139** (2000), no. 3, 509–523.

[14] A. Granville and T. J. Tucker, It's as easy as *abc*, Notices Amer. Math. Soc. **49** (2002), no. 10, 1224–1231.

[15] R. K. Guy, *Unsolved problems in Number Theory*, Second Edition, Springer-Verlag 1994.

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

[17] K. Gyarmati, Hatvány-, hatványteli és hatványmentes számok összegsorozatokban és multiplikatív struktúrákban (Hungarian), (Powers, powerful and powerfree numbers in sumsets and multiplicative structures), Master thesis, Eötvös Loránd University (2001).

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

[19] L. J. Lander, T. R. Parkin, and J. L. Selfridge, A Survey of Equal Sums of Like Powers, Math. Comput. **21** (1967), 446–459.

[20] D. W. Masser, Open problems, *Proc. Symp. Analytic. Number Th.* (1985), W. W. L. Chen (ed.), London, Imperial College.

[21] J. Rivat, A. Sárközy, and C. L. Stewart, Congruence properties of the Ω-function on sumsets, *Illinois J. Math.* **43** (1999), 1–18.

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

[23] C. L. Stewart and R. Tijdeman, On the greatest prime factor of $(ab+1)(ac+1)(bc+1)$, Acta Arith. **79** (1997), 93–101.

[24] P. Turán, On an extremal problem in graph theory (Hungarian), Mat. Fiz. Lapok **48** (1941), 436–452.

[25] P. Turán, On the theory of graphs, *Coll. Math.* **3** (1954), 19–30.

Author's addresses:

Rainer Dietmann
Institut für Algebra und Zahlentheorie
Pfaffenwaldring 57
D-70550 Stuttgart
Germany
dietmarr@mathematik.uni-stuttgart.de

Christian Elsholtz
Department of Mathematics
Royal Holloway, University of London
Egham
Surrey TW20 0EX
UK
christian.elsholtz@rhul.ac.uk

Katalin Gyarmati
Eötvös Loránd University
Department of Algebra and Number Theory
H-1117 Budapest
Pazmany Peter Setany 1/C
Hungary
gykati@cs.elte.hu

Miklós Simonovits
Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences
H-1053 Budapest
Reáltanoda u. 13-15
Hungary
miki@renyi.hu