Illinois Journal of Mathematics
Volume 48, Number 4, Winter 2004, Pages 1105–1115
S 0019-2082

ON GENERALIZATIONS OF A PROBLEM OF DIOPHANTUS

YANN BUGEAUD AND KATALIN GYARMATI

Abstract. Let $k \geq 2$ be an integer and let $\mathcal{A}$ and $\mathcal{B}$ be two sets of integers. We give upper bounds for the number of perfect k-th powers of the form $ab+1$, with a in $\mathcal{A}$ and b in $\mathcal{B}$. We further investigate several related questions.

1. Introduction

The Greek mathematician Diophantus of Alexandria noted that the rational numbers 1/16, 33/16, 17/4, and 105/16 have the following property: the product of any two of them increased by 1 is a square of a rational number. Later, Fermat found that the set of four positive integers $\{1, 3, 8, 120\}$ shares the same property. A finite set of m positive integers $a_1 < \cdots < a_m$ such that $a_i a_j + 1$ is a perfect square whenever $1 \leq i < j \leq m$ is commonly called a Diophantine m-tuple. A famous conjecture asserts that there does not exist a Diophantine 5-tuple. This question has been nearly solved in a remarkable paper by Dujella [3], who proved that there does not exist a Diophantine 6-tuple and that the elements of any Diophantine 5-tuple are less than $10^{10^{26}}$. We direct the reader to [3] for further references.

This problem was extended to higher powers by Bugeaud and Dujella [2]. They proved that if $k \geq 3$ is a given integer and $\mathcal{A}$ is a set of positive integers such that $aa'+1$ is a perfect k-th power for all distinct a and a' in $\mathcal{A}$, then $\mathcal{A}$ has at most 7 elements. In the present paper, we investigate related questions and, among other results, we provide, for an arbitrary set $\mathcal{A}$ of positive integers, estimates for the number $n_{\mathcal{A}}$ of pairs (a, a') with a, a' in $\mathcal{A}$ such that $aa' + 1$ is a perfect k-th power. It is clear that, for all m, there exists a set $\mathcal{A} = \{a_1, a_2, \ldots, a_m\}$ such that the $m-1$ integers $a_1a_2+1,\ a_2a_3+1, \ldots,\ a_{m-1}a_m+1$ are perfect k-th powers; for such sets $\mathcal{A}$, the number $n_{\mathcal{A}}$ is at least equal to the cardinality of $\mathcal{A}$ minus one. In the present paper, we combine results from

Received November 13, 2003; received in final form August 18, 2004.
2000 *Mathematics Subject Classification.* 11D99, 11B99.
Research partially supported by Hungarian Scientific Research Grants OTKA T043631 and T043623.

[2] with graph theory (see Theorem 1) to give an upper estimate for $n_{\mathcal{A}}$ that is much sharper than the trivial bound (which is the square of the cardinality of $\mathcal{A}$).

Acknowledgements. We warmly thank the referee for having detected many inaccuracies in an earlier version, and for having made numerous remarks, which helped us to considerably improve the presentation of the paper.

2. Results

Throughout this paper, the cardinality of a set $\mathcal{S}$ is denoted by $|\mathcal{S}|$. Given an integer $k \geq 3$ and two finite sets $\mathcal{A}$ and $\mathcal{B}$, our first result provides us with an upper bound for the number of perfect k-th powers of the form $ab+1$, with a in $\mathcal{A}$ and b in $\mathcal{B}$.

Theorem 1. *Let $k \geq 3$ be an integer. Let $\mathcal{A}$ and $\mathcal{B}$ be two sets of positive integers with $|\mathcal{A}| \geq |\mathcal{B}|$ and set*

$$\mathcal{S} = \{(a,b) : \ a \in \mathcal{A}, b \in \mathcal{B}, \ ab+1 \quad \textit{is a } k\textit{-th power}\}.$$

We then have

$$|\mathcal{S}| \leq 2 \cdot 6^{1/3} \, |\mathcal{A}| \cdot |\mathcal{B}|^{2/3} + 4 \, |\mathcal{A}| \leq 7.64 \, |\mathcal{A}| \cdot |\mathcal{B}|^{2/3} \quad \textit{if } k = 3,$$
$$|\mathcal{S}| \leq 2\sqrt{3} \, |\mathcal{A}| \cdot |\mathcal{B}|^{1/2} + 2 \, |\mathcal{A}| \leq 5.47 \, |\mathcal{A}| \cdot |\mathcal{B}|^{1/2} \quad \textit{if } k \geq 4.$$

It follows from Theorem 1 that, if $\mathcal{A}$ and $\mathcal{B}$ have same cardinality (in particular, if $\mathcal{A} = \mathcal{B}$), then the number of pairs (a, b) with a in $\mathcal{A}$ and b in $\mathcal{B}$ such that $ab + 1$ is a k-th power for a fixed k is less than $8 \, |\mathcal{A}|^{5/3}$ if $k = 3$ and is less than $6 \, |\mathcal{A}|^{3/2}$ if $k \geq 4$. We further notice that there is no positive integer a such that $a^2 + 1$ is a perfect power, a result due to V. A. Lebesgue [9].

We were unable to treat the case $k = 2$ in Theorem 1. However, if the sets $\mathcal{A}$ and $\mathcal{B}$ are equal, it is possible to slightly improve the trivial estimate.

Theorem 2. *Let $\mathcal{A}$ be a set of positive integers with $|\mathcal{A}| \geq 6$. Then the set*

$$\{(a, a') : \ a, a' \in \mathcal{A}, \ a > a', \ aa' + 1 \quad \textit{is a square}\}$$

has at most $0.4 \, |\mathcal{A}|^2$ elements.

The results from [2] also enable us to improve upon Theorems 1 and 2 of Gyarmati, Sárközy and Stewart [6]. For any integer $k \geq 2$, set

$$V_k = \{x^\ell : x \in \mathbb{Z}^+ \text{ and } 2 \leq \ell \leq k\}.$$

THEOREM 3. *Let $k \geq 2$ be an integer. Let $\mathcal{A}$ be a set of positive integers with the property that $aa' + 1$ is in V_k whenever a and a' are distinct integers from $\mathcal{A}$. We then have*

$$|\mathcal{A}| < 85000\left(\frac{k}{\log k}\right)^2. \tag{1}$$

Theorem 3 considerably improves Theorem 2 of [6], where the authors obtained the upper bound

$$|\mathcal{A}| < 160\left(\frac{k}{\log k}\right)^2 \log\log\left(\max_{a\in\mathcal{A}} a\right), \tag{2}$$

instead of (1). We point out that the right-hand side of (2) depends on the maximum of the elements of $\mathcal{A}$, unlike the right-hand side of (1).

The next result follows from Theorem 3 by noticing that if x^k is a positive integer in $\{2, \ldots, N\}$, then k is at most equal to $(\log N)/(\log 2)$.

COROLLARY 1. *Let $\mathcal{A}$ be a set of positive integers at most equal to N. If $aa' + 1$ is a perfect power for all distinct integers a and a' in $\mathcal{A}$, then we have*

$$|\mathcal{A}| < 177000\left(\frac{\log N}{\log\log N}\right)^2. \tag{3}$$

Corollary 1 slightly refines Theorem 1 of [6], where the upper bound

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

is proved, instead of (3).

In Theorem 3, we make the strong assumption that $aa' + 1$ is *always* a power. Our method also provides new results under the weaker assumption that $aa' + 1$ is a power for *many* pairs (a, a') in $\mathcal{A}^2$. For any integer $k \geq 3$, set

$$W_k = \{x^\ell : x \in \mathbb{Z}^+ \text{ and } 3 \leq \ell \leq k\},$$

and, if $k \geq 4$, define

$$X_k = \{x^\ell : x \in \mathbb{Z}^+ \text{ and } 4 \leq \ell \leq k\}.$$

THEOREM 4. *Let $k \geq 3$ be an integer. Let $\mathcal{A}$ and $\mathcal{B}$ be two sets of positive integers. If $ab + 1$ is in W_k for at least $15(\max\{|\mathcal{A}|, |\mathcal{B}|\})^{5/3}$ pairs (a, b) with a in $\mathcal{A}$ and b in $\mathcal{B}$, then*

$$\max\{|\mathcal{A}|, |\mathcal{B}|\} < \left(\frac{k}{\log k}\right)^6.$$

If $k \geq 4$ and if there exists $\alpha > 3/2$ such that $ab+1$ is in X_k for at least $(\max\{|\mathcal{A}|, |\mathcal{B}|\})^\alpha$ pairs (a,b) with a in $\mathcal{A}$ and b in $\mathcal{B}$, then

$$\max\{|\mathcal{A}|, |\mathcal{B}|\} < c(\alpha)\left(\frac{k}{\log k}\right)^{2/(2\alpha-3)},$$

for a suitable constant $c(\alpha)$, depending only on α.

Erdős [4] and Moser [12] posed the following additive analogue of the problem of Diophantus: Is it true that, for all m, there are integers $a_1 < a_2 < \cdots < a_m$ such that $a_i + a_j$ is a perfect square for all $i \neq j$? Rivat, Sárközy and Stewart [10] proved that, if $\mathcal{A}$ is contained in $\{1, 2, \ldots, N\}$ and $a + a'$ is a perfect square for all $a, a' \in \mathcal{A}$ with $a \neq a'$, then $|\mathcal{A}| \ll \log N$. We can also investigate what happens if the sums $a + a'$ are replaced by other polynomials in a and a', and perfect squares by higher powers (see, e.g., Gyarmati, Sárközy and Stewart [7]). First we study the case of $a - a'$. For a given integer $k \geq 3$ and an arbitrary set $\mathcal{A}$ of distinct positive integers, the set

$$\{(a, a') : \ a, a' \in \mathcal{A}, \ a > a', \ a - a' \ \text{ is a } k\text{-th power}\}$$

has at most $0.25\,|\mathcal{A}|^2$ elements, since the related graph (the graph whose vertices are the elements of $\mathcal{A}$ and two vertices are joined if, and only if, their difference is a k-th power) does not contain a triangle (apply Lemma 3 below). Indeed, otherwise we would have three elements a_1, a_2, a_3 in $\mathcal{A}$ such that $a_1 - a_2 = x^k$, $a_2 - a_3 = y^k$, $a_3 - a_1 = z^k$ for some integers x, y, z, and so $x^k + y^k + z^k = 0$. By Fermat's Last Theorem [13] this is not possible.

So far, we have studied problems for which shifted products $aa' + 1$ are perfect powers for many pairs (a, a') in $\mathcal{A}^2$. Theorem 5 below deals with the polynomial $a^2 + {a'}^2$.

Theorem 5. *There exists a positive integer N_0 with the following property: For any integer $N \geq N_0$ and any set $\mathcal{A}$ contained in $\{1, 2, \ldots, N\}$ such that $a^2 + {a'}^2$ is a perfect square for all $a, a' \in \mathcal{A}$, $a \neq a'$, we have $|\mathcal{A}| \leq 4(\log N)^{1/2}$.*

The remainder of the paper is organized as follows. Section 3 is devoted to auxiliary results taken from [2] and to classical results from graph theory. Proofs of Theorems 1–4 are given in Section 4, whereas Theorem 5 is established in Section 5.

3. Auxiliary results

We shall need the following lemmas, extracted from [2]. Their proofs rest heavily on Baker's theory of linear forms in logarithms.

LEMMA 1. *Assume that the integers* $0 < a < b < c < d_1 < \cdots < d_m$ *are such that* $ad_i + 1$, $bd_i + 1$ *and* $cd_i + 1$ *are perfect cubes for any* $1 \leq i \leq m$. *Then we have* $m \leq 6$.

Proof. This is [2, Theorem 3]. □

LEMMA 2. *Let* $k \geq 4$ *be an integer. Assume that the integers* $0 < a < b < c_1 < \cdots < c_m$ *are such that* $ac_i + 1$ *and* $bc_i + 1$ *are perfect* k*-th powers for any* $1 \leq i \leq m$. *Then there exists an effectively computable constant* $C_1(k)$ *depending only on* k, *such that* $m \leq C_1(k)$. *More precisely, we may take* $C_1(4) = 3$, $C_1(k) = 2$ *for* $5 \leq k \leq 176$, $C_1(k) = 1$ *for* $177 \leq k$.

Proof. This is [2, Theorems 1 and 2]. □

We further need two results from graph theory. Throughout this paper, for a graph G, we denote by $v(G)$ the number of its vertices and by $e(G)$ the number of its edges.

LEMMA 3. *Let* G *be a graph on* n *vertices having at least*

$$\frac{r-2}{2(r-1)}\, n^2$$

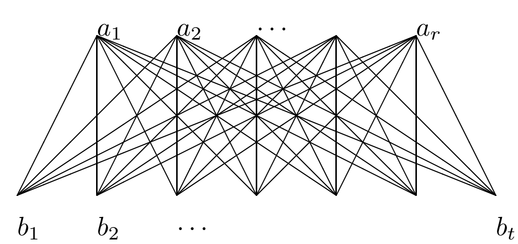
edges for some positive integer $r \geq 3$. *Then* G *contains a complete subgraph on* r *edges.*

Proof. This is a consequence of Turán's graph theorem (see, for example, [1, p. 294, Theorem 1.1]) combined with the upper bound

$$\sum_{0 \leq i < j < r-1} \left[\frac{n+i}{r-1}\right] \left[\frac{n+j}{r-1}\right] \leq \frac{r-2}{2(r-1)}\, n^2,$$

which follows from the method of Lagrange multipliers. □

LEMMA 4. *Assume that* $G(V_1, V_2)$ *is a bipartite graph with* $|V_1| = n \leq |V_2| = m$, *and the vertices are labelled by positive real numbers. Suppose that* $G(V_1, V_2)$ *does not contain a* $K_{r,t}$ *subgraph* G_0 *of the form*

$G_0 =$ 

with $a_i < b_j$ *for all* $1 \le i \le r$, $1 \le j \le t$ *(where the a's belong to* V_1 *and the b's belong to* V_2 *or vice versa). Then* G *has at most*

$$e(G) \le 2(t-1)^{1/r} m n^{1-1/r} + 2(r-1)m$$

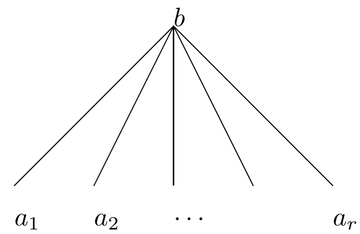
edges.

Proof. The proof is very similar to that of the Kővári–Sós–Turán theorem [8]. For any vertex x, set

$$d_x = \left|\{y \in v(G) :\ y < x,\ (x, y) \text{ is an edge in } G\}\right|,$$

$e_1 = \sum_{x \in V_1} d_x$ and $e_2 = \sum_{x \in V_2} d_x$. Then we have $e(G) = e_1 + e_2$. First we get an upper bound for e_1.

Denote by H the number of subgraphs G_1 of G of the form

$G_1 =$ 

with $b \in V_1$, $a_i \in V_2$ and $b > a_i$ for $1 \le i \le r$. Since the graph G does not contain G_0 we have

$$H \le (t-1)\binom{m}{r}, \tag{4}$$

by Dirichlet's *Schubfachprinzip*. We further have

$$H = \sum_{x \in V_1} \binom{d_x}{r}$$

and, by the Cauchy-Schwarz inequality, we get

$$H \ge n \binom{e_1/n}{r} \tag{5}$$

Combining (4) and (5) yields

$$e_1 \le (t-1)^{1/r} m n^{1-1/r} + (r-1)n,$$

and, similarly, exchanging the roles of V_1 and V_2 in the definition of G_1 ($b \in V_2$, $a_i \in V_1$ and $b > a_i$ for $1 \le i \le r$), we obtain

$$e_2 \le (t-1)^{1/r} n m^{1-1/r} + (r-1)m.$$

It then follows that

$$\begin{aligned} e(G) = e_1 + e_2 &\le 2\max\{(t-1)^{1/r} m n^{1-1/r},\ (t-1)^{1/r} n m^{1-1/r}\} + 2(r-1)m \\ &\le 2(t-1)^{1/r} m n^{1-1/r} + 2(r-1)m, \end{aligned}$$

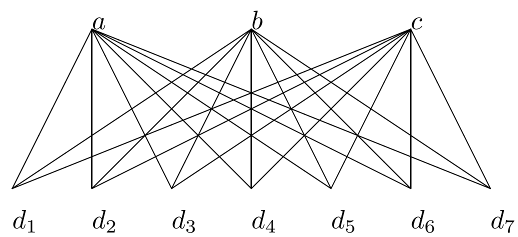
which completes the proof of the lemma. □

4. Proofs of Theorems 1–4

Proof of Theorem 1. Let $k \geq 2$ be an integer. Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_m$ denote the elements of $\mathcal{A}$ and $\mathcal{B}$, respectively. We define a graph G on the $n+m$ vertices $v_1, \ldots, v_{n+m}$ in the following way. For any integers i and j with $1 \leq i \leq n$ and $1 \leq j \leq m$, an edge joins the vertices v_i and v_{n+j} if, and only if, $a_i b_j + 1$ is a perfect k-th power. No edge joins two vertices v_i and v_j if either $1 \leq i, j \leq n$ or $n+1 \leq i, j \leq n+m$.

For $k = 3$, Lemma 1 implies that G does not contain a subgraph G_0 defined by

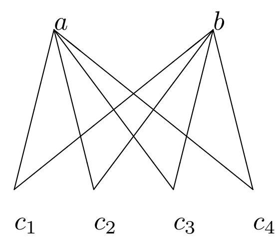
$G_0 =$



with $a < b < c < d_i$ for $1 \leq i \leq 7$.

When $k \geq 4$, Lemma 2 implies that the graph G does not contain a subgraph G_0 defined by

$G_0 =$



with $a < b < c_i$ for $1 \leq i \leq 4$.

These two remarks combined with Lemma 4 give Theorem 1. □

Proof of Theorem 2. Let $a_1, a_2, \ldots, a_n$ denote the elements of $\mathcal{A}$. We define a graph G on n vertices $v_1, \ldots, v_n$ as in the proof of Theorem 1. For any integers i and j with $1 \leq i < j \leq n$, an edge joins the vertices v_i and v_j if, and only if, $a_i a_j + 1$ is a square. By Dujella's result [3] recalled in the Introduction, the graph G does not contain K_6 as a subgraph. Lemma 3 then implies that G has at most $0.4n^2 = 0.4\,|\mathcal{A}|^2$ edges. This proves Theorem 2. □

Proof of Theorem 3. The proof of Theorem 3 is very similar to that of Theorem 2 from [6]. However, instead of introducing the sets $\mathcal{A}_m$ as in [6], we use Theorem 1 and we work directly with the complete graph G labelled by the elements of $\mathcal{A}$. We colour the edge joining the vertices a and a' by the smallest integer ℓ larger than one for which $aa'+1$ is a perfect ℓ-th power. Thus, each edge is coloured by a prime number. For $i = 2, 3, \dots, k$, let b_i denote the number of edges of G which are coloured with the integer i. Set $n = |\mathcal{A}|$ and assume that $n \geq 85000(k/\log k)^2$. By Theorem 2, we have $b_2 \leq 0.4n^2$. Thus $k \geq 3$ and

$$b_3 + \cdots + b_k \geq \frac{n(n-1)}{2} - \frac{2n^2}{5} = \frac{n^2}{10} - \frac{n}{2}.$$

Furthermore, we infer from Theorem 1 that $b_3 \leq 7.64n^{5/3}$. Consequently, we have $k \geq 5$. By Corollary 2 of Rosser and Schoenfeld [11], the number of prime numbers up to k is at most $(5k)/(4\log k)$. Thus, there exists a prime number p with $5 \leq p \leq k$ such that

$$b_p \geq \frac{4\log k}{5k}\left(\frac{n^2}{10} - \frac{n}{2} - 7.64n^{5/3}\right) \geq 5.5n^{3/2},$$

since $n > 85000(k/\log k)^2$. Let G_p be the subgraph of G whose vertices are those of G and whose edges are the edges of G coloured by the prime p. Theorem 1 implies that $b_p \leq 5.47n^{3/2}$, which is the desired contradiction. □

Proof of Theorem 4. Let $k \geq 3$ be an integer. Let $a_1, \dots, a_n$ and $b_1, \dots, b_m$ denote the elements of $\mathcal{A}$ and $\mathcal{B}$, respectively. For simplicity, we assume that $m \geq n$. We define a graph G on the $n+m$ vertices $v_1, \dots, v_{n+m}$ in the following way. No edge joins two vertices v_i and v_j if either $1 \leq i, j \leq n$ or $n+1 \leq i, j \leq n+m$. For any integers i and j with $1 \leq i \leq n$ and $1 \leq j \leq m$, an edge joins the vertices v_i and v_{n+j} if, and only if, $a_i b_j + 1$ is a perfect cube or a higher power. We colour it with the smallest integer ℓ at least equal to 3 such that $ab+1$ is a perfect ℓ-th power. Observe that each edge is coloured by 4 or by an odd prime number. For any integer $i = 3, \dots, k$, denote by b_i the number of edges of G which are coloured by the integer i. Denoting by N the number of edges of G, we have

$$b_3 + \cdots + b_k = N.$$

By Theorem 1, we have $b_3 \leq 7.64\ m^{5/3}$. Since, by assumption, N is greater than $15\ m^{5/3}$, we get

$$b_4 + \cdots + b_k = N - b_3 \geq 7.36\ m^{5/3}.$$

Arguing now as in [6] and in the proof of Theorem 3, we infer that there exists an integer p with $4 \leq p \leq k$ such that

$$b_p \geq \left(\frac{4\log k}{5k}\right) 7.36\ m^{5/3} > 5.88\ m^{5/3}\frac{\log k}{k}.$$

By Theorem 1, we have $b_p \leq 5.47\ m^{3/2}$. Hence the desired result follows.

The proof of the second assertion of Theorem 4 follows along the same lines, but in this case we obtain

$$b_4 + \cdots + b_k = N \geq m^{\alpha}.$$

Thus, there exists an integer p with $4 \leq p \leq k$ such that

$$b_p \geq \frac{4 \log k}{5k} m^{\alpha}.$$

By Theorem 1 we have $b_p \leq 5.47 m^{3/2}$. Hence the desired result follows. □

5. Proof of Theorem 5

We begin by proving an auxiliary lemma.

LEMMA 5. *For any sufficiently large integer N and any set $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$ contained in $\{1, 2, \ldots, N\}$, there exists a prime p such that $p \equiv \pm 3 \pmod 8$, p divides at most $[n/3]$ numbers from the set $\mathcal{A}$, and p satisfies*

$$p \leq \frac{3}{\log 1.6} \log N.$$

Proof. We argue by contradiction. Suppose that all prime numbers $p \equiv \pm 3 \pmod 8$ with $p \leq \frac{3}{\log 1.6} \log N$ divide at least $[n/3]$ numbers from the set $\mathcal{A}$. Each of these primes satisfies

$$p^{[n/3]} \mid a_1 a_2 \ldots a_n.$$

Hence we get

$$\Big(\prod_{\substack{p \leq \frac{3}{\log 1.6} \log N \\ p \equiv \pm 3 \pmod 8}} p \Big)^{[n/3]} \mid a_1 a_2 \ldots a_n. \tag{6}$$

It follows from the prime number theorem for arithmetic progressions of small moduli that for all sufficiently large x we have

$$1.6^x < \prod_{p \leq x,\ p \equiv \pm 3 \pmod 8} p.$$

Thus, by (6), we get

$$N^n \leq \Big(1.6^{\frac{3}{\log 1.6} \log N}\Big)^{[n/3]} < \Big(\prod_{\substack{p \leq \frac{3}{\log 1.6} \log N \\ p \equiv \pm 3 \pmod 8}} p \Big)^{[n/3]} \leq a_1 a_2 \ldots a_n \leq N^n,$$

which is a contradiction. □

Let N and $\mathcal{A}$ be as in the statement of Lemma 5, and let p be a prime which satisfies the conclusion of that lemma. Assume that $a^2 + {a'}^2$ is a square for any a, a' in $\mathcal{A}$ with $a \neq a'$. Let us consider the numbers from the set $\mathcal{A}$ which are not divisible by p. These are $b_1, b_2, \ldots, b_t$, $t \geq \lceil 2n/3 \rceil$. If $b_i^2 \equiv b_j^2 \pmod p$ for $i \neq j$, then $b_i^2 + b_j^2 \equiv 2b_i^2$ is a quadratic residue modulo p. Therefore 2 is also a quadratic residue modulo p. But this contradicts the assumption $p \equiv \pm 3 \pmod 8$. Thus $b_1^2, b_2^2, \ldots, b_t^2$ are incongruent modulo p.

We further need the following lemma.

Lemma 6. *Let p be a prime number. Let $\mathcal{B}$ be a set of positive integers coprime with p and whose residues modulo p are all distinct. Assume that for all $b, b' \in \mathcal{B}$ with $b \neq b'$ the number $b + b'$ is a perfect square modulo p. Then we have $|\mathcal{B}| \leq p^{1/2} + 3$.*

Proof of Lemma 6. See [5]. □

We now have all the tools for the proof of Theorem 5. The sum of any two elements of the set $\{b_1^2, b_2^2, \ldots, b_t^2\}$ is a perfect square, so we get by Lemma 5 and Lemma 6 that

$$2n/3 \leq t \leq p^{1/2} + 3 \leq \left(\frac{3}{\log 1.6} \log N \right)^{1/2} + 3.$$

From this we obtain

$$|\mathcal{A}| = n \leq 4(\log N)^{1/2},$$

for N sufficiently large. This completes the proof of Theorem 5. □

References

[1] B. Bollobás, *Extremal graph theory*, London Mathematical Society Monographs, vol. 11, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978. MR 506522 (80a:05120)

[2] Y. Bugeaud and A. Dujella, *On a problem of Diophantus for higher powers*, Math. Proc. Cambridge Philos. Soc. **135** (2003), 1–10. MR 1990827 (2004b:11035)

[3] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214. MR 2039327 (2004m:11037)

[4] P. Erdős, *Quelques problèmes de théorie des nombres*, Monographies de L'Enseignement Mathématique, No. 6, L'Enseignement Mathématique, Université, Geneva, 1963, pp. 81–135. MR 0158847 (28 #2070)

[5] K. Gyarmati, *On a problem of Diophantus*, Acta Arith. **97** (2001), 53–65. MR 1819622 (2002d:11031)

[6] K. Gyarmati, A. Sárközy, and C. L. Stewart, *On shifted products which are powers*, Mathematika **49** (2002), 227–230 (2004). MR 2059056

[7] ———, *On sums which are powers*, Acta Math. Hungar. **99** (2003), 1–24. MR 1973081 (2004c:11191)

[8] T. Kövari, V. T. Sós, and P. Turán, *On a problem of K. Zarankiewicz*, Colloquium Math. **3** (1954), 50–57. MR 0065617 (16,456a)

[9] V. A. Lebesgue. *Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$*, Nouv. Ann. Math **9** (1850), 178–181.

[10] J. Rivat, A. Sárközy, and C. L. Stewart, *Congruence properties of the Ω-function on sumsets*, Illinois J. Math. **43** (1999), 1–18. MR 1665708 (99m:11112)

[11] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94. MR 0137689 (25 #1139)

[12] W. Sierpiński, *A selection of problems in the theory of numbers*, Translated from the Polish by A. Sharma. A Pergamon Press Book, The Macmillan Co., New York, 1964. MR 0170843 (30 #1078)

[13] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), 443–551. MR 1333035 (96d:11071)

Yann Bugeaud, Université Louis Pasteur, U. F. R. de mathématiques, 7, rue René Descartes, 67084 Strasbourg, France

E-mail address: bugeaud@math.u-strasbg.fr

Katalin Gyarmati, University Eötvös Lorand, Algebra and Number Theory Department, Pázmány Péter sétány 1/c, H-1117 Budapest, Hungary

E-mail address: gykati@cs.elte.hu