On shifted products which are powers

K. Gyarmati, A. Sárközy[1] and C. L. Stewart[2]

1 Introduction

Fermat gave the first example of a set of four positive integers $\{a_1, a_2, a_3, a_4\}$ with the property that $a_i a_j + 1$ is a square for $1 \leq i < j \leq 4$. His example was $\{1, 3, 8, 120\}$. Baker and Davenport [1] proved that the example could not be extended to a set of 5 positive integers such that the product of any two of them plus one is a square. Kangasabapathy and Ponnudurai [6], Sansone [9] and Grinstead [4] gave alternative proofs. The construction of such sets originated with Diophantus who studied the problem when the a_i's are rational numbers. It is conjectured that there do not exist five positive integers such that their pairwise products are all one less than the square of an integer. Recently Dujella [3] proved that there do not exist nine such integers. In this note we address the following related problem. Let V denote the set of pure powers, that is the set of positive integers of the form x^k with x and k positive integers and $k > 1$. How large can a set of positive integers A be if $aa' + 1$ is in V whenever a and a' are distinct integers from A? We expect that there is an absolute bound for $|A|$, the cardinality of A. While we have not been able to establish this result, we have been able to prove that such sets cannot be very dense.

Theorem 1 *Let N be a positive integer and let A be a subset of $\{1, \ldots, N\}$ with the property that $aa' + 1$ is in V whenever a and a' are distinct integers from A. There exists a positive real number N_0 such that if N exceeds N_0 then*

$$|A| < 340(\log N)^2 / \log\log N.$$

We shall deduce our result from the theorem below. For each integer k, with k at least 2, define V_k by

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

Theorem 2 *Let k be an integer with $k \geq 2$. Let N be a positive integer and let A be a subset of $\{1, \ldots, N\}$ with the property that $aa' + 1$ is in V_k whenever a and a' are distinct integers from A. There exists a positive real number N_1, such that if N exceeds N_1, then*

$$|A| < 160 \frac{k^2}{(\log k)^2} \log\log N.$$

[1]Research partially supported by the Hungarian National Foundation for Scientific Research, Grant No. T029759.

[2]Research supported in part by the Natural Sciences and Engineering Research Council of Canada, Grant A3528.

Notice that Theorem 1 follows from Theorem 2 on observing that if x^k is a positive integer from $\{2, \ldots, N\}$ then k is at most $(\log N)/\log 2$.

The proof of Theorem 2 depends upon a simple gap principle, the result of Dujella and two results from extremal graph theory.

2 Preliminary lemmas

Lemma 1 *Let k be an integer with $k \geq 2$ and let a, b, x and y be positive integers with $a < b$ and $x < y$. If $ax+1,\ ay+1,\ bx+1$ and $by+1$ are k-th powers then*

$$yb > (xa)^{k-1}.$$

Proof. This follows from the proof of Theorem 1 of [5].

Lemma 2 *(Turán's Theorem) Let n and r be positive integers with $r \geq 2$ and let G be a graph with n vertices. If the number of edges in G exceeds*

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

then G contains a complete graph of order r.

Proof. This is Theorem 1.1, Chapter VI of [2], see also [10].

Lemma 3 *Let G be a graph with $n(\geq 1)$ vertices and m edges and suppose that*

$$m > \frac{1}{2}\left(n^{\frac{3}{2}} + n - n^{\frac{1}{2}}\right).$$

Then G contains a cycle of length 4.

Proof. This is a special case of Theorem 2.3, Chapter VI of [2] and is due to Kövári, Sós and Turán [7].

3 Proof of Theorem 2

We shall suppose that

$$|A| \geq 160(k/\log k)^2 \log\log N,$$

and show that this leads to a contradiction. For N sufficiently large there is an integer m with $1 \leq m \leq 1+(\log(\log N/\log 2))/\log 2$ such that A has more than $110(k/\log k)^2$ elements from $\{2^{2^m}, 2^{2^m}+1, \ldots, 2^{2^{m+1}}-1\}$. Let us denote the set of these elements by A_m and put $n = |A_m|$. Then

$$n > 110(k/\log k)^2. \tag{1}$$

Form the complete graph G whose vertices are the elements of A_m. Next, colour the edges between two vertices a and a' by the smallest integer ℓ larger than one for which $aa'+1$ is a perfect ℓ-th power. Note that each edge is coloured by a prime number.

For $i = 2, 3, \ldots, k$ let b_i denote the number of edges of G which are coloured with the integer i. It now follows readily from the method of Lagrange multipliers that

$$\sum_{0 \le i < j < 8} \left[\frac{n+i}{8}\right]\left[\frac{n+j}{8}\right] \le \binom{8}{2}\left(\frac{n}{8}\right)^2 = \frac{7}{16}n^2$$

and so, by Lemma 2, if b_2 exceeds $7n^2/16$ there is a complete graph on 9 vertices coloured with the integer 2. But Dujella [3] has proved that there do not exist 9 such positive integers. Accordingly,

$$b_3 + \ldots + b_k \ge \binom{n}{2} - \frac{7}{16}n^2 = \frac{n^2}{16} - \frac{n}{2}.$$

By Corollary 2 of Rosser and Schoenfeld [8], the number of primes up to k is at most $5k/4\log k$. Thus, there exists a prime p with $3 \le p \le k$ such that

$$b_p \ge \frac{4\log k}{5k}\left(\frac{n^2}{16} - \frac{n}{2}\right). \tag{2}$$

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. By (1),

$$\frac{4\log k}{5k}\left(\frac{n^2}{16} - \frac{n}{2}\right) = \frac{\log k}{k}\,\frac{n^2}{20}\left(1 - \frac{8}{n}\right) > n^{\frac{3}{2}}\frac{\sqrt{110}}{20}\left(1 - \frac{8}{110}\left(\frac{\log 3}{3}\right)^2\right) > .519n^{\frac{3}{2}}. \tag{3}$$

Further,

$$\frac{1}{2}\left(n^{\frac{3}{2}} + n - n^{\frac{1}{2}}\right) < \frac{1}{2}n^{\frac{3}{2}}\left(1 + \frac{1}{\sqrt{n}}\right) < \frac{1}{2}n^{\frac{3}{2}}\left(1 + \frac{1}{\sqrt{110}}\,\frac{\log 3}{3}\right) < .518n^{\frac{3}{2}}. \tag{4}$$

Therefore, by (2), (3) and (4),

$$b_p > \frac{1}{2}\left(n^{\frac{3}{2}} + n - n^{\frac{1}{2}}\right),$$

whence, by Lemma 3, there is a cycle of length 4 in G_p. In particular, there exist integers a, b, x, y which are vertices of G_p with a and b both connected by edges to x and y. Without loss of generality, we may assume that $a < b$ and $x < y$. Then $ax+1$, $bx+1$, $ay+1$ and $by+1$ are p-th powers and so, by Lemma 1,

$$yb > (xa)^{p-1} \ge (xa)^2. \tag{5}$$

But a, b, x and y are in $\{2^{2^m}, \ldots, 2^{2^{m+1}} - 1\}$ hence

$$yb < \left(2^{2^{m+1}} - 1\right)^2 < 2^{2^{m+2}} \le (xa)^2$$

which contradicts (5). The result now follows.

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, *London Mathematical Society Monographs No. 11, Academic Press, London, New York, San Francisco* (1978).

[3] A. Dujella, An absolute bound for the size of Diophantine m-tuples, *Acta Arith.*, to appear.

[4] C.M. Grinstead, On a method of solving a class of Diophantine equations, *Math. Comp.* **32** (1978), 936–940.

[5] K. Gyarmati, On a problem of Diophantus, *Acta Arith.*, to appear.

[6] P. Kangasabapathy and T. Ponnudurai, The simultaneous Diophantine equations $y^2 - 3x^2 = -2$ and $z^2 - 8x^2 = -7$, *Quart. J. Math. Oxford Ser. (2)* **26** (1975), 275–278.

[7] P. Kövári, V. Sós and P. Turán, On a problem of K. Zarankiewicz, *Colloq. Math.* **3** (1954), 50-57.

[8] J. Barkley Rosser and Lowell Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* (1962), 64–94.

[9] G. Sansone, El sistema diofanteo $N + 1 = x^2,\ 3N + 1 = y^2,\ 8N + 1 = z^2$, *Ann. Mat. Pura Appl. (4)* **111** (1976), 125–151.

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

K. Gyarmati and A. Sárközy
Department of Algebra and Number Theory
University Eötvos Loránd
H-1053 Budapest
Hungary
email: gykati@cs.elte.hu
sarkozy@cs.elte.hu

C.L. Stewart
Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario
Canada
N2L 3G1
email: cstewart@watserv1.uwaterloo.ca