ON POWERS IN SHIFTED PRODUCTS

K. Gyarmati and C.L. Stewart
Alfred Rényi Institute of Mathematics, Hungary
University of Waterloo, Canada

Abstract. In this note we give an estimate for the size of a subset A of $\{1, \dots, N\}$ which has the property that the product of any two distinct elements of A plus 1 is a perfect power.

1. Introduction

Let V denote the set of all positive integers which are of the form x^k with x and k integers and k at least 2. Thus V is the set of positive integers which are perfect powers. In [6] Gyarmati, Sárközy and Stewart showed that if N is a positive integer and A is a subset of $\{1, \dots, N\}$ with the property that $aa' + 1$ is in V whenever a and a' are distinct elements of A then $|A|$, the cardinality of A, is not large. In particular, they showed that for N sufficiently large

$$|A| \leq 340(\log N)^2 / \log\log N. \tag{1.1}$$

In addition they conjectured that $|A|$ is bounded by an absolute constant. In [8] Luca showed that this follows as a consequence of the *abc* conjecture. Further he improved on (1.1) by showing that there is a positive number c_0 such that for N sufficiently large

$$|A| < c_0(\log N / \log\log N)^{3/2}. \tag{1.2}$$

Estimate (1.1) was proved by combining results from extremal graph theory with a gap principle due to Gyarmati [5] which allows one to push apart integers whose shifted product is a fixed power. The improvement (1.2) of Luca was due to his more efficient treatment of the large powers which might occur. He introduced estimates for linear forms in the logarithms of algebraic

2000 *Mathematics Subject Classification.* 11B75, 11D99.
Key words and phrases. perfect powers, extremal graph theory.

numbers into his argument to this end. The linear forms Luca considers consist of 4 terms. The purpose of this note is to show that a further improvement of (1.2) is possible by a modification of Luca's argument which allows one to deal with linear forms in only 2 terms. We shall prove the following result.

THEOREM 1.1. *There exists an effectively computable positive number* c_1 *such that if* N *is a positive integer with* $N \geq 2$ *and* A *is a subset of* $\{1, \dots, N\}$ *with the property that* $aa' + 1$ *is a perfect power whenever* a *and* a' *are distinct integers from* A *then*

$$|A| < c_1 \log N.$$

2. Preliminary lemmas

LEMMA 2.1. *There is no set of six positive integers* $\{a_1, \dots, a_6\}$ *with the property that* $a_i a_j + 1$ *is a square for* $1 \leq i < j \leq 6$.

PROOF. This is Theorem 2 of [4]. □

LEMMA 2.2. *Let* n *and* r *be integers with* $3 \leq r \leq n$. *Let* G *be a graph on* n *vertices with at least*

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

edges. Then G *contains a complete subgraph on* r *edges.*

PROOF. This follows from Turán's graph theorem, see [9] or Lemma 3 of [3]. □

LEMMA 2.3. *Let* G *be a graph with* n (> 1) *vertices and* e *edges and suppose that*

$$e > \frac{1}{2}(n^{3/2} + n - n^{1/2}).$$

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]. □

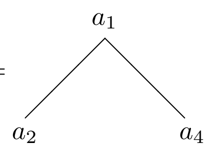
We shall need an extension of Lemma 2.3 to the case when G is a graph of k colours and the cycle of length 4 is coloured in a certain way.

LEMMA 2.4. *Let* G *be a graph with* n *vertices and* e *edges with the edges coloured by* k *colours. Suppose that* G *does not contain a cycle through vertices* a_1, a_2, a_3, a_4 *where the edges from* a_1 *to* a_2 *and from* a_1 *to* a_4 *have the same colour and where the edges from* a_2 *to* a_3 *and from* a_3 *to* a_4 *have the same colour. Then*

$$e \leq k^{1/2} n^{3/2} + kn.$$

PROOF. We will count the number of subgraphs G_0 of G of the form

$G_0 =$



where the edges (a_1, a_2) and (a_1, a_4) are coloured by the same colour. Let the degree of a_i coloured by the j-th colour be $d_{i,j}$. Then the number of subgraphs G_0 is exactly

$$\sum_{i=1}^{n} \sum_{j=1}^{k} \binom{d_{i,j}}{2}.$$

On the other hand this number is less or equal to $\binom{n}{2}$ since for every pair (a_2, a_4) there exists at most one a_1 such that the edges (a_1, a_2) and (a_1, a_4) have the same colour. Thus

$$\sum_{i=1}^{n} \sum_{j=1}^{k} \binom{d_{i,j}}{2} \le \binom{n}{2}.$$

Since $\sum_{i=1}^{n} \sum_{j=1}^{k} d_{i,j} = 2e$ we get

$$\frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{k} d_{i,j}^2 - e \le \frac{n(n-1)}{2}.$$

By the Cauchy-Schwarz inequality

$$\frac{\left(\sum_{i=1}^{n} \sum_{j=1}^{k} d_{i,j}\right)^2}{2kn} - e \le \frac{n(n-1)}{2}$$

and so

$$\frac{2e^2}{kn} - e \le \frac{n(n-1)}{2}.$$

Thus

$$e \le ((4kn^2(n-1) + k^2n^2)^{1/2} + kn)/4$$

and the result now follows. □

LEMMA 2.5. *Let k be an integer with $k \ge 2$ and let a_1, a_2, a_3 and a_4 be positive integers with $a_1 < a_3$ and $a_2 < a_4$. If $a_1a_2 + 1$, $a_1a_4 + 1$, $a_2a_3 + 1$ and $a_3a_4 + 1$ are k-th powers, then*

$$a_3a_4 > (a_1a_2)^{k-1}.$$

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

For any non-zero rational number α, where $\alpha = a/b$ with a and b coprime integers, we put $H(\alpha) = \max\{|a|, |b|\}$.

LEMMA 2.6. *Let b_1 and b_2 be non-zero integers and let α_1 and α_2 be non-zero rational numbers. Put $A_i = \max\{2, H(\alpha_i)\}$ for $i = 1, 2$, $B = \max\{|b_1|, |b_2|, 2\}$ and $\Lambda = b_1 \log \alpha_1 + b_2 \log \alpha_2$ where the logarithms take their principal values. There exists an effectively computable positive constant C such that if $\Lambda \neq 0$ then*

$$|\Lambda| > \exp(-C \log A_1 \log A_2 \log B).$$

PROOF. This follows from the Main Theorem of [1]. ◻

3. PROOF OF THEOREM 1.1

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. We may suppose that

$$|A| > \log N, \tag{3.3}$$

since otherwise our result holds. Let $c_1, c_2, \ldots$ denote effectively computable positive numbers. We shall suppose that N is sufficiently large that

$$(\log N)/2 \log\log N > 16. \tag{3.4}$$

Notice that there is an integer m with

$$1 \leq m \leq \frac{\log((\log N)/\log 2)}{\log 2},$$

such that A has more than $(|A| - 3)/((\log((\log N)/\log 2))/\log 2)$ elements from $\{2^{2^m}, 2^{2^m} + 1, \ldots, 2^{2^{m+1}} - 1\}$. We shall denote these elements by A_m and put $n = |A_m|$ and $M = 2^{2^{m+1}}$. Then, for $N > c_1$,

$$n > \frac{|A|}{2 \log\log N}. \tag{3.5}$$

Further, by (3.3), (3.4) and (3.5),

$$M > 16. \tag{3.6}$$

Form the complete graph G whose vertices are the elements of A_m. G has $\binom{n}{2}$ edges and for each pair (a, a') of vertices of G we colour the edge between a and a' with the smallest prime p for which $aa' + 1$ is a perfect p-th power.

By Lemma 2.2, if the number of edges of G with the colour 2 exceeds $(2/5)n^2$ then there is a complete subgraph of G on 6 vertices coloured with 2 and this is impossible by Lemma 2.1. Therefore the number of edges of G with a colour different from 2 is at least $\binom{n}{2} - (2/5)n^2 = (n^2/10) - (n/2)$.

Put

$$t = (9C \log M \log\log M)^{1/2}, \tag{3.7}$$

where C is the positive number which occurs in Lemma 2.6. Let G_1 be the subgraph of G consisting of the vertices of G together with the edges of G which are coloured with a prime p for which

$$3 \leq p \leq t \tag{3.8}$$

and let G_2 be the subgraph of G consisting of the vertices of G together with the edges of G which are coloured with a prime p for which

$$t < p < (2\log M)/\log 2. \tag{3.9}$$

Suppose that G_1 contains at least $(n^2/20) - (n/2)$ edges. The number of colours of G_1 is $\pi(t) - 1$ and, by the prime number theorem and (3.7), this is at most $c_2((\log M)/\log\log M)^{1/2}$. Thus there is a colour of G_1 which occurs on at least $((n^2/20) - (n/2))/c_2((\log M)/\log\log M)^{1/2}$ different edges. Since $M \leq N$ we see from (3.5) that if

$$|A| > c_3 \log N, \tag{3.10}$$

then there is a colour associated with more than $(n^{3/2} + n - n^{1/2})/2$ edges. Therefore, by Lemma 2.3, G_1 contains a monochromatic cycle of length 4. In particular, there exist integers $a_1,\ a_2,\ a_3$ and a_4 from A_m and a prime p satisfying (3.8) for which $a_1a_2 + 1,\ a_2a_3 + 1,\ a_3a_4 + 1$ and $a_1a_4 + 1$ are p-th powers. Without loss of generality one may suppose that $a_1 < a_3$ and $a_2 < a_4$. Thus, by Lemma 2.5,

$$a_3a_4 > (a_1a_2)^2. \tag{3.11}$$

But $a_1,\ a_2,\ a_3$ and a_4 are in $\{2^{2^m}, \ldots, 2^{2^{m+1}} - 1\}$ and so

$$a_3a_4 < 2^{2^{m+2}} \leq (a_1a_2)^2,$$

which contradicts (3.11). Accordingly either (3.10) is false, in which case our result follows, or G_1 has fewer than $(n^2/20) - (n/2)$ edges. We may assume the latter possibility and so G_2 has at least $n^2/20$ edges.

It follows from (3.6), (3.9) and the prime number theorem that the number of colours of G_2 is at most $c_4(\log M)/\log\log M$. Therefore since $N \geq M$ and (3.5) holds, if $|A|$ exceeds $c_5 \log N$ then by Lemma 2.4, G_2 contains a cycle through vertices $a_1,\ a_2,\ a_3$ and a_4 for which the edge between a_1 and a_2 and the edge between a_1 and a_4 have the same colour and the edge between a_2 and a_3 and the edge between a_3 and a_4 have the same colour. In particular, there exist primes p_1 and p_2 in the range given by (3.9) and integers $x_1,\ x_2,\ x_3$ and x_4 for which

$$a_1a_2 + 1 = x_1^{p_1}, \quad a_2a_3 + 1 = x_2^{p_2},$$
$$a_3a_4 + 1 = x_3^{p_2}, \quad a_4a_1 + 1 = x_4^{p_1}.$$

We observe, as in Lemma 3.1 of [8], that

$$(x_1^{p_1} - 1)(x_3^{p_2} - 1) = (x_2^{p_2} - 1)(x_4^{p_1} - 1),$$

hence

$$x_1^{p_1}x_3^{p_2} - x_2^{p_2}x_4^{p_1} = x_1^{p_1} + x_3^{p_2} - x_2^{p_2} - x_4^{p_1}. \tag{3.12}$$

Since $x_1^{p_1} + x_3^{p_2} - x_2^{p_2} - x_4^{p_1} = (a_1 - a_3)(a_2 - a_4)$ and since the a_i's are distinct we see that

$$x_1^{-p_1}x_3^{-p_2}x_2^{p_2}x_4^{p_1} \neq 1.$$

Thus, if we put

$$\Lambda = p_1 \log(x_4/x_1) + p_2 \log(x_2/x_3) \tag{3.13}$$

we see that $\Lambda \neq 0$. We may assume, without loss of generality, that

$$x_1^{p_1} = \max\{x_1^{p_1}, x_2^{p_2}, x_3^{p_2}, x_4^{p_1}\}.$$

Therefore, by (3.12),

$$\left| \frac{x_2^{p_2}x_4^{p_1}}{x_1^{p_1}x_3^{p_2}} - 1 \right| \leq \frac{2}{x_3^{p_2}}. \tag{3.14}$$

Since a_3 and a_4 are at least $M^{1/2}$ in size

$$x_3^{p_2} > M,$$

and so, by (3.13) and (3.14),

$$\left| e^{\Lambda} - 1 \right| < \frac{2}{M}.$$

Observe that if y is a real number and $|e^y - 1| < 1/8$ then $|y| < 1/2$. Further $|e^y - 1| \geq |y|/2$ for $|y| < 1/2$ and so, since $M \geq 16$,

$$|\Lambda| < \frac{4}{M},$$

whence

$$\log|\Lambda| < -\frac{1}{2}\log M. \tag{3.15}$$

We now apply Lemma 2.6 with $\alpha_1 = x_1/x_4$, $\alpha_2 = x_2/x_3$ and $B = \max(p_1, p_2, 2)$. Note that, for $i = 1, 2$,

$$\log H(\alpha_i) \leq (2\log M)/t.$$

By Lemma 2.6,

$$\log|\Lambda| > -4C((\log M)/t)^2 \log\log M,$$

and so, by (3.15),

$$t^2 < 8C \log M \log\log M.$$

However, this contradicts our choice of t in (3.7). Accordingly $|A|$ is less than $c_5 \log N$ and the result follows.

Acknowledgements.

The research of C.L. Stewart was supported in part by the Canada Research Chairs Program and by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

References

[1] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties,* J. reine angew. Math. **442** (1993), 19–62.

[2] B. Bollobás, Extremal Graph Theory, London Mathematical Society Monographs No. 11, Academic Press, London, New York, San Francisco, 1978.

[3] Y. Bugeaud and K. Gyarmati, *On generalizations of a problem of Diophantus,* Illinois J. Math. **48** (2004), 1105–1115.

[4] A. Dujella, *There are only finitely many Diophantine quintuples,* J. reine angew. Math. **566** (2004), 183–214.

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

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

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

[8] F. Luca, *On shifted products which are powers,* Glasnik Math. **40** (2005), 13–20.

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

K. Gyarmati
Alfréd Rényi Institute of Mathematics
13-15 Reáltanoda u. 1053 Budapest
Hungary
E-mail: gykati@renyi.hu

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