ON POWERS IN SHIFTED PRODUCTS

K. GYARMATI AND C. L. STEWART
Alfred Rényi Institute of Mathematics, Hungary and University of Waterloo, Canada

Abstract. In this note we give an estimate for the size of a subset \( A \) of \( \{1, \ldots, N\} \) 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 \( \{1, \ldots, N\} \) 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

\[
|A| \leq 340(\log N)^2 / \log \log N.
\]

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

\[
|A| < c_0(\log N / \log \log N)^{3/2}.
\]

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

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

Research partially supported by Hungarian National Foundation for Scientific Research, Grants K49693 and K67676.
occur. He introduced estimates for linear forms in the logarithms of algebraic 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 \( \{1, \ldots, N\} \) 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 \( \{a_1, \ldots, a_6\} \) with the property that \( a_ia_j + 1 \) is a square for \( 1 \leq i < j \leq 6 \).

**Proof.** This is [4, Theorem 2].

**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 [3, Lemma 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 [2, Theorem 2.3, Chapter VI] and is due to Kővári, 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

$$G_0 = \begin{array}{c}
\vdots \\
\downarrow \\
\vdots
\end{array}$$

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

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

On the other hand this number is less or equal to $\left( \frac{n}{2} \right)^2$ 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

$$\sum_{i=1}^{n} \sum_{j=1}^{k} \left( \frac{d_{i,j}}{2} \right) \leq \left( \frac{n}{2} \right)^2.$$

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

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

By the Cauchy-Schwarz inequality

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

and so

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

Thus

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

and the result now follows.

**Lemma 2.5.** Let $k$ be an integer with $k \geq 2$ 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 [5, Theorem 1].
For any non-zero rational number \( \alpha \), 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 \( \alpha_1 \) and \( \alpha_2 \) 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]. \( \square \)

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

\[ |A| > \log N, \]

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

\[ (\log N)/2 \log \log N > 16. \]

Notice that there is an integer \( m \) with

\[ 1 \leq m \leq \log((\log N)/2) \log 2, \]

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

\[ n > \frac{|A|}{2 \log \log N}. \]

Further, by (3.1), (3.2) and (3.3),

\[ M > 16. \]

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

\[ t = (9C \log M \log \log M)^{1/2}, \]
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
\[(3.6)\quad 3 \leq p \leq t\]
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
\[(3.7)\quad t < p < (2 \log M)/\log 2.\]
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 (3.5), 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 $M \leq N^2$ we see from (3.3) that if
\[(3.8)\quad |A| > c_3 \log N,\]
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 (3.6) 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,
\[(3.9)\quad a_3a_4 > (a_1a_2)^2.\]
But $a_1, a_2, a_3$ and $a_4$ are in $\{2^m, \ldots, 2^{2m+1} - 1\}$ and so
\[a_3a_4 < 2^{m+2} \leq (a_1a_2)^2,\]
which contradicts (3.9). Accordingly either (3.8) 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 (3.4), (3.7) 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 $N^2 \geq M$ and (3.3) 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 (3.7) and integers $x_1, x_2, x_3$ and $x_4$ for which
\[a_1a_2 + 1 = x_1^{p_1}, \quad a_2a_3 + 1 = x_2^{p_2}, \quad a_3a_4 + 1 = x_3^{p_2}, \quad a_4a_1 + 1 = x_4^{p_1}.\]
We observe, as in [8, Lemma 3.1], that
\[(x_1^{p_1} - 1)(x_3^{p_2} - 1) = (x_2^{p_2} - 1)(x_4^{p_1} - 1),\]
hence

\[ x_1^{p_1} x_3^{p_2} - x_2^{p_2} x_4^{p_1} = x_1^{p_1} + x_3^{p_2} - x_2^{p_2} - x_4^{p_1}. \]

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

\[ \Lambda = p_1 \log(x_4/x_1) + p_2 \log(x_2/x_3) \]

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 (3.10),

\[ \left| \frac{x_2^{p_2} x_4^{p_1}}{x_1^{p_1} x_3^{p_2}} - 1 \right| \leq \frac{2}{x_3^{p_2}}. \]

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

\[ x_3^{p_2} > M, \]

and so, by (3.11) and (3.12),

\[ |e^\Lambda - 1| < \frac{2}{M}. \]

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

\[ \log |\Lambda| < -\frac{1}{2} \log M. \]

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 (3.13),

\[ t^2 < 8C \log M \log \log M. \]

However, this contradicts our choice of \( t \) in (3.5). Accordingly \( |\Lambda| \) 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


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

Received: 8.6.2006.