Available online at www.sciencedirect.com

ScienceDirect

Journal of Combinatorial Theory, Series A 115 (2008) 662–673

Journal of Combinatorial Theory Series A

www.elsevier.com/locate/jcta

On sets of integers whose shifted products are powers ☆

C.L. Stewart

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

Received 15 March 2007

Available online 27 September 2007

Abstract

Let N be a positive integer and let A be a subset of $\{1, \dots, N\}$ with the property that $aa' + 1$ is a pure power whenever a and a' are distinct elements of A. We prove that $|A|$, the cardinality of A, is not large. In particular, we show that $|A| \ll (\log N)^{2/3} (\log \log N)^{1/3}$.

Keywords: Pure powers; Extremal graph theory; Linear forms in logarithms

1. Introduction

Diophantus initiated the study of sets of positive rational numbers with the property that the product of any two of them is one less than the square of a rational number. For instance, he found the set $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$. Fermat was apparently the first to find a set of four positive integers with the property that the product of any two of the integers plus one is a square. His example was $\{1, 3, 8, 120\}$. Dujella [6] has recently shown that there are no sets of six integers and that there are only finitely many sets of five positive integers with the above property. In [3] Bugeaud and Dujella considered the analogous property with the squares replaced by the set of kth powers. For each integer k larger than one let $C(k)$ denote the largest cardinality of a set of integers for which the product of any two of the integers plus one is a kth power of an integer. They proved that $C(3) \leqslant 7$, $C(4) \leqslant 5$, $C(k) \leqslant 4$ for $5 \leqslant k \leqslant 176$ and that $C(k) \leqslant 3$ for $k > 176$.

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 $k > 1$. In [9], Gyarmati, Sárközy and Stewart asked how large a set

☆ This research was supported in part by the Canada Research Chairs Program and by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

E-mail address: cstewart@uwaterloo.ca.

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2007.07.010

of positive integers A can be if $aa' + 1$ is in V whenever a and a' are distinct elements of A. They conjectured that there is an absolute bound for $|A|$ and recently Luca [12] has shown that this follows as a consequence of the abc conjecture. While Gyarmati, Sárközy and Stewart could not establish an absolute bound for $|A|$ they were able to show that $|A|$ cannot be very dense. In particular, they proved 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 integers from A then, for N sufficiently large,

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

The proof of (1) depends on a gap principle, the result of Dujella and two results from extremal graph theory. By means of an improved gap principle, which depends on the work in [3], Bugeaud and Gyarmati [4] proved that for N sufficiently large, (1) may be replaced with

$$|A| < 177\,000 \left(\frac{\log N}{\log\log N} \right)^2.$$

Recently Luca [12] introduced estimates for linear forms in the logarithms of rational numbers into the mix to efficiently treat the large powers which might occur and as a consequence he has shown that there is a positive number c_0 such that for N sufficiently large

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

The linear forms which Luca employs consist of 4 terms. In [8] Gyarmati and Stewart introduced a modification of Luca's argument which allows one to deal with linear forms in only 2 terms. They were able to prove that there is a positive number c_1 such that for N sufficiently large

$$|A| < c_1 \log N. \tag{3}$$

Somewhat earlier, Dietmann, Elsholtz, Gyarmati and Simonovits [5] had proved that for N sufficiently large

$$|A| < 8000 \frac{\log N}{\log\log N}, \tag{4}$$

under the additional assumption that any two terms of the form $aa' + 1$ are coprime.

Our objective in this note is to establish the following improvement of (3) and (4).

Theorem. *Let N be an integer with $N \geqslant 3$ and let A be a subset $\{1, \ldots, N\}$ with the property that $aa' + 1$ is in V whenever a and a' are distinct integers from A. There exists an effectively computable positive real number c such that*

$$|A| < c(\log N)^{2/3} (\log\log N)^{1/3}. \tag{5}$$

We shall follow Luca [12] and Gyarmati and Stewart [8] by making use of estimates for linear forms in the logarithms of rational numbers in order to treat the large powers. For powers of intermediate size we appeal to an estimate for simultaneous linear forms in the logarithms of algebraic numbers due to Loxton [11]. As in [9] we shall also employ a gap principle and results from extremal graph theory.

2. Preliminary lemmas

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

Proof. This is Theorem 2 of [6]. □

Lemma 2. *Let* n *and* r *be integers with* $3 \leqslant r \leqslant n$. *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 [15] or Lemma 3 of [4]. □

Lemma 3. *Let* G *be a graph with* n (> 1) *vertices and* e *edges and suppose that*

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

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 [10]. □

For the proof of (3) Gyarmati and Stewart [8] modified Lemma 3 to treat graphs whose edges are coloured and which do not contain cycles of length four consisting of two monochromatic paths of length two. We shall need to deal with a slightly more complicated situation where we replace a cycle of length four with several monochromatic paths of length two which have the same starting vertex and the same finishing vertex. The result which we shall establish below is a generalisation of Lemma 2.4 of [8] and is proved by a minor alteration of the proof of Theorem 2.3, Chapter VI, of [2] which gives a bound for the number of edges of a graph on n vertices which does not contain a $K(\ell, 2)$, a bipartite graph which contains all edges between a vertex set of size ℓ and a vertex set of size 2.

Lemma 4. *Let* G *be a graph with* n *vertices and* e *edges coloured by* k *different colours. Suppose that* G *does not contain distinct vertices* $a, c, b_1, \ldots, b_\ell$, *with the property that for* $j = 1, \ldots, \ell$ *the edges* ab_j *and* cb_j *are in* G *and of the same colour. Then*

$$e \leqslant \left((\ell - 1)kn^3\right)^{1/2} + kn.$$

Proof. We first count the number of monochromatic paths of G of length 2. Let $a_1, \ldots, a_n$ be the vertices of G and let $d_{i,j}$ denote the number of edges emanating from a_i of colour j. The number of monochromatic paths of G of length 2 is exactly

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

However this number is less than or equal to $(\ell-1)\binom{n}{2}$ since for every pair (a,c) there exist at most $\ell-1$ vertices $b_1,\dots,b_{\ell-1}$ such that ab_j and cb_j have the same colour for $j=1,\dots,\ell-1$. Thus

$$\sum_{i=1}^{n}\sum_{j=1}^{k}\binom{d_{i,j}}{2}\leqslant(\ell-1)\binom{n}{2}.$$

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

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

By the Cauchy–Schwarz inequality,

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

hence

$$2e^2-kne\leqslant(\ell-1)n^2(n-1)k/2.$$

Thus

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

whence

$$e\leqslant\left((\ell-1)n^3k\right)^{1/2}+kn.\qquad\square$$

Lemma 5. *Let k be an integer with $k\geqslant 2$ 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, a_3a_4+1 are kth powers then*

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

Proof. This follows from the proof of Theorem 1 of [7]. □

For any non-zero rational number α, where $\alpha=a/b$ with a and b coprime integers, we put $H(\alpha)=\max\{|a|,|b|\}$. Further, for any real number x let $\lceil x\rceil$ denote the smallest integer greater than or equal to x.

Recall that non-zero rational numbers $\alpha_1,\dots,\alpha_t$ are said to be multiplicatively dependent if there exist integers $\ell_1,\dots,\ell_t$, not all zero, for which

$$\alpha_1^{\ell_1}\cdots\alpha_t^{\ell_t}=1.$$

They are said to be multiplicatively independent otherwise. Our next lemma will be used in the proof of our main theorem to produce a set of multiplicatively independent rational numbers which satisfy the hypotheses of Lemma 9.

Lemma 6. *Let ε be a positive real number with $0<\varepsilon<1$ and let t be an integer with $t\geqslant 2$. Let $\alpha_1,\dots,\alpha_k$ be non-zero rational numbers with the property that any t of them are multiplicatively dependent. Suppose that*

$$k\geqslant t\left(1+\left\lceil\frac{t-1}{\varepsilon}\right\rceil^{t-1}\right).$$

Then there exist distinct integers $i_0, \dots, i_t$ for which

$$H\left(\frac{\alpha_{i_0}}{\alpha_{i_1}}\right) \leqslant \left(H(\alpha_{i_2}) \cdots H(\alpha_{i_t})\right)^{\varepsilon/(t-1)}.$$

Proof. This follows from Theorem 1 of [14] on replacing ε with $\varepsilon/(t-1)$. □

Lemma 7. *Let B_1 and B_2 be non-zero integers and let α_1 and α_2 be positive rational numbers with $H(\alpha_1) \leqslant A_1$ and $H(\alpha_2) \leqslant A_2$. Put $\Lambda = B_1 \log \alpha_1 + B_2 \log \alpha_2$. There exists an effectively computable positive number c such that if $\Lambda \neq 0$ then*

$$|\Lambda| > \exp\left(-c \log(2A_1) \log(2A_2) \left(1 + \log\left(\frac{|B_2|}{\log(2A_1)} + \frac{|B_1|}{\log(2A_2)}\right)\right)\right).$$

Proof. This follows from Theorem 2.2 of Philippon and Waldschmidt [13]. □

Lemma 8. *Let M be an integer with $M \geqslant 16$ and let a_1, a_2, a_3 and a_4 be distinct integers with $M^{1/2} \leqslant a_i \leqslant M$ for $i = 1, 2, 3, 4$ and put $a_5 = a_1$. Suppose that x_1, x_2, x_3, x_4 and b_1, b_2, b_3, b_4 are positive integers and that*

$$a_i a_{i+1} + 1 = x_i^{b_i},$$

for $i = 1, 2, 3, 4$. Put $b = \min\{b_1, b_2, b_3, b_4\}$ and $t = \max_{1 \leqslant i \leqslant 4}\{b_i - b\}$. There exists an effectively computable positive number C such that

$$t + 1 > \frac{Cb^2}{\log M}. \tag{6}$$

Proof. Following the proof of Lemma 3.1 of [12] we observe that

$$a_1 a_2 a_3 a_4 = \left(x_1^{b_1} - 1\right)\left(x_3^{b_3} - 1\right) = \left(x_2^{b_2} - 1\right)\left(x_4^{b_4} - 1\right)$$

hence

$$\left(x_1^{b_1} - 1\right)\left(x_3^{b_3} - 1\right) - \left(x_2^{b_2} - 1\right)\left(x_4^{b_4} - 1\right) = 0$$

or, equivalently,

$$x_1^{b_1} x_3^{b_3} - x_2^{b_2} x_4^{b_4} = x_1^{b_1} + x_3^{b_3} - x_2^{b_2} - x_4^{b_4}. \tag{7}$$

Since $x_1^{b_1} + x_3^{b_3} - x_2^{b_2} - x_4^{b_4} = (a_1 - a_3)(a_2 - a_4)$ and since the a_i's are distinct we find that

$$x_1^{-b_1} x_3^{-b_3} x_2^{b_2} x_4^{b_4} \neq 1.$$

Thus, if we put

$$\Lambda = b \log\left(\frac{x_2 x_4}{x_1 x_3}\right) + \log\left(\frac{x_2^{b_2 - b} x_4^{b_4 - b}}{x_1^{b_1 - b} x_3^{b_3 - b}}\right), \tag{8}$$

we see that $\Lambda \neq 0$. We may assume, without loss of generality, that $x_1^{b_1} \geqslant x_i^{b_i}$ for $i = 2, 3, 4$. Thus, by (7),

$$\left|\frac{x_2^{b_2} x_4^{b_4}}{x_1^{b_1} x_3^{b_3}} - 1\right| \leqslant \frac{2}{x_3^{b_3}}. \tag{9}$$

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

$$x_3^{b_3} > M,$$

and, therefore, by (8) and (9),

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

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

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

hence

$$\log|\Lambda| < -\frac{1}{2}\log M. \tag{10}$$

We now apply Lemma 7 with $\alpha_1 = (x_2x_4)/(x_1x_3)$, $\alpha_2 = (x_2^{b_2-b}x_4^{b_4-b})/(x_1^{b_1-b}x_3^{b_3-b})$, $B_1 = b$ and $B_2 = 1$. Note that $\log x_i \leqslant (2\log M)/b$ for $i = 1, 2, 3, 4$. Therefore

$$\log H(\alpha_1) \leqslant \log x_1 + \log x_2 + \log x_3 + \log x_4 \leqslant \frac{8\log M}{b}$$

and

$$\log H(\alpha_2) \leqslant 6(t+1)\frac{\log M}{b}.$$

Put $\log A_1 = (8\log M)/b$ and $\log A_2 = (6(t+1)\log M)/b$. Let $C_1, C_2, \ldots$ denote effectively computable positive numbers. By Lemma 7

$$\log|\Lambda| > -C_1\frac{(t+1)(\log M)^2}{b^2}\left(1 + \log\left(1 + \frac{b^2}{(t+1)\log M}\right)\right)$$

and so, by (10),

$$\frac{b^2}{(t+1)\log M}\left(1 + \log\left(1 + \frac{b^2}{(t+1)\log M}\right)\right)^{-1} < C_2.$$

Therefore

$$\frac{b^2}{(t+1)\log M} < C_3,$$

and Lemma 8 now follows. □

In 1986 Loxton gave an estimate for simultaneous linear forms in the logarithms of algebraic numbers. We shall state his result for the special case when the algebraic numbers are rationals. Let n and t be integers with $n \geqslant 2$ and $t \geqslant 1$ and let $\alpha_1, \ldots, \alpha_n$ be non-zero multiplicatively independent rational numbers. Let $b_{i,j}$ for $i = 1, \ldots, t$ and $j = 1, \ldots, n$ be rational numbers and suppose that the matrix $(b_{i,j})$ formed by the b_{ij}'s has rank t. Put

$$\Lambda_i = b_{i,1}\log\alpha_1 + \cdots + b_{i,n}\log\alpha_n, \quad \text{for } i = 1, \ldots, t,$$

where the logarithms are principal. We shall suppose that $H(\alpha_j) \leqslant A_j$ with $A_j \geqslant 4$ for $j = 1, \ldots, n$ and that $H(b_{i,j}) \leqslant B$ with $B \geqslant 4$ for $i = 1, \ldots, t$ and $j = 1, \ldots, n$. Put

$$\Omega = \log A_1 \cdots \log A_n.$$

Building on an estimate of Baker [1] for the case $t = 1$, Loxton [11] proved the following result.

Lemma 9.

$$\max_{1\leqslant i\leqslant t} |\Lambda_i| > \exp\bigl(-C(\Omega\log\Omega)^{1/t}\log(B\Omega)\bigr),$$

where $C = (16n)^{200n}$.

3. Proof of the main theorem

Let A be a subset of $\{1,\dots,N\}$ with the property that $aa'+1$ is in V whenever a and a' are distinct integers from A. We may suppose that

$$|A| > (\log N)^{2/3}(\log\log N)^{1/3}, \tag{11}$$

since otherwise our result holds. Let $c_1, c_2, \dots$ denote positive numbers which are effectively computable. We shall suppose that

$$\frac{1}{2}\left(\frac{\log N}{\log\log N}\right)^{2/3} > 16. \tag{12}$$

There is an integer m with

$$1 \leqslant m \leqslant \frac{\log((\log N)/\log 2)}{\log 2}, \tag{13}$$

such that A has more than $(|A|-3)/((\log((\log N)/\log 2))/\log 2)$ elements from $\{2^{2^m}, 2^{2^m}+1, \dots, 2^{2^{m+1}}-1\}$. Let us denote the set of these elements by A_m and put $n = |A_m|$ and $M = 2^{2^{m+1}}$. Then, by (11), for $N > c_1$,

$$n > \frac{|A|}{2\log\log N}. \tag{14}$$

Further, by (11) and (14),

$$M > n > \frac{(\log N)^{2/3}}{2(\log\log N)^{2/3}} \tag{15}$$

and since (12) holds,

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

Form the complete graph G whose vertices are the elements of A_m. Associate to each edge between two vertices a and a' the smallest prime p for which $aa'+1$ is a perfect pth power. For any real number x let $[x]$ denote the greatest integer less than or equal to x. We next define a sequence $t_1, t_2, \dots$ inductively by putting

$$t_1 = 1 + \bigl[\bigl((\log M)^2\log\log M\bigr)^{1/3}\bigr] \tag{17}$$

and

$$t_{i+1} = t_i - 1 + \left[\frac{Ct_i^2}{\log M}\right], \tag{18}$$

for $i = 1, 2, 3, \dots$, where C is the positive number given in Lemma 8. By (15), (17) and (18) we see that for N greater than c_2, as we shall suppose, the sequence $t_1, t_2, \dots$ is strictly increasing.

We are now in a position to give a colouring of G. If the edge between a and a' is associated with a prime p which is smaller than t_1 we colour the edge with the prime p. On the other hand,

if $p \geqslant t_1$ we colour the edge with the integer t_i for which $t_i \leqslant p < t_{i+1}$. For any real number x let $\pi(x)$ denote the number of prime numbers less than or equal to x. Notice that the total number of colours of G is bounded from above by

$$\pi(t_1) + h \tag{19}$$

where h counts the number of colours t_i for which t_i is smaller than

$$(2\log M)/\log 2.$$

In order to estimate h we first estimate the number of t_i's in each interval of the form $(2^k, 2^{k+1}]$. By (17) we need only consider such intervals for which

$$k + 1 > \frac{1}{3\log 2}\log\big((\log M)^2 \log\log M\big). \tag{20}$$

Further, if a and a' are distinct elements of A_m then $aa' + 1$ is at most M^2 and so we may also suppose that

$$k < \big(\log\big((2/\log 2)\log M\big)\big)/\log 2.$$

By (18), if t_i is in $(2^k, 2^{k+1}]$ then $t_{i+1} - t_i > ((C2^{2k})/\log M) - 2$ and so, by (15) and (20), we see that for N greater than c_3,

$$t_{i+1} - t_i > \frac{C2^{2k}}{2\log M}.$$

Thus the number of t_i's in the interval $(2^k, 2^{k+1}]$ is at most $1 + (2\log M)/C2^k$.

We may assume that N exceeds c_1, c_2 and c_3, since the result is immediate otherwise. Therefore

$$h \leqslant \sum_{(\frac{1}{3\log 2}\log((\log M)^2\log\log M))-1<k<\frac{1}{\log 2}\log(\frac{2}{\log 2}\log M)} \left(1 + \frac{2\log M}{C2^k}\right)$$

and so

$$h \leqslant c_4\big((\log M)/\log\log M\big)^{1/3}. \tag{21}$$

Thus, by (19), (21) and the prime number theorem, the number of colours of G is at most $c_5((\log M)/\log\log M)^{2/3}$.

By Lemma 2, if the number of edges of G coloured with 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 1. Therefore the number of edges of G coloured with something other than 2 is at least $\binom{n}{2} - (2/5)n^2 = (n^2/10) - (n/2)$. 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

$$(\log M)^{3/10} < p < t_1$$

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 an integer t_i with $1 \leqslant i \leqslant h$ or with a prime p satisfying

$$2 < p \leqslant (\log M)^{3/10}. \tag{22}$$

We shall suppose first that G_2 has at least $(n^2/20) - (n/2)$ edges. The number of colours of G_2 is at most

$$\pi\big((\log M)^{3/10}\big) + h.$$

Thus by (21) the number of colours of G_2 is at most $c_6((\log M)/\log\log M)^{1/3}$. Accordingly, there is a colour of G_2 which appears on

$$\frac{(n^2/20)-(n/2)}{c_6(\frac{\log M}{\log\log M})^{1/3}}$$

different edges. Since $M \leqslant N$ we see from (14) that if

$$|A| > c_7\big((\log N)^2 \log\log N\big)^{1/3}, \tag{23}$$

then there is a colour which appears on more than $(n^{3/2}+n-n^{1/2})/2$ edges and so, by Lemma 3, G_2 contains a monochromatic cycle of length 4. By (16), (18) and Lemma 8 there is no cycle of length 4 with a colour t_i in G, hence in G_2, and thus G_2 must contain a cycle of length 4 coloured with a prime p, satisfying (22). In particular there exist integers a_1, a_2, a_3 and a_4 with $a_1 < a_3$ and $a_2 < a_4$ for which a_1a_2+1, a_1a_4+1, a_2a_3+1 and a_3a_4+1 are pth powers. Thus, by Lemma 5,

$$a_3a_4 > (a_1a_2)^2. \tag{24}$$

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

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

which contradicts (24). Thus either the supposition (23) is false, in which case our result follows, or G_2 has fewer than $(n^2/20)-(n/2)$ edges. We may assume the latter possibility and therefore G_1 contains at least $n^2/20$ edges.

The number of colours of G_1 is at most the number of colours of G hence is at most $c_5((\log M)/\log\log M)^{2/3}$. Since $N > M$ the number of colours of G is at most $c_5((\log N)/\log\log N)^{2/3}$. Thus we may apply Lemma 4 to the graph G_1. Since G_1 has at least $n^2/20$ edges we see by (14), that if

$$|A| > c_8\big((\log N)^2 \log\log N\big)^{1/3}, \tag{25}$$

then there are integers $a_1, a_2, \ldots, a_{870}$ with the property that a_1a_j and a_2a_j are edges of G_1 and are of the same colour for $j = 3, \ldots, 870$.

Put

$$\gamma_j = \frac{a_1a_j+1}{a_2a_j+1} \quad \text{for } j = 3, \ldots, 870.$$

We claim that we can find a subset of $\{\gamma_3, \ldots, \gamma_{870}\}$ consisting of 4 multiplicatively independent numbers. If this is not so then we may apply Lemma 6 with $\varepsilon = 1/2$ and $t = 4$. Since $4(1+6^3) = 868$ there exist distinct integers $i_0, \ldots, i_4$ for which

$$H\left(\frac{\gamma_{i_0}}{\gamma_{i_1}}\right) \leqslant \big(H(\gamma_{i_2})H(\gamma_{i_3})H(\gamma_{i_4})\big)^{1/6}.$$

But

$$H(\gamma_{i_s}) < M^2, \quad \text{for } s = 2, 3, 4,$$

so

$$H\left(\frac{\gamma_{i_0}}{\gamma_{i_1}}\right) < M. \tag{26}$$

Notice that

$$\frac{\gamma_{i_0}}{\gamma_{i_1}} = \frac{(a_1a_{i_0}+1)(a_2a_{i_1}+1)}{(a_2a_{i_0}+1)(a_1a_{i_1}+1)},$$

and so

$$H\left(\frac{\gamma_{i_0}}{\gamma_{i_1}}\right) \geqslant \frac{a_1a_2a_{i_0}a_{i_1}}{\gcd((a_1a_{i_0}+1)(a_2a_{i_1}+1),(a_2a_{i_0}+1)(a_1a_{i_1}+1))}.$$

But

$$(a_1a_{i_0}+1)(a_2a_{i_1}+1) - (a_2a_{i_0}+1)(a_1a_{i_1}+1) = (a_1-a_2)(a_{i_0}-a_{i_1})$$

and therefore

$$\gcd\big((a_1a_{i_0}+1)(a_2a_{i_1}+1),(a_2a_{i_0}+1)(a_1a_{i_1}+1)\big) \leqslant \max(a_1,a_2)\max(a_{i_0},a_{i_1}).$$

Accordingly

$$H\left(\frac{\gamma_{i_0}}{\gamma_{i_1}}\right) \geqslant \min(a_1,a_2)\min(a_{i_0},a_{i_1})$$

and, since a_1, a_2, a_{i_0} and a_{i_1} are all at least $M^{1/2}$,

$$H\left(\frac{\gamma_{i_0}}{\gamma_{i_1}}\right) \geqslant M. \tag{27}$$

Since (26) and (27) are incompatible there exists a subset of $\{\gamma_3,\dots,\gamma_{870}\}$ consisting of 4 multiplicatively independent numbers.

Without loss of generality we may suppose that $\gamma_3,\dots,\gamma_6$ are multiplicatively independent. We have

$$\gamma_i = x_i^{p_i}, \quad \text{for } i = 3,4,5,6,$$

with p_3, p_4, p_5, p_6 primes satisfying

$$(\log M)^{3/10} < p_i \leqslant (\log M)^{2/3}(\log\log M)^{1/3},$$

for $i = 3,4,5,6$. Further x_3, x_4, x_5 and x_6 are multiplicatively independent since γ_3, γ_4, γ_5 and γ_6 are multiplicatively independent.

We have

$$a_1a_j + 1 = y_j^{p_j}, \tag{28}$$

$$a_2a_j + 1 = z_j^{p_j} \tag{29}$$

and $x_j = y_j/z_j$ for $j = 3,4,5,6$. Then, as in the proof of Lemma 8,

$$a_1a_2a_3a_j = \big(y_3^{p_3}-1\big)\big(z_j^{p_j}-1\big) = \big(y_j^{p_j}-1\big)\big(z_3^{p_3}-1\big)$$

so

$$y_3^{p_3}z_j^{p_j} - y_j^{p_j}z_3^{p_3} = y_3^{p_3} + z_j^{p_j} - y_j^{p_j} - z_3^{p_3}. \tag{30}$$

Again, since $y_3^{p_3} + z_j^{p_j} - y_j^{p_j} - z_3^{p_3} = (a_1-a_2)(a_3-a_j)$ and since the a_i's are distinct, we find that

$$\left(\frac{y_3}{z_3}\right)^{p_3}\left(\frac{z_j}{y_j}\right)^{p_j} \neq 1. \tag{31}$$

For $j = 4, 5, 6$, put

$$\Lambda_j = p_3 \log x_3 - p_j \log x_j,$$

and note, by (31), that $\Lambda_j \neq 0$. Put

$$g_j = x_3^{p_3} x_j^{-p_j}$$

and

$$G_j = \max\bigl(g_j, g_j^{-1}\bigr),$$

for $j = 4, 5, 6$. It follows from (30), as in the proof of Lemma 8, that

$$|G_j - 1| \leqslant \frac{2}{M},$$

for $j = 4, 5, 6$. But $G_j = e^{|\Lambda_j|}$ for $j = 4, 5, 6$. As before, we remark that if y is a real number and $|e^y - 1| \leqslant 1/8$ then $|y| < 1/2$. Therefore, by (16), $|\Lambda_j| < 1/2$ for $j = 4, 5, 6$. Since $M > 16$ and since $|e^y - 1| \geqslant |y|/2$ for $|y| < 1/2$ we have

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

hence

$$\log|\Lambda_j| < -\frac{1}{2}\log M, \tag{32}$$

for $j = 4, 5, 6$.

We now apply Lemma 9 with $\alpha_j = x_{j+2}$ for $j = 1, 2, 3, 4$ and with $b_j = p_{j+2}$ for $j = 1, 2, 3, 4$. Note that

$$\log H(\alpha_j) = \log H(x_{j+2}) \leqslant \log\bigl(\max\bigl(|y_{j+2}|, |z_{j+2}|\bigr)\bigr)$$

and so, by (28) and (29),

$$\log H(\alpha_j) \leqslant \frac{2\log M}{p_{j+2}}, \tag{33}$$

for $j = 1, 2, 3, 4$. Further $B = \max\{p_3, p_4, p_5, p_6\}$ and so

$$B \leqslant \frac{2\log M}{\log 2}. \tag{34}$$

Furthermore, the matrix

$$\begin{pmatrix} p_3 & -p_4 & 0 & 0 \\ p_3 & 0 & -p_5 & 0 \\ p_3 & 0 & 0 & -p_6 \end{pmatrix}$$

has rank 3. Thus, by (32), (33), (34) and Lemma 9 with $t = 3$,

$$\log M < c_9 \left(\frac{(\log M)^4}{p_3 p_4 p_5 p_6} \log\log M \right)^{1/3} \log\log M$$

hence

$$p_3 p_4 p_5 p_6 < c_{10} \log M (\log\log M)^4. \tag{35}$$

But p_3, p_4, p_5 and p_6 exceed $(\log M)^{3/10}$ and this is incompatible with (35) for M larger than c_{11}, hence by (15), for N larger than c_{12}. Thus (25) does not hold and the result follows.

References

[1] A. Baker, The theory of linear forms in logarithms, in: A. Baker, D.W. Masser (Eds.), Transcendence Theory, Advances and Applications, Academic Press, 1977, pp. 1–27.
[2] B. Bollobás, Extremal Graph Theory, London Math. Soc. Monogr., vol. 11, Academic Press, London, 1978.
[3] Y. Bugeaud, A. Dujella, On a problem of Diophantus for higher powers, Math. Proc. Cambridge Philos. Soc. 135 (2003) 1–10.
[4] Y. Bugeaud, K. Gyarmati, On generalizations of a problem of Diophantus, Illinois J. Math. 48 (2004) 1105–1115.
[5] R. Dietmann, C. Elsholtz, K. Gyarmati, M. Simonovits, Shifted products that are coprime pure powers, J. Combin. Theory Ser. A 111 (2005) 24–36.
[6] A. Dujella, There are only finitely many Diophantine quintuples, J. Reine Angew. Math. 566 (2004) 183–214.
[7] K. Gyarmati, On a problem of Diophantus, Acta Arith. 97 (2001) 53–65.
[8] K. Gyarmati, C.L. Stewart, On powers in shifted products, Glas. Mat., in press.
[9] K. Gyarmati, A. Sárközy, C.L. Stewart, On shifted products which are powers, Mathematika 49 (2002) 227–230.
[10] T. Kövári, V. Sós, P. Turán, On a problem of K. Zarankiewicz, Colloq. Math. 3 (1954) 50–57.
[11] J.H. Loxton, Some problems involving powers of integers, Acta Arith. 46 (1986) 113–123.
[12] F. Luca, On shifted products which are powers, Glas. Mat. 40 (2005) 13–20.
[13] P. Philippon, M. Waldschmidt, Lower bounds for linear forms in logarithms, in: A. Baker (Ed.), New Advances in Transcendence Theory, Cambridge University Press, 1988, pp. 280–312.
[14] C.L. Stewart, On heights of multiplicatively dependent algebraic numbers, Acta Arith., in press.
[15] P. Turán, On an extremal problem in graph theory, Mat. Fiz. Lapok 48 (1941) 436–452 (in Hungarian).