GLASNIK MATEMATIČKI
Vol. 40(60)(2005), 13 – 20

ON SHIFTED PRODUCTS WHICH ARE POWERS

Florian Luca
Universidad Nacional Autónoma de México, México

Abstract. In this note, we improve upon results of Gyarmati, Sárközy and Stewart from [9] and Bugeaud and Gyarmati from [3] concerning the size of a subset $\mathcal{A}$ of $\{1,\ldots,N\}$ such that the product of any two distinct elements of $\mathcal{A}$ plus 1 is a perfect power. We also show that the cardinality of such a set is uniformly bounded assuming the *ABC*-conjecture, thus improving upon a result from [4].

1. Introduction

Write V for the set of all perfect powers; i.e., the set of all numbers of the form x^k with integers $x \geq 1$ and $k \geq 2$. In [9], subsets $\mathcal{A}$ of positive integers such that $aa'+1$ is in V whenever $a \neq a'$ are in $\mathcal{A}$ were investigated. The main result of [9] shows that such sets are not too "dense":

Theorem 1.1. *Let $\mathcal{A}$ be a subset of $\{1,\ldots,N\}$ with the property that $aa'+1$ is in V whenever $a \neq a'$ are in $\mathcal{A}$. Then there exists a constant N_0 such that the inequality*

$$\#\mathcal{A} \leq 340\frac{(\log N)^2}{\log\log N} \tag{1}$$

holds whenever $N > N_0$.

The proof of the above result ingeniously combines graph theoretical results with a "gap principle" from [8]. The above bound was slightly improved to $177000(\log N/\log\log N)^2$ in [3]. The improvement in the result from [3] is due to an improved gap principle which first appeared in [2]. In this note, we improve upon the above estimates. Our result is the following.

2000 *Mathematics Subject Classification.* 11B75, 11D99.
Key words and phrases. Shifted products, perfect powers.

Theorem 1.2. *Let $\mathcal{A}$ be as in the statement of the previous theorem. Then the inequality*

$$\#\mathcal{A} \ll \left(\frac{\log N}{\log\log N}\right)^{3/2} \tag{2}$$

holds for all sufficiently large values of N.

Under a strong technical coprimality condition, it is shown in [4] that the bound (2) can be strengthened to $8000(\log N/\log\log N)$.

For every positive integer n we write $N(n) = \prod_{p|n} p$ for the *algebraic radical* of n. We recall the statement of the ABC-conjecture.

Conjecture 1.3. *For every $\varepsilon > 0$ there exists a constant $c = c(\varepsilon)$ such that if A, B, C are nonzero integers with $\gcd(A, B) = 1$ and $A + B = C$, then*

$$\max\{|A|, |B|, |C|\} \le c\,(N(ABC))^{1+\varepsilon}.$$

Under the ABC-conjecture, in [4] it is shown that the bound (2) can be improved to $\#\mathcal{A} \ll \log\log N$. Here, we improve this to $\#\mathcal{A} = O(1)$ under the same assumption.

Theorem 1.4. *The ABC conjecture implies that if $\mathcal{A}$ satisfies the hypothesis of Theorem 1.1, then $\#\mathcal{A}$ is bounded by an absolute constant.*

2. The Idea behind the Proofs

In principle, for both proofs, we follow the method from [9], but we use a new ingredient. The method from [9] is roughly as follows. Let G be the complete graph with vertex set $\mathcal{A}$. Color each edge of G with $\pi(\log(N^2)/\log 2)$ colors, where the edge aa' is colored by a color p, a prime $\le \log(N^2)/\log 2$, if $aa' + 1 = x^p$ holds for some positive integer x (note that $aa' + 1 \le N(N-1) + 1 \le N^2$). Using a result of Dujella [5] to the effect that Diophantine sets have bounded cardinalities, as well as results of Túran et. al. [10, 11] concerning upper bounds on the number of edges of graphs without four cycles or without complete subgraphs with eight vertices, the authors of [9] show that if G has too many edges (i.e., more than the number shown in the right hand side of inequality (1)), then for large N there exists some $y \in [1, N]$ such that the interval $[y, y^2]$ contains four members of $\mathcal{A}$ with the property that G has a monochromatic cycle on those four vertices colored with a color $p > 2$, which in turn contradicts a gap principle from [8]. The same graph theoretical approach combined with Theorem 1 from [3] allows one to simply eliminate the "slicing step" in which all four vertices where in an interval of the form $[y, y^2]$ for some y, which results in an extra saving by a factor of $\log\log N$, as in Theorem 3 from [3].

Our improvement in Theorem 1.2 stems from the following direction. We show that there exists a positive computable constant α such that if we set

$p_0 = \lfloor \alpha(\log N)^{3/4}(\log\log N)^{1/4}\rfloor$, and if we change all the colors $p > p_0$ to one single color, which we will call the "large" color, then G cannot contain a cycle of length four colored with the large color. This part of the proof uses lower bounds for linear forms in logarithms of algebraic numbers. As for Theorem 1.4, we show that under the ABC conjecture, one may take p_0 to be absolute, after which we apply the main result from [2] and Ramsey's Theorem to conclude.

3. The "Large" Color

In this section, we prove the following lemma.

Lemma 3.1. *There exists a computable positive constant α such that if N is large, and if we set $p_0 = \lfloor \alpha(\log N)^{3/4}(\log\log n)^{1/4}\rfloor$, then $\mathcal{A}$ does not contain a subset with four elements $\{a_1, a_2, a_3, a_4\}$ such that $a_i a_{i+1} + 1 = x_i^{p_i}$ holds for with integers $x_i > 1$ and $p_i > p_0$ for $i = 1, \ldots, 4$. Here, we make the convention that $a_5 = a_1$.*

Proof. Multiplying the relations

$$a_1a_2 = x_1^{p_1} - 1 \qquad \text{and} \qquad a_3a_4 = x_3^{p_3} - 1,$$

as well as

$$a_2a_3 = x_2^{p_2} - 1 \qquad \text{and} \qquad a_4a_1 = x_4^{p_4} - 1,$$

and identifying we get the equation

$$(x_1^{p_1} - 1)(x_3^{p_3} - 1) = (x_2^{p_2} - 1)(x_4^{p_4} - 1),$$

which can be rewritten as

$$x_1^{p_1}x_3^{p_3} - x_2^{p_2}x_4^{p_4} = x_1^{p_1} + x_3^{p_3} - x_2^{p_2} - x_4^{p_4}. \tag{3}$$

One checks easily that the number appearing in both sides of the above equation is nonzero. Indeed, if it were equal to zero, we would then get

$$0 = x_1^{p_1} + x_3^{p_3} - x_2^{p_2} - x_4^{p_4} = a_1a_2 + a_3a_4 - a_2a_3 - a_4a_1 = (a_1 - a_3)(a_2 - a_4),$$

contradicting the fact that the a_i's are distinct. Let $M = \max\{x_i^{p_i} : i = 1, \ldots, 4\}$. Without loss of generality, we may assume that $M = x_1^{p_1}$. From (3), we get the estimate

$$Mx_3^{p_3}|1 - x_1^{-p_1}x_2^{p_2}x_3^{-p_3}x_4^{p_4}| \le 4M,$$

which leads to

$$p_3 \log x_3 + \log|1 - x_1^{-p_1}x_2^{p_2}x_3^{-p_3}x_4^{p_4}| \le \log 4. \tag{4}$$

We now use a linear form in logarithms to bound the logarithmic term above. Let p_0 to be determined later and assume that $p_i \ge p_0$ holds for all $i = 1, \ldots, 4$. Then $x_i^{p_0} \le x_i^{p_i} \le 1 + N(N-1) < N^2$, therefore $\log x_i \le (2\log N)/p_0$ holds for $i = 1, 2, 4$. Finally, it is clear that since $x_i \ge 2$, it follows that if we write $P = \max\{p_i : i = 1, \ldots, 4\}$, then $P \le 2\log N/\log 2$.

A classical application of lower bounds for linear forms in logarithms of algebraic numbers (see, for example, [1]) shows that there exists a computable positive constant β such that

$$\begin{aligned} \log|1 - x_1^{-p_1}x_2^{p_2}x_3^{-p_3}x_4^{-p_4}| &> -\beta\log(P)\prod_{i=1}^{4}\log(x_i) \\ &> -8\beta(\log x_3)\log\left(\frac{2\log N}{\log 2}\right)\left(\frac{\log N}{p_0}\right)^3. \end{aligned} \tag{5}$$

Thus, writing $\gamma = 9\beta$, we get that if N is large enough then the inequality

$$\log|1 - x_1^{-p_1}x_2^{p_2}x_3^{-p_3}x_4^{-p_4}| > -\gamma\log x_3\log\log N\left(\frac{\log N}{p_0}\right)^3 \tag{6}$$

holds. Inserting inequality (6) into inequality (4), we get

$$\log x_3\left(p_0 - \gamma\log\log N\left(\frac{\log N}{p_0}\right)^3\right) \le \log 4$$

and the above inequality is impossible for large N if

$$\frac{p_0}{2} > \gamma\log\log N\left(\frac{\log N}{p_0}\right)^3.$$

This completes the proof of the lemma with the choice

$$p_0 = \lfloor\alpha(\log N)^{3/4}(\log\log N)^{1/4}\rfloor$$

and $\alpha = (2\gamma+1)^{1/4}$. ∎

4. The Proof of Theorem 1.2

We put $n = \lfloor\delta\pi(p_0)^2\rfloor + 1$, where $p_0 = p_0(N)$ is defined in Lemma 3.1, and we show that if δ is a sufficiently large constant then the inequality $\#\mathcal{A} < n$ holds once N is sufficiently large.

We write G for the graph whose vertices are the elements of $\mathcal{A}$. We write q_i for the ith prime number and we color the edges of G with $t = \pi(p_0) + 1$ colors $\mathcal{C} = \{q_1, \ldots, q_t, \infty\}$ as follows: if $aa' + 1 = x^p$ holds with some integer $x > 1$ and a prime p, we then assign to aa' the color q_i if $p = q_i$ for some $i = 1, \ldots, t$, and ∞ otherwise (if more such choices for i are possible, we pick the smallest one). For each color c, we write b_c for the number of edges of color c in G. It is clear that

$$\sum_{c\in\mathcal{C}} b_c = \binom{n}{2} = \frac{n(n-1)}{2}.$$

A result of Dujella from [5], shows that there does not exist a set with 8 elements such that the product of any two plus one is a square (see [6] for a better result). In particular, the subgraph of G colored by the color $c = 2$

does not contain a complete graph with 8 edges. Túran's result from [11] (see also the argument on the bottom of page 228 in [9]) implies that $b_2 \leq 7n^2/16$, therefore

$$\sum_{c\in\mathcal{C}\backslash\{2\}} b_c \geq \frac{n(n-1)}{2} - \frac{7n^2}{16} > \frac{n^2}{17}$$

if n is large. Theorem 1 in [3] now shows that $b_3 \leq 7.64n^{5/3}$ and that $b_c \leq 5.47n^{3/2}$ if $c \in \mathcal{C}\backslash\{2,3,\infty\}$. Finally, a result from [10] implies that if $b_\infty > n^{3/2}$ then there exists a cycle of length four colored with the color ∞, which contradicts Lemma 3.1. Hence,

$$\frac{n^2}{17} \leq \sum_{c\in\mathcal{C}\backslash\{2\}} b_c \leq n^{3/2}(5.47(\pi(p_0)-2)+1) + 7.64n^{5/3} < 6n^{3/2} + 8n^{5/3}.$$

The above inequality implies that the inequality

$$\pi(p_0) \geq \frac{n^{1/2}}{17\cdot 7} > \frac{\sqrt{\delta}}{109}\pi(p_0)$$

holds for large values of n (hence, of N), which is impossible once $\delta > 109^2$. ∎

Remark 4.1. Since the constant β appearing in the lower bound (5) is effectively computable, it follows that both the constant α from Lemma 3.1 and the constant implied in the inequality (2) are effectively computable as well.

5. The proof of Theorem 1.4

Assume $a_1 < a_2 < a_3 \in \mathcal{A}$ are such that $a_1a_3 + 1 = u^k$ and $a_2a_3 + 1 = v^\ell$ hold with u, v, k, ℓ integers and both $k, \ell > 10$. We then have the equation

$$a_2u^k - a_1v^\ell = a_2 - a_1.$$

Let $d = \gcd(a_2u^k, a_1v^\ell)$. Applying the ABC conjecture to the equation

$$\frac{a_2u^k}{d} - \frac{a_1v^\ell}{d} = \frac{a_2-a_1}{d},$$

we get

$$\begin{aligned}\frac{a_2u^k}{d} &\ll N(a_2a_1u^kv^\ell(a_2-a_1))^{1+\varepsilon} \ll (a_2^3uv)^{1+\varepsilon}\\ &\ll \left(a_2^3(a_1a_3)^{1/k}(a_2a_3)^{1/\ell}\right)^{1+\varepsilon}\\ &\ll a_2^{(3+1/k+1/\ell)(1+\varepsilon)}a_3^{(1/k+1/\ell)(1+\varepsilon)}.\end{aligned}$$

Setting $\varepsilon = 1/10$ and recalling that $k, \ell \geq 11$, we get $(1/k + 1/\ell)(1+\varepsilon) \leq 2/10 = 1/5$, while $(3 + 1/k + 1/\ell)(1+\varepsilon) < 4$. Furthermore, since $d|a_2 - a_1$, we get that $a_2 > d$. We thus get

$$a_3 < u^k \leq \frac{a_2 u^k}{d} \ll a_2^4 a_3^{2/5},$$

therefore

$$a_3^{3/5} \ll a_2^4,$$

leading to $a_3 \ll a_2^7$.

In particular, if $a_1 < a_2 < a_3 < a_4 < a_5$ are five elements of $\mathcal{A}$ such that $a_i a_j + 1 = x_{ij}^{\kappa_{ij}}$ holds with integers x_{ij} and $\kappa_{ij} > 10$, then $a_5 \ll a_4^7 \ll a_3^{49} \ll a_2^{343}$.

We now assume that $a_1 < a_2 < a_3 < a_4$ are in $\mathcal{A}$ such that

$$a_1 a_2 = x_1^{k_1} - 1 \qquad \text{and} \qquad a_3 a_4 = x_3^{k_3} - 1,$$

as well as

$$a_2 a_3 = x_2^{k_2} - 1 \qquad \text{and} \qquad a_1 a_4 = x_4^{k_4} - 1.$$

Arguing as in Section 3, we get

$$x_1^{k_1} x_3^{k_3} - x_2^{k_2} x_4^{k_4} = x_1^{k_1} + x_3^{k_3} - x_2^{k_2} - x_4^{k_4}. \tag{7}$$

The argument used at equation (3) shows that the number appearing in either side of equation (7) is not zero. We let $D = \gcd(x_1^{k_1} x_3^{k_3}, x_2^{k_2} x_4^{k_4})$. We apply the ABC conjecture to equation (7) with $A = x_1^{k_1} x_3^{k_3}/D$, $B = -x_2^{k_2} x_4^{k_4}/D$ and $C = M/D$, with M being the right hand side of (7). Note that $|M| \ll x_3^{k_3}$. We get

$$\frac{x_1^{k_1} x_3^{k_3}}{D} \ll \left(x_1 x_2 x_3 x_4 \frac{|M|}{D} \right)^{1+\varepsilon},$$

leading to

$$\begin{aligned} x_1^{k_1} x_3^{k_3} &\ll (x_1 x_2 x_3 x_4 x_3^{k_3})^{1+\varepsilon} \\ &\ll \left((a_1 a_2)^{1/k_1} (a_2 a_3)^{1/k_3} (a_3 a_4)^{1/k_3} (a_4 a_1)^{1/k_4} \right)^{1+\varepsilon} (x_3^{k_3})^{1+\varepsilon}. \end{aligned}$$

Assume that $k_i \geq k_0$, where k_0 will be determined later. We then get

$$a_1^2 < a_1 a_2 < x_1^{k_1} \ll a_4^{8(1+\varepsilon)/k_0} (x_3^{k_3})^{\varepsilon} \ll a_4^{8(1+\varepsilon)/k_0 + 2\varepsilon}.$$

We now choose $\varepsilon = 1/800$ and $k_0 = 3205$ and note that $8(1+\varepsilon)/k_0 + 2\varepsilon < 1/200$. Hence,

$$a_1^2 \ll a_4^{1/200},$$

therefore $a_4 \gg a_1^{400}$.

Assume now that $a_1 < a_2 < a_3 < a_4 < a_5$ are such that $a_i a_j + 1 = x_{ij}^{k_{ij}}$ hold with integers x_{ij} and $k_{ij} \geq k_0$. On the one hand, we saw that $a_5 \ll a_2^{343}$. On the other hand, we also saw that $a_5 \gg a_2^{400}$. From those two inequalities we conclude that $a_2 < \eta$, where η is a constant.

We are now ready to prove that $\#\mathcal{A} = O(1)$. We first eliminate from $\mathcal{A}$ all the elements smaller than η. The above argument then shows that from the remaining elements there does not exist a subset of five such that the product of any two plus one is a perfect power of exponent ≥ 3205.

Let $t = \pi(3205)$ and let p_i be the ith prime. We let G be the graph whose vertices are the elements of $\mathcal{A}$. We color the edges of G with the $t+1$ colors $p_1, \ldots, p_t, \infty$ in such a way that if a, a' are in $\mathcal{A}$ then we assign to aa' the color p_i for some $i \in \{1, \ldots, t\}$ if $aa' + 1 = x^{p_i}$ holds with some positive integer x, and ∞ otherwise (of course, if there are multiple choices for i, we can again just pick the smallest one). We now recall that for every prime number p (see [5, 6] for $p = 2$ and [2] for $p > 2$), there exists a positive integer m_p such that there does not exist a set $\mathcal{A}_p$ with m_p elements such that the product of any two plus 1 is a pth power. For example, it is known that we can take $m_2 = 6$ and $m_p = 4$ if $p > 177$.

Now let A be the value of the Ramsey number $R(m_2, \ldots, m_{p_t}, 5; 2)$. Recall that the Ramsey number $R(n_1, \ldots, n_s; 2)$ is the smallest positive integer R such that no matter how we color the edges of the complete graph with R vertices with the colors $1, 2, \ldots, s$, there exist i and a complete monochromatic subgraph with n_i vertices colored with color i. The fact that this number exists is Ramsey's Theorem (see, for example, Theorem 1 on page 3 of [7]).

It is now clear that $\#\mathcal{A} < A$. Indeed, if $\#\mathcal{A} \geq A$, then either there exist some prime number $p \leq p_t$ and at least m_p elements of $\mathcal{A}$ such that the product of any two increased by 1 is a pth power, or there exist at least five elements of $\mathcal{A}$ the product of any two of which increased by one is a kth power with some $k \geq 3205$, and both instances are impossible. ∎

Acknowledgements.

The author thanks professors Yann Bugeaud, Andrej Dujella and Katalin Gyarmati for useful discussions which lead to an improvement of his original Theorem 1.2. This work was supported by grants SEP-CONACYT 37259-E and 37260-E.

References

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

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

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

[4] R. Dietmann, C. Elsholtz, K. Gyarmati and M. Simonovits, *Shifted products that are coprime pure powers*, J. Comb. Theor. A, to appear.

[5] A. Dujella, *An absolute bound for the size of Diophantine m-tuples*, J. Number Theory **89** (2001), 126–150.

[6] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

[7] R.L. Graham, B.L. Rothschild, J.H. Spencer, Ramsey Theory, John Wiley & Suns, 1980.

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

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

[10] P. Kövari, V. Sós and P. Túran, *On a problem of K. Zarankiewicz*, Colloq. Math. **3** (1954), 50–57.

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

F. Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán
México
E-mail: fluca@matmor.unam.mx

Received: 2.11.2004.