UNIFORM BOUNDS FOR THE NUMBER OF POWERS IN ARITHMETIC PROGRESSIONS

L. HAJDU AND Á. PAPP

Abstract. We give sharp, in some sense uniform bounds for the number of ℓ-th powers and arbitrary powers among the first N terms of an arithmetic progression, for N large enough.

1. Introduction

The problem of giving (sharp) upper bounds for the number of powers among N consecutive terms of an arithmetic progression is a classical one with many deep results and open problems and conjectures. Here we only give a brief introduction; for a more precise account of the topic the interested reader may consult e.g. the papers [1] and [6].

Let a, b, ℓ be integers with $a > 0$ and let $\ell \geq 2$. Write $P_{a,b;N}(\ell)$ for the number of ℓ-th powers among the first N terms of the arithmetic progression $ax + b$ $(x \geq 0)$. Denote by $P_N(\ell)$ the maximum of these values taken over all arithmetic progressions $ax + b$. (Note that this maximum obviously exists.) The case of squares (i.e, $\ell = 2$) has been studied by many authors. Erdős [3] conjectured and Szemerédi [10] proved that $P_N(2) = o(N)$. Later, by deep tools (such as e.g. elliptic and higher genus curves, Falting's theorem, the distribution of primes etc.) Bombieri, Granville and Pintz [1] proved $P_N(2) < O(N^{2/3+o(1)})$, which subsequently was improved to $P_N(2) < O(N^{3/5+o(1)})$ by Bombieri and Zannier [2]. See also Granville [5] for related results and remarks. A strong conjecture of Rudin (see [9], end of paragraph 4.6) predicts that $P_N(2) = O(\sqrt{N})$, or in an even more precise form, that

$$P_N(2) = P_{24,1;N}(2) = \sqrt{\frac{8}{3}N} + O(1) \quad (N \geq 6) \tag{1}$$

should hold.

2010 *Mathematics Subject Classification.* 11B25.

Key words and phrases. Arithmetic progressions, powers, ℓ-th powers.

L.H. was Research supported in part by the Eötvös Loránd Research Network (ELKH), the NKFIH grants 115479, 128088, and 130909, and the project EFOP-3.6.1-16-2016-00022 co-financed by the European Union and the European Social Fund.

In case $\ell \geq 3$ there is hardly anything known. The authors of [1] noted (without proof) that their methods probably make it possible to prove $P_N(3) \ll N^{3/5+\varepsilon}$ and $P_N(\ell) \ll N^{1/2+\varepsilon}$ ($\ell \geq 4$). Hajdu and Tengely [6] showed that (up to equivalence) for any $\ell \geq 2$ there is a unique arithmetic progression $ax+b$ which contains the most ℓ-th powers asymptotically, that is, which maximizes the expression

$$\lim_{N\to\infty} \frac{|\{x : ax+b \text{ is an } \ell\text{-th power, } 0 \leq x < N\}|}{\sqrt[\ell]{N}}.$$

(In fact, for $\ell = 4$ there are two such progressions.) They could describe these arithmetic progressions $a_\ell x + b_\ell$ explicitly. Based upon their results, they extended Rudin's conjecture (1) for any $\ell \geq 2$ (by replacing $24x+1$ by $a_\ell x + b_\ell$ and changing the right hand side accordingly), and proved that for $\ell = 3, 4$ for certain small values of N. Note that this asymptotic ('global') version of the problem is simpler than the original 'local' one, namely when we concentrate on a finite part of the progressions. The reason is that the asymptotic approach brings in an 'averaging' effect, which roughly speaking makes it possible to concentrate on a complete (finite) period of a progression $ax+b$ modulo a.

In this note we prove that for any positive ε there is an ℓ_0 depending only on ε such that for $\ell > \ell_0$ the number of ℓ-th powers among the first N terms of any integral arithmetic progression is below $(1+\varepsilon)\sqrt[\ell]{N}$, provided that N is large enough in terms of ε, ℓ and the parameters of the progression. The important feature of ℓ_0 is that it is uniform in the sense that it depends only on ε, it is independent of the progression. This result is sharp in the sense that for infinitely many ℓ, one can find a constant $c_1 = c_1(\ell) > 1$ and an arithmetic progression having more than $c_1\sqrt[\ell]{N}$ ℓ-th powers among its first N terms, for all N large enough. We also give a uniform, sharp upper bound for the number of powers (with not fixed exponents) among the first N terms of arithmetic progressions. In our proofs we combine a classical result of Wigert [11] concerning the number of divisors of positive integers, a recent result of Hajdu and Tengely [6] concerning arithmetic progressions containing the most ℓ-th powers asymptotically, and a new assertion answering a question of Hajdu and Tengely from [6].

2. New results

Now we give our main results. We use the notation from the introduction.

Theorem 2.1. *For every $\varepsilon > 0$ there is an ℓ_0 depending only on ε such that for any $\ell > \ell_0$ we have $P_{a,b;N}(\ell) \leq (1+\varepsilon)\sqrt[\ell]{N}$, whenever $N > N_0$. Here $N_0 = N_0(\varepsilon, \ell, a, b)$ depends on ε, ℓ, a, b.*

Remarks. The above theorem is sharp in the sense that $1+\varepsilon$ cannot be replaced by 1, and $\ell > \ell_0$ is also necessary. Indeed, Theorem 1 of [6] (see also the Remarks after it) implies that for infinitely many exponents $\ell \geq 2$ there exists a $\delta_\ell > 0$ and an arithmetic progression $a_\ell x + b_\ell$ with $P_{a_\ell,b_\ell;N}(\ell) > (1+\delta_\ell)\sqrt[\ell]{N}$ for all $N > N_0$. Here $N_0 = N_0(\ell)$ depends only on ℓ.

It is clear that if an arithmetic progression $ax+b$ contains an ℓ-th power then it contains infinitely many, and we have

$$P_{a,b;N}(\ell) > \frac{1}{2a}\sqrt[\ell]{N}$$

for $N > N_0$, where N_0 depends on a, b.

We also mention that on our way to prove Theorem 2.1, we answer a question of Hajdu and Tengely [6] (see Proposition 3.1).

We also give a uniform upper bound for the number of powers in arithmetic progressions. For this, let $P_{a,b;N}(*)$ denote the number of (arbitrary) powers among the first N terms of the arithmetic progression $ax+b$ $(x \geq 0)$.

Theorem 2.2. *Let $ax+b$ $(x \geq 0)$ be an arithmetic progression. Then for any $\varepsilon > 0$ there exists an N_0 such that*

$$P_{a,b;N}(*) < \left(\sqrt{\frac{8}{3}} + \varepsilon\right)\sqrt{N} \tag{2}$$

for any $N > N_0$. Here $N_0 = N_0(\varepsilon, a, b)$ depends only on ε, a, b.

Remark. One can easily check (see also e.g. Theorem 1 of [6]) that

$$\lim_{N\to\infty} \frac{P_{24,1;N}(2)}{\sqrt{N}} = \sqrt{\frac{8}{3}}.$$

This shows that the above result is sharp.

Further, it is also easy to see that if $\gcd(a,b) = 1$ then there exist infinitely many exponents ℓ such that $ax+b$ contains ℓ-th powers. Note that here the condition $\gcd(a,b) = 1$ cannot be dropped: for example, the arithmetic progression $4x+2$ $(x \geq 0)$ contains no powers at all.

3. Proofs

To prove Theorem 2.1 we shall need some known and new assertions. The next lemma is a result of Hajdu and Tengely [6]. For its formulation, we need to introduce some new notions and notation (which will play important roles also later on). For any $\ell \geq 2$ and arithmetic progression $ax+b$ put

$$M_{a,b}(\ell) := |\{u : 0 \leq u < a,\ u^\ell \equiv b \pmod a\}|$$

and $S_{a,b}(\ell) := M_{a,b}(\ell) a^{\frac{1}{\ell}-1}$.

Lemma 3.1. *For any $\ell \geq 2$ and for any arithmetic progression $ax+b$ we have $S_{a,b}(\ell) \leq S(\ell)$, where*

$$S(\ell) = \begin{cases} \sqrt{\frac{8}{3}}, & \text{if } \ell = 2, \\ \prod\limits_{\substack{p \text{ prime},\ p-1 \mid \ell, \\ \frac{\log p}{\log p - \log(p-1)} > \ell}} (p-1) p^{\frac{1}{\ell}-1}, & \text{otherwise.} \end{cases}$$

Proof. The statement is the first half of Theorem 1 of [6]; see also the notation in its proof on p. 970 of [6]. □

Remark. The inequality $S_{a,b}(\ell) \leq S(\ell)$ is sharp: for any ℓ, by an appropriate choice of $ax+b$ (given in [6]) we get equality. Observe that for ℓ odd, we have $S(\ell) = 1$.

In the proofs of Theorems 2.1 and 2.2 we shall need the following new assertion. This answers a question of Hajdu and Tengely concerning the limit of the sequence $S(\ell)$ (see the 'concrete question' on p. 966 in the Remarks after Theorem 1 in [6]), and we find it of possible independent interest.

Proposition 3.1. *By the notation of Lemma 3.1, for any $\gamma > 0$ there exists an $\ell_1 = \ell_1(\gamma)$ depending only on γ such that for $\ell > \ell_1$ we have*

$$S(\ell) < \exp\left(\ell^{-1+\gamma}\right). \tag{3}$$

In particular, $\lim\limits_{\ell\to\infty} S(\ell) = 1$ holds.

Remark. One can easily check that (3) implies that

$$S(\ell) < 1 + 2\ell^{-1+\gamma}$$

for ℓ large enough.

To prove the above statement, we need the next classical theorem concerning the number of divisors $d(n)$ of a positive integer n.

Lemma 3.2. *If $\varepsilon > 0$, $X > X_0(\varepsilon)$ then we have*

$$\max_{n \leq X} d(n) < \exp\left((\log 2 + \varepsilon)\frac{\log X}{\log\log X}\right).$$

Proof. This is a classical result of Wigert [11]. Note that in [7], p. 56 a stronger form of this assertion is given, however, the above inequality is sufficient for our present purposes. □

Proof of Proposition 3.1. As one can easily check by a direct calculation, the function $(t-1)t^{1/\ell-1}$ is strictly monotone increasing for $t>0$, for any fixed $\ell \geq 3$. Thus, as for $\ell \geq 3$ the product appearing in $S(\ell)$ has at most $d(\ell)$ terms and in every term $p \leq \ell+1$ holds, we have

$$1 \leq S(\ell) \leq \left(\ell(\ell+1)^{1/\ell-1}\right)^{d(\ell)} < \left(\sqrt[\ell]{\ell}\right)^{d(\ell)}.$$

Here we also used that by the condition $\frac{\log p}{\log p - \log(p-1)} > \ell$, the terms appearing in $S(\ell)$ are greater than 1. Now by Lemma 3.2 we get that

$$S(\ell) < \exp\left(\frac{d(\ell)\log\ell}{\ell}\right) < \exp\left(\frac{\exp\left(\frac{\log\ell}{\log\log\ell}\right)\log\ell}{\ell}\right) =$$

$$= \exp\left(\exp\left(\frac{\log\ell}{\log\log\ell} + \log\log\ell - \log\ell\right)\right) < \exp(\ell^{-1+\gamma})$$

hold, for any $\gamma > 0$ with $\ell > \ell_1$, where $\ell_1 = \ell_1(\gamma)$ depends only on γ. Thus the first part of the statement is proved. The second part of the claim, taking any γ with $0 < \gamma < 1$, from this immediately follows. □

Now we can give the

Proof of Theorem 2.1. To bound $P_{a,b;N}(\ell)$, we need to give an upper bound for the number of ℓ-th powers among the numbers

$$b, a+b, \dots, a(N-1)+b.$$

In view of that N_0 depends on a, b, we may assume that $a(N-1)+b \geq 0$. An ℓ-th power u^ℓ belongs to the above terms if its size is 'between' b and $a(N-1)+b$, and $u^\ell \equiv b \pmod{a}$. Thus we see that

$$P_{a,b;N}(\ell) \leq \left(\sqrt[\ell]{aN+|b|} + \sqrt[\ell]{|b|}\right)\frac{M_{a,b}(\ell)}{a} + M_{a,b}(\ell).$$

Here the term in brackets on the right hand side provides an upper bound for the number of (consecutive) integers (forming an interval I) with ℓ-th power of the 'appropriate' size, the factor $M_{a,b}(\ell)/a$ is the ratio of ℓ-th powers in the residue class $b \pmod{a}$, while the last term is to bound the number of possible ℓ-th powers in the progression coming from the last part of I (having less than a elements). This yields

$$P_{a,b;N}(\ell) \leq M_{a,b}(\ell)a^{\frac{1}{\ell}-1}\sqrt[\ell]{N}\left(\sqrt[\ell]{1+\frac{|b|}{aN}} + \sqrt[\ell]{\frac{|b|}{aN}} + \frac{a}{\sqrt[\ell]{aN}}\right). \qquad (4)$$

Let $\varepsilon > 0$ arbitrary. Clearly, there exists an $N_1 = N_1(\varepsilon, \ell, a, b)$ depending on ε, ℓ, a, b such that for $N > N_1$ we have

$$\sqrt[\ell]{1+\frac{|b|}{aN}} + \sqrt[\ell]{\frac{|b|}{aN}} + \frac{a}{\sqrt[\ell]{aN}} < 1 + \frac{\varepsilon}{2}.$$

By Lemma 3.1 this together with (4) implies

$$P_{a,b;N}(\ell) < \left(1+\frac{\varepsilon}{2}\right) S(\ell)\sqrt[\ell]{N}. \tag{5}$$

In view of Proposition 3.1 we can take an ℓ_0 such that

$$S(\ell) < \frac{2+2\varepsilon}{2+\varepsilon}$$

for $\ell > \ell_0$. This by (5) yields that

$$P_{a,b;N}(\ell) < (1+\varepsilon)\sqrt[\ell]{N}$$

under the assumptions made for ℓ and N. Hence our claim follows. □

Now we give the

Proof of Theorem 2.2. Throughout the proof we use the phrase 'N is large enough' to express that N is larger than an appropriate bound depending only on ε, a, b.

Combining (4) and Lemma 3.1 we obtain

$$P_{a,b;N}(2) < \left(\sqrt{\frac{8}{3}} + \frac{\varepsilon}{2}\right)\sqrt{N} \tag{6}$$

for $\ell = 2$ and

$$P_{a,b;N}(\ell) < S(\ell)(a+3)\sqrt[\ell]{N}$$

for $\ell \geq 3$, respectively, for N large enough. In view of Proposition 3.1, the latter assertion implies that there exists an absolute constant C such that

$$P_{a,b;N}(\ell) < C(a+3)\sqrt[\ell]{N} \tag{7}$$

for any $\ell \geq 3$, for N large enough. Further, if N is large enough then we have $aN + b \geq |b|$. Hence if u^ℓ with $|u| > 1$ belongs to $ax + b$ $(0 \leq x < N)$ then we have

$$\ell \leq \frac{\log(aN + |b|)}{\log 2}.$$

(If $u \in \{-1, 0, 1\}$, then we may assume that $\ell \leq 3$.) This together with (6) and (7) gives

$$P_{a,b;N}(*) \leq \sum_{2 \leq \ell \leq \frac{\log(aN+|b|)}{\log 2}} P_{a,b;N}(\ell) = P_{a,b;N}(2) + \sum_{3 \leq \ell \leq \frac{\log(aN+|b|)}{\log 2}} P_{a,b;N}(\ell) <$$

$$< \left(\sqrt{\frac{8}{3}} + \frac{\varepsilon}{2}\right)\sqrt{N} + C(a+3)\frac{\log(aN+|b|)}{\log 2}\sqrt[3]{N} < \left(\sqrt{\frac{8}{3}} + \varepsilon\right)\sqrt{N}$$

for N large enough. This proves the statement. □

Acknowledgements

The authors are grateful to the referees for their helpful and insightful remarks and suggestions. They also would like to express their thanks to Attila Bérczes for driving their attention to the problem solved by Theorem 2.2.

References

[1] E. Bombieri, A. Granville and J. Pintz, *Squares in arithmetic progressions*, Duke Math. J. **66** (1992), 369–385.

[2] E. Bombieri and U. Zannier, *A note on squares in arithmetic progressions. II*, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei **13** (2002), 69–75.

[3] P. Erdős, *Quelques problémes de théorie des nombres*, Monographies de L'Enseignement Mathématique **6** 81–135, L'Enseignement Mathématique, Université Geneva, 1963.

[4] S. Finch, G. Martin and P. Sebah, *Roots of unity and nullity modulo n*, Proc. Amer. Math. Soc. **138** (2010), 2729–2743.

[5] A. Granville, *Squares in Arithmetic Progressions and Infinitely Many Primes*, Amer. Math. Monthly **124** (2017), 951–954.

[6] L. Hajdu and Sz. Tengely, *Powers in arithmetic progressions*, Ramanujan J. **55** (2021), 965–986.

[7] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory, I. Classical Theory*, Cambridge Univ. Press, Cambridge, 2007.

[8] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, Inc., New York, 1991.

[9] W. Rudin, *Trigonometric series with gaps*, J. Math. Mech. **9** (1960), 203–227.

[10] E. Szemerédi, *The number of squares in an arithmetic progression*, Stud. Sci. Math. Hungar. **9** (1974), 417.

[11] S. Wigert, *Sur l'ordre de grandeur du nombre des diviseurs d'un entier*, Ark. Mat. **3** (1906/7), 1–9.

L. Hajdu, Á. Papp
University of Debrecen, Institute of Mathematics
H-4002 Debrecen, P.O. Box 400.
Hungary
Email address: hajdul@science.unideb.hu
Email address: papp.agoston@science.unideb.hu