Noname manuscript No.
(will be inserted by the editor)

Powers in arithmetic progressions

Lajos Hajdu · Szabolcs Tengely

Received: date / Accepted: date

Abstract We investigate the function $P_{a,b;N}(\ell)$ describing the number of ℓ-th powers among the first N terms of an arithmetic progression $ax+b$. We completely describe the arithmetic progressions containing the most ℓ-th powers asymptotically. Based upon these results we formulate problems concerning the maximum of $P_{a,b;N}(\ell)$, and we give affirmative answers to these questions for certain small values of ℓ and N.

Keywords perfect powers · arithmetic progressions

Mathematics Subject Classification (2010) 11B25 · 11N64 · 11G30 · 11D25

1 Introduction

Let a, b, ℓ be integers with $a > 0$ and $\ell \geq 2$, and write $P_{a,b;N}(\ell)$ for the number of ℓ-th powers among the first N terms $b, \ldots, a(N-1)+b$ of the arithmetic progression $ax+b$ ($x \geq 0$). Let $P_N(\ell)$ be the maximum of these values taken over all arithmetic progressions $ax+b$. The case of squares has

Research supported in part by the NKFIH grants K115479 and K128088 and by the projects EFOP-3.6.1-16-2016-00022 and EFOP-3.6.2-16-2017-00015, co-financed by the European Union and the European Social Fund.

Lajos Hajdu
University of Debrecen, Institute of Mathematics
H-4002 Debrecen, P.O. Box 400
Hungary
E-mail: hajdul@science.unideb.hu

Szabolcs Tengely
University of Debrecen, Institute of Mathematics
H-4002 Debrecen, P.O. Box 400
Hungary
E-mail: tengely@science.unideb.hu

been intensively studied. An old conjecture of Erdős [7] predicted that $P_N(2) = o(N)$ should hold. This was proved by Szemerédi [17]. Later, the bound has been considerably improved. Bombieri, Granville and Pintz [1] showed that $P_N(\ell) < O(N^{2/3+o(1)})$. This bound was refined to $O(N^{3/5+o(1)})$ by Bombieri and Zannier [2]. Both papers applied deep methods based upon elliptic and higher genus curves, Falting's theorem, the distribution of primes and other ingredients; see also the neat short paper of Granville [10] for related results and remarks. In fact, there is a conjecture due to Rudin (see [12], end of paragraph 4.6) which predicts a much stronger behavior of $P_N(2)$, namely, that $P_N(2) = O(\sqrt{N})$ should be valid. A stronger form of this conjecture even says that we have

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

for $N \geq 6$. The first equality here has been recently verified to be true up to $N \leq 52$ by González-Jiménez and Xarles [9]. Note that by a classical result formulated by Fermat, with first published proof due to Euler, there are no four squares in arithmetic progression. This in view of the progression $1, 25, 49$ implies the first equality in (1) for $N \leq 4$. (The case $N = 5$ is exceptional; for details, see [9].)

As far as we know, except for a few related remarks in [1], the case of general ℓ-th powers has not been studied yet. In this paper we consider the problem in this generality. First we establish a theorem which completely describes the arithmetic progressions containing the most ℓ-th powers asymptotically. It will turn out that for every $\ell \neq 4$, this progression is unique (up to trivial transformations). In the case $\ell = 4$ there are two 'best' progressions. Based upon this theorem, we suggest two problems, which are the extensions of Rudin's conjecture to the case of general exponents ℓ. We think that the answer to the questions proposed is affirmative. To support this, using elliptic and higher genus curves we provide numerical results for $\ell = 3$ (up to $N < 20$) and $\ell = 4$ (up to $N < 6$).

The structure of the paper is the following. In the next section we give our principal result (together with its proof) and formulate our problems. Then in the last section we provide our numerical results supporting that the answer to our questions should be affirmative.

2 Arithmetic progressions containing the most ℓ-th powers asymptotically

First we need to introduce some notation. Fix any exponent $\ell \geq 2$. Let a be a positive integer (the difference of our progression), b be an integer, and put

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

It is clear that for any ℓ, a, b this limit exists, but it will also be obvious from our arguments. So in particular, we have $S_{a,b}(\ell) = O(\sqrt[\ell]{N})$. Then we let

$$S_a(\ell) = \max_{b \in \mathbb{Z}} S_{a,b}(\ell).$$

Note that clearly, $S_{a,b}(\ell)$ does not actually depend on b, only on the residue class of b modulo a. Thus the above maximum is taken only over a finite set, hence it exists. Finally, set

$$S(\ell) = \max_{a \in \mathbb{N}} S_a(\ell).$$

It is not that obvious that this maximum also exists. Our theorem below shows that $S(\ell)$ actually exists, it even provides a precise formula for it, furthermore, it completely describes the arithmetic progressions on which it is taken.

For its smooth formulation we need a further notion. Let $\ell \geq 2$ and let $ax+b$ be an arithmetic progression. By an ℓ-transformation of this progression we mean an arithmetic progression of the shape

$$(az^\ell)x + (b + ta)z^\ell,$$

where z is a positive integer and t is an arbitrary integer.

Theorem 1 *$S(\ell)$ exists for any $\ell \geq 2$ and we have*

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

Further, for the arithmetic progression $ax + b$ we have $S_{a,b}(\ell) = S(\ell)$ if and only if it is an ℓ-transformation of

$$a^*x + b^*$$

with

$$a^* = \begin{cases} 24, & \text{if } \ell = 2, \\ 5 \text{ or } 80, & \text{if } \ell = 4, \\ \displaystyle\prod_{\substack{p \text{ prime, } p-1 \mid \ell, \\ \frac{\log p}{\log p - \log(p-1)} > \ell}} p, & \text{otherwise,} \end{cases}$$

and

$$b^* = \begin{cases} 0, & \text{if } a^* = 1, \\ 1, & \text{otherwise.} \end{cases}$$

Remarks. First note that clearly, we could take $b^* = 1$ for $a^* = 1$ as well. Our choice for b^* in the theorem in this case is just to keep the convention $0 \leq b^* < a^*$.

Observe that for ℓ odd, the products in the statement are empty, so we have

$$S(\ell) = a^* = 1$$

in this case. That is, for odd values of ℓ, the 'best' progression (in the above sense) is the trivial one x, or any of its ℓ-transformations. On the other hand, there are infinitely many even values of ℓ with $S(\ell) > 1$ and $a^* > 1$. For example, taking $\ell = p - 1$ with any odd prime p, a simple calculation shows that $p \mid a^*$ and $S(\ell) \geq \ell(\ell+1)^{\frac{1}{\ell}-1} > 1$.

We also mention that the expression $\log p/(\log p - \log(p-1))$ appearing in the products above is strictly monotone increasing. So after a certain point all primes p with $p - 1 \mid \ell$ will be included in these products. One can easily construct (even) values of ℓ such that a^* is divisible 'many' primes. We omit the details, and just say that it could be interesting to explore further properties of the values a^* and the sequence $S(\ell)$. As a concrete question, we propose the following. Is it true that

$$\lim_{\ell \to \infty} S(\ell) = 1 \ ?$$

We think that the answer is affirmative, and probably it is not that difficult to check this assertion.

Extending the problems and conjectures concerning $\ell = 2$ to the general case $\ell \geq 2$, one may wonder whether the asymptotically 'best' progression for ℓ-th powers is also the 'best' up to any N, or at least up to any N which is large enough. More precisely, we suggest the following problems.

Problem 1. For fixed $\ell \geq 2$, for any arithmetic progression $ax + b$ and $N \geq 1$ set

$$P_{a,b;N}(\ell) = |\{x : ax + b \text{ is an } \ell\text{-th power}, \ 0 \leq x < N\}|.$$

Is it true that there exists an N_0 such that for any $N > N_0$

$$\max_{a>0, \ b\geq 0} P_{a,b;N}(\ell) = P_{a^*,b^*;N}(\ell)$$

holds? Here for the special case $\ell = 4$ we use the convention that

$$P_{a^*,b^*;N}(4) = \max(P_{5,1;N}(4), P_{80,1;N}(4)).$$

Problem 2. Use the notation from Problem 1, and for ℓ odd and $N \geq 1$ let $b^\times$ be the largest ℓ-th power being at most $(N-1)/2$, that is

$$b^\times = \left\lfloor \sqrt[\ell]{\frac{N-1}{2}} \right\rfloor.$$

Is it true that for any odd ℓ there exists an N_0 such that for any $N > N_0$

$$\max_{a>0, \ b\in\mathbb{Z}} P_{a,b;N}(\ell) = P_{1,-b^\times;N}(\ell)$$

holds?

Remarks. First we note that affirmative answers for the questions in the above problems would yield that

$$\max_{a>0,\ b\in\mathbb{Z}} P_{a,b;N}(\ell) = O(\sqrt[\ell]{(N)}),$$

providing a positive answer to the conjecture of Rudin, extended to any exponent ℓ.

We also mention that in case of $\ell = 4$ none of the two 'best' progressions is 'better' then the other. In fact, though

$$|P_{5,1;N}(4) - P_{80,1;N}(4)| \le 1$$

for any N,

$$P_{5,1;N}(4) - P_{80,1;N}(4)$$

changes sign infinitely often. These assertions can be easily verified. This is the reason of the exceptional case of $\ell = 4$ in Problem 1.

Our next point here concerns why we distinguish Problems 1 and 2. The reason is that when ℓ is odd, then a shift to the negative direction may increase the value of $P_{a,b;N}(\ell)$. For example, for $\ell = 3$, the progression $x-1$ will contain more cubes then the progression x for $x = 0, 1, \dots, N-1$, for any $N \ge 1$. On the other hand, a shift into the positive direction does not seem to be 'wise' heuristically: the reason is that close to zero the 'density' of ℓ-th powers is larger than away from zero. So it seems to be the best to keep b in the interval $0 \le b < a$ for given a in this case.

We mention that in Problem 1 one certainly needs to take $N_0 > 2$, at least for many ℓ. Indeed, if $a^* > 1$ and $a^* + 1$ is not an ℓ-th power then we have e.g.

$$P_{1,0;2}(\ell) = 2 > 1 = P_{a^*,b^*;2}(\ell).$$

Finally, we note that in case of Problem 2 it might be the case that $N_0 = 1$ is a good choice. However, here we do not have a fixed progression: we always (or at least time to time) 'shift' the 'asymptotically best' progression x to the left to get the 'best' progression for N: our $b^\times$ depends also on N. (As ℓ is odd, we know that now $a^* = 1$.)

We shall be concerned with Problems 1 and 2 in the next section, now we head forward the proof of Theorem 1. For this we shall need the following lemma. (See [11] Corollaries 2.42 and 2.44, or Lemma 6 of [8] for a formulation similar to the one below.)

Lemma 1 *Let ℓ and n be positive integers greater than one, and write $U_\ell(n)$ for the number of ℓ-th roots of unity modulo n. Further, let $\nu_p(\ell)$ denote the exponent of a prime p in the factorization of ℓ.*

i) We have $U_\ell(2) = 1$, and if ℓ is odd, then $U_\ell(2^\alpha) = 1$ for any $\alpha \ge 1$. If ℓ is even, then we have

$$U_\ell(2^\alpha) = 2^{\min(\nu_2(\ell)+1,\alpha-1)}$$

for any $\alpha \ge 2$.

ii) Let p be an odd prime. Then for any $\alpha \geq 1$ we have

$$U_\ell(p^\alpha) = p^{\min(\nu_p(\ell),\alpha-1)} \gcd(\ell, p-1)$$

.

Proof (Proof of Theorem 1.) Let a, b be integers with $a > 0$. As we mentioned earlier, without loss of generality we may assume that $0 \leq b < a$. In what follows, we shall always use this convention, unless stated differently. The total number of ℓ-th powers between the first term b and the N-th term $a(N-1)+b$ of the progression $ax + b$ ($x \geq 0$) is clearly $\sqrt[\ell]{aN} + o(1)$. The question is that how many of these (roughly) $\sqrt[\ell]{aN}$ ℓ-th powers belong to the progression $ax+b$, for a given b. Obviously, any ℓ-th power belongs to *some* progression $ax + b$ with $0 \leq b < a$. In what follows, we shall use these observations without any further mentioning.

To determine $S_a(\ell)$ for given a, we should decide which is the 'best' choice for b. Clearly, those ℓ-th powers u^ℓ will belong to the progression $ax + b$ for which

$$u^\ell \equiv b \pmod{a}.$$

That is, we should find the b for which

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

is maximal. Write

$$M_a(\ell) = \max_{0 \leq b < a} M_{a,b}(\ell)$$

for this maximum. Observe that these quantities are of utmost importance for us indeed, as we clearly have

$$S_{a,b}(\ell) = \frac{\frac{M_{a,b}(\ell)}{a}\sqrt[\ell]{aN}}{\sqrt[\ell]{N}} = M_{a,b}(\ell) a^{\frac{1}{\ell}-1}$$

and hence

$$S_a(\ell) = M_a(\ell) a^{\frac{1}{\ell}-1}.$$

To get $S(\ell)$ for an arbitrary but fixed $\ell \geq 2$, we need to maximize the above expression as a runs through $\mathbb{N}$.

We make two simple, but important observations. Firstly, note that we have

$$S(\ell) = \max_{a \in \mathbb{N}} S_a(\ell) \geq S_1(\ell) = M_1(\ell) \cdot 1^{\frac{1}{\ell}-1} = 1,$$

when our progression is just $1 \cdot x + 0 = x$. Secondly, observe that $S_a(\ell)$, or equivalently, $M_a(\ell)$ is multiplicative in a, for any fixed ℓ. To see this, write $a = a_1 a_2$ with $\gcd(a_1, a_2) = 1$. In this part of the argument it is more convenient to work with general $b \in \mathbb{Z}$ instead of b-s with $0 \leq b < a$. So let $b \in \mathbb{Z}$ be such that $M_a(\ell) = M_{a,b}(\ell)$. Clearly,

$$u^\ell \equiv b \pmod{a}$$

if and only if

$$u^\ell \equiv b \pmod{a_1} \quad \text{and} \quad u^\ell \equiv b \pmod{a_2}.$$

This by the Chinese Remainder Theorem shows that

$$M_a(\ell) = M_{a,b}(\ell) = M_{a_1,b}(\ell) M_{a_2,b}(\ell) \le M_{a_1}(\ell) M_{a_2}(\ell). \tag{2}$$

Let now $b_1, b_2 \in \mathbb{Z}$ be such that

$$M_{a_1}(\ell) = M_{a_1,b_1}(\ell) \quad \text{and} \quad M_{a_2}(\ell) = M_{a_2,b_2}(\ell).$$

Let b be such that

$$\begin{cases} b \equiv b_1 \pmod{a_1}, \\ b \equiv b_2 \pmod{a_2}. \end{cases}$$

Now if

$$u^\ell \equiv b_1 \pmod{a_1} \quad \text{and} \quad v^\ell \equiv b_2 \pmod{a_2},$$

and w is such that

$$\begin{cases} w \equiv u \pmod{a_1}, \\ w \equiv v \pmod{a_2} \end{cases}$$

then

$$w^\ell \equiv b \pmod{a}.$$

This by the Chinese Remainder Theorem implies that

$$M_a(\ell) \ge M_{a,b}(\ell) \ge M_{a_1,b_1}(\ell) M_{a_2,b_2}(\ell) = M_{a_1}(\ell) M_{a_2}(\ell). \tag{3}$$

Then (2) and (3) together give

$$M_a(\ell) = M_{a_1}(\ell) M_{a_2}(\ell),$$

so $M_a(\ell)$ is multiplicative, indeed. As we clearly also have

$$S_a(\ell) = M_a(\ell) a^{\frac{1}{\ell}-1} = M_{a_1}(\ell) M_{a_2}(\ell) {a_1}^{\frac{1}{\ell}-1} {a_2}^{\frac{1}{\ell}-1} = S_{a_1}(\ell) S_{a_2}(\ell),$$

we see that $S_a(\ell)$ is multiplicative, as well.

Thus to find $S(\ell)$, and the a-s which provide

$$S(\ell) = S_a(\ell),$$

and ultimately the b-s which provide

$$S_a(\ell) = S_{a,b}(\ell)$$

for these a-s, we may restrict our attention to arithmetic progressions $ax + b$ with $a = p^\alpha$ and

$$S_{p^\alpha,b}(\ell) \ge 1.$$

From this point on we switch back to use the convention $0 \le b < a$ again. (As $S_{a,b}(\ell)$ and $M_{a,b}(\ell)$ depend on b only through its residue modulo a, we can do

that without any problem.) For any b with $0 \leq b < p^\alpha$, by the definition of $M_{p^\alpha,b}(\ell)$ there exist integers

$$0 \leq u_1 < \cdots < u_{M_{p^\alpha,b}(\ell)} < p^\alpha$$

such that

$$u_1^\ell \equiv \cdots \equiv u_{M_{p^\alpha,b}(\ell)}^\ell \equiv b \pmod{p^\alpha}. \tag{4}$$

To find those values of p^α and b for which $S_{p^\alpha,b}(\ell) \geq 1$, we distinguish three cases.

CASE 1. Suppose first that $p \nmid b$. Then of course we also have $p \nmid u_i$ ($i = 1, \ldots, M_{p^\alpha,b}(\ell)$). Thus multiplying the sequence of congruences (4) with $u_1^{-\ell}$ modulo p^α, we see that $M_{p^\alpha,b}(\ell) = M_{p^\alpha,1}(\ell)$. So for any b with $p \nmid b$ Lemma 1 shows that

$$S_{p^\alpha,b}(\ell) = \begin{cases} 2^{\alpha\left(\frac{1}{\ell}-1\right)}, & \text{if } p = 2 \text{ and } \ell \text{ is odd,} \\ 2^{\min(\nu_2(\ell)+1,\alpha-1)} \cdot 2^{\alpha\left(\frac{1}{\ell}-1\right)}, & \text{if } p = 2 \text{ and } \ell \text{ is even,} \\ p^{\min(\nu_p(\ell),\alpha-1)} \gcd(\ell, p-1) \cdot p^{\alpha\left(\frac{1}{\ell}-1\right)}, & \text{if } p \text{ is an odd prime.} \end{cases} \tag{5}$$

We (naturally) distinguish two subcases. Take first $p = 2$. If $S_{p^\alpha,b}(\ell) \geq 1$ then by (5) we clearly have that ℓ is even, $\alpha > 1$ and

$$\min(\nu_2(\ell) + 1, \alpha - 1) + \alpha\left(\frac{1}{\ell} - 1\right) \geq 0. \tag{6}$$

If

$$\nu_2(\ell) + 1 \geq \alpha - 1$$

then on the one hand

$$\ell \geq 2^{\alpha-2},$$

and on the other hand, by (6)

$$\alpha \geq \ell.$$

Hence we get that

$$(p^\alpha, \ell) = (4, 2),\ (8, 2),\ (16, 4)$$

in this case, with equality in (6) for the first and third pairs and strict inequality in (6) for the second one. Otherwise, if

$$\nu_2(\ell) + 1 < \alpha - 1$$

then as (6) implies

$$\nu_2(\ell) + \frac{\alpha}{\ell} \geq \alpha - 1, \tag{7}$$

we get

$$\alpha > \ell.$$

As $\ell \geq 2^{\nu_2(\ell)}$ this gives

$$\nu_2(\ell) < \frac{\log \alpha}{\log 2}.$$

So as $\ell \geq 2$, inequality (7) by a simple calculation yields that $\alpha \leq 8$. Hence we easily get that the only possible value of p^α and ℓ with $S_{p^\alpha}(\ell) \geq 1$ is given by

$$(p^\alpha, \ell) = (16, 2),$$

when in fact we have $S_{16}(2) = 1$.

Let now p be an odd prime. Then by (5) we know that $S_{p^\alpha,b}(\ell) \geq 1$ if and only if

$$\min(\nu_p(\ell), \alpha - 1) + \log_p \gcd(\ell, p-1) + \alpha\left(\frac{1}{\ell} - 1\right) \geq 0. \tag{8}$$

Suppose first that

$$\nu_p(\ell) \geq \alpha. \tag{9}$$

Then (8) implies that

$$p^\alpha \geq \left(\frac{p}{\gcd(\ell, p-1)}\right)^\ell,$$

whence by (9)

$$\ell \geq \left(\frac{p}{\gcd(\ell, p-1)}\right)^\ell.$$

This gives that

$$\frac{p}{\gcd(\ell, p-1)} < 2,$$

therefore

$$\gcd(\ell, p-1) = p - 1,$$

that is

$$p - 1 \mid \ell.$$

Write $\ell = t(p-1)$ with $t \geq 1$, and let $t = p^\beta s$ with $p \nmid s$. Thus, obviously, $\nu_p(\ell) = \beta$. In view of (9), as $\alpha \geq 1$, we have $\beta \geq 1$. Hence from (8) and (9) we obtain

$$\frac{\beta}{p^\beta s(p-1)} \geq \log_p \frac{p}{p-1},$$

so

$$\frac{\beta \log p}{p^\beta} \geq \log\left(1 + \frac{1}{p-1}\right)^{p-1}.$$

As $\beta \geq 1$, a simple calculation yields that the above inequality is impossible, so we cannot have $S_{p^\alpha}(\ell) \geq 1$ in this case.

Suppose next that

$$\nu_p(\ell) < \alpha. \tag{10}$$

Then (as $\nu_p(\ell) \leq \alpha - 1$) (8) implies that

$$\nu_p(\ell) + \log_p \gcd(\ell, p-1) + \alpha\left(\frac{1}{\ell} - 1\right) \geq 0. \tag{11}$$

If we would have $\nu_p(\ell)+1<\alpha$, then certainly $\nu_p(\ell)+2\le\alpha$, which by the above inequality yields

$$\log_p \gcd(\ell,p-1)+\frac{\alpha}{\ell}\ge 2.$$

Hence

$$\alpha>\ell$$

in this case. As $\ell\ge 3^{\nu_p(\ell)}$, this gives

$$\frac{\log\alpha}{\log 3}>\nu_p(\ell).$$

Then using (11) we easily obtain a contradiction. That is, we are left with the only possibility

$$\alpha=\nu_p(\ell)+1.$$

Then (11) implies that

$$\frac{\nu_p(\ell)+1}{\ell}\ge\log_p\frac{p}{\gcd(\ell,p-1)}.$$

Set $d=\gcd(\ell,p-1)$, $\ell=dt$ and $t=p^\beta s$ with $p\nmid s$. Then we have

$$\frac{\beta+1}{dp^\beta s}\ge\log_p\frac{p}{d}. \tag{12}$$

We show that (12) implies that $\beta=0$. For this, observe that for any $\beta\ge 1$ we have

$$\frac{2}{dp}\ge\frac{\beta+1}{dp^\beta s}.$$

So to prove that (12) implies $\beta=0$ indeed, it is sufficient to check that

$$g_p(d):=1-\frac{\log d}{\log p}-\frac{2}{dp}>0$$

for any odd prime p and $1\le d\le p-1$. Taking the derivative (in d) of $g_p(d)$, one can easily see that $g_p(d)$ is strictly monotone decreasing in d (even as a positive real variable). So to check the above inequality, it is sufficient to verify that

$$g_p(p-1)=1-\frac{\log(p-1)}{\log p}-\frac{2}{(p-1)p}>0.$$

We rewrite the above inequality as

$$\log\left(1+\frac{1}{p-1}\right)^{p-1}>\frac{2\log p}{p}.$$

Since the left hand side is strictly monotone increasing (and tends to 1) while the right hand side is strictly monotone decreasing (and tends to 0), and the

assertion is valid for $p = 3$, our claim follows. That is, we get $\beta = 0$, whence $\nu_p(\ell) = 0$ and $\alpha = 1$. So (12) reads as

$$\frac{1}{ds} \geq \log_p \frac{p}{d}.$$

We show that it is possible only for $d = p - 1$. Observe that $d = 1$ can be immediately excluded, since then by $\ell \geq 2$, $s > 1$ must hold. Thus the case $p = 3$ is done: then we can only have $d = p - 1 = 2$. So it is sufficient to prove that

$$h_p(d) := 1 - \frac{1}{d} - \frac{\log d}{\log p} > 0$$

for all odd primes p with $p \geq 5$ and d with $2 \leq d \leq (p-1)/2$. Taking the derivative of $h_p(d)$ in d, we get that it it is strictly monotone increasing for $2 \leq d < \log p$ and strictly monotone decreasing for $d > \log p$. Thus to show our claim, we only need to verify that

$$h_p(2) > 0 \quad \text{and} \quad h_p\left(\frac{p-1}{2}\right) > 0,$$

that is

$$\frac{1}{2} - \frac{\log 2}{\log p} > 0 \quad \text{and} \quad 1 - \frac{2}{p-1} - \frac{\log(p-1) - \log 2}{\log p} > 0,$$

respectively. Recalling that $p \geq 5$, the first inequality trivially holds. The second inequality can be directly checked for $p = 5$, and for $p \geq 7$ it immediately follows from the stronger assertion

$$(p-1)\log 2 - 2\log p > 0$$

which is easy to check. That is, altogether we get that $d = p - 1$ must hold. Thus (12) gives

$$\ell \leq \frac{\log p}{\log p - \log(p-1)}.$$

Summarizing, $S_{p^\alpha,b}(\ell) \geq 1$ for an odd prime p for some b with $p \nmid b$ if and only if the following properties hold:

$$\alpha = 1, \quad p \nmid \ell, \quad p - 1 \mid \ell, \quad \frac{\log p}{\log p - \log(p-1)} \geq \ell,$$

and $S_{p^\alpha}(\ell) > 1$ precisely when the inequality is strict in the last point. A simple calculation shows that the last two assertions imply the second one. Indeed, if both $p - 1 \mid \ell$ and $p \mid \ell$ would hold, then writing $\ell = \ell_0 p(p-1)$, the last assertion would give

$$\log\left(1 + \frac{1}{p-1}\right)^{p-1} \leq \frac{\log p}{\ell_0 p}$$

with $\ell_0 \geq 1$. However, this does not hold for $p \geq 3$. Further, observe that we cannot have equality in the last assertion. That is, altogether we have that $S_{p^\alpha,b}(\ell) \geq 1$ for an odd prime p for some b with $p \nmid b$ if and only if:

(i) $\alpha = 1$,
(ii) $p - 1 \mid \ell$,
(iii) $\frac{\log p}{\log p - \log(p-1)} > \ell$.

Further, if (i), (ii), (iii) are valid than in fact we have with $S_{p^\alpha}(\ell) > 1$.

To close this case, we make the following simple, but important observation. If $S_{p^\alpha,b}(\ell) \geq 1$ with $p \nmid b$ then we have $b = 1$ with the sole exception of $(p^\alpha, \ell, b) = (16, 2, 9)$. This can be directly checked for $p = 2$. When $p \geq 3$, then recalling $\alpha = 1$, this assertion follows by noting that as $p - 1 \mid \ell$, we have

$$u^\ell \equiv 1 \pmod{p}$$

whenever $p \nmid u$.

CASE 2. Consider next the case where $p \mid b$, but $b \neq 0$. Then writing $u_1 = p^\beta v_1$ with $p \nmid v_1$ in (4), we clearly have $\ell\beta < \alpha$ and certainly also $u_i = p^\beta v_i$ with $p \nmid v_i$ $(i = 1, \ldots, M_{p^\alpha,b}(\ell))$. Thus

$$v_1^\ell \equiv \cdots \equiv v_{M_{p^\alpha,b}(\ell)}^\ell \equiv b' \pmod{p^{\alpha-\ell\beta}}$$

where $b' = b/p^{\ell\beta}$, that is, this case is reduced to CASE 1. There are precisely $M_{p^{\alpha-\ell\beta},b'}(\ell)$ such v_i-s modulo $p^{\alpha-\ell\beta}$. Hence as we may assume that $v_i < p^{\alpha-\beta}$ $(i = 1, \ldots, M_{p^\alpha,b}(\ell))$, we conclude that

$$M_{p^\alpha,b}(\ell) = M_{p^{\alpha-\ell\beta},b'}(\ell) p^{(\ell-1)\beta}. \tag{13}$$

We distinguish two cases. If $p = 2$ then (13) by (5) gives

$$S_{p^\alpha,b}(\ell) = \begin{cases} 2^{(\ell-1)\beta} \cdot 2^{\alpha\left(\frac{1}{\ell}-1\right)}, & \text{if } \ell \text{ is odd,} \\ 2^{\min(\nu_2(\ell)+1,\alpha-\ell\beta-1)} \cdot 2^{(\ell-1)\beta} \cdot 2^{\alpha\left(\frac{1}{\ell}-1\right)}, & \text{if } \ell \text{ is even.} \end{cases}$$

This shows that if $S_{p^\alpha,b}(\ell) \geq 1$ in this case, then ℓ must be even. If ℓ is even, then we get

$$S_{p^\alpha,b}(\ell) = 2^{\min(\nu_2(\ell)+1,\alpha-\ell\beta-1)} \cdot 2^{(\alpha-\ell\beta)\left(\frac{1}{\ell}-1\right)} = S_{p^{\alpha-\ell\beta},1}(\ell).$$

In the second equality we used what we got in CASE 1. So applying again our results obtained in CASE 1, we get that $S_{p^\alpha,b}(\ell) \geq 1$ in this case implies that we have one of

$$(p^{\alpha-\ell\beta}, \ell) = (4, 2),\ (8, 2),\ (16, 2),\ (16, 4),$$

and $S_{p^\alpha,b}(\ell) > 1$ only in the second case. Further, $b = 2^{\ell\beta}$ in all cases except the third one, when $b = 9 \cdot 2^{\ell\beta}$ is also possible.

Let now $p > 2$. Then (13) through (5) gives

$$\begin{aligned} S_{p^\alpha,b}(\ell) &= p^{\min(\nu_p(\ell),\alpha-\ell\beta-1)} \gcd(\ell, p-1) p^{\alpha\left(\frac{1}{\ell}-1\right)} p^{(\ell-1)\beta} = \\ &= p^{\min(\nu_p(\ell),\alpha-\ell\beta-1)} \gcd(\ell, p-1) p^{(\alpha-\ell\beta)\left(\frac{1}{\ell}-1\right)}. \end{aligned}$$

Thus by what we have proved in CASE 1, $S_{p^\alpha,b}(\ell) \geq 1$ implies that $\alpha - \ell\beta = 1$ and $b = p^{\ell\beta}$, and p satisfies the points (ii) and (iii) at the end of CASE 1. In fact, for these values of the parameters we have $S_{p^\alpha,b}(\ell) > 1$.

CASE 3. Finally, assume that $p^\alpha \mid b$, that is, $b = 0$. Then in (4), $u_1, \ldots, u_{M_{p^\alpha,0}(\ell)}$ are just the multiples of $p^{\lceil \alpha/\ell \rceil}$. Thus $M_{p^\alpha,0}(\ell) = p^{\alpha - \lceil \alpha/\ell \rceil}$ and we have

$$S_{p^\alpha,0}(\ell) \leq 1,$$

with equality if and only if $\ell \mid \alpha$.

Now we can build the 'best' modulus a, and even the 'best' arithmetic progressions $ax+b$ based upon the information we gained. For given ℓ, in view of that $S_a(\ell)$ is multiplicative, if

$$S(\ell) = S_a(\ell)$$

then a must be divisible by all prime powers p^α for which $S_{p^\alpha}(\ell) > 1$. By what we have proved so far, if we take a to be the product of these prime powers (taking e.g. the smallest possible exponent for all these primes) then $S_a(\ell)$ is maximal indeed; in particular, $S(\ell)$ exists, and its value is just what is given in the statement. To show that the 'best' a is essentially unique, we need some further discussion. From CASE 1 we see that for $\ell = 4$ there are two possible choices for the 'best' a, given by $a^* = 5, 80$, while in all the other cases from here we get only one possibility, given by $a^* = 2^3 \cdot 3 = 24$ for $\ell = 2$ and

$$a^* = \prod_{\substack{p \text{ is an odd prime} \\ p-1 \mid \ell,\ \frac{\log p}{\log p - \log(p-1)} > \ell}} p$$

for the other choices of ℓ. In all cases with $a^* \neq 1$ we have $b = b^* = 1$. When $a^* = 1$, we could choose b freely. We take $b = b^* = 0$ in this case, to keep our convention $0 \leq b < a$. Observe that in the above expression for a^*, the condition that the prime p is odd in the product is superfluous: the inequality $\log p/(\log p - \log(p-1)) > \ell$ does not hold with $p = 2$ for any ℓ. So these parameters just provide the progressions in the statement. Observe that CASES 2 and 3 show that these progressions (both a^* and b^*) can be multiplied by any ℓ-th power - and then the value $S_{a^*,b^*}(\ell)$ just remains unchanged. Note that this is obvious: $a^*x + b^*$ is an ℓ-th power if and only if $(a^*z^\ell)x + b^*z^\ell$ is an ℓ-th power (for $x \geq 0$), for any $z \geq 1$. Finally, as we already noted, $S_{a^*,b^*}(\ell)$ depends on b^* only through its residue class modulo a^*, so b^* can be shifted by any multiple of a^*. Hence the theorem follows. □

3 Numerical results concerning Problems 1 and 2

In this section we deal with Problems 1 and 2, for $\ell = 3, 4$ for small values of N. We shall start with Problem 2 in case of $\ell = 3$, with $N < 20$. For these values of N Problem 2 suggests that the 'best' progression (containing the

most cubes among its first N terms $b, \dots, a(N-1)+b)$ is given by $a = 1$ and $b = -b^{\times}$, with

$$b^{\times} = \left\lfloor \sqrt[\ell]{\frac{N-1}{2}} \right\rfloor.$$

In particular, for $N < 20$ we have

$$b = -b^{\times} = \begin{cases} 0 & \text{if } N = 1, 2 \\ -1 & \text{if } 3 \le N \le 16, \\ -8 & \text{if } 17 \le N < 20, \end{cases}$$

and the number of cubes in these progressions among the first N terms are given by

$$P_{1,-b^{\times};N}(3) = \begin{cases} 1 & \text{if } N = 1, \\ 2 & \text{if } N = 2, \\ 3 & \text{if } 3 \le N \le 9, \\ 4 & \text{if } 10 \le N \le 16, \\ 5 & \text{if } 17 \le N < 20. \end{cases} \tag{14}$$

Our first result in this section verifies that the above progressions are really the 'best' for $N < 20$, hence providing an affirmative answer for Problem 2 in these cases.

Theorem 2 *Let a, b be integers with $a > 0$. Then for any $N < 20$ we have*

$$P_{a,b;N}(3) \le P_{1,-b^{\times};N}(3).$$

Proof For $N \le 3$ the statement is obvious, so we may assume that $4 \le N \le 19$. To prove the statement, by (14) we need to check that

$$P_{a,b;N}(3) \le \begin{cases} 3 & \text{if } 4 \le N \le 9, \\ 4 & \text{if } 10 \le N \le 16, \\ 5 & \text{if } 17 \le N < 20. \end{cases}$$

So it is natural to split the proof into three subcases.

Suppose first that $4 \le N \le 9$, and assume to the contrary that among the first N terms of the progressions there are four cubes. Then there exists integers n_0, n_1, n_2, n_3 with $0 \le n_0 < n_1 < n_2 < n_3 < N$ such that

$$an_i + b = x_i^3 \quad (i = 0, 1, 2, 3) \tag{15}$$

with some integers x_0, x_1, x_2, x_3. The system (15) yields four genus one curves of the form

$$(n_j - n_i)X^3 + (n_i - n_k)Y^3 + (n_k - n_j)Z^3 = 0, \tag{16}$$

where $0 \le i < j < k \le 3$. We shall check all the possible systems (15). However, some of them can be easily excluded. First, observe that if the indices n_i, n_j, n_k

form an arithmetic progression, then the corresponding genus one curve (16) is just

$$X^3 - 2Y^3 + Z^3 = 0.$$

By a classical result of Dénes [6] we know that this equation has the only solutions

$$(X, Y, Z) = (-u, 0, u), (u, u, u) \ (u \in \mathbb{Z}).$$

So by $N \leq 9$, in this case we cannot have four cubes among the first N terms of our progression. That is, we may assume that n_0, n_1, n_2, n_3 does not contain an arithmetic progression. By symmetry, we may clearly assume further that $n_3 - n_2 \geq n_1 - n_0$, moreover, by shifting the terms that $n_0 = 0$, too. There are 18 quadruples (n_0, n_1, n_2, n_3) with $0 \leq n_0 < n_1 < n_2 < n_3 \leq 8$ with these properties. If we can exclude them all, then we may conclude that our statement is valid for $4 \leq N \leq 9$ indeed. For such a given tuple (n_0, n_1, n_2, n_3) (recalling that we may assume that $n_0 = 0$) we get three genus one curves as follows:

$$\begin{aligned} C_1 : &\quad n_1 x_2^3 - n_2 x_1^3 + (n_2 - n_1) x_0^3 = 0, \\ C_2 : &\quad n_1 x_3^3 - n_3 x_1^3 + (n_3 - n_1) x_0^3 = 0, \\ C_3 : &\quad n_2 x_3^3 - n_3 x_2^3 + (n_3 - n_2) x_0^3 = 0. \end{aligned}$$

In fact we could get a fourth equation as well - however, that is a consequence of the above three ones. We use ideas from [4] (see p. 293) to construct genus two quotients of curves defined by two equations from the above system. Define morphisms

$$\begin{aligned} \zeta_0 &: (x_0 : x_1 : x_2 : x_3) \to (\zeta x_0 : x_1 : x_2 : x_3), \\ \zeta_1 &: (x_0 : x_1 : x_2 : x_3) \to (x_0 : \zeta x_1 : x_2 : x_3), \\ \zeta_2 &: (x_0 : x_1 : x_2 : x_3) \to (x_0 : x_1 : \zeta x_2 : x_3), \\ \zeta_3 &: (x_0 : x_1 : x_2 : x_3) \to (x_0 : x_1 : x_2 : \zeta x_3), \end{aligned}$$

where ζ denotes a primitive cube root of unity. We will use subgroups of the form $H_{i,j} = \langle \zeta_0 \zeta_i, \zeta_0 \zeta_j \rangle$ with $1 \leq i < j \leq 3$. For example, if we take the first two genus one curves C_1 and C_2 defined above with the subgroup $H_{1,2} = \langle \zeta_0 \zeta_1, \zeta_0 \zeta_2 \rangle$, then the corresponding quotient is isomorphic to the genus two hyperelliptic curve given by

$$\begin{aligned} C_{H_{1,2}}^{1,2} : &\quad y^2 = ((n_2 - n_1)(n_3 - n_1)n_3)^2 x^6 + \\ &+ 2((n_3 - n_1)n_3)^2 (2n_1 n_2 - n_1 n_3 - n_2 n_3) x^3 + ((n_3 - n_1)n_3^2)^2. \end{aligned}$$

For given n_1, n_2, n_3 one can compute the quotient by using the Magma [3] procedure `CurveQuotient` and having many numerical examples the general pattern is not too difficult to guess and to prove afterwards. We note that $(1, (n_3 - n_1)(n_1 + n_2 - n_3)n_3)$ is a point on $C_{H_{1,2}}^{1,2}$ (and similarly, we can always find a parametric point on the other curves arising), so we cannot use local arguments to eliminate cases. We use the following strategy. For every

tuple (n_0, n_1, n_2, n_3) we construct all genus two curves $C^{i,j}_{H_{k,m}}$ with $i, j, k, m \in \{1, 2, 3\}$, $i < j$, $k < m$ and select those having Mordell-Weil group of rank at most one. For these curves we can apply the classical Chabauty's method [5] to determine all rational points. For this, and all the other computations we use the program package Magma [3]. We provide some details only for $(n_0, n_1, n_2, n_3) = (0, 1, 3, 8)$, the other cases are similar. We obtain the three genus one curves

$$\begin{aligned} C_1: &\quad x_2^3 - 3x_1^3 + 2x_0^3 = 0, \\ C_2: &\quad x_3^3 - 8x_1^3 + 7x_0^3 = 0, \\ C_3: &\quad 3x_3^3 - 8x_2^3 + 5x_0^3 = 0. \end{aligned}$$

We get the hyperelliptic curve

$$C^{1,2}_{H_{1,2}} : y^2 = 12544x^6 - 163072x^3 + 200704,$$

which is isomorphic to

$$C' : y^2 = 784x^6 - 10192x^3 + 12544.$$

Based on Stoll's articles [14], [15], [16] one computes generators for the Mordell-Weil group. We get that the rank of the Jacobian of the curve is one and

$$\mathrm{Jac}(C')(\mathbb{Q}) = \langle (x^2, -112, 2), (x, 28x^3 + 112, 2), (x - 1, 28x^3 - 84, 2) \rangle,$$

where the first two generators are of order three and the last generates the free part. A standard application of Chabauty's method yields that the only affine rational points on C' are given by

$$\{(0, \pm 112), (1, \pm 56)\}.$$

These points do not give rise to non-constant arithmetic progressions. In a similar way we could eliminate all the other possible quadruples (n_0, n_1, n_2, n_3).

Suppose next that $10 \leq N \leq 16$, and assume to the contrary of our claim that among the first N terms of a progressions $ax+b$ there are five cubes. Then there exists integers n_0, n_1, n_2, n_3, n_4 with $0 \leq n_0 < n_1 < n_2 < n_3 < n_4 < N$ such that

$$an_i + b = x_i^3 \quad (i = 0, 1, 2, 3, 4) \tag{17}$$

with some integers x_0, x_1, x_2, x_3, x_4. Following the steps provided in the case $4 \leq N \leq 9$, we obtain the six genus one curves

$$\begin{aligned} C_1: &\quad (n_1 - n_0)x_2^3 + (n_0 - n_2)x_1^3 + (n_2 - n_1)x_0^3 = 0, \\ C_2: &\quad (n_1 - n_0)x_3^3 + (n_0 - n_3)x_1^3 + (n_3 - n_1)x_0^3 = 0, \\ C_3: &\quad (n_2 - n_0)x_3^3 + (n_0 - n_3)x_2^3 + (n_3 - n_2)x_0^3 = 0, \\ C_4: &\quad (n_1 - n_0)x_2^3 + (n_0 - n_4)x_1^3 + (n_4 - n_1)x_0^3 = 0, \\ C_5: &\quad (n_2 - n_0)x_2^3 + (n_0 - n_4)x_1^3 + (n_4 - n_2)x_0^3 = 0, \\ C_6: &\quad (n_3 - n_0)x_2^3 + (n_0 - n_4)x_1^3 + (n_4 - n_3)x_0^3 = 0. \end{aligned}$$

In fact, we could get more curves, but these are sufficient for our purposes. Using the same morphisms and subgroups $H_{i,j} = \langle \zeta_0\zeta_i, \zeta_0\zeta_j \rangle$ as earlier, we construct genus two curves. If we can find the rational points on one of these curves, then we are finished. However, to do this can be rather troublesome. The question is how to select the 'right' curves for which the computation is feasible and relatively fast. We applied the following method. For a given tuple $(n_0, n_1, n_2, n_3, n_4)$ we considered the collection of genus two curves described above. We computed an upper bound for the rank of the Mordell-Weil group by the Magma procedure `RankBounds`. If the bound was larger than one, or the computation took more than three minutes (when it was interrupted) then we put the curve into a set called 'BadCurves'. Otherwise we computed the Minkowski bound for the maximal order of the number field defined by the degree six polynomial related to the genus two curve and we determined the height constant bound corresponding to the naive height and the canonical height. In the first round we only considered curves with Minkowski bound less than 40000 and height constant at most 16. Having a curve satisfying all the previous conditions we tried to determine generators of the Mordell-Weil group and apply Chabauty's method. Again, we stopped the computation after three minutes if no output had appeared and we enlarged the set 'BadCurves'. If everything went fine, i.e. the rank of the curve (quickly) proved to be at most one, then we included the curve into the set 'GoodCurves' to speed up later computations. In this way, in case of every tuple $(n_0, n_1, n_2, n_3, n_4)$ we could find an arising curve for which all its rational points could be determined. We found that these points do not lead to any arithmetic progression with the required properties, and our statement follows also in this case.

Finally, when $17 \le N \le 19$, then we may already assume that there are at least six cubes among the first N terms of the progression. In this case we followed the method described in the previous situation. We omit the details, and only mention that now we selected curves having Minkowski bound less than 300000 and height constant bound at most 22. Ultimately, we could exclude all the tuples $(n_0, \dots, n_5)$, so we came to a similar conclusion also in this case as before.

The total computational time was 16.6 hours on a Core I7 computer. As a result of them, we concluded that the theorem is valid. □

Now we turn to Problem 1 in case of $\ell = 4$. For this value of ℓ Problem 1 suggests that there are two 'best' progressions (containing the most fourth powers among its first N terms $b, \dots, a(N-1)+b$), given by $(a, b) = (5, 1)$ and $(80, 1)$. A simple calculation shows that for $1 \le N \le 5$ we have

$$P_{5,1;N}(4) \le P_{80,1;N}(4),$$

and the number of fourth powers in the latter progression among its first N terms is given by

$$P_{80,1;N}(4) = \begin{cases} 1 & \text{if } N = 1, \\ 2 & \text{if } 2 \le N \le 5. \end{cases} \tag{18}$$

Our last result verifies that this progression is the 'best' indeed for $N \leq 5$, hence providing an affirmative answer for Problem 1 for these values of N. In fact we prove more: we allow the initial term b of the progression be an arbitrary integer. The reason that in this case we go only up to $N \leq 5$ is that following a similar method as in the proof of Theorem 2, we just could not handle some cases (curves) appearing for $N = 6$.

Theorem 3 *Let a, b be integers with $a > 0$. Then for any $N \leq 5$ we have*

$$P_{a,b;N}(4) \leq P_{80,1;N}(4).$$

Proof The statement is obvious for $N = 1, 2$, so we may assume that $3 \leq N \leq 5$. In view of (18), we need to show that

$$P_{a,b;N}(4) \leq 2$$

for these values of N. Assume to the contrary that for a progression $ax + b$ there are at least three fourth powers among its first N terms ($3 \leq N \leq 5$). So let (n_0, n_1, n_2) with $0 \leq n_0 < n_1 < n_2 \leq N$ be such that

$$an_i + b = x_i^4 \quad (i = 0, 1, 2). \tag{19}$$

If n_0, n_1, n_2 is an arithmetic progression, then we get

$$x_0^4 + x_2^4 = 2x_1^4.$$

Again, by the classical result of Dénes [6] implies that then $x_0 = x_1 = x_2$, a contradiction. So by symmetry, we may assume that we only need to consider the cases

$$(n_0, n_1, n_2) = (0, 1, 3), (0, 1, 4).$$

We shall handle these tuples separately. However, before that it is important to show that here without loss of generality we may assume that x_0, x_1, x_2 are pairwise coprime. (It will play an important technical role in our arguments below.) First we show that we may restrict our attention to coprime arithmetic progressions, i.e. to the case $\gcd(a, b) = 1$. For this, assume that there is a prime p with $p \mid a$, $p \mid b$. Then, as $n_0 = 0$ and $n_1 = 1$ in both cases, (19) with $i = 0, 1$ implies that $p^4 \mid x_0^4, x_1^4$, and then $p^4 \mid a, b$. Hence we can cancel p^4 from a and b, since a term of the arithmetic progression $(a/p^4)x + (b/p^4)$ obtained is a fourth power if and only if the corresponding term of the original progression $ax + b$ was a fourth power itself. So we can gradually get rid of all the common prime factors of a, b. Hence we may assume that $\gcd(a, b) = 1$ indeed. Assume now that x_0, x_1, x_2 in (19) are not pairwise coprime. Certainly, $\gcd(x_0, x_1) = 1$, since otherwise (as $n_0 = 0$, $n_1 = 1$) by (19) we obtain $\gcd(a, b) > 1$, which is excluded. So assume that $\gcd(x_j, x_2) > 1$ where $j = 0, 1$. Let p be a prime with $p \mid x_j, x_2$. Then, certainly $p^4 \mid x_j^4, x_2^4$, and (19) with $i = j, 2$ easily gives

$$p^4 \mid (2 - j)a, \ (2 - j)b.$$

However, then of course $p \mid a, b$, which is excluded. Consequently, we may assume without loss of generality that $\gcd(a, b) = 1$ and x_0, x_1, x_2 are pairwise coprime, indeed.

If $(n_0, n_1, n_2) = (0, 1, 3)$ then from (19) we get

$$3x_1^4 - 2x_0^4 = x_2^4.$$

The pairwise coprime integral solutions of the above equation can be parametrized by standard arguments (see e.g. [13], Chapter IV.4). In our case we get

$$\begin{aligned} rx_0^2 &= -2p^2 - 2pq + q^2, \\ rx_1^2 &= 2p^2 + q^2, \\ rx_2^2 &= 2p^2 - 4pq - q^2, \end{aligned}$$

where $p, q, r \in \mathbb{Z}$ and $r \mid 12$. From the second equation we immediately get that $r > 0$. If $r \in \{1, 3, 4, 12\}$, then the equation

$$rx_2^2 = 2p^2 - 4pq - q^2 = 6p^2 - (2p + q)^2$$

has only the trivial solution $(p, q, x_2) = (0, 0, 0)$. This follows from that $6p^2$ cannot be the sum of two squares if $r = 1, 4$. By checking the exponents of 3 in the three terms (and ultimately from that $u^2 \equiv 2v^2 \pmod 3$ is not solvable if $3 \nmid uv$) if $r = 3, 12$. Further, if $r = 2$ then the equation

$$rx_0^2 = -2p^2 - 2pq + q^2 = (q - p)^2 - 3p^2$$

has only the trivial solution. (This follows again by checking the exponents of 3 in the three terms.) So we are left with $r = 6$ as the only possibility. In this case multiplying the three equations above, after dividing by q^6 and writing $x = p$, $y = 36x_0x_1x_2$ we obtain the genus two hyperelliptic curve

$$D: \quad y^2 = -48x^6 + 48x^5 + 120x^4 + 60x^2 - 12x - 6.$$

Using Magma [3] we compute generators of its Mordell-Weil group. We get that

$$\mathrm{Jac}(D)(\mathbb{Q}) = \langle (x^2 + \frac{1}{2}, 0, 2), (x^2 + x - \frac{1}{2}, 0, 2), (x^2 + x + \frac{1}{4}, 12x + \frac{3}{2}, 2) \rangle,$$

where the first two elements are of order two and the last one generates the free part. Finally, using the Magma function `Chabauty` we obtain that

$$D(\mathbb{Q}) = \{(-\frac{1}{2}, \pm\frac{9}{2})\}.$$

This gives rise to the trivial solution with $(x_0^4, x_1^4, x_2^4) = (1, 1, 1)$. The case with $(n_0, n_1, n_2) = (0, 1, 4)$ can be excluded in a similar way, so we omit the details. Thus the proof of the theorem is complete. □

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. W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language.*, J. Symbolic Comput., **24** (1997), 235–265.
4. M. A. Bennett, N. Bruin, K. Győry and L. Hajdu, *Powers from products of consecutive terms in arithmetic progression*, Proc. London Math. Soc. **92** (2006), 273–306.
5. C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.
6. P. Dénes, *Über die Diophantische Gleichung* $x^\ell + y^\ell = cz^\ell$, Acta Math. **88** (1952), 241–251.
7. P. Erdős, *Quelques problémes de théorie des nombres*, Monographies de L'Enseignement Mathématique **6** 81–135, L'Enseignement Mathématique, Université Geneva, 1963.
8. S. Finch, G. Martin and P. Sebah, *Roots of unity and nullity modulo n*, Proc. Amer. Math. Soc. **138** (2010), 2729–2743.
9. E. González-Jiménez and X. Xarles, *On a conjecture of Rudin on squares in arithmetic progressions*, LMS J. Comput. Math. **17** (2014), 58–76.
10. A. Granville, *Squares in Arithmetic Progressions and Infinitely Many Primes*, Amer. Math. Monthly **124** (2017), 951–954.
11. 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.
12. W. Rudin, *Trigonometric series with gaps*, J. Math. Mech. **9** (1960), 203–227.
13. N. P. Smart, *The algorithmic resolution of Diophantine equations*, London Mathematical Society Student Texts **41**, Cambridge University Press, Cambridge, 1998.
14. M. Stoll, *On the height constant for curves of genus two*, Acta Arith. **90** (1999), 183–201.
15. M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), 245–277.
16. M. Stoll, *On the height constant for curves of genus two II*, Acta Arith. **104** (2002), 165–182.
17. E. Szemerédi, *The number of squares in an arithmetic progression*, Stud. Sci. Math. Hungar. **9** (1974), 417.