POWERFUL ARITHMETIC PROGRESSIONS

L. HAJDU[1]

Abstract. We give a complete characterization of so called powerful arithmetic progressions, i.e. of progressions whose kth term is a kth power for all k. We also prove that the length of any primitive arithmetic progression of powers can be bounded both by any term of the progression different from 0 and ± 1, and by its common difference. In particular, such a progression can have only finite length.

1. Introduction

In this paper we consider arithmetic progressions of mixed powers. We start with a question concerning a special but interesting case, then we turn to the general problem.

In 1998 Boklan [1] asked the following question: what is the length of the longest nonconstant arithmetic progression of integers with the property that the kth term (for all $k \geq 1$) is a perfect kth power? Such progressions are called powerful arithmetic progressions.

The problem was solved by Robertson [15], who proved that there are no such progressions of length six. He gave a particular example of a length five progression, too. Note that the same result was obtained by Manoharmayum, Reid, the GCHQ Problems Group, and Boklan and Elkies, as well (see [15] again).

In this paper we give a complete characterization of possible lengths of powerful arithmetic progressions. For this we need a simple notion. A (finite or infinite) arithmetic progression $a_1, a_2, \dots, a_n, \dots$ of integers is called *primitive*, if $\gcd(a_1, a_2) = 1$ is valid. Throughout the paper we shall write d for the common difference of such a progression. Note that the progression is primitive if and only if a_1 and d are coprime. We prove that the only primitive powerful arithmetic progression of length five is the trivial one, but there are infinitely many such progressions of length four. We also prove that in the nonprimitive case

---

2000 *Mathematics Subject Classification.* 11D61, 11B25, 11Y50.

Key words and phrases. Perfect powers, arithmetic progression.

1) Research supported in part by the Hungarian Academy of Sciences, and by the OTKA grants T48791 and T67580.

there are infinitely many pairwise nonproportional powerful arithmetic progressions of length five. In view of the above mentioned result of Robertson, our results (and their proofs) provide a complete characterization of the possible lengths of powerful arithmetic progressions. For some related results we refer to the papers [6], [10] and the references there. For example, in [6], all arithmetic progressions of squares and cubes are completely described. The main tool of our proofs is the elliptic Chabauty method (see e.g. [3], [4] and the references given there).

We also prove some results about more general arithmetic progressions of powers. That is, we consider progressions of the form

$$x_1^{k_1}, x_2^{k_2}, \ldots, x_n^{k_n}, \ldots \tag{1}$$

with $x_i \in \mathbb{Z}$, $k_i \geq 2$ $(i = 1, 2, \ldots)$. Obviously, such arithmetic progressions are closely related to generalized Fermat-type equations of the form

$$AX^p + BY^q = CZ^r,$$

where A, B, C, p, q, r are integers with $ABC \neq 0$, $p, q, r \geq 2$, and X, Y, Z are unknown integers. For general finiteness results about such equations (in the case when the exponents p, q, r are arbitrary, but fixed), see the excellent paper [8] and the references there.

We are interested in bounding the length of (1). Under some conditions, there are certain related results in the literature. The author in [9] proved that if $k_i \leq K$ holds in (1) for all i, then the length of the progression is bounded in terms of K only. Later, under the further assumption of primitivity, the number of such progressions has been bounded, as well (see [6]). In [9] it is also proved that assuming the *abc* conjecture, the condition $k_i \leq K$ can be replaced by primitivity, and the length of the progression is still bounded.

In the present paper we show that the length of a progression (1) can be bounded both by the help of any of its terms different from $0, \pm 1$, and with its common difference. As an immediate consequence we obtain that the length of any nonconstant arithmetic progression of powers is finite. Though the latter theorem can also be obtained as a simple consequence of a classical result of Dirichlet, we were unable to find it in the literature.

2. Results

We start with characterizing powerful arithmetic progressions. Our main result in this direction is the following.

Theorem 2.1. *The only primitive powerful arithmetic progression of length five is the trivial one, given by* $1, 1, 1, 1, 1$.

For the complete characterization of lengths, we also need

Theorem 2.2. *There are infinitely many primitive powerful arithmetic progressions of length four.*

Note that in the proof of Theorem 2.2 we give a complete description of length four primitive powerful arithmetic progressions.

The next result shows why it is necessary to impose the primitivity condition in the above two theorems. Note that having a particular primitive powerful arithmetic progression, after multiplying by appropriate factors one can obtain infinitely many nonprimitive progressions. Hence to get some meaningful statement we need to avoid this triviality.

Theorem 2.3. *There are infinitely many pairwise nonproportional powerful arithmetic progressions of length five.*

The result of Robertson and others mentioned in the introduction yields that there are no length six nonconstant powerful arithmetic progressions. So the above theorems provide a complete characterization of the lengths of powerful arithmetic progressions.

We also prove some results about general arithmetic progressions of powers. First we show that the length of such a progression can be bounded by its terms different from $0, \pm 1$.

Theorem 2.4. *Let x and k be integers, with $|x| \geq 2$ and $k \geq 2$. Then there exists a constant $C(x, k)$, depending only on x and k, such that the length of any arithmetic progression of powers containing x^k is at most $C(x, k)$.*

The next result shows that the assumption $x \neq 0$ is necessary in the previous theorem. We mention that the cases $x = \pm 1$ remain open; see also the problem posed in Remark 2.3.

Proposition 2.1. *There exist arithmetic progressions of powers of arbitrary (finite) length containing* 0 *as a term.*

Now we prove that the length of an arithmetic progression of powers can also be bounded by its common difference.

Theorem 2.5. *Let d denote the common difference of a nonconstant arithmetic progression* (1) *of powers and write n for the length of the progression. Then we have both estimates:*

i) $n \leq \max(3.125 \log(d) - 1, 73)$, *ii)* $n \leq \max(2(\omega(d)+1)(\log(\omega(d)+1)+\log\log(\omega(d)+1))-1, 21)$, *where* $\omega(d)$ *denotes the number of prime divisors of* d.

Remark 2.1. Note that in view of the proof, for small values of d, both bounds i) and ii) for the length of the progression can be improved. As the most interesting example, in case of $d = 1$ the first two terms of the progression give rise to the famous Catalan-equation

$$X^u - Y^v = 1$$

in unknown integers X, Y, u, v with $u, v \geq 2$. As is well-known, the only solution to this equation with $XY \neq 0$ is given by $(X, Y, u, v) = (3, 2, 2, 3)$ (see [13]). Hence in this case, taking into account the trivial progression $-1, 0, 1$, the length of (1) is at most three.

Remark 2.2. In [17], Shorey and Tijdeman investigated the equation

$$x(x+d)\dots(x+(n-1)d) = by^k, \tag{2}$$

where x, d, n, b, y, k are unknown positive integers with $\gcd(x, d) = 1$, $k \geq 2$ and $P(b) \leq n$ where $P(b)$ denotes the greatest prime divisor of b (with the convention $P(1) = 1$). They proved for the solutions of (2) that $n < C(\omega(d))$ must be valid for some effective constant $C(\omega(d))$ depending only on $\omega(d)$. By a simple standard argument, one can show that equation (2) is equivalent to having an arithmetic progression of the form

$$a_1x_1^k, a_2x_2^k, \dots, a_nx_n^k$$

with some positive integers a_i with $P(a_i) \leq n$. Thus interestingly (though with different settings) we have similar bounds for the lengths of arithmetic progressions of powers with "equal" and "different" exponents, in terms of the common difference d.

As a simple and immediate consequence of both Theorem 2.4 and Theorem 2.5, we obtain the following result.

Corollary 2.1. *The length of any nonconstant arithmetic progression of powers is finite.*

Remark 2.3. One can easily construct progressions (1) of arbitrary finite length, see e.g. Proposition 2.1 and Remark 2 of [9]. Hence Corollary 2.1 is best possible in the qualitative sense. However, by the constructions in Proposition 2.1 and in [9], only nonprimitive progressions can be obtained. We propose the following problem: prove that the length of any primitive nonconstant arithmetic progression of powers is bounded by an absolute constant.

3. Proofs

Proof of Theorem 2.1. Suppose that

$$x_1^1,\ x_2^2,\ x_3^3,\ x_4^4,\ x_5^5 \tag{3}$$

is a primitive powerful arithmetic progression of integers. We observe from the primitivity condition that $\gcd(x_2, x_3) = 1$. Further we have

$$3(x_4^2)^2 - x_2^2 = 2x_5^5. \tag{4}$$

Let $K = \mathbb{Q}(\alpha)$ with $\alpha = \sqrt{3}$, and let $\mathcal{O}_K$ denote the ring of integers of K. Factorizing the above equation in $\mathcal{O}_K$ we get

$$(\alpha x_4^2 - x_2)(\alpha x_4^2 + x_2) = 2x_5^5. \tag{5}$$

It is well known that $\varepsilon = \alpha + 2$ is a fundamental unit of K of norm $N_{K/\mathbb{Q}}(\varepsilon) = -1$, the only roots of unity of K are ± 1 and we have $2 = \varepsilon(\alpha - 1)^2$. Further $\{1, \alpha\}$ is an integral basis of K.

By the primitivity condition one can easily check that $\gcd(x_2, x_4) \leq 2$. If $\gcd(x_2, x_4) = 2$, then we get $2d = x_4^4 - x_2^2$. Hence d is even which violates the primitivity condition. So we conclude that $\gcd(x_2, x_4) = 1$. Using this assertion, keeping in mind the well-known fact that $\mathcal{O}_K$ is a Euclidean ring, we obtain from (5) that

$$\alpha x_4^2 + x_2 = \varepsilon^{t_1}(\alpha + 1)^{t_2}(\alpha u + v)^5 \tag{6}$$

holds with some integers u, v, t_1, t_2 with $-2 \leq t_1 \leq 2$ and $0 \leq t_2 \leq 4$. Here we used the fact that -1 is a full fifth power. By $\gcd(x_2, x_4) = 1$, we have $\gcd(u, v) = 1$. We shall use this fact later on without any reference. Further, taking the field norms of both sides of (6), we immediately get that $t_2 = 1$. Finally, taking field conjugates over K and substituting $-x_2$ and $-v$ in places of x_2 and v, respectively, we may assume without loss of generality that $t_1 \in \{0, 1, 2\}$. We investigate these cases in turn.

The case $t_1 = 0$. Using that $t_2 = 1$, by comparing the coefficients of α on both sides of (6), we get

$$v^5 + 5v^4u + 30v^3u^2 + 30v^2u^3 + 45vu^4 + 9u^5 = x_4^2. \tag{7}$$

Let $f_0(v, u)$ denote the left hand side of (7), and define the polynomial g_0 by $g_0(x) = x^5 + 5x^4 + 30x^3 + 30x^2 + 45x + 9$ (i.e. $g_0(x) = f_0(x, 1)$). A simple check, for e.g. by Magma [2], assures that g_0 is irreducible over $\mathbb{Q}$. Let β denote a root of g_0, and put $L = \mathbb{Q}(\beta)$. Write $\mathcal{O}_L$ for the ring of integers of L.

To proceed smoothly, we need some information about L. These data are available by the use of Magma again. The class number of L

is one,

$$\vartheta_0 = 1, \quad \vartheta_1 = \beta, \quad \vartheta_2 = (\beta^2+1)/2,$$
$$\vartheta_3 = (\beta^3+5\beta^2+9\beta+9)/12, \quad \vartheta_4 = (\beta^4+8\beta^2+15)/24$$

is an integral basis of L, and

$$\eta_1 = -\vartheta_1 + 2\vartheta_3 - 2\vartheta_4, \quad \eta_2 = -\vartheta_0 - \vartheta_1 - 2\vartheta_2 + 2\vartheta_3 + \vartheta_4$$

is a system of fundamental units for L, with $N_{L/\mathbb{Q}}(\eta_1) = N_{L/\mathbb{Q}}(\eta_2) = 1$. Further, the only roots of unity in L are ± 1, and we also have

$$2 = \gamma_1\gamma_2^2, \quad 3 = \gamma_3\vartheta_1^2, \quad 5 = \eta_2\gamma_4^5,$$

where the γ_i $(i = 1, \dots, 4)$ are some prime elements in $\mathcal{O}_L$, with

$$N_{L/\mathbb{Q}}(\gamma_1) = 2, \quad N_{L/\mathbb{Q}}(\gamma_2) = 4, \quad N_{L/\mathbb{Q}}(\gamma_3) = 3, \quad N_{L/\mathbb{Q}}(\gamma_4) = 5.$$

As the γ_i do not play any role later on, we suppress the concrete values. Note that ϑ_1 is also a prime in $\mathcal{O}_L$, and $N_{L/\mathbb{Q}}(\vartheta_1) = -9$.

Factorizing the left hand side of (7) over $\mathcal{O}_L$ (using Magma again) we get

$$(v - \vartheta_1 u)h_0(v,u) = x_4^2 \tag{8}$$

with

$$h_0(v,u) = v^4 + (5\vartheta_0 + \vartheta_1)v^3u + (29\vartheta_0 + 5\vartheta_1 + 2\vartheta_2)v^2u^2 +$$
$$+ (21\vartheta_0 + 21\vartheta_1 + 12\vartheta_3)vu^3 - (12\vartheta_0 + 15\vartheta_1 + 6\vartheta_2 - 60\vartheta_3 - 24\vartheta_4)u^4.$$

Using that the only prime divisors of the discriminant of g_0 are $2, 3, 5$, we obtain from (8) that both

$$v - \vartheta_1 u = (-1)^{s_1}\ \eta_1^{s_2}\ \eta_2^{s_3}\ \gamma_1^{s_4}\ \gamma_2^{s_5}\ \gamma_3^{s_6}\ \vartheta_1^{s_7}\ \gamma_4^{s_8}\ \gamma_5^{s_9}\ \delta_1^2 \tag{9}$$

and

$$h_0(v,u) = (-1)^{s_1}\ \eta_1^{s_2}\ \eta_2^{s_3}\ \gamma_1^{s_4}\ \gamma_2^{s_5}\ \gamma_3^{s_6}\ \vartheta_1^{s_7}\ \gamma_4^{s_8}\ \gamma_5^{s_9}\ \delta_2^2 \tag{10}$$

must hold, with some $\delta_1, \delta_2 \in \mathcal{O}_L$ and $s_i \in \{0,1\}$ $(i = 1, \dots, 9)$. (As the product of the right hand sides of (9) and (10) should be a full square, one can easily check that the exponents s_i must indeed coincide in (9) and (10).) Taking field norms of both sides of (9), we immediately get that $s_4 = s_5 = s_6 = s_8 = s_9 = 0$ and $s_1 + s_7 \neq 1$. Hence we are left with eight possibilities.

In case of $s_2 = 1$, all the four corresponding equations can be excluded locally. If $u = 0$, then $v = \pm 1$ and using (7) and (6), we get that the progression (3) is given by $1, 1, 1, 1, 1$. Otherwise, after dividing both sides of equation (10) by u^4 and merging it into δ_2^2, we consider the corresponding equations as hyperelliptic curves over L (using the `HyperellipticCurve` command of Magma). Then we determine those prime ideals of $\mathcal{O}_L$, where the equation might not be solvable locally (by the procedure `BadPrimes`). Finally, we test whether these equations are locally solvable at all these prime ideals or not (using the procedure `IsLocallySolvable`). In all four cases mentioned above, we could find a prime ideal where the curves has no points locally. Hence these cases can be excluded.

Suppose next that, together with $s_2 = 0$, we have $s_1 = s_3 = s_7 = 1$. Then writing $\delta_1 = z_0\vartheta_0 + z_1\vartheta_1 + z_2\vartheta_2 + z_3\vartheta_3 + z_4\vartheta_4$ in (9) and expanding both sides of the equation, we obtain from matching the coefficients of $\vartheta_0, \vartheta_1, \vartheta_4$ that the integers

$$z_0^2 + z_1^2 + z_3^2 + v, \quad u, \quad z_0^2 + z_1^2 + z_3^2$$

must all be even. Hence we conclude that both v and u are even. However, by (7), this implies that x_4 is even which contradicts the primitivity of the arithmetic progression, in a similar manner as before.

Assume next that (beside $s_2 = 0$) we have $s_1 = s_7 = 0$, $s_3 = 1$. Then by the same method used in the previous paragraph, following the same notation (but now matching the coefficients of $\vartheta_0, \vartheta_1, \vartheta_3, \vartheta_4$) we get that the integers

$$z_0^2 + z_1^2 + z_3^2 + z_4^2 + v, \quad z_0^2 + z_1^2 + z_3^2 + z_4^2 + u, \quad z_4^2, \quad z_0^2 + z_1^2 + z_3^2$$

are all even. Hence we easily obtain that both v and u are even, thus by (7), x_4 is even once again. So this case is also excluded by contradiction.

Consider now the case $s_1 = s_3 = s_7 = 0$ (and $s_2 = 0$). Then (10) defines a projective genus 1 curve $C_1^{(0)}$ over L (considering v, u, δ_2 to be unknowns from L). By the help of the point $P = (0 : 1 : 0)$ the curve $C_1^{(0)}$ can be transformed into an elliptic curve. More precisely, by a method of Cassels (see [7]) using P, one can find a homogeneous elliptic curve C' in the usual form

$$C' : \quad y^2z + r_1xyz + r_3yz^2 = x^3 + r_2x^2z + r_4xz^2 + r_6z^3$$

with coefficients $r_1, r_2, r_3, r_4, r_6 \in L$ such that $C_1^{(0)}$ and C' are birationally equivalent. After dehomogenizing C' we get a plane elliptic curve over L. In our case the resulting dehomogenized elliptic curve has a minimal model

$$E_1^{(0)} : \ Y^2 = X^3 - (\vartheta_1 + \vartheta_2 + \vartheta_3 + \vartheta_4)X^2 + (73\vartheta_0 + 95\vartheta_1 + \\ + 26\vartheta_2 - 287\vartheta_3 - 125\vartheta_4)X + 125\vartheta_0 + 158\vartheta_1 + 48\vartheta_2 - 466\vartheta_3 - 204\vartheta_4.$$

Note that all the curves, together with the transformations among them can be handled by Magma. For more explanation about the techniques we use we refer to [5]. Now, as v and u are known to be rational coordinates of $C_1^{(0)}$, one can apply the elliptic Chabauty method to solve (10) completely. Here we only indicate the main steps of the solution, without explaining the background theory. For the theory of the method we refer to [3] and [4] and the references given there. To see how the method works in practice, in particular by the help of Magma, [5] is an excellent source. For applying elliptic Chabauty in similar context, beside the above references see also [6], [10], [11], [12], [19]. So, to have the method work, the rank of $E_1^{(0)}(L)$ should be strictly less than the degree of L (which is five). In the present case it turns out that the rank of $E_1^{(0)}(L)$ is three, so elliptic Chabauty is applicable. Further, the procedure `PseudoMordellWeilGroup` of Magma is able to find a subgroup $G_1^{(0)}$ of $E_1^{(0)}(L)$ of finite odd index. Then, using the procedure `Chabauty` with the prime 11, we get that all solutions to (10) with v, u coprime rational integers are

$$(v,u,\delta_2) = (\pm 1, 0, \pm 1), (-1, 4, \pm(51\vartheta_0 + 50\vartheta_1 + 18\vartheta_2 - 168\vartheta_3 - 68\vartheta_4)).$$

The first solution by (7) yields that $x_4 = \pm 1$. Further, (6) implies that $x_2 = \pm 1$, so the arithmetic progression (3) is given by $1, 1, 1, 1, 1$. In the second case (7) gives an immediate contradiction.

Finally, assume that $s_1 = s_7 = 1$, $s_3 = 0$ (and also $s_2 = 0$). Then similarly as in the previous paragraph, (10) defines a projective genus 1 curve $C_2^{(0)}$ over L. Using the point $(0 : 3/\vartheta_1 : 1)$, $C_2^{(0)}$ can be transformed into an elliptic curve, which has a minimal model

$$E_2^{(0)}: \; Y^2 = X^3 + (\vartheta_1 - \vartheta_3 + \vartheta_4)X^2 - (1261\vartheta_0 + 1657\vartheta_1 + $$
$$+ 2245\vartheta_2 - 2691\vartheta_3 - 701\vartheta_4)X - 110\vartheta_0 - 4684\vartheta_1 - 487\vartheta_2 + 8571\vartheta_3 - 9096\vartheta_4.$$

The rank of $E_2^{(0)}(L)$ is one, so elliptic Chabauty can be applied for $E_2^{(0)}$. Note that here the procedure `PseudoMordellWeilGroup` with the default settings fails to find a subgroup $G_2^{(0)}$ of $E_2^{(0)}(L)$ of finite odd index. However, using the procedure `SelmerGroup` and the nontorsion point

$$\left(\frac{28\vartheta_0 + 44\vartheta_1 + 54\vartheta_2 - 68\vartheta_3 - 5\vartheta_4}{5}, \frac{266\vartheta_0 + 200\vartheta_1 + 461\vartheta_2 - 296\vartheta_3 - 450\vartheta_4}{5}\right)$$

of $E_2^{(0)}(L)$, by a slightly more involved procedure (explained in detail in [5], pp. 18 and 19), we can find such a subgroup $G_2^{(0)}$. Then again, using the procedure `Chabauty` now with the prime 7, we get all solutions to (10) with v, u rational. Note that now by the procedure `IsPSaturated` we also need to check that the index $[E_2^{(0)}(L) : G_2^{(0)}]$ is not divisible by 5. After all, we get that

$$(v,u,\delta_2) = (0, \pm 1, \pm(4\vartheta_0 + 5\vartheta_1 + 2\vartheta_2 - 20\vartheta_3 - 8\vartheta_4))$$

are the only solutions to (10) with coprime integers v, u. Then (7) implies $x_4 = \pm 3$ and (6) yields that $x_2 = \pm 27$. Though this with $x_5 = -3$ extends to a solution of (4), however, as one can easily check, does not yield any (even nonprimitive) arithmetic progression of the form (3).

The case $t_1 = 1$. Noting that $t_2 = 1$, comparing again the coefficients of α on both sides of (6) in this case, we obtain

$$3v^5 + 25v^4u + 90v^3u^2 + 150v^2u^3 + 135vu^4 + 45u^5 = x_4^2. \tag{11}$$

Let $f_1(v, u)$ denote the left hand side of (11) and define the polynomial g_1 as $g_1(x) = 3x^5 + 25x^4 + 30x^3 + 30x^2 + 45x + 9$ (that is $g_1(x) = f_1(x, 1)$). Using Magma we get that g_1 is irreducible over $\mathbb{Q}$. Let L denote the same number field as in case of $t_1 = 0$ and keep all the related notation as well. (Note that g_0 and g_1 define the same number field L.) Factorizing the left hand side of (11), we get

$$\begin{aligned}((-27\vartheta_0 - 32\vartheta_1 - 10\vartheta_2 + 96\vartheta_3 + 40\vartheta_4)v+\\ + (26\vartheta_0 + 25\vartheta_1 + 8\vartheta_2 - 72\vartheta_3 - 30\vartheta_4)u)h_1(v, u) = x_4^2\end{aligned} \tag{12}$$

where

$$\begin{aligned}h_1(v, u) = (-\vartheta_0 + 2\vartheta_2)v^4 - (5\vartheta_0 - 3\vartheta_1 - 14\vartheta_2+\\ +2\vartheta_4)v^3u - (3\vartheta_0 - 13\vartheta_1 - 40\vartheta_2 + 8\vartheta_3 + 14\vartheta_4)v^2u^2 - (9\vartheta_0 - 3\vartheta_1 - 30\vartheta_2 - 12\vartheta_3+\\ + 18\vartheta_4)vu^3 - 6\vartheta_0 - 3\vartheta_1 + 6\vartheta_2 + 12\vartheta_3 - 6\vartheta_4.\end{aligned}$$

As the only prime divisors of the discriminant of g_1 are $2, 3, 5$, from (12), we get that both

$$\begin{aligned}(-27\vartheta_0 - 32\vartheta_1 - 10\vartheta_2 + 96\vartheta_3 + 40\vartheta_4)v + (26\vartheta_0 + 25\vartheta_1+\\ + 8\vartheta_2 - 72\vartheta_3 - 30\vartheta_4)u = (-1)^{k_1}\ \eta_1^{k_2}\ \eta_2^{k_3}\ \gamma_1^{k_4}\ \gamma_2^{k_5}\ \gamma_3^{k_6}\ \vartheta_1^{k_7}\ \gamma_4^{k_8}\ \gamma_5^{k_9}\ \xi_1^2\end{aligned} \tag{13}$$

and

$$h_1(v, u) = (-1)^{k_1}\ \eta_1^{k_2}\ \eta_2^{k_3}\ \gamma_1^{k_4}\ \gamma_2^{k_5}\ \gamma_3^{k_6}\ \vartheta_1^{k_7}\ \gamma_4^{k_8}\ \gamma_5^{k_9}\ \xi_2^2 \tag{14}$$

hold, with some $\xi_1, \xi_2 \in \mathcal{O}_L$ and $k_i \in \{0, 1\}$. (Similarly as in case of $t_1 = 0$, the k_i must coincide in (13) and (14).) Taking field norms of both sides of (13) yields $k_4 = k_5 = k_6 = k_8 = k_9 = 0$ and $k_1 + k_7 \neq 1$. Hence we are left with eight possibilities again.

In case of $k_2 = 1$, all the four corresponding equations (14) can be excluded locally. As it can be done in the same way as for $t_1 = 0$, we suppress the details.

If $k_3 = 1$ (together with $k_2 = 0$), then, in both possible cases, we can apply the same method as with $t_1 = 0$. Looking at the coefficients of the ϑ_i in (13), modulo 2 we obtain that both v and u should be even which gives a contradiction in a similar manner as previously. We suppress the details once again.

Consider now the case $k_1 = k_3 = k_7 = 0$ (and $k_2 = 0$). Then similarly as with $t_1 = 0$, (14) defines a projective genus 1 curve $C_1^{(1)}$ over L. By the help of the point $(0 : 1 : 0)$ (after dividing each coefficients by the leading coefficient ϑ_1^2 of $h_1(v, u)$, and also merging it into ξ_2^2), $C_1^{(1)}$ can be transformed into an elliptic curve which has a minimal model

$$E_1^{(1)} :\ Y^2 = X^3 - (\vartheta_1 + \vartheta_2 + \vartheta_3)X^2 + (26\vartheta_0 + 50\vartheta_1 + \\ + 47\vartheta_2 - 84\vartheta_3 + 18\vartheta_4)X + 148\vartheta_0 + 140\vartheta_1 + 260\vartheta_2 - 216\vartheta_3 - 192\vartheta_4.$$

Using elliptic Chabauty as previously, by the procedure `Chabauty` of Magma with the prime 7, we obtain that all solutions to (14) with coprime integers v, u are

$$(v, u, \xi_2) = (\pm 1, 0, \pm\vartheta_1).$$

This by (11) yields a contradiction.

Finally let $k_1 = k_7 = 1$, $k_3 = 0$ (together with $k_2 = 0$). Then as before, (14) defines a projective genus 1 curve $C_2^{(1)}$ over L. Using the point $(0 : 7\vartheta_0 + 7\vartheta_1 + 2\vartheta_2 - 19\vartheta_3 - 8\vartheta_4 : 1)$, $C_2^{(1)}$ can be transformed into an elliptic curve having a minimal model

$$E_2^{(1)} :\ Y^2 = X^3 - (\vartheta_0 - \vartheta_1 + \vartheta_2 - \vartheta_3 - \vartheta_4)X^2 + (12\vartheta_0 + 17\vartheta_1 + \\ + 24\vartheta_2 - 29\vartheta_3 - 7\vartheta_4)X - 11\vartheta_0 - 26\vartheta_1 - 21\vartheta_2 + 44\vartheta_3 - 16\vartheta_4.$$

By the help of the procedure `Chabauty` with the prime 11, we obtain that

$$(v, u, \xi_2) = (0, \pm 1, \pm(2\vartheta_0 - 5\vartheta_3 - 2\vartheta_4)), \\ (12, 17, \pm(728\vartheta_0 - 642\vartheta_1 + 402\vartheta 2 - 317\vartheta_3 + 298\vartheta_4))$$

are the only solutions to (14) with coprime integers v, u. In case of the first possibility, (11) immediately implies a contradiction. In the second case, (11) and (7) give $x_4 = \pm 3 \cdot 6323$ and $x_2 = \pm 3^3 \cdot 23094391$, respectively. These values with $x_5 = -3 \cdot 241$ yield a solution to (4). However, as one can readily check, they do not give rise to any (even nonprimitive) arithmetic progression (3).

The case $t_1 = 2$. In this case, from equation (6), we obtain

$$(v + u)f_2(v, u) = x_4^2 \qquad (15)$$

with $f_2(v,u) = 11v^4 + 84v^3u + 246v^2u^2 + 324vu^3 + 171u^4$. Put $g_2(x) = f_2(x,1)$. As the discriminant of $(v+u)f_2(v,u)$ is divisible by the primes $2, 3, 5$ only, from (15), we get

$$f_2(v,u) = (-1)^{m_1}\ 2^{m_2}\ 3^{m_3}\ 5^{m_4}\ w^2 \tag{16}$$

with some integer w and $m_i \in \{0,1\}$ $(i = 1,2,3,4)$. If $m_2 = 1$, then by (15) x_4 is even, which leads to a contradiction in a similar manner as many times before. Hence we may assume that $m_2 = 0$ in (16). In the remaining eight cases, after dividing both sides by u^4 (which by (15) cannot be zero), (16) gives rise to hyperelliptic equations of the form

$$(-1)^{m_1}3^{m_3}5^{m_4}g_2(x) = y^2, \tag{17}$$

where $g_2(x) = f_2(x,1)$. In the cases where $m_3 = 1$ and also in case of $m_1 = 1$, $m_3 = m_4 = 0$, the procedure `IsLocallySolvable` of Magma gives a contradiction modulo one of $2, 3, 5$. In the cases $m_1 = m_3 = m_4 = 0$ and $m_1 = m_4 = 1$, $m_3 = 0$, by (16), one can easily check that $3 \mid v$ must be valid. Then, in view of (15), we obtain $3 \mid x_4$ and by (6) also that $3 \mid x_2$ which contradicts the primitivity of the progression (3). Finally, if $m_1 = m_3 = 0$, $m_4 = 1$ then checking (16) modulo 4, we easily obtain that w must be even. However, then x_4 is also even by (15), which leads to a contradiction in the usual fashion. □

Proof of Theorem 2.2. To prove the theorem, it is obviously sufficient to show that there are infinitely many primitive arithmetic progressions of integers of the form

$$x_2^2,\quad x_3^3,\quad x_4^4. \tag{18}$$

We give a full characterization of progressions of the form (18). For this purpose, in fact we need to completely describe the solution set of the equation

$$x_2^2 + x_4^4 = 2x_3^3. \tag{19}$$

As is well-known, the solutions of equation (19) can be parametrized. More precisely, x_2, x_3, x_4 are coprime solutions to (19) if and only if

$$x_2 = u^3 - 3u^2v - 3uv^2 + v^3,\ x_3 = u^2 + v^2,\ x_4^2 = u^3 + 3u^2v - 3uv^2 - v^3 \tag{20}$$

hold with some coprime integers u, v, $u \not\equiv v \pmod 2$ (see e.g. [14]). Trivially, we need to focus only on the last item of (20). Having it satisfied, the values of x_2 and x_3 are automatically chosen.

Obviously, we can find integers t, z such that $v = tz^2$ uniquely if we assume t to be square-free. As $z = 0$ leads to the constant progression

$1, 1, 1$ in (18), we may also suppose that $z \neq 0$. Then the last item of (20) gives

$$E_t : \; Y^2 = X^3 + 3tX^2 - 3t^2X - t^3 \tag{21}$$

where

$$X = v/z^2 \quad \text{and} \quad Y = x_4/z^3. \tag{22}$$

We may consider (21) as a parametric family of elliptic curves E_t, taking t to be a square-free integral parameter and X, Y to be unknown rationals. As is well-known, any rational point on this curve has the property that the square of the denominator of Y is the same as the cube of the denominator of X (see e.g. [18]). That is, the transformation in (22) can be reversed.

Hence, taking any square-free t and choosing any rational point (X, Y) of E_t, we can write $X = U_1/V^2$ and $Y = U_2/V^3$ with integers U_1, U_2, V such that $\gcd(U_1U_2, V) = 1$. If $U_1 \not\equiv tV^2 \pmod 2$, then putting $u = U_1$ and $v = tV^2$ we get a parametrization by (20) leading to a primitive arithmetic progression of the form (18). Already the choice $t = 1$ is sufficient to find infinitely many such solutions. Indeed, by Magma, we get that the rank of E_1 is one and the point $P = (-1, 2)$ generates the free part of the Mordell-Weil group of E_1. In particular, there are infinitely many rational points on E_1 leading to (different) arithmetic progressions of the shape (18). As one can easily see, this is the case for all points nP where n is a power of 2. To see an example, consider the point

$$4P = (10961/1936, \; -1372655/85184)$$

on E_1. Then putting $u = 10961$ and $v = 1936$ in (20), we get the primitive arithmetic progression

$$503107236801^2, \; 123891617^3, \; 1372655^4.$$

Observe that by the above procedure all progressions (18) can be determined. □

Proof of Theorem 2.3. By Theorem 2.2 we know that there are infinitely many primitive arithmetic progression of integers of the form

$$x_1^1, \; x_2^2, \; x_3^3, \; x_4^4. \tag{23}$$

Choose any progression of the shape (23) and put $s = x_4^4 + d$, where d denotes the common difference of the progression. Observe that by writing

$$y_1 = x_1 s^{24}, \; y_2 = x_2 s^{12}, \; y_3 = x_3 s^8, \; y_4 = x_4 s^6, \; y_5 = s^5,$$

the progression

$$y_1^1,\ y_2^2,\ y_3^3,\ y_4^4,\ y_5^5$$

is of the desired shape, and further the progressions obtained in this way are pairwise nonproportional. Hence the theorem follows. □

To prove Theorem 2.4 we need the following lemma.

Lemma 3.1. *Suppose that for a nonconstant arithmetic progression of powers of the form* (1) *we have* $k_i \le K$ *for all* i. *Then the length of the progression is bounded by a constant depending only on* K.

Proof. The statement is a simple consequence of Theorem 2 of [9]. □

Proof of Theorem 2.4. Suppose that x^k is a member of an arithmetic progression of the form (1) where x and k are integers with $|x| \ge 2$, $k \ge 2$. Let p be a prime divisor of x and put $\alpha = \mathrm{ord}_p(x)$. Further, write d for the common difference of the progression, and set $\beta = \mathrm{ord}_p(d)$. Let γ be an arbitrary integer with $\gamma \ge \max(0, k\alpha + 1 - \beta)$. Observe that, for any $t \in \mathbb{Z}$, we have $\mathrm{ord}_p(y_t) = k\alpha$ where $y_t = x^k + tp^\gamma d$. Hence if $y_t = x_t^{k_t}$ holds for some t, then $k_t \le k\alpha$ must be valid. As the numbers y_t form an arithmetic progression (with common difference $p^\gamma d$), by Lemma 3.1 we obtain that the length of this progression is bounded in terms of $k\alpha$. Hence the length of the original progression must be bounded by a constant $C(k, p, \alpha)$ depending only on k, p, α. As $p \le x$ and $\alpha \le \log(x)/\log(2)$, the statement follows. □

Proof of Proposition 2.1. Let p_i denote the ith prime. Take an arbitrary positive integer n. Then all integers m with $1 \le m < p_{n+1}$ can be uniquely written in the form $m = p_1^{\alpha_{1m}} \dots p_n^{\alpha_{nm}}$ with nonnegative integers α_{im} $(i = 1, \dots, n)$. Put

$$H = \{(\alpha_{1m}, \dots, \alpha_{nm}) \ : \ 1 \le m < p_{n+1}\}.$$

Further, for each $(h_1, \dots, h_n) \in H$ pick up an odd prime $q_{(h_1,\dots,h_n)}$. Then for every $i = 1, \dots, n$ choose a positive β_i such that

$$\beta_i \equiv -h_i \pmod{q_{(h_1,\dots,h_n)}} \quad \text{for all } (h_1, \dots, h_n) \in H. \tag{24}$$

By the Chinese remainder theorem we know that such β_i exists for all i. Let $d = p_1^{\beta_1} \dots p_n^{\beta_n}$, and observe that for every t from the interval $[-p_{n+1} + 1, p_{n+1} - 1]$, by (24), td is a $q_{(h_1,\dots,h_n)}$th power for the appropriate $(h_1, \dots, h_n) \in H$. Hence these numbers td form an arithmetic progression of powers of length $2p_{n+1} - 1$, and the statement follows.

We illustrate the construction with a simple example. Take $n = 2$. Then we have

$$H = \{(0, 0), (1, 0), (0, 1), (2, 0)\},$$

corresponding to the exponents of $p_1 = 2$ and $p_2 = 3$ in the numbers $1, 2, 3, 4$. Let

$$q_{(0,0)} = 3,\ q_{(1,0)} = 5,\ q_{(0,1)} = 7,\ q_{(2,0)} = 11.$$

Then (24) yields $\beta_1 = 504$ and $\beta_2 = 825$. Hence setting $d = 2^{504}3^{825}$, the numbers td $(-4 \le t \le 4)$ form a progression of the shape (1) of length $2 \cdot p_3 - 1 = 9$. □

Proof of Theorem 2.5. Let p be any prime which does not divide d. Then among any $2p$ consecutive terms of the progression there are two, say y_0 and $y_p = y_0 + pd$, which are divisible by p. Further, either $\mathrm{ord}_p(y_0) = 1$ or $\mathrm{ord}_p(y_p) = 1$ must be valid. However, as these terms are perfect powers, this is impossible. Hence $n \le 2p - 1$.

To derive the bound i), write $\vartheta^*(p)$ for the logarithm of the product of all primes $< p$, with the convention $\vartheta^*(2) = 0$. Then the Corollary of Theorem 4 of [16] implies that

$$\vartheta^*(p) > p(1 - 1/\log(p)) - \log(p)$$

provided that $p \ge 41$. Hence a simple calculation yields that for $p \ge 41$ we have

$$\vartheta^*(p)/p > 0.64.$$

As clearly $\log(d) \ge \vartheta^*(p)$ if $p \ge 41$, we have

$$2p - 1 < 3.125\log(d) - 1$$

in this case. Otherwise, trivially $2p - 1 \le 73$ holds, and the bound i) follows.

To get the estimate ii), write p_i for the ith prime. The Corollary of Theorem 3 of [16] gives that for $i \ge 6$

$$p_i < i(\log(i) + \log\log(i))$$

holds. Noting that $p \le p_{\omega(d)+1}$, the above inequality immediately yields ii), and the theorem follows. □

Proof of Corollary 2.1. Obviously, the statement is a trivial and immediate consequence both of Theorem 2.4 and of Theorem 2.5. However we show here that the result easily follows also from Dirichlet's famous theorem about primes in arithmetic progressions. Let

$$a_1, a_2, \ldots, a_n, \ldots \tag{25}$$

be a nonconstant arithmetic progression of integers. Suppose that $a_i = x_i^{k_i}$ holds with $k_i \ge 2$ for all $i = 1, 2, \ldots$. Let $D = \gcd(a_1, a_2)$. Then we can write $a_i = Db_i$ for all $i = 1, 2, \ldots$. Observe that then

$$b_1, b_2, \ldots, b_n, \ldots$$

is also an arithmetic progression, and we have $\gcd(b_1, b_2) = 1$, as well. Thus if the length of this progression is infinite, by Dirichlet's theorem we obtain that it contains infinitely many primes. Let p be any prime in the progression with $p > D$. Then $b_i = p$ is valid for some i, hence we should have $x_i^{k_i} = Dp$. However p divides the right hand side exactly on the first power which contradicts the assumption $k_i \geq 2$. Hence any progression of the shape (25) must have finite length and the statement follows. □

4. Acknowledgment

The author is grateful to the referee for his useful remarks.

References

[1] K. D. Boklan, *Problem 10702*, Amer. Math. Monthly **105** (1998), p. 956.

[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[3] N. Bruin, *Chabauty methods and covering techniques applied to generalized Fermat equations*, CWI Tract, Vol. 133, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 2002.

[4] N. Bruin, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. **562** (2003), 27–49.

[5] N. Bruin, *Diophantine equations of signature* $(n, n, 2)$, In: Discovering mathematics with Magma, Algorithms Comput. Math. **19** (2006), 63–91.

[6] N. Bruin, K. Győry, L. Hajdu, Sz. Tengely, *Arithmetic progressions consisting of unlike powers*, Indag. Math. **17** (2006), 539–555.

[7] J. W. S. Cassels, *Lectures on elliptic curves*, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991.

[8] H. Darmon, A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), 513–543.

[9] L. Hajdu, *Perfect powers in arithmetic progression. A note on the inhomogeneous case*, Acta Arith. **113** (2004), 343–349.

[10] L. Hajdu, Sz. Tengely, *Arithmetic progressions of squares, cubes and* n*-th powers*, Functiones et Approximatio (to appear).

[11] L. Hajdu, Sz. Tengely, R. Tijdeman, *Cubes in products of terms in arithmetic progression*, Publ. Math. Debrecen **74** (2009), 215–232.

[12] S. Laishram, T. N. Shorey, Sz. Tengely, *Squares in products in arithmetic progression with at most one term omitted and common difference a prime power*, Acta Arith. **135** (2008), 143–158.

[13] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.

[14] I. Pink, Sz. Tengely, *Full powers in arithmetic progressions*, Publ. Math. Debrecen **57** (2000), 535–545.

[15] J. P. Robertson, *The Maximum Length of a Powerful Arithmetic Progression: 10702*, Amer. Math. Monthly **107** (2000), p. 951.

[16] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64-94.

[17] T. N. Shorey, R. Tijdeman, *Perfect powers in products of terms in arithmetical progression*, Compositio Math. **75** (1990), 307–344.

[18] J. H. Silverman, J. Tate *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.

[19] Sz. Tengely, *Note on the paper "An extension of a theorem of Euler" by Hirata-Kohno et al.*, Acta Arith. **134** (2008), 329–335.

University of Debrecen, Institute of Mathematics
and the Number Theory Research Group
of the Hungarian Academy of Sciences
Debrecen
P.O. Box 12.
H-4010
Hungary
E-mail address: hajdul@math.klte.hu