ON GEOMETRIC PROGRESSIONS ON PELL EQUATIONS AND LUCAS SEQUENCES

ATTILA BÉRCZES AND VOLKER ZIEGLER

Abstract. We consider geometric progressions on the solution set of Pell equations and give upper bounds for such geometric progressions. Moreover, we show how to find for a given four term geometric progression a Pell equation such that this geometric progression is contained in the solution set. In the case of a given five term geometric progression we show that at most finitely many essentially distinct Pell equations exist, that admit the given five term geometric progression.

1. Introduction

Let H be the set of solutions of a norm form equation

$$\mathrm{N}_{K/\mathbb{Q}}(x_1\alpha_1 + \cdots + x_n\alpha_n) = m, \tag{1}$$

where K is a number field, $\alpha_1, \ldots, \alpha_n \in K$ and $m \in \mathbb{Z}$, and arrange H in an $|H| \times n$ array $\mathcal{H}$. Then two questions in view of arithmetic (geometric) progressions occur.

The horizontal problem: Do there exist infinitely many rows of $\mathcal{H}$ which form arithmetic (geometric) progressions, i.e. are there infinitely many solutions that are in arithmetic progression?

The vertical problem: Do there exist arbitrary long arithmetic (geometric) progressions in some column of $\mathcal{H}$?

Note, the first question is only meaningful if $n > 2$. This paper is devoted to the vertical problem. General, but ineffective results for the vertical problem in the case of arithmetic progressions have been established by Bérczes, Hajdu and Pethő [1].

Let us note that the vertical problem can be considered for any Diophantine equation. In particular, the case of elliptic curves has been investigated by several authors. Let us note that Bremner, Silverman and Tzanakis [4] showed that a subgroup Γ of the elliptic curve $E(\mathbb{Q})$ with $E : Y^2 = X(X^2 - n^2)$ of rank 1 does not have non-trivial integral arithmetic progressions in the X-component, provided that $n \geq 1$.

In this paper we want to consider geometric progressions on Pell equations

$$X^2 - dY^2 = m, \tag{2}$$

2000 *Mathematics Subject Classification.* 11D09,11B25,11G05.

Key words and phrases. Pell equations, geometric progressions, elliptic curves.

The second author was supported by the Austrian Science Found (FWF) under the project J2886-N18. The research of the first author was supported in part by grants T67580 and T75566 of the Hungarian National Foundation for Scientific Research, and the János Bolyai Research Scholarship. The work is supported by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, co-financed by the European Social Fund and the European Regional Development Fund.

TABLE 1. Non-trivial geometric progressions of (2) in the X-components, with $|m| \leq 100$.

m	d	X-components	m	d	X-components
-99	$3, 27$	$3, 24, 192$	-98	11	$1, 21, 441$
-91	35	$7, 28, 112$	-82	2	$16, 40, 100$
-80	$21, 84$	$2, 16, 128$	-68	$2, 8, 18, 72$	$2, 110, 6050$
-66	3	$3, 21, 147$	-62	14	$8, 48, 288$
-56	$2, 8$	$4, 12, 36$	-49	2	$1, 7, 49$
-44	$2, 12$	$2, 16, 128$	-20	21	$1, 8, 64$
-17	$2, 18$	$1, 55, 3025$	-14	2	$2, 6, 18$
-11	3	$1, 8, 64$	14	2	$4, 8, 16$
34	2	$6, 126, 2646$	56	2	$8, 16, 32$
77	11	$11, 44, 176$	81	7	$9, 12, 16$
82	2	$18, 42, 98$			

i.e. norm form equations (1) with $K = \mathbb{Q}(\sqrt{d})$ a quadratic field, $\alpha_1 = 1$ and $\alpha_2 = \sqrt{d}$, where d is some integer not a square. Note that usually an equation of type (2) is called a Pell equation only if $d > 0$ and square-free. However in this paper we consider equation (2) for all $d, m \in \mathbb{Z}$. Some years ago Pethő and Ziegler [8] considered the vertical problem for this case, i.e. they considered arithmetic progressions on such Diophantine equations and obtained effective results. In particular, they proved upper bounds for $\max |X_i|$ and $\max |Y_i|$ respectively, where X_1, X_2 and X_3 or Y_1, Y_2 and Y_3 are in arithmetic progression and are also solutions to (2). Moreover, Pethő and Ziegler considered also fixed arithmetic progressions and asked whether there exist integers d and m such that these arithmetic progressions are part of the solution set of (2). They established results for arithmetic progressions of length 3 and ≥ 5. The case of length 4 was settled by Dujella, Pethő and Tadić [5].

Our intention is to prove analogous results for geometric progressions as obtained by Pethő and Ziegler [8] and by Dujella, Pethő and Tadić [5] for arithmetic progressions, respectively. For technical reasons we exclude trivial geometric progressions X_1, X_2, X_3, with $|X_1| = |X_2| = |X_3|$ or $X_1X_2X_3 = 0$.

Theorem 1. *Let $X_1 < X_2 < X_3$ be the X-components of three positive distinct solutions to* (2) *such that they form a geometric progression, i.e. fulfill $X_1X_3 = X_2^2$. Then we have*

$$X_3 < 1645683|m|^{20}.$$

Similarly assume that $Y_1 < Y_2 < Y_3$ are the Y-components of three positive distinct solutions to (2) *which form a geometric progression. Then we have*

$$Y_3 < \frac{1645683|m|^{20}}{d}.$$

Similarly as in [8] we obtain as a corollary that for small m there are no three term geometric progressions, in particular we find a method to determine for fixed m all d such that (2) provides geometric progressions in their solution set.

Corollary 1. *Let $m \in \mathbb{Z}$, $m \neq 0$ be fixed and assume* (2) *provides a non-trivial geometric progression in its solution set. Then we have*

$$d \leq \frac{m^2(13+\sqrt{7})}{2}.$$

In particular this yields an effective algorithm to find all geometric progressions in the solution set of Pell equations (2) *with $|m| \leq C$, with C a given constant. For $C = 100$ all geometric progressions are listed in Tables 1 and 2.*

Table 2. Non-trivial geometric progressions of (2) in the Y-components, with $|m| \leq 100$.

m	d	Y-components	m	d	Y-components
-80	21	$2, 6, 18$	-80	84	$1, 3, 9$
-77	78	$1, 3, 9$	-69	70	$1, 5, 25$
-68	2	$6, 126, 2646$	-68	8	$3, 63, 1323$
-68	18	$2, 42, 882$	-68	72	$1, 21, 441$
-63	2	$6, 12, 24$	-63	8	$3, 6, 12$
-63	11	$3, 12, 48$	-63	18	$2, 4, 8$
-63	72	$1, 2, 4$	-63	99	$1, 4, 16$
-55	14	$2, 4, 8$	-55	56	$1, 2, 4$
-41	2	$9, 21, 49$	-38	87	$1, 7, 49$
-31	14	$2, 10, 50$	-31	56	$1, 5, 25$
-28	2	$4, 8, 16$	-28	8	$2, 4, 8$
-28	11	$2, 8, 32$	-28	32	$1, 2, 4$
-28	44	$1, 4, 16$	-26	35	$1, 3, 9$
-20	21	$1, 3, 9$	-17	2	$3, 63, 1323$
-17	18	$1, 21, 441$	-7	2	$2, 4, 8$
-7	8	$1, 2, 4$	-7	11	$1, 4, 16$
7	2	$1, 3, 9$	22	3	$1, 7, 49$
28	2	$2, 6, 18$	28	8	$1, 3, 9$
33	3	$1, 8, 64$	34	2	$1, 55, 3025$
37	21	$2, 22, 242$	37	84	$1, 11, 121$
41	2	$8, 20, 50$	41	8	$4, 10, 25$
56	11	$2, 10, 50$	56	44	$1, 5, 25$
57	7	$1, 4, 16$	57	87	$1, 8, 64$
63	2	$3, 9, 27$	63	18	$1, 3, 9$
65	14	$2, 4, 8$	65	35	$1, 4, 16$
65	56	$1, 2, 4$	70	11	$1, 3, 9$
78	22	$1, 7, 49$	85	21	$2, 6, 18$
85	84	$1, 3, 9$	86	110	$1, 7, 49$
88	3	$2, 14, 98$	88	12	$1, 7, 49$
90	31	$1, 13, 169$	98	2	$1, 7, 49$
100	21	$1, 5, 25$			

It is very surprising that the following theorem on linear relations on the solution set of Pell equations contains as a corollary an upper bound for three term arithmetic progressions (cf. [8, Theorem 1]) as well as an upper bound for three term geometric progressions (Theorem 1).

Theorem 2. *Let (X_1,Y_1), (X_2,Y_2) and (X_3,Y_3) be three non-zero solutions to (2), i.e. $X_1X_2X_3Y_1Y_2Y_3 \neq 0$, such that they fulfill the inhomogeneous linear equation*

$$aX_1 + bX_2 + cX_3 + f = 0,$$

where $a,b,c,f \in \mathbb{Z}$ and $abc \neq 0$. In the case of $f = 0$ we additionally assume that $|a|,|b|,|c|$ are the sides of a triangle, i.e. the maximum $\max\{|a|,|b|,|c|\}$ is smaller than the sum of the other two. Let $\tilde{c} = \max\{|a|,|b|,|c|\}$ and

$$C := C(\tilde{c}, f, m) = \max\{a_0, a_1, a_2\}$$

with

$$\begin{aligned}
|a_0| \leq & 394347\tilde{c}^8|f|^8|m|^4 + 564133\tilde{c}^{10}|f|^7|m|^5 + 469762\tilde{c}^{12}|f|^6|m|^6 \\
& + 187909\tilde{c}^{12}|f|^5|m|^7 + 29534\tilde{c}^{12}|f|^4|m|^8; \\
|a_1| \leq & 817797\tilde{c}^9|f|^7|m|^4 + 582364\tilde{c}^{11}|f|^6|m|^5 + 192227\tilde{c}^{11}|f|^5|m|^6 \\
& + 8986\tilde{c}^{11}|f|^3|m|^7; \\
|a_2| \leq & 768542\tilde{c}^{10}|f|^6|m|^4 + 317902\tilde{c}^{11}|f|^5|m|^5 + 118821\tilde{c}^{12}|f|^4|m|^6;
\end{aligned}$$

in the case $f \neq 0$ and

$$a_0 = 304\tilde{c}^{12}|m|^8, \quad a_1 = 240\sqrt{2}\tilde{c}^{11}|m|^7, \quad a_2 = 400\tilde{c}^{12}|m|^6$$

if $f = 0$. Then we have

$$\max\{|X_1|,|X_2|,|X_3|\} \leq C$$

or one of the four exceptional cases holds:

- *$X_1 = \min\{|X_i|\}$, $f = -aX_1$, $b = \pm c$ and $X_2 = \mp X_3$;*
- *$X_2 = \min\{|X_i|\}$, $f = -bX_2$, $a = \pm c$ and $X_1 = \mp X_3$;*
- *$X_3 = \min\{|X_i|\}$, $f = -cX_3$, $b = \pm a$ and $X_2 = \mp X_1$;*
- *$f = 0$, $a = \pm b \pm c$ and $|X_1| = |X_2| = |X_3|$ and $|Y_1| = |Y_2| = |Y_3|$.*

Remark 1. If we choose $a = c = 1$, $b = -2$ and $f = 0$ we immediately get an upper bound for non-constant positive arithmetic progressions by applying Theorem 2. To see that also Theorem 1 is a consequence of Theorem 2 is a little bit more tricky and will be discussed in Section 3.

Obviously the Theorems 1 and 2 are trivial if d is not positive or d is a square. However, to find $d,m \in \mathbb{Z}$ such that a given geometric progression is admitted by (2) is not easy, even if we allow negative d. In view of [8, Theorem 5 and Theorem 7] we show:

Theorem 3. *Let $0 < Y_1 < Y_2 < Y_3 < Y_4 < Y_5$ be a given geometric progression. Then there are at most finitely many $d,m \in \mathbb{Z}$ such that d is not a square, $m \neq 0$ and $\gcd(d,m)$ is square-free such that Y_1,Y_2,Y_3,Y_4,Y_5 are the Y-components of solutions to $X^2 - dY^2 = m$.*

On the other hand for a given geometric progression $0 < X_1 < X_2 < X_3$ there exist at most finitely many $d,m \in \mathbb{Z}$ such that d is not a square, $m \neq 0$ and $\gcd(d,m)$ is square-free such that X_1,X_2,X_3 are the X-components of solutions to $X^2 - dY^2 = m$.

And in view of [5] we show:

Theorem 4. *Let $0 < Y_1 < Y_2 < Y_3 < Y_4$ be a given geometric progression. Then there exist infinitely many $d, m \in \mathbb{Z}$ such that d is not a square, $m \neq 0$ and $\gcd(d, m)$ is square-free such that Y_1, Y_2, Y_3, Y_4 are the Y-components of solutions to $X^2 - dY^2 = m$.*

Remark 2. Note that the condition that $\gcd(d, m)$ is square-free is important to avoid Pell equations that are essentially the same. Note that if $Y_1 < Y_2 < \cdots$ is an arithmetic or geometric progression on the Pell equation $X^2 - dY^2 = m$, then it is also an arithmetic or geometric progression on the Pell equation $X^2 - dd_0^2Y^2 = md_0^2$.

Closely related to the solution set of Pell equations are so-called Lucas sequences, i.e. sequences of the form

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

where

$$\alpha = \frac{a + \sqrt{b}}{2} \quad \text{and} \quad \beta = \frac{a - \sqrt{b}}{2},$$

with a, b non-zero integers. Furthermore we assume $\alpha + \beta$ and $\alpha\beta$ are non-zero, co-prime integers and α/β is not a root of unity. For these Lucas sequences we prove the following theorem.

Theorem 5. *Let $(u_n)_{n\geq 1}$ be a Lucas sequence and assume that there are three distinct indices n, k, l such that $u_k u_l = u_n^2$. Except the trivial case where $u_k, u_l, u_n \in \{\pm 1\}$ the only solutions are $(u_1, u_2, u_4) = (u_3, u_2, u_4) = (1, -2, 4)$ with $a = -2$ and $b = -8$.*

In the next section we will prove Theorem 2, which is essential for proving Theorem 1 in Section 3. The proof of Theorem 2 is, beside the use of Gröbner bases, elementary. After showing that for a fixed Pell Equations effective upper bounds for geometric progressions exist we discuss the existence of Pell equations that admit a fixed geometric progression. The cases of fixed three and five term geometric progressions is discussed in Section 4 and the case of fixed four term geometric progressions is treated in Section 5. The treatment of fixed five term geometric progressions makes use of Faltings' theorem [6] on rational points of curves of genus > 1 and the result is therefore non-effective. On the other hand in the case of four term geometric progressions we are led to elliptic curves and therefore we get more information and we can describe how to find all Pell equations that admit a given geometric four term progression. The last section is devoted to geometric progressions in Lucas sequences. The use of the primitive divisor Theorem due to Bilu, Hanrot and Voutier [2] breaks the problem down to some elementary considerations.

2. Pell equations with linear Restriction

As mentioned above the case of non-positive or square d is trivial in the proof of Theorems 1 and 2. Therefore we assume in the next two sections that d is positive and not a perfect square.

Let us assume that $(X_1, Y_1), (X_2, Y_2)$ and (X_3, Y_3) are three non-zero solutions, i.e. $X_1X_2X_3Y_1Y_2Y_3 \neq 0$ to (2) and assume they fulfill the linear relation

$$aX_1 + bX_2 + cX_3 + f = 0, \tag{3}$$

with $a, b, c, f \in \mathbb{Z}$ and $abc \neq 0$. Without loss of generality we may assume that $\operatorname{sign}(X_i) = \operatorname{sign}(Y_i)$ for $i = 1, 2, 3$. First, we show that the homogeneous variant of (3) cannot hold for the Y-components simultaneously provided X is not too small. In order to keep notations short we write $\tilde{c} = \max\{|a|, |b|, |c|\}$.

Lemma 1. *Let* $(X_1, Y_1), (X_2, Y_2)$ *and* (X_3, Y_3) *be non-zero solutions to* (2) *that satisfy* (3). *Then*

$$aY_1 + bY_2 + cY_3 = 0 \tag{4}$$

implies

$$\max\{|X_i|\} \leq \frac{2|m|\tilde{c}^2(3|m|\tilde{c}^2 + |f|^2)(2\sqrt{d}+1)}{|f|(\sqrt{d}-1)} + |f|$$

or $f = 0$ *and* $|a| = |b \pm c|$ *and* $|X_1| = |X_2| = |X_3|$.

Before we start with the proof of Lemma 1 we state a useful Diophantine inequality for square roots.

Lemma 2. *Let* p, q, d *be integers, with* $d, q > 0$ *and* d *not a perfect square. Then*

$$|p - q\sqrt{d}| > \frac{\sqrt{d}-1}{\max\{1, |p|\}(2\sqrt{d}+1)}. \tag{5}$$

Proof of Lemma 2. The case $p \leq 0$ is obvious, therefore we assume $p > 0$.

First, let us consider the case, where $\sqrt{d} - 1 < p/q < \sqrt{d} + 1$, i.e. $q(\sqrt{d}-1) < p < q(\sqrt{d}+1)$ respectively $p + q\sqrt{d} < q(2\sqrt{d}+1)$ and $q < \frac{p}{\sqrt{d}-1}$. Therefore

$$1 \leq |p^2 - q^2 d| = |p - q\sqrt{d}||p + q\sqrt{d}| < |p - q\sqrt{d}||q|(2\sqrt{d}+1) < |p - q\sqrt{d}||p|\frac{2\sqrt{d}+1}{\sqrt{d}-1},$$

hence we obtain (5) in this case.

Now assume $\sqrt{d} - 1 > p/q$. Then we obtain $p - q\sqrt{d} < -q$, i.e.

$$|p - q\sqrt{d}| > q \geq 1 > \frac{\sqrt{d}-1}{|p|(2\sqrt{d}+1)}$$

and the lemma is also proved in this case.

The case $\sqrt{d} + 1 < p/q$ is similar to the case above and is omitted. □

Proof of Lemma 1. We split the proof up into two cases: $f = 0$ and $f \neq 0$.

Let us start with the second case and assume (4) holds. Then by combining (3) and (4) and using the fact that

$$|X - Y\sqrt{d}| = \frac{|m|}{|X + Y\sqrt{d}|}$$

for a solution (X, Y) to (2) we get

$$\begin{aligned}|f| =& |a(X_1 - Y_1\sqrt{d}) + b(X_2 - Y_2\sqrt{d}) + c(X_3 - Y_3\sqrt{d})| \\ \leq& \frac{3|m|\max\{|a|, |b|, |c|\}}{\min\{|X_i|\}}.\end{aligned}$$

We remind the reader that we assumed $\operatorname{sign}(X_i) = \operatorname{sign}(Y_i)$ for $i = 1, 2, 3$. Hence, we deduce that

$$\min\{|X_i|\} \leq \frac{3|m|\tilde{c}}{|f|} =: B.$$

Without loss of generality we may assume that $|X_1| = \min\{|X_i|\}$ and Lemma 2 applied to $\lambda = f + aX_1 - aY_1\sqrt{d}$ with $p = |f + aX_1|$ and $q = |aY_1|$ yields

$$|\lambda| \geq \frac{\sqrt{d}-1}{(|a|B+|f|)(2\sqrt{d}+1)} := B'.$$

Hence

$$|B'| \leq |\lambda| = \left|b(X_2 - Y_2\sqrt{d}) + c(X_3 - Y_3\sqrt{d})\right| \leq \frac{2|m|\max\{|b|,|c|\}}{\min\{|X_2|,|X_3|\}},$$

and

$$\min\{|X_2|,|X_3|\} \leq \frac{2|m|\tilde{c}(3|m|\tilde{c}^2+|f|^2)(2\sqrt{d}+1)}{|f|(\sqrt{d}-1)}.$$

Now let us assume without loss of generality that $|X_2| = \min\{|X_2|,|X_3|\}$. Then (3) yields together with the bounds for $|X_1|$ and $|X_2|$ the statement of the lemma.

Now let us assume that $f = 0$. By the assumptions of the lemma we assume that $|a|,|b|,|c|$ are the sides of a triangle. Together with the other constraints we obtain several equations in several variables. In order to eliminate at least some of the variables we use Groebner Bases. In particular, we compute the Groebner basis of the ideal

$$I := \langle X_1^2 - dY_1^2 - m, X_2^2 - dY_2^2 - m, X_3^2 - dY_3^2 - m, aX_1 + bX_2 + cX_3, aY_1 + bY_2 + cY_3\rangle$$

over the ring $\mathbb{Q}[X_1, X_2, X_3, Y_1, Y_2, Y_3]$, with respect to the lexicographic term order implied by $X_1 < X_2 < \cdots < Y_3$. The smallest element of the Groebner basis (computed with the computer algebra program Mathematica) gives us the following quadratic polynomial in Y_3

$$\begin{aligned}-m^2\big(&a^4m^2 + b^4m^2 + c^4m^2 - 4b^3cdY_2Y_3 - 4bc^3dY_2Y_3 + \\ &2a^2(2bcdY_2Y_3 - (b^2+c^2)m^2) - 2b^2c^2(m^2 + 2d(Y_2^2+Y_3^2))\big)\end{aligned}$$

which has discriminant

$$\delta = 16db^2(m^2 + dY_2^2)((b+c)^2 - a^2)((b-c)^2 - a^2).$$

Therefore the quadratic equation yields a solution only if $\delta \geq 0$. But, we have $\delta < 0$ if and only if $|b| + |c| > |a| > |b| - |c|$. By permuting indices we get similar inequalities for $|b|$ and $|c|$, which are exactly fulfilled by the sides of a triangle, hence by our assumptions either $\delta = 0$ or no solution exists. Therefore we have to consider the corner cases, i.e. we may assume that the case $|a| = |b \pm c|$ holds. The first element of the Groebner basis yields in this case

$$4b^2c^2d(Y_2 \mp Y_3)^2.$$

Therefore we conclude $Y_2 = \pm Y_3$. Hence we obtain

$$aY_1 + (b \pm c)Y_2 = \pm(b \pm c)Y_1 + (b \pm c)Y_2 = 0$$

and therefore $Y_1 = \pm Y_2$ which implies $|X_1| = |X_2| = |X_3|$. □

Let us write

$$\Delta_Y = aY_1 + bY_2 + cY_3$$

and the lemma above shows that either $|\Delta_Y| \geq 1$ or $\max\{|X_i|\}$ is "small" or exceptional. Therefore we may assume for the rest of the section that $\Delta_Y \neq 0$. Our next aim is to show that $|\Delta_Y|$ stays relatively small.

Lemma 3. *We have*

$$|\Delta_Y| \leq \frac{|m|(|a|+|b|+|c|)}{\min\{|X_i|\}\sqrt{d}} + \frac{|f|}{\sqrt{d}} \leq \frac{|m|(|a|+|b|+|c|)+|f|}{\sqrt{d}}.$$

Proof. We have

$$\begin{aligned}|\Delta_Y|\sqrt{d} =& |a(X_1-Y_1\sqrt{d})+b(X_2-Y_2\sqrt{d})+c(X_3-Y_3\sqrt{d})-f|\\ \leq& |m|\left(\frac{|a|}{|X_1+\sqrt{d}Y_1|}+\frac{|b|}{|X_2+\sqrt{d}Y_2|}+\frac{|c|}{|X_3+\sqrt{d}Y_3|}\right)+|f|\\ \leq& \frac{|m|(|a|+|b|+|c|)}{\min\{|X_i|\}}+|f|\end{aligned}$$

which proves the lemma. Note that we still assume $\mathrm{sign}(X_i)=\mathrm{sign}(Y_i)$. □

We apply (5) to $\Delta_Y\sqrt{d}+f$ and obtain

$$|\Delta_Y\sqrt{d}+f| > \frac{\sqrt{d}-1}{|f|(2\sqrt{d}+1)}$$

if $f\neq 0$ and $|\Delta_Y|\geq 1$ if $f=0$. Hence, by the proof of Lemma 3 we obtain in any case

$$\min\{|X_i|\} \leq \frac{|m|\max\{|f|,1\}(|a|+|b|+|c|)(2\sqrt{d}+1)}{\sqrt{d}-1} \tag{6}$$

For the rest of the proof of Theorem 2 we may assume without loss of generality that $|X_1|\leq|X_2|\leq|X_3|$. Therefore we have to find upper bounds for $|X_3|$. By (6) we have already found an upper bound for $|X_1|$. Now let us write $\Delta=\Delta_Y$ and $\tilde{c}=\max\{|a|,|b|,|c|\}$. We consider the ideal

$$\begin{aligned}I := \langle X_1^2-dY_1^2-m, X_2^2-dY_2^2-m, X_3^2-dY_3^2-m,&\\ aX_1+bX_2+cX_3-f, aY_1+bY_2+cY_3-\Delta\rangle&\end{aligned}$$

in the polynomial ring $\mathbb{Q}[X_1,X_2,X_3,Y_1,Y_2,Y_3]$, and we compute the Groebner basis of I with respect to the lexicographic term order implied by $Y_2<Y_1<Y_3<X_2<X_1<X_3$. The smallest element g_1 of the Groebner basis is of degree 4 in X_3. Let us write

$$g_1 = X_3^4a_4+X_3^3a_3+X_3^2a_2+X_3a_1+a_0.$$

For reasons of space we do not write down the polynomial (it consists of 362 monomials in $\mathbb{Z}[a,b,c,d,f,m,\Delta,X_1,X_3]$). However, our purpose is to find upper bounds for the roots of g_1. We have to distinguish between the cases $a_4\neq 0$ and $a_4=0$. Let us consider the case $a_4\neq 0$ first.

We note that every integral root of an integral polynomial divides the constant term. Therefore $|a_0|$ is an upper bound for $|X_3|$ provided $a_0\neq 0$. But, in the case of $a_0=0$ we divide g_1 by X_3, hence a_1 is the new constant term and is therefore the new upper bound, provided $a_1\neq 0$. Applying similar arguments we end in the estimate

$$|X_3| \leq \max_{0\leq i\leq 3}\{|a_i|\}.$$

Hence, we have to estimate the coefficients a_i. This can be done by assuming that every monomial is positive and replacing a,b,c by $\tilde{c}=\max\{|a|,|b|,|c|\}$, Δ by the upper bound obtained in Lemma 3 and X_1 by the upper bound (6). We also distinguish between the case $f=0$ and $f\neq 0$.

Let us consider first the case $f \neq 0$. In this case we also use the inequality $\frac{2\sqrt{d}-1}{\sqrt{d}-1} < \frac{2\sqrt{2}+1}{\sqrt{2}-1}$ and therefore we obtain

$$\begin{aligned}
|a_0| \leq & 394347\tilde{c}^8|f|^8|m|^4 + 564133\tilde{c}^{10}|f|^7|m|^5 + 469762\tilde{c}^{12}|f|^6|m|^6 \\
& + 187909\tilde{c}^{12}|f|^5|m|^7 + 29534\tilde{c}^{12}|f|^4|m|^8; \\
|a_1| \leq & 817797\tilde{c}^9|f|^7|m|^4 + 582364\tilde{c}^{11}|f|^6|m|^5 + 192227\tilde{c}^{11}|f|^5|m|^6 \\
& + 8986\tilde{c}^{11}|f|^3|m|^7; \\
|a_2| \leq & 768542\tilde{c}^{10}|f|^6|m|^4 + 317902\tilde{c}^{11}|f|^5|m|^5 + 118821\tilde{c}^{12}|f|^4|m|^6; \\
|a_3| \leq & 141653\tilde{c}^9|f|^5|m|^3 + 84103\tilde{c}^{10}|f|^4|m|^4 + 35941\tilde{c}^{11}|f|^3|m|^5.
\end{aligned}$$

These bounds yield the result of Theorem 2 in the case $f \neq 0$.

In the case of $f = 0$ we obtain

$$\begin{aligned}
|a_0| \leq & 304\tilde{c}^{12}m^8, & |a_1| \leq & 240\sqrt{2}\tilde{c}^{11}m^7, \\
|a_2| \leq & 400\tilde{c}^{12}m^6, & |a_3| \leq & 160\sqrt{2}\tilde{c}^{11}m^5,
\end{aligned}$$

which settles Theorem 2 in the case $a_4 \neq 0$.

Now we consider the case $a_4 = 0$. Therefore we have a closer look on a_4:

$$a_4 = 16c^4\left(-(f^2 + a^2m - 2afX_1)^2 + 2d(f^2 - 2afX_1 - a^2(m - 2X_1^2))\Delta^2 - d^2\Delta^4\right).$$

Obviously this is a quadratic polynomial in X_1 and a rational root exists if and only if the discriminant of this polynomial is a square. But the discriminant of this polynomial is

$$4096a^2c^8d\Delta^2(-f^2 + a^2m + d\Delta^2)^2$$

which cannot be a square by the assumption that d is not a perfect square, unless $f^2 = a^2m + d\Delta^2$. Substituting $f^2 = a^2m + d\Delta^2$ into a_4 we obtain

$$a_4 = -64c^4(f + aX_1)^2(f^2 - d\Delta^2)$$

which vanishes if and only if $f = -aX_1$. Now, let us compute g_1 under the assumptions $f = -aX_1$ and $f^2 = a^2m + d\Delta^2$ and we obtain

$$g_1 = m^2(b^2 - c^2)^2\left((b^2 - c^2)^2m^2 + 8d(b^2m + c^2(m - 2X_3^2))\Delta^2 + 16d^2\Delta^4\right).$$

Therefore either $b = \pm c$ or X_3 fulfills a quadratic equation (note the coefficient of X_3^2 is $-16c^2d\Delta^2 \neq 0$). But, $b = \pm c$ and $f = -aX_1$ yields

$$0 = aX_1 + bX_2 + cX_3 + f = c(X_2 \pm X_3)$$

an exceptional case. Therefore we are left to estimate X_3. Solving $g_1 = 0$ for X_3 under the assumptions $f = -aX_1$ and $f^2 = a^2m + d\Delta^2$ we obtain

$$\begin{aligned}
|X_3| = & \frac{\sqrt{(b^2 - c^2)^2m^2 + 8(b^2 + c^2)dm\Delta^2 + 16d^2\Delta^4}}{4c\Delta\sqrt{d}} \\
\leq & \sqrt{\frac{4\tilde{c}^4m^2 + 16\tilde{c}^2dm\Delta^2 + 16d^2\Delta^4}{16d\Delta^2}} \\
\leq & \sqrt{\tilde{c}^4m^2 + \tilde{c}^2m + d\Delta^2} \\
\leq & \sqrt{\tilde{c}^4m^2 + \tilde{c}^2m + 4m^2\tilde{c}^2} \\
\leq & \tilde{c}^2m\sqrt{6} < C(\tilde{c}, m, f).
\end{aligned}$$

Note that we used by estimating Δ the fact that $f = -aX_1$ and hence $|f| \le |a| \le \tilde{c}$. Therefore Theorem 2 is proved completely.

Remark 3. As an immediate consequence of Theorem 2 we obtain an upper bound for the length of arithmetic progressions $0 < X_1 < X_2 < X_3$ by noting that $X_1 - 2X_2 + X_3 = 0$ implies $X_3 \le 19 \cdot 2^{16}|m|^8$ provided $|m| > 1$ and $X_3 < 25 \cdot 2^{16}$ if $|m| = 1$. Note that the bounds given in [8] are sharper.

3. Upper bounds for geometric progressions

The main aim of this section is to prove Theorem 1. First, we note that for a positive solution (X, Y) to Pell equation (2), we have

$$X = \frac{\alpha\epsilon^n + \bar{\alpha}\epsilon^{-n}}{2}, \tag{7}$$

where n is some integer, α is some algebraic integer coming form a finite set, $\bar{\alpha}$ is its (Galois) conjugate and $\epsilon > 1$ is the fundamental unit of $\mathbb{Z}[\sqrt{d}]$. Assume now that the X-components $X_1 < X_2 < X_3$ of the solutions (X_i, Y_i), $i = 1, 2, 3$, to (2) form a geometric progression, i.e. $X_2^2 = X_1X_3$ and let us write $X_i = \frac{\alpha_i\epsilon^{n_i} + \bar{\alpha}_i\epsilon^{-n_i}}{2}$. This leads us to the equation

$$\begin{aligned} 0 =& X_1X_3 - X_2^2 \\ =& \frac{\overbrace{\epsilon^{n_1+n_3}\alpha_1\alpha_3 + \bar{\alpha}_1\bar{\alpha}_3\epsilon^{-n_1-n_3}}^{:=\xi_1/2}}{4} + \frac{\overbrace{\epsilon^{n_1-n_3}\alpha_1\bar{\alpha}_3 + \bar{\alpha}_1\alpha_3\epsilon^{-n_1+n_3}}^{:=\xi_2/2}}{4} \\ & - \frac{\overbrace{\epsilon^{2n_2}\alpha_2^2 + \bar{\alpha}_2^2\epsilon^{2n_2}}^{:=\xi_3/2}}{4} - \frac{m}{2} \\ =& \frac{\xi_1 + \xi_2 - \xi_3 - m}{2} \end{aligned}$$

where ξ_i, $i = 1, 2, 3$ are solutions to the Pell equation

$$\xi^2 - d\eta^2 = M := m^2.$$

Note that the norm of α_i is m for $i = 1, 2, 3$. We apply Theorem 2 to this situation and obtain for $i = 1, 2, 3$

$$\max\{|\xi_i|\} \le 1645683|m|^{20}$$

or one of the exceptional cases holds. Assume that we are not in an exceptional case, then we know that

$$1645683|m|^{20} \ge \frac{\xi_1 + \xi_2}{2} = |X_1||X_3| \ge |X_3| = \max\{|X_i|\},$$

which proves the first part of Theorem 1.

Now let us consider the case that $0 < Y_1 < Y_2 < Y_3$ forms a geometric progression. In this case for a solution (X, Y) to the Pell equation (2) we have

$$Y = \frac{\alpha\epsilon^n - \bar{\alpha}\epsilon^{-n}}{2\sqrt{d}}, \tag{8}$$

hence we obtain

$$\begin{aligned}0 =& Y_1Y_3 - Y_2^2\\ =& \frac{\overbrace{\epsilon^{n_1+n_3}\alpha_1\alpha_3 + \bar\alpha_1\bar\alpha_3\epsilon^{-n_1-n_3}}^{:=\xi_1/2d}}{4d} - \frac{\overbrace{\epsilon^{n_1-n_3}\alpha_1\bar\alpha_3 + \bar\alpha_1\alpha_3\epsilon^{-n_1+n_3}}^{:=\xi_2/2d}}{4d}\\ & - \frac{\overbrace{\epsilon^{2n_2}\alpha_2^2 + \bar\alpha_2^2\epsilon^{2n_2}}^{:=\xi_3/2d}}{4d} + \frac{m}{2d}\\ =& \frac{\xi_1 - \xi_2 - \xi_3 + m}{2d},\end{aligned}$$

where again ξ_i, $i = 1, 2, 3$ are solutions to the Pell equation

$$\xi^2 - d\eta^2 = M := m^2.$$

Obviously this yields the same upper bound for $\max\{|\xi|\}$. Further, this time we obtain

$$\frac{1645683|m|^{20}}{d} \geq \frac{\xi_1 - \xi_2}{2d} = |Y_1||Y_3| \geq |Y_3| = \max\{|Y_i|\}.$$

We are left to exclude the exceptional cases and the cases $\xi_i = 0$ and $\eta_i = 0$ for $i = 1, 2, 3$. The case $\xi_i = 0$ for $i = 1, 2, 3$ cannot occur, since $M = m^2 > 0$. If an exceptional case occurs we have $f \neq 0$ and since $|a| = |b| = |c| = 1$ we would obtain $\xi = m$ for some $i = 1, 2, 3$, hence $\eta_i = 0$. Therefore we are left to the three cases $\eta_1 = 0$, $\eta_2 = 0$ and $\eta_3 = 0$.

Let us first note that if $\alpha = u + v\sqrt{d}$ is a fundamental solution to an ambigous class with $u \geq 0$ and $v > 0$ and assume $x + y\sqrt{d} = \epsilon > 1$ is the fundamental solution to

$$X^2 - dY^2 = 1$$

we note that $\alpha = \epsilon\bar\alpha$. This is true since v_n^+ from $u_n^+ + v_n^+\sqrt{d} = \alpha\epsilon^n$ g and v_n^- from $u_n^- - v_n^-\sqrt{d} = \bar\alpha\epsilon^{-n}$ are strictly increasing and since we assume v was chosen minimal.

First, we consider the case $\eta_1 = 0$. In this case we have $\xi_1 = M$ and therefore we conclude

$$\epsilon^{n_1+n_3}\alpha_1\alpha_3 = m$$

which yields $\alpha_1 = \epsilon^n\bar\alpha_3$ for some n. This yields $\epsilon^{n_1+n_3}\alpha_1\alpha_3 = \epsilon^{n_1+n_3+n}\alpha_3\bar\alpha_3 = m$, hence $n_1 = -n_3 - n$. Therefore we have

$$\epsilon^{n_1}\alpha_1 = \epsilon^{-n_3-n}\epsilon^n\bar\alpha_3 = \overline{\epsilon^{n_3}\alpha_3}.$$

But this yields $X_1 = X_3$ and $Y_1 = -Y_3$ a contradiction. The case $\eta_2 = 0$ is similar and we omit this case. In the case $\eta_3 = 0$ we have

$$\epsilon^{2n_2}\alpha_2^2 = m$$

and therefore we have $\alpha_2 = \bar\alpha_2\epsilon^n$ for some n. Since α_2 is fundamental we deduce $\alpha_2 = \bar\alpha_2$, hence $\alpha_2 = \sqrt{m} \in \mathbb{Z}$ and $n_2 = 0$, or $\alpha_2 = \epsilon\bar\alpha_2$. The first case yields $X_2 = \sqrt{m}$ and $Y_2 = 0$. If we consider geometric progressions in the Y-components we are done, since we assume that $0 < Y_1 < Y_2 < Y_3$. In the case of considering geometric progressions in the X-component we note that $X = \sqrt{m} \in \mathbb{Z}$ is smallest possible, but we assume $|X_1| < |X_2| = \sqrt{m}$, hence a contradiction. In the second case we have

$$\epsilon^{2n_2}\alpha_2^2 = \epsilon^{2n_2+1}\alpha_2\bar{\alpha}_2 = m,$$

hence $2n_2 + 1 = 0$ a contradiction and Theorem 1 is proved completely.

The rest of this section is devoted to the proof of Corollary 1.

Proof of Corollary 1. As explained above we have to consider the linear relations on the solution set of the Pell equation $\xi^2 - d\eta^2 = M$ with $M = m^2$. Let us reconsider Lemma 3. In this case we have $|a| = |b| = |c| = 1$, $|f| = |m|$ and $M = m^2$ and therefore

$$|\Delta_\eta \sqrt{d}| \leq \frac{3m^2}{\sqrt{d}} + |m|, \tag{9}$$

provided that $\eta_1\eta_2\eta_3 \neq 0$. Note that since we assume that $|\eta_i| \geq 1$ the denominators in the second line of the estimate in the proof of Lemma 3 are at least $|\sqrt{d}|$. On the other hand, if we assume $|\Delta_\eta| \geq 1$ we obtain

$$d \leq 3m^2 + |m|\sqrt{d}.$$

Therefore by solving the above inequality for d we obtain in any case a bound for d depending on m:

$$d \leq \frac{m^2(7+\sqrt{13})}{2}.$$

Now assume $\Delta_\eta = 0$. Then we have $\eta_3 = \eta_1 + \eta_2$ and $\xi_3 = \xi_1 + \xi_2 - m$ and the Pell Equation for ξ_3 and η_3 yields

$$\xi_1^2 + \xi_2^2 + m^2 + 2\xi_1\xi_2 - 2m(\xi_1 + \xi_2) - d(\eta_1^2 + \eta_2^2 + 2\eta_1\eta_2) - m^2 = 0.$$

We replace η_i^2 by $\frac{\xi_i^2 - m^2}{d}$ for $i = 1, 2$ and obtain

$$m^2 - m(\xi_1 + \xi_2) + \xi_1\xi_2 = d\eta_1\eta_2.$$

Squaring this equation and replacing the η's again we obtain

$$2m(m - \xi_1)(m - \xi_2)(\xi_1 + \xi_2) = 0.$$

Therefore either $m = 0$ or $\xi_i = m$ for some $i = 1, 2$, but $\xi_i = m$ yields $\eta_i = 0$ in any case a contradiction. Therefore the case $\Delta_\eta = 0$ cannot occur. This proves the first part of Corollary 1.

Therefore to find all geometric progressions of Pell equations (2) with $m < C$ for some fixed constant C we only have to consider finitely many Pell equations. Moreover, we need not solve the whole Pell equation, we are only interested in relatively small solutions, i.e. solutions that satisfy the bounds given in Theorem 1. Based on these estimates we wrote a search program in Mathematica, which checks all instances for the pair (m, d) with $m \leq 100$. This computation yields the lists in Corollary 1. □

4. Pell equations with fixed geometric progressions

Now let us consider the case, where we fix the geometric progression and we want to find Pell equations (2) that have this geometric progression in the X or Y-components of their solution sets. Note that in this and the next section we consider all $d \in \mathbb{Z}$ and do not restrict ourselves to positive and non-square d's. We start to prove the statement on the X-components in Theorem 3 (see the proposition below).

Proposition 1. *For a given geometric progression $0 < X_1 < X_2 < X_3$ there exist at most finitely many $d, m \in \mathbb{Z}$ such that d is not a square, $m \neq 0$ and $\gcd(d, m)$ is square-free such that X_1, X_2, X_3 are the X-components of solutions to $X^2 - dY^2 = m$.*

Proof. Assume that $X_1 = q$, $X_2 = qa$ and $X_3 = qa^2$ for fixed q and a. We obtain the system of equations

$$q^2 - dY_1^2 = m, \quad q^2a^2 - dY_2^2 = m, \quad q^2a^4 - dY_3^2 = m.$$

The first two equations yield

$$q^2(a^2 - 1) = d(Y_2^2 - Y_1^2)$$

Since we assume that $a > 1$ we deduce that there are only finitely many possibilities for d, since $d|q^2(a^2 - 1)$. On the other hand also $(Y_2 + Y_1)|q^2(a^2 - 1)$ is fulfilled and therefore we have only finitely many possibilities for Y_1 and Y_2. However, this also yields finitely many possibilities for m. $\square$

Now let us consider what happens, if we fix a five-term geometric progression that should be included in the Y-components of the solution set of (2). Similarly as in the proof above we obtain the following system of equations:

$$X_1^2 - dq^2 = m, \quad X_2^2 - dq^2a^2 = m, \quad X_3^2 - dq^2a^4 = m$$
$$X_4^2 - dq^2a^6 = m, \quad X_5^2 - dq^2a^8 = m.$$

Eliminating m from these equations we obtain the system of equations

$$X_2^2 - X_1^2 = dq^2(a^2 - 1), \qquad X_3^2 - X_2^2 = dq^2a^2(a^2 - 1),$$
$$X_4^2 - X_3^2 = dq^2a^4(a^2 - 1), \qquad X_5^2 - X_4^2 = dq^2a^6(a^2 - 1).$$

Now eliminating dq^2 yields

$$a^2X_1^2 - (a^2 + 1)X_2^2 + X_3^2 = 0, \qquad a^2X_2^2 - (a^2 + 1)X_3^2 + X_4^2 = 0,$$
$$a^2X_3^2 - (a^2 + 1)X_4^2 + X_5^2 = 0$$

It is easy to prove that this is a projective curve $\mathfrak{C}$ for every $a \in \mathbb{Q}$ in the 4-dimensional projective space $\mathbb{P}^4$. We use the following lemma proved in [8, Lemma 5]:

Lemma 4. *Let $a_{i,j}$ be non-zero integers, and let the non-singular curve X be defined by*

$$\begin{aligned} X_1^2a_{1,1} + X_2^2a_{1,2} + X_3^2a_{1,3} &= 0, \\ X_2^2a_{2,1} + X_3^2a_{2,2} + X_4^2a_{2,3} &= 0, \\ X_3^2a_{3,1} + X_4^2a_{3,2} + X_5^2a_{3,3} &= 0. \end{aligned} \tag{10}$$

Let

$$\begin{aligned} F_1 &= a_{2,2}a_{3,2} - a_{2,3}a_{3,1}, \\ F_2 &= a_{1,2}a_{2,2} - a_{1,3}a_{2,1}, \\ F_3 &= a_{2,2}a_{3,2}a_{1,2} - a_{2,3}a_{1,2}a_{3,1} - a_{3,2}a_{1,3}a_{2,1}. \end{aligned}$$

If $F_1F_2F_3 \neq 0$, then the genus of X is 5.

According to Lemma 4 we compute
$$F_1 = F_2 = (a^2+1)^2 - a^2 = a^4 + a^2 + 1$$
and
$$F_3 = (a^2+1)^3 + 2a^2(a^2+1).$$
Therefore the curve $\mathfrak{C}$ is of genus 5. Hence, by Faltings' theorem [6] there are only finitely many rational points on the curve $\mathfrak{C}$, i.e. there exist only finitely many X_1, X_2, X_3, X_4 and X_5 and hence only finitely many d and m that fulfill the conditions of Theorem 3.

5. Pell equations with fixed four term arithmetic progressions

Assume that $X_k = qa^k$ for $k = 1, 2, 3, 4$ are solutions to a Pell equation (2). Then similarly as in the section above we obtain a curve $\mathfrak{C} \subset \mathbb{P}^3$ given by
$$a^2X_1^2 - (a^2+1)X_2^2 + X_3^2 = 0, \qquad a^2X_2^2 - (a^2+1)X_3^2 + X_4^2 = 0.$$
We parameterize the first equation of $\mathfrak{C}$ by projecting the corresponding conic from the point $P = (1,1,1,1) \in \mathfrak{C}$ to the plane $X_4 = 0$. The line from P to $Q = (x, y, z, 0)$ is given by the system
$$\begin{aligned} zX_2 - yX_3 + (y-z)X_4 &= 0,\\ zX_1 - xX_3 + (x-z)X_4 &= 0. \end{aligned}$$
and intersecting the conic with the line yields
$$\begin{aligned} X_1 =& a^2(x-y)^2 - 2xy + y^2 + 2xz - z^2\\ X_2 =& a^2(x-y)^2 + (y-z)^2\\ X_3 =& a^2(x-y)(x+y-2z) - (y-z)^2\\ X_4 =& a^2(x^2-y^2) + z^2 - y^2. \end{aligned}$$
Substituting this parametrization into the second equation defining $\mathfrak{C}$ we obtain a plane curve E_1 given by
$$\begin{aligned} &\big(a^2(x-y) - y + z\big) \times\\ &\qquad \big(a^4(x-y)(x-z)(y-z) + y(y-z)z - a^2(x-y)(x+y-z)z\big) = 0. \end{aligned}$$
Under the assumption the first factor is 0 we would obtain $X_1 = X_2 = X_3 = X_4$ contrary to our assumptions. Therefore we want to have a closer look on the second factor. Using a computer algebra program like MAGMA [3] we see that the second factor yields a cubic curve of genus 1. We want to transform this elliptic curve into Weierstrass form, therefore we make the transformations suggested in [9, pages 22-23]. As $\mathcal{O}$ we choose the point $(1,1,1)$ and the tangent at $\mathcal{O}$ is given by
$$(a^2+1)y - a^2x - z = 0.$$
Furthermore this tangent intersects the elliptic curve E_1 in $A = (a^4+a^2+1, a^4+a^2, a^4)$. The tangent at A is given by
$$x\frac{a^4}{a^4+a^2+1} - y + \frac{z}{a^2} = 0.$$
Now we choose $B = (0, 1, a^2)$ and the line from B to $\mathcal{O}$ is given by
$$x(a^2-1) - ya^2 + z = 0.$$

These three lines represent the new coordinate axes and we therefore perform the transformation

$$\begin{aligned} \xi &= \frac{a^4}{a^4+a^2+1}x - y + \frac{z}{a^2} \\ \eta &= (a^2-1)x - a^2y + z \\ \zeta &= -a^2x + (a^2+1)y - z. \end{aligned}$$

and obtain the elliptic curve E_2 given by

$$\begin{aligned} a^2\zeta\xi(\xi(a^4+a^2+1) - 2(2a^2+1)\eta) + \zeta^2(\xi(-a^4+a^2-1) - 2\eta a^2) \\ + (a^2-1)\zeta^3 - \eta^2\xi a^2(1+a^2) = 0. \end{aligned}$$

For the next step we have to consider the case $\xi\zeta = 0$ separately. We start with the case $\xi = 0$. In this case we obtain $\zeta = 0$ or $\zeta = \eta\frac{2a^2}{1-a^2}$. The case $\xi = \zeta = 0$ yields $\eta = 1$ (we are in projective space) and we obtain for this choice $-X_1 = X_2 = X_3 = X_4 = a^4 + a^2$ a contradiction to our assumptions. In the other case we obtain

$$\begin{aligned} X_1 &= 3a^2 + a^4 + a^6 - a^8, & X_2 &= a^2 + 3a^4 - a^6 + a^8, \\ X_3 &= a^2 - a^4 + 3a^6 + a^8, & X_4 &= a^2 - a^4 - a^6 - 3a^8. \end{aligned}$$

From the system $X_i^2 - dq^2a^{2i-2} = m$ for $i = 1,2,3,4$ we can compute d and m. In particular we obtain

$$d = 8\frac{a^4+a^6+a^8+a^{10}}{q^2}$$

and

$$m = a^4 - 2a^6 - a^8 - 12a^{10} - a^{12} - 2a^{14} + a^{16}.$$

By multiplying the equation $X^2 - dY^2 = m$ by a suitable rational square we obtain indeed a Pell equation such that there exist solutions (X_i, Y_i) with $Y_i = qa^{i-1}$ for $i = 1,2,3,4$. Obviously m cannot be zero and if d is a square we would obtain that $2(a^6 + a^4 + a^2 + 1)$ is a square. But the only rational point on the elliptic curve

$$(2a^2)^3 + 2(2a^2)^2 + 4(2a^2) + 8 = X^3 + 2X^2 + 4X + 8 = 4Y^2$$

is $(X,Y) = (-2,0)$ which yields no rational a. Therefore we have proved that for every four term geometric progression there exists a Pell equation containing it in the Y-components of the solution set.

Now, let us consider the case $\zeta = 0$. We obtain $\xi = 0$ or $\eta = 0$. The case $\xi = 0$ has been considered above and the case $\eta = 0$ yields by similar computations $X_i = 0$ for $i = 1,2,3,4$.

Now we may assume that $\xi\zeta \neq 0$ and therefore we multiply the defining equation of E_2 by ξ/ζ and substitute $\eta' = \eta\xi/\zeta$. Moreover by writing

$$\eta'' = \eta' - \frac{\zeta}{a^2+1} - \frac{\xi(2a^2+1)}{a^2+1}$$

we also eliminate the linear term of η' and obtain the elliptic curve E_3 given (as affine curve) by

$$\frac{(\xi a^2+1)(\xi(a^2+1)+1)(\xi(a^4+a^2+1)+a^2)}{a^2(1+a^2)^2} = (\eta'')^2.$$

In order to obtain E_3 in Weierstrass form we put

$$Y = \eta''(a+a^3)(a^8+2a^6+2a^4+a^2), \qquad X = \xi(a^8+2a^6+2a^4+a^2)$$

and obtain the elliptic curve E in Weierstrass form

$$(X+a^6+a^4)(X+a^6+a^4+a^2)(X+a^6+2a^4+2a^2+1) = Y^2. \tag{11}$$

Beside the three torsion points $T_1 = (-a^6-a^4, 0), T_2 = (-a^6-a^4-a^2, 0)$ and $T_3 = (-a^6-2a^4-2a^2-1, 0)$ also the point $P = (-a^6-a^4-a^2-1, a^3+a)$ lies on the elliptic curve E. If P is a torsion point, then according to the Lutz-Nagel theorem (see e.g. [7][Theorem 5.1])

$$2P = \left(-\frac{3a^8+4a^6+2a^4-1}{4a^2}, \frac{(a^2-1)(a^2+1)^3(a^4+1)}{8a^3}\right)$$

should have integer coordinates. But the X-component of $2P$ is an element of $\frac{1}{4}\mathbb{Z} - \frac{1}{4a^2}$, hence we would have $a=1$ which is excluded. Therefore P is of infinite order.

Let $(X,Y) \in E$ be a rational point, then this point yields d and m according to our transformations described above. In particular we obtain

$$d = -4(2a^5+2a^7+a^9+a^3(1+X)-Y)((a+a^3)(a^2+a^4+a^6+X)-Y) \times \frac{((1+a^2+a^4)(a^4+a^6+X)-aY)}{q^2(a^2-1)(a+a^3)^2X^3}.$$

Multiplying by a suitable square we may assume

$$\begin{aligned} d = {}& 4(a^2-1)X(2a^5+2a^7+a^9+a^3(1+X)-Y) \\ & \times ((a+a^3)(a^2+a^4+a^6+X)-Y)((1+a^2+a^4)(a^4+a^6+X)-aY). \end{aligned}$$

We want to show that for a given integer d_0 there are only finitely many integers Z such that $d = d_0Z^2$. Since d is not constant as a function on the elliptic curve E, we deduce that infinitely many d_0 exist and therefore also infinitely many pairs (d,m) exist, such that $\gcd(d,m)$ is square-free. Hence it is enough to prove that the curve $C \subset \mathbb{C}^3$ defined by

$$\begin{aligned} Y^2 = {}&(X+a^6+a^4)(X+a^6+a^4+a^2)(X+a^6+2a^4+2a^2+1) \\ d_0Z^2 = {}&4(a^2-1)X(2a^5+2a^7+a^9+a^3(1+X)-Y) \\ & \times ((a+a^3)(a^2+a^4+a^6+X)-Y)((1+a^2+a^4)(a^4+a^6+X)-aY) \end{aligned}$$

has at most finitely many rational points for fixed a and d_0. Let us expand the second equation defining C and replace Y^2 by $(X+a^6+a^4)(X+a^6+a^4+a^2)(X+a^6+2a^4+2a^2+1)$ and Y^3 by $Y(X+a^6+a^4)(X+a^6+a^4+a^2)(X+a^6+2a^4+2a^2+1)$. Then we have a linear equation in Y and solving this equation for Y we obtain $Y = P(X,Z)/Q(X)$, where P and Q are certain polynomials. Squaring this last equation and again replacing Y^2 by $(X+a^6+a^4)(X+a^6+a^4+a^2)(X+a^6+2a^4+2a^2+1)$ we obtain a polynomial equation in X and $Z' = Z^2$ with the parameters a and d_0. Moreover this polynomial equation is quadratic in Z' and under the assumption that (X,Y,Z) is a rational point the according discriminant has to be square, i.e. we obtain the Diophantine equation

$$\square = (a^2-1)X(a^4+a^6+X)(a^2+a^4+a^6+X)(1+2a^2+2a^4+a^6+X)R(X),$$

where $R(X)$ is a polynomial of degree 7 with parameters a and d_0. But this hyperelliptic equation has only finitely many rational solutions, i.e. we have finished the proof of Theorem 4.

Remark 4. Although we performed an intensive computer search we could not find geometric progressions of length 5. In particular we computed all pairs (d, m) corresponding to the points $T_i + kP$ with $k = 0, \dots, 10$ and $i = 0, \dots 3$, where $T_0 = \mathcal{O}$ is the point at infinity, for $1 \leq a \leq 10^3$ and $a \in \mathbb{Z}$. But, none of these pairs provides a geometric progression of length 5. For small $a \in \mathbb{Z}$, i.e. $a \leq 35$ we computed the Mordell-Weil group and considered for all points with relatively small height the pairs d, m but none of these yield a geometric progressions of length 5. In particular let $\{G_1, \dots, G_r\}$ be the generators of the Mordell-Weil group that are computed by SAGE, then we computed all points of the form $T + \sum_{i=1}^{r} a_i G_i$, such that $\sum_{i=1}^{r} a_i \leq 10$ and T is some torsion point.

6. Lucas Sequences

The basic tool for the proof of Theorem 5 is the ingenious theorem of Bilu, Hanrot and Voutier [2] on primitive prime divisors of Lucas sequences. Let us recall some basic facts about Lucas sequences, which will be needed in our proofs.

Let α, β be two algebraic integers, such that $\alpha + \beta$ and $\alpha\beta$ are non-zero co-prime integers, and α/β is not a root of unity. The sequence

$$u_n := \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

is called the Lucas sequence corresponding to the Lucas pair (α, β). Two Lucas pairs (α_1, β_1) and (α_2, β_2) are said to be equivalent if $\alpha_1/\alpha_2 = \beta_1/\beta_2 = \pm 1$ In fact u_n is a binary recurrence sequence defined by $u_n = Au_{n-1} + Bu_{n-2}$, $u_0 := 0$, $u_1 := 1$, where $A := \alpha + \beta$ and $B := -\alpha\beta$.

For convenience of the reader we state a shortened version of the above mentioned deep theorem on primitive divisors of Lucas sequences.

Proposition 2 (Bilu, Hanrot, Voutier [2])**.** *Consider the Lucas sequence*

$$u_n := \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

We have

- *For $n > 30$ u_n always has a primitive prime divisor.*
- *For $n = 5$ and $7 \leq n \leq 30$ u_n always has a primitive prime divisor, except when (up to equivalence) $(\alpha, \beta) = \Big((a + \sqrt{b})/2, (a - \sqrt{b})/2\Big)$ with the pairs (a, b) listed in Table 3.*

Remark 5. In [2] the authors give a complete answer also for the cases $n = 2, 3, 4, 6$, but we have not used these cases in our proof, so we decided not to quote the result in its precise form.

Proof of Theorem 5. If u_k, u_l, u_m form a geometric progression for pairwise distinct indices u, k, m, then we have

$$u_k u_m = u_l^2. \tag{12}$$

Let us write $n := \max\{k, l, m\}$ and without loss of generality suppose that $k < m$. Clearly, $u_0 = 0$ cannot appear in a non-trivial geometric progression, so we have

Table 3. Exceptional pairs (a, b)

n	(a,b)
5	$(1,5),(1,-7),(2,-40),(1,-11),(1,-15),(12,-76),(12,-1364)$
7	$(1,-7),(1,-19)$
8	$(2,-24),(1,-7)$
10	$(2,-8),(5,-3),(5,-47)$
12	$(1,5),(1,-7),(1,-11),(2,-56),(1,-15),(1,-19)$
13	$(1,-7)$
18	$(1,-7)$
30	$(1,-7)$

$n \geq 3$. Now, if u_n has a primitive prime divisor, this contradicts (12). This means, that u_n has no primitive prime divisor. If $n = 5$ or $n \geq 7$ we have to check the exceptional cases listed in Table 3. By a short Magma [3] program we checked equation (12) for all exceptional cases listed in Table 3. But, we obtained only solutions that yield trivial geometric progression.

It remains to consider the cases $n = 3, 4, 6$. In these cases we use a direct computation. The first 7 terms of a Lucas sequence can be expressed as

$$u_0 = 0, \quad u_1 = 1, \quad u_2 = A, \quad u_3 = A^2 + B, \quad u_4 := A^3 + 2AB,$$
$$u_5 = A^4 + 3A^2B + B^2, \quad u_6 = A^5 + 4A^3B + 3AB^2.$$

Let $n = 6$. We have to consider the equations

$$u_k u_m = u_6^2 \qquad u_k u_6 = u_l^2 \tag{13}$$

Let p be an odd prime with $p^k \| A$ then we get $p \nmid u_1, u_3, u_5$ and $p^k \| u_2, u_4, u_6$. Similarly if $2^k \| A$ we have $2 \nmid u_1, u_3, u_5$, $2^k \| u_2, u_6$ and $2^{k+1} \| u_4$. Therefore either $k, l, m \in \{2, 4, 6\}$ or $A = \pm 1, \pm 2$

In the case $A \neq \pm 1, \pm 2$ we have to consider the three equations

$$\begin{aligned} A \cdot A(A^2 + 2B) &= A^2(A^4 + 4A^2B + 3B^2)^2 \\ A \cdot A(A^4 + 4A^2B + 3B^2) &= A^2(A^2 + 2B)^2 \\ A(A^2 + 2B)A(A^4 + 4A^2B + 3B^2) &= A^2 \end{aligned} \tag{14}$$

Let us note that $A^4 + 4A^2B + 3B^2 = (A^2 + 2B)^2 - B^2 = (A^2 + B)(A^2 + 3B)$. Then the first equation of (14) yields

$$(A^2 + 2B) = (A^2 + B)^2(A^2 + 3B)^2,$$

but $|A^2 + 2B| < \max\{|A^2 + B|, |A^2 + 3B|\}$ provided that $B \neq 0$ and therefore the right hand side is larger then the left hand side, i.e. the equation has no solution. The second equation of (14) yields

$$(A^2 + 2B)^2 - B^2 = (A^2 + 2B)^2$$

an obvious contradiction for $B \neq 0$. The last equation of (14) can be written as

$$(A^2 + 2B)(A^2 + B)(A^2 + 3B) = 1$$

which is possible only if $A = 1$ and $B = 0$.

Now we have to handle the case $n = 6$, $A = \pm 1, \pm 2$. However, for fixed values of A the two equations in (13) are polynomial equations in one variable. The integer solutions of such equations can be easily computed, even by hand, but since we have many equations to consider, as (k, m) and (k, l) vary we used a Magma [3] program to check all cases. However, no solution was found that yields a non-trivial geometric progression.

The case $n = 4$ is handled similarly. We have to consider the equations

$$u_k u_m = u_4^2 \qquad u_k u_4 = u_l^2$$

The p-adic considerations made in the case $n = 6$ show that the case $n = 4$ is not possible unless $A = \pm 1, \pm 2$. The case $n = 4$, $A = \pm 1, \pm 2$ is treated the same way as above. But, in this case we find the non-trivial geometric progressions $(u_1, u_2, u_4) = (u_3, u_2, u_4) = (1, -2, 4)$ for $A = -2$ and $B = -3$.

The easiest case, namely $n = 3$, remains. We are left to consider the equations

$$A = (A^2 + B)^2, \quad A^2 + B = A^2, \quad A(A^2 + B) = 1. \tag{15}$$

The last two equations have solutions only if $B = 0$, which is excluded, therefore we are left to the first equation of (15). Since A and B are coprime we deduce that $A = \pm 1$ and since the right-hand side is positive we have $A = 1$. Therefore we have $1 = (1 + B)^2$ and therefore $B = 0$, a contradiction. □

References

[1] A. Bérczes, L. Hajdu, and A. Pethő. Arithmetic progressions in the solution sets of norm form equations. *Rocky Mountain J. Math.*, 40(2):383–395, 2010.

[2] Y. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[4] A. Bremner, J. Silverman, and N. Tzanakis. Integral points in arithmetic progressions on $y^2 = x(x^2 - n^2)$. *Journal of Number Theory*, 80(2):187–208, 2000.

[5] A. Dujella, A. Pethő, and P. Tadić. On arithmetic progressions on Pellian equations. *Acta Math. Hungar.*, 120(1-2):29–38, 2008.

[6] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[7] A. W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[8] A. Pethő and V. Ziegler. Arithmetic progressions on Pell equations. *J. Number Theory*, 128(6):1389–1409, 2008.

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

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

V. Ziegler
Institute for Analysis and
Computational Number Theory,
Graz University of Technology
Steyrergasse 30/IV,
A-8010 Graz, Austria
E-mail address: `ziegler@finanz.math.tugraz.at`