ARITHMETIC PROGRESSIONS ON PELL EQUATIONS

ATTILA PETHŐ AND VOLKER ZIEGLER

1. Introduction

In 1999 Bremner [1] considered arithmetic progressions on elliptic curves. Bremner constructed elliptic curves with arithmetic progressions of length 7, i.e. rational points (X, Y) whose X-coordinates are in arithmetic progression. In a following paper Bremner, Silverman and Tzanakis [2] 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, provided $n \geq 1$.

Contrary to the results of Bremner, Silverman and Tzanakis [2], Campbell [3] found an infinite family of elliptic curves with 9 integral points in arithmetic progressions. This result was improved by Ulas [12], where an infinite family was found with an arithmetic progression consisting of 12 integral points.

In this paper we consider curves of genus 0, in particular hyperbola, with integral arithmetic progressions. Inspired by the results of Bremner [1], Bremner, Silverman and Tzanakis [2], Campbell [3] and Ulas [12] the aim of this paper is to prove the following theorems.

Theorem 1. *Let $0 < d \in \mathbb{Z}$, d not a square and $0 \neq m \in \mathbb{Z}$. If there are three solutions $(X_1, Y_1), (X_2, Y_2)$ and (X_3, Y_3) to the Pell equation*

$$X^2 - dY^2 = m \tag{1}$$

such that $X_1 < X_2 < X_3$ respectively $Y_1 < Y_2 < Y_3$ form a non-trivial arithmetic progression, i.e. $X_2 \neq 0$ respectively $Y_2 \neq 0$, then $\max_i\{|X_i|\} \leq \max\{17.015|m|^2\sqrt{d}, 12.911|m|\sqrt{d^3}\}$ respectively $\max_i\{|Y_i|\} \leq 21.055\frac{|m|^2}{\sqrt{d}}$. For more details see table 1.

Table 1. Upper bounds for $\max_{i=1,2,3}\{|X_i|\}$ resp. $\max_{i=1,2,3}\{|Y_i|\}$.

X	$\lvert m\rvert/d$	$\lvert m\rvert$	$B := \max\{\lvert X_i\rvert\}$	Y	$\lvert m\rvert/d$	$\lvert m\rvert$	$B := \max\{\lvert Y_i\rvert\}$
	$\lvert m\rvert/d \geq 1$	$\lvert m\rvert \geq 1$	$B \leq 17.015\lvert m\rvert^2\sqrt{d}$		$\lvert m\rvert/d \geq 1$	$\lvert m\rvert \geq 1$	$B \leq 21.055\frac{\lvert m\rvert^2}{\sqrt{d}}$
	$\lvert m\rvert/d \geq 1$	$\lvert m\rvert \geq 2$	$B \leq 15.368\lvert m\rvert^2\sqrt{d}$		$\lvert m\rvert/d \geq 1$	$\lvert m\rvert \geq 2$	$B \leq 18.047\frac{\lvert m\rvert^2}{\sqrt{d}}$
	$\lvert m\rvert/d < 1$	$\lvert m\rvert \geq 1$	$B \leq 12.911\lvert m\rvert\sqrt{d^3}$		$\lvert m\rvert/d < 1$	$\lvert m\rvert \geq 1$	$B \leq 20.217\frac{\lvert m\rvert^2}{\sqrt{d}}$
	$\lvert m\rvert/d < 1$	$\lvert m\rvert \geq 2$	$B \leq 12.696\lvert m\rvert\sqrt{d^3}$		$\lvert m\rvert/d < 1$	$\lvert m\rvert \geq 2$	$B \leq 18.047\frac{\lvert m\rvert^2}{\sqrt{d}}$

By Theorem 1 we deduce an upper bound for the length of an arithmetic progression.

Corollary 1. *Let $d, m \in \mathbb{Z}$ with $d > 0$ not a square and $m \neq 0$. An arithmetic progression on $X^2 - dY^2 = m$ has length at most $c(d, m)\tau_d(m)$. Where $\tau_d(\cdot)$ is following arithmetic function*

$$\tau_d(m) = \prod_{\substack{p^\alpha \| m \\ p \ \text{splits in} \ \mathbb{Q}(\sqrt{d})}} (\alpha + 1)$$

Date: May 20, 2006.

The second author gratefully acknowledges support from the Austrian Science Fund (FWF) under project Nr. P18079-N12.

and the product runs over all primes. Furthermore one can compute

$$c(d,m) = \begin{cases} \frac{2\log(|m|^3 d)+15.94}{\log d} + \frac{3}{2} & \text{if } d/|m| \geq 1, \\ \frac{2\log(|m|d^3)+14.83}{\log d} + \frac{3}{2} & \text{if } d/|m| < 1. \end{cases}$$

Since Theorem 1 we know that there are only finitely many non-trivial arithmetic progressions for fixed d, m. This leads to several questions: Are there for fixed d only finitely many m resp. for fixed m only finitely many d such that (1) admits non-trivial arithmetic progressions. In the second case the answer is yes (see Theorem 2).

Theorem 2. *Let $0 \neq m \in \mathbb{Z}$ be fixed. Then there are only finitely many $0 < d \in \mathbb{Z}$ such that there are three solutions $(X_1, Y_1), (X_2, Y_2)$ and (X_3, Y_3) to the Pell equation*

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

such that $X_1 < X_2 < X_3$ or $Y_1 < Y_2 < Y_3$ is an arithmetic progression, except the trivial cases $(Y_1, Y_2, Y_3) = (-y, 0, y)$, $(X_1, X_2, X_3) = (-x, 0, x)$. Moreover if a non-trivial arithmetic progression $X_1 < X_2 < X_3$ exists then we have $d \leq 3|m|$ if m is not a perfect square and $d \leq 9|m|$ otherwise. In the case of $Y_1 < Y_2 < Y_3$ we obtain $d \leq 9|m|^2$.

Note that in the second case of the theorem above, we do not get better estimates if we assume m is not a square. In the special case $m = \pm 1$ we obtain

Corollary 2. *Let $0 < d \in \mathbb{Z}$ be not a perfect square. Then there are no three solutions (X_1, Y_1), (X_2, Y_2) and (X_3, Y_3) to the Pell equation*

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

such that $X_1 < X_2 < X_3$ or $Y_1 < Y_2 < Y_3$ is an arithmetic progression, except the trivial case $(Y_1, Y_2, Y_3) = (-y, 0, y)$ and the progressions $(X_1, X_2, X_3) = (-3, -1, 1), (-1, 1, 3)$ in the case of $m = 1$ and $d = 2$ or $d = 8$.

Let us reverse the questions stated above. Given an arithmetic progression $Y_1 < Y_2 < Y_3$ does there exist a hyperbola such that Y_1, Y_2, Y_3 are solutions? The answer is given by

Theorem 3. *For every arithmetic progression $Y_1 < Y_2 < Y_3$ 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 and Y_3 are the Y-components of solutions to $X^2 - dY^2 = m$.*

The next problem we consider is, whether there are $d, m \in \mathbb{Z}$ with $0 < d$ not a square and $m \neq 0$, such that there exists a certain arithmetic progression of length four on $X^2 - dY^2 = m$. In particular we are interested in the arithmetic progression $1 < 3 < 5 < 7$ respectively $0 < 1 < 2 < 3$.

Theorem 4. *There are $d, m \in \mathbb{Z}$ such that $d > 0$ is not a perfect square and $m \neq 0$, such that $1, 3, 5$ and 7 are the Y-components of solutions to $X^2 - dY^2 = m$. We may choose $(d, m) = (570570, 4406791)$. In particular there exist arithmetic progressions of length 8.*

On the other hand there are no $d, m \in \mathbb{Z}$ with d not a perfect square, such that $0, 1, 2$ and 3 are the Y-components of solutions to $X^2 - dY^2 = m$.

We also prove a converse to Theorem 3:

Theorem 5. *Let $Y_1 < Y_2 < Y_3 < Y_4 < Y_5$ be an arithmetic progression such that $|Y_i| \neq |Y_j|$ for any $i \neq j$. 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 $X^2 - dY^2 = m$.*

In the next section (section 2) we prove two simple auxiliary results that will help us to prove our theorems. In the following sections 3, 4, 5 and 6 we prove the theorems stated above. The proof of Theorems 1-3 are elementary (but technical). However the proof of Theorem 4 needs some basic knowledge on elliptic curves and the proof of Theorem 5 needs some basic knowledge on algebraic geometry, i.e. we apply a theorem of Faltings [5] (Mordell's conjecture). In Section 7 we consider the dual question to Theorems 3, 4 and 5 and show that the situation is much more simple for the X-component. In the last section we discuss some open questions that arise by studying this paper.

2. Auxiliary Results

Since with $X_1 < X_2 < X_3$ also $-X_3 < -X_2 < -X_1$ respectively with $Y_1 < Y_2 < Y_3$ also $-Y_3 < -Y_2 < -Y_1$ is an arithmetic progression, we assume $X_2 > 0$ respectively $Y_2 > 0$ in the following.

We call the number $X + Y\sqrt{d}$ a solution to (1) if $(X, Y) \in \mathbb{Z}^2$ is a solution to (1). We start with the following lemma:

Lemma 1. *Let $\alpha_1 = X_1 + Y_1\sqrt{d}, \alpha_2 = X_2 + Y_2\sqrt{d}$ and $\alpha_3 = X_3 + Y_3\sqrt{d}$ be solutions to (1) such that $\alpha_1 + \alpha_3 = 2\alpha_2$. Then $\alpha_1 = \alpha_2 = \alpha_3$.*

In other words not both $X_1 < X_2 < X_3$ and $Y_1 < Y_2 < Y_3$ can be arithmetic progressions.

Proof. Since 1 and $\sqrt{d}$ are linear independent over $\mathbb{Q}$ we deduce, that both (X_1, X_2, X_3) and (Y_1, Y_2, Y_3) form arithmetic progressions. Therefore we write $X_1 = x - k_1, X_2 = x, X_3 = x + k_1$ and similarly $Y_1 = y - k_2, Y_2 = y, Y_3 = y + k_2$. Subtracting $X_2^2 - dY_2^2 = m$ two times from $X_1^2 + X_3^2 - d(Y_1^2 + Y_3^2) = 2m$ yields $k_1^2 - dk_2^2 = 0$. But the Diophantine equation $X^2 - dY^2 = 0$ has no solution except $(X, Y) = (0, 0)$, if d is not a perfect square, hence $X_1 = X_2 = X_3$ and $Y_1 = Y_2 = Y_3$.

The lemma also follows from Bézout's theorem, i.e. a quadratic curve with a line has at most two intersections. □

Let us assume $X_1 < X_2 < X_3$ is an arithmetic progression, i.e. $\frac{X_1+X_3}{2} = X_2$, on the hyperbola (1) then the corresponding Y-components cannot fulfill the equation $\frac{Y_1+Y_3}{2} = Y_2$. Therefore we have $Y_2 - \frac{Y_1+Y_3}{2} = \Delta_Y$ with $\Delta_Y \in \frac{1}{2}\mathbb{Z}$ and $\Delta_Y \neq 0$. Similarly we define $\Delta_X := X_2 - \frac{X_1+X_3}{2} \in \frac{1}{2}\mathbb{Z}$, if $Y_1 < Y_2 < Y_3$ is an arithmetic progression. Because of Lemma 1 we have $\Delta_X \neq 0$. In any case we have the lower bound $|\Delta| \geq 1/2$, where $\Delta = \Delta_X, \Delta_Y$ depending on which component is an arithmetic progression. The next lemma yields an upper bound for $|\Delta|$.

Lemma 2. *Let $X_1 < X_2 < X_3$ be an arithmetic progression on the hyperbola (1) such that no $Y_i = 0$ for $i = 1, 2, 3$, then*

$$|\Delta_Y| \leq \frac{3|m|}{2d}.$$

If one (or more) $Y_i = 0$ then we have

$$|\Delta_Y| \leq \begin{cases} \frac{3|m|}{2d} & \text{if } \frac{|m|}{d} \geq 1, \\ \frac{3\sqrt{|m|}}{2\sqrt{d}} & \text{if } \frac{|m|}{d} < 1. \end{cases}$$

Now let $Y_1 < Y_2 < Y_3$ be an arithmetic progression. Then

$$|\Delta_X| \leq \frac{3|m|}{2\sqrt{d}},$$

if no $Y_i = 0$ (i.e. $Y_1 \neq 0$) and

$$|\Delta_X| \leq \frac{\sqrt{|m|}}{2} + \frac{|m|}{\sqrt{d}}$$

otherwise.

Proof. Let us consider the case where $X_1 < X_2 < X_3$ is an arithmetic progression. Then

$$(X_i - \sqrt{d}Y_i)(X_i + \sqrt{d}Y_i) = m,\ i = 1, 2, 3.$$

Let us choose Y_i such that $|X_i - \sqrt{d}Y_i| \leq |X_i + \sqrt{d}Y_i|$ i.e. both X_i and Y_i are non-negative or non-positive integers. We obtain

$$X_i - \sqrt{d}Y_i = \frac{m}{X_i + \sqrt{d}Y_i}, i = 1, 2, 3,$$

which implies

$$\left|X_i - \sqrt{d}Y_i\right| \leq \frac{|m|}{\sqrt{d}|Y_i|} \leq \frac{|m|}{\sqrt{d}}, \tag{3}$$

if $Y_i \neq 0$. If $Y_i = 0$ we obviously have

$$\left|X_i - \sqrt{d}Y_i\right| = \sqrt{|m|}. \tag{4}$$

Further, we obtain

$$\frac{X_1 + X_3}{2} - \sqrt{d}\frac{Y_1 + Y_3}{2} = \frac{m}{2}\left(\frac{1}{X_1 + \sqrt{d}Y_1} + \frac{1}{X_3 + \sqrt{d}Y_3}\right),$$

which together with $X_2 = \frac{X_1+X_3}{2}$ implies

$$\sqrt{d}\left(Y_2 - \frac{Y_1 + Y_3}{2}\right) = \sqrt{d}\Delta_Y = \frac{m}{2}\left(\frac{1}{X_1 + \sqrt{d}Y_1} + \frac{1}{X_3 + \sqrt{d}Y_3} - \frac{2}{X_2 + \sqrt{d}Y_2}\right). \tag{5}$$

Similar we obtain in the case of $Y_1 < Y_2 < Y_3$ is an arithmetic progression

$$\left(X_2 - \frac{X_1 + X_3}{2}\right) = \Delta_X = \frac{m}{2}\left(\frac{1}{X_1 + \sqrt{d}Y_1} + \frac{1}{X_3 + \sqrt{d}Y_3} - \frac{2}{X_2 + \sqrt{d}Y_2}\right). \tag{6}$$

We remark that only $X_1 + \sqrt{d}Y_1$ and $X_3 + \sqrt{d}Y_3$ resp. $X_1 + \sqrt{d}Y_1$ and $-X_2 - \sqrt{d}Y_2$ can have the same sign. Using the estimation (3) if $Y_i \neq 0$ and the identity (4) otherwise we obtain the lemma if we also distinguish between the cases $\frac{|m|}{d} \geq 1$ and $\frac{|m|}{d} < 1$. □

3. Proof of Theorem 1

We have four different cases. We distinguish whether $X_1 < X_2 < X_3$ or $Y_1 < Y_2 < Y_3$ is an arithmetic progression and whether $|X_1| < |X_2|$ or $|X_2| < |X_1|$ respectively $|Y_1| < |Y_2|$ or $|Y_2| < |Y_1|$. Because the idea for all four cases is the same, we give the details only for the case $X_1 < X_2 < X_3$ and $|X_1| < |X_2|$ and sketch only the proofs of the other cases.

We claim that $\min\{|X_1|, |X_2|\} > \frac{3|m|}{\sqrt{d}}$ is impossible. This is easy to see if one estimates from above the right side of (5) by $\frac{3|m|}{2\min\{|X_1|,|X_2|\}}$ and reminds that $|\Delta_Y| \geq 1/2$. Similarly we obtain $\min\{|Y_1|, |Y_2|\} \leq \frac{3|m|}{\sqrt{d}}$ (in the case of $X_1 < X_2 < X_3$ is an arithmetic progression) by utilizing inequality (6).

Now we claim that $\min\{|Y_1|, |Y_2|\} \leq \frac{3|m|}{d} + \frac{1}{6}$. We know $X^2 - dY^2 = m$, hence

$$Y^2 \leq \frac{X^2 + |m|}{d} \leq \frac{9|m|^2}{d^2} + \frac{|m|}{d} \leq \left(\frac{3|m|}{d} + \frac{1}{6}\right)^2.$$

Similarly we obtain $\min\{|X_1|, |X_2|\} \leq 3|m| + \frac{1}{6}$ in the other case.

Let us consider the equation $X_2^2 - dY_2^2 = m$ and let us insert the expressions for X_2 and Y_2. We obtain

$$\left(\frac{X_1 + X_3}{2}\right)^2 - d\left(\frac{Y_1 + Y_3}{2} + \Delta_Y\right)^2 = m.$$

Using the other two equations this implies

$$X_1X_3 = dY_1Y_3 + 2d\Delta_Y(Y_1 + Y_3 + \Delta_Y) + m.$$

On the other hand

$$(X_1X_3)^2 = (m + dY_1^2)(m + dY_3^2).$$

Inserting the expression for X_1X_3 we get $a_2Y_3^2 + a_1Y_3 + a_0 = 0$, where

$$\begin{aligned}
a_2 =& 4d\Delta^2 + 4dY_1\Delta - m,\\
a_1 =& 8d\Delta^3 + 4\Delta m + 4dY_1^2\Delta + 12dY_1\Delta^2 + 2Y_1m\\
=& a_2(Y_1 + 2\Delta) + 3m(Y_1 + 2\Delta),\\
a_0 =& -Y_1^2m + 4d\Delta^4 + 4\Delta^2m + 4Y_1\Delta m + 8dY_1\Delta^3 + 4dY_1^2\Delta^2\\
=& \frac{a_2^2}{4d} + \frac{3a_2m}{2d} + \frac{5m^2}{4d} - mY_1^2,
\end{aligned}$$

and we write Δ for Δ_Y. In the case of $|X_2| < |X_1|$ we use the equation $X_1^2 - dY_1^2 = m$ and insert $Y_1 = 2Y_2 - Y_3 + 2\Delta$ respectively $X_1 = 2X_2 - X_3$. Similar as above we obtain $a_2Y_3^2 + a_1Y_3 + a_0 = 0$ with

$$\begin{aligned}
a_2 =& m + 2dY_2\Delta - d\Delta^2,\\
a_1 =& -2mY_2 + 2m\Delta - 4dY_2^2\Delta + 6dY_2\Delta^2 - 2d\Delta^3\\
=& a_2(-2Y_2 + 2\Delta),\\
a_0 =& mY_2^2 - 4mY_2\Delta + 2m\Delta^2 - 4dY_2^2\Delta^2 + 4dY_2\Delta^3 - d\Delta^4\\
=& -\frac{a_2^2}{d} + \frac{m^2}{d} + mY_2^2.
\end{aligned}$$

In the case of $Y_1 < Y_2 < Y_3$ forms an arithmetic progression we obtain

$$\begin{aligned}
a_2 =& m + 4X_1\Delta + 4\Delta^2,\\
a_1 =& -2mX_1 - 4m\Delta + 4X_1^2\Delta + 12X_1\Delta^2 + 8\Delta^3\\
=& a_2(X_1 + 2\Delta) + 3m(X_1 + 2\Delta),\\
a_0 =& mX_1^2 - 4mX_1\Delta - 4m\Delta^2 + 4X_1^2\Delta^2 + 8X_1\Delta^3 + 4\Delta^4\\
=& \frac{a_2^2}{4} + \frac{3a_2m}{2} + \frac{5m^2}{4} - mX_1^2,
\end{aligned}$$

provided $|Y_1| \le |Y_2|$ respectively

$$\begin{aligned}
a_2 =& m - 2X_2\Delta + \Delta^2,\\
a_1 =& -2mX_2 + 2m\Delta + 4X_2^2\Delta - 6X_2\Delta^2 + 2\Delta^3\\
=& a_2(-2X_2 + 2\Delta),\\
a_0 =& mX_2^2 - 4mX_2\Delta + 2m\Delta^2 + 4X_2^2\Delta^2 - 4X_2\Delta^3 + \Delta^4\\
=& a_2^2 - m^2 + mX_2^2,
\end{aligned}$$

in the case of $|Y_2| < |Y_1|$.

We have $a_2 = 0$ in the cases discussed above if and only if $m = 4d\Delta(Y_1 + \Delta), -2dY_2\Delta + d\Delta^2, -4X_1\Delta - 4\Delta^2$ and $2X_2\Delta - \Delta^2$ respectively. Then

$$\begin{aligned}
X_1^2 = m + dY_1^2 = d(Y_1 + 2\Delta)^2,\\
X_2^2 = m + dY_2^2 = d(Y_2 - \Delta)^2,\\
dY_1^2 = X_1^2 - m = (X_1 + 2\Delta)^2 \text{ and}\\
dY_2^2 = X_2^2 - m = (X_2 - \Delta)^2
\end{aligned}$$

respectively. These relations are absurd, as d is not a square, thus $a_2 \neq 0$.

Now we solve the quadratic equation $a_2Y_3^2 + a_1Y_3 + a_0 = 0$ and distinguish whether $m \ge 1$ or $m \ge 2$ and whether $m/d \ge 1$ or $m/d < 1$. Taking care of all these different cases we can estimate now Y_3 by using the formula $Y_3 = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2a_0}}{2a_2}$. The estimates for the worst cases are given in table 2.

TABLE 2. Upper bounds for $|Y_3|$ resp. $|X_3|$.

Y	$\lvert m\rvert/d$	$\lvert m\rvert$	$B := \lvert Y_3\rvert$	X	$\lvert m\rvert/d$	$\lvert m\rvert$	$B := \lvert X_3\rvert$
	$\lvert m\rvert/d \ge 1$	$\lvert m\rvert \ge 1$	$B \le 17\lvert m\rvert^2$		$\lvert m\rvert/d \ge 1$	$\lvert m\rvert \ge 1$	$B \le 21.032\lvert m\rvert^2$
	$\lvert m\rvert/d \ge 1$	$\lvert m\rvert \ge 2$	$B \le 15.366\lvert m\rvert^2$		$\lvert m\rvert/d \ge 1$	$\lvert m\rvert \ge 2$	$B \le 18.044\lvert m\rvert^2$
	$\lvert m\rvert/d < 1$	$\lvert m\rvert \ge 1$	$B \le 12.906\lvert m\rvert d$		$\lvert m\rvert/d < 1$	$\lvert m\rvert \ge 1$	$B \le 20.192\lvert m\rvert^2$
	$\lvert m\rvert/d < 1$	$\lvert m\rvert \ge 2$	$B \le 12.694\lvert m\rvert d$		$\lvert m\rvert/d < 1$	$\lvert m\rvert \ge 2$	$B \le 18.044\lvert m\rvert^2$

We use once more the equation $X^2 - dY^2 = m$ to obtain Theorem 1. □

The idea for the proof of Corollary 1 is to compute the number of solutions to $X^2 - dY^2 = m$ with $X \leq M$ resp. $Y \leq M$. Therefore we have to discuss first properties of the solutions to $X^2 - dY^2 = m$. We prove following lemma:

Lemma 3. *Let M be given. Then the equation $X^2 - dY^2 = m$ has at most $c(\epsilon, m, M)\tau_d(m)$ solutions with $|X| \leq M$ respectively $|Y| \leq M$, with*

$$c(\epsilon, m, M) = \left\lfloor \frac{\log\left(\frac{M\epsilon\sqrt{2}}{(\epsilon-2)\sqrt{|m|}}\right)}{\log \epsilon} + \frac{1}{2} \right\rfloor + \left\lfloor \frac{\log\left(\frac{M\epsilon^2}{(\epsilon^2-1)\sqrt{|m|}}\right)}{\log \epsilon} \right\rfloor + 1$$

and $\epsilon > 1$ is the fundamental solution to $X^2 - dY^2 = 1$.

We start with some general remarks on Diophantine equation (1). If $\alpha = u + v\sqrt{d}$ is a solution to (1) and $\epsilon = x + y\sqrt{d}$ is a solution to

$$X^2 - dY^2 = 1, \tag{7}$$

then also $\alpha\epsilon = (ux + vyd) + (uy + vx)\sqrt{d}$ is a solution to (1). We say that two solutions $\alpha_1 = u_1 + v_1\sqrt{d}$ and $\alpha_2 = u_2 + v_2\sqrt{d}$ belong to the same class of solutions if there exists a solution $\epsilon = x + y\sqrt{d}$ to (7), such that $\alpha_1 = \epsilon\alpha_2$. Let $\alpha_1, \ldots, \alpha_l$ be representatives for each class (note that there are only finitely many classes, see [10]). Then we obtain by the formula $\alpha\epsilon^k$, where $0 \leq k \in \mathbb{Z}$, ϵ is a fundamental solution to (7) and α runs through the representative system $\alpha_1, \ldots, \alpha_l$, a set of solutions $\mathcal{L}^-$ which can be extended to the set of all solutions by adjoining $(\pm x, \pm y)$ to $\mathcal{L}^-$ for all $(x, y) \in \mathcal{L}^-$.

Let $\alpha = u + v\sqrt{d}$ be a solution to (1) in a certain class C, such that v is non-negative and least possible, then we call α the fundamental solution of the class C (if u is not uniquely determined then choose u positive). Note that every solution can be written uniquely as $\alpha\epsilon^k$ where α is a fundamental solution and $k \in \mathbb{Z}$. We call $|k|$ the exponent of the solution.

We use following notation: Let $\alpha = x + y\sqrt{d}$ be a solution to (1), then we call $\bar{\alpha} := x - y\sqrt{d}$ its conjugate solution. Warning: Do not disturb this notation with the complex conjugation!

A theorem due to Nagell states (see [10] or [9]).

Theorem 6 (Nagell)**.** *Let $\alpha = u + v\sqrt{d}$ be a fundamental solution to (2) and $\epsilon = x + y\sqrt{d}$ a fundamental solution to (7) with $x, y > 0$. Then*

$$\begin{aligned} 0 < |u| &\leq \sqrt{\frac{1}{2}(x+1)m}, \\ 0 \leq v &\leq \frac{y}{\sqrt{2(x+1)}}\sqrt{m}, \end{aligned} \quad \text{if } m > 0 \text{ and } \quad \begin{aligned} 0 \leq |u| &\leq \sqrt{-\frac{1}{2}(x-1)m}, \\ 0 < v &\leq \frac{y}{\sqrt{2(x-1)}}\sqrt{-m}, \end{aligned} \quad \text{if } m < 0.$$

As a corollary we prove following lemma:

Lemma 4. *Let α be a fundamental solution and ϵ the fundamental solution to (7). Then*

$$\sqrt{\frac{|m|}{2\epsilon}} \leq |\alpha| \leq \sqrt{2\epsilon|m|}. \tag{8}$$

Proof. We write $\alpha = u + v\sqrt{d}$ and $\epsilon = x + y\sqrt{d}$. Since $\alpha = u + v\sqrt{d} \leq u + |v|\sqrt{d}$ we may assume $u, v \geq 0$. By Nagell's Theorem 6 we have

$$u \leq \sqrt{\frac{1}{2}(x+1)|m|}, \qquad v \leq \frac{y}{\sqrt{2(x-1)}}\sqrt{|m|}.$$

Obviously $\epsilon = x + y\sqrt{d} \geq x + 1$. Since $x^2 - dy^2 = 1$ we have $\frac{y^2}{x-1} = \frac{x+1}{d} \leq \frac{\epsilon}{d}$. These estimations yield

$$\alpha = u + v\sqrt{d} \leq \sqrt{\frac{1}{2}\epsilon|m|} + \sqrt{\frac{\epsilon|m|}{2d}}\sqrt{d} = \sqrt{2\epsilon|m|}.$$

For the proof of the lower bound we may assume $u, -v \geq 0$, since $\alpha = u + v\sqrt{d} > u - |v|\sqrt{d}$. The upper bound yields $|\bar{\alpha}| \leq \sqrt{2\epsilon|m|}$. Multiplication by $|\alpha|$ yields $|m| \leq \sqrt{2\epsilon|m|}|\alpha|$, hence the lower bound for $|\alpha|$. □

Let us count first the possibilities for the exponents. Let $\alpha\epsilon^k$ be a solution, where α is a fundamental solution and $k \in \mathbb{Z}$. Since $\alpha\bar{\alpha} = m$ and $\alpha\epsilon^k = \overline{\bar{\alpha}\epsilon^{-k}}$, we may assume $|\alpha| \leq \sqrt{|m|}$. We claim

$$|\bar{\alpha}\epsilon^{-k}| \leq |\frac{2}{\epsilon}\alpha\epsilon^k| \quad \text{if } k \geq 1,$$

and

$$|\alpha\epsilon^k| \leq |\epsilon^{-2}\bar{\alpha}\epsilon^{-k}| \quad \text{if } k \leq -1.$$

These statements are easily verified using Lemma 4 and the relation $\alpha\bar{\alpha} = m$. Now we consider for $k \geq 1$

$$M \geq \max\{|\alpha\epsilon^k + \bar{\alpha}\epsilon^{-k}|, |\alpha\epsilon^k - \bar{\alpha}\epsilon^{-k}|\} \geq \left|\alpha\epsilon^k\left(1 - \frac{2}{\epsilon}\right)\right|$$

and for $k \leq -1$

$$M \geq \max\{|\alpha\epsilon^k + \bar{\alpha}\epsilon^{-k}|, |\alpha\epsilon^k - \bar{\alpha}\epsilon^{-k}|\} \geq |\bar{\alpha}\epsilon^{-k}(1 - \epsilon^{-2})|.$$

Solving these inequalities with respect to k an integer and taking into account the possibility of $k = 0$. We obtain that there are at most

$$c(\epsilon, m, M) := \left\lfloor \frac{\log\left(\frac{M\epsilon\sqrt{2}}{(\epsilon-2)\sqrt{|m|}}\right)}{\log\epsilon} + \frac{1}{2} \right\rfloor + \left\lfloor \frac{\log\left(\frac{M\epsilon^2}{(\epsilon^2-1)\sqrt{|m|}}\right)}{\log\epsilon} \right\rfloor + 1$$

possible k's.

Next we want to count the possible classes of solutions. Therefore we write

$$m = \pm\prod_{i=1}^{l} p_i^{\alpha_i} \prod_{i=1}^{m} q_i^{\beta_i} \prod_{i=1}^{n} r_i^{\gamma_i}$$

such that the prime ideals $(p_i) = \mathfrak{p}_i\bar{\mathfrak{p}}_i$ split, the $(q_i) = \mathfrak{q}_i^2$ ramify and the $(r_i) = \mathfrak{r}_i$ are inert. The following relations are well known or are easy to see:

$$\begin{aligned} \mathfrak{p}_i^N|(\alpha) &\Leftrightarrow \bar{\mathfrak{p}}_i^N|(\bar{\alpha}), \\ \mathfrak{q}_i^N|(\alpha) &\Leftrightarrow \mathfrak{q}_i^N|(\bar{\alpha}), \\ \mathfrak{r}_i^N|(\alpha) &\Leftrightarrow \mathfrak{r}_i^N|(\bar{\alpha}), \end{aligned}$$

where N is an integer. This means that the exponents of the primes $\mathfrak{r}_i$ and $\mathfrak{q}_i$ in (α) respectively $(\bar{\alpha})$ are fixed. Only the exponents of the $\mathfrak{p}_i$ can vary. This means that we have $\prod_{i=1}^{l}(\alpha_i + 1)$ possibilities for α, which proves Lemma 3.

Now using $\epsilon > \sqrt{d}$ Corollary 1 follows from Lemma 3, Theorem 1 and some estimations.

4. Proof of Theorem 2

The proof of Theorem 2 is rather easy, if we use Lemma 2. If m is not a square then $Y = 0$ is impossible and we obtain $\Delta_Y \leq \frac{3|m|}{2d}$ respectively $\Delta_X \leq \frac{3|m|}{2\sqrt{d}}$. By Lemma 1 we know Δ_X and Δ_Y are non-zero and therefore their absolute value is at least $1/2$. This yields immediately the theorem in this case.

If m is a square then the case $Y = 0$ is possible. Let us consider first the case of $X_1 < X_2 < X_3$ is an arithmetic progression. Then by Lemma 2 we have $\Delta_Y \leq \frac{3\sqrt{m}}{2\sqrt{d}}$. The same argument as above yields Theorem 2 in this case.

Now we investigate the case of $Y_1 < Y_2 < Y_3$ is an arithmetic progression, $Y_1 = 0$ and $m = c^2$, with $c \in \mathbb{Z}$. This yields $X_1 = c, Y_3 = 2Y_2$ and

$$\Delta_X = \frac{c}{2} + \overbrace{\frac{m}{2}\left(\frac{1}{X_3 + 2Y_2\sqrt{d}} - \frac{2}{X_2 + Y_2\sqrt{d}}\right)}^{\delta :=}.$$

Since $\Delta_X \in \frac{1}{2}\mathbb{Z}$ also $\delta \in \frac{1}{2}\mathbb{Z}$. Let us exclude the case $\delta = 0$. In this case we would obtain

$$2X_3 + 4Y_2\sqrt{d} = X_2 + Y_2\sqrt{d},$$

hence $4Y_2 = Y_2$, i.e. $Y_2 = 0$ which is a contradiction. On the other hand we get

$$|\delta| \le \frac{|m|}{2}\left(\frac{2}{\sqrt{d}} + \frac{1}{2\sqrt{d}}\right) = \frac{5|m|}{4\sqrt{d}}.$$

By a similar argument as above we obtain $d \le 6.25|m|^2 < 9|m|^2$.

Now we can prove Corollary 2. We only have to check for $d = 2, 3, 5, 6, 7, 8$ if there are any solutions with absolute value at most $12.911d^3$ that form an arithmetic progression. This can easily be done by a computer.

5. Proof of Theorem 3

Let $Y_1 = a, Y_2 = a + k, Y_3 = a + 2k$ with $a, k \in \mathbb{Z}$ be the given arithmetic progression. Since $d_0^2X^2 - (dd_0^2)Y^2 = md_0^2$ is equivalent to the equation $X^2 - dY^2 = m$ we may assume a, k are coprime. If there are $d, m \in \mathbb{Z}$ that fulfill Theorem 3 then the system

$$\begin{aligned} X_1^2 - da^2 &= m, \\ X_2^2 - d(a+k)^2 &= m, \\ X_3^2 - d(a+2k)^2 &= m, \end{aligned} \tag{9}$$

of Diophantine equations has a solution. But then also the system

$$X_2^2 - X_1^2 = dk(2a + k), \qquad X_3^2 - X_2^2 = dk(2a + 3k),$$

has the same solution and also the equation

$$\mathfrak{C}: \quad X_2^2(4a + 4k) = X_1^2(2a + 3k) + X_3^2(2a + k) \tag{10}$$

has this solution. It is not hard to see that this projective curve $\mathfrak{C}$ has genus 0 and can be parameterized by a line. The projective point $P = (1, 1, 1) \in \mathbb{P}^2$ lies on $\mathfrak{C}$ and let $Q = (p, q, 0)$ lie on the line $\mathfrak{L} : X_3 = 0$. By Bézout's theorem the straight line from P to Q has only two intersections (with multiplicities) with $\mathfrak{C}$. One intersection is P and let the other intersection be R. Because the genus of $\mathfrak{C}$ is 0 the point R must be rational if Q was rational. Let us compute R in dependance of Q to obtain all rational points.

Of course d and m depend on the representative of the projective solution (X_1, X_2, X_3) but since $d(\lambda X_1, \lambda X_2, \lambda X_3) = \lambda^2 d(X_1, X_2, X_3)$ and similarly $m(\lambda X_1, \lambda X_2, \lambda X_3) = \lambda^2 m(X_1, X_2, X_3)$. We can derive for each rational projective solution to (10) exactly one pair (d, m) such that $\gcd(d, m)$ is square-free. Therefore every pair (d, m) that fulfills the properties stated in Theorem 3 corresponds to exactly one rational point on the projective curve $\mathfrak{C}$.

The line from P to Q is given by the equation

$$qX_1 - pX_2 + (p - q)X_3 = 0.$$

Inserting this in equation (10) yields

$$\begin{aligned} (p^2(2a + 3k) - 4q^2(a + k))X_2^2 + (p(q - p)(2a + 3k))2X_2X_3 \\ + (4q^2(a + k) + p(p - 2q)(2a + 3k))X_3^2 = 0. \end{aligned}$$

This equation has two solutions for X_2. The first solution is $X_2 = X_3$ and the second solution is

$$X_2 = \frac{2a(p^2 - 2pq + 2q^2) + k(3p^2 - 6pq + 4q^2)}{p^2(2a + 3k) - 4q^2(a + k)} X_3.$$

The first solution yields $X_1 = X_2 = X_3$, which implies $|Y_1| = |Y_2| = |Y_3|$. But this has been excluded. In the other case we get

$$X_1 = -\frac{2a(p^2 - 4pq + 2q^2) + k(3p^2 - 8pq + 4q^2)}{p^2(2a + 3k) - 4q^2(a + k)} X_3.$$

Let $X_3 = k(p^2(2a + 3k) - 4q^2(a + k))$, then we obtain by system (9)

$$\begin{aligned} d =& 4kp(p - q)q((2a + 3k)p - 4(a + k)q), \\ m =& k(p - 2q)((2a + 3k)p - 2kq)(kp - 2(a + k)q)((2a + 3k)p - 2(a + k)q). \end{aligned}$$

Let us keep p fixed, non-zero and choose q such that q is square-free and

$$\gcd(q, 2) = \gcd(q, p) = \gcd(q, a) = \gcd(q, k) = \gcd(q, 2a + 3k) = 1.$$

Let us note that for such q's d is not a perfect square. Moreover, also $\gcd(q, m) = 1$. Note that there are infinitely many q's with the properties stated above, hence we can construct infinitely many pairs (d, m) that satisfy the conditions of Theorem 3. The condition $d > 0$ is fulfilled whenever we choose $p > 0$ and q large enough.

6. Proof of Theorem 5 and 4

The first part of the proof of Theorem 4 is rather easy. One has to check that $1, 3, 5, 7$ are part of the solutions of the Pell equations given in Theorem 4. In this section we want to show how to find a pair (d, m) that fulfills the conditions of Theorem 4 or to prove that there does not exists such a pair. Similar as in the proof of Theorem 3 we are led to projective curves lying in $\mathbb{P}^3$ respectively $\mathbb{P}^4$ (Theorem 5). In the case of Theorem 4 we will get an elliptic curve for which we will find some rational points. One of these rational points will yield a pair (d, m) such that d is positive and square-free. In the case of Theorem 5 the curve will have genus 5 and will therefore have only finitely many rational points. Therefore we obtain at most finitely many pairs (d, m).

Let us start with the proof of Theorem 5. As mentioned in the section above we may assume that a and k are relative prime. Similar as in the proof of Theorem 3 we obtain from

$$\begin{aligned} X_1^2 - da^2 &= m, & X_2^2 - d(a + k)^2 &= m, \\ X_3^2 - d(a + 2k)^2 &= m, & X_4^2 - d(a + 3k)^2 &= m, \\ X_5^2 - d(a + 4k)^2 &= m, \end{aligned} \tag{11}$$

the system

$$\begin{aligned} X_2^2 - X_1^2 &= dk(2a + k), & X_3^2 - X_2^2 &= dk(2a + 3k), \\ X_4^2 - X_3^2 &= dk(2a + 5k), & X_5^2 - X_4^2 &= dk(2a + 7k) \end{aligned} \tag{12}$$

respectively

$$\begin{aligned} X_2^2(4a + 4k) &= X_1^2(2a + 3k) + X_3^2(2a + k), \\ X_3^2(4a + 8k) &= X_2^2(2a + 5k) + X_4^2(2a + 3k), \\ X_4^2(4a + 12k) &= X_3^2(2a + 7k) + X_5^2(2a + 5k). \end{aligned} \tag{13}$$

which defines a curve X in the projective space $\mathbb{P}^4$. By the conditions of Theorem 5 we have to exclude the cases $a = -k, -2k, -3k, k/2, 3k/2, 5k/2, 7k/2$, i.e. none of the coefficients in (13) is zero.

Lemma 5. *Let $a_{i,j}$ be non-zero integers, and let the curve X be defined by*

$$\begin{aligned} X_1^2 a_{1,1} + X_2^2 a_{1,2} + X_3^2 a_{1,3} &= 0, \\ X_2^2 a_{2,1} + X_3^2 a_{2,2} + X_4^2 a_{2,3} &= 0, \\ X_3^2 a_{3,1} + X_4^2 a_{3,2} + X_5^2 a_{3,3} &= 0. \end{aligned} \tag{14}$$

Let

$$F_1 = a_{2,2}a_{3,2} - a_{2,3}a_{3,1},$$
$$F_2 = a_{1,2}a_{2,2} - a_{1,3}a_{2,1},$$
$$F_3 = a_{2,2}a_{3,2}a_{1,2} - a_{2,3}a_{1,2}a_{3,1} - a_{3,2}a_{1,3}a_{2,1}.$$

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

Proof. We use Hurwitz's formula (see [6, Corollary IV.2.4] or any other book on algebraic geometry) in order to prove Lemma 5. Let X be the curve defined by (14) and Y the curve given by (14) where the last equation is replaced by $X_5 = 0$. Let $f : X \to Y$ be the morphism, given by

$$(X_1, X_2, X_3, X_4, X_5) \mapsto (X_1, X_2, X_3, X_4, 0).$$

We see that a point $P = (X_1, X_2, X_3, X_4, 0) \in Y$ has two distinct points as preimage, if and only if X_5 is not zero. Otherwise P has only one point as preimage and is therefore ramified with ramification index $e_P = 2$. Let p_1 be the number of ramification points. Then we obtain

$$2g_X - 2 = 2(2g_Y - 2) + p_1.$$

We apply this reduction also to the curves $Y \subseteq \mathbb{P}_3$ and $Z \subseteq \mathbb{P}_3$, where Y is given by

$$\begin{aligned} X_1^2a_{1,1} + X_2^2a_{1,2} + X_3^2a_{1,3} = 0,\\ X_2^2a_{2,1} + X_3^2a_{2,2} + X_4^2a_{2,3} = 0, \end{aligned} \tag{15}$$

and Z is given by

$$X_1^2a_{1,1} + X_2^2a_{1,2} + X_3^2a_{1,3} = 0 \text{ and } X_4 = 0.$$

Note that the curve Y in this paragraph is the same as in the paragraph above just imbedded into $\mathbb{P}_3$ where $\mathbb{P}_3 \subset \mathbb{P}_4$ and $P = (X_1, X_2, X_3, X_4, X_5) \in \mathbb{P}_3$ if and only if $X_5 = 0$. Obviously the curve Z has genus 0. Let now $f : Y \to Z$ be the morphism given by $(X_1, X_2, X_3, X_4) \mapsto (X_1, X_2, X_3, 0)$. In this case P is ramified if and only if $X_4 = 0$. Let p_2 be the number of points on Y that are ramified. By Hurwitz's formula we obtain

$$2g_Y - 2 = 2(0 - 2) + p_2,$$

hence $g_X = p_2 + p_1/2 - 3$. In order to prove the lemma we have to compute p_1 and p_2.

Let us compute first p_1. Note that if $X_5 = 0$ then $X_4 \neq 0$, since otherwise $X_3 = X_2 = X_1 = 0 = X_4 = X_5$, which does not yield an element of $\mathbb{P}^4$. We obtain

$$\frac{X_3^2}{X_4^2} = -\frac{a_{3,2}}{a_{3,1}}.$$

Since $a_{3,2}$ and $a_{3,1}$ are not zero we have for fixed X_4 exactly two possibilities to choose X_3. Now we insert this relation into the second line of (14) and obtain

$$\frac{X_2^2}{X_4^2} = \frac{a_{2,2}a_{3,2} - a_{2,3}a_{3,1}}{a_{2,1}a_{3,1}} = \frac{F_1}{a_{2,1}a_{3,1}}.$$

Therefore we have exactly two possibilities for X_2 if $F_1 \neq 0$ for fixed X_4. Next we compute by the formulae above and the first equation of (14)

$$\frac{X_1^2}{X_4^2} = \frac{-a_{2,2}a_{3,2}a_{1,2} + a_{2,3}a_{1,2}a_{3,1} + a_{3,2}a_{1,3}a_{2,1}}{a_{2,1}a_{3,1}a_{1,1}} = -\frac{F_3}{a_{2,1}a_{3,1}a_{1,1}}.$$

Since this formula there are exactly two possibilities for X_1 if $F_3 \neq 0$ for fixed X_4. Now we have $p_1 = 8$, if $F_1F_3 \neq 0$.

Similar we obtain in the case of (15) that if $X_4 = 0$ there are exactly two possibilities for X_2 if X_3 is fixed. There are exactly two possibilities for X_1 if $F_2 \neq 0$. Therefore $p_2 = 4$, if $F_1 \neq 0$.

Sticking together these results yields the lemma. □

Corollary 3. *The curve defined by* (13) *under the assumption $a \neq -k, -2k, -3k, k/2, 3k/2, 5k/2, 7k/2$ has genus $g = 5$.*

Proof. We have only to show that $F_1F_2F_3 \neq 0$. Some computations show

$$\begin{aligned} F_1 =& 3(2a+5k)^2 \neq 0,\\ F_2 =& 3(2a+3k)^3 \neq 0,\\ F_3 =& 8(a+2k)(2a+3k)(2a+5k) \neq 0. \end{aligned}$$

□

Because of Falting's theorem [5] (Mordell's conjecture) the curve given by (13) has at most finitely many rational solutions, hence there are only finitely many pairs (d, m), which satisfy the conditions of Theorem 5 and therefore we have proved this theorem.

The proof of Lemma 5 shows that to find the examples given in Theorem 4 one has to deal with curves of genus 1, i.e. elliptic curves. First we want to transform the curve X given by

$$\begin{aligned} X_2^2(4a+4k) &= X_1^2(2a+3k) + X_3^2(2a+k),\\ X_3^2(4a+8k) &= X_2^2(2a+5k) + X_4^2(2a+3k), \end{aligned} \tag{16}$$

into a plane curve. Similar as in Section 5 we project X onto the plane $X_4 = 0$ from the point $P = (1, 1, 1, 1) \in X$. The line from P to $Q = (x, y, z, 0)$ is given by the system

$$\begin{aligned} zX_2 - yX_3 + (y-z)X_4 &= 0,\\ zX_1 - xX_3 + (x-z)X_4 &= 0. \end{aligned}$$

If we solve the system

$$\begin{aligned} X_3^2(4a+8k) - X_2^2(2a+5k) - X_4^2(2a+3k) &= 0,\\ zX_2 - yX_3 + (y-z)X_4 &= 0,\\ zX_1 - xX_3 + (x-z)X_4 &= 0, \end{aligned} \tag{17}$$

we obtain

$$\begin{aligned} X_1 =& \frac{k(-10xy+5y^2+16xz-8z^2) + a(-4xy+2y^2+8xz-4z^2)}{(2a+5k)y^2 - 4(a+2k)z^2} X_4,\\ X_2 =& \frac{-(2a+5k)y^2 + 8(a+2k)yz - 4(a+2k)z^2}{(2a+5k)y^2 - 4(a+2k)z^2} X_4,\\ X_3 =& \frac{(2a+5k)y^2 - 2(2a+5k)yz + 4(a+2k)z^2}{(2a+5k)y^2 - 4(a+2k)z^2} X_4. \end{aligned} \tag{18}$$

Since we are working with projective coordinates we may choose

$$\begin{aligned} X_1 =& k(-10xy+5y^2+16xz-8z^2) + a(-4xy+2y^2+8xz-4z^2),\\ X_2 =& -(2a+5k)y^2 + 8(a+2k)yz - 4(a+2k)z^2,\\ X_3 =& (2a+5k)y^2 - 2(2a+5k)yz + 4(a+2k)z^2,\\ X_4 =& (2a+5k)y^2 - 4(a+2k)z^2. \end{aligned}$$

Note that $X_4 = 0$ would yield $a + 2k$ and $2a + 5k$ are both squares, which is a contradiction if $a = 1$ and $k = 2$ respectively $a = 0$ and $k = 1$. If we insert the expressions for X_1, X_2, X_3 and X_4 into the first equation of (16) we obtain

$$\begin{aligned} &4(2a+3k)((2a+5k)y - 4(a+2k)z)\times\\ &\qquad (xy(x-y)(2a+5k) + 4xz(z-x)(a+2k) + 3yz(y-z)(2a+3k)) = 0. \end{aligned} \tag{19}$$

The first factor $2a+3k$ of (19) cannot be zero because of our assumption $a \neq \frac{3}{2}k$. Also the second factor $(2a+5k)y - 4(a+2k)z$ is not zero, since otherwise

$$d = \frac{4(y-x)((2a+5k)y - 4(a+2k)z)((2a+5k)xy - 4(a+2k)(x+y)z + 4(a+2k)z^2)}{k(2a+k)} = 0$$

which is a contradiction. Now let us insert the special values for a and k. Then we obtain from (19)

$$3x^2y - 3xy^2 + 5xz^2 - 5x^2z + 6y^2z - 6yz^2 = 0, \qquad (a = 1, k = 2), \tag{20}$$

$$5x^2y - 5xy^2 + 8xz^2 - 8x^2z + 9y^2z - 9yz^2 = 0, \qquad (a = 0, k = 1). \tag{21}$$

Using Hoeij's algorithm (see [7]) we transform these elliptic curves into Weierstrass normal form, with the substitutions

$$\begin{aligned} x &:= 3(2\xi^2 + 6\xi\zeta + 6\eta\zeta - 108\zeta^2), \\ y &:= (-6\xi + 36\zeta - \eta)(-\xi - 9\zeta), \\ z &:= (3\xi^2 - 243\zeta^2), \end{aligned}$$

in the case of $a = 1$, $k = 2$, respectively

$$\begin{aligned} x &:= 81\xi'^2 + 594\xi'\zeta' + 324\eta'\zeta' - 19647\zeta'^2, \\ y &:= (-3\xi' - 59\zeta')(-27\xi' - 3\eta' + 333\zeta'), \\ z &:= 45\xi'^2 + 150\xi'\zeta' - 14455\zeta'^2, \end{aligned}$$

in the case of $a = 0$, $k = 1$. With these relations we are led to

$$\begin{aligned} 0 =& 54(\xi + \eta + 9\zeta)(\xi^2 - 81\zeta^2)(\xi^3 - \eta^2\zeta - 63\xi\zeta^2 + 162\zeta^3), \\ 0 =& 180(3\xi' - 49\zeta')(3\xi' + 59\zeta')(3(\xi' + \eta') + 59\zeta')(27\xi'^3 - 27\eta'^2\zeta' - 8001\xi'\zeta'^2 + 48026\zeta'^3). \end{aligned}$$

If $\xi + \eta + 9\zeta = 0$ or $\xi^2 - 81\zeta^2 = 0$, then also $d = 0$ in the first case. Similarly if $(3\xi' - 49\zeta')(3\xi' + 59\zeta')(3(\xi' + \eta') + 59\zeta') = 0$, then also $d = 0$. Indeed, if we compute d as a function in ξ, η and ζ, respectively ξ', η' and ζ' we obtain

$$\begin{aligned} d =& -72\eta(\xi + 9\zeta)(\xi + \eta + 9\zeta)(\xi^2 - 81\zeta^2) \\ & \times (9\xi^3 - 9(2\eta - 27\zeta)\zeta(\eta + 27\zeta) - \xi^2(\eta + 117\zeta) - 9\xi\zeta(4\eta + 117\zeta)), \\ d =& -300\eta'(3\xi' - 49\zeta')(3\xi' + 59\zeta')^2(3(\xi' + \eta') + 59\zeta') \\ & \times (621\xi'^3 - 27\xi'^2(\eta' + 371\zeta') - 9\xi'\zeta'(226\eta' + 30529\zeta') - \zeta'(972\eta'^2 + 29559\eta'\zeta' - 3194437\zeta'^2)). \end{aligned}$$

Therefore we are reduced to consider the elliptic curves

$$\eta^2\zeta = \xi^3 - 63\xi\zeta^2 + 162\zeta^3, \tag{22}$$

$$\xi'^2\zeta' = \xi'^3 - \frac{889}{3}\xi'\zeta'^2 + \frac{48026}{27}\zeta'^3. \tag{23}$$

A computation in PARI [11] shows that the elliptic curve (22) is a minimal integral model of an elliptic curve (see [8, Section X.1]). On the other hand the elliptic curve (23) can be transformed into its minimal integral model by the transformation

$$\xi' = 4\xi + \frac{\zeta}{3}, \qquad \eta' = 8\eta + 4\xi + 4\zeta, \qquad \zeta' = \zeta.$$

So we have to consider

$$\eta^2\zeta = \xi^3 - 63\xi\zeta^2 + 162\zeta^3 \qquad (a = 1, k = 2), \tag{24}$$

$$\eta^2\zeta + \xi\eta\zeta + \eta\zeta^2 = \xi^3 - 19\xi\zeta^2 + 26\zeta^3 \qquad (a = 0, k = 1), \tag{25}$$

the minimal integral models of the elliptic curves (22) and (23). Further computations in PARI show that the torsion group of (24) is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ with generators $(\xi, \eta, \zeta) = (3, 0, 1)$ and $(6, 0, 1)$. The torsion group of (25) is isomorphic to $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with generators $(-2, 8, 1)$ and $(3, -2, 1)$. A look on Cremona's tables [4] shows that the curve (25) has rank 0 and the curve (24) has rank 1 and its free group is generated by $(-3, 18, 1)$. With this information we may compute all rational points of (25) and sufficient many rational points on (24).

If we go back all substitutions for all rational points on (25) we get all solutions for (16). But no solution yields a pair (d, m) that satisfies the conditions of Theorem 4. Therefore we have proved this theorem.

At the end of this section we want to show some examples of pairs (d, m) for which $1, 3, 5$ and 7 are the Y-components of solutions to the Pell equation $X^2 - dY^2 = m$. Let $T_1 = (3, 0, 1)$, $T_2 = (6, 0, 1)$ and $P = (-3, 18, 1)$, then $-2P = (7, 8, 1)$ yields the pair $(d, m) = (-105, 5434)$. This is almost an example for Theorem 4, but is also remarkable, since the corresponding Diophantine equation $X^2 + 105Y^2 = 5434$ has only finitely many solutions. The smallest example we have found is $T_2 - 3P = \left(-\frac{71}{9}, -\frac{350}{27}, 1\right)$, which yields $d = 570570$ and $m = 4406791$. The next example is $T_1 - 4P = \left(-\frac{369}{361}, -\frac{102960}{6859}, 1\right)$ which yields $d = 23946502294$ and $m = 374134995675$.

7. Dual Theorem

Theorems 3, 4 and 5 only take care on the case for which the Y-component forms an arithmetic progression. In this section we consider the dual case, when the X-component forms an arithmetic progression. It turns out that this time the situation is much more simple. We prove the following theorem.

Theorem 7. *Let $X_1 < X_2 < X_3$ be an arithmetic progression such that $|X_i| \neq |X_j|$ for any $i \neq j$. Then there are at most finitely many $d, m \in \mathbb{Z}$ such that X_1, X_2, X_3 are the X-components of solutions to $X^2 - dY^2 = m$.*

Proof. The proof of this theorem starts in the same way as the proof of the dual Theorems 3, 4 and 5. As in Section 6 we have

$$a^2 - dY_1^2 = m, \qquad (a+k)^2 - dY_2^2 = m,$$
$$(a+2k)^2 - dY_3^2 = m,$$

which implies the system

$$Y_2^2 - Y_1^2 = k(2a+k)/d, \qquad Y_3^2 - Y_2^2 = k(2a+3k)/d.$$

We may assume $Y_1, Y_2, Y_3 > 0$. If $k \neq -2a$ then $k(2a+k) \neq 0$. As $Y_1, Y_2 \in \mathbb{Z}$ the integer d has to divide the fixed integer $k(2a+k)$, i.e. there are finitely many possibilities for d. Keeping d fixed too, $Y_1 + Y_2$ is a positive integer divisor of $k(2a+k)/d$, i.e. it is bounded, thus there are only finitely many possibilities for Y_1 and Y_2. Hence there are only finitely many possibilities for m too. If $k = -2a$ then we apply the same consideration to the second equation. □

8. Open Questions

There are a lot of questions that arise reading this paper. In this section we want to discuss some of them.

- Is there an absolute constant C such that there is no Pell equation with arithmetic progression of length $\geq C$. Although Theorem 1 and Corollary 1 suggest that C depends on d and m, Theorem 5 indicates that only exceptional curves will have a certain arithmetic progression of length 5. So we guess that such a constant C exists.

- Can one find an arithmetic progression of length at least 5 such that $Y_i \neq -Y_j$ for $i \neq j$?

- Can one proof or disprove that there are d and m with $d > 0$ and not a perfect square such that $Y = 1, 3, 5, 7, 9$ is an arithmetic progression on the curve $X^2 - dY^2 = m$?

- We have shown that the elliptic curve which is linked with the arithmetic progression $1, 3, 5, 7$ has rank 1, hence has infinitely many rational solutions. Can one show that these solutions yield infinitely many pairs d, m which satisfy the conditions of Theorem 4? We conjecture the answer is yes!

- We have found an arithmetic progression of length 4 that lies on some curve $X^2 - dY^2 = m$ and we have found an arithmetic progression such that there does not exist such a curve. Arise both cases with the same probability or is one of these cases an exception? Are there

simple criteria for a and k such that the arithmetic progression $a, a+k, a+2k, a+3k$ lies on a hyperbola? Or is there a criteria for which the associated elliptic curve has rank ≥ 1?

References

[1] A. Bremner, On arithmetic progressions on elliptic curves, *Experimental Mathematics*, **8** (4):409–413, 1999.

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

[3] G. Campbell, A note on arithmetic progressions on elliptic curves, *J. Integer Sequences*, **6** (2003), Article 03.1.3, 5 pp. (electronic)

[4] J. E. Cremona, Elliptic curve data, available at `http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html`.

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

[6] R. Hartshorne, *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1977.

[7] M. van Hoeij, An algorithm for computing the Weierstrass normal form, In *Proceedings of the 1995 international symposium on symbolic and algebraic computation, ISSAC '95, Montreal, Canada, July 10–12, 1995*, pages 90–95, 1964.

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

[9] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, New York, 1998.

[10] T. Nagell, *Introduction to Number Theory*, Almqvist & Wiksell Boktryckerei, Stockholm, 1951.

[11] The PARI Group, Bordeaux, *PARI/GP, version* `2.1.5`, 2004. available from `http://pari.math.u-bordeaux.fr/`.

[12] M. Ulas, A note on arithmetic progressions on quartic elliptic curves, *J. Integer Sequences*, **8** (2005), Article 05.3.1, 5 pp. (electronic).

A. Pethő
Faculty of Informatics, University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: `pethoe@inf.unideb.hu`

V. Ziegler
Institute of Mathematics, University of Natural Resources and Applied Life Sciences
Gregor-Mendel-Strasse 33,
A-1180 Vienna, Austria
E-mail address: `ziegler@finanz.math.tugraz.at`