On arithmetic progressions on Pellian equations

Andrej Dujella, Attila Pethő and Petra Tadić

Abstract

We consider arithmetic progressions consisting of integers which are y-components of solutions of an equation of the form $x^2 - dy^2 = m$. We show that for almost all four-term arithmetic progressions such an equation exists. We construct a seven-term arithmetic progression with the given property, and also several five-term arithmetic progressions which satisfy two different equations of the given form. These results are obtained by studying the properties of a parametric family of elliptic curves.

1 Introduction

In [8] it was shown that for the four-term arithmetic progression $1, 3, 5, 7$ there exists Pellian equation $x^2 - dy^2 = m$, where d is not a square, such that $1, 3, 5, 7$ are y-components of the solutions of this equation. On the other hand, it was shown that for the arithmetic progressions $0, 1, 2, 3$ such an equation does not exist.

In this paper, we will show that the progression $0, 1, 2, 3$ (and its companion progression $-3, -2, -1, 0$) is unique with this property. Namely, for any other four-term arithmetic progression consisting of integers there exist infinitely many equations of the form $x^2 - dy^2 = m$, where d is not a square (if d is a square and $m = 0$, the problem is trivial) and $\gcd(d, m)$ is square-free (so that the equations are essentially distinct) for which the elements of the given progression form y-components of solutions.

0

The authors were supported by the Croatian-Hungarian bilateral project *Investigations in number theory and cryptography.*
The first and the third author were supported supported by the Ministry of Science, Education and Sports, Republic of Croatia, Grant 0037110.
The second author was supported partially by the Hungarian National Foundation for Scientific Research Grant Nos. T42985.

We will also construct longer arithmetic progressions with the same property, namely, progressions with five, six and seven elements.

2 Four-term arithmetic progressions

Let $Y_1 = a$, $Y_2 = a + k$, $Y_3 = a + 2k$, $Y_4 = a + 3k$, with $a, k \in \mathbb{Z}$, be the given four-term arithmetic progression. We may assume that $\gcd(a, k) = 1$ and $k > 0$. If there are $d, m \in \mathbb{Z}$ such that Y_1, Y_2, Y_3, Y_4 are solutions of the Diophantine equation $x^2 - dy^2 = m$, then the system

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

of Diophantine equations has a solution. This system defines the curve of genus 1. In [8, Section 6], it was shown that the with transformations

$$\begin{aligned} X_1 &= k(-10uv + 5v^2 + 16u - 8) + a(-4uv + 2v^2 + 8u - 4), \\ X_2 &= -(2a + 5k)v^2 + 8(a + 2k)v - 4(a + 2k), \\ X_3 &= (2a + 5k)v^2 - 2(2a + 5k)v + 4(a + 2k), \\ X_4 &= (2a + 5k)v^2 - 4(a + 2k) \end{aligned}$$

the above system leads to the cubic curve (in variables u and v):

$$uv(u - v)(2a + 5k) + 4u(1 - u)(a + 2k) + 3v(v - 1)(2a + 3k) = 0. \quad (1)$$

Each rational point on (1) induces a pair (d, m) by the formulas

$$d = \frac{4(v-u)((2a+5k)v - 4(a+2k))((2a+5k)uv - 4(a+2k)(u+v) + 4(a+2k))}{k(2a+k)}, \quad (2)$$

$$m = X_1^2 - da^2. \quad (3)$$

Finally, the substitutions

$$\begin{aligned} u &= (-28800xk^4 - 56640xk^3a - 41088xk^2a^2 - 340x^2k^2 - 13056xa^3k + 2xyk \\ &\quad - 336x^2ak - x^3 + 4xya - 1536xa^4 - 80x^2a^2)/ \\ &\quad (98304a^6 + 5529600k^6 + 1179648ka^5 + 5849088k^2a^4 + 15335424k^3a^3 + 17326080k^5a \\ &\quad + 22419456k^4a^2 + 36096xa^3k + 104832xk^2a^2 + 133824xk^3a + 192x^2ak + 180x^2k^2 \\ &\quad + 4608xa^4 + 63360xk^4 + 48x^2a^2 - 4xya - 10xyk - 1920k^3y - 256a^3y - 1536a^2ky - 3008ak^2y), \\ v &= (-x^2 - 160xk^2 - 144xak - 32a^2x)/ \\ &\quad (28800k^4 + 56640k^3a + 41088k^2a^2 + 180xk^2 - 10yk + 13056a^3k + 192xak - 4ya + 48a^2x + 1536a^4), \end{aligned}$$

(obtained by APECS [2] command `Gcub`) give the elliptic curve

$$y^2 = x^3 + (176a^2 + 672ak + 628k^2)x^2 + (9216a^4 + 72192a^3k + 209664a^2k^2 + 267648ak^3 + 126720k^4)x + 147456a^6 + 1769472a^5k + 8773632a^4k^2 + 23003136a^3k^3 + 33629184a^2k^4 + 25989120ak^5 + 8294400k^6. \quad (4)$$

The discriminant of (4) is

$$D = 150994944(5k + 2a)^2(2k + a)^2(k + 2a)^2(k + a)^2(2a + 3k)^4.$$

Hence, the curve is singular exactly when $(a, k) = (-5, 2), (-2, 1), (-1, 2), (-1, 1), (-3, 2)$. We give the images of the obvious rational points on (1):

$$[1, 0] \mapsto T_1 := [-160k^2 - 144ak - 32a^2, 0],$$

$$[0, 1] \mapsto T_2 := [-180k^2 - 192ak - 48a^2, 0],$$

$$[1, 1] \mapsto P := [-64a^2 - 256ak - 240k^2, 128a^3 + 640a^2k + 992ak^2 + 480k^3],$$

$$[3(2a+3k)/(2a+5k), 4(a+2k)/(2a+5k)] \mapsto T_3 := [-288k^2 - 336ak - 96a^2, 0].$$

It is clear that T_1, T_2, T_3 are torsion points on (4) of order 2, and we will show that, in general, the point P is of infinite order. Indeed, we have

$$3P = \Big[\frac{-16(2a + 3k)(2a + 5k)(3k^2 + 3ak + a^2)}{(a + 2k)^2}, \frac{-32a(2a + 3k)(2a + 5k)(a + 3k)(k + a)^2}{(a + 2k)^3}\Big],$$

$$4P = \Big[\frac{16(a + 3k)(-3k^3 + 3a^2k + a^3)}{k^2}, \frac{32(3k^2 + 6ak + 2a^2)(3k^2 + 3ak + a^2)(k^2 + 3ak + a^2)}{k^3}\Big].$$

If P has finite order then, by Lutz-Nagell theorem, the points $3P$ and $4P$ have integer coordinates. This implies $(a + 2k)|4$ and $k|4$, which gives only six (nonsingular) possible values for (a, k). Testing the coordinates of $5P$ for these six points, we find that only possible values are $(a, k) = (-3, 1)$ and $(a, k) = (0, 1)$. In both cases we obtain that the point P is of order 6. Using *mwrank* [3], we checked that for $(a, k) = (-3, 1), (0, 1)$ the rank of (4) is equal to 0. So, it is easy to compute all values for (d, m) in these cases, and it follows that we always have a trivial situation: $d = 0$ or $m = 0$.

If a, k are such that P has infinite order, then there exist infinitely many rational points $[x, y]$ on (4). Each such (non-torsion) point (assuming that (4) is nonsingular) induces the rational point $[u, v]$ on (1). By formulas (2) and (3) we obtain infinitely many (rational) pairs (d, m). Only finitely many rational points induce the pair (d, m) such that d is a square. Also, for given d_0, there are only finitely many rational points which induce the pairs (d, m) such that $d = d_0 \times$ square (both conditions lead to curves with genus > 1). Hence, after multiplying by a suitable square, we obtain infinitely many distinct pairs of integers (d, m), such that d is not a square and $\gcd(d, m)$ is square-free.

Let us consider the singular cases. They correspond to the sequences $-5,-3,-1,1;\ -2,-1,0,1;\ -1,1,3,5;\ -1,0,1,2;\ -3,-1,1,3$. Thus, it suffices to consider the three-term sequences $1,3,5$ and $0,1,2$. Both cases, of course, correspond to curves of genus 0, and it is easy to find infinitely many solutions, i.e. pairs (d,m):

$$1,3,5 \to d=\beta\alpha(\alpha+2\beta)(\alpha-\beta)/2,\ m=(-4\beta+\alpha)(-2\beta+\alpha)(\beta+2\alpha)(\beta+\alpha)/2,$$

$$0,1,2 \to d=4\beta\alpha(\alpha+3\beta)(\alpha-\beta),\ m=(\beta+\alpha)^2(\alpha-3\beta)^2.$$

Therefore, we proved

Proposition 1 *All four-term arithmetic progressions, except* $0,1,2,3$ *and* $-3,-2,-1,0$*, are y-components of infinitely many equations of the form* $x^2-dy^2=m$*, where* d *is not a square and* $\gcd(d,m)$ *is square-free.*

3 An elliptic surface

In the previous section, we have seen that the problem of determining the generic rank of the family of elliptic curves (4) is relevant to our problem. In this section, we will compute this rank.

We consider the elliptic curve $\mathcal{E}$ over $\mathbb{Q}(T)$:

$$\begin{aligned}\mathcal{E}:\ y^2 &= x^3+(176T^2+672T+628)x^2+(9216T^4+72192T^3+209664T^2+267648T+126720)x\\ &\quad +147456T^6+1769472T^5+8773632T^4+23003136T^3+33629184T^2+25989120T+8294400.\end{aligned}$$

The short Weierstrass form of $\mathcal{E}$ is

$$\mathcal{E}^*:\ y^2=x^3+A(T)x+B(T),$$

$$\begin{aligned}A(T) &= -5616T^4-33696T^3-73656T^2-69336T-24003,\\ B(T) &= 120960T^6+1088640T^5+4077216T^4+8133696T^3+9089496T^2+5363496T+1296702\\ &= 54(4T^2+12T+11)(20T^2+60T+37)(28T^2+84T+59).\end{aligned}$$

The discriminant of $\mathcal{E}$ is

$$D=150994944(T+1)^2(T+2)^2(2T+1)^2(2T+5)^2(2T+3)^4.$$

We will compute $\mathrm{rang}_{\mathbb{C}(T)}\mathcal{E}$ using Shioda's formula [9, Corollary 5.3]:

$$\mathrm{rang}_{\mathbb{C}(T)}\mathcal{E}=\mathrm{rang}\ NS(\mathcal{E},\mathbb{C})-2-\sum_s(m_s-1).$$

Here $NS(\mathcal{E},\mathbb{C})$ is the Néron-Severi group of $\mathcal{E}$ over $\mathbb{C}$, and the sum ranges over all singular fibres of the pencil $\mathcal{E}_t$, with m_s the number of irreducible components of the fibre. Since $\deg A = 4$ and $\deg B = 6$, we conclude that $\mathcal{E}$ is a rational surface. Hence, by [9, Lemma 10.1], we have rang $NS(\mathcal{E},\mathbb{C}) = 10$. The numbers m_s can be easily determined from Kodaira types of singular fibres (see [6, Section 4]), which are given in the following table (with the notation: $\alpha = \mathrm{ord}_{T=t}A(T)$, $\beta = \mathrm{ord}_{T=t}B(T)$, $\delta = \mathrm{ord}_{T=t}D(T)$):

	coefficients				
t	α	β	δ	Kodaira type	$m_s - 1$
-1	0	0	2	I_2	1
-2	0	0	2	I_2	1
$-\frac{1}{2}$	0	0	2	I_2	1
$-\frac{5}{2}$	0	0	2	I_2	1
$-\frac{3}{2}$	0	0	4	I_4	3

Therefore, we have

$$\mathrm{rang}_{\mathbb{C}(T)}\mathcal{E} = 10 - 2 - 4\cdot 1 - 1\cdot 3 = 1.$$

We claim that also $\mathrm{rang}_{\mathbb{Q}(T)}\mathcal{E} = 1$.

A result of Shioda [9, Theorem 10.10] suggests that the generators of $\mathcal{E}^*(\mathbb{Q}(T))$ can be found among the points of the form $[\alpha_1T^2+\beta_1T+\gamma_1, \alpha_2T^3+\beta_2T^2+\gamma_2T+\delta_2]$, $\alpha_i,\beta_i,\gamma_i,\delta_i \in \mathbb{Q}$. It is not hard to find all such points since the conditions on α_1 and γ_1 both lead to elliptic curves of rank $= 0$:

$$\alpha_1^3 - 5616\alpha_1 + 120960 = \square,$$

$$\gamma_1^3 - 24003\gamma_1 + 1296702 = \square.$$

Here we list all such points ($\pm$):

$$P := [-12T^2 - 72T - 69, 432T^3 + 2160T^2 + 3348T + 1620],$$

$$T_1 := [60T^2 + 180T + 111, 0],$$

$$T_2 := [24T^2 + 72T + 66, 0],$$

$$T_3 := [-84T^2 - 252T - 177, 0],$$

$$[-12T^2+39, -432T^3-1728T^2-2052T-648] = P+T_1,$$
$$[132T^2+288T+147, 1296T^3+3888T^2+3564T+972] = P+T_2,$$
$$[132T^2+504T+471, -1296T^3-7776T^2-15228T-9720] = P+T_3,$$
$$[60T^2+180T+147, -432T^2-1296T-972] = 2P,$$
$$[-84T^2-252T-69, -1296T^2-3888T-1620] = 2P+T_2,$$
$$[24T^2+72T+39, 324T^2+972T+648] = 2P+T_3$$

(the points P, T_1, T_2, T_3 correspond to the points with the same names in the previous section). This list suggests that the point P is the generator of $\mathcal{E}^*(\mathbb{Q}(T))$. In order to prove this statement it suffices to find a specialization $T \mapsto t$ for which the point $P(t)$ is the generator of $\mathcal{E}_t^*(\mathbb{Q})$.

We took the specialization $t = 1$, and both *mwrank* [3] and *APECS* [2] confirmed that the rank for this specialization

$$y^2 = x^3 - 206307x + 29170206$$

is equal to 1, with the generator $P(1) = [-153, 7560]$ (it is the curve 630E2 in Cremona's tables).

Proposition 2

$$\mathrm{rang}_{\mathbb{Q}(T)}\mathcal{E} = 1$$

4 Five-term arithmetic progression for two different equations

By [8, Theorem 5], for each five-term arithmetic progression (with different absolute values) 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 and such that these five numbers are y-components of solutions to $x^2 - dy^2 = m$. However, there are many five-term arithmetic progressions for which there exists at least one such pair (d, m). Moreover, we found several examples of five-term arithmetic progression for which two such pairs exist. They are listed in the following table:

a	k	equations	rank
-36	41	$x^2 - 87945y^2 = 160389376$ $x^2 + 615y^2 = 10506496$	3
-174	277	$x^2 - 1008280y^2 = 55523430369$ $x^2 + 831y^2 = 887286400$	4
-157	97	$x^2 - 208065y^2 = 848087296$ $x^2 - 81480y^2 = -111536711$	2
-453	218	$x^2 + 545y^2 = 111945834$ $x^2 - 2289y^2 = 59230600$	2
-471	362	$x^2 - 41811y^2 = 1406035150$ $x^2 - 1810y^2 = 143643591$	3
-337	144	$x^2 - 195y^2 = 3195201$ $x^2 + 51y^2 = 5796375$	2
-240	139	$x^2 - 27105y^2 = 4156531456$ $x^2 - 5560y^2 = 63864801$	3
-174	277	$x^2 - 1008280y^2 = 55523430369$ $x^2 + 831y^2 = 887286400$	4

Note that all above examples correspond to curves with rank > 1. This is not surprising since we checked that small multiples of P do not lead to five-term progressions with $\max(|a|, |k|) < 10^6$. Therefore we considered only curves with rank ≥ 2 (the rank and the generator are computed by *mwrank*) and, using a program written in PARI/GP [1], we checked whether the pairs (d, m) induced by small linear combinations of the generator satisfy the additional condition that the fifth term in the arithmetic progression satisfies the same Pellian equation.

Standard conjectures imply that (at least) 50% of curves in the studied family should have rank ≥ 2. Indeed, we have found many curves with rank $= 2$, but also some with the higher rank. The largest rank found in the range $\max(|a|, |k|) < 7000$ is 7, and it is obtained for $a/k = 619/6089$, $1015/5416$, $5864/1971$, $5945/5706$, $6029/1024$. These high-rank curves were found using

the sieving procedure similar to that used in [5]. The ranks were computed by *mwrank*. We give here some details only for the curve corresponding to $a/k = 619/6089$. Its minimal equation is

$$y^2 + xy = x^3 - x^2 - 33780966884736864x + 21245174187230790496095 20,$$

and seven independent points of infinite order are:

$$[40037861, 914409675367],$$
$$[71401901, 276578796412],$$
$$[28598884, 1087096726324],$$
$$[-62156636, -1995987404696],$$
$$[52021816, 712683760852],$$
$$[8142580, 1360140428200],$$
$$[304582516, 4482224368552].$$

Remark 1 The above examples also suggest (somewhat surprisingly) that long arithmetic progression appears almost with the same frequency in the equations $x^2 - dy^2 = m$ with d positive as with d negative. We give here some support to this observation (the similar arguments were used e.g. in [4]). Let us consider the case $(a, k) = (1, 2)$, treated in [8], where the corresponding elliptic curve is

$$y^2 = x^3 - 63x + 162.$$

Then, the points with

$$y > 0 \quad \text{and} \quad (-3 < x < 3 \quad \text{or} \quad x > 9),$$

$$y < 0 \quad \text{and} \quad (-9 < x < 1 \quad \text{or} \quad 6 < x < 21)$$

induce positive d (only finitely many of them will give $d =$ square). These conditions can be transformed in conditions for periods z, in parametrization by Weierstrass function $\wp(z)$. We have noted that for a point Q, the points $Q + T_1$, $Q + T_2$, $Q + T_3$, $-Q + P$ induce the same pair (d, m) as the point Q. So, in this particular case, it suffices to consider the points kP, $k > 0$. We obtain (e.g. using PARI) the periods $w_1 \approx 1.1656168$, $w_2 \approx 0.8570259$, and $w(P) := \delta + w_2/2 \cdot i \approx 0.22122488 + w_2/2 \cdot i$. The condition of positivity of d now becomes

$$k \cdot (\delta/w_1) \bmod 1/2 \in \langle \delta/w_1, 0.5 \rangle,$$

which is certainly satisfied for infinitely many k's (by Bohl-Sierpiński-Weyl theorem [7, pp. 24-27]); the smallest are: $k = 2, 4, 5, 7, 9, 10$ ($k = 2$ gives $d =$

square). Hence, the smallest solutions correspond to points $4P$, $5P$, $7P$. The first two appeared in [8]; the third gives $d = 603638196016911937479885$, $m = -475682124977406960077036$. But the same argument shows that there are infinitely many k's for which d is negative (the smallest are: $k = 3, 6, 8$).

5 A seven-term arithmetic progression

For $(a, k) = (-461, 166)$ we obtain the elliptic curve

$$y^2 = x^3 + 3283392x^2 + 1816362270720x + 233361525187805184$$

of rank 2, with generators $P_1 = [2025472, 5068743680]$, $P_2 = [-183168, 68382720]$. Using the point P_2, the above construction gives the equation

$$x^2 + 1245y^2 = 375701326$$

with the property that the seven numbers $a, a+k, a+2k, a+3k, a+4k, a+5k, a+6k$, i.e. $y = -461, -295, -129, 37, 203, 369, 535$ are solutions of this equation. This is the longest known arithmetic progression (with distinct absolute values) on curves of the form $x^2 - dy^2 = m$.

We also found several six-term arithmetic progressions:

a	k	equation	rank
-67	24	$x^2 + 10y^2 = 46046$	2
-318	83	$x^2 - 2905y^2 = 45752256$	3
-309	262	$x^2 - 587535y^2 = 14550679066$	3
-295	166	$x^2 + 1245y^2 = 375701326$	3
-271	158	$x^2 - 2370y^2 = 12731719$	2
-237	71	$x^2 - 1065y^2 = 4548544$	3

References

[1] C. Batut, D. Bernardi, H. Cohen and M. Olivier, GP/PARI, Université Bordeaux I, 1994.

[2] I. Connell, APECS, ftp://ftp.math.mcgill.ca/pub/apecs/

[3] J. E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, Cambridge, 1997.

[4] A. Dujella, An extension of an old problem of Diophantus and Euler. II, Fibonacci Quart. **40** (2002), 118–123.

[5] A. Dujella, An example of elliptic curve over $\mathbb{Q}$ with rank equal to 15. Proc. Japan Acad. Ser. A Math. Sci. **78** (2002) 109–111.

[6] R. Miranda, An overview of algebraic surfaces, in Algebraic Geometry (Ankara, 1995), Lecture Notes in Pure and Appl. Math. **193**, Dekker, New York, 1997, pp. 157–217.

[7] I. Niven, Diophantine Approximations, Wiley, New York, 1963.

[8] A. Pethő and V. Ziegler, Arithmetic progressions on Pell equations, preprint.

[9] T. Shioda, On the Mordell - Weil lattices, *Comment. Math. Univ. St. Pauli* **39** (1990), 211–240.

Andrej Dujella
Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb, Croatia
E-mail address: duje@math.hr

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

Petra Tadić
Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb, Croatia
E-mail address: petrat@math.hr