Canadian Mathematical Bulletin
doi:10.4153/CMB-2011-058-1

Rational Points in Arithmetic Progressions on $y^2 = x^n + k$

Maciej Ulas

Abstract. Let C be a hyperelliptic curve given by the equation $y^2 = f(x)$ for $f \in \mathbb{Z}[x]$ without multiple roots. We say that points $P_i = (x_i, y_i) \in C(\mathbb{Q})$ for $i = 1, 2, \ldots, m$ are in arithmetic progression if the numbers x_i for $i = 1, 2, \ldots, m$ are in arithmetic progression.

In this paper we show that there exists a polynomial $k \in \mathbb{Z}[t]$ with the property that on the elliptic curve $\mathcal{E}' : y^2 = x^3 + k(t)$ (defined over the field $\mathbb{Q}(t)$) we can find four points in arithmetic progression that are independent in the group of all $\mathbb{Q}(t)$-rational points on the curve $\mathcal{E}'$. In particular this result generalizes earlier results of Lee and Vélez. We also show that if $n \in \mathbb{N}$ is odd, then there are infinitely many k's with the property that on curves $y^2 = x^n + k$ there are four rational points in arithmetic progressions. In the case when n is even we can find infinitely many k's such that on curves $y^2 = x^n + k$ there are six rational points in arithmetic progression.

1 Introduction

Many problems in number theory are equivalent to the problem of solving certain equations or system of equations in integers or in rational numbers. Problems of this type are called *diophantine problems*. In the case when a problem has infinitely many solutions a natural question arises as to whether it is possible to show the existence of rational parametric solutions *i.e.,* solutions in polynomials or in rational functions. In general, problems of this kind are difficult, and we do not have any general theory that can even partially answer to such kind questions. For example, N. Elkies showed in [3] that the set of rational points on the surface $x^4 + y^4 + z^4 = t^4$ is dense in the set of all real points on this surface. However, we still do not known if this equation has non-trivial rational parametric solutions *i.e.,* a solution $x, y, z, t \in \mathbb{Z}[u] \setminus \{0\}$.

In this paper we meet with a problem of a similar type. Our question is related to the construction of integers k with the property that on the elliptic curve $E_k : y^2 = x^3 + k$ there are four rational points in arithmetic progression. Let us recall that for the curve $C : f(x, y) = 0$ defined over $\mathbb{Q}$, the rational points $P_i = (x_i, y_i)$ on C are in arithmetic progression if the numbers x_i for $i = 1, 2, \ldots, n$ are in arithmetic progression.

In connection with this problem Lee and Vélez showed in [5] that each rational point on the elliptic curve $E : y^2 = x^3 - 39x - 173$ gives an integer k with the property that on the elliptic curve $E_k : y^2 = x^3 + k$ there are four rational points in arithmetic progression. Due to the fact that the set $E(\mathbb{Q})$ of all rational points on E is generated by the point $(11, 27)$ of infinite order, we get infinitely many k's that satisfy the demanded conditions.

Received by the editors January 20, 2009; revised May 19, 2009.
Published electronically March 31, 2011.
AMS subject classification: **11G05**.
Keywords: arithmetic progressions, elliptic curves, rational points on hyperelliptic curves.

It should be noted that S. P. Mohanty stated the following conjecture.

Conjecture 1.1 (S. P. Mohanty [6]) *Let $k \in \mathbb{Z}$ and suppose that the rational points $P_i = (x_i, y_i)$ for $i = 1, \ldots, n$ are in arithmetic progression on the elliptic curve $y^2 = x^3 + k$. Then $n \leq 4$.*

We think that the above conjecture is not true. It is likely that in order to find a counterexample we should have plenty of k's for which we have four points in arithmetic progression on the curve $E_k : y^2 = x^3 + k$. Integers that satisfy this condition will be called *numbers of AP4 type*. It is clear that we are interested in the numbers k that are sixth power free *i.e.,* $p^6 \nmid k$ for any prime p.

The main aim of this paper is to construct parametric families of numbers of AP4 type. We should note that it is unclear how the method employed in [5] can be used in order to find families of this kind.

In Section 2 we show that each rational point on the surface

$$\mathcal{S} : (p^2 - 3q^2 + 3r^2 - s^2)(11p^2 - 18q^2 + 9r^2 - 2s^2) = 3(2p^2 - 5q^2 + 4r^2 - s^2)^2$$

gives us an integer k of AP4 type. In particular, we prove that there are infinitely many rational curves on $\mathcal{S}$. Using this result we deduce that the set of rational points on the surface $\mathcal{S}$ is dense in the set of all real points on $\mathcal{S}$ in the Euclidean topology. Moreover, using this result we show that there exists a polynomial $k \in \mathbb{Z}[t]$ with the property that on the corresponding elliptic curve $\mathcal{E}' : y^2 = x^3 + k(t)$ defined over $\mathbb{Q}(t)$ there are four $\mathbb{Q}(t)$-rational points, and these points are independent in the set $\mathcal{E}'(\mathbb{Q}(t))$.

In Section 3 we consider natural generalizations of the problem of constructing rational points in arithmetic progressions on hyperelliptic curves of the form $y^2 = x^n + k$.

In Section 4 we give a special sextic hypersurface that is connected with the problem of construction of integers k with the property that there are five points in arithmetic progression on the curve $y^3 = x^3 + k$.

2 Rational Points on $\mathcal{S}$

In this section we are interested in constructing numbers of AP4 type. Let $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Q}[a, b, c, d][x]$, and consider the curve $C : y^2 = f(x)$. Using now the change of coordinates

$$(x, y) = \Big(\frac{X - 3b}{9a}, \frac{Y}{27a}\Big) \text{ with inverse } \quad (X, Y) = (9ax + 3b, 27ay), \tag{2.1}$$

we can see that the curve C is birationally equivalent to the curve

$$E : Y^2 = X^3 + 27(3ac - b^2)X + 27(27a^2d - 9abc + 2b^3).$$

Let p, q, r, s be rational parameters, and let us put

$$\begin{aligned} a &= -(p^2 - 3q^2 + 3r^2 - s^2)/6, & b &= (2p^2 - 5q^2 + 4r^2 - s^2)/2, \\ c &= -(11p^2 - 18q^2 + 9r^2 - 2s^2)/6, & d &= p^2. \end{aligned} \tag{2.2}$$

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

For a, b, c, d defined in this way we have

$$f(0) = p^2, \quad f(1) = q^2, \quad f(2) = r^2, \quad f(3) = s^2.$$

We can see that in order to prove that the set of numbers of AP4 type contains the image of a certain polynomial we must consider the surface $3ac = b^2$, where a, b, c, d are defined as in (2.2).

Indeed, the points $(0, p), (1, q), (2, r), (3, s)$ are in arithmetic progression on the curve C, and due to the fact that our mapping from C to E given by (2.1) is affine, we deduce that the images of these points will be in arithmetic progression on the curve E. So we consider the surface in $\mathbb{P}^3$ given by the equation

$$\mathcal{S} : (p^2 - 3q^2 + 3r^2 - s^2)(11p^2 - 18q^2 + 9r^2 - 2s^2) = 3(2p^2 - 5q^2 + 4r^2 - s^2)^2.$$

It is easy to see that the surface S is singular and that the set $(\pm 1, \pm 1, \pm 1, \pm 1)$ is the set of all singular points (the signs + and − are independent of each other). The surface S has eight singular points. Let us recall that if $\mathbb{K}$ is a field, then by $\mathcal{S}(\mathbb{K})$ we denote the set of $\mathbb{K}$-rational points on $\mathcal{S}$.

We will show the following theorem.

Theorem 2.1 *The set of rational curves on the surface $\mathcal{S}$ is infinite. In particular, the set $\mathcal{S}(\mathbb{Q})$ is dense in the set of all real points $\mathcal{S}(\mathbb{R})$ in the Euclidean topology.*

Proof In order to show that on the surface $\mathcal{S}$ there are infinitely many rational curves defined over $\mathbb{Q}$, let us consider the following system of equations

$$\begin{cases} t(p^2 - 3q^2 + 3r^2 - s^2) = (2p^2 - 5q^2 + 4r^2 - s^2), \\ (11p^2 - 18q^2 + 9r^2 - 2s^2) = 3t(2p^2 - 5q^2 + 4r^2 - s^2), \end{cases}$$

or equivalently

$$\begin{cases} (3t^2 + 3t + 1)r^2 = -(3t^2 + 9t + 7)p^2 + 2(3t^2 + 6t + 4)q^2, \\ (3t^2 + 3t + 1)s^2 = -2(3t^2 + 12t + 13)p^2 + 9(t^2 + 3t + 3)q^2, \end{cases} \tag{2.3}$$

where t is indeterminate. It is easy to see that each rational solution of the system (2.3) leads us to the rational point on the surface $\mathcal{S}$. From a geometric point of view the system (2.3), as an intersection of two quadratic surfaces with rational point $(p, q, r, s) = (1, 1, 1, 1)$, is birationally equivalent to an elliptic curve defined over the field $\mathbb{Q}(t)$. Now we will show the construction of an appropriate mapping.

Using the standard substitution $(p, q, r) = (u + r, v + r, r)$ we can parametrize all rational solutions of the first equation of the system (2.3) in the following way:

$$\begin{cases} p = (3t^2 + 9t + 7)u^2 - 4(3t^2 + 6t + 4)uv + 2(3t^2 + 6t + 4)v^2, \\ q = (3t^2 + 9t + 7)u^2 - 2(3t^2 + 9t + 7)uv + 2(3t^2 + 6t + 4)v^2, \\ r = (3t^2 + 9t + 7)u^2 - 2(3t^2 + 9t + 4)v^2. \end{cases}$$

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

Without loss of generality we can assume that $u = 1$. We then substitute the parametrization we have obtained into the second equation in system (2.3) and we get the curve defined over the field $\mathbb{Q}(t)$ with the equation

$$\begin{aligned}\mathcal{C} : s^2 &= 4(3t^2+6t+4)^2v^4 + 8(3t^2+6t+4)(3t^2+15t+19)v^3\\ &\quad - 4(36t^4+243t^3+618t^2+702t+313)v^2\\ &\quad + 4(3t^2+9t+7)(3t^2+15t+19)v + (3t^2+9t+7)^2\end{aligned}$$

with $\mathbb{Q}(t)$-rational point $Q = (0, 3t^2+9t+7)$. Let us define the following quantities

$$\begin{aligned}C(t) &= (99t^4+756t^3+2253t^2+3114t+1709)/3,\\ D(t) &= 36(t^2+3t+3)(3t^2+12t+13)(3t^2+15t+19).\end{aligned}$$

Regarding Q as a point at infinity on the curve $\mathcal{C}$ and using the method described in [7, p. 77], we conclude that $\mathcal{C}$ is birationally equivalent over $\mathbb{Q}(t)$ to the elliptic curve with the Weierstrass equation

$$\mathcal{E} : Y^2 = X^3 + f(t^2+3t)X + g(t^2+3t),$$

where

$$\begin{aligned}f(u) &= -27(1053u^4+10152u^3+37530u^2+62616u+39673),\\ g(u) &= 54(9u^2+60u+85)(45u^2+192u+227)(63u^2+312u+397).\end{aligned}$$

The mapping $\varphi\colon \mathcal{E} \ni (X,Y) \mapsto (v,s) \in \mathcal{C}$ is given by

$$\begin{aligned}v &= \frac{2Y - 27D(t) - 6(3t^2+15t+19)(X-9C(t))}{12(X-9C(t))(3t^2+6t+4)},\\ s &= \frac{-(2Y-27D(t))^2 + 4(2X+9C(t))(X-9C(t))^2}{72(3t^2+6t+4)(X-9C(t))^2}.\end{aligned}$$

The discriminant of $\mathcal{E}$ is

$$\begin{aligned}&2^8 3^{16}(3+3t+t^2)^2(1+3t+3t^2)^2(4+6t+3t^2)^2\\ &\qquad\times (7+9t+3t^2)^2(13+12t+3t^2)^2(19+15t+3t^2)^2,\end{aligned}$$

so $\mathcal{E}_t$ is singular for the values $t \in \mathcal{A}$, where

$$\mathcal{A} = \left\{ \frac{-15\pm\sqrt{-3}}{6}, \frac{-9\pm\sqrt{-3}}{6}, \frac{-3\pm\sqrt{-3}}{6}, \frac{-6\pm\sqrt{-3}}{3}, \frac{-3\pm\sqrt{-3}}{3}, \frac{-3\pm\sqrt{-3}}{2} \right\}.$$

For $t \in \mathcal{A}$, the decomposition is of Kodaira classification type I_2. Let us note that $\mathcal{E}$ is a K3-surface. As we know, the Néron–Severi group over $\mathbb{C}$, denoted by $\mathrm{NS}(\mathcal{E}) = \mathrm{NS}(\mathcal{E},\mathbb{C})$, is a finitely generated $\mathbb{Z}$-module. From Shioda [8], we have

$$\operatorname{rank}\mathrm{NS}(\mathcal{E},\mathbb{C}) = \operatorname{rank}\mathcal{E}(\mathbb{C}(t)) + 2 + \sum_{\nu}(m_\nu - 1),$$

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

where the sum ranges over all fibers of the pencil $\mathcal{E}_t$, with m_ν the number of irreducible components of the fiber. Let us recall that if the fiber in the pencil $\mathcal{E}_t$ is smooth, then $m_\nu - 1 = 0$, thus the series on the right-hand side is finite. We have

$$\operatorname{rank} \mathrm{NS}(\mathcal{E}, \mathbb{C}) = \operatorname{rank} \mathcal{E}(\mathbb{C}(t)) + 2 + 6 \cdot 2 \cdot (2 - 1).$$

Since the rank of the Néron–Severi group of a K3-surface cannot exceed 20, the $\operatorname{rank} \mathcal{E}(\mathbb{C}(t)) \leq 6$. Although it would be interesting to know the rank of $\mathcal{E}(\mathbb{C}(t))$ precisely, we are interested instead in the rank of $\mathcal{E}(\mathbb{Q}(t))$. We will show that $\operatorname{rank} \mathcal{E}(\mathbb{Q}(t)) \geq 1$.

Let us note that the curve $\mathcal{E}$ has three points of order two

$$T_1 = (6(9(t^2 + 3t)^2 + 60(t^2 + 3t) + 85), 0),$$
$$T_2 = (3(45(t^2 + 3t)^2 + 192(t^2 + 3t) + 227), 0),$$
$$T_3 = (-3(63(t^2 + 3t)^2 + 312(t^2 + 3t) + 397), 0).$$

On the curve $\mathcal{E}$ we have also the point $P = (X_P, Y_P)$, where

$$X_P = -3(9t^4 + 108t^3 + 357t^2 + 468t + 229),$$
$$Y_P = 54(3t^2 + 6t + 4)(3t^2 + 9t + 7)(3t^2 + 15t + 19).$$

It is easy to see that the point P is of infinite order on the curve $\mathcal{E}$. In order to prove this let us consider the curve $\mathcal{E}_1$ that is the specialization of the curve $\mathcal{E}$ at $t = 1$. We have $\mathcal{E}_1 : Y^2 = X^3 - 48867651X + 115230640770$. On the curve $\mathcal{E}_1$ we have the point $P_1 = (-3513, 493506)$, which is the specialization of the point P at $t = 1$. Now, let us note that

$$3P_1 = \Big(\frac{3953140143}{1408969}, \frac{24183154596042}{1672446203} \Big).$$

As we know, the points of finite order on the elliptic curve $y^2 = x^3 + ax + b, a, b \in \mathbb{Z}$ have integer coordinates [9, p. 177], while $3P_1$ is not an integral point; therefore, P_1 is not a point of finite order on $\mathcal{E}_1$, which means that P is not a point of finite order on $\mathcal{E}$. Therefore, $\mathcal{E}$ is a curve of positive rank. In particular, we have proved that $1 \leq \operatorname{rank} \mathcal{E}(\mathbb{Q}(t)) \leq \operatorname{rank} \mathcal{E}(\mathbb{C}(t)) \leq 6$. However, we have not identified the $\mathbb{Q}(t)$ rank of $\mathcal{E}$ exactly. Numerical calculations give that for many specializations of $\mathcal{E}$ at $t \in \mathbb{Q}$ we obtain that the rank of $\mathcal{E}_t(\mathbb{Q})$ is equal to one, and this suggests that $\operatorname{rank} \mathcal{E}(\mathbb{Q}(t)) = 1$.

Before proving that the set of rational points on the surface $\mathcal{S}$ is dense in Euclidean topology, we prove the Zariski density of the set of rational points. Because the curve $\mathcal{E}$ is of positive rank over $\mathbb{Q}(t)$, the set of multiples of the point P, *i.e.,* $mP = (X_m(t), Y_m(t))$ for $m = 1, 2, \ldots$, gives infinitely many $\mathbb{Q}(t)$-rational points on the curve $\mathcal{E}$. Now, if we look at the curve $\mathcal{E}$ as an elliptic surface in the space with coordinates (X, Y, t), we can see that each rational curve (X_m, Y_m, t) is included in the Zariski closure, say $\mathcal{R}$, of the set of rational points on $\mathcal{E}$. Because this closure consists of only finitely many components, it has dimension two, and as the surface

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

$\mathcal{E}$ is irreducible, $\mathcal{R}$ is the whole surface. Thus the set of rational points on $\mathcal{E}$ is dense in the Zariski topology, and the same is true for the surface $\mathcal{S}$.

To obtain the statement of our theorem, we have to use two beautiful results: a theorem of Hurwitz [10, p. 78] and a theorem of Silverman [9, p. 368]. Let us recall that Hurwitz's theorem states that if an elliptic curve E defined over $\mathbb{Q}$ has positive rank and one torsion point of order two (defined over $\mathbb{Q}$), then the set $E(\mathbb{Q})$ is dense in $E(\mathbb{R})$. The same result holds if E has three torsion points of order two under the assumption that we have a rational point of infinite order that lives on the bounded branch of the set $E(\mathbb{R})$.

Silverman's theorem states that if $\mathcal{E}$ is an elliptic curve defined over $\mathbb{Q}(t)$ with positive rank, then for all but finitely many $t_0 \in \mathbb{Q}$, the curve $\mathcal{E}_{t_0}$ obtained from the curve $\mathcal{E}$ by the specialization $t = t_0$ has positive rank. From this result we see that for all but finitely many $t \in \mathbb{Q}$, the elliptic curve $\mathcal{E}_t$ is of a positive rank.

In order to finish the proof of our theorem let us define the polynomial $X_i(t)$ to be the X-coordinate of the torsion point T_i for $i = 1, 2, 3$. Tying these two cited theorems together and the fact that we have inequalities $X_3(t) < X_P(t) < X_1(t) < X_2(t)$ for each $t \in \mathbb{R}$, we conclude that for all but finitely many t the set $\mathcal{E}_t(\mathbb{Q})$ is dense in the set $\mathcal{E}_t(\mathbb{R})$. This proves that the set $\mathcal{E}(\mathbb{Q})$ is dense in the set $\mathcal{E}(\mathbb{R})$ in Euclidean topology. Thus, the set $\mathcal{S}(\mathbb{Q})$ is dense in the set $\mathcal{S}(\mathbb{R})$ in Euclidean topology. ■

Using the above result we can deduce the following theorem.

Theorem 2.2 *There exists a polynomial $k \in \mathbb{Z}[t]$ with the property that there are four independent $\mathbb{Q}(t)$-rational points in arithmetic progression on the elliptic curve $\mathcal{E}' : y^2 = x^3 + k(t)$.*

Proof In order to construct a polynomial $k \in \mathbb{Z}[t]$ with the property that for all $t \in \mathbb{Z}$ the value $k(t)$ is a number of AP4 type, we use the points P and T_1 we have constructed in the proof of Theorem 2.1. Let us note that

$$P+T_1 = \left(3(99t^4+432t^3+795t^2+684t+251, -486(t^2+3t+3)(3t^2+3t+1)(3t^2+6t+4)\right).$$

Let us note that this point leads us to the point

$$\varphi(P+T_1) = \Big(\frac{3t^2+9t+10}{3(2t+3)}, -\frac{(1+3t+3t^2)(18t^4+162t^3+516t^2+738t+413)}{9(2t+3)^2}\Big)$$

that belongs to the curve $\mathcal{C}$ constructed in the proof of the previous theorem. Performing all necessary simplifications we find that the point $\varphi(P+T_1)$ gives the polynomial solution of the equation defining the surface $\mathcal{S}$ in the form

$$\begin{aligned} p &= 18t^4+54t^3+30t^2-72t-73, & q &= 18t^4+90t^3+192t^2+210t+107,\\ r &= 18t^4+126t^3+354t^2+456t+233, & s &= 18t^4+162t^3+516t^2+738t+413. \end{aligned}$$

Using this parametric solution and the remark on the beginning of our proof we define the curve $\mathcal{E}' : y^2 = x^3 + k(t)$, where

$$k(t) = -324^2(2t+3)^2(3t^2+9t+10)^2(6t^2+18t+17)^2h(t),$$

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

and

$$h(t) = (t^2 + 3t)^4 + 612(t^2 + 3t)^3 + 300(t^2 + 3t)^2 - 3504(t^2 + 3t) - 5329.$$

On the curve $\mathcal{E}'$ we have four points in arithmetic progression:

$$\begin{aligned}
P_1 &= (tp(t), p(t)(18t^4 + 54t^3 + 30t^2 - 72t - 73)),\\
P_2 &= ((t+1)p(t), p(t)(18t^4 + 90t^3 + 192t^2 + 210t + 107)),\\
P_3 &= ((t+2)p(t), p(t)(18t^4 + 126t^3 + 354t^2 + 456t + 233)),\\
P_4 &= ((t+3)p(t), p(t)(18t^4 + 162t^3 + 516t^2 + 738t + 413)),
\end{aligned}$$

where $p(t) = 108(2t + 3)(3t^2 + 9t + 10)(6t^2 + 18t + 17)$.

We will show that the above points are independent in the group $\mathcal{E}'(\mathbb{Q}(t))$ of all $\mathbb{Q}(t)$-rational points on the curve $\mathcal{E}'$. We specialize the curve $\mathcal{E}'$ at $t = 1$ and get the elliptic curve $\mathcal{E}'_1$ given by the equation

$$\mathcal{E}'_1 : y^2 = x^3 - 111610206808689600.$$

On the curve $\mathcal{E}'_1$ we have the points

$$\begin{aligned}
P_{1,1} &= (487080, 62833320) & P_{2,1} &= (974160, 901585080)\\
P_{3,1} &= (1461240, 1734491880) & P_{4,1} &= (1948320, 2698910280),
\end{aligned}$$

which are specializations of the points P_1, P_2, P_3, P_4 at $t = 1$. Using the APECS program ([2]) we obtain that the determinant of the height matrix of the points $P_{1,1}, P_{2,1}, P_{3,1}, P_{4,1}$ is equal to 266.618020487005. This proves that the points $P_{1,1}$, $P_{2,1}$, $P_{3,1}$, $P_{4,1}$ are independent on the curve $\mathcal{E}'_1$, and thus we get that that the points P_1, P_2, P_3, P_4 are independent on the curve $\mathcal{E}'$. ■

Remark 2.3 Let us consider the polynomial $g(t, x) = x^3 + k(t)$, where $k \in \mathbb{Z}[t]$ was defined in the proof of the above theorem. Then in order to find a rational value of t that gives five points in arithmetic progression on the curve $\mathcal{E}_t$ we must have $g(t, (t-1)p(t)) = \square$ or $g(t, (t+4)p(t)) = \square$. In other words we must be able to find a rational point on one of the hyperelliptic curves of genus 3:

$$\begin{aligned}
C_1 : v^2 &= 324t^8 + 648t^7 - 4428t^6 - 21384t^5 - 34884t^4 +\\
&\quad - 17388t^3 + 12828t^2 + 12804t - 791,\\
C_2 : v^2 &= 324t^8 + 7128t^7 + 63612t^6 + 309096t^5 + 912816t^4\\
&\quad + 1704132t^3 + 1985988t^2 + 1332624t + 397009.
\end{aligned}$$

Unfortunately, we are unable to find a rational point on any of these curves giving a nonzero value of $k(t)$.

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

3 Rational Points in Arithmetic Progressions on $y^2 = x^n + k$ for $n \geq 4$

In this section we consider a natural generalization of the problem we have considered in Section 1. To be more precise we consider the following question.

Question 3.1 Let $n \in \mathbb{N}$ be fixed and suppose that $n \geq 4$. Is it possible to find an integer k with the property that there are at least four rational points in arithmetic progression on the hyperelliptic curve $y^2 = x^n + k$?

We show that if n is odd then the answer to the above question is affirmative, and it is possible to find infinitely many such k's.

For even n we will show that it is possible to construct infinitely many k's with the property that on the curve $y^2 = x^n + k$ there exists three a term arithmetic progression of rational points with x-coordinates belonging to the set $\{a, 3a, 5a\}$, where $a \in \mathbb{Q}$. Using the involution $(x, y) \mapsto (-x, y)$ we can see that on these curves we will have six rational points in arithmetic progression with x-coordinates belonging to the set $\{-5a, -3a, -a, a, 3a, 5a\}$.

We start with the following theorem.

Theorem 3.2 *Let us fix an $n \geq 2$. Then there are infinitely many integers k with the property that there are four points in arithmetic progression on the hyperelliptic curve $H : y^2 = x^{2n+1} + k$.*

Proof In order to prove our theorem let us consider a hyperelliptic curve with the equation $y^2 = ax^{2n+1} + bx^2 + cx + d =: f(x)$, where

$$a = \frac{-p^2 + 3q^2 - 3r^2 + s^2}{2^{2n+1} - 2}, \qquad b = \frac{p^2 - 2q^2 + r^2}{2}, \tag{3.1}$$

$$c = \frac{-(2^{2n} - 2)p^2 - 3q^2 + (2^{2n} + 2)r^2 - s^2}{2^{2n+1} - 2}, \qquad d = q^2.$$

For a, b, c, d defined above, the points $(-1, p), (0, q), (1, r), (2, s)$ are on the curve and are in arithmetic progression. If the system of equations in the variables p, q, r, s given by

$$\begin{cases} p^2 - 2q^2 + r^2 = 0, \\ -(2^{2n} - 2)p^2 - 3q^2 + (2^{2n} + 2)r^2 - s^2 = 0, \end{cases} \tag{3.2}$$

has infinitely many rational solutions, then the points

$$(-a, pa^n), \quad (0, qa^n), \quad (a, ra^n), \quad (2a, sa^n)$$

are in arithmetic progression on the curve $y^2 = x^{2n+1} + da^{2n}$, where a, b are given by (3.1).

Now, we show that system (3.2) has infinitely many solutions in rational numbers. In order to do this let us parametrize all solutions of the first equation in system (3.2). Using the standard method we find parametrization given by

$$p = 2u^2 - 4uv + v^2, \quad q = 2u^2 - 2uv + v^2, \quad r = -2u^2 + v^2.$$

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

Putting the calculated values of p, q, r into the second equation of the system (3.2) and taking $u = 1$, we define

$$\mathcal{C}_n^o : s^2 = v^4 + 4(2^{2n+1} - 1)v^3 - 8(3 \cdot 2^{2n} - 1)v^2 + 8(2^{2n+1} - 1)v + 4.$$

The curve $\mathcal{C}_n^o$ is a quartic curve with rational point $Q^o = (0, -2)$, and the "o" in the notation $\mathcal{C}_n^o$ refers to the fact that $2n + 1$ is odd. If we treat Q^o as a point at infinity on the curve $\mathcal{C}_n^o$ and use the method described in [7, page 77] one more time, we conclude that $\mathcal{C}_n^o$ is birationally equivalent over $\mathbb{Q}$ to the elliptic curve with the Weierstrass equation

$$\mathcal{E}_n^o : Y^2 = X^3 - 27(3 \cdot 2^{4n+2} + 1)X + 54(9 \cdot 2^{4n+2} - 1).$$

The mapping $\varphi : \mathcal{E}_n^o \ni (X, Y) \mapsto (v, s) \in \mathcal{C}_n^o$ is given by

$$v = \frac{2Y - 27 \cdot 2^{2n+2}(2^{4n+2} - 1)}{6(X - 3(3 \cdot 2^{4n+2} - 1))} - (2^{2n+1} - 1),$$

$$s = -(v + 2^{2n+1} - 1)^2 + \frac{2X + 3(3 \cdot 2^{4n+2} - 1)}{9}.$$

Inverse mapping $\psi : \mathcal{C}_n^o \ni (v, s) \mapsto (X, Y) \in \mathcal{E}_n^o$ has the form

$$X = \tfrac{3}{2}\left(3v^2 + 6(2^{2n+1} - 1)v + 3s - 4(3 \cdot 2^{2n} - 1)\right),$$

$$Y = \tfrac{27}{2}(v^3 + 3(2^{2n+1} - 1)v^2 - 4\left(3 \cdot 2^{2n} - 1)v + (2^{2n+1} - 1)s + 2(2^{2n+1} - 1)\right).$$

Let us note that the curve $\mathcal{E}_n^o$ has three points of order two

$$T_1 = (6, 0), \quad T_2 = (3(3 \cdot 2^{2n+1} - 1), 0), \quad T_3 = (-3(3 \cdot 2^{2n+1} + 1), 0).$$

On the curve $\mathcal{E}_n^o$ we also have the point P_n^o given by

$$P_n^o = \left(-3(3 \cdot 2^{2n+1} - 5), 54(2^{2n+1} - 1)\right).$$

It is easy to see that the point P_n^o is of infinite order on the curve $\mathcal{E}_n^o$. In order to prove this we compute $4P_n^o = (X, Y)$, where

$$X = \frac{3 \cdot 2^{-4n-2}(3 + 3 \cdot 2^{16n} - 2^{4n+4} + 13 \cdot 2^{8n+1} + 2^{12n+5})}{(2^{4n} - 1)^2},$$

$$Y = \frac{3 \cdot 2^{-2n-1}(3 \cdot 2^{8n} + 1)}{2^{4n} - 1}X + 27 \cdot 2^{2n}(2^{4n} - 1).$$

It is easy to see that under our assumption ($n \geq 2$) the X-coordinate of the point $4P_n^o$ is not an integer. Thus, a theorem of Nagell and Lutz ([9, p. 177]) implies that the point P_n^o is of infinite order. This implies that the set of rational solutions of system (3.2) is infinite, and thus our theorem is proved. ■

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

Remark 3.3 Using the APECS program we calculated the rank r_n of elliptic curve $\mathcal{E}_n^o$ and generators for the free part of the group $\mathcal{E}_n^o(\mathbb{Q})$ for $2 \leq n \leq 8$. The results of our computations are given below.

n	r_n	Generators for the free part of the group $\mathcal{E}_n^o(\mathbb{Q})$
2	1	$(303, 17820)$
3	1	$(1167, 6966)$
4	2	$(4623, 27702), (11773, 1175552)$
5	2	$(18447, 110646), (350011167/6241, 6184493104374/493039)$
6	1	$(73743, 442422)$
7	3	$(294927, 1769526), (153394089/400, 1214402001813/800),$ $(124356529/256, 1101957449705/4096)$
8	1	$(1179663, 7077942)$

From the above theorem we get an interesting corollary.

Corollary 3.4 *Let $n \geq 2$ and consider the family of hyperelliptic curves given by the equation $C_k : y^2 = x^{2n+1} + k$. Then the set $\mathcal{A}$ of integers k with the property that there exist at least 8 rational points on the curve C_k, is infinite. Moreover, we can construct the set $\mathcal{A}$ such that for each pair $k_1, k_2 \in \mathcal{A}$ the curves C_{k_1}, C_{k_2} are not isomorphic over $\mathbb{Q}$.*

Proof The first part of our corollary is an immediate consequence of the previous theorem. The second part of our corollary is a simple consequence of the following reasoning. Curves C_{k_1} and C_{k_2} are isomorphic over $\mathbb{Q}$ if and only if $k_1/k_2 \in \mathbb{Q}^{4n+2}$. From the previous theorem we can take $k = q^2 = (v^2 - 2v + 2)^2$ for some $v \in \mathbb{Q}$ that is calculated from the point that lies on the elliptic curve $\mathcal{C}_n^o$. Let us suppose that we have constructed the integers $k_1, k_2, \ldots, k_m$ such that the curves C_{k_i} are pairwise non-isomorphic over $\mathbb{Q}$. We have that $k_i = q_i^2 = (v_i^2 - 2v_i + 2)^2$ for $i = 1, 2, \ldots, m$. Then curves $(2v^2 - 2v + 2)^2 = (v_i^2 - 2v_i + 2)^2 w^{4n+2}$ for $i = 1, 2 \ldots, m$ are all of genus ≥ 2, thus the set of $C_1(\mathbb{Q}) \cup \cdots \cup C_m(\mathbb{Q})$ is finite (Faltings Theorem [4]). Because the elliptic curve $\mathcal{C}_n^o$ has infinitely many rational points, we can find v_{m+1} such that the curve $C_{k_{m+1}}$ with $k_{m+1} = (v_{m+1}^2 - 2v_{m+1} + 2)^2$ is not isomorphic over $\mathbb{Q}$ to any of the curves C_i for $i = 1, 2 \ldots, m$. By induction we can construct an infinite set $\mathcal{A}$ with the demanded property. ■

The above corollary and Corollary 3.10 give a generalization of A. Bremner's result from [1, Theorem 2.1 and Theorem 3.1].

Theorem 3.2 suggests the following question.

Question 3.5 Let us fix an integer $n \geq 1$. What is the least value $|k_{2n+1}| \in \mathbb{N}$, say M_{2n+1}, with the property that on the curve $y^2 = x^{2n+1} + k_{2n+1}$ there are at least four rational points in arithmetic progression?

Example 3.6 Taking $n = 2$, by the existence of rational point of infinite order on the curve $\mathcal{E}_2^o$ we get that

$$M_5 \leq 339154139517070836868816998 0^4 \cdot 2609^2 \cdot 127165689041^2.$$

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

Moreover, by Corollary 3.4 it is natural to ask the following question.

Question 3.7 Let us fix an integer $n \geq 2$ and consider the hyperelliptic curve $H_{2n+1} : y^2 = x^{2n+1} + k_{2n+1}$, where k_{2n+1} is constructed with the method presented in the proof of the Theorem 3.2. In particular, we have four points in arithmetic progression on the curve H_{2n+1}, say P_i for $i = 1, 2, 3, 4$. Are the classes of divisors $(P_i) - (\infty)$ independent in the jacobian variety associated with the curve H_{2n+1}?

Now, we prove the following theorem.

Theorem 3.8 *Let us fix an $n \geq 2$. Then there are infinitely many integers k with the property that there are six points in arithmetic progression on the hyperelliptic curve $H : y^2 = x^{2n} + k$.*

Proof In order to prove our theorem let us consider a hyperelliptic curve with the equation $y^2 = x^{2n} + ax^2 + bx + c =: f(x)$, where

$$a = \frac{p^2 - 2q^2 + r^2 - 5^{2n} + 2 \cdot 3^{2n} - 1}{8},$$
$$b = \frac{-2p^2 + 3q^2 - r^2 + 5^{2n} - 3^{2n+1} + 2}{2},$$
$$c = \frac{15p^2 - 10q^2 + 3r^2 - 3 \cdot 5^{2n} + 10 \cdot 3^{2n} - 15}{8}.$$

We have that $f(1) = p^2$, $f(3) = q^2$, $f(5) = r^2$. It is easy to see that in order to prove our theorem it is enough to find infinitely many solutions of the system of equations $a = b = 0$ in rational numbers p, q, r. Indeed, if $a = b = 0$, then on the curve $y^2 = x^{2n} + c$ we will have six points in arithmetic progression that x-coordinates belonging to the set $\{-5, -3, -1, 1, 3, 5\}$.

System $a = b = 0$ is equivalent to the system of equations

$$\begin{cases} q^2 = p^2 + 3^{2n} - 1, \\ r^2 = p^2 + 5^{2n} - 1. \end{cases} \tag{3.3}$$

Putting $p = u + 1, q = tu + 3^n$ we find that all rational solutions of the equation $q^2 = p^2 + 3^{2n} - 1$ are contained in the formulas

$$p = \frac{t^2 - 2 \cdot 3^n t + 1}{t^2 - 1}, \qquad q = -\frac{3^n t^2 - 2t + 3^n}{t^2 - 1}.$$

Putting the calculated value of p into the second equation of the system (3.3) we get the equation of the quartic curve

$$\mathcal{C}_n^e : s^2 = 5^{2n}t^4 - 4 \cdot 3^n t^3 - 2(5^{2n} - 2 \cdot 3^{2n} - 2)t^2 - 4 \cdot 3^n t + 5^{2n} =: g(t),$$

where $s = (t^2 - 1)r$ and the "e" in the notation $\mathcal{C}_n^e$ refers to the fact that $2n$ is even. For convenience let us put $u = 3^n$ and $v = 5^n$. Then, the polynomial g takes the form

$$g_{u,v}(t) = v^2t^4 - 4ut^3 - 2(v^2 - 2u^2 - 2)t^2 - 4u + v^2.$$

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

The curve $\mathcal{C}_n^e : s^2 = g_{u,v}(t)$ is a quartic curve with rational point $Q^e = (0, v)$. Regarding Q^e as a point at infinity on the curve $\mathcal{C}_n^e$ and using the method described in [7, p. 77] one more time, we conclude that $\mathcal{C}_n^e$ is birationally equivalent over $\mathbb{Q}$ to the elliptic curve with the Weierstrass equation

$$\mathcal{E}_n^e : Y^2 = X^3 - 27(v^4 - (u^2+1)v^2 + u^4 - u^2 + 1)X + 27(1 + u^2 - 2v^2)(2u^2 - v^2 - 1)(u^2 + v^2 - 2).$$

The mapping $\varphi\colon \mathcal{E}_n^e \ni (X, Y) \mapsto (t, s) \in \mathcal{C}_n^e$ is given by

$$t = \frac{v^3 Y - 27u(u^2 - v^2)(v^2 - 1)}{3v^2(v^2 X - 3(3u^2 - 2v^2 + v^4 - 2u^2v^2)} + \frac{u}{v^2},$$
$$s = -\frac{1}{v^3}\left(v^2 t - \frac{u}{v^2}\right)^2 + \frac{v^2 X + 9u^2 - 6(u^2+1)v^2 + 3v^4}{9v^3}.$$

Inverse mapping $\psi\colon \mathcal{C}_n^e \ni (t, s) \mapsto (X, Y) \in \mathcal{E}_n^e$ has the form

$$X = \frac{2 - 6tu + 2u^2 + 3sv + (3t^2 - 1)v^2}{2},$$
$$Y = -\frac{27}{2}\left(su + \left((3t^2+1)u - 2t(u^2+1)\right)v - stv^2 - (t^3 - t)v^3\right).$$

Let us note that the curve $\mathcal{E}_n^e$ has three points of order two

$$T_1 = \left(3(1+u^2-2v^2), 0\right), \quad T_2 = \left(3(u^2+v^2-2), 0\right), \quad T_3 = \left(-3(1-2u^2+v^2), 0\right).$$

On the curve $\mathcal{E}_n^e$ we also have the point P_n^e given by

$$P_n^e = \left(3(u^2 + v^2 + 1), -27uv\right).$$

It is easy to see that the point P_n^e is of infinite order on the curve $\mathcal{E}_n^e$. Indeed, $2P_n = (X_2, Y_2)$, where

$$X_2 = \frac{3(3u^4 - 2(u^2+1)u^2v^2 + (3 - 2u^2 + 3u^4)v^4)}{4u^2v^2}.$$

Due to the fact that $u = 3^n$ and $v = 5^n$ it is easy to see that for any choice of $n \geq 2$ the above fraction is not an integer. From the Nagell–Lutz theorem we get that the point P_n^e is not of finite order on the curve $\mathcal{E}_n^e$. This implies that the set of rational solutions of system (3.3) is infinite. As a consequence we get that for any $n \geq 2$ we can construct infinitely many k's with the property that on the curve $y^2 = x^{2n} + k$ we have three points in arithmetic progression with x-coordinates belonging to the set $\{m, 3m, 5m\}$ with $m > 0$. Note that on this curve we also have rational points with x-coordinates belonging to the set $\{-m, -3m, -5m\}$. This observation finishes the proof of our theorem. ■

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

Remark 3.9 Using the program APECS we calculated the rank r_n of elliptic curve $\mathcal{E}_n^e$ and generators for the free part of the group $\mathcal{E}_n^e(\mathbb{Q})$ for $2 \leq n \leq 8$. The results of our computations are given below.

n	r_n	Generators for the free part of the group $\mathcal{E}_n^e(\mathbb{Q})$
2	1	$(3840, 176256)$
3	2	$(80808, 14478912), (130704, 40007520)$
4	2	$(1230432, 116328960), (31769376/25, 24804389376/125)$
5	1	$(36278088, 68748343488)$
6	1	$(836384640, 5022400795776)$
7	1	$(19863352968, 370669722011712)$
8	1	$(480955252992, 27480236025415680)$

Using a similar argument as in the proof of the Corollary 3.4 we can prove the following corollary.

Corollary 3.10 *Let $n \geq 2$, and consider the family of hyperelliptic curves given by the equation $C_k : y^2 = x^{2n} + k$. Then the set $\mathcal{A}$ of integers k with the property that there are at least 12 rational points on the curve C_k, is infinite. Moreover, we can construct the set $\mathcal{A}$ such that for each pair $k_1, k_2 \in \mathcal{A}$ the curves C_{k_1}, C_{k_2} are not isomorphic over $\mathbb{Q}$.*

As in the case of odd exponents we can ask the following questions.

Question 3.11 Let us fix an integer $n \geq 2$. What is the least value $|k_{2n}| \in \mathbb{N}$, say M_{2n}, with the property that there are at least three rational points in arithmetic progression on the curve $y^2 = x^{2n} + k_{2n}$?

Question 3.12 Let us fix an integer $n \geq 2$ and consider the hyperelliptic curve $H_{2n} : y^2 = x^{2n} + k_{2n}$, where k_{2n} is constructed using the method we presented in the proof of the Theorem 3.8. In particular, we have three points in arithmetic progression on the curve H_{2n}, say P_i for $i = 1, 2, 3$. Are the classes of divisors $(P_i) - (\infty)$ independent in the jacobian variety associated with the curve H_{2n}?

4 Sextic Threefold Related to Five Rational Points in Arithmetic Progression on $y^2 = x^3 + k$

In the Section 2 we used very natural reasoning in order to construct quartic surface closely related to the problem of existence of numbers of AP4 type. A natural question arises as to whether we can construct an algebraic variety, say $\mathcal{T}$, with the property that each (nontrivial) rational point on $\mathcal{T}$ gives a number k of AP5 type, so an integer k such that we have five rational points in arithmetic progression on the curve $y^2 = x^3 + k$. In order to construct the demanded hypersurface we will use a method similar to the one used in Section 2.

Let $f(x, y) = y^2 + ay - (bx^3 + cx^2 + dx + e) \in \mathbb{Q}[a, b, c, d, e][x]$, and consider the curve $C : f(x, y) = 0$. By the change of coordinates

$$(x, y) = \Big(\frac{X - 12c}{36b}, \frac{Y - 108ab}{216b} \Big) \text{ with inverse } (X, Y) = \big(12(c+3bx), 108b(a+2y) \big),$$

https://doi.org/10.4153/CMB-2011-058-1 Published online by Cambridge University Press

we can see that the curve C is birationally equivalent to the curve

$$E : Y^2 = X^3 - 432(c^2 - 3bd)X + 432(27a^2b^2 + 8c^3 - 36bcd + 108b^2e).$$

Let p, q, r, s, t be free parameters, and consider the system of equations

$$f(-2, p) = f(-1, q) = f(0, r) = f(1, s) = f(2, t) = 0.$$

This system has exactly one solution with respect to a, b, c, d, e. This solution belongs to the field $\mathbb{Q}(p, q, r, s, t)$ and has the form

$$a = \frac{A}{6H}, \quad b = \frac{B}{6H}, \quad c = \frac{C}{6H}, \quad D = \frac{D}{6H}, \quad e = \frac{E}{6H},$$

where $A, \ldots, E \in \mathbb{Z}[p, q, r, s, t]$ are homogeneous, A is of degree two, and $B, \ldots, E$ are of degree three. Moreover, we have $H = p - 4q + 6r - 4s + t$. From these computations we can see that in order to find an integer k with the property that there are five points in arithmetic progression on the curve $y^2 = x^3 + k$, it is enough to find rational points on the sextic threefold given by the equation

$$\mathcal{T} : C(p, q, r, s, t)^2 = 3B(p, q, r, s, t)D(p, q, r, s, t),$$

where

$$\begin{aligned}
B &= (p - 3q + 3r - s)t^2 - (p^2 - 3q^2 + 3r^2 - s^2)t + (q - 3r + 3s)p^2 \\
&\quad - (q^2 - 3r^2 + 3s^2)p + 2(q - s)(3qr - 3r^2 - 4qs + 3rs), \\
C &= -3((t^2 + p^2)(q - 2r + s) - (t + p)(q^2 - 2r^2 + s^2) + 2r(q^2 - qr - rs + s^2)), \\
D &= -(p - 6q + 3r + 2s)t^2 + (p^2 - 6q^2 + 3r^2 + 2s^2)t + (2q + 3r - 6s)p^2 \\
&\quad - (2q^2 + 3r^2 - 6s^2)p - 8(q - s)(3qr - 3r^2 - 4qs + 3rs).
\end{aligned}$$

There are obvious automorphisms of order two acting on $\mathcal{T}$ by

$$(p, q, r, s, t) \mapsto (t, s, r, q, p), \quad (p, q, r, s, t) \mapsto (-p, -q, -r, -s, -t).$$

By a trivial rational point on the hypersurface $\mathcal{T}$ we will understand the point (p, q, r, s, t) that lies on one of the lines

$$L_1 : p = q = r, s = t, \quad L_2 : p = q = s, r = t, \ldots, \quad L_{10} : r = s = t, p = q,$$

or on the hyperplane $H : p - 4q + 6r - 4s + t = 0$.

We performed numerical calculations in order to find a non-trivial rational point on $\mathcal{T}$. We computed all integer solutions of the equation defining the hypersurface $\mathcal{T}$ under the assumption that $\max\{|p|, |q|, |r|, |s|, |t|\} \leq 10^2$. Unfortunately within this range all solutions are trivial. This suggests the following question.

Question 4.1 Is the set of non-trivial rational points on the hypersurface $\mathcal{T}$ non-empty?

Acknowledgment I would like to thank the anonymous referee for several helpful suggestions that improved the original presentation.

References

[1] A. Bremner, *On the equation $Y^2 = X^5 + k$.* Experiment. Math. **17**(2008), no. 3, 371–374.
[2] I. Connell, *APECS: Arithmetic of plane elliptic curves, 2001.* http://www.math.mcgill.ca/connell/public/apecs.
[3] N. D. Elkies, *On $A^4 + B^4 + C^4 = D^4$.* Math. Comp. **51**(1988), no. 184, 825–835.
[4] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73**(1983), no. 3, 349–366. doi:10.1007/BF01388432
[5] J.-B. Lee and W. Y. Vélez, *Integral solutions in arithmetic progression for $y^2 = x^3 + k$.* Period. Math. Hungar. **25**(1992), no. 1, 31–49. doi:10.1007/BF02454382
[6] S. P. Mohanty, *Integral solutions in arithmetic progression for $y^2 = x^3 + k$.* Acta Math. Acad. Sci. Hungar. **34**(1980), no. 3–4, 261–265. doi:10.1007/BF01898141
[7] L. J. Mordell, *Diophantine equations.* Pure and Applied Mathematics, 30, Academic Press, London-New York, 1969.
[8] T. Shioda, *On elliptic modular surfaces.* J. Math. Soc. Japan **24**(1972), 20–59. doi:10.2969/jmsj/02410020
[9] J. H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106, Springer-Verlag, New York, 1986.
[10] T. Skolem, *Diophantische Gleichungen.* Ergebnisse der Mathematik und ihrer Grenzgebiete, 5, no. 4, Berlin, Springer, 1938.

Jagiellonian University, Institute of Mathematics, 30 - 348 Kraków, Poland
e-mail: maciej.ulas@gmail.com