*Publ. Math. Debrecen*
**82/3-4** (2013), 669–683
DOI: 10.5486/PMD.2013.5438

# Rational points in geometric progressions on certain hyperelliptic curves

By ANDREW BREMNER (Tempe) and MACIEJ ULAS (Kraków)

**Abstract.** We pose a simple Diophantine problem which may be expressed in the language of geometry. Let $C$ be a hyperelliptic curve given by the equation $y^2 = f(x)$, where $f \in \mathbb{Z}[x]$ is without multiple roots. We say that points $P_i = (x_i, y_i) \in C(\mathbb{Q})$ for $i = 1, 2, \dots, k$, are in geometric progression if the numbers $x_i$ for $i = 1, 2, \dots, k$, are in geometric progression.

Let $n \geq 3$ be a given integer. In this paper we show that there exist polynomials $a, b \in \mathbb{Z}[t]$ such that on the curve $y^2 = a(t)x^n + b(t)$ (defined over the field $\mathbb{Q}(t)$) we can find four points in geometric progression. In particular this result generalizes earlier results of Berczes and Ziegler concerning the existence of geometric progressions on Pell type quadrics $y^2 = ax^2 + b$. We also investigate for fixed $b \in \mathbb{Z}$, when there can exist rationals $y_i$, $i = 1, \dots, 4$, with $\{y_i^2 - b\}$ forming a geometric progression, with particular attention to the case $b = 1$. Finally, we show that there exist infinitely many parabolas $y^2 = ax + b$ which contain five points in geometric progression.

## 1. Introduction

Let $f \in \mathbb{Z}[x]$ be without multiple roots, and consider the hyperelliptic curve $C : y^2 = f(x)$. We say that the rational points $P_i = (x_i, y_i)$, $i = 1, 2, \dots, k$, lying on the curve $C$, are in geometric progression if the numbers $x_1, x_2, \dots, x_k$ are in geometric progression, i.e. there exist $p, t \in \mathbb{Q}$ such that $x_i = pt^i$ for $i = 1, \dots, k$. In a recent paper, Bérczes and Ziegler [1, Theorem 4] proved that for any four term geometric progression $0 < x_1 < x_2 < x_3 < x_4$ there exist infinitely many $a, b \in \mathbb{Z}$ such that there exist $y_i \in \mathbb{Q}$ with the property that the points $P_i = (x_i, y_i)$

*Mathematics Subject Classification:* 11G05.
*Key words and phrases:* geometric progressions, rational points, hyperelliptic curves.

for $i = 1, 2, 3, 4$ lie on the curve $y^2 = ax^2 + b$. Moreover one can choose $a, b$ in such a way that $a$ is not a square, $b \neq 0$, and $\gcd(a, b)$ is squarefree. In view of this result it may be asked what can be proved in the case of a more general curve such as $y^2 = ax^n + b$, where $n \in \mathbb{N}_+$ is a fixed integer. More precisely: can one obtain a straight generalization of the cited result for the curve $y^2 = ax^n + b$, for all $n$? This problem is most interesting in the case $n = 1$. In order to see this, note that we may concentrate on geometric progressions of the form $x_i = t^i$ for $i = 0, 1, \ldots, k$; for if the points $P_i' = (x_i', y_i)$ are in geometric progression on $C' : y^2 = ax^n + b$, with $x_i' = pt^i$, then the points $P_i = (t^i, y_i)$ lie in geometric progression on the curve $C : y^2 = ap^n x^n + b$, which is of the same type. We say that the geometric progression of the form $t^i$ for $i = 0, 1, \ldots, k-1$, is *the geometric progression generated by $t$ of length $k$*. Next, note that we can indeed reduce the investigation to the case $n = 1$. For if the points $P_i = (t^i, y_i)$ lie in geometric progression on $C : y^2 = ax^n + b$, then the points $Q_i = (t^{in}, y_i)$ lie in geometric progression on the curve $y^2 = ax + b$. Thus, the problem for a given positive integer $n$ is equivalent to the investigation of geometric progressions of the form $x_i = t^{in}$ on the parabola $y^2 = ax + b$. In other words, if we denote by $S(t, n)$ the problem of existence of four term geometric progressions generated by $t$ on curves of type $y^2 = ax^n + b$, then we have the equivalence $S(t, n) \Leftrightarrow S(t^n, 1)$. We thus see that the cited result from [1] immediately implies that if $n$ is even then the problem $S(t, n)$ has an affirmative answer. Henceforth, in this paper we shall consider only the case $n$ odd. Moreover, we should note that the problem $S(t, 1)$ can also be rephrased as a problem of the existence of four values of the polynomial $(y^2 - b)/a$ which are in geometric progression. This is clearly equivalent to the investigation of the Diophantine system

$$\frac{Y^2 - b}{X^2 - b} = \frac{Z^2 - b}{Y^2 - b} = \frac{W^2 - b}{Z^2 - b}. \tag{1}$$

This system was investigated in [8], where it is shown that there exists a homogeneous polynomial $b \in \mathbb{Z}[u, v]$ of degree 18 such that there is a solution $X, Y, Z, W \in \mathbb{Z}[u, v]$ of (1). However, the discussion presented there is far from exhaustive. Indeed, in [8] we were interested in *integer* solutions of (1) only. This assumption is very restrictive, and rational solutions of the system are missed. For example when $b = -6$ there is a solution $(X, Y, Z, W) = (3/11, 3, 39/7, 453/49)$. A natural question arises as to whether there are infinitely many parametric solutions of the system (1) (where $b$ is treated as a variable for this question).

The strategy we adopt is the following. The variety which parameterizes the instances of $a$, $b$ such that there is a four term geometric progression, say

$1, t, t^2, t^3$, on the curve $y^2 = ax + b$ results in the study of a certain elliptic curve $\mathcal{C}$ defined over the field $\mathbb{Q}(t)$. Now $\mathcal{C}$ may also be viewed as an elliptic surface, and using the Shioda theory of elliptic surfaces, we compute the rank of $\mathcal{C}$ over $\mathbb{C}(t)$ (it is equal to one) and find on $\mathcal{C}$ a point of infinite order. This allow us to find infinitely many $b \in \mathbb{Q}(t)$ such that the system (1) has a non-trivial solution in polynomials $X, Y, Z, W \in \mathbb{Q}(t)$. Moreover, using the Silverman specialization theorem and a theorem of Hurwitz we prove that the set of all rational points on $\mathcal{C}$, that is, the set $\mathcal{C}(\mathbb{Q})$, is dense in the real topology in the set of all real points on $\mathcal{C}$.

Secondly, we investigate when there can exist solutions of the system (1) for a fixed value of $b$, and show that there exist infinitely many solutions for $b$ of certain type, including $b = 1$. Note that the "three-term geometric progression" corresponding to the system

$$\frac{Y^2 - 1}{X^2 - 1} = \frac{Z^2 - 1}{Y^2 - 1}$$

has been much studied in the past; see, for example, Guy [3], Section D23, and the references given there; and Ulas [10].

Thirdly, we prove that there exist infinitely many distinct parabolas $y^2 = ax + b$ which contain *five* points in geometric progression. Finally, some computational remarks are made.

## 2. A parameterizing curve

In this section we construct a curve $\mathcal{E}$ defined over the field $\mathbb{Q}(t)$ which parameterizes pairs of rational functions $a, b$ with the property that on the parabola $y^2 = f(x) = ax + b$ there lie four points in geometric progression, say the geometric progression $1, t, t^2, t^3$ generated by $t$ of length 4. Demanding $a + b = U^2$, $at + b = V^2$, gives

$$a = \frac{U^2 - V^2}{1 - t}, \quad b = \frac{V^2 - tU^2}{1 - t}. \tag{2}$$

It remains to satisfy $f(t^2)$, $f(t^3)$ both squares. Thus we investigate the curve $\mathcal{C}$ given by the intersection of the following two quadrics:

$$\mathcal{C} : -tU^2 + (1 + t)V^2 = R^2, \quad -t(1 + t)U^2 + (1 + t + t^2)V^2 = S^2. \tag{3}$$

We prove the following result.

**Theorem 2.1.** *Consider the curve $\mathcal{C}$ in $\mathbb{P}^3$ over $\mathbb{Q}(t)$ defined by* (3). *Then $\mathcal{C}$ is birationally equivalent over $\mathbb{Q}(t)$ to an elliptic curve $\mathcal{E}$ with* $\operatorname{rank}\mathcal{E}(\mathbb{Q}(t)) = 1$. *Moreover, regarding $\mathcal{E}$ as a surface in $\mathbb{R}^3$ then the set $\mathcal{E}(\mathbb{Q}) \subset \mathbb{R}^3$ of all rational points is dense in the set $\mathcal{E}(\mathbb{R})$ of all real points lying on $\mathcal{E}$.*

Proof. Taking $(1,1,1,1)$ as the zero point, then a cubic model for the elliptic curve $\mathcal{C}$ is given by

$$\mathcal{E} : Y^2 = X(X+t^2)(X+t(1+t)^2).$$

The discriminant $\Delta(\mathcal{E})$ of $\mathcal{E}$ is

$$\Delta(\mathcal{E}) = 16t^8(1+t)^4(1+t+t^2)^2,$$

so the specialization of $\mathcal{E}$ at $t \in \mathbb{C}$ is singular for the values $t \in \mathcal{A}$, where

$$\mathcal{A} = \left\{\infty, -1, 0, -\frac{1+\sqrt{-3}}{2}, -\frac{1-\sqrt{-3}}{2}\right\}.$$

Now $\mathcal{E}$ represents a K3-surface, and 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 [5], we have

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

where the sum ranges over all fibers of the pencil $\mathcal{E}_t$, with $m_\nu$ the number of irreducible components of the fiber. 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. For $t \in \mathcal{A}$, the decomposition is of Kodaira classification as follows. For $t = 0$ and $t = \infty$ we have type $I_2^*$, each with $m_\nu = 7$. For $t = -\frac{1\pm\sqrt{-3}}{2}$ we have type $I_2$ and then $m_\nu = 2$. For $t = -1$ we have type $I_4$ and then $m_\nu = 4$. Summing up gives

$$\operatorname{rank}\mathrm{NS}(\mathcal{E},\mathbb{C}) = \operatorname{rank}\mathcal{E}(\mathbb{C}(t)) + 2 + 2(7-1) + (4-1) + 2(2-1).$$

Since the rank of the Néron–Severi group of a K3-surface cannot exceed 20, then $\operatorname{rank}\mathcal{E}(\mathbb{C}(t)) \leq 1$. The curve $\mathcal{E}$ has three two-torsion points

$$T_1 = (0,0), \quad T_2 = (-t^2, 0), \quad T_3 = (-t(1+t)^2, 0)$$

and the point

$$P = (t^3(1+t),\, t^3(1+t)(1+t+t^2)).$$

The height of $P$ equals $3/4$, so that $P$ is of infinite order; and hence $\mathcal{E}(\mathbb{Q}(t))$ (and so $\mathcal{E}(\mathbb{C}(t)))$ has rank 1.

We will prove that the set of rational points on the surface $\mathcal{E}$ is dense in the Euclidean topology. However, we first prove 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, regarding the curve $\mathcal{E}$ as an elliptic surface in the space with coordinates $(X, Y, t)$ we 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 $\mathcal{E}$ is irreducible, $\mathcal{R}$ is the whole surface. Thus the set of rational points on $\mathcal{E}$ is dense in the Zariski topology.

To obtain the density of the set $\mathcal{E}(\mathbb{Q})$ in the Euclidean topology, we use two beautiful results: a theorem of Hurwitz [4] (see also [7, p. 78]) and a theorem of Silverman [6, p. 368]. The theorem of Hurwitz 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 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 specialization at $t = t_0$ 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 positive rank. Denote by $\mathcal{G}$ the set of $t \in \mathbb{Q}$ such that the specialization $P_t$ of the point $P$ at $t \in \mathbb{Q}$ is of infinite order on the curve $\mathcal{E}_t$. From Mazur's theorem we know that the order of a torsion point on an elliptic curve defined over $\mathbb{Q}$ is at most 12. Thus, in order to find $\mathcal{G}$ it is enough to find all $t \in \mathbb{Q}$ such that $P_t$ has finite order. This is straightforward: compute the expression $mP = (X(m), Y(m))$ for $m \in \mathbb{N}$ and $m \leq 12$, and determine for any given $m$ those $t \in \mathbb{Q}$ such that the denominator of $X(m)$ has a zero at $t$. The only $t \in \mathbb{Q}$ with such a property for which $\mathcal{E}_t$ is nonsingular is $t = 1$. In this case $P_1$ is of order four on the curve $\mathcal{E}_1$. Moreover the rank of $\mathcal{E}_1(\mathbb{Q})$ is equal to zero. We thus get that $\mathcal{G} = \mathbb{Q} \setminus \{-1, 0, 1\}$. Note that the values $t = -1, 0, 1$ are without interest because they lead to trivial geometric progressions.

Now define the polynomial $X_i(t)$ to be the $X$-coordinate of the torsion point $T_i$ for $i = 1, 2, 3$. We have the following equalities

$$P + T_1 = (t + 1, -(1 + t)(1 + t + t^2)),$$
$$P + T_2 = (-t(t + 1), t^2(t + 1)),$$

$$P+T_3=(-t^2(t+1),-t^3(t+1)),$$

and it is straightforward to verify the following inequalities:

$$\begin{aligned}
&X_2(t)<X_{P+T_1}(t)<X_1(t)<X_3(t) &&\text{for } t\in(-\infty,-1),\\
&X_2(t)<X_{P+T_3}(t)<X_1(t)<X_2(t) &&\text{for } t\in(-1,0),\\
&X_3(t)<X_{P+T_3}(t)<X_2(t)<X_1(t) &&\text{for } t\in(0,\infty).
\end{aligned}$$

For each $i=1,2,3$, the point $P+T_i$ is of infinite order on the curve $\mathcal{E}$. Moreover, for all $t\in\mathcal{G}$ and $i=1,2,3$, the specialization of the point $P+T_i$ is of infinite order on the curve $\mathcal{E}_t$. From the above inequalities we deduce that for all $t\in\mathcal{G}$ there is a point of infinite order lying on the bounded branch of the real curve $\mathcal{E}_t$. Using the Hurwitz theorem, it follows that for all $t\in\mathcal{G}$ 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 the Euclidean topology. Note, it follows from the birational equivalence that $\mathcal{C}(\mathbb{Q})$ is dense in $\mathcal{C}(\mathbb{R})$. □

*Remark 2.2.* Consider the system (1). If $X$, $Y$, $Z$, $W$ is a solution of (1) for some $b$, and the common value of the equalities is $t$, it follows immediately that there exists $a$ such that

$$X^2-b=a,\quad Y^2-b=at,\quad Z^2-b=at^2,\quad W^2-b=at^3.$$

Solving the first three equations with respect to $a,b,t$ gives

$$a=\frac{(X^2-Y^2)^2}{X^2-2Y^2+Z^2},\quad b=\frac{-Y^4+X^2Z^2}{X^2-2Y^2+Z^2},\quad t=\frac{Y^2-Z^2}{X^2-Y^2}.$$

Substituting into the fourth equation,

$$t=\frac{Y^2-Z^2}{X^2-Y^2}=\frac{Z^2-W^2}{Y^2-Z^2}. \tag{4}$$

If we are not interested in the value of $t$, we need to investigate the projective surface $(Y^2-Z^2)^2=(X^2-Y^2)(Z^2-W^2)$, and essentially this approach was used in [8] in order to find one polynomial solution of the system. If we are interested in the solutions (4) with given $t$, this leads to the intersection of the two quadratic surfaces

$$Z^2=-tX^2+(1+t)Y^2,\quad W^2=-t(t+1)X^2+(1+t+t^2)Y^2,$$

which, on renaming the variables, is exactly the same intersection defining the curve $\mathcal{C}$ from (3). Theorem 2.1 now implies that the set of rational points on the surface $(Y^2-Z^2)^2=(X^2-Y^2)(Z^2-W^2)$ is dense in the Euclidean topology.

*Example 2.3.* Using the pullbacks on $\mathcal{C}$ of the points $P$ and $mP + T_i$ for $m \in \mathbb{Z}$ and $i = 1, 2, 3$, one can compute $a(t)$, $b(t)$, given by (2); and without loss of generality, $a$, $b$ may be taken as polynomials in $\mathbb{Z}[t]$. For such $b$, provided that $a \neq 0$, we get a solution of the system (1). The pullbacks when $m = 1$ lead only to trivial solutions; the pullback of $2P$ however leads to

$$a = 8(1+t)(1+t^2), \quad b = (-1-t-3t^2+t^3)(-1+3t+t^2+t^3),$$

with solution of system (1) given by

$$(X,Y,Z,W) = (t^3-t^2-t-3,\ t^3-t^2+3t+1,\ t^3+3t^2-t+1,\ -3t^3-t^2-t+1).$$

Note that the degree of $b$ is equal to six. This improves upon the degree 18 polynomial obtained in [8]. The expressions $X^2-b$, $Y^2-b$, $Z^2-b$, $W^2-b$ are in geometric progression with quotient $t$. This progression is clearly non-trivial for $t \neq -1, 0, 1$.

Returning to the initial question about the existence of geometric progressions on hyperelliptic curves of the form $y^2 = ax^n + b$, we note the following.

**Corollary 2.4.** *Let $n$ be a given positive (odd) integer. For any nontrivial four term geometric progression $x_i$, $i = 1, 2, 3, 4$, there exist infinitely many pairwise non-isomorphic hyperelliptic curves $C : y^2 = ax^n + b$ such that $x_i$ is the $x$-coordinate of a rational point on $C$.*

Proof. It is clear that we may assume $x_i = u^i$, say, for $i = 0, 1, 2, 3$. In the previous example it was shown that there exist infinitely many rational functions $a_m(t)$, $b_m(t)$ (corresponding to the point $mP$) such that $a_m(t)t^i + b_m(t)$ is the square of a rational function, say $r_m(t)$, for $i = 0, 1, 2, 3$, and $m = 1, 2, \ldots$ . Putting $t = u^n$ we immediately obtain $a_m(u^n)(u^i)^n + b_m(u^n) = r_m(u^n)^2$. This implies that for $i = 0, 1, 2, 3$, the point $(x_i, r_m(t))$ lies on the hyperelliptic curve $C : y^2 = a_m(t)x^n + b_m(t)$ for $m = 1, 2, \ldots$ . That there are infinitely many distinct such curves is a simple consequence of the following reasoning. Let $C_m : y^2 = a_m(t)x^n + b_m(t)$, where $m$ is a positive integer. The coefficients $a_m$ and $b_m$ are given by (2) and are calculated from the $\mathbb{Q}(t)$-rational point $mP$ on the curve $\mathcal{C}$, where $P$ is the point of infinite order on $\mathcal{E}$ given in the proof of Theorem 2.1. Note that the curves $C_p$ and $C_q$ are isomorphic if and only if

$$a_p(t)^{n-1}b_p(t) = a_q(t)^{n-1}b_q(t)W^{2n}$$

for some $W \in \mathbb{Q}(t)$. Suppose we have constructed the integers $k_1, k_2, \ldots, k_m$ such that the curves $C_{k_i}$ are pairwise non-isomorphic over $\mathbb{Q}(t)$. Consider the $m$ curves

$$C^i : a(U,V)^{n-1}b(U,V) = a_{k_i}(t)^{n-1}b_{k_i}(t)W^{2n}$$

for $i = 1, 2 \ldots, m$, where $a(U, V)$, $b(U, V)$ are given by (2). The polynomial defining the curve $C^i$ is homogenous of degree $2n$ in the coordinates $(U : V : W)$; and it is clear from (2) that $C^i$ is defined over $\mathbb{Q}(t)$. The curve $C^i$ for $i = 1, 2, \ldots, m$ is of genus $\geq 2$, so that the set $C^1(\mathbb{Q}(t)) \cup \ldots \cup C^m(\mathbb{Q}(t))$ is finite (this is just the function field analogue of Faltings Theorem [2]). Because the elliptic curve $\mathcal{C}$ has infinitely many rational points we can find an integer $k_{m+1} > k_m$ such that the curve $C_{k_{m+1}}$ is not isomorphic over $\mathbb{Q}(t)$ to any of the curves $C_{k_i}$ for $i = 1, 2 \ldots, m$. By induction we can construct an infinite set $\mathcal{A}$ with the required property. □

**Corollary 2.5.** *There exists $k \in \mathbb{Z}[t]$ such that on the elliptic curve $\mathcal{C} : y^2 = x^3 + k$ there are four independent rational points in geometric progression.*

Proof. In order to prove the result it is enough to take

$$k(t) = (1 + t^3)^2(1 + t^6)^2(-1 - t^3 - 3t^6 + t^9)(-1 + 3t^3 + t^6 + t^9).$$

This corresponds to the values of $a, b$ presented in Example 2.3, and is equal to $\frac{1}{64}a(t^3)^2 b(t^3)$. Then on the curve $\mathcal{C} : y^2 = x^3 + k(t)$ we have the four points in geometric progression:

$$\begin{aligned}
P_1 =& (2(1 + t^3)(1 + t^6), (1 + t^3)(1 + t^6)(-3 - t^3 - t^6 + t^9)),\\
P_2 =& (2t(1 + t^3)(1 + t^6), (1 + t^3)(1 + t^6)(1 + 3t^3 - t^6 + t^9)),\\
P_3 =& (2t^2(1 + t^3)(1 + t^6), (1 + t^3)(1 + t^6)(1 - t^3 + 3t^6 + t^9)),\\
P_4 =& (2t^3(1 + t^3)(1 + t^6), (1 + t^3)(1 + t^6)(-1 + t^3 + t^6 + 3t^9)).
\end{aligned}$$

The above points are seen to be independent in the group $\mathcal{C}(\mathbb{Q}(t))$ by means of a simple specialization argument. Specialize the curve $\mathcal{C}$ at $t = 2$ to get the elliptic curve

$$\mathcal{C}_2 : y^2 = x^3 + 63752753025.$$

The points $P_i$, $i = 1, 2, 3, 4$, specialize respectively to

$$\begin{aligned}
R_1 &= (1170, 255645), & R_2 &= (2340, 276705),\\
R_3 &= (4680, 407745), & R_4 &= (9360, 940095),
\end{aligned}$$

and the determinant of the height pairing matrix of the four points is equal to 326.8430126208496567501056976. This proves independence of the points $R_i$ on the curve $\mathcal{C}_2$, and thus the independence of the points $P_i$ on the curve $\mathcal{C}$. □

*Remark 2.6.* The result above is very similar to the one obtained in ULAS [9], where it is proved that there exists $k \in \mathbb{Z}[t]$ such that on the curve $\mathcal{E} : y^2 = x^3 + k(t)$ there are four points in arithmetic progression which are independent in the group $\mathcal{E}(\mathbb{Q}(t))$.

Further, it is possible to prove that for each odd $n$ which is divisible by 3 there exists $k \in \mathbb{Z}[t]$ such that the rank of the Jacobian of the curve $A : Y^2 = X^n + K(t)$ defined over $\mathbb{Q}(t)$ is greater than or equal to 4. Indeed, it is enough to take $K(t) = k(t^{n/3})$, where $k \in \mathbb{Z}[t]$ is given above. Then there is a map from $A$ to the elliptic curve $C' : y^2 = x^3 + K(t)$ given by $(X, Y) \mapsto (X^{n/3}, Y)$. Thus $C'$ is a factor of the Jacobian $\mathcal{J}(A)$ (up to isogeny), which implies that $\operatorname{rank} \mathcal{J}(A(\mathbb{Q}(t))) \geq \operatorname{rank} C'(\mathbb{Q}(t))$. From the reasoning presented in Corollary 2.5 it follows that the rank of $C'$ over $\mathbb{Q}(t)$ is greater than or equal to 4, and thus the same is true for $\mathcal{J}(A(\mathbb{Q}(t)))$.

## 3. The case of fixed $b$

It is interesting to ask whether there exist solutions in rationals of the system (1) for a given squarefree integer value of $b$. We do not know how to answer this question, but can make some inroads.

Consider the intersection of (1) with

$$X^2 Z^2 = (4X^2 - 3Y^2)Y^2.$$

It follows from the first equation at (1) that

$$Y^2(4X^2 - 3b) = bX^2. \tag{5}$$

We suppose that $b$ is of the form $b = c^2 + 3d^2$, so that this latter curve (5) of genus 0 may be parametrized by

$$X = b(m^2 + 3n^2)/(2(dm^2 - 2cmn - 3dn^2)), \tag{6}$$

$$Y = b(m^2 + 3n^2)/(2(cm^2 + 6dmn - 3cn^2)); \tag{7}$$

and the requirement that $4X^2 - 3Y^2 = (XZ/Y)^2$ gives

$$Z = b(m^2 + 3n^2)k/(2(cm^2 + 6dmn - 3cn^2)^2), \tag{8}$$

where

$$(4c^2-3d^2)m^4+60cdm^3n \\ -18(2c^2-9d^2)m^2n^2-180cdmn^3+9(4c^2-3d^2)n^4=k^2. \quad (9)$$

The second equation at (1) gives, on eliminating $Z$, then $Y$:

$$W^2=bX^2(8X^2-9b)^2/(4X^2-3b)^3=(8X^2-9b)^2Y^6/(b^2X^4),$$

so that

$$\begin{aligned} W &= (8X^2-9b)Y^3/(bX^2) \\ &= \frac{b(m^2+3n^2)((2c^2-3d^2)m^4+36cdm^3n}{2(cm^2+6dmn-3cn^2)^3} \\ &\quad + \frac{-6(4c^2-15d^2)m^2n^2-108cdmn^3+9(2c^2-3d^2)n^4)}{2(cm^2+6dmn-3cn^2)^3}. \end{aligned} \quad (10)$$

Then $(X,Y,Z,W)$ at (6), (7), (8), (10), give a solution of (1) with $b=c^2+3d^2$, and common ratio equal to

$$-3(dm^2-2cmn-3dn^2)^2/(cm^2+6dmn-3cn^2)^2.$$

It follows that when the quartic (9) represents an elliptic curve of positive rank, then there will be infinitely many distinct rational solutions of the system (1) when $b=c^2+3d^2$. In the range $1\leq b<100$, the only such values of $b$ occur for $b=1,19,31,61,79$.

Perhaps the most interesting case is $(c,d)=(1,0)$, with $b=1$. The curve (9) is now

$$k^2=4(m^4-9m^2n^2+9n^4),$$

with cubic model

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

of rational rank 1, and generator $(x,y)=(1,10)$. Modulo torsion, the multiples of the generator pull back to $(m,n)=(0,1)$, $(1,1)$, $(4,1)$, $(-45,7)$, ... The first two result in trivial solutions, and the next two give the following solutions of (1), in the case $b=1$:

$$(X,Y,Z,W)=(-19/16,19/26,209/169,1387/2197), \\ (181/105,181/313,108419/97969,29478203/30664297),\ldots$$

More generally, the rank of (9) can be forced to be positive by setting $4c^2-3d^2=e^2$, say. Take

$$(c,d,e)=(g^2+3h^2,\quad g^2+2gh-3h^2,\quad g^2-6gh-3h^2),$$

so that

$$b = 4(g^4 + 3g^3h - 9gh^3 + 9h^4),$$

and (9) becomes

$$\begin{aligned} k^2 = (g^2 - 6gh - 3h^2)^2m^4 + 60(g-h)(g+3h)(g^2+3h^2)m^3n \\ + 18(7g^4 + 36g^3h - 30g^2h^2 - 108gh^3 + 63h^4)m^2n^2 \\ - 180(g-h)(g+3h)(g^2+3h^2)mn^3 + 9(g^2 - 6gh - 3h^2)^2n^4. \end{aligned}$$

With $(m, n, k) = (0, 1, 3(g^2 - 6gh - 3h^2))$ as zero of the group, then the point $(m, n, k) = ((0, 1, -3(g^2 - 6gh - 3h^2))$ has height 4, and is of infinite order. Thus the system (1) has infinitely many solutions in the case that

$$b \equiv (g^4 + 3g^3h - 9gh^3 + 9h^4) \bmod \mathbb{Q}^{*2}.$$

## 4. Some remarks on five points in geometric progression on $y^2 = ax + b$

The problem of finding five points in geometric progression on the parabola $y^2 = ax + b$ reduces to considering the system

$$x^2 - b = A/q^2, \quad y^2 - b = A/q, \quad z^2 - b = A, \quad t^2 - b = Aq, \quad u^2 - b = Aq^2, \tag{11}$$

where, by absorbing squares into $x, y, z, t, u$, and $A$, we may assume without loss of generality that $b$ is a squarefree integer.

We show that there are infinitely many essentially distinct solutions of this system.

Solving for $A, b, q$,

$$A = \frac{(z^2 - t^2)(y^2 - z^2)}{t^2 + y^2 - 2z^2}, \quad b = \frac{t^2y^2 - z^4}{t^2 + y^2 - 2z^2}, \quad q = \frac{z^2 - t^2}{y^2 - z^2},$$

and substituting into the remaining two equations,

$$x^2(t^2 - z^2) = y^2(t^2 - y^2) + y^2z^2 - z^4, \quad u^2(y^2 - z^2) = t^2(y^2 - t^2) + t^2z^2 - z^4.$$

Equivalently,

$$(t^2 - z^2)(y^2(t^2 - y^2) + y^2z^2 - z^4) = \square, \quad (y^2 - z^2)(t^2(y^2 - t^2) + t^2z^2 - z^4) = \square.$$

If we set

$$t^2(y^2-4z^2)=-3z^4,$$

then

$$(t^2-z^2)(y^2(t^2-y^2)+y^2z^2-z^4)=\left(\frac{z(y^2-z^2)(y^2-2z^2)}{y^2-4z^2}\right)^2,$$

and

$$(y^2-z^2)(t^2(y^2-t^2)+t^2z^2-z^4)=(-4y^2+13z^2)\left(\frac{z^2(y^2-z^2)}{y^2-4z^2}\right)^2.$$

Accordingly, we demand

$$-4y^2+13z^2=\square,\qquad y^2-4z^2=-3\square, \tag{12}$$

the equation of an elliptic curve on taking $(1,1,3,1)$ as zero. The curve has rational rank 1 with $P=(-1,-1,-3,1)$ as generator. It follows that we can construct an infinite chain of solutions to the system (11) by pulling back multiples of the generator. Note that $b=(t^2y^2-z^4)/(t^2+y^2-2z^2)$ and $t^2(y^2-4z^2)=-3z^4$ imply that $b(y^2-5z^2)=-4z^4$. Thus, with (12), we have for fixed $b$ that

$$b(y^2-5z^2)=-\square,\qquad -4y^2+13z^2=\square,\qquad y^2-4z^2=-3\square,$$

the equation of a curve of genus 5, with only finitely many rational points. Accordingly, infinitely many $b$ arise from this construction. In particular, this implies that there are infinitely many distinct quadratic polynomials $f(x)=x^2-b$ such that the set $f(\mathbb{Q})$ contains a non-constant geometric progression of length 5. This shows that the conjecture of Ulas [8, Conjecture 3.3] is false.

As example, the points

$$2P=(-23,13,9,7),\qquad 3P=(-1873,-1117,1479,703),\qquad \dots$$

give rise to $(y,z)=(-23,13)$, $(-1873,-1117)$, … giving the following solutions to the system (11):

$$(b,A,q)=\left(79,-\frac{7110}{169},-\frac{169}{147}\right),\qquad (x,y,z,t,u)=\left(\frac{15089}{2197},\frac{1817}{169},\frac{79}{13},\frac{79}{7},\frac{237}{49}\right),$$

and

$$(b,A,q)=\left(682579,-\frac{385732218690}{1247689},-\frac{1247689}{1482627}\right),$$

$$(x,y,z,t,u)=\left(\frac{691282564829}{1393668613},\frac{1278470467}{1247689},\frac{682579}{1117},\frac{682579}{703},\frac{336511447}{494209}\right),$$

etc.

## 5. Computational remarks

Finally, a search was undertaken for small solutions of (1) in the range $-100 < b < 100$, and the results are presented in the Table in the Appendix. The parameterization at (6)–(10) above was discovered by focussing on solutions in which the common ratio was of type $-3\square$. It seems highly plausible that there should be other parameterizable solutions corresponding (say) to the common ratio being a square.

Two solutions found exhibit $Z = 0$. It is straightforward to analyze those solutions in which $XYZW = 0$. By symmetry, we may suppose $W = 0$ or $Z = 0$. In the former case, (1) reduces to

$$-tX^2 + (1+t)Y^2 = Z^2, \qquad -t(1+t)X^2 + (1+t+t^2)Y^2 = 0.$$

But then $t(1+t)(1+t+t^2) = \square$, representing an elliptic curve of rational rank 0. The finite rational points occur for $t = 0, -1$, affording no solution to the original problem.

In the latter case, (1) reduces to

$$-tX^2 + (1+t)Y^2 = 0, \qquad -t(1+t)X^2 + (1+t+t^2)Y^2 = W^2.$$

Thus $t(1+t) = \square$; set $t = 1/(u^2-1)$. Then $X^2 = u^2Y^2$, $Y^2 = (1-u^2)W^2$, so put $u = 2v/(v^2+1)$, giving $X = 2v/(v^2+1)Y$, $W = (v^2+1)/(v^2-1)Y$, $b = (v^2+1)^2/(2(v^4+1))Y^2$. Accordingly, we have the infinite family

$$(X,Y,Z,W) = \left(\frac{4v(1+v^4)}{(1+v^2)^2},\quad \frac{2(1+v^4)}{1+v^2},\quad 0,\quad \frac{2(1+v^4)}{v^2-1}\right), \qquad b = 2(1+v^4),$$

with common ratio $t = -(1+v^2)^2/(1-v^2)^2$. It is worth remarking that there will be infinitely many distinct solutions of the system (1) for $b$ of the form $2(1+v_0^4)$. For a solution with such $b$, we demand $v \in \mathbb{Q}$ such that $b = 2(1+v_0^4) = 2(1+v^4)y^2$, equivalently, $(1+v_0^4)(1+v^4) = w^2$, say. This latter equation is that of an elliptic curve, with points given by $(\pm v, \pm w) = (v_0, 1+v_0^4)$, $(1/v_0, (1+v_0^4)/v_0^2)$. Taking $(v_0, 1+v_0^4)$ as zero of the group, then the point $(v_0, -1-v_0^4)$ has height 4, and so is non-torsion. Its multiples $(v, w)$ correspond to the solution

$$(X,Y,Z,W) = \left(\frac{4vw}{(1+v^2)^2},\quad \frac{2w}{1+v^2},\quad 0,\quad \frac{2w}{1-v^2}\right), \qquad b = 2(1+v_0^4),$$

with common ratio $-(1+v^2)^2/(1-v^2)^2$.

## 6. Appendix

| $b$ | $X$ | $Y$ | $Z$ | $W$ | ratio |
|---|---|---|---|---|---|
| -95 | 16 | 29 | 49 | 81 | 8/3 |
| -87 | 145/64 | 29/4 | 145/13 | 2581/169 | 256/169 |
| -79 | 79/135 | 7979/765 | 82871/4335 | 766221/24565 | 684/289 |
| -79 | 419/15 | 119/3 | 167/3 | 233/3 | 25/13 |
| -74 | 3086/529 | 578/23 | 202/3 | 4678/27 | 529/81 |
| -59 | 3599/361 | 1711/19 | 649 | 4661 | 361/7 |
| -39 | 3 | 21 | 69 | 219 | 10 |
| -39 | 5 | 11 | 19 | 31 | 5/2 |
| -29 | 29/64 | 551/16 | 899/4 | 1450 | 208/5 |
| -23 | 5251/1681 | 181/41 | 17/3 | 188/27 | 1681/1296 |
| -11 | 3 | 7 | 13 | 23 | 3 |
| -11 | 19/3 | 37 | 193 | 1003 | 27 |
| -11 | 2085/529 | 3485/644 | 11105/1568 | 794405/87808 | 4761/3136 |
| -7 | 23/27 | 29/9 | 17/3 | 9 | 9/4 |
| -6 | 3/11 | 3 | 39/7 | 453/49 | 121/49 |
| 1 | 299/289 | 23/17 | 23/7 | 529/49 | 578/49 |
| 1 | 19/16 | 19/26 | 209/169 | 1387/2197 | -192/169 |
| 1 | 9951/7168 | 771/448 | 699/308 | 2649/847 | 256/121 |
| 1 | 2201/1849 | 155/43 | 93/5 | 7471/75 | 12943/450 |
| 1 | 475799/243049 | 5357/493 | 487/7 | 21915/49 | 243049/5880 |
| 1 | 181/105 | 181/313 | 108419/97969 | 29478203/30664297 | -33075/97969 |
| 2 | 557/368 | 13/8 | 229/124 | 4343/1922 | 2116/961 |
| 11 | 83/25 | 17/5 | 5 | 19 | 25 |
| 14 | 19/5 | 5 | 17 | 83 | 25 |
| 15 | 453/121 | 39/11 | 3 | 3/7 | 121/49 |
| 19 | 1349/343 | 247/49 | 19/7 | 19/3 | -49/27 |
| 22 | 9/2 | 17/4 | 29/8 | 23/16 | 9/4 |
| 22 | 230/49 | 34/7 | 10 | 62 | 49 |
| 23 | 187933/52822 | 3335/1078 | 2231/946 | 24265/40678 | 2401/1849 |
| 29 | 6887/1331 | 733/121 | 17/11 | 11 | -121/35 |
| 29 | 37/7 | 41/7 | 11/7 | 89/7 | -5 |
| 31 | 31/5 | 31/7 | 341/49 | 713/343 | -75/49 |
| 31 | 188/41 | 17/4 | 181/48 | 5251/1728 | 1681/1296 |
| 34 | 136/25 | 34/5 | 0 | 34/3 | -25/9 |
| 34 | 10 | 32 | 122 | 472 | -25/9 |
| 41 | 123/25 | 41/5 | 0 | 41/4 | -25/16 |
| 41 | 4343/529 | 229/23 | 13 | 557/31 | 2116/961 |
| 43 | 6 | 31/4 | 19/16 | 769/64 | -39/16 |
| 51 | 9771/961 | 579/31 | 543/13 | 16629/169 | 961/169 |
| 61 | 262/21 | 138/7 | 242/7 | 442/7 | 45/13 |
| 69 | 933/125 | 249/25 | 3/5 | 15 | -25/11 |
| 69 | 7187/729 | 1267/81 | 307/9 | 83 | 81/13 |
| 78 | 62/7 | 10 | 34 | 230 | 49 |
| 79 | 97/11 | 103/11 | 47/11 | 247/11 | -7 |
| 79 | 15089/2197 | 1817/169 | 79/13 | 79/7 | -169/147 |
| 79 | 1817/169 | 79/13 | 79/7 | 237/49 | -169/147 |

| | | | | | |
|---|---|---|---|---|---|
| 89 | 13 | 43 | 197 | 923 | 22 |
| 91 | 9 | 11 | 1 | 19 | -3 |
| 93 | 2445/361 | 111/19 | 75/17 | 309/289 | 361/289 |
| 93 | 5815/529 | 337/23 | 25 | 541/11 | 529/121 |

ACKNOWLEDGMENTS The results presented in this paper were obtained during a short research visit of the second author to Arizona State University (Tempe, USA). Research of the second author was supported by Polish Government funds for science, grant IP 2011 057671 for the years 2012–2013.

## References

[1] A. BÉRCZES, V. ZIEGLER, On geometric progressions on Pell equations and Lucas sequences, *Glasnik Matematički* (*to appear*).

[2] G. FALTINGS, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366.

[3] R. GUY, Unsolved Problems in Number Theory, 3rd ed., *Springer-Verlag, New York*, 2004.

[4] A. HURWITZ, Über ternäre diophantische Gleichungen dritten Grades, *Vierteljahrschrift d. Naturforsch. Ges. Zürich* **62** (1917), 207–229.

[5] T. SHIODA, On elliptic modular surfaces, *J. Math. Soc. Japan* **24** (1972), 20–59.

[6] J. SILVERMAN, The Arithmetic of Elliptic Curves, *Springer-Verlag, New York*, 1986.

[7] TH. SKOLEM, Diophantische Gleichungen, *Chelsea Publishing Company, New York*, 1950.

[8] M. ULAS, On the diophantine equation $(x^2+k)(y^2+k)=(z^2+k)^2$, *Rocky Mountain J. Math.* **38**(6) (2008), 2091–2099.

[9] M. ULAS, Rational points in arithmetic progressions on $y^2=x^n+k$, *Can. Math. Bull.* **55** (1) (2012), 193-207.

[10] M. ULAS, On the diophantine equation $f(x)f(y)=f(z)^2$, *Colloq. Math.* **107** (2007), 1–6.

ANDREW BREMNER
SCHOOL OF MATHEMATICAL
AND STATISTICAL SCIENCES
ARIZONA STATE UNIVERSITY
TEMPE AZ 85287-1804
USA

*E-mail:* bremner@asu.edu

MACIEJ ULAS
JAGIELLONIAN UNIVERSITY
FACULTY OF MATHEMATICS
AND COMPUTER SCIENCE
INSTITUTE OF MATHEMATICS
ŁOJASIEWICZA 6
30-348 KRAKÓW
POLAND

*E-mail:* maciej.ulas@uj.edu.pl

*(Received January 31, 2012; revised June 24, 2012)*