Publ. Math. Debrecen
76/1-2 (2010), 183–201

On the Diophantine equation $z^2 = f(x)^2 \pm f(y)^2$

By MACIEJ ULAS (Kraków and Warszawa) and ALAIN TOGBÉ (Westville)

Abstract. Let $f \in \mathbb{Q}[X]$ and let us consider a Diophantine equation $z^2 = f(x)^2 \pm f(y)^2$. In this paper, we show that if $\deg f = 2$ and there exists a rational number t such that on the quartic curve $V^2 = f(U)^2 + f(t)^2$ there are infinitely many rational points, then the set of rational parametric solutions of the equation $z^2 = f(x)^2 + f(y)^2$ is non-empty. Without any assumptions we show that the surface related to the Diophantine equation $z^2 = f(x)^2 - f(y)^2$ is unirational over the field $\mathbb{Q}$ in this case. If $\deg f = 3$ and f has the form $f(x) = x(x^2 + ax + b)$ with $a \neq 0$ then both of the equations $z^2 = f(x)^2 \pm f(y)^2$ have infinitely many rational parametric solutions. A similarly result is proved for the equation $z^2 = f(x)^2 - f(y)^2$ with $f(X) = X^3 + aX^2 + b$ and $a \neq 0$.

1. Introduction

Let $f \in \mathbb{Q}[X]$ and let us consider the Diophantine equation

$$z^2 = f(x)^2 \pm f(y)^2. \tag{1}$$

We are interested in the existence of infinitely many rational solutions (x, y, z) of equation (1). A similar problem was studied by the first author in [3]. In fact, he considered the Diophantine equation

$$f(x)f(y) = f(z)^2, \tag{2}$$

where $f \in \mathbb{Q}[X]$ is a polynomial function of $\deg f \leq 3$. In [3], he proved that if f is a quadratic function, then the Diophantine equation $f(x)f(y) = f(z)^2$ has

---

Mathematics Subject Classification: Primary: 11D25, 11D41; Secondary: 11G052.
Key words and phrases: pythagorean triples, Diophantine equations, elliptic curves.
The second author is partially supported by Purdue University North Central.

infinitely many nontrivial solutions in $\mathbb{Q}(t)$. Let us recall that a triple (x, y, z) of rational numbers is a nontrivial solution of equation (2) if $f(x) \neq f(y)$ and $f(z) \neq 0$. In the case where f is a cubic polynomial function of the form $f(X) = X(X^2 + aX + b)$, a, b being nonzero integers such that if $p|a$, then $p^2 \nmid b$, he showed that for all but finitely many integers a, b satisfying these conditions, equation (2) has infinitely many nontrivial solutions in rational numbers.

In this paper, we study equation (1). This type of equations has a strong geometric flavor. Indeed, each non-trivial solution (i.e. with $f(x)f(y) \neq 0$) of the equation $z^2 = f(x)^2 + f(y)^2$ gives a right triangle with legs of the length $f(x)$, $f(y)$ and hypotenuse z. Similarly, each non-trivial solution (i.e. $f(x)^2 \neq f(y)^2$) of the equation $z^2 = f(x)^2 - f(y)^2$ gives a right triangle with legs z, $f(y)$ and hypotenuse $f(x)$.

In Section 2, we consider equation (1) under the assumption that f is a polynomial of degree two with rational coefficients. It is obvious to observe that one can consider a polynomial of the form $f(X) = X^2 + a$, $a \neq 0$. We prove that if there exists a rational number t_0 such that the set of rational points on the quartic curve $V^2 = (U^2 + a)^2 + (t_0^2 + a)^2$ is infinite then the set of rational parametric solutions of the equation $z^2 = (x^2 + a)^2 + (y^2 + a)^2$ is non-empty (Theorem 2.3). Next, we prove that if f is of degree two and has two distinct roots over the field $\mathbb{C}$ then the surface related to the Diophantine equation $z^2 = f(x)^2 - f(y)^2$ is unirational over the field $\mathbb{Q}$ (Theorem 2.4). Finally in Section 2, we consider a quadratic polynomial of the form $f(X) = (aX + b)(cX + d)$ where $a, b, c, d \in \mathbb{Z}$ and we prove that if $b/a \neq d/c$ then the quartic equation $f(z)^2 = f(x)^2 + f(y)^2$ has infinitely many rational parametric solutions. For the proof, we make a correspondence between solutions of this equation and rational points on an elliptic curve $\mathcal{E}_f$ in Weierstrass form, defined over the field $\mathbb{Q}(t)$. We show that the rank of $\mathcal{E}_f$ (as a curve defined over the field $\mathbb{Q}(t)$) is at least one (Theorem 2.5).

Section 3 is devoted to equation (1) when f is a cubic polynomial. We start with a cubic polynomial of the form $f(X) = X(X^2 + aX + b)$ with $a \in \mathbb{Z}\setminus\{0\}$, $b \in \mathbb{Z}$. The method used is similar to that of the quadratic polynomial. Using suitable (non-invertible) change of variables we reduce the study of our problem to the problem of existence of $\mathbb{Q}(t)$-rational points on an elliptic curve $\mathcal{E}_f$. Again here, we show that the set of $\mathbb{Q}(t)$-rational points on the appropriate chosen elliptic curve $\mathcal{E}_f$ is not finite by showing the existence of $\mathbb{Q}(t)$-rational points of infinite order. Therefore, by means of this reduction, we prove that equation (1) has infinitely many solutions in $\mathbb{Q}(t)$ (Theorem 3.1, Theorem 3.2). We finish the section by using the same method for polynomials of the form $f(x) = X^3 + aX^2 + b$, $(a \neq 0)$ and obtain a similar result for the equation $z^2 = f(x)^2 - f(y)^2$ (Theorem 3.3).

In the last section, we consider the equation $z^2 = f(x)^2 - f(y)^2$ with $f(x) = x^4 + a$, $(a \neq 0)$. Under some additional assumptions we proved that the set of rational solutions of this equation is infinite.

2. The equation $z^2 = f(x)^2 \pm f(y)^2$ for some quadratic functions

In this section, we are interested in the rational solutions of the Diophantine equation $z^2 = (x^2 + a)^2 \pm (y^2 + a)^2$. We start our study with the " + " equation. However, before we state and prove theorems concerning this equation we will prove a quite general result about rational points on certain geometrically rational elliptic surfaces (it means that such a surface is rational over the field of complex numbers $\mathbb{C}$). More precisely, we will prove the following result.

Theorem 2.1. *Let $f_4, g_4 \in \mathbb{Q}[t]$ be two even functions of degree 4 and let us consider an elliptic surface given by the equation $\mathcal{E} : Y^2 = X^3 + f_4(t)X + g_4(t)$. Suppose that there exist a rational number $t = t_0$ such that the curve $\mathcal{E}_{t_0}$ has infinitely many rational points. Then the set of rational curves on the surface $\mathcal{E}$ is non-empty.*

Proof. Without loss of generality we can assume that $f_4(t) = at^4 + bt^2 + c$, $g_4(t) = dt^4 + et^2 + f$, where $a, b, c, d, e, f \in \mathbb{Z}$ and $ad \neq 0$. Let us define $F(X, Y, t) = Y^2 - (X^3 + f_4(t)X + g_4(t))$. From the assumption we know that there exists a rational number t_0 such that the curve $F(X, Y, t_0) = 0$ has infinitely many rational points. Let us take x_0, y_0 such that $F(x_0, y_0, t_0) = 0$. In order to prove our theorem we put $X = pT^2 + qT + x_0$, $Y = rT^3 + sT^2 + uT + y_0$, $t = T + t_0$. Then, for X, Y, t defined in this way we get $F(X, Y, t) = \sum_{i=1}^{6} a_i T^i$, where

$$\begin{aligned}
a_1 &= -aqt_0^4 - (4d + 4ax_0)t_0^3 - bqt_0^2 - (2e + 2bx_0)t_0 + 2uy_0 - 3qx_0^2 - cq,\\
a_2 &= -apt_0^4 - 4aqt_0^3 - (6d + bp + 6ax_0)t_0^2 - 2bqt_0 - bx_0 - 3q^2x_0 - 3px_0^2\\
&\quad + 2sy_0 - e - cp + u^2,\\
a_3 &= -4apt_0^3 - 6aqt_0^2 - (4d + 2bp + 4ax_0)t_0 - 6pqx_0 + 2ry_0 - bq + q^3 + 2su,\\
a_4 &= -6apt_0^2 - 4aqt_0 - ax_0 - 3p^2x_0 - d - bp - 3pq^2 + s^2 + 2ru,\\
a_5 &= -4apt_0 - aq + 3p^2q + 2rs,\\
a_6 &= -ap + p^3 + r^2.
\end{aligned}$$

The system of equations $a_1 = a_2 = a_3 = a_4 = 0$ in variables p, q, r, u has exactly one solution defined over the field $\mathbb{Q}(s)$. This solution is given by

$$q = -\frac{2(et_0 + 2dt_0^3 + bt_0x_0 + 2at_0^3x_0 - uy_0)}{c + bt_0^2 + at_0^4 + 3x_0^2},$$
$$p = -\frac{e - u^2 + 2bqt_0 + 6dt_0^2 + 4aqt_0^3 + bx_0 + 3q^2x_0 + 6at_0^2x_0 - 2sy_0}{c + bt_0^2 + at_0^4 + 3x_0^2},$$
$$r = \frac{bq + q^3 - 2su + 4dt_0 + 2bpt_0 + 6aqt_0^2 + 4apt_0^3 + 6pqx_0 + 4at_0x_0}{2y_0},$$
$$u = \frac{d + bp + 3pq^2 - s^2 + 4aqt_0 + 6apt_0^2 + ax_0 + 3p^2x_0}{2r}.$$

Due to the fact that the curve $\mathcal{E}_{t_0} : Y^2 = X^3 + f_4(t_0)X + g_4(t_0)$ has infinitely many rational points, we can choose x_0, y_0 such that the quantities $p, q, r, u \in \mathbb{Q}(s)$ given above are well defined i.e. all denominators are non-zero. Moreover, we can assume that $p, q, r, u \in \mathbb{Q}(s) \setminus \{0\}$. Thus, if we take p, q, r, u defined above, then the equation $F(x, y, t) = 0$ treated as equation over the field $\mathbb{Q}(s)$ has two $\mathbb{Q}(s)$-rational roots: $T = 0$ of multiplicity five and the root

$$T = \frac{-aq - 3p^2q + 2rs - 4apt_0}{ap + p^3 - r^2} =: \varphi(s).$$

Therefore, on the surface $\mathcal{E}$, we have a parametric rational curve given by the equations

$$X = p\varphi(s)^2 + q\varphi(s) + x_0, \quad Y = r\varphi(s)^3 + s\varphi(s)^2 + u\varphi(s) + y_0, \quad t = \varphi(s) + t_0,$$

where $p, q, r, u \in \mathbb{Q}(s) \setminus \{0\}$ are defined above. This observation finishes the proof of our theorem. $\square$

Remark 2.2. The above result is a complementary result of Theorem 5.1 of [4].

Now, we are ready to prove the following result.

Theorem 2.3. *Let $f \in \mathbb{Q}[X]$ and suppose that $\deg f = 2$ and f has two distinct roots over $\mathbb{C}$. Let us suppose that there exists a rational number $y = t_0$ such that the set of rational solutions on the (quartic) curve $C_{t_0} : V^2 = f(U)^2 + f(t_0)^2$ is infinite. Then there exists a rational parametric solution of the Diophantine equation $z^2 = f(x)^2 + f(y)^2$.*

Proof. It is clear that without loss of generality we can assume that $f(X) = X^2 + a$ with $a \in \mathbb{Z} \setminus \{0\}$. Let us consider the curve $\mathcal{C} : v^2 = (u^2 + a)^2 + (t^2 + a)^2$ defined over the field $\mathbb{Q}(t)$. This curve is birationally equivalent with the elliptic curve $\mathcal{E}$ given by the equation in Weierstrass form

$$\mathcal{E} : Y^2 = X^3 - 108(3t^4 + 6at^2 + 7a^2)X - 432a(9t^4 + 18at^2 + 17a^2).$$

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

$$u = \frac{Y}{6(X + 12a)}, \quad v = -\left(\frac{Y}{6(X + 12a)}\right)^2 + \frac{X - 6a}{18}.$$

The discriminant of $\mathcal{E}$ is given by $\Delta(\mathcal{E}) = 2^8 3^{12}(t^2 + a)^4(t^4 + 2at^2 + 2a^2)$, and thus $\mathcal{E}$ is non-singular over $\mathbb{Q}(t)$ for any choice of $t \in \mathbb{Q}$.

From the assumption we know that there exists a rational number t_0 such that the elliptic curve $\mathcal{E}_{t_0}$ is of positive rank. From this observation and Theorem 2.1, we get the desired result. $\square$

Next, we prove a similar result when we take equation (1) for the sign "$-$".

Theorem 2.4. *Suppose $f \in \mathbb{Q}[X]$ where $\deg f = 2$ and f has two distinct roots over $\mathbb{C}$. Let us consider the surface $\mathcal{S}_f^2 : z^2 = f(x)^2 - f(y)^2$. Then $\mathcal{S}_f^2$ is unirational over the field $\mathbb{Q}$. In other words, the Diophantine equation $z^2 = f(x)^2 - f(y)^2$ has rational parametric solutions in two parameters.*

Proof. Without loss of generality we can assume that $f(X) = X^2 + a$ for some $a \in \mathbb{Z} \setminus \{0\}$. In order to prove Theorem 2.4, let us put $z = xz_1,\ y = tx$ where t is an indeterminate. Then we have the equality

$$z^2 - (f(x)^2 - f(y)^2) = x^2(z_1^2 - (1 - t^2)(2a + (t^2 + 1)x^2)).$$

Let us note that the curve $z_1^2 = (1 - t^2)(2a + (t^2 + 1)x^2) =: h(x, t)$ is a quadric curve defined over the field of rational functions $\mathbb{Q}(t)$. Now, we want to find a substitution $t = g(u)$ such that the function $h(0, g(u))$ is a square of a rational function. If $x = 0$, then $h(0, t) = 2a(1 - t^2)$. The equation $z_1^2 = 2a(1 - t^2)$ defines a quadric curve, say $\mathcal{Q}_1$, with a rational point $(t, z_1) = (1, 0)$. Using the standard method of the projection from the point $(1, 0)$, we can parameterize all rational points on $\mathcal{Q}_1$. In order to use this method, we put $t = uz_1 + 1$. We find the parametrization in the form

$$t = \frac{1 - 2au^2}{1 + 2au^2} =: g(u), \quad z_1 = -\frac{4au}{1 + 2au^2}.$$

Now, let us note that the curve $\mathcal{Q}_2 : z_1^2 = h(x, g(u))$ is a quadric curve defined over the field of rational functions $\mathbb{Q}(u)$. On the curve $\mathcal{Q}_2$, we have a $\mathbb{Q}(u)$-rational point $P = \left(0, \frac{g(u)-1}{u}\right)$. Similarly as in the case of the curve $\mathcal{Q}_1$, we can parameterize all $\mathbb{Q}(u)$-rational points on $\mathcal{Q}_2$. In order to do this, we put $x = v\left(z_1 + \frac{g(u)-1}{u}\right)$ and we find that

$$x = v\left(z_1 + \frac{g(u)-1}{u}\right), \quad z_1 = -\frac{4au((1+2au^2)^4 + 16au^2(1+4a^2u^4)v^2)}{(1+2au^2)((1+2au^2)^4 - 16au^2(1+4a^2u^4)v^2)}.$$

Finally, we find a two-parametric solution of the equation defining the surface $\mathcal{S}_f^2$ in the form

$$\begin{aligned}
x(u,v) &= -\frac{8au(1+2au^2)^3 v}{(1+2au^2)^4 - 16au^2(1+4a^2u^4)v^2},\\
y(u,v) &= \frac{1-2au^2}{1+2au^2}\, x(u,v),\\
z(u,v) &= -\frac{4au((1+2au^2)^4 + 16au^2(1+4a^2u^4)v^2)}{(1+2au^2)((1+2au^2)^4 - 16au^2(1+4a^2u^4)v^2)}\, x(u,v).
\end{aligned}$$

Let us define the set

$$B_a = \{(u,v) \in \mathbb{Q}^2 : (1+2au^2)((1+2au^2)^4 - 16au^2(1+4a^2u^4)v^2) = 0\},$$

which is the set where the functions x, y, z are not defined. Using the above definition of $x(u,v)$, $y(u,v)$, $z(u,v)$ and of the set B_a, then we get a rational function

$$\Phi : \mathbb{Q}^2 \setminus B_a \ni (u,v) \mapsto (x(u,v), y(u,v), z(u,v)) \in \mathbb{Q}^3.$$

Because

$$\det\begin{pmatrix} x(u,v) & y(u,v) & z(u,v)\\ \partial_u x(u,v) & \partial_u y(u,v) & \partial_u z(u,v)\\ \partial_v x(u,v) & \partial_v y(u,v) & \partial_v z(u,v)\end{pmatrix} = \frac{2^{20}a^6u^7(1+2au^2)^{10}(1+4a^2u^4)v^4}{(16au^2(1+4a^2u^4)v^2 - (1+2au^2)^4)^5}$$

is a non-zero element of the field $\mathbb{Q}(u,v)$, we see that the closure (in the Zariski topology) of the image $\operatorname{Im}\Phi$ is of dimension two in $\mathbb{C}^3$. This means that the surface $\mathcal{S}_f^2$ is unirational. $\square$

Although our main object of study is the Diophantine equation of the form $z^2 = f(x)^2 + f(y)^2$, we couldn't resist to prove the following result.

Theorem 2.5. *Let us consider the polynomial $f(X) = (aX + b)(cX + d) \in \mathbb{Z}[X]$ and suppose that the equation $f(X) = 0$ has two distinct roots. Then the set of rational parametric solutions of the Diophantine equation $f(x)^2+f(y)^2 = f(z)^2$ is infinite.*

Proof. Without loss of generality, we can assume that $f(X) = X(X + 1)$. Indeed, using the substitution $(x, y, z) \mapsto (Ax + B, Ay + B, Az + B)$, where $A = (ad-bc)/ac$ and $B = -b/a$, we can transform the equation $f(x)^2 + f(y)^2 = f(z)^2$ into the form $x^2(x+1)^2 + y^2(y+1)^2 = z^2(z+1)^2$. So we consider the surface $\mathcal{S}_f$ given by the equation

$$\mathcal{S}_f : x^2(x + 1)^2 + y^2(y + 1)^2 = z^2(z + 1)^2. \tag{3}$$

Let us define $f(x, y, z) = x^2(x + 1)^2 + y^2(y + 1)^2 - z^2(z + 1)^2$. In order to prove our theorem, let us put

$$x = T, \quad y = \frac{2t}{t^2 - 1}T, \quad z = UT, \tag{4}$$

where t, T, U are indeterminate variables. For x, y, z defined in this way we have the equality

$$f(x, y, z) = -\frac{T^2}{(t^2 - 1)^4}F_U(T),$$

where $F_U(T) = a_0T^2 + a_1T + a_2$ and

$$\begin{aligned}
a_0 &= -1 + 4t^2 - 22t^4 + 4t^6 - t^8 + (t^2 - 1)^4U^4,\\
a_1 &= 2(t^2 - 1)(1 - 3t^2 - 8t^3 + 3t^4 - t^6 + (t^2 - 1)^3U^3),\\
a_2 &= (t^2 - 1)^2(-(t^2 + 1)^2 + (t^2 - 1)^2U^2).
\end{aligned}$$

To prove Theorem 2.5, it is enough to show that the set of such $U \in \mathbb{Q}(t)$ for which the equation $F_U(T) = 0$ (treated as equation in the variable T) has roots in the field $\mathbb{Q}(t)$, is infinite. It is equivalent that the discriminant $\Delta(U) = 4\Delta'(U)$, where

$$\begin{aligned}
\Delta'(U) = {} & (U - 1)((t^2 - 1)U - 2t)\\
& \times ((t^2 - 1)(t^2 + 1)^2U^2 - (t^2 - 2t - 1)^2(t^2 + 2t - 1)U - 2t(t^2 - 2t - 1)^2),
\end{aligned}$$

of the polynomial F_U should be a square in the field $\mathbb{Q}(t)$. In other words, we must consider the curve $\mathcal{C}_f$ defined over the field $\mathbb{Q}(t)$ by the equation

$$\mathcal{C}_f : V^2 = \Delta'(U).$$

The discriminant of the polynomial $\Delta'(U)$ is equal to

$$D = 2^{12}t^6(t^2-1)^8(1+t^2)^2(t^2-4t-1)^2(t^2-2t-1)^4(t^2-t-1)^2 \\ \times (1-8t-12t^2-8t^3+38t^4+8t^5-12t^6+8t^7+t^8),$$

and due to the fact that $D \neq 0$ as an element of the field $\mathbb{Q}(t)$, we see that the curve $\mathcal{C}_f$ is smooth over $\mathbb{Q}(t)$. Let us also note that the $\mathbb{Q}(t)$-rational point $P=(U,V)=(1,0)$ lies on $\mathcal{C}_f$. If we treat Q as a point at infinity on the curve $\mathcal{C}_f$, we conclude that $\mathcal{C}_f$ is birationally equivalent over $\mathbb{Q}(t)$ to the elliptic curve with the Weierstrass equation

$$\mathcal{E}_f : Y^2 = X^3 - 27A(t)X + 54B(t),$$

where

$$\begin{aligned} A(t) &= 1-56t^2-192t^3-36t^4+192t^5-136t^6+384t^7+710t^8+ \\ &\quad -384t^9-136t^{10}-192t^{11}-36t^{12}+192t^{13}-56t^{14}+t^{16}, \\ B(t) &= (1+4t-6t^2-4t^3+t^4)(1-4t-6t^2+4t^3+t^4) \\ &\quad \times (A(t)+96t^3(t^2-1)^3(t^2-4t-1)(t^2-t-1)). \end{aligned}$$

The mapping $\varphi : \mathcal{C}_f \ni (U,V) \mapsto (X,Y) \in \mathcal{E}_f$ is given by

$$\begin{aligned} U &= \frac{144t^2(-1-2t+t^2)(-1-t+t^2)}{X-3(1+20t^2+48t^3-26t^4-48t^5+20t^6+t^8} + 1, \\ V &= \frac{48t^2(-1-2t+t^2)(-1-t+t^2)Y}{(X-3(1+20t^2+48t^3-26t^4-48t^5+20t^6+t^8)^2}. \end{aligned}$$

Note that on the curve $\mathcal{E}_f$ we have a torsion point of order two given by

$$T = (3(1+4t-6t^2-4t^3+t^4)(1-4t-6t^2+4t^3+t^4), 0).$$

Moreover on the curve $\mathcal{E}_f$, we have the point $P=(X_P, Y_P)$, where

$$\begin{aligned} X_P &= \frac{3F_1(t)}{(3+2t+2t^2-2t^3+3t^4)^2}, \\ Y_P &= \frac{432(t^2-1)^3(t^2+1)(t^2-2t-1)(t^2-t-1)(1+t+4t^2-t^3+t^4)F_2(t)}{(3+2t+2t^2-2t^3+3t^4)^3}, \end{aligned}$$

and

$$\begin{aligned} F_1(t) &= 57+156t+100t^2-148t^3-476t^4-292t^5+ \\ &\quad -612t^6+1036t^7+2886t^8-1036t^9-612t^{10} \\ &\quad +292t^{11}-476t^{12}+148t^{13}+100t^{14}-156t^{15}+57t^{16}, \end{aligned}$$

$$F_2(t) = 5 + t + 8t^2 + t^3 + 54t^4 - t^5 + 8t^6 - t^7 + 5t^8.$$

In order to finish the proof, it is enough to show that the point P is of infinite order on the curve $\mathcal{E}_f$. Now, if we specialize the curve $\mathcal{E}_f$ for $t = 2$, we obtain the elliptic curve

$$\mathcal{E}_{f,2} : Y^2 = X^3 - 1899963X + 947964438,$$

with the point

$$P_2 = \left(-\frac{658077}{2209}, -\frac{4004309520}{103823}\right),$$

which is the point P at $t = 2$. 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 [2, p. 177], while P_2 is not integral; therefore, P_2 is not a point of finite order on $\mathcal{E}_{f,2}$, which means that P is not a point of finite order on $\mathcal{E}_f$. Therefore, $\mathcal{E}_f$ is a curve of positive rank. Hence, its set of $\mathbb{Q}(t)$-rational points is infinite and our theorem is proved. $\square$

Corollary 2.6. *Let us consider the polynomial $f(X) = (aX + b)(cX + d) \in \mathbb{Z}[X]$ and suppose that the equation $f(X) = 0$ has two distinct roots. Then the set of rational points on the surface $\mathcal{S} : f(x)^2 + f(y)^2 = f(z)^2$ is dense in the Zariski topology.*

Proof. Because the curve $\mathcal{E}$ we have constructed in the proof of Theorem 2.5 is of positive rank over $\mathbb{Q}(t)$, the set of multiplicities of the point P i.e. $mP = (X_m(t),\ Y_m(t))$ for $m = 1, 2, \ldots$, gives us infinitely many $\mathbb{Q}(t)$-rational points on the curve $\mathcal{E}$. Now, if we look on the curve $\mathcal{E}$ as on the 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 $\mathcal{E}$ 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 $\mathcal{S}$. $\square$

3. The equation $z^2 = f(x)^2 \pm f(y)^2$ for some cubic functions

In this section we will solve equation (1) for most cubic polynomial functions. So we start this section with the following result in which we consider a cubic function of the form $f(X) = X(X^2 + aX + b)$ with $a \in \mathbb{Z} \setminus \{0\},\ b \in \mathbb{Z}$.

Theorem 3.1. *Let us put $f(X) = X(X^2 + aX + b)$ with $a \in \mathbb{Z} \setminus \{0\},\ b \in \mathbb{Z}$. Then the Diophantine equation $z^2 = f(x)^2 + f(y)^2$ has infinitely many rational parametric solutions defined over $\mathbb{Q}$.*

Proof. Let us note that without loss of generality we can assume that $f(X) = X(X^2 + X + c)$ where $c \in \mathbb{Q} \setminus \{0\}$. Indeed, after the change of variables $(x, y, z) \mapsto (ax, ay, a^3 z)$ we transform the surface $z^2 = x^2(x^2 + ax + b)^2 + y^2(y^2 + ay + b)^2$ into the surface with the equation $z^2 = f(x)^2 + f(y)^2$, where $f(X) = X(X^2 + X + b/a^2)$.

Let us put $f(x, y, z) = z^2 - f(x)^2 - f(y)^2$. In order to prove our theorem we put

$$x = (t^2 - 1)U, \quad y = 2tU, \quad z = UV.$$

For x, y, z defined in this way we get

$$f(x, y, z) = U^2(V^2 - F(U)),$$

where $F(U) = a_0U^4 + a_1U^3 + a_2U^2 + a_3U + a_4$, and $a_i \in \mathbb{Z}[t]$ are defined in the following way

$$\begin{aligned}
a_0 &= (t^2 + 1)^2(1 - 8t^2 + 30t^4 - 8t^6 + t^8),\\
a_1 &= 2(t^2 + 2t - 1)(1 + 2t + 2t^3 + 14t^4 - 2t^5 - 2t^7 + t^8),\\
a_2 &= (2c + 1)(1 - 4t^2 + 22t^4 - 4t^6 + t^8),\\
a_3 &= 2c(t^2 + 2t - 1)(1 + 2t + 2t^2 - 2t^3 + t^4),\\
a_4 &= c^2(t^2 + 1)^2.
\end{aligned}$$

From the above computations, we can see that in order to prove our theorem we must show that on the curve $\mathcal{C}$ defined over the field $\mathbb{Q}(t)$ by the equation

$$\mathcal{C} : V^2 = F(U),$$

there are infinitely many $\mathbb{Q}(t)$-rational points. The curve $\mathcal{C}$ is a quartic curve with rational point $Q' = (0, c(t^2 + 1))$. Using this point we can produce another point $Q = (U,\ V)$ which satisfy the condition $UV \neq 0$. Indeed, in order to construct a such point Q we put $V = pU^2 + qU + c(t^2 + 1)$, where $p,\ q$ are indeterminate variables. Then we have that $V^2 - F(U) = \sum_{i=1}^{4} f_iU^i$, where the quantities $f_i = f_i(p, q)$ are given by

$$\begin{aligned}
f_1 &= -2c(-1 - q + (3 - q)t^2 + 8t^3 - 3t^4 + t^6),\\
f_2 &= 2cp - 2c - 1 + q^2 + 2(2 + 4c + cp)t^2 - 22(2c + 1)t^4 + 4(2c + 1)t^6 - (2c + 1)t^8,\\
f_3 &= 2(1 + pq - 5t^2 + 10t^4 - 32t^5 - 10t^6 + 5t^8 - t^{10}),\\
f_4 &= -1 + p^2 + 6t^2 - 15t^4 - 44t^6 - 15t^8 + 6t^{10} - t^{12}.
\end{aligned}$$

The system of equations $f_1 = f_2 = 0$ in p, q has a solution given by

$$p = \frac{2t^2(1+2t-2t^2-2t^3+t^4)^2 + c(t^2+1)^2(1-4t^2+22t^4-4t^6+t^8)}{c(t^2+1)^3},$$

$$q = \frac{(t^2+2t-1)(t^4-2t^3+2t^2+2t+1)}{t^2+1}.$$

This implies that the equation $\sum_{i=1}^{4} f_i U^i = 0$ has double root $T = 0$ and a rational root $T = -f_3(p,q)/f_4(p,q)$, where p, q are given above. It is easy to check that for $c \in \mathbb{Q} \setminus \{0\}$ we have $f_4 \neq 0$ as an element of $\mathbb{Q}(t)$. So, we get that the $\mathbb{Q}(t)$-rational point

$$Q = (U_Q, V_Q) = \left(-\frac{f_3}{f_4}, \frac{pf_3^2 - qf_3f_4 + cf_4^2 + ct^2f_4^2}{f_4^2}\right) \tag{5}$$

lies on the curve $\mathcal{C}$. We do not give the exact values of the coordinates of the point Q because they are huge rational functions. Note that for the coordinates U, V of the point Q we have $UV \neq 0$ for any choice of $c \in \mathbb{Q}$. Later we will use the point Q in order to finish the proof of our theorem.

Now, we construct an appropriate map from $\mathcal{C}$ to an elliptic curve $\mathcal{E}$ with Weierstrass equation. In order to construct the desired mapping we treat $Q' = (0, c(t^2+1))$ as a point at infinity on the curve $\mathcal{C}$ and we use the method described in [1, p. 77]. One more time, we conclude that $\mathcal{C}$ is birationally equivalent over $\mathbb{Q}(t)$ to the elliptic curve with the Weierstrass equation

$$\mathcal{E} : Y^2 = X^3 - 27A(t)X - 54(4c-1)(1-4t^2+22t^4-4t^6+t^8)B(t),$$

where $A(t) = \sum_{i=0}^{16} A_i(c)t^i$, $B(t) = \sum_{i=0}^{16} B_i(c)t^i$. Because $A_i(c) = (-1)^i A_{16-i}(c)$ and $B_i(c) = (-1)^i B_{16-i}(c)$ it is enough to know A_i, B_i for $i = 1, 2, \ldots, 8$. These coefficients are given below.

$$A_0(c) = (4c-1)^2, \qquad B_0(c) = (4c-1)^2,$$

$$A_1(c) = 0, \qquad B_1(c) = 0,$$

$$A_2(c) = -8(10c^2-8c+1), \qquad B_2(c) = -8(c-1)(7c-1),$$

$$A_3(c) = 96c, \qquad B_3(c) = 144c,$$

$$A_4(c) = 12(24c^2-8c+5), \qquad B_4(c) = -12(2c-5)(2c+1),$$

$$A_5(c) = -96c, \qquad B_5(c) = -144c,$$

$$A_6(c) = 8(10c^2 - 8c - 23), \qquad B_6(c) = 8(199c^2 - 104c - 23),$$
$$A_7(c) = -192c, \qquad B_7(c) = -288c,$$
$$A_8(c) = 2(1744c^2 - 920c + 259), \quad B_8(c) = 2(544c^2 - 344c + 259).$$

The mapping $\varphi : \mathcal{E} \ni (X, Y) \mapsto (U, V) \in \mathcal{C}$ is given by

$$\begin{aligned} U &= 2c^2(t^2+1)^2 \\ &\quad\times \left(\frac{2c^3(t^2+1)^3 Y - 27D(t)}{6(c^2(t^2+1)^2 X - 9C(t))} - c(t^2+2t-1)(1+2t+2t^2-2t^3+t^4) \right)^{-1}, \\ V &= -\frac{9}{4c^3(t^2+1)^3U^2} \left(\frac{2c^2(1+t^2)}{U} + c(t^2+2t-1)(1+2t+2t^2-2t^3+t^4) \right)^2 \\ &\quad + \frac{1}{36c^3(t^2+1)^3U^2}(2c^2(t^2+1)^2X + 9C(t)), \end{aligned}$$

where

$$\begin{aligned} C(t) &= -\frac{c^2}{3}((4c-1)t^{12} - 2(4c-7)t^{10} - 48t^9 + 15(4c-1)t^8 + 144t^7 \\ &\qquad + 12(12c-5)t^6 - 144t^5 + 15(4c-1)t^4 + 48t^3 - 2(4c-7)t^2 + 4c - 1), \\ D(t) &= 8c^3t^2(t^2-1)^2(t^2-2t-1)^2(t^2+2t-1) \\ &\qquad \times ((2c-1)t^4 + 2t^3 + 2(2c-1)t^2 - 2t + 2c - 1). \end{aligned}$$

Let us note that on the curve $\mathcal{E}$ we have a $\mathbb{Q}(t)$-rational point of order two given by

$$T = (-3(4c-1)(1-4t^2+22t^4-4t^6+t^8),\ 0).$$

Now, we will show that the point

$$P = (X_P, Y_P) = \varphi^{-1}(Q) = \varphi^{-1}((U_Q, V_Q)),$$

where Q is defined by (5), is of infinite order on the curve $\mathcal{E}$. In order to do this, let us put $t = -2$ and consider the point

$$\begin{aligned} Q_{-2} = \Bigg(&\frac{25c(50c-37)}{625c^2 - 8425c - 1764}, \\ &\frac{5c(5526612 + 19933200c + 62865000c^2 + 9375000c^3 + 390625c^4)}{(625c^2 - 8425c - 1764)^2} \Bigg), \end{aligned}$$

which is the point Q at $t = -2$. It is clear that the point Q_{-2} lies on the curve $\mathcal{C}_{-2}$ which is the curve $\mathcal{C}$ at $t = -2$. We have that the point $P_{-2} = \varphi^{-1}(Q_{-2}) = (X_{P,-2}, Y_{P,-2})$, where

$$X_{P,-2} = \frac{3(48874177 + 240212200c + 847212500c^2 + 28250000c^3 + 4687500c^4)}{25(50c-37)^2},$$

$$Y_{P,-2} = \frac{108(25c+6)(25c+294)G(c)}{125(50c-37)^3},$$

$$G(c) = 781250c^4 - 2312500c^3 - 148214375c^2 - 36125700c - 8638308,$$

is the point $P = \varphi^{-1}(Q)$ at $t = -2$ and lies on the curve $\mathcal{E}_{-2}$. If $c = p/q \in \mathbb{Q}$, with $\mathrm{GCD}(p,q) = 1$, satisfies the condition $(50c-37)(25c+6)(25c+294) \neq 0$ then the coordinates of the point $P'_{-2} = (q^2 X_{P,-2}, q^3 Y_{P,-2})$ are not integers. Moreover the point P'_{-2} lies on the curve

$$\begin{aligned}\mathcal{E}'_{-2} : Y^2 = X^3 &- 27q^2(113569q^2 + 107512pq + 1901776p^2)X + \\ &- 18198q^3(4p-q)(113569q^2 + 615544pq + 1944112p^2).\end{aligned}$$

The curve $\mathcal{E}'_{-2}$ is isomorphic to $\mathcal{E}$ by the transformation $(X,Y) \mapsto (q^2X, q^3Y)$ and the point P'_{-2} is the image of the point P_{-2} under this transformation. So P'_{-2} is not integral on the curve $\mathcal{E}'_{-2}$. Using now Nagell–Lutz theorem we get that the point P'_{-2} is not of finite order on the curve $\mathcal{E}'_{-2}$, thus the point P_{-2} is not of finite order on the curve $\mathcal{E}_{-2}$. Finally, one can see that the $\mathbb{Q}(t)$-rational point P is not of finite order on the curve $\mathcal{E}$. Therefore, we exclude three rational values of c in order to prove that the point P_{-2} is not of finite order. But is easy to see that in order to cover these values we can take another specialization at $t = t_0$, where t_0 is a suitable chosen integer. For example we can take $t = 8$ and then we exclude only $c = 3217/8450$ and in particular we cover these values of c for which $(50c-37)(25c+6)(25c+294) = 0$. This observation finishes the proof of our theorem. □

Using a similar method we will prove the following result.

Theorem 3.2. *Let us put $f(X) = X(X^2 + aX + b)$ with $a \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{Z}$. Then the Diophantine equation $z^2 = f(x)^2 - f(y)^2$ has infinitely many rational parametric solutions defined over $\mathbb{Q}$.*

Proof. Similarly as in the proof of previous theorem we can assume that $f(X) = X(X^2+X+c)$ where $c \in \mathbb{Q}\setminus\{0\}$. Let us put $f(x,y,z) = z^2 - f(x)^2 + f(y)^2$. In order to prove our theorem we put

$$x = (t^2+1)U, \quad y = 2tU, \quad z = (t-1)UV.$$

For x, y, z defined in this way we get

$$f(x,y,z) = (t-1)^2U^2(V^2 - G(U)),$$

where

$$\begin{aligned} G(U) = {} & ((1+2t+6t^2+2t^3+t^4)U^2 + (t+1)^2U + c) \\ & \times ((1+t)^2(1-2t+6t^2-2t^3+t^4)U^2 + (1+6t^2+t^4)U + c(t+1)^2)). \end{aligned}$$

From the above computations, we can see that in order to prove our theorem we must show that on the curve $\mathcal{C}$ defined over the field $\mathbb{Q}(t)$ by the equation

$$\mathcal{C} : V^2 = G(U),$$

there are infinitely many $\mathbb{Q}(t)$-rational points. The curve $\mathcal{C}$ is a quartic curve with rational point $Q = (0, c(t+1))$. We treat $Q = (0, c(t+1))$ as a point at infinity on the curve $\mathcal{C}$ and we use the method described in [1, p. 77]. One more time, we conclude that $\mathcal{C}$ is birationally equivalent over $\mathbb{Q}(t)$ to the elliptic curve with the Weierstrass equation

$$\mathcal{E} : Y^2 = X^3 - 27A(t)X - 54(4c-1)(t+1)^2(1+6t^2+t^4)B(t),$$

where $A(t) = \sum_{i=0}^{12} A_i(c)t^i$, $B(t) = \sum_{i=0}^{12} B_i(c)t^i$. Because $A_i(c) = A_{12-i}(c)$ and $B_i(c) = B_{12-i}(c)$ it is enough to know A_i, B_i for $i = 1, 2, \dots, 6$. These coefficients are given below.

$$\begin{aligned} A_0(c) &= (4c-1)^2, & B_0(c) &= (4c-1)^2, \\ A_1(c) &= 4(4c-1)^2, & B_1(c) &= 4(4c-1)^2, \\ A_2(c) &= 6(40c^2-24c+3), & B_2(c) &= 18(2c-1)(6c-1), \\ A_3(c) &= 4(160c^2-80c+13), & B_3(c) &= 4(136c^2-68c+13), \\ A_4(c) &= 3(464c^2-296c+37), & B_4(c) &= 3(400c^2-296+37), \\ A_5(c) &= 8(328c^2-164c+25), & B_5(c) &= 8(292c^2-146c+25), \\ A_6(c) &= 84(40c^2-24c+3), & B_6(c) &= 252(2c-1)(6c-1). \end{aligned}$$

The mapping $\varphi : \mathcal{E} \ni (X,Y) \mapsto (U,V) \in \mathcal{C}$ is given by

$$U = \left(\frac{2(t+1)^3Y - 27D(t)}{12c(t+1)^2((t+1)^2X - 9C(t))} - \frac{1+2t+6t^2+2t^3+t^4}{2c(t+1)^2} \right)^{-1}$$

$$V = \frac{U^2}{4c(t+1)^3}\Bigg(-4c^2(t+1)^4\left(U^{-1} + \frac{1+2t+6t^2+2t^3+t^4}{2c(t+1)^2}\right)^2 + \frac{2(t+1)^2X}{9} + C(t)\Bigg).$$

where

$$\begin{aligned} C(t) &= \frac{1}{3}\big((1-4c)(t^8+1) + 4(1-4c)t(t^6+1) \\ &\quad + 24(1-2c)t^2(t^4+1) + 28(1-4c)t^3(t^2+1) + 2(31-76c)t^4\big), \\ D(t) &= -8t^2(t^2+1)^2((2c-1)(t^4+1) + 2(4c-1)t(t^2+1) + 6(2c-1)t^2). \end{aligned} \tag{6}$$

Let us note that on the curve $\mathcal{E}$ we have two $\mathbb{Q}(t)$-rational points: the point of order two given by

$$T = (-3(4c-1)(t+1)^2(t^4+6t^2+1),\ 0),$$

and the point

$$P = (X_P,\ Y_P) = \left(\frac{9C(t)}{(t+1)^2},\ \frac{27D(t)}{2(t+1)^3}\right),$$

where $C(t)$, $D(t)$ are given by (6). We will show that the point P is of infinite order on the curve $\mathcal{C}$. In order to do this, let us specialize the curve $\mathcal{E}$ at $t = 2$ and let us consider a rational number $c = p/q$ with $\mathrm{GCD}(p,q) = 1$. Then the curve

$$\begin{aligned} \mathcal{E}_2' : Y^2 = X^3 &- 81q^2(596592p^2 - 331096pq + 45387q^2)X + \\ &- 179334(4p-q)q^3(177264p^2 - 105032pq + 15129q^2) \end{aligned}$$

has the point $P_2' = (-(4428p - 1507q)q, -400(162p - 61q)q^2)$. The curve $\mathcal{E}_2'$ is isomorphic to $\mathcal{E}_2$ by the transformation $(X,Y) \mapsto (q^2X, q^3Y)$ and the point P_2' is the image of the point P_2 under this transformation. We have that

$$\begin{aligned} 2P_2' = \Bigg(&T - (4428p - 1507q)q, \\ &-\frac{3(4374p^2 - 5508pq + 1307q^2)}{162p - 61q}T - 400(162p - 61q)q^2\Bigg), \end{aligned}$$

where

$$T = \frac{12(6561p^2 - 710q^2)(2187p^2 - 1080pq + 170q^2)}{(162p - 61q)^2}.$$

We see that for all but finitely many $p,q\in\mathbb{Z}\setminus\{0\}$ with $\mathrm{GCD}(p,q)=1$ the point $2P_2'$ is not integral. Therefore, from Nagell–Lutz theorem we deduce that the point P_2' is of infinite order on the curve $\mathcal{E}_2'$. Finally, we deduce that the point P is not of finite order on the curve $\mathcal{E}$. We exclude some values of $c=p/q$ in order to prove that the point P_2' is not of finite order. But is easy to see that in order to cover these values we can take another specialization at $t=t_0$, where t_0 is suitable chosen integer. Thus our theorem is proved. □

A natural question arises whether similar results could be proved for irreducible cubic polynomials. We prove the following result.

Theorem 3.3. *Let us put $f(X)=X^3+aX^2+b$ with $a\in\mathbb{Z}\setminus\{0\},\ b\in\mathbb{Z}$. Then the Diophantine equation $z^2=f(x)^2-f(y)^2$ has infinitely many rational parametric solutions defined over $\mathbb{Q}$.*

Proof. Let us note that without loss of generality we can assume that $f(X)=X^3+X^2+c$ where $c\in\mathbb{Q}\setminus\{0\}$. Indeed, after change of variables $(x,y,z)\mapsto(ax,ay,a^3z)$ we transform the surface $z^2=(x^3+ax^2+b)^2-(y^3+ay^2+b)^2$ into the surface with the equation $z^2=f(x)^2-f(y)^2$, where $f(X)=X^3+X^2+b/a^3$.

Let us put $f(x,y,z)=z^2-(f(x)^2-f(y)^2)$. In order to prove our theorem, we put

$$x=(t^2+2c)U,\quad y=(t^2-2c)U,\quad z=UV.$$

For x, y, z defined in this way, we get

$$f(x,y,z)=U^2(V^2-F(U)),$$

where

$$F(U)=8c(2t^2+(4c^2+3t^4)U)(c+(4c^2+t^4)U^2+t^2(12c^2+t^4)U^3).$$

So, we see that in order to prove our theorem we must consider a quartic curve $\mathcal{C}:V^2=F(U)$ defined over the field $\mathbb{Q}(t)$. Note that on the curve $\mathcal{C}$ we have two $\mathbb{Q}(t)$-rational points: $Q'=(-2t^2/(4c^2+3t^4),\ 0)$ and $Q=(0,4ct)$. We treat the point Q' as a point at infinity on the curve $\mathcal{C}$ and we conclude that $\mathcal{C}$ is birationally equivalent over $\mathbb{Q}(t)$ with an elliptic curve given by the Weierstrass equation

$$\mathcal{E}:Y^2=X^3+108c^2f(t^4)X+216c^3t^2g(t^4),$$

where

$$f(t)=192c^7-16c^4(33c+4)t-4c^2(135c+8)t^2-(27c+4)t^3,$$

$$\begin{aligned}g(t)&=2304c^9(9c+4)+256c^6(4-9c+189c^2)t\\&\quad+96c^4(8+222c+405c^2)t^2+48c^2(9c+1)(27c+4)t^3+(27c+4)^2t^4.\end{aligned}$$

The mapping $\varphi : \mathcal{E} \ni (X, Y) \mapsto (U, V) \in \mathcal{C}$ is given by

$$U = \frac{2(-t^2X + 144c^6 + 24c^3(9c+2)t^4 + 3c(27c+4)t^8)}{96c^3t^2(4c^2 - 5t^4) + (4c^2 + 3t^4)X},$$
$$V = \frac{12c(64c^7 + 16c^4(9c+4)t^4 + 4c^2(27c-8)t^8 + (27c+4)t^{12})Y}{(96c^3t^2(4c^2 - 5t^4) + (4c^2 + 3t^4)X)^2}.$$

Now we will show that $\mathcal{E}$ has a positive rank over $\mathbb{Q}(t)$. In order to do this, we consider the point $P = \varphi^{-1}(Q) = (X_P, Y_P)$, where

$$X_P = \frac{3c(48c^5 + 8c^2(9c+2)t^4 + (27c+4)t^8)}{t^2},$$
$$Y_P = \frac{27c^2(64c^7 + 16c^4(9c+4)t^4 + 4c^2(27c-8)t^8 + (27c+4)t^{12})}{t^3}.$$

Let us note that for any choice of rational number $c = p/q$ the polynomials $108q^9c^2f(t^4)$ and $216q^{13}c^3t^3g(t^4)$ have integer coefficients. These polynomials are coefficients of elliptic curve $\mathcal{E}'$ which is isomorphic to the $\mathcal{E}$ by the transformation $(X,\ Y) \mapsto (q^4X, q^6Y)$. Now, we can choose an integer $t = t_0$ such that the point $P'_{t_0} = (q^3X_{P,t_0}, q^6Y_{P,t_0})$ is not an integral point on the curve $\mathcal{E}'_{t_0}$. Using now Nagell–Lutz theorem we get that the point P'_{t_0} is not of finite order on the curve $\mathcal{E}'_{t_0}$, thus the point P' is not of finite order on the curve $\mathcal{E}'$. Finally, one can see that the $\mathbb{Q}(t)$-rational point P is not of finite order on the curve $\mathcal{E}$. This completes the proof of our theorem. $\square$

In the view of the above theorem and the results of this section we state the following

Question 3.4. Does it exist an irreducible polynomial $f \in \mathbb{Q}[X]$ of degree three such that the equation $z^2 = f(x)^2 + f(y)^2$ has infinitely many solutions in rationals?

4. Some other results

In the previous section, we have proved that for most cubic polynomials, the Diophantine equations $z^2 = f(x)^2 \pm f(y)^2$ have infinitely many rational parametric solutions. What's about quartic polynomial functions? We prove the following result.

Theorem 4.1. *Let $a \in \mathbb{Z}\setminus\{0\}$. Suppose that there exists a non-zero rational number t such that the curve*

$$\mathcal{C}_t : V^2 = (1 - t^8)U^4 + 2a(1 - t^4)$$

has infinitely many rational points. Then the set of rational solutions of the Diophantine equation $z^2 = (x^4+a)^2-(y^4+a)^2$ satisfying the conditions $0 < y < x$, $z \neq 0$, is infinite.

Proof. Let us put $f(x, y, z) = z^2 - ((x^4 + a)^2 - (y^4 + a)^2)$. From the assumption, we know that there is a rational number $t \neq 0$ such that the set of rational points on the curve $\mathcal{C}_t$ is infinite. Moreover we know that for all but finitely many points on the curve $\mathcal{C}_t$ with coordinates U, V we have $UV \neq 0$. Note the following identity

$$f(U, tU, U^2V) = U^4(V^2 - (1 - t^8)U^4 - 2a(1 - t^4)).$$

Therefore, we conclude that if (U, V) is the rational point on the curve $\mathcal{C}_t$ than the triple $(x, y, z) = (U, tU, U^2V)$ is a rational solution of the Diophantine equation $z^2 = (x^4 + a)^2 - (y^4 + a)^2$. □

In the view of the above theorem, it is natural to ask the following question.

Question 4.2. Let us take $a \in \mathbb{Z}\setminus\{0\}$. Is it possible to find a rational number t such that the set of rational points on the curve

$$\mathcal{C}_t : V^2 = (1 - t^8)U^4 + 2a(1 - t^4)$$

is infinite?

Finally, one can thing about the following general question.

Question 4.3. Does there exist a polynomial $f \in \mathbb{Q}[X]$ of degree greater than three without multiple roots such that the equation $z^2 = f(x)^2 + f(y)^2$ has infinitely many solutions in rational numbers?

Acknowledgments. The authors express their gratitude to the anonymous referee for constructive suggestions to improve an earlier draft of this paper.

References

[1] L. J. Mordell, Diophantine Equations, *Academic Press*, *London*, 1969.

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

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

[4] M. Ulas, Rational points on certain elliptic surfaces, *Acta Arith.* **129** (2007), 167–185.

MACIEJ ULAS
INSTITUTE OF MATHEMATICS
JAGIELLONIAN UNIVERSITY
ŁOJASIEWICZA 6
30-348 KRAKÓW
POLAND

AND

INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
ŚNIADECKICH 8
00-950 WARSZAWA
POLAND

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

ALAIN TOGBÉ
MATHEMATICS DEPARTMENT
PURDUE UNIVERSITY NORTH CENTRAL
1401 S, U.S. 421
WESTVILLE IN 46391
USA

E-mail: atogbe@pnc.edu

(Received January 9, 2009)