On the classical diophantine equation $x^4 + y^4 + kx^2y^2 = z^2$

Cite as: AIP Conference Proceedings **2333**, 110002 (2021); https://doi.org/10.1063/5.0042739
Published Online: 08 March 2021

Miroslav Stoenchev, and Venelin Todorov

On the Classical Diophantine Equation $x^4 + y^4 + kx^2y^2 = z^2$

Miroslav Stoenchev[1,a)] and Venelin Todorov[2,3,b)]

[1]*Department of Mathematics, Technical University, Sofia, Bulgaria*
[2]*Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria*
[3]*Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, Sofia, Bulgaria*

[a)]Corresponding author: mrs@tu-sofia.bg
[b)]venelin@parallel.bas.bg, vtodorov@math.bas.bg

Abstract. The purpose of this article is to describe parametrically all nontrivial solutions of the diophantine equation in the title. One parameter family of elliptic curves is naturally associated with the equation, for which family we apply "*complete 2-descend*" algorithm to obtain a parametric description of all possible values of parameter $k \in \mathbb{Z}$, for which nontrivial solutions exist. The article is a natural continuation of [1].

INTRODUCTION

We consider the diophantine equation $x^4 + y^4 + kx^2y^2 = z^2$, where $k \in \mathbb{Z}$ is a parameter. Our aim is to determine the integers k for which the equation has a solution in positive integers (x, y, z) and to describe parametrically all solutions. Each diophantine equation can be considered as an equation that defines affine variety in the corresponding affine space, or after homogenization, projective variety in the corresponding projective space. Thus the initial equation defines affine surface in a three dimensional affine space over algebraic closure of $\mathbb{Q}$, denoted by

$$T_k = \{(x, y, z) \in \mathbb{A}^3(\overline{\mathbb{Q}}) \mid x^4 + y^4 + kx^2y^2 = z^2\} \text{ or } T_k : \ x^4 + y^4 + kx^2y^2 = z^2,$$

and for the corresponding projective case, after homogenization with introducing a new variable t, the notation is:

$$T_k = \{[x, y, z, t] \in \mathbb{P}^3(\overline{\mathbb{Q}}) \mid x^4 + y^4 + kx^2y^2 = z^2t^2\} \text{ or } T_k : \ x^4 + y^4 + kx^2y^2 = z^2t^2$$

For convenience, we will use affine equations, but with the comprehension that we work with projective varieties (curves and surfaces). The difference is at the points at infinity, given by intersection of projective variety with the hyperplane at infinity $H_\infty : \ t = 0$.
Basic objects of consideration are smooth projective curves and surfaces, and the main apparatus is related to algebraic and analytic invariants of elliptic curves.

BASIC DEFINITIONS

In this section are given definitions of affine and projective spaces, elliptic curves over an arbitrary field, and the structure preserving maps between elliptic curves. The following definitions are necessary ([4],[8],[9],[13]).

Definition 1 *Affine n-space over* $\mathbb{Q}$ *is the set* $\mathbb{A}^n(\overline{\mathbb{Q}}) = \{(x_1, x_2, \dots, x_n) \mid x_i \in \overline{\mathbb{Q}}\}$.

The zero point of $\mathbb{A}^n$ is $O_{\mathbb{A}^n} = (0, \dots, 0)$, and if A, B are sets then $A - B$ means the set-theoretical subtraction.

Definition 2 *Projective n-space over* $\mathbb{Q}$*, denoted by* $\mathbb{P}^n$*, is the quotient space* $(\mathbb{A}^{n+1}(\overline{\mathbb{Q}}) - O_{\mathbb{A}^{n+1}})/ \sim$*, where the factorization by* $\sim$ *means that the points* $(x_0, \dots, x_n)$, $(y_0, \dots, y_n) \in \mathbb{A}^{n+1}(\overline{\mathbb{Q}}) - O_{\mathbb{A}^{n+1}}$ *are equivalent, if there exists* $\lambda \in \overline{\mathbb{Q}}^*$*, such that* $y_0 = \lambda x_0, \dots, y_n = \lambda x_n$*. An equivalence class* $\{(\lambda x_0, \dots, \lambda x_n) \mid \lambda \in \overline{\mathbb{Q}}^*\}$ *is denoted by* $[x_0, \dots, x_n]$*, and the individual* $x_0, \dots, x_n$ *are called homogeneous coordinates for the corresponding point of* $\mathbb{P}^n$.

Applications of Mathematics in Engineering and Economics (AMEE'20)
AIP Conf. Proc. 2333, 110002-1–110002-14; https://doi.org/10.1063/5.0042739
Published by AIP Publishing. 978-0-7354-4077-7/$30.00

Thus, the projective space consists of lines through the origin in affine space, with one dimension higher.

Definition 3 *Elliptic curve over $\mathbb{Q}$ is a smooth projective curve with affine equation*

$$y^2 = x^3 + ax^2 + bx + c, \tag{1}$$

where $a, b, c \in \mathbb{Q}$. In general, elliptic curve E over field k is denoted by E/k.

The smoothness condition is equivalent to the condition that the polynomial $x^3 + ax^2 + bx + c$ has distinct roots. The unique point at infinity that lies on the elliptic curve is denoted by $O = [0, 1, 0]$. The discriminant of $E/k: \; y^2 = f(x)$ given by (1) is defined as $\Delta_E = 16\Delta_f = 16(-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2)$.

Let $E/\mathbb{Q}$ be an elliptic curve given by equation (1). Therefore $E \subset \mathbb{P}^2(\overline{\mathbb{Q}})$ consists of the points $P = (x, y)$ satisfying the equation (1), together with the point at infinity $O = [0, 1, 0]$. Let $l \subset \mathbb{P}^2(\overline{\mathbb{Q}})$ be a line, then by Bezout's theorem, the number of points of intersection for $l \cap E$, taken with multiplicities, is exactly 3, say P, Q, R (need not be distinct). The definition of composition law $\oplus$ on elliptic curve E is as follows:

Definition 4 *The composition law $E \times E \longrightarrow E \quad (P, Q) \longmapsto -R$, is denoted by $P \oplus Q := -R$, where the map $E \longrightarrow E \quad P = (x, y) \longmapsto -P = (x, -y)$ is an orthogonal symmetry with respect to the coordinate axis.*

Remark 1 *The composition law is in fact a group law, i.e. makes E into an abelian group, with $O = [0, 1, 0]$ as neutral element for the group operation, and each element P has inverse $-P$. By the definition above, it follows that three points on E have zero sum, if and only if they lie on the same line.*

As notation : $E = E(\overline{\mathbb{Q}}) = \{(x, y) \in \mathbb{A}^2(\overline{\mathbb{Q}}) \mid y^2 = x^3 + ax^2 + bx + c\} \cup \{O\}$, and for every subfield $k \subset \overline{\mathbb{Q}}$ denote by $E(k)$ the set of k-rational points on E:

$$E(k) = \{(x, y) \in \mathbb{A}^2(k) \mid y^2 = x^3 + ax^2 + bx + c\} \cup \{O\}. \tag{2}$$

For elliptic curve E/k, the set $E(k)$ is a group, $E(k) \triangleleft E(\overline{\mathbb{Q}})$, in particular let $k = \mathbb{Q}$:

Definition 5 *The group $E(\mathbb{Q})$ is called the Mordell-Weil group of rational points on E.*

Elliptic curves have an algebraic structure as abelian groups and a geometric structure as smooth projective curves. The structure preserving maps between elliptic curves are called *isogenies*. Let k be a field and E/k be an elliptic curve, given by equation $f(x, y, z) = x^3 + ax^2z + bxz^2 + cz^3 - y^2z = 0$.

Definition 6 *The function field $k(E)$ of elliptic curve E/k consists of rational functions $\frac{g}{h}$, where*
1) $g,\ h \in k[x, y, z]$ are homogeneous polynomials of the same degree,
2) $h \notin (f)$, i.e. h is not divisible by f,
3) $\frac{g_1}{h_1}$ and $\frac{g_2}{h_2}$ are considered equivalent whenever $g_1h_2 - g_2h_1 \in (f)$.

Definition 7 *Let E_1/k and E_2/k be elliptic curves. A rational map $\varphi : E_1 \longrightarrow E_2$ is a projective triple $\varphi = [\varphi_1, \varphi_2, \varphi_3] \in \mathbb{P}^2(k(E_1))$, such that for every point $P \in E_1(\overline{k})$, where $\varphi_1(P), \varphi_2(P), \varphi_3(P)$ are defined, are not all zero and the projective point $[\varphi_1(P), \varphi_2(P), \varphi_3(P)]$ lies in $E_2(\overline{k})$. The map φ is regular at P if there exists $\lambda \in k(E_1)^*$, such that $\lambda\varphi_1, \lambda\varphi_2, \lambda\varphi_3$ are defined at P and are not all zero at P. Everywhere regular rational map is called a morphism.*

Remark 2 *Every rational map between elliptic curves is a morphism and every morphism between smooth projective curves is either constant or surjective.*

Let E_1/k and E_2/k be elliptic curves.

Definition 8 *An isogeny* $\varphi : E_1 \longrightarrow E_2$ *is a surjective morphism of curves that induces a group homomorphism* $E_1(\bar{k}) \longrightarrow E_2(\bar{k})$. *The elliptic curves* E_1 *and* E_2 *are then said to be isogenous.*

Example 1 *For* $m \in \mathbb{N}$ *denote by* $[m]P := P \oplus P \oplus \cdots \oplus P$ *(m - times addition). The map* $[m] : E \longrightarrow E \quad P \longmapsto [m]P$ *is an isogeny. Denote its kernel by* $E[m]$. *The elements of* $E[m]$ *are called m-torsion points of E. For* E/k *with* $char\, k = 0$ *holds that* $E[m] \cong \mathbb{Z}/m\mathbb{Z} \bigoplus \mathbb{Z}/m\mathbb{Z}$.

Remark 3 *Let* $\varphi : E_1 \longrightarrow E_2$ *be an isogeny. Then there exists a unique isogeny* $\tilde{\varphi} : E_2 \longrightarrow E_1$ *satisfying* $\tilde{\varphi} \circ \varphi = [m]$ *and* $\varphi \circ \tilde{\varphi} = [m]$, *for appropriate positive integer m. The isogeny* $\tilde{\varphi}$ *is called dual isogeny for* φ, *and the integer m is called degree of* φ.

BASIC THEOREMS

The Structure of Mordell-Weil Group

Let $E/\mathbb{Q}$ be an elliptic curve.

Theorem 1 *The Mordell-Weil group* $E(\mathbb{Q})$ *is finitely generated and abelian.*

Theorem 2 *Every finitely generated abelian group A is a direct sum of a free subgroup and a torsion subgroup, i.e.* $A = A_{free} \bigoplus A_{torsion} \cong \mathbb{Z}^r \bigoplus A_{torsion}$, *where the integer* $r \geq 0$ *is called rank of A and is denoted by* $\text{rank}\, A = r$.

Remark 4 *From the theorems above it follows that* $E(\mathbb{Q}) \cong \mathbb{Z}^r \bigoplus E(\mathbb{Q})_{tor}$.

Theorems for Torsions

The torsion group $E(\mathbb{Q})_{tor}$ is finite and effectively computable by algorithms as *Lutz-Nagell* theorem, the *reduction* theorem and the general theorem of *Mazur*. The necessary definitions for $\mathbb{Q}_p$, $\mathbb{Z}_p$, $\mathbb{F}_p$ and the reduction map modulo p are given in the Appendix.

Theorem 3 *(Lutz-Nagell) Let* $E : y^2 = x^3 + ax^2 + bx + c$ *be an elliptic curve with integer coefficients and* $P = (x, y)$ *be a torsion point of E. Then x and y are integers, and either* $y = 0$ *or* y^2 *is a divisor of the discriminant* Δ *of polynomial* $f(x) = x^3 + ax^2 + bx + c$. $(\Delta_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2)$

Theorem 4 *(Reduction) Let p be a prime number, m be a positive integer not divisible by p, and* $E/\mathbb{Q}_p$ *be an elliptic curve. If the reduction modulo p* $E/\mathbb{Q}_p \longrightarrow \tilde{E}/\mathbb{F}_p$ *gives a nonsingular curve* $\tilde{E}/\mathbb{F}_p$, *then the reduction map* $E(\mathbb{Q}_p)[m] \longrightarrow \tilde{E}(\mathbb{F}_p)$ *is an injective homomorphism of groups.*

Theorem 5 *(Mazur) Let* $E/\mathbb{Q}$ *be an elliptic curve. Then the torsion group* $E(\mathbb{Q})_{tor}$ *is isomorphic to one of the following fifteen groups:*

$$\mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 10 \text{ or } n = 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \qquad 1 \leq n \leq 4.$$

Theorems for the Rank

In general, an effective algorithm for determining the rank of every elliptic curve over $\mathbb{Q}$, for finite amount of time, is not known. In the case, when all two-torsions for $E/\mathbb{Q}$ are rational, i.e. $E[2] = E(\mathbb{Q})[2]$, one rank searching algorithm is the *Complete 2-Descent* ([8]), formulated as two theorems with common assumptions:

Theorem 6 ***(Complete 2-Descent)*** *Let* $E/\mathbb{Q} : y^2 = (x - e_1)(x - e_2)(x - e_3),\ e_1, e_2, e_3 \in \mathbb{Q}$ *be an elliptic curve. Let S be a finite set of primes, including* $2, \infty$ *and all primes that divide the discriminant of E.*
Let $\mathbb{Q}(S, 2) = \{b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 \mid ord_p(b) \equiv 0 \bmod 2\ \forall p \notin S\}$. *Then there is injective group homomorphism*

$$E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2),$$

defined by

$$P=(x,y)\longmapsto\begin{cases}(x-e_1,\ x-e_2), & x\neq e_1,e_2\\ \left(\frac{e_1-e_3}{e_1-e_2},\ e_1-e_2\right), & x=e_1\\ \left(e_2-e_1,\ \frac{e_2-e_3}{e_2-e_1}\right), & x=e_2\\ (1,1), & P=O\end{cases}$$

Theorem 7 *(**Complete 2-Descent**) Let $(b_1,b_2)\in\mathbb{Q}(S,2)\times\mathbb{Q}(S,2)$ be a pair that is not an image of any of the points O, $(e_1,0)$, $(e_2,0)$, $(e_3,0)$. Then (b_1,b_2) is the image of a point $P=(x,y)\in E(\mathbb{Q})/2E(\mathbb{Q})$ if and only if, the equations*

$$b_1z_1^2-b_2z_2^2=e_2-e_1,\quad b_1z_1^2-b_1b_2z_3^2=e_3-e_1,$$

have a solution $(z_1,z_2,z_3)\in\mathbb{Q}^*\times\mathbb{Q}^*\times\mathbb{Q}^*$. If such a solution exists, then

$$P=(x,y)=(b_1z_1^2+e_1,\ b_1b_2z_1z_2z_3).$$

Remark 5 *Complete 2-Descent algorithm has a geometric interpretation: the two equations in theorem 7 define quadric surfaces in $\mathbb{P}^3$, which intersect in smooth quartic curve in $\mathbb{P}^3$, called a homogeneous space for $E/\mathbb{Q}$.*
In the case when $E[2]\neq E(\mathbb{Q})[2]$, the general algorithm for determining the rank of an elliptic curve uses Selmer and Shafarevich-Tate groups ([6],[8]).

Theorem 8 *The rank is invariant under isogeny maps, hence isogenous elliptic curves have the same rank.*

RESULTS

The Main Idea

Let E_k, E'_k and H_k be the curves with affine equations:

$$E_k:\ Y^2=X(X-k+2)(X-k-2),$$

$$E'_k: y'^2=x'(x'^2+kx'+1),$$

$$H_k:\ v^2=u^4+ku^2+1.$$

Determining the solutions of the initial diophantine equation means to determine integral points on surface T_k : $x^4+y^4+kx^2y^2-z^2=0$. Finding integral points on quartic surface T_k is equivalent to finding rational points on quartic curve H_k, which is contained in T_k. The map $T_k\longrightarrow H_k$ $(x,y,z)\longmapsto(u,v)$, defined by $u=\frac{x}{y}$, $v=\frac{z}{y^2}$, transforms the equation $x^4+y^4+kx^2y^2=z^2$ to $v^2=u^4+ku^2+1$. For $k\neq\pm2$ the family of curves H_k is nonsingular and contains a rational point, for example $(0,\pm1)$, therefore for fixed $k\neq\pm2$, H_k is birational equivalent to an elliptic curve E_k, hence the map

$$H_k\longrightarrow E_k\ \ (u,v)\longmapsto(X,Y)\text{ defined by }X=2u^2+2v+k,\ Y=2u(2u^2+2v+k),$$

is an isomorphism, with inverse

$$E_k\longrightarrow H_k\ \ (X,Y)\longmapsto(u,v),\ \text{ defined by }\ u=\frac{Y}{2X},\ v=\frac{X-k}{2}-\left(\frac{Y}{2X}\right)^2.$$

The map $E_k\longrightarrow E'_k$ $(X,Y)\longmapsto(x',y')$, defined by $x'=\left(\frac{Y}{2X}\right)^2$, $y'=\frac{Y(k^2-4-X^2)}{8X^2}$ is an isogeny,

and the dual isogeny $E'_k\longrightarrow E_k$ $(x',y')\longmapsto(X,Y)$, is defined by $X=\left(\dfrac{y'}{x'}\right)^2$, $Y=\dfrac{y'(1-x'^2)}{x'^2}$.

Let $S_k = \{(x,y,z) \in \mathbb{N}^3 \mid x^4 + y^4 + kx^2y^2 = z^2,\ \gcd(x,y,z) = 1,\ xy > 1\}$ be the set of nontrivial solutions. Using the map $T_k \longrightarrow H_k$, the isomorphism $H_k \longrightarrow E_k$ and the isogenies $E_k \longrightarrow E'_k \longrightarrow E_k$, we obtain for the cardinality of S_k:

$$|S_k| \geq 1 \Leftrightarrow \left| \begin{array}{c} x' = \left(\frac{x}{y}\right)^2 \\ y' = \pm\frac{x}{y}\cdot\frac{z}{y^2} \\ (x,y,z) \in S_k \end{array} \right. \Leftrightarrow \left| \begin{array}{c} x = y\sqrt{x'} \\ y = y,\ z = \frac{y'y^2}{\sqrt{x'}} \\ (x',y') \in E'_k(\mathbb{Q}) - E'_k(\mathbb{Q})_{tor} \end{array} \right. \Leftrightarrow \text{ rank } E'_k(\mathbb{Q}) \geq 1,$$

where $E'_k(\mathbb{Q})$ and $E'_k(\mathbb{Q})_{tor}$ are respectively Mordell-Weil group of rational points and its torsion subgroup for E'_k. Consequently, the initial equation has a solution in S_k, if and only if the rank of $E'_k(\mathbb{Q})$ is at least 1 (as noted in [2]):

$$\{k \in \mathbb{Z} \mid \text{card } S_k \geq 1\} = \{k \in \mathbb{Z} \mid \text{rank } E'_k(\mathbb{Q}) \geq 1\}.$$

The rational torsion points of E'_k generate only the trivial solutions $x = y = 1$, with k in the form $k = n^2 - 2$, which are not included in S_k. In what follows, the above statements are formulated as lemmas with their proofs.

Lemma 1 *The rational torsion points of E'_k generate only the trivial solutions $x = y = 1$, with k in the form $k = n^2 - 2$, which are not included in S_k.*

Proof 1 *Let $P = (x', y') \in E'_k$ and denote $[m]P = (x'_m, y'_m)$, where $(x', y') = (x'_1, y'_1)$. Then by the group law of E'_k, (using duplication formula [8]) one obtains*

$$x'_2 = \frac{(x'^2 - 1)^2}{(2y')^2}, \quad y'_2 = \frac{(x'^2 - 1)(x'^4 + 2kx'^3 + 6x'^2 + 2kx' + 1)}{(2y')^3} \tag{3}$$

Assume that $P \in E'_k(\mathbb{Q})[m]$, i.e. $P \in E'_k(\mathbb{Q})$ with $[m]P = O$. Then, by theorem 3, it follows that x'_m and y'_m are integers. By theorem 5, it follows $1 \leq m \leq 12$ and $m \neq 11$.

case 1: *$m = 2$. Then $[2]P = O \iff P = -P \iff (x', y') = (x', -y') \iff y' = 0$. Consequently $x' = 0$ or $x'^2 + kx' + 1 = 0$ which is equivalent to $x' = 0$ or $k^2 - 4$ is a perfect square, i.e. $k = \pm 2$. Therefore the only point of order 2 is $P = (0, 0)$.*

case 2: *$m = 4$. So $[4]P = O \iff [2]P = -[2]P \iff (x'_2, y'_2) = (x'_2, -y'_2) \iff y'_2 = 0$. Consequently $x'_2 = 0$ and by (3) we obtain $x'^2 - 1 = 0$, i.e. $x' = \pm 1$. Therefore every rational torsion of order 4 must be of the type: $P(1, n)$ with k necessarily in the form $k = n^2 - 2,\ n \neq 0, 2$, or $P(-1, n)$ with k necessarily in the form $k = n^2 + 2,\ n \neq 0$. Therefore there are no rational torsion points of order 4, if $k \neq n^2 \pm 2$.*

case 3: *$m = 8$. So $[8]P = O \iff [4]P = -[4]P \iff (x'_4, y'_4) = (x'_4, -y'_4) \iff y'_4 = 0$. Consequently $[4]P$ is a two-torsion point and $[2]P$ must be a four-torsion. Then by cases 1 and 2, it follows that, $x'_4 = y'_4 = 0$ and $x'_2 = \pm 1,\ y'_2 = n,\ k = n^2 \mp 2$. We obtain $[4]P = (0, 0),\ [2]P = (\pm 1, n)$ and by (3), it follows that $\frac{(x'^2-1)^2}{4(x'^3+kx'^2+x')} = \pm 1$ which have no solutions in integers x'. Therefore rational torsion points of order 8 do not exist.*

case 4: *$m = 3$. Then $[3]P = O \iff [2]P = -P \iff (x'_2, y'_2) = (x', -y') \iff x'_2 = x'$. Consequently $\frac{(x'^2-1)^2}{4(x'^3+kx'^2+x')} = \pm x'$ which has no solutions in integers x'. Therefore rational torsion points of order 3 do not exist which means that $E'_k(\mathbb{Q})_{tors}$ has no subgroups of order 3. Consequently rational torsion points of order 6, 9 and 12 do not exist.*

case 5: *$m = 5$. So $[5]P = O \iff [4]P = -P \iff (x'_4, y'_4) = (x', -y') \iff x'_4 = x'$. Let us denote $f(x) = \frac{(x^2-1)^2}{4(x^3+kx^2+x)}$. Then $x'_2 = f(x')$ and $x'_4 = f(x'_2) = f(f(x'))$. Consequently $f(f(x')) = x'$ which has no solutions in integers x'. Indeed, let us write the rational function $f(f(x)) - x$ as a quotient of two polynomials: $f(f(x)) - x = \frac{P(x)}{Q(x)}$. Then $P(0) = 1$, therefore from $P(x') = 0$ it follows that $x' = \pm 1$, which is impossible. Therefore rational torsion points of order 5 do not exist, which means that $E'_k(\mathbb{Q})_{tors}$ has no subgroups of order 5. The latter implies that rational torsion points of order 10 do not exist.*

case 6: *$m = 7$. Then $[7]P = O \iff [8]P = P \iff (x'_8, y'_8) = (x', y') \iff x'_8 = x'$. We obtain the equation $x'_1 = f(f(f(x')))$ which has no solutions in integers x' with the same arguments as in case 5. Therefore rational* *torsion points of order 7 do not exist.*

Summarizing the results: $E'_k(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/4\mathbb{Z}, & k = n^2 \pm 2 \\ \mathbb{Z}/2\mathbb{Z}, & k \neq n^2 \pm 2 \end{cases}$

Lemma 2 *The rational torsion points of* E_k *generate only the trivial solutions* $x = y = 1$*, with* k *in the form* $k = n^2 - 2$ *which are not included in* S_k*.*

Proof 2 *Similar to the proof of lemma 1. Some considerations may be reduced by using theorem 4. Since* E_k *and* E'_k *are isogenous under isogeny* $E'_k \longrightarrow E_k$ *with kernel of order 2 (kernel =* $\{O, (0,0)\}$*), then odd torsion subgroups of that curves are isomorphic (and hence trivial by lemma 1), but even torsion subgroups are not the same:*

$$E_k(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, & k = n^2 - 2 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, & k \neq n^2 - 2 \end{cases} \text{, i.e.}$$

$$E_k(\mathbb{Q})_{tors} = \begin{cases} \{O, (0,0), (n^2-4, 0), (n^2, 0), (n^2 \pm 2n, 2\epsilon(n^2 \pm 2n))\}, & k = n^2 - 2 \\ \{O,\ (0,0),\ (k-2, 0),\ (k+2, 0)\}, & k \neq n^2 - 2 \end{cases}$$

with $\epsilon = \pm 1$*.*

Lemma 3 $\{k \in \mathbb{Z} \mid \text{card}\, S_k \geq 1\} = \{k \in \mathbb{Z} \mid \text{rank}\, E'_k(\mathbb{Q}) \geq 1\}$.

Proof 3 *From a direct application of lemma 1 and the calculations above: if* $(x, y, z) \in S_k$*, then the point* $P(x', y') \in E'_k$ *with coordinates* $x' = (x/y)^2$, $y' = \pm\, xz/y^3$ *is rational and by lemma 1 that point is nontorsion, since* $x' = (x/y)^2 \neq 0, \pm 1$*. Thus rank* $E'_k(\mathbb{Q}) \geq 1$*.*

Let assume that rank $E'_k(\mathbb{Q}) \geq 1$ *and let* $P(x', y') \in E'_k$ *is a rational nontorsion point. Let* $x' = x_1/x_2$, $y' = y_1/y_2$, $\gcd(x_1, x_2) = \gcd(y_1, y_2) = 1$ *and let substitute in the equation of* E'_k*:*

$$x_2^3 y_1^2 = y_2^2 x_1 (x_1^2 + k x_1 x_2 + x_2^2), \tag{4}$$

so $x_2^3 = \pm y_2^2$*, therefore* $x_2 = \pm s^2$, $y_2 = s^3$ *and* $y_1^2 = \pm x_1(x_1^2 \pm k x_1 s^2 + s^4)$*. From* $\gcd(x_1, s) = 1$*, one obtains* $\gcd(x_1, x_1^2 \pm k x_1 s^2 + s^4) = 1$*. Then* $x_1 = t^2$, $y_1 = tw$ *and consequently* $w^2 = \pm(t^4 \pm k t^2 s^2 + s^4)$*. Then every nontorsion point on* $E'_k(\mathbb{Q})$ *has the type* $(x', y') = \left(\pm\frac{t^2}{s^2},\ \frac{t}{s}\cdot\frac{w}{s^2}\right)$ *with* $t^2 \neq s^2$ *and* $ts \neq 0$*. If the sign is +, then* $(t, s, w) \in S_k$*. Otherwise, if* $P = (x', y') = \left(-\frac{t^2}{s^2},\ \frac{t}{s}\cdot\frac{w}{s^2}\right)$*, then* $[2]P = (x'_2, y'_2)$ *such that*

$$x'_2 = \left(\frac{t^4 - s^4}{2stw}\right)^2, \quad y'_2 = \frac{(t^4 - s^4)[(t^4 + s^4)^2 + 4t^4 s^4 - 2k t^2 s^2 (t^4 + s^4)]}{(2stw)^3}. \tag{5}$$

Therefore $\left(\frac{|t^4 - s^4|}{d},\ \frac{2stw}{d},\ \frac{|w^4 - (k^2-4)t^4 s^4|}{d^2}\right) \in S_k$*, where* $\gcd(t^4 - s^4,\ 2stw) = d$*.*

Remark 6 *In the case* $k = \pm 2$ *the surface* T_k *is degenerate:* T_{-2} *consists of two hyperbolic paraboloids, since* $T_{-2} : (x^2 - y^2 + z)(x^2 - y^2 - z) = 0$*;* T_{+2} *consists of two elliptic paraboloids:* $T_{+2} : (x^2 + y^2 + z)(x^2 + y^2 - z) = 0$*. The corresponding positive integral solutions are* $(a, b, |a^2 - b^2|)$, $(a, b, a^2 + b^2)$, $a \neq b$*.*

CONCLUSION

In this subsection is given a complete parametric description of the non-trivial solutions, an example of higher rank curves in the elliptic family E_k, motivation and a description via matrix equations of theorem 9. Our main result is the following.

Theorem 9 *The equation $x^4+y^4+kx^2y^2=z^2$ has a non trivial solution, i.e. solution in S_k, if and only if k satisfies at least one of the following systems:*

$$\left|\begin{array}{c} x_1,x_2,y_1,y_2 - odd \\ \beta y_2^2-\alpha y_1^2=x_1^2 \\ \delta y_2^2-\gamma y_1^2=x_2^2 \\ \alpha\delta-\beta\gamma=1 \\ k=4\alpha\delta-2 \end{array}\right. \qquad \left|\begin{array}{c} y_1,y_2 - odd \\ \beta y_2^2-\alpha y_1^2=4x_1^2 \\ \delta y_2^2-\gamma y_1^2=4x_2^2 \\ \alpha\delta-\beta\gamma=4 \\ k=\alpha\delta-2 \end{array}\right. \qquad \left|\begin{array}{c} x_1,x_2,y_1,y_2 - odd \\ \beta y_2^2-\alpha y_1^2=2x_1^2 \\ \delta y_2^2-\gamma y_1^2=2x_2^2 \\ \alpha\delta-\beta\gamma=4 \\ k=\alpha\delta-2, \end{array}\right.$$

where $\alpha,\beta,\gamma,\delta,x_1,x_2,y_1,y_2$ are nonzero integers satisfying the conditions $\gcd(x_1,x_2)=\gcd(y_1,y_2)=\gcd(x_1x_2,y_1y_2)=1$, $x_1x_2y_1y_2>1$, (with equality $x_1x_2y_1y_2=1$ only possible for the second system of equations). Solutions of the equation for the corresponding three cases are:

$$\left|\begin{array}{c} x=x_1x_2 \\ y=y_1y_2 \\ z=\left|\beta\delta y_2^4-\alpha\gamma y_1^4\right| \end{array}\right. \qquad \left|\begin{array}{c} x=2x_1x_2 \\ y=y_1y_2 \\ z=\frac{\left|\beta\delta y_2^4-\alpha\gamma y_1^4\right|}{4} \end{array}\right. \qquad \left|\begin{array}{c} x=x_1x_2 \\ y=y_1y_2 \\ z=\frac{\left|\beta\delta y_2^4-\alpha\gamma y_1^4\right|}{4} \end{array}\right.$$

Proof 4 *E_k and E'_k are isogenous, then by theorem 8 it follows that rank E_k = rank E'_k. Lemma 3 gives card $S_k\geq 1$ if and only if rank $E_k\geq 1$. For E_k we may apply complete 2 descent algorithm, since all two-torsions of E_k are rational, i.e. $E_k[2]=E_k(\mathbb{Q})[2]=\{O,\ (0,0),\ (k-2,0),\ (k+2,0)\}$.*
Assume that k has the form $k=\epsilon\alpha\delta-2=\epsilon\beta\gamma+2$, $\epsilon=1$ or $\epsilon=4$, with $(\alpha,\ \beta,\ \gamma,\ \delta,\ x_1,\ x_2,\ y_1,\ y_2)$ as in the theorem. Then, one could check directly that the triple (x,y,z) corresponding to k (as in the theorem) is a nontrivial solution, and by lemma 3 that solution comes from a rational nontorsion point of E. Thus rank $E_k\geq 1$.
Assume that rank $E_k\geq 1$. We are going to prove that k has the form $k=\epsilon\alpha\delta-2=\epsilon\beta\gamma+2$. Applying theorems 6 and 7 to E_k, with $e_1=0$, $e_2=k-2$, $e_3=k+2$, we obtain the following: there exist a square-free integers $b_1,b_2\in\mathbb{Q}(S,2)$, such that the system of equations

$$b_1z_1^2-b_2z_2^2=k-2,\quad b_1z_1^2-b_1b_2z_3^2=k+2, \tag{6}$$

has a solution $(z_1,z_2,z_3)\in\mathbb{Q}^*\times\mathbb{Q}^*\times\mathbb{Q}^*$ and $P=(b_1z_1^2,\ b_1b_2z_1z_2z_3)$ is a nontorsion point. The condition $b_1,b_2\in\mathbb{Q}(S,2)$ is equivalent to:

- $16(k^2-4)=\Delta_{E_k}\equiv 0$ *mod* b_i *for* $i=1,2$
- $p^2\nmid b_1,\ p^2\nmid b_2$ *for all primes* p.

The proof will be accomplished in several steps, formulated belows as lemmas.

Lemma 4 *System (6) with the condition $\gcd(b_1,b_2)=1$ is equivalent to the union of the following four systems:*

$$b_1Z_1^2\pm Z_2^2=(k-2)Z^2,\quad b_1Z_1^2\pm b_1Z_3^2=(k+2)Z^2; \tag{7}$$

$$b_1Z_1^2\pm 2Z_2^2=(k-2)Z^2,\quad b_1Z_1^2\pm 2b_1Z_3^2=(k+2)Z^2; \tag{8}$$

where Z,Z_1,Z_2,Z_3 are positive integers, satisfying $\gcd(Z,Z_i)=\gcd(Z,b_1)=1$, $i=1,2,3$ and $k+2\equiv 0$ mod b_1.

Lemma 4 states that $b_2=\pm1$ or $b_2=\pm2$, and if $z_i=\frac{Z_i}{Z_{ii}}$, $\gcd(Z_i,Z_{ii})=1$, $i=1,2,3$, then $Z_{11}=Z_{22}=Z_{33}$ (we set them equal to Z). Now we prove that statement for all four cases. System (6) is equivalent to

$$b_1Z_1^2Z_{22}^2-b_2Z_2^2Z_{11}^2=(k-2)Z_{11}^2Z_{22}^2,\quad b_1Z_1^2Z_{33}^2-b_1b_2Z_3^2Z_{11}^2=(k+2)Z_{11}^2Z_{33}^2. \tag{9}$$

From the first equation one obtains $b_1Z_{22}^2\equiv 0$ mod Z_{11}^2 and $b_2Z_{11}^2\equiv 0$ mod Z_{22}^2. Then by the square-free property of b_1,b_2, it follows that Z_{11} and Z_{22} have the same set of prime divisors and the same powers for each prime in the product decomposition, so $Z_{11}=Z_{22}$. From the second equation of (9), one could imply that $Z_{11}=Z_{33}$. Thus $Z_{11}=Z_{22}=Z_{33}\ (=Z)$ and dividing by Z^2 in (9), we obtain:

$$b_1Z_1^2-b_2Z_2^2=(k-2)Z^2,\quad b_1Z_1^2-b_1b_2Z_3^2=(k+2)Z^2. \tag{10}$$

If $\gcd(b_1, Z) = d_1$*, then by the first equation of (10), we will get* $b_2Z_2^2 \equiv 0 \mod d_1$*. Thus* $Z_2^2 \equiv 0 \mod d_1$ *and* $\gcd(Z, Z_2) \equiv 0 \mod d_1$*. Since* $\gcd(Z, Z_2) = 1$*, then* $d_1 = 1$ *and by the second equation of (10), we will have that* $k + 2 \equiv 0 \mod b_1$*. Subtracting the equations of (10), we obtain* $b_2(Z_2^2 - b_1Z_3^2) = 4Z^2$*. Therefore* $4 \equiv 0 \mod b_2$*, since* $\gcd(b_1, b_2) = 1$ *and* $\gcd(Z, b_2) = 1$*. This means that* $b_2 = \pm1$ *or* $b_2 = \pm2$ *which completes the proof of lemma 4.*

A generalization of lemma 4 is:

Lemma 5 *Let* $\gcd(b_1, b_2) = d$*. System (6) is equivalent to the union of the following four systems:*

$$d(eZ_1^2 \pm Z_2^2) = (k-2)Z^2, \quad e(dZ_1^2 \pm Z_3^2) = (k+2)Z^2; \tag{11}$$

$$d(eZ_1^2 \pm 2Z_2^2) = (k-2)Z^2, \quad e(dZ_1^2 \pm 2Z_3^2) = (k+2)Z^2; \tag{12}$$

where Z, Z_1, Z_2, Z_3 *are positive integers, satisfying* $\gcd(Z, Z_i) = \gcd(Z, e) = \gcd(e, d) = 1$*,* $i = 1, 2, 3$ *and* $k + 2 \equiv 0 \mod e$*,* $k - 2 \equiv 0 \mod d$*, and* $p^2 \nmid de$ *for all primes* p*.*

If $b_1 = de$*,* $b_2 = df$*, then* $\gcd(d, e) = \gcd(d, f) = \gcd(e, f) = 1$ *and* d, e, f *are square-free. As in lemma 4, we obtain* $Z_{11} = Z_{22} = Z$ *and (6) is equivalent to:*

$$b_1Z_1^2 - b_2Z_2^2 = (k-2)Z^2, \quad b_1Z_1^2Z_{33}^2 - b_1b_2Z_3^2Z^2 = (k+2)Z_{33}^2Z^2. \tag{13}$$

From the second equation of (13), one obtains $b_1Z_{33}^2 \equiv 0 \mod Z^2$ *and* $b_1b_2Z^2 \equiv 0 \mod Z_{33}^2$*. Then by the square-free property of* b_1, b_2*, there exists divisor* d_1 *of* d *such that* $Z_{33} = d_1Z$*. Thus (13) is equivalent to*

$$b_1Z_1^2 - b_2Z_2^2 = (k-2)Z^2, \quad b_1Z_1^2 - ef\left(\frac{d}{d_1}\right)^2 Z_3^2 = (k+2)Z^2. \tag{14}$$

Subtracting the equations of (14), we obtain

$$b_2Z_2^2 - ef\left(\frac{d}{d_1}\right)^2 Z_3^2 = 4Z^2, \tag{15}$$

Therefore $4Z^2 \equiv 0 \mod \frac{d}{d_1}$ *and* $4Z^2 \equiv 0 \mod f$*. By the second equation of (14),* $\gcd(f,\ Z) = \gcd(d/d_1,\ Z) = 1$ *which implies that the square-free integers* d/d_1 *and* f *are divisors of 4. Hence* $d/d_1 = 1$ *or* 2*,* $f = \pm1$ *or* ±2*. There are four cases:*

- $(d/d_1,\ f) = (1, \pm1)$*. Then (14) is equivalent to (11),*
- $(d/d_1,\ f) = (1, \pm2)$*. Then (14) is equivalent to (12),*
- $(d/d_1,\ f) = (2, \pm1)$*. Then (14) is equivalent to a subsystem of (11),*
- $(d/d_1,\ f) = (2, \pm2)$*. Then (14) is equivalent to a subsystem of (12).*

It is straightforward that $\gcd(e,\ Z) = \gcd(d,\ Z) = 1$ *which implies* $k + 2 \equiv 0 \mod e$ *and* $k - 2 \equiv 0 \mod d$*. This completes the proof of lemma 5.*

By using lemma 5, equation (11) gives us

$$eZ_1^2 - \frac{k-2}{d}Z^2 = \mp Z_2^2, \quad dZ_1^2 - \frac{k+2}{e}Z^2 = \mp Z_3^2. \tag{16}$$

There are three cases:

case 1: Z_1, Z_2, Z_3*-even,* Z*-odd. Then* $k \equiv 2 \mod 4$ *and* $Z_i = 2Z_i'$*,* $i = 1, 2, 3$ *and* Z_i' *are odd. If the sign in (16) is minus, then we have*

$$(\alpha, \beta, \gamma, \delta) = \left(e, \frac{k-2}{4d}, d, \frac{k+2}{4e}\right) \text{ and } (x_1, x_2, y_1, y_2) = (Z_2', Z_3', Z_1', Z).$$

Otherwise, if the sign is plus, then we have

$$(\alpha, \beta, \gamma, \delta) = \left(\frac{k+2}{4e}, d, \frac{k-2}{4d}, e\right) \text{ and } (x_1, x_2, y_1, y_2) = (Z_3', Z_2', Z, Z_1').$$

Therefore $k = 4\alpha\delta - 2 = 4\beta\gamma + 2$ *and we obtain the first system of theorem 9.*

In ***case 1****, it is impossible to have* $Z = Z_1' = Z_2' = Z_3' = 1$ *since the point* $P = (b_1 z_1^2,\ b_1 b_2 z_1 z_2 z_3)$ *is a torsion. Indeed, by lemma 2 and the calculations above*

$$z_1 = z_2 = 2,\ z_3 = \frac{2}{d},\ k = (2d \pm 2)^2 - 2,\ b_1 = d^2 \pm d,\ b_2 = \pm d,$$

$$P = (4(d^2 \pm d),\ 8(d^2 \pm d)) \in E_k(\mathbb{Q})_{tor}.$$

case 2: *Z and Z_1 are odd, Z_2 and Z_3 are even. Hence* $Z_2 = 2Z_2',\ Z_3 = 2Z_3'$ *and* $\gcd(Z_2',\ Z_3') = 1$*. If the sign in (16) is minus, then we have*

$$(\alpha,\beta,\gamma,\delta) = \left(e, \frac{k-2}{d}, d, \frac{k+2}{e}\right) \text{ and } (x_1,x_2,y_1,y_2) = (Z_2', Z_3', Z_1, Z).$$

Otherwise, if the sign is plus, then we have

$$(\alpha,\beta,\gamma,\delta) = \left(\frac{k+2}{e}, d, \frac{k-2}{d}, e\right) \text{ and } (x_1,x_2,y_1,y_2) = (Z_3', Z_2', Z, Z_1).$$

It is possible to have $Z = Z_1 = Z_2' = Z_3' = 1$
since the point $P = (b_1 z_1^2,\ b_1 b_2 z_1 z_2 z_3)$ *in this case is not a torsion. Indeed, by lemma 2 and the calculations above, we obtain*

$$z_1 = 1,\ z_2 = 2,\ z_3 = \frac{2}{d},\ k = d^2 \pm 5d - 2,\ b_1 = d^2 \pm d,\ b_2 = \pm d,$$

$$P = (d^2 \pm d,\ 4(d^2 \pm d)) \notin E_k(\mathbb{Q})_{tor}.$$

Therefore $k = \alpha\delta - 2 = \beta\gamma + 2$ *and we obtain the second system of theorem 9.*

By using lemma 5, equation (12), we obtain

$$eZ_1^2 - \frac{k-2}{d}Z^2 = \mp 2Z_2^2, \quad dZ_1^2 - \frac{k+2}{e}Z^2 = \mp 2Z_3^2. \tag{17}$$

case 3: $k \equiv 1 \bmod 2$ *and Z, Z_i are odd. Hence* $d \equiv e \equiv 1 \bmod 2$*. If the sign in (17) is minus, then we have*

$$(\alpha,\beta,\gamma,\delta) = \left(e, \frac{k-2}{d}, d, \frac{k+2}{e}\right) \text{ and } (x_1,x_2,y_1,y_2) = (Z_2, Z_3, Z_1, Z).$$

Otherwise, if the sign is plus, we have

$$(\alpha,\beta,\gamma,\delta) = \left(\frac{k+2}{e}, d, \frac{k-2}{d}, e\right) \text{ and } (x_1,x_2,y_1,y_2) = (Z_3, Z_2, Z, Z_1).$$

Consequently $k = \alpha\delta - 2 = \beta\gamma + 2$ *and we obtain the third system of theorem 9.*

For ***case 3****, it is impossible to have* $Z = Z_1 = Z_2 = Z_3 = 1$ *since the point* $P = (b_1 z_1^2,\ b_1 b_2 z_1 z_2 z_3)$ *is a torsion. Indeed, by lemma 2 and the calculations above*

$$z_1 = z_2 = 1,\ z_3 = \frac{1}{d},\ k = (d \pm 2)^2 - 2,\ b_1 = d^2 \pm 2d,\ b_2 = \pm 2d,$$

$$P = (d^2 \pm 2d,\ 2(d^2 \pm 2d)) \in E_k(\mathbb{Q})_{tor}.$$

All the other possibilities for the parity of Z and Z_i lead to the same results, as already obtained above, which completes the proof of the theorem.

Remark 7 *Theorem 9 allows compact description by matrix equations. Let $\mathcal{M}_2(\mathbb{Z})$ be the set of 2×2 matrices with integral elements and for convenience, let us introduce the following definition: two 2-dimensional vectors X and Y are called perfect pair if their coordinates are integral, perfect squares and pairwise coprime, with product greater than 1. Then theorem 9 states that all values of k come from such matrix $g \in \mathcal{M}_2(\mathbb{Z})$, with nonzero elements, for which the equation*

$$g \circ Y = \epsilon X \tag{18}$$

has a solution (X, Y) which is a perfect pair. In correspondence with the notations above, let

$$g = \begin{pmatrix} -\alpha & \beta \\ -\gamma & \delta \end{pmatrix},\ \ X = \begin{pmatrix} x_1^2 \\ x_2^2 \end{pmatrix},\ \ Y = \begin{pmatrix} y_1^2 \\ y_2^2 \end{pmatrix},\ \ \varepsilon \in \{1, 2, 4\}. \tag{19}$$

There are three cases that correspond to the three systems of equations in the theorem:

case 1: $\det(g) = -1,\ \varepsilon = 1,\ k = 4\alpha\delta - 2,$
case 2: $\det(g) = -4,\ \varepsilon = 4,\ k = \alpha\delta - 2,$
case 3: $\det(g) = -4,\ \varepsilon = 2,\ k = \alpha\delta - 2.$

Case 1 gives all solutions (x, y, z), with x, y odd, z even, and k even.
Case 2 gives all (x, y, z), with x even, y, z odd, and k can be even or odd.
Case 3 gives all solutions (x, y, z), with x, y, z odd, and k odd.

Remark 8 *To every generator P of the Mordell-Weil group $E_k(\mathbb{Q})$, corresponds a unique matrix $g_P \in \mathcal{M}_2(\mathbb{Z})$ given by following short non-exact sequence:*

$$0 \longrightarrow E_k(\mathbb{Q})/2E_k(\mathbb{Q}) \longrightarrow \mathbb{Q}(S,2)\times\mathbb{Q}(S,2) \longrightarrow \mathcal{M}_2(\mathbb{Z})$$

$$P = (x, y)\ \longmapsto (b_1,\ b_2)\ \longmapsto g_P = \begin{pmatrix} -\alpha & \beta \\ -\gamma & \delta \end{pmatrix}.$$

The middle map is an injective group homomorphism, defined in theorem 6 where $S = \{p-\ prime \mid\ \Delta_{E_k} \equiv 0\ mod\ p\} \cup \{\pm 1\}$. The third map is defined as follows. Let $d = \gcd(b_1, b_2)$. Set $\rho = 4$, when $k \equiv 2\ mod\ 4$ and $x = r/s$, r-even, s-odd; and $\rho = 1$ otherwise. There are two cases that correspond to $sign(b_2) = -1$ and $sign(b_2) = +1$:

$$g_P = \begin{pmatrix} -\frac{b_1}{d} & \frac{k-2}{\rho d} \\ -d & \frac{(k+2)d}{\rho b_1} \end{pmatrix},\qquad g_P = \begin{pmatrix} -\frac{(k+2)d}{\rho b_1} & d \\ -\frac{k-2}{\rho d} & \frac{b_1}{d} \end{pmatrix}.$$

Example 2 *Using remark 7 and the Magma software ([12]), we obtain higher rank curves in the elliptic family E_k, with solutions of the general equation that correspond to generators of the Mordell-Weil group for these curves. Consider the matrix $g_i \in \mathcal{M}_2(\mathbb{Z})$*

$$g_1 = \begin{pmatrix} -2 & 102 \\ -287 & 14639 \end{pmatrix},\ \ g_2 = \begin{pmatrix} -2 & 4182 \\ -7 & 14639 \end{pmatrix},$$

$$g_3 = \begin{pmatrix} -29278 & 1394 \\ -21 & 1 \end{pmatrix},\ \ g_4 = \begin{pmatrix} -2 & 6 \\ -4879 & 14639 \end{pmatrix}.$$

The following equalities are satisfied, i.e. solutions of the equation (18) $g_i \circ Y = 4X$:

$$g_1 \circ \begin{pmatrix} 7^2 \\ 1^2 \end{pmatrix} = 4\begin{pmatrix} 1^2 \\ 12^2 \end{pmatrix},\ \ g_2 \circ \begin{pmatrix} 503^2 \\ 11^2 \end{pmatrix} = 4\begin{pmatrix} 1^2 \\ 8^2 \end{pmatrix},$$

$$g_3 \circ \begin{pmatrix} 5^2 \\ 23^2 \end{pmatrix} = 4\begin{pmatrix} 37^2 \\ 1^2 \end{pmatrix},\ \ g_4 \circ \begin{pmatrix} 19^2 \\ 11^2 \end{pmatrix} = 4\begin{pmatrix} 1^2 \\ 50^2 \end{pmatrix}.$$

Since $\det(g_i) = -4,\ \epsilon = 4$, *then case 2 of theorem 9 states that* $k = \alpha_i\delta_i - 2 = 29\,276$ *and the solutions of the general equation are* (x_i, y_i, z_i), *such that*

$$(x_1,\ y_1,\ z_1) = (24,\ 7,\ 28\,751),\quad (x_2,\ y_2,\ z_2) = (16,\ 5533,\ 34\,156\,471),$$

$$(x_3,\ y_3,\ z_3) = (74,\ 115,\ 1\,456\,151),\ \ (x_4,\ y_4,\ z_4) = (100,\ 209,\ 3\,576\,319).$$

By remark 8, g_i *corresponds to a generator* $P_i \in E_{29\,276}(\mathbb{Q})$ *for* $i = 1, 2, 3, 4$. *Then* (x_i, y_i, z_i) *correspond to generators of* $E_{29\,276}(\mathbb{Q})$ *and rank* $E_{29\,276}(\mathbb{Q}) \geq 4$. *It can be shown that rank* $E_{29\,276}(\mathbb{Q}) = 4$ *(see Table 1).*

Example 3 *Another rank four elliptic curve from the elliptic family* E_k *is given by* $k = 70\,808$. *As in example 2, the calculation of matrix generators* g_1', g_2', g_3', g_4' *corresponding to generators of* $E_{70\,808}(\mathbb{Q})$ *is as follows: consider the matrix* $g_i' \in \mathcal{M}_2(\mathbb{Z})$:

$$g_1' = \begin{pmatrix} -6 & 70810 \\ -1 & 11801 \end{pmatrix},\quad g_2' = \begin{pmatrix} -73 & 11801 \\ -6 & 970 \end{pmatrix},$$

$$g_3' = \begin{pmatrix} -14162 & 70806 \\ -1 & 5 \end{pmatrix},\quad g_4' = \begin{pmatrix} -2 & 70806 \\ -1 & 35405 \end{pmatrix}.$$

The following equalities are satisfied, i.e. solutions of the equation (18) $g_i \circ Y = 4X$:

$$\begin{pmatrix} -6 & 70810 \\ 1 & 11801 \end{pmatrix}\begin{pmatrix} 101^2 \\ 1^2 \end{pmatrix} = 4\begin{pmatrix} 49^2 \\ 20^2 \end{pmatrix},\qquad \begin{pmatrix} -73 & 11801 \\ -6 & 970 \end{pmatrix}\begin{pmatrix} 89^2 \\ 7^2 \end{pmatrix} = 4\begin{pmatrix} 2^2 \\ 1^2 \end{pmatrix}.$$

$$\begin{pmatrix} -14162 & 70806 \\ -1 & 5 \end{pmatrix}\begin{pmatrix} 199^2 \\ 89^2 \end{pmatrix} = 4\begin{pmatrix} 79^2 \\ 1^2 \end{pmatrix},\qquad \begin{pmatrix} -2 & 70806 \\ -1 & 35405 \end{pmatrix}\begin{pmatrix} 179^2 \\ 1^2 \end{pmatrix} = 4\begin{pmatrix} 41^2 \\ 29^2 \end{pmatrix}.$$

Since $\det(g_i') = -4,\ \epsilon = 4$, *then case 2 of theorem 9 states that* $k = \alpha_i\delta_i - 2 = 70\,808$ *and the solutions of the general equation are* (x_i, y_i, z_i), *such that*

$$(x_1, y_1, z_1) = (1960,\ 101,\ 52\,816\,601),\ (x_2, y_2, z_2) = (4,\ 623,\ 768\,353),$$

$$(x_3, y_3, z_3) = (158,\ 17711,\ 808\,004\,167),\ (x_4, y_4, z_4) = (2378,\ 179,\ 113\,408\,767).$$

By remark 8, g_i' *corresponds to a generator* $P_i \in E_{70\,808}(\mathbb{Q})$ *for* $i = 1, 2, 3, 4$. *Then* (x_i, y_i, z_i) *correspond to generators of* $E_{70\,808}(\mathbb{Q})$ *and rank* $E_{70\,808}(\mathbb{Q}) \geq 4$. *It can be shown that rank* $E_{70\,808}(\mathbb{Q}) = 4$ *(Table 1).*

TABLE 1. Higher rank curves in the elliptic family E_k

k	**x**	**y**	**z**	**rank** E_k	**generators**
29 276	24	7	28 751	4	g_1
	16	5 533	34 156 471		g_2
	74	115	1 456 151		g_3
	100	209	3 576 319		g_4
70 808	1960	101	52 816 601	4	g_1'
	4	623	768 353		g_2'
	158	17 711	808 004 167		g_3'
	2378	179	113 408 767		g_4'

Example 4 *There are infinitely many integers k for which the main considered equation has a solution (x, y, z) in distinct odd prime numbers. It is a necessary and sufficient condition that k is in the form*

$$k = \pm 2 + n(2p^2 \pm 2q^2 + np^2q^2), \tag{20}$$

where p, q and $|p^2 \pm q^2 + np^2q^2|$ are primes, for some $n \in \mathbb{Z}$.

Proof: When p and q are distinct odd primes, the arithmetic progression $\{p^2 \pm q^2 + np^2q^2\}_{n\in\mathbb{Z}}$ contains infinitely many primes, by the Dirichlet theorem. When k has the form (20), then a solution in prime numbers is

$$(x, y, z) = (p, q, |p^2 \pm q^2 + np^2q^2|).$$

If $(x, y, z) = (p, q, r)$ is a solution in primes, then by theorem 9, case 3 of remark 7 and the following identities

$$\begin{pmatrix} -(2+np^2) & 2p^2+2q^2+np^2q^2 \\ -n & 2+nq^2 \end{pmatrix} \begin{pmatrix} q^2 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} p^2 \\ 1 \end{pmatrix},$$

$$\begin{pmatrix} -n & 2+nq^2 \\ -(np^2-2) & 2p^2-2q^2+np^2q^2 \end{pmatrix} \begin{pmatrix} q^2 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} 1 \\ p^2 \end{pmatrix},$$

it follows that $r = |p^2 \pm q^2 + np^2q^2|$ for some $n \in \mathbb{Z}$ and k has the form (20).

Remark 9 *The motivation for theorem 9 is the following observation concerning the possible values of k:*

$$k = \frac{z^2 - x^4 - y^4}{x^2y^2} = \frac{1}{y^2}\left(\frac{(z-y^2)(z+y^2)}{x^2} - x^2\right), \tag{21}$$

where $(x, y, z) \in S_k$ and we may assume that y is odd since $\gcd(x, y, z) = 1$. There are two cases:

case 1: *$z \equiv 0 \bmod 2$. Then x is odd and $\gcd(z - y^2, z + y^2) = 1$. From (21), one could see that $(z - y^2)(z + y^2)/x^2$ is an integer. Therefore there exist odd integers x_1, x_2, t_1, t_2 such that:*

$$z - y^2 = t_1x_1^2, \quad z + y^2 = t_2x_2^2, \quad x = x_1x_2, \quad \gcd(t_1x_1,\ t_2x_2) = 1. \tag{22}$$

We obtain $k = (t_1t_2 - x_1^2x_2^2)/y^2$ and $2y^2 = t_2x_2^2 - t_1x_1^2$. Consequently,

$$t_1t_2 \equiv x_1^2x_2^2 \bmod y^2, \quad t_1x_1^2 \equiv t_2x_2^2 \bmod y^2, \tag{23}$$

where $\gcd(y,\ t_1t_2x_1x_2) = 1$ and $t_1t_2^2 \equiv t_2(x_1x_2)^2 \equiv x_1^2(t_2x_2^2) \equiv t_1x_1^4 \bmod y^2$. Thus $(t_2 - x_1^2)(t_2 + x_1^2) \equiv 0 \bmod y^2$ and similarly $(t_1 - x_2^2)(t_1 + x_2^2) \equiv 0 \bmod y^2$. In addition, there exist nonzero even integers A, B, C, D such that:

$$t_2 - x_1^2 = Ay_1^2, \quad t_2 + x_1^2 = By_2^2, \quad t_1 - x_2^2 = Cy_1^2, \quad t_1 + x_2^2 = Dy_2^2, \quad y = y_1y_2, \tag{24}$$

where $\gcd(y_1, y_2) = 1$. Solving the equations (24), we obtain

$$t_1 = (Cy_1^2 + Dy_2^2)/2, \quad t_2 = (Ay_1^2 + By_2^2)/2, \tag{25}$$

$$x_1^2 = (By_2^2 - Ay_1^2)/2, \quad x_2^2 = (Dy_2^2 - Cy_1^2)/2. \tag{26}$$

Finally, $k = (t_1t_2 - x_1^2x_2^2)/y^2 = (AD + BC)/2$ and $2y^2 = t_2x_2^2 - t_1x_1^2 = (AD - BC)y^2/2$. Therefore $AD = k + 2$ and $BC = k - 2$. Let $(\alpha, \beta, \gamma, \delta) = (A/2, B/2, C/2, D/2)$. Then case 1 is equivalent to the existence of nonzero integers $\alpha, \beta, \gamma, \delta$, such that:

$$x_1^2 = \beta y_2^2 - \alpha y_1^2, \quad x_2^2 = \delta y_2^2 - \gamma y_1^2, \quad \alpha\delta = (k+2)/4, \quad \beta\gamma = (k-2)/4. \tag{27}$$

Hence, we obtain the first system for k in theorem 9.

case 2: $z \equiv 1$ *mod* 2. *Then* $\gcd(\frac{z-y^2}{2}, \frac{z+y^2}{2}) = 1$. *There are two cases for the parity of x.*

case 2.1: $x \equiv 0$ *mod* 2. *Then* $x = 2x_1x_2,\ \gcd(x_1, x_2) = 1$. *Similarly as in case 1, we obtain*

$$z - y^2 = 2t_1x_1^2, \quad z + y^2 = 2t_2x_2^2, \quad \gcd(t_1x_1,\ t_2x_2) = 1. \tag{28}$$

There exist nonzero integers A, B, C, D *such that:*

$$t_2 - 2x_1^2 = Ay_1^2, \quad t_2 + 2x_1^2 = By_2^2, \quad t_1 - 2x_2^2 = Cy_1^2, \quad t_1 + 2x_2^2 = Dy_2^2, \quad y = y_1y_2, \tag{29}$$

where $\gcd(y_1, y_2) = 1$, $A \equiv B$ *mod* 4 *and* $C \equiv D$ *mod* 4, $A - C \equiv 1$ *mod* 2.

$$t_1 = (Cy_1^2 + Dy_2^2)/2, \quad t_2 = (Ay_1^2 + By_2^2)/2, \tag{30}$$

$$x_1^2 = (By_2^2 - Ay_1^2)/4, \quad x_2^2 = (Dy_2^2 - Cy_1^2)/4. \tag{31}$$

Finally, $k = (t_1t_2 - 4x_1^2x_2^2)/y^2 = (AD + BC)/2$ *and* $y^2 = t_2x_2^2 - t_1x_1^2 = (AD - BC)y^2/4$. *Therefore* $AD = k + 2$ *and* $BC = k - 2$. *Let* $(\alpha, \beta, \gamma, \delta) = (A, B, C, D)$. *Then case 2.1 is equivalent to the existence of nonzero integers* $\alpha, \beta, \gamma, \delta$, *such that:*

$$(2x_1)^2 = \beta y_2^2 - \alpha y_1^2, \quad (2x_2)^2 = \delta y_2^2 - \gamma y_1^2, \quad \alpha\delta = k + 2, \quad \beta\gamma = k - 2 \tag{32}$$

Therefore, we obtain the second system for k in theorem 9.

case 2.2: $x \equiv 1$ *mod* 2. *Then* $x = x_1x_2,\ \gcd(x_1, x_2) = 1$. *Similarly to the previous cases, we obtain*

$$z - y^2 = 2t_1x_1^2, \quad z + y^2 = 2t_2x_2^2, \quad \gcd(t_1x_1,\ t_2x_2) = 1, \quad t_1 - t_2 \equiv 1 \text{ mod } 2. \tag{33}$$

There exist nonzero integers A, B, C, D *such that:*

$$2t_2 - x_1^2 = Ay_1^2, \quad 2t_2 + x_1^2 = By_2^2, \quad 2t_1 - x_2^2 = Cy_1^2, \quad 2t_1 + x_2^2 = Dy_2^2, \quad y = y_1y_2, \tag{34}$$

where $\gcd(y_1, y_2) = 1$, $A + B \equiv C + D \equiv A + C \equiv B + D \equiv 0$ *mod* 4. *Therefore:*

$$t_1 = (Cy_1^2 + Dy_2^2)/4, \quad t_2 = (Ay_1^2 + By_2^2)/4, \tag{35}$$

$$x_1^2 = (By_2^2 - Ay_1^2)/2, \quad x_2^2 = (Dy_2^2 - Cy_1^2)/2. \tag{36}$$

Finally, $k = (4t_1t_2 - x_1^2x_2^2)/y^2 = (AD + BC)/2$ *and* $y^2 = t_2x_2^2 - t_1x_1^2 = (AD - BC)y^2/4$. *Consequently,* $AD = k + 2$ *and* $BC = k - 2$. *Let* $(\alpha, \beta, \gamma, \delta) = (A, B, C, D)$. *Then case 2.2 is equivalent to the existence of nonzero odd integers* $\alpha, \beta, \gamma, \delta$, *such that:*

$$2x_1^2 = \beta y_2^2 - \alpha y_1^2, \quad 2x_2^2 = \delta y_2^2 - \gamma y_1^2, \quad \alpha\delta = k + 2, \quad \beta\gamma = k - 2 \tag{37}$$

Hence, we obtain the third system for k in theorem 9 *which completes the survey.*[1].

APPENDICES

In this section are given definitions of $\mathbb{Z}_p$, $\mathbb{Q}_p$ and the reduction map modulo p. Let p be a prime number, $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$, and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ be a finite field with p elements. Let us denote by

$$\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}, \qquad \rho_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \qquad a + p^{n+1}\mathbb{Z} \longmapsto a + p^n\mathbb{Z}$$

the direct product of the rings $\mathbb{Z}/p^n\mathbb{Z}$, $n = 1, 2, \ldots$ and the cannonical projections.

[1]Important results for considered diophantine problem are obtained in [2],[3],[5],[7],[10],[11]

Definition 9 *The ring $\mathbb{Z}_p$ of p-adic integers is defined by*

$$\mathbb{Z}_p = \{(x_n) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \mid \rho_n(x_{n+1}) = x_n\},$$

with operations given by componentwise addition and multiplication.

Remark 10 *The map $\mathbb{Z} \longrightarrow \mathbb{Z}_p \quad n \longmapsto (n+p\mathbb{Z}, n+p^2\mathbb{Z}, \ldots, n+p^n\mathbb{Z}, \ldots)$ is inclusion, therefore $\mathbb{Z}$ can be considered as subring of $\mathbb{Z}_p$.*

Definition 10 *The field $\mathbb{Q}_p$ of the p-adic rational numbers is defined as a field of fractions for $\mathbb{Z}_p$.*

Remark 11 *The map $\mathbb{Q} \longrightarrow \mathbb{Q}_p \quad a \longmapsto a$ is inclusion, thus $\mathbb{Q}$ can be considered as subfield of $\mathbb{Q}_p$.*

Remark 12 *The map $\mathbb{Z}_p \longrightarrow \mathbb{F}_p \quad a \longmapsto a + p\mathbb{Z}$ is surjective ring homomorphism with kernel $p\mathbb{Z}_p$. Therefore*

$$\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p.$$

Remark 13 *$E/\mathbb{Q} \; : \; y^2 = x^3 + ax^2 + bx + c$ can be transformed to an elliptic curve with integral coefficients: let u be the least common multiplier of the denominators of the coefficients a, b, c. The change $(x, y) \longmapsto (X, Y)$ defined by $X = u^2x, \; Y = u^3y$ transforms the equation to the equation $Y^2 = X^3 + au^2X^2 + bu^4X + cu^6$ which has integral coefficients.*

Remark 14 *Let $E/\mathbb{Q}_p$ be an elliptic curve over $\mathbb{Q}_p$. With a modification of the above remark, we may assume that $E/\mathbb{Q}_p$ has coefficients in $\mathbb{Z}_p$. By reduction of the coefficients of E modulo $p\mathbb{Z}_p$, we obtain a curve $\tilde{E}$ with coefficients in $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. The map $E/\mathbb{Q}_p \longrightarrow \tilde{E}/\mathbb{F}_p$ is called* reduction.

Acknowledgement

Miroslav Stoenchev is supported by the Bulgarian National Science Fund under Young Scientists Project KP-06 M32/2-17.12.2019. Venelin Todorov is supported by the NSP ”Information and Communication Technologies for a Single Digital Market in Science, Education and Security (ICT in SES)”, contract No DO1-205/23.11.2018 and by the BNSF under Project DN 12/5-2017.

REFERENCES

[1] S. Apostolov, M. Stoenchev, V. Todorov, One parameter family of elliptic curves and the equation $x^4 + y^4 + kx^2y^2 = z^4$, Studies in Computational Intelligence, Springer, (2020)

[2] A. Bremner, J. Jones, On the equation $x^4 + y^4 + mx^2y^2 = z^2$, Journal of Number Theory 50, 286-298 (1995).

[3] E. Brown, $x^4 + y^4 + mx^2y^2 = z^2$: Some cases with only trivial solutions - and a solution Euler missed, Glasgow Math. J.31 (1989) 297-307.

[4] J.W.S. Cassels, Lectures on elliptic curves, Cambridge University Press, 1991.

[5] L. Euler, De casibus quibus formulam $x^4 + mxxyy + y^4$ ad quadratum reducere licet, Mem.acad.sci. St. Petersbourg 7 (1815/16, 1820), 10-22; Opera Omnia, ser. I, V, 35-47, Geneva, 1944.

[6] V. A. Kolyvagin, On the Mordell-Weil Group and the Shafarevich-Tate Group of Modular Elliptic Curves , Proceedings of the International Congress of Mathematicians, Kyoto, Japan, 1990 ,pp. 429-436.

[7] H. C. Pocklington, Some diophantine impossibilities, Proc. Cambridge Phil. Soc. 17 (1914), 108-121.

[8] J. H. Silverman, The arithmetic of elliptic curves, Springer Verlag, New York/Berlin, 1986.

[9] J. H. Silverman, J. Tate, Rational points on elliptic curves, Springer Verlag, New York, 1992.

[10] T. N. Sinha, A class of quartic diophantine equations with only trivial solutions, *Amer.J.Math.* **100** (1978), 585-590.

[11] M. Z. Zhang, On the diophantine equation $x^4 + kx^2y^2 + y^4 = z^2$, *Sichuan Daxue Xuebao* **2** (1983), 24-31.

[12] http://magma.maths.usyd.edu.au/calc/

[13] https://math.mit.edu/classes/18.783/2017/lectures.html