Symmetric Diophantine Systems

Miroslav Stoenchev
Department of Mathematics,
Technical University of Sofia,
Bulgaria

INTRODUCTION

In the present work we consider Diophantine systems, i.e. systems of polynomial equations of several variables with rational coefficients. Such a sistem is called *locally trivial*, if it has a nonzero p-adic rational solution for all primes p, including $p=\infty$, or moreover, *globally trivial*, if it has a nonzero rational solution in $\mathbb{Q}$. From *global triviality* follows *local triviality*, but the converse is not valid by Selmer's counterexample $3x^3+4y^3+5z^3=0$. An interesting question is (see [2]): *for which classes of Diophantine systems, the notions of local and global triviality* are equivalent? Systems fulfilling this condition are said to satisfy the *local-to-global principle*. Natural examples of symmetric Diophantine systems arise in Euclidean Geometry, in problems for integer lengths of elements of geometric figures. As a result of considering many examples, we formulate conjecture, that *any symmetric Diophantine system derived from Euclidean Geometry, satisfies the local-to-global principle*.Below we consider several examples confirming the conjecture, without formalizing it in general.

BASIC DEFINITIONS AND THEOREMS

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 ([1], [3], [4], [7]).

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

The zero point of $\mathbb{A}^n$ is $O_{\mathbb{A}^n}=(0,\ldots,0)$, 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 $(x_0,\ldots,x_n)$, $(y_0,\ldots,y_n)\in\mathbb{A}^{n+1}(\overline{\mathbb{Q}})-O_{\mathbb{A}^{n+1}}$ are equivalent, if there exists $\lambda\in\overline{\mathbb{Q}}^*$, such that $y_0=\lambda x_0,\ldots,y_n=\lambda x_n$. An equivalence class $\{(\lambda x_0,\ldots,\lambda x_n)\mid\lambda\in\overline{\mathbb{Q}}^*\}$ is denoted by $[x_0,\ldots,x_n]$, and the individual $x_0,\ldots,x_n$ are called homogeneous coordinates for the corresponding point of $\mathbb{P}^n$.*

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*

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6, \tag{1}$$

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

If $char(k)\neq 2$, the substitution $y\longmapsto(y-a_1x-a_3)/2$ simplify the equation (1) to $y^2=x^3+ax^2+bx+c$. 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 $E/k:\ y^2=f(x)$ is defined as $\Delta_E=16\Delta_f=16(-4a^3c+a^2b^2+18abc-4b^3-27c^2)$.

Let E/k be an elliptic curve given by equation $y^2=f(x)$. Therefore $E\subset\mathbb{P}^2(\bar{k})$ consists of the points $P=(x,y)$ satisfying the equation of E, together with the point at infinity $O=[0,1,0]$. Let $l\subset\mathbb{P}^2(\bar{k})$ 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 a 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, $E(k) \lhd E(\overline{\mathbb{Q}})$, 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 $P \in E_1(\bar{k})$, 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 $E_2(\bar{k})$. 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.*

Remark 3 *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 $E[m] \cong \mathbb{Z}/m\mathbb{Z} \bigoplus \mathbb{Z}/m\mathbb{Z}$.*

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 rank $A = r$.*

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

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*.

Theorem 3 *(Lutz-Nagell) Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve with integer coefficients and $P = (x,y)$ be a rational torsion point for E, of order not dividing 2. Then x and y are integers.*

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:*

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

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

THE MAIN CONJECTURE AND EXAMPLES

In this section we formulate the main conjecture and consider several examples of symmetric diophantine systems that confirm it. Examples 3 and 4 below are open-ended questions: they are locally trivial systems for which it is not known whether they have solutions in positive integers.

Conjecture 1 *Any symmetric system derived from Euclidean Geometry, satisfies the local-to-global principle.*

Example 1 *Is there a quadrilateral, without pairs of equal sides, with integer lengths of the sides, diagonals and radii of the inscribed and circumscribed circle?*

The question is equivalent to the solvability of the Diophantine system

$$a+c=b+d, \ \ r^2=\frac{abcd}{(a+c)^2}, \ \ R^2=\frac{(ab+cd)(ac+bd)(ad+bc)}{16abcd}, \tag{3}$$

where (a,b,c,d,R,r,e,f) are the lengths of the sides, the radii and the diagonals. Let

$$a+c=b+d=l, \ abcd=m^2, \ (ab+cd)(ac+bd)(ad+bc)=n^2, \ \ \frac{m}{l}\in\mathbb{Z}, \frac{n}{4m}\in\mathbb{Z}. \tag{4}$$

The systems (3) and (4) are equivalent to each other, and their solvability is equivalent to (5), see Appendix A:

$$(x^2+y^2)(z^2+t^2)[(xz+yt)^2+(xt+yz)^2]=w^2, \ \gcd(x,y)=\gcd(z,t)=1, \ \min\{xy,zt\}>1. \tag{5}$$

Equation (5) is equivalent to each of the following systems (6) and (7):

$$(x^2+y^2)(z^2+t^2)=s(u-v)^2, \ \ xyzt=suv, \ \ p^2\nmid s. \tag{6}$$

$$\frac{x^2+y^2}{s_1}\frac{z^2+t^2}{s_2}=(u-v)^2, \ \ \frac{xy}{s_2}\frac{zt}{s_1}=uv, \ \ p^2\nmid s_1s_2=s. \tag{7}$$

In particular, the substitution $s_1=1, \ s_2=z^2+t^2$ leads to

$$x^2+y^2=(u-v)^2, \ \ xyzt=(z^2+t^2)uv. \tag{8}$$

Therefore $x=m^2-n^2, \ y=2mn, \ u-v=m^2+n^2, \ \gcd(m,n)=1$, and then substitute in the second equation of (8):

$$(z^2+t^2)v^2+(z^2+t^2)(m^2+n^2)v-2ztmn(m^2-n^2)=0. \tag{9}$$

The discriminant of the last equation needs to be a perfect square $D=r^2$:

$$r^2 = D = (z^2+t^2)^2(m^2+n^2)^2 + 8zt(z^2+t^2)mn(m^2-n^2). \tag{10}$$

Set $X' = m/n,\ Y' = r/n^2,\ \alpha = z^2+t^2,\ \beta = zt$ and thus we obtain a two-parameter elliptic family:

$$\mathbf{E}_{\alpha,\beta} : Y'^2 = \alpha^2 X'^4 + 8\alpha\beta X'^3 + 2\alpha^2 X'^2 - 8\alpha\beta X' + \alpha^2. \tag{11}$$

Weierstrass normal form for $\mathbf{E}_{\alpha,\beta}$ is (see Appendix B)

$$\mathbf{E}_{\alpha,\beta} : Y^2 + 4\beta XY - 4\beta(\alpha^2-4\beta^2)Y = X^3 - (\alpha^2-8\beta^2)X^2 - 4\beta^2(\alpha^2-4\beta^2)X. \tag{12}$$

Lemma 1 *The rational torsions of $\mathbf{E}_{\alpha,\beta}$ do not generate a solution of (3), and satisfy*

$$\mathbf{E}_{\alpha,\beta}(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 1 \text{ or } 2.$$

Proof 1 *Let $P = (x,y) \in \mathbf{E}_{\alpha,\beta}$ and denote $[m]P = (x_m, y_m)$, where $(x,y) = (x_1,y_1)$. Then by the group law of $\mathbf{E}_{\alpha,\beta}$, (using duplication formula [3]) one obtains*

$$x_2 = \frac{x^4 + 24\beta^2(\alpha^2-4\beta^2)x^2 - 32\beta^2(\alpha^2-4\beta^2)^2x + 16\beta^2(\alpha^2-3\beta^2)(\alpha^2-4\beta^2)^2}{4x^3 - 4(\alpha^2-12\beta^2)x^2 - 48\beta^2(\alpha^2-4\beta^2)x + 16\beta^2(\alpha^2-4\beta^2)^2}, \tag{13}$$

$$y_2 = \frac{x^3 + 4\beta(\alpha^2-4\beta^2)[5\beta x + y - 4\beta(\alpha^2-4\beta^2)] - [3x^2 - 2(\alpha^2-16\beta^2)x + 4\beta y - 20\beta^2(\alpha^2-4\beta^2)]x_2}{2y + 4\beta x - 4\beta(\alpha^2-4\beta^2)}. \tag{14}$$

Assume that $P \in \mathbf{E}_{\alpha,\beta}(\mathbb{Q})[m]$, i.e. $P \in \mathbf{E}_{\alpha,\beta}(\mathbb{Q})$ with $[m]P = O$. Then, by theorem 3, it follows that x_m and y_m are integers, or $P \in \mathbf{E}_{\alpha,\beta}(\mathbb{Q})[2]$. By theorem 5, it follows $1 \le m \le 12$ and $m \ne 11$. We will consider several cases with $P \ne O$:

1. *$m = 2$. Then $[2]P = O \Longleftrightarrow P = -P \Longleftrightarrow (x,y) = (x, -y - 4\beta x + 4\beta(\alpha^2-4\beta^2)) \Longleftrightarrow y = -2\beta x + 2\beta(\alpha^2-4\beta^2)$. Substituting in equation 12 we obtain the equation $-4\beta^2[x-(\alpha^2-4\beta^2)]^2 = x(x+4\beta^2)[x-(\alpha^2-4\beta^2)]$. Hence the points $(\alpha^2-4\beta^2, 0),\ (2\beta(\alpha-2\beta), 2\alpha\beta(\alpha-2\beta)),\ (-2\beta(\alpha+2\beta), 2\alpha\beta(\alpha+2\beta))$ are all torsions of order 2 for $\mathbf{E}_{\alpha,\beta}$. These three points together with $O = [0,1,0]$ form a group $\mathbf{E}_{\alpha,\beta}(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Now using Mazur's theorem 5 we obtain that $\mathbf{E}_{\alpha,\beta}(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, for some $n \in \{1,2,3,4\}$. We will prove that the possible values for n are 1 and 2.*

2. *$m = 3$. Then $[3]P = O \Longleftrightarrow [2]P = -P \Longleftrightarrow (x_2,y_2) = (x, -y - 4\beta x + 4\beta(\alpha^2-4\beta^2))$. Let us denote equation (12) by $\mathbf{E}_{\alpha,\beta} : h(X,Y) = f(X)$ and we will prove that from $x_2 = x$ follows $y_2 = -y - 4\beta x + 4\beta(\alpha^2-4\beta^2)$. Indeed we have*

$$h(x,y) = f(x) = f(x_2) = h(x_2,y_2) = h(x,y_2)$$

$$\Rightarrow h(x,y) = h(x,y_2) \Rightarrow (y_2-y)[y_2+y+4\beta x - 4\beta(\alpha^2-4\beta^2)] = 0.$$

Since $P \ne O$, then $[2]P \ne O$ and therefore $y_2 \ne y$. Finally we have $y_2 + y + 4\beta x - 4\beta(\alpha^2-4\beta^2) = 0$. Consequently $P = (x,y)$ is a rational 3-torsion point of $\mathbf{E}_{\alpha,\beta}$, if and only if the equation $x_2 = x$ has an integer solution. Using (13) this equation is

$$g(x) = 3x^4 - 4(\alpha^2-12\beta^2)x^3 - 72\beta^2(\alpha^2-4\beta^2)x^2 + 48\beta^2(\alpha^2-4\beta^2)^2x - 16\beta^2(\alpha^2-3\beta^2)(\alpha^2-4\beta^2)^2 = 0 \tag{15}$$

Direct calculation shows that $g'(x) = [x-(\alpha^2-4\beta^2)][x+(2\alpha\beta+4\beta^2)][x-(2\alpha\beta-4\beta^2)]$ and $g(\alpha^2-4\beta^2) = -\alpha^2$, $g(-2\alpha\beta-4\beta^2) < 0,\ g(2\alpha\beta-4\beta^2) < 0$. Then $g(x) = 0$ has exactly two real roots x', x'', such that $x' < -(2\alpha\beta + 4\beta^2)$, $x'' > \alpha^2-4\beta^2$, and none of them are integers. Therefore rational torsion points of order 3 do not exist, which means that $\mathbf{E}_{\alpha,\beta}(\mathbb{Q})$ has no subgroups of order 3.

3. *$m=4$. Then $[4]P=O \Longleftrightarrow [2]P=-[2]P \Longleftrightarrow (x_2,y_2)=-(x_2,y_2) \Longleftrightarrow y_2=-y_2-4\beta x_2+4\beta(\alpha^2-4\beta^2)$. Hence $[2]P$ is a 2-torsion point, i.e. $[2]P \in \mathbf{E}_{\alpha,\beta}(\mathbb{Q})[2]$. From case **1** it follows that*

$$[2]P=(x_2,y_2) \in \{(\alpha^2-4\beta^2,0),\ (2\beta(\alpha-2\beta),2\alpha\beta(\alpha-2\beta)),\ (-2\beta(\alpha+2\beta),2\alpha\beta(\alpha+2\beta))\}.$$

We may assume that $[2]P=(\alpha^2-4\beta^2,0)$, hence $x_2=\alpha^2-4\beta^2, y_2=0$. Using formulas (13) and (14), the following system of equations for coordinates (x,y) of P is obtained:

$$\left| \begin{array}{r} x^4-4(\alpha^2-4\beta^2)x^3+4(\alpha^2-6\beta^2)(\alpha^2-4\beta^2)x^2+16\beta^2(\alpha^2-4\beta^2)^2x+16\beta^4(\alpha^2-4\beta^2)^2=0 \\ x^3-3(\alpha^2-4\beta^2)x^2+2(\alpha^2-6\beta^2)(\alpha^2-4\beta^2)x+4\beta^2(\alpha^2-4\beta^2)^2=0 \end{array} \right.$$

Multiplying by x the second equation of the system and subtracting from it the sum of the two equations of the system, one obtains $x^2-2(\alpha^2-4\beta^2)x-4\beta^2(\alpha^2-4\beta^2)=0$. Using that $\alpha=m^2+n^2, \beta=mn$, for the roots of the equation we find $x=2m^2(m^2-n^2)$ and $x=2n^2(n^2-m^2)$. Substituting $x=2m^2(m^2-n^2)$ in equation 12, we obtain the equation:

$$y^2+4mn(m^4-n^4)y-4m^4(m^4-n^4)^2=0,$$

with roots $y=-4m(m^4-n^4)(n\mp\sqrt{m^2+n^2})$. Therefore m^2+n^2 must be a perfect square and then

$$P=(x,y)=\left(2m^2(m^2-n^2),-4m(m^4-n^4)(n\mp\sqrt{m^2+n^2})\right),\ m=\gamma^2-\delta^2,\ n=2\gamma\delta. \tag{16}$$

All other possibilities for $[2]P$, that is $[2]P=(2\beta(\alpha-2\beta),2\alpha\beta(\alpha-2\beta))$ or $[2]P=(-2\beta(\alpha+2\beta),2\alpha\beta(\alpha+2\beta))$ leads to the same result as obtained above: m^2+n^2 must be a perfect square and P has the form (16).

4. *$m=8$. Thus $[8]P=O \Longleftrightarrow [4]P=-[4]P \Longleftrightarrow (x_4,y_4)=-(x_4,y_4)=(x_4,-y_4-4\beta x_4+4\beta(\alpha^2-4\beta^2))$. Consequently $[4]P$ is a two-torsion point and $[2]P$ must be a four-torsion. Then by (16), it follows that*

$$x_2=2m^2(m^2-n^2),\ \ y_2=-4m(m^4-n^4)(n\mp\sqrt{m^2+n^2}),\ \ m=\gamma^2-\delta^2,\ n=2\gamma\delta.$$

Using (13), the equation $x_2=2m^2(m^2-n^2)$ is reduced to quartic equation, which have no solutions in integers x. Therefore rational torsion points of order 8 do not exist.

It remains to prove that the elements of $\mathbf{E}_{\alpha,\beta}(\mathbb{Q})_{tors}$ do not generate a solution of (3). Let $P=(X,Y)$ be a 2-torsion, then by formulas (33) and (9) it follows that $m/n=X'=Y/\alpha X \in \{-1,0,1\}$. The latter result leads to $m=0$ or $m=n$, but in both cases it is valid that $x=m^2-n^2 \leq 0$, which is impossible. The case when P is a 4-torsion is analogous. The proof of lemma 1 is complete.

Remark 5 *Summarizing the results:* $\mathbf{E}_{\alpha,\beta}(\mathbb{Q})_{tors} \cong \left\{ \begin{array}{l} \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z},\ \ \sqrt{\alpha}\notin\mathbb{Q} \\ \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z},\ \ \sqrt{\alpha}\in\mathbb{Q} \end{array} \right.$, *where $\alpha=m^2+n^2, \beta=mn$.*

Lemma 2 *For all positive integers $\alpha=m^2+n^2, \beta=mn$, the inequality* $\mathbf{rank}\ \mathbf{E}_{\alpha,\beta}(\mathbb{Q}) \geq 1$ *holds.*

Proof 2 *It is sufficient to prove that the point $P=(0,0)$ has infinite order in $\mathbf{E}_{\alpha,\beta}(\mathbb{Q})$. Straightforward calculation for $[2]P=(x_2,y_2)$ shows that $[2]P=(\alpha^2-3\beta^2,-\beta(\alpha^2+\beta^2)) \neq O$, hence P is not a 2-torsion point. Moreover $[2]P$ is not a 2-torsion point, because*

$$[2]P \notin \mathbf{E}_{\alpha,\beta}(\mathbb{Q})[2]=\{(\alpha^2-4\beta^2,0),\ (2\beta(\alpha-2\beta),2\alpha\beta(\alpha-2\beta)),\ (-2\beta(\alpha+2\beta),2\alpha\beta(\alpha+2\beta)),\ O\}.$$

Indeed, the following equations have no solutions in nonzero integers: $(\alpha^2-3\beta^2,-\beta(\alpha^2+\beta^2))=(\alpha^2-4\beta^2,0)$,

$$(\alpha^2-3\beta^2,-\beta(\alpha^2+\beta^2))=(2\beta(\alpha-2\beta),2\alpha\beta(\alpha-2\beta)),$$

$$(\alpha^2-3\beta^2,-\beta(\alpha^2+\beta^2))=(-2\beta(\alpha+2\beta),2\alpha\beta(\alpha+2\beta)).$$

Since $[2]P$ is not a 2-torsion point, it follows that P is not a 4-torsion. Finally $P=(0,0)$ is not a two-torsion or a four-torsion, now from lemma 1 we obtain that P is not a torsion, which means that it has infinite order.

Remark 6 *In lemma 2 it is not necessary to use that 3-torsions and 8-torsions for* $\mathbf{E}_{\alpha,\beta}(\mathbb{Q})$ *do not exist. It is enough to prove that* $P=(0,0)$ *is not a 3 or 8-torsion point. Indeed, using (15) one obtains* $g(0)\neq 0$*, which shows that* $(0,0)$ *is not a 3-torsion. Similarly, P has order 8, if and only if* $[2]P$ *has order 4, which is reduced to* $x_2=2m^2(m^2-n^2)$*, or equivalently* $(m^2+n^2)^2-3m^2n^2=2m^2(m^2-n^2)$ *with no nonzero rational solutions.*

Lemma 3 *Each generator of* $\mathbf{E}_{\alpha,\beta}(\mathbb{Q})$*, which is not a torsion, generates an infinite series of solutions to (3).*

Proof 3 *By lemma 2 one have that, for any positive integers* z,t *the rank of* $\mathbf{E}_{z^2+t^2,zt}(\mathbb{Q})$ *is at least 1. Let* $P=(X,Y)$ *be a generator of infinite order for* $\mathbf{E}_{z^2+t^2,zt}(\mathbb{Q})$*, with* $Y/\alpha X>1$*. By the transformation (33) we obtain the point* (X',Y') *on the curve (11), and we determine positive integers* m,n *from the equality* $m/n=X'$*. Then set* $x=m^2-n^2,\ y=2mn$*, and using the 4-tuple* (x,y,z,t) *and the formulas in Appendix B, one obtains integer 8-tuple* (a,b,c,d,R,r,e,f)*. Let us denote by* (X_n,Y_n) *for all* $n\in\mathbb{Z}$ *the coordinates of* $[n]P$*. It remains to prove that there are infinitely many n, for which* $Y_n/\alpha X_n>1,\ \alpha=z^2+t^2$*. Finally, for every* $n\in\mathbb{Z}$ *at least one of the points* $\pm[n]P,\pm[n+1]P,\pm[n+2]P,\pm[n+3]P$ *satisfies the desired inequality* $Y/\alpha X>1$*, which completes the proof.*

As an example, the minimal integral quadrilateral without equal sides is given below

$$(a,b,c,d,R,r,e,f)=(546,1890,1560,216,975,280,1680,750).$$

Remark 7 *Quadrilateral is inscribed in a circle and circumscribed around another circle. If the lengths of the sides and the radii are rational numbers, then the lengths of the diagonals are also rational. Thus each rational 6-tuple* (a,b,c,d,R,r)*, up to homothety, generates a unique integer 8-tuple* (a,b,c,d,R,r,e,f)*. Applying the described method, we obtain an infinite series of integral quadrilaterals, without pairs of equal sides, none of which are homothetic, and for which* $(a,b,c,d,R,r,e,f)\in\mathbb{N}^8$*.*

Remark 8 *From lemma 2 follows that there are infinitely many non-equivalent solutions for system (3) and moreover, equation (5) has infinitely many solutions for each pair* (x,y) *of positive integers. In table* **I** *below are given some solutions of equation (5). The proof of lemma 3 describes an algorithm for obtaining integral quadrilaterals through these solutions. The corresponding quadrilaterals are given in table* **II***, such that k-th row of table* **I** *corresponds to k-th row of table* **II***.*

TABLE I: **Integral quadrilaterals** $(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d},\mathbf{R},\mathbf{r})$ **via** $(\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{t},\mathbf{w})$

(z,t)	$P=(X,Y)$	$[n]P=(X_n,Y_n)$	(m,n)	(x,y,z,t,w)
$(2,1)$	$(-16,0)$	$[3]P=\left(\frac{3344}{841},\frac{543400}{24389}\right)$	$(65,58)$	$(861,7540,2,1,312856525)$
$(3,1)$	$(-36,1200)$	$[-3]P=\left(\frac{227484}{11881},\frac{553544400}{1295029}\right)$	$(730,327)$	$(425971,477420,3,1,5172025730050)$
$(4,1)$	$(56,520)$	*	$(28,11)$	$(663,616,4,1,16877345)$
$(4,3)$	$(21/4,525/8)$	*	$(31,2)$	$(957,124,4,3,25972975)$
$(5,2)$	$(702,9918)$	$P+(0,0)$	$(25099,6279)$	$(590533960,315193242,5,2,16297119093004699156)$

TABLE II: **Integral quadrilaterals** $(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d},\mathbf{R},\mathbf{r})$

a	**b**	**c**	**d**	**R**	**r**
27450402	139670960	120195140	7974582	$312856525/4$	12983880
2374657551903	2514093242580	887156644020	747720953343	$2586012865025/2$	610101224460
8292804	8052352	1926232	2166684	$16877345/4$	1633632
12888876	2083200	1252524	12058200	$25972975/4$	1424016
8140611413220274000	5646775632112163640	1737997051478698920	4231832832586809280	4074279773251174789	1861323133634983200

In table **III** are given higher rank curves in the elliptic family $\mathbf{E}_{\alpha,\beta}$. It is an interesting question to find an upper-bound for the rank of $\mathbf{E}_{\alpha,\beta}$.

TABLE III: **Higher rank curves in the elliptic family $\mathbf{E}_{\alpha,\beta}$**

(α,β)	**rank $\mathbf{E}_{\alpha,\beta}$**	**generators of $\mathbf{E}_{\alpha,\beta}$**
$(442,21)$	3	$(0,0)$
		$(-17000,3978000)$
		$(-154052/9,368297792/27)$
$(1768,84)$	3	$(-28224,0)$
		$(6594500,-12959511400)$
		$(155648,894353408)$
$(442k^2,21k^2)$	3	$(0,0)$
		*
		*

Example 2 *Find all $N \in \mathbb{N}$, such that there exist N numbers with the properties*
(i) all numbers are perfect squares of positive integers,
(ii) the sum of any two numbers is a perfect square.

The question for $N = 3$ is equivalent to the solvability of the Diophantine system

$$x^2+y^2=u^2,\ \ y^2+z^2=v^2,\ \ z^2+x^2=w^2. \tag{17}$$

The system (17) is equivalent to each of the following systems (18) and (19):

$$x=(k^2-l^2)d_1,\ y=2kld_1,\ z=(m^2-n^2)d_2, y=2mnd_2,\ z=2std_3,\ x=(s^2-t^2)d_3 \tag{18}$$

$$(k^2-l^2)d_1=(s^2-t^2)d_3,\ kld_1=mnd_2,\ (m^2-n^2)d_2=2std_3. \tag{19}$$

The elimination of d_i's from system (19) leads to the following equivalent equations (20) - (24):

$$\frac{m^2-n^2}{2mn}\frac{s^2-t^2}{2st}=\frac{k^2-l^2}{2kl}. \tag{20}$$

$$2mnstk^2-l(m^2-n^2)(s^2-t^2)k-2mnstl^2=0. \tag{21}$$

The discriminant of the last equation needs to be a perfect square $D=r^2$:

$$r^2=D=l^2\left[(m^2-n^2)^2(s^2-t^2)^2+(4mnst)^2\right]. \tag{22}$$

Therefore

$$(m^2-n^2)(s^2-t^2)=(a^2-b^2)c,\ \ 2stmn=abc,\ \ (m,n)=(s,t)=(a,b)=1. \tag{23}$$

$$\frac{m^2-n^2}{c_2}\frac{s^2-t^2}{c_1}=a^2-b^2,\ \ 2\frac{mn}{c_1}\frac{kl}{c_2}=ab,\ \ c=c_1c_2. \tag{24}$$

In particular, set $c_1=1,\ c_2=m^2-n^2$ and thus we obtain

$$s^2-t^2=a^2-b^2,\ \ 2mnst=(m^2-n^2)ab. \tag{25}$$

$$s^2-t^2=a^2-b^2,\ \ ab=2mnh,\ \ st=(m^2-n^2)h \tag{26}$$

In particular, the substitution $a=2mnh_1h_2,\ b=h_3h_4,\ s=h_1h_4,\ t=(m^2-n^2)h_2h_3$, leads to

$$\left[(2mnh_1)^2+(m^2-n^2)^2h_3^2\right]h_2^2=(h_1^2+h_3^2)h_4^2 \tag{27}$$

$$h_1^2+h_3^2=rh_2^2,\ \ (2mnh_1)^2+(m^2-n^2)^2h_3^2=rh_4^2 \tag{28}$$

Put $r=1$ in (28), therefore $h_1=2UV,\ h_3=U^2-V^2$ and (28) is equivalent to

$$U^4+V^4+\rho U^2V^2=W^2,\ \text{where } \rho=\left(\frac{4mn}{m^2-n^2}\right)^2-2,\ W=\frac{h_4}{m^2-n^2}. \tag{29}$$

Consequently, the problem for $N=3$ is reduced to finding a non-trivial rational point on quartic surface $U^4+V^4+\rho U^2V^2=W^2S^2$. From [5], page 4, it follows that the problem is equivalent to finding ρ, such that the elliptic curve $\mathbf{E}_\rho: Y'^2=X'^3+\rho X'^2+X'$ has rank greater or equal to 1. Using transformation formulas from [5], i.e.

$$X'=\left(\frac{V}{U}\right)^2,\quad X=q^2X',\quad Y=q^3Y', \tag{30}$$

and substitute $p=16m^2n^2-2(m^2-n^2)^2, q=m^2-n^2, \rho=\frac{p}{q^2}$, we obtain isomorphic elliptic curves $\mathbf{E}_\rho\simeq\mathbf{E}_{p,q}$ where $\mathbf{E}_{p,q}: Y^2=X^3+pX^2+q^4X$. We use Magma software [6] to find the generators of Mordell-Weil group for the elliptic curves in tables **I**, **III** and below.

Set $m=4,n=3$, then $p=2206, q=7$ and **rank** $\mathbf{E}_{2206,7}(\mathbb{Q})=1$. The point $\left(\frac{121}{9},\frac{17776}{27},1\right)$ is a generator for $\mathbf{E}_{2206,7}(\mathbb{Q})$. By the formulas (30) it follows that $\left(\frac{V}{U}\right)^2=X'=X/q^2=\left(\frac{11}{21}\right)^2\Rightarrow U=21, V=11$

$$(h_1,h_2,h_3,h_4)=(320,562,462,11\ 312),$$

$$(a,b,s,t)=(6\ 231\ 456,\ 3\ 619\ 840,\ 5\ 226\ 144,1\ 258\ 880),$$

$$x=(s^2-t^2)d_3,\ y=2mnd_2=2mn\frac{2std_3}{m^2-n^2}=2d_3\frac{2mnst}{m^2-n^2}=2abd_3,\ z=2std_3.$$

Putting $d_3=1$ and dividing by $2^{10}.7^2$ leads to solution

$$(x,y,z,u,v,w)=(512\ 751\ 161,\ 899\ 110\ 080,\ 262\ 240\ 440,\ 1\ 035\ 042\ 361,\ 936\ 573\ 000,\ 575\ 919\ 961).$$

Remark 9 *The described method gives an infinite series of non-equivalent solutions to example 2, in the case $N=3$. We will consider the case $N\geq 4$ and the examples below, as well as the formalization of the main conjecture in our next publications.*

Example 3 $x^2+y^2=u^2,\ y^2+z^2=v^2,\ z^2+x^2=w^2,\ x^2+y^2+z^2=s^2$.

Example 4 $x^2+y^2=u^2,\ y^2+z^2=v^2,\ z^2+x^2=w^2,\ x^2+y^2+z^2=s^2,\ x^2y^2+y^2z^2+z^2x^2=t^2$.

APPENDIX A

We will find parametric description for all two by two different integers a,b,c,d, for wich

$$(*)\ \ a+c=b+d=l,\ \ abcd=m^2,\ \ (ab+cd)(ac+bd)(ad+bc)=n^2.$$

Then we separate these (a,b,c,d) having the property: $m\equiv 0 \mod l,\ n\equiv 0 \mod 4m$. Let $\gcd(a,b,c,d)=k$, then $\frac{l}{k},\frac{m}{k^2},\frac{n}{k^3}$ are integers, and we can consider the system $(*)$ by changing $(l,m,n)\longmapsto(\frac{l}{k},\frac{m}{k^2},\frac{n}{k^3})$ and $\gcd(a,b,c,d)=1$. Therefore, we can assume that $\gcd(a,b,c,d)=1$. Let $\gcd(a,l)=l_a, \gcd(b,l)=l_b$, easily showing that the following equalities are valid:

$$\gcd(a,l)=\gcd(c,l)=\gcd(a,c),\ \gcd(b,l)=\gcd(d,l)=\gcd(b,d),$$

$$\gcd(l_a,l_b)=\gcd(\gcd(a,c),\gcd(b,d))=\gcd(a,b,c,d)=1.$$

Then $a=a_1l_a,\ b=b_1l_b,\ l=l_al_bL,\ m=lM$ and from $ab(l-a)(l-b)=m^2$ we obtain

$$a_1b_1(l_bL-a_1)(l_aL-b_1)=L^2M^2.$$

Since $\gcd(a_1,l_bL)=\gcd(b_1,l_aL)=1$, then $\gcd(a_1b_1(l_bL-a_1)(l_aL-b_1),L)=1$ and therefore $L=1$. Thus $l=l_al_b$ and $a_1b_1(l_b-a_1)(l_a-b_1)=M^2$. Let $\gcd(a_1,b_1)=u,\ \gcd(l_b-a_1,l_a-b_1)=v,\ a_1=ua_2,\ b_1=ub_2$, then $\gcd(a_2,b_2)=\gcd(u,v)=1$ and $M=uvM_1$, with the equality

$$a_2b_2\frac{l_b-ua_2}{v}\frac{l_a-ub_2}{v}=M_1^2.$$

From $\gcd(a_2b_2,v)=\gcd(a_2\frac{l_a-ub_2}{v},b_2\frac{l_b-ua_2}{v})=1$ it follows that $M_1=\alpha\beta$ and the following equations are valid

$$a_2\frac{l_a-ub_2}{v}=\alpha^2,\ \ b_2\frac{l_b-ua_2}{v}=\beta^2.$$

We represent a_2,b_2 in the form $a_2=\alpha_1\alpha_2^2,\ b_2=\beta_1\beta_2^2$, hence $\alpha=\alpha_1\alpha_2A,\ \beta=\beta_1\beta_2B$, $\gcd(\alpha_1\alpha_2A,\beta_1\beta_2B)=1$, $p^2\nmid\alpha_1\beta_1$, and thus we obtain the equalities

$$l_a=v\alpha_1A^2+u\beta_1\beta_2^2,\ \ l_b=v\beta_1B^2+u\alpha_1\alpha_2^2.$$

We express a,b,c,d and replace in the third equation of $(*)$

$$a=u\alpha_1\alpha_2^2(v\alpha_1A^2+u\beta_1\beta_2^2),\ b=u\beta_1\beta_2^2(v\beta_1B^2+u\alpha_1\alpha_2^2),$$

$$c=v\beta_1B^2(v\alpha_1A^2+u\beta_1\beta_2^2),\ d=v\alpha_1A^2(v\beta_1B^2+u\alpha_1\alpha_2^2),$$

$$ab+cd=\alpha_1\beta_1l_al_b[(u\alpha_2\beta_2)^2+(vAB)^2],$$

$$ac+bd=uv\alpha_1\beta_1[(\alpha_2l_aB)^2+(\beta_2l_bA)^2],$$

$$ad+bc=uvl_al_b[(\alpha_1\alpha_2A)^2+(\beta_1\beta_2B)^2].$$

After substitution, we find that $n=uv\alpha_1\beta_1l_al_bN$, for some positive integer N. Therefore

$$[(u\alpha_2\beta_2)^2+(vAB)^2][(\alpha_2l_aB)^2+(\beta_2l_bA)^2][(\alpha_1\alpha_2A)^2+(\beta_1\beta_2B)^2]=N^2. \tag{31}$$

To simplify the above equation, set $\alpha_2=A,\beta_2=B$ and replace in (31):

$$(u^2+v^2)(l_a^2+l_b^2)[(\alpha_1A^2)^2+(\beta_1B^2)^2]=\left(\frac{N}{A^2B^2}\right)^2.$$

Then $N=A^2B^2N_1$ and set $x=a_2=\alpha_1A^2,y=b_2=\beta_1B^2,z=u,t=v,w=N_1$, thus $l_a=vx+uy,l_b=ux+vy$ and the equation is transformed in the form

$$(x^2+y^2)(z^2+t^2)[(xz+yt)^2+(xt+yz)^2]=w^2. \tag{32}$$

APPENDIX B

Using the notation and results of appendix A, one obtains that each solution of equation (5) corresponds to a rational 6-tuple (a,b,c,d,R,r) in the form

$$a = xz(xt+yz),\ b = yz(xz+yt),$$

$$c = yt(xt+yz),\ d = xt(xz+yt),$$

$$R = \frac{w}{4},\ r = xyzt.$$

In the case when (a,b,c,d,R,r) is rational, it is a straightforward to prove that the diagonals are also rational, since

$$e = \frac{(ad+bc)(ac+bd)}{4rR(a+c)},\ \ f = \frac{(ab+cd)(ac+bd)}{4rR(a+c)}.$$

Then we multiply (a,b,c,d,R,r,e,f) by the least common multiply of the denominators to obtain an integer 8-tuple.

Now we describe the birational isomorphism between the curves (11) and (12), ([1], p35). For any positive integers $\alpha = m^2+n^2, \beta = mn, m \neq n$, the quartic curve $\mathbf{E}_{\alpha,\beta}$ defined by (11) is nonsingular and contains a rational point, for example $(0,\pm\alpha)$, therefore $\mathbf{E}_{\alpha,\beta}$ is birational equivalent to an elliptic curve defined by (12). The isomorphism is given by

$$(X',Y') \longmapsto (X,Y)$$

$$X = \frac{1}{2}\left(\alpha^2 X'^2 + \alpha Y'^2 + 4\alpha\beta X' + \alpha^2 - 8\beta^2\right),\ \ Y = \frac{\alpha X'}{2}\left(\alpha^2 X'^2 + \alpha Y'^2 + 4\alpha\beta X' + \alpha^2 - 8\beta^2\right).$$

The inverse transformation is given by

$$X' = \frac{Y}{\alpha X},\ \ Y' = \frac{1}{\alpha}\left(2X - \frac{Y^2}{X^2} - 4\beta\frac{Y}{X} - (\alpha^2 - 8\beta^2)\right). \tag{33}$$

ACKNOWLEDGMENTS

The author would like to thank the Research and Development Sector at the Technical University of Sofia for the financial support.

REFERENCES

1. J.W.S. Cassels, Lectures on elliptic curves, Cambridge University Press, 1991.
2. B. Mazur, On the passage from local to global in number theory, American Mathematical Society, Volume 29, Number 1, July 1993, Pages 14-50.
3. J. H. Silverman, The arithmetic of elliptic curves, Springer Verlag, New York/Berlin, 1986.
4. J. H. Silverman, J. Tate, Rational points on elliptic curves, Springer Verlag, New York, 1992.
5. M. Stoenchev, V. Todorov, On the classical diophantine equation $x^4+y^4+kx^2y^2 = z^2$, AIP Conference Proceedings 2333, 110002 (2021), https://doi.org/10.1063/5.0042739
6. http://magma.maths.usyd.edu.au/calc/
7. https://math.mit.edu/classes/18.783/2017/lectures.html