On the vertices of the elliptic curves

Cristina-Liliana Pripoae, Gabriel-Teodor Pripoae

Abstract. We investigate the elliptic curves, expressed in the Weierstrass form, from a differential geometric viewpoint. The curvature function is carefully studied and bounds for the number of vertices of the elliptic curves are given. As a generalization, a program for the classification of algebraic curves is sketched, using geometric invariants.

M.S.C. 2010: 53A04, 14H52, 11G05.
Key words: metric classification of elliptic curves; metric classification of algebraic curves; vertices; curvature function.

1 Introduction

The growing interest in the study of elliptic curves is motivated, mainly, by their applications in Criptography ([1], [2]). Despite a huge amount of litterature about them, several important problems remain still open. One such a problem is their classification over the real field. The topological and the affine classification follow from the respective classifications of cubics ([5], [6]; see also [3]).

The metric clasification of the cubics (in particular, of the elliptic curves) was pointed as an interesting open field in 2007 by Viro, in a widely disseminated lecture.

In §2, we begin the study of elliptic curves (in their Weierstrass form), using techniques of classical differential geometry. We show that these elliptic curves are completely determined by a point and the velocity vector in that point, behaving like geodesics. We look for the number of their vertices. Numerical simulations lead us to the following conjecture:

Any elliptic curve in the Weierstrass form $y^2 = x^3 + ax + b$ *has: 4 or 6 vertices, if* $4a^3 + 27b^2 > 0$*; 8 or 10 vertices, if* $4a^3 + 27b^2 < 0$.

Additional support for the conjecture is provided by the main result of this paper (§3):

Consider an elliptic curve in the Weierstrass form.

(i) If $4a^3 + 27b^2 > 0$*, then the number of vertices is an even number between 4 and 16.*

Balkan Journal of Geometry and Its Applications, Vol.21, No.2, 2016, pp. 73-81.

(ii) If $4a^3+27b^2<0$, then the number of vertices is an even number between 8 and 18.

(iii) Suppose $a=0$. If $b<\frac{1}{27}$, then the number of vertices is 4. If $b>\frac{1}{27}$, then then the number of vertices is 6.

(iv) Suppose $b=0$. If $a>0$, then the number of vertices is 4. If $a<-\frac{1}{9}$, then the number of vertices is 10.If $-\frac{1}{9}\leq a<0$, then the number of vertices is 8.

Several examples, supporting the conjecture, are also provided.

In §4 we sketch a program for classifying the real, non-singular, irreducible algebraic curves, using three integer invariants. For conics and (partially) for cubics, we give the tables with the respective classes.

2 The differential geometry of elliptic curves

All the elliptic curves considered herein will have real coefficients. Define

$$EL_1=\{(a,b)\in\mathbb{R}^2\mid 4a^3+27b^2>0\}\ ,\ \ EL_2=\{(a,b)\in\mathbb{R}^2\mid 4a^3+27b^2<0\}$$

and $EL=EL_1\cup EL_2$. For each $(a,b)\in EL$, consider the elliptic curve $E_{a,b}$, given by the implicit equation in $\mathbb{R}^2$, written in the Weierstrass form:

$$y^2=x^3+ax+b. \tag{2.1}$$

The set $E_{a,b}$ has one or two connected components if (a,b) belongs to EL_1 or EL_2, respectively. We may parameterize the upper branch of $E_{a,b}$ as

$$c(t)=(t,\sqrt{t^3+at+b}). \tag{2.2}$$

The geometric properties corresponding to the lower branch will be deduced by symmetry; for the properties around the points of intersection of $E_{a,b}$ with the horizontal axis, we shall use the implicit form. The curve c is defined on $D=\{t\in\mathbb{R}\mid t^3+at+b>0\}$. The curvature function of c is $k:D\to\mathbb{R}$,

$$k(t)=2\frac{3t^4+6at^2+12bt-a^2}{(9t^4+4t^3+6at^2+4at+a^2+4b)^{3/2}} \tag{2.3}$$

and its derivative

$$\begin{aligned} k'(t)= \ & 12[-9t^7-t^6-33at^5-(5a+90b)t^4+(5a^2-20b)t^3+\\ & +(5a^2-24ab)t^2+(5a^3+4ab)t+a^3+8b^2+2a^2b]\times\\ & \times(9t^4+4t^3+6at^2+4at+a^2+4b)^{-5/2}. \end{aligned} \tag{2.4}$$

We can express the curvature function, using the implicit equation of $E_{a,b}$:

$$k(x,y)=-2\frac{9x^4+6ax^2-12xy^2+a^2}{(9x^4+6ax^2+4y^2+a^2)^{3/2}}. \tag{2.5}$$

Proposition 2.1. *Let $t_1\in D$ be an arbitrary fixed parameter for c. Then the curve c (hence also $E_{a,b}$) is completely determined by $c(t_1)$ and $\dot{c}(t_1)$.*

Proof. Denote $(x_1, y_1) := c(t_1)$ and $(1, z_1) := \dot{c}(t_1)$. A short calculation leads to

$$a = 2y_1z_1 - 3x_1^2 \ , \ b = y_1^2 - 4x_1^3 - 2x_1y_1z_1. \tag{2.6}$$

It follows that both c and $E_{a,b}$ are completely determined. □

Remarks 2.2. (i) The Proposition 2.1 exhibits an interesting similarity of elliptic curves with the geodesics: both kinds of curves are completely determined by (their value in) a point and the "velocity" vector there.

(ii) Let x_1, y_1 and z_1 three (arbitrary and fixed) real numbers ($y_1 > 0$), such that $4(2y_1z_1 - 3x_1^2)^3 + 27(y_1^2 - 4x_1^3 - 2x_1y_1z_1)^2 \neq 0$, i.e. the triple (x_1, y_1, z_1) does not belong to the algebraic surface

$$32y^3z^3 - 36x^2y^2z^2 + 648x^4yz + 324x^6 + 27y^4 - 216x^3y^2 - 108xy^3z = 0. \tag{2.7}$$

Then there exists a unique elliptic curve $y^2 = x^3 + ax + b$, with a and b subject to (2.6), such that it passes through (x_1, y_1) and its velocity there be $(1, z_1)$.

The surface (2.7) is cone-like; the two halves correspond to EL_1 and EL_2, and may be characterized by strict inequalities in (2.7), instead of equality.

Proposition 2.3. *There exists a unique non-negative $t_0 \in D$, zero of the curvature function k.*

Proof. Consider the equation $k(t) = 0$. From (2.3), we get

$$3t^4 + 6at^2 + 12bt - a^2 = 0 \tag{2.8}$$

or, in equivalent form,

$$12t(t^3 + at + b) = (3t^2 + a)^2$$

and deduce that the solutions of (2.8) must be positive. Denote by $\varphi(t)$ the left side of (2.8). The function $\varphi : D \to \mathbb{R}$ has the derivative $\varphi' = 12(t^3 + at + b)$ strictly positive on D.

Denote by $(t_1, 0)$ a point of intersection of $E_{a,b}$ with the axis Ox; as $sgn\varphi(t_1) = sgnk(t_1, 0) < 0$, we deduce that equation (2.8) has a unique solution $t_0 > 0$. We denote $A = (t_0, \sqrt{t_0^3 + at_0 + b})$. □

Remarks 2.4. (i) In fact, the core of Proposition 2.3. is well-known, under another formalism, in the algebraic theory of elliptic curves. The point A has order three in the group associated to $E_{a,b}$ and is the inflexion point, unique on the upper branch of the curve $E_{a,b}$.

(ii) Consider $E_{a,b}$ an elliptic curve given by (2.1). Fix a non-null real number α and make a coordinate change

$$x = \alpha^2\tilde{x} \ \ , \ \ y = \alpha^3\tilde{y}. \tag{2.9}$$

Thus, $E_{a,b}$ transforms to $\tilde{E}_{\tilde{a},\tilde{b}}$, where $a = \alpha^4\tilde{a}$ and $b = \alpha^6\tilde{b}$.

A simple calculation shows that, in general, $E_{a,b}$ and $\tilde{E}_{\tilde{a},\tilde{b}}$ have distinct curvature functions k and $\tilde{k}$, so the curvature is not an invariant for (2.9). Instead, we have the

Proposition 2.5. *Let $E_{a,b}$ and $\tilde{E}_{\tilde{a},\tilde{b}}$ be as in the previous remark. Let t_0 be the zero of the curvature function k. Then the zero of the curvature function $\tilde{k}$ is $\tilde{t}_0 = \alpha^{-2}t_0$.* (The zero of the curvature function is an invariant with respect to (2.9)).

3 The vertices of the elliptic curves

Theorem 3.1. The following assertions hold true:

(i) The number of vertices of an elliptic curve is an even number from 4 to 18.

(ii) If $4a^3 + 27b^2 > 0$, then the number of vertices is an even number from 4 to 16.

(iii) If $4a^3 + 27b^2 < 0$, then the number of vertices is an even number from 8 to 18.

(iv) Suppose $a = 0$. If $b < \frac{1}{27}$, then the number of vertices is 4. If $b > \frac{1}{27}$, then then the number of vertices is 6.

(v) Suppose $b = 0$. If $a > 0$, then the number of vertices is 4. If $a < -\frac{1}{9}$, then the number of vertices is 10. If $-\frac{1}{9} \leq a < 0$, then the number of vertices is 8.

Proof. We use a "brute force" method, by checking case-by-case.

(i) Step 1. Consider $E_{a,b}$ an elliptic curve, given by (2.1). A vertex is a critical point of the curvature function (2.5). So, we are looking for solutions of the system:

$$f(x,y) = 0 \ , \ \ k_x(x,y)\, f_y(x,y) - k_y(x,y)\, f_x(x,y) = 0.$$

The second equation writes, successively:

$$2y\, k_x(x,y) + (3x^2 + a)\, k_y(x,y) = 0 \ \ \Leftrightarrow$$

$$y\{y^2(9x^4 + 6ax^2 + 4y^2 + a^2) + 2x(3x^2 + a)(9x^4 + 6ax^2 - 12xy^2 + a^2)\} = 0.$$

The points $(x, 0)$ on the curve are solutions, so any point of order 2 is a vertex (by abuse, the point at infinity $\mathcal{O}$ is considered a vertex also). (Hence, there exist at least 2 or 4 vertices, accordingly to the type of the curve).

The other vertices come in pairs; so, it suffices to look for those of the form $c(t)$, where t is a solution of the equation $k'(t) = 0$, with the function k' given in (2.4). By symmetry with respect to the Ox-axis, we find their opposites. Obviously, the total number of vertices must be even.

We consider the function $h : D \to \mathbb{R}$,

$$h(t) = -9t^7 - t^6 - 33at^5 - (5a + 90b)t^4 + (5a^2 - 20b)t^3 +$$

$$+(5a^2 - 24ab)t^2 + (5a^3 + 4ab)t + a^3 + 8b^2 + 2a^2b.$$

The equation $k'(t) = 0$ is equivalent to $h(t) = 0$. As this polynomial function has the degree 7, it may have 1,3,5 or 7 real roots. It may also happen that some of these real roots do not belong to D.

We deduce that the number of vertices is: at least 2 and at most 16, if $(a, b) \in EL_1$; at least 4 and at most 18, if $(a, b) \in EL_2$. In what follows, we shall refine the lower bounds.

Step 2. Denote $t_1 \in D$ the (biggest) root of the equation $t_1^3 + at_1 + b = 0$ (if $(a, b) \in EL_1$, there is only one root). From relation (2.5), we deduce $k(t_1, 0) = -2(3t_1^2 + a)^{-1}$; this value of the curvature is strictly negative, as $(3t_1^2 + a) > 0$ nearby t_1. Thus the curvature function k has a (strictly negative) minimum in t_1, then goes toward the (unique) zero t_0. We have $k'(t_1) = 0$ and for some values greater than t_1, the function k' is positive. As $\lim_{t\to\infty} k'(t) < 0$, it follows that there exists at least one more zero

of k', greater than t_1. Together with its opposite, it increases the lower bound of the numbers of vertices by 2.

On another hand, if $(a,b) \in EL_2$, the bounded component of $E_{a,b}$ is a simple, closed curve; using the Four Vertices Theorem, it follows that on that component there exist at least 4 vertices of that curve.

From these two arguments, we deduce that there exist at least 4 vertices, if $(a,b) \in EL_1$ and at least 8 vertices, if $(a,b) \in EL_2$. The lower bound estimate in (i),(ii) and (iii) is proved.

(iv) Suppose $a = 0$. The function h and its derivative become

$$h(t) = -9t^7 - t^6 - 90bt^4 - 20bt^3 + 8b^2$$

$$h'(t) = -3t^2 g(t) \ , \ \text{where} \ \ g(t) = 9t^4 + 3t^2 + 60bt + 10b$$

As $g'' > 0$, it follows that g' has a unique real root; we deduce that g has at most two real roots. Hence h has at most three real roots.

Denote $t_1 = (-b)^{\frac{1}{3}}$; we have $D = (t_1, \infty)$.

Consider the case $b < 0$. We have $g'(t_1) > 0$, $h(t_1) > 0$, g' positive and strictly increasing on D.

If $g(t_1) > 0$, then h is strictly decreasing on D from positive values to $-\infty$. If $g(t_1) \leq 0$, then h is strictly increasing from $h(t_1)$ to a positive maximum, and strictly decreasing afterthat to $-\infty$. In both cases, h has one, and only one, zero on D; in this case, the curve has 4 vertices.

Consider the case $b > 0$. We have $g'(0) > 0$, $g(0) > 0$, $h'(0) = 0$ and $h(0) > 0$.

Suppose first that $b > 0.125$, i.e. $g'(t_1) > 0$. We deduce $g(t_1) < 0$ and $h(t_1) < 0$; it follows that h passes on D from negative to positive, then again to negative values, so it has exactly two zeroes.This implies that the elliptic curve has 6 vertices.

Suppose now that $0 < b < 0.125$, so $g'(t_1) < 0$. As in the previous case, h has a unique zero on $(0, \infty)$.We shall refine the study for $(t_1, 0)$.

Denote $b_1 = ((-5 + \sqrt{178})/51)^3 \approx 0.00437$ and $b_2 = ((5 + \sqrt{178})/51)^3 \approx 0.0465$. We have $g(t_1) > 0$ if, and only if, $b \in (b_1, b_2)$.

It is an easy calculation to show that $h(t_1) > 0$ if, and only if, $b < 1/27 \approx 0.037$.

For $b \in (b_2, 0.125)$ we have $g'(t_1) < 0$, $g(t_1) < 0$, $h'(t_1) > 0$ and $h(t_1) < 0$. We derive that h has a unique zero on $(t_1, 0)$; in this case, the curve has 6 vertices.

For $b \in (1/27, b_2)$ we have $g'(t_1) < 0$, $g(t_1) > 0$, $h'(t_1) < 0$ and $h(t_1) < 0$. The function h has a unique zero on $(t_1, 0)$; in this case, the curve has 6 vertices.

For $b \in (0, b_1)$ we have $g'(t_1) < 0$, $g(t_1) > 0$, $h'(t_1) < 0$ and $h(t_1) > 0$. The function h has no zero on $(t_1, 0)$; in this case, the curve has 4 vertices.

For $b \in (b_1, 1/27)$, we have $g'(t_1) < 0$, $g(t_1) > 0$, $h'(t_1) < 0$ and $h(t_1) > 0$. There exist $t_5 \in (t_1, 0)$ such that $g'(t_5) = 0$. As $g(t_5) \geq 0$, we get h strictly decreasing on $(t_1, 0)$, and has no more zeros there.In this case, the curve has 4 vertices.

(v) Suppose $b = 0$. The function h becomes

$$h(t) = -9t^7 - t^6 - 33at^5 - 5at^4 + 5a^2t^3 + 5a^2t^2 + 5a^3t + a^3$$

Consider the case $a > 0$. Then, the derivatives $h^{(4)}$, $h^{(5)}$, $h^{(6)}$ are strictly negative on $D = (0, \infty)$ and $h(0) > 0$, $h'(0) > 0$, $h''(0) > 0$,$h^{(3)}(0) > 0$, $h^{(4)}(0) < 0$, $h^{(5)}(0) < 0$, $h^{(6)}(0) < 0$.By studying the variation of h, h', h'', h''', we conclude that on D, the function h has at most one zero. This implies that the elliptic curve has 4 vertices.

Consider the case $a < 0$. Then $D = (-\sqrt{-a}, 0) \bigcup (\sqrt{-a}, \infty)$.

We calculate $h^{(6)}(\sqrt{-a}) < 0$, $h^{(5)}(\sqrt{-a}) < 0$, $h^{(4)}(\sqrt{-a}) < 0$, $h^{(3)}(\sqrt{-a}) > 0$, $h''(\sqrt{-a}) > 0$,$h'(\sqrt{-a}) > 0$,$h(\sqrt{-a}) > 0$. By studying the variation of h on $(\sqrt{-a}, \infty)$, we deduce h is strictly increasing up to a positive value, then strictly decreasing to $-\infty$; thus, on $(\sqrt{-a}, \infty)$, h has one, and only one, zero.

If $-1/3969 < a < 0$, then $h^{(6)}(-\sqrt{-a}) < 0$, $h^{(5)}(-\sqrt{-a}) > 0$, $h^{(4)}(-\sqrt{-a}) < 0$, $h^{(3)}(-\sqrt{-a}) > 0$, $h''(-\sqrt{-a}) > 0$, $h'(-\sqrt{-a}) < 0$, $h(-\sqrt{-a}) > 0$. Moreover, $h^{(6)} < 0$ on D. By studying the variation of h on $(-\sqrt{-a}, 0)$, we deduce h in strictly decreasing from a positive value to a negative value; thus, on $(-\sqrt{-a}, 0)$, h has one, and only one, zero.This implies that the elliptic curve has 8 vertices.

If $a \leq -1/3969$, then $h^{(6)} > 0$ on $[-\sqrt{-a}, -1/63) < 0$, $h^{(6)}(-1/63) = 0$ and $h^{(6)} < 0$ on $(-1/63, 0] < 0$. We study the variation of h and its derivatives up to the fifth, on $[-\sqrt{-a}, -1/63)$ and $[-1/63, 0)$. The key which provides the two different behaviors is given by the sign of $h(-\sqrt{-a})$. In fact, we have $h(-\sqrt{-a}) > 0$ if, and only if, $a > -\frac{1}{9}$, leading to a unique zero of h in $[-\sqrt{-a}, 0)$ and to a total of 8 vertices for the elliptic curve. The complementary case involves two zeros of h in $[-\sqrt{-a}, 0)$ and to a total of 10 vertices. □

Remark 3.2. The number of vertices is not invariant under the transformations (2.9). Indeed, the curve $E_{0,1}$ has 6 vertices and the curve $E_{0,10^{-6}}$ has 4 vertices (in this case, $\alpha = 10$).

Examples 3.3. (Case $4a^3 + 27b^2 > 0$) (i) Suppose $a = b = 1$. Then $y^2 = x^3 + x + 1$. The unique real root of the equation $x^3 + x + 1 = 0$ is -0.68233. The function k vanishes in 0.08014 (and -1.2226, not in D). The function k' vanishes in -0.475927, in 0.521333 (and -1.66173, not in D). So, the curve has 6 vertices: $\mathcal{O}$, (-0.68233,0), (-0.475927,0.645579), (0.521333,0.580495), (-0.475927,-0.645579), (0.521333,-0.580495).

(ii)Suppose $a = 1, b = 0$. Then $y^2 = x^3 + x$. The unique real root of the equation $x^3 + x = 0$ is 0. The function k vanishes in 0.39332 (and -0.39332, not in D). The function k' vanishes in 1.86 (and -0.234415 and -2.06399, not in D). So, the curve has 4 vertices: $\mathcal{O}$, (0,0), (1.86,2.88), (1.86,-2.88).

Examples 3.4. (Case $4a^3 + 27b^2 < 0$) (i)Suppose $a = -3, b = 1.9$. Then $y^2 = x^3 - 3x + 1.9$. The real roots of the equation $x^3 - 3x + 1.9 = 0$ are -1.9881, 0.811401,1.1774. The function k vanishes in 1.51176 (and -2.9811, not in D). The function k' vanishes in -1.14733, 0.38675, 1.92053 (and -0.99721 and -3.93491, not in D). So, the curve has 10 vertices: $\mathcal{O}$, (-1.9881,0), (0.811401,0),(1.1774,0),(-1.14733,1.957), (-1.14733,-1.957), (0.38675,0.893), ((0.38675,-0.893), (1.92053,2.285), (1.92053,-2.285).

(ii) Suppose $a = -3, b = -1$. Then $y^2 = x^3 - 3x - 1$. The real roots of the equation $x^3 + x = 0$ are -1.53, -0.347,1.879. The function k vanishes in 2.79. The function k' vanishes in -1.04, 3.75 (and -2.83, -0.33 and 0.89, not in D). So, the curve has 8 vertices: $\mathcal{O}$, (-1.53,0), (-0.347,0),(1.879,0),(-1.04,0.99), (-1.04,-0.99), (3.75,6.36), (3.75,-6.36).

4 Program for the metric classification of algebraic curves

Consider $f \in \mathbb{R}[X,Y]$ an irreducible polynomial of degree n and $C : f(x,y) = 0$ a non-singular algebraic curve. Denote $f_x = \frac{\partial f}{\partial x}$, $f_{xy} = \frac{\partial^2 f}{\partial x \partial y}$,... and so on. The curvature function of C is given by

$$k(x,y) = \frac{\alpha(x,y)}{(\beta(x,y))^{3/2}},$$

where $\alpha, \beta \in \mathbb{R}[X,Y]$ and

$$\alpha = f_y^2 f_{xx} - 2 f_x f_y f_{xy} + f_x^2 f_{yy} \quad , \quad \beta = f_x^2 + f_y^2.$$

Obviously, $deg\ \beta = (n-1)^2$; also, $deg\ \alpha \leq n^2 - n - 1$ and one can easily provide examples with the upper limit effectively reached. We denote the number of the roots of α by $zer(k)$. The number $deg\ \alpha$ is invariant under projective transformations, but (in general) is not invariant under Cremona transformations.

A vertex of $\mathcal{C}$ is a critical point of the curvature function. We denote the number of vertices by $ver(\mathcal{C})$. The number $zer(k)$ (or $ver(\mathcal{C})$) is infinite, if and only if $\mathcal{C}$ is a line (or a line or a circle, respectively).

Theorem 4.1. (i) *If $zer(k)$ is finite, then $zer(k) \leq n^3 - n^2 - n$.*

(ii) *If $ver(\mathcal{C})$ is finite, then $ver(\mathcal{C}) \leq 2n^3 - 2n^2 - 2n$.*

Proof. (i) We have $deg\ f = n$, $deg\ \alpha \leq n^2 - n - 1$. By the theorem of Bezout, the number of solutions for the system

$$f(x,y) = 0 \ , \ \alpha(x,y) = 0$$

is at most $n(n^2 - n - 1)$.

(ii) The critical points of the curvature function are solutions of the system

$$(2\alpha_x\ \beta - 3\alpha\ \beta_x) f_y - (2\alpha_y\ \beta - 3\alpha\ \beta_y) f_x = 0 \ , \ f(x,y) = 0.$$

The degree of the first polynomial is at most $2n^2 - 2n - 2$. We apply the theorem of Bezout and obtain as maximum number of solutions $n(2n^2 - 2n - 2)$. □

Remark 4.2. We propose a *classification program for the real, algebraic, non-singular, irreducible curves* having as only invariants the following positive integers: $deg\ \alpha$, $zer(k)$ and $ver(\mathcal{C})$.

We exclude the lines (i.e. n=1), for which we have: $deg\ \alpha = 0$, $zer(k) = \infty$ and $ver(\mathcal{C}) = \infty$.

For the conics (i.e. n=2), the classification is contained in Table 1. For the cubics (i.e. n=3), we give the (uncomplete) classification, in Table 2. Here, the families of cubics are those in "canonical form" (Newton [4]), described by: (I): $xy = ax^3 + bx^2 + cx + d$; (II): $y^2 = ax^3 + bx^2 + cx + d$; (III): $xy^2 + ey = ax^3 + bx^2 + cx + d$; (IV): $y = ax^3 + bx^2 + cx + d$.

Table 1: Conics classification

Conic	$deg\ \alpha$	$zer(k)$	$ver(\mathcal{C})$
parabola	0	0	1
hyperbola	2	0	2
(proper)ellipse	2	0	4
circle	0	0	∞

Table 2: Cubics classification

cubic	$deg\alpha$	$zer(k)$	$ver(\mathcal{C})$
I	2	1	≤ 7
II	4	2	≤ 18
III	5	≤ 15	≤ 24
IV	1	1	2

We remark that the family (IV) is completely classified, by an elementary study of a real function of one variable (which we omit here). For the family (II), the (partial) result rests on our study in §3. For the resting two families, the exact classification (beyond the upper limitation for $zer(k)$ and $ver(\mathcal{C})$) is (still) an open problem.

Remark 4.3. Another important (open) problem is the maximal invariance group of this (projected) classification for the algebraic curves. Obviously, the isometries group of $\mathbb{R}^n$ must be a subgroup into it. As seen in the elliptic curves classification, it may be enlarged. To what extent - this needs further investigation.

References

[1] I. F. Blake, G. Seroussi, N. P. Smart (eds.), *Advances in Elliptic Curve Cryptography*, Cambridge Univ. Press, N.Y. 2005.

[2] D. Hankerson, A. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography* , Springer Verlag, 2004.

[3] M. Nadjafikah, *Affine differential invariants for planar curves*, Balkan J. Geom. Appl. 7, 1 (2002), 69-78.

[4] I. Newton, *Mathematical Works*, **2**, N.Y., Johnson Reprint Corp., 1967, 135-161.

[5] D. Weinberg, *The affine classification of cubic curves*, Rocky Mount. J. Math. 18, 3 (1988), 655-664.

[6] D. Weinberg, *The topological classification of cubic curves*, ibid., (1988).

Authors' addresses:

Cristina Liliana Pripoae
Academy of Economics Studies, Department of Applied Mathematics,
Piata Romana 6, Bucharest, 010374, Romania.

Gabriel Teodor Pripoae

University of Bucharest, Department of Mathematics,
14 Academiei Str., Bucharest, 010014, Romania.
E-mail: gpripoae@yahoo.com