Multiplicative group law on the folium of Descartes

Steluţa Pricopie and Constantin Udrişte

Abstract. The folium of Descartes is still studied and understood today. Not only did it provide for the proof of some properties connected to Fermat's Last Theorem, or as Hessian curve associated to an elliptic curve, but it also has a very interesting property over it: a multiplicative group law. While for the elliptic curves, the *addition* operation is compatible with their geometry (additive group), for the folium of Descartes, the *multiplication* operation is compatible with its geometry (multiplicative group).

The original results in this paper include: points at infinity described by the Legendre symbol, a group law on folium of Descartes, the fundamental isomorphism and adequate algorithms, algorithms for algebraic computation.

M.S.C. 2010: 11G20, 51E15.
Key words: group of points on Descartes folium, algebraic groups, Legendre symbol, algebraic computation.

1 Introduction

An elliptic curve is in fact an abelian variety G that is, it has an addition defined algebraically, with respect to which it is a group G (necessarily commutative) and 0 serves as the identity element. Elliptic curves are especially important in number theory, and constitute a major area of current research; for example, they were used in the proof, by Andrew Wiles (assisted by Richard Taylor), of Fermat's Last Theorem. They also find applications in cryptography and integer factorization (see, [1]-[5]).

Our aim is to show that the folium of Descartes also has similar properties and perhaps more. Section 2 refers to the folium of Descartes and its rational parametrization. Section 3 underlines to connection between the points at infinity for this curve and the Legendre symbol. Section 4 gives the geometrical meaning of the multiplicative group law on folium of Descartes, excepting the critical point. The law was proposed by the second author and to our knowledge is the first time it appears in

Balkan Journal of Geometry and Its Applications, Vol. 18, No. 1, 2013, pp. 54-70.

the mathematical literature. Section 5 spotlights an isomorphism between the group on the folium of Descartes and a multiplicative group of integers congruence classes. Section 6 formulates to conclusions and open problems.

2 Folium of Descartes

The folium of Descartes is an algebraic curve defined by the equation

$$x^3 + y^3 - 3axy = 0.$$

Descartes was first to discuss the folium in 1638. He discovered it in an attempt to challenge Fermat's extremum-finding techniques. Descartes challenged Fermat to find the tangent straightline at arbitrary points and Fermat solved the problem easily, something Descartes was unable to do. In a way, the folium played a role in the early days of the development of calculus.

If we write $y = tx$ we get $x^3 + t^3x^3 - 3atx^2 = 0$. Solving this for x and y in terms of t ($t^3 \neq -1$) yields the parametric equations

$$x(t) = \frac{3at}{1+t^3}, \quad y(t) = \frac{3at^2}{1+t^3}.$$

The folium is symmetrical about the straightline $y = x$, forms a loop in the first quadrant with a double point at the origin and has an asymptote given by $x+y+a = 0$.

The foregoing parametrization of folium is not defined at $t = -1$. The left wing is formed when t runs from -1 to 0, the loop as t runs from 0 to $+\infty$, and the right wing as t runs from $-\infty$ to -1.

It makes sense now why this curve is called "folium"- from the latin word folium which means "leaf". It's worth mentioning that, although Descartes found the correct shape of the curve in the positive quadrant, he believed that this leaf shape was repeated in each quadrant like the four petals of a flower.

3 Points at infinity

According to Eves [1], infinity has been introduced into geometry by Kepler, but it was Desargues, one of the founders of projective geometry, who actually used this idea. Addition of the points and the straightline at infinity metamorphoses the Euclidean plane into the projective plane. Projective geometry allows us to make sense of the fact that parallel straightlines meet at infinity, and therefore to interpret the points at infinity.

Even if in projective geometry no two straightlines are parallel, the essential features of points and straightlines are inherited from Euclidean geometry: any two distinct points determine a unique straightline and any two distinct straightlines determine a unique point.

Let K be a field. The two-dimensional affine plane over K is denoted

$$\mathbf{A}_K^2 = \{(x, y) \in K \times K\}.$$

The two-dimensional projective plane $\mathbf{P}^2_K$ over K is given by equivalence classes of triples (x, y, z) with $x, y, z \in K$ and at least one of x, y, z nonzero.

Two triples (x_1, y_1, z_1) and (x_2, y_2, z_2) are said to be *equivalent* if there exists a nonzero element $\lambda \in K^*$ such that

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2).$$

We denote by $(x : y : z)$ the equivalence class whose representative is the triple (x, y, z).

The points in $\mathbf{P}^2_K$ with $z \neq 0$ are the "finite" points in $\mathbf{P}^2_K$ (because they can be identified with points in the affine plane). If $z = 0$ then, considering that dividing by zero gives ∞, we call the points $(x : y : 0)$ "points at infinity" in $\mathbf{P}^2_K$.

Now let's return to our cubic given by $x^3 + y^3 - 3axy = 0$. Its homogeneous form is $x^3 + y^3 - 3axyz = 0$.

The points (x, y) on the affine space correspond to the points $(x : y : 1)$ in the projective space. To see what points lie at infinity, we set $z = 0$ and obtain $x^3+y^3 = 0$, which is equivalent with $(x + y)(x^2 - xy + y^2) = 0$. We now have two possibilities:

1. $x + y = 0$. In this case we find the point at infinity $\infty_1 = (-1 : 1 : 0)$.
2. $x^2 - xy + y^2 = 0$. We consider this as an equation in the unknown x, with the parameter y, and we compute the discriminant $\Delta = -3y^2$. If there is an element $\alpha \in K$ such that $\alpha^2 = -3$, then, rescaling by y, we have the following two points at infinity

$$\infty_2 = \left(\frac{1+\alpha}{2} : 1 : 0\right), \qquad \infty_3 = \left(\frac{1-\alpha}{2} : 1 : 0\right).$$

Remark If we have 3 points at infinity, the sum of their x coordinates is zero. For example, when $K = \mathbb{R}$, since $(-1 : 1 : 0) = (1 : -1 : 0)$, we can imagine that the point at infinity ∞_1 lies on the "bottom" and on the "top" of every straightline that has slope -1.

3.1 Legendre symbol

Of course, we want to know when we have just one point at infinity and when we have 3 points at infinity. To decide we need the *Legendre symbol* which helps us decide whether an integer a is a perfect square modulo a prime number p.

For an odd prime p and an integer a such that $p \not| a$, the Legendre symbol $\left(\dfrac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} \ \ 1, \text{ if } a \text{ is a quadratic residue of } p \\ -1, \text{ otherwise.} \end{cases}$$

The Legendre symbol has the following properties:

1. (Euler's Criterion) Let p be an odd prime and a any integer with $p \not| a$. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ mod \ (p).$$

2. Let p be an odd prime, and a and b be any integers with $p \not| ab$. Then

   (a) If $a \equiv b \bmod (p)$, then $\left(\dfrac{a}{p}\right) \equiv \left(\dfrac{b}{p}\right)$.

   (b) $\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right) = \left(\dfrac{ab}{p}\right)$.

   (c) $\left(\dfrac{a^2}{p}\right) = 1$.

3. If p is an odd prime, then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, \text{ if } a \equiv 1 \bmod (4) \\ -1, \text{ if } a \equiv -1 \bmod (4). \end{cases}$$

4. If p is an odd prime, then

$$\left(\frac{2}{p}\right) = \begin{cases} 1, \text{ if } a \equiv \pm 1 \bmod (8) \\ -1, \text{ if } a \equiv \pm 3 \bmod (8). \end{cases}$$

5. (Law of Quadratic Reciprocity) Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Now we can give the following result.

Proposition 3.1. *Let K be a finite field of prime cardinal $p \neq 2, 3$ and let $\alpha^2 = -3$ (so α might lie in an extension of K).*

1. *If $p = 3r + 1$, then $\alpha \in K$.*
2. *If $p = 3r + 2$, then $\alpha \notin K$.*

Proof. First let us make the following two remarks: when $p = 3r + 1$, the element r cannot be an odd integer and when $p = 3r + 2$, the element r cannot be an even integer.

Now, the proof actually consists in computing the Legendre symbol $(\frac{-3}{p})$, in the sense that if this Legendre symbol is 1, then $\alpha \in K$ and if it equals -1, then $\alpha \notin K$.

1. Consider $p = 3r + 1$, where the element r is an even integer. We first compute the Legendre symbol

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} = (-1)^{3r} = 1.$$

   Consequently, there is an element $\alpha \in K$ such that $\alpha^2 = -3 \bmod (p)$.

2. Consider $p = 3r + 2$, where r is an odd integer. We have

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} = (-1)^{3r+2} = -1.$$

So in this case $\alpha \notin K$.

□

4 The group law on folium of Descartes

We shall define and study a multiplicative group on the non-singular points of folium of Descartes in an analogous way as the additive group on an elliptic curve. The group law is called "multiplication" and it is denoted by the symbol $\star$ (we underline that the operation over elliptic curves, motivated by geometry, is represented by the addition sign $+$).

For a better understanding of how the multiplicative law works on the folium of Descartes, we describe it for the field $\mathbb{R}$, because in this case we have a clear geometric interpretation.

Let $\mathcal{F}$ be the cubic given by the equation $x^3 + y^3 - 3axy = 0$, $a \in \mathbb{R}^*$, i.e., $\mathcal{F}$ is the folium of Descartes.

A first remark is that when $K = \mathbb{R}$ there is only one point at infinity in $\mathbf{P}^2_K$, so we denote it simply by ∞, keeping in mind that this is actually ∞_1.

Start with two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on $\mathcal{F}$. Define a new point S as follows. Draw the straightline ℓ through P_1 and P_2. This straightline intersects $\mathcal{F}$ in three points, namely P_1, P_2 and one other point P_3. We take that point P_3 and consider its symmetric S with respect to the bisectrix $y = x$. We define $P_1 \star P_2 = S$.

Of course there are a few subtleties to this law that need to be addressed. First, what happened when $P_1 = P_2$, i.e., how does $P_1 \star P_1$ work? In this case, the straightline ℓ becomes the tangent straightline to $\mathcal{F}$ at P_1. Then ℓ intersects $\mathcal{F}$ in one other point P_3 (in some sense, ℓ still intersects $\mathcal{F}$ in three points, but P_1 counts as two af them), and we consider that $P_1 \star P_1$ is the reflection of P_3 across the straightline $y = x$. We define $\infty \star \infty = \infty$.

Now we can assume that $P_1 \neq \infty$. The tangent ℓ has the slope

$$m = \frac{-x_1^2 + ay_1}{y_1^2 - ax_1}.$$

If $y_1^2 - ax_1 = 0$, then ℓ is the vertical straightline $x = x_1$, and this straightline intersects $\mathcal{F}$ in two points P_1 and P_3 that have same abscissa x. So $x_3 = x_1$ and to find y_3 we consider $y^3 - 3axy + x^3 = 0$ as an equation in terms of y. Because y_1 appears as a double root, we find that $y_3 = -2y_1$. So in this case $P_1 \star P_1 = (-2y_1, x_1)$.

If $y_1^2 - ax_1 \neq 0$, the equation of the straightline ℓ is given by the point-slope formulae $y = m(x - x_1) + y_1$. Next we substitute this into the equation for $\mathcal{F}$ and get

$$x^3 + (m(x - x_1) + y_1)^3 - 3ax(m(x - x_1) + y_1) = 0.$$

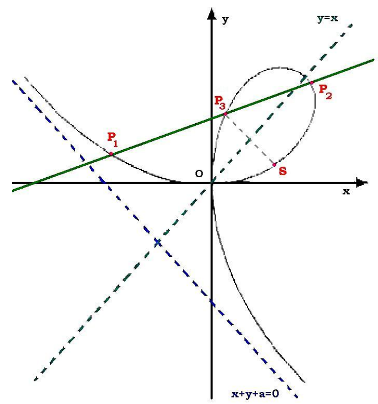

Figure 1: The group law on Folium of Descartes (main idea)

Now we can assume that $P_1 \neq \infty$. The tangent ℓ has the slope

$$m = \frac{-x_1^2 + ay_1}{y_1^2 - ax_1}.$$

If $y_1^2 - ax_1 = 0$, then ℓ is the vertical straightline $x = x_1$, and this straightline intersects $\mathcal{F}$ in two points P_1 and P_3 that have same abscissa x. So $x_3 = x_1$ and to find y_3 we consider $y^3 - 3axy + x^3 = 0$ as an equation in terms of y. Because y_1 appears as a double root, we find that $y_3 = -2y_1$. So in this case $P_1 \star P_1 = (-2y_1, x_1)$.

If $y_1^2 - ax_1 \neq 0$, the equation of the straightline ℓ is given by the point-slope formulae $y = m(x - x_1) + y_1$. Next we substitute this into the equation for $\mathcal{F}$ and get

$$x^3 + (m(x - x_1) + y_1)^3 - 3ax(m(x - x_1) + y_1) = 0.$$

This can be rearranged to the form

$$(m^3 + 1)x^3 + (-3m^3x_1 + 3m^2y_1 - 3ma)x^2 + \cdots = 0.$$

The three roots of this cubic equation correspond to the three points of intersection of ℓ with $\mathcal{F}$ (as mentioned before, P_1 is counted twice).

If $m = -1$ (this happens when $x_1 = y_1$), then $P_1 \star P_1 = \infty$. Otherwise, denote

$$s = \frac{3m^3x_1 - 3m^2y_1 + 3ma}{m^3 + 1}.$$

We can now say that $x_3 = s - 2x_1$ and, substituting in the equation for ℓ, $y_3 = m(s - 3x_1) + y_1$. We thus obtain that $P_1 \star P_1 = (m(s - 3x_1) + y_1, s - 2x_1)$.

Next we consider the case when $P_1 \neq P_2$. A special case here is when $x_1 = x_2$ (see Figure 5, left). Then ℓ is the vertical straightline $x = x_1$ and it intersects $\mathcal{F}$ in the point P_3, with $x_3 = x_1$ and $y_3 = -y_1 - y_2$. So $P_1 \star P_2 = (-y_1 - y_2, x_1)$.

If $x_1 \neq x_2$, then the straightline ℓ has the slope

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

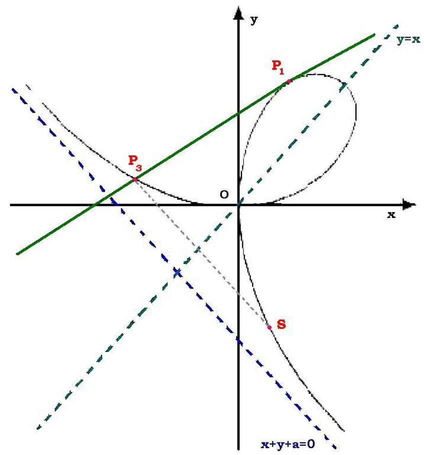

Figure 2: Multiplying a point P_1 to itself

and equation $y = m(x - x_1) + y_1$.

To find the intersection with $\mathcal{F}$, substitute to get

$$x^3 + (m(x - x_1) + y_1)^3 - 3ax(m(x - x_1) + y_1) = 0.$$

As seen before, this can be rearranged to the form

$$\begin{aligned} 0 &= (m^3 + 1)x^3 + (-3x_1 m^3 + 3y_1 m^2 - 3am)x^2 + (3{x_1}^2 m^3 - 6y_1 x_1 m^2 + \\ &\quad +(3ax_1 + 3y_1^2)m - 3ay_1)x + (-x_1^3 m^3 + 3y_1 x_1^2 m^2 - 3y_1^2 x_1 m + y_1^3). \end{aligned}$$

If $m = -1$, then $P_1 \star P_2 = \infty$ (this happens when $x_1 = y_2$ and $x_2 = y_1$ - see Figure 3, right).

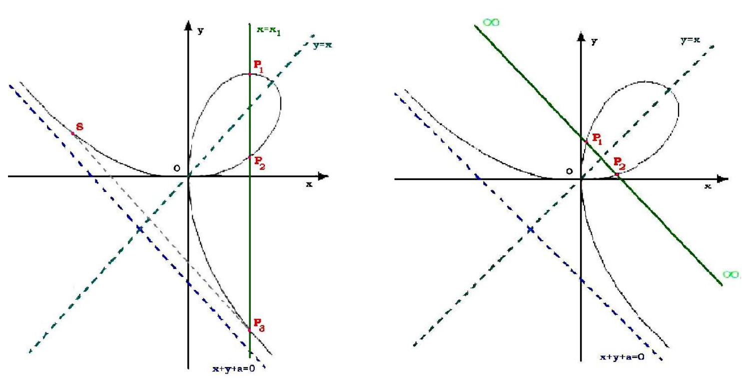

Figure 3: Special cases of point multiplication on Folium of Descartes

If $m \neq -1$, then we can consider

$$s = \frac{3x_1m^3 - 3y_1m^2 + 3am}{m^3 + 1}.$$

Keeping in mind that $s = x_1 + x_2 + x_3$, we can recover $x_3 = s - x_1 - x_2$ and then we find (substituting as we did many times before) $y_3 = m(s - 2x_1 - x_2) + y_1$. Therefore, we have $P_1 \star P_2 = (m(s - 2x_1 - x_2) + y_1, s - x_1 - x_2)$.

Theorem 4.1. *Let $\mathcal{F}_a(\mathbb{R}) = \{(x, y) \in \mathbb{R}^* \times \mathbb{R}^* | x^3 + y^3 - 3axy = 0\} \cup \{\infty\}$. Then $(\mathcal{F}_a(\mathbb{R}), \star)$ is a commutative group.*

Proof. The commutativity is obvious, the identity element is ∞ and the inverse of a point is its reflection across the straightline $y = x$. In fact all of the group properties are trivial to check except for the associative law. The associative law can be verified by a lengthy computation using explicit formulas, or by using more advanced algebraic or analytic methods (we do not present here a rigorous proof because we will do this later, in a different approach). $\square$

We consider next the case when the field K is a finite field with p elements, i.e. $K = F_p$. Although we do not have a geometric interpretation, the ideas presented before remain the same.

4.1 Case $p = 3r + 2$

In this case, because $m^3 = -1$ has the unique solution $m = -1$, we have only one point at infinity. So practically, all the results presented in the case $K = R$ are available here too.

We now give two algorithms, the first one being for the multiplication of a point P_1 with itself, and the second one is for the multiplication of two points P_1 and P_2 in general. In all that follows, the computations are made modulo p.

Algorithm: $StarSquare(P_1)$

1. If $P_1 = \infty$, then $P_1 \star P_1 = \infty$.
2. Otherwise, if $y_1^2 - ax_1 = 0$, then $P_1 \star P_1 = (-2y_1, x_1)$.
3. Otherwise, define m by $m = \dfrac{-x_1^2 + ay_1}{y_1^2 - ax_1}$.
4. If $m^3 + 1 = 0$, then $P_1 \star P_1 = \infty$.
5. Otherwise, define $s = \dfrac{3m^3x_1 - 3m^2y_1 + 3am}{m^3 + 1}$.

   Then $P_1 \star P_1 = (m(s - 3x_1) + y_1, s - 2x_1)$.

Algorithm: $StarProduct(P_1, P_2)$

1. If $P_1 = \infty$, then $P_1 \star P_2 = P_2$.
2. Otherwise, if $P_2 = \infty$, then $P_1 \star P_2 = P_1$.

3. Otherwise, if $P_1 = P_2$, then $P_1 \star P_2 = starsquare(P_1)$.
4. Otherwise, if $x_1 = x_2$ and $y_1 \neq y_2$, then $P_1 \star P_2 = (-y_1 - y_2, x_1)$.
5. Otherwise, define m by $m = \dfrac{y_2 - y_1}{x_2 - x_1}$.
6. If $m^3 + 1 = 0$, then $P_1 \star P_2 = [1, 0]$.
7. Otherwise let $s = \dfrac{3m^3x_1 - 3m^2y_1 + 3am}{m^3 + 1}$.

   Then $P_1 \star P_2 = (m(s - 2x_1 - x_2) + y_1, s - x_1 - x_2)$.

4.2 Case $p = 3r + 1$

In this case, we know that we have 3 points at infinity, each of them corresponding (in a way that we will see in the next section) to an element $\omega \in K$ with $\omega^3 = 1$.

We described point multiplication of non-singular points of folium of Descartes for all "finite" points. Because in this case we have more than one point at infinity, it is preferable to present this group law in the projective version. If we look at all points like points in projective plane, then we can treat all of them just in the same way.

The idea is the same. Let us start with two distinct points $P = (P_1 : P_2 : P_3)$ and $Q = (Q_1 : Q_2 : Q_3)$. They determine a unique straightline ℓ given by the following equation

$$\ell : \quad \begin{vmatrix} P_1 & P_2 & P_3 \\ Q_1 & Q_2 & Q_3 \\ x & y & z \end{vmatrix} = 0$$

or, equivalently

$$\ell : \quad (P_2Q_3 - P_3Q_2)x + (P_3Q_1 - P_1Q_3)y + (P_1Q_2 - P_2Q_1)z = 0.$$

A first remark is that if both P_3 and Q_3 equals 0, so they are both points at infinity, ℓ is the "ideal" straightline. So, when we intersect ℓ with our curve we also get a point at infinity. More precisely, we get the point R at infinity that is different from both P and Q. Using the observation made earlier we have that $R = (-P_1 - Q_1 : 1 : 0)$, so $P \star Q = (1 : -P_1 - P_2 : 0)$, which is the same as $P \star Q = \left(-\dfrac{1}{P_1 + P_2} : 1 : 0 \right)$.

If one of the point is finite, say P (so $P_3 = 1$), and the other one, Q, is a point at infinity (so $Q_1^3 = -1$, $Q_2 = 1$ and $Q_3 = 0$), then $P \star Q$ will be a finite point.

The equation of ℓ becomes $P_1 + Q_1y - x - P_2Q_1 = 0$.

Denote $m = \dfrac{1}{Q_1}$ and $n = \dfrac{P_2Q_1 - P_1}{Q_1}$ and replace $y = mx + n$ in $x^3 + y^3 - 3axy = 0$. We will get a quadratic equation in x, $a_2x^2 + a_1x + a_0 = 0$ with a known solution P_1. So the x coordinate of the point R is just the other solution on this equation, $R_1 = -\dfrac{a_1}{a_2} - P_1$ and $R_2 = mR_1 + n$.

Therefore, in this case $P \star Q = \left(m\left(-\dfrac{a_1}{a_2} - P_1 \right) + n : -\dfrac{a_1}{a_2} - P_1 : 1 \right)$.

In the same way, if P is a point at infinity and Q is a finite point, we have $P \star Q = \left(m\left(-\frac{a_1}{a_2} - Q_1 \right) + n : -\frac{a_1}{a_2} - Q_1 : 1 \right)$, where $m = \frac{1}{P_1}$, $n = \frac{P_1 Q_2 - Q_1}{P_1}$ and a_1, a_2 are coefficients obtained the same way as before.

In all the cases that remain, both points are finite, so we can apply the same rules as in the affine version from Algorithm 2.

Algorithm 1: *StarSquare*(P)

1. If $P_3 = 0$, then $P \star P = (-P_1^2 : 1 : 0)$.
2. Otherwise, if $P_2^2 - aP_1 = 0$, then $P \star P = (-2P_2 : P_1 : 1)$.
3. Otherwise, define m by
$$m = \frac{-P_1^2 + aP_2}{P_2^2 - aP_1}.$$
4. If $m^3 + 1 = 0$, then $P \star P = (m : 1 : 0)$.
5. Otherwise, define s by
$$s = \frac{3m^3 P_1 - 3m^2 P_2 + 3am}{m^3 + 1}.$$
Then $P \star P = (m(s - 3P_1) + P_2 : s - 2P_1 : 1)$.

Algorithm 2: *StarProduct*(P, Q)

1. If $P = Q$, then $P \star Q = StarSquare(P)$.
2. Otherwise, if $P_3 = 0$ and $Q_3 = 0$, then $P \star Q = \left(-\frac{1}{P_1 + Q_1} : 1 : 0 \right)$.
3. Otherwise, if $P_3 = 1$ and $Q_3 = 1$ and $P_1 = Q_1$, then $P \star Q = (-P_2 - Q_2 : P_1 : 1)$.
4. Otherwise, if $P_3 = 1$ and $Q_3 = 0$, denote $m = \frac{1}{Q_1}$ and $n = \frac{Q_1 P_2 - P_1}{Q_1}$.
Replace $y = mx + n$ in $x^3 + y^3 - 3axy = 0$ and obtain $a_2 x^2 + a_1 x + a_0 = 0$.
Let $s = -\frac{a_1}{a_2}$. Then $P \star Q = \big(m(s - P_1) + n : s - P_1 : 1 \big)$.
5. Otherwise, if $P_3 = 0$ and $Q_3 = 1$, denote $m = \frac{1}{P_1}$ and $n = \frac{P_1 Q_2 - Q_1}{P_1}$.
Replace $y = mx + n$ in $x^3 + y^3 - 3axy = 0$ and obtain $a_2 x^2 + a_1 x + a_0 = 0$.
Let $s = -\frac{a_1}{a_2}$. Then $P \star Q = \big(m(s - Q_1) + n : s - Q_1 : 1 \big)$.
6. Otherwise, compute $m = \frac{Q_2 - P_2}{Q_1 - P_1}$.
7. If $m^3 + 1 = 0$, then $P \star Q = (m : 1 : 0)$.

8. Otherwise, let $n = \dfrac{P_2Q_1 - P_1Q_2}{Q_1 - P_1}$ and replace $y = mx + n$ in $x^3 + y^3 - 3axy = 0$ to obtain $a_3x^3 + a_2x^2 + a_1x + a_0 = 0$.

   Let $s = -\dfrac{a_2}{a_3}$. Then $P \star Q = \Big(m(s - P_1 - Q_1) + n : s - P_1 - Q_1 : 1\Big)$

5 The fundamental isomorphism

Like group, the folium of Descartes is one of the most important objects in mathematics. Let us spotlight an isomorphism between the group on the folium of Descartes and a multiplicative group of integers congruence classes. In what follows, we denote by Z_p the set of integers modulo the prime number p and we consider the multiplicative group $(Z_p^*, \cdot)$, where $\cdot$ denotes the usual multiplication. Also, let $\mathcal{F}_{a,p} = \{(x, y) \in F_p^* \times F_p^* | x^3 + y^3 - 3axy = 0\} \cup \{\infty\}$ and consider the operation $\star$ that endows this set whith a group structure as seen before.

5.1 Case $p \equiv 2 \bmod 3$

Theorem 5.1. *There is an isomorphism between $(Z_p^*, \cdot)$ and $(\mathcal{F}_{a,p}, \star)$, given by*

$$\varphi : Z_p^* \to \mathcal{F}_{a,p};\ 1 \mapsto \infty;\ t \mapsto P_t = \left(\frac{-3at}{1 - t^3}, \frac{3at^2}{1 - t^3}\right), \forall t \neq 1.$$

Proof. We first prove that $P_t \star P_t = P_{t^2}$ following the steps in Algorithm 1.

1) If $P_t = \infty$, i.e., $t = 1$, then from Algorithm 1 we have that $P_t \star P_t = \infty$ and obviously, because $t_2 = 1$, we find that also $P_{t^2} = \infty$, so $P_t \star P_t = P_{t^2}$.

2) If ${y_t}^2 - ax_t = 0$, then $\frac{(6t^4+3t)a^2}{t^6-2t^3+1} = 0 \Rightarrow \frac{3t(2t^3+1)a^2}{(t^3-1)^2} = 0 \Rightarrow 2t^3 + 1 = 0$.

From Algorithm 1, we obtain $P_t \star P_t = (-2y_t, x_t) = \left(\dfrac{-6t^2a}{1 - t^3}, \dfrac{-3ta}{1 - t^3}\right)$.

We want to show that $P_t \star P_t = P_{t^2} = \left(\dfrac{-3t^2a}{1 - t^6}, \dfrac{3t^4a}{1 - t^6}\right)$, i.e., $\dfrac{-6t^2a}{1 - t^3} = \dfrac{-3t^2a}{1 - t^6}$ and $\dfrac{-3ta}{1 - t^3} = \dfrac{3t^4a}{1 - t^6}$. Both of them hold because of the relation $2t^3 + 1 = 0$.

3) If ${y_t}^2 - ax_t \neq 0$, we can compute $m = \dfrac{-x_t^2 + at_t}{y_t^2 - ax_t} = \dfrac{t^4 - 4t}{2t^3 + 1}$.

If $m^3 + 1 = 0$, i.e., if $m = -1$, from Algorithm 1, we find $P_t \star P_t = \infty$.

We want to show that $P_{t^2} = \infty$, i.e., $t^2 = 1$.

From $m = -1$ we get $x_t^2 - ay_t = y_t^2 - ax_t$, so $(x_t - y_t)(x_t + y_t + a) = 0$.

If $x_t - y_t = 0$, we get $\dfrac{-3at}{1 - t^3} = \dfrac{3at^2}{1 - t^3}$, so $t^2 + t = 0$. Because $t \neq 0$, it remains $t = -1$, so $t^2 = 1$ and $P_{t^2} = \infty$.

If $x_t + y_t + a = 0$, we get $\dfrac{(t^2 - 2t + 1)a^2}{t^2 + t + 1} = 0$ so $t = 1$, meaning P_t is actually ∞, so from the first case, we know that $P_{t^2} = \infty$.

4) Otherwise we compute $s = \dfrac{3m^3x_t - 3m^2y_t + 3am}{m^3+1} = \dfrac{(3t^4+6t)a}{t^6-1}$ and using Algorithm 1, we deduce $P_t \star P_t = \Big(m(s-3x_t)+y_t, s-2x_t\Big) = \left(\dfrac{-3at^2}{1-t^6}, \dfrac{3at^4}{1-t^6}\right)$.

Because $P_{t^2} = \left(\dfrac{-3at^2}{1-(t^2)^3}, \dfrac{3a(t^2)^2}{1-(t^2)^3}\right)$, we obtain $P_t \star P_t = P_{t^2}$.

We next prove the relation $P_t \star P_u = P_{tu}$ following the steps in Algorithm 2.

1) Let $P_t = \infty$, i.e., $t = 1$. Then from Algorithm 2 we have $P_t \star P_u = P_u$, and obviously $P_{tu} = P_{1\cdot u} = P_u$, so in this case $P_t \star P_u = P_{tu}$.

2) In the same way, if $P_u = \infty$, then from Algorithm 2 we have $P_t \star P_u = P_t$, and because $P_{tu} = P_{t\cdot} = P_t$ we also get $P_t \star P_u = P_{tu}$.

3) If $P_t = P_u$, i.e., $t = u$, then we are in the settings of Algorithm 1, and we proved that in this case $P_t \star P_u = P_{tu}$.

4) If $x_t = x_u$, but $y_t \neq y_u$, then we obtain the following relation between t and u $\dfrac{-3at}{1-t^3} = \dfrac{-3au}{1-u^3} \Rightarrow t - tu^3 = u - ut^3 \Rightarrow (t-u)(1+t^2u+tu^2) = 0$. Because $t \neq u$, it remains $1 + t^2u + tu^2 = 0$.

We want to prove that the following two equalities hold

$x_{tu} = -y_t - y_u$, i.e., $\dfrac{tu}{1-(tu)^3} = -\dfrac{t^2}{1-t^3} - \dfrac{u^2}{1-u^3}$ and $y_{tu} = x_t$, i.e. $\dfrac{(tu)^2}{1-(tu)^3} = \dfrac{-t}{1-t^3}$.

We prove first that $y_{tu} = x_t$.

From $\dfrac{(tu)^2}{1-(tu)^3} = \dfrac{-t}{1-t^3}$ we get that $tu^2 - t^4u^2 - t^3u^3 + 1$ must be 0.

Using $1 + t^2u + tu^2 = 0$, we we can write $tu^2 = -1 - t^2u$, so replacing tu^2 in $tu^2 - t^4u^2 - t^3u^3 + 1$ we get $-1 - t^2u - t^4u^2 - t^3u^3 + 1$, which is equal to $-t^2u(1 + t^2u + tu^2) = 0$.

What is left to prove is $-t^2u - t^4u^2 - t^3u^3 = 0$.

From $\dfrac{-3at}{1-t^3} = \dfrac{-3au}{1-u^3}$ we can say that $\dfrac{-u^2}{1-t^3} = \dfrac{-tu}{1-t^3}$, and now we replace it in $\dfrac{tu}{1-(tu)^3} = -\dfrac{t^2}{1-t^3} - \dfrac{u^2}{1-u^3}$ and obtain $-\dfrac{tu}{1-(tu)^3} = -\dfrac{t^2}{1-t^3} - \dfrac{tu}{1-t^3}$, i.e., $\dfrac{tu}{1-(tu)^3} = \dfrac{-t^2-u^2}{1-t^3}$.

So the equality $ut^3 + t - t^4u^3 - t^3u^4 = 0$ must hold. Using again the relation $1+t^2u+tu^2 = 0$, but this time replacing $t^2u = -1-tu^2$, we get $-tu^2-t^3u^3-t^2u^4 = 0$, which is equivalent to $-tu^2(1 + t^2u + tu^2) = 0$.

Because $tu^2 \neq 0$ and we know that $1 + t^2u + tu^2 = 0$, we are done proving also that in this case $P_t \star P_u = P_{tu}$.

5) If $x_t \neq x_u$, we can compute

$$\begin{aligned} m &= \frac{y_u - y_t}{x_u - x_t} = \frac{u^2(1-t^3) - t^2(1-u^3)}{-u(1-t^3) + t(1-u^3)} = \frac{u^2 - t^2 + u^3t^2 - u^2t^3}{-u + t + ut^3 - tu^3} \\ &= \frac{(u-t)(u+t) + u^2t^2(u-t)}{-(u-t) - ut(u-t)(u+t)} = \frac{u + t + u^2t^2}{-1 - u^2t - ut^2}. \end{aligned}$$

6) If $m^3+1=0$, i.e., $m=-1$, then $u+t+u^2t^2=1+ut(u+t)$.

We denote $u+t=v$ and $ut=w$. This yields $w^2-vw+v-1=0$.

One solution is $w_1=1$. From this we get $ut=1$, so $P_{tu}=\infty$. Solution $w_2=v-1$ yields $ut=u+t-1$ so $u=1$ or $t=1$, but this cannot be the case.

It remains, in this case, $P_t\star P_u=\infty$, as in Algorithm 2.

7) If $m\neq -1$, we can compute

$$s=\frac{3m^3x_t-3m^2y_t+3am}{1+m^3}=\frac{3aA}{B},$$

where

$$\begin{aligned} A &= -u^4t^6+(u^5-u^2)t^5+(-u^6+u^3)t^4+(u^4+u)t^3+(-u^5+u^2)t^2+\\ &\quad +(u^3-1)t-u,\\ B &= (-u^6+u^3)t^6+(u^6-1)t^3+(-u^3+1). \end{aligned}$$

From Algorithm 2, we have that x_{tu} should be equal to $m(s-2x_t-x_u)+y_t$ and y_{tu} should be equal to $s-x_t-x_u$. Therefore we compute $m(s-2x_t-x_u)+y_t$ and obtain $\dfrac{-3atu}{1-t^3u^3}$ which is indeed x_{tu}, and also computing $s-x_t-x_u$, we get $\dfrac{3at^2u^2}{1-t^3u^3}$, which is equal to y_{tu}. □

5.2 Case $p\equiv 1$ mod 3

In what follows, we also denote by $(Z_p^*),\cdot$ the multiplicative group of integers modulo n. This time, let

$$P\mathcal{F}_{a,p}=\{(x:y:z)\in F_p^*\times F_p^*\times\{0,1\}|x^3+y^3-3axyz=0\}$$

and consider the operation $\star$ that endows this set whith a group structure as seen before, in the projective version.

Theorem 5.2. *There is an isomorfism between $(Z_p^*,\cdot)$ and $(P\mathcal{F}_{a,p},\star)$, given by*

$$t\mapsto P_t=\begin{cases}\left(\dfrac{-3at}{1-t^3}:\dfrac{3at^2}{1-t^3}:1\right), & \text{if } t^3\neq 1\\ (-t^2:1:0), & \text{otherwise.}\end{cases}$$

Proof. **Algorithm** 3:

1) If $z_t=0$, then $P_t=(-t^2:1:0)$ and $t^3=1$. We want to show that $P_t\star P_t=(-t^4:1:0)$. But this is exactly what Algorithm 2 says.

2) If $z_t=1$, then $y_t^2-ax_t=0$. From this condition we find $2t^3+1=0$.

From the foregoing Algorithm 3, we have

$$P_t\star P_t=(-2y_t:x_t:1)=\left(\frac{-6at^2}{1-t^3}:\frac{-3at}{1-t^3}:1\right).$$

So we want to show that $\dfrac{-6at^2}{1-t^3}=\dfrac{-3at^2}{1-t^6}$ and $\dfrac{-3at}{1-t^3}=\dfrac{3at^4}{1-t^6}$.

For both equalities we need $2t^6 - t^3 - 1 = 0$ and this holds because $2t^3 + 1 = 0$.

3) If $z_t = 1$ and $y_t^2 - ax_t \neq 0$, we can compute $m = \dfrac{-x_t^2 + ay_t}{y_t^2 - ax_t} = -\dfrac{t^4 + 2t}{2t^3 + 1}$.

4) If $m^3 + 1 = 0$, then $\dfrac{t^{12} - 2t^9 + 2t^3 - 1}{8t^9 + 12t^6 + 6t^3 + 1} = 0$, i.e., $\dfrac{(t^3 - 1)^3(t^3 + 1)}{(2t^3 + 1)^3} = 0$.

Because we are in a case where $z_t = 1$, we know that $t^3 \neq 1$, so it remains $t^3 + 1 = 0$.

Therefore $t^6 = 1$, so $(t^2)^3 = 0$, which means that $P_{t^2} = (-t^4 : 1 : 0)$.

It remains to show $-\dfrac{t^4 + 2t}{2t^3 + 1} = -t^4$. This reduces to $t^7 = t$, and because $t \neq 0$, to $t^6 = 1$, which is a true equality, as mentioned before.

5) Otherwise, we can compute $s = \dfrac{3m^3x_t - 3m^2y_t + 3am}{m^3 + 1} = \dfrac{3at^4 + 6at}{t^6 - 1}$.

Algorithm 3 says that $P_t \star P_t = (m(s - 3x_t) + y_t : s - 2x_t : 1)$.

Replacing m, s, x_t and y_t, we obtain that $P_t \star P_t = \left(\dfrac{-3at^2}{1 - t^6} : \dfrac{3at^4}{1 - t^6} : 1\right)$ and because $P_{t^2} = \left(\dfrac{-3at^2}{1 - (t^2)^3} : \dfrac{3a(t^2)^2}{1 - (t^2)^3} : 1\right)$ we have that $P_t \star P_t = P_{t^2}$.

Algorithm 4:

1) If $P_t = P_u$, then we proved $P_t \star P_u = P_{tu}$.

2) If $z_t = z_u = 0$, it means that $t^3 = u^3 = 1$, from where we have that $(tu)^3 = 1$, so $P_{tu} = (-(tu)^2 : 1 : 0)$.

From Algorithm 4, we have $P_t \star P_u = \left(-\dfrac{1}{x_t + x_u} : 1 : 0\right)$, where $x_t = -t^2$ and $x_u = -u^2$.

So we need to show $\dfrac{1}{t^2 + u^2} = -t^2u^2$, i.e., $t^4u^2 + t^2u^4 + 1 = 0$. Because $t^3 = u^3 = 1$, this is equivalent to $tu^2 + t^2u + 1 = 0$.

We also have $t^3 - u^3 = 0$, i.e., $(t - u)(t^2 + tu + u^2) = 0$ and, because $t \neq u$, it remains that $t^2 + tu + u^2 = 0$. If we multiply this by t^2u^2 and keep in mind that $t^3 = u^3 = 1$, we get that $tu^2 + t^2u + 1 = 0$, which proves that in this case $P_t \star P_u = P_{tu}$.

3) If $z_t = z_u = 1$ and $x_t = x_u$ (but $y_t \neq y_u$, so $P_t \neq P_u$), then, from Algorithm 4, we find $P_t \star P_u = (-y_t - y_u : x_t : 1)$, so what we have to show is that $\dfrac{tu}{1 - (tu)^3} = -\dfrac{t^2}{1 - t^3} - \dfrac{u^2}{1 - u^3}$ and $\dfrac{(tu)^2}{1 - (tu)^3} = \dfrac{-t}{1 - t^3}$.

We prove first that $y_{tu} = x_t$, using $x_t = x_u$

From $\dfrac{(tu)^2}{1 - (tu)^3} = \dfrac{-t}{1 - t^3}$ we get $tu^2 - t^4u^2 - t^3u^3 + 1$ must be 0.

Using the equality $1 + t^2u + tu^2 = 0$, i.e., $tu^2 = -1 - t^2u$, and replacing tu^2 in $tu^2 - t^4u^2 - t^3u^3 + 1$, we find $-1 - t^2u - t^4u^2 - t^3u^3 + 1$, which is equal to $-t^2u(1 + t^2u + tu^2) = 0$.

What is left to prove is $-t^2u - t^4u^2 - t^3u^3$.

From $\dfrac{-3at}{1 - t^3} = \dfrac{-3au}{1 - u^3}$, we can say that $\dfrac{-u^2}{1 - t^3} = \dfrac{-tu}{1 - t^3}$, and now we replace it in $\dfrac{tu}{1-(tu)^3} = -\dfrac{t^2}{1-t^3} - \dfrac{u^2}{1-u^3}$ and obtain $-\dfrac{tu}{1-(tu)^3} = -\dfrac{t^2}{1-t^3} - \dfrac{tu}{1-t^3}$, i.e., $\dfrac{tu}{1-(tu)^3} = \dfrac{-t^2-u^2}{1-t^3}$.

So the equality $ut^3 + t - t^4u^3 - t^3u^4 = 0$ must hold. Using again the relation $1+t^2u+tu^2 = 0$, but this time replacing $t^2u = -1-tu^2$, we get $-tu^2-t^3u^3-t^2u^4 = 0$, which is equivalent to $-tu^2(1+t^2u+tu^2) = 0$.

Because $tu^2 \neq 0$ and we know that $1+t^2u+tu^2 = 0$, we are done proving also that in this case $P_t \star P_u = P_{tu}$.

4) If $z_t = 1$ $\left(x_t = \dfrac{-3at}{1-t^3}, y_t = \dfrac{3at^2}{1-t^3}\right)$ and $z_u = 0$ $(x_u = -u^2, y_u = 1)$, then let $m = \dfrac{1}{x_u} = -\dfrac{1}{u^2}$ and $n = \dfrac{x_u y_t - x_t}{x_u} = \dfrac{3u^2t^2a - 3ta}{u^2 - u^2t^3}$.

We next replace $y = mx+n$ in $x^3+y^3-3axy = 0$ and obtain $a_3x^3+a_2x^2+a_1x+a_0 = 0$, where

$$a_3 = \frac{u^6-1}{u^6}$$

(which is 0, because $u^3 = 1$)

$$a_2 = \frac{(-3u^4t^3 + 9u^2t^2 - 9t + 3u^4)a}{-u^6t^3 + u^6}$$

$$a_1 = \frac{(9u^6t^5 - 36u^4t^4 + 54u^2t^3 + (-9u^6 - 27)t^2 + 9u^4t)a^2}{u^6t^6 - 2u^6t^3 + u^6}$$

$$a_0 = \frac{(27u^6t^6 - 81u^4t^5 + 81u^2t^4 - 27t^3)a^3}{-u^6t^9 + 3u^6t^6 - 3u^6t^3 + u^6}.$$

It remains a quadratic equation in x, $a_2x^2 + a_1x + a_0 = 0$, and we know that one solution is x_t.

To find the other solution, we compute $s = -\dfrac{a_1}{a_2} = \dfrac{(3u^2t^2 - 3t)a}{1-t^3}$. So the second solution is $s - x_t = \dfrac{-3u^2t^2a}{t^3-1}$. This should be equal to $y_{tu} = \dfrac{3a(tu)^2}{1-(tu)^3}$, so the equality $\dfrac{-3u^2t^2a}{t^3-1} = \dfrac{3a(tu)^2}{1-(tu)^3}$ must hold, which is true because $u^3 = 1$.

It remains to show that $x_{tu} = m(s - x_t) + n$, i.e., $\dfrac{-3atu}{1-(tu)^3} = \dfrac{3ta}{u^2t^3 - u^2}$. This is also true, for the same reason that $u^3 = 1$.

5) The case $z_t = 0$ and $z_u = 1$ are treated the same way, and we also get that $P_t \star P_u = P_{tu}$.

6) Otherwise (if $z_t = z_u = 1$ and $x_t \neq x_u$), we can compute

$$m = \frac{y_t - y_u}{x_t - x_u} = \frac{-u^2t^2 - t - u}{ut^2 + u^2t + 1}.$$

7) If $m^3 + 1 = 0$, then

$$\frac{(-u^6 + u^3)t^6 + (u^6 - 1)t^3 - u^3 + 1}{u^3t^6 + 3u^4t^5 + (3u^5 + 3u^2)t^4 + (u^6 + 6u^3)t^3 + (3u^4 + 3u)t^2 + 3u^2t + 1} = 0$$

$$\Rightarrow (-u^6 + u^3)t^6 + (u^6 - 1)t^3 - u^3 + 1 = 0 \Rightarrow (1 - u^3)(1 - t^3)(1 - t^3u^3) = 0.$$

Because $t^3 \neq 1$ and $u^3 \neq 1$, it remains that $(tu)^3 = 1$, so $P_{tu} = (-t^2u^2 : 1 : 0)$.

From Algorithm 4, we have that $P_t \star P_u = (m : 1 : 0)$, so we have to show that $\dfrac{-u^2t^2 - u - t}{ut^2 + tu^2 + 1} = -t^2u^2$, which yields to $-t^4u^3 - t^3u^4 = -t - u$ and this is true because $t^3u^3 = 1$.

8) And finally, if $m^3 \neq 1$, then compute $n = \dfrac{x_u y_t - x_t y_u}{x_u - x_t}$ and replace $y = mx + n$ in $x^3 + y^3 - 3axy = 0$. We get a cubic equation $a_3x^3 + a_2x^2 + a_1x + a_0 = 0$ in the unknown x, with the coefficients

$$a_3 = \frac{P}{N},\ a_2 = \frac{Q}{N},\ a_1 = \frac{R}{N},\ a_0 = \frac{S}{N},$$

where

$$\begin{array}{rcl}
P & = & (-u^6 + u^3)t^6 + (u^6 - 1)t^3 + (-u^3 + 1), \\
Q & = & 3a(u^4t^6 + (-u^5 + u^2)t^5 + (u^6 - u^3)t^4 + (-u^4 - u)t^3 + (u^5 - u^2)t^2 + \\
& & (-u^3 + 1)t + u), \\
R & = & 9u^3a^2t^5 - 9u^4a^2t^4 + (9u^5 - 9u^2)a^2t^3 - 9u^3a^2t^2 + 9ua^2t, \\
S & = & -27u^3a^3t^3, \\
N & = & u^3t^6 + 3u^4t^5 + 3(u^5 + u^2)t^4 + (u^6 + 6u^3)t^3 + 3(u^4 + u)t^2 + 3u^2t + 1.
\end{array}$$

For this cubic equation, we know two solutions, namely x_t and x_u, so we can easily find out the third solution. □

6 Conclusions and open problems

The folium of Descartes can have points with coordinates in any field, such as F_p, Q, R, or C. The folium of Descartes with points in F_p is a finite group.

There are still many applications to be found for folium of Descartes, related to the fact that there is a multiplicative group law over the curve. For example, folium of Descartes cryptography.

Open problems (i) Folium of Descartes Discrete Logarithm Problem (FDDLP) is the discrete logarithm problem for the group of points on folium of Descartes over a finite field.

(ii) The best algorithm to solve the FDDLP is exponential. That is why the folium of Descartes group can be used for cryptography. More precisely, we estimate that the best way to solve FDDLP for folium of Descartes over F_p takes time $O(\sqrt{p})$.

The goal of our future papers is about such type of problems, with an emphasis on those aspects which are of interest in cryptography.

Acknowledgements Partially supported by University Politehnica of Bucharest, and by Academy of Romanian Scientists, Bucharest, Romania.

References

[1] H. W. Eves, *A Survey of Geometry*, Allyn and Bacon, Inc., 1972.

[2] N. Koblitz, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics, 114, Springer, 1995.

[3] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.

[4] N. Smart, *Cryptography: an Introduction*, McGraw-Hill, 2003.

[5] L. C. Washington, *Elliptic Curves. Number Theory and Cryptography*, Chapman & Hall, 2008.

Authors' address:

Constantin Udrişte and Steluţa Pricopie,
University Politehnica of Bucharest, Faculty of Applied Sciences,
Department of Mathematics-Informatics, 313 Splaiul Independentei,
RO-060042 Bucharest, Romania.
E-mail: udriste@mathem.pub.ro , anet.udri@yahoo.com ; maty_star@yahoo.com