Eph - International Journal Of Mathematics And Statistics

ISSN (Online): 2208-2212
Volume 7 Issue 1 January 2021

DOI:https://doi.org/10.53555/eijms.v7i1.57

PARAMETRIZATION OF ALGEBRAIC POINTS OF LOW DEGREES ON THE AFFINE CURVE $Y^2 = X^5 + 144^2$

EL Hadji SOW[1*], Pape Modou SARR[2], Oumar SALL[3]
[*123]Department of Mathematics Facutly of Science and Technology University Assane SECK of Ziguinchor (SENEGAL)
[2] p.sarr597@zig.univ.sn, [3] osall@univ-zig.sn

Corresonding Author:-
Email:-elpythasow@yahoo.fr

Abstract:-
In this work, we determine a parametrization of algebraic points of degrees at most 3 over Q on curve C of affine equation $y^2 = x^5 + 20736$. This result extends a result of S. Siksek and M. Stoll who described in [4] the set of Q-rational points on this curve.

Keywords:- *Planes curves - Degree of algebraic points - Rationals points - Algebraic extensions – Jacobian*

Mathematics Subject Classification: *14H50 - 14H40 - 11D68 - 12F05*

INTRODUCTION

Let C be a smooth algebraic curve defined over Q. Let K be a numbers field. We note by C (K) the set of points of C with coordinates in K and[C (K) the set of points of $[K: Q] \leq d$

C with coordinates in K of degree at most d over Q.

We denote by J the jacobian of C and by j (P) the class $[P - \infty]$ of $P - \infty$, that is to say that j is the Jacobian diving $C \longrightarrow J$ (Q). The Mordell-Weil group J (Q) of rational points of the jacobian is a finite set (refer to [4]). We denote by $P = (0, 144)$, $\bar{P} = (0, -144)$ and ∞ the point at infinity. In [4], S. Siksek ET M. Stoll gave a description of the rational points over Q on this curve. This description is as follows:

Proposition. The Q-rational points on C are given by

$$C\,(Q) = \{\infty, P, \bar{P}\}$$

In this note, we determine the algebraic parametrization of all algebraic points of degrees at most 3 over Q on curve C of affine equation

$$y^2 = x^5 + 20736$$

Our essential tools are:

- The Mordell-Weil group J (Q) of rational points of the jacobian (refer to [4])
- Abel Jacobi's theorem (refer to [1])
- Linear systems on the curve C.

Our main result is given by the following theorem:

Theorem.

1. The set of quadratic points on C are given by

$$N\ ^5 + 20736,\ \alpha \in Q_* o.\ S = \alpha,\ \pm\alpha$$

2. The set of cubic points on C are given by

$$A = \{(x, \pm 144 - \alpha x^2) \mid \alpha \in Q^* \text{ and } x \text{ root of } E(x) = x^3 - \alpha^2 x^2 \pm 288\alpha\}$$

Auxiliary results

For a divisor D on C, we note L (D) the Q - vector space of rational functions F defined

On $\bar{Q}$ such that $F = 0$ or $div\,(F) \geq -D$; $l\,(D)$ designates Q-dimension of $L\,(\bar{D})$. In [4], the Mordell-Weil group J (Q) of C is isomorph to Z/5Z and C is a hyperelliptic curve of genus $g = 2$. Let x, y be two rational functions on Q defined as follow:

$$X(X, Y, Z) - \frac{X}{Z} \text{ ET } y(X, Y, Z) = YZ$$

The projective equation of C is

$$C\!: Y^2Z^3 = X^5 + 20736Z^5 = X^5 + 144^2Z^5$$

We denote by $\eta_2 = e^{\frac{2i\Pi}{5}}$ and let's put $B_k = (\sqrt[5]{20736}\,\eta^{2k+1}, 0)$ for $k \in \{0, 1, 2, 3, 4\}$.

Let us designate by $D.C$ the intersection cycle of algebraic curve D defined on Q and C.

Lemma 1. .

- $div(x) = P + \bar{P} - 2\infty$
- $div(y - 144) = 5P - 5\infty$
- $div(y + 144) = 5\bar{P} - 5\infty$
- $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$

Proof. $C\!: Y^2Z^3 = X^5 + 20736Z^5$ (projective equation)

• $Div(x) = div\,(\frac{X}{Z}) = (X = 0).C - (Z = 0).C.$

For $X = 0$, we have $Y^2Z^3 = 20736Z^5$ according to (3), which gives $Z^3 = 0$ or $Y^2 = (144Z)^2$.

On the one hand for $X = 0$, we have $Z^3 = 0$ with $Y = 1$. We obtain the point $\infty = (0, 1, 0)$ with multiplicity 3.

On the other hand for $X = 0$, we $Y = 144Z$ or $Y = -144Z$ with $Z = 1$. We obtain the points $P = (0, 144, 1)$ with multiplicity 1 and $\bar{P} = (0, -144, 1)$ with multiplicity

1. Hence $(X = 0).C = P + \bar{P} + 3\infty$ $(*)$

Even if $Z = 0$, then $X^5 = 0$; and for $Y = 1$, we have the point $\infty = (0, 1, 0)$ with multiplicity 5. Hence $(Z = 0).C = 5\infty$ $(**)$.

The relations $(*)$ and $(**)$ imply that $div(x) = P + \bar{P} - 2\infty$.

• Similarly we show that $div(y - 144) = 5P - 5\infty$, $div(y + 144) = 5\bar{P} - 5\infty$ and $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$.

Consequences of lemma 1 : $5j\,(P) = 5j\,\bar{P} = 0$ et $j\,(P) + j\,\bar{P} = 0$

Lemma 2.

• $L(\infty) = \langle 1 \rangle$
• $L(2\infty) = \langle 1, x \rangle = L(3\infty)$
• $L(4\infty) = \langle 1, x, x^2 \rangle$

• $L(5\infty) = h1, x, x^2, yi$
• $L(6\infty) = h1, x, x^2, y, x^3i$
• $L(7\infty) = h1, x, x^2, y, x^3, xyi$
Proof Results from lemma 1 and from the fact that according to the theorem of RiemannRoch we have $l(m\infty) = m - 1$ as soon as $m \geq 3$.
Lemma 3. $J(Q) \simeq Z/5Z = h[P - \infty]i = \{a[P - \infty], a \in \{0,1,2,3,4\}\}$.
Proof Refer to [4].
Proof of theorem

Quadratic points (algebraic points of degree 2) on C
The set of quadratic points on C are given by

$$S = \{\sqrt{}(\alpha, \pm \alpha^5 + 20736), \alpha \in Q\}$$

Proof: Given $R \in C(\bar{Q})$ with $[Q[R]: Q] = 2$. Note that $R_1, R2$ are the Galois conjugates of R. Let's work with $t = [R_1 + R_2 - 2\infty] \in J(Q)$, according to lemma 3 we have $t = a[P - \infty]$, $0 \leq a \leq 4$. So we have $[R_1 + R_2 - 2\infty] = a[P - \infty] = -a^h\bar{P} - {}^{\infty i}$ according to the consequences of lemma 1
Our proof is divided in three cases:

Case $a = 0$

We have $[R_1 + R_2 - 2\infty] = 0$; then there exist a function F with coefficient in Q such that $div(F) = R_1 + R_2 - 2\infty$, then $F \in L(2\infty)$ and according to lemma 2 we have $F(x,y) = a_1 + a_2x$ with $a_2 6= 0$ otherwise one of the R_i should be ∞.
For the points R_i, we have $a_1 + a_2x = 0$ hence $x = -\frac{a^1}{a^2} = \alpha \in Q$.

By replacing x by α in (1), we have:

$$y^2 = \alpha^5 + 20736$$

And then we have

$$\sqrt{y = \pm \alpha^5 + 20736}$$

So we find a family of quadratic points

$$S = \{(\alpha, \pm \sqrt{\alpha^5 + 20736}, \alpha) \in Q\}$$

Cases $a = 1$ **and** $a = 4$

For $a = 1$, we have $hR_1 + R_2 + \bar{P} - 3\infty^i = 0$, then there exist a function F with coefficient in Q such that $div(F) = R_1 + R_2 + \bar{P} - 3\infty$, then $F \in L(3\infty)$ and as $L(2\infty) = L(3\infty)$ then one of the R_i should be equal to ∞, we obtain a contradiction.

For $a = 4$, we have $[R_1 + R_2 + P - 3\infty] = 0$, then there exist a function F with coefficient in Q such that $div(F) = R_1 + R_2 + P - 3\infty$, then $F \in L(3\infty)$ and as $L(2\infty) = L(3\infty)$ then one of the R_i should be equal to ∞, we obtain a contradiction.

Cases $a = 2$ **and** $a = 3$

For $a = 2$, we have $[R_1+R_2+2\bar{P}-4\infty] = 0$; then there exist a function F with coefficient in Q such that $div(F) = R_1+R_2+2\bar{P}-4\infty$, then $F \in L(4\infty)$ and according to lemma 2 we have $F(x, y) = a_1 + a_2x + a_3x^2$ with $a_3 = 06$ otherwise one of the R_i should be ∞. The function F is of order 2 at point $\bar{P}$ so we must have $a_1 = a_2 = 0$, so $F(x, y) = a_3x^2$ and we should have $R_1 = R_2 = P$, we obtain a contradiction.

For $a = 3$, we have $[R_1 + R_2 + 2P - 4\infty] = 0$; then there exist a function F with coefficient in Q such that $div(F) = R_1+R_2+2P-4\infty$, then $F \in L(4\infty)$ and according to lemma 2 we have $F(x, y) = a_1+a_2x+a_3x^2$ with $a_3 6= 0$ otherwise one of the R_i should be ∞. The function F is of order 2 at point P so we must have $a_1 = a_2 = 0$, so $F(x, y) = a_3x^2$ and we should have $R_1 = R_2 = \bar{P}$, we obtain a contradiction.

Cubic points (algebraic points of degree 3) on C
The set of cubic points on C are given by

$$C = {}^n(x, \pm 144 - \alpha x^2) | \alpha \in Q^* \textit{ and x root of } E(x) = x^3 - \alpha^2x^2 \pm 288\alpha^o$$

Proof: Given $R \in C(\bar{Q})$ with $[Q[R]: Q] = 3$. Note that $R_1, R2, R3$ are the Galois conjugates of R. Let's work with $t = [R_1 + R_2 + R_3 - 3\infty] \in J(Q)$, according to lemma 3 we have $t = a[P - \infty]$, $0 \leq a \leq 4$.
So we have $[R_1+R_2+R_3-3\infty] = a[P - \infty] = -a^h\bar{P} - \infty^i$ according to the consequences of lemma 1.

Our proof is divided in three cases:

Case $a = 0$

We have $[R_1 + R_2 + R_3 - 3\infty] = 0$; then there exist a function F with coefficient in Q such that $div(F) = R_1 + R_2 + R_3 - 3\infty$, then $F \in L(3\infty)$ and as $L(2\infty) = L(3\infty)$ then one of the R_I should be equal to ∞, we obtain a contradiction.

Cases $a = 1$ **and** $a = 4$

For $a = 1$, we have $\langle R_1 + R_2 + R_3 + \overline{P} - 4\infty \rangle = 0$, then there exist a function F with coefficient in Q such that $div\,(F) = R_1 + R_2 + R_3 + \overline{P} - 4\infty$, then $F \in L\,(4\infty)$, then $F \in L\,(2\infty)$ and according to lemma 2 we have $F(x, y) = a_1 + a_2x + a_3x^2$ *with* $a_3 \neq 0$ otherwise one of the R_i should be ∞. For the point $\overline{P}$, we have $F\,(\overline{P}) = 0$, so $a_1 = 0$ and we have $F(x, y) = x\,(a_2 + a_3x)$. For the points R_I, we have $x\,(a_2 + a_3x) = 0$, then $x \in$ Q and therefore the R_I should be of degree ≤ 2, we obtain a contradiction.

For $a = 4$, by a similar argument as in case $a = 1$, we obtain the same contradiction.

Cases $a = 2$ **and** $a = 3$

For $a = 2$, we have $[R_1 + R_2 + R_3 - 3\infty] = 2j\,(P) = -2j\,(\overline{P})$. Then there exist a function F with coefficient in Q such that $div\,(F) = R_1 + R_2 + R_3 + 2\overline{P} - 5\infty$, so $F \in L\,(5\infty)$ and therefore $F(x, y) = a_1 + a_2x + a_3x^2 + a_4y$ with $a_4 \neq 0$ otherwise one of the R_I should be ∞. The function F is of order 2 at point $\overline{P}$ so we must have $a_1 - 144a_4 = 0$ and $a_2 = 0$ hence $F(x, y) = a_4(y + 144) + a_3x^2$.
For the points R_I, we have $a_4(y + 144) + a_3x^2 = 0$ hence $y = -144 - \frac{a_3}{a_4}x^2$. We see that y is of the form $y = -144 - \alpha x^2$ with $\alpha \in \mathbb{Q}^*$ otherwise one of the R_I should be $\overline{P}$, ET par suite on an $y^2 = x^5 + 20736 \Leftrightarrow (-144 - \alpha x^2)^2 = x^5 + 20736 \Leftrightarrow x^5 - \alpha^2x^4 - 288\alpha x^2 = 0 \Leftrightarrow x^2(x^3 - \alpha^2x^2 - 288\alpha) = 0$. We must have $x^2 \neq 0$ and $\alpha \in \mathbb{Q}^*$, we obtain a family of cubic points given by

$$A = \left\{(x, -144 - \alpha x^2) \mid \alpha \in \mathbb{Q}^* \text{ et } x \text{ racine de } E_1(x) = x^3 - \alpha^2x^2 - 288\alpha\right\}$$

For $a = 3$, by a similar argument as in case $a = 2$, we obtain a family of cubic points given by

$$B = \left\{(x, 144 - \alpha x^2) \mid \alpha \in \mathbb{Q}^* \text{ et } x \text{ racine de } E_2(x) = x^3 - \alpha^2x^2 + 288\alpha\right\}$$

By combining these two families of cubic points, we obtain

$$C = \left\{(x, \pm 144 - \alpha x^2) \mid \alpha \in \mathbb{Q}^* \text{ and } x \text{ root of } E(x) = x^3 - \alpha^2x^2 \pm 288\alpha\right\}$$

References

[1] P. A. Griffiths, Introduction to algebraic curves, Translations of mathematical monographs volume 76. American Mathematical Society, Providence (1989).

[2] O. Sall, Points algébriques sur certains quotients de courbes de Fermat, C. R. Acad. Sci. Paris Ser. I 336 (2003) 117-120.

[3] O. Sall, M. Fall, C. M. Coly, Points algébriques de degré donné sur la courbe d'équation affine $y^2 = x^5 + 1$, International Journal Of Development Research Vol. 06, Issue, 11, pp. 10295-10300, November, 2016.

[4] S. Siksek, M. Stoll, Partial descent on hyperelliptic curves and the generalized Fermat equation $x^3 + y^4 + z^5 = 0$, Bull. London Math. Soc. 44 (2012) 151-166.