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]

Department of Mathematics

Facutly of Science and Technology University

Assane SECK of Ziguinchor (SENEGAL)

E-mails : [1] elpythasow@yahoo.fr

[2] p.sarr597@zig.univ.sn [3] osall@univ-zig.sn

Abstract. In this work, we determine a parametrization of algebraic points of degrees at most 3 over $\mathbb{Q}$ on curve $\mathcal{C}$ 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 $\mathbb{Q}$-rational points on this curve.

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

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

1 Introduction

Let $\mathcal{C}$ be a smooth algebraic curve defined over $\mathbb{Q}$. Let K be a numbers field. We note by $\mathcal{C}$(K) the set of points of C with coordinates in K and $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$ the set of points of $\mathcal{C}$ with coordinates in K of degree at most d over $\mathbb{Q}$.
We denote by J the jacobian of $\mathcal{C}$ and by $j(P)$ the class $[P - \infty]$ of $P - \infty$, that is to say that j is the Jacobian diving $\mathcal{C} \longrightarrow J(\mathbb{Q})$. The Mordell-Weil group $J(\mathbb{Q})$ 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 $\mathbb{Q}$ on this curve. This description is as follows :
Proposition. The $\mathbb{Q}$-rational points on $\mathcal{C}$ are given by

$$\mathcal{C}(\mathbb{Q}) = \left\{\infty, P, \bar{P}\right\} \tag{1}$$

In this note, we determine the algebraic parametrization of all algebraic points of degrees at most 3 over $\mathbb{Q}$ on curve $\mathcal{C}$ of affine equation

$$y^2 = x^5 + 20736 \tag{2}$$

Our essential tools are :

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

Our main result is given by the following theorem :
Theorem.

1. The set of quadratic points on $\mathcal{C}$ are given by

$$\mathcal{S} = \left\{ \left(\alpha, \pm\sqrt{\alpha^5 + 20736} \right),\ \alpha \in \mathbb{Q}^* \right\}.$$

2. The set of cubic points on $\mathcal{C}$ are given by

$$\mathcal{A} = \left\{ (x, \pm 144 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ and } x \textit{ root of } E(x) = x^3 - \alpha^2 x^2 \pm 288\alpha \right\}$$

2 Auxiliary results

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

$$x(X, Y, Z) = \frac{X}{Z} \textit{ et } y(X, Y, Z) = \frac{Y}{Z}$$

The projective equation of $\mathcal{C}$ is

$$\mathcal{C} : Y^2Z^3 = X^5 + 20736Z^5 = X^5 + 144^2Z^5 \tag{3}$$

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 $\mathcal{D}.\mathcal{C}$ the intersection cycle of algebraic curve $\mathcal{D}$ defined on $\mathbb{Q}$ and $\mathcal{C}$.

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. $\mathcal{C} : Y^2Z^3 = X^5 + 20736Z^5$ (projective equation).

- $div(x) = div(\frac{X}{Z}) = (X = 0).\mathcal{C} - (Z = 0).\mathcal{C}$.
  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 $(X = 0).\mathcal{C} = P + \bar{P} + 3\infty$ $(*)$

Even if $Z=0$, then $X^5=0$; and for $Y=1$, we have the point $\infty=(0,1,0)$ with multiplicity 5. Hence $(Z=0).\mathcal{C}=5\infty$ $(**)$.
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 : $5j(P)=5j\left(\bar{P}\right)=0$ et $j(P)+j\left(\bar{P}\right)=0$

Lemma 2.

- $\mathcal{L}(\infty)=\langle 1\rangle$
- $\mathcal{L}(2\infty)=\langle 1,\ x\rangle=\mathcal{L}(3\infty)$
- $\mathcal{L}(4\infty)=\langle 1,\ x,\ x^2\rangle$
- $\mathcal{L}(5\infty)=\langle 1,\ x,\ x^2,\ y\rangle$
- $\mathcal{L}(6\infty)=\langle 1,\ x,\ x^2,\ y,\ x^3\rangle$
- $\mathcal{L}(7\infty)=\langle 1,\ x,\ x^2,\ y,\ x^3,\ xy\rangle$

Proof Results from lemma 1 and from the fact that according to the theorem of Riemann-Roch we have $l(m\infty)=m-1$ as soon as $m\geq 3$.

Lemma 3. $J(\mathbb{Q})\cong\mathbb{Z}/5\mathbb{Z}=\langle[P-\infty]\rangle=\{a[P-\infty],a\in\{0,1,2,3,4\}\}$.

Proof Refer to [4].

3 Proof of theorem

3.1 Quadratic points (algebraic points of degree 2) on $\mathcal{C}$

The set of quadratic points on $\mathcal{C}$ are given by

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

Proof : Given $R\in\mathcal{C}(\bar{\mathbb{Q}})$ with $[\mathbb{Q}[R]:\mathbb{Q}]=2$. Note that R_1,R_2 are the Galois conjugates of R. Let's work with $t=[R_1+R_2-2\infty]\in J(\mathbb{Q})$, according to lemma 3 we have $t=a[P-\infty]$, $0\leq a\leq 4$. So we have $[R_1+R_2-2\infty]=a[P-\infty]=-a\left[\bar{P}-\infty\right]$ 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 $\mathbb{Q}$ such that $div(F)=R_1+R_2-2\infty$, then $F\in\mathcal{L}(2\infty)$ and according to lemma 2 we have $F(x,y)=a_1+a_2x$ with $a_2\neq 0$ otherwise one of the R_i should be ∞.
For the points R_i, we have $a_1+a_2x=0$ hence $x=-\dfrac{a_1}{a_2}=\alpha\in\mathbb{Q}$.
By replacing x by α in (1), we have :

$$y^2=\alpha^5+20736 \tag{4}$$

and then we have

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

So we find a family of quadratic points

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

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

For $a = 1$, we have $\left[R_1 + R_2 + \bar{P} - 3\infty\right] = 0$, then there exist a function F with coefficient in $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + \bar{P} - 3\infty$, then $F \in \mathcal{L}(3\infty)$ and as $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$ 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 $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + P - 3\infty$, then $F \in \mathcal{L}(3\infty)$ and as $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$ 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 $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + 2\bar{P} - 4\infty$, then $F \in \mathcal{L}(4\infty)$ 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 ∞. 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 $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + 2P - 4\infty$, then $F \in \mathcal{L}(4\infty)$ 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 ∞. 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.

3.2 Cubic points (algebraic points of degree 3) on $\mathcal{C}$

The set of cubic points on $\mathcal{C}$ are given by

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

Proof : Given $R \in \mathcal{C}(\bar{\mathbb{Q}})$ with $[\mathbb{Q}[R] : \mathbb{Q}] = 3$. Note that R_1, R_2, R_3 are the Galois conjugates of R. Let's work with $t = [R_1 + R_2 + R_3 - 3\infty] \in J(\mathbb{Q})$, according to lemma 3 we have $t = a[P - \infty],\ 0 \leq a \leq 4$.
So we have $[R_1 + R_2 + R_3 - 3\infty] = a[P - \infty] = -a\left[\bar{P} - \infty\right]$ 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 $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + R_3 - 3\infty$, then $F \in \mathcal{L}(3\infty)$ and as $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$ 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 $\left[R_1 + R_2 + R_3 + \bar{P} - 4\infty\right] = 0$, then there exist a function F with coefficient in $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + R_3 + \bar{P} - 4\infty$, then $F \in \mathcal{L}(4\infty)$, then $F \in \mathcal{L}(2\infty)$ 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 $\bar{P}$, we have $F(\bar{P}) = 0$, 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 $x \in \mathbb{Q}$ 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 $[R_1 + R_2 + R_3 - 3\infty] = 2j(P) = -2j(\bar{P})$. then there exist a function F with coefficient in $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + R_3 + 2\bar{P} - 5\infty$, so $F \in \mathcal{L}(5\infty)$ 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 $\bar{P}$ 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 $\bar{P}$, et par suite on a $y^2 = x^5 + 20736 \Leftrightarrow (-144 - \alpha x^2)^2 = x^5 + 20736 \Leftrightarrow x^5 - \alpha^2x^4 - 288\alpha x^2 = 0 \Leftrightarrow x^2(x^3 - \alpha^2x^2 - 288\alpha) = 0$. We must have $x^2 \neq 0$ and $\alpha \in \mathbb{Q}^*$, we obtain a family of cubic points given by

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

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

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

By combining these two families of cubic points, we obtain

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

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.