Journal of Contemporary Applied Mathematics
V. 13, No 1, 2023, July
ISSN 2222-5498

Parametrization of Algebraic Points of Low Degrees on the Hindry-Silverman Curve

EL Hadji SOW, Moussa FALL and Oumar SALL

Abstract. In this paper, we give a parametrization of algebraic points of degrees at most 3 over $\mathbb{Q}$ on the curve $\mathcal{C}$ given by the affine equation $y^2 + y = x^5$. This result extends a result of Hindry and Silverman described in [4] the set of $\mathbb{Q}$-rational points i.e the set of points of degree one over $\mathbb{Q}$ on this curve.

Key Words and Phrases: Degree of algebraic point; curves; Linear system; Mordell-Weil Group; Jacobian.
2010 Mathematics Subject Classifications: Primary 14L40 - 14H40 - 14C20.

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 $\mathcal{C}$ 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 propose to study in detail a parametrization of algebraic points of degrees at most 3 on $\mathbb{Q}$ on the curve $\mathcal{C}$ of affine equation:

$$y^2 + y = x^5 \tag{1}$$

The curve $\mathcal{C}$ is hyperelliptic of genus $g = 2$ and rank null by [4].
Let's denote $P_0 = (0, 0)$,; $P_1 = (0, -1)$; and $;\infty$ the point at infinity.
In [4] Hindry and Silverman gave a description of rational points and this description is as follows:
Proposition. The $\mathbb{Q}$-rational points on the $\mathcal{C}$ curve are given by

$$\mathcal{C}(\mathbb{Q}) = \{P_0,\ P_1,\ \infty\} \tag{2}$$

We extend this result by giving a parametrization of algebraic points of degree at most 3 on the curve over the rational number field $\mathbb{Q}$ using our ideas in [6] (SCIREA Journal of Mathematics, Volume 6, Issue 6, 2021) and using our ideas in [7] (Asian Research Journal of Mathematics, 51-58, 2021).

2. Auxiliary results

For a divisor D on the curve $\mathcal{C}$, we denote $\mathcal{L}(D)$ the $\bar{\mathbb{Q}}$-vector space of rational functions F on the curve $\mathcal{C}$ such that $F = 0$ or $div(F) \geq -D$; $l(D)$ denotes the $\bar{Q}$-dimension of $\mathcal{L}(D)$. Let x and y be the rational functions defined on $\mathcal{C}$ by :

$$x(X,Y,Z) = \frac{X}{Z} \qquad and \qquad y(X,Y,Z) = \frac{Y}{Z}.$$

The projective equation of the curve $\mathcal{C}$ is :

$$\mathcal{C} : Y^2Z^3 + YZ^4 = X^5 \tag{3}$$

We denote by J the Jacobian of $\mathcal{C}$ and by $j(P)$ the class $[P - \infty]$ of $P - \infty$, i.e 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 finite.(See [4])
Let us denote by $\mathcal{C}'.\mathcal{C}$ the intersection cycle of an algebraic curve $\mathcal{C}'$ defined on $\mathbb{Q}$ and $\mathcal{C}$.

Lemma 2.1.

- $div(x) = P_0 + P_1 - 2\infty$
- $div(y) = 5P_0 - 5\infty$
- $div(y+1) = 5P_1 - 5\infty$

Proof.
Let's calculate only $div(y)$ and by proceeding in the same way, we find the others.
We have $div(y) = div\left(\frac{Y}{Z}\right) = (Y = 0).\mathcal{C} - (Z = 0).\mathcal{C}$.
For $Y = 0$, we have $X^5 = 0$ according to (3); and with $Z = 1$, we obtain the point $P_0 = (0,0,1)$ with multiplicity 5. Hence $(Y = 0).\mathcal{C} = 5P_0$. (i)
Similarly for $Z = 0$, then we have $X^5 = 0$ from (3); and with $Y = 1$, we have the point $\infty = (0,1,0)$ with multiplicity 5 hence $(Z = 0).\mathcal{C} = 5\infty$. (ii)
The relations (i) and (ii) imply that $div(y) = 5P_0 - 5\infty$.

Consequences of Lemma 1: $5j(P_0) = 5j(P_1) = 0$ et $j(P_0) + j(P_1) = 0$

Lemma 2.2.

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

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

Lemma 2.3. *The Mordell-Weil group of the curve $\mathcal{C}$ is*

$$J(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} = \langle [P_0 - \infty] \rangle = \{a\,[P_0 - \infty]\,, a \in \{0, 1, 2, 3, 4\}\}$$

.

Proof. See [4].

3. Main results

Our main result is the following theorem.
Theorem:

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

$$\mathcal{S} = \left\{ \left(\alpha, -\frac{1}{2} \pm \sqrt{\alpha^5 + \frac{1}{4}} \right),\ \alpha \in \mathbb{Q}^* \right\}.$$

2. The set of cubic points on $\mathcal{C}$ is given by $\mathcal{A} \cup \mathcal{B}$ with

$$\mathcal{A} = \left\{ (x, -1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ and } x \textit{ root of } C_1(x) = x^3 - \alpha^2 x^2 - \alpha \right\},$$

$$\mathcal{B} = \left\{ (x, \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ and } x \textit{ root of } C_2(x) = x^3 - \alpha^2 x^2 - \alpha \right\}.$$

Proof of the theorem

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

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

$$\mathcal{S} = \left\{ \left(\alpha, -\frac{1}{2} \pm \sqrt{\alpha^5 + \frac{1}{4}} \right),\ \alpha \in \mathbb{Q}^* \right\}$$

Proof:
Let $R \in \mathcal{C}(\overline{\mathbb{Q}})$ with $[\mathbb{Q}(R) : \mathbb{Q}] = 2$. Let R_1, R_2 be the Galois conjugates of R.
Let's work with $t = [R_1 + R_2 - 2\infty] \in J(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$, hence

$$t = [R_1 + R_2 - 2\infty] = aj(P_0) = -aj(P_1),\ 0 \leq a \leq 4 \quad (*)$$

We note that $R \notin \{\infty, P_0, P_1\}$.
Case $a = 0$

The relation $(*)$ becomes $[R_1 + R_2 - 2\infty] = 0$.
The Abel Jacobi theorem involves the existence of a rational function F on $\mathbb{Q}$ such that

$$div(F) = R_1 + R_2 - 2\infty \tag{4}$$

so $F \in \mathcal{L}(2\infty)$, hence $F(x, y) = a_1 + a_2 x, \ \ (a_2 \neq 0)$.
At the points R_i, we have $a_1 + a_2 x = 0$ so $x = -\dfrac{a_1}{a_2} = \alpha \in \mathbb{Q}^*$.
Replacing x by its expression in (1), we have

$$y^2 + y = \alpha^5 \Leftrightarrow \left(y + \frac{1}{2}\right)^2 - \frac{1}{4} = \alpha^5 \tag{5}$$

and therefore we have:

$$y = -\frac{1}{2} \pm \sqrt{\alpha^5 + \frac{1}{4}} \tag{6}$$

We thus have a family of quadratic points

$$\mathcal{S} = \left\{ \left(\alpha, -\frac{1}{2} \pm \sqrt{\alpha^5 + \frac{1}{4}} \right), \ \alpha \in \mathbb{Q}^* \right\}$$

Case $a = 1$
The relation $(*)$ gives $[R_1 + R_2 - 2\infty] = j(P_0) = -j(P_1)$. The Abel Jacobi theorem involves the existence of a rational function F on $\mathbb{Q}$ such that

$$div(F) = R_1 + R_2 + P_1 - 3\infty \tag{7}$$

so $F \in \mathcal{L}(3\infty)$ and since $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$, P_1 should be equal to ∞; we obtain a contradiction.

Case $a = 2$
The relation $(*)$ gives $[R_1 + R_2 - 2\infty] = 2j(P_0) = -2j(P_1)$. The Abel Jacobi theorem involves the existence of a rational function F on $\mathbb{Q}$ such that

$$div(F) = R_1 + R_2 + 2P_1 - 4\infty \tag{8}$$

so $F(x, y) = a_1 + a_2 x + a_3 x^2$ and since $ord_{P_1}(F) = 2$, we must have $a_1 = a_2 = 0$, so $F(x, y) = a_3 x^2$ and we should have $R_1 = R_2 = P_0$, we obtain a contradiction.

Case $a = 3$
The relation $(*)$ gives $[R_1 + R_2 - 2\infty] = 3j(P_0) = -2j(P_0)$.
Abel Jacobi's theorem leads to the existence of a rational function F on $\mathbb{Q}$ such that

$$div(F) = R_1 + R_2 + 2P_0 - 4\infty \tag{9}$$

so $F(x, y) = a_1 + a_2 x + a_3 x^2$ and since $ord_{P_0}(F) = 2$, we must have $a_1 = a_2 = 0$, so $F(x, y) = a_3 x^2$ and we should have $R_1 = R_2 = P_1$, we obtain a contradiction.

Case $a = 4$
The relation $(*)$ gives $[R_1 + R_2 - 2\infty] = 4j(P_0) = -j(P_0)$. The Abel Jacobi theorem involves the existence of a rational function F on $\mathbb{Q}$ such that

$$div(F) = R_1 + R_2 + P_0 - 3\infty \tag{10}$$

so $F \in \mathcal{L}(3\infty)$ and since $\mathcal{L}(2\infty) = \mathcal{L}(3\infty)$, P_0 should be equal to ∞; we obtain a contradiction.
Conclusion: The set of quadratic points on $\mathcal{C}$ is:

$$\mathcal{S} = \left\{ \left(\alpha, -\frac{1}{2} \pm \sqrt{\alpha^5 + \frac{1}{4}} \right),\ \alpha \in \mathbb{Q}^* \right\}.$$

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

The set of cubic points on $\mathcal{C}$ is given by $\mathcal{A} \cup \mathcal{B}$ with

$$\mathcal{A} = \left\{ (x, -1 - \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ and } x \textit{ root of } C_1(x) = x^3 - \alpha^2 x^2 - \alpha \right\},$$

$$\mathcal{B} = \left\{ (x, \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ and } x \textit{ root of } C_2(x) = x^3 - \alpha^2 x^2 - \alpha \right\}.$$

Proof:
Let $R \in \mathcal{C}(\overline{\mathbb{Q}})$ with $[\mathbb{Q}(R) : \mathbb{Q}] = 3$. Let R_1, R_2, R_3 be the Galois conjugates of R and let's work with $t = [R_1 + R_2 + R_3 - 3\infty] \in J(\mathbb{Q}) = \{aj(P_0),\ 0 \le a \le 4\}$, hence $t = aj(P_0) = -aj(P_1),\ 0 \le a \le 4$.
We note that $R \notin \{\infty, P_0, P_1\}$.
Case $a = 0$
So we have $[R_1 + R_2 + R_3 - 3\infty] = 0$. Then there exists a rational function F on $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + R_3 - 3\infty$, so we have $F \in \mathcal{L}(3\infty)$ and as $\mathcal{L}(3\infty) = \mathcal{L}(2\infty)$, then one of R_i should be equal to ∞, we obtain a contradiction.

Case $a = 1$
So we have $[R_1 + R_2 + R_3 - 3\infty] = j(P_0) = -j(P_1)$. Then there exists a rational function F on $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + R_3 + P_1 - 4\infty$, so we have $F \in \mathcal{L}(4\infty)$ and therefore $F(x, y) = a_1 + a_2 x + a_3 x^2$, $(a_3 \neq 0)$.
For the point P_1, we have $F(P_1) = 0$ so $a_1 = 0$ hence $F(x, y) = x(a_2 + a_3 x)$.
For the points R_i, we have $x(a_2 + a_3 x) = 0$, so $x \in \mathbb{Q}$ and therefore the R_i should be of degree ≤ 2.

Case $a = 2$
So we have $[R_1 + R_2 + R_3 - 3\infty] = 2j(P_0) = -2j(P_1)$. Then there exists a rational function F on $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + R_3 + 2P_1 - 5\infty$, so $F \in \mathcal{L}(5\infty)$ and therefore $F(x, y) = a_1 + a_2 x + a_3 x^2 + a_4 y$, $(a_4 \neq 0)$.
The function F is of order 2 at the point P_1 so $a_1 - a_4 = 0$ and $a_2 = 0$, hence

$F(x,y) = a_4(y+1) + a_3x^2$. For the points R_i, we must have $a_4(y+1) + a_3x^2 = 0$, hence $y = -1 - \frac{a_3}{a_4}x^2$. We see that y is of the form $y = -1 - \alpha x^2$ with $\alpha \in \mathbb{Q}^*$, and therefore we have $y(y+1) = x^5 \Leftrightarrow \left(-1-\alpha x^2\right)\left(-\alpha x^2\right) = x^5 \Leftrightarrow x^2(x^3 - \alpha^2x^2 - \alpha) = 0$.
We must have $x^2 \neq 0$ and $\alpha \in \mathbb{Q}^*$, we obtain a family of cubic points

$$\mathcal{A} = \left\{(x, -1-\alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ and } x \textit{ root of } C_1(x) = x^3 - \alpha^2x^2 - \alpha\right\}$$

Case $a = 3$
So we have $[R_1 + R_2 + R_3 - 3\infty] = 3j(P_0) = -2j(P_0)$. Then there exists a rational function F on $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + R_3 + 2P_0 - 5\infty$, hence $F \in \mathcal{L}(5\infty)$ and therefore we have $F(x,y) = a_1 + a_2x + a_3x^2 + a_4y$, $(a_4 \neq 0)$.
The function F is of order 2 at the point P_0 so $a_1 = 0$ and $a_2 = 0$, hence $F(x,y) = a_3x^2 + a_4y$. For the points R_i, we must have $a_3x^2 + a_4y = 0$, hence $y = -\frac{a_3}{a_4}x^2$. We see that y is of the form $y = \alpha x^2$ with $\alpha \in \mathbb{Q}^*$, and therefore we have $y^2 + y = x^5 \Leftrightarrow (\alpha x^2)^2 + \alpha x^2 = x^5 \Leftrightarrow x^2(x^3 - \alpha^2x^2 - \alpha) = 0$.
We must have $x^2 \neq 0$ and $\alpha \in \mathbb{Q}^*$, we obtain a family of cubic points

$$\mathcal{B} = \left\{(x, \alpha x^2) |\ \alpha \in \mathbb{Q}^* \textit{ and } x \textit{ root of } C_2(x) = x^3 - \alpha^2x^2 - \alpha\right\}$$

Case $a = 4$
So we have $[R_1 + R_2 + R_3 - 3\infty] = 4j(P_0) = -j(P_0)$. Then there exists a rational function F on $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + R_3 + P_0 - 4\infty$, so $F \in \mathcal{L}(4\infty)$ and therefore we have $F(x,y) = a_1 + a_2x + a_3x^2$, $a_3 \neq 0$.
For the point P_0, we have $F(P_0) = 0$ so $a_1 = 0$ hence $F(x,y) = x(a_2 + a_3x)$.
For the points R_i, we have $x(a_2 + a_3x) = 0$, hence $x \in \mathbb{Q}$ and therefore the R_i should be of degree ≤ 2.
Conclusion: The set of cubic points on $\mathcal{C}$ is given by $\mathcal{A} \cup \mathcal{B}$.

References

[1] The LMFDB Collaboration, The L-functions and Modular Forms Database. https://www.lmfdb.org/Genus2Curve/Q/ [Online; accessed 8 November 2021].

[2] E. L. García, Diophantine Geometry, Course notes from the CIMPA school "Functional Equations: Theory, Practice and Interactions" held in Hanoi from 12-23 April 2021.

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

[4] M. Hindry, J. H. Silverman, Diophantine Geometry, An Introduction, Graduate Texts in Mathematics, January 1, 2000.

[5] 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.

[6] E. H. Sow, M. Fall, O. Sall, Points algébriques de degrés au-plus 5 sur la courbe d'équation affine $y^2 = 4x^5 + 1$, SCIREA Journal of Mathematics, Volume 6, 2021.

[7] E. H. Sow, P. M. Sarr, O. Sall, Algebraic Points of Degree at Most 5 on the Affine Curve $y^2 = x^5 - 243$, Asian Research Journal of Mathematics, 51-58, 2021.

EL Hadji SOW
Assane Seck University, Departement of mathematics, Ziguinchor, Senegal
E-mail: elpythasow@yahoo.fr

Moussa FALL
Assane Seck University, Departement of mathematics, Ziguinchor, Senegal
E-mail: m.fall@univ-zig.sn

Oumar SALL
Assane Seck University, Departement of mathematics, Ziguinchor, Senegal
E-mail: osall@univ-zig.sn

Received 14 February 2023
Accepted 01 March 2023