International Journal of Mathematics and
Computer Science, **18**(2023), no. 4, 613–617

Algebraic Points of Degree at most 4 on the Affine Curve $y^2 + y = x^5$

EL Hadji Sow

Department of Mathematics and Applications Laboratory
Faculty of Science and Technology
Assane SECK University
Ziguinchor, Senegal

email: elpythasow@yahoo.fr

(Received March 2, 2023, Accepted April 13, 2023,
Published May 31, 2023)

Abstract

We determine explicitly algebraic points of degree at most 4 on the curve $\mathcal{C}$ given by the affine equation $y^2 + y = x^5$. This result extends our previous result in [8].

1 Introduction

Let $\mathcal{C}$ be a smooth algebraic curve defined over $\mathbb{Q}$. Let K be a numbers field. We denote by $\mathcal{C}$(K) the set of K-rational points of $\mathcal{C}$ and $\bigcup_{[K:\mathbb{Q}]\leq d} \mathcal{C}(K)$ the set of points of algebraic of degree $\leq d$ over $\mathbb{Q}$. The degree of an algebraic point R is the degree of its field of definition on $\mathbb{Q} : deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$.
The curve $\mathcal{C}$ is hyperelliptic of genus $g = 2$ and rank null by [4]. The Mordell-Weil group $J(\mathbb{Q})$ of rational points of the Jacobain is finite [4].
Previous works in [4] and [8] have dealt with the algebraic points of degree at most 3 on the Hindry-Silverman curve of affine equation $y^2 + y = x^5$.
Let $P_0 = (0, 0)$, $P_1 = (0, -1)$ and ∞ be the point at infinity.
Using ideas in [8], our goal is to determine the set of algebraic points of degree at most 4 on the curve $\mathcal{C}$ over the rational numbers field $\mathbb{Q}$.

Key words and phrases: Degree of algebraic points, Plane curves, Rational points.
AMS (MOS) Subject Classifications: 14H40, 11D68, 12F05.
ISSN 1814-0432, 2023, http://ijmcs.future-in-tech.net

2 Auxiliary results

For a divisor D on the curve $\mathcal{C}$, we let $\mathcal{L}(D)$ denote 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: $x(X,Y,Z) = \frac{X}{Z} and y(X,Y,Z) = \frac{Y}{Z}$.

Lemma 2.1. *[8]* $div(x) = P_0 + P_1 - 2\infty$, $div(y) = 5P_0 - 5\infty$, $div(y+1) = 5P_1 - 5\infty$.
Consequences of lemma 2.1: $5j(P_0) = 5j(P_1) = 0$ *and* $j(P_0) = -j(P_1)$.

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* 2.1 *and of the fact that according to the Riemann-Roch theorem,* $l(m\infty) = m - 1$ *as soon as* $m \geq 3$.

Lemma 2.3 (4). *The Mordell-Weil group of the curve* $\mathcal{C}$ *is*

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

3 Main result

Theorem: The algebraic points of degree 4 over $\mathbb{Q}$ on the curve $\mathcal{C}$ are given by the union $\mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4$ with

$$\mathcal{C}_0 = \left\{ \left(x, -\frac{1}{2} \pm \sqrt{x^5 + \frac{1}{4}} \right) \mid x \in \mathbb{Q},\ [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$

$$\mathcal{C}_1 = \left\{ \begin{array}{l} (x, -1 - \alpha x(x+\beta)) \mid \alpha, \beta \in \mathbb{Q}^\star \text{ and } x \text{ root of} \\ \\ B_1(x) = x^4 - \alpha^2 x^3 - 2\alpha^2 \beta x^2 - (\alpha + \alpha^2\beta^2)x - \alpha\beta \end{array} \right\}$$

$$\mathcal{C}_2 = \left\{ \begin{array}{l} (x, -1 - \alpha x^2(x+\beta)) \mid \alpha, \beta \in \mathbb{Q}^\star \text{ and } x \text{ root of} \\ \\ B_2(x) = \alpha^2 x^4 + (2\alpha^2 - 1)x^3 + \alpha^2\beta^2 x^2 + \alpha x + \alpha\beta \end{array} \right\}$$

.

$$\mathcal{C}_3 = \left\{ \begin{array}{l} (x, -\alpha x^2(x+\beta)) \mid \alpha, \beta \in \mathbb{Q}^\star \text{ and } x \text{ root of} \\ \\ B_3(x) = \alpha^2 x^4 + (2\alpha^2 - 1)x^3 + \alpha^2\beta^2 x^2 - \alpha x - \alpha\beta \end{array} \right\}$$

.

$$\mathcal{C}_4 = \left\{ \begin{array}{l} (x, -\alpha x(x+\beta)) \mid \alpha, \beta \in \mathbb{Q}^\star \text{ and } x \text{ root of} \\ \\ B_4(x) = x^4 - \alpha^2 x^3 - 2\alpha^2 \beta x^2 + (\alpha + \alpha^2\beta^2)x + \alpha\beta \end{array} \right\}$$

.

Proof. Let $R \in \mathcal{C}(\overline{\mathbb{Q}})$ with $[\mathbb{Q}(R) : \mathbb{Q}] = 4$. Let R_1, R_2, R_3, R_4 be the Galois conjugates of R. We have $[R_1 + R_2 + R_3 + R_4 - 4\infty] \in J(\mathbb{Q})$. From lemma 2.3,

$$[R_1 + R_2 + R_3 + R_4 - 4\infty] = aj(P_0) = -aj(P_1),\ 0 \le a \le 4\ \ (*).$$

We note that $R \notin \{\infty, P_0, P_1\}$ and our proof is divided into five cases:
Case $a = 0$. Formula $(*)$ becomes $[R_1 + R_2 + R_3 + R_4 - 4\infty] = 0$. Then there exists a rational function F such that $div(F) = R_1 + R_2 + R_3 + R_4 - 4\infty$, we have $F \in \mathcal{L}(4\infty)$ and lemma 2.1 gives $F(x, y) = a_1 + a_2 x + a_3 x^2$. At points R_i, we have $a_1 + a_2 x + a_3 x^2 = 0$. The relation $y^2 + y = x^5 \Leftrightarrow \left(y + \dfrac{1}{2}\right)^2 - \dfrac{1}{4} = x^5$ gives $y = -\frac{1}{2} \pm \sqrt{x^5 + \dfrac{1}{4}}$.
We thus have a family of quartic points

$$\mathcal{C}_0 = \left\{ \left(x, -\frac{1}{2} \pm \sqrt{x^5 + \frac{1}{4}} \right) \mid x \in \mathbb{Q},\ [\mathbb{Q}(x) : \mathbb{Q}] = 2 \right\}$$

Case $a = 1$. By $(*)$, $[R_1 + R_2 + R_3 + R_4 - 4\infty] = j(P_0) = -j(P_1)$.
Then there exists a rational function F such that
$div(F) = R_1 + R_2 + R_3 + R_4 + P_1 - 5\infty$, so $F \in \mathcal{L}(5\infty)$ and lemma 2.1 gives $F(x, y) = a_1 + a_2 x + a_3 x^2 + a_4 y$, $(a_4 \neq 0)$.
At point P_1, we have $F(P_1) = 0$ so $a_1 - a_4 = 0$ hence
$F(x, y) = a_4(y+1) + a_2 x + a_3 x^2$. At points R_i, we have $a_4(y+1) + a_2 x + a_3 x^2 = 0$. Hence $y = -1 - \dfrac{a_2}{a_4} x - \dfrac{a_3}{a_4} x^2 = -1 - \dfrac{a_3}{a_4} x(x + \dfrac{a_2}{a_3})$. We have $y = -1 - \alpha x(x+\beta)$ with $\alpha, \beta \in \mathbb{Q}^\star$. Therefore, $y(y+1) = x^5 \Leftrightarrow (-1 - \alpha x(x+\beta))(-\alpha x(x+\beta)) = x^5$
$\Leftrightarrow x^5 - \alpha^2 x^4 - 2\alpha^2 \beta x^3 - (\alpha + \alpha^2 \beta^2) x^2 - \alpha\beta x = 0$
$\Leftrightarrow x(x^4 - \alpha^2 x^3 - 2\alpha^2 \beta x^2 - (\alpha + \alpha^2\beta^2)x - \alpha\beta) = 0$.
We must have $x \neq 0$ and $\alpha, \beta \in \mathbb{Q}^\star$, and we obtain a family of quartic points

$$\mathcal{C}_1 = \left\{ \begin{array}{l} (x, -1 - \alpha x(x+\beta)) \mid \alpha, \beta \in \mathbb{Q}^\star \text{ and } x \text{ root of} \\ \\ B_1(x) = x^4 - \alpha^2 x^3 - 2\alpha^2 \beta x^2 - (\alpha + \alpha^2\beta^2)x - \alpha\beta \end{array} \right\}$$

Case $a=2$. By $(*)$, $[R_1+R_2+R_3+R_4-4\infty]=2j(P_0)=-2j(P_1)$. Then there exists a rational function F such that
$div(F)=R_1+R_2+R_3+R_4+2P_1-6\infty$, so $F\in\mathcal{L}(6\infty)$ and therefore $F(x,y)=a_1+a_2x+a_3x^2+a_4y+a_5x^3$, $(a_5\neq 0)$. The function F is of order 2 at point P_1 so $a_1-a_4=0$ et $a_2=0$, hence $F(x,y)=a_4(y+1)+a_3x^2+a_5x^3$. At points R_i, we must have $a_4(y+1)+a_3x^2+a_5x^3=0$, hence $y=-1-\frac{a_5}{a_4}x^2\left(x+\frac{a_3}{a_5}\right)$. We see that y is of the form $y=-1-\alpha x^2\left(x+\beta\right)$ with $\alpha,\beta\in\mathbb{Q}^*$. Therefore, $y(y+1)=x^5\Leftrightarrow\left(-1-\alpha x^2\left(x+\beta\right)\right)\left(-\alpha x^2\left(x+\beta\right)\right)=x^5\Leftrightarrow x^2\left(\alpha^2x^4+(2\alpha^2-1)x^3+\alpha^2\beta^2x^2+\alpha x+\alpha\beta\right)=0$.
We must have $x^2\neq 0$ and $\alpha,\beta\in\mathbb{Q}^*$, and we obtain a family of quartic points

$$\mathcal{C}_2=\left\{\begin{array}{l}\left(x,-1-\alpha x^2\left(x+\beta\right)\right)\mid\alpha,\beta\in\mathbb{Q}^\star\text{ and }x\text{ root of}\\[2ex] B_2(x)=\alpha^2x^4+(2\alpha^2-1)x^3+\alpha^2\beta^2x^2+\alpha x+\alpha\beta\end{array}\right\}$$

Case $a=3$. By $(*)$, $[R_1+R_2+R_3+R_4-4\infty]=3j(P_0)=-2j(P_0)$. Then there exists a rational function F such that $div(F)=R_1+R_2+R_3+R_4+2P_0-6\infty$, so $F\in\mathcal{L}(6\infty)$ and therefore $F(x,y)=a_1+a_2x+a_3x^2+a_4y+a_5x^3$, $(a_5\neq 0)$.
The function F is of order 2 at point P_0 so $a_1=0$ and $a_2=0$, hence
$F(x,y)=a_3x^2+a_4y+a_5x^3$. At points R_i, we must have $a_3x^2+a_4y+a_5x^3=0$. Hence $y=-\frac{a_5}{a_4}x^2\left(x+\frac{a_3}{a_5}\right)$. We see that y is of the form $y=-\alpha x^2\left(x+\beta\right)$ with $\alpha,\beta\in\mathbb{Q}^*$. Also, $y(y+1)=x^5\Leftrightarrow\left(-\alpha x^2\left(x+\beta\right)\right)\left(1-\alpha x^2\left(x+\beta\right)\right)=x^5$ $\Leftrightarrow x^2\left(\alpha^2x^4+(2\alpha^2-1)x^3+\alpha^2\beta^2x^2-\alpha x-\alpha\beta\right)=0$. We must have $x^2\neq 0$ and $\alpha,\beta\in\mathbb{Q}^*$, and we obtain a family of quartic points

$$\mathcal{C}_3=\left\{\begin{array}{l}\left(x,-\alpha x^2\left(x+\beta\right)\right)\mid\alpha,\beta\in\mathbb{Q}^\star\text{ and }x\text{ root of}\\[2ex] B_3(x)=\alpha^2x^4+(2\alpha^2-1)x^3+\alpha^2\beta^2x^2-\alpha x-\alpha\beta\end{array}\right\}$$

Case $a=4$. By $(*)$, $[R_1+R_2+R_3+R_4-4\infty]=4j(P_0)=-j(P_0)$. Then there exists a rational function F such that
$div(F)=R_1+R_2+R_3+R_4+P_0-5\infty$, so $F\in\mathcal{L}(5\infty)$ and lemma 2.1 gives $F(x,y)=a_1+a_2x+a_3x^2+a_4y$, $(a_4\neq 0)$. At point P_0, we have $F(P_0)=0$ and so $a_1=0$. Hence $F(x,y)=a_2x+a_3x^2+a_4y$. At points R_i, we have $a_2x+a_3x^2+a_4y=0$. Thus $y=-\dfrac{a_2}{a_4}x-\dfrac{a_3}{a_4}x^2=-\dfrac{a_3}{a_4}x(x+\dfrac{a_2}{a_3})$. We see that y is of the form $y=-\alpha x(x+\beta)$ with $\alpha,\beta\in\mathbb{Q}^\star$. Therefore, $y(y+1)=x^5\Leftrightarrow(-\alpha x(x+\beta))\left(1-\alpha x(x+\beta)\right)=x^5\Leftrightarrow x^5-\alpha^2x^4-2\alpha^2\beta x^3-(\alpha+\alpha^2\beta^2)x^2-\alpha\beta x=0\Leftrightarrow x(x^4-\alpha^2x^3-2\alpha^2\beta x^2-(\alpha+\alpha^2\beta^2)x-\alpha\beta)=0$.

So $x \neq 0$ and $\alpha, \beta \in \mathbb{Q}^*$, we obtain a family of quartic points

$$\mathcal{C}_4 = \left\{ \begin{array}{l} (x, -\alpha x(x+\beta)) \mid \alpha, \beta \in \mathbb{Q}^\star \text{ and } x \text{ root of} \\ \\ B_4(x) = x^4 - \alpha^2 x^3 - 2\alpha^2\beta x^2 + (\alpha + \alpha^2\beta^2)x + \alpha\beta \end{array} \right\}$$

.

Conclusion. The set of quartic points on $\mathcal{C}$ is given by $\mathcal{C}_0 \cup \mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3 \cup \mathcal{C}_4$.

References

[1] The LMFDB Collaboration, The L-functions and Modular Forms Database. https://www.lmfdb.org/Genus2Curve/Q/

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

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

[4] M. Hindry, J. H. Silverman, Diophantine Geometry, An Introduction, Graduate Texts in Mathematics, 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, **6,** no. 11, (2016), 10295–10300.

[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 J. Math., **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 J. Math., (2021), 51–58.

[8] E. H. Sow, M. Fall, O. Sall, Parametrization of Algebraic Points of Low Degrees on the Hindry-Silverman Curve, Journal of Contemporary Applied Mathematics, **13,** no. 1, (2023), 64–70.