American Journal of Mathematics and Statistics 2022, 12(1): 5-8
DOI: 10.5923/j.ajms.20221201.02

Algebraic Points of Given Degree on the Affine Curve $C: y^2 = 4x^5 + 1$

El Hadji Sow*, Moussa Fall, Oumar Sall

U.F.R. of Science and Technology, Mathematics and Applications Laboratory, Assane SECK University of Ziguinchor, Senegal

Abstract In this work, we determine the set of algebraic points of given degree over $\mathbb{Q}$ on the curve of affine equation $y^2 = 4x^5 + 1$. This note extends a result of Booker, Sijsling, Sutherland, Voight and Yasak in [1] who gave a description of the set of $\mathbb{Q}$-rational points i.e the set of points of degree one over $\mathbb{Q}$ on this curve.

Keywords Planes curves, Degree of algebraic points, Rationals points, Algebraic extensions, Jacobian

1. Introduction

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

The goal is to determine the set of algebraic points of given degree over $\mathbb{Q}$ on the curve C given by the affine equation

$$y^2 = 4x^5 + 1$$

The Mordell-Weil group $J(\mathbb{Q})$ of rational points of the Jacobian is a finite set (refer to [1,4]).

We denote by: $P = (0,1)$, $\bar{P} = (0,-1)$ and ∞ the point at infinity. In [1] Booker, Sijsling, Sutherland, Voight and Yasak 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 C are given by

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

In this note, we give an explicit description of algebraic points of given degree over $\mathbb{Q}$ on the curve C.

Our main result is given by the following theorem:

Theorem: The set of algebraic points of given degree over $\mathbb{Q}$ on the curve C is
given by:

$$\coprod_{[K:\mathbb{Q}]\leq d} C(K) = \mathcal{F}_0 \cup A_1 \cup A_2$$

With:

$$\mathcal{F}_0 = \left\{ \left(x, -\frac{\sum_{i\leq \frac{n}{2}} a_i x^i}{\sum_{j\leq \frac{n-5}{2}} b_i x^j} \right) | \; a_i, b_j \in \mathbb{Q} \; and \; x \; root \; of \; E_0 \right\};$$

$$A_1 = \mathcal{F}_1 \cup \mathcal{F}_2 = \left\{ \left(x, -\frac{\sum_{i\leq \frac{n+1}{2}} a_i x^i}{\sum_{j\leq \frac{n-4}{2}} b_i x^j} \right) | \; a_i, b_j \in \mathbb{Q} \; with \; a_0 \pm b_0 = 0 \; and \; x \; root \; of \; E_1 \right\}$$

and

$$A_2 = G_1 \cup G_2 = \left\{ \left(x, -\frac{\sum_{i\leq \frac{n+1}{2}} a_i x^i}{\sum_{j\leq \frac{n-4}{2}} b_i x^j} \right) | \; a_i, b_j \in \mathbb{Q} \; with \; a_0 \pm b_0 = 0, a_1 \pm b_1 \; and \; x \; root \; of \; E_2 \right\}$$

where

$$E_0 = \left(\sum_{i\leq \frac{n}{2}} a_i x^i \right)^2 = \left(\sum_{j\leq \frac{n}{2}} b_i x^j \right)^2 (4x^5 + 1),$$

$$E_1 = \left(\sum_{i\leq \frac{n+1}{2}} a_i x^i \right)^2 = \left(\sum_{j\leq \frac{n-4}{2}} b_i x^j \right)^2 (4x^5 + 1)$$

and

$$E_2 = \left(\sum_{i\leq \frac{n+2}{2}} a_i x^i \right)^2 = \left(\sum_{j\leq \frac{n-3}{2}} b_i x^j \right)^2 (4x^5 + 1)$$

2. Auxiliary Results

For a divisor D on C, we note $\mathcal{L}(D)$ the $\mathbb{Q}$-vector space of rational functions F defined on $\mathbb{Q}$ such that $F = 0$ or $div(F) \geq -D$; $l(D)$ designates the $\overline{\mathbb{Q}}$-dimension of $\mathcal{L}(D)$. In [1, 4] the Mordell-Weil group $J(\mathbb{Q})$ of C is isomorph to $\mathbb{Z}/5\mathbb{Z}$ and C is a hyperelliptic curve of genus $g = 2$. Let x, y be two rational functions on $\mathbb{Q}$ defined as follow:

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

* Corresponding author:
elpythasow@yahoo.fr (El Hadji Sow)
Received: Feb. 16, 2022; Accepted: Mar. 4, 2022; Published: Mar. 15, 2022
Published online at http://journal.sapub.org/ajms

The projective equation of C is $Y^2Z^3 = 4X^5 + Z^5$

We denote by $\theta = e^{i\frac{\pi}{2}} \in \mathbb{C}$ and let's put $B_k = \left(\sqrt[5]{\frac{1}{4}}\,\theta^{2k+1}, 0\right)$ for $k \in \{0,1,2,3,4\}$.

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

Lemma 1:

- $div(x) = P + \bar{P} - 2\infty$
- $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$
- $div(y-1) = 5P - 5\infty$
- $div(y+1) = 5\bar{P} - 5\infty$

Proof: (See [10]).

Consequence of lemma 1:

$5j(P) = 5j(\bar{P})$ and $j(P) + j(\bar{P}) = 0$.

Lemma 2:

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

Proof:

- We have $l(\infty) = 1$ since if $l(\infty) = 2$, then the curve C is of genus zero (see [1,4]), which is not the case.
- Since the genus of C is equal to 2, then 2∞ is a canonical divisor of C, so $l(\infty) = g = 2$.
- For the rest we apply the Riemann-Roch theorem which says that $l(m\infty) = m - 1$ if $m \geq 3$.

Lemma 3:

A $\mathbb{Q}$-base of $\mathcal{L}(m\infty)$ is given by

$$\mathfrak{B}_m = \left\{x^i \mid i \in \mathbb{N} \text{ and } i \leq \frac{n}{2}\right\} \cup \left\{x^j y \mid j \in \mathbb{N} \text{ and } j \leq \frac{m-5}{2}\right\}.$$

Proof:

It is clear that $\mathfrak{B}_m$ is free and it remains to show that

$$card(\mathfrak{B}_m) = \dim \mathcal{L}\big((m\infty)\big).$$

According to the Riemann-Roch theorem, we have

$$\dim \mathcal{L}\big((m\infty)\big) = m - g + 1.$$

According to the parity of m, we have the following two cases:

Case 1: Suppose that m is even and let $m = 2h$. Thus we have $i \leq$ m/2 $= h$ and we have $j \leq$ (2h-5)/2 $\Leftrightarrow$ $j \leq$ (2h-5-1)/2 $= h - 3 = h - g - 1$. Then we get $\mathfrak{B}_m = \{1, x, \dots, x^h\} \cup \{y, yx, \dots, yx^{h-g-1}\}$. we have $card(\mathfrak{B}_m) = h + 1 + (h - g - 1 + 1) = m - g + 1 = \dim \mathcal{L}\big((m\infty)\big)$.

Case 2: Suppose that m is odd and let $m = 2h + 1$. Thus we have $i \leq$ m/2 $\Leftrightarrow$ $i \leq$ (2h+1)/2 $\Leftrightarrow$ $i \leq$ 2h/2 $= h$ and $j \leq$(m-5)/2$\Leftrightarrow$ $j \leq$(2h+1-5)/2$= h - g$.

Then we get $\mathfrak{B}_m = \{1, x, \dots, x^h\} \cup \{y, yx, \dots, yx^{h-g}\}$. We have $card(\mathfrak{B}_m) = h + 1 + (h - g + 1) = m + 1 - g = \dim \mathcal{L}\big((m\infty)\big)$.

Lemma 4:

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

Proof: (See [1,4]).

3. Proof of Theorem

Given $R \in C$ with $[\mathbb{Q}(R): \mathbb{Q}] = n$. The work of Booker, Sijsling, Sutherland, Voight and Yasak in [1] allows us to assume that $n \geq 2$.

Note that $R_1, R_2, \dots, R_n$ are the Galois conjugates of R. Let's work with

$t = [R_1 + R_2 + \cdots + R_n - n\infty] \in J(\mathbb{Q})$, according to lemma 4 we have $t = a[P - \infty]$, $0 \leq a \leq 4$.

So we have $[R_1 + R_2 + \cdots + R_n - n\infty] = a[P - \infty]$.

Our proof is divided in three cases:

Case $a = 0$

We have $[R_1 + R_2 + \cdots + R_n - n\infty] = 0$; then there exist a function F with coefficient in $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + \cdots + R_n - n\infty$, then $F \in \mathcal{L}(n\infty)$ and according to lemma 3 we have

$$F(x,y) = \sum_{i \leq \frac{n}{2}} a_i x^i + y \sum_{j \leq \frac{n-5}{2}} b_j x^j$$

For the points R_i, we have

$$\sum_{i \leq \frac{n}{2}} a_i x^i + y \sum_{j \leq \frac{n-5}{2}} b_j x^j = 0$$

hence $y = -\frac{\sum_{i \leq \frac{n+1}{2}} a_i x^i}{\sum_{j \leq \frac{n-5}{2}} b_j x^j}$ and the relation $y^2 = 4x^5 + 1$ gives the equation

$$E_0 = \left(\sum_{i \leq \frac{n}{2}} a_i x^i\right)^2 = \left(\sum_{j \leq \frac{n}{2}} b_i x^j\right)^2 (4x^5 + 1)$$

We find a family of points

$$\mathcal{F}_0 = \left\{\left(x, -\frac{\sum_{i \leq \frac{n}{2}} a_i x^i}{\sum_{j \leq \frac{n}{2}} b_i x^j}\right) \mid a_i, b_j \in \mathbb{Q} \text{ and } x \text{ root of } E_0\right\}$$

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

For $a = 1$, we have $[R_1 + R_2 + \cdots + R_n - n\infty] = [P - \infty] = -[\bar{P} - \infty]$, then there exist a function F with coefficient in $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + \cdots + R_n + \bar{P} - (n+1)\infty$, then $F \in \mathcal{L}((n+1)\infty)$ and according to lemma 3 we have

$$F(x,y) = \sum_{i \leq \frac{n+1}{2}} a_i x^i + y \sum_{j \leq \frac{n-4}{2}} b_j x^j$$

We have $F(\bar{P}) = 0 \Longrightarrow a_0 - b_0 = 0$.

For the points R_i, we have

$$\sum_{i\leq\frac{n+1}{2}} a_i x^i + y \sum_{j\leq\frac{n-4}{2}} b_j x^j = 0$$

hence $y = -\frac{\sum_{i\leq\frac{n+1}{2}} a_i x^i}{\sum_{j\leq\frac{n-4}{2}} b_j x^j}$ and the relation $y^2 = 4x^5 + 1$ gives the equation

$$E_1 = \left(\sum_{i\leq\frac{n+1}{2}} a_i x^i\right)^2 = \left(\sum_{j\leq\frac{n-4}{2}} b_i x^j\right)^2 (4x^5 + 1)$$

We find a family of points

$$\mathcal{F}_1 = \left\{ \begin{pmatrix} x, -\frac{\sum_{i\leq\frac{n+1}{2}} a_i x^i}{\sum_{j\leq\frac{n-4}{2}} b_i x^j} \end{pmatrix} | \, a_i, b_j \in \mathbb{Q} \; with \\ a_0 - b_0 = 0 \; and \; x \; root \; of \; E_1 \right\}$$

For $\boldsymbol{a = 4}$, we have $[R_1 + R_2 + \cdots + R_n - n\infty] = 4[P - \infty] = -[P - \infty]$.

By a similar argument as in case $a = 1$, we have

$$\mathcal{F}_2 = \left\{ \begin{pmatrix} x, -\frac{\sum_{i\leq\frac{n+1}{2}} a_i x^i}{\sum_{j\leq\frac{n-4}{2}} b_i x^j} \end{pmatrix} | \, a_i, b_j \in \mathbb{Q} \; with \\ a_0 + b_0 = 0 \; and \; x \; root \; of \; E_1 \right\}$$

Finally, we have the family

$$A_1 = \mathcal{F}_1 \cup \mathcal{F}_2 = \left\{ \begin{pmatrix} x, -\frac{\sum_{i\leq\frac{n+1}{2}} a_i x^i}{\sum_{j\leq\frac{n-4}{2}} b_i x^j} \end{pmatrix} | \, a_i, b_j \in \mathbb{Q} \; with \\ a_0 \pm b_0 = 0 \; and \; x \; root \; of \; E_1 \right\}$$

Cases $\boldsymbol{a = 2}$ and $\boldsymbol{a = 3}$

For $\boldsymbol{a = 2}$, we have $[R_1 + R_2 + \cdots + R_n - n\infty] = 2[P - \infty] = -2[\bar{P} - \infty]$, then there exist a function F with coefficient in $\mathbb{Q}$ such that

$div(F) = R_1 + R_2 + \cdots + R_n + 2\bar{P} - (n+2)\infty$, then $F \in \mathcal{L}((n+1)\infty)$ and according to lemma 3 we have

$$F(x, y) = \sum_{i\leq\frac{n+2}{2}} a_i x^i + y \sum_{j\leq\frac{n-3}{2}} b_j x^j$$

The function F is of order 2 at point P so we must have

$$\begin{cases} F(\bar{P}) = 0 \\ F_x'(\bar{P}) = 0 \end{cases} \Rightarrow \begin{cases} a_0 - b_0 = 0 \\ a_1 - b_1 = 0 \end{cases}$$

For the points R_i, we have

$$\sum_{i\leq\frac{n+2}{2}} a_i x^i + y \sum_{j\leq\frac{n-3}{2}} b_j x^j = 0$$

hence $y = -\frac{\sum_{i\leq\frac{n+2}{2}} a_i x^i}{\sum_{j\leq\frac{n-3}{2}} b_j x^j}$ and the relation

$y^2 = 4x^5 + 1$ gives the equation

$$E_2 = \left(\sum_{i\leq\frac{n+2}{2}} a_i x^i\right)^2 = \left(\sum_{j\leq\frac{n-3}{2}} b_i x^j\right)^2 (4x^5 + 1)$$

We find a family of points

$$G_1 = \left\{ \begin{pmatrix} x, -\frac{\sum_{i\leq\frac{n+2}{2}} a_i x^i}{\sum_{j\leq\frac{n-3}{2}} b_i x^j} \end{pmatrix} | \, a_i, b_j \in \mathbb{Q} \; with \\ a_0 - b_0 = 0 \, , \; a_1 - b_1 = 0 \; and \; x \; root \; of \; E_2 \right\}$$

For $\boldsymbol{a = 3}$, we have $[R_1 + R_2 + \cdots + R_n - n\infty] = 3[P - \infty] = -2[P - \infty]$.

By a similar argument as in case $a = 2$, we have

$$G_2 = \left\{ \begin{pmatrix} x, -\frac{\sum_{i\leq\frac{n+2}{2}} a_i x^i}{\sum_{j\leq\frac{n-3}{2}} b_i x^j} \end{pmatrix} | \, a_i, b_j \in \mathbb{Q} \; with \\ a_0 + b_0 = 0 \, , \; a_1 + b_1 = 0 \; and \; x \; root \; of \; E_2 \right\}$$

Finally, we have the family

$$A_2 = G_1 \cup G_2 = \left\{ \begin{pmatrix} x, -\frac{\sum_{i\leq\frac{n+1}{2}} a_i x^i}{\sum_{j\leq\frac{n-4}{2}} b_i x^j} \end{pmatrix} | \, a_i, b_j \in \mathbb{Q} \; with \\ a_0 \pm b_0 = 0, a_1 \pm b_1 \; and \; x \; root \; of \; E_2 \right\}$$

REFERENCES

[1] A. R. Booker, J. Sijsling, A. V. Sutherland, J. Voight and D. Yasak, A database of genus-2 curves over the rational numbers. LMS Journal of Computation and Mathematics, 19(A), 235-254, 2016.

[2] N. Bruin, On powers as sums of two cubes, International Algorithmic Number Theory Symposium. Springer, Berlin, Heidelberg, 2000.

[3] A. Chenciner, Courbes algébriques planes. Springer, 2008.

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

[5] 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.

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

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

[8] J. TH. Mulholland, Elliptic curves with rational 2-torsion and related ternary Diophantine equations. ProQuest LLC. Ann Arbor, MI (2006).

[9] S. Siksek, Explicit Chabauty over number fields, Algebra & Number Theory, Volume 7, No. 4, 765-793, 2013.

[10] 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, Issue 6, 2021.

[11] 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.