Journal of Contemporary Applied Mathematics
V. 14, No 1, 2024, July
ISSN 2222-5498
DOI 10.5281/zenodo.10464631

Algebraic Points on the Genus 2 Curve $\mathcal{C} : y^2 = 5(1 - x^5)$

EL Hadji SOW, Moussa FALL and Oumar SALL

Abstract. Using Abel-Jacobi Theorem (see [1], p.155) and linear systems on the curve $\mathcal{C}$, we give the set of algebraic points of given degree over $\mathbb{Q}$ on the hyperelliptic curve $\mathcal{C}$ given by the affine equation $y^2 = 5(1 - x^5)$. This result extends a result of Tsuzuki, Yamauchi who described in ([3], p.30, Theorem 7.3) the $\mathbb{Q}$-rational points on this curve.

Key Words and Phrases: Plane curve; Degree of algebraic points; Rational points; Algebraic extensions.

2010 Mathematics Subject Classifications: Primary 14H50, 14H40, 11D68

---

1. Introduction

Let $\mathcal{C}$ be a smooth algebraic curve of genus $g = 2$ defined 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 $\mathcal{C} \longrightarrow J(\mathbb{Q})$. Mordell-Weil Theorem states that the group $J(\mathbb{Q})$ of rational points of J is a abelian group of finite type e. g. $J(\mathbb{Q}) \cong \mathbb{Z}^r \times J(\mathbb{Q})_{torsion}$ where $J(\mathbb{Q})_{torsion}$ and the integer r are called respectily the torsion group and the rank of J. We denote by $\mathcal{C}^{(l)}(\mathbb{Q})$ the set of algebraic points of degree at most l over $\mathbb{Q}$ on the curve $\mathcal{C}$. Let $P = (1, 0)$ and ∞ on $\mathcal{C}$. Using Abel-Jacobi Theorem (see [1], p.155) and linear systems on the curve $\mathcal{C}$, the goal of this paper is to determine the set $\mathcal{C}^{(l)}(\mathbb{Q})$ on the curve $\mathcal{C}$ of affine equation

$$y^2 = 5(1 - x^5). \tag{1}$$

The $\mathbb{Q}$-rational points on $\mathcal{C}$ (see [3], p.30, Theorem 7.3) are given by $\mathcal{C}(\mathbb{Q}) = \{\infty, P\}$. The Mordell-Weil group $J(\mathbb{Q})$ of rational points of the jacobian is a finite set (see [3], p.30, Remark 7.4). Let x, y be two rational functions over $\mathbb{Q}$ defined as follow:
$x(X, Y, Z) = \frac{X}{Z}$ *et* $y(X, Y, Z) = \frac{Y}{Z}$. The projective equation of $\mathcal{C}$ is

$$\mathcal{C} : Y^2 Z^3 = 5(Z^5 - X^5). \tag{2}$$

2. Auxiliary results

For a divisor D on $\mathcal{C}$, we note $\mathcal{L}(D)$ the $\bar{\mathbb{Q}}$-vector space of rational functions F defined over $\mathbb{Q}$ such that $F=0$ or $div(F) \geq -D$; $l(D)$ designates the $\bar{\mathbb{Q}}$-dimension of $\mathcal{L}(D)$.

Lemma 2.1.

- $div(x-1) = 2P - 2\infty$;
- $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$;
- $div(x) = A_0 + A_1 - 2\infty$.

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

- $div(x-1) = (X - Z = 0).\mathcal{C} - (Z = 0).\mathcal{C}$
  For $X = Z$, we have $Y^2 = 0$ with $Z = 1$ or $Z^3 = 0$ with $Y = 1$. We obtain the point $P = (1, 0, 1)$ with multiplicity 2 and the point $\infty = (0, 1, 0)$ with multiplicity 3. Hence $(X - Z = 0).\mathcal{C} = 2P + 3\infty$ $(*)$.
  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 $(**)$ implies that $div(x-1) = 2P - 2\infty$.
- Similarly we show that $div(y) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$ and $div(x) = A_0 + A_1 - 2\infty$.

$\square$

Lemma 2.2. *A $\mathbb{Q}$-base of $\mathcal{L}(m\infty)$ is given by*

$$\mathcal{B}_m = \left\{x^i \mid i \in \mathbb{N} \; and \; i \leq \frac{m}{2}\right\} \cup \left\{yx^j \mid j \in \mathbb{N} \; and \; j \leq \frac{m-5}{2}\right\}. \tag{3}$$

Proof. As $\mathcal{B}_m$ is free, it suffices to show that $card(\mathcal{B}_m) = dim\mathcal{L}(m\infty)$. And according to the Riemann-Roch Theorem, $dim\mathcal{L}(m\infty) = m - g + 1 = m - 2 + 1 = m - 1$ as $m \geq 2g - 1 = 3$ and with the parity of m, two cases are possible:
1^{st} **case**: if m is odd, then by putting $m = 2h + 1$, we have
$i \leq \frac{m}{2} \Leftrightarrow i \leq \frac{2h+1}{2} \Leftrightarrow i \leq h + \frac{1}{2} \Rightarrow i \leq h$ and $j \leq \frac{m-5}{2} \Leftrightarrow j \leq \frac{2h-4}{2} \Rightarrow j \leq h - 2$.
Thus $\mathcal{B}_m = \{1, x, \ldots, x^h\} \cup \{y, yx, \ldots, yx^{h-2}\}$ and so we have

$$card(\mathcal{B}_m) = h + 1 + h - 2 + 1 = 2h = m - 1 = dim\mathcal{L}(m\infty).$$

Second case: We suppose that m is even then $m = 2h$ and we hawe $i \leq \frac{m}{2} \Leftrightarrow i \leq \frac{2h}{2} \Rightarrow i \leq h$ and $j \leq \frac{m-5}{2} \Leftrightarrow j \leq \frac{2h-5}{2} \Leftrightarrow j \leq h - \frac{5}{2} \Rightarrow j \leq h - \frac{4}{2} = h - 2 \Rightarrow j \leq h - 3$. It follows that $\mathcal{B}_m = \{1, x, \ldots, x^h\} \cup \{y, yx, \ldots, yx^{h-3}\}$ and so we have

$$card(\mathcal{B}_m) = h + 1 + h - 3 + 1 = 2h - 1 = m - 1 = dim\mathcal{L}(m\infty).$$

$\square$

Lemma 2.3. $J(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} = \langle [P-\infty] \rangle = \{a\,[P-\infty]\,, a \in \{0,1\}\}$.

Proof. Refer to [3]. $\square$

3. Main results

Our main result is given by the following theorem:

Theorem 3.1. *The set of algebraic points of degree $l \geq 2$ over $\mathbb{Q}$ on the curve $\mathcal{C}$ is given by:*

$$\mathcal{C}^{(l)}(\mathbb{Q}) = \mathcal{F}_0 \cup \mathcal{F}_1$$

with

$$\mathcal{F}_0 = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{i \leq \frac{l}{2}} a_i x^i}{\sum\limits_{j \leq \frac{l-5}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \text{ and } x \text{ root of the equation} \\ \\ (\mathcal{E}_0) : (\sum_{i \leq \frac{l}{2}} a_i x^i)^2 + 5(\sum_{j \leq \frac{l-5}{2}} b_j x^j)^2 (x^5 - 1) = 0 \end{array} \right\},$$

$$\mathcal{F}_1 = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{i \leq \frac{l+1}{2}} a_i x^i}{\sum\limits_{j \leq \frac{l-4}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q}\ ,\ a_0 = 0 \text{ and } x \text{ root of the equation} \\ \\ (\mathcal{E}_1) : (\sum_{i \leq \frac{l+1}{2}} a_i x^i)^2 + 5(\sum_{j \leq \frac{l-4}{2}} b_j x^j)^2 (x^5 - 1) = 0 \end{array} \right\}.$$

Proof. Given $R \in \mathcal{C}(\bar{\mathbb{Q}})$ with $[\mathbb{Q}[R] : \mathbb{Q}] = l$. The work of Tsuzuki and Yamauchi who described in ([3], p.30, Theorem 7.3) allows us to assume that $l \geq 2$. Note that $R_1, R_2, \ldots, R_l$ are the Galois conjugates of R. Let's work with $t = [R_1+R_2+\cdots+R_l-l\infty] \in J(\mathbb{Q})$, according to lemma 2.3; we have $t = a\,[P-\infty]\,,\ 0 \leq a \leq 1$. So we have $[R_1+R_2+\cdots+R_l-l\infty] = a\,[P-\infty]$.

For $a = 0$, we have $[R_1 + R_2 + \cdots + R_l - l\infty] = 0$; then there exist a function F with coefficient in $\mathbb{Q}$ such that $div(F) = R_1+R_2+\cdots+R_l-l\infty$, then $F \in \mathcal{L}(l\infty)$ and according to lemma 2.2; we have

$$F(x,y) = \left(\sum_{i \leq \frac{l}{2}} a_i x^i \right) + y \left(\sum_{j \leq \frac{l-5}{2}} b_j x^j \right). \tag{4}$$

For the points R_i, we have

$$\left(\sum_{i \leq \frac{l}{2}} a_i x^i \right) + y \left(\sum_{j \leq \frac{l-5}{2}} b_j x^j \right) = 0. \tag{5}$$

hence $y = -\dfrac{\sum\limits_{i \le \frac{l}{2}} a_i x^i}{\sum\limits_{j \le \frac{l-5}{2}} b_j x^j}$ and the relation (1.1) gives the equation

$$(\mathcal{E}_0) : \left(\sum_{i \le \frac{l}{2}} a_i x^i \right)^2 = 5 \left(\sum_{j \le \frac{l-5}{2}} b_j x^j \right)^2 (1 - x^5).$$

We find a family of points

$$\mathcal{F}_0 = \left\{ \begin{array}{l} \left(x, -\dfrac{\sum\limits_{i \le \frac{l}{2}} a_i x^i}{\sum\limits_{j \le \frac{l-5}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \text{ and } x \text{ root of the equation} \\ \\ (\mathcal{E}_0) : (\sum_{i \le \frac{l}{2}} a_i x^i)^2 + 5(\sum_{j \le \frac{l-5}{2}} b_j x^j)^2 (x^5 - 1) = 0 \end{array} \right\}.$$

For $a = 1$, we have $[R_1 + R_2 + \cdots + R_l - l\infty] = [P - \infty] = -[P - \infty]$; then there exist a function F with coefficient in $\mathbb{Q}$ such that $div(F) = R_1 + R_2 + \cdots + R_l + P - (l+1)\infty$, then $F \in \mathcal{L}((l+1)\infty)$ and according to lemma 2.2; we have

$$F(x, y) = \left(\sum_{i \le \frac{l+1}{2}} a_i x^i \right) + y \left(\sum_{j \le \frac{l-4}{2}} b_j x^j \right). \tag{6}$$

We have $F(P) = 0$ implies the relation

$$\sum_{i \le \frac{l+1}{2}} a_i = 0.$$

For the points R_i, we have

$$\left(\sum_{i \le \frac{l+1}{2}} a_i x^i \right) + y \left(\sum_{j \le \frac{l-4}{2}} b_j x^j \right) = 0 \tag{7}$$

hence $y = -\dfrac{\sum\limits_{i \le \frac{n+1}{2}} a_i x^i}{\sum\limits_{j \le \frac{n-4}{2}} b_j x^j}$ and the relation (1.1) gives the equation

$$(\mathcal{E}_1) : \left(\sum_{i \le \frac{l+1}{2}} a_i x^i \right)^2 = 5 \left(\sum_{j \le \frac{l-4}{2}} b_j x^j \right)^2 (1 - x^5).$$

We find a family of points

$$\mathcal{F}_1 = \left\{ \begin{array}{l} \left(x, -\dfrac{\displaystyle\sum_{i \leq \frac{l+1}{2}} a_i x^i}{\displaystyle\sum_{j \leq \frac{l-4}{2}} b_j x^j} \right) \mid a_i, b_j \in \mathbb{Q} \ , \ \sum_{i \leq \frac{l+1}{2}} a_i = 0 \text{ and } x \text{ root of the equation} \\ \\ (\mathcal{E}_1) : (\sum_{i \leq \frac{l+1}{2}} a_i x^i)^2 + 5(\sum_{j \leq \frac{l-4}{2}} b_j x^j)^2 (x^5 - 1) = 0 \end{array} \right\}.$$

$\square$

4. Concluding Remarks

Despite the study carried out on this curve, the field of investigation is still very vast, so even if we have determined the algebraic points of any degree on $\mathcal{C}$, we still have to explicitly determine the algebraic points of degree exactly l.

References

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

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

[3] N. Tsuzuki, T. Yamauchi, Automorphy of mod 2 Galois representations associated to the quintic Dwork family and reciprocity of some quintic trinomials, arXiv:2008.09852v4 [math.NT] 28 Sep 2022.

El Hadji Sow
Assane Seck University, Ziguinchor, SENEGAL
E-mail: elpythasow@yahoo.fr

Moussa Fall
Assane Seck University, Ziguinchor, SENEGAL
E-mail: moussafalls@yahoo.fr

Oumar Sall
Assane Seck University, Ziguinchor, SENEGAL
E-mail: osall@univ-zig.sn

Received 20 June 2023
Accepted 06 January 2024