Journal of Contemporary Applied Mathematics
V. 15, No 1, 2025, June
ISSN 2222-5498, E-ISSN 3006-3183
https://doi.org/10.62476/jcam.151.10

Algebraic Points of Degree $l \geq 2$ over $\mathbb{Q}$ on the Affine Curve $\mathcal{X} : n^2 = 3(m^5 - 1)$

E. H. Sow, O. Sall

Abstract. We determine the set of algebraic points of degree degree $l \geq 2$ over $\mathbb{Q}$ on the curve $\mathcal{X}$ given by the affine equation $n^2 = 3(m^5 - 1)$ and this result extends a result of Siksek who described in [5] the set of algebraic points of degree 1 on this curve.

Key Words and Phrases: Planes curves, Degree of algebraic points, Rationals points, Algebraic extensions - Jacobian

2010 Mathematics Subject Classifications: 14H50, 14H40, 11D68, 12F05

1. Introduction and main result

Let $\mathcal{X}$ be a smooth algebraic curve of genus 2 defined over a numbers field K. We note by $\mathcal{X}$(K) the set of points of $\mathcal{X}$ with coordinates in K.
We denote by J the jacobian of $\mathcal{X}$ and by $j(P)$ the class $[T - \infty]$ of $T - \infty$, that is to say that j is the Jacobian diving $\mathcal{X} \longrightarrow J(\mathbb{Q})$. The Mordell-Weil group $J(\mathbb{Q})$ of rational points of the jacobian is a finite set (refer to [5]).
For a divisor D on $\mathcal{X}$, 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 $\overline{Q}$-dimension of $\mathcal{L}(D)$. The goal is to determine the set of algebraic points of given degree $l \geq 2$ over $\mathbb{Q}$ on the curve $\mathcal{C}$ given by the affine equation

$$n^2 = 3(m^5 - 1) \tag{1}$$

From [5] we have $T = (1, 0)$ et ∞ the rational points over $\mathbb{Q}$ on this curve.
Our main result is given by the following theorem:
Theorem. The set of algebraic points of given degree $l \geq 2$ over $\mathbb{Q}$ on the curve $\mathcal{X}$ is given by:

$$\bigcup_{[K:\mathbb{Q}] \leq l} \mathcal{X}(K) = \mathcal{V}_0 \cup \mathcal{V}_1$$

with

$$\mathcal{V}_0 = \left\{ \left(m, -\frac{\sum\limits_{i \le \frac{l}{2}} a_i m^i}{\sum\limits_{j \le \frac{l-5}{2}} b_j m^j} \right) \mid a_i, b_j \in \mathbb{Q} \textit{ and } m \textit{ root of the equation } (\mathcal{E}_0) \right\},$$

$$\mathcal{V}_1 = \left\{ \left(m, -\frac{\sum\limits_{i \le \frac{l+1}{2}} a_i m^i}{\sum\limits_{j \le \frac{l-4}{2}} b_j m^j} \right) \mid a_i, b_j \in \mathbb{Q} \textit{ with } \sum_{i \le \frac{l+1}{2}} a_i = 0 \textit{ et and } m \textit{ root of the equation } (\mathcal{E}_1) \right\}$$

where

$$(\mathcal{E}_0) : \left(\sum_{i \le \frac{l}{2}} a_i m^i \right)^2 = 3 \left(\sum_{j \le \frac{l-5}{2}} b_j m^j \right)^2 (m^5 - 1),$$

$$(\mathcal{E}_1) : \left(\sum_{i \le \frac{l+1}{2}} a_i m^i \right)^2 = 3 \left(\sum_{j \le \frac{l-4}{2}} b_j m^j \right)^2 (m^5 - 1).$$

2. Auxiliary results

In [5], the Mordell-Weil group $J(\mathbb{Q})$ of $\mathcal{X}$ is isomorph to $\mathbb{Z}/2\mathbb{Z}$ and $\mathcal{X}$ is a hyperelliptic curve of genus $g = 2$. Let m, n be two rational functions on $\mathbb{Q}$ defined as follow:

$$m(M, N, Z) = \frac{M}{Z} \textit{ et } n(M, N, Z) = \frac{N}{Z}$$

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

$$\mathcal{M} : N^2 Z^3 = 3(M^5 - Z^5) \tag{2}$$

We denote by $\eta_1 = e^{i\frac{\Pi}{2}}$ and let's put $A_k = (0, \sqrt{3}\eta_1^{2k+1})$ for $k \in \{0, 1\}$.
We denote by $\eta_2 = e^{i\frac{\Pi}{5}}$ and let's put $B_k = (\eta_2^{2k}, 0)$ for $k \in \{0, 1, 2, 3, 4\}$.
Let us designate by $\mathcal{D}.\mathcal{X}$ the intersection cycle of algebraic curve $\mathcal{D}$ defined on $\mathbb{Q}$ and $\mathcal{X}$.

Lemma 1.

- $div(m-1) = 2T - 2\infty$
- $div(n) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$
- $div(m) = A_0 + A_1 - 2\infty$

Proof $\mathcal{X} : N^2Z^3 = 3(M^5 - Z^5)$ (projective equation)

- $div(m-1) = (M - Z = 0).\mathcal{X} - (Z = 0).\mathcal{X}$
  For $M = Z$, we have $N^2 = 0$ with $Z = 1$ or $Z^3 = 0$ with $N = 1$. We obtain the point $T = (1, 0, 1)$ with multiplicity 2 and the point $\infty = (0, 1, 0)$ with multiplicity 3. Hence $(M - Z = 0).\mathcal{X} = 2T + 3\infty$ $(*)$.
  Even if $Z = 0$, then $M^5 = 0$; and for $N = 1$, we have the point $\infty = (0, 1, 0)$ with multiplicity 5. Hence $(Z = 0).\mathcal{X} = 5\infty$ $(**)$.
  The relations $(*)$ and $(**)$ implies that $div(m-1) = 2T - 2\infty$.
- Similarly we show that $div(n) = B_0 + B_1 + B_2 + B_3 + B_4 - 5\infty$ and $div(m) = A_0 + A_1 - 2\infty$

Lemma 2. *[6]*

- $\mathcal{L}(\infty) = \langle 1 \rangle$
- $\mathcal{L}(2\infty) = \langle 1,\, m \rangle = \mathcal{L}(3\infty)$
- $\mathcal{L}(4\infty) = \left\langle 1,\, m,\, m^2 \right\rangle$
- $\mathcal{L}(5\infty) = \left\langle 1,\, m,\, m^2,\, n \right\rangle$
- $\mathcal{L}(6\infty) = \left\langle 1,\, m,\, m^2,\, n,\, m^3 \right\rangle$

Lemma 3. *[6]*
A $\mathbb{Q}$-base of $\mathcal{L}(r\infty)$ is given by

$$\mathcal{B}_r = \left\{ m^i \mid i \in \mathbb{N} \text{ and } i \leq \frac{r}{2} \right\} \cup \left\{ m^j n \mid j \in \mathbb{N} \text{ and } j \leq \frac{r-5}{2} \right\}$$

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

3. Proof of theorem

Given $S \in \mathcal{X}(\bar{\mathbb{Q}})$ with $[\mathbb{Q}[S] : \mathbb{Q}] = l$. The work of Siksek in [5] allows us to assume that $l \geq 2$. Note that $S_1, S_2, \ldots, S_l$ are the Galois conjugates of S. Let's work with $t = [S_1 + S_2 + \cdots + S_l - l\infty] \in J(\mathbb{Q})$, according to Lemma 4 we have $t = a\,[T - \infty]\,,\ 0 \leq a \leq 1$. So we have $[S_1 + S_2 + \cdots + S_l - l\infty] = a\,[T - \infty]$.
For $a = 0$, we have $[S_1 + S_2 + \cdots + S_l - l\infty] = 0$; then there exist a function F

with coefficient in $\mathbb{Q}$ such that $div(F) = S_1 + S_2 + \cdots + S_l - l\infty$, then $F \in \mathcal{L}(l\infty)$ and according to Lemma 3 we have

$$F(m,n) = \left(\sum_{i \leq \frac{l}{2}} a_i m^i \right) + \left(n \sum_{j \leq \frac{l-5}{2}} b_j m^j \right). \tag{3}$$

For the points S_i, we have

$$\left(\sum_{i \leq \frac{l}{2}} a_i m^i \right) + \left(n \sum_{j \leq \frac{l-5}{2}} b_j m^j \right) = 0. \tag{4}$$

hence $n = -\dfrac{\sum_{i \leq \frac{l}{2}} a_i m^i}{\sum_{j \leq \frac{l-5}{2}} b_j m^j}$ and the relation $n^2 = 3(m^5 - 1)$ gives the equation

$$(\mathcal{E}_0) : \left(\sum_{i \leq \frac{l}{2}} a_i m^i \right)^2 = 3 \left(\sum_{j \leq \frac{l-5}{2}} b_j m^j \right)^2 (m^5 - 1).$$

We find a family of points

$$\mathcal{V}_0 = \left\{ \left(m, -\frac{\sum_{i \leq \frac{l}{2}} a_i m^i}{\sum_{j \leq \frac{l-5}{2}} b_j m^j} \right) \mid a_i, b_j \in \mathbb{Q} \textit{ and } m \textit{ root of the equation } (\mathcal{E}_0) \right\}.$$

For $a = 1$, we have $[S_1 + S_2 + \cdots + S_l - l\infty] = [T - \infty] = -[T - \infty]$; then there exist a function F with coefficient in $\mathbb{Q}$ such that $div(F) = S_1 + S_2 + \cdots + S_l + T - (l+1)\infty$, then $F \in \mathcal{L}((l+1)\infty)$ and according to Lemma 3 we have

$$F(m,n) = \left(\sum_{i \leq \frac{l+1}{2}} a_i m^i \right) + \left(n \sum_{j \leq \frac{l-4}{2}} b_j m^j \right). \tag{5}$$

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

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

.
For the points S_i, we have

$$\left(\sum_{i\leq\frac{l+1}{2}} a_i m^i\right) + \left(n \sum_{j\leq\frac{l-4}{2}} b_j m^j\right) = 0. \qquad (6)$$

hence $n = -\frac{\sum_{i\leq\frac{l+1}{2}} a_i m^i}{\sum_{j\leq\frac{l-4}{2}} b_j m^j}$ and the relation $n^2 = 3(m^5 - 1)$ gives the equation

$$(\mathcal{E}_1) : \left(\sum_{i\leq\frac{l+1}{2}} a_i m^i\right)^2 = 3\left(\sum_{j\leq\frac{l-4}{2}} b_j m^j\right)^2 (m^5 - 1).$$

We find a family of points

$$\mathcal{V}_1 = \left\{\left(m, -\frac{\sum_{i\leq\frac{l+1}{2}} a_i m^i}{\sum_{j\leq\frac{l-4}{2}} b_j m^j}\right) \mid a_i, b_j \in \mathbb{Q}\ with \sum_{i\leq\frac{l+1}{2}} a_i = 0\ et\ and\ m\ root\ of\ the\ equation\ (\mathcal{E}_1)\right\}.$$

References

[1] R. F. Coleman, Effective Chabauty method, Duke Math. J. vol.52, no. 3, 765–770, 1985.

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

[3] M. Hindry and J. H. Silverman, Introduction to algebraic curves, An Introduction, Graduate Texts in Mathematics, January 1, 2000.

[4] S. Siksek and M. Stoll, Partial descent on hyper elliptic curves and the generalized Fermat equation $x^3 + y^4 + z^5 = 0$, Bulletin of the LMS 44, 151–166, 2012.

[5] S. Siksek, Explicit Chabauty over number fields, Algebra & Number Theory, Volume 7, 2013.

[6] E. H. Sow et al, Algebraic points on the genus 2 curve $C : y^2 = 5(1 - x^5)$, J. Contemp. Appl. Math. 14, No. 1, 28–32, J. Contemp. Appl. Math. 14, No. 1, 28–32, 2024.

[7] L. C. Washington, Elliptic curves, Number Theroy and Cryptography, Second Edition, 2008.

El Hadji Sow
Assane Seck University, Ziguinchor, SENEGAL
E-mail: elpythasow@yahoo.fr ; e.sow4727@zig.univ.sn

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

Received 23 December 2024
Accepted 26 March 2025