sciendo
Ann. Univ. Paedagog. Crac. Stud. Math. 22 (2023), 21-31
DOI: 10.2478/aupcsm-2023-0003

FOLIA 385

Annales Universitatis Paedagogicae Cracoviensis
Studia Mathematica 22 (2023)

Moustapha Camara, Moussa Fall and Oumar Sall

Algebraic points on the hyperelliptic curves $y^2 = x^5 + n^2$

Abstract. We give an algebraic description of the set of algebraic points of degree at most d over $\mathbb{Q}$ on hyperelliptic curves $y^2 = x^5 + n^2$.

1. Introduction and result

Let $\mathbb{Q}$ be the field of rational numbers and $\overline{\mathbb{Q}}$ a algebraic closure of $\mathbb{Q}$. Let $\mathcal{C}$ be an algebraic curve of genus $g \geq 2$ defined over $\mathbb{Q}$, and $J_{\mathcal{C}}$ its jacobian variety. A celebrated theorem of Mordell-Weil states that the group $J_{\mathcal{C}}(\mathbb{Q})$ of rational points of the jacobian $J_{\mathcal{C}}$ is a abelian group of finite type, e.g. $J_{\mathcal{C}}(\mathbb{Q}) \cong \mathbb{Z}^r \times J_{\mathcal{C}}(\mathbb{Q})_{\mathrm{tors}}$, where the integer r is called the rank of the variety $J_{\mathcal{C}}$ and $J_{\mathcal{C}}(\mathbb{Q})_{\mathrm{tors}}$ the torsion subgroup. In this note, we study the algebraic points of degree at most d on hyperelliptic curves $\mathcal{C}_A$ of genus 2 of affine equations

$$\mathcal{C}_A : y^2 = x^5 + A \qquad \text{for some integer } A.$$

The degree of an algebraic point on $\mathcal{C}_A$ is the degree of its field of definition over $\mathbb{Q}$. Note that the case $A = 1$ goes back to Schaefer ([8]), Fall ([3]) and Sall, et al ([7]). The purpose of this note is to settle the case $A = n^2$ with $n \in \{4, 5, 8, 10, 12, 16, 20, 27, 36, 144, 162, 216, 400, 432, 625, 648, 1250, 1296, 5000\}$. Let η be a primitive 10-th root of unity in $\overline{\mathbb{Q}}$ and we put $A_k^n = (\sqrt[5]{n^2}\eta^{2k+1}, 0)$ with $0 \leq k \leq 4$. Also let $P_n = (0, n)$, $\overline{P_n} = (0, -n)$ and P_∞ the point at infinity on $\mathcal{C}_{n^2}$. Various works study these curves (see [9], [10], [11]).

AMS (2020) Subject Classification: 14H50, 14hH40, 11D68, 12FO5.
Keywords and phrases: Hyperelliptic curves, rational points, 2-descent, Mordell-Weil groups.
ISSN: 2081-545X, e-ISSN: 2300-133X.

Combining the results given by Mulholland ([5], p. 177-178) and Bruni ([1], p. 142), we obtain the following theorem

Theorem 1
The $\mathbb{Q}-$rational points on the curve $\mathcal{C}_{n^2}$ are given by

$$\mathcal{C}_{n^2}(\mathbb{Q}) = \{P_n, \overline{P_n}, P_\infty\}.$$

It is also known since Faltings ([2]), for a number field K, the set $\mathcal{C}_{n^2}(K)$ of K-rational points on $\mathcal{C}_{n^2}$ is finite. We are interested mostly in this note in describing this set. More precisely, we give an algebraic description of the set of algebraic points of degree at most d over $\mathbb{Q}$ on the curve $\mathcal{C}_{n^2}$. We denote this set by $\mathcal{C}^d_{n^2}(\mathbb{Q})$. The underlying principle of the method used to study these algebraic points in this paper is as follows. It is assumed that one knows or determines the structure of the Mordell-Weil group $J_{\mathcal{C}_{n^2}}(\mathbb{Q})$ and that it is finite (e.g. $r = 0$),

$$J_{\mathcal{C}_{n^2}}(\mathbb{Q}) \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}.$$

Consider a base point $P_\infty \in \mathcal{C}_{n^2}(\mathbb{Q})$; the Abel–Jacobi map associated to P_∞ is the embedding $j\colon \mathcal{C}_{n^2} \to J_{\mathcal{C}_{n^2}},\ P \mapsto [P - P_\infty]$, where $[P - P_\infty]$ denotes the class of the divisor $P - P_\infty$. We then determine $D_1, \ldots, D_s$ divisors on $\mathcal{C}_{n^2}$ defined over $\mathbb{Q}$ such that $j(D_i)$ is of order n_i and $j(D_1), \ldots, j(D_s)$ generate $J_{\mathcal{C}_{n^2}}(\mathbb{Q})$. Let then R be an algebraic point on $\mathcal{C}_{n^2}$ of degree d. Let $R_1, \ldots, R_d$ be its conjugates under the Galois action, then $j(R_1 + \cdots + R_d) \in J_{\mathcal{C}_{n^2}}(\mathbb{Q})$ and consequently, there exist m_i with $0 \le m_i \le n_i - 1$ such that $j(R_1 + \cdots + R_d) = m_1 j(D_1) + \cdots + m_s j(D_s)$. The Abel-Jacobi theorem (see [4], p. 155) leads to the existence of a rational function f defined over $\mathbb{Q}$ such that

$$\mathrm{div}(f) = R_1 + \cdots + R_d - m_1 D_1 - \cdots - m_s D_s + \big(\textstyle\sum_{1\le i\le s} m_i \deg(D_i) - d\big) P_\infty.$$

Our main result is the following theorem.

Theorem 2

1. *The algebraic points of degree 2 on $\mathcal{C}_{n^2}$ over $\mathbb{Q}$ are given by*

$$\mathcal{C}^{(2)}_{n^2}(\mathbb{Q}) = \{(x, \pm\sqrt{x^5 + n^2}) :\ x \in \mathbb{Q}^*\}.$$

2. *The algebraic points of degree 3 on $\mathcal{C}_{n^2}$ over $\mathbb{Q}$ are given by*

$$\mathcal{C}^{(3)}_{n^2}(\mathbb{Q}) = \{(x, \pm n - \lambda x^2) :\ \lambda \in \mathbb{Q}^* \textit{ and } x \textit{ root of } x^3 - \lambda^2 x^2 \pm 2\lambda n = 0\}.$$

3. *The algebraic points of degree 4 on $\mathcal{C}_{n^2}$ over $\mathbb{Q}$ are given by*

$$\mathcal{C}^{(4)}_{n^2}(\mathbb{Q}) = \mathcal{A}^n_0 \cup \mathcal{A}^n_1 \cup \mathcal{A}^n_2$$

with

$$\mathcal{A}^n_0 = \{(x, \pm\sqrt{x^5 + n^2}) :\ [\mathbb{Q}(x) : \mathbb{Q}] = 2\};$$

$$\mathcal{A}^n_1 = \{(x, \pm n - \lambda x - \mu x^2) :\ \lambda \in \mathbb{Q}^*, \mu \in \mathbb{Q} \textit{ and } x \textit{ root of}$$

$$\mathcal{B}_1^n(x) = x^4 - \mu^2 x^3 - 2\lambda\mu x^2 + (-\lambda^2 \pm 2\mu n)x \pm 2\lambda n\};$$

$$\mathcal{A}_2^n = \{(x, \pm n - \lambda x^2 - \mu x^3) : \ \lambda, \mu \in \mathbb{Q}^* \textit{ and } x \textit{ root of}$$
$$\mathcal{B}_2^n(x) = \mu^2 x^4 + (2\lambda\mu - 1)x^3 + \lambda^2 x^2 \mp 2\mu n x \mp 2\lambda n\}.$$

4. *The algebraic points of degree at most d with $d \geq 5$ on $\mathcal{C}_{n^2}$ over $\mathbb{Q}$ are given by*

$$\mathcal{C}_{n^2}^d(\mathbb{Q}) = \mathcal{D}_0^n \cup \mathcal{D}_1^n \cup \mathcal{D}_2^n \cup \mathcal{D}_3^n$$

with

$$\mathcal{D}_0^n = \{(x, \pm\sqrt{x^5 + n^2}) : \ [\mathbb{Q}(x) : \mathbb{Q}] \leq \frac{d}{2} \textit{ if } d \textit{ is even}\};$$

$$\mathcal{D}_1^n = \Bigg\{ \left(x, -\frac{\sum_{0 \leq i \leq \frac{d}{2}} a_i x^i}{\sum_{0 \leq j \leq \frac{d-5}{2}} b_j x^j} \right) : \ a_{\frac{d}{2}} \neq 0 \textit{ and } \exists\, b_j \neq 0 \textit{ if } d \textit{ is even},$$
$$b_{\frac{d-5}{2}} \neq 0 \textit{ if } d \textit{ odd and } x \textit{ root of}$$
$$\mathcal{F}_1^n(x) = \big(\textstyle\sum_{0 \leq i \leq \frac{d}{2}} a_i x^i\big)^2 - \big(\textstyle\sum_{0 \leq j \leq \frac{d-5}{2}} b_j x^j\big)^2 (x^5 + n^2) \Bigg\};$$

$$\mathcal{D}_2^n = \Bigg\{ \left(x, -\frac{\sum_{0 \leq i \leq \frac{d+1}{2}} a_i x^i}{\sum_{0 \leq j \leq \frac{d-4}{2}} b_j x^j} \right) : \ a_0 = \pm n b_0, \ a_{\frac{d+1}{2}} \neq 0 \textit{ if } d \textit{ is odd},$$
$$b_{\frac{d-4}{2}} \neq 0 \textit{ if } d \textit{ is even and } x \textit{ root of}$$
$$\mathcal{F}_2^n(x) = \big(\textstyle\sum_{0 \leq i \leq \frac{d+1}{2}} a_i x^i\big)^2 - \big(\textstyle\sum_{0 \leq j \leq \frac{d-4}{2}} b_j x^j\big)^2 (x^5 + n^2) \Bigg\};$$

$$\mathcal{D}_3^n = \Bigg\{ \left(x, -\frac{\sum_{0 \leq i \leq \frac{d+2}{2}} a_i x^i}{\sum_{0 \leq j \leq \frac{d-3}{2}} b_j x^j} \right) : \ a_0 = \pm n b_0, \ a_1 = \pm n b_1, \ a_{\frac{d+2}{2}} \neq 0$$
$$\textit{if } d \textit{ is even}, \ b_{\frac{d-3}{2}} \neq 0 \textit{ if } d \textit{ is odd and } x \textit{ root of}$$
$$\mathcal{F}_3^n(x) = \big(\textstyle\sum_{0 \leq i \leq \frac{d+2}{2}} a_i x^i\big)^2 - \big(\textstyle\sum_{0 \leq j \leq \frac{d-3}{2}} b_j x^j\big)^2 (x^5 + n^2) \Bigg\}.$$

2. Fundamental lemmas

Let D be a divisor on $\mathcal{C}_{n^2}$. The vector space $\mathcal{L}(D)$ is defined to be the set of rational functions

$$\mathcal{L}(D) = \{f \in \overline{\mathbb{Q}}(\mathcal{C}_{n^2})^* : \ \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

The dimension of $\mathcal{L}(D)$ as a $\overline{\mathbb{Q}}-$vector space is denoted by $l(D)$. Let x and y denote the functions on $\mathcal{C}_{n^2}$ given by

$$x(X, Y, Z) = \frac{X}{Z} \quad \text{and} \quad y(X, Y, Z) = \frac{Y}{Z^3}.$$

The smooth projective form of the curve $\mathcal{C}_{n^2}$ is

$$\mathcal{C}_{n^2} : Y^2 = X^5 Z + n^2 Z^6.$$

The following lemma gives the structure of the Mordell-Weil group $J_{\mathcal{C}_{n^2}}(\mathbb{Q})$ and that the finiteness of the latter group is essential for this work.

Lemma 1
$J_{\mathcal{C}_{n^2}}(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$.

Proof. Using of MAGMA for 2-descent on jocabians of hyperelliptic curves we obtain the desired result (for more detaits, we refer to [12], [5], [1]).

Lemma 2
(i) $\operatorname{div}(y-n) = 5P_n - 5P_\infty$, $\operatorname{div}(y+n) = 5\overline{P_n} - 5P_\infty$;
(ii) $\operatorname{div}(x) = P_n + \overline{P_n} - 2P_\infty$, $\operatorname{div}(y) = A_0^n + \cdots + A_4^n - 5P_\infty$.

Proof. It suffices to apply the following relation

$$\operatorname{div}(x-\alpha) = (X - \alpha Z = 0).\mathcal{C}_{n^2} - (Z = 0).\mathcal{C}_{n^2}$$

with $\alpha \in \mathbb{Z}$, where $\Gamma.\mathcal{C}_{n^2}$ is the intersection cycle of a algebraic curve Γ defined over $\mathbb{Q}$ and the curve $\mathcal{C}_{n^2}$.

From Lemma 2, we see that $5j(P_n) = 5j(\overline{P_n}) = 0$, and $j(P_n) + j(\overline{P_n}) = 0$. Thus, $j(P_n)$ and $j(\overline{P_n})$ generate the same group $J_{\mathcal{C}_{n^2}}(\mathbb{Q})$ which is isomorphic to $\mathbb{Z}/5\mathbb{Z}$.

Lemma 3
We have

$$\mathcal{L}(P_\infty) =< 1 >, \quad \mathcal{L}(2P_\infty) = \mathcal{L}(3P_\infty) =< 1, x >, \quad \mathcal{L}(4P_\infty) =< 1, x, x^2 >,$$
$$\mathcal{L}(5P_\infty) =< 1, x, x^2, y >, \quad \mathcal{L}(6P_\infty) =< 1, x, x^2, y, x^3 > .$$

More generally, for $p \geq 5$, a $\overline{\mathbb{Q}}$-basis for $\mathcal{L}(pP_\infty)$ is given by

$$\mathcal{B}_p = \left\{x^i : \ i \in \mathbb{N} \text{ and } 0 \leq i \leq \frac{p}{2}\right\} \cup \left\{yx^j : \ j \in \mathbb{N} \text{ and } 0 \leq j \leq \frac{p-5}{2}\right\}.$$

Proof.
- It is clear that $l(P_\infty) = 1$. But $\mathcal{L}(P_\infty)$ certainly contains the constant functions, thus $\mathcal{L}(P_\infty) =< 1 >$.
- Since the genus of $\mathcal{C}_{n^2}$ is equal to 2, then $2P_\infty$ is a canonical divisor on $\mathcal{C}_{n^2}$, so $l(2P_\infty) = 2$, thus $\{1, x\}$ provides a basis for $\mathcal{L}(2P_\infty)$.
- For $p \geq 3$, we can see that the elements of $\mathcal{B}_p$ are linearly independent and are in $\mathcal{L}(pP_\infty)$. Thus, it suffices to show that the cardinality of $\mathcal{B}_p$ is equal to $l(pP_\infty)$. According to the Riemann-Roch theorem (see [6], p. 71), we have $l(pP_\infty) = p - 1$. Two cases arise:

  1st case: if p is even, then by setting $p = 2h$, we have

  $$i \leq \frac{p}{2} = h, \qquad j \leq \frac{p-5}{2} = \frac{2h-5}{2} \Leftrightarrow j \leq h - 3.$$

  Therefore, we get $\mathcal{B}_p = \{1, x, \ldots, x^h\} \cup \{y, yx, \ldots, yx^{h-3}\}$ and hence

  $$\#\mathcal{B}_p = (h+1) + (h-3+1) = 2h - 1 = p - 1.$$

2nd case: if p is odd, then by putting $p = 2h+1$, we obtain

$$i \leq \frac{p}{2} = \frac{2h+1}{2} \Leftrightarrow i \leq h, \qquad j \leq \frac{p-5}{2} = \frac{2h-4}{2} = h-2.$$

Thus, we have $\mathcal{B}_p = \{1, x, \ldots, x^h\} \cup \{y, yx, \ldots, yx^{h-2}\}$ and therefore

$$\#\mathcal{B}_p = (h+1) + (h-2+1) = 2h = p-1.$$

3. Proof of Theorem 2

Let R be an algebraic point on $\mathcal{C}_{n^2}$ of degree d over $\mathbb{Q}$; if $d = 1$ these points are given by Theorem 1, so we can assume that $d \geq 2$. Let $R_1, \ldots, R_d$ be the Galois conjugates of R. We have $[R_1 + \cdots + R_d - dP_\infty] \in J_{\mathcal{C}_{n^2}}(\mathbb{Q})$ and Lemma 1 gives

$$[R_1 + \cdots + R_d - dP_\infty] = mj(P_n) \qquad \text{with } 0 \leq m \leq 4. \tag{1}$$

3.1. The algebraic points of degree 2 on $\mathcal{C}_{n^2}$ over $\mathbb{Q}$

Case $m = 0$. The formula (1) becomes $[R_1 + R_2 - 2P_\infty] = 0$. The Abel-Jacobi theorem implies the existence of a function f such that

$$\operatorname{div}(f) = R_1 + R_2 - 2P_\infty.$$

Therefore $f \in \mathcal{L}(2P_\infty)$, hence $f = a_0 + a_1 x$ with $a_i \neq 0$ otherwise one of the R_i would be equal to P_n, $\overline{P_n}$ or P_∞, which is absurd. At points R_i, we have $a_0 + a_1 x = 0$, hence $x \in \mathbb{Q}^*$. The relation $y^2 = x^5 + n^2$ gives $y = \pm\sqrt{x^5 + n^2}$, thus we obtain a family of points of degree 2,

$$\{(x, \pm\sqrt{x^5 + n^2}) : \ x \in \mathbb{Q}^*\}.$$

For the cases $m = 1, 2, 3, 4$, we obtain an absurdity.
Thus, we obtain a family of points of degree 2,

$$\mathcal{C}^{(2)}_{n^2}(\mathbb{Q}) = \{(x, \pm\sqrt{x^5 + n^2}) : \ x \in \mathbb{Q}^*\}.$$

3.2. The algebraic points of degree 3 on $\mathcal{C}_{n^2}$ over $\mathbb{Q}$

For the cases $m = 0, 1, 4$, we obtain an absurdity.
Cases $m = 2$ and $m = 3$.

- For $m = 2$, (1) becomes $[R_1 + R_2 + R_3 + 2\overline{P_n} - 5P_\infty] = 0$. There exists a function f such that

$$\operatorname{div}(f) = R_1 + R_2 + R_3 + 2\overline{P_n} - 5P_\infty.$$

Therefore $f \in \mathcal{L}(5P_\infty)$, hence $f = a_0 + a_1 x + a_2 x^2 + b_0 y$ with $b_0 \neq 0$ otherwise one of the R_i would be equal to P_∞, which is absurd. The function f is of order 2 in $\overline{P_n}$, so $a_0 - nb_0 = 0$ and $a_1 = 0$. Thus $f = b_0(y+n) + a_2x^2$. At points R_i, we have $b_0(y+n) + a_2x^2 = 0$. By putting $\lambda = \frac{a_2}{b_0}$, we obtain

$$y = -n - \lambda x^2.$$

Replacing the expression of y in $y^2 - x^5 - n^2 = 0$, we have

$$-x^2(x^3 - \lambda^2 x^2 - 2\lambda n) = 0.$$

We must have $x^2 \neq 0$, $\lambda \neq 0$ and $x^3 - \lambda^2 x^2 - 2\lambda n$ an irreducible polynomial, so we get a family of points of degree 3,

$$\{(x, -n - \lambda x^2) :\ \lambda \in \mathbb{Q}^* \text{ and } x \text{ root of } x^3 - \lambda^2 x^2 - 2\lambda n = 0\}. \tag{2}$$

– For $m = 3$, by analogous reasoning to the case $m = 2$, we obtain a family of points of degree 3,

$$\{(x, n - \lambda x^2) :\ \lambda \in \mathbb{Q}^* \text{ and } x \text{ root of } x^3 - \lambda^2 x^2 + 2\lambda n = 0\}. \tag{3}$$

Finally combining (2) and (3), we obtain

$$\mathcal{C}_{n^2}^{(3)}(\mathbb{Q}) = \{(x, \pm n - \lambda x^2) :\ \lambda \in \mathbb{Q}^* \text{ and } x \text{ root of } x^3 - \lambda^2 x^2 \pm 2\lambda n = 0\}.$$

3.3. The algebraic points of degree 4 on $\mathcal{C}_{n^2}$ over $\mathbb{Q}$

Case $m = 0$. The formula (1) becomes $[R_1 + R_2 + R_3 + R_4 - 4P_\infty] = 0$. The Abel-Jacobi theorem implies the existence of a function f such that

$$\operatorname{div}(f) = R_1 + R_2 + R_3 + R_4 - 4P_\infty.$$

Therefore $f \in \mathcal{L}(4P_\infty)$, hence $f = a_0 + a_1x + a_2x^2$ with $a_2 \neq 0$. At points R_i, we have $a_0 + a_1x + a_2x^2 = 0$. The relation $y^2 = x^5 + n^2$ gives $y = \pm\sqrt{x^5 + n^2}$, thus we obtain a family of points of degree 4,

$$\mathcal{A}_0^n = \{(x, \pm\sqrt{x^5 + n^2}) :\ [\mathbb{Q}(x) : \mathbb{Q}] = 2\}.$$

CASES $m = 1$ AND $m = 4$.

- For $m = 1$, (1) becomes $[R_1 + R_2 + R_3 + R_4 + \overline{P_n} - 5P_\infty] = 0$. Then there exists a function f such that

$$\mathrm{div}(f) = R_1 + R_2 + R_3 + R_4 + \overline{P_n} - 5P_\infty.$$

Therefore $f \in \mathcal{L}(5P_\infty)$, hence $f = a_0 + a_1x + a_2x^2 + b_0y$ with $b_0 \neq 0$. The function f is of order 1 in $\overline{P_n}$, so $a_0 - nb_0 = 0$, thus $f = b_0(y+n) + a_1x + a_2x^2$. At points R_i, we have $b_0(y+n)+a_1x+a_2x^2 = 0$. By setting $\lambda = \frac{a_1}{b_0}$ and $\mu = \frac{a_2}{b_0}$, we obtain

$$y = -n - \lambda x - \mu x^2.$$

The substitution y in $y^2 - x^5 - n^2 = 0$ gives

$$x(x^4 - \mu^2x^3 - 2\lambda\mu x^2 + (-\lambda^2 - 2\mu n)x - 2\lambda n) = 0.$$

We must have $x \neq 0$, $\lambda \neq 0$ and $x^4 - \mu^2x^3 - 2\lambda\mu x^2 + (-\lambda^2 - 2\mu n)x - 2\lambda n$ an irreducible polynomial. We obtain a family of points of degree 4,

$$\mathcal{A}^n_{1,1} = \{(x, -n - \lambda x - \mu x^2) : \ \lambda \in \mathbb{Q}^*, \mu \in \mathbb{Q} \text{ and } x \text{ root of } \mathcal{B}^n_{1,1}(x)\}$$

with $\mathcal{B}^n_{1,1}(x) = x^4 - \mu^2x^3 - 2\lambda\mu x^2 + (-\lambda^2 - 2\mu n)x - 2\lambda n$.

- If $m = 4$, by similar reasoning to the case $m = 1$, we obtain a family of points of degree 4,

$$\mathcal{A}^n_{1,4} = \{(x, n - \lambda x - \mu x^2) : \ \lambda \in \mathbb{Q}^*, \mu \in \mathbb{Q} \text{ and } x \text{ root of } \mathcal{B}^n_{1,4}(x)\}$$

with $\mathcal{B}^n_{1,4}(x) = x^4 - \mu^2x^3 - 2\lambda\mu x^2 + (-\lambda^2 + 2\mu n)x + 2\lambda n$.

Finally, we put $\mathcal{A}^n_1 = \mathcal{A}^n_{1,1} \cup \mathcal{A}^n_{1,4}$ and $\mathcal{B}^n_1 = \mathcal{B}^n_{1,1} \cup \mathcal{B}^n_{1,4}$.

CASES $m = 2$ AND $m = 3$.

- For $m = 2$, (1) becomes $[R_1 + R_2 + R_3 + R_4 + 2\overline{P_n} - 6P_\infty] = 0$. According to the Abel-Jacobi theorem, there exists a function f such that

$$\mathrm{div}(f) = R_1 + R_2 + R_3 + R_4 + 2\overline{P_n} - 6P_\infty.$$

Therefore $f \in \mathcal{L}(6P_\infty)$, hence $f = a_0+a_1x+a_2x^2+b_0y+a_3x^3$ with $a_3 \neq 0$. The function f is of order 2 in $\overline{P_n}$, so $a_0 - nb_0 = 0$ and $a_1 = 0$, thus $f = b_0(y+n)+a_2x^2+a_3x^3$. At points R_i, we have $b_0(y+n)+a_2x^2+a_3x^3 = 0$. Noting that $b_0 \neq 0$ and by putting $\lambda = \frac{a_2}{b_0}$ and $\mu = \frac{a_3}{b_0}$, we have

$$y = -n - \lambda x^2 - \mu x^3.$$

Replacing the expression of y in $y^2 - x^5 - n^2 = 0$, we obtain

$$x^2(\mu^2x^4 + (2\lambda\mu - 1)x^3 + \lambda^2x^2 + 2\mu nx + 2\lambda n) = 0.$$

We must have $x^2 \neq 0$, $\lambda \neq 0$ and $\mu^2x^4 + (2\lambda\mu - 1)x^3 + \lambda^2x^2 + 2\mu nx + 2\lambda n$ an irreducible polynomial.

We obtain a family of points of degree 4,

$$\mathcal{A}^n_{2,2} = \{(x, -n - \lambda x^2 - \mu x^3) : \ \lambda, \mu \in \mathbb{Q}^* \text{ and } x \text{ root of } \mathcal{B}^n_{2,2}(x)\}$$

with $\mathcal{B}^n_{2,2}(x) = \mu^2 x^4 + (2\lambda\mu - 1)x^3 + \lambda^2 x^2 + 2\mu n x + 2\lambda n$.

– If $m = 3$, by analogous reasoning to the case $m = 2$, we obtain a family of points of degree 4,

$$\mathcal{A}^n_{2,3} = \{(x, n - \lambda x^2 - \mu x^3) : \ \lambda, \mu \in \mathbb{Q}^* \text{ and } x \text{ root of } \mathcal{B}^n_{2,3}(x)\}$$

with $\mathcal{B}^n_{2,3}(x) = \mu^2 x^4 + (2\lambda\mu - 1)x^3 + \lambda^2 x^2 - 2\mu n x - 2\lambda n$.

Finally, we put $\mathcal{A}^n_2 = \mathcal{A}^n_{2,2} \cup \mathcal{A}^n_{2,3}$ and $\mathcal{B}^n_2 = \mathcal{B}^n_{2,2} \cup \mathcal{B}^n_{2,3}$.

3.4. The algebraic points of degree at most d with $d \geq 5$ on $\mathcal{C}_{n^2}$ over $\mathbb{Q}$

Case $m = 0$. The formula (1) becomes $[R_1 + \cdots + R_d - dP_\infty] = 0$. The Abel-Jacobi theorem implies the existence of a rational function f defined over $\mathbb{Q}$ such that

$$\operatorname{div}(f) = R_1 + \cdots + R_d - dP_\infty.$$

Therefore $f \in \mathcal{L}(dP_\infty)$, hence $f = \sum_{0 \leq i \leq \frac{d}{2}} a_i x^i + y \sum_{0 \leq j \leq \frac{d-5}{2}} b_j x^j$ with:

(i) $a_{\frac{d}{2}} \neq 0$ if d is even:

- if for $0 \leq j \leq \frac{d-5}{2}, b_j = 0$, then at points R_i, we have $\sum\limits_{0 \leq i \leq \frac{d}{2}} a_i x^i = 0$, then the relation $y^2 = x^5 + n^2$ gives $y = \pm\sqrt{x^5 + n^2}$, thus we obtain a family of points of degree at most d

$$\mathcal{D}^n_0 = \big\{(x, \pm\sqrt{x^5 + n^2}) : \ [\mathbb{Q}(x) : \mathbb{Q}] \leq \frac{d}{2} \text{ if } d \text{ is even}\big\};$$

- otherwise there exists j with $0 \leq j \leq \frac{d-5}{2}$ such that $b_j \neq 0$, then $y = -\dfrac{\sum_{0 \leq i \leq \frac{d}{2}} a_i x^i}{\sum_{0 \leq j \leq \frac{d-5}{2}} b_j x^j}$, which after substitution for y in $y^2 - x^5 - n^2 = 0$ gives

$$\Big(\sum\nolimits_{0 \leq i \leq \frac{d}{2}} a_i x^i\Big)^2 - \Big(\sum\nolimits_{0 \leq j \leq \frac{d-5}{2}} b_j x^j\Big)^2 (x^5 + n^2) = 0,$$

and we obtain a family of points of degree at most d,

$$\begin{aligned}\mathcal{D}^n_{1,0} = \Bigg\{\Bigg(x, -\frac{\sum_{0 \leq i \leq \frac{d}{2}} a_i x^i}{\sum_{0 \leq j \leq \frac{d-5}{2}} b_j x^j}\Bigg) : \ & a_{\frac{d}{2}} \neq 0, \exists\, b_j \neq 0 \text{ if } d \text{ is even} \\ & \text{and } x \text{ root of} \\ & \mathcal{F}^n_{1,0}(x) = \big(\sum\nolimits_{0 \leq i \leq \frac{d}{2}} a_i x^i\big)^2 - \big(\sum\nolimits_{0 \leq j \leq \frac{d-5}{2}} b_j x^j\big)^2 (x^5 + n^2)\Bigg\}.\end{aligned}$$

(ii) $b_{\frac{d-5}{2}} \neq 0$ if d is odd, at points R_i, we have

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

hence $y = -\dfrac{\sum_{0\leq i\leq \frac{d}{2}} a_i x^i}{\sum_{0\leq j\leq \frac{d-5}{2}} b_j x^j}$. Replacing the expression of y in $y^2 - x^5 - n^2 = 0$, we obtain

$$\big(\sum_{0\leq i\leq \frac{d}{2}} a_i x^i\big)^2 - \big(\sum_{0\leq j\leq \frac{d-5}{2}} b_j x^j\big)^2 (x^5 + n^2) = 0.$$

Thus, we obtain a family of points of degree at most d,

$$\mathcal{D}^n_{1,1} = \Bigg\{ \Bigg(x, -\frac{\sum_{0\leq i\leq \frac{d}{2}} a_i x^i}{\sum_{0\leq j\leq \frac{d-5}{2}} b_j x^j} \Bigg) : \ b_{\frac{d-5}{2}} \neq 0 \text{ if } d \text{ is odd}$$
$$\text{and } x \text{ root of}$$
$$\mathcal{F}^n_{1,1}(x) = \big(\sum_{0\leq i\leq \frac{d}{2}} a_i x^i\big)^2 - \big(\sum_{0\leq j\leq \frac{d-5}{2}} b_j x^j\big)^2 (x^5 + n^2) \Bigg\}$$

Finally, we put $\mathcal{D}^n_1 = \mathcal{D}^n_{1,0} \cup \mathcal{D}^n_{1,1}$ and $\mathcal{F}^n_1 = \mathcal{F}^n_{1,0} \cup \mathcal{F}^n_{1,1}$.

Cases $m = 1$ and $m = 4$.

- for $m = 1$, the formula (1) becomes $[R_1 + \cdots + R_d + \overline{P_n} - (d+1)P_\infty] = 0$. There exists a function f such that

$$\operatorname{div}(f) = R_1 + \cdots + R_d + \overline{P_n} - (d+1)P_\infty.$$

Therefore $f \in \mathcal{L}((d+1)P_\infty)$, hence $f = \sum_{0\leq i\leq \frac{d+1}{2}} a_i x^i + y \sum_{0\leq j\leq \frac{d-4}{2}} b_j x^j$ with $a_{\frac{d+1}{2}} \neq 0$ if d is odd or $b_{\frac{d-4}{2}} \neq 0$ if d is even. The function f is of order 1 in $\overline{P_n}$, hence $a_0 = nb_0$. At points R_i, we have $\sum_{0\leq i\leq \frac{d+1}{2}} a_i x^i + y \sum_{0\leq j\leq \frac{d-4}{2}} b_j x^j = 0$, which implies that $y = -\dfrac{\sum_{0\leq i\leq \frac{d+1}{2}} a_i x^i}{\sum_{0\leq j\leq \frac{d-4}{2}} b_j x^j}$. The substitution y in $y^2 - x^5 - n^2 = 0$ gives

$$\big(\sum_{0\leq i\leq \frac{d+1}{2}} a_i x^i\big)^2 - \big(\sum_{0\leq j\leq \frac{d-4}{2}} b_j x^j\big)^2 (x^5 + n^2) = 0.$$

Thus, we obtain a family of points of degree at most d,

$$\mathcal{D}^n_{2,1} = \Bigg\{ \Bigg(x, -\frac{\sum_{0\leq i\leq \frac{d+1}{2}} a_i x^i}{\sum_{0\leq j\leq \frac{d-4}{2}} b_j x^j} \Bigg) : \ a_0 = nb_0, \text{ and } x \text{ root of } \mathcal{F}^n_{2,1}(x) \Bigg\}$$

with $\mathcal{F}^n_{2,1}(x) = \big(\sum_{0\leq i\leq \frac{d+1}{2}} a_i x^i\big)^2 - \big(\sum_{0\leq j\leq \frac{d-4}{2}} b_j x^j\big)^2 (x^5 + n^2)$.

- for $m = 4$, by similar reasoning to the case $m = 1$, we obtain a family of points of degree at most d,

$$\mathcal{D}^n_{2,4} = \Bigg\{ \Bigg(x, -\frac{\sum_{0\leq i\leq \frac{d+1}{2}} a_i x^i}{\sum_{0\leq j\leq \frac{d-4}{2}} b_j x^j} \Bigg) : \ a_0 = -nb_0, \text{ and } x \text{ root of } \mathcal{F}^n_{2,4}(x) \Bigg\}$$

with $\mathcal{F}^n_{2,4}(x) = \big(\sum_{0\leq i\leq \frac{d+1}{2}} a_i x^i\big)^2 - \big(\sum_{0\leq j\leq \frac{d-4}{2}} b_j x^j\big)^2 (x^5 + n^2)$.

Finally, we put $\mathcal{D}_2^n = \mathcal{D}_{2,1}^n \cup \mathcal{D}_{2,4}^n$ and $\mathcal{F}_2^n = \mathcal{F}_{2,1}^n \cup \mathcal{F}_{2,4}^n$.

Cases $m = 2$ and $m = 3$.

- for $m = 2$, the formula (1) becomes $[R_1 + \cdots + R_d + 2\overline{P_n} - (d+2)P_\infty] = 0$. According to the Abel-Jacobi theorem, there exists a function f such that

$$\mathrm{div}(f) = R_1 + \cdots + R_d + 2\overline{P_n} - (d+2)P_\infty.$$

Therefore $f \in \mathcal{L}((d+2)P_\infty)$, hence $f = \sum_{0\le i\le \frac{d+2}{2}} a_i x^i + y \sum_{0\le j\le \frac{d-3}{2}} b_j x^j$ with $a_{\frac{d+2}{2}} \neq 0$ if d is even or $b_{\frac{d-3}{2}} \neq 0$ if d is odd. The function f is of order 2 in $\overline{P_n}$, so $a_0 = nb_0$ and $a_1 = nb_1$. At points R_i, we have $\sum_{0\le i\le \frac{d+2}{2}} a_i x^i + y \sum_{0\le j\le \frac{d-3}{2}} b_j x^j = 0$, which leads to $y = -\dfrac{\sum_{0\le i\le \frac{d+2}{2}} a_i x^i}{\sum_{0\le j\le \frac{d-3}{2}} b_j x^j}$. The substitution of y in $y^2 - x^5 - n^2 = 0$ gives

$$\Big(\sum_{0\le i\le \frac{d+2}{2}} a_i x^i\Big)^2 - \Big(\sum_{0\le j\le \frac{d-3}{2}} b_j x^j\Big)^2 (x^5 + n^2) = 0.$$

Thus, we find a family of points of degree at most d,

$$\mathcal{D}_{3,2}^n = \left\{ \left(x, -\frac{\sum_{0\le i\le \frac{d+2}{2}} a_i x^i}{\sum_{0\le j\le \frac{d-3}{2}} b_j x^j}\right) : \ a_0 = nb_0, a_1 = nb_1 \right.$$
$$\left. \text{and } x \text{ root of } \mathcal{F}_{3,2}^n(x) \right\}$$

with $\mathcal{F}_{3,2}^n(x) = \Big(\sum_{0\le i\le \frac{d+2}{2}} a_i x^i\Big)^2 - \Big(\sum_{0\le j\le \frac{d-3}{2}} b_j x^j\Big)^2 (x^5 + n^2)$.

- for $m = 3$, by analogous reasoning to the case $m = 2$, we find a family of points of degree at most d,

$$\mathcal{D}_{3,3}^n = \left\{ \left(x, -\frac{\sum_{0\le i\le \frac{d+2}{2}} a_i x^i}{\sum_{0\le j\le \frac{d-3}{2}} b_j x^j}\right) : \ a_0 = -nb_0, a_1 = -nb_1 \right.$$
$$\left. \text{and } x \text{ root of } \mathcal{F}_{3,3}^n(x) \right\}$$

with $\mathcal{F}_{3,3}^n(x) = \Big(\sum_{0\le i\le \frac{d+2}{2}} a_i x^i\Big)^2 - \Big(\sum_{0\le j\le \frac{d-3}{2}} b_j x^j\Big)^2 (x^5 + n^2)$.

Finally, we put $\mathcal{D}_3^n = \mathcal{D}_{3,2}^n \cup \mathcal{D}_{3,3}^n$, $\mathcal{F}_3^n = \mathcal{F}_{3,2}^n \cup \mathcal{F}_{3,3}^n$ and $\mathcal{C}_{n^2}^d(\mathbb{Q}) = \mathcal{D}_0^n \cup \mathcal{D}_1^n \cup \mathcal{D}_2^n \cup \mathcal{D}_3^n$.

Remark 1

The result obtained remains true for any integer n for which $J_{\mathcal{C}_{n^2}}(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$ and that the set of $\mathbb{Q}$-rational points on $\mathcal{C}_{n^2}$ is given by $\{P_n, \overline{P_n}, P_\infty\}$.

References

[1] Carmen Anthony Bruni. *Twisted Extensions of Fermat's Last Theorem.* PhD diss. The University of British Columbia (Canada), 2015. Cited on 22 and 24.

[2] Faltings, Gerd. "Endlichkeitsätze für abelsch Varietäten über Zahlkörpen." *Invent. Math.* , 73 no. 3 (1983): 349-366. Cited on 22.

[3] Moussa, Fall. "Parametrization of Algebraic Points of Low Degrees on the Schaeffer Curve." *J. Math. Sci. Model.*, 4 no. 2 (2021): 51-55. Cited on 21.

[4] Griffiths, Phillip Augustus. *Introduction to algebraic curves.* Vol. 76 of *Translations of mathematical monographs.* Providence, RI: American Mathematical Society, 1989. Cited on 22.

[5] Mulholland, J. T. *Elliptic curves with rational* 2*-torsion and related ternary Diophantine equations.* PhD diss. The University of British Columbia (Canada), 2006. Cited on 22 and 24.

[6] Hindry, Marc, and Joseph Hillel Silverman. *Diophantine geometry, an introduction.* Vol. 201 of *Graduade Texts in Mathematics.* New York: Springer-Verlag, 2000. Cited on 24.

[7] Sall, Oumar, and Moussa Fall, and Chérif Mamina Coly. "Points algbriques 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. Cited on 21.

[8] Schaefer, Edward Frank. "Computing a Selmer group of a Jacobian using functions on the curve." *Math. Ann.* 310, no. 3 (1998): 447-471. Cited on 21.

[9] Stoll, Michael. "On the arithmetic of the curves $y^2 = x^l + A$; and their Jacobians." *J. Reine Angew. Math.* 501 (1998): 171-189. Cited on 21.

[10] Stoll, Michael. "On the arithmetic of the curves $y^2 = x^l + A$. II." *J. Number Theory* 93, no. 2 (2002): 183-206. Cited on 21.

[11] Stoll, Michael, and Tonghai Yang. "On the L-function of the curves $y^2 = x^5 + A$." *J. London Math. Soc. (2)* 68, no. 2 (2003): 273-287. Cited on 21.

[12] Stoll, Michael. "Implementing 2-descent for Jacobians of hyperelliptic curves." *Acta Arith.* 98, no. 3 (2001): 245-277. Cited on 24.

Moustapha Camara
Moussa Fall
Oumar Sall
Mathematics and Applications Laboratory
U.F.R of Sciences and Technologie
University Assane Seck of Ziguinchor
Senegal
E-mail: m.camara5367@zig.univ.sn
m.fall@univ-zig.sn
o.sall@univ-zig.sn

Received: February 14, 2022; final version: March 17, 2023; available online: April 29, 2023.