

**GOCE DELCEV UNIVERSITY - STIP**  
**FACULTY OF COMPUTER SCIENCE**

The journal is indexed in

**EBSCO**

ISSN 2545-4803 on line

DOI: 10.46763/BJAMI

**BALKAN JOURNAL**  
**OF APPLIED MATHEMATICS**  
**AND INFORMATICS**  
**(BJAMI)**



YEAR 2024

VOLUME 7, Number 2

**AIMS AND SCOPE:**

BJAMI publishes original research articles in the areas of applied mathematics and informatics.

**Topics:**

1. Computer science;
2. Computer and software engineering;
3. Information technology;
4. Computer security;
5. Electrical engineering;
6. Telecommunication;
7. Mathematics and its applications;
8. Articles of interdisciplinary of computer and information sciences with education, economics, environmental, health, and engineering.

**Managing editor**

**Mirjana Kocaleva Vitanova** Ph.D.

**Zoran Zlatev** Ph.D.

**Editor in chief**

**Biljana Zlatanovska** Ph.D.

**Lectoure**

**Snezana Kirova**

**Technical editor**

**Biljana Zlatanovska** Ph.D.

**Mirjana Kocaleva Vitanova** Ph.D.

**BALKAN JOURNAL  
OF APPLIED MATHEMATICS AND INFORMATICS  
(BJAMI), Vol 7**

**ISSN 2545-4803 on line  
Vol. 7, No. 2, Year 2024**

## EDITORIAL BOARD

- Adelina Plamenova Aleksieva-Petrova**, Technical University – Sofia,  
Faculty of Computer Systems and Control, Sofia, Bulgaria
- Lyudmila Stoyanova**, Technical University - Sofia , Faculty of computer systems and control,  
Department – Programming and computer technologies, Bulgaria
- Zlatko Georgiev Varbanov**, Department of Mathematics and Informatics,  
Veliko Tarnovo University, Bulgaria
- Snezana Scepanovic**, Faculty for Information Technology,  
University “Mediterranean”, Podgorica, Montenegro
- Daniela Veleva Minkovska**, Faculty of Computer Systems and Technologies,  
Technical University, Sofia, Bulgaria
- Stefka Hristova Bouyuklieva**, Department of Algebra and Geometry,  
Faculty of Mathematics and Informatics, Veliko Tarnovo University, Bulgaria
- Vesselin Velichkov**, University of Luxembourg, Faculty of Sciences,  
Technology and Communication (FSTC), Luxembourg
- Isabel Maria Baltazar Simões de Carvalho**, Instituto Superior Técnico,  
Technical University of Lisbon, Portugal
- Predrag S. Stanimirović**, University of Niš, Faculty of Sciences and Mathematics,  
Department of Mathematics and Informatics, Niš, Serbia
- Shcherbacov Victor**, Institute of Mathematics and Computer Science,  
Academy of Sciences of Moldova, Moldova
- Pedro Ricardo Morais Inácio**, Department of Computer Science,  
Universidade da Beira Interior, Portugal
- Georgi Tuparov**, Technical University of Sofia Bulgaria
- Martin Lukarevski**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Ivanka Georgieva**, South-West University, Blagoevgrad, Bulgaria
- Georgi Stojanov**, Computer Science, Mathematics, and Environmental Science Department  
The American University of Paris, France
- Iliya Guerguiev Bouyukliev**, Institute of Mathematics and Informatics,  
Bulgarian Academy of Sciences, Bulgaria
- Riste Škrekovski**, FAMNIT, University of Primorska, Koper, Slovenia
- Stela Zhelezova**, Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Bulgaria
- Katerina Taskova**, Computational Biology and Data Mining Group,  
Faculty of Biology, Johannes Gutenberg-Universität Mainz (JGU), Mainz, Germany.
- Dragana Glušac**, Tehnical Faculty “Mihajlo Pupin”, Zrenjanin, Serbia
- Cveta Martinovska-Bande**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Blagoj Delipetrov**, European Commission Joint Research Centre, Italy
- Zoran Zdravev**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Aleksandra Mileva**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Igor Stojanovik**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Saso Koceski**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Natasa Koceska**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Aleksandar Krstev**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Biljana Zlatanovska**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Natasa Stojkovik**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Done Stojanov**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Limonka Koceva Lazarova**, Faculty of Computer Science, UGD, Republic of North Macedonia
- Tatjana Atanasova Pacemska**, Faculty of Computer Science, UGD, Republic of North Macedonia



---

## CONTENT

<b>Moussa Fall, Pape Modou Sarr</b> DETERMINATION OF ALGEBRAIC POINTS OF LOW DEGREE ON A FAMILI CURVES .....	7
<b>Mohamadou Mor Diogou Diallo</b> EXIBITION OF PARAMETRIC FAMILY OF ALGEBRAIC POINTS OF GIVEN DEGREE ON AFINE EQUATION CURVE: $-y^2 = x^6 - 20x^3 - 8$ .....	15
<b>Milan Mladenovski, Saso Gelev</b> DIGITAL FORENSICS ON ANDROID DEVICE .....	25
<b>Darko Cebov, Aleksandra Mileva</b> MULTI-ACTION GRID AUTHENTICATION: A SECURE AND USABLE AUTHENTICATION SYSTEM FOR SMART TOUCH DEVICES .....	39
<b>Aleksandra Nikolova, Aleksandar Velinov, Zoran Zdravev</b> USE CASES FOR BPMN AND UML TOOLS .....	51
<b>Aleksandra Nikolova, Aleksandar Velinov, Zoran Zdravev</b> COMPARATIVE ANALYSIS OF BPMN TOOLS .....	61
<b>Sara Aneva, Dragan Minovski</b> POSSIBILITIES FOR INSTALLATION OF PHOTOVOLTAIC SYSTEMS IN CATERING FACILITIES IN MACEDONIA .....	71
<b>Dejan Krstev, Aleksandar Krstev</b> APPLICATION OF CENTER OF GRAVITY METHOD FOR LOCATIONS OF FACILITIES ...	83
<b>Biljana Zlatanovska, Boro M. Piperevski</b> ON THE INTERGRABILITY OF A SUBCLASS OF 2D MATRIX DIFFERENTIAL EQUATIONS .....	91



## DETERMINATION OF ALGEBRAIC POINTS OF LOW DEGREE ON A FAMILY CURVES

MOUSSA FALL AND PAPE MODOU SARR

**Abstract.** The purpose of this paper is to determine explicitly algebraic points of low degree over  $\mathbb{Q}$  on the family curves of affine equation  $C_n : y^{3n} = x^{4n} - 1$  where  $n$  is a positive integer. Our goal is to extends the result of O. Debarre and M. Klassen who determined the algebraic points of low degree in the curve  $C_1$ .

### 1. Introduction

Let  $\mathcal{C}$  be an algebraic curve defined over a number field  $K$ , we denote by  $\mathcal{C}(K)$  the set of rational points on  $K$  and by  $\mathcal{C}^{(d)}(\mathbb{Q})$  the set of algebraic points of degree at most  $d$  over the field of rational numbers  $\mathbb{Q}$ .

If  $\mathcal{C}$  is a curve of genus  $g \geq 2$ , it has been known since Faltings that the set of rational points  $\mathcal{C}(K)$  is finite. Currently, there is no general method for computing the set  $\mathcal{C}(K)$ ; but there are several methods for finding  $\mathcal{C}(K)$  in special cases. These methods include the local method, the Chabauty elliptic method [3], the descent method [9], the Mordell-Weil Sieves method [1], the Sall-Fall method [2] and [5]. These methods can be used only when the rank of the Mordell-Weil group  $J(\mathbb{Q})$  is finite.

More generally, there is no algorithm to determine the set  $\mathcal{C}^{(d)}(\mathbb{Q})$ . The situation is more favorable when the Mordell-Weil group of the Jacobian  $J(\mathbb{Q})$  is finite; in this case  $\mathcal{C}^{(d)}(\mathbb{Q})$  can be effectively determined (see [5], [2]). If we don't know the structure of the Mordell-Weil group, then we need to find a way around it.

In this paper, we propose to work around the finiteness of the Mordell-Weil group by using the Chevalley-Weil theorem and the work of Debarre and Klassen [4] to determine explicitly the set  $\mathcal{C}_n^{(2)}(\mathbb{Q})$  on the family curves of affine equation  $C_n : y^{3n} = x^{4n} - 1$ .

The main result of this paper is the following theorem :

---

*Date:* December 4, 2024.

**Keywords.** algebraic point of low degree, Chevalley-Weil theorem, cyclotomic polynomial, morphism.

**Theorem 1.1.** *Let  $n \geq 2$  be an integer and  $\alpha$  a cube root of unity and  $\beta$  a fourth root of unity. The set  $\mathcal{C}_n^{(2)}(\mathbb{Q})$  of algebraic points of degree at most 2 on the curve  $\mathcal{C}_n : y^{3n} = x^{4n} - 1$  is given by :*

- If  $n \equiv +0$  [12], then  $\mathcal{C}_n^{(2)}(\mathbb{Q}) = \{\infty, (\pm\alpha, 0), (\beta, 0)\}$*
- If  $n \equiv \pm 1$  [12], then  $\mathcal{C}_n^{(2)}(\mathbb{Q}) = \{\infty, (1, 0), (0, -1)\}$*
- If  $n \equiv \pm 2$  [12], then  $\mathcal{C}_n^{(2)}(\mathbb{Q}) = \{\infty, (\beta, 0), (0, \pm i)\}$*
- If  $n \equiv \pm 3$  [12], then  $\mathcal{C}_n^{(2)}(\mathbb{Q}) = \{\infty, (\pm\alpha, 0), (0, -\alpha)\}$*
- If  $n \equiv \pm 4$  [12], then  $\mathcal{C}_n^{(2)}(\mathbb{Q}) = \{\infty, (\beta, 0)\}$*
- If  $n \equiv \pm 5$  [12], then  $\mathcal{C}_n^{(2)}(\mathbb{Q}) = \{\infty, (\pm 1, 0), (0, -1)\}$*
- If  $n \equiv +6$  [12], then  $\mathcal{C}_n^{(2)}(\mathbb{Q}) = \{\infty, (\pm\alpha, 0), (\beta, 0), (0, \pm i)\}$ .*

## 2. Preliminary results

### 2.1. Algebraic extension.

A complex number  $\lambda \in \mathbb{C}$  is called algebraic if there is a non-zero polynomial  $f \in \mathbb{Q}[X]$  with  $f(\lambda) = 0$ . We define the algebraic closure of  $\mathbb{Q}$  by

$$\overline{\mathbb{Q}} = \{\lambda \in \mathbb{C} \mid \lambda \text{ algebraic}\}.$$

**Definition 2.1.** *An algebraic extension is a field extension  $L/K$  such that every element of the larger field  $L$  is algebraic over the smaller field  $K$  ; that is every element of  $L$  is a root of a non-zero polynomial with coefficients in  $K$ .*

Suppose that  $L/K$  is a field extension. Then  $L$  may be considered as a vector space over  $K$  (the field of scalars). The dimension of this vector space is called the degree of the field extension, and it is denoted by  $[L : K]$ .

The algebraic extensions of the field  $\mathbb{Q}$  of the rational numbers are called algebraic number fields.

Let  $\theta \in L$ . If  $\theta$  is algebraic over  $K$ , then the smallest subfield of  $L$  that contains  $K$  and  $\theta$  is commonly denoted  $K(\theta)$ . In this case  $K(\theta)$  is an algebraic extension of  $K$  which has finite degree over  $K$ .

We have the classical lemma:

**Lemma 2.1.** *Let  $K(\mu)$  and  $K(\nu)$  be two algebraic extensions of the field  $K$ , such that  $[K(\mu) : K] = m > 0$  and  $[K(\nu) : K] = n > 0$ . Then the extension  $K(\mu, \nu)$  is of finite degree on  $K$ . In particular, this degree is a multiple of  $m$  and  $n$  such that  $1 \leq [K(\mu, \nu) : K] \leq mn$ . Moreover, if  $m$  and  $n$  are prime to each other, then  $[K(\mu, \nu) : K] = mn$ .*

*Proof.* See [7].

□

We give the definition of the Euler function  $\varphi$ .



**Definition 2.2.** (*Euler  $\varphi$ -function*). Let  $n \in \mathbb{N}^*$  where  $\mathbb{N}^*$  is the set of non-zero positive integers. Then

- $\varphi(1) = 1$
- For  $n = n_1^{m_1} n_2^{m_2} \dots n_r^{m_r}$  where  $n_i$ ,  $1 \leq i \leq r$ , are distinct primes and  $m_i \in \mathbb{N}^*$ ,

$$\varphi(n) = n \left(1 - \frac{1}{n_1}\right) \dots \left(1 - \frac{1}{n_r}\right).$$

In particular, for a prime number  $n$ , we have  $\varphi(n) = n - 1$ .

We have the following lemma:

**Lemma 2.2.** Let  $n, k \in \mathbb{N}^*$ ,  $n \geq 2$ ,  $1 \leq k \leq n - 1$  and  $\zeta_n = e^{2i\pi \frac{1}{n}}$  be an  $n$ th root of unity. Then

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) \quad \text{and} \quad \left[\mathbb{Q}\left(\zeta_n^k\right) : \mathbb{Q}\right] = \varphi\left(\frac{n}{\gcd(n,k)}\right).$$

*Proof.* The first assertion is clear and to prove the second assertion, we combined the first with

$$\left[\mathbb{Q}\left(\zeta_n^k\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\zeta_n^{\gcd(n,k)}\right) : \mathbb{Q}\right].$$

□

**Definition 2.3.** Let  $\mathcal{C}$  be a algebraic plane curve defined over  $\mathbb{Q}$ . The degree of an algebraic point  $P \in \mathcal{C}$  is the degree of its field of definition over  $\mathbb{Q}$ .

In other words, if we denote by  $\deg(P)$  the degree of  $P$  over  $\mathbb{Q}$ , then

$$\deg(P) = [\mathbb{Q}(P) : \mathbb{Q}].$$

- If  $\deg(P) = 1$ , then  $P$  is a rational point.
- If  $\deg(P) = 2$ , then  $P$  is a quadratic point.
- If  $\deg(P) = 3$ , then  $P$  is a cubic point.

## 2.2. Cyclotomic polynomial.

**Definition 2.4.** Let  $n$  be any positive integer. The  $n^{\text{th}}$  cyclotomic polynomial is the irreducible polynomial with integer coefficients that is a divisor of the polynomial  $x^n - 1$  and is not a divisor of the polynomial  $x^p - 1$  for any  $p < n$ . Its roots are all  $n$ th primitive roots of unity  $e^{2i\pi \frac{p}{n}}$ , where  $p$  runs over the positive integers not greater than  $n$  and coprime to  $n$  (and  $i^2 = -1$ ). This means, the  $n$ th cyclotomic polynomial is equal to the polynomial

$$\Phi_n(x) = \prod_{\substack{1 \leq p \leq n \\ \gcd(n,p)=1}} \left(x - e^{2i\pi \frac{p}{n}}\right).$$

A fundamental relation linking cyclotomic polynomials and primitive roots of unity is

$$\prod_{d|n} \Phi_d(x) = x^n - 1.$$

shows that  $x$  is a root of  $x^n - 1$  if and only if it is a  $d^{\text{th}}$  primitive root of unity for some  $d$  that divides  $n$ .

**Example 2.1.** For  $n$  up to 6, the cyclotomic polynomials are the following:

- $\Phi_1(x) = x - 1$
- $\Phi_2(x) = x + 1$
- $\Phi_3(x) = x^2 + x + 1$
- $\Phi_4(x) = x^2 + 1$
- $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$
- $\Phi_6(x) = x^2 - x + 1$

$\Phi_n$  is monic polynomial of degree  $\varphi(n)$  with integer coefficients that is irreducible over the field  $\mathbb{Q}$ .

### 2.3. Chevalley-Weil theorem.

The Chevalley-Weil theorem that we use here is the following

**Theorem 2.1.** Let  $\phi : X \rightarrow Y$  be an unramified covering of normal projective varieties defined over a numbers field  $K$ . Then there exists a finite extension  $L/K$  of  $K$  such that

$$\phi^{-1}(\phi(Y(K))) \subset X(L).$$

*Proof.* See [7]. □

If  $X$  is a curve of genus  $g \geq 2$ , then theorem 2.1 ensures the finiteness of  $\phi^{-1}(\phi(Y(K)))$  because according to Faltings [6], the set  $X(L)$  is finite. We can then determine  $X(K)$  by using the following trivial lemma:

**Lemma 2.3.** Let  $\phi : X \rightarrow Y$  be a morphism of projective curves defined over a number field  $K$ , then  $\phi(X(K)) \subset Y(K)$ .

*Proof.* See [8]. □

If we know or determine the set  $Y(K)$  then, we can easily determine  $X(K)$  by the inclusion  $X(K) \subset \phi^{-1}(\phi(Y(K)))$ .

**Theorem 2.2.** Let  $\alpha$  be a cube root of unity and  $\beta$  a fourth root of unity. The set of algebraic points of degree at most 2 on the curve  $\mathcal{C}_1 : y^3 = x^4 - 1$  is given by :

$$\mathcal{C}_1^{(2)}(\mathbb{Q}) = \left\{ \infty, (0, -\alpha), (\beta, 0), (\beta\sqrt{3}, 2\alpha) \right\}.$$

*Proof.* See [4]. □

### 3. Proof of the Theorem [1.1](#)

Let us consider the morphism :

$$\begin{aligned} f: \mathcal{C}_n &\longrightarrow \mathcal{C}_1 \\ (x, y) &\longmapsto (x^n, y^n) \end{aligned}$$

where  $n$  is a positive integer and  $n \geq 1$ .

We have the following inclusion:

$$\mathcal{C}_n^{(d)}(\mathbb{Q}) \subset f^{-1}(\mathcal{C}_1^{(d)}(\mathbb{Q})).$$

In Theorem [2.2](#), the set of algebraic points of degree at most 2 of  $\mathcal{C}_1$  is given by :

$$\mathcal{C}_1^{(2)}(\mathbb{Q}) = \left\{ \infty, (0, -\alpha), (\beta, 0), (\beta\sqrt{3}, 2\alpha) \right\}.$$

According to the Theorem [2.1](#), for any quadratic number field  $K$  over  $\mathbb{Q}$ , there exists an algebraic extension  $L/K$  such that

$$\mathcal{C}_n(K) \subset f^{-1}(\mathcal{C}_1(K)) \subset \mathcal{C}_n(L).$$

We obtain the inclusion

$$\mathcal{C}_n^2(\mathbb{Q}) \subset f^{-1}(\mathcal{C}_1^2(\mathbb{Q})).$$

The set  $f^{-1}(\mathcal{C}_1^2(\mathbb{Q}))$  is given by:

$$f^{-1}(\mathcal{C}_1^2(\mathbb{Q})) = f^{-1}(\{\infty\}) \cup f^{-1}(\{(\beta, 0)\}) \cup f^{-1}(\{(0, -\alpha)\}) \cup f^{-1}(\{(\beta\sqrt{3}, 2\alpha)\}).$$

Let the point  $(a, b) \in \mathcal{C}_1^2(\mathbb{Q})$  and the point  $(x, y) \in \mathcal{C}_n^2(\mathbb{Q})$  :

$$(x, y) \in f^{-1}(\{(a, b)\}) \iff f(x, y) = (a, b) \iff (x^n, y^n) = (a, b).$$

The equation  $(x^n, y^n) = (a, b)$  have exactly  $n$  solutions given by :

$$(x_k, y_k) = \left( \sqrt[n]{ae^{\frac{2ik\pi}{n}}}, \sqrt[n]{be^{\frac{2ik\pi}{n}}} \right) \quad \text{where } 0 \leq k \leq n-1.$$

There are three possible cases for computing  $f^{-1}(\mathcal{C}_1^2(\mathbb{Q}))$  :

**Case 1** : If  $(a, b) = \infty$ , We have  $f^{-1}(\infty) = \infty$ , so  $\infty \in \mathcal{C}_n^2$  for all integer  $n \geq 1$ .

**Case 2 :** If  $(a, b) \in \mathcal{C}_1^2(\mathbb{Q})$  and  $a \neq \pm 1$  or  $b \neq \pm 1$ , then we have :

$$[\mathbb{Q}(x_k, y_k) : \mathbb{Q}] > [\mathbb{Q}(\sqrt[n]{a}, \sqrt[n]{b}) : \mathbb{Q}] > 2.$$

The degree of  $(x_k, y_k)$  is strictly greater than 2, therefore:

$$(x_k, y_k) \notin \mathcal{C}_n^2(\mathbb{Q}).$$

**Case 3 :** If  $(a, b) \in \{(0, -1), (1, 0), (-1, 0)\} \subset \mathcal{C}_1^2(\mathbb{Q})$ . Then the solution  $(x_k, y_k)$  verifies:

$$(x_k, y_k) \in \left\{ \left( 0, e^{\frac{i(2k+1)\pi}{n}} \right), \left( e^{\frac{i(2k+1)\pi}{n}}, 0 \right), \left( e^{\frac{i2k\pi}{n}}, 0 \right) \mid 0 \leq k \leq n-1 \right\}.$$

We have the following equalities for the degrees of the points:

$$\left[ \mathbb{Q} \left( 0, e^{\frac{i(2k+1)\pi}{n}} \right) : \mathbb{Q} \right] = \left[ \mathbb{Q} \left( e^{\frac{i(2k+1)\pi}{n}}, 0 \right) : \mathbb{Q} \right] = \varphi \left( \frac{n}{\gcd(n, k+1)} \right).$$

The complex number  $e^{\frac{i(2k+1)\pi}{n}}$  is solution of the equation  $u^n + 1 = 0$ .

We have also the following equalities for the degrees of the points:

$$\left[ \mathbb{Q} \left( e^{\frac{i(2k)\pi}{n}}, 0 \right) : \mathbb{Q} \right] = \left[ \mathbb{Q} \left( e^{\frac{i(2k)\pi}{n}} \right) : \mathbb{Q} \right] = \varphi \left( \frac{n}{\gcd(n, k)} \right).$$

The complex number  $e^{\frac{i(2k)\pi}{n}}$  is solution of  $u^n - 1 = 0$ .

If  $(x, y) \in \mathcal{C}_n^{(2)}(\mathbb{Q})$ , then  $y$  is solution of the equation  $u^n + 1 = 0$  and  $x$  is solution of the equation  $(u^n - 1)(u^n + 1) = 0$ .

This case 3 is subdivided into 7 sub-cases:

(1) If  $n \equiv 0[12]$ , then :

- $u^n + 1 = 0$  have no solution of degree at most 2 over  $\mathbb{Q}$ .
- $u^n - 1 = \prod_{d|n} \Phi_d(u) = 0$ , so  $u$  is solution of degree at most 2 if  $x$  is a root of  $\Phi_d(u)$  for  $d \in \{1, 2, 3, 4, 6\}$ . We obtain  $\prod_{1 \leq d \leq 6} \Phi_d(u) = 0$ , then  $(u^4 - 1)(u^3 - 1)(u^3 + 1) = 0$ . Therefore

$$\mathcal{C}_n^2(\mathbb{Q}) = \{\infty, (\pm\alpha, 0), (\beta, 0)\}.$$

(2) If  $n \equiv \pm 1[12]$ , then :

- $u^n + 1 = 0$  have solution of degree at most 2 if and only if  $u$  is a root of  $\Phi_2(u) = 0$  then  $u = -1$ .
- $u^n - 1 = \prod_{d|n} \Phi_d(u) = 0$ , so  $u$  is solution of degree at most 2 if  $u$  is the root of  $\Phi_1(u) = 0$ , then  $u = 1$ . Therefore :

$$\mathcal{C}_n^2(\mathbb{Q}) = \{\infty, (\pm 1, 0), (0, -1)\}.$$

(3) If  $n \equiv \pm 2[12]$ , then :

- $u^n + 1 = 0$  have a solution  $u$  of degree at most 2 if and only if  $\Phi_4(u) = 0$ , then  $u = \pm i$ .
- $u^n - 1 = \prod_{d|n} \Phi_d(u) = 0$ , so  $u$  is solution of degree at most 2 if and only if  $u$  is a root of  $\Phi_1(u)\Phi_2(u) = 0$ , then  $u = \pm 1$ . Therefore :

$$\mathcal{C}_n^2(\mathbb{Q}) = \{\infty, (\beta, 0), (0, \pm i)\}.$$

(4) If  $n \equiv \pm 3[12]$ , then :

- $u^n + 1 = 0$  have a solution  $u$  of degree at most 2 if and only if  $u$  is a root of  $\Phi_2(y)\Phi_6(u) = 0$ , then  $u = -\alpha$ .
- $u^n - 1 = \prod_{d|n} \Phi_d(u) = 0$ , so  $u$  is solution of degree at most 2 if and only if  $u$  is a root of  $\Phi_1(u)\Phi_3(u) = 0$ , then  $u = \alpha$ . Therefore :

$$\mathcal{C}_n^2(\mathbb{Q}) = \{\infty, (\pm\alpha, 0), (0, -\alpha)\}.$$

(5) If  $n \equiv \pm 4[12]$ , then :

- $u^n + 1 = 0$  have no solution of degree at most 2 over  $\mathbb{Q}$ .
- $u^n - 1 = \prod_{d|n} \Phi_d(u) = 0$ , so  $u$  is solution of degree at most 2 if  $u$  is a root of  $\Phi_1(u)\Phi_2(u)\Phi_4(u) = 0$ , then  $u = \beta$ . Therefore :

$$\mathcal{C}_n^2(\mathbb{Q}) = \{\infty, (\beta, 0)\}.$$

(6) If  $n \equiv \pm 5[12]$ , then :

- $u^n + 1 = 0$  have a solution  $u$  of degree at most 2 if and only if  $\Phi_2(u) = 0$ , then  $u = -1$ .
- $u^n - 1 = \prod_{d|n} \Phi_d(u) = 0$ , so  $u$  is solution of degree at most 2 if and only if  $u$  is the root of  $\Phi_1(u) = 0$ , then  $u = 1$ . Therefore :

$$\mathcal{C}_n^2(\mathbb{Q}) = \{\infty, (\pm 1, 0), (0, -1)\}.$$

(7) If  $n \equiv 6[12]$ , then :

- $u^n + 1 = 0$  have a solution  $u$  of degree at most 2 if and only if  $\Phi_4(u) = 0$ , then  $u = \pm i$ .
- $u^n - 1 = \prod_{d|n} \Phi_d(u) = 0$ , so  $u$  is solution of degree at most 2 if  $u$  is a root of  $\Phi_d(u) = 0$ ,  $d \in \{1, 2, 3, 6\}$  We obtain  $(u^3 - 1)(u^3 + 1) = 0$ . Therefore :

$$\mathcal{C}_n^2(\mathbb{Q}) = \{\infty, (\pm\alpha, 0), (\beta, 0), (0, \pm i)\}. \blacksquare$$

We deduced in Theorem [1.1](#) the following corollary :

**Corollary 3.1.** *Let  $n \geq 2$  a positive integer, the set of rational points on  $\mathbb{Q}$  of the family curves  $\mathcal{C}_n : y^{3n} = x^{4n} - 1$  is given by*

*If  $n$  is odd, then  $\mathcal{C}_n(\mathbb{Q}) = \{\infty, (\pm 1, 0)\}$*

*If  $n$  is even, then  $\mathcal{C}_n(\mathbb{Q}) = \{\infty, (\pm 1, 0), (0, -1)\}$ .*

## REFERENCES

- [1] *Bruin, N. and Stoll, M.*(2010) The Mordell-Weil sieve: proving the non-existence of rational points on curves, LMS Journal of Computing Mathematics 13 , (272-306).
- [2] *Camara, M., Fall, M., and Sall O.* (2024). Parametrization of Algebraic Points of Low Degree on the Hyperelliptic Curves  $y^2 = x(x^2 - n^2)(x^2 - 4n^2)$ . In: Seck, D., Kangni, K., Sambou, M.S., Nang, P., Fall, M.M. (eds) Nonlinear Analysis, Geometry and Applications. Trends in Mathematics. Birkhäuser, Cham
- [3] *Coleman, R.F.* (1985) Effective Chabauty. Duke Math. J. 52, no. 3, (765-770).
- [4] *Debarre, O. Klassen, M.* (1994). Points of low degree on smooth plane curves, J. Reine Angew. Math. 446 (81-87).
- [5] *Fall, M.*(2021) Algebraic points of low degrees in the Shaeffer curve, Journal of Mathematical Sciences and Modelling, Vol. IV issue II, August,(51-55).
- [6] *Faltings, G.* (1983). Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. 73, (349-366)
- [7] *Hindry, M. and Silverman J. H.* (2000) Diophantie geometry, an introduction, springer verlage. Graduate Texts in Mathematics, 201.
- [8] *Sall, O. Top, T. and Fall, M.* (2010) Paramétrisation des points algébriques de degré donné sur la courbe d'équation affine  $y^3 = x(x - 1)(x - 2)(x - 3)$ . C. R. Acad. Sci. Paris Sér I 348, (1147-1150).
- [9] *Siksek, S. and Stoll, M.*(2012). Partial descent on hyper elliptic curves and the generalized Fermat equation  $x^3 + y^4 + z^5 = 0$ , Bulletin of the LMS 44 .

Moussa FALL  
 Assane Seck University  
 Ziguinchor, Senegal  
 mail : m.fall@univ-zig.sn

Pape Modou SARR  
 Assane Seck University  
 Ziguinchor, Senegal  
 mail : p.sarr597@zig.univ.sn