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.

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

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

EDITORIAL BOARD

CONTENT

Moussa Fall, Pape Modou Sarr
DETERMINATION OF ALGEBRIC POINTS OF LOW DEGREE ON A FAMILI CURVES 7

Mohamadou Mor Diogou Diallo
EXIBITION OF PARAMETRIC FAMILY OF ALGEBRAIC POINTS OF GIVEN DEGREE ON AFINE EQUATION CURVE: $-y^2 = x^6 - 20x^3 - 8$ 15

Milan Mladenovski, Saso Gelev
DIGITAL FORENSICS ON ANDROID DEVICE 25

Darko Cebov, Aleksandra Mileva
MULTI-ACTION GRID AUTHENTICATION: A SECURE AND USABLE AUTHENTICATION SYSTEM FOR SMART TOUCH DEVICES 39

Aleksandra Nikolova, Aleksandar Velinov, Zoran Zdravev
USE CASES FOR BPMN AND UML TOOLS 51

Aleksandra Nikolova, Aleksandar Velinov, Zoran Zdravev
COMPARATIVE ANALYSIS OF BPMN TOOLS 61

Sara Aneva, Dragan Minovski
POSSIBILITIES FOR INSTALLATION OF PHOTOVOLTAIC SYSTEMS IN CATERING FACILITIES IN MACEDONIA 71

Dejan Krstev, Aleksandar Krstev
APPLICATION OF CENTER OF GRAVITY METHOD FOR LOCATIONS OF FACILITIES ... 83

Biljana Zlatanovska, Boro M. Piperevski
ON THE INTERGRABILITY OF A SUBCLASS OF 2D MATRIX DIFFERENTIAL EQUATIONS 91

Balkan Journal of Applied Mathematics and Informatics | Online ISSN 2545-4083
Volume 7 Number 2 Year 2024 | UDC: 514.754:511.235

EXIBITION OF PARAMETRIC FAMILY OF ALGEBRAIC POINTS OF GIVEN DEGREE ON AFFINE EQUATION CURVE: $-y^2 = x^6 - 20x^3 - 8$

MOHAMADOU MOR DIOGOU DIALLO

Abstract. We determine explicitly the set of algebraic points of given degree in the hyperelliptic curve of affine equation $-y^2 = x^6 - 20x^3 - 8$.
This curve has rang null, so we can use the Riemann-roch espaces and the Abel-jacobi theorem to determine all the algebraic points of given degree.

1. Introduction

Let $\mathcal{C}$ be a projective algebraic curve defined over $\mathbb{Q}$. For any number field $\mathbb{K}$,we denote by $\mathcal{C}(\mathbb{K})$ the set of points on $\mathcal{C}$ with coordinates are in $\mathbb{K}$ and $\bigcup\limits_{[\mathbb{K}:\mathbb{Q}]\leqslant \ell} \mathcal{C}(\mathbb{K}) = \mathcal{C}^{\ell}(\mathbb{K})$ the set of algebric points of degree at most ℓ over $\mathbb{Q}$. The degree of an algebraic point R is the degree of its field of definition on $\mathbb{Q}$ $i.e$ $\deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$. We denote by J the Jacobian of $\mathcal{C}$ and by $j(T)$ the class $[T - \infty]$ of $T - \infty$, i.e. j is the Jacobian folding (see [6]):

$$\begin{array}{cccc} j & : & \mathcal{C} & \longrightarrow & J(\mathbb{Q}), \\ & & T & \longmapsto & [T - \infty] \end{array}$$

where $J(\mathbb{Q})$ is the Mordell-Weil group of rational points of the Jacobian of $\mathcal{C}$ (see [10]); this group is finite (cf. [1]).
The curve $\mathcal{C}$ of affine equation $-y^2 = x^6 - 20x^3 - 8$ is smooth and is studied in [1] by Nils BRUIN. The projective equation of the curve $\mathcal{C}$ is given by:

$$-Z^4Y^2 = X^6 - 20X^3Z^3 - 8Z^6, \tag{1.1}$$

Date: December 4, 2024.
Keywords. Mordell-Weill group, Rational Points, Jacobian, Galois Conjugate, Linear Systems.

which can be written in this form

$$\mathcal{C} : \begin{cases} Z^4 \prod_{t=0}^{1}(Y - \gamma_t Z) = -X^3 \prod_{r=0}^{2}(X - \delta_r Z) \\ \text{where} \\ -Z^4Y^2 = \prod_{k=0}^{2}\prod_{p=0}^{1}(X - \eta_{k_p} Z) \end{cases} \tag{1.2}$$

which also corresponds to the affine equation

$$\mathcal{C} : \begin{cases} \prod_{t=0}^{1}(y - \gamma_t) = -x^3 \prod_{r=0}^{2}(x - \delta_r) \\ \text{where} \\ y^2 = \prod_{k=0}^{2}\prod_{p=0}^{1}(\eta_{k_p} - x) \end{cases} \tag{1.3}$$

with $\gamma_t = (-1)^t 2\sqrt{2}$, $\delta_r = \sqrt[3]{20}e^{\frac{2r\pi}{3}}$ and depending on the values respectively taken by $k_p = 0,\ 1$ and 2; we have $\eta_{k_p} = 1 + (-1)^p\sqrt{3}$, $\dfrac{-1+\sqrt{3}+(\imath)^{2p+1}\sqrt{12-6\sqrt{3}}}{2}$ and $\dfrac{-1-\sqrt{3}+(\imath)^{2p+1}\sqrt{12+6\sqrt{3}}}{2}$; explained in the following table:

$k=0,\ p\in\{0,1\}$	$k=1,\ p\in\{0,1\}$	$k=2,\ p\in\{0,1\}$
$\eta_{0_0} = 1+\sqrt{3}$	$\eta_{1_0} = \dfrac{-1+\sqrt{3}+\imath\sqrt{12-6\sqrt{3}}}{2}$	$\eta_{2_0} = \dfrac{-1-\sqrt{3}+\imath\sqrt{12+6\sqrt{3}}}{2}$
$\eta_{0_1} = 1-\sqrt{3}$	$\eta_{1_1} = \dfrac{-1+\sqrt{3}-\imath\sqrt{12-6\sqrt{3}}}{2}$	$\eta_{2_1} = \dfrac{-1-\sqrt{3}-\imath\sqrt{12+6\sqrt{3}}}{2}$

such that $\imath^2 = -1$. Let I_t, P_{k_p}, $Q_{r,t}$ and ∞ be the points of $\mathcal{C}$ defined by:
$I_t = [0 : \gamma_t : 1]$, $P_{k_p} = [\eta_{k_p} : 0 : 1]$, $Q_{r,t} = [\delta_r : \gamma_t : 1]$ and $\infty = [0 : 1 : 0]$.
In this note, we explicitly determine the set of algebric points of given degree over $\mathbb{Q}$, denoted $\mathcal{C}^{\ell}(\mathbb{Q})$, which is an extension of the result in [1] which exibited the set of rational points therefore of degree one and that its group $\mathcal{J}(\mathbb{Q})$.

2. **Main result**

The main result of our work is given by the following theorem:

Theorem 2.1. *The set $\mathcal{C}^{\ell}(\mathbb{Q})$ with $\ell \geq 5$ is given by $\mathcal{C}^{\ell}(\mathbb{Q}) = \bigcup_{n\in\{0,1\}} \mathcal{E}_n$; with:*

$$\mathcal{E}_n = \left\{ \left(x, \left(\frac{\sum_{i=n}^{\frac{\ell+2n}{2}} a_i\left(x^i + n\rho^i\right)}{\sum_{j=0}^{\frac{\ell+2n-5}{2}} b_j x^{j+2}} \right)^6 \right) \middle| \begin{array}{c} \rho^i = -\frac{1}{2}\sum_{p=0}^{1}\left(1+(-1)^p\sqrt{3}\right)^i, \textit{ the } a_i \\ \textit{and } b_j \textit{ are scalars such that } a_i \in \mathbb{Q}, \\ b_j \in \mathbb{Q}, a_0 \neq 0,\ a_{\frac{\ell+2n}{2}} \neq 0 \textit{ if } \ell \textit{ is even}, \\ b_{\frac{\ell+2n-5}{2}} \neq 0 \textit{ if } \ell \textit{ if odd and } x \\ \textit{is a root of the equation:} \end{array} \right. \\ \left. \left(\sum_{i=n}^{\frac{\ell+2n}{2}} a_i \left(\frac{x^i + n\rho^i}{x^{\frac{5\ell}{12}+n}} \right) \right)^{12} = \left(\sum_{j=0}^{\frac{\ell+2n-5}{2}} b_j x^{j+\frac{24-12n-5\ell}{12}} \right)^{12} \prod_{k=0}^{2}\prod_{p=0}^{1}(\eta_{k_p} - x) \right\}$$

2.1. **Auxiliary results.**

For a divisor ω on $\mathcal{C}$, let $\mathcal{L}(\omega)$ denote the $\bar{Q}$-vector space of rational functions f defined over $\mathbb{Q}$ such that $f = 0$ or $div(f) \geq -\omega$; $l(\omega)$ denotes the $\bar{Q}$-dimension of $\mathcal{L}(\omega)$ (see [8]).

Lemma 2.1. *For curve $\mathcal{C}$, we have the following rational divisors:*

i: $div(x) = \sum_{t=0}^{1} Q_{r,t} - 2\infty,$

ii: $div(x - \delta_r) = \sum_{t=0}^{1} Q_{r,t} - 2\infty,$

iii: $div(x - \gamma_t) = 3I_t + \sum_{r=0}^{2} Q_{r,t} - 6\infty,$

iv: $div(y) = \sum_{k=0}^{2}\sum_{p=0}^{1} P_{k_p} - 6\infty.$

Proof. Let x, y be the affine coordinates and X, Y and Z the projective coordinates. Let's: $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$. We have:

i: $div(x) = div(\frac{X}{Z}) = (X = 0)\cdot\mathcal{C} - (Z = 0)\cdot\mathcal{C}.$

- For $X = 0$, it follows from (1.2) implie that $Z^4 \prod_{t=0}^{1}(Y - \gamma_t Z) = 0$ which is equivalent to $Z^4 = 0$ or $(Y - \gamma_t Z) = 0$.
  This gives the points $Q_{r,t}$ with $t \in \{0, 1\}$ and ∞ with a the order of

the multiplication 1 and 4 respectively. Hence

$$(X=0)\cdot\mathcal{C}=\sum_{t=0}^{1}Q_{r,t}+4\infty. \tag{2.1}$$

- Similarly for $Z=0$, then it follows from (1.1) that: $X^6=0$.
  We therefore obtain the point ∞ with a multiplicitous order equal to 6 . Hence
  $$(Z=0)\cdot\mathcal{C}=6\infty. \tag{2.2}$$
  Thus from relations (2.1) and (2.2), we deduce that:
  $$div(x)=\sum_{t=0}^{1}Q_{r,t}-2\infty.$$

ii: Let's calculate: $div(x-\delta_r)=div(X-\delta_rZ)-div(Z)=(X=\delta_rZ)\cdot\mathcal{C}-(Z=0)\cdot\mathcal{C}$.

- For $X=\delta_rZ$, it follows (1.2) that: $Y^2=0$ or $Z^4=0$.
  This gives the points $Q_{r,t}$ with $t\in\{0,1\}$ and ∞ whose order of multiplicity is 1 and 4 respectively. Hence
  $$(X=\delta_rZ)\cdot\mathcal{C}=\sum_{t=0}^{1}Q_{r,t}+4\infty. \tag{2.3}$$
- For $Z=0$, we find the relation (2.2).

  Thus from relations (2.2) and (2.3), we deduce that:
  $$div(x-\delta_r)=\sum_{t=0}^{1}Q_{r,t}-2\infty.$$

iii: Let's calculate: $div(y-\gamma_t)=div(Y-\gamma_tZ)-div(Z)=(Y=\gamma_tZ)\cdot\mathcal{C}-(Z=0)\cdot\mathcal{C}$.

- For $Y=\gamma_tZ$, it follows (1.2) that: $X^3\prod_{r=0}^{2}(X-\delta_rZ)=0$ the result $X^3=0$ or $(X-\delta_rZ)=0$. This gives the points $Q_{r,t}$ with $r\in\{0,1,2\}$ and I_t order of multiplicity is 1 and 3 respectively. Hence
  $$(Y=\gamma_tZ)\cdot\mathcal{C}=3I_t+\sum_{r=0}^{2}Q_{r,t}. \tag{2.4}$$
- For $Z=0$, we find the relation (2.2).

  Thus from relations (2.2) and (2.4), we deduce that:
  $$div(x-\gamma_t)=3I_t+\sum_{r=0}^{2}Q_{r,t}-6\infty.$$

iv: $div(y) = div(\frac{Y}{Z}) = (Y=0)\cdot\mathcal{C} - (Z=0)\cdot\mathcal{C}$.

- For $Y = 0$, it follows from (1.2) that: $\prod_{k=0}^{2}\prod_{p=0}^{1}(X - \eta_{k_p} Z) = 0$. This gives the points: P_{k_p} with a multiplicative order of 1 for each point. Hence

$$(Y=0)\cdot\mathcal{C} = \sum_{k=0}^{2}\sum_{p=0}^{1} P_{k_p}. \tag{2.5}$$

Thus the relations (2.2) and (2.5), we deduce that:

$$div(y) = \sum_{k=0}^{2}\sum_{p=0}^{1} P_{k_p} - 6\infty.$$

□

Corollary 2.1. *The following results are the consequences of* **Lemma 2.1**, *we have:*

a: $\sum_{t=0}^{1} j(Q_{r,t}) = 0$ *and* $\sum_{k=0}^{2}\sum_{p=0}^{1} j(P_{k_p}) = 0,$

b: $3j(I_t) + \sum_{r=0}^{2} j(Q_{r,t}) = 0.$

Lemma 2.2. *According to* [1], *we have:*

$$\begin{array}{rcl} J(\mathbb{Q}) & = & \langle j(P_{0_0}) + j(P_{0_1})\rangle \otimes \mathbb{Z}/2\mathbb{Z} \\ & = & \{n\,(j(P_{0_0}) + j(P_{0_1}))\,, \textit{with } n \in \{0,1\}\} \end{array}$$

Remark 2.1: Note that, if $\lambda \in \mathcal{J}(\mathbb{Q})$ then:
$$\begin{array}{rcl} \lambda & = & n\,(j(P_{0_0}) + j(P_{0_1})), \\ & = & -n\,([P_{0_0} - \infty] + [P_{0_1} - \infty]), \\ & = & -n\left(\sum_{p=0}^{1} P_{0_p} - 2\infty\right). \end{array}$$

Lemma 2.3.

1: *We have the following linear systems:*

- $\mathcal{L}(\infty) = \langle 1\rangle,$
- $\mathcal{L}(2\infty) = \mathcal{L}(3\infty) = \langle 1, x\rangle,$
- $\mathcal{L}(4\infty) = \langle 1, x, x^2\rangle,$
- $\mathcal{L}(5\infty) = \left\langle 1, x, x^2, y^{\frac{1}{6}}x^2\right\rangle,$
- $\mathcal{L}(6\infty) = \left\langle 1, x, x^2, y^{\frac{1}{6}}x^2, x^3\right\rangle,$
- $\mathcal{L}(7\infty) = \left\langle 1, x, x^2, y^{\frac{1}{6}}x^2, x^3, y^{\frac{1}{6}}x^3\right\rangle,$

- $\mathcal{L}(8\infty) = \left\langle 1, x, x^2, y^{\frac{1}{6}}x^2, x^3, y^{\frac{1}{6}}x^3, x^4 \right\rangle$,
- $\mathcal{L}(9\infty) = \left\langle 1, x, x^2, y^{\frac{1}{6}}x^2, x^3, y^{\frac{1}{6}}x^3, x^4, y^{\frac{1}{6}}x^4 \right\rangle$,
- $\mathcal{L}(10\infty) = \left\langle 1, x, x^2, y^{\frac{1}{6}}x^2, x^3, y^{\frac{1}{6}}x^3, x^4, y^{\frac{1}{6}}x^4, x^5 \right\rangle$.

2: *Generally, for d intiger a $\mathbb{Q}$-base of $\mathcal{L}(d\infty)$ is given by:*

$$\mathcal{B}_d = \left\{ x^i \middle| i \in \mathbb{N} \text{ and } i \leq \frac{d}{2} \right\} \bigcup \left\{ y^{\frac{1}{6}}x^{j+2} \middle| j \in \mathbb{N} \text{ and } j \leq \frac{d-5}{2} \right\}.$$

Proof.

1: There are direct consequences of **Lemma 2.1** and the use of Clifford's theorem (see [3]).

2: It is easy to show that $\mathcal{B}_d$ is a free family, it then remains to show that $\#\mathcal{B}_d = \dim \mathcal{L}(d\infty)$. We know that the genus of $\mathcal{C}$ is $g = 2$ (see [2]). Since the curve has genus 2, according to the Riemann-Roch theorem (see [4, 8]), we have $\dim \mathcal{L}(d\infty) = d - g + 1 = d - 1$ since $d \geq 2g - 1 = 3$.
Two cases are possible:
First case: suppose that d is even, then $d = 2h$, we obtain:
$i \leq \frac{d}{2} \Leftrightarrow i \leq \frac{2h}{2} = h$ the same $j \leq \frac{d-5}{2} \Leftrightarrow j \leq \frac{2h-5}{2} \Leftrightarrow j \leq h - \frac{5}{2}$ $\Longrightarrow j < h - \frac{4}{2} = h - 2 \Longrightarrow j \leqslant h - 3$. It follows that:

$$\mathcal{B}_d = \left\{ 1, x, \ldots, x^h \right\} \bigcup \left\{ y^{\frac{1}{6}}x^2, y^{\frac{1}{6}}x^3, \ldots, y^{\frac{1}{6}}x^{h-1} \right\}.$$

So we have:

$$\#\mathcal{B}_d = h + 1 + h - 3 + 1 = 2h - 1 = d - 1 = \dim \mathcal{L}(d\infty).$$

Second case: suppose that d is odd, then $d = 2h + 1$, we get:
$i \leq \frac{d}{2} \Leftrightarrow i \leq \frac{2h+1}{2} \Leftrightarrow i \leq h + \frac{1}{2} \Longrightarrow i < h + 1 \Longrightarrow i \leqslant h$ the same $j \leq \frac{d-5}{2} \Leftrightarrow j \leq \frac{2h-4}{2} = h - 2$. Thus we have:

$$\mathcal{B}_d = \left\{ 1, x, \ldots, x^h \right\} \bigcup \left\{ y^{\frac{1}{6}}x^2, y^{\frac{1}{6}}x^3, \ldots, y^{\frac{1}{6}}x^h \right\}.$$

It follows that:

$$\#\mathcal{B}_d = h + 1 + h - 2 + 1 = (2h + 1) - 1 = d - 1 = \dim \mathcal{L}(d\infty).$$

□

2.2. Proof of the main theorem.

The following proof coorrespond to the demonstration of our main theorem.

Proof. Let $R \in \mathcal{C}(\bar{\mathbb{Q}})$ be of degree $[\mathbb{Q}(R) : \mathbb{Q}] = \ell$ with $\ell \geq 5$ and $R \notin \left\{I_t, Q_{r,t}, P_{k_p}, \infty\right\}$. Consider $R_1, \ldots, R_\ell$ the Galois conjugates of R and let $\lambda = \left[\sum_{\varsigma=0}^{\ell} R_\varsigma - \ell\infty\right] \in \mathcal{J}(\mathbb{Q})$.
From **Remark 2.1**, we have $\lambda = -n\left(\sum_{p=0}^{1} P_{0_p} - 2\infty\right)$ with $n \in \{0, 1\}$, and hence

$$\left[\sum_{\varsigma=0}^{\ell} R_\varsigma - \ell\infty\right] = \left(2n\infty - n\sum_{p=0}^{1} P_{0_p}\right). \tag{2.6}$$

The expression (2.6) gives the following equation:

$$\left[\sum_{\varsigma=0}^{\ell} R_\varsigma + n\sum_{p=0}^{1} P_{0_p} - (\ell + 2n)\infty\right] = 0. \tag{2.7}$$

From equation (2.7), we have deduced that, according to the Abel-Jacobi theorem [5, 9], there exists a rational function $\zeta(x, y)$ defined on $\mathbb{Q}$ such that :

$$div(\zeta) = \sum_{\varsigma=0}^{\ell} R_\varsigma + n\sum_{p=0}^{1} P_{0_p} - (\ell + 2n)\infty. \tag{2.8}$$

Two cases are possible:

1^{st}**case:** $n = 0$**.**

The formula (2.8) becomes:

$$div(\zeta) = \sum_{\varsigma=0}^{\ell} R_\varsigma - \ell\infty. \tag{2.9}$$

From expression (2.9), we deduce that $\zeta \in \mathcal{L}(\ell P_\infty)$. From **Lemma 2.3**, we have:

$$\zeta(x, y) = \sum_{i=0}^{\frac{\ell}{2}} a_i x^i + \sum_{j=0}^{\frac{\ell-5}{2}} b_j y^{\frac{1}{6}} x^{j+2}, \tag{2.10}$$

where a_i and b_j are scalars such that $b_j \in \mathbb{Q}$ and $a_i \in \mathbb{Q}^*$ (otherwise one of the R_ς's should be at P_{0_0}, which would be absurd), $a_{\frac{\ell}{2}} \neq 0$ (otherwise one of the R_ς's should be at ∞, which would be absurd) and $b_{\frac{\ell-5}{2}} \neq 0$ (otherwise one of the R_ς's should be at ∞, which would be absurd).

$2^{\mathbf{nd}}$**case:** $n = 1$**.**

The formula (2.8) implies that $\zeta \in \mathcal{L}((\ell+2)\infty)$, according to **Lemma 2.3**, we have

$$\zeta(x,y)=\sum_{i=0}^{\frac{\ell+2}{2}}a_ix^i+\sum_{j=0}^{\frac{\ell-3}{2}}b_jy^{\frac{1}{6}}x^{j+2} \tag{2.11}$$

and since $ord_{P_{0_0}}\zeta=ord_{P_{0_1}}\zeta=1$ so $\zeta(P_{0_0})=\zeta(P_{0_1})=0$ thus implied that $a_0=\sum_{i=1}^{\frac{\ell+2}{2}}a_i\rho^i$ where $\rho^i=-\frac{1}{2}\sum_{p=0}^{1}\left(1+(-1)^p\sqrt{3}\right)^i$, then the equation (2.11) is then written as follows:

$$\zeta(x,y)=\sum_{i=1}^{\frac{\ell+2}{2}}a_i\left(x^i+\rho^i\right)+\sum_{j=0}^{\frac{\ell-3}{2}}b_jy^{\frac{1}{6}}x^{j+2} \tag{2.12}$$

where a_i and b_j are scalars such that $a_{i_{i\geq 1}}$, $b_j\in\mathbb{Q}$, $a_{\frac{\ell+2}{2}}\neq 0$ if ℓ is even (otherwise one of the R_ς's should be at ∞, which would be absurd) and $b_{\frac{\ell-3}{2}}\neq 0$ if ℓ is odd (otherwise one of the R_ς's should be at ∞, which would be absurd).

So, from equations (2.10) and (2.12), we deduce that for all $n\in\{0,1\}$, we have:

$$\zeta_n(x,y)=\sum_{i=n}^{\frac{\ell+2n}{2}}a_i\left(x^i+n\rho^i\right)+\sum_{j=0}^{\frac{\ell+2n-5}{2}}b_jy^{\frac{1}{6}}x^{j+2}.$$

At point R_ς, we have $\zeta_n(x,y)=0$, this implies that $y=\left(\frac{\sum_{i=n}^{\frac{\ell+2n}{2}}a_i\left(x^i+n\rho^i\right)}{\sum_{j=0}^{\frac{\ell+2n-5}{2}}b_jx^{j+2}}\right)^6$.

By replacing the expression for y in (1.3), we obtain the following equation:

$$\left(\sum_{i=n}^{\frac{\ell+2n}{2}}a_i\left(x^i+n\rho^i\right)\right)^{12}=\left(\sum_{j=0}^{\frac{\ell+2n-5}{2}}b_jx^{j+2}\right)^{12}\prod_{k=0}^{2}\prod_{p=0}^{1}(\eta_{k_p}-x). \tag{2.13}$$

Equation (2.13) can be written as follows:

$$\left(\sum_{i=n}^{\frac{\ell+2n}{2}}a_i\left(\frac{x^i+n\rho^i}{x^{\frac{5\ell}{12}+n}}\right)\right)^{12}=\left(\sum_{j=0}^{\frac{\ell+2n-5}{2}}b_jx^{j+\frac{24-12n-5\ell}{12}}\right)^{12}\prod_{k=0}^{2}\prod_{p=0}^{1}(\eta_{k_p}-x). \tag{2.14}$$

The expression (2.14) is an equation of degree ℓ.
Indeed, the first member is degree $12 \times \left(\dfrac{\ell+2n}{2} - \dfrac{5\ell}{12} - n\right) = \ell$ and the second one is degree $12 \times \left(\dfrac{\ell+2n-5}{2} + \dfrac{24-12n-5\ell}{12} + 6\right) + 6 = \ell$.
This gives a degree point family ℓ:

$$\mathcal{E}_n = \left\{ \left(x, \left(\frac{\sum_{i=n}^{\frac{\ell+2n}{2}} a_i \left(x^i + n\rho^i\right)}{\sum_{j=0}^{\frac{\ell+2n-5}{2}} b_j x^{j+2}} \right)^6 \right) \;\middle|\; \begin{array}{c} \rho^i = -\dfrac{1}{2}\sum_{p=0}^{1}\left(1+(-1)^p\sqrt{3}\right)^i, \text{ the } a_i \\ \text{and } b_j \text{ are scalars such that } a_i \in \mathbb{Q}, \\ b_j \in \mathbb{Q}, a_0 \neq 0,\ a_{\frac{\ell+2n}{2}} \neq 0 \text{ if } \ell \text{ is even,} \\ b_{\frac{\ell+2n-5}{2}} \neq 0 \text{ if } \ell \text{ if odd and } x \\ \text{is a root of the equation:} \end{array} \right.$$
$$\left. \left(\sum_{i=n}^{\frac{\ell+2n}{2}} a_i \left(\frac{x^i + n\rho^i}{x^{\frac{5\ell}{12}+n}} \right) \right)^{12} = \left(\sum_{j=0}^{\frac{\ell+2n-5}{2}} b_j x^{j+\frac{24-12n-5\ell}{12}} \right)^{12} \prod_{k=0}^{2}\prod_{p=0}^{1}(\eta_{k_p} - x) \right\}$$

$\square$

References

[1] *Bruin, N* (2000). On powers as sums of two cubes, Algorithmic Number Theory, Tome 21, 4th International Symposium, ANTS-IV Leiden, The Netherlands, pp. 169–184.

[2] *Bruin, N. and Flynn, E.V* (2006). Exhibiting SHA [2] on hyperelliptic Jacobians, Journal of Number Theory, No.2, Vol.118, pp. 266–291.

[3] *Coppens, M. and Martens, G* (1991). Secant spaces and Clifford's theorem, Compositio Mathematica, No.2, Vol.78, pp. 193–212.

[4] *Faltings, G* (1992). Lectures on the arithmetic Riemann-Roch theorem, Princeton University Press, Vol.127.

[5] *Arbarello, E., Cornalba, M., Griffiths P. A. and Harris, J* (1985). The Basic Results of the Brill-Noether Theory, Geometry of Algebraic Curves, No.3, Vol.133, pp. 203–224.

[6] *Fuchs, L. and Kahane, J.P. and Robertson, A.P. and Ulam, S* (1960). Abelian groups, Vol.960.

[7] *Borel, A. and Serre, J.P* (1958). Le théoréme de Riemann-Roch, Bultin de la Société mathématiques de france, Vol.86, pp. 97–136.

[8] *Faddeev, D* (1961). On the divisor class groups of some algebraic curves, Dokl. Akad. Nauk SSSR, Vol.136, pp. 296–298. English translation : Soviet Math. Dokl, No.1, Vol.2, pp. 67–69.

[9] *Griffiths, P. A* (1989). Introduction to algebraic curves, Translations of mathematical monographs, American Mathematical Society, Providence, RI, Vol.76.

[10] *Gross, B. and Rohrlich, D* (1978). Some results on the Mordell-Weil group of the jacobian of the Fermat curve, Invent. Math, Vol.44 , pp. 201–224.

Mohamadou Mor Diogou Diallo
Assane Seck University of Ziguinchor,
Faculty of Sciences and Technology,
Diabir, BP:523, Ziguinchor,
Senegal
Email address: m.diallo1836@zig.univ.sn