Journal of Mathematical Sciences and Modelling, 4 (2) (2021) 51-55
Research Article

Journal of Mathematical Sciences and Modelling

Journal Homepage: www.dergipark.gov.tr/jmsm
ISSN 2636-8692
DOI: http://dx.doi.org/10.33187/jmsm.931258

Parametrization of Algebraic Points of Low Degrees on the Schaeffer Curve

Moussa Fall[1]

[1] *Department of Mathematics, Faculty of Science and Technology University, Assane Seck, Ziguinchor*

Article Info

Keywords: *Degree of algebraic points, Plan curve, Rational points.*
2010 AMS: *11D68, 12FO5, 14H40, 14H50*
Received: *2 May 2021*
Accepted: *19 August 2021*
Available online: *31 August 2021*

Abstract

In this paper, we give a parametrization of algebraic points of degree at most 4 over $\mathbb{Q}$ on the schaeffer curve $\mathscr{C}$ of affine equation : $y^2 = x^5 + 1$. The result extends our previous result which describes in [5] (Afr. Mat 29:1151-1157, 2018) the set of algebraic points of degree at most 3 over $\mathbb{Q}$ on this curve.

1. Introduction

Let $\mathscr{C}$ be a smooth projective plane curve defined over K. For all algebraic extension field K of $\mathbb{Q}$, we denote by $\mathscr{C}(K)$ the set of K-rational points of $\mathscr{C}$ over K and $\mathscr{C}^{(d)}(\mathbb{Q})$ the set of algebraic points of $\leq d$ over $\mathbb{Q}$. The degree of an algebraic point R is the degree of its field of definition on $\mathbb{Q}$: $deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$.
A famous theorem of Fatling show that if $\mathscr{C}$ is a smooth projective plane curve defined over K of genus $g \geq 2$, then $\mathscr{C}(K)$ is finite. Fatling's proof is still ineffective in the sense that it does not provide an algorithm for computing $\mathscr{C}(K)$. A most precise theorem of Debarre and Klasen [4] show that if $\mathscr{C}$ be a smooth projective plane curve defined by an equation of degree $d \geq 7$ with rational coefficients then $\mathscr{C}^{(d-2)}(\mathbb{Q})$ is finite. This theorem often us to characterize the set $\mathscr{C}^{(2)}(\mathbb{Q})$ of all algebraic points of degree ≤ 2 over $\mathbb{Q}$.
Currently for curve $\mathscr{C}$ defined over a numbers field K of genus $g \geq 2$, there is no known algorithm for computing the set $\mathscr{C}(K)$ or for deciding if $\mathscr{C}(K)$ is empty. But there is a bag of strikes that can be used to show that $\mathscr{C}(K)$ is empty, or to determine $\mathscr{C}(K)$ if it is not empty. Among these methods, we can cite the local method, Chabauty method [2], Descent method [7], mordell-weil sieves method [1]. These methods often succeed with less than full knowledge of the jacobian $J(\mathbb{Q})$ of the curve . If $J(\mathbb{Q})$ is finite then it is no hard to determine $\mathscr{C}(\mathbb{Q})$ and to generalize for all number field K.
Previous works ([3] and [5]) have studied the algebraic points of degree at most 3 on the schaeffer curve of affine equation $y^2 = x^5 + 1$ denoted $\mathscr{C}$. The curve $\mathscr{C}$ is hyperelliptic of genus $g = 2$ and of rank null by [3].
Let's denote $P_0 = (-1, 0)$, $P_1 = (0, 1)$, $\overline{P_1} = (0, -1)$, $Q_1 = (1+i, 1-2i), Q_2 = (1-i, 1+2i)$, $\overline{Q_1} = (1+i, -1+2i)$, $\overline{Q_2} = (1-i, -1-2i)$ and ∞ the point at infinity.
The purpose of this note is to determine the algebraic parametrization of all algebraic points of degree at most four on the curve $\mathscr{C}_s$ over the rationnal numbers field $\mathbb{Q}$ using ideas in [5] (Afr. Mat 29:1151-1157, 2018).

2. Auxiliary results

Lemma 2.1. *Let x and y be the rational functions defined on $\mathscr{C}_s$ by $x(X,Y,Z) = \frac{X}{Z}$ and $y(X,Y,Z) = \frac{Y}{Z}$:*

- $div(y-1) = 5P_1 - 5\infty$; $div(y+1) = 5\overline{P}_1 - 5\infty$;
- $div(x) = P_1 + \overline{P}_1 - 2\infty$; $div(x+1) = 2P_0 - 2\infty$
- $div(y) = A_0 + A_1 + A_2 + A_3 + A_4 - 5\infty$ *where* $A_i = exp(i(2k+1)\frac{\pi}{5})$.

Email addresses and ORCID numbers: **m.fall@univ-zig.sn, 0000-0003-3880-7603 (M. Fall)**

Denote by $\mathscr{L}(m\infty)$ the $\overline{\mathbb{Q}}$−vector space of rational functions defined by $\mathscr{L}(m\infty) = \left\{ f \in \overline{\mathbb{Q}}(\mathscr{C}_s)^* \mid div(f) \geq -m\infty \right\} \cup \{0\}$ *:*

- $\mathscr{L}(\infty) = \langle 1 \rangle$
- $\mathscr{L}(2\infty) = \mathscr{L}(3\infty) = \langle 1, x \rangle$
- $\mathscr{L}(4\infty) = \langle 1, x, x^2 \rangle$
- $\mathscr{L}(5\infty) = \langle 1, x, x^2, y \rangle$
- $\mathscr{L}(6\infty) = \langle 1, x, x^2, y, x^3 \rangle$

Proof. See [5]

Lemma 2.2. *We consider the divisor D on the curve $\mathscr{C}_s$:*

- $D = [(-1, 0) + (0, 1) - 2\infty] = [P_0 + P_1 - 2\infty]$
- $2D = [2(0, 1) - 2\infty] = [2P_1 - 2\infty]$
- $3D = [(1+i, 1-2i) + (1-i, 1+2i) - 2\infty] = [Q_1 + Q_2 - 2\infty]$
- $4D = [(0, -1) - \infty] = [\overline{P}_1 - \infty]$
- $5D = [(-1, 0) - \infty] = [P_0 - \infty]$
- $6D = [(0, 1) - \infty] = [P_1 - \infty]$
- $7D = [(1+i, -1+2i) + (1-i, -1-2i) - 2\infty] = [\overline{Q}_1 + \overline{Q}_2 - 2\infty]$
- $8D = [2(0, -1) - 2\infty] = [2\overline{P}_1 - 2\infty]$
- $9D = [(-1, 0) + (0, -1) - 2\infty] = [P_0 + \overline{P}_1 - 2\infty]$
- $10D = 0.$

The Mordell-weil groupe of the curve $\mathscr{C}_s$ is $J(\mathbb{Q}) \cong (\mathbb{Z}/10\mathbb{Z}) \cong \langle D \rangle = \{mD \mid 0 \leq m \leq 9\}$.

Proof. See [3].

3. Main result

Our main result is the following theorem

Theorem 3.1. *The algebraic points of degree 4 over $\mathbb{Q}$ on the curve $\mathscr{C}_s$ are given by the union of the following sets :* $\mathscr{G}_0 \cup \mathscr{G}_1 \cup \mathscr{G}_2 \cup \mathscr{G}_3 \cup \mathscr{G}_4 \cup \mathscr{G}_5$ *with*

- $\mathscr{G}_0 = \left\{ \left(x, \pm\sqrt{x^2+1}\right) \mid [\mathbb{Q}(x) : \mathbb{Q}] = 2, x^2 - 2x + 2 \neq 0 \right\}$;
- $\mathscr{G}_1 = \left\{ \begin{array}{l} \left(x, \pm(-1 + (-1-a+c)x - ax^2 - cx^3\right) \mid a, c \in \mathbb{Q}, c \neq 0 \, et \, a \neq c-1, \; x \text{ root of} \\ B_1(x) = c^2x^4 + \left(2ac - c^2 - 1\right)x^3 + \left(a^2 - c^2 + 2c + 1\right)x^2 + \left(a^2 + 2a - 2ac + c^2 - 1\right)x + 2a - 2c + 2 = 0 \end{array} \right\}$;
- $\mathscr{G}_2 = \left\{ \left(x, \pm\left(cx^3 + ax^2 - 1\right)\right) \mid a, c \in \mathbb{Q}^*, a \neq c+1, \; x \text{ root of } B_2(x) = c^2x^4 + 2acx^3 - x^3 + a^2x^2 - 2cx - 2a = 0 \right\}$;
- $\mathscr{G}_3 = \left\{ \begin{array}{l} \left(x, \pm(-3 - 2a - 4c + (2+2a+2c)x - ax^2 - cx^3)\right) \mid a, c \in \mathbb{Q}, a \neq -1-2c, c \neq 0, \; x \text{ root of } B_3(x) = c^2x^4 + \\ \left(2c^2 + 2ac - 1\right)x^3 + \left(-2c^2 - 4c + a^2 - 2\right)x^2 + \left(-4ac - 2c - 2a^2 - 4a - 2\right)x + 8c^2 + 8ac + 12c + 2a^2 + 6a + 4 \end{array} \right\}$;
- $\mathscr{G}_4 = \left\{ \left(x, \pm(1 + ax + cx^2)\right) \mid a, c \in \mathbb{Q}, a \neq 0, \; x \text{ root of } B_4(x) = -x^4 + c^2x^3 + 2acx^2 + \left(2c + a^2\right)x + 2 \right\}$;
- $\mathscr{G}_5 = \left\{ \begin{array}{l} \left(x, \pm(-a + (-a-c)x - cx^2)\right) \mid, a, c \in \mathbb{Q}, a \neq \pm 1, \; x \text{ root of} B_5(x) = -x^4 + \left(c^2+1\right)x^3 + \left(c^2 + 2ac - 1\right)x^2 \\ + \left(2ac + a^2 + 1\right)x + a^2 - 1 \end{array} \right\}$.

Proof of theoreme.
Let $R \in \mathscr{C}_s\left(\overline{\mathbb{Q}}\right)$ with $[\mathbb{Q}(R) : \mathbb{Q}] = 4$. Let R_1, R_2, R_3, R_4 be the Galois conjugates of R. We have

$$[R_1 + R_2 + R_3 + R_4 - 4\infty] \in J(\mathbb{Q})$$

from lemma (2.2) , we get

$$[R_1 + R_2 + R_3 + R_4 - 4\infty] = mD, \quad 0 \leq m \leq 9$$

Now for any integer m such that $0 \leq m \leq 9$, we have $mD = (m-10)D$, so

$$[R_1 + R_2 + R_3 + R_4 - 4\infty] = (m-10)D, \quad 0 \leq m \leq 9. \qquad (\star)$$

Our proof is divided in five cases

Case $m = 0$

Formula $(\star)$ becomes

$$[R_1 + R_2 + R_3 + R_4 - 4\infty] = 0.$$

The Abel Jacobi theorem involves the existence of a function F such that

$$div(F) = R_1 + R_2 + R_3 + R_4 - 4\infty$$

so $F \in \mathscr{L}(4\infty)$, and lemma (2.1) gives $F(x,y) = a + bx + cx^2$; x must be in the $\overline{\mathbb{Q}}$ such as $[\mathbb{Q}(x) : \mathbb{Q}] = 2$ and $x^2 - 2x + 2 \neq 0$. We get a family of quartic points

$$\mathscr{G}_0 = \left\{ \left(x, \pm\sqrt{x^5+1}\right) \mid x \in [\mathbb{Q}(x) : \mathbb{Q}] = 2, \, x^2 - 2x + 2 \neq 0 \right\}.$$

Cases $m = 1$ and $m = 9$

For $m=1$: The formula $(\star)$ and lemma (2.2) give

$$[R_1+R_2+R_3+R_4-4\infty]=-9D=-\left[P_0+\overline{P}_1-2\infty\right].$$

This means

$$\left[R_1+R_2+R_3+R_4+P_0+\overline{P}_1-6\infty\right]=0$$

The Abel Jacobi theorem involves the existence of a function F such that

$$div(F)=R_1+R_2+R_3+R_4+P_0+\overline{P}_1-6\infty.$$

So $F\in\mathscr{L}(6\infty)$, then $F(x,y)=u+vx+wx^2+dx^3+ey$ $(e\neq 0)$. We have $F\left(\overline{P}_1\right)=F(P_0)=0$, so $u-e=0$ and $u-v+w-d=0$, thus

$$F(x,y)=u+(u+w-d)x+wx^2+dx^3+uy\quad u\neq 0.$$

At the points R_i, we have $y=-1+(-1-a+c)x-ax^2-cx^3$ with $a=\frac{w}{u}$ and $c=\frac{d}{u}$. By substituting y in $y^2-x^5-1=0$ and simplifying by $x(x+1)$ we obtain

$$B_1(x)=c^2x^4+\left(2ac-c^2-1\right)x^3+\left(a^2-c^2+2c+1\right)x^2+\left(a^2+(2-2c)a+c^2-1\right)x+2a-2c+2=0$$

We must have $B_1(0)\neq 0$ and $B_1(-1)\neq 0$ which involves $a\neq c-1$ and $c\neq 0$. We have a family of quartic points

$$\mathscr{G}_{1,1}=\left\{\ \left(x,\ +(-1+(-1-a+c)x-ax^2-cx^3)\right)\mid a,c\in\mathbb{Q},\ a\neq c-1,\ c\neq 0,\ x\text{ root of }B_1(x)=0\ \right\}$$

For $m=9$: The formula $(\star)$ and lemma (2.2) give

$$[R_1+R_2+R_3+R_4-4\infty]=-D=-[P_0+P_1-2\infty]$$

This means

$$[R_1+R_2+R_3+R_4+P_0+P_1-6\infty]=0$$

The Abel Jacobi theorem involves the existence of a function F such that

$$div(F)=R_1+R_2+R_3+R_4+P_0+P_1-6\infty.$$

So $F\in\mathscr{L}(6\infty)$, hence $F(x,y)=u+vx+wx^2+dx^3+ey$ $(e\neq 0)$. We have $F(P_1)=F(P_0)=0$, so $u-e=0$ et $u-v+w-d=0$, then

$$F(x,y)=u+(u+w-d)x+wx^2+dx^3+uy\quad u\neq 0.$$

At the points R_i, we have $y=1+(1+a-c)x+ax^2+cx^3$ with $a=-\frac{w}{u}$ and $c=-\frac{d}{u}$. By substituting y in $y^2-x^5-1=0$ and simplifying by $x(x+1)$, we have

$$B_1(x)=c^2x^4+\left(2ac-c^2-1\right)x^3+\left(a^2-c^2+2c+1\right)x^2+\left(a^2+(2-2c)a+c^2-1\right)x+2a-2c+2=0$$

We must have $B_1(0)\neq 0$ and $B_1(-1)\neq 0$ involving $a\neq c-1$ and $c\neq 0$. We get a family of quartic points

$$\mathscr{G}_{1,2}=\left\{\ \left(x,\ -(-1+(-1-a+c)x-ax^2-cx^3)\right)\mid a,c\in\mathbb{Q},\ a\neq c-1,\ c\neq 0,\ x\text{ root of }B_1(x)=0\ \right\}.$$

Finally, we get a second family of quartic points $\mathscr{G}_1=\mathscr{G}_{1,1}\cup\mathscr{G}_{1,2}$.

<u>Cases $m=2$ and $m=8$</u>

For $m=2$: the formula $(\star)$ becomes

$$[R_1+R_2+R_3+R_4-4\infty]=-8D=-\left[2\overline{P_1}-2\infty\right]$$

This means

$$\left[R_1+R_2+R_3+R_4+2\overline{P_1}-6\infty\right]=0$$

The Abel Jacobi theorem involves the existence of a function F such that

$$div(F)=R_1+R_2+R_3+R_4+2\overline{P_1}-6\infty$$

So $F\in\mathscr{L}(6\infty)$, hence $F(x,y)=a+bx+cx^2+dx^3+ey$ $(e\neq 0)$. The point $\overline{P}_1$ is order 2, so $u-e=0$ and $v=0$, thus

$$F(x,y)=u+wx^2+dx^3+uy$$

At the points R_i, we have $-uy=u+wx^2+dx^3$ $(u\neq 0)$, so $y=-1+ax^2+cx^3$ with $a=-\frac{w}{u}$ and $k=-\frac{d}{u}$. Substuting y to $y^2=x^5+1$, we have

$$x^2\left(a^2x^4+2acx^3-x^3+a^2x^2-2cx-2a\right)=0.$$

Simplifying by x^2, we have

$$B_2(x)=c^2x^4+2acx^3-x^3+a^2x^2-2cx-2a.$$

We must have $ac\neq 0$ and $a\neq c+1$. We obtain a family of quartic points :

$$\mathscr{G}_{2,1}=\left\{\left(x,\ \left(cx^3+ax^2-1\right)\right)\ \mid\ a,c\in\mathbb{Q}^*,\ a\neq c+1,\ x\text{ root of }B_2(x)=0\right\}.$$

For $m=8$: by a similar argument as in case $m=2$, we have

$$\mathscr{G}_{2,2}=\left\{\left(x,\ -\left(cx^3+ax^2-1\right)\right)\ \mid\ a,c\in\mathbb{Q}^*,\ a\neq c+1,\ x\text{ root of }B_2(x)=0\right\}.$$

Finally, we have the third family $\mathscr{G}_2=\mathscr{G}_{2,1}\cup\mathscr{G}_{2,2}$.

Cases $m=3$ and $m=7$

For $m=3$: the formula $(\star)$ becomes

$$[R_1+R_2+R_3+R_4-4\infty]=-7D=-\left[\overline{Q_1}+\overline{Q_2}-2\infty\right]$$

This means

$$\left[R_1+R_2+R_3+R_4+\overline{Q_1}+\overline{Q_2}-6\infty\right]=0$$

The Abel Jacobi theorem involves the existence of a function F such that

$$div(F)=R_1+R_2+R_3+R_4+\overline{Q_1}+\overline{Q_2}-6\infty.$$

Then $F(x,y)=u+vx+wx^2+dx^3+ey\ (e\neq 0)$. We have $F\left(\overline{Q}_1\right)=F\left(\overline{Q}_2\right)=0$, so $u+v-2d-e=0$ and $v+2w+2d+2e=0$, hence

$$F(x,y)=2w+4d+3e+(-2w-2d-2e)x+wx^2+dx^3+ey\ (e\neq 0).$$

At points R_i, we have $y=(-3-2a-4c)+(2+2a+2c)x-ax^2-cx^3$ with $a=\frac{w}{e}$ and $c=\frac{d}{e}$. Substuting y into $y^2=x^5+1$ and simplifying by x^2-2x+2, we have

$$B_3(x)=c^2x^4+\left(2c^2+2ac-1\right)x^3+\left(-2c^2-4c+a^2-2\right)x^2+\left((-4a-2)c-2a^2-4a-2\right)x+8c^2+(8a+12)c+2a^2+6a+4=0.$$

We must have $c\neq 0$ and $a\neq -1-2c$. We get a family of quartic points

$$\mathscr{G}_{3,1}=\left\{\ \left(x,\ (-3-2a-4c+(2+2a+2c)x-ax^2-cx^3)\right)\mid a,c\in\mathbb{Q}\, c\neq 0, a\neq -1-2c, x \text{ root of } B_3(x)=0\ \right\}$$

For $m=7$: by a similar argument as in previous case, we get a family of quartic points

$$\mathscr{G}_{3,2}=\left\{\ \left(x,\ -(-3-2a-4c+(2+2a+2c)x-ax^2-cx^3)\right)\mid a,c\in\mathbb{Q}\, c\neq 0, a\neq -1-2c, x \text{ root of } B_3(x)=0\ \right\}$$

Therefore, we have the fourth family $\mathscr{G}_3=\mathscr{G}_{3,1}\cup\mathscr{G}_{3,2}$.

Cases $m=4$ and $m=6$

For $m=4$: it exists a fonction F such that $div(F)=R_1+R_2+R_3+R_4+P_1-5\infty$, hence $F\in\mathscr{L}(5\infty)$,

$$F(x,y)=u+vx+wx^2+dy\quad (d\neq 0).$$

We have $F(P_1)=0$, therefore $u+d=0$, then $F(x,y)=u+vx+wx^2-uy$, $(u\neq 0)$. At points R_i, we have $y=1+ax+cx^2$. Substiting y to $y^2=x^5+1$, we have

$$x\left(x^4+c^2x^3+2acx^2+\left(2c+a^2\right)x+2a\right)=0.$$

Simplifiying by x, we have the minimal polynomial

$$B_4(x)=x^4+c^2x^3+2acx^2+\left(2c+a^2\right)x+2a=0.$$

We must have $a\neq 0$. We obtain a family of quartic points :

$$\mathscr{G}_{4,1}=\left\{\left(x,\ +(1+ax+cx^2)\right)\mid a,c\in\mathbb{Q}, a\neq 0, x \text{ root of } B_4(x)=0\right\}.$$

For $m=6$: by a similar argument as in previous case, we get a family of quartic points :

$$\mathscr{G}_{4,2}=\left\{\left(x,\ -(1+ax+cx^2)\right)\mid a,c\in\mathbb{Q}, a\neq 0, x \text{ root of } B_4(x)=0\right\}$$

Therefore, we have the firth family : $\mathscr{G}_4=\mathscr{G}_{4,1}\cup\mathscr{G}_{4,2}$.

Case $m=5$

It exists F such that $div(F)=R_1+R_2+R_3+R_4+P_0-5\infty$, so $F\in\mathscr{L}(5\infty)$, then

$$F(x,y)=u+vx+wx^2+dy\quad (d\neq 0).$$

We have $F(P_0)=0$, so $v=u+w$, therefore $F(x,y)=u+(u+w)x+wx^2+dy$. At points R_i, we have $y=-a+(-a-c)x-cx^2$ with $a=\frac{u}{d}$ and $c=\frac{w}{d}$. Substiting y to $y^2=x^5+1$, we have

$$(x+1)\left(x^4+\left(c^2+1\right)x^3+\left(c^2+2ac-1\right)x^2+\left(2ac+a^2+1\right)x+a^2-1\right)=0.$$

Simplifliying by $x+1$, we have the polynomial

$$B_5(x)=x^4+\left(c^2+1\right)x^3+\left(c^2+2ac-1\right)x^2+\left(2ac+a^2+1\right)x+a^2-1.$$

We must have $a\neq\pm 1$, therefore, we have the fifth family :

$$\mathscr{G}_5=\left\{\left(x,\ (-a+(-a-l)x-cx^2)\right)\mid a,c\in\mathbb{Q}, a\neq\pm 1, x \text{ root of } B_5(x)=0\right\}.$$

References

[1] N. Bruin, M. Stoll, *The Mordell-Weil sieve : proving the nonexistence of Rational points on curves*, LMS J. Comp. Math., **13** (2010), 272 -306.
[2] R. F. Coleman, *Effective Chabauty* Duke Math. J. **52**(3) (1985), 765-770.
[3] E. F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Mathematische Annalen, **310** (1998), 447–471.
[4] M. J. Klassen, E. F. Schaefer, *Arithmetic and geometry of the curve* $x^4 = y^3 + 1$, Acta Arithmetica LXXIV.**3** (1996) 241-257.
[5] M. Fall, O. Sall, *Ponts algébriques de petit degré sur la courbe d'équation affine* $y^2 = x^5 + 1$, Afr. Mat. **29** (2018) 1151-1157.
[6] O. Sall, *Points algébriques sur certains quotients de courbes de Fermat*, C. R. Acad. Sci. Paris Sér I **336** (2003) 117-120.
[7] S. Siksek, 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** (2012) 151 -166