TJMM
16 (2024), No. 1-2, 59-64

ALGEBRAIC POINTS OF LOW DEGREES ON CURVES OF AFFINE EQUATION $y^{2n} = x^5 + 1$

MOUSSA FALL, PAPE MODOU SARR AND EL HADJI SOW

ABSTRACT. IIn this paper, we use the Chevalley-Weil theorem and the result of Schaeffer (see [5]) to determine explicitly the algebraic points of degree at most two over $\mathbb{Q}$ of the family curves of affine equations $y^{2n} = x^5 + 1$. This result extends the work of Schaeffer who determined the algebraic points of degree two over $\mathbb{Q}$ of the curve $y^2 = x^5 + 1$.

1. INTRODUCTION AND MAIN RESULT

1.1. Introduction

Let $\mathcal{C}$ be a smooth projective plane curve defined over $\mathbb{Q}$. For all algebraic extension field K of $\mathbb{Q}$, we denote by $C(K)$ the set of K-rational points of $\mathcal{C}$ on K and by $\mathcal{C}^{(d)}(\mathbb{Q})$ the set of algebraic points of degree d over $\mathbb{Q}$. The degree of an algebraic point R is the degree of its field of definition on $\mathbb{Q}$ i.e $deg(R) = [\mathbb{Q}(R) : \mathbb{Q}]$. A famous theorem of Faltings [6] shows that if $\mathcal{C}$ is a smooth projective plane curve defined over K of genus $g \geq 2$, then $\mathcal{C}(K)$ is finite. Faltings's proof is still ineffective in the sense that it does not provide an algorithm for computing $\mathcal{C}(K)$. A most precise theorem of Debarre and Klassen [4] show that if $\mathcal{C}$ be a smooth projective plane curve defined by an equation of degree $d \geq 7$ with rational coefficients then $\mathcal{C}^{(d-2)}(\mathbb{Q})$ is finite. This theorem often us to characterize the set $\mathcal{C}^{(2)}(\mathbb{Q})$ of all algebraic points of degree at most 2 over $\mathbb{Q}$.
Currently for curve $\mathcal{C}$ defined over a numbers field K of genus $g \geq 2$, there is no know algorithm for computing the set $\mathcal{C}(K)$ or for deciding if $\mathcal{C}(K)$ is empty. But there is a bag of strikes that can be used to show that $\mathcal{C}(K)$ is empty, or to determine $\mathcal{C}(K)$ if it is not empty. These include local method, Chabauty method [3], Descent method [12], Mordell-Weil sieves method [1]. These methods often succeed with less than full knowledge of the jacobian of the curve. If it is finite it is not hard to determine $\mathcal{C}(Q)$ and to generalize for all number field K. So we can easily deduce $\mathcal{C}^{(d)}(\mathbb{Q})$ [8].
Let n be a positive integer and $\mathcal{C}_n$ the family curves defined over the rational numbers $\mathbb{Q}$ by affines equations $\mathcal{C}_n : y^{2n} = x^5 + 1$. The Mordell-Weil group of the Jacobian of each curve of the family is not known except for $\mathcal{C}_1$ whose Mordell-Weil group is given by schaeffer in [11].
The purpose of this note is to work around the finiteness of the Mordell-Weil group by using the Chevalley-Weil theorem and the results obtained by Schaeffer on the curve $\mathcal{C}_1$ to determine explicitly the set of rational points and quadratic points of the curves $\mathcal{C}_n$.
In [11] Schaefer gave a description of the rational points and the quadratic points over $\mathbb{Q}$ on the algebraic curve $\mathcal{C}$ of affine equation : $y^2 = x^5 + 1$.

2010 *Mathematics Subject Classification.* MSC2020 subject classifications: 14H50, 14G05, 12F05, 14A10 .

Key words and phrases. rational point on curve, degree of algebraic point, cyclotomic polynomial, Chevalley-Weil theorem.

Let $P_0 = (-1, 0),\ P_1 = (0, 1),\ \overline{P}_1 = (0, -1),\ \infty$ be the point at infinity and $\mathcal{C}^{(d)}(\mathbb{Q})$ be the set of algebraic points of degree d over $\mathbb{Q}$ on a curve $\mathcal{C}$.
Let us denote by $Q_1 = (1 + i, 1 - 2i),\ Q_2 = (1 - i, 1 + 2i),\ \overline{Q}_1 = (1 + i, -1 + 2i),$
$\overline{Q}_2 = (1 - i, -1 - 2i),\ R_0 = P_0 + P_1$.
The following proposition describes the rational and quadratic points on the curve $\mathcal{C}_1$ (see [11]) :

Proposition 1.
The $\mathbb{Q}$-rational points on $\mathcal{C}_1$ are given by the set :

$$\mathcal{C}_1^{(1)}(\mathbb{Q}) = \{P_0\ ,\ P_1\ ,\ \overline{P}_1\ ,\ \infty\}.$$

The quadratic points on $\mathcal{C}_1$ over $\mathbb{Q}$ are given by the set :

$$\mathcal{C}_1^{(2)}(\mathbb{Q}) = \left\{Q_1\ ,\ Q_2\ ,\ \overline{Q}_1\ ,\ \overline{Q}_2\right\} \cup \left\{\left(a, \pm\sqrt{a^5+1}\ \right)\ \mid\ a \in \mathbb{Q}^{\text{ffl}*} \setminus \{-1\}\right\}$$

Proof. See [11]. □

1.2. Main result

Our main result describes the rational and quadratic points on the curves $\mathcal{C}_n$ is given by the following theorem :

Theorem 1. *Let n be a positive integer and $n \geq 2$.*

(**1**) *The $\mathbb{Q}$-rational points on $\mathcal{C}_n$ are given by the set :*

$$\bigcup_{n\geq 2} \mathcal{C}_n^{(1)}(\mathbb{Q}) = \left\{P_0\ ,\ P_1\ ,\ \overline{P}_1\ ,\ \infty\right\}.$$

(**2**) *The quadratic points on $\mathcal{C}_n$ over $\mathbb{Q}$ are given by the set :*

$$\bigcup_{n\geq 2} \mathcal{C}_n^{(2)}(\mathbb{Q}) = \left\{(0, y)\ \mid\ (y^2+1)(y^2+y+1)(y^2-y+1) = 0\right\}$$

2. Preliminary results

2.1. Algebraic extension

An algebraic extension is a field L/K such that every element of the larger field L is algebraic over the smaller field K ; that is, if every element of L is a root of a non-zero polynomial with coefficients in K. A field extension that is not algebraic, is said to be transcendental equation.
Let L be an extension field of K, and $a \in L$. If a is algebraic over K, then $K(a)$, the set of all polynomials in a with coefficients in K, is not only a ring but a field: $K(a)$ is an algebraic extension of K which has finite degree over K.
We have the classical lemma:

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

Proof. See [2]. □

2.2. Mordell-Weil group

Let j be the jacobian embedding $\mathcal{C} \to J_{\mathcal{C}}(\mathbb{Q})$. The class $[P - \infty]$ of $P - \infty$ is denoted $j(P)$. We have the following lemma :

Lemma 2. $J_{\mathcal{C}}(\mathbb{Q}) \cong (\mathbb{Z} \ / \ 10\mathbb{Z}) \cong \langle \ j(R_0) \ \rangle$.

Proof. See [11]. □

2.3. Cyclotomic polynomial

Definition 1. *Let n be a positive integer and ξ_n the complex number $exp(\frac{2i\pi}{n})$. The n^{th} cyclotomic polynomial is equal to*

$$\Phi_n(x) = \prod_{1 \leq k < n, k \wedge n = 1} \left(x - \xi_n^k\right)$$

An important relation linking cyclotomic polynomials and primitive roots of unity is given by this following lemma

Lemma 3. *For any n positive integer, the polynomial $P_n(x) = x^n - 1$ can be factored as:*

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

Proof. See [10] □

Remark 1. *We have the following properties*

- *For any positive integer n, the cyclotomic polynomials Φ_n are monic polynomials with integer coefficients that are irreducible over the field $\mathbb{Q}$ of the rational numbers.*
- *The degree of Φ_n , or in other words the number of nth primitive roots of unity, is $\varphi(n)$, where φ is Euler's quotient function.*
- *The only cyclotomic polynomials of degree at most 2 are the following:* $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$ *and* $\Phi_6(x) = x^2 - x + 1$.

2.4. Chevalley-Weil theorem

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

Theorem 2. *Let $\phi : X \longrightarrow Y$ 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*

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

Proof. See [7]. □

3. Proof of the main theorem

Let us consider the morphism

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

where n is an integer and $n \geq 1$. Thus, we have (See [9]):

$$\mathcal{C}_n^{(d)}(\mathbb{Q}) \subset f^{-1}\left(\bigcup_{1 \leq k \leq d} \mathcal{C}^{(k)}(\mathbb{Q})\right) \qquad and \qquad J_{\mathcal{C}_n}(\mathbb{Q}) \twoheadrightarrow J_{\mathcal{C}}(\mathbb{Q})$$

We know that $J_{\mathcal{C}}(\mathbb{Q})$ is finite and the curve $\mathcal{C}_1$ has been studied in [5]. The Chevalley-Weil theorem will allow us to determine some algebraic points on $\mathcal{C}_n$ from those on $\mathcal{C}_1$.

3.1. Rational points on $\mathcal{C}_n$ over $\mathbb{Q}$

We know in [11] that the $\mathbb{Q}$-rational points on $\mathcal{C}$ are given by :

$$\mathcal{C}^{(1)}(\mathbb{Q}) = \{P_0\ ,\ P_1\ ,\ \overline{P}_1\ ,\ \infty\}.$$

Then we have $\mathcal{C}_n^{(1)}(\mathbb{Q}) \subset f^{-1}\left(\{P_0,\ P_1,\ \overline{P}_1,\ \infty\}\right).$

$$f^{-1}\left(\{P_0,\ P_1,\ \overline{P}_1,\ \infty\}\right) = f^{-1}\left(\{P_0\}\right) \cup f^{-1}\left(\{P_1\}\right) \cup f^{-1}\left(\{\overline{P_1}\}\right) \cup f^{-1}\left(\{\infty\}\right)$$

We remark that if $n = 1$, the problem is solved in [11]. Let us suppose $n \geq 2$ and determine the rational points on the curves $\mathcal{C}_n$:

(1) The point $(x, y) \in f^{-1}(\{P_0\}) \Longleftrightarrow f(x, y) = (0, 0)$.
$f(x, y) = (0, 0) \Longleftrightarrow (x, y^n) = (0, 0) \Longleftrightarrow (x, y) = (0, 0)$.
So we get $f^{-1}(\{P_0\}) = \{P_0\}$.

(2) The point $(x, y) \in f^{-1}(\{P_1\}) \Longleftrightarrow f(x, y) = (0, 1)$.
$f(x, y) = (0, 1) \Longleftrightarrow (x, y^n) = (0, 1) \Longleftrightarrow x = 0$ et $y^n - 1 = 0$.
By the remark 1, $y^n - 1$ is divisible by the cyclotomic polynomials of degree 1 which are :
- $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$ if n is even,
- $\Phi_1(x) = x - 1$ if n is odd.
So we get $f^{-1}(\{P_1\}) = \left\{P_1,\ \overline{P_1}\right\}$.

(3) The point $(x, y) \in f^{-1}\left(\left\{\overline{P_1}\right\}\right) \Longleftrightarrow f(x, y) = (0, -1)$
$f(x, y) = (0, -1) \Longleftrightarrow (x, y^n) = (0, -1) \Longleftrightarrow x = 0$ and $y^n + 1 = 0$. By the remark 1, $y^n + 1$ is divisible by the cyclotomic polynomial of degree 1 which is $\Phi_2(x) = x + 1$ if n is odd.
So we get $f^{-1}\left(\left\{\overline{P_1}\right\}\right) = \left\{\overline{P_1}\right\}$.

(4) The point $(x, y) \in f^{-1}(\{\infty\}) \Leftrightarrow f(x, y) = (0, 1) = \infty$ and we find the case (2).

(5) The point at infinity of $\mathcal{C}_n$ noted ∞ is either $(1, 0)$ if $n \geq 3$ or $(0, 1)$ if $n \leq 2$ is a rational point.

We obtain then the set

$$\bigcup_{n \geq 2} \mathcal{C}_n^{(1)}(\mathbb{Q}) = \{P_0\ ,\ P_1\ ,\ \overline{P}_1\ ,\ \infty\}.$$

3.2. Quadratic points on $\mathcal{C}_n$

The quadratic points on $\mathcal{C}_1$ are given by :

$$\mathcal{C}^{(2)}(\mathbb{Q}) = \left\{Q_1\ ,\ Q_2\ ,\ \overline{Q}_1\ ,\ \overline{Q}_2\right\} \cup \left\{\left(a, \pm\sqrt{a^5 + 1}\ \right)\ \mid\ a \in \mathbb{Q}^* \setminus \{-1\}\right\}.$$

We get

$$\mathcal{C}_n^{(2)}(\mathbb{Q}) \subset f^{-1}\left(\mathcal{C}^{(1)}(\mathbb{Q}) \cup \mathcal{C}^{(2)}(\mathbb{Q})\right)$$

If $n = 1$, then the problem is solved [11]. We assume that $n \geq 2$. There are two different cases :

Case 1: We compute the quadratic points contained in $f^{-1}\left(\mathcal{C}^{(2)}(\mathbb{Q})\right)$.

(1) The point $(x, y) \in f^{-1}(\{Q_1\}) \Longleftrightarrow f(x, y) = Q_1 = (1 + i,\ 1 - 2i)$. We have $x = 1 + i$ and $y^n = 1 - 2i$. The equation $y^n = 1 - 2i$ has exactly n roots

$y_k = \sqrt[n]{1-2i}\xi_n^k$ with $0 \leq k \leq n-1$.
let be $R_k = \left(1+i,\ \sqrt[n]{1-2i}\xi_n^k\right)$ and Let's study of the point R_k. We have :

$$[\mathbb{Q}(R_k):\mathbb{Q}] = \left[\mathbb{Q}\left(1+i,\ \sqrt[n]{1-2i}\xi_n^k\right):\mathbb{Q}\right] \text{ et } 1+i \notin \mathbb{Q}.$$

$$n \geq 2 \Longrightarrow \left[\mathbb{Q}\left(1+i,\ \sqrt[n]{1-2i}\xi_n^k\right):\mathbb{Q}\right] > \left[\mathbb{Q}\left(\sqrt{1-2i}\right):\mathbb{Q}\right] = 4$$
$$\Longrightarrow \left[\mathbb{Q}\left(1+i,\ \sqrt[n]{1-2i}\xi_n^k\right):\mathbb{Q}\right] > 4.$$

The point $R_k = \left(1+i,\ \sqrt[n]{1-2i}\xi_n^k\right)$ has a degree greater than 2, and we show in the same way that the reciprocal images of the points $\overline{Q_1},\ Q_2$ and $\overline{Q_2}$ are also degree greater than 2.

(2) The point $(x,y) \in f^{-1}\left(\left\{\left(a, \pm\sqrt{a^5+1}\right)\right\}\right) \Leftrightarrow f(x,y) = \left(a, \pm\sqrt{a^5+1}\right)$ i.e $x = a$ and $y^n = \pm\sqrt{a^5+1}$. The equation $y^n = \pm\sqrt{a^5+1}$ has exactly n roots $y_k = \sqrt[n]{\pm\sqrt{a^5+1}}\xi_n^k$ with $0 \leq k \leq n-1$.
Let's study the degree of $R_{a,k} = \left(a,\ \sqrt[n]{\pm\sqrt{a^5+1}}\xi_n^k\right)$. We have :

$$[\mathbb{Q}(R_{a,k}):\mathbb{Q}] \geq [\mathbb{Q}(R_{a,0}):\mathbb{Q}] = \left[\mathbb{Q}\left(a,\ \sqrt[n]{\pm\sqrt{a^5+1}}\right):\mathbb{Q}\right].$$

In addition, $\mathbb{Q}(R_{a,0})$ contains $\mathbb{Q}(a)$ and $\mathbb{Q}\left(\sqrt[n]{\pm\sqrt{a^5+1}}\right)$ which are respectively fields of degree 1 and $2n$ with $n \geq 2$.
Let $n \geq 2$ and by the lemma 1, we have :

$$\left[\mathbb{Q}\left(a,\ \sqrt[n]{\pm\sqrt{a^5+1}}\right):\mathbb{Q}\right] = [\mathbb{Q}(a):\mathbb{Q}] \times \left[\mathbb{Q}\left(\sqrt[n]{\pm\sqrt{a^5+1}}\right):\mathbb{Q}\right] = 2n.$$

The point $R_{a,0} = \left(a,\ \sqrt[n]{\pm\sqrt{a^5+1}}\right)$ is a point of degree $2n > 2$.

So the set of quadratic points on $\mathcal{C}_n$ over $\mathbb{Q}$ in $f^{-1}\left(\mathcal{C}_n^{(2)}(\mathbb{Q})\right)$ is empty.

Case 2: Let us determine the quadratic points contained in $f^{-1}\left(\mathcal{C}^{(1)}(\mathbb{Q})\right)$:

(1) The point $(x,y) \in f^{-1}(\{P_0\}) \Longleftrightarrow f(x,y) = (0,0)$
$f(x,y) = (0,0) \Longleftrightarrow (x, y^n) = (0,0) \Longleftrightarrow x = 0$ and $y = 0$.
We see that P_0 is rational and therefore not of degree 2.

(2) The point $(x,y) \in f^{-1}(\{P_1\}) \Longleftrightarrow f(x,y) = (0,1)$.
$f(x,y) = (0,1) \Longleftrightarrow (x,y^n) = (0,1) \Longleftrightarrow x = 0$ and $y^n - 1 = 0$.
By remark 1, $y^n - 1$ is divisible by the cyclotomic polynomials of degree 2 which are
- $\Phi_3(y) = y^2 + y + 1$ if n is a multiple of 3;
- $\Phi_4(y) = y^2 + 1$ if n is a multiple of 4;
- $\Phi_6(y) = y^2 - y + 1$ if n is a multiple of 6.
So $f^{-1}(\{P_1\}) = \left\{(0,y) \mid (y^2+1)(y^2+y+1)(y^2-y+1) = 0\right\}$.

(3) The point $(x,y) \in f^{-1}\left(\left\{\overline{P_1}\right\}\right) \Longleftrightarrow f(x,y) = (0,-1)$.
$f(x,y) = (0,-1) \Longleftrightarrow (x,y^n) = (0,-1) \Longleftrightarrow x = 0$ et $y^n + 1 = 0$.
By remark 1, $y^n + 1$ is divisible by the cyclotomic polynomial of degree 2 which is $\Phi_2(y) = y^2 + 1$ if n is even.

So $f^{-1}\left(\{\overline{P_1}\}\right)=\left\{(0,y)\ \mid\ y \text{ root of the equation : } y^2+1=0\right\}$.

(4) The point $(x,y)\in f^{-1}(\{\infty\}) \Longleftrightarrow f(x,y)=(-1,0)=\infty$. We see that ∞ is rational so it is not of degree 2.

In summary, the set of quadratic points on the curves $\mathcal{C}_n$ over $\mathbb{Q}$ is given by

$$\bigcup_{n\geq 2}\mathcal{C}_n^{(2)}(\mathbb{Q})=\left\{(0,y)\ \mid\ (y^2+1)(y^2+y+1)(y^2-y+1)=0\right\}.$$

References

[1] Bruin, N. and Stoll, M., *The Mordell-Weil sieve : proving the nonexistence of Rational points on curves*, LMS Journal of Computing Mathematics **13**(2010), 272–306.

[2] Calais, J., *Field extensions, Galois theory, Level M1 - M2 (Extensions de corps, Théorie de Galois*, Niveau M1 - M2)(French), Mathématiques à l'Université, Paris: Ellipses (ISBN 2 - 7298 - 2780 - 3 / pbk), xii, 218 p., 2006.

[3] Coleman, R.F., *Effective Chabauty method*, Duke Math. J. **52**(1985), No. 3, 765–770.

[4] Debarre, O., Klassen, M., *Points of low degree on smooth plane curves*, J. Reine Angew. Math., **446**(1994), 81–87.

[5] Fall, M., Sall, O., *Points algébriques de petits degrés sur la courbe d'équation affine* $y^2=x^5+1$,, Afrika Matematika **29**(2018), 1151–1157.

[6] Faltings, G., *Finiteness theorems for abelian varieties over number fields*, (Endlichkeitssätze für abelscheVarietäten über Zahlkörpern)(German), Invent. Math. **73**(1983), No. 3, 349–366.

[7] Hindry, M, Silverman, J., *Diophantine geometry, an introduction*, Springer-Verlag, New York, (2000), Graduate Texts Mathematics, 201.

[8] Sall, O., *Points algébriques sur certains quotients de courbes de Fermat*, C.R. Acad. Sci. Paris, Sér I, **336**(2003), 117–120.

[9] Sall, O., Fall, M., Top, T., *Points algébriques de petits degrés sur les courbes* $\mathcal{C}_n$ *d'équation affine* $y^{3n}=x(x-1)(x-2)(x-3)$, Annales Mathématiques Africaines, **5**(2015), 25–28.

[10] Perrin, D., *Cours d'algèbre*, Ellipses, p. 79, 1996.

[11] Schaefer, E.F., *Computing a Selmer group of Jacobian using functions on the curve*, Math. Ann., **310**(1998), 447–471.

[12] Siksek, S. and Stoll, M., *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.

University of Assane SECK
Department of Mathematics
DIabir, BP 523, Ziguinchor, Senegal
E-mail address: m.fall@univ-zig.sn
E-mail address: p.sarr597@zig.univ.sn
E-mail address: elpythasow@yahoo.fr