ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 12, Issue, 01, pp. 53106-53110, January, 2022
https://doi.org/10.37118/ijdr.23634.01.2022

RESEARCH ARTICLE OPEN ACCESS

DÉTERMINATION DES POINTS ALGÉBRIQUES DE DEGRÉ DONNE QUELCONQUE SUR LA COURBE D'ÉQUATION AFFINE $y^2 = x^3 - 8x^2 + x$.

Mohamadou Mor Diogou Diallo[1], Boubacar Balde[2] and Oumar Sall[3]

U.F.R des Sciences et Technologies, Université Assane Seck de Ziguinchor, Senegal

ARTICLE INFO

Article History:
Received 09th October, 2021
Received in revised form
17th November, 2021
Accepted 29th December, 2021
Published online 28th January, 2022

Key Words:

Mordell-Weil Group,
Jacobian, Galois Conjugates

Corresponding author:
Ana Paula Fidelis de Oliveira Santos

ABSTRACT

We determine explicitly the set of algebraic points of given degreeover $\mathbb{Q}$ on the affine curve $y^2 = x^3 - 8x^2 + x$mentioned in ([Fly, page 207]). where, we have shown that the Mordell-Weil group of this curve is finite. This note treat a special case of elliptic curves $C : y^2 = (x - e_1)(x - e_2)(x - e_3)$These curves are described by Leopoldo KULESZ in ([Kul, page 107]).

Citation: ***Mohamadou Mor Diogou Diallo, Boubacar Balde and Oumar Sall.*** "Détermination des points algébriques de degré donne quelconque sur la courbe d'équation affine $y^2 = x^3 - 8x^2 + x$", *International Journal of Development Research*, 12, (01), 53106-53110.

INTRODUCTION

Soit $\mathcal{C}$ une courbe algébrique projective définie sur $\mathbb{Q}$. Pour tout corps de nombres $\mathbb{K}$, on note $\mathcal{C}(\mathbb{K})$ l'ensemble des points sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ et $\bigcup_{[\mathbb{Q}(R):\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K})$ l'ensembledes points sur $\mathcal{C}$ à coordonnées dans $\mathbb{K}$ de degré au-plus l sur $\mathbb{Q}$. Le degré d'un point R est le degré de son corps de définition sur $\mathbb{Q}$, c'est-à-dire qu'on a $deg(R) = [\mathbb{Q}(R):\mathbb{Q}]$. On désignera par □ la jacobienne de $\mathcal{C}$ et par j(P) la classe notée $[P - P_\infty]$ de $P - P_\infty$, c'est à dire que j est le plongement jacobien :

$$j: C \longrightarrow (\mathbb{Q}) ; \quad P \mapsto [P - P_\infty]$$

où $(\mathbb{Q})$ représente le groupe de Mordell-Weil des points rationnels de la jacobienne de $\mathcal{C}$; ce groupe est fini (voir [Fly, page 287]).
Notre courbe $\mathcal{C}$ qui est lisse d'équation affine $y^2 = x^3 - 8x^2 + x$est un cas spécial de famille de courbes

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3)$$

étudiées dans [Kul, page 107]. Notre courbe $\mathcal{C}$ a pour équation projective $ZY^2 = X(X - (4 - \sqrt{15})Z)(X - (4 + \sqrt{15})Z)$, on note P_0, P_1, P_2 et P_∞ les points de $\mathcal{C}$, définis par : $P_0 = [0 : 0 : 1]$, $P_1 = [4 - \sqrt{15} : 0 : 1]$, $P_2 = [4 + \sqrt{15} : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$.

Dans cette note, on détermine l'ensemble :

$\bigcup_{[\mathbb{Q}(R):\,\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K})$

Notre résultat principal est donné par :

Théorème

L'ensemble des points algébriques de degré au plus l sur $\mathbb{Q}$ sur la courbe $\mathcal{C}$ est donné par : $\bigcup_{[\mathbb{Q}(R):\,\mathbb{Q}]\leq l} \mathcal{C}(\mathbb{K}) = \mathcal{F}_1 \cup \mathcal{F}_2$avec

$$\mathcal{F}_1 = \left\{ \left(x, -\frac{\sum_{i=0}^{\frac{l}{2}} a_i x^i}{\sum_{j=0}^{\frac{l-3}{2}} b_j x^j} \right) \middle| \begin{array}{c} (a_0 \wedge b_0) \neq 0, \quad a_{\frac{l}{2}} \neq 0 \ si \ \ l \text{ est pair}, b_{\frac{l-3}{2}} \neq 0 \text{ si } l \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{l}{2}} a_i x^i \right)^2 = \left(\sum_{j=0}^{\frac{l-3}{2}} b_j x^j \right)^2 (x^3 - 8x^2 + x) \end{array} \right\}$$

$$\mathcal{F}_2 = \left\{ \left(x, -\frac{\sum_{i=1}^{\frac{l+1}{2}} a_i \, (x^i + n^i)}{\sum_{j=0}^{\frac{l-2}{2}} b_j x^j} \right) \middle| \begin{array}{c} b_0 \neq 0, \quad a_{\frac{l+1}{2}} \neq 0 \ si \ \ l \text{ est pair}, b_{\frac{l-2}{2}} \neq 0 \text{ si } l \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \\ \left(\sum_{i=1}^{\frac{l+1}{2}} a_i x^{i-\frac{1}{2}} \right)^2 = \left(\sum_{j=0}^{\frac{l-2}{2}} b_j x^j \right)^2 \left(x - \left(4 - \sqrt{15}\right)\right)\left(x - \left(4 + \sqrt{15}\right)\right) \end{array} \right\}$$

RÉSULTATS AUXILIAIRES

Pour un diviseur $\mathfrak{D}$sur $\mathcal{C}$, on note $\mathcal{L}(\mathfrak{D})$ le $\overline{\mathbb{Q}}$-espace vectoriel des fonctions rationnelles $f$définies sur $\mathbb{Q}$ telles que $f = 0$ ou $div(f) \geq -\mathfrak{D}$;$\ell(\mathfrak{D})$\$ désigne la $\overline{\mathbb{Q}}$-dimension de $\mathcal{L}(\mathfrak{D})$.

Lemme 1 On a: $(\mathbb{Q}) \cong {}^{\mathbb{Z}}/_{2\mathbb{Z}}$

Démonstration: (voir [Fly, page 272])

Lemme 2 Pour la courbe$\mathcal{C}$: $y^2 = x^3 - 8x^2 + x$, on a :

- $div(x) = 2P_0 - 2P_\infty$,
- $div\left(x - \left(4 - \sqrt{15}\right)\right) = 2P_1 - 2P_\infty$,
- $div\left(x - \left(4 + \sqrt{15}\right)\right) = 2P_2 - 2P_\infty$,
- $div(y) = P_0 + P_1 + P_2 - 3P_\infty$.

Démonstration: Considérons$x$, y les coordonnées affine de la courbe $\mathcal{C}$ définie par : $x = \frac{X}{Z}$et $y = \frac{Y}{Z}$.

L'équation projective de la courbe $\mathcal{C}$ est définie par : $\left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^3 - 8\left(\frac{X}{Z}\right)^2 + \left(\frac{X}{Z}\right)$.

Cette équation devient: $ZY^2 = X\left(X - \left(4 - \sqrt{15}\right)Z\right)\left(X - \left(4 + \sqrt{15}\right)Z\right)$.

- **Calculons $div(x)$.**

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

- Pour $X = 0$, implique que : $Y^2 = 0$ ou $Z = 0$. On obtient donc les points $P_0 = [0 : 0 : 1]$ et $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égale à respectivement 2 et 1. D'où

$(X = 0) \cdot \mathcal{C} = 2P_0 + P_\infty$ (0.1)

- De même pour $Z = 0$, cela implique : $X^3 = 0$. On obtient donc le point $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égale 3. D'où

$(Z = 0) \cdot \mathcal{C} = 3P_\infty$(0.2)

Des relations (0.1) et (0.2), induisent que : $div(x) = 2P_0 - 2P_\infty$.

- Calculons $div\left(x - \left(4 - \sqrt{15}\right)\right)$.
  Notons tout d'abord que :

$div\,(x - \gamma) = div(X - \gamma Z) - div(Z) = (X = \gamma Z) \cdot \mathcal{C} - (Z = 0) \cdot \mathcal{C}$.
On a:
$div\left(x - \left(4 - \sqrt{15}\right)\right) = \left(X = \left(4 - \sqrt{15}\right)Z\right) \cdot \mathcal{C} - (Z = 0) \cdot \mathcal{C}$.

- Pour $X = \left(4 - \sqrt{15}\right)Z$, implique que : $Y^2 = 0$ ou $Z = 0$. On obtient donc les points $P_1 = \left[4 - \sqrt{15} : 0 : 1\right]$ et $P_\infty = [0 : 1 : 0]$ avec un ordre multiplicité égale à respectivement 2 et 1. D'où

$\left(X = \left(4 - \sqrt{15}\right)Z\right) \cdot \mathcal{C} = 2P_0 + P_\infty$(0.3)

- De même pour $Z = 0$, on obtient donc la relation (0.2). Des relations (0.2) et (0.3), induisent que : $div\left(x - \left(4 - \sqrt{15}\right)\right) = 2P_1 - 2P_\infty$.

NB : On procède de la même maniéré pour iii).

Calculons $div(y)$.

$$div(y) = div\left(\frac{Y}{Z}\right) = (Y = 0) \cdot \mathcal{C} - (Z = 0) \cdot \mathcal{C}$$

- Pour $Y = 0$, on a déduit que : $X\left(X - \left(4 - \sqrt{15}\right)Z\right)\left(X - \left(4 + \sqrt{15}\right)Z\right) = 0$. On obtient donc les points $P_0 = [0 : 0 : 1]$, $P_1 = \left[4 - \sqrt{15} : 0 : 1\right]$ et $P_2 = \left[4 + \sqrt{15} : 0 : 1\right]$ avec un ordre multiplicité égale 1 pour chacun des points. D'où

$(Y = 0) \cdot \mathcal{C} = P_0 + P_1 + P_2$

- Pour $Z = 0$, revient à l'obtention de la relation (0.2). Ainsi des relations (0.2) et (0.5), entraînent donc que : $div(y) = P_0 + P_1 + P_2 - 3P_\infty$

Corollaire

Les résultats suivants sont des conséquences du lemme 2 :

- $j(P_0) = -(j(P_1) + j(P_2))$,
- $2j(P_0) = 2j(P_1) = 2j(P_2) = 0$

Lemme 3: On a : $(\mathbb{Q}) = < j(P_0) >$

Lemme 4 : Une $\mathbb{Q}$-base de $\mathcal{L}(mP_\infty)$ est donnée par :

$$\mathfrak{B}_m = \left\{x^i, \quad 0 \le i \le \frac{m}{2}\right\} \bigcup \left\{ yx^j, \quad 0 \le j \le \frac{m-3}{2}\right\}$$

Démonstration: On montre aisément que $\mathfrak{B}_m$ est une famille libre, il reste alors à montrer que $\text{card}\mathfrak{B}_m = dim\,\mathcal{L}(mP_\infty)$. La courbe étant de genre 1, d'après le théorème de Riemann-Roch, on a : $\dim \mathcal{L}(mP_\infty) = m - g + 1 = m$ dès que $m \ge 2g - 1 = 1$. Deux cas sont possibles :

- 1er cas : supposons que m soit pair, on pose alors $m = 2h$, on obtient ainsi : $i \le \frac{m}{2} \Leftrightarrow i \le \frac{2h}{2} = h$ même $j \le \frac{m-3}{2} \Leftrightarrow j \le \frac{2h-3}{2} \Leftrightarrow j < h - 1 \Leftrightarrow j \le h - 2$. Donc on a :

$\mathfrak{B}_m = \{1, x, \ldots\ldots\ldots, x^h\} \cup \{1, yx, \ldots\ldots\ldots, yx^{h-2}\}$ On en déduit que : $\text{card}\,\mathfrak{B}_m = h + 1 + h - 2 + 1 = 2h = m = \dim\,\mathcal{L}(mP_\infty)$.

- 2éme cas : supposons que m soit impair, on pose alors $m = 2h + 1$, on obtient ainsi : $i \le \frac{m}{2} \Leftrightarrow i \le \frac{2h+1}{2} \Leftrightarrow i \le h + \frac{1}{2} \Rightarrow i < h + 1 \Rightarrow i \le h$ de même

$$j \le \frac{m-3}{2} \Leftrightarrow j \le \frac{2h-2}{2} = h - 1$$

Donc on a:

$\mathfrak{B}_m = \{1, \quad x, \ldots\ldots\ldots, \quad x^h\} \bigcup \{1, \quad yx, \ldots\ldots\ldots, \quad yx^{h-1}\}$

On en déduit que: card $\mathfrak{B}_m = h + 1 + h - 1 + 1 = 2h + 1 = m = \dim \mathcal{L}(mP_\infty)$.

Démonstration du Théorème: Soit $R \in \mathcal{C}(\mathbb{Q})$ avec $[\mathbb{Q}(R): \mathbb{Q}] = l$. Considérons $R_1, \ldots\ldots\ldots, R_l$ les conjugués de Galois de R et notons $t = [R_1 + \ldots\ldots\ldots + R_l - lP_\infty] \in (\mathbb{Q}) = \{\alpha\, j(P_0), \text{ avec } \alpha \in \{0\ ,\ 1\}\}$ donc $t = \alpha\, j(P_0)$, avec $\alpha \in \{0\ ,\ 1\}$, ce qui donne la formule suivante

$[\ t = [R_1 + \ldots\ldots\ldots + R_l - lP_\infty] = \{\alpha\, j(P_0), \text{ avec } \alpha \in \{0\ ,\ 1\}\}$ (*)

Deux cas sont possibles:

1er cas : $\alpha = 0$:

La formule $(\star)$ devient : $[R_1 + \ldots\ldots\ldots + R_l - \alpha P_0 - (l + \alpha)P\infty] = 0$, D'après le théorème d'Abel Jacobi ([Gri, page 156]), il existe une fonction rationnelle sur $\mathbb{Q}$ telle que: div(f) = $R_1 + \ldots\ldots\ldots + R_l$ - lP∞, donc $f \in \mathcal{L}(lP_\infty)$ d'après le Lemme 4, on a : $f = \sum_{i=0}^{\frac{l}{2}} a_i x^i + \sum_{j=0}^{\frac{l-3}{2}} b_j y x^j$ avec a_0 et b_0 non simultanément nuls (sinon un des R_i devrait être égal à P_0, ce qui serait absurde), $a_{\frac{l}{2}} \neq 0$ si l est pair (sinon un des un des R_i devrait être égal à P_∞, ce qui serait absurde) et $b_{\frac{l-3}{2}} \neq 0$ $ si l est pair (sinon un des un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux point R_i, on a : $\sum_{i=0}^{\frac{l}{2}} a_i x^i + \sum_{j=0}^{\frac{l-3}{2}} b_j y x^j = 0$, qui donne :$y = -\frac{\sum_{i=0}^{\frac{l}{2}} a_i x^i}{\sum_{j=0}^{\frac{l-3}{2}} b_j x^j}$

En remplaçant l'expression de y dans $y^2 = x^3 - 8x^2 + x$, on en déduit que :

$$\left(\sum_{i=0}^{\frac{l}{2}} a_i x^i\right)^2 = \left(\sum_{j=0}^{\frac{l-3}{2}} b_j x^j\right)^2 (x^3 - 8x^2 + x)(0.5)$$

L'équation (0.5) est une équation de degré l en x ; en effet: Pour l pair (ou impair), le premier membre de l'équation est de degré égal à $2 \times \left(\frac{l}{2}\right) = l$

et le second membre de l'équation est de degré égal à $2 \times \left(\frac{l-3}{2}\right) + 3 = l$.

On obtient ainsi une famille de points de degré l :

$$\mathcal{F}_1 = \left\{ \left(x, -\frac{\sum_{i=0}^{\frac{l}{2}} a_i x^i}{\sum_{j=0}^{\frac{l-3}{2}} b_j x^j} \right) \middle| \begin{array}{c} (a_0 \wedge b_0) \neq 0, \quad a_{\frac{l}{2}} \neq 0 \ si \ \ l \text{ est pair, } b_{\frac{l-3}{2}} \neq 0 \text{ si } l \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \\ \left(\sum_{i=0}^{\frac{l}{2}} a_i x^i\right)^2 = \left(\sum_{j=0}^{\frac{l-3}{2}} b_j x^j\right)^2 (x^3 - 8x^2 + x) \end{array} \right\}$$

2er cas : $\alpha = 1$

La formule $(\star)$ devient: $R_1 + \ldots\ldots\ldots + R_l + lP_\infty] = j(P_0)$, du corolaire on en déduit que [$R_1 + \ldots\ldots\ldots + R_l + P_1 + P_2\ (l+2)\ P\infty] = 0$, D'après le théorème d'Abel Jacobi, il existe une fonction rationnelle sur $\mathbb{Q}$ telle que : *div (f) = R_1+ ... .+ R_l + P_1 + P_2 – (l+2)* P∞, donc $f \in \mathcal{L}((l+1)P_\infty)$ d'après le Lemme 4, on a : $f = \sum_{i=0}^{\frac{l+1}{2}} a_i x^i + \sum_{j=0}^{\frac{l-2}{2}} b_j y x^j$, et puisque $ord_{P_0} f = 1$, donc$f(P_0) = 0$ entraîne donc que $a_0 = 0$, impliquant ainsi donc que $f = \sum_{i=1}^{\frac{l+1}{2}} a_i x^i + \sum_{j=0}^{\frac{l-2}{2}} b_j y x^j$ avec $b_0 \neq 0$ (sinon un des R_i devrait être égal à P_0, ce qui serait absurde) , $a_{\frac{l+1}{2}} \neq 0$ si l est pair (sinon un des un des R_i devrait être égal à P_∞, ce qui serait absurde) et $b_{\frac{l-2}{2}} \neq 0$ si l est pair (sinon un des un des R_i devrait être égal à P_∞, ce qui serait absurde). Aux point R_i, on a : $\sum_{i=0}^{\frac{l+1}{2}} a_i x^i + \sum_{j=0}^{\frac{l-2}{2}} b_j y x^j = 0$, qui donne : $y = -\frac{\sum_{i=0}^{\frac{l+1}{2}} a_i x^i}{\sum_{j=0}^{\frac{l-2}{2}} b_j x^j}$. En remplaçant l'expression de y dans $y^2 = x^3 - 8x^2 + x$, on en déduit que :

$$\left(\sum_{i=1}^{\frac{l+2}{2}} a_i (x^i + ni)\right)^2 = \left(\sum_{j=0}^{\frac{l-1}{2}} b_j x^j\right)^2 (x^3 - 8x^2 + x)$$

Cette équation équivaux à :

$$\left(\sum_{i=1}^{\frac{l+1}{2}} a_i = \left(\frac{x^i + n_i}{x}\right)\right)^2 = \left(\sum_{j=0}^{\frac{l-1}{2}} b_j x^{j-1}\right)^2 \left(x - \left(4 - \sqrt{15}\right)\right)\left(x - \left(4 + \sqrt{15}\right)\right) (0.6)$$

L'équation (0.6) est une équation de degré l en x ; en effet : Pour l pair (ou impair), le premier membre de l'équation est de degré égal à

$2 \times \left(\frac{l+2}{2} - \frac{1}{2}\right) = l$et le second membre de l'équation est de degré égal à

$2 \times \left(\frac{l-1}{2}\right) + 2 = l$.

On obtient ainsi une famille de points de degré l :

$$\mathcal{F}_2 = \left\{ \left(x, -\frac{\sum_{i=1}^{\frac{l+2}{2}} a_i (x^i + n_i)}{\sum_{j=0}^{\frac{l-1}{2}} b_j x^j} \right) \middle| \begin{array}{c} b_0 \neq 0,\ a_{\frac{l+1}{2}} \neq 0 \ si \ \ l \text{ est pair, } b_{\frac{l-2}{2}} \neq 0 \text{ si } l \text{ est} \\ \text{impair et } x \text{ solution de l'équation :} \\ \left(\sum_{i=1}^{\frac{l+1}{2}} a_i x^{i-\frac{1}{2}}\right)^2 = \left(\sum_{j=0}^{\frac{l-2}{2}} b_j x^j\right)^2 \left(x - \left(4 - \sqrt{15}\right)\right)\left(x - \left(4 + \sqrt{15}\right)\right) \end{array} \right\}$$

REFERENCES

[Fly] Bruin N. & Flynn E.V : *Exhibiting SHA[2] on hyperelliptic Jacobians*, Journal of Number Theory 118 (2006) 266 - 291.
[Gri] Griffiths P.A : *Introduction to algebric curves*, Translation mathematical monograhs volume 76. (1989).
[Kul] Kulesz L. : *Courbes algébriques de genre ≥ 2 possédant de nombreux pointsrationnels*, ACTA Arithmetica LXXXVII.2 (1998) 103 - 120.
[SAL] O. Sall : *Points algébriques sur certains quotients de courbes de Fermat*, C. R.Acad. Sci. Paris Ser. I 336 (2003) 117 –120.

****