Introduction

Étant donnés un nombre premier $p \geq 7$ et un entier naturel non nul c sans facteurs carrés, on s'intéresse à l'étude de l'équation diophantienne

$$x^p - y^p = cz^2. \tag{1}$$

Dans ce travail, une solution $(x, y, z) \in \mathbb{Z}^3$ de l'équation (1) sera dite *propre* si l'on a $\mathrm{pgcd}(x, y, z) = 1$, et *non triviale* si xyz n'est pas nul. On note $S_p(c)$ l'ensemble des solutions propres non triviales de l'équation (1). C'est un ensemble fini.

Il résulte des travaux de H. Darmon et L. Merel que $S_p(1)$ est vide (cf. [6]). De plus, on a $S_p(2) = \{(1, -1, -1), (1, -1, 1)\}$ (cf. [10]). On considère ici l'ensemble $\mathfrak{N}_p$ des entiers $c \geq 3$, sans facteurs carrés, possédant la propriété suivante :

$$\text{pour tout diviseur premier } \ell \text{ de } c, \text{ on a } \ell \not\equiv 1 \bmod p. \tag{2}$$

On obtient quelques résultats nouveaux sur la question ci-dessous, qui est un cas particulier de celle posée dans [12] :

QUESTION 1. Soit p un nombre premier ≥ 7. Existe-t-il un entier $c \in \mathfrak{N}_p$ tel que $S_p(c)$ soit non vide ?

L'analogue de cette question avec $p = 3$ ou $p = 5$ a une réponse positive. À titre indicatif, on a les égalités suivantes :

$$11^3 - 2^3 = 3 \cdot 21^2, \qquad 8^5 + 11^5 = 19 \cdot 101^2.$$

En fait, si $p = 3$ ou $p = 5$, il est plausible de penser qu'il existe une infinité d'entiers $c \in \mathfrak{N}_p$ tel que $S_p(c)$ soit non vide (cf. [12]). En revanche, on ne connaît pas d'exemples d'entiers $c \in \mathfrak{N}_p$ répondant positivement à la question 1. Il est démontré dans [12] les résultats suivants :

1. Pour tout $p \geq 7$, l'ensemble des entiers $c \in \mathfrak{N}_p$ tels que $S_p(c)$ soit non vide est fini.
2. Supposons $p \in \{5, 7\}$. Pour tout $c \in \mathfrak{N}_p$ divisible par p, l'ensemble $S_p(c)$ est vide.

De plus, dans le cas où p est égal à 7, il a été démontré indépendamment par G. Walsh et W. Ivorra que l'ensemble $S_7(c)$ est vide pour tout c appartenant à $\mathfrak{N}_p$ (cf. [16] et [11, chap. IV]).

On va prouver ici le résultat suivant :

THÉORÈME 1. *Supposons que $p \in \{11, 13, 17\}$. Alors, pour tout $c \in \mathfrak{N}_p$ l'ensemble $S_p(c)$ est vide.*

Au vu de ces résultats et de certaines constatations numériques il est tentant de conjecturer que la réponse à la question 1 est négative dès que p est plus grand qu'une

constante absolue. Néanmoins, on ne sait pas démontrer par exemple que la conjecture (abc) entraîne cette assertion.

Notons $\Phi_p(X) \in \mathbb{Z}[X]$ le p-ième polynôme cyclotomique. On a $\Phi_p(X) = \sum_{k=0}^{n-1} X^k$. Soient $C_p/\mathbb{Q}$ et $D_p/\mathbb{Q}$ les courbes hyperelliptiques d'équations

$$C_p : y^2 = \Phi_p(x), \qquad D_p : py^2 = \Phi_p(x).$$

Ce sont des courbes de genre $(p-3)/2$.

L'étude de la question 1 se ramène en fait à la détermination des points rationnels sur $\mathbb{Q}$ de C_p et D_p ([12, lemme 1]). Rappelons quelle en est la raison : soient c un entier de $\mathfrak{N}_p$ et (u,v,w) un élément de $S_p(c)$. Un nombre premier ℓ qui divise $u^p - v^p$ sans diviser $u-v$ est congru à 1 modulo p ; en effet, ℓ ne divise pas v et p est l'ordre de $u/v \bmod \ell$ dans $\mathbb{F}_\ell^*$. Il en résulte que c divise $u-v$. On a $u \neq v$. Posons

$$\Phi_p(u,v) = \frac{u^p - v^p}{u-v}.$$

Les entiers $u-v$ et $\Phi_p(u,v)$ sont premiers entre eux en dehors de p et l'on a $\Phi_p(u,v) \geq 0$. On en déduit l'existence d'un entier s tel que

$$\Phi_p(u,v) = s^2 \quad \text{ou} \quad \Phi_p(u,v) = ps^2.$$

Par suite, en posant

$$x = \frac{u}{v}, \qquad y = \frac{s}{v^{(p-1)/2}}, \tag{3}$$

on constate que (x,y) appartient à $C_p(\mathbb{Q})$ ou à $D_p(\mathbb{Q})$. D'où notre assertion. Si $p \geq 7$, les courbes C_p et D_p sont de genre ≥ 2, donc les ensembles $C_p(\mathbb{Q})$ et $D_p(\mathbb{Q})$ sont finis. On démontre dans cette direction l'énoncé suivant :

THÉORÈME 2. *Supposons que $p \in \{11, 13, 17\}$. On a alors*

$$C_p(\mathbb{Q}) = \{(-1,-1),(-1,1),(0,-1),(0,1)\}, \qquad D_p(\mathbb{Q}) = \{(1,-1),(1,1)\}. \tag{4}$$

Ajoutons que ce théorème reste vrai dans le cas où $p = 7$ (cf. [12], [16] et [11, chap. IV]), c'est-à-dire que l'on a

$$C_7(\mathbb{Q}) = \{(-1,-1),(-1,1),(0,-1),(0,1)\} \quad \text{et} \quad D_7(\mathbb{Q}) = \{(1,-1),(1,1)\}.$$

Ces résultats et le théorème 2 suggèrent en fait de poser la question suivante :

QUESTION 2. Les égalités (4) sont-elles valables pour tout $p \geq 7$?

Si les égalités (4) sont vraies pour un nombre premier $p \geq 7$, alors pour tout $c \in \mathfrak{N}_p$ l'ensemble $S_p(c)$ est vide : considérons en effet un entier $c \in \mathfrak{N}_p$ et supposons qu'il existe un élément $(u,v,w) \in S_p(c)$. Les entiers u et v sont premiers entre eux. D'après les égalités (3) et (4), on a donc $u = 0$ ou bien $uv = \pm 1$. La condition $uv = \pm 1$ conduit à $c = 2$ ou $w = 0$. On obtient ainsi une contradiction et notre assertion. En particulier, le théorème 2 entraîne le théorème 1. Toute la suite est consacrée à la démonstration du théorème 2.

Je souhaite remercier A. Kraus pour l'aide qu'il m'a apportée pendant l'élaboration de ce travail.

1. Principe de démonstration du théorème 2

Le principe de démonstration que l'on utilise est le même pour la description de $C_p(\mathbb{Q})$ et de $D_p(\mathbb{Q})$. Voici comment l'on procède pour déterminer $C_p(\mathbb{Q})$.

On commence par expliciter, dans le paragraphe 2, deux courbes hyperelliptiques $Y_p/\mathbb{Q}$ et $Z_p/\mathbb{Q}$ et deux applications rationnelles définies sur $\mathbb{Q}$ de degré 2 :

$$\varphi_1 : C_p \to Y_p, \quad \varphi_2 : C_p \to Z_p.$$

Soit $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$. Pour tout point $P = (x, y) \in C_p(\overline{\mathbb{Q}})$ tel que $x \neq 0$, les abscisses de $\varphi_1(P)$ et de $\varphi_2(P)$ sont égales à $(x^2 + 1)/x$. On décrit dans la suite les images $\varphi_1(C_p(\mathbb{Q}))$ et $\varphi_2(C_p(\mathbb{Q}))$, ce qui permet alors de démontrer directement notre résultat.

Soit ζ un générateur du sous-groupe μ_p des racines p-ièmes de l'unité de $\overline{\mathbb{Q}}^*$. Posons $m = (p-1)/2$ et notons G_m le polynôme minimal sur $\mathbb{Q}$ de $\zeta + \zeta^{-1}$. C'est un polynôme unitaire de $\mathbb{Z}[X]$, de degré m, qui définit le sous-corps réel maximal $\mathbb{Q}(\mu_p)^+$ du corps $\mathbb{Q}(\mu_p)$. Soit $G_m(X, Y) \in \mathbb{Z}[X, Y]$ l'homogénéisé de G_m : on a $G_m(X, Y) = Y^m G_m(X/Y)$. Considérons un point $M = (\alpha, \beta)$ appartenant par exemple à $\varphi_1(C_p(\mathbb{Q}))$ et posons

$$\alpha = s/t,$$

où s et t sont deux entiers premiers entre eux. On démontre dans la proposition 3.1 qu'en changeant au besoin (s, t) en $-(s, t)$, la condition suivante est satisfaite :

$$s^2 - 4t^2 \in \mathbb{Z}^2 \quad \text{et} \quad G_m(s, t) \in \mathbb{Z}^2.$$

On choisit ensuite un sous-corps K convenable de $\mathbb{Q}(\mu_p)^+$ sur lequel on factorise le polynôme $G_m(X, Y)$ en produit de polynômes irréductibles sur K. Soit A l'anneau des entiers de K. On obtient une décomposition de $G_m(s, t)$ en un produit d'éléments $F_i \in A$ qui sont conjugués sur $\mathbb{Q}$ et qui dépendent de s et t. En utilisant le fait que $G_m(s, t)$ est un carré dans $\mathbb{Z}$, on vérifie alors que les F_i sont, à des unités près, des carrés dans K. On en déduit l'existence d'un polynôme homogène non nul $P(X, Y) \in A[X, Y]$ de degré 4 (qui *a priori* n'est pas unique) tel que

$$P(s, t) \in A^2. \tag{5}$$

On a $\alpha \neq 0$ et il résulte de (5) que $1/\alpha$ est l'abscisse d'un point rationnel sur K d'une quartique $\mathcal{D}/K$ donnée par une équation de la forme

$$v^2 = au^4 + bu^3 + cu^2 + du + e \quad \text{avec } a, b, c, d \in A \text{ et } e \in \{0, 1\}.$$

On est ainsi amené à rechercher l'ensemble des points $(u, v) \in \mathcal{D}(K)$ tels que u appartienne à $\mathbb{Q}$. La méthode de Chabauty elliptique permet dans notre situation de le déterminer. La démarche que l'on a suivie dans son application est précisée dans les appendices A et B. Signalons que les travaux de N. Bruin et E. V. Flynn contiennent des exposés plus généraux de la méthode de Chabauty (cf. [3] et [5]). Les techniques développées dans ces articles ont été implémentées sur le logiciel Magma et le lecteur pourra trouver dans [4] un exemple d'utilisation de ce logiciel pour résoudre des équations diophantiennes ternaires de signature $(n, n, 2)$.

La désingularisée de $\mathcal{D}/K$ est une courbe elliptique E/K. On explicite dans l'appendice A une équation de Weierstrass de E/K de la forme

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

où les $a_i \in A$ sont fonctions de a, b, c et d, et l'on décrit un isomorphisme birationnel défini sur K entre E et $\mathcal{D}$, i.e. un isomorphisme ψ sur K d'un ouvert de E sur un ouvert de $\mathcal{D}$: pour tout $N = (x, y) \in E(\overline{\mathbb{Q}})$, on a $\psi(N) = (u, v)$ où u et v sont des fractions rationnelles en x et y. En considérant l'application de première projection sur $\mathcal{D}$, on obtient ainsi une fonction sur E, que l'on note encore u, dont la définition se trouve dans le paragraphe 3 de l'appendice A. Notre problème est alors équivalent à la recherche des points $N \in E(K)$ pour lesquels $u(N)$ appartient à $\mathbb{Q}$. Dans l'appendice B, on décrit la façon dont on applique la méthode de Chabauty elliptique pour résoudre ce problème.

Tous les calculs nécessaires à la démonstration du théorème 2 ont été effectués à l'aide du logiciel PARI ([1]). Dans le formulaire, il se trouve, pour chacun des nombres premiers intervenant dans l'énoncé du théorème, des tableaux qui fournissent les informations suivantes :

1) les données arithmétiques de K utilisées : un élément primitif de $K/\mathbb{Q}$, ses conjugués sur $\mathbb{Q}$, une $\mathbb{Z}$-base de A, un système d'unités fondamentales u_i de A, qui figure dans la ligne «unités» du tableau, leurs normes $N_{K/\mathbb{Q}}(u_i)$ de K sur $\mathbb{Q}$. Pour chacun des corps K envisagés, l'anneau d'entiers A est principal, nous omettons ainsi cette information dans les tableaux. On fournit par ailleurs des générateurs de certains idéaux premiers de A ; par exemple, l'égalité $2A = \mathfrak{p}_2$ signifie que $2A$ est un idéal premier $\mathfrak{p}_2$ de A. On indique aussi la factorisation de $G_m(s, t)$ mentionnée plus haut.
2) La liste des quartiques sur $\mathcal{D}/K$ dont il nous faut effectuer la recherche des points d'abscisses dans $\mathbb{Q}$.
3) Les courbes elliptiques E/K qui sont les désingularisées des quartiques $\mathcal{D}/K$ précédentes. Elles sont obtenues par les formules (24), (31) et (32) de l'appendice A.

Dans l'utilisation de la méthode de Chabauty elliptique, il est nécessaire de connaître le rang r de $E(K)$ ainsi que r points de $E(K)$ qui sont $\mathbb{Z}$-linéairement indépendants. C'est une condition difficile à réaliser en pratique. On a utilisé pour cela le programme écrit par D. Simon fonctionnant avec le logiciel PARI, qui permet d'obtenir ces informations pour les courbes elliptiques intervenant dans la démonstration ([15]). Dans l'utilisation de ce programme, on a procédé de la façon suivante : on s'est principalement servi du sous-programme de 2-descente via une 2-isogénie. Il fournit en particulier les dimensions sur $\mathbb{F}_2$ des deux groupes de Selmer intervenant dans cette 2-descente. Le calcul de ces dimensions, disons d_1 et d_2, nécessite des arguments de nature locale et l'on a $r \leq d_1 + d_2 - 2$ (cf. [13, Chap. X]). Si l'on dispose par ailleurs de $d_1 + d_2 - 2$ points de $E(K)$ qui sont $\mathbb{Z}$-indépendants, on a alors $r = d_1 + d_2 - 2$.

Pour chaque courbe elliptique E/K, on précise dans un tableau ces données, ainsi que le sous-groupe de torsion de $E(K)$ qui est facile à obtenir par des arguments standard de réduction. Au cours de la démonstration, si $p = 11$ ou 13 on constate que l'on a toujours $r \leq 1$. Seul le cas où $p = 17$ nécessite l'étude d'une courbe elliptique de rang 2.

On pourra trouver à l'adresse http://www.math.jussieu.fr/~ivorra le programme *Chab* permettant de vérifier tous les calculs numériques intervenant dans la démonstration. On a aussi utilisé des sous-programmes écrits par Simon dans [15] permettant de décider si un élément donné de K est un carré dans un complété de K.

La méthode suivie pour déterminer $D_p(\mathbb{Q})$ est la même. Signalons que les courbes elliptiques sur K intervenant dans la description de $D_p(\mathbb{Q})$ sont toutes de rang au plus 1.

REMARQUES. Au sujet des limites de la méthode utilisée dans ce travail, on peut faire les deux commentaires suivants :

1. Il semble que la démarche utilisée ici ne puisse pas s'appliquer pour l'instant lorsque $p \geq 23$. En effet, dans cette situation, on est amené à travailler avec un corps K de degré relativement grand. À titre indicatif, si $p = 23$, il est nécessaire de travailler sur un corps de degré 11, ce qui dépasse les capacités de calcul actuelles.
2. Lorsque $p = 19$, la méthode semble pouvoir s'appliquer. On trouvera à l'adresse http://www.math.jussieu.fr/~ivorra la démonstration du fait que
$$C_{19}(\mathbb{Q}) = \{(-1,-1),(-1,1),(0,-1),(0,1)\}.$$
La détermination de l'ensemble $D_{19}(\mathbb{Q})$ paraît plus délicate. Pour cet ensemble, la méthode suivie ici conduit à considérer deux courbes elliptiques E_1 et E_2 définies sur un corps K convenable et à rechercher les points $N \in E_i(K)$ pour lesquels $u(N)$ appartient à $\mathbb{Q}$ pour $i = 1$ et 2. L'une de ces courbes est de rang 0 sur K, par contre l'autre est de rang 1 et on ne dispose pas de point libre sur cette courbe pour l'instant pour terminer la détermination de $D_{19}(\mathbb{Q})$.

2. Courbes quotients de $C_p/\mathbb{Q}$ et $D_p/\mathbb{Q}$

Soit p un nombre premier ≥ 5. Étant donné un entier $d \geq 1$, sans facteurs carrés, on note $X_{d,p}/\mathbb{Q}$ la courbe d'équation
$$X_{d,p} : dy^2 = \Phi_p(x).$$
On va expliciter deux courbes $Y_{d,p}/\mathbb{Q}$ et $Z_{d,p}/\mathbb{Q}$ et des applications rationnelles, que l'on notera simplement
$$\varphi_1 : X_{d,p} \to Y_{d,p}, \qquad \varphi_2 : X_{d,p} \to Z_{d,p},$$
qui sont définies sur $\mathbb{Q}$ et de degré 2. La définition de ces courbes va dépendre en fait de la parité de $(p-1)/2$. On obtiendra en particulier, avec $d \in \{1, p\}$, deux courbes quotients de C_p et D_p.

On considère la suite $(T_j)_{j\geq 0}$ des polynômes de Tchebycheff de $\mathbb{Z}[X]$, qui est définie par les conditions
$$T_0 = 1, \qquad T_1 = X, \qquad T_{j+2} = 2XT_{j+1} - T_j \quad \text{pour } j \geq 0.$$
Le degré de T_j est j et si $j \geq 1$ son terme dominant est 2^{j-1}. Posons
$$m = \frac{p-1}{2}, \qquad H_m(X) = 1 + 2\sum_{j=1}^{m} T_j \in \mathbb{Z}[X], \qquad G_m(X) = H_m(X/2).$$

Le polynôme $G_m(X)$ appartient à $\mathbb{Z}[X]$ et est irréductible unitaire de degré m. C'est le polynôme minimal de $\zeta + \zeta^{-1}$ où ζ est un générateur de μ_p. On a l'égalité

$$\Phi_p(X) = X^m \, G_m(X + 1/X). \tag{6}$$

On en déduit les deux énoncés ci-dessous :

PROPOSITION 2.1. *Supposons m pair. Soient $Y_{d,p}/\mathbb{Q}$ et $Z_{d,p}/\mathbb{Q}$ les courbes d'équations*

$$Y_{d,p} : dv^2 = G_m(u), \qquad Z_{d,p} : dv^2 = (u^2 - 4)G_m(u).$$

Il existe deux applications rationnelles définies sur $\mathbb{Q}$, de degré 2,

$$\varphi_1 : X_{d,p} \to Y_{d,p}, \qquad \varphi_2 : X_{d,p} \to Z_{d,p},$$

définies pour tout point $P = (x, y) \in X_{d,p}(\overline{\mathbb{Q}})$ tel que $x \neq 0$ par les égalités

$$\varphi_1(P) = \left(\frac{x^2+1}{x}, \frac{y}{x^{m/2}}\right), \qquad \varphi_2(P) = \left(\frac{x^2+1}{x}, \frac{y(x^2-1)}{x^{(m+2)/2}}\right). \tag{7}$$

PROPOSITION 2.2. *Supposons m impair. Soient $Y_{d,p}/\mathbb{Q}$ et $Z_{d,p}/\mathbb{Q}$ les courbes d'équations*

$$Y_{d,p} : dv^2 = (u + 2)G_m(u), \qquad Z_{d,p} : dv^2 = (u - 2)G_m(u).$$

Il existe deux applications rationnelles définies sur $\mathbb{Q}$, de degré 2,

$$\varphi_1 : X_{d,p} \to Y_{d,p}, \qquad \varphi_2 : X_{d,p} \to Z_{d,p},$$

définies pour tout point $P = (x, y) \in X_{d,p}(\overline{\mathbb{Q}})$ tel que $x \neq 0$ par les égalités

$$\varphi_1(P) = \left(\frac{x^2+1}{x}, \frac{y(x+1)}{x^{(m+1)/2}}\right), \qquad \varphi_2(P) = \left(\frac{x^2+1}{x}, \frac{y(x-1)}{x^{(m+1)/2}}\right). \tag{8}$$

REMARQUE 1.

1) Soient $g(Y_{d,p})$ le genre de $Y_{d,p}$ et $g(Z_{d,p})$ celui de $Z_{d,p}$.

   a) Si m est pair on a

   $$g(Y_{d,p}) = \frac{p-5}{4}, \qquad g(Z_{d,p}) = \frac{p-1}{4}.$$

   b) Si m est impair on a

   $$g(Y_{d,p}) = g(Z_{d,p}) = \frac{p-3}{4}.$$

2) La courbe $X_{d,p}$ possède deux involutions σ_1 et σ_2 définies pour tout point $M = (x, y)$ de $X_{d,p}(\overline{\mathbb{Q}})$ tel que $x \neq 0$ par

   $$\sigma_1(M) = \left(\frac{1}{x}, \frac{y}{x^m}\right), \qquad \sigma_2(M) = \left(\frac{1}{x}, -\frac{y}{x^m}\right).$$

   La courbe $Y_{d,p}$ (resp. $Z_{d,p}$) est, à $\mathbb{Q}$-isomorphisme près, la courbe quotient de $X_{d,p}$ modulo le sous-groupe des automorphismes de $X_{d,p}$ engendré par σ_1 (resp. σ_2) (pour cette notion, voir par exemple [13, ex. 3.13, p. 107]).

3. Résultats préliminaires

On reprend les notations du paragraphe précédent. On utilisera de manière essentielle la proposition 3.1 ci-dessous. Elle repose sur le lemme suivant, qui est une conséquence immédiate de la définition des applications rationnelles φ_1 et φ_2.

LEMME 1. *L'ensemble des abscisses des points de $\varphi_1(X_{d,p}(\mathbb{Q}))$ est égal à l'ensemble des abscisses des points de $\varphi_2(X_{d,p}(\mathbb{Q}))$.*

Supposons désormais, ce qui n'est pas restrictif pour les applications que l'on a en vue, que d soit *impair*.

PROPOSITION 3.1. *Soit α l'abscisse d'un point de $\varphi_1(X_{d,p}(\mathbb{Q}))$. Posons*

$$\alpha = s/t, \qquad G_m(s,t) = t^m G_m(s/t) \in \mathbb{Z},$$

où s et t sont deux entiers premiers entre eux.

1. *Si m est pair, on a $G_m(s,t) \in d\mathbb{Z}^2$ et $s^2 - 4t^2$ est un carré.*
2. *Si m est impair, quitte à changer (s,t) en $-(s,t)$, la condition suivante est réalisée :*

$$s + 2t \in \mathbb{Z}^2, \qquad s - 2t \in \mathbb{Z}^2, \qquad G_m(s,t) \in d\mathbb{Z}^2. \tag{9}$$

3. *L'entier st est pair.*

Démonstration. Le polynôme G_m est de degré m dans $\mathbb{Z}[X]$, donc $G_m(s,t)$ est un entier. Par hypothèse, il existe $\beta \in \mathbb{Q}$ tel que (α, β) appartienne à $\varphi_1(X_{d,p}(\mathbb{Q}))$. D'après le lemme 1, il existe $\gamma \in \mathbb{Q}$ tel que (α, γ) soit dans $\varphi_2(X_{d,p}(\mathbb{Q}))$.

1. Supposons m pair. Dans ce cas, on a

$$G_m(s,t) = d(\beta t^{m/2})^2, \qquad (s^2 - 4t^2)G_m(s,t) = d(\gamma t^{(m+2)/2})^2.$$

Puisque d est sans facteurs carrés et que $G_m(s,t)$ est dans $\mathbb{Z}$, le rationnel $\beta t^{m/2}$ appartient à $\mathbb{Z}$. Par suite, $G_m(s,t)$ est dans $d\mathbb{Z}^2$, ce qui entraîne l'assertion 1.

2. Supposons m impair. On a les égalités

$$(s+2t)G_m(s,t) = d(\beta t^{(m+1)/2})^2, \qquad (s-2t)G_m(s,t) = d(\gamma t^{(m+1)/2})^2. \tag{10}$$

Comme ci-dessus, puisque d est sans facteurs carrés et que $G_m(s,t) \in \mathbb{Z}$, on a

$$\beta t^{(m+1)/2} \in \mathbb{Z}, \qquad \gamma t^{(m+1)/2} \in \mathbb{Z}. \tag{11}$$

Les entiers s et t étant premiers entre eux et d étant impair, on en déduit que

$$d \text{ divise } G_m(s,t). \tag{12}$$

D'après l'égalité (6), on a $\Phi_p(-1) = -G_m(-2)$. Puisque $\Phi_p(-1) = 1$, on a $G_m(-2) = -1$, ce qui entraîne que

$$X + 2 \text{ divise } 1 + G_m(X),$$

autrement dit, qu'il existe un polynôme $R \in \mathbb{Z}[X]$ de degré $m-1$ tel que

$$1 = (X+2)R(X) - G_m(X).$$

En posant $R(s,t) = t^{m-1}R(s/t)$, on obtient l'égalité

$$t^m = (s+2t)R(s,t) - G_m(s,t).$$

Il en résulte que les entiers $s+2t$ et $G_m(s,t)$ sont premiers entre eux. D'après (10) et les conditions (11) et (12), on a ainsi

$$\pm(s+2t) \in \mathbb{Z}^2, \qquad \pm G_m(s,t) \in d\mathbb{Z}^2.$$

Par ailleurs, $G_m(s,t)$ étant un polynôme homogène de degré impair m en s et t, on a

$$G_m(-s,-t) = -G_m(s,t).$$

Quitte à changer (s,t) en $-(s,t)$, on obtient donc la condition

$$s+2t\in\mathbb{Z}^2,\quad G_m(s,t)\in d\mathbb{Z}^2.$$

D'après la deuxième égalité de (10), $s-2t$ est alors un carré. D'où le résultat.

3. Il résulte de ce qui précède que s^2-4t^2 est un carré. Si st était impair, on aurait $s^2-4t^2\equiv 1 \bmod 8$, ce qui n'est pas si $s^2\equiv t^2\equiv 1 \bmod 8$. D'où la proposition. ∎

Dans le cas où m est impair, on supposera implicitement, dans toute la suite, que pour tout point de $\varphi_1(X_{d,p}(\mathbb{Q}))$, la condition (9) est satisfaite.

4. Notations

Précisons quelques notations que l'on utilisera dans toute la suite. On reprendra librement toutes les notations et les informations qui se trouvent dans le formulaire. Précisons à ce propos que, dans les tableaux, les courbes elliptiques notées E/K, E'/K, E''/K et E'''/K sont les désingularisées respectivement des quartiques $\mathcal{D}/K$, $\mathcal{D}'/K$, $\mathcal{D}''/K$ et $\mathcal{D}'''/K$.

Considérons l'un des corps K intervenant dans ces tableaux. Étant donné un idéal premier $\mathfrak{p}$ de l'anneau d'entiers A de K, on notera :

- $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$;
- $v_\mathfrak{p}$ la valuation $\mathfrak{p}$-adique de $K_\mathfrak{p}$ normalisée par $v_\mathfrak{p}(K_\mathfrak{p}^*)=\mathbb{Z}$;
- $A_\mathfrak{p}$ l'anneau de valuation de $K_\mathfrak{p}$;
- $\mathfrak{M}_\mathfrak{p}$ l'idéal maximal de $A_\mathfrak{p}$;
- $k_\mathfrak{p}=A_\mathfrak{p}/\mathfrak{M}_\mathfrak{p}$ le corps résiduel ;
- $\eta_\mathfrak{p}:K_\mathfrak{p}^*\to k_\mathfrak{p}^*$ l'application de projection définie par (appendice B, paragraphe 2.5)

$$\eta_\mathfrak{p}(x)=\frac{x}{p^{v_\mathfrak{p}(x)}} \bmod \mathfrak{M}_\mathfrak{p}\quad \text{pour } x\in K_\mathfrak{p}^*.$$

Soit θ l'élément primitif implicitement choisi de K sur $\mathbb{Q}$. C'est une unité de A. On constate que le nombre premier 3 est inerte dans K ; on a $3A=\mathfrak{p}_3$. On désignera par ξ l'image de θ dans $k_{\mathfrak{p}_3}$; on a ainsi

$$\xi=\eta_{\mathfrak{p}_3}(\theta)\in k_{\mathfrak{p}_3},\quad k_{\mathfrak{p}_3}=\mathbb{F}_3(\xi).$$

Si E/K est une courbe elliptique, ayant bonne réduction en $\mathfrak{p}$, on notera par ailleurs :

- $\widetilde{E}_\mathfrak{p}$ la courbe elliptique sur $k_\mathfrak{p}$ déduite de E par réduction modulo $\mathfrak{p}$;
- $\pi_\mathfrak{p}:E(K_\mathfrak{p})\to\widetilde{E}_\mathfrak{p}(k_\mathfrak{p})$ l'homomorphisme de réduction ;
- $E_1(K_\mathfrak{p})$ le noyau de $\pi_\mathfrak{p}$;
- $E_1(K)$ l'intersection de $E_1(K_\mathfrak{p})$ avec $E(K)$; on omettra dans cette notation de préciser $\mathfrak{p}$, le contexte ne prêtera pas à confusion ;
- $z(R)$ la z-coordonnée d'un point R de $E_1(K)$; on a $z(O)=0$.

Sauf précisions supplémentaires comme ci-dessus, on ne redéfinira pas les notations utilisées dans les appendices A et B que l'on conserve systématiquement. En particulier, étant donnée une quartique $\mathcal{D}/K$ définie par une équation de la forme (23) ou (30) de l'appendice A et la courbe elliptique E/K déduite de $\mathcal{D}$ par les formules (24), (31) et (32) de cet appendice, on évoquera dans la suite :

- l'isomorphisme birationnel $\psi : E \to \mathcal{D}$,
- l'ouvert U de E,
- la fonction u sur E,
- les points O et M_1 de $E(K)$,

sans plus de précision.

5. Détermination de $C_{11}(\mathbb{Q})$ et $D_{11}(\mathbb{Q})$

5.1. L'ensemble $C_{11}(\mathbb{Q})$. On considère dans ce paragraphe un point (α, β) appartenant à $\varphi_1(C_{11}(\mathbb{Q}))$ et l'on pose $\alpha = s/t$, où s et t sont deux entiers premiers entre eux.

LEMME 2. *L'élément $s - t\theta$ est un carré dans K.*

Démonstration. Pour $i \neq j$, les éléments $s - t\theta_i$ et $s - t\theta_j$ sont premiers entre eux en dehors de π_{11} et $G_5(s,t) \in \mathbb{Z}^2$ (prop. 3.1). Il existe donc des entiers n_i égaux à 0 ou 1 tels que

$$s - t\theta \equiv (-1)^{n_0} \prod_{i=1}^{4} u_i^{n_i}\ \pi_{11}^{n_5} \bmod K^{*2}.$$

Puisque $N_{K/\mathbb{Q}}(s - t\theta) \in \mathbb{Z}^2$, on a $n_5 = 0$ et $n_0 + n_1$ est pair. Cette congruence vaut en particulier modulo les carrés du complété $K_{\mathfrak{p}_2}$. On a $v_{\mathfrak{p}_2}(s - t\theta) = 0$: en effet, θ est une unité de A, st est pair (prop. 3.1) et s et t sont premiers entre eux. Par ailleurs, une unité de $A_{\mathfrak{p}_2}$ congrue à 1 modulo 8 est un carré dans $K_{\mathfrak{p}_2}$. La classe de $s - t\theta$ modulo $K_{\mathfrak{p}_2}^{*2}$ ne dépend donc que des classes de s et t modulo 8. On distingue alors deux cas :

1) Supposons s pair et t impair. Puisque $s + 2t$ est un carré (prop. 3.1), on en déduit que $s \equiv 2$ ou $6 \bmod 8$. Pour $s \in \{2, 6\}$ et $t \in \{1, 3, 5, 7\}$, on a donc

$$(s - t\theta)(-1)^{n_0} \prod_{i=1}^{4} u_i^{n_i} \in K_{\mathfrak{p}_2}^{*2}.$$

En tenant compte du fait que $n_0 + n_1$ est pair, on vérifie que cela entraîne

$$n_0 = n_1 = n_2 = n_3 = n_4 = 0.$$

D'où le résultat dans ce cas.

2) Supposons s impair et t pair. Les entiers $s + 2t$ et $s^5 + s^4t - 4s^3t^2 - 3s^2t^3 + 3st^4 + t^5$ sont des carrés impairs, donc sont congrus à 1 modulo 8. On en déduit que $(s,t) \equiv (1,0) \bmod 8$. On vérifie que cela entraîne de nouveau

$$n_0 = n_1 = n_2 = n_3 = n_4 = 0.$$

D'où le lemme. ∎

On en déduit que (lemme 2 et prop. 3.1)

$$(s^2 - 4t^2)(s - t\theta)(s - t\theta_2) \in K^2.$$

On a $s \neq 0$, il en résulte que $(t/s, \delta/s^2) \in \mathcal{D}(K)$, où $\mathcal{D}/K$ est la quartique indiquée dans le formulaire (pour $p = 11$). Compte tenu des égalités

$$\psi(2N_1) = (-1/2, 0), \qquad \psi(T_0 + 2N_1) = (1/2, 0),$$

l'assertion du théorème 2 relative à $C_{11}(\mathbb{Q})$ est une conséquence du résultat suivant :

PROPOSITION 5.1. *Les seuls points $N \in E(K) \setminus \{O, -M_1\}$ tels que $u(N) \in \mathbb{Q}$ sont $2N_1$ et $T_0 + 2N_1$.*

Démonstration. Considérons un point N appartenant à $E(K) \setminus \{O, -M_1\}$ tel que

$$N \neq 2N_1 \quad \text{et} \quad N \neq T_0 + 2N_1,$$

et prouvons que $u(N)$ n'est pas dans $\mathbb{Q}$. On peut supposer que $N \in U$. La courbe E/K a bonne réduction en $\mathfrak{p}_3$. Le groupe $\widetilde{E}_{\mathfrak{p}_3}(k_{\mathfrak{p}_3})$ est d'ordre $240 = 2^4 \cdot 3 \cdot 5$ et $\pi_{\mathfrak{p}_3}(N_1)$ est d'ordre 15. On pose

$$Q_1 = 15N_1 \in E_1(K). \tag{13}$$

Notons G le sous-groupe de $E(K)$ engendré par $\{O, T_0, T_1, T_2\}$ et le point N_1.

LEMME 3. *On a $\pi_{\mathfrak{p}_3}(E(K)) = \pi_{\mathfrak{p}_3}(G)$.*

Démonstration. Il s'agit de démontrer que la condition 7 de l'appendice B est satisfaite, i.e. que l'indice de G dans $E(K)$ est premier à 30 (lemme 25, appendice B). Supposons le contraire. Dans ce cas, il existe $q \in \{2, 3, 5\}$ et $M \in E(K)$ tel que qM soit dans G sans que M le soit. Considérons un entier $n \in \mathbb{Z}$ et un point $T \in \{O, T_0, T_1, T_2\}$ tels que $qM = T + nN_1$. L'entier n n'est pas divisible par q : sinon, $M - (n/q)N_1$ est un point de torsion (d'ordre divisant $2q$), par suite M est dans G, ce qui n'est pas. On en déduit que la condition suivante est réalisée :

$$N_1 + T \in qE(K) \quad \text{ou bien} \quad 2N_1 + T \in 5E(K) \quad (\text{si } q = 5).$$

Supposons qu'il existe $R \in E(K)$ tel que $N_1 + T = 2R$. On a $2N_1 = 4R$. Considérons l'idéal $\mathfrak{p}$ de A engendré par $-1 + 2\theta + \theta^2$. C'est l'un des cinq idéaux premiers de A au-dessus de 23. On vérifie que $\widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}})$ est d'ordre 24 et que le point $\pi_{\mathfrak{p}}(N_1)$ est d'ordre 12. Par ailleurs, $\pi_{\mathfrak{p}}(T_0)$ et $\pi_{\mathfrak{p}}(N_1)$ engendrent $\widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}})$. En particulier, $\widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}})$ n'est pas un groupe cyclique. Si d est l'ordre de $\pi_{\mathfrak{p}}(R) \in \widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}})$, on a l'égalité $6\,\mathrm{pgcd}(d, 4) = d$. Cela entraîne $d = 24$ puis une contradiction.

Supposons qu'il existe $R \in E(K)$ tel que $N_1 + T = 3R$. On a $2N_1 = 6R$. Soit d l'ordre de $\pi_{\mathfrak{p}_3}(R) \in \widetilde{E}_{\mathfrak{p}_3}(k_{\mathfrak{p}_3})$. On a $d = 15\ \mathrm{pgcd}(6, d)$. Puisque 3 divise d, on a $\mathrm{pgcd}(6, d) = 3$ ou 6 et d est multiple de 9. Le fait que d divise 240 entraîne alors une contradiction.

Supposons qu'il existe $R \in E(K)$ tel que $2N_1 + T = 5R$. On a $4N_1 = 10R$. Si d est l'ordre de $\pi_{\mathfrak{p}_3}(R)$, on a $d = 15\,\mathrm{pgcd}(10, d)$. Mais $\mathrm{pgcd}(10, d) = 5$ ou 10, donc d est multiple de 25, d'où une contradiction. En particulier, $N_1 + T$ n'est pas dans $5E(K)$. D'où le lemme. ∎

On considère alors l'ensemble $\mathfrak{S}$ des points de $E(K)$ qui s'écrivent sous la forme

$$T + jN_1 \quad \text{où } T \in \{O, T_0, T_1, T_2\} \text{ et } j = -7, \ldots, 7.$$

D'après le lemme 3 et la condition (13), il existe $S \in \mathfrak{S}$ tel que $N - S \in E_1(K)$. En utilisant le lemme 24 (appendice A), quitte à remplacer N par $-M_1 - N$, on peut supposer que

$$N = S + P \quad \text{où } S \in \{-4N_1, O, 2N_1, T_0 + 2N_1\} \text{ et } P \in E_1(K).$$

LEMME 4. *Soit R un point de $E_1(K)$ non nul. On a*

$$\eta_{\mathfrak{p}_3}(z(R)) = \pm(\xi^4 + 2\xi + 2).$$

Démonstration. On a $z(Q_1) \equiv 3\theta^4 + 6\theta + 6 \bmod 9$ et $v_{\mathfrak{p}_3}(3\theta^4 + 6\theta + 6) = 1$, d'où l'on déduit que

$$\eta_{\mathfrak{p}_3}(z(Q_1)) = \xi^4 + 2\xi + 2.$$

Le sous-$\mathbb{F}_3$-espace vectoriel Γ de $k_{\mathfrak{p}_3}$ intervenant dans le paragraphe 3 de l'appendice B est donc ici la droite vectorielle engendrée par $\xi^4 + 2\xi + 2$. Par ailleurs, les points T_0, T_1 et T_2 ne sont pas dans $E_1(K)$ ([13, prop. 3.1, p. 176]; on peut aussi vérifier notre assertion directement). D'après le lemme 26 (appendice B), $\eta_{\mathfrak{p}_3}\big(z(R)\big)$ est donc dans Γ, d'où le résultat. ∎

1) Supposons $S = O$. On a $u(N) \equiv -2z(P) \bmod z(P)^2$, ce qui, d'après le lemme 4, conduit à l'égalité $\eta_{\mathfrak{p}_3}(u(N)) = \pm(\xi^4 + 2\xi + 2)$.

2) Si $S = 2N_1$, on vérifie que

$$u(N) = -1/2 + (\theta^3 + 2\theta^2)z(P)^2 \bmod z(P)^3.$$

Puisque $v_{\mathfrak{p}_3}(\theta^3+2\theta^2) = 0$, on déduit du lemme 4 que $\eta_{\mathfrak{p}_3}(u(N)+1/2) = \xi^4+2\xi^3+\xi^2+\xi+1$.

3) Si $S = T_0 + 2N_1$, on obtient

$$u(N) = 1/2 + (-\theta^3 + 2\theta^2 + 4\theta - 8)z(P)^2 \bmod z(P)^3,$$

ce qui conduit à $\eta_{\mathfrak{p}_3}(u(N) - 1/2) = 2\xi^4 + \xi^2 + 2$.

4) Si $S = -4N_1$, on constate que $\eta_{\mathfrak{p}_3}(u(N)) = \xi^4 + \xi^3 + 2\xi^2$.

Dans tous les cas, les projections considérées ne sont pas dans $\mathbb{F}_3$, ce qui prouve que $u(N)$ n'est pas dans $\mathbb{Q}$. D'où la proposition 5.1. ∎

Cela termine la démonstration du théorème en ce qui concerne l'ensemble $C_{11}(\mathbb{Q})$.

5.2. L'ensemble $D_{11}(\mathbb{Q})$. Soit (α, β) un point de $\varphi_1(D_{11}(\mathbb{Q}))$. On pose $\alpha = s/t$, où s et t sont deux entiers premiers entre eux. Posons

$$\tau_1 = \theta^4 + \theta^3 - \theta, \qquad \tau_2 = -\theta^4 - 2\theta^3 - \theta^2 + \theta + 1.$$

Ce sont des éléments de A associés à π_{11}.

LEMME 5. *L'un des éléments $(s - t\theta)\tau_1$ et $(s - t\theta)\tau_2$ est un carré dans K.*

Démonstration. On a $N_{K/\mathbb{Q}}(s - t\theta) = G_5(s, t) \in 11\mathbb{Z}^2$ (prop. 3.1). Les $s - t\theta_i$ étant premiers entre eux en dehors de π_{11}, il existe donc des entiers n_i égaux à 0 ou 1 tels que

$$s - t\theta \equiv \pi_{11}(-1)^{n_0} \prod_{i=1}^{4} u_i^{n_i} \bmod K^{*2}, \qquad n_0 + n_1 \equiv 1 \bmod 2.$$

En exprimant de nouveau cette congruence dans $K^*_{\mathfrak{p}_2}$, on vérifie que cela entraîne

$$(n_0, n_1, n_2, n_3, n_4) \in \{(1, 0, 0, 1, 1), (0, 1, 1, 0, 1)\}.$$

Le lemme en résulte compte tenu du fait que $u_1u_2u_4\pi_{11} = \tau_1$ et $-u_3u_4\pi_{11} = \tau_2$. ∎

On note dans la suite σ_j l'élément du groupe de Galois de K sur $\mathbb{Q}$ tel que $\sigma_j(\theta) = \theta_j$ $(1 \le j \le 5)$.

Supposons que $(s-t\theta)\tau_2$ est un carré dans K. Il existe alors $\delta \in K$ tel que

$$\prod_{j=1}^{4} \sigma_j(\tau_2)(s-t\theta_j) = \delta^2,$$

d'où il résulte que

$$\left(\frac{t}{s} - \frac{1}{\theta}, \frac{\delta}{s^2}\right) \in \mathcal{D}''(K).$$

Par ailleurs, on a $E''(K) = \{O, T_0, T_1, T_2\}$. D'après la proposition A.1 (appendice A), on a donc $\mathcal{D}''(K) = \{(0,0), \psi(T_0), \psi(T_1), \psi(T_2)\}$. En explicitant les coordonnées des points $\psi(T_i)$, on constate que cela contredit le fait que t/s soit dans $\mathbb{Q}$. Par suite, $(s-t\theta)\tau_2$ n'est pas un carré dans K. On déduit alors du lemme 5 que

$$(s-t\theta)\tau_1 \in K^2.$$

Posons $\pi = \tau_1\sigma_2(\tau_1)\sigma_3(\tau_1)$. On a $\pi = 4\theta^4 - 8\theta^2 + 3\theta + 6$. Il existe $\nu \in K$ tel que (lemme 5 et prop. 3.1)

$$\pi(s-2t)(s-t\theta)(s-t\theta_2)(s-t\theta_3) = \nu^2.$$

Il en résulte que

$$\left(\frac{t}{s} - \frac{1}{2}, \frac{2\nu}{s^2}\right) \in \mathcal{D}'(K).$$

La description annoncée de $D_{11}(\mathbb{Q})$ se déduit alors du résultat suivant :

PROPOSITION 5.2. *Soit (u,v) un point de $\mathcal{D}'(K)$ tel que u soit dans $\mathbb{Q}$. Alors $(u,v) = (0,0)$.*

La proposition 5.2 est une conséquence de l'énoncé qui suit (prop. A.1, appendice A) :

PROPOSITION 5.3. *Il n'existe pas de points $N \in E'(K) \setminus \{O\}$ tels que $u(N)$ soit dans $\mathbb{Q}$.*

Démonstration. Considérons un point N de $E'(K) \setminus \{O\}$. La courbe elliptique E'/K a bonne réduction en $\mathfrak{p}_3$, le groupe $\widetilde{E'}_{\mathfrak{p}_3}(k_{\mathfrak{p}_3})$ est d'ordre $248 = 2^3 \cdot 31$ et $\pi_{\mathfrak{p}_3}(N_1)$ est d'ordre 62. On pose

$$Q_1 = 62N_1 \in E'_1(K). \tag{14}$$

Soit G le sous-groupe de $E'(K)$ engendré par $\{O, T_0, T_1, T_2\}$ et le point N_1.

LEMME 6. *On a $\pi_{\mathfrak{p}_3}(E'(K)) = \pi_{\mathfrak{p}_3}(G)$.*

Démonstration. Elle est identique à celle du lemme 3 : il s'agit ici de prouver que l'indice h de G dans $E'(K)$ est premier à 62.

1) Supposons que h soit pair. Il existe alors un point de torsion T de $E'(K)$ tel que $N_1 + T \in 2E'(K)$. On a $2N_1 = 4R$ avec $R \in E'(K)$. Soit $\mathfrak{p}$ l'idéal de A au-dessus de 23 engendré par $2 - 3\theta - 3\theta^2 + \theta^3 + \theta^4$. Le groupe $\widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}})$ est d'ordre 16 et l'ordre de $\pi_{\mathfrak{p}}(N_1)$ est 8. Ainsi, l'ordre de $\pi_{\mathfrak{p}}(R)$ est 16 et l'on vérifie par ailleurs que $\widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}})$ n'est pas cyclique, d'où une contradiction.

2) Si 31 divise h, il existe $j \in \{1, \ldots, 30\}$ tel que $jN_1 + T \in 31E'(K)$. Soit R un point de $E'(K)$ tel que $jN_1 + T = 31R$. On a $2jN_1 = 62R$ et l'ordre de $\pi_{\mathfrak{p}_3}(2jN_1)$ est 31. Si d est l'ordre de $\pi_{\mathfrak{p}_3}(R)$, on a donc $d = 31\,\mathrm{pgcd}(62, d)$, et 31^2 doit diviser d, ce qui n'est pas. D'où le lemme. ∎

Soit $\mathfrak{S}$ l'ensemble des points de $E'(K)$ qui s'écrivent sous la forme

$$T + jN_1 \quad \text{où } T \in \{O, T_0, T_1, T_2\} \text{ et } j = -30, \ldots, 31.$$

Il existe $S \in \mathfrak{S}$ tel que $N - S \in E'_1(K)$ (lemme 6 et (14)). En utilisant le lemme 24 (appendice A), on vérifie que l'on se ramène au cas où $S = O$, autrement dit, on peut supposer que N appartient à $E'_1(K)$. On a $u(N)z(N) \neq 0$ et d'après la formule (91) (appendice B) avec $e = 0$, on a

$$u(N) \equiv dz(N)^2 \bmod z(N)^3.$$

On a $v_{\mathfrak{p}_3}(d) = 0$, d'où $\eta_{\mathfrak{p}_3}(u(N)) = \eta_{\mathfrak{p}_3}(d)\eta_{\mathfrak{p}_3}(z(N))^2$. Par ailleurs, d'après le lemme 26 (appendice B), on a $\eta_{\mathfrak{p}_3}(z(N)) = \pm\eta_{\mathfrak{p}_3}(z(Q_1))$ et l'on vérifie que

$$\eta_{\mathfrak{p}_3}(z(Q_1)) = \xi^4 + 2\xi^3 + \xi^2 + \xi + 1.$$

Il en résulte que $\eta_{\mathfrak{p}_3}(u(N)) = 2\xi^4 + 2\xi^3 + \xi + 2$, qui n'est pas dans $\mathbb{F}_3$, ce qui prouve que $u(N)$ n'est pas dans $\mathbb{Q}$. D'où la proposition 5.3. ∎

Cela termine la démonstration du théorème 2 si $p = 11$.

6. Détermination de $C_{13}(\mathbb{Q})$ et $D_{13}(\mathbb{Q})$

6.1. L'ensemble $C_{13}(\mathbb{Q})$. Soit (α, β) un point de $\varphi_1(C_{13}(\mathbb{Q}))$. On pose $\alpha = s/t$, où s et t sont deux entiers premiers entre eux.

LEMME 7. *L'élément $F_1 = s^2 - \theta st + (\theta^2 + \theta - 3)t^2$ est un carré dans K.*

Démonstration. Pour tous i et j distincts, F_i et F_j sont premiers entre eux en dehors de π_{13} : en effet, en posant

$$h_1 = (3\theta^2 + 2\theta - 4)s + (2\theta^2 + 10\theta - 7)t, \qquad h_2 = (-3\theta^2 - 2\theta + 4)s + (-2\theta^2 + 3\theta + 7)t,$$

on vérifie que $h_1F_1 + h_2F_2 = 13t^3$, ce qui, compte tenu de l'action du groupe de Galois de K sur $\mathbb{Q}$, entraîne notre assertion. On a $G_6(s,t) \in \mathbb{Z}^2$, donc il existe des entiers $n_i = 0, 1$ tels que (cf. la factorisation du formulaire)

$$F_1 \equiv (-1)^{n_0} u_1^{n_1} u_2^{n_2} \pi_{13}^{n_3} \bmod K^{*2}.$$

On a $n_3 = 0$ et $n_0 + n_1$ est pair. Par ailleurs, on a $v_{\mathfrak{p}_2}(F_1) = 0$. En effet, si t est pair, alors s est impair, et l'on a $F_1 \equiv s^2 \equiv 1 \bmod 2$. Si s est pair, t est impair, on a dans ce cas $F_1 \equiv \theta^2 + \theta - 3 \bmod 2$ et $\theta^2 + \theta - 3$ est une unité de A, d'où l'assertion. La classe de F_1 modulo les carrés du complété $K_{\mathfrak{p}_2}$ ne dépend donc que des classes de s et t modulo 8. On constate alors que cela conduit à $n_0 = n_1 = 0$. D'où le lemme. ∎

On en déduit qu'il existe $\delta \in K$ tel que (lemme 7 et prop. 3.1)

$$(s^2 - 4t^2)(s^2 - \theta st + (\theta^2 + \theta - 3)t^2) = \delta^2,$$

et l'on a $(t/s, \delta/s^2) \in \mathcal{D}(K)$. Comme dans les cas précédents, on démontre donc que si (u, v) est un point de $\mathcal{D}(K)$ tel que u soit dans $\mathbb{Q}$, alors

$$(u, v) \in \{(-1/2, 0), (1/2, 0), (0, -1), (0, 1)\}.$$

On a

$$\psi(2N_1) = (-1/2, 0), \qquad \psi(T_0 + 2N_1) = (1/2, 0),$$

et l'on est ainsi amené à prouver le résultat suivant :

PROPOSITION 6.1. *Les seuls points $N \in E(K) \setminus \{O, -M_1\}$ tels que $u(N) \in \mathbb{Q}$ sont $2N_1$ et $T_0 + 2N_1$.*

Démonstration. Soit N un point de $E(K) \setminus \{O, -M_1\}$ distinct de $2N_1$ et de $T_0 + 2N_1$. On suppose que $N \in U$, ce qui n'est pas restrictif. La courbe E/K a bonne réduction en $\mathfrak{p}_3$. Le groupe $\widetilde{E}_{\mathfrak{p}_3}(k_{\mathfrak{p}_3})$ est d'ordre 24 et $\pi_{\mathfrak{p}_3}(N_1)$ est d'ordre 12. On pose

$$Q_1 = 12N_1 \in E_1(K). \tag{15}$$

Soit G le sous-groupe de $E(K)$ engendré par T_0 et N_1.

LEMME 8. *On a les assertions suivantes :*

1. $\pi_{\mathfrak{p}_3}(G) = \pi_{\mathfrak{p}_3}(E(K))$.
2. *L'indice dans $E_1(K)$ du sous-groupe engendré par Q_1 est premier à 3.*

Démonstration. 1. On démontre que l'indice h de G dans $E(K)$ est premier à 6 : si h est pair, il existe $T \in \{O, T_0\}$ tel que $N_1 + T \in 2E(K)$; on vérifie que ni $\pi_{\mathfrak{p}_3}(N_1)$ ni $\pi_{\mathfrak{p}_3}(N_1 + T_0)$ ne sont des doubles dans $\widetilde{E}_{\mathfrak{p}_3}(k_{\mathfrak{p}_3})$, d'où une contradiction. Si 3 divise h, il existe $T \in \{O, T_0\}$ tel que $N_1 + T \in 3E(K)$. On a $2N_1 = 6R$ avec $R \in E(K)$. Si d est l'ordre de $\pi_{\mathfrak{p}_3}(R)$, on a $d = 6\,\mathrm{pgcd}(d, 6)$, alors 9 divise d, et l'on obtient de nouveau une contradiction. D'où l'assertion 1.

2. Supposons le contraire. Dans ce cas, il existe $M \in E_1(K)$ tel que $3M = Q_1$. D'après (15), on obtient $3(M - 4N_1) = O$. Cela entraîne $M = 4N_1$, puis une contradiction car $4N_1$ n'appartient pas à $E_1(K)$. D'où le lemme. ∎

Soit $\mathfrak{S}$ l'ensemble des points de $E(K)$ qui s'écrivent sous la forme

$$hT_0 + jN_1 \quad \text{avec } h = 0, 1 \text{ et } j = -5, \ldots, 6.$$

D'après l'assertion 1 du lemme 8 et la condition (15), il existe $S \in \mathfrak{S}$ tel que $N - S \in E_1(K)$. Par ailleurs, quitte à remplacer N par $-M_1 - N$ on peut supposer que (lemme 24, appendice A)

$$N = S + P \quad \text{où } S \in \{-5N_1, -4N_1, -3N_1, O, 2N_1, T_0 + 2N_1\} \text{ et } P \in E_1(K).$$

Pour tout point S comme ci-dessus non nul, on pose $S = (x_S, y_S)$.

LEMME 9. *Soit R un point de $E_1(K)$ non nul. On a*

$$\eta_{\mathfrak{p}_3}(z(R)) = \pm 1.$$

Démonstration. On a $z(Q_1) \equiv 6 \bmod 9$. Par suite, $\eta_{\mathfrak{p}_3}(z(Q_1)) = -1$. Le lemme 26 (appendice B) entraîne alors le résultat. ∎

La condition 12 de l'appendice B n'est donc pas satisfaite et, tout au moins en ce qui concerne l'étude du cas où $S = O$, on ne peut pas conclure directement. Cela étant, la condition 13 de cet appendice est réalisée (assertion 2 du lemme 8). Par suite, il existe $n_1 \in \mathbb{Z}_3$ tel que $P = n_1 Q_1$. En utilisant l'égalité (95) (appendice B), on constate que

$$z(P) \equiv (9\theta^2 + 9\theta + 18)n_1^3 + (45\theta^2 + 63\theta + 42)n_1 \bmod 3^4. \tag{16}$$

1) Supposons $S = O$, i.e. $N = P$. On a

$$u(N) \equiv -2z(P) - \theta z(P)^2 + (-2\theta^2 - 2\theta + 14)z(P)^3 \bmod z(P)^4. \tag{17}$$

Il résulte alors des congruences (16) et (17) que

$$u(N) = \Phi_S^{(0)} + \Phi_S^{(1)}\theta + \Phi_S^{(2)}\theta^2$$

avec

$$\Phi_S^{(0)} \equiv 27n_1^4 + 72n_1^3 + 54n_1^2 + 78n_1 \bmod 3^4,$$
$$\frac{\Phi_S^{(1)}}{9n_1} \equiv 4n_1^2 + 5n_1 + 4 \bmod 9, \qquad \frac{\Phi_S^{(2)}}{9n_1} \equiv 4n_1^2 + 3n_1 + 8 \bmod 9.$$

On constate que la série $\Phi_S^{(1)}(X_1)/X_1$ n'a pas de zéro modulo 9, en particulier elle n'a pas de zéro dans $\mathbb{Z}_3$. Cela prouve que $u(N)$ n'est pas dans $\mathbb{Q}$.

2) Supposons $S = -5N_1$, i.e. $N = -5N_1 + n_1Q_1$. On a $v_{\mathfrak{p}_3}(x_S - \lambda) = 0$ et la condition 8 de l'appendice B est vérifiée. On obtient dans $A_{\mathfrak{p}_3}$ la congruence

$$\frac{1}{u(N)} \equiv \sum_{i=0}^{3} \varrho_i z(P)^i \bmod 3^4 \tag{18}$$

avec

$$\varrho_0 = 45\theta^2 + 27\theta + 57, \quad \varrho_1 = 52\theta^2 + 29\theta + 48, \quad \varrho_2 = 6\theta^2 + \theta + 66, \quad \varrho_3 = 12\theta^2 + 74\theta + 28.$$

On a $v_{\mathfrak{p}_3}(\varrho_0) = 1$ et $v_{\mathfrak{p}_3}(\varrho_1) = 0$, par suite, on ne peut pas conclure directement. On déduit de (16) et (18) que

$$\frac{1}{u(N)} = \Phi_S^{(0)} + \Phi_S^{(1)}\theta + \Phi_S^{(2)}\theta^2,$$

avec

$$\Phi_S^{(0)} \equiv 54n_1^4 + 9n_1^3 + 54n_1^2 + 18n_1 + 57 \bmod 3^4,$$
$$\Phi_S^{(1)} \equiv 18n_1^3 + 36n_1^2 + 12n_1 + 27 \bmod 3^4, \qquad \Phi_S^{(2)} \equiv 27n_1^2 + 6n_1 + 45 \bmod 3^4.$$

On constate alors que les séries formelles $\Phi_S^{(1)}(X_1)$ et $\Phi_S^{(2)}(X_1)$ n'ont pas de zéros communs modulo 3^4. Cela prouve de nouveau que $u(N)$ n'est pas dans $\mathbb{Q}$.

3) Supposons $S = -4N_1$ i.e. $S = M_1$. La condition 9 de l'appendice B est satisfaite. On vérifie que $u(N) \equiv 2\theta + 1 \bmod 3$, d'où $\eta_{\mathfrak{p}_3}(u(N)) = 2\xi + 1$.

4) Supposons $S = -3N_1$. On a $v_{\mathfrak{p}_3}(x_S - \lambda) = 0$, et l'on obtient

$$\frac{1}{u(N)} \equiv \sum_{i=0}^{3} \varrho_i z(P)^i \bmod 3^4, \tag{19}$$

avec

$$\varrho_0 = 78\theta^2 + 12\theta + 30, \quad \varrho_1 = 2\theta^2 + 4\theta + 60, \quad \varrho_2 = 78\theta^2 + 79\theta + 15, \quad \varrho_3 = 24\theta^2 + 13\theta + 32.$$

On a $v_{\mathfrak{p}_3}(\varrho_0) = 1$, $v_{\mathfrak{p}_3}(\varrho_1) = 0$ et de nouveau on ne peut pas conclure directement. Il résulte de (16) et (19) que l'on a dans ce cas

$$\frac{1}{u(N)} = \Phi_S^{(0)} + \Phi_S^{(1)}\theta + \Phi_S^{(2)}\theta^2,$$

avec

$$\Phi_S^{(0)} \equiv 54n_1^4 + 18n_1^3 + 36n_1 + 30 \bmod 3^4,$$

$$\Phi_S^{(1)} \equiv 63n_1^3 + 9n_1^2 + 24n_1 + 12 \bmod 3^4, \quad \Phi_S^{(2)} \equiv 27n_1^2 + 21n_1 + 78 \bmod 3^4.$$

On constate encore une fois que les séries formelles $\Phi_S^{(1)}(X_1)$ et $\Phi_S^{(2)}(X_1)$ n'ont pas de zéros communs modulo 3^4, par suite $u(N)$ n'est pas dans $\mathbb{Q}$.

5) Si $S = 2N_1 + T_0$, on constate que

$$u(N) - 1/2 \equiv (-\theta^2 + \theta - 1)z(P)^2 \bmod z(P)^3.$$

On a $v_{\mathfrak{p}_3}(-\theta^2 + \theta - 1) = 0$ et l'on déduit alors du lemme 9 que

$$\eta_{\mathfrak{p}_3}(u(N) - 1/2) = \eta_{\mathfrak{p}_3}(-\theta^2 + \theta - 1) = 2\xi^2 + \xi + 2.$$

6) Si $S = 2N_1$, on a

$$u(N) + 1/2 \equiv (\theta^2 + 3\theta + 1)z(P)^2 \bmod z(P)^3,$$

et $v_{\mathfrak{p}_3}(\theta^2 + 3\theta + 1) = 0$, d'où $\eta_{\mathfrak{p}_3}(u(N) + 1/2) = \xi^2 + 1$.

Cela termine la démonstration de la proposition 6.1 et la description de $C_{13}(\mathbb{Q})$. ∎

6.2. L'ensemble $D_{13}(\mathbb{Q})$. Soit (α, β) un point de $\varphi_1(D_{13}(\mathbb{Q}))$. Posons $\alpha = s/t$, où s et t sont deux entiers premiers entre eux. Rappelons que l'on note $F_1 = s^2 - \theta st + (\theta^2 + \theta - 3)t^2$. Posons $\tau = \theta^2 - \theta + 1$. C'est un élément de A associé à π_{13}.

Lemme 10. *L'élément τF_1 est un carré dans K.*

Démonstration. On a $N_{K/\mathbb{Q}}(F_1) \in 13\mathbb{Z}^2$ et les F_i sont premiers entre eux en dehors de π_{13}, donc il existe des entiers n_i égaux à 0 ou 1 tels que

$$F_1 \equiv \pi_{13}(-1)^{n_0} u_1^{n_1} u_2^{n_2} \bmod K^{*2}, \quad n_0 + n_1 \equiv 0 \bmod 2.$$

En exprimant cette congruence dans $K^*_{\mathfrak{p}_2}$, on vérifie que cela entraîne $(n_0, n_1, n_2) = (1, 1, 0)$. Le lemme en résulte car on a $-u_1\pi_{13} = \tau$. ∎

On déduit du lemme 10 et de la proposition 3.1 que

$$\tau(s^2 - 4t^2)(s^2 - \theta st + (\theta^2 + \theta - 3)t^2) \in K^2,$$

et $t/s + 1/2$ est l'abscisse d'un point de $\mathcal{D}'(K)$. Par ailleurs, on a $E'(K) = \{T_0\}$ et $\psi(T_0) = (1, 0)$. Il en résulte que les seuls points de $\mathcal{D}'(K)$ sont $(0, 0)$ et $(1, 0)$, ce qui conduit à $\alpha = \pm 2$ et à l'ensemble $D_{13}(\mathbb{Q})$ annoncé.

Cela termine la démonstration du théorème si $p = 13$.

7. Détermination de $C_{17}(\mathbb{Q})$ et $D_{17}(\mathbb{Q})$

7.1. L'ensemble $C_{17}(\mathbb{Q})$. Considérons l'abscisse α d'un point de $\varphi_1(C_{17}(\mathbb{Q}))$. On pose $\alpha = s/t$, où s et t sont deux entiers premiers entre eux et $F_1 = s^2 - \theta_4 st + \theta t^2$ (cf. le formulaire).

Lemme 11. *L'un des éléments F_1 et θF_1 est un carré dans K.*

Démonstration. Les conjugués de F_1 sont premiers entre eux deux à deux en dehors de π_{17}. Puisque $G_8(s, t) \in \mathbb{Z}^2$, il existe des entiers n_i égaux à 0 ou 1 tels que

$$F_1 \equiv (-1)^{n_0} \prod_{i=1}^{3} u_i^{n_i} \pi_{17}^{n_4} \bmod K^{*2}. \tag{20}$$

On a $n_3 = n_4 = 0$. On exprime alors la condition (20) dans les complétés de K en les deux idéaux premiers $\mathfrak{p}_2$ et $\mathfrak{p}_2'$ de A. En utilisant le fait que $v_{\mathfrak{p}_2}(F_1) = v_{\mathfrak{p}_2'}(F_1) = 0$, on obtient le résultat. ∎

7.1.1. *Cas où $F_1 \in K^2$.* Supposons que F_1 soit un carré dans K. Dans ce cas, on a

$$(s^2 - 4t^2)F_1 \in K^2,$$

d'où il résulte que t/s est l'abscisse d'un point de $\mathcal{D}(K)$. Démontrons que si $(u, v) \in \mathcal{D}(K)$ est un point d'abscisse dans $\mathbb{Q}$, on a

$$(u, v) \in \{(-1/2, 0), (1/2, 0), (0, -1), (0, 1)\}.$$

On a $\psi(T_0 + 2N_1) = (1/2, 0)$, $\psi(2N_1) = (-1/2, 0)$ et il s'agit de démontrer l'énoncé suivant :

PROPOSITION 7.1. *Les seuls points $N \in E(K) \setminus \{O, -M_1\}$ tels que $u(N) \in \mathbb{Q}$ sont $2N_1$ et $T_0 + 2N_1$.*

Démonstration. Vérifions d'abord que les points N_1 et N_2 de $E(K)$ sont $\mathbb{Z}$-linéairement indépendants. On calcule pour cela le régulateur R_E de E/K (cf. [13, p. 233]), en utilisant l'algorithme écrit par J. Silverman permettant de déterminer la hauteur canonique d'un point d'une courbe elliptique sur un corps de nombres ([14]). On a programmé cet algorithme et l'on pourra trouver le programme *hc* (à l'adresse http://www.math.jussieu.fr/~ivorra) fonctionnant avec le logiciel PARI, où cet algorithme est implanté. En notant $\widehat{h}_E$ la hauteur canonique sur E, on constate que

$$\widehat{h}_E(N_1) \approx 0.0694452, \quad \widehat{h}_E(N_2) \approx 0.2957562, \quad \widehat{h}_E(N_1 + N_2) \approx 0.5491700,$$

ce qui conduit à $R_E \approx 0.048311$. Puisque R_E est non nul, cela prouve notre assertion.

Considérons alors un point $N \in E(K) \setminus \{O, -M_1\}$ distinct de $2N_1$ et de $T_0 + 2N_1$. On peut supposer comme dans les cas précédents que N appartient à U. La courbe E/K a bonne réduction en $\mathfrak{p}_3$. Le groupe $\widetilde{E}_{\mathfrak{p}_3}(k_{\mathfrak{p}_3})$ est d'ordre 86 et les points $\pi_{\mathfrak{p}_3}(N_1)$, $\pi_{\mathfrak{p}_3}(N_2)$ sont d'ordre 43. On pose

$$Q_1 = 43N_1 \in E_1(K), \quad Q_2 = 43N_2 \in E_1(K).$$

On a

$$\widetilde{E}_{\mathfrak{p}_3}(k_{\mathfrak{p}_3}) = \mathbb{Z}\pi_{\mathfrak{p}_3}(N_1) \oplus \mathbb{Z}\pi_{\mathfrak{p}_3}(T_0). \tag{21}$$

Soit $\mathfrak{S}$ l'ensemble des points de $E(K)$ qui s'écrivent sous la forme

$$hT_0 + jN_1, \quad h = 0, 1 \text{ et } j = -21, \ldots, 21.$$

On a $M_1 = -4N_1$. D'après (21), l'application $\pi_{\mathfrak{p}_3}$ induit une bijection de $\mathfrak{S}$ sur $\widetilde{E}_{\mathfrak{p}_3}(k_{\mathfrak{p}_3})$. Il existe donc $S \in \mathfrak{S}$ tel que $N - S$ soit dans $E_1(K)$. En utilisant le lemme 24 (appendice A), on constate qu'en changeant au besoin N par $-M_1 - N$, on peut supposer que

$$N = S + P \quad \text{où } S \in \{-6N_1, -4N_1, O, 2N_1, T_0 + 2N_1\} \text{ et } P \in E_1(K).$$

Soient H le sous-groupe d'indice fini de $E_1(K)$ engendré par Q_1 et Q_2 et Γ le sous-$\mathbb{F}_3$-espace vectoriel de $k_{\mathfrak{p}_3}$ engendré par les $\eta_{\mathfrak{p}_3}(z(Q))$ où $Q \in H \setminus \{O\}$ (cf. l'appendice B). Notons Γ' le sous-$\mathbb{F}_3$-espace vectoriel de $k_{\mathfrak{p}_3}$ engendré par $1 + 2\xi + 2\xi^2 + \xi^3$ et $2\xi + \xi^2$.

LEMME 12. *On a $\Gamma = \Gamma'$. En particulier, pour tout $R \in E_1(K)$ non nul, $\eta_{\mathfrak{p}_3}(z(R))$ appartient à Γ' et l'on a $\eta_{\mathfrak{p}_3}(z(R)) \neq \pm 1$.*

Démonstration. On a

$$\eta_{\mathfrak{p}_3}(z(Q_1)) = 1 + 2\xi + 2\xi^2 + \xi^3, \quad \eta_{\mathfrak{p}_3}(z(Q_2)) = 2\xi + \xi^2.$$

Par suite, Γ' est contenu dans Γ. Inversement, soit Q un élément de $H \setminus \{O\}$. Il s'agit de démontrer que $\eta_{\mathfrak{p}_3}(z(Q))$ appartient à Γ'. Il existe n_1 et n_2 dans $\mathbb{Z}$ tels que $Q = n_1Q_1 + n_2Q_2$.

Si $n_1n_2 = 0$, alors $\eta_{\mathfrak{p}_3}(z(Q))$ est égal à $\pm\eta_{\mathfrak{p}_3}(z(Q_1))$ ou à $\pm\eta_{\mathfrak{p}_3}(z(Q_2))$, d'où le résultat dans ce cas.

Supposons $n_1n_2 \neq 0$. Posons $z_1 = z(n_1Q_1)$ et $z_2 = z(n_2Q_2)$. On a

$$\eta_{\mathfrak{p}_3}(z_1) = \pm(1 + 2\xi + 2\xi^2 + \xi^3), \quad \eta_{\mathfrak{p}_3}(z_2) = \pm(2\xi + \xi^2).$$

Puisque $\eta_{\mathfrak{p}_3}(z_1) + \eta_{\mathfrak{p}_3}(z_2) \neq 0$, $\eta_{\mathfrak{p}_3}(z_1 + z_2)$ appartient à Γ' (condition (82), appendice B). Par ailleurs,

$$z(Q) = \mathfrak{F}(z_1, z_2).$$

Le fait que $v_{\mathfrak{p}_3}(z_1 + z_2) = \mathrm{Min}(v_{\mathfrak{p}_3}(z_1), v_{\mathfrak{p}_3}(z_2))$ (car $\eta_{\mathfrak{p}_3}(z_1) + \eta_{\mathfrak{p}_3}(z_2) \neq 0$) et l'égalité (70) (appendice B) impliquent alors

$$\eta_{\mathfrak{p}_3}(z(Q)) = \eta_{\mathfrak{p}_3}(z_1 + z_2),$$

ce qui prouve notre assertion.

Le lemme 26 (appendice B) entraîne alors le résultat. ∎

LEMME 13. *L'indice de H dans $E_1(K)$ est premier à 3.*

Démonstration. Supposons que cet indice soit divisible par 3. Dans ce cas, il existe un point $P \in E_1(K)$ tel que $3P$ soit dans H sans que P le soit. Compte tenu du fait que le sous-groupe de torsion de $E(K)$ soit d'ordre 2, il en résulte que l'un des points N_1, N_2, $N_1 + N_2$ et $N_1 - N_2$ appartient à $3E(K)$.

Supposons qu'il existe $R \in E(K)$ tel que $N_1 = 3R$. Considérons l'idéal $\mathfrak{p}$ de A engendré par $-\theta^3 - 2\theta^2 + 5\theta + 5$. C'est l'un des quatre idéaux de A au-dessus de 47. L'ordre de $\widetilde{E}_{\mathfrak{p}}(k_{\mathfrak{p}})$ est 54 et celui de $\pi_{\mathfrak{p}}(N_1)$ est 27. On en déduit que $\pi_{\mathfrak{p}}(R)$ est d'ordre multiple de 81, d'où une contradiction dans ce cas. De même, on vérifie que $\pi_{\mathfrak{p}}(N_2)$ et $\pi_{\mathfrak{p}}(N_1 - N_2)$ sont d'ordre 54, ce qui entraîne de nouveau que N_2 et $N_1 - N_2$ ne sont pas dans $3E(K)$.

Supposons qu'il existe $R \in E(K)$ tel que $N_1 + N_2 = 3R$. On considère l'idéal $\mathfrak{p}'$ de A engendré par $-\theta^3 + 7\theta - 1$. C'est l'un des quatre idéaux de A au-dessus de 89. L'ordre de $\widetilde{E}_{\mathfrak{p}'}(k_{\mathfrak{p}'})$ est 90 et celui de $\pi_{\mathfrak{p}'}(N_1)$ est 45. Par suite, l'ordre de $\pi_{\mathfrak{p}'}(R)$ est multiple de 27, d'où une contradiction et le lemme. ∎

1) Supposons $S = O$. On a $u(N) \equiv -2z(P) \bmod z(P)^2$, et donc par conséquent $\eta_{\mathfrak{p}_3}(u(N)) = \eta_{\mathfrak{p}_3}(z(P))$, qui, d'après le lemme 12, n'est pas dans $\mathbb{F}_3$, donc $u(N)$ n'est pas dans $\mathbb{Q}$.

2) Supposons $S = -6N_1$. La condition 8 de l'appendice B est réalisée et l'on a dans $A_{\mathfrak{p}_3}$ la congruence

$$\frac{1}{u(N)} \equiv \sum_{i=0}^{3} \varrho_i z(P)^i \bmod 3^4,$$

avec

$$\varrho_0 = 3\theta^3 + 75\theta^2 + 45\theta + 6, \qquad \varrho_2 = 37\theta^3 + 35\theta^2 + 17\theta + 6,$$
$$\varrho_1 = 78\theta^3 + 73\theta^2 + 14\theta + 4, \qquad \varrho_3 = 70\theta^3 + 61\theta^2 + 59\theta + 29.$$

On a $v_{\mathfrak{p}_3}(\varrho_0) = 1$ et $v_{\mathfrak{p}_3}(\varrho_1) = 0$, de sorte que l'on ne peut pas conclure directement. D'après le lemme 13, il existe deux éléments n_1 et n_2 de $\mathbb{Z}_3$ tels que $P = n_1 Q_1 + n_2 Q_2$. On déduit alors de l'égalité (95) (appendice B) que

$$\frac{1}{u(N)} = \Phi_S^{(0)} + \Phi_S^{(1)}\theta + \Phi_S^{(2)}\theta^2 + \Phi_S^{(3)}\theta^3,$$

avec

$$\begin{aligned}
\Phi_S^{(0)} &= 54n_1^4 + (27n_2 + 45)n_1^3 + 72n_1^2 + (27n_2^3 + 54n_2^2 + 63n_2 + 21)n_1 \\
&\quad + (27n_2^4 + 72n_2^3 + 9n_2^2 + 15n_2 + 6), \\
\Phi_S^{(1)} &= 63n_1^3 + (54n_2 + 9)n_1^2 + 72n_2 n_1 + (45n_2^3 + 72n_2^2 + 9n_2 + 45), \\
\Phi_S^{(2)} &= 27n_1^4 + 27n_2 n_1^3 + (27n_2 + 18)n_1^2 + (27n_2^2 + 63n_2 + 69)n_1 \\
&\quad + (54n_2^4 + 72n_2^3 + 9n_2^2 + 51n_2 + 75), \\
\Phi_S^{(3)} &= 54n_1^4 + 72n_1^3 + 54n_2 n_1^2 + (54n_2^3 + 27n_2^2 + 45n_2 + 75)n_1 \\
&\quad + (27n_2^4 + 27n_2^3 + 36n_2^2 + 54n_2 + 3).
\end{aligned}$$

On constate alors que les séries $\Phi_S^{(j)}(X_1, X_2)$ pour $j = 1, 2, 3$ n'ont pas de zéros communs modulo 81, ce qui prouve que $u(N)$ n'est pas dans $\mathbb{Q}$.

3) Supposons $S = -4N_1$, i.e. $S = M_1$. Alors $v_{\mathfrak{p}_3}(3x_S^2 + 2a_2 x_S + a_4 - dy_S) = 0$, la condition 9 de l'appendice B est satisfaite et

$$u(N) \equiv \theta^3 + \theta^2 + 2\theta + 2 \bmod 3\,;$$

puisque $v_{\mathfrak{p}_3}(\theta^3 + \theta^2 + 2\theta + 2) = 0$, on obtient $\eta_{\mathfrak{p}_3}(u(N)) = \xi^3 + \xi^2 + 2\xi + 2$.

4) Supposons $S = 2N_1$. Dans ce cas

$$u(N) + 1/2 \equiv \varrho_2 z(P)^2 \bmod z(P)^3, \quad \text{avec } \varrho_2 = -\theta^3 - 2\theta^2 + 5\theta + 7 \text{ et } v_{\mathfrak{p}_3}(\varrho_2) = 0.$$

Il en résulte que

$$\eta_{\mathfrak{p}_3}(u(N) + 1/2) = \eta_{\mathfrak{p}_3}(\varrho_2)\eta_{\mathfrak{p}_3}(z(P))^2.$$

D'après le lemme 12, il existe α_1 et α_2 dans $\mathbb{F}_3$ non tous les deux nuls tels que

$$\eta_{\mathfrak{p}_3}(z(P)) = \alpha_1(1 + 2\xi + 2\xi^2 + \xi^3) + \alpha_2(2\xi + \xi^2) \in \Gamma'.$$

Par ailleurs, on a $\eta_{\mathfrak{p}_3}(\varrho_2) = 2\xi^3 + \xi^2 + 2\xi + 1$. On vérifie alors que $\eta_{\mathfrak{p}_3}(\varrho_2)\eta_{\mathfrak{p}_3}(z(P))^2$ n'est pas dans $\mathbb{F}_3$ et $u(N)$ n'est pas dans $\mathbb{Q}$.

5) Supposons $S = T_0 + 2N_1$. On a

$$u(N) - \frac{1}{2} \equiv \varrho_2 z(P)^2 \bmod z(P)^3, \quad \text{avec } \varrho_2 = -\theta^3 - 2\theta^2 + 3\theta - 1 \text{ et } v_{\mathfrak{p}_3}(\varrho_2) = 0.$$

et l'on vérifie comme ci-dessus que $\eta_{\mathfrak{p}_3}(\varrho_2)\eta_{\mathfrak{p}_3}(z(P))^2$ n'est pas dans $\mathbb{F}_3$.

Cela prouve la proposition 7.1. ∎

On a ainsi démontré que si F_1 est un carré dans K, alors on a $\alpha = \pm 2$.

7.1.2. *Cas où* $F_1 \in \theta K^2$. On suppose que θF_1 est un carré dans K. Dans ce cas,

$$(s^2 - 4t^2)\theta F_1 \in K^2,$$

d'où il résulte que $t/s + 1/2$ est l'abscisse d'un point de $\mathcal{D}'(K)$. Par ailleurs, $E'(K)$ est de rang 0 et l'on a $E'(K) = \{O, T_0\}$. Les égalités $\psi(O) = (0,0)$ et $\psi(T_0) = (1,0)$ entraînent alors $t/s = \pm 1/2$.

Dans les deux cas envisagés ci-dessus, on a $\alpha = \pm 2$, et l'on obtient ainsi la description de $C_{17}(\mathbb{Q})$.

7.2. L'ensemble $D_{17}(\mathbb{Q})$**.** Considérons l'abscisse α d'un point de $\varphi_1(D_{17}(\mathbb{Q}))$. On pose $\alpha = s/t$, où s et t sont deux entiers premiers entre eux.

LEMME 14. *L'un des éléments* $-u_3\pi_{17}F_1$ *et* $-u_1u_3\pi_{17}F_1$ *est un carré dans* K.

Démonstration. On a $G_8(s,t) \in 17\mathbb{Z}^2$, donc il existe des entiers n_i égaux à 0 ou 1 tels que

$$F_1 \equiv \pi_{17}(-1)^{n_0} \prod_{i=1}^{3} u_i^{n_i} \bmod K^{*2}.$$

On a dans ce cas $n_3 = 1$. En exprimant cette congruence dans $K^*_{\mathfrak{p}_2}$ et $K^*_{\mathfrak{p}'_2}$, on vérifie que cela entraîne $(n_0, n_1, n_2) = (1,0,0)$ ou $(1,1,0)$. D'où le lemme. ∎

1) Supposons que $-u_3\pi_{17}F_1$ soit un carré dans K. Dans ce cas,

$$-(s^2 - 4t^2)u_3\pi_{17}F_1 \in K^2,$$

d'où il résulte que $t/s + 1/2$ est l'abscisse d'un point de $\mathcal{D}''(K)$. On a $E''(K) = \{O, T_0\}$, ce qui conduit, comme ci-dessus, à $\alpha = \pm 2$.

2) Si $-u_1u_3\pi_{17}F_1$ est un carré dans K, on écrit

$$-(s^2 - 4t^2)u_1u_3\pi_{17}F_1 \in K^2,$$

et l'on constate que $t/s + 1/2$ est l'abscisse d'un point de $\mathcal{D}'''(K)$. On a $E'''(K) = \{O, T_0\}$ et l'on obtient de nouveau $\alpha = \pm 2$.

On en déduit alors la détermination de $D_{17}(\mathbb{Q})$.

Cela termine la démonstration du théorème 2.

Formulaire

I. Cas où $p = 11$

Le corps K

K	$K = \mathbb{Q}(\theta)$	$\theta^5 + \theta^4 - 4\theta^3 - 3\theta^2 + 3\theta + 1 = 0$	
Conjugués de θ	$\theta_1 = \theta$ $\theta_4 = \theta^3 - 3\theta$	$\theta_2 = \theta^2 - 2$ $\theta_5 = \theta^4 - 4\theta^2 + 2$	$\theta_3 = -\theta^4 - \theta^3 + 3\theta^2 + 2\theta - 1$
Anneau d'entiers	$A = \mathbb{Z}[\theta]$		
Unités	$u_1 = \theta$ $u_4 = \theta^2 + \theta - 1$ $N_{K/\mathbb{Q}}(u_1) = -1$ $N_{K/\mathbb{Q}}(u_4) = 1$	$u_2 = \theta^4 - 3\theta^2 + 1$ $N_{K/\mathbb{Q}}(u_2) = 1$	$u_3 = \theta^3 - 2\theta$ $N_{K/\mathbb{Q}}(u_3) = 1$
Idéaux	$2.A = \mathfrak{p}_2$	$3.A = \mathfrak{p}_3$ $\pi_{11} = \theta^4 + \theta^3 - 3\theta^2 - \theta + 1$	$11.A = (\mathfrak{p}_{11}.A)^5$ $N_{K/\mathbb{Q}}(\pi_{11}) = -11$
$G_5(s,t)$ Factorisation	$s^5 + s^4t - 4s^3t^2 - 3s^2t^3 + 3st^4 + t^5$ $\prod_{i=1}^{5}(s - t\theta_i)$		

Les quartiques

Quartiques: $v^2 = au^4 + bu^3 + cu^2 + du + e$		
$\mathcal{D}/K$	$a = -4\theta^3 + 8\theta$ $c = \theta^3 - 2\theta - 4$ $e = 1$	$b = 4\theta^2 + 4\theta - 8$ $d = -\theta^2 - \theta + 2$
$\mathcal{D}'/K$	$a = -64\theta^3 - 56\theta^2 + 24\theta - 16$ $c = -88\theta^3 + 198\theta^2 + 242\theta - 220$ $e = 0$	$b = 48\theta^4 - 120\theta^3 - 36\theta^2 + 180\theta - 112$ $d = -44\theta^4 - 22\theta^3 + 165\theta^2 + 55\theta - 132$
$\mathcal{D}''/K$	$a = -8\theta^4 - 24\theta^3 + 17\theta^2 + 58\theta + 15$ $c = -66\theta^4 - 99\theta^3 + 154\theta^2 + 275\theta + 77$ $e = 0$	$b = -44\theta^4 - 99\theta^3 + 99\theta^2 + 242\theta + 55$ $d = -22\theta^4 - 33\theta^3 + 66\theta^2 + 110\theta + 11$

Les courbes elliptiques

E/K: $y^2 = x^3 + a_2x^2 + a_4x + a_6$		
Coefficients	$a_2 = \theta^3 - 2\theta - 4$ $a_6 = 28\theta^4 - 56\theta^3 - 72\theta^2 + 108\theta + 72$	$a_4 = -4\theta^4 + 8\theta^3 + 12\theta^2 - 16\theta - 16$
Torsion : $(\mathbb{Z}/2\mathbb{Z})^2$	$T_0 = (-\theta^3 + 2\theta + 4, 0)$ $T_2 = (-2\theta^2 + 2\theta + 4, 0)$	$T_1 = (2\theta^2 - 2\theta - 4, 0)$
Rang r de $E(K)$ Point d'ordre infini	$r = 1$ $N_1 = (-2\theta^4 + 2\theta^3 + 8\theta^2 - 8\theta, 10\theta^4 - 8\theta^3 - 36\theta^2 + 30\theta + 10)$	

E'/K: $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = -88\theta^3 + 198\theta^2 + 242\theta - 220$ $a_4 = -484\theta^4 + 10648\theta^3 - 101640^2 - 19360\theta + 17424$ $a_6 = -532400^4 - 234256\theta^3 + 308792\theta^2 + 393976\theta - 383328$
Torsion : $(\mathbb{Z}/2\mathbb{Z})^2$	$T_0 = (-44\theta^3 - 66\theta^2 + 22\theta + 44, 0)$ $T_1 = (44\theta^4 + 44\theta^3 - 154\theta^2 - 110\theta + 88, 0)$ $T_2 = (-44\theta^4 + 88\theta^3 + 22\theta^2 - 154\theta + 88, 0)$
Rang r de $E(K)$ Point d'ordre infini	$r = 1$ $N_1 = (-44\theta^4 + 44\theta^3 + 66\theta^2 - 22\theta + 88, -1232\theta^4 + 2464\theta^2 + 528\theta + 88)$

E'''/K: $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = -66\theta^4 - 99\theta^3 + 154\theta^2 + 275\theta + 77$ $a_4 = -5566\theta^4 - 10043\theta^3 + 13068\theta^2 + 26741\theta + 6413$ $a_6 = -1450790^4 - 271524\theta^3 + 352715\theta^2 + 736043\theta + 175692$
Torsion : $(\mathbb{Z}/2\mathbb{Z})^2$	$T_0 = (33\theta^4 + 55\theta^3 - 88\theta^2 - 165\theta - 44, 0)$, $T_1 = (22\theta^4 + 11\theta^3 - 55\theta^2 - 44\theta - 11, 0)$ $T_2 = (11\theta^4 + 33\theta^3 - 11\theta^2 - 66\theta - 22, 0)$
Rang r de $E(K)$	$r = 0$

II. Cas où $p = 13$

Le corps K

K	$K = \mathbb{Q}(\theta)$	$\theta^3 + \theta^2 - 4\theta + 1 = 0$	
Conjugués de θ	$\theta_1 = \theta$	$\theta_2 = -\theta^2 - 2\theta + 2$	$\theta_3 = \theta^2 + \theta - 3$
Anneau d'entiers	$A = \mathbb{Z}[\theta]$		
Unités	$u_1 = \theta$ $N_{K/\mathbb{Q}}(u_1) = -1$	$u_2 = \theta - 1$ $N_{K/\mathbb{Q}}(u_2) = 1$	
Idéaux	$2.A = \mathfrak{p}_2$ $\pi_{13} = \theta^2 - 3$	$3.A = \mathfrak{p}_3$ $N_{K/\mathbb{Q}}(\pi_{13}) = 13$	$13.A = (\pi_{13}.A)^3$
$G_6(s,t)$ Factorisation	$-t^6 + 3st^5 + 6s^2t^4 - 4s^3t^3 - 5s^4t^2 + s^5t + s^6$ $(s^2 - \theta st + \theta_3t^2)(s^2 - \theta_2st + \theta t^2)(s^2 - \theta_3st + \theta_2t^2)$		

Les quartiques

Quartiques $v^2 = au^4 + bu^3 + cu^2 + du + e$					
$\mathcal{D}/K$	$a = -4\theta^2 - 4\theta + 12$	$b = 4\theta$	$c = \theta^2 + \theta - 7$	$d = -\theta$	$e = 1$
$\mathcal{D}'/K$	$a = -8\theta^2 + 4\theta + 8$	$b = 8\theta^2 + 12\theta - 20$	$c = -2\theta^2 - 21\theta + 12$	$d = 2\theta^2 + 5\theta$	$e = 0$

Les courbes elliptiques

E/K: $y^2 = x^3 + a_2x^2 + a_4x + a_6$			
Coefficients	$a_2 = \theta^2 + \theta - 7$	$a_4 = 12\theta^2 + 16\theta - 48$	$a_6 = -84\theta^2 - 108\theta + 320$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = (-\theta^2 - \theta + 7, 0)$		
Rang r de $E(K)$ Point d'ordre infini	$r = 1$ $N_1 = (-2\theta^2 - 4\theta + 8, 2\theta)$		

E'/K: $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = -2\theta^2 - 21\theta + 12 \quad a_4 = 36\theta^2 + 76\theta - 48 \quad a_6 = -52\theta^2 - 104\theta + 52$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = (2\theta^2 + 5\theta, 0)$
Rang r de $E(K)$	$r = 0$

III. Cas où $p = 17$

Le corps K

K	$K = \mathbb{Q}(\theta)$ $\quad \theta^4 + \theta^3 - 6\theta^2 - \theta + 1 = 0$
Conjugués de θ	$\theta_1 = \theta \quad \theta_2 = \theta^3 + \theta^2 - 6\theta - 1 \quad \theta_3 = -\frac{1}{2}\theta^3 + 3\theta - \frac{3}{2}$ $\theta_4 = -\frac{1}{2}\theta^3 - \theta^2 + 2\theta + \frac{3}{2}$
Anneau d'entiers	$A = \mathbb{Z}[1, \theta, \theta^2, (\theta^3 + 1)/2]$
Unités	$u_1 = \theta \quad u_2 = \frac{1}{2}\theta^3 + \theta^2 - 2\theta - \frac{3}{2} \quad u_3 = \frac{1}{2}\theta^3 + \theta^2 - 3\theta - \frac{3}{2}$ $N_{K/\mathbb{Q}}(u_1) = 1 \quad N_{K/\mathbb{Q}}(u_2) = 1 \quad N_{K/\mathbb{Q}}(u_3) = -1$
Idéaux	$2.A = \mathfrak{p}_2\mathfrak{p}_2' \quad \mathfrak{p}_2 = (\theta + 1)A \quad \mathfrak{p}_2' = (-\frac{1}{2}\theta^3 - \theta^2 + 2\theta + \frac{1}{2})A$ $3.A = \mathfrak{p}_3$ $17.A = (\pi_{17}.A)^4 \quad \pi_{17} = -\frac{1}{2}\theta^3 - \theta^2 + \theta + \frac{3}{2} \quad N_{K/\mathbb{Q}}(\pi_{17}) = -17$
$G_8(s,t)$ Factorisation	$t^8 - 4st^7 - 10s^2t^6 + 10s^3t^5 + 15s^4t^4 - 6s^5t^3 - 7s^6t^2 + s^7t + s^8$ $(s^2 - \theta_4st + \theta t^2)(s^2 - \theta_3st + \theta_2t^2)(s^2 - \theta st + \theta_3t^2)(s^2 - \theta_2st + \theta_4t^2)$

Les quartiques

Quartiques $v^2 = au^4 + bu^3 + cu^2 + du + e$			
$\mathcal{D}/K$	$a = -4\theta$	$b = -2\theta^3 - 4\theta^2 + 8\theta + 6$	$c = \theta - 4$
	$d = \frac{1}{2}\theta^3 + \theta^2 - 2\theta - \frac{3}{2}$	$e = 1$	
$\mathcal{D}'/K$	$a = -4\theta^2$	$b = -2\theta^3 + 4\theta^2 + 4\theta + 2$	$c = 3\theta^3 + \theta^2 - 10\theta - 3$
	$d = -\theta^3 - \theta^2 + 6\theta + 1$	$e = 0$	
$\mathcal{D}''/K$	$a = 2\theta^3 - 8\theta^2 - 8\theta - 2$	$b = -14\theta^3 + 56\theta + 26$	$c = \frac{39}{2}\theta^3 + 18\theta^2 - 90\theta - \frac{91}{2}$
	$d = -\frac{15}{2}\theta^3 - 10\theta^2 + 42\theta + \frac{43}{2}$	$e = 0$	
$\mathcal{D}'''/K$	$a = -10\theta^3 + 4\theta^2 - 2$	$b = 14\theta^3 - 28\theta^2 + 12\theta + 14$	$c = -\frac{3}{2}\theta^3 + 27\theta^2 - 26\theta - \frac{39}{2}$
	$d = -\frac{5}{2}\theta^3 - 3\theta^2 + 14\theta + \frac{15}{2}$	$e = 0$	

Les courbes elliptiques

E/K: $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = \theta - 4 \quad a_4 = 2\theta^3 - 4\theta - 10 \quad a_6 = -10\theta^3 + 8\theta^2 + 8\theta + 38$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = (4 - \theta, 0)$
Rang r de $E(K)$ Point d'ordre infini $\mathbb{Z}$-indépendants	$r = 2$ $N_1 = (-2\theta + 4, \theta^3 - 4\theta + 1)$ $N_2 = (-\theta^3 - \theta^2 + 7\theta + 1, \theta^3 - \theta^2 - 4\theta + 2)$

E'/K: $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = 3\theta^3 + \theta^2 - 10\theta - 3 \quad a_4 = -2\theta^3 - 4\theta^2 + 16\theta + 6 \quad a_6 = -4$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = (-\theta^3 - \theta^2 + 6\theta + 1, 0)$
Rang r de $E(K)$	$r = 0$

E''/K: $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = \frac{39}{2}\theta^3 + 18\theta^2 - 90\theta - \frac{91}{2}$ $\quad a_4 = -328\theta^3 - 456\theta^2 + 1848\theta + 972$ $a_6 = 1448\theta^3 + 1936\theta^2 - 8016\theta - 4204$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = (-\frac{15}{2}\theta^3 - 10\theta^2 + 42\theta + \frac{43}{2}, 0)$
Rang r de $E(K)$	$r = 0$

E'''/K: $y^2 = x^3 + a_2x^2 + a_4x + a_6$	
Coefficients	$a_2 = -\frac{3}{2}\theta^3 + 27\theta^2 - 26\theta - \frac{39}{2}$ $\quad a_4 = 8\theta^3 - 124\theta^2 + 200\theta + 128$ $a_6 = -12\theta^3 + 144\theta^2 - 304\theta - 184$
Torsion : $\mathbb{Z}/2\mathbb{Z}$	$T_0 = (-\frac{5}{2}\theta^3 - 3\theta^2 + 14\theta + \frac{15}{2}, 0)$
Rang r de $E(K)$	$r = 0$

Appendice A. Quartiques et équations de Weierstrass

Soient K_0 un corps algébriquement clos de caractéristique différente de 2 et K un sous-corps de K_0. On considère des éléments a, b, c, d et e de K et le polynôme

$$f = aX^4 + bX^3 + cX^2 + dX + e \in K[X].$$

Soit $\mathcal{D}/K$ la courbe affine d'équation

$$v^2 = f(u). \tag{22}$$

On suppose que les conditions suivantes sont satisfaites :

1. on a $a \neq 0$;
2. $\mathcal{D}$ est lisse, i.e. le discriminant de f est non nul ;
3. $\mathcal{D}$ a un point (α, β) rationnel sur K.

On note $\widehat{\mathcal{D}}$ la complétée projective de $\mathcal{D}$ d'équation homogène

$$v^2w^2 = w^4 f(u/w).$$

Le point $J = [0, 1, 0] \in \widehat{\mathcal{D}}(K)$ est l'unique point à l'infini de $\mathcal{D}$. C'est un point singulier de $\widehat{\mathcal{D}}(K)$. La compactifiée lisse de $\mathcal{D}$ est une courbe de genre 1. Plus précisément, il résulte des hypothèses faites qu'il existe une courbe elliptique E/K et un isomorphisme birationnel $\psi : E \to \widehat{\mathcal{D}}$ défini sur K. La détermination d'équations explicites décrivant cette équivalence birationnelle est bien connue. On pourra à ce sujet consulter par exemple le chapitre II de [13]. On explicite dans cet appendice les équations que l'on utilisera dans le texte d'un tel couple (E, ψ). Elles s'obtiennent par des procédés standard utilisant le théorème de Riemann–Roch que l'on ne rappelera pas ici (cf. [13]). On définit par ailleurs au paragraphe 3 de cet appendice une fonction sur E obtenue en composant la première fonction coordonnée sur $\mathcal{D}$ avec ψ. Au cours de la démonstration du théorème 2, on est confronté à l'étude de certaines propriétés de rationalité de cette fonction. On démontre aux paragraphes 4 et 5 de cet appendice certains résultats que l'on utilisera concernant cette étude.

Quitte à effectuer une translation sur u, on peut supposer que $\alpha = 0$; alors $e = \beta^2$. On examinera dans la suite deux cas selon que β est nul ou non.

A.1. Le cas $\beta = 0$. Si β est nul, l'équation (22) s'écrit

$$v^2 = au^4 + bu^3 + cu^2 + du. \tag{23}$$

On dispose du point $P = (0,0) \in \mathcal{D}(K)$. On a $d \neq 0$.

A.1.1. *La courbe elliptique E/K.* Soit E/K la cubique définie sur K par l'équation

$$y^2 = x^3 + cx^2 + bdx + ad^2. \tag{24}$$

Son discriminant est 16 fois celui de f, de sorte que E est une courbe elliptique sur K. Comme il est d'usage, on notera encore E la complétée projective de E d'équation

$$y^2 z = x^3 + cx^2 z + bdxz^2 + ad^2 z^3.$$

On note $O = [0,1,0] \in E(K)$ le point à l'infini de E.

A.1.2. *Les ouverts U et V.* Soit γ une racine carré de ad^2 dans K_0. On considère les points de $E(K_0)$ suivants :

$$M_1 = (0,\gamma), \qquad M_2 = (0,-\gamma). \tag{25}$$

On note U et V les ouverts de E et $\mathcal{D}$ respectivement, définis par

$$U = E \setminus \{O, M_1, M_2\}, \qquad V = \mathcal{D} \setminus \{P\}. \tag{26}$$

A.1.3. *L'isomorphisme de U sur V.* On a l'énoncé suivant :

PROPOSITION A.1. *L'application $\psi : U \to \mathcal{D}$ définie pour tout point $M = (x,y) \in U$ par $\psi(M) = (u,v)$ où*

$$u = d/x, \qquad v = dy/x^2, \tag{27}$$

est un isomorphisme de U sur V. L'application réciproque $\varphi : V \to U$ est définie pour tout point $N = (u,v) \in V$ par $\varphi(N) = (x,y)$ où

$$x = d/u, \qquad y = dv/u^2. \tag{28}$$

Démonstration. Les formules (27) et (28) sont bien définies sur les ouverts U et V respectivement. On vérifie ensuite directement les assertions annoncées. ∎

A.1.4. *Le morphisme $\psi : E \to \widehat{\mathcal{D}}$.* Puisque E est lisse et que $\widehat{\mathcal{D}}$ est projective, l'application rationnelle ψ se prolonge en un unique morphisme, que l'on notera encore ψ, de E sur $\widehat{\mathcal{D}}$. Il est donné par l'énoncé suivant :

LEMME 15.

1. *Pour tout point $M = [x,y,z] \in E \setminus \{O\}$,*

$$\psi(M) = [dxz, dyz, x^2]. \tag{29}$$

   En particulier, $\psi(M_1) = \psi(M_2) = J$.
2. *$\psi(O) = P$.*

Démonstration. En homogénéisant les formules (27), on obtient la formule (29) tout au moins si M est distinct de M_1 et M_2. Par ailleurs, la formule (29) définit un morphisme de $E \setminus \{O\}$ dans $\widehat{\mathcal{D}}$ qui se prolonge en un morphisme χ de E sur $\widehat{\mathcal{D}}$. Les morphismes ψ et χ coïncident sur l'ouvert $E \setminus \{O, M_1, M_2\}$, ils sont donc égaux ; d'où l'assertion 1.

Puisque ψ est surjectif de E sur $\widehat{\mathcal{D}}$ et que P n'appartient pas à $\psi(E \setminus \{O\})$, on a donc $\psi(O) = P$. ∎

A.2. Le cas $\beta \neq 0$. Quitte à remplacer v par v/β et f par f/β^2, on peut supposer que $\beta^2 = 1$. L'équation (22) s'écrit dans ce cas

$$v^2 = au^4 + bu^3 + cu^2 + du + 1, \tag{30}$$

et l'on dispose des points $P = (0, -1)$ et $Q = (0, 1)$ de $\mathcal{D}(K)$.

A.2.1. *La courbe elliptique E/K.* Soit E/K la cubique définie sur K par l'équation

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \tag{31}$$

où les coefficients a_2, a_4 et a_6 sont

$$a_2 = c, \quad a_4 = bd - 4a, \quad a_6 = ad^2 + b^2 - 4ac. \tag{32}$$

Son discriminant est 16 fois celui de f, c'est donc une courbe elliptique définie sur K. On note encore E la complétée projective de E et $O = [0, 1, 0] \in E(K)$.

A.2.2. *Les ouverts U et V.* On définit ici des ouverts U et V de E et $\widehat{\mathcal{D}}$ respectivement, analogues à ceux intervenant dans le paragraphe A.1.2. Considérons une racine carrée γ de $4a$ dans K_0. Posons

$$\lambda = d^2/4 - c. \tag{33}$$

Lemme 16. *Les points $(x, y) \in E(K_0)$ tels que $y - dx/2 - b = 0$, sont*

$$M_1 = (\lambda, d\lambda/2 + b), \quad M_2 = (\gamma, d\gamma/2 + b), \quad M_3 = (-\gamma, -d\gamma/2 + b).$$

Démonstration. L'équation (31) s'écrit aussi

$$y^2 - (dx/2 + b)^2 = (x - \lambda)(x^2 - 4a),$$

d'où le lemme. ∎

On définit U comme étant l'ouvert de E formé des points à distance finie $(x, y) \in E(K_0)$ tels que $x - \lambda \neq 0$ et $y - dx/2 - b \neq 0$. D'après le lemme 16, on a

$$U = E \setminus \{O, -M_1, M_1, M_2, M_3\}. \tag{34}$$

Posons

$$u_0 = \frac{2(\lambda d + 2b)}{\lambda^2 - 4a}, \quad P' = \left(u_0, \frac{\lambda u_0^2}{2} - \frac{du_0}{2} - 1\right) \quad \text{si } \lambda^2 \neq 4a, \tag{35}$$

$$P' = P \quad \text{si } \lambda^2 = 4a. \tag{36}$$

On vérifie que P' appartient à $\mathcal{D}(K)$. L'ouvert V est alors défini par l'égalité

$$V = \mathcal{D} \setminus \{P, P', Q\}. \tag{37}$$

Remarque 2. On utilisera le fait que

$$\lambda^2 \neq 4a \quad \text{ou bien} \quad \lambda d + 2b \neq 0. \tag{38}$$

En effet, les égalités $\lambda^2 = 4a$ et $\lambda d + 2b = 0$ conduisent à une équation de $\mathcal{D}$ de la forme

$$v^2 = (\lambda u^2/2 - du/2 - 1)^2,$$

ce qui contredit la condition 2 du début.

A.2.3. *L'isomorphisme de U sur V.* Il est donné par l'énoncé suivant :

PROPOSITION A.2. *L'application $\psi : U \to \mathcal{D}$ définie pour tout point $M = (x, y) \in U$ par $\psi(M) = (u, v)$ où*

$$u = \frac{2(x - \lambda)}{y - dx/2 - b}, \tag{39}$$

$$v = -1 + \frac{(x - \lambda)(2x^2 + 2cx + bd - dy)}{(y - dx/2 - b)^2}, \tag{40}$$

est un isomorphisme de U sur V. L'application réciproque $\varphi : V \to U$ est définie pour tout point $N = (u, v) \in V$ par $\varphi(N) = (x, y)$ où

$$x = \frac{2(v + 1) + du}{u^2}, \tag{41}$$

$$y = \frac{(du + 4)(v + 1) + 2du + 2cu^2 + bu^3}{u^3}. \tag{42}$$

Démonstration. On remarque d'abord que les formules (39) et (40) sont bien définies sur $E \setminus \{O, M_1, M_2, M_3\}$. Soit M un point de U. On vérifie formellement que $\psi(M)$ appartient à $\mathcal{D}$; le fait que M soit distinct de $-M_1$ et M_1 entraîne l'inclusion $\psi(U) \subseteq V$.

Inversement, on observe que les formules (41) et (42) sont bien définies sur $\mathcal{D} \setminus \{P, Q\}$. Soit $N = (u, v)$ un point de V. On vérifie que $\varphi(N) \in E$. Démontrons que

$$\varphi(N) \neq \pm M_1. \tag{43}$$

Supposons le contraire. On a alors $x - \lambda = 0$, où x est donné par la formule (41). Ainsi

$$v = -1 + \frac{u(\lambda u - d)}{2},$$

et en utilisant l'égalité (30), on obtient

$$u^3((4a - \lambda^2)u/4 + b + \lambda d/2) = 0.$$

On déduit alors de (38) que l'on a $N = P'$, d'où une contradiction et l'assertion (43). On démontre de manière analogue que $\varphi(N)$ est distinct de M_2 et M_3, d'où $\varphi(V) \subseteq U$.

On constate enfin que les applications ψ et φ sont inverses l'une de l'autre. ∎

A.2.4. *Le morphisme $\psi : E \to \widehat{\mathcal{D}}$.* L'application $\psi : U \to V$ se prolonge en un morphisme que l'on note encore ψ de E sur $\widehat{\mathcal{D}}$. L'objectif de ce paragraphe est de l'expliciter.

LEMME 17. *Pour tout point $M = [x, y, z] \in E(K_0)$ distinct de O et M_1 on a l'égalité $\psi(M) = [u, v, w]$ où*

$$u = 2z(x - \lambda z)(y - dx/2 - bz), \tag{44}$$

$$v = (x - \lambda z)(2x^2 + 2cxz + bdz^2 - dyz) - z(y - dx/2 - bz)^2, \tag{45}$$

$$w = z(y - dx/2 - bz)^2. \tag{46}$$

Démonstration. En homogénéisant les formules (39) et (40), on obtient les formules ci-dessus. Il s'agit alors de montrer que u, v et w ne s'annulent pas simultanément si M est

distinct de O et M_1. Supposons pour cela que $u = v = w = 0$ et $M \neq O$; on peut aussi supposer $z = 1$. On a alors

$$y = dx/2 + b, \qquad (x - \lambda)(2x^2 + 2cx + bd - dy) = 0. \tag{47}$$

On en déduit que $x = \lambda$ ou $x^2 = 4a$ (cf. la preuve du lemme 16). Si l'on a $x \neq \lambda$, il résulte de la deuxième égalité de (47) que $x = 0$, d'où $a = 0$, ce qui conduit à une contradiction. On obtient ainsi $x = \lambda$, $y = d\lambda/2 + b$, i.e. $M = M_1$ et le résultat. ∎

Déterminons $\psi(M_1)$. On considère pour cela l'ouvert W de E formé des points à distance finie $(x, y) \in E(K_0)$ tels que

$$x \neq \lambda, \qquad y + dx/2 + b \neq 0. \tag{48}$$

On a

$$W = E \setminus \{O, M_1, -M_1, -M_2, -M_3\}. \tag{49}$$

Lemme 18. *Soit $M = (x, y)$ un point de W. On a $\psi(M) = [u', v', w']$ avec*

$$u' = 2(x^2 - 4a)(y + dx/2 + b), \tag{50}$$

$$v' = 2x(y + dx/2 + b)^2 - d(x^2 - 4a)(y + dx/2 + b) - (x^2 - 4a)^2, \tag{51}$$

$$w' = (x^2 - 4a)^2. \tag{52}$$

Démonstration. On a l'égalité

$$\frac{y - dx/2 - b}{x - \lambda} = \frac{x^2 - 4a}{y + dx/2 + b}.$$

Par ailleurs, on vérifie que

$$2x^2 + 2cx + bd - dy = (x - \lambda)(4\lambda + 2c) + 2(x - \lambda)^2 - d\left(y - \frac{dx}{2} - b + \frac{d}{2}(x - \lambda)\right).$$

D'après les formules (44)–(46), on a donc

$$\frac{u}{(x-\lambda)^2} = 2\left(\frac{x^2 - 4a}{y + dx/2 + b}\right), \qquad \frac{v}{(x-\lambda)^2} = 2x - d\left(\frac{x^2 - 4a}{y + dx/2 + b}\right) - \left(\frac{x^2 - 4a}{y + dx/2 + b}\right)^2,$$

$$\frac{w}{(x-\lambda)^2} = \left(\frac{x^2 - 4a}{y + dx/2 + b}\right)^2.$$

On en déduit que $\psi(M) = [u', v', w']$. ∎

Corollaire A.3. *On a*

$$\psi(M_1) = \begin{cases} P' & \text{si } \lambda^2 \neq 4a, \\ J & \text{si } \lambda^2 = 4a. \end{cases} \tag{53}$$

Démonstration. Les formules (50)–(52) définissent un morphisme $\chi : E \to \widehat{\mathcal{D}}$ qui coïncide avec ψ sur un ouvert non vide de E. Il en résulte que χ et ψ sont égaux sur E. Par ailleurs, compte tenu de (38), on constate que χ est défini au point M_1. On a donc $\psi(M_1) = \chi(M_1)$, d'où le corollaire. ∎

Corollaire A.4. *On a*

$$\psi(M_2) = \psi(M_3) = J. \tag{54}$$

Démonstration. Si $\lambda^2 \neq 4a$, le point M_1 est distinct de M_2 et M_3. Les formules (44)–(46) impliquent alors (54). Supposons $\lambda^2 = 4a$ et par exemple $\lambda = \gamma$. Dans ce cas, on a $M_1 = M_2$, d'où $\psi(M_2) = J$. Par ailleurs, puisque γ est non nul (car $a \neq 0$), M_3 est distinct de $\pm M_1$ et de $-M_2$, $-M_3$. Le lemme 18 entraîne alors le résultat. ∎

COROLLAIRE A.5. *On a*

$$\psi(-M_1) = P. \tag{55}$$

Démonstration. Si $M_1 \neq -M_1$, les formules (44)–(46) impliquent (55). Supposons $M_1 = -M_1$, autrement dit que

$$d\lambda/2 + b = 0.$$

D'après (38), on a $\lambda^2 \neq 4a$ et $\psi(M_1) = P'$ (cor. A.3). D'après (35), on a $u_0 = 0$, puis $P' = P$, d'où le résultat. ∎

LEMME 19. *On a*

$$\psi(O) = Q. \tag{56}$$

Démonstration. En considérant l'équation projective de E, on vérifie que pour tout point $M = [x, y, z]$ dans un ouvert de $E(K_0)$ qui contient O, on a $\psi(M) = [u, v, w]$ avec

$$u = 2(x - \lambda z)(y - dx/2 - bz),$$
$$v = 2(y^2 - a_2x^2 - a_4xz - a_6z^2) - 2\lambda x^2 + (x - \lambda z)(2cx + bdz - dy) - (y - dx/2 - bz)^2,$$
$$w = (y - dx/2 - bz)^2.$$

On en déduit l'égalité (56). ∎

Cela termine la détermination de ψ.

On utilisera l'énoncé suivant :

LEMME 20. *L'application ψ induit une surjection de l'ensemble $E(K) \setminus \{O, -M_1\}$ sur l'ensemble $\mathcal{D}(K) \setminus \{P, Q\}$.*

Démonstration. Considérons un point $R \in \mathcal{D}(K) \setminus \{P, Q\}$. Si R est distinct de P', alors R est dans l'ouvert V, et il existe $M \in E(K) \cap U$ tel que $\psi(M) = R$. Supposons que $R = P'$. On a alors $P \neq P'$. Cela entraîne que $M_1 \neq -M_1$; en effet, si $M_1 = -M_1$, on a $d\lambda + 2b = 0$ et, d'après (38), cela implique $\lambda^2 \neq 4a$. La formule (35) conduit alors à $P = P'$, d'où une contradiction et notre assertion. Par ailleurs, on a $\psi(M_1) = P'$ (cor. A.3), d'où $\psi(M_1) = R$ et le résultat.

A.3. La fonction u sur E. En composant la première fonction coordonnée sur $\mathcal{D}$ avec le morphisme ψ, on obtient une fonction sur E, que l'on notera u, i.e. un morphisme $u : E \to \mathbb{P}^1$ que l'on va expliciter. Considérons pour cela un point $M \in E(K_0)$. En utilisant les propositions A.1 et A.2, le lemme 15 et les résultats ci-dessus, on constate que l'on a les formules suivantes :

1. si $\beta = 0$:

$$u(M) = d/x \quad \text{si } M = (x, y) \in U, \qquad u(M_1) = u(M_2) = \infty, \qquad u(O) = 0.$$

2. si $\beta \neq 0$:

$$u(M) = \frac{2(x-\lambda)}{y - dx/2 - b} \quad \text{si } M = (x,y) \in U,$$
$$u(O) = u(-M_1) = 0, \quad u(M_2) = u(M_3) = \infty,$$
$$u(M_1) = \begin{cases} \dfrac{2(\lambda d + 2b)}{\lambda^2 - 4a} & \text{si } \lambda^2 \neq 4a, \\ \infty & \text{sinon.} \end{cases}$$

A.4. L'involution hyperelliptique. La courbe $\widehat{\mathcal{D}}$ possède un automorphisme d'ordre 2, à savoir l'involution hyperelliptique $i : \widehat{\mathcal{D}} \to \widehat{\mathcal{D}}$ qui est définie pour tout point $(u,v) \in \widehat{\mathcal{D}}(K_0)$ par

$$i((u,v)) = (u,-v), \quad i(J) = J.$$

On en déduit l'existence d'un unique automorphisme I d'ordre 2 de E tel que

$$\psi \circ I = i \circ \psi. \tag{57}$$

On se propose ici de décrire I.

A.4.1. *Cas où $\beta = 0$*

LEMME 21. *Pour tout $M \in E(K_0)$, on a $I(M) = -M$.*

Démonstration. Soit $M = (x,y)$ un point de U. Il suffit de démontrer que

$$\psi(-M) = i \circ \psi(M).$$

Il existe un point $(u,v) \in V$ tel que $x = d/u$ et $y = dv/u^2$. Par définition, on a

$$I(M) = (d/u, -dv/u^2),$$

d'où le lemme. ∎

A.4.2. *Cas où $\beta \neq 0$*

LEMME 22. *Pour tout $M \in E(K_0)$, on a $I(M) = -M_1 - M$.*

Démonstration. Soit $M = (x,y)$ un point de U. Vérifions que

$$\psi(-M_1 - M) = i \circ \psi(M).$$

Il existe un point $(u,v) \in V$ tel que $x = x(u,v)$ et $y = y(u,v)$, où $x(u,v)$ et $y(u,v)$ sont donnés par les formules (41) et (42). Par définition, on a

$$I(M) = (x(u,-v), y(u,-v)).$$

Notons (x_1, y_1) les coordonnées de M_1. On vérifie que le déterminant de la matrice

$$\begin{pmatrix} x(u,v) & x(u,-v) & x_1 \\ y(u,v) & y(u,-v) & y_1 \\ 1 & 1 & 1 \end{pmatrix}$$

est nul, ce qui signifie que les points M, M_1 et $I(M)$ sont alignés, autrement dit, qu'ils sont de somme nulle. D'où le résultat. ∎

Dans les deux cas, que β soit nul ou non, on a l'énoncé suivant :

LEMME 23. *Pour tout $M \in E(K_0)$, on a $u(M) = u(I(M))$.*

Démonstration. Cela résulte des définitions de u et i ainsi que de l'égalité (57). ∎

A.5. Une condition de rationalité. On suppose dans ce paragraphe que K est un corps de nombres et que $K_0 = \mathbb{C}$. On est confronté dans ce travail au problème de la détermination des points de $M \in E(K)$ tels que $u(M)$ appartienne à $\mathbb{Q}$. Notre objectif est ici de démontrer un résultat que l'on utilise pour la résolution de ce problème.

Soit A l'anneau des entiers de K. On suppose que la condition suivante est réalisée :

$$a,\ b,\ c \text{ et } d \text{ appartiennent à } A. \tag{58}$$

Soit $\mathfrak{p}$ un idéal premier de A, de caractéristique résiduelle $p \geq 3$, en lequel E/K a bonne réduction. On note :

- $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$, $A_\mathfrak{p}$ son anneau de valuation et $\mathfrak{M}_\mathfrak{p}$ l'idéal maximal de $A_\mathfrak{p}$;
- $k = A_\mathfrak{p}/\mathfrak{M}_\mathfrak{p}$ le corps résiduel ; c'est une extension finie de $\mathbb{F}_p$;
- $\nu : A_\mathfrak{p} \to k$ la surjection canonique ;
- $\widetilde{E}$ la courbe elliptique sur k déduite de E par réduction ;
- $\pi : E(K_\mathfrak{p}) \to \widetilde{E}(k)$ le morphisme de réduction ;
- $E_1(K_\mathfrak{p})$ le noyau de π et $E_1(K)$ son intersection avec $E(K)$; rappelons que les points à distance finie $(x, y) \in E(K_\mathfrak{p})$ qui n'appartiennent pas à $E_1(K_\mathfrak{p})$ sont caractérisés par le fait que x et y sont dans $A_\mathfrak{p}$ (cf. par exemple [13, chapitre VII]).

Considérons alors deux points N et S de $E(K)$ vérifiant les conditions suivantes :

(i) N n'appartient pas à $E_1(K)$;
(ii) $N - S$ est dans $E_1(K)$;
(iii) $u(N)$ est dans $\mathbb{Q}$.

On a $S \neq O$; posons $S = (x_S, y_S)$. Voici le résultat que l'on a en vue :

LEMME 24.

1. *Si $\beta = 0$, la condition suivante est satisfaite* :

$$x_S \in \mathfrak{M}_\mathfrak{p} \quad \textit{ou bien} \quad \nu(d/x_S) \in \mathbb{F}_p.$$

2. *Si $\beta \neq 0$, la condition suivante est satisfaite* :

$$y_S - dx_S/2 - b \in \mathfrak{M}_\mathfrak{p} \quad \textit{ou bien} \quad \nu\left(\frac{2(x_S - \lambda)}{y_S - dx_S/2 - b}\right) \in \mathbb{F}_p.$$

Démonstration. Posons $N = (x, y)$. Remarquons d'abord que, d'après (58) et le fait que N et S ne soient pas dans $E_1(K)$, les éléments

$$x_S,\ y_S,\ x,\ y,\ y_S - dx_S/2 - b \text{ et } x_S - \lambda$$

sont dans $A_\mathfrak{p}$. Par ailleurs, $\pi(N) = \pi(S)$. On a donc les égalités

$$\nu(x) = \nu(x_S), \qquad \nu(y) = \nu(y_S). \tag{59}$$

1. Supposons $\beta = 0$. Il résulte des hypothèses faites que N appartient à l'ouvert U. Par suite, $u(N) = d/x$ (formule (27)). Supposons que x_S ne soit pas dans $\mathfrak{M}_\mathfrak{p}$, i.e. que

$\nu(x_S) \neq 0$. D'après (59), on a $\nu(x) \neq 0$ et

$$\nu(d/x) = \nu(d/x_S).$$

Puisque $u(N)$ est dans $\mathbb{Q} \cap A_{\mathfrak{p}}$, on a $\nu(d/x) \in \mathbb{F}_p$, d'où notre assertion.

2. Supposons $\beta \neq 0$.

2.1. Supposons que N soit dans U. Dans ce cas, $u(N)$ est donné par la formule (39). Si

$$y_S - dx_S/2 - b \notin \mathfrak{M}_{\mathfrak{p}},$$

alors, d'après (59), $y - dx/2 - b$ n'est pas non plus dans $\mathfrak{M}_{\mathfrak{p}}$. Le fait que $u(N)$ soit dans $\mathbb{Q} \cap A_{\mathfrak{p}}$ entraîne, comme ci-dessus, le résultat.

2.2. Si N n'est pas dans U, on a $N \in \{-M_1, M_1, M_2, M_3\}$. Puisque $u(M_2)$ et $u(M_3)$ ne sont pas dans $\mathbb{Q}$, en fait $N = \pm M_1$. Si $N = M_1$, on a $y = dx/2 + b$, et d'après (59), $y_S - dx_S/2 - b$ est dans $\mathfrak{M}_{\mathfrak{p}}$. Si $N = -M_1$, on a $x = \lambda$ d'où $\nu(x_S - \lambda) = 0$, ce qui entraîne de nouveau le résultat. D'où le lemme. ∎

Appendice B. Méthode de Chabauty elliptique

Soient K un corps de nombres contenu dans $\mathbb{C}$ et A l'anneau d'entiers de K. On considère des éléments a, b, c et d de A et $\mathcal{D}/K$ la quartique affine d'équation

$$v^2 = au^4 + bu^3 + cu^2 + du + e \quad \text{avec} \quad e = 0 \text{ ou } e = 1. \tag{60}$$

Comme dans l'appendice A, on suppose que a est non nul et que $\mathcal{D}$ est lisse. Les points $(0, e)$ et $(0, -e)$ appartiennent à $\mathcal{D}(K)$. Dans la démonstration du théorème 2 de cet article, on est confronté au problème suivant :

Problème 1. Comment déterminer tous les points $(u, v) \in \mathcal{D}(K)$ tels que $u \in \mathbb{Q}$?

Ce problème est facile si $\mathcal{D}(K)$ est fini. Dans le cas où $\mathcal{D}(K)$ est infini, on utilise la méthode dite de Chabauty elliptique, qui permet parfois la détermination complète de ces points. Cette méthode a déjà été présentée dans de nombreux travaux. On pourra à ce sujet consulter par exemple [8], [2], [9] et [7]. L'objectif de cet appendice est d'exposer la démarche que l'on suit dans son utilisation.

B.1. Reformulation du problème. D'après l'étude faite dans l'appendice A, la quartique $\mathcal{D}$ est birationnellement équivalente à la courbe elliptique E/K d'équation de Weierstrass

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \tag{61}$$

à coefficients dans A, qui est définie par les formules (24) et (32), suivant que e soit 0 ou 1 (cf. appendice A). Afin de résoudre notre problème, on est ainsi amené à déterminer les points $N \in E(K)$ tels que

$$u(N) \in \mathbb{Q},$$

où $u : E \to \mathbb{P}^1$ est la fonction sur E définie dans le paragraphe A.3. Rappelons que sur des ouverts de E convenables, si $N = (x, y)$ est un point de $E(K)$ à distance finie, on a

$$u(N) = \begin{cases} d/x & \text{si } e = 0, \\ \dfrac{2(x-\lambda)}{y - dx/2 - b} & \text{avec } \lambda = d^2/4 - c \text{ si } e = 1. \end{cases} \tag{62}$$

La détermination des points $N \in E(K)$ tels que $u(N) \in \mathbb{Q}$ est simple si le rang r de $E(K)$ est nul, car dans ce cas il est facile d'expliciter $E(K)$ et donc aussi $\mathcal{D}(K)$. Si l'on a $r \geq 1$, on utilise des arguments de nature locale que l'on va présenter maintenant.

B.2. Groupe formel associé à E. Pour tout ce qui concerne ce paragraphe, on pourra par exemple consulter le chapitre IV de [13], ainsi que [9].

Soient p un nombre premier impair et $\mathfrak{p}$ un idéal premier de A au-dessus de p. On suppose que les deux conditions suivantes sont satisfaites :

1. l'idéal $\mathfrak{p}$ est non ramifié ;
2. la courbe elliptique E/K a bonne réduction en $\mathfrak{p}$.

Soient $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$, $A_\mathfrak{p}$ son anneau de valuation, $\mathfrak{M}_\mathfrak{p}$ l'idéal maximal de $A_\mathfrak{p}$. On pose $k = A_\mathfrak{p}/\mathfrak{M}_\mathfrak{p}$; c'est une extension finie de $\mathbb{F}_p$. Notons v la valuation $\mathfrak{p}$-adique de $K_\mathfrak{p}$ normalisée par $v(K_\mathfrak{p}^*) = \mathbb{Z}$: on a $v(p) = 1$. Une clôture algébrique $\overline{\mathbb{Q}}_p$ de $\mathbb{Q}_p$ étant choisie, on identifie $K_\mathfrak{p}$ avec l'extension finie non ramifiée de $\mathbb{Q}_p$ contenue dans $\overline{\mathbb{Q}}_p$ dont le degré sur $\mathbb{Q}_p$ est celui de k sur $\mathbb{F}_p$. On identifie par ailleurs K à un sous-corps de $K_\mathfrak{p}$.

B.2.1. *Développements formels.* Le changement de variables

$$z = -x/y, \qquad w = -1/y \tag{63}$$

conduit au nouveau modèle de E :

$$w = z^3 + a_2 z^2 w + a_4 z w^2 + a_6 w^3. \tag{64}$$

Dans l'anneau des séries formelles $A[[z]]$, il existe une unique série formelle w vérifiant l'égalité (64). On a

$$w = z^3 + a_2 z^5 + (a_2^2 + a_4) z^7 + (a_2^3 + 3a_2 a_4 + a_6) z^9 + O(z^{11}). \tag{65}$$

En posant

$$x = z/w, \qquad y = -1/w,$$

dans le modèle (61) on obtient x et y comme série de Laurent de z à coefficients dans A :

$$x = \frac{1}{z^2} - a_2 - a_4 z^2 - (a_2 a_4 + a_6) z^4 + O(z^6), \tag{66}$$

$$y = -\frac{1}{z^3} + \frac{a_2}{z} + a_4 z + (a_2 a_4 + a_6) z^3 + (a_2^2 a_4 + 2a_2 a_6 + a_4^2) z^5 + O(z^7). \tag{67}$$

Le couple (x, y) est alors un point de E rationnel sur le corps $K((z))$. Soit $S = (x_S, y_S)$ un point de $E(K_\mathfrak{p})$ vérifiant l'équation (61) tel que x_S et y_S soient dans $A_\mathfrak{p}$. On peut considérer le nouveau point de E rationnel sur $K_\mathfrak{p}((z))$:

$$M = S + (x, y).$$

En posant $M=(x_M,y_M)$, la formule d'addition sur E conduit à des développements en série de x_M et y_M en fonction de z à coefficients dans $A_\mathfrak{p}$:

$$x_M = x_S + 2y_S z + (3x_S^2 + 2a_2x_S + a_4)z^2 + O(z^3), \tag{68}$$

$$y_M = y_S + (3x_S^2 + 2a_2x_S + a_4)z + 2y_S(3x_S + a_2)z^2 + O(z^3). \tag{69}$$

B.2.2. *Loi de groupe formelle.* On dispose d'une loi de groupe formelle $\mathfrak{F}$ associée au modèle (61) de E sur $K_\mathfrak{p}$. C'est une série formelle en deux indéterminées z_1, z_2 à coefficients dans A et l'on a

$$\mathfrak{F}(z_1,z_2) = z_1 + z_2 - a_2z_1z_2(z_1+z_2) + \text{des termes de degré} \geq 5. \tag{70}$$

On notera log et exp le logarithme et l'exponentielle associés à $\mathfrak{F}$. Ce sont deux séries formelles de $K_\mathfrak{p}[[z]]$ réciproques l'une de l'autre, que l'on peut écrire sous la forme

$$\log = \sum_{n\geq 1} \frac{\alpha_n}{n}\, z^n, \qquad \exp = \sum_{n\geq 1} \frac{\beta_n}{n!}\, z^n,$$

où les α_n, β_n appartiennent à A. On a

$$\log = z + \frac{a_2}{3}\, z^3 + \frac{a_2^2 + 2a_4}{5}\, z^5 + O(z^7), \tag{71}$$

$$\exp = z - \frac{a_2}{3}\, z^3 + \frac{2a_2^2 - 6a_4}{15}\, z^5 + O(z^7). \tag{72}$$

B.2.3. *Groupe formel associé à $E/K_\mathfrak{p}$.* En prenant pour z_1 et z_2 des éléments de $\mathfrak{M}_\mathfrak{p}$, la série (70) est convergente à valeurs dans $\mathfrak{M}_\mathfrak{p}$. Le groupe formel associé à $E/K_\mathfrak{p}$ est le groupe, parfois noté $\mathfrak{F}(\mathfrak{M}_\mathfrak{p})$, ayant pour ensemble sous-jacent $\mathfrak{M}_\mathfrak{p}$ et dont la loi interne $\oplus$ est définie pour tous $z_1, z_2 \in \mathfrak{M}_\mathfrak{p}$ par

$$z_1 \oplus z_2 = \mathfrak{F}(z_1,z_2). \tag{73}$$

De même, si z est un élément non nul de $\mathfrak{M}_\mathfrak{p}$, les séries (66) et (67) sont convergentes dans $K_\mathfrak{p}$. On obtient ainsi une application

$$\varphi : \mathfrak{M}_\mathfrak{p} \to E(K_\mathfrak{p}),$$

définie pour tout z non nul dans $\mathfrak{M}_\mathfrak{p}$ par

$$\varphi(z) = (x(z), y(z)), \tag{74}$$

où $x(z)$ et $y(z)$ sont les éléments de $K_\mathfrak{p}$ définis par les égalités (66) et (67).

Soit $\widetilde{E}$ la courbe déduite de E par réduction. D'après la condition 2, $\widetilde{E}$ est une courbe elliptique définie sur k. Soient

$$\pi : E(K_\mathfrak{p}) \to \widetilde{E}(k)$$

le morphisme de réduction et $E_1(K_\mathfrak{p})$ son noyau. L'application φ réalise un isomorphisme de groupes

$$\varphi : \mathfrak{F}(\mathfrak{M}_\mathfrak{p}) \simeq E_1(K_\mathfrak{p}).$$

L'application réciproque

$$\varphi^{-1} : E_1(K_\mathfrak{p}) \simeq \mathfrak{F}(\mathfrak{M}_\mathfrak{p})$$

associe à tout point à distance finie $P=(x,y) \in E_1(K_\mathfrak{p})$ l'élément

$$z(P) = -x/y \in \mathfrak{M}_\mathfrak{p}. \tag{75}$$

On dira que $z(P)$ est la *z-coordonnée* de P. Si P, P' sont dans $E_1(K_\mathfrak{p})$, on a donc (cf. (73))

$$z(P+P') = \mathfrak{F}(z(P), z(P')). \tag{76}$$

D'après la condition 1 et l'inégalité $p \geq 3$, pour tout $z \in \mathfrak{M}_\mathfrak{p}$, les séries log et exp sont convergentes dans $\mathfrak{M}_\mathfrak{p}$. On notera $\log(z)$ et $\exp(z)$ leurs sommes. Le logarithme induit un isomorphisme de groupes de $\mathfrak{F}(\mathfrak{M}_\mathfrak{p})$ sur $\mathfrak{M}_\mathfrak{p}$ et l'isomorphisme réciproque est donné par l'exponentielle. Pour tout $z \in \mathfrak{M}_\mathfrak{p}$, on a les congruences

$$\log(z) \equiv z \equiv \exp(z) \bmod p^{1+v(z)}. \tag{77}$$

En effet, il suffit de prouver que si n est un entier ≥ 2, on a

$$v(z^n/n!) \geq v(z) + 1,$$

ce qui résulte de l'inégalité

$$v(n!) \leq (n-1)/2.$$

Par ailleurs, pour tout point $P \in E_1(K_\mathfrak{p})$ et tout entier $n \in \mathbb{Z}$, on a

$$z(nP) = \exp(n \log(z(P))). \tag{78}$$

Étant donnés un entier $k \geq 1$, des points $P_1, \ldots, P_k \in E_1(K_\mathfrak{p})$ et des entiers $n_1, \ldots, n_k$, on en déduit l'égalité

$$z\Big(\sum_{i=1}^{k} n_i P_i\Big) = \exp\Big(\sum_{i=1}^{k} n_i \log(z(P_i))\Big). \tag{79}$$

B.2.4. *Le $\mathbb{Z}_p$-module $E_1(K_\mathfrak{p})$.* L'application $z \mapsto \log(z)$ réalise un isomorphisme de groupes de $\mathfrak{F}(\mathfrak{M}_\mathfrak{p})$ sur $\mathfrak{M}_\mathfrak{p}$. On en déduit que $\mathfrak{F}(\mathfrak{M}_\mathfrak{p})$ est muni d'une structure de $\mathbb{Z}_p$-module telle que cette application soit un morphisme de $\mathbb{Z}_p$-modules : elle est donnée par la formule

$$n.z = \exp(n \log(z)) \quad \text{pour } n \in \mathbb{Z}_p \text{ et } z \in \mathfrak{F}(\mathfrak{M}_\mathfrak{p}).$$

Par ailleurs, les groupes $\mathfrak{F}(\mathfrak{M}_\mathfrak{p})$ et $E_1(K_\mathfrak{p})$ sont isomorphes via l'application φ. Il en résulte l'existence d'une structure de $\mathbb{Z}_p$-module sur $E_1(K_\mathfrak{p})$ telle que

$$n.z(P) = z(nP) \quad \text{pour } n \in \mathbb{Z}_p \text{ et } P \in E_1(K_\mathfrak{p}).$$

On a ainsi l'égalité

$$z(nP) = \exp(n \log(z(P))) \quad \text{pour } n \in \mathbb{Z}_p \text{ et } P \in E_1(K_\mathfrak{p}), \tag{80}$$

et la formule (79) est alors valable en prenant pour les n_i des éléments de $\mathbb{Z}_p$.

B.2.5. *La projection $\eta : K_\mathfrak{p}^* \to k^*$.* Soit $\eta : K_\mathfrak{p}^* \to k^*$ l'application de $K_\mathfrak{p}^*$ dans k^* définie par

$$\eta(x) = x/p^{v(x)} \bmod \mathfrak{M}_\mathfrak{p}. \tag{81}$$

C'est un homomorphisme de groupes surjectif de $K_\mathfrak{p}^*$ sur k^*. L'objectif de ce paragraphe est de préciser quelques propriétés de η que l'on utilise dans la démonstration des résultats.

Soient x et x' deux éléments de $K_\mathfrak{p}^*$. On pose

$$y = x + x', \quad x/p^{v(x)} = u, \quad x'/p^{v(x')} = u'.$$

1) Si $v(x) < v(x')$, on a $\eta(y) = \eta(x)$. En effet,

$$y = up^{v(x)}(1 + p^{v(x')-v(x)}u'/u),$$

On a $\eta(1 + p^{v(x')-v(x)}u'/u) = 1$, d'où l'assertion.

2) Supposons $\eta(x) + \eta(x') \neq 0$. Vérifions que

$$y \neq 0, \quad \eta(y) \in \{\eta(x), \eta(x'), \eta(x) + \eta(x')\}. \tag{82}$$

On a $y \neq 0$ sinon $\eta(x) = \eta(-x') = -\eta(x')$, ce qui n'est pas. Par ailleurs, on peut supposer d'après l'alinéa 1) que $v(x) = v(x')$. On a alors $v(y) = v(x)$. En effet, l'inégalité $v(y) > v(x)$ conduit à

$$\eta(x) + \eta(x') = y/p^{v(x)} \bmod \mathfrak{M}_{\mathfrak{p}} = 0.$$

On obtient ainsi $\eta(y) = \eta(x) + \eta(x')$. D'où la condition (82).

3) Supposons que x soit dans $\mathbb{Q}_p^*$. Vérifions que $\eta(x)$ appartient à $\mathbb{F}_p^*$. Il existe un entier a compris entre 1 et $p-1$, et $b \in \mathfrak{M}_p$, tels que

$$u = a + b.$$

On a $\eta(u) = \eta(x)$ et d'après 1), $\eta(u) = \eta(a) \in \mathbb{F}_p^*$, d'où l'assertion.

4) Soit z un élément non nul de $\mathfrak{M}_{\mathfrak{p}}$. On a

$$\eta(\log(z)) = \eta(z) = \eta(\exp(z)). \tag{83}$$

Ces égalités résultent de 1) et des congruences (77).

5) Soient $P \in E_1(K_{\mathfrak{p}})$ et $m \in \mathbb{Z}_p$ tels que mP soit non nul. On a

$$\eta(z(mP)) = \eta(m)\eta(z(P)). \tag{84}$$

D'après (80) et (83), on a

$$\eta(z(mP)) = \eta(\exp(m\log(z(P)))) = \eta(m\log(z(P))),$$

d'où

$$\eta(z(mP)) = \eta(m)\eta(\log(z(P))) = \eta(m)\eta(z(P)),$$

puis l'égalité (84).

B.3. Méthode de Chabauty elliptique. Cette méthode consiste, dans sa généralité, à majorer le nombre de points (u, v) de $\mathcal{D}(K)$ tel que u soit dans $\mathbb{Q}$. Les points $(0, e)$ et $(0, -e)$ de $\mathcal{D}(K)$ réalisent cette condition. En pratique, on dispose parfois d'autres points «évidents» $(u, v) \in \mathcal{D}(K)$ tels que u soit dans $\mathbb{Q}$. Si le majorant obtenu coïncide avec le nombre de points déjà connus sur $\mathcal{D}(K)$ possédant cette propriété, le problème du début est alors résolu. On va décrire ici cette méthode et présenter les étapes que l'on suivra dans la démonstration du théorème 2.

Première étape. Le groupe $E(K)$ est de type fini. La première étape consiste à déterminer :

1. le sous-groupe de torsion de $E(K)$;
2. le rang r de $E(K)$;
3. un système de r points $(N_1, \ldots, N_r)$ de $E(K)$ qui sont $\mathbb{Z}$-linéairement indépendants.

Cette étape est en général difficile à réaliser. Il existe néanmoins des algorithmes, implantés par D. Simon sur le logiciel de calculs PARI, qui permettent parfois cette détermination (cf. [15]). Il est important de noter que, tout au moins pour les applications

que l'on a en vue, il est inutile de se préoccuper de savoir si le système $(N_1, \ldots, N_r)$ forme ou non une base de $E(K)$ modulo son sous-groupe de torsion. Par ailleurs, dans les situations rencontrées dans ce travail, on a toujours $r \leq 2$. Cela étant, la suite de ce paragraphe est valable pour r quelconque.

Deuxième étape. On suppose qu'il existe un nombre premier $p \geq 3$ tel que :

4. p ne divise pas le discriminant de K ;
5. il existe un idéal premier $\mathfrak{p}$ de A au-dessus de p dont le degré résiduel f sur p vérifie l'inégalité

$$r \leq f - 1 ; \tag{85}$$

6. la courbe elliptique E/K a bonne réduction en $\mathfrak{p}$.

Soit $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$, $A_\mathfrak{p}$ son anneau de valuation et k le corps résiduel. On conserve les identifications faites au début du paragraphe 2. Soient $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$ et ξ un élément de $\overline{\mathbb{F}}_p$ tel que $k = \mathbb{F}_p(\xi)$. Si $\tau \in A_\mathfrak{p}$ est un relèvement de ξ, on a

$$K_\mathfrak{p} = \mathbb{Q}_p(\tau), \qquad A_\mathfrak{p} = \mathbb{Z}_p[\tau]. \tag{86}$$

L'anneau $A_\mathfrak{p}$ est un $\mathbb{Z}_p$-module libre de base $(1, \tau, \ldots, \tau^{f-1})$.

La courbe elliptique E a bonne réduction sur $K_\mathfrak{p}$. Soient $\widetilde{E}$ la courbe elliptique sur k déduite de E par réduction et

$$\pi : E(K_\mathfrak{p}) \to \widetilde{E}(k)$$

le morphisme de réduction. Soit $E_1(K)$ l'intersection du noyau de π avec $E(K)$. L'objectif de cette étape est alors d'expliciter un système de représentants de $E(K)/E_1(K)$ qui contient O. Il est facile d'obtenir un tel système de représentants pour peu que l'on sache démontrer, si tel est le cas, que $\{N_1, \ldots, N_r\}$ est une base de $E(K)$ modulo son sous-groupe de torsion. On procède ici autrement : on considère le sous-groupe G de $E(K)$ engendré par son sous-groupe de torsion et $\{N_1, \ldots, N_r\}$. Notons h l'indice de G dans $E(K)$ et supposons que la condition suivante soit satisfaite :

7. h est premier avec l'ordre de $\widetilde{E}(k)$.

Cette condition est souvent réalisée en pratique, et est toujours vérifiée dans les applications que l'on a en vue. Elle implique le résultat suivant :

Lemme 25. *On a* $\pi(G) = \pi(E(K))$.

Démonstration. L'application π induit un morphisme de groupes surjectif de $E(K)/G$ sur $\pi(E(K))/\pi(G)$. En particulier, l'indice de $\pi(G)$ dans $\pi(E(K))$ divise h. Par ailleurs, $\pi(E(K))$ étant un sous-groupe de $\widetilde{E}(k)$, l'indice de $\pi(G)$ dans $\pi(E(K))$ divise aussi l'ordre de $\widetilde{E}(k)$. La condition 7 entraîne alors le résultat. ∎

Pour tout i entre 1 et r, notons ensuite m_i l'ordre de $\pi(N_i)$ et posons

$$Q_i = m_i N_i. \tag{87}$$

Les points Q_i appartiennent à $E_1(K)$. Soit $\mathfrak{S}$ le sous-ensemble de $E(K)$ formé des points qui s'écrivent sous la forme

$$T + \sum_{i=1}^{r} k_i N_i,$$

où T est un point de torsion de $E(K)$ et où les k_i sont des entiers tels que

$$[-m_i/2] + 1 \leq k_i \leq [m_i/2].$$

Il résulte alors du lemme 25 que tout point N de $E(K)$ s'écrit sous la forme

$$N = S + P \quad \text{où} \quad S \in \mathfrak{S} \text{ et } P \in E_1(K). \tag{88}$$

Cette condition permet alors d'expliciter un système de représentants comme souhaité. Dans certaines situations favorables, on constate qu'il existe un sous-ensemble $\mathfrak{S}'$ de $E(K)$ tel que π induise une bijection de $\mathfrak{S}'$ sur $\widetilde{E}(k)$; on obtient alors directement un tel système de représentants et l'on évite ainsi de vérifier la condition 7.

Signalons que dans les situations rencontrées au cours de la démonstration du théorème 2, on considère toujours le nombre premier $p = 3$.

Troisième étape. Comme on le signalait au paragraphe B.1, on est amené pour résoudre notre problème à déterminer les points $N \in E(K)$ tels que $u(N)$ soit dans $\mathbb{Q}$. On connaît en pratique un certain ensemble $\mathcal{P}$ formé de points « évidents » de $E(K)$ ayant cette propriété qui sont en fait implicitement liés à la situation considérée. Notre objectif est de démontrer, si tel est le cas, qu'il n'y en a pas d'autres.

Considérons pour cela un point $N \in E(K)$ qui n'appartienne pas à notre ensemble $\mathcal{P}$ dont on dispose *a priori*. On suppose, ce qui n'est pas restrictif, que N appartient à l'ouvert U de E défini aux paragraphes 1.2 et 2.2 de l'appendice A. La valeur de $u(N)$ est alors donnée par la formule (62). Il s'agit de prouver si possible que $u(N)$ n'est pas dans $\mathbb{Q}$.

1) Le lemme 24 de l'appendice A apporte déjà une contrainte sur les éventuels points $S \in \mathfrak{S}$ pour lesquels, N s'écrivant sous la forme (88), $u(N)$ appartient à $\mathbb{Q}$. En tenant compte du fait que la fonction u est invariante par l'involution hyperelliptique (lemme 23, appendice A), cela permet de remplacer $\mathfrak{S}$ par un ensemble $\mathfrak{S}_0$ contenant O, qui est en pratique strictement contenu dans $\mathfrak{S}$. On a alors

$$N = S + P \quad \text{où } S \in \mathfrak{S}_0 \text{ et } P \in E_1(K). \tag{89}$$

On peut supposer de plus que N n'est pas dans $\mathfrak{S}_0$, auquel cas P est non nul.

2) Posons $z = z(P)$ et $N = (x, y)$. Pour chaque point $S \in \mathfrak{S}_0$, on exprime $u(N)$ ou $1/u(N)$ à partir de la formule (62), en série entière de z. Dans le cas où S est non nul cela est possible pour peu que certaines conditions soient satisfaites par S. On obtient ces développements comme suit :

2.1) Supposons $S = O$. On a alors $N = P \in E_1(K)$ et l'on dispose des développements en série de Laurent de x et y en fonction de z donnés par les formules (66) et (67). On peut ainsi développer $u(N)$ en série :

$$u(N) = \sum_{n \geq 1} \nu_n z^n \quad \text{où } \nu_n \in A_{\mathfrak{p}}. \tag{90}$$

On vérifie que

$$u(N) \equiv \begin{cases} -2z \bmod z^2 & \text{si } e = 1, \\ dz^2 \bmod z^3 & \text{si } e = 0. \end{cases} \tag{91}$$

2.2) Supposons $S \neq O$. Posons $S = (x_S, y_S)$ et notons v la valuation $\mathfrak{p}$-adique de $K_\mathfrak{p}$. On suppose que l'une des conditions suivantes est réalisée :

8. on a $e = 1$ ainsi que $v(x_S - \lambda) = 0$ ou $v(y_S - dx_S/2 - b) = 0$;
9. on a $e = 1$, $S = M_1$ (lemme 16, appendice A) et $v(3x_S^2 + 2a_2x_S + a_4 - dy_S) = 0$;
10. on a $e = 0$ et $v(x_S) = 0$.

En utilisant les formules (68) et (69), on obtient alors un développement de la forme

$$u(N) \text{ ou } \frac{1}{u(N)} = \sum_{n \geq 0} \varrho_n z^n, \tag{92}$$

où les ϱ_n sont dans $A_\mathfrak{p}$. Dans le cas simple où $e = 0$, on a

$$u(N) \equiv \frac{d}{x_S}\left(1 - \frac{2y_S z}{x_S}\right) \bmod z^2.$$

3) Soient H le sous-groupe d'indice fini de $E_1(K)$ engendré par les points $\{Q_1, \ldots, Q_r\}$ et Γ le sous-$\mathbb{F}_p$-espace vectoriel de k engendré par les $\eta(z(Q))$ où $Q \in H \setminus \{O\}$. Dans certains cas favorables, la connaissance d'une $\mathbb{F}_p$-base de Γ, ainsi que celle des premiers coefficients des développements en séries entières de $u(N)$, suffit pour démontrer directement que $\eta(u(N))$ n'appartient pas à $\mathbb{F}_p^*$, ce qui entraîne alors la conclusion souhaitée. Illustrons ce propos à travers un exemple typique. Supposons pour cela que la condition suivante soit satisfaite :

11. L'intersection de $E_1(K)$ et du sous-groupe de torsion de $E(K)$ est réduite à $\{O\}$.

On a alors l'énoncé suivant :

LEMME 26. *Pour tout point $R \in E_1(K)$ non nul, l'élément $\eta(z(R))$ appartient à Γ.*

Démonstration. Soit R un point non nul de $E_1(K)$. Puisque H est d'indice fini dans $E_1(K)$, il existe un entier n non nul tel que nR appartienne à H. D'après la condition 11, on a $nR \neq O$ et il résulte alors de la formule (84) que

$$\eta(z(R)) = \frac{\eta(z(nR))}{\eta(n)} \in \Gamma. \ \blacksquare$$

Dans le cas particulier où $S = O$ et $e = 1$, il est alors facile de conclure si la condition suivante est réalisée :

12. L'élément 1 n'appartient pas à Γ.

En effet, $u(N)z \neq 0$ et d'après (91) on a l'égalité

$$\eta(u(N)) = -2\eta(z). \tag{93}$$

On déduit alors du lemme 26 que $\eta(u(N))$ n'est pas dans $\mathbb{F}_p^*$ et ainsi $u(N)$ n'est pas dans $\mathbb{Q}$.

La plupart des cas auxquels on est confronté dans la démonstration du théorème 2 se traitent en fait suivant cette idée en utilisant le lemme 26, à des modifications mineures

près qui correspondent au choix de S. Toutefois, on est amené dans cette démonstration à l'étude de certains cas pour lesquels la condition 12 n'est pas réalisée. Comme il est classique dans la méthode de Chabauty elliptique, il nous faut alors examiner les zéros communs éventuels de certaines séries formelles à coefficients dans $\mathbb{Z}_p$.

Rappelons plus précisément en quoi cela consiste. Considérons un point quelconque $S \in \mathfrak{S}_0$ pour lequel les arguments présentés ci-dessus ne permettent pas de conclure. On construit alors f séries formelles

$$\Phi_S^{(j)} \in \mathbb{Z}_p[[X_1, \ldots, X_r]], \quad j = 0, \ldots, f-1,$$

telles que le coefficient de $X_1^{j_1} \cdots X_r^{j_r}$ converge vers 0 quand $j_1 + \cdots + j_r$ tend vers plus l'infini, et que les zéros dans $\mathbb{Z}_p^r$ de $\Phi_S^{(j)}$, avec $1 \leq j \leq f-1$, correspondent aux éventuelles possibilités que $u(N)$ soit dans $\mathbb{Q}$. La condition (85) sert en fait à assurer qu'il y a au moins autant d'équations $\Phi_S^{(j)} = 0$ que de variables.

Indiquons comment construire ces séries formelles. On suppose pour cela que la condition suivante est satisfaite :

13. L'indice de H dans $E_1(K)$ est premier à p.

Dans ce cas, il existe un entier n, non divisible par p, tel que nP appartienne à H. En utilisant la structure de $\mathbb{Z}_p$-module de $E_1(K)$, on en déduit l'existence d'éléments $n_1, \ldots, n_r$ de $\mathbb{Z}_p$ tels que

$$P = \sum_{i=1}^{r} n_i Q_i. \tag{94}$$

Pour tout i entre 1 et r, posons $z_i = z(Q_i)$. On a l'égalité (cf. 2.4)

$$z = \exp\Big(\sum_{i=1}^{r} n_i \log(z_i)\Big). \tag{95}$$

Remarque 3. Si $r = 1$ et $p = 3$, on vérifie que

$$z \equiv n_1 \log(z_1) - a_2 n_1^3 \frac{(\log(z_1))^3}{3} \bmod 3z_1^3,$$

ce qui conduit à la congruence

$$z \equiv \left(z_1 + a_2 \frac{z_1^3}{3}\right) n_1 - a_2 \frac{z_1^3}{3} n_1^3 \bmod 3z_1^3, \tag{96}$$

et l'on obtient ainsi z modulo 3^4 (au moins).

En utilisant (90) ou (92) ainsi que (95), on constate qu'il existe des éléments $a_{j_1 \cdots j_r}$ qui appartiennent à $A_{\mathfrak{p}}$ tels que

$$(a_{j_1 \cdots j_r}) \text{ converge vers 0 quand } j_1 + \cdots + j_r \to +\infty, \tag{97}$$

et que

$$u(N) \text{ ou } \frac{1}{u(N)} = \sum_{j_1, \ldots, j_r \geq 0} a_{j_1 \cdots j_r} n_1^{j_1} \cdots n_r^{j_r}. \tag{98}$$

En décomposant les éléments $a_{j_1 \cdots j_r}$ dans la base $(1, \tau, \ldots, \tau^{f-1})$ de $A_\mathfrak{p}$ sur $\mathbb{Z}_p$, on obtient ainsi f séries formelles

$$\Phi_S^{(j)}(X_1, \ldots, X_r) \in \mathbb{Z}_p[[X_1, \ldots, X_r]], \qquad j = 0, \ldots, f-1,$$

telles que le coefficient de $X_1^{j_1} \cdots X_r^{j_r}$ converge vers 0 quand $j_1 + \cdots j_r$ tend vers plus l'infini, et que

$$u(N) \text{ ou } \frac{1}{u(N)} = \Phi_S^{(0)} + \Phi_S^{(1)}\tau + \cdots + \Phi_S^{(f-1)}\tau^{f-1}, \tag{99}$$

où $\Phi_S^{(j)} = \Phi_S^{(j)}(n_1, \ldots, n_r)$. On en déduit que si $u(N)$ appartient à $\mathbb{Q}$, on a

$$\Phi_S^{(j)} = 0 \quad \text{pour } j = 1, \ldots, f-1. \tag{100}$$

On est ainsi amené à examiner les zéros communs dans $\mathbb{Z}_p^r$ des $f-1$ séries formelles $\Phi_S^{(j)}(X_1, \ldots, X_r)$ pour j compris entre 1 et $f-1$. En connaissant ces séries modulo une puissance de p assez grande, on peut alors parfois démontrer qu'il n'existe pas de tels zéros, auquel cas on déduit que $u(N)$ n'est pas dans $\mathbb{Q}$. La situation rencontrée à ce sujet dans la démonstration du théorème 2 est assez simple, car on démontre directement qu'il n'existe pas de zéros communs à ces séries modulo la puissance de p considérée.

Références

[1] K. Belabas, D. Bernardi, C. Batut, H. Cohen and M. Olivier, *User's guide to pari-gp* (*version 2.0.12*), LAB A2X, Univ. Bordeaux I, Bordeaux, 1998.

[2] N. Bruin, *Chabauty Methods and Covering Techniques Applied to Generalized Fermat Equations*, CWI Tract 133, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 2002.

[3] —, *Chabauty methods using elliptic curves*, J. Reine Angew. Math. 562 (2003), 27–49.

[4] —, *Some ternary Diophantine equations of signature* $(n, n, 2)$, in: Discovering Mathematics with Magma, W. Bosma and J. Cannon (eds.), Springer, 2006.

[5] N. Bruin and E. V. Flynn, *Towers of 2-covers of hyperelliptic curves*, Trans. Amer. Math. Soc. 357 (2005), 4329–4347.

[6] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. 490 (1997), 81–100.

[7] S. Duquesne, *Rational points on hyperelliptic curves and an explicit Weierstrass preparation theorem*, Manuscripta Math. 108 (2002), 191–204.

[8] E. V. Flynn, *A flexible method for applying Chabauty's theorem*, Compos. Math. 105 (1997), 79–94.

[9] E. V. Flynn and J. L. Wetherell, *Finding rational points on bielliptic genus 2 curves*, Manuscripta Math. 100 (1999), 519–533.

[10] W. Ivorra, *Sur les équations* $x^p + 2^\beta y^\beta = z^2$ *et* $x^p + 2^\beta y^\beta = 2z^2$, Acta Arith. 108 (2003), 327–338.

[11] —, *Équations diophantiennes ternaires de type* $(p, p, 2)$ *et courbes elliptiques*, Thèse de l'Université Pierre et Marie-Curie, Paris, 2004.

[12] A. Kraus, *Une question sur les équations* $x^m - y^m = Rz^n$, Compos. Math. 132 (2002), 1–26.

[13] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.
[14] —, *Computing heights on elliptic curves*, Math. Comp. 51 (1988), 339–358.
[15] D. Simon, *Programme, pour pari gp, de calcul du rang des courbes elliptiques définies sur des corps de nombres*, http://www.math.unicaen.fr/~simon/, 2002.
[16] P. G. Walsh, *Squares in Lucas sequences with rationnal roots*, Integers 5 (2005), no. 3, 8 pp.