ACTA ARITHMETICA
125.2 (2006)

Principe de Hasse et rang pour des courbes de genre 2 à jacobienne simple

par

Victor Gonzalo Lopez Neumann (Uberlândia)

1. Introduction. On cherche une courbe de genre 2, contre-exemple au principe de Hasse, à jacobienne simple dont le groupe de Mordell–Weil soit de rang le plus grand possible. Des exemples de ce type existent déjà dans la littérature, voir par exemple l'article de Flynn [Fly]. Flynn cherche des exemples parmi des courbes définies par des équations dont les coefficients sont bornés. Il a besoin de calculer le rang du groupe de Mordell–Weil de la jacobienne d'une courbe pour montrer que la courbe est un contre-exemple au principe de Hasse. Cette méthode est liée à l'obstruction de Brauer–Manin.

Dans cet article, on obtient des courbes de genre 2 comme intersection résiduelle d'une surface de Del Pezzo S de degré 4 et d'une quadrique dans $\mathbb{P}^4$. L'arithmétique dans S permet de trouver des éléments du groupe de Mordell–Weil $\mathfrak{S}$ de la jacobienne de $\mathcal{C}$ et des relations entre ces éléments. Avec un choix judicieux, une courbe de genre 2, ainsi construite, aura les propriétés cherchées.

Pour les courbes trouvées à l'aide des surfaces de Del Pezzo, on ne peut pas calculer le rang du groupe de Mordell–Weil de la jacobienne associée. On doit donc utiliser une autre méthode pour montrer que ces courbes sont des contre-exemples au principe de Hasse. La méthode utilisée ici est similaire à celle utilisée par Wuthrich (voir [Wu]) qui consiste à travailler simultanément avec deux normes. Comme Colliot-Thélène fait remarquer à Wuthrich, cette technique est aussi liée à l'obstruction de Brauer–Manin.

Voici les deux exemples construits à l'aide des surfaces de Del Pezzo :

Théorème 1.1. *La courbe projective lisse $\mathcal{C}$ de genre* 2, *dont un morceau affine est définie par*

$$Y^2 = -68X^6 + 96X^5 + 25X^4 - 624X^3 + 1360X^2 - 1440X + 896, \tag{1}$$

2000 *Mathematics Subject Classification*: Primary 11G30; Secondary 11G10, 14H40.
Supported by CNPq-Brasil.

est un contre-exemple au principe de Hasse. De plus la jacobienne $J(\mathcal{C})$ est simple et le groupe de Mordell–Weil $\mathfrak{S} = J(\mathcal{C})(\mathbb{Q})$ est sans torsion et de rang supérieur ou égal à 3.

Par construction, deux éléments indépendants de $\mathfrak{S}$ proviennent de la surface de Del Pezzo. Le troisième élément a été trouvé par M. Stoll en faisant une recherche sur la surface de Kummer associée à la jacobienne de cette courbe. Les coordonées X des couples des points de la courbe qui représentent trois éléments indépendants de la jacobienne sont :

$$X^2 - 2X + 2, \quad X^2 + 2X + 8, \quad 14X^2 - 17X + 22.$$

En utilisant le programme que Stoll décrit dans [St2] et en supposant que le groupe de classes du corps sextique engendré par une racine du polynôme de droite dans l'équation (1) est engendré par des idéaux premiers de norme plus petite à 500, il a calculé que le rang du groupe de Mordell–Weil de la jacobienne est plus petit ou égal à 5.

THÉORÈME 1.2. *La courbe projective lisse $\mathcal{C}$ de genre* 2, *dont un morceau affine est définie par*

$$Y^2 = -2295X^6 - 68630X^5 + 28383X^4 + 519710X^3 - 128799X^2 - 705880X + 376992, \tag{2}$$

est un contre-exemple au principe de Hasse. De plus la jacobienne $J(\mathcal{C})$ est simple et le groupe de Mordell–Weil $\mathfrak{S} = J(\mathcal{C})(\mathbb{Q})$ est sans torsion et de rang supérieur ou égal à 4.

Ces deux exemples étant traités dans ma thèse ([Lo]), on ne se concentrera que sur le théorème 1.2 tout au long de cet article ; la preuve du théorème 1.1 étant similaire.

On commencera par expliciter la construction d'une courbe de genre 2 sur une surface de Del Pezzo, ensuite on montrera comment la courbe (2) est trouvée et on démontrera le théorème 1.2.

2. Courbes de genre 2 sur les surfaces de Del Pezzo de degré 4.

Le but de cette section est de donner la construction géométrique d'une courbe de genre 2 à partir d'une surface de Del Pezzo de degré 4 (surface lisse dont la classe anticanonique est ample de self-intersection 4).

2.1. *Surfaces de Del Pezzo de degré 4.* On peut se référer à [Be], à [Ma] et à [Ha] pour de plus amples informations sur les propriétés des surfaces de Del Pezzo. Pour les besoins de cet article, il nous suffit de considérer celles de degré 4, qu'on notera dP_4.

On considère cinq points distincts $p_1, \ldots, p_5 \in \mathbb{P}^2$ (le plan projectif sur le corps $\overline{\mathbb{Q}}$). On dit que ces points se trouvent *en position générale* s'il n'existe pas de droite passant par trois d'entre eux. Le système linéaire des cubiques

passant par $p_1, \ldots, p_5$ définit une application rationnelle $\lambda : \mathbb{P}^2 \dashrightarrow \mathbb{P}^4$. La surface $S_4 = \overline{\lambda(\mathbb{P}^2)}$ est une surface dP_4. C'est donc l'intersection complète de deux quadriques dans $\mathbb{P}^4$. Voir [Be, proposition IV.9]. L'inverse de λ est un morphisme $\varepsilon : S_4 \to \mathbb{P}^2$ qui contracte cinq droites sur $p_1, \ldots, p_5$.

S_4 contient un nombre fini de droites (voir [Be, proposition IV.12]). Ce sont :

(i) les courbes exceptionnelles $l_i = \varepsilon^{-1}(p_i)$;
(ii) les transformées strictes l_{ij} des droites $\overline{p_i p_j}$ $(i \neq j)$;
(iii) la transformée stricte l de la conique passant par tous les points p_i.

On remarque que l_i a une intersection non vide avec l et avec l_{ij} pour tout $j \neq i$; l_{ij} intersecte l_i, l_j et l_{mn} où m et n sont choisis tels que i, j, m, n sont tous distincts. Finalement, l intersecte l_i pour tout i. Ainsi, chaque droite intersecte cinq autres qui sont gauches deux à deux et si l'on prend cinq droites disjointes, une sixième va ou bien les couper toutes ou bien couper deux d'entre elles.

Les deux lemmes suivants caractérisent de façon assez précise les surfaces dP_4.

LEMME 2.1. *Soit S une surface dP_4 décrite comme intersection complète de deux quadriques dans $\mathbb{P}^4$. Alors, étant donné cinq droites disjointes de S, il existe un morphisme $\varepsilon : S \to \mathbb{P}^2$ tel que ces cinq droites sont les courbes exceptionnelles de ε.*

Preuve. Voir [Be, proposition IV.16]. ∎

LEMME 2.2. *Soit S_4 une surface de Del Pezzo de degré 4. Soient*

$$l_i = \varepsilon^{-1}(p_i), \quad 1 \leq i \leq 5, \quad l_0 = \varepsilon^{-1}(L),$$

où L est une droite quelconque dans $\mathbb{P}^2$ qui ne passe par aucun des points $p_1, \ldots, p_5$. Alors $(l_0, l_1, \ldots, l_5)$ est une base de $\operatorname{Pic} S_4$ telle que

(i) $K_{S_4} \cong -3l_0 + \sum_{i=1}^{5} l_i \cong -H$ *(où H est une section hyperplane)* ;
(ii) $(l_0, l_0) = 1$, $(l_i, l_i) = -1$ *pour* $i \geq 1$, *et* $(l_i, l_j) = 0$ *pour* $i \neq j$.

Preuve. Voir [Ma, proposition 25.1]. ∎

REMARQUE 2.3. La courbe l_0 est une courbe rationnelle de degré 3, ce n'est pas une droite.

2.2. *Construction géométrique des courbes de genre 2*

LEMME 2.4. *Soit S une surface dP_4 dans $\mathbb{P}^4$ et Q une quadrique dans $\mathbb{P}^4$ ne contenant pas S. Supposons que $S \cap Q = D \cup \mathcal{F}$ où D est une réunion de droites et $\mathcal{F}$ une courbe irréductible. Alors $\mathcal{F}$ est de genre arithmétique 2 si et seulement si D est réunion de deux droites d'intersection non vide.*

Preuve. Si D est une réunion de deux droites s'intersectant et $\mathcal{F}$ une courbe telle que $S \cap Q = D \cup \mathcal{F}$, alors on montre, à l'aide de la formule d'adjonction et du lemme 2.2, que $p_a(\mathcal{F}) = 2$.

Supposons maintenant $p_a(\mathcal{F}) = 2$. Soit m le nombre de droites dans D ; alors $(H, D) = m$ et $(H, 4D - mH) = 0$. Par [Ma, proposition 25.2], on a

$$(4D - mH)^2 \leq 0.$$

Par ailleurs avec la formule d'adjonction et le lemme 2.2 on obtient

$$(D, D) = 3m - 6.$$

On en déduit que $m = 0, 1$ ou 2 (car $m \leq 8$). En vérifiant les trois cas, on conclut que le seul possible est $m = 2$ et que D est réunion de deux droites d'intersection non vide. ∎

Ce lemme nous indique la façon de procéder pour obtenir une courbe de genre arithmétique 2. Pour que le genre géométrique de la courbe $\mathcal{F}$ soit aussi 2, il suffira de choisir les paramètres de telle sorte que la courbe soit lisse. On va donc supposer par la suite que la courbe $\mathcal{F}$ est lisse.

Par la section 2.1, on peut choisir, sans perte de généralité, $D = l + l_1$ où l_1 est la droite exceptionnelle au-dessus de p_1 et l est la seule droite qui coupe les cinq droites exceptionnelles de la contraction ε. Dans ce cas, l est la transformée stricte de la conique qui passe par les cinq points $p_1, \ldots, p_5$. On a ainsi $S \cap Q = l_1 \cup l \cup \mathcal{F}$ et $\mathcal{F} \sim 2H - l - l_1$. D'où

$$(\mathcal{F}, l_1) = (\mathcal{F}, l) = 2, \quad (\mathcal{F}, l_i) = 1 \quad (2 \leq i \leq 5). \tag{3}$$

Comme on suppose que $\mathcal{F}$ est lisse, $\varepsilon(\mathcal{F})$ est une quartique plane de genre géométrique 2 dans $\mathbb{P}^2$ avec point double en p_1 et passant par $p_2, \ldots, p_5$.

Puisque l'on va travailler sur le corps $\mathbb{Q}$, on choisit S, Q et le 5-cycle $\sum p_i$, tous définis sur $\mathbb{Q}$. Cela veut dire que la réunion de droites D, la courbe $\mathcal{F}$, la contraction ε et la droite l sont aussi définies sur $\mathbb{Q}$. Comme p_1 est le seul point double de $\mathcal{F}$, alors l_1 est définie sur $\mathbb{Q}$.

Puisque $p_1 \in \mathbb{P}^2_{\mathbb{Q}}$, on peut prendre $p_1 = (1 : 0 : 0)$. Alors $\varepsilon(\mathcal{F})$ s'écrit

$$G(x, y, z) = G_2(y, z)x^2 + G_3(y, z)x + G_4(y, z) = 0, \tag{4}$$

où G_j est un polynôme homogène de degré j défini sur $\mathbb{Q}$.

Soient $p_1 = (1 : 0 : 0)$, $p_i = (1, \omega_i, \omega_i^2)$, où ω_i parcourt les racines du polynôme $P(X) = X^4 + g_3X^3 + g_2X^2 + g_1X + g_0$ $(2 \leq i \leq 5)$; la conique $\varepsilon(l)$ est donc définie par $g = xz - y^2 = 0$.

Une base définie sur $\mathbb{Q}$ du système linéaire des cubiques passant par les points p_i est

$$\begin{aligned}
&u_0 = x(xz - y^2), \quad u_1 = y(xz - y^2), \quad u_2 = z(xz - y^2),\\
&u_3 = g_0x^2y + g_1x^2z + g_2xyz + g_3xz^2 + yz^2,\\
&u_4 = g_0x^2z + g_1xyz + g_2xz^2 + g_3yz^2 + z^3.
\end{aligned}$$

On peut en déduire que la surface de Del Pezzo S est l'intersection complète de deux quadriques

$$\begin{aligned}\mathcal{Q}_1\colon\ & u_0u_4 - u_1u_3 = g_0u_0^2 + g_2u_0u_2 + u_2^2,\\ \mathcal{Q}_2\colon\ & u_2u_3 - u_1u_4 = g_1u_0u_2 + g_3u_2^2.\end{aligned}$$

En intersectant S avec la quadrique d'équation $u_0u_2 - u_1^2 = 0$, on trouve les droites $l, l_1, \dots, l_5$. Celles qui nous intéressent sont

$$l\colon\ u_0 = u_1 = u_2 = 0 \quad \text{et} \quad l_1\colon\ u_4 - g_0u_0 = u_1 = u_2 = 0.$$

Soit Q la quadrique du lemme 2.4. Comme elle doit contenir l et l_1, alors Q est une combinaison linéaire du système linéaire de quadriques contenant l et l_1 et ne contenant pas la surface S (voir [Lo, section 3] pour plus de détails).

La quartique $\varepsilon(\mathcal{F})$ s'écrit alors

$$G(x,y,z) = \sum \lambda_i T_i = x^2G_2(y,z) + xG_3(y,z) + G_4(y,z) = 0, \tag{5}$$

où

$$\begin{aligned}G_2(y,z) &= \lambda_6g_0y^2 + (\lambda_1 + \lambda_6g_1 + \lambda_7g_0)yz + (\lambda_2 + \lambda_8g_0)z^2,\\ G_3(y,z) &= -\lambda_1y^3 + (-\lambda_2 + \lambda_3 + \lambda_6g_2 + \lambda_7g_1)y^2z\\ &\quad + (\lambda_4 + \lambda_6g_3 + \lambda_7g_2 + \lambda_8g_1)yz^2 + (\lambda_5 + \lambda_8g_2)z^3,\\ G_4(y,z) &= -\lambda_3y^4 - \lambda_4y^3z + (-\lambda_5 + \lambda_6 + \lambda_7g_3)y^2z^2\\ &\quad + (\lambda_7 + \lambda_8g_3)yz^3 + \lambda_8z^4.\end{aligned}$$

Pour écrire la courbe $\varepsilon(\mathcal{F})$ d'équation (5) sous sa forme canonique, on fixe (voir [CF, §1] pour plus des détails)

$$yX = z \quad \text{et} \quad Y = 2G_4(1,X)\,\frac{y}{x} + G_3(1,X), \tag{6}$$

et l'équation (5) prend finalement la forme $Y^2 = F(X)$, avec

$$F(X) = G_3(1,X)^2 - 4G_2(1,X)G_4(1,X). \tag{7}$$

La courbe $\mathcal{C}$ est la courbe projective, dont un morceau affine est défini par l'équation (7).

3. Exemple de courbe de genre 2 sur une surface de Del Pezzo de degré 4. On doit maintenant choisir des contraintes sur les coefficients $\lambda_1, \dots, \lambda_8$ et $g_0, \dots, g_3$ de telle sorte que la courbe $\mathcal{C}$ satisfasse certaines propriétés.

On veut que la courbe $\mathcal{C}$ soit un contre-exemple au principe de Hasse, on veut aussi que la jacobienne de cette courbe soit simple et que son groupe de Mordell–Weil soit de rang aussi grand que possible.

Il existe des critères pour vérifier si la jacobienne de la courbe est simple et pour trouver le sous-groupe de torsion du groupe de Mordell–Weil.

Comme on veut que le rang du groupe de Mordell–Weil soit le plus grand possible, il faut trouver un maximum des points rationnels sur $J(\mathcal{C})$ (comme la courbe $\mathcal{C}$ n'a pas de points rationnels, cela correspond à des couples des points sur $\mathcal{C}$ conjugués sur $\mathbb{Q}$). Le polynôme $P(X) = X^4 + g_3X^3 + g_2X^2 + g_1X + g_0$ est choisi de telle sorte qu'il se factorise en deux polynômes irréductibles de degré deux. Ceci nous fournira deux couples de points $\{p_2, p_3\}$ et $\{p_4, p_5\}$ qui sont définis dans une extension quadratique de $\mathbb{Q}$, conjugués sur $\mathbb{Q}$. Sur l'intersection

$$\varepsilon(\mathcal{F}) \cap (xz - y^2 = 0) \supset \{p_1, \dots, p_5\},$$

où p_1 compte double, il manque deux points ; ces deux nouveaux points nous fournissent encore un point sur $\mathfrak{S}$. Le fait de choisir que le polynôme G_4 puisse se factoriser en deux polynômes irréductibles de degré deux, génère deux nouveaux couples de points sur la courbe, définis sur une extension quadratique de $\mathbb{Q}$. Le point p_1 lui-même génère un couple de points sur $\mathcal{C}$. On obtient ainsi six couples distincts liés par certaines relations (voir la section 3.5).

Pour montrer que $\mathcal{C}$ n'a pas de points rationnels, j'utilise la méthode de [Wu] qui consiste à travailler avec des normes d'une extension de $\mathbb{Q}$. Cette méthode est liée à l'obstruction de Brauer–Manin. Dans mon cas je travaille avec le seul sous-corps réel $F = \mathbb{Q}[\xi]$ de $K = \mathbb{Q}(\zeta)$, où ζ est une racine primitive $5^{\text{ème}}$ de l'unité et ξ est l'une des racines du polynôme $X^2 - X - 1$. L'anneau des entiers de F est $\mathfrak{O}_F = \mathbb{Z}[\xi]$, qui est un anneau principal. Le premier 5 est totalement ramifié : $5\mathcal{O}_F = (2\xi - 1)^2$. Un premier rationnel reste inerte dans F si $p \equiv \pm 2 \pmod 5$. Il se décompose en deux idéaux premiers dans les autres cas. L'élément ξ est une unité de $\mathcal{O}_F$.

Pour utiliser la méthode de deux normes, il faut faire en sorte qu'après le changement de variable $y = x - v$ et $z = w$ dans G, on obtienne une équation $H(x, v, w) = G(x, x - v, w) = 0$ où les termes sans x s'écrivent comme $\mathrm{N}_{K/\mathbb{Q}}(v + \eta w)$ et les termes sans v s'écrivent comme

$$\mathrm{N}_{F/\mathbb{Q}}(v + \xi^j w) \cdot \mathrm{N}_{F/\mathbb{Q}}(v + \xi^{j+4} w).$$

On a pris j et $j+4$ puisque de cette façon, on trouvera qu'il n'y a qu'une seule solution (v, w) modulo 5 de

$$\mathrm{N}_{F/\mathbb{Q}}(v + \xi^j w) \cdot \mathrm{N}_{F/\mathbb{Q}}(v + \xi^{j+4} w) = 0.$$

On choisit donc à l'aide de l'ordinateur :

$$\begin{aligned} &\lambda_1 = -612, \quad &&\lambda_2 = 570, \quad &&\lambda_3 = -1, \quad &&\lambda_4 = 33, \\ &\lambda_5 = 8, \quad &&\lambda_6 = -18, \quad &&\lambda_7 = 28, \quad &&\lambda_8 = 1, \\ &g_0 = 34, \quad &&g_1 = -10, \quad &&g_2 = -19, \quad &&g_3 = 5. \end{aligned}$$

Ainsi les points éclatés sont $p_1 = (1 : 0 : 0)$ et $p_i = (1 : \omega_i : \omega_i^2)$ pour

$2 \le i \le 5$, où les ω_i sont les racines du polynôme

$$P(X) = X^4 + 5X^3 - 19X^2 - 10X + 34 = (X^2 - 2)(X^2 + 5X - 17).$$

Les termes sans x de $H(x, v, w) = G(x, x - v, w)$ s'écrivent comme

$$\mathrm{N}_{F/\mathbb{Q}}(v + \xi^3 w) \cdot \mathrm{N}_{F/\mathbb{Q}}(v + \xi^7 w).$$

Les termes sans v dans $H(x, v, w)$ s'écrivent

$$\mathrm{N}_{K/\mathbb{Q}}(x + (1 + \zeta)^5 w) = (x^2 - 11xw - w^2)^2.$$

En fait, le terme $x^2 - 11xw - w^2$ est la norme d'un élément de F car

$$(1 + \zeta)^5 = (\zeta^5 + \zeta)^5 = (\zeta^4 + 1)^5 = (1 + \overline{\zeta})^5 \in F.$$

La quartique plane $\varepsilon(\mathcal{F})$ obtenue est

$$G(x, y, z) = x^2 G_2(y, z) + xG_3(y, z) + G_4(y, z) = 0, \tag{8}$$

où

$$\begin{aligned} G_2(y, z) &= -612y^2 + 520yz + 604z^2, \\ G_3(y, z) &= 612y^3 - 509y^2 z - 599yz^2 - 11z^3, \\ G_4(y, z) &= y^4 - 33y^3 z + 114y^2 z^2 + 33yz^3 + z^4 \\ &= (y^2 - 29yz - z^2)(y^2 - 4yz - z^2). \end{aligned}$$

La courbe $\mathcal{C}$ est la courbe projective dont un morceau affine est défini par (2).

3.1. *Points rationnels sur la courbe*

Proposition 3.1. *La courbe projective plane $\varepsilon(\mathcal{F})$, définie par* (8), *de genre géométrique* 2, *ne possède comme point rationnel que le point double p_1.*

Preuve. On effectue le changement de variable $y = x - v$ et $z = w$ dans l'équation (8), pour obtenir

$$\begin{aligned} H = x^4 &+ (-616v - 22w)x^3 + (1230v^2 + 597vw + 119w^2)x^2 \\ &+ (-616v^3 - 608v^2 w + 371vw^2 + 22w^3)x \\ &+ v^4 + 33v^3 w + 114v^2 w^2 - 33vw^3 + w^4 = 0. \end{aligned} \tag{9}$$

On pose ensuite

$$\begin{aligned} r &= \mathrm{N}_{F/\mathbb{Q}}(v + \xi^3 w)\mathrm{N}_{F/\mathbb{Q}}(v + \xi^7 w) = (v^2 + 4vw - w^2)(v^2 + 29vw - w^2), \\ s &= (\mathrm{N}_{F/\mathbb{Q}}(x - \xi^5 w))^2 = (x^2 - 11xw - w^2)^2 \end{aligned}$$

et on constate que l'équation (9) peut être récrite sous chacune des deux formes suivantes :

$$x \cdot f + r = 0, \qquad v \cdot g + s = 0,$$

où f et g sont les polynômes homogènes de degré 3 suivants :

$$\begin{aligned} f &= x^3 + (-616v - 22w)x^2 + (1230v^2 + 59727vw + 119w^2)x \\ &\quad - 616v^3 - 608v^2w + 371vw^2 + 22w^3, \\ g &= v^3 + (-616x + 33w)v^2 + (1230x^2 - 608xw + 114w^2)v \\ &\quad - 616x^3 + 597x^2w + 371xw^2 - 33w^3. \end{aligned}$$

Soit $(x : v : w)$ une solution rationnelle de (9). On peut supposer que x, v, w sont des entiers sans facteurs communs.

Si un nombre premier p divise deux des variables, alors il divise aussi la troisième. On en conclut que x, v, w sont premiers deux à deux.

Par la suite, on va étudier les nombres premiers p susceptibles de diviser x, v ou w.

Soit p un premier rationnel, avec $p \equiv \pm 2 \pmod 5$. Dans ce cas p reste inerte dans F. Cela veut dire que si p divise r, alors

$$p \mid v + \xi^3 w = v + w + 2w\xi,$$

ou

$$p \mid v + \xi^7 w = v + 8w + 13w\xi.$$

Puisque l'anneau des entiers de F est $\mathbb{Z}[\xi]$, alors $p \mid v + w$ et $p \mid 2w$ ou bien $p \mid v + 8w$ et $p \mid 13w$. Comme v et w sont premiers entre eux, alors ou bien $p = 2$ ou bien $p = 13$ respectivement. En particulier,

$$p^2 \nmid v + w + 2w\xi \quad \text{et} \quad p^2 \nmid v + 8w + 13w\xi.$$

Cela veut dire que si $2 \mid r$ alors $2^2 \parallel r$ et si $13 \mid r$ alors $13^2 \parallel r$.

Si $2 \mid x$ alors $2^2 \parallel r$. D'un autre côté, comme x est paire et v et w sont impaires, alors $2 \nmid f$ et $2^2 \parallel x$.

Si $13 \mid x$, alors $f \equiv w^3 \pmod{13}$, car $v \equiv -8w \pmod{13}$. Il en résulte que $13^2 \parallel x$.

Si p divise s (pour $p \equiv \pm 2 \pmod 5$), alors p divise

$$x - \xi^5 w = x - 3w - 5w\xi.$$

Maintenant comme p ne divise pas 5, on a forcément que p divise $x - 3w$ et w. Comme x et w sont premiers entre eux, p ne divise pas s.

On en déduit donc que s, v et g sont composés de facteurs premiers de la forme $p \equiv 0, \pm 1 \pmod 5$ et r, x et f sont composés de facteurs premiers de la forme $p \equiv 0, \pm 1 \pmod 5$ et éventuellement de 2 et 13. Mieux encore :

REMARQUE 3.2. On peut donc en conclure que s, v, g, r, x et f s'écrivent comme des puissances de 5 fois un nombre congru à ± 1 modulo 5.

Montrons maintenant que 5 ne divise ni x, ni v.

En fait, si $5 \mid x$, alors 5 divise r, autrement dit :

$$\left.\begin{aligned} &v + w + 2w\xi = v - 3w + 2w(\xi + 2) \text{ ou} \\ &v + 8w + 13w\xi = v - 3w - 15w + 13w(\xi + 2) \end{aligned}\right\} \in (\xi + 2)\mathfrak{O}_F,$$

où $(\xi+2)\mathfrak{O}_F$ est le seul idéal dont la norme est 5. Cela veut dire que $v - 3w$ est multiple de 5, ou autrement dit,

$$w \equiv 2v \pmod 5.$$

On a alors

$$f \equiv -616v^3 - 608v^2(2v) + 371v(2v)^2 + 22(2v)^3 \equiv 3v^3 \pmod 5. \tag{10}$$

Par ailleurs, 5 ne divise pas v (puisqu'il divise déjà x). Ainsi, par la remarque 3.2, $v \equiv \pm 1 \pmod 5$. L'équation (10) devient maintenant $f \equiv \pm 3 \pmod 5$. Il en résulte une contradiction par la remarque 3.2.

Supposons maintenant que $5 \mid v$. Dans ce cas 5 divise s. Comme

$$s = (\mathrm{N}_{F/\mathbb{Q}}(x - 3w - 5w\xi))^2,$$

on a alors $5 \mid x - 3w$. Cela veut dire que $w \equiv 2x \pmod 5$. Dans ce cas on a

$$g \equiv -616x^3 + 597x^2(2x) + 371x(2x)^2 - 33(2x)^3 \equiv 3x^3 \pmod 5. \tag{11}$$

Comme $x \equiv \pm 1 \pmod 5$, alors $g \equiv \pm 3 \pmod 5$. Ceci est impossible par la remarque 3.2.

Il s'ensuit que x et v sont premiers à 5, et donc $x, v \equiv \pm 1 \pmod 5$. Comme $(x : v : w) = (-x : -v : -w)$ dans $\mathbb{P}^2$, alors on peut supposer $x \equiv 1 \pmod 5$ et $v \equiv \pm 1 \pmod 5$.

1$^{\text{e}}$ CAS : Il existe une solution de $G = 0$ avec $x \equiv 1 \pmod 5$ et $v \equiv -1 \pmod 5$. Dans ce cas, l'équation (9) : $H = 0$ devient modulo 5

$$\begin{aligned} 0 &\equiv 1 + (616 - 22w) + (1230 - 597w + 119w^2) \\ &\quad + (616 - 608w - 371w^2 + 22w^3) + (1 - 33w + 114w^2 + 33w^3 + w^4) \\ &\equiv 4 + 2w^2 + w^4 \pmod 5, \end{aligned}$$

qui n'a pas de solution modulo 5.

2$^{\text{e}}$ CAS : Il existe une solution de $G = 0$ avec $x \equiv 1 \pmod 5$ et $v \equiv 1 \pmod 5$. Dans ce cas, l'équation (9) : $H = 0$ devient modulo 5

$$\begin{aligned} 0 &\equiv 1 + (-616 - 22w) + (1230 + 597w + 119w^2) \\ &\quad + (-616 - 608w + 371w^2 + 22w^3) + (1 + 33w + 114w^2 - 33w^3 + w^4) \\ &\equiv w^2(w - 3)^2 \pmod 5, \end{aligned}$$

qui a comme solutions $w \equiv 0$ et $3 \pmod 5$.

La solution avec $w \equiv 0 \pmod 5$ correspond à la solution

$$(x : y : z) = (x, x - v, w)$$

de l'équation (8), avec $x \equiv 1 \pmod 5$ et y et z multiples de 5. En écartant la solution $(x : y : z) = (1 : 0 : 0)$ qui est de cette forme, on peut supposer que y ou z est non nul.

Dans ce cas, il existe $\gamma \in \mathbb{N}_{>0}$ telle que 5^γ est la plus grande puissance de 5 qui divise y et z en même temps. On a alors

$$5^{3\gamma} \mid xG_3(y,z) + G_4(y,z)$$

et donc $5^{3\gamma}$ divise $G_2(y,z)$, car x est premier à 5.

Si l'on note $y = 5^\gamma \widetilde{y}$ et $z = 5^\gamma \widetilde{z}$, on voit que

$$5^\gamma \mid G_2(\widetilde{y}, \widetilde{z}) \quad \text{avec } \gamma \geq 1.$$

Mais ceci est satisfait seulement pour $\widetilde{y}$ et $\widetilde{z}$ multiples de 5, car le polynôme $G_2(y,z)$ est irréductible sur $\mathbb{F}_5$. Ceci contredit la maximalité de γ.

Il ne reste qu'à voir ce qui arrive si $w \equiv 3 \pmod 5$. Cette solution de $H = 0$ correspond à la solution $(x : y : z) = (x, x - v, w)$ de l'équation (5), avec $x \equiv 1 \pmod 5$, y multiple de 5 et $z \equiv 3 \pmod 5$. D'où l'on trouve

$$G \equiv 20 \pmod{25}. \ \blacksquare$$

3.2. *Démonstration de la proposition 3.1 par la théorie du corps de classes.* J.-L. Colliot-Thélène a remarqué qu'on peut interpréter cette preuve à l'aide de la théorie du corps de classes. Il suffit de regarder la fonction $h = v/x$ définie sur l'ouvert $\mathcal{U}$, de la courbe $\mathcal{H}$ définie par (9), défini par les éléments $(x : v : w) \in \mathcal{H}$ tels que $x \neq 0$, dont le diviseur est une norme (voir [CCS, paragraphe 4] pour la relation avec l'obstruction de Brauer–Manin). Commençons par donner quelques définitions. Soit k un corps de nombres et F une extension abélienne finie de k. On note Σ l'ensemble des places ν de k. Pour $\nu \in \Sigma$, on note k_ν le complété de k par ν. On note $\mathfrak{O}_\nu$ l'anneau des entiers de k_ν (si ν est une place finie) et U_ν les unités de $\mathfrak{O}_\nu$.

Le groupe des idèles de k est

$$\mathfrak{I}_k = \left\{ (\alpha_\nu) \in \prod k_\nu^* \;\middle|\; \alpha_\nu \in U_\nu \text{ sauf pour un nombre fini de places } \nu \right\}.$$

On a l'inclusion naturelle $i : k^* \to \mathfrak{I}_k$ qui envoie

$$a \mapsto (a_\nu), \quad \text{où} \quad a_\nu = a \in k^* \subset k_\nu^*.$$

Cette inclusion est bien définie car $a \in U_\nu^*$ pour presque toute place finie ν.

On note $\varphi_\nu : k_\nu^* \to \mathrm{Gal}(F/k)$ l'homomorphisme local d'Artin et on définit l'application $\varphi : \mathfrak{I}_k \to \mathrm{Gal}(F/k)$ par

$$\varphi((\alpha_\nu)_{\nu \in \Sigma}) = \prod_\nu \varphi_\nu(\alpha_\nu).$$

Cette application est bien définie car on a $\varphi_\nu(\alpha_\nu) = 1$ sauf pour un nombre fini de places (voir [Neu, chapitre IV.6]). En particulier si $a \in k^*$, alors $\varphi(a) = 1$. Pour notre exemple, $k = \mathbb{Q}$ et $F = \mathbb{Q}[\xi]$, où ξ est une racine du

polynôme $X^2 - X - 1$. On identifie $\mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q})$ avec $\{\pm 1\}$. Pour $a \in \mathbb{R}^*$ on a $\varphi_\infty(a) = 1$. Pour $p \neq 5$, $\varphi_p(a)$ est le résidu quadratique de p^l et 5 où $a = up^l \in \mathbb{Q}_p^*$ avec $u \in U_p$. Pour $p = 5$, $\varphi_5(a)$ est le résidu quadratique de u et 5 où $a = u5^l \in \mathbb{Q}_5^*$ avec $u \in U_5$.

On considère maintenant la fonction

$$h : \mathcal{U}(\mathbb{Q}) \to \mathbb{Q}^*, \qquad (x : v : w) \mapsto v/x.$$

Supposons que $\mathcal{U}(\mathbb{Q}) \neq \emptyset$. On considère la composition

$$\varphi \circ i \circ h : \mathcal{U}(\mathbb{Q}) \xrightarrow{h} \mathbb{Q}^* \xrightarrow{i} \mathfrak{I}_{\mathbb{Q}} \xrightarrow{\varphi} \mathrm{Gal}(\mathbb{Q}[\xi]/\mathbb{Q}),$$

dont l'image est $\{1\}$. D'autre part,

$$\varphi \circ i \circ h = \prod_{p \in \Sigma} (\varphi_p \circ h).$$

Soit $(x : v : w) \in \mathcal{U}(\mathbb{Q})$; par la définition de φ_∞ et par la preuve de la proposition 3.1, pour $p = \infty$ et $p \nmid 5$ on a

$$\mathrm{Im}(\varphi_p \circ h) = \{1\}.$$

Cela implique

$$\mathrm{Im}(\varphi_5 \circ h) = \{[1]\}.$$

Ensuite, on montre que 5 n'intervient pas dans la factorisation de $h(x : v : w)$ et que la seule préimage de 1 par $\varphi_5 \circ h$ est

$$(x : v : w) = (1 : 1 : 0).$$

Ce point correspond au point double $(x : y : z) = (1 : 0 : 0)$.

3.3. *Solutions locales de l'exemple*

Proposition 3.3. *La courbe projective $\mathcal{C}$ de genre* 2, *dont un morceaux affine est défini par l'équation* (2) :

$$\begin{aligned} Y^2 &= F(X) \\ &= -2295X^6 - 68630X^5 + 28383X^4 \\ &\quad + 519710X^3 - 128799X^2 - 705880X + 376992, \end{aligned}$$

possède des points lisses dans tous les complétés de $\mathbb{Q}$.

Preuve. C'est clair dans $\mathbb{R}$. Par le théorème de Hasse–Weil et le lemme de Hensel, il suffit d'étudier les solutions sur $\mathbb{Q}_p$ pour les premiers $p \leq 13$ et pour les premiers p de mauvaise réduction de $\mathcal{C}$.

Pour $p = 2$ on pose $X = 1$ et on obtient $F(X) = 19481 \equiv 1 \pmod 8$.

Pour $p = 3$, 5, 7 et 11 on trouve une solution avec $X = 2$; pour $p = 13$, avec $X = 4$.

Pour connaître les premiers p de mauvaise réduction, on calcule le discriminant de F :

$$\operatorname{disc}(F) = 2^{22} \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 17 \cdot 71^2 \cdot 14929^2 \cdot 6581857 \cdot 70765958057049924786314 53.$$

On remarque que pour $p = 3$ et pour $p = 17$, F est un polynôme de degré 5 sans racines multiples, donc la réduction modulo 3 et modulo 17 de $\mathcal{C}$ est lisse. C'est-à-dire, les premiers de mauvaise réduction sont :

$$2,\ 5,\ 7,\ 11,\ 71,\ 14929,\ 6581857,\ 70765958057049924786314 53. \tag{12}$$

Cela veut dire qu'il faut encore trouver des solutions lisses dans $\mathbb{F}_p$, pour $p_1 = 71$, $p_2 = 14929$, $p_3 = 6581857$ et $p_4 = 70765958057049924786314 53$.

Si l'on remplace $X = -1$, on a $F(-1) = 529081$ qui est un carré modulo p_1, p_2 et p_4. En faisant $X = 1$, on a $F(1) = 19481$, qui est un carré modulo p_3. ∎

3.4. *Étude de la jacobienne de l'exemple*

Proposition 3.4. *La jacobienne de la courbe lisse $\mathcal{C}$ de genre* 2, *définie par* (2), *est simple et son groupe de Mordell–Weil est sans torsion.*

Preuve. Pour voir que la jacobienne de $\mathcal{C}$ est simple, il suffit d'appliquer l'argument de [St1] avec le premier $p = 13$.

Pour la torsion, il suffit de calculer le nombre d'éléments de la jacobienne sur $\mathbb{F}_p$, pour $p = 13$ et $p = 23$:

$$\#\widetilde{J}(\mathbb{F}_{13}) = 128 = 2^7, \qquad \#\widetilde{J}(\mathbb{F}_{23}) = 789 = 3 \cdot 263.$$

Comme $\#\widetilde{J}(\mathbb{F}_{13})$ et $\#\widetilde{J}(\mathbb{F}_{23})$ n'ont pas de facteurs en commun, on a bien $\#\mathfrak{S}_{\mathrm{tor}} = 1$ (voir [CF, corollaire du théorème 7.4.1 et §8.2]). ∎

Il ne nous reste qu'à trouver quatre éléments indépendants du groupe de Mordell–Weil pour montrer complètement le théorème 1.2.

3.5. *Rang du groupe de Mordell–Weil de la jacobienne de la courbe de genre 2*

Notation 3.5. Soient $\mathfrak{a}, \mathfrak{b} \in \overline{\mathcal{C}}$. On note $\{\mathfrak{a}, \mathfrak{b}\}$ la classe dans $J(\mathcal{C})$ du diviseur $\mathfrak{a} + \mathfrak{b} - K_{\mathcal{C}} \in \operatorname{Div}^0 \overline{\mathcal{C}}$, où $K_{\mathcal{C}}$ est un diviseur rationnel dans la classe canonique. L'involution de $\mathfrak{r} = (x, y) \in \mathcal{C}$ est notée $\overline{\mathfrak{r}} = (x, -y)$. L'involution s'étend de façon naturelle à $\operatorname{Div}\overline{\mathcal{C}}$ et à $\operatorname{Pic}\overline{\mathcal{C}}$.

Considérons la quartique plane $\varepsilon(\mathcal{F})$ définie par (8). Comme expliqué au début de la section 3, en intersectant la quartique $\varepsilon(\mathcal{F})$ avec la conique définie par $xz = y^2$, on obtient les points $p_1 = (1 : 0 : 0)$ et $p_i = (1 : \omega_i : \omega_i^2)$ pour $2 \le i \le 7$ où ω_2 et ω_3 sont les racines de $X^2 - 2$, ω_4 et ω_5 les racines de $X^2 + 5X - 17$ et ω_6 et ω_7 les racines de $X^2 + 28X - 18$.

En considérant $x = 0$, on obtient $G_4(y, z) = 0$, où

$$G_4(y, z) = (y^2 - 4yz - z^2)(y^2 - 29yz - z^2).$$

On note p_8, p_9, p_{10}, p_{11} les points correspondants.

Si l'on pose $x = y$ dans $G = 0$, on obtient

$$(y^2 - 11yz - z^2)^2 = 0.$$

On note p_{12}, p_{13} ces derniers points.

Sur $\mathcal{C}$, p_1 s'éclate en deux points $P_0, P_1 \in \mathcal{C}$. On note $P_j \in \mathcal{C}$ les points qui correspondent aux points $p_j \in \varepsilon(\mathcal{F})$ pour $2 \leq j \leq 13$.

En appelant h le morphisme

$$h : \mathcal{C} \to \varepsilon(\mathcal{F}),$$

défini par la relation (6) et à partir des diviseurs des fonctions

$$\frac{y^2 - xz}{y^2} \circ h, \quad \frac{x}{y} \circ h, \quad \frac{x - y}{y} \circ h,$$

on obtient les relations suivantes sur $\mathfrak{S}$:

$$\begin{aligned} \{P_0, P_1\} &= \{P_2, P_3\} + \{P_4, P_5\} + \{P_6, P_7\}, \\ \{P_0, P_1\} &= \{P_8, P_9\} + \{P_{10}, P_{11}\}, \\ \{P_0, P_1\} &= 2\{P_{12}, P_{13}\}. \end{aligned} \tag{13}$$

Ces éléments engendrent donc un sous-groupe de rang ≤ 4 sur $\mathfrak{S}$. Le lemme suivant termine la démonstration du théorème 1.2 :

LEMME 3.6. *Les points*

$$\{P_2, P_3\},\ \{P_4, P_5\},\ \{P_8, P_9\} \text{ et } \{P_{12}, P_{13}\}$$

du groupe de Mordell–Weil $\mathfrak{S}$ *sont indépendants.*

Preuve. On considère le morphisme Φ défini par Cassels (voir [Cas]),

$$\Phi : \mathfrak{S} \to \mathcal{L} \quad \text{avec} \quad \Phi(\{(x, y), (u, v)\}) = (x - X)(u - X),$$

où $\mathcal{L} = L^*/\mathbb{Q}^*(L^*)^2$ et $L = \mathbb{Q}[X]/(F(X))$. Les images dans $\mathcal{L}$ de ces points sont

$$X^2 - 2, \quad X^2 + 5X - 17, \quad X^2 + 4X - 1 \quad \text{et} \quad X^2 + 11X - 1$$

respectivement.

On conclut en travaillant sur certains complétés p-adiques de $\mathbb{Q}$ (comme dans [St1]), où le polynôme F se factorise complètement. Dans ce cas particulier, on travaille avec les premiers 8017, 8069 et 12821. Voir ma thèse [Lo] pour les détails. ∎

REMARQUE 3.7. Le noyau de Φ est $\ker \Phi = 2\mathfrak{S} \cup \mathcal{M}$, où $\mathcal{M}$ est l'ensemble d'éléments $\mathcal{U} \in \mathrm{Pic}^0 \mathcal{C}$ tels qu'il existe $\mathcal{V} \in (\mathrm{Pic}^1 \overline{\mathcal{C}})^G$ avec $\mathcal{U} = \mathcal{V} - \overline{\mathcal{V}}$ (voir [PS, théorème 11.3]).

D'autre part si $\mathcal{M} \neq \emptyset$, alors $\mathcal{M} \in 2\mathfrak{S}$ si et seulement s'il existe un point de Weierstrass $\mathfrak{a} = (\theta, 0) \in \mathcal{C}(\mathbb{Q})$ ou s'il existe trois points de Weierstrass $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$ tels que la classe du diviseur $\mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3$ est définie sur $\mathbb{Q}$ (voir [CF, lemme 6.5.1]).

Dans le cas de la courbe définie par (2), on ne sait pas si $\mathcal{M}$ est vide ou pas ; mais si $\mathcal{M} \neq \emptyset$ alors $\mathcal{M} \notin \text{Ш}$. Par [CM, proposition 2.4], l'existence d'une classe rationnelle de degré 1 est equivalente à l'existence d'un diviseur rationnel de degré 1, puisque la courbe a des points dans tous les complétés de $\mathbb{Q}$. Si l'on arrivait à trouver un tel diviseur sur la courbe, on trouverait un élément de Ш indépendant des précédents.

Remerciements. Je remercie le professeur Daniel Coray pour le temps qu'il m'a consacré, son intérêt et ses conseils, le professeur Constantin Manoil pour ses encouragements, sa patience et son amitié, et le referee pour son avis et ses conseils.

Références

[Be] A. Beauville, *Surfaces algébriques complexes*, Soc. Math. France, Paris, 1978.

[Cas] J. W. S. Cassels, *The Mordell–Weil group and curves of genus 2*, in: Arithmetic and Geometry. Papers dedicated to I. R. Shafarevich, Vol. I, Arithmetic, Birkhäuser, Boston, MA, 1983, 29–60.

[CF] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, London Math. Soc. Lecture Note Ser. 230, Cambridge Univ. Press, 1996.

[CCS] J.-L. Colliot-Thélène, D. Coray et J.-J. Sansuc, *Descente et principe de Hasse pour certaines variétés rationnelles*, J. Reine Angew. Math. 320 (1980), 150–191.

[CM] D. Coray and C. Manoil, *On large Picard groups and the Hasse Principle for curves and* K3 *surfaces*, Acta Arith. 76 (1996), 165–189.

[Fly] E. V. Flynn, *The Hasse principle and the Brauer–Manin obstruction for curves*, Manuscripta Math. 115 (2004), 437–466.

[Ha] R. Hartshorne, *Algebraic Geometry*, Springer, 1977.

[Lo] V. G. Lopez Neumann, *Points rationnels et jacobienne des courbes de genre 2*, thèse, Genève, 2004.

[Ma] Ju. I. Manin, *Cubic Forms*, North-Holland, Amsterdam, 1974.

[Neu] J. Neukirch, *Class Field Theory*, Springer, Berlin, 1986.

[PS] B. Poonen and E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. 488 (1997), 141–188.

[St1] M. Stoll, *Two simple* 2*-dimensional abelian varieties defined over* $\mathbb{Q}$ *with Mordell–Weil group of rank at least* 19, C. R. Acad. Sci. Paris Sér. I 321 (1995), 1341–1344.

[St2] —, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. 98 (2001), 245–277.

[Wu] C. Wuthrich, *Une quintique de genre 1 qui contredit le principe de Hasse*, Enseign. Math. 47 (2001), 161–172.

Departamento de Matemática
Universidade Federal de Uberlândia
av. J. N. de Ávila 2160
38408-100, Uberlândia-MG, Brazil
E-mail: gonzalo@famat.ufu.br

Reçu le 19.1.2005
et révisé le 6.8.2006 (4926)