Hauteurs et descente infinie sur les courbes hyperelliptiques

S. Duquesne

Résumé

Nous calculons les traces de la loi de groupe sur la variété de Kummer d'une courbe hyperelliptique de genre 3 définie par un polynôme de degré 7. Cela permet de définir une théorie des hauteurs sur la jacobienne de telles courbes et devrait fournir, à terme, des algorithmes de calculs de la torsion et de descente infinie pour ces jacobiennes.

Abstract

We compute traces of the group structure on the Kummer variety of a hyperelliptic curve of genus 3 defined by a polynomial of degree 7. This allows to define a height function on the jacobian of such curves and will give algorithms for computing torsion subgroup and for infinite descent on these jacobians.

Introduction

Nous nous intéressons ici aux courbes hyperelliptiques de genre 2 et 3. Ces courbes peuvent être données par des équations du type :

$$\mathcal{C} : y^2 = f(x) \tag{1}$$

où $f \in \mathbb{Q}[x]$ est sans facteur carré.
Nous avons choisi de prendre $\mathbb{Q}$ comme corps de base dans la suite, bien que tout soit généralisable aux corps de nombres, car les algorithmes énoncés ne sont, en général, pas applicables en pratique sur les corps de nombres.
Le degré du polynôme f détermine dans ce cas le genre de la courbe (g=2 si le degré vaut 5 ou 6, g=3 si il vaut 7 ou 8, ...). Dans le cas des courbes elliptiques (genre 1 et $\deg(f)$=3 ou 4), nous disposons d'une structure de groupe sur l'ensemble des points de la courbe, et c'est cette structure qui explique leur succès.
En genre supérieur, nous disposons d'un analogue, appelé jacobienne et que nous noterons $\mathcal{J}$ dans la suite. Cette jacobienne est construite à partir des sommes finies formelles de points de la courbe et il est possible de démontrer, en utilisant le théorème de Riemann-Roch, que chacun de ses éléments rationnels peut être représenté par g points de la courbe $\mathcal{C}$ conjugués sur une extension de $\mathbb{Q}$ de degré g. C'est cette représentation que nous utiliserons dans la suite.
Il existe bien sûr une définition géométrique de la loi de groupe. Par exemple, dans le cas du genre 2, si $\mathcal{A}$ et $\mathcal{B}$ sont deux éléments de la jacobienne J représentés chacun par 2 points de la courbe, il existe une unique cubique passant par ces 4 points. L'intersection de cette cubique et de la courbe $\mathcal{C}$ est alors constituée de 6 points dont les 4 initiaux. Les deux points restants permettent de définir un troisième élément de la jacobienne tel que $\mathcal{A} + \mathcal{B} + \mathcal{C} = \mathcal{O}$. La somme de $\mathcal{A}$ et $\mathcal{B}$ est donc $-\mathcal{C}$.

Comme dans le cas des courbes elliptiques, l'ensemble des points rationnels de la

jacobienne est un groupe abélien libre de type fini. La détermination effective de la structure de ce groupe est actuellement l'un des principaux problèmes concernant ces courbes. Elle se décompose en trois parties, la détermination du sous-groupe de torsion, dont nous dirons deux mots, la 2-descente qui consiste à calculer $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$, et la descente infinie qui permet d'en déduire un système de générateurs. La 2-descente peut être effectuée grâce à des algorithmes développés en grande partie par Stoll [Sto 01] et qui sont des analogues de ceux de Cremona [Cre 97] pour les courbes elliptiques. La principale motivation des travaux qui suivent est la descente infinie.

1 Variété de Kummer

La jacobienne d'une courbe de genre 2 ou 3 est un objet trop lourd à manipuler, même avec les ressources informatiques actuelles, c'est la raison pour laquelle, Flynn [Fly-Sma 97], [Fly 93] définit la variété de Kummer qui consiste essentiellement à identifier deux éléments de la jacobienne si ils sont reliés par l'involution hyperelliptique (c'est à dire, dans le cas des courbes de la forme (1), l'application qui à un point $[x, y]$ de la courbe associe le point $[x, -y]$). Dans le cas des courbes elliptiques, cela revient à ne prendre en compte que l'abscisse des points. Dans le cas des courbes de genre 2, Flynn définit l'application κ suivante:

$$\begin{array}{rcl} \kappa : J(\mathbf{Q}) & \longrightarrow & \mathbb{P}^3(\mathbb{Q}) \\ \{[x_1, y_1], [x_2, y_2]\} & \longmapsto & [\xi_1, \xi_2, \xi_3, \xi_4] \ , \end{array}$$

où

$$\begin{array}{rcl} \xi_1 & = & 1 \ , \\ \xi_2 & = & x_1 + x_2 \ , \\ \xi_3 & = & x_1 x_2 \ , \\ \xi_4 & = & \dfrac{F_0(x_1, x_2) - 2y_1 y_2}{(x_1 - x_2)^2} \ , \end{array}$$

avec

$$F_0(x_1,x_2)=2f_0+f_1(x_1+x_2)+2f_2x_1x_2+f_3(x_1+x_2)x_1x_2+2f_4x_1^2x_2^2+f_5(x_1+x_2)x_1^2x_2^2+2f_3x_1^3x_2^3.$$

La variété de Kummer $\mathcal{K}$ est alors le lieu projectif de ces quatres éléments donné par une quartique explicite qui correspond à une traduction de l'équation de la courbe $\mathcal{C}$. L'image de l'élément neutre $\mathcal{O}$ pour la loi de groupe sur la jacobienne par cette application est $[0, 0, 0, 1]$, et deux éléments distincts ont la même image dans $\mathcal{K}$ s'ils sont opposés l'un de l'autre.
Ainsi, sur la variété de Kummer, il n'est plus possible de distinguer l'élément $\mathcal{A}$ de l'élément $-\mathcal{A}$. Il devient donc impossible d'additionner un élément $\mathcal{A}$ et un élément $\mathcal{B}$ puisque le résultat peut être soit $\pm(\mathcal{A}+\mathcal{B})$ soit $\pm(\mathcal{A}-\mathcal{B})$. En passant de la jacobienne à la variété de Kummer, nous avons donc perdu la structure de groupe qui constituait pourtant le principal intérêt de la jacobienne. Il en subsiste cependant des traces que nous verrons dans le paragraphe suivant. Notons toutefois que cela permet de considérablement simplifier les calculs de ces traces de la loi de groupe, en particulier au niveau de la place mémoire.

Dans le cas des courbes de genre 3, Stubbs, un élève de Flynn a pu construire la variété de Kummer pour une courbe de la forme (1) avec

$$f(x) = f_7 x^7 + \cdots + f_1 x + f_0 \in \mathbb{Q}[x] \ ,$$

Soient $[x_1, y_1]$, $[x_2, y_2]$ et $[x_3, y_3]$ trois points quelconques de $\mathcal{C}\left(\overline{\mathbf{Q}}\right)$ tels que le 3-uplet $\{[x_1, y_1], [x_2, y_2], [x_3, y_3]\}$ représente un élément de la jacobienne $J(\mathbf{Q})$. Stubbs définit alors les fonctions suivantes :

$$
\begin{aligned}
a_0 &= 1 \ , \\
a_1 &= x_1 + x_2 + x_3 \ , \\
a_2 &= x_1x_2 + x_1x_3 + x_2x_3 \ , \\
a_3 &= x_1x_2x_3 \ , \\
c_0 &= a_0b_0^2 - f_7a_1^3 + f_7a_2a_1 - f_6a_1^2 + 3f_7a_3 + 2f_6a_2 \ , \\
c_1 &= a_1b_0^2 + 2a_0b_0b_1 - f_7a_1^4 + 3f_7a_2a_1^2 - f_6a_1^3 - f_7a_2^2 - f_7a_3a_1 + 2f_6a_2a_1 - f_5a_1^2 + 2f_5a_2 \ , \\
c_2 &= a_0b_1^2 - a_2b_0^2 + f_7a_2a_1^3 - 2f_7a_2^2a_1 + f_6a_2a_1^2 + f_7a_3a_2 - f_6a_2^2 + f_5a_2a_1 - 3f_5a_3 \ , \\
c_3 &= a_1b_1^2 + 2a_2b_0b_1 + a_3b_0^2 + f_7a_2^2a_1^2 - f_7a_3a_1^3 + f_7a_3a_2a_1 - f_7a_2^3 + f_6a_2^2a_1 - f_6a_3a_1^2 + f_5a_2^2 - f_5a_3a_1 \ ,
\end{aligned}
$$

avec

$$
\begin{aligned}
\delta &= (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \ , \\
b_0 &= (x_1y_2 - x_2y_1 - x_3y_2 + x_3y_1 - x_1y_3 + x_2y_3)/\delta \ , \\
b_1 &= \left(x_3^2y_2 - x_3^2y_1 + x_2^2y_1 + y_3x_1^2 - y_2x_1^2 - y_3x_2^2\right)/\delta \ .
\end{aligned}
$$

Dans ces conditions, l'application

$$
\begin{aligned}
\mathcal{J}(\mathbf{Q}) &\rightarrow \mathbb{P}^7(\mathbf{Q}) \\
\{[x_1, y_1], [x_2, y_2], [x_3, y_3]\} &\mapsto [a_0, a_1, a_2, a_3, c_0, c_1, c_2, c_3]
\end{aligned}
$$

définit un plongement de la variété de Kummer dans $\mathbb{P}^7(\mathbf{Q})$.

Dans le cas du genre 2, la variété de Kummer était définie par une équation en les ξ_1, ξ_2, ξ_3, ξ_4 qui reflétait l'équation définissant la courbe. Dans le cas présent, les choses sont bien moins simples puisque la variété de Kummer d'une courbe de genre 3 est définie par 27 équations explicites en les a_0, a_1, a_2, a_3, c_0, c_1, c_2, c_3, du moins conjecturellement. Ces équations sont données dans la thèse de Stubbs [Stu 00] et sur le site ftp de Flynn (ftp.liv.ac.uk/pub/genus2/stubbs).

Nous allons donner ici la plus simple de ces équations car elle jouera un rôle particulier dans la suite :

$$
a_0c_3 - a_1c_2 - a_2c_1 - a_3c_0 - 2f_5a_1a_3 + f_5a_2^2 + 2f_6a_2a_3 + 3f_7a_3^2 = 0 \ . \tag{2}
$$

Toutes les autres équations sont des quartiques en a_0, a_1, a_2, a_3, c_0, c_1, c_2 et c_3.

Exactement comme dans le cas des courbes de genre 2, nous perdons la structure de groupe de la jacobienne en passant dans la variété de Kummer mais les calculs s'en retrouvent considérablement simplifiés. Il reste cependant des traces de la loi de groupe qui sont d'ailleurs les mêmes que dans le cas des courbes de genre 2. Nous allons maintenant étudier ces traces.

2 Calcul des traces de la loi de groupe sur la variété de Kummer

Sur la variété de Kummer, le problème principal est que l'on ne sait pas distinguer l'élément $\mathcal{A} + \mathcal{B}$ de l'élément $\mathcal{A} - \mathcal{B}$. Nous pouvons cependant par exemple

toujours définir la multiplication par 2. Il paraît en effet difficile de confondre $2\mathcal{A} = \mathcal{A} + \mathcal{A}$ et $\mathcal{A} - \mathcal{A} = \mathcal{O}$. C'est aussi le cas de l'addition d'un élément d'ordre 2 puisqu'un tel élément est égal à son opposé. D'autre part, il est également possible d'exprimer les $\xi_i(\mathcal{A}+\mathcal{B})\xi_j(\mathcal{A}-\mathcal{B}) + \xi_i(\mathcal{A}-\mathcal{B})\xi_j(\mathcal{A}+\mathcal{B})$ en fonction des coordonnées de $\mathcal{A}$ et $\mathcal{B}$ (c'est à dire en fonction des $\xi_i(\mathcal{A})$ et $\xi_i(\mathcal{B})$). Nous avons en effet le théorème suivant ([Fly 93] en genre 2, [Duq 01] en genre 3) :

Théorème 1 *Il existe des polynômes explicites B_{ij} biquadratiques en $\xi_i(\mathcal{A})$, $\xi_i(\mathcal{B})$ tels que projectivement,*

$$(\xi_i(\mathcal{A}+\mathcal{B})\xi_j(\mathcal{A}-\mathcal{B}) + \xi_i(\mathcal{A}-\mathcal{B})\xi_j(\mathcal{A}+\mathcal{B}))_{1\leqslant i,j\leqslant 2^g} = (2B_{ij}(\mathcal{A},\mathcal{B}))_{1\leqslant i,j\leqslant 2^g} \quad .$$

Si, de plus, les coordonnées sont normalisées de telle sorte que $\xi_1(\mathcal{A}) = \xi_1(\mathcal{B}) = \xi_1(\mathcal{A}\pm\mathcal{B}) = 1$, alors les coefficients des B_{ij} sont dans $\mathbb{Z}[(f_i)_i]$ où les f_i sont les coefficients de la courbe $\mathcal{C}$.

Nous allons maintenant expliquer comment calculer explicitement ces traces de la loi de groupe sur la jacobienne.

2.1 Addition d'un élément d'ordre 2

Comme expliqué précédemment, l'addition d'un élément de 2-torsion est bien définie sur la variété de Kummer. De plus, cette application est linéaire dans $\mathbb{P}^{2^g-1}(\mathbf{Q})$. Pour calculer la matrice correspondante, nous utilisons la version géométrique de la loi de groupe sur la jacobienne. Par exemple dans le cas du genre 2, nous voulons sommer un élément quelconque représenté par deux points de la courbe, $[x_1, y_1]$ et $[x_2, y_2]$ et un élément d'ordre 2 représenté par deux points de Weierstrass de la courbe, $[\theta_1, 0]$ et $[\theta_2, 0]$. Nous construisons pour cela la cubique passant par ces quatres points. L'intersection résiduelle de cette cubique et de la courbe $\mathcal{C}$ permet de définir la somme cherchée, sous la forme d'un polynôme de degré 2 dont les racines sont les abscisses des deux points de la courbe représentants cette somme. La forme spécifique des coordonnées dans la variété de Kummer permet alors d'exprimer les coordonnées dans la variété de Kummer de la somme en fonction des coefficients du polynôme de degré 2 obtenu (et non en fonction de ces racines ce qui obligerait à changer de corps de base).

Un travail analogue permet d'obtenir également la matrice de l'addition d'un élément d'ordre 2 pour les courbes de genre 3 définies par un polynôme de degré 7. Le programme maple correspondant ainsi que la matrice dans le cas général sont disponibles sur ma page web ainsi que sur mon site ftp [Duq].

2.2 Les formes biquadratiques

L'objet de ce paragraphe est de donner l'idée du calcul explicite des formes biquadratiques

$$(\xi_i(\mathcal{A}+\mathcal{B})\xi_j(\mathcal{A}-\mathcal{B}) + \xi_i(\mathcal{A}-\mathcal{B})\xi_j(\mathcal{A}+\mathcal{B}))_{1\leqslant i,j\leqslant 2^g} \quad = \quad (2B_{ij}(\mathcal{A},\mathcal{B}))_{1\leqslant i,j\leqslant 2^g} \quad (3)$$

qui interviennent dans le théorème 1.
La façon dont Flynn traite ce problème en genre 2 est quelque peu surprenante mais très ingénieuse. En effet, il part de l'idée que ces formules sont connues lorsque $\mathcal{B}$ est un élément d'ordre 2 grâce aux calculs du paragraphe précédent et en déduit la formule générale en regardant formellement les coordonnées de cet élément d'ordre 2.

Pour être plus précis, si $\mathcal{B} = \{[\theta_1, 0], [\theta_2, 0]\}$ est un élément d'ordre 2 général et si $\mathbf{W}$ désigne la matrice de l'addition par $\mathcal{B}$ obtenue au paragraphe 2.1, les formes

biquadratiques (3) sont projectivement égales à $2\xi_i\left(\mathbf{W}(\mathcal{A})\right)\xi_j\left(\mathbf{W}(\mathcal{A})\right)$. Ceci est une forme quadratique en $(\xi_1(\mathcal{A}),\xi_2(\mathcal{A}),\xi_3(\mathcal{A}),\xi_4(\mathcal{A}))$ et en regardant les coefficients de chaque produit $\xi_l(\mathcal{A})\xi_m(\mathcal{A})$ comme une forme quadratique en $(\xi_1(\mathcal{B}),\ldots,\xi_4(\mathcal{B}))$, nous pouvons en déduire facilement les coefficients des B_{ij}.
Il est ainsi possible de déduire les formes biquadratiques B_{ij} pour un $\mathcal{B}$ quelconque à partir du cas particulier des éléments d'ordre 2.

Dans le cas du genre 2, le succès de cette méthode est assuré par le fait que les 10 produits $\xi_i(\mathcal{B})\xi_j(\mathcal{B})$ sont linéairement indépendants sur $\mathbb{Q}(f_0,\ldots,f_6)$ pour un élément d'ordre 2 arbitraire.

Cette condition n'est plus vérifiée dans le cas des courbes hyperelliptiques de genre 3 du fait de l'équation (2) et cette méthode nécessite donc des modifications. Ce problème peut être contourné, entre autres, en remarquant que l'équation (2) n'est pas valable seulement pour les éléments de torsion mais pour tous les éléments de la jacobienne.

On peut ensuite aisément déduire de ces formes biquadratiques l'expression de la loi de duplication sur la variété de Kummer en remplaçant simplement $\mathcal{B}$ par $\mathcal{A}$ dans les formes biquadratiques (3). Les expressions explicites de ces formes biquadratiques ainsi que les formules de la loi de duplication en genre 2 peuvent être trouvées soit dans l'article originel de Flynn, [Fly 93], soit sur son site ftp (ftp.liv.ac.uk) dans le répertoire ∽ftp/pub/genus2/kummer. En ce qui concerne les courbes hyperelliptiques de genre 3 les programmes (maple et magma) ainsi que les formules sont disponibles sur [Duq].

Nous allons maintenant voir quelques unes des applications de ces traces de la loi de groupe sur la variété de Kummer.

3 Théorie des hauteurs et descente infinie

Ces traces de la loi de groupe, et plus particulièrement les formes biquadratiques (3), permettent de définir une fonction hauteur sur la jacobienne. Dans le cas des courbes elliptiques, on choisit classiquement la hauteur standard dans $\mathbb{P}^1(\mathbb{Q})$ de l'abscisse du point [Sil 90]. Il apparait donc naturel, dans le cas des courbes de genre supérieur, de prendre la hauteur standard H dans $\mathbb{P}^{2^g-1}(\mathbb{Q})$ des coordonnées de la variété de Kummer ; nous noterons $H_\mathcal{K}$ cette fonction. Le théorème 1 permet alors de démontrer que $H_\mathcal{K}$ est une fonction hauteur ([Fly 95] en genre 2, [Duq 01] en genre 3) :

Théorème 2 *La fonction*

$$\begin{array}{rccl} H_\mathcal{K} & : & \mathcal{J}(\mathbb{Q}) & \longrightarrow & \mathbb{Z}^+ \\ & & \mathcal{A} & \longmapsto & H\left(\xi_1(\mathcal{A}),\ldots,\xi_{2^g}(\mathcal{A})\right) \end{array}$$

vérifie les propriétés suivantes

- *Pour toute constante C, $\{\mathcal{A}\in\mathcal{J}(\mathbb{Q}), H_\mathcal{K}(\mathcal{A})\leqslant C\}$ est fini.*
- *Il existe une constante C_1 telle que pour tout $\mathcal{A}$ et $\mathcal{B}$ dans $\mathcal{J}(\mathbb{Q})$,*
$$H_K(\mathcal{A}+\mathcal{B})H_\mathcal{K}(\mathcal{A}-\mathcal{B})\leqslant C_1 H_K(\mathcal{A})^2 H_K(\mathcal{B})^2 \ .$$
- *Il existe une constante C_2 telle que pour tout $\mathcal{A}$ dans$\mathcal{J}(\mathbb{Q})$,*
$$H_\mathcal{K}(2\mathcal{A})\geqslant\frac{1}{C_2}H_\mathcal{K}(\mathcal{A})^4 \ .$$

Remarque : Outre l'application qui va suivre, ce théorème, via la troisième propriété, permet d'obtenir une procédure efficace pour calculer le groupe de torsion de $\mathcal{J}(\mathbb{Q})$ grâce à la proposition suivante :

Proposition 1 *Si $H_{\mathcal{K}}$ est une fonction hauteur sur $\mathcal{J}(\mathbb{Q})$, alors, avec les notations du théorème 2, tout élément $\mathcal{A}$ de $\mathcal{J}(\mathbb{Q})$ d'ordre fini satisfait $H_{\mathcal{K}}(\mathcal{A}) \leqslant C_2^{\frac{1}{3}}$.*

Une telle théorie des hauteurs est très importante car elle permet d'obtenir une méthode de descente infinie pour les courbes de genre 2 proposée par Flynn et Smart [Fly 95], [Fly-Sma 97]. La descente infinie est la technique qui consiste à déduire de $\mathcal{J}(\mathbb{Q})/2\mathcal{J}(\mathbb{Q})$ (obtenu par une 2-descente) une base pour le groupe de Mordell-Weil de la jacobienne. Le principe de base est le même que pour les courbes elliptiques [Cre 97], [Sil 86], [Sik 95].
Il consiste à déterminer une borne pour la hauteur telle que tous les éléments ayant une hauteur inférieure à cette borne engendrent le groupe de Mordell-Weil. La borne en question est obtenue à partir des deux constantes caractéristiques de la hauteur : C_1 et C_2.

Cependant la constante C_2 obtenue à partir des formes biquadratiques du théorème 1 est bien trop élevée dans le cas des courbes de genre 2 pour espérer opérer effectivemment une descente infinie. Pour pallier ce problème, Flynn [Fly 95] a développé une autre méthode, basée sur l'isogénie de Richelot, pour calculer cette constante C_2.
Le principe est de décomposer la multiplication par 2 sur la variété de Kummer en un produit d'application linéaires et quadratiques en utilisant la matrice de l'addition d'un élément d'ordre 2 obtenue au paragraphe 2.1. Plus précisement, Flynn exhibe trois matrices W_1, W_2 et W_3 telles que

$$[2] = W_1 \tau W_2 \tau W_3 \ ,$$

où $[2]$ désigne la multiplication par 2 sur la variété de Kummer et τ est l'application qui à $[\xi_1, \xi_2, \xi_3, \xi_4]$ associe $\left[\xi_1^2, \xi_2^2, \xi_3^2, \xi_4^2\right]$.
Il en déduit que la constante C_2 est donnée par la formule

$$C_2 \ = \ H(W_1^{-1}) H(W_2^{-1})^2 H(W_3^{-1})^4 \ .$$

Cette nouvelle constante C_2 permet alors d'effectuer effectivement des descentes infinies sur des courbes de genre 2 dont les coefficients ne sont pas trop grands.

Dans le cas des courbes hyperelliptiques de genre 3 définies par un polynôme de degré 7, le théorème 2, permet théoriquement de developper un algorithme de descente infinie analogue à celui du genre 2. Cependant, les constantes C_1 et C_2 sont encore plus inexploitables qu'en genre 2. Une amélioration de ces constantes s'avère donc nécessaire. Elle pourrait être obtenue, par exemple, via une décomposition de la multiplication par 2 comme en genre 2. Cela constitue des travaux en cours mais il faut bien voir que nous ne disposons plus de l'isogénie de Richelot comme en genre 2, ce qui complique considérablement les choses.

4 Généralisations

D'autre part, ce travail fait sur les courbes hyperelliptiques de genre 3 définies par un polynôme de degré 7 est probablement généralisable au degré 8. Stubbs

propose dans ce cas de nouvelles fonctions c'_i pour définir la variété de Kummer:

$$\begin{aligned}
c'_0 &= c_0 + f_8\left(2a_2a_1^2 - a_1^4 - a_2^2\right) \ , \\
c'_1 &= c_1 + f_8\left(4a_2a_1^3 - a_1^5 - 3a2^2a_1 - 2a_3a_1^2 + 2a_3a_2^3\right) \ , \\
c'_2 &= c_2 + f_8\left(a_2a_1^4 - 3a_2^2a_1^2 + a_2^3 + 2a_3a_2a_1 - a_3^2\right) \ , \\
c'_3 &= c_3 + f_8\left(a_2^2a_1^3 - a_3a_1^4 - 2a_2^3a_1 + 2a_3a_2a_1^2 + a_3a_2^2 - a_3^2a_1\right) \ .
\end{aligned}$$

De nouveaux problèmes se posent toutefois mais semblent surmontables. Ce ne sera par contre certainement pas le cas des quartiques planes lisses (toute courbe de genre 3 est soit une courbe hyperelliptique soit une quartique plane lisse). Enfin, ces méthodes sont théoriquement applicables aux courbes hyperelliptiques de genre 4 mais les calculs deviendront probablement infaisables avec les moyens actuels.
Remarque : Ces travaux font encore l'objet de recherches et un article comprenant plus de détails est en cours de préparation.

Références

[Cre 97] J. E. Cremona, *Algorithms For Modular Elliptic Curves*, Cambridge University Press (1997), Second Edition.

[Duq] S. Duquesne, *Page web*, `http://www.math.u-bordeaux.fr/~duquesne` et *Site ftp*, `ftp://megrez.math.u-bordeaux.fr/pub/duquesne`.

[Duq 01] S. Duquesne, *Calculs effectifs des points entiers et rationnels sur les courbes*, Thèse de doctorat, Université Bordeaux I (2001).

[Fly 93] E. V. Flynn, *The group law on the Jacobian of a curve of genus* 2, J. reine angew. Math., vol. 439 (1993), pp. 45-69.

[Fly 95] E. V. Flynn, *An explicit theory of heights*, Trans. Amer. Math. Soc., Vol. 347 (1995), pp. 3003-3015.

[Fly-Sma 97] E. V. Flynn, N. P. Smart, *Canonical height on the Jacobians of curves of genus 2 and the infinite descent*, Acta Artih., Vol. 79:4 (1997), pp. 333-352.

[Sik 95] S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain Journal of Mathematics, Vol. 25:4 (1995), pp. 1501-1538.

[Sil 86] J. H. Silverman, *The arithmetic of Elliptic Curves*, Graduate Texts in Math., Vol. 106, Springer-Verlag (1986).

[Sil 90] J. H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp., Vol. 55:192 (1990), 723-743.

[Sto 01] M. Stoll, it Implementing 2-descent for Jacobians of hyperelliptic curves, Acta Arith. 98:3 (2001), pp. 245–277.

[Stu 00] A. Stubbs, *Hyperelliptic Curves*, Thesis, University of Liverpool (2000).

Sylvain Duquesne, Laboratoire A2X, Université Bordeaux I, 351 Cours de la Libération, 33405 Talence Cedex, France (duquesne@math.u-bordeaux.fr).