N$^{\text{O}}$ d'ordre : 2447.

THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

PAR **Sylvain Duquesne**

POUR OBTENIR LE GRADE DE

DOCTEUR

SPÉCIALITÉ : MATHÉMATIQUES PURES

Calculs Effectifs des Points Entiers et Rationnels sur les Courbes

---

Soutenue le 7 décembre 2001

Après avis de :

MM	J. Cremona	Professeur	University of Nottingham	Rapporteurs
	E. V. Flynn	Professeur	University of Liverpool	
	J. F. Mestre	Professeur	Université de Paris 7	

Devant la commission d'examen formée de :

MM	F. Morain	Professeur	École Polytechnique	Président
	M. Matignon	Professeur	Université Bordeaux I	Rapporteur
	Y. Bilu	Professeur	Université Bordeaux I	Examinateurs
	H. Cohen	Professeur	Université Bordeaux I	
	E. V. Flynn	Professeur	University of Liverpool	
	J. F. Mestre	Professeur	Université de Paris 7	

– 2001 –

Je voudrais tout d'abord remercier mon directeur de thèse Henri Cohen. Il a su diriger mes recherches tout en me laissant une grande liberté de manoeuvre et en me procurant tous les moyens nécessaires à leurs réalisations.
Je tiens également à exprimer toute ma reconnaissance à Victor Flynn dont les travaux ont été à l'origine d'une grande partie de cette thèse. Il a su me faire profiter de ses connaissances et de son expérience entre autres à l'occasion d'un long séjour très instructif à l'université de Liverpool. Il a également bien voulu se charger du travail de rapporteur qu'il a accompli scrupuleusement malgré l'obstacle de la langue.

Les Professeurs Jean-François Mestre et John Cremona ont, eux aussi, accepté de rapporter cette thèse. Je les remercie vivement pour le temps qu'ils y ont consacré et l'intérêt qu'ils ont porté à ce travail. Je suis par ailleurs honoré que Victor Flynn, Jean-François Mestre et François Morain se soient déplacés pour faire partie de mon jury.

Je suis également très sensible à la présence, dans ce jury, des professeurs Yuri Bilu et Michel Matignon. Je voudrais les remercier pour les discussions que j'ai pu avoir avec eux mais aussi pour leur disponibilité, leurs commentaires et leur gentillesse.

Mes remerciements vont bien sûr plus généralement à tous les chercheurs qu'il n'est pas possible de citer ici et qui, de près ou de loin, ont contribué à l'élaboration de mes travaux. Je tiens par la même occasion à exprimer ma reconnaissance aux organisateurs des divers congrès auxquels j'ai été conviés.

J'en profite pour remercier Michel Olivier, le directeur de l'A2X, ainsi que Véronique et Maud, les organisateurs des différents séminaires et plus généralement tous les membres de ce laboratoire où il règne une excellente ambiance de travail.

J'aimerais aussi remercier mes amis doctorants, Sami, Bill, Stéphane, Denis, Thomas, Vincent, Marc, ... acteurs de la vie de tous les jours et tout particulièrement Christophe pour ses corrections, ses remarques, ses conseils et tant d'autres choses que je ne pourrais citer ici.

Je tiens également à remercier ma famille et mes amis pour l'aide et les encouragements qu'ils ont su m'apporter et en particulier Nathalie, ma femme, pour son aide, son soutien et sa patience dans les périodes les plus difficiles.

Je suis particulièrement reconnaissant envers tous ceux qui ont participé à cette thèse et à l'organisation de la soutenance.

Enfin, je terminerais en remerciant toutes les personnes, étrangères à la noosphère mathématique, et qui, après m'avoir demandé ce que je faisais, ont eu la patience d'écouter jusqu'au bout mes explications que j'ai essayé de rendre les plus pédagogiques possible.

Table des matières

Introduction

Les équations diophantiennes, c'est à dire les équations polynomiales dont on recherche les solutions entières ou rationnelles, ont fasciné les hommes depuis de nombreux siècles. Diophante (325-409) est à l'origine de leur nom pour y avoir consacré *Arithmetica* constitué originellement de treize livres qui n'ont malheureusement pas tous survécu au moyen âge. Diophante pose dans ces livres de nombreux problèmes se ramenant à la résolution de telles équations qui ont servi de base de travail à de nombreux mathématiciens de la renaissance à nos jours. Pour l'anecdote, son travail a été poursuivi par Hypatia, la seule femme mathématicienne connue de l'antiquité. Cependant, leur origine remonte beaucoup plus loin dans l'histoire de l'humanité. Une tablette babylonienne datant d'entre 1600 et 1900 avant Jésus Christ énumère en effet 15 solutions de ce qui est sans doute l'un des premiers exemples d'équation diophantienne :

$$x^2 + y^2 = z^2 \text{ avec } x, y, z \in \mathbb{Z} \ .$$

Cette équation revient à trouver les triangles rectangles dont les cotés sont entiers. Cela ne peut manquer d'évoquer en nous tant de souvenirs de jeunes collégiens : théorème de Pythagore et triplets pythagoriciens...
De nombreux mathématiciens ont donc, de tout temps, cherché à déterminer la structure des solutions de diverses équations diophantiennes : y-a-t'il un nombre fini ou infini de solutions ? Peut-on donner une procédure effective pour les déterminer toutes ? Ces solutions forment-elles un groupe d'une quelconque sorte ? Comment sont réparties les solutions parmi les solutions réelles ? Et bien d'autres questions encore. C'est ainsi que les équations diophantiennes ont été l'un des moteurs de développement de la théorie des nombres. L'exemple le plus frappant en est bien sûr l'équation de Fermat :

$$x^p + y^p = z^p \text{ avec } x, y, z \in \mathbb{Z} \text{ et } xyz \neq 0 \ ,$$

pour p supérieur à 3. C'est une généralisation de l'équation de Pythagore précédemment décrite. Le dernier théorème de Fermat, qui consiste à démontrer que cette équation n'a pas de solutions entières non triviales, a été l'un des problèmes centraux en théorie des nombres au cours des trois derniers siècles.

Le cadre approprié pour étudier les équations diophantiennes est celui de la géométrie algébrique. Les équations diophantiennes peuvent, dans ce cadre, être interprétées comme des questions sur l'existence de points sur des variétés algébriques. Dans cette thèse, nous

nous contenterons d'étudier le cas des courbes. Les géomètres classifient les courbes à l'aide d'un entier positif, le genre. La théorie des courbes de genre 0 est maintenant bien connue. Pour les courbes de genre 1, il existe désormais de nombreux outils et d'importantes conjectures commencent à succomber à des recherches intensives. Par contre, en ce qui concerne les courbes de genre supérieur, les connaissances, en particulier au niveau algorithmique, sont encore relativement succinctes.
Nous allons dans un premier temps rappeler les outils mathématiques qui nous serviront dans les chapitres suivants.

Arithmétique des courbes algébriques

Préliminaires géométriques

Soit $\mathbf{k}$ un corps que l'on supposera de caractéristique 0 et $\overline{\mathbf{k}}$ une clôture algébrique de $\mathbf{k}$. Soit $\mathcal{C}$ une courbe projective plane de genre g supérieur à 1 définie sur $\overline{\mathbf{k}}$. Une telle courbe sera, dans les cas qui nous concernent, la normalisation projective d'une courbe affine donnée par une équation $\mathcal{C}(x,y) = 0$.

Points rationnels

La recherche de tous les points rationnels sur de telles courbes, c'est à dire la résolution des équations diophantiennes correspondantes est l'un des principaux problèmes de la géométrie arithmétique. L'arithmétique des courbes de genre 0 est bien résolue puisque l'ensemble des solutions est soit vide soit isomorphe à $\mathbb{P}^1(\overline{\mathbf{k}})$.
En ce qui concerne les courbes de genre 1, elles sont appelées courbes elliptiques et sont données par une équation du type

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 \quad .$$

On sait que, lorsque $\mathbf{k}$ est un corps de nombres, l'ensemble des points rationnels forme un groupe abélien libre de type fini, et de nombreux progrès ont été faits ces dernières années dans le calcul explicite de ce groupe [Cre 99], [Sim]. Le deuxième problème diophantien que l'on peut se poser concernant les courbes elliptiques est le calcul de leurs points entiers dans le cas où le corps de base est $\mathbb{Q}$. Un théorème de Siegel montre en effet qu'ils sont en nombre fini. Il parait donc naturel de rechercher une méthode permettant de les calculer explicitement. De nombreuses méthodes ont été développées dans ce but, nous exposerons au premier chapitre la plus répandue actuellement et nous nous en servirons pour calculer des points entiers sur une famille de courbes elliptiques.
Pour les courbes de genre plus grand, les résultats sont par contre beaucoup moins riches. Faltings [Fal 83] a démontré en 1983 qu'une courbe de genre supérieur ou égal à 2 sur un corps de nombres $\mathbf{k}$ possède un nombre fini de points rationnels. Malheureusement la preuve de Faltings n'est pas explicite et ne permet même pas de borner le nombre de points rationnels. L'un des plus importants problèmes actuels concernant les courbes de

genre supérieur à 2 est le calcul explicite de ces points rationnels. Le premier résultat revient à Chabauty [Cha 41] qui, dès 1941, a démontré ce résultat de manière explicitable dans le cas où le rang de la jacobienne est strictement inférieur au genre de la courbe. Nous citerons ensuite Coleman [Col 85] qui a obtenu une borne explicite pour le nombre de points dans les conditions du théorème de Chabauty. Enfin Flynn [Fly 97] a décrit une méthode permettant de borner effectivement le nombre de points rationnels sur une courbe de genre 2. Le cas des courbes de genre 2 constitue en effet le premier exemple non trivial d'application du théorème de Chabauty. L'avantage de la méthode de Flynn est qu'elle donne, dans la plupart des cas, une borne égale au nombre de points rationnels. Elle permet alors de calculer tous les points rationnels d'une courbe donnée lorsque le rang de sa jacobienne est inférieur à 1.
Reste maintenant à savoir calculer (ou même borner) les points rationnels dans les cas qui ne satisfont pas aux hypothèses du théorème de Chabauty. Plusieurs méthodes ont été développées pour des courbes particulières par différents mathématiciens ([Dem 68], [Bru 99], [Fly 01], [Wet 97]...). La plupart de ces méthodes utilisent des revêtements de la courbe par d'autres courbes sur lesquels on dispose d'outils supplémentaires. C'est en particulier le cas de la méthode de Chabauty elliptique développée par Flynn et Wheterell [Fly-Wet 99] que nous exposerons dans le second chapitre.
Nous allons maintenant donner les définitions de base ainsi que les objets que nous allons manipuler dans la suite de cette thèse.

Diviseurs

Un diviseur D est une somme finie formelle de points sur la courbe $\mathcal{C}(\overline{\mathbf{k}})$. Le groupe des diviseurs $\mathrm{Div}(\mathcal{C})$ est défini comme le groupe abélien libre engendré par les points de $\mathcal{C}$ définis sur $\overline{\mathbf{k}}$. Autrement dit, un diviseur D de $\mathrm{Div}(\mathcal{C})$ s'écrit

$$D = \sum_{P \in \mathcal{C}(\overline{\mathbf{k}})} m_P P \ .$$

On dit alors que le point P de $\mathcal{C}$ a la multiplicité m_P pour le diviseur D. Cette multiplicité est un nombre entier relatif et est nulle pour tous les points sauf pour un nombre fini. Pour un diviseur D donné, la somme de ses multiplicités sur tous les points de la courbe est donc finie. Cette somme définit le degré du diviseur D :

$$\deg(D) = \sum_{P \in \mathcal{C}} m_P \ .$$

L'ensemble des diviseurs de degré 0 forme un sous-groupe de $\mathrm{Div}(\mathcal{C})$ et est noté $\mathrm{Div}^0(\mathcal{C})$. On définit d'autre part le corps des fonctions de $\mathcal{C}$ et on note $\overline{\mathbf{k}}(\mathcal{C})$ l'extension algébrique de $\overline{\mathbf{k}}(x)$ donnée par

$$\overline{\mathbf{k}}(\mathcal{C}) = \overline{\mathbf{k}}(x)[y]/\left(\mathcal{C}(x,y)\right) \ .$$

À une fonction f appartenant au corps des fonctions de $\mathcal{C}$, on peut associer un diviseur, que nous noterons $\mathrm{div}(f)$, en définissant sa multiplicité en un point P par l'ordre d'annulation de la fonction f au point P. De tels diviseurs, provenant d'une fonction, sont

appelés des diviseurs principaux. Les diviseurs principaux sont de degré 0 et forment un sous-groupe de $\mathrm{Div}^0(\mathcal{C})$.
L'arithmétique des corps de fonctions présente de grandes similitudes avec celle des corps de nombres. Le groupe des diviseurs de degré 0 est en effet analogue au groupe des idéaux fractionnaires d'un corps de nombres. Il est donc naturel de considérer les classes d'équivalence des diviseurs de degré 0 modulo les diviseurs principaux.
Deux diviseurs différant d'un diviseur principal sont dit linéairement équivalents ou appartenant à la même classe de diviseurs. Le groupe des classes de diviseurs modulo les diviseurs principaux ainsi défini est appelé groupe de Picard de la courbe $\mathcal{C}$ et est noté $\mathrm{Pic}(\mathcal{C})$. On définit de même $\mathrm{Pic}^0(\mathcal{C})$ le groupe des classes de diviseurs de degré 0 modulo les diviseurs principaux.
Cantor [Can 87] a développé un algorithme permettant d'additionner deux points de ce groupe dans le cas des courbes hyperelliptiques en se servant de l'analogie avec les corps de nombres déjà évoquée. Cette méthode est toujours utilisée pour additionner des points, y compris lorsque le corps $\mathbf{k}$ est un corps fini, en cryptographie par exemple. Cependant, nous n'allons pas nous en servir dans la suite et nous ne la détaillerons donc pas.

Dans le cas des courbes elliptiques, le groupe $Pic^0(\mathcal{C})$ est isomorphe à la courbe $\mathcal{C}$ elle-même. Les intégrales elliptiques permettent dans ce cas de construire un isomorphisme de la courbe $\mathcal{C}(\mathbb{C})$ vers un tore $\mathbb{C}/\Lambda$ où Λ est un réseau de $\mathbb{C}$ (on pourra trouver plus de détails dans le premier chapitre à ce sujet). L'application d'Abel-Jacobi est une généralisation de cet isomorphisme en genre supérieur à 1. Elle permet d'identifier le groupe $\mathrm{Pic}^0(\mathcal{C})$ au tore $\mathbb{C}^g/\Lambda$ où Λ est un réseau de $\mathbb{C}^g$. Cet isomorphisme munit donc le groupe $\mathrm{Pic}^0(\mathcal{C})$ d'une structure de variété algébrique. Le groupe $\mathrm{Pic}^0(\mathcal{C})$ est alors appelé jacobienne de la courbe $\mathcal{C}$ que nous noterons $J(\mathcal{C})$. D'autre part, l'application d'Abel-Jacobi commute avec l'action du groupe de Galois absolu $G = \mathrm{Gal}\left(\overline{\mathbf{k}}/\mathbf{k}\right)$. Ainsi G agit sur les objets précédemment introduits. On dit qu'un diviseur est défini sur $\mathbf{k}$ ou rationnel s'il est fixé par l'action de Galois. La classe d'un tel diviseur sera alors appelée un point rationnel sur la jacobienne et on notera $J_{\mathbf{k}}(\mathcal{C})$ l'ensemble de ces points.

Remarque : Il est important de noter qu'un diviseur défini sur $\mathbf{k}$ n'est pas nécessairement la somme de points de la courbe définis sur $\mathbf{k}$.
Par exemple si on considère la courbe $\mathcal{C}$ définie sur $\mathbb{Q}$ par l'équation suivante.

$$\mathcal{C} : y^2 = (x^2+1)(x^2+3)(x^2+7) \ .$$

Le point $[i, 0]$ n'est pas un point rationnel alors que le diviseur $[i, 0] + [-i, 0]$ est défini sur $\mathbb{Q}$ car invariant par l'action de $Gal\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$.

Courbes hyperelliptiques

Nous allons maintenant restreindre notre étude au cas des courbes hyperelliptiques définies sur un corps de nombres, c'est à dire aux courbes de la forme

$$Y^2 = F(X)$$

où F est un polynôme de degré $2g+1$ ou $2g+2$ (g désigne le genre de la courbe) à coefficients dans $\mathbf{k}$ et de discriminant non nul. Notons que, dans le cas le plus général, le degré de F doit être égal à $2g+2$. Cependant, lorsque F possède une racine dans $\mathbf{k}$, on peut toujours se ramener au cas où F est de degré $2g+1$. On supposera de plus que pour les courbes de genre impair, F est de degré impair également. D'autre part, remarquons que dans le cas où le degré est impair, la courbe possède un point à l'infini noté ∞ et que lorsque le degré est pair, elle possède deux points à l'infini notés ∞^+ et ∞^-. Ces points correspondent aux branches infinies de l'équation $Y^2 = F(X)$.

Remarque : La forme sous laquelle nous écrivons les courbes hyperelliptiques est bien sûr analogue à la forme de Weierstrass courte pour les courbes elliptiques.

La restriction que nous opérons ici n'en est véritablement une que lorsque le genre de la courbe est supérieur ou égal à 3. En effet, en utilisant le théorème de Riemann-Roch, on démontre, comme dans le cas des courbes elliptiques, que toute courbe de genre 2 est hyperelliptique et peut donc s'écrire sous la forme

$$Y^2 = f_6X^6 + \ldots\cdots + f_1X + f_0 \ . \tag{1}$$

Ce phénomène n'est cependant plus valable en genre supérieur.
Nous allons maintenant étudier plus précisément la jacobienne d'une telle courbe. Les courbes hyperelliptiques sont munies d'une involution canonique : l'involution hyperelliptique, obtenue en changeant Y en $-Y$ et en laissant X invariant lorsque $\mathcal{C}$ est écrite sous la forme (1). Ainsi, si le point $[x, y]$ est un point de la courbe $\mathcal{C}$, alors $[x, -y]$ est également un point de $\mathcal{C}$.
Les points $[x, y]$ et $[x, -y]$ sont les seuls zéros de la fonction $X - x$. Cette fonction a soit ∞ comme pôle double (lorsque le degré est impair), soit ∞^+ et ∞^- comme pôles simples (lorsque le degré est pair). Le diviseur $[x, y] + [x, -y]$ est donc un diviseur principal. Dans le groupe de Picard, un tel élément est donc dans la classe triviale que nous noterons $\mathcal{O}$ dans toute la suite. On en déduit, en utilisant le théorème de Riemann-Roch, que toute classe de diviseurs possède un représentant de la forme

$$D = \sum_{i=1}^{g} P_i - g\infty \ .$$

lorsque le degré de F est impair, ou

$$D = \sum_{i=1}^{g} P_i - \frac{g}{2}\infty^+ - \frac{g}{2}\infty^- \ ,$$

lorsque le degré de F est pair (et dans ce cas, on a supposé le genre pair).
Pour plus de clarté on notera $\{P_1, \ldots, P_g\}$ un tel élement. L'élément neutre pour la loi de groupe de la jacobienne est le point à l'infini. Dans le cas des courbes de genre 2, il sera

par exemple représenté par:

$$\begin{aligned} \mathcal{O} &= \{[x,y],[x,-y]\} \ , \\ &= \{\infty^+,\infty^-\} \text{ (si le degré est pair)} \ , \end{aligned}$$

et pour les courbes de genre 3, il peut entre autres être représenté par :

$$\begin{aligned} \mathcal{O} &= \{[x,y],[x,-y],\infty\} \ , \\ &= \{\infty,\infty,\infty\} \ , \end{aligned}$$

Comme nous l'avons déjà expliqué, un tel g-uplet de points est défini sur $\mathbf{k}$ s'il est invariant par le groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbf{k}}/\mathbf{k})$. Par exemple, dans le cas du genre 2, un élément de la jacobienne est défini sur $\mathbf{k}$ si les deux points de la représentation précédente sont conjugués sur une extension quadratique de $\mathbf{k}$.
Nous allons maintenant définir la loi de groupe sur la Jacobienne, du moins du point de vue géométrique.

Loi de groupe sur la jacobienne

Rappelons tout d'abord rapidement le cas des courbes elliptiques. Nous avons déjà vu que, dans ce cas, la jacobienne était isomorphe à la courbe elle-même. On pourra donc représenter un diviseur par un point de la courbe. Soit D une droite du plan définie par une équation $Y = aX + b$. Une telle droite possède trois points d'intersection P, Q et R avec la courbe elliptique. Le diviseur de la fonction $y - ax - b$ est alors $P + Q + R - 3\infty$. Ainsi, si trois diviseurs correspondent à trois points de la courbe elliptique alignés, leur somme vaut trois fois le point à l'infini plus un diviseur principal, autrement dit leur somme vaut l'élément neutre dans la jacobienne. Cette remarque permet de définir la loi de groupe sur la jacobienne par $P+Q = -R$ si P, Q et R sont trois points alignés de la courbe elliptique.

Considérons maintenant le cas des courbes de genre 2. Nous allons utiliser le même type de méthode que pour les courbes elliptiques. Si $\mathcal{A}$ et $\mathcal{B}$ sont deux éléments de la jacobienne $J_{\mathbf{k}}(\mathcal{C})$ définis sur $\mathbf{k}$. Les diviseurs $\mathcal{A}$ et $\mathcal{B}$ sont alors chacun représentés par 2 points de la courbe. Il existe une unique cubique $M(X)$ dans $\mathbf{k}[X]$ telle que $Y = M(X)$ passe par ces 4 points. L'intersection affine de cette cubique et de la courbe $Y^2 = F(X)$ est alors constituée de 6 points dont les 4 initiaux. Les deux points restants permettent de définir un troisième diviseur de la jacobienne défini sur $\mathbf{k}$, tel que $\mathcal{A} + \mathcal{B} + \mathcal{C} = \mathcal{O}$. En effet, les points de la courbe qui représentent $\mathcal{A}$, $\mathcal{B}$ et $\mathcal{C}$ sont les zéros de la fonction $Y - M(X)$ de telle sorte que $\mathcal{A} + \mathcal{B} + \mathcal{C}$ est un diviseur principal et est donc trivial dans la jacobienne. La somme des deux diviseurs $\mathcal{A}$ et $\mathcal{B}$ est donc le diviseur $-\mathcal{C}$, c'est à dire $\mathcal{C}$ à qui on a appliqué l'involution hyperelliptique.

En ce qui concerne les cas de genre supérieur, la situation se complique un peu puisque l'on ne considère plus une fonction de la forme $Y = m(X)$. Il faut chercher deux polynômes p et q de $\mathbf{k}[X]$ tels que $Yp(X) = q(X)$ passe par les $2g$ points définissant $\mathcal{A}$ et $\mathcal{B}$.

Il n'est plus possible de prendre $p=1$ car l'intersection de $Yp(X)=q(X)$ avec $\mathcal{C}$ doit donner $3g$ points.
En genre 3 par exemple, un diviseur de la jacobienne est défini par 3 points et il existe un unique polynôme q de $\mathbf{k}[X]$ de degré 5 tel que $Y=q(X)$ passe par les 6 points définissant $\mathcal{A}$ et $\mathcal{B}$. Cependant l'intersection avec $\mathcal{C}$ donne 10 points dont les 6 initiaux, c'est à dire un point de trop. Dans ce cas, il faudra trouver des constantes α et β et une quartique M dans $\mathbf{k}[X]$ tels que la courbe $Y(\alpha X+\beta)=M(X)$ passe par les 6 points de la courbe définissant $\mathcal{A}$ et $\mathcal{B}$. L'intersection avec la courbe $\mathbb{C}$ donne alors 3 nouveaux points qui permettent de définir la somme de $\mathcal{A}$ et de $\mathcal{B}$.

Maintenant que l'on connait la loi de groupe sur $J_{\mathbf{k}}(\mathcal{C})$, il est naturel de se demander quelle est la structure de ce groupe. Comme dans le cas des courbes elliptiques, le théorème de Mordell-Weil énonce que $J_{\mathbf{k}}(\mathcal{C})$ est un groupe abélien libre de type fini. Dans la suite, nous appellerons rang de la jacobienne le rang de ce groupe. Le calcul explicite de cette structure, dans le cadre des courbes hyperelliptiques est très proche du calcul du groupe de Mordell-Weil des courbes elliptiques [Sto 01], [Sch 95].
Pour les calculs explicites que j'ai eu besoin de faire au cours de cette thèse, je me suis servi du programme mwrank de Cremona pour les courbes elliptiques définies sur $\mathbb{Q}$, du programme de Simon [Sim] dans le cas des corps de nombres et des programmes écrits par Stoll [Sto 01] inclus dans les dernières versions de magma pour les courbes de genre supérieur à 2.

Nous connaissons maintenant les outils de base pour les courbes hyperelliptiques. Cependant, ces outils ne sont pas très manipulables dans la pratique. Nous allons donc introduire de nouveaux objets qui sont plus simples à manipuler, du moins du point de vue algorithmique.

La surface de Kummer

Flynn a introduit de nouveaux objets pour travailler sur les jacobiennes de courbes hyperelliptiques de genre 2 [Fly 93]. Il décrit en particulier un plongement de la jacobienne dans $\mathbb{P}^{15}$. Cependant, une telle représentation de la jacobienne est trop lourde à manipuler. C'est pourquoi il introduit la surface de Kummer que nous noterons $\mathcal{K}$. Si $\mathcal{X}=\{[x_1,y_1],[x_2,y_2]\}$ désigne une paire de points généraux d'une courbe hyperelliptique $\mathcal{C}$ de genre 2, la surface de Kummer est le lieu projectif dans $\mathbb{P}^3$ de 4 fonctions symétriques en (x_1,y_1), (x_2,y_2) données par :

$$\begin{aligned}
\xi_1 &= 1 \ , \\
\xi_2 &= x_1+x_2 \ , \\
\xi_3 &= x_1x_2 \ , \\
\xi_4 &= \frac{F_0(x_1,x_2)-2y_1y_2}{(x_1-x_2)^2} \ ,
\end{aligned}$$

avec

$F_0(x_1,x_2)=2f_0+f_1(x_1+x_2)+2f_2x_1x_2+f_3(x_1+x_2)x_1x_2+2f_4x_1^2x_2^2+f_5(x_1+x_2)x_1^2x_2^2+2f_6x_1^3x_2^3$.

Ce lieu projectif est donné par une quartique explicite en $(\xi_1,\xi_2,\xi_3,\xi_4)$. La surface de Kummer présente l'avantage qu'il y est très facile de représenter un diviseur de la jacobienne de la courbe $\mathcal{C}$. Cependant, il est important de remarquer que deux points ont la même image dans $\mathcal{K}$ s'ils sont opposés l'un de l'autre, c'est à dire quand ils sont reliés par l'involution hyperelliptique. Ainsi sur la surface de Kummer, il est impossible de distinguer le diviseur $\mathcal{A}$ du diviseur $-\mathcal{A}$. Il est donc malheureusement impossible d'additionner un diviseur $\mathcal{A}$ et un diviseur $\mathcal{B}$ car le résultat peut être soit $\pm(\mathcal{A}+\mathcal{B})$ soit $\pm(\mathcal{A}-\mathcal{B})$. En passant de la jacobienne à la surface de Kummer, on perd donc la structure de groupe. Cependant, il en subsiste des traces comme par exemple la multiplication par 2 ou l'addition d'un diviseur d'ordre 2 (puisqu'un tel diviseur est égal à son opposé).

Dans le cas des courbes de genre 3, Stubbs [Stu 00], un élève de Flynn a pu construire la surface de Kummer dans $\mathbb{P}^7$ pour une courbe hyperelliptique donnée par une équation de la forme

$$\mathcal{C} : Y^2 = f_7X^7 + \cdots + f_1X + f_0 \ .$$

Remarque : La surface de Kummer est bien sûr définissable pour les courbes elliptiques où elle consiste à restreindre l'étude des points rationnels sur la courbe à l'étude de leurs abscisses. Cette démarche est d'ailleurs souvent employée lorsque l'on travaille sur des courbes elliptiques pour simplifier les calculs. Nous y aurons par exemple recours dans le premier chapitre de cette thèse.

Cette surface de Kummer est l'outil de base qui permet à Flynn [Fly 97] d'élaborer une méthode explicite pour appliquer le théorème de Chabauty à une courbe de genre 2 quelconque dont le rang de la jacobienne est strictement inférieur à 2. Cette méthode permet de borner de façon fine le nombre de points rationnels d'une telle courbe et, dans la plupart des cas, on peut en connaître effectivement tous les points rationnels. Nous n'allons cependant pas rappeler cette méthode car cela demande de nombreuses définitions et notations et nécessite un exposé relativement long. D'autre part cela n'apporterait pas grand chose à cette thèse puisque nous exposons au second chapitre la méthode de Chabauty elliptique qui est fondée sur les mêmes idées mais a le mérite d'utiliser les outils plus connus des courbes elliptiques. On pourra cependant se reporter au livre de Cassels et Flynn [Cas-Fly 96] pour plus de détails sur la question. La surface de Kummer est également à la base de la théorie des hauteurs pour les courbes de genre 2 développée par Flynn [Fly 95] qui permet d'effectuer une descente infinie. Comme dans le cas des courbes elliptiques, cette descente infinie est nécessaire pour déterminer une base du groupe de Mordell-Weil $\mathcal{J}(\mathbf{k})$ une fois connu $\mathcal{J}(\mathbf{k})/2\mathcal{J}(\mathbf{k})$. Le but de la troisième partie de cette thèse est d'ébaucher, à la suite de Stubbs, de tels outils pour les courbes de genre 3. Nous nous attacherons en particulier à calculer, pour ces courbes, ce qui subsiste de la loi de groupe sur la surface de Kummer. Ce travail nous laisse espérer de futures généralisations aux courbes de genre 3 des nombreuses applications de la surface de Kummer.

Plan de la thèse

Dans le premier chapitre de cette thèse nous étudions les points entiers d'une famille de courbes elliptiques indéxées par l'entier m et données par l'équation

$$y^2 = x^3 + mx^2 - (m+3)x + 1 \ .$$

Nous calculons tous les points entiers de ces courbes pour les valeurs du paramètre m inférieures à 1000. À partir des observations faites sur les résultats, nous calculons exactement tous les points entiers de ces courbes lorsque le rang du groupe de Mordell-Weil vaut 1 quelque soit la valeur du paramètre m. Ce travail a fait l'objet d'une publication à Experimental Mathematics [Duq 01].

Le second chapitre traite quant à lui de la recherche des points rationnels sur des courbes pour lesquelles le théorème de Chabauty ne s'applique pas. Nous exposons entre autres la méthode de Chabauty elliptique et nous proposons une généralisation. Nous utilisons ensuite cette méthode pour calculer les points rationnels d'une courbe hyperelliptique de genre 4 dont le rang de la jacobienne vaut 4. Cette généralisation fait l'objet d'une publication à Manuscripta Mathematica [Duq 02].

Enfin le dernier chapitre traite de la généralisation des outils de la surface de Kummer aux courbes de genre 3. Il fait partie de mes travaux en cours et permet d'envisager des applications futures comme la descente infinie pour les courbes de genre 3 par exemple.

Chapitre I

Points Entiers sur les Courbes Elliptiques Associées aux "Simplest Cubic Fields"

I.1 Les "simplest cubic fields"

Soit m un entier positif tel que

$$\Delta = m^2 + 3m + 9$$

soit sans facteur carré.
Le corps cubique $\mathbf{K}_m$, défini par le polynôme irréductible sur $\mathbb{Q}$,

$$f(X) = X^3 + mX^2 - (m+3)X + 1$$

a été introduit par Shanks ([Sha 74]) et est appelé un "simplest cubic field".
Shanks a introduit cette classe de corps car les calculs sont particulièrement faciles à effectuer sur de tels corps, ce qui leur a valu leur nom. Ces corps ont été par la suite beaucoup étudiés car leur régulateur est explicite et petit. Ainsi leur nombre de classes a tendance à être particulièrement grand.
Dans ce premier chapitre nous allons nous intéresser aux courbes elliptiques définies sur $\mathbb{Q}$ par les équations :

$$E_m : Y^2 = X^3 + mX^2 - (m+3)X + 1 \ , \tag{I.1}$$

pour un entier m définissant un "simplest cubic field".
Cette famille de courbes elliptiques a été introduite par Washington [Was 87]. Ce dernier relie le rang de la courbe elliptique E_m sur $\mathbb{Q}$ et le 2-rang du groupe des classes de $\mathbf{K}_m$.
On peut ainsi espérer que le rang des courbes elliptiques de cette famille ne sera pas trop petit, du moins qu'il sera suffisamment grand pour que ces courbes contiennent des points entiers. C'est la raison pour laquelle nous nous intéresserons au calcul des points entiers

sur les courbes de cette famille qui semblent si bien s'y prêter.

Nous allons donc, dans un premier temps, exposer une méthode permettant de calculer les points entiers sur une courbe elliptique lorsque son groupe de Mordell-Weil est connu. Cette méthode due, entre autres, à Stroeker et Tzanakis [Str-Tza 94], Gebel Pethö et Zimmer [Geb-Pet-Zim 94], et Smart [Sma 94] nous a permis de calculer tous les points entiers sur les courbes elliptiques E_m pour les valeurs du paramètre m inférieures à 1000 et définissant un "simplest cubic field". Des tables de ces calculs figurent dans l'annexe A. À partir de ces tables nous avons émis plusieurs conjectures concernant bien sûr les points entiers de ces courbes mais aussi la structure du groupe de Mordell-Weil $E(\mathbb{Q})$. Nous avons finalement démontré ces conjectures dont la principale concerne le point $[0, 1]$ qui joue un rôle central dans ce travail. Les résultats les plus intéressants sont en effet :

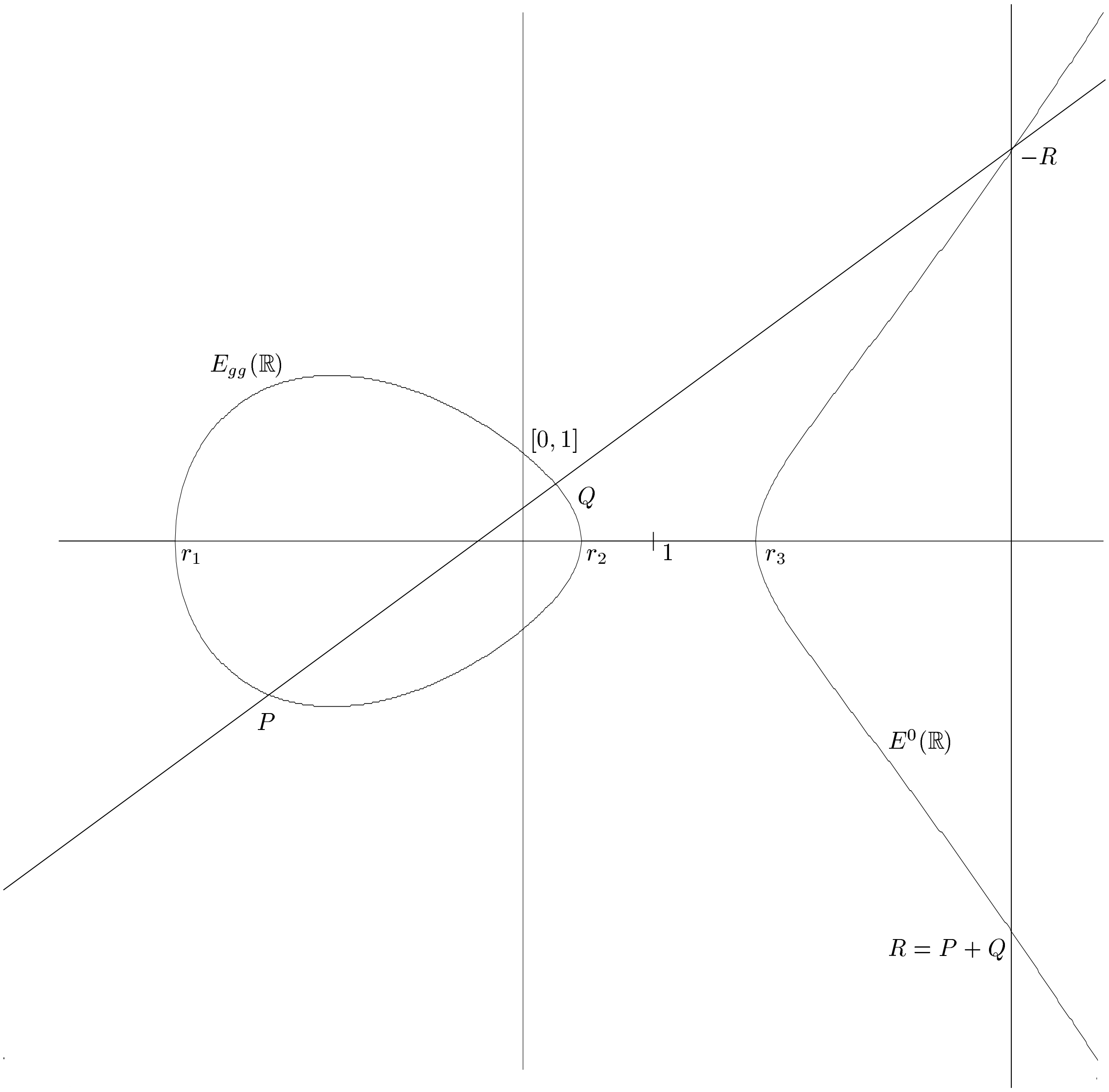
- d'une part la preuve que ce point est un générateur du groupe de Mordell Weil,
- d'autre part le calcul explicite de tous les multiples entiers de ce point $[0, 1]$.

Ces résultats sont bien sûr démontrés pour un entier m quelconque définissant un "simplest cubic field".

I.2 Courbes elliptiques associées aux "simplest cubic fields"

On considère donc les courbes elliptiques E_m définies par l'équation (I.1). Nous allons dans un premier temps donner quelques propriétés basiques de ces courbes ainsi que quelques définitions.

Rappelons que $\Delta = m^2+3m+9$ est sans facteur carré lorsque m définit un "simplest cubic field". L'invariant j de E_m est égal à 256Δ, son discriminant vaut $16\Delta^2$. De plus, si m est pair (respectivement congru à 1 et à 3 modulo 4) le conducteur vaut $16\Delta^2$ (respectivement $8\Delta^2$ et $4\Delta^2$). Le discriminant de E_m étant toujours positif, la courbe $E(\mathbb{R})$ possède deux composantes connexes. Notons $E^0(\mathbb{R})$ la composante connexe du point à l'infini de E et $E_{gg}(\mathbb{R})$ la partie compacte de $E(\mathbb{R})$ (E_{gg} faisant référence à la forme ovoïdale de cette partie). Le polynôme $f(X)$ possède quant à lui 3 racines réelles distinctes que nous noterons dans l'ordre croissant r_1, r_2 et r_3. Nous présentons maintenant un graphique de la courbe elliptique E_m où figurent les éléments que nous venons de définir. Y figure également la classique représentation de l'addition de 2 points P et Q sur cette courbe elliptique.



Nous allons maintenant énoncer un théorème dû à Washington.
Si $C\ell$ désigne le groupe des classes du "simplest cubic field" $\mathbf{K}_m$ et si $C\ell_2 = \{x \in C\ell, x^2 = 1\}$ désigne la 2-torsion du groupe des classes, on appelle 2-rang de $C\ell_2$ (et on note $rg_2(C\ell_2)$) la dimension de $C\ell_2$ en tant que $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. Le corps $\mathbf{K}_m$ étant un corps cubique cyclique, ce 2-rang doit être pair. Enfin, nous notons $Ш_2$ la 2-torsion du groupe de Tate-Shafarevich.

Théorème I (Washington [Was 87]) *Le rang de la courbe elliptique $rg(E_m(\mathbb{Q}))$ est au plus égal à $1 + rg_2(C\ell_2)$. En fait la suite suivante est exacte :*

$$1 \to E_m^0(\mathbb{Q})/2E_m(\mathbb{Q}) \to C\ell_2 \to Ш_2 \to 1.$$

Washington en déduit alors le corollaire suivant.

Corollaire I.2.1 *Si m est un entier positif tel que m^2+3m+9 soit sans facteur carré, alors le rang de la courbe elliptique E_m est impair, du moins en supposant que le groupe de Tate-Shafarevich soit fini.*

Comme le montre le théorème de Washington, chercher de telles courbes de grand rang revient à chercher des "simplest cubic fields" dont le groupe des classes possède un grand 2-rang. Ce problème est une généralisation au degré 3 du problème consistant à trouver des corps quadratiques ayant un 3-rang élevé qui a fait l'objet de nombreuses publications. De plus, espérant un grand nombre de classes pour le corps $\mathbf{K}_m$, si la 2-torsion du groupe de Tate-Shafarevich n'est pas trop grande par rapport au 2-rang du groupe de classes, nous pouvons aussi espérer obtenir des courbes de grand rang. Ainsi, en cherchant des entiers m pour lesquels la courbe $E_m(\mathbb{F}_p)$ a de nombreux points pour p premier petit, Mestre a montré que pour $m = 27038$, le rang de $E_m(\mathbb{Q})$ était supérieur ou égal à 7 [Mes 82]. Nous allons maintenant montrer que de telles courbes ont un sous-groupe de torsion trivial.

Proposition I.2.2 *Si m est un entier positif tel que m^2+3m+9 soit sans facteur carré, alors la courbe elliptique $E_m(\mathbb{Q})$ possède un groupe de torsion trivial.*

Preuve : Nous utilisons le fait que si la courbe E_m a bonne réduction en un nombre premier p, alors le groupe de torsion $E_m(\mathbb{Q})_{tors}$ s'injecte dans $E_m(\mathbb{F}_p)$. En appliquant ce résultat aux nombres premiers 3 et 5, il ne subsiste qu'une seule possibilité pour le groupe de torsion :
$E_m(\mathbb{Q})_{tors} = \mathbb{Z}/3\mathbb{Z}$ lorsque m est congru à 1 modulo 3 et 0 modulo 5.
Nous éliminons ce cas en montrant que l'équation donnée par $3P = 0$ n'a pas de solution dans $\mathbb{F}_5$ quand $m \equiv 0 \pmod 5$. □

Nous allons maintenant exposer une méthode de recherche de points entiers sur les courbes elliptiques. Cette méthode a été suggérée par Lang [Lan 78] (Chapitre VI, §8) et Zagier [Zag 87]. Elle a ensuite été développée simultanément par plusieurs chercheurs : Stroeker et Tzanakis [Str-Tza 94], Gebel, Pethö et Zimmer [Geb-Pet-Zim 94], et Smart [Sma 94]. Elle requiert cependant la connaissance d'une base pour le groupe de Mordell-Weil. Cette base peut être calculée en utilisant le programme `mwrank` de Cremona [Cre]. Cette méthode requiert également une borne inférieure explicite sur les formes linéaires de logarithmes elliptiques due à S. David [Dav 95]. Pour un point de vue plus général sur la résolution des équations diophantiennes et pour de plus amples détails sur cette méthode, on se référera au livre de Smart [Sma 98].

I.3 Préliminaires à la recherche de points entiers

I.3.1 Logarithmes elliptiques

Soit E une courbe elliptique donnée par son équation de Weierstrass

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \ ,$$

avec les a_i dans $\mathbb{Z}$. Notons de plus, comme à l'accoutumée, b_2 la quantité $a_1^2 + 4a_2$. Cette courbe est isomorphe sur $\mathbb{Q}$ à la courbe E' d'équation

$$Y^2 = 4X^3 - g_2X - g_3 \ ,$$

avec g_2 et g_3 dans $\mathbb{Z}$. On définit $\wp(z)$ la solution de l'équation différentielle

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 \ .$$

Cette fonction est appelée fonction de Weierstrass. Elle est doublement périodique et ses périodes, que nous noterons ω_1 et ω_2 forment une base d'un réseau Λ du plan complexe. De plus la théorie des fonctions elliptiques permet d'écrire ces périodes sous forme d'intégrales :

$$\begin{aligned} \omega_1 &= 2\int_{e_1}^{e_2} \frac{dX}{\sqrt{4X^3 - g_2X - g_3}} \ , \\ \omega_2 &= 2\int_{e_2}^{e_3} \frac{dX}{\sqrt{4X^3 - g_2X - g_3}} \ , \end{aligned}$$

où e_1, e_2 et e_3 désignent les racines du polynôme $4X^3 - g_2X - g_3$. Notons qu'il est toujours possible de choisir $\omega_1 \in \mathbb{R}$ et $\Im m(\omega_1/\omega_2) > 0$.

Dans la suite, nous choisirons pour le réseau Λ le parallélogramme fondamental suivant:

$$\{a\omega_1 + b\omega_2; a, b \in \mathbb{R}, 0 < a \leqslant 1, 0 \leqslant b < 1\} \ .$$

Considérons maintenant l'application :

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\longrightarrow E(\mathbb{C}) \\ z &\longmapsto P = \begin{cases} \left[x = \wp(z) - \frac{b_2}{12}, y = \frac{\wp'(z) - a_1x - a_3}{2}\right] & \text{si } z \notin \Lambda \\ \infty & \text{si } z \in \Lambda \end{cases} \ , \end{aligned}$$

qui n'est autre que l'application qui à z associe le point $[\wp(z), \wp'(z)]$ sur la courbe E'. Cette application est un isomorphisme entre la courbe et le tore $\mathbb{C}/\Lambda$ (une fois choisi le parallélogramme fondamental pour le réseau Λ). Désignons par ψ la fonction réciproque de ϕ. Cette fonction est appelée logarithme elliptique et est donnée pour un point $P = [x, y]$ par la formule

$$\psi(P) = \int_{\infty}^{x + b_2/12} \frac{dt}{\sqrt{4t^3 - g_2t - g_3}} \qquad (\mathrm{mod}\ \Lambda) \ .$$

Cette fonction ψ est ainsi nommée car elle vérifie la propriété suivante caractéristique des logarithmes :

$$\psi(P+Q) = \psi(P) + \psi(Q) \qquad (\mathrm{mod}\ \Lambda)\ .$$

Remarque : Pour calculer cette fonction, on utilise le lien entre les intégrales elliptiques et la moyenne arithmetico-géométrique. Pour plus de précisions et des algorithmes effectifs, on pourra consulter le livre de Cohen [Coh 93].

Ces objets étant maintenant bien définis, nous pouvons nous interesser aux formes linéaires de logarithmes elliptiques.

I.3.2 Formes linéaires de logarithmes elliptiques

Rappelons tout d'abord la définition de la hauteur sur les courbes elliptiques afin de fixer les notations.
Si $P = [x, y]$ est un point de $E(\mathbb{Q})$ et si $x = p/q$ avec $(p, q) = 1$, on définit

$$h(P) = h(x(P)) = \max\{\log|p|, \log|q|\}\ .$$

Cette hauteur est appelée hauteur naïve. Elle peut être modifiée pour obtenir la hauteur canonique

$$\hat{h}(P) = \frac{1}{2} \lim_{N\to\infty} 4^{-N} h(2^N P)\ .$$

La hauteur canonique sur les courbes elliptiques est un outil plus naturel du point de vue théorique que la hauteur naïve. Cependant, la hauteur naïve est beaucoup plus simple à calculer. Pour pallier ce problème, Silverman a établit un lemme permettant de borner la différence entre la hauteur naïve h et la hauteur canonique $\hat{h}$.

Lemme I.3.1 (Silverman [Sil 90]) *Il existe des constantes C_1 et C_2 telles que*

$$-C_1 \leqslant \hat{h}(P) - \frac{h(P)}{2} \leqslant C_2\ .$$

De plus quand le corps de base est $\mathbb{Q}$ et que la courbe est définie par une équation de Weierstrass à coefficients entiers, nous pouvons prendre

$$C_2 = 1.07 + \frac{\log|\Delta| + \max(1, \log|j|)}{12} + \frac{1}{2}\max(1, \log|\frac{b_2}{12}|) + \frac{\log 2}{2}\ .$$

Lorsque $b_2 = 0$, le dernier terme $(\log 2/2)$ *est inutile.*

Remarque : Dans le cadre des courbes elliptiques définies par des "simplest cubic fields", on pourra choisir pour les paramètres $m \geqslant 9$ la constante C_2 suivante :

$$C_2 = 1.57 + \frac{\log(m^2 + 3m + 9)}{4} + \frac{\log(m)}{2}\ .$$

Nous allons maintenant présenter une version simplifiée d'un résultat de David [Dav 95] qui permet de minorer une forme linéaire de logarithmes elliptiques.
Soit E une courbe elliptique donnée par l'équation

$$Y^2 = 4X^3 - g_2X - g_3 \ ,$$

d'invariant j et de périodes ω_1 et ω_2 avec ω_1 réel et $\Im m(\omega_1/\omega_2) > 0$. Soient $P_1, \ldots, P_n$ des points de la courbe E. Définissons

- la hauteur de la courbe $h_E = \max(1, h_2(1, g_2, g_3), h(j))$ où h_2 désigne la hauteur logarithmique absolue sur $\mathbb{P}^2_{\mathbb{Q}}$,
- la constante $d_1 = \dfrac{3\pi}{|\omega_1|^2 \Im m(\omega_1/\omega_2)}$,
- le poids modifié $h_m(P_i) = \max\{2\hat{h}(P_i), h_E, d_1|\psi(P_i)|^2\}$,
- les constantes

$$\begin{aligned}
d_2 &= \max\{eh_E, h_m(P_1), \ldots, h_m(P_n)\} \ , \\
d_3 &= \min_{i=1\ldots n} \left\{ \frac{e\sqrt{h_m(P_i)}}{\sqrt{d_1}|\psi(P_i)|} \right\} \ , \\
d_4 &= 2.10^{8+7n} \left(\frac{2}{e}\right)^{2n^2} (n+1)^{4n^2+10n} (\log d_3)^{-2n-1} \prod_{i=1}^{n} h_m(P_i) \ .
\end{aligned}$$

Nous pouvons maintenant énoncer le théorème :

Théorème II (David [Dav 95]) *Soit* $L(x) = \sum_{i=1}^{n} x_i\psi(P_i)$ *avec* $x \in \mathbb{Z}^n$ *une forme linéaire de logarithmes elliptiques. Soit* A *le maximum des coefficients* x_i*. Si* $L(x)$ *est non nulle et si* $A \geqslant \exp(d_2)$*, alors*

$$\log|L(x)| > -d_4 \log A + \log d_3 (\log\log A + h_E + \log d_3)n + 1 \ .$$

Autrement dit, si la forme linéaire de logarithmes elliptiques n'est pas trop grande, ses coefficients ne sont pas trop grands non plus. Nous avons maintenant tous les ingrédients pour calculer des points entiers sur une courbe elliptique.

I.4 Calcul des points entiers sur une courbe elliptique

Soit E une courbe elliptique associée à un "simplest cubic field". Supposons que l'on ait réussi à calculer une base $P_1, P_2, \ldots, P_n$ de générateurs pour son groupe de Mordell-Weil.
On observe aisément que la somme de deux points de $E^0(\mathbb{R})$ reste dans $E^0(\mathbb{R})$. D'autre part, le point $[0, 1]$ est dans la partie compacte $E_{gg}(\mathbb{R})$, il y a donc nécessairement au moins un élément de la base dans $E_{gg}(\mathbb{R})$.
De plus, la somme de deux éléments de $E_{gg}(\mathbb{R})$ appartient à $E^0(\mathbb{R})$ (on peut voir ces propriétés directement sur le graphique de la courbe ; par exemple, sur le graphique (I.2)

les points P et Q appartiennent à la partie compacte de la courbe et leur somme R n'y appartient pas). Nous pouvons donc supposer dans la suite que seul P_1 est dans $E_{gg}(\mathbb{Q})$.

Soit désormais P un point entier. La méthode que nous exposons ici est valable en toute généralité, cependant, nous avons démontré que les courbes elliptiques associées aux "simplest cubic fields" ne possédaient pas de torsion. Nous décrivons donc la méthode dans ce cas pour plus de simplicité. On peut alors écrire

$$P = p_1 P_1 + \cdots + p_n P_n \quad ,$$

avec $p_i \in \mathbb{Z}$. Le but de cette méthode est de déterminer les valeurs des coefficients p_i pour lesquelles le point P est un point entier.
En utilisant une rechercche systématique, il est très facile de calculer tous les points entiers contenus dans la partie compacte de la courbe, nous allons donc supposer dans toute la suite que le point entier P appartient à la partie non compacte de la courbe. On définit alors

- $Q_1 = 2P_1 \ \in E^0(\mathbb{R})$,
- q_1 tel que $p_1 = 2q_1 + r, \quad r = 0$ ou 1 ,
- $Q_i = P_i$ et $q_i = p_i$ pour $i \neq 1, i \leqslant n$,
- $Q_{n+1} = P_1$,

de telle sorte que

$$P = q_1 Q_1 + \cdots + q_n Q_n + r Q_{n+1} \quad .$$

Les points $P, Q_1, \ldots, Q_n$ étant dans $E^0(\mathbb{R})$, leur somme l'est aussi. L'entier r est donc nécessairement nul.
Posons maintenant $H = \max |q_i|$. Si on peut trouver une borne suffisamment petite pour H, il sera possible d'énumérer tous les points susceptibles d'être entiers et de vérifier s'ils le sont effectivement.
Dans un premier temps, nous allons relier H à l'abscisse du point P.

Proposition I.4.1 *Si $P = [x, y]$ est un point entier,*

$$\frac{1}{|x|} \leqslant c_1 e^{-c_2 H^2} \quad ,$$

où c_1 et c_2 sont des constantes calculables.
Preuve : Comme P est un point entier, $h(P) = \log |x|$. Grâce au lemme I.3.1 de Silverman, on en déduit

$$\frac{\log |x|}{2} \geqslant \hat{h}(P) - C_2 \quad .$$

Considérons maintenant la matrice du régulateur R dont les coefficients sont les

$$< P_i, P_j >= \hat{h}(P_i + P_j) - \hat{h}(P_i) - \hat{h}(P_j) \quad .$$

Si p désigne le vecteur dont les coordonnées sont les p_i, nous avons $\hat{h}(P) = \frac{1}{2}{}^t pRp$. Soit alors ${}^tO\Lambda O$ une décomposition orthogonale de R avec O une matrice orthogonale et Λ la matrice diagonale des valeurs propres de R. Posons $c_2 = \min_{i=1\ldots r} \Lambda_{i,i}$ la plus petite de ces valeurs propres et $m = Op$, alors comme ${}^tOO = I$, et on a

$$\begin{aligned} 2\hat{h}(P) &= {}^tpRp = {}^tm\Lambda m = \sum_{i=1}^{n} \Lambda_{i,i} m_i^2 \quad , \\ &\geqslant c_2 \sum_{i=1}^{n} m_i^2 = c_2{}^tmm = c_2{}^tp{}^tOOp = c_2{}^tpp = c_2 \sum_{i=1}^{r} p_i^2 \quad , \\ &\geqslant c_2 \sum_{i=1}^{r} q_i^2 \geqslant c_2 H^2 \quad . \end{aligned}$$

Nous concluons alors en posant $c_1 = \exp(2C_2)$. □

Nous allons maintenant relier l'abscisse de P et la taille du logarithme elliptique de P. Comme nous l'avons déjà vu précédemment, la courbe E est isomorphe à une courbe de la forme

$$Y^2 = 4X^3 - g_2X - g_3 = g(X) \quad ,$$

et e_1, e_2, e_3 désignent les racines de g(X). Posons alors $c_4 = 2 \max_{i=1,2,3} |e_i|$.

Proposition I.4.2 *Si $P = [x, y] \in E^0(\mathbb{R})$ et si $|x + b_2/12| > c_4$, alors*

$$|\psi(P)|^2 \leqslant \frac{c_5}{|x|} \quad ,$$

avec $c_5 = 8 + \frac{|\omega_1^2|}{12}$.

Preuve : Posons $X = x + b_2/12$.
Soit $t \geqslant |X| > c_4$, nous avons, pour tout i, $t/2 > |t - e_i|$ et donc $|g(t)| > \frac{1}{2}|t|^3$.
Pour $N \geqslant X$, on a donc

$$\left| \int_N^{|X|} \frac{dt}{\sqrt{g(t)}} \right| \leqslant \sqrt{2} \left| \int_N^{|X|} t^{-\frac{3}{2}}\, dt \right| = 2\sqrt{2} \left(|X|^{-\frac{1}{2}} - N^{-\frac{1}{2}} \right) \quad .$$

En faisant tendre N vers l'infini, nous obtenons

$$\begin{aligned} |\psi(P)| &\leqslant 2\sqrt{2}|X|^{-\frac{1}{2}} \quad , \\ |x + \frac{b_2}{12}| &\leqslant \frac{8}{|\psi(P)|^2} \quad . \end{aligned}$$

En écrivant $x = x + b_2/12 - b_2/12$, nous en déduisons que

$$|x| \leqslant \frac{8 + |\psi(P)|^2|b_2|/12}{|\psi(P)|^2} \quad .$$

La conclusion vient alors en utilisant le fait que le point P est dans $E^0(\mathbb{R})$. Son abscisse est donc plus grande que les racines de f et son logarithme elliptique est donc réel. Cela entraîne alors que $|\psi(P)| \leqslant |\omega_1|$. $\square$

En combinant les deux propositions I.4.1 et I.4.2, nous obtenons une inégalité entre H et le logarithme elliptique de P.

Proposition I.4.3 *Si $P = (x, y)$ est un point entier de $E^0(\mathbb{Q})$ tel que $|x + b_2 \,/\, 12| \geqslant c_4$,*

$$|\psi(P)| \leqslant \sqrt{c_5 c_1} e^{-c_2 H^2/2} = c_6 e^{-c7H^2} \quad .$$

D'après la propriété du logarithme elliptique et comme $Q_i \in E^0(\mathbb{R})$ pour tout i,

$$\psi(P) - q_1\psi(Q_1) - \cdots - q_n\psi(Q_n) = m\omega_1 \quad ,$$

avec $|m| \leqslant nH+1$. Or $q_1\psi(Q_1)+\cdots+q_n\psi(Q_n)+m\omega_1$ est une forme linéaire de logarithmes elliptiques car $\omega_1 = \psi(\infty)$. Il est donc possible de minorer cette quantité d'après le résultat de David précédemment cité (théorème II). En comparant cette minoration et la majoration de la proposition I.4.3, on déduit une borne H_0 pour H. Cependant la borne ainsi obtenue est bien trop élevée. Heureusement, la théorie de l'approximation des formes linéaires va nous permettre de réduire cette borne de façon significative. La borne ainsi obtenue (en $O(\sqrt{\log H_0})$) sera alors suffisamment petite pour pouvoir énumérer tous les points susceptibles d'être entiers.

I.4.1 Approximation des formes linéaires

Nous nous intéressons, dans ce paragraphe, au problème suivant : soient n nombres complexes $\alpha_1, \ldots, \alpha_n$, deux constantes réelles positives c_6 et c_7 ainsi qu'une forme linéaire

$$L(x) = \sum_{i=1}^{n} x_i \alpha_i \quad ,$$

où les x_i sont des entiers bornés par des constantes X_i. On pose par ailleurs $X_0 = \max_{i=1\ldots n} X_i$. On veut déduire de l'inégalité

$$|L(x)| \leqslant c_6 e^{-c_7 H^2} \quad ,$$

une borne pour H en $O(\sqrt{\log X_0})$. En d'autres termes, nous aimerions montrer que la forme linéaire ne peut pas devenir trop petite si les coefficients sont bornés.

Ce problème a été étudié par Baker et Davenport [Bak-Dav 69] dans le cas $n = 2$. Il existe plusieurs façons de le généraliser pour des valeurs de $n > 2$. Nous allons présenter la méthode la plus utilisée ces dernières années.
L'idée de base de cette méthode, due à De Weger, consiste à approcher la forme linéaire par un réseau d'approximation, puis à trouver une base réduite pour ce réseau à l'aide de

l'algorithme LLL. Le premier vecteur de cette nouvelle base donne alors une approximation du plus petit vecteur du réseau et permet ainsi d'obtenir des renseignements sur la taille de la forme linéaire. Nous n'allons ici traiter que le cas où les α_i sont réels car c'est celui dont nous aurons besoin.

Nous choisissons tout d'abord une constante C de l'ordre de X_0^n, et nous considérons le réseau Λ engendré par les colonnes de la matrice

$$A = \begin{pmatrix} & & & 0 \\ & \mathbf{I_{n-1}} & & \vdots \\ & & & 0 \\ \lfloor C\alpha_1 \rfloor & \ldots & \lfloor C\alpha_{n-1} \rfloor & \lfloor \alpha_n \rfloor \end{pmatrix} \in \mathcal{M}_{n,n}(\mathbb{Z}) \ ,$$

où $\mathbf{I_{n-1}}$ désigne l'identité de $\mathcal{M}_{n-1,n-1}(\mathbb{Z})$. Le déterminant de cette matrice est alors de l'ordre de X_0^n et nous pouvons ainsi espérer que le premier élément de la base réduite sera de l'ordre de X_0. Nous exprimons dans un premier temps que le premier élément dans une base réduite par l'algorithme LLL fournit une bonne approximation de la taille du plus petit vecteur du réseau :

Lemme I.4.4 *Soit $B = (b_1, \ldots, b_n)$ une base réduite pour un réseau Λ de dimension n. Pour tout vecteur non nul x de Λ, on a*

$$\|b_1\|^2 \leqslant d\|x\|^2 \ ,$$

avec $d = \max\{\|b_1\|^2/\|b_i^*\|^2, 1 \leqslant i \leqslant n\}$ si B^* désigne la base orthogonale de Gram-Schmidt associée à B.

Preuve : L'inégalité est clairement vérifiée pour les b_i^*. Écrivons

$$x = \sum_{i=1}^{n} r_i b_i = \sum_{i=1}^{n} r_i' b_i^* \ ,$$

avec r_i dans $\mathbb{Z}$ et r_i' dans $\mathbb{R}$. Soit i_0 le plus grand indice tel que $r_i \neq 0$, nous avons alors $r_{i_0} = r_{i_0}'$ et

$$\begin{aligned} \|x\|^2 &= \sum_{i=1}^{n} r_i'^2 \ \|b_i^*\|^2 \geqslant r_{i_0}'^2 \ \|b_{i_0}^*\|^2 \geqslant \|b_{i_0}^*\|^2 \ , \\ &\geqslant d^{-1}\|b_1\|^2 \ . \end{aligned}$$

Ce qui prouve le lemme. □

Proposition I.4.5 *Soient $c_8 = \dfrac{\|b_1\|}{\sqrt{d}}$, $S = \sum_{i=1}^{n-1} X_i^2$ et $T = \dfrac{1}{2}\sum_{i=1}^{n} X_i$.
Si $c_8^2 \geqslant T^2 + S$ et si $x = {}^t(x_1, \ldots, x_n) \neq 0$ alors*

$$H \leqslant \sqrt{\frac{1}{c_7}\left(\log(Cc_6) - \log\left(\sqrt{c_8^2 - S} - T\right)\right)} \ .$$

Remarquons que si une telle borne pour H existe, elle est de l'ordre de $\sqrt{\log X_0}$.

Preuve : Posons $a = \sum_{i=1}^{n} x_i \lfloor C\alpha_i \rfloor$,

$$\left| |a| - |C\sum_{i=1}^{n} x_i\alpha_i| \right| \leqslant |a - C\sum_{i=1}^{n} x_i\alpha_i| \leqslant \sum_{i=1}^{n} \frac{X_i}{2} = T \ ,$$

$$\text{on en déduit} \qquad |a| \leqslant T + Cc_6 e^{-c_7 H^2} \ .$$

Considérons maintenant le vecteur $y = Ax$ du réseau. Si $x \neq 0$, d'après le lemme I.4.4 appliqué à y,

$$\begin{aligned} \sum_{i=1}^{n-1} x_i^2 + a^2 \ &\geqslant \ \frac{\|b_1\|^2}{d} = c_8^2 \ , \\ S + \left(T + Cc_6 e^{-c_7 H^2}\right)^2 \ &\geqslant \ c_8^2 \ . \end{aligned}$$

La borne sur H suit alors immédiatement. □

Si cette méthode échoue (c'est à dire si la condition sur c_8 n'est pas vérifiée), il suffit d'augmenter la constante C et de recommencer.

Revenons maintenant au cas qui nous préoccupe. Le résultat de David nous a permis d'obtenir une borne H_0 pour H dans le cas de la forme linéaire

$$q_1\psi(Q_1) + \cdots + q_n\psi(Q_n) + m\omega_1 \ .$$

Ainsi, les coefficients de cette forme sont bornés par nH_0+1 (car m est borné par $nH+1$). Cette forme linéaire est bornée grâce à la proposition I.4.3. La méthode que nous venons d'exposer permet donc de trouver une nouvelle borne pour H en $O(\sqrt{\log H_0})$ qui s'averera beaucoup plus exploitable.
En effet, dès l'instant où l'on dispose d'une borne suffisamment petite pour H, il devient possible de calculer toutes les combinaisons linéaires des Q_i dont les coefficients sont inférieurs à la borne obtenue et de regarder si elles donnent effectivement des points entiers. Cependant, si la nouvelle borne est encore trop grande pour pouvoir énumérer toutes les combinaisons linéaires (dans le cas où le rang est grand par exemple), il est tout à fait possible de réappliquer cet algorithme d'approximation à cette nouvelle borne afin d'en obtenir une encore plus petite.

Nous allons maintenant appliquer cette méthode de recherche de points entiers sur un exemple afin d'illustrer ce paragraphe.

I.4.2 Exemple

Nous traitons dans ce paragraphe le cas $m = 11$. Considérons pour cela la courbe E_{11} donnée par l'équation :

$$Y^2 = X^3 + 11X^2 - 14X + 1 \quad .$$

Le théorème I nous indique que le rang de cette courbe est au plus égal à 3. En appliquant à cette courbe le programme `mwrank` de Cremona [Cre], nous obtenons une base pour le groupe de Mordell-Weil

$$P_1 = [-12, 5],\ P_2 = [2, 5],\ P_3 = \left[\frac{5}{4}, \frac{13}{8}\right] \quad .$$

Le point P_1 est le seul de cette base appartenant à la partie compacte de la courbe. En conservant les notations des paragraphes précédents, nous avons donc

$$Q_1 = 2P_1 = \left[\frac{6254}{25}, -\frac{505283}{125}\right],\ Q_2 = P_2,\ Q_3 = P_3 \quad .$$

D'après la proposition I.4.1, si $P = q_1Q_1 + q_2Q_2 + q_3Q_3$ est un point entier et si H désigne le maximum des coefficients q_i,

$$\frac{1}{|x|} \leqslant 3183.064\, e^{-0.376H^2} \quad .$$

D'autre part, d'après la proposition I.4.2, si $|x + 11/3| > 16.98$, alors

$$|\psi(P)|^2 \leqslant \frac{16.123}{|x|} \quad .$$

Soit, en combinant les deux,

$$|\psi(P)| \leqslant 226.538\, e^{-0.188H^2} \quad .$$

Mais $\psi(P)$ est une forme linéaire de logarithmes elliptiques donnée par

$$\psi(P) = q_1\psi(Q_1) + q_2\psi(Q_2) + q_3\psi(Q_3) + m\omega_1 \quad ,$$

avec $|m| \leqslant 3H + 1$.
Le résultat de David permet d'obtenir

$$\log|\psi(P)| > -5.53.10^{107}(\log(3H+1) + 1.323)(\log\log(3H+1) + 11.96)^4 \quad ,$$

si $3H + 1 \geqslant 3627641006450$. Cela nous permet d'en déduire que

$$H \leqslant 1.4\ 10^{57} \quad .$$

Cette borne est bien sûr complètement inexploitable telle quelle. Nous la réduisons donc en utilisant la méthode exposée au paragraphe I.4.1. Nous obtenons ainsi $H \leqslant 46$, mais ce n'est encore pas suffisant. En réappliquant une seconde fois l'algorithme nous obtenons finalement

$$H \leqslant 11 \ .$$

Il est alors facile d'énumérer tous les points susceptibles d'être entiers et de vérifier s'ils sont bien entiers. On trouve ainsi les points :

$$\begin{aligned}
Q_1 - 2Q_3 &= [38, 265] \ , \\
Q_2 &= [2, 5] \ , \\
-Q_2 - Q_3 &= [6, 23] \ , \\
-Q_1 - Q_2 + Q_3 &= [26, 157] \ , \\
-Q_1 + 2Q_2 + 3Q_3 &= [3170, 178789] \ , \\
2Q_2 + Q_3 &= [30, 191] \ , \\
-Q_1 - 3Q_2 &= [7502, 650255] \ ,
\end{aligned}$$

ainsi que leurs opposés obtenus en changeant le signe de la seconde coordonnée. Reste maintenant à trouver les points contenus dans la partie compacte $E_{gg}(\mathbb{R})$ ainsi que ceux vérifiant $|x + 11/3| \leqslant 16.98$. Nous trouvons rapidement les points (d'ordonnée positive) suivants en plus des précédents :

$$[-12, 5], [-9, 17], [-4, 13], [-1, 5], [0, 1] \ .$$

I.4.3 Tables

Nous donnons en appendice les tables obtenues par les méthodes expliquées ci-dessus. Nous avons calculé les points entiers des courbes elliptiques E_m pour tous les paramètres m inférieurs à 1000 définissant un "simplest cubic field". Il est à noter que nous n'avons écrit dans ces tables que la moitié des points entiers, l'autre moitié étant obtenue en remplaçant la seconde coordonnée par son opposé.
Ces tables contiennent de gauche à droite, la valeur du paramètre m, la liste des générateurs du groupe de Mordell-Weil fournie par `mwrank` puis simplifiée, la liste des points entiers de la partie compacte $E_{gg}(\mathbb{R})$ obtenue par recherche directe et les points entiers de la partie non compacte obtenus par la méthode des logarithmes elliptiques.

Remarque : Dans certains cas, que nous avons pris soin d'indiquer par une * dans les tables, le programme `mwrank` n'est pas capable de conclure. Dans ces cas, nous avons vérifié le rang par la conjecture de Birch et Swinnerton-Dyer et la liste des points entiers donnée est complète si cette conjecture est vraie (en particulier cela signifie que la liste est complète dans le cas où les courbes elliptiques sont de rang 1).

L'examen de ces tables nous a permis d'observer certains phénomènes :

– lorsque le paramètre m est impair, il existe toujours un ou plusieurs points entiers dans la partie non compacte de la courbe. En revanche, lorsque ce paramètre est pair, il semble qu'il n'y ait jamais de points entiers dans la partie non compacte.

– Lorsque le rang de la courbe elliptique vaut 1, il semble que le point $[0, 1]$ forme une base du groupe de Mordell-Weil et qu'il n'existe pas d'autres points entiers que le point $[0, 1]$ et son double quand m est impair.

– Plus généralement, il semble que $[0, 1]$ puisse toujours faire partie d'un système de générateurs et même qu'il soit de hauteur minimum. Cependant cette dernière remarque n'est plus valable lorsque le paramètre m ne définit pas un "simplest cubic field", elle est par exemple fausse si $m = 5$ (auquel cas $m^2 + 3m + 9 = 7^2$).

La suite de ce chapitre est dédiée à la démonstration de ces observations ainsi qu'à d'autres résultats généraux concernant les points entiers de ces courbes elliptiques

I.5 Résultats généraux à propos des points entiers sur les courbes elliptiques $y^2 = x^3+mx^2-(m+3)x+1$

De nombreux articles traitent de la résolution d'équations diophantiennes paramétrées. En particulier, les équations de Thue en représentent une partie importante [Pet 91], [Nik-Sma 98]. Dans ce chapitre, on obtient des résultats intéressants sur des courbes elliptiques paramétrées. Toutes les courbes de cette famille possèdent le point entier $[0, 1]$, et cette particularité est essentielle pour notre étude. Il est probablement possible de généraliser ces méthodes à d'autres familles de courbes ayant un point fixé qui ne soit pas de torsion.

I.5.1 Étude arithmétique des points entiers

Nous allons tout d'abord démontrer la première observation que nous avons faite à partir des tables car elle est triviale :

Proposition I.5.1 *Lorsque le paramètre m est impair, il y a toujours au moins un point entier dans la partie non compacte de la courbe E_m.*

Preuve : Il est très facile de calculer les coordonnées du double du point $[0, 1]$ à l'aide des formules explicites pour la loi de duplication sur les courbes elliptiques :

$$2[0,1] = \left[\frac{m^2+2m+9}{4}, \frac{m^3+5m^2+15m+19}{8}\right] .$$

Ainsi le double du point $[0, 1]$ est un point entier si et seulement si le paramètre m est un entier impair. □

Nous démontrons maintenant que lorsque le paramètre m est pair, il ne peut pas y avoir de points entiers dans la partie non compacte de la courbe E_m. Cela se démontre par de simples considérations arithmétiques élémentaires.

Lemme I.5.2 *Si m est pair et si $P = [x, y]$ est un point entier, alors $x \equiv 0 \pmod 8$.*

Preuve : Posons $m = 2k$, de telle sorte que x et y vérifient l'équation

$$y^2 = x^3 + 2kx^2 - (2k+3)x + 1 \ .$$

- Si x est pair, y^2 est alors impair. Le seul carré impair modulo 8 étant 1, nous en déduisons que $(2k+3)x \equiv 0 \pmod 8$. $2k+3$ étant inversible modulo 8, il vient $x \equiv 0 \pmod 8$.
- Si x est impair un raisonnement analogue entraîne une contradiction. □

Lemme I.5.3 *Si le paramètre m est impair et si $P = [x, y]$ est un point entier, alors 4 ne divise pas $|x - 1|$.*

Preuve : Si on suppose $x \equiv 1 \pmod 4$, en utilisant une fois de plus le fait qu'un carré impair modulo 8 est forcément égal à 1, on obtient :

$$x + m - (m+3)x \equiv 0 \pmod 8$$

Ce qui conduit à une contradiction. □

Théorème III *Soit x un entier. Posons $a = x^2 - x$ et $b = x^3 - 3x + 1$. Il existe alors un entier m tel que $am + b$ soit un carré si et seulement si tout nombre premier impair divisant $|x - 1|$ est congru à 1 modulo 4 et si de plus 4 ne divise pas $|x - 1|$.*

Preuve : Remarquons tout d'abord que b est premier avec x et $x - 1$ et donc avec a. Il existe alors un entier m tel que $am + b$ soit un carré

$$\begin{aligned} &\Leftrightarrow \quad b \text{ est un carré modulo } a \ , \\ &\Leftrightarrow \quad \forall\, p|a, b \text{ est un carré modulo } p^n \text{ pour tout } n \leqslant v_p(a) \ , \end{aligned}$$

où, comme à l'accoutumée, $v_p(a)$ est la valuation p-adique de a. D'après le lemme de Hensel, si p est un nombre premier différent de 2,

$$b \text{ est un carré modulo } p^n \text{ pour tout } n \Leftrightarrow b \text{ est un carré modulo } p \ .$$

Soit donc p un nombre premier impair divisant a, de deux choses l'une :

- Soit $p|x$ et alors $\left(\frac{b}{p}\right) = \left(\frac{1}{p}\right) = 1$. Dans ce cas, b est un carré modulo p.
- Soit $p|(x-1)$ et $\left(\frac{b}{p}\right) = \left(\frac{(x^2-2)(x-1)-1}{p}\right) = \left(\frac{-1}{p}\right)$.

Finalement, b est un carré $\Leftrightarrow p \equiv 1 \pmod 4$.

Reste à montrer que si $2|a$, b est un carré modulo les puissances de 2 divisant a. Supposons donc a pair (auquel cas b est impair).

- Si $2||a$, b est toujours un carré modulo 2.
- Si $4||a$, $x^2 - x \equiv 0 \pmod 4$.
  - x pair $\Rightarrow b \equiv 1 \pmod 4$ et donc b est un carré modulo 4.
  - x impair $\Rightarrow x \equiv 3 \pmod 4$ par hypothèse, et alors $x^2 - x \equiv 2 \pmod 4$, d'où une contradiction.
- Si $8|a$, b est impair et une récurrence élémentaire montre que

$$\forall n,\ b \text{ est un carré} \pmod{2^n} \Leftrightarrow b \equiv 1 \pmod 8.$$

  - $x \equiv 0 \pmod 4 \Rightarrow b \equiv 1 \pmod 8$.
  - $x \equiv 1 \pmod 4$ n'a jamais lieu d'après les hypothèses.
  - $x \equiv 2$ ou $3 \pmod 4 \Rightarrow a = x^2 - x \equiv 2 \pmod 4$ ce qui est contradictoire. □

Corollaire I.5.4 *Soit $P = [x, y]$ un point entier sur la courbe E_m. Alors,*
si $x > 1$ on a $x \equiv 2 \pmod 4$ ou $x \equiv 3 \pmod 8$, et
si $x < 1$ on a $x \equiv 0 \pmod 8$ ou $x \equiv 7 \pmod 8$.

Preuve : Supposons tout d'abord que $x > 1$. Si $[x, y]$ est un point entier de la courbe E_m, $x^3 + mx^2 - (m+3)x + 1$ est un carré. Le théorème III implique alors que tout nombre premier divisant $x - 1$ est congru à 1 modulo 4. Si x est pair, on en déduit que $x - 1$ lui-même est congru à 1 modulo 4. Si x est impair, on sait que 4 ne divise pas $x - 1$ par les lemmes I.5.2 et I.5.3 et donc

$$\begin{aligned} x - 1 &= 2 \prod_{p|x-1,\, p\neq 2} p\ , \\ &\equiv 2 \pmod 8\ . \end{aligned}$$

La preuve est similaire dans le cas $x < 1$. □

Corollaire I.5.5 *Si m est pair, il n'y a pas de point entier d'abscisse strictement positive c'est à dire dans $E_m^0(\mathbb{Q})$.*

Preuve : Il n'y a jamais de point d'abscisse $x = 1$ sur la courbe. D'autre part, si $x > 1$, il y a une contradiction entre le corollaire I.5.4 et le lemme I.5.2. □

Ces corollaires peuvent être résumés comme suit :

Proposition I.5.6 *Il existe un entier m (ne définissant pas nécessairement un "simplest cubic field") tel que le point $[x, y]$ est dans $E_m(\mathbb{Z})$ si et seulement si les conditions suivantes sont vérifiées :*

1. *$y \equiv \pm 1 \pmod{q^{v_q(x)}}$ pour tout nombre premier impair q divisant x,*

2. $y \equiv \pm\sqrt{-1} \pmod{p^{v_p(x)}}$ *pour tout nombre premier impair* p *divisant* $x-1$,

3. y *est impair,*

4. si $x < 1$ *et* $x \equiv 0 \pmod 8$, *alors*

$$y \equiv \pm 1 \pmod{2^{v_2(x)-1}} \ .$$

Cette caractérisation nous permet d'effectuer plus rapidement une recherche systématique de points entiers si besoin est. On en aura par exemple l'utilité lorsqu'il s'agira de calculer tous les points entiers dans la partie compacte de la courbe puisque ces points n'entrent pas en ligne de compte dans la méthode des logarithmes elliptiques telle que nous l'avons exposée dans les paragraphes précédents.

Avant de démontrer les autres résultats annoncés, nous allons nous attarder quelques instants sur des solutions paramétrées à l'équation (I.1).

I.5.2 Solutions paramétrées de $y^2 = x^3 + mx^2 - (m+3)x + 1$

Dans ce paragraphe, on regarde l'équation (I.1) comme une surface affine dans $\mathbb{R}^3$. Cette méthode a également été récemment employée par Lecacheux dans [Lec 01]. Posons $x = u+1$. Comme $[0,1,m]$ appartient toujours à la surface, on peut poser $y-1 = (t-1)x$. En raison de la linéarité en m de l'équation $y^2 = x^3 + mx^2 - (m+3)x + 1$, on obtient une paramétrisation rationnelle de notre surface :

$$\left\{ \begin{array}{lcl} x & = & u+1 \ , \\ y & = & tu + t - u \ , \\ m & = & t^2 - 2t - u - 1 + \frac{t^2+1}{u} \ . \end{array} \right.$$

Il est cependant probablement impossible d'en trouver une paramétrisation polynomiale. Toutefois, notre but étant de trouver des solutions paramétrées entières à l'équation (I.1), il est naturel de poser

$$k = \frac{t^2+1}{u} \ .$$

Nous notons alors $P(k)$ la solution paramétrée ainsi obtenue. On peut par exemple écrire celle-ci pour $k = 1$:

$$P(1) = \left\{ \begin{array}{lcl} x & = & t^2 + 2 \\ y & = & -t^3 - 2t - t^2 - 1 \\ m & = & 2t - 1 \end{array} \right.$$

Dans ce cas, la solution est le double du point $[0,1]$ lorsque le paramètre m est impair, mais cette remarque a déjà été faite à la proposition I.5.1.

Les solutions paramétrées $P(-1)$ donnent un point entier lorsque $m = 2t^2 + 2t - 1$ où t est bien sûr un entier. Dans ce cas , les points

$$P_0 = [-1, 2t+1], P_1 = [0,1] \text{ et } P_2 = [2, 2t+1]$$

sont indépendants. Cela peut être prouvé en utilisant les hauteurs de Néron-Tate sur $\mathbb{Q}(t)$ [Shi 90]. De plus, les points

$$2P_1, P_0 + P_1, P_0 - P_1, P_2 + P_1, P_0 + P_2 \text{ et } P_2 - P_1$$

sont tous des points entiers de la courbe elliptique E_{2t^2+2t-1}. On remarquera que le dernier de ces points entiers est celui obtenu par la paramétrisation $P(-1)$. Ainsi, dans le cas où le paramètre m est de la forme $2t^2 + 2t - 1$, on obtient une courbe de rang au moins égal à 3 et possédant au moins 9 points entiers. Bien que ce ne soit pas évident au premier abord, nos tables suggéraient ce phénomène.

Des considérations analogues avec $k = -5$ donnent (après avoir remplacé t par $-\frac{5}{2}t + 2$) un point entier lorsque le paramètre m est de la forme $5t^2 - 3t + 3$. De plus, dans ces conditions, on trouve également 3 points entiers indépendants sur cette courbe. En combinant ces deux observations, on peut espérer trouver des valeurs du paramètre m pour lesquelles la courbe elliptique E_m ait un rang plus élevé et de nombreux points entiers. Il faudrait alors que le paramètre m satisfasse les deux équations données par $P(-1)$ et $P(-5)$. En d'autres termes, on doit avoir

$$2t_1^2 + 2t_1 - 1 = m = 5t_2^2 - 3t_2 + 3 \ .$$

Posons alors $T_1 = 2t_1 + 1$ et $T_2 = 10t_2 - 3$.
On doit alors résoudre l'équation $T_2^2 - 10\,T_1^2 = -81$ avec les conditions

- T_1 impair ,
- $T_2 \equiv -3 \pmod{10}$,
- T_1 et T_2 non multiples de 3 .

Un argument simple dans le corps $\mathbb{Q}\left(\sqrt{10}\right)$ permet de montrer que la solution générale à cette équation est

$$T_2 + T_1\sqrt{10} = (-1)^{\ell+1}\left(3+\sqrt{10}\right)^{2\ell+1}\left(11 + 2\sqrt{10}\right).$$

avec ℓ appartenant à $\mathbb{Z}$.

- Si $\ell = 0$, on obtient de cette façon $m = 11$. Dans ce cas, les 3 points de la première paramétrisation sont confondus avec ceux de la seconde. On obtient avec cette valeur de ℓ la plus petite valeur du paramètre m pour laquelle le rang de la courbe E_m vaut 3. De plus il y a 24 points entiers sur cette courbe.

- Si $\ell = -1$, on obtient $m = 143$ qui est la plus petite valeur du paramètre m pour laquelle le rang de la courbe E_m vaut 5 et la courbe E_{143} possède 46 points entiers.

- Enfin, si $\ell = 1$, on obtient $m = 14963$ et la courbe E_m est de rang 7. Nos paramétrisations permettent d'obtenir les 5 points indépendants :

$$[0,1], [-1,173], [2,173], [-4,547] \text{ et } [-11884, 659563].$$

  Les générateurs supplémentaires

$$[-64, 7873] \text{ et } [90, 10981]$$

  ont été obtenus par une recherche systématique en s'aidant de la proposition I.5.6. D'autre part, cette courbe possède au moins 62 points entiers. On remarque cependant que ce n'est pas là la plus petite valeur de m pour laquelle la courbe E_m est de rang 7. En effet, la valeur 12563 pour m est probablement la plus petite pour laquelle le rang vaut 7.

Nous allons maintenant prouver les résultats concernant le point $[0,1]$ qui sont les principaux résultats de ce chapitre. Nous allons en particulier démontrer que le point $[0,1]$ peut toujours faire partie d'un système de générateurs du groupe de Mordell-Weil de la courbe elliptique E_m si m définit un "simplest cubic field" (Théorème IV) et que les seuls points entiers multiples du point $[0,1]$ sont $[0,1]$ lui-même et son double dans le cas où le paramètre m est impair (ainsi que leurs opposés) (Théorème V).
Pour démontrer ces théorèmes, nous allons devoir approcher la hauteur canonique d'un point de la courbe. Ce calcul nécessitera de connaître le comportement asymptotique des périodes associées à la courbe E_m en fonction du paramètre m.

I.5.3 Approximations des périodes ω_1 et ω_2

La courbe elliptique E_m définie par (I.1) est isomorphe à la courbe

$$E' : Y^2 = 4\ g(X)\ ,$$

avec

$$g(X) = X^3 - \left(\frac{m^2}{3} + m + 3\right) X + \frac{2}{27}m^3 + \frac{m^2}{3} + m + 1\ .$$

Soient $e_1 \leqslant e_2 \leqslant e_3$ les racines réelles de $g(X)$ (le discriminant est toujours positif). Les périodes du réseau associé à la courbe E_m sont données par les intégrales suivantes :

$$\omega_1 = \int_{e_1}^{e_2} \frac{dx}{\sqrt{g(x)}} \text{ et } \omega_2 = -\int_{e_2}^{e_3} \frac{dx}{\sqrt{g(x)}}\ .$$

Une étude élémentaire de la fonction g nous permet d'obtenir des encadrements précis pour ces racines :

$$\begin{array}{rcccl} -\frac{2m}{3} - 1 - \frac{2}{m} & \leqslant & e_1 & \leqslant & -\frac{2m}{3} - 1 - \frac{1}{m} \quad \text{si } m \geqslant 2 \ , \\ \frac{m}{3} & \leqslant & e_2 & \leqslant & \frac{m}{3} + \frac{1}{m} \ , \\ \frac{m}{3} + 1 & \leqslant & e_3 & \leqslant & \frac{m}{3} + 1 + \frac{1}{m} \ . \end{array}$$

Commençons par approcher ω_2

$$\omega_2 = i \int_{e_2}^{e_3} \frac{dx}{\sqrt{(x-e_1)(x-e_2)(e_3-x)}} \in i\mathbb{R} \ .$$

Si $x \in [e_2, e_3]$, alors $m + 1 + \frac{1}{m} \leqslant x - e_1 \leqslant m + 2 + \frac{3}{m}$. On en déduit

$$\begin{array}{rcccl} \frac{1}{\sqrt{m+2+\frac{3}{m}}} & \leqslant & \frac{1}{\sqrt{x-e_1}} & \leqslant & \frac{1}{\sqrt{m+1+\frac{1}{m}}} \ , \\ \text{d'où } \frac{I}{\sqrt{m+2+\frac{3}{m}}} & \leqslant & \frac{\omega_2}{i} & \leqslant & \frac{I}{\sqrt{m+1+\frac{1}{m}}} \ , \end{array}$$

$$\text{avec } I = \int_{e_2}^{e_3} \frac{dx}{\sqrt{(x-e_2)(e_3-x)}} = \int_{-1}^{1} \frac{dt}{\sqrt{1-t^2}} = \pi \ .$$

Nous obtenons donc finalement l'encadrement

$$\frac{\pi}{\sqrt{m+2+\frac{3}{m}}} \leqslant \frac{\omega_2}{i} \leqslant \frac{\pi}{\sqrt{m+1+\frac{1}{m}}} \ .$$

Remarque : Cet encadrement nous permet bien sûr d'écrire que $\omega_2 \sim \frac{i\pi}{\sqrt{m}}$. Cependant dans la suite nous aurons surtout besoin de l'approximation suivante :

$$\frac{\omega_2}{i} \geqslant \frac{3.13}{\sqrt{m}} \quad \text{pour } m \geqslant 500 \ .$$

Considérons maintenant le cas, plus complexe, de la période réelle ω_1.
Nous allons ici découper l'intégrale en deux parties : $\omega_1 = \omega_1^+ + \omega_1^-$, avec

$$\omega_1^- = \int_{e_1}^{0} \frac{dx}{\sqrt{g(x)}} \text{ et } \omega_1^+ = \int_{0}^{e_2} \frac{dx}{\sqrt{g(x)}} \ .$$

Traitons tout d'abord le cas de ω_1^-. Les racines e_2 et e_3 sont éloignées des bornes de l'intégrale. Nous avons ainsi, pour $x \in [e_1, 0]$:

$$\begin{array}{rcccl} \frac{m}{3} & \leqslant & e_2 - x & \leqslant & m + 1 + \frac{3}{m} \ , \\ \frac{m}{3} + 1 & \leqslant & e_3 - x & \leqslant & m + 2 + \frac{3}{m} \ , \end{array}$$

d'où

$$\begin{aligned}
\frac{1}{\sqrt{(m+1+\frac{3}{m})(m+2+\frac{3}{m})}}\int_{e_1}^{0}\frac{dx}{\sqrt{x-e_1}} &\leqslant \omega_1^- \leqslant \frac{1}{\sqrt{(\frac{m}{3})(\frac{m}{3}+1)}}\int_{e_1}^{0}\frac{dx}{\sqrt{x-e_1}} ,\\
\frac{2\sqrt{-e_1}}{\sqrt{(m+1+\frac{3}{m})(m+2+\frac{3}{m})}} &\leqslant \omega_1^- \leqslant \frac{2\sqrt{-e_1}}{\sqrt{(\frac{m}{3})(\frac{m}{3}+1)}} ,\\
\frac{2\sqrt{\frac{2m}{3}+1+\frac{1}{m}}}{\sqrt{(m+1+\frac{3}{m})(m+2+\frac{3}{m})}} &\leqslant \omega_1^- \leqslant \frac{2\sqrt{\frac{2m}{3}+1+\frac{2}{m}}}{\sqrt{(\frac{m}{3})(\frac{m}{3}+1)}} .
\end{aligned}$$

Nous en déduisons alors les inégalités :

$$\frac{1.63}{\sqrt{m}} \leqslant \omega_1^- \leqslant \frac{4.9}{\sqrt{m}} \quad \text{pour } m \geqslant 500 .$$

Passons désormais au cas de ω_1^+.
Cette fois, seul e_1 est assez éloigné du domaine d'intégration pour pouvoir approcher $x-e_1$ de façon suffisamment fine. Pour $x \in [0, e_2]$, on a ainsi les inégalités

$$\frac{2m}{3}+1+\frac{1}{m} \leqslant x-e_1 \leqslant m+1+\frac{3}{m} .$$

On en déduit alors

$$\frac{I}{\sqrt{m+1+\frac{3}{m}}} \leqslant \omega_1^+ \leqslant \frac{I}{\sqrt{\frac{2m}{3}+1+\frac{1}{m}}} ,$$

avec

$$\begin{aligned}
I &= \int_0^{e_2}\frac{dx}{\sqrt{(x-e_2)(x-e_3)}} ,\\
&= \log\left(\frac{\sqrt{e_3}+\sqrt{e_2}}{\sqrt{e_3}-\sqrt{e_2}}\right) .
\end{aligned}$$

Or on peut approcher I grâce aux inégalités suivantes :

$$\frac{4\frac{m}{3}}{1+\frac{1}{m}} \leqslant \frac{\sqrt{e_3}+\sqrt{e_2}}{\sqrt{e_3}-\sqrt{e_2}} \leqslant \frac{4\left(\frac{m}{3}+1+\frac{1}{m}\right)}{1-\frac{1}{m}} .$$

Nous pouvons maintenant écrire :

$$\frac{1}{\sqrt{m+1+\frac{3}{m}}}\log\left(\frac{4m}{3\left(1+\frac{1}{m}\right)}\right) \leqslant \omega_1^+ \leqslant \frac{1}{\sqrt{\frac{2m}{3}+1+\frac{1}{m}}}\log\left(\frac{4\left(m+3+\frac{3}{m}\right)}{3\left(1-\frac{1}{m}\right)}\right) ,$$

$$\frac{\log\left(\frac{4}{3\left(1+\frac{1}{m}\right)}\right)}{\sqrt{m+1+\frac{3}{m}}}+\frac{\log(m)}{\sqrt{m+1+\frac{3}{m}}} \leqslant \omega_1^+ \leqslant \frac{\log\left(\frac{4}{3\left(1-\frac{1}{m}\right)}\right)}{\sqrt{\frac{2m}{3}+1+\frac{1}{m}}}+\frac{\log\left(m+3+\frac{3}{m}\right)}{\sqrt{\frac{2m}{3}+1+\frac{1}{m}}} .$$

Nous obtenons finalement, pour $m \geqslant 500$,

$$\frac{0.28}{\sqrt{m}} + \frac{0.99\log(m)}{\sqrt{m}} \leqslant \omega_1^+ \leqslant \frac{0.36}{\sqrt{m}} + \frac{1.23\log(m)}{\sqrt{m}} \quad .$$

$$\frac{1.91}{\sqrt{m}} + \frac{0.99\log(m)}{\sqrt{m}} \leqslant \omega_1 \leqslant \frac{5.26}{\sqrt{m}} + \frac{1.23\log(m)}{\sqrt{m}} \quad .$$

Remarque : En fait il est facile de démontrer que

$$\omega_1 = \frac{\log m + 4\log 2 + o(1)}{\sqrt{m}} \quad ,$$

mais nous n'en avons pas besoin dans la suite.
Nous allons maintenant pouvoir approcher la hauteur canonique d'un point sur E_m.

I.5.4 Approximation de la hauteur canonique

Dans un premier temps, nous allons trouver une borne supérieure pour la hauteur canonique d'un point entier P appartenant à E_m. En utilisant le lemme de Silverman I.3.1, on peut écrire

$$\hat{h}(P) - \frac{1}{2}h(P) \leqslant 1.57 + \frac{1}{4}\log(m^2 + 3m + 9) + \frac{1}{2}\log m \quad .$$

Comme P est supposé entier, $h(P) = \log\max\{1, |x_P|\}$. Et donc

$$\hat{h}(P) \leqslant \frac{32}{25}\log m + \frac{1}{2}\log\max\{1, |x_P|\} \text{ si } m \geqslant 500 \quad . \tag{I.2}$$

Nous devons maintenant trouver une borne inférieure pour la hauteur canonique d'un point rationnel de E_m. Pour cela nous allons décomposer cette hauteur canonique en une somme de contributions locales.
Soit donc $P = \left[\frac{\alpha}{d^2}, \frac{\beta}{d^3}\right]$ un point rationnel de E_m avec $(\alpha, d) = (\beta, d) = 1$. On calcule tout d'abord la contribution non archimédienne. Pour cela on utilise l'algorithme décrit dans [Sil 88] et dans [Coh 93] section 7.5.2.
L'équation de la courbe elliptique entraîne

$$\beta^2 = \alpha^3 + md^2\alpha^2 - (m+3)d^4\alpha + 1 \quad .$$

On a donc $\beta \equiv \alpha + 1 \pmod 2$ et d ne peut donc pas être pair. Un argument similaire montre que d n'est pas un multiple de 3. Posons maintenant

- $\Delta = m^2 + 3m + 9$,
- $A = 3\alpha^2 + 2md^2\alpha - (m+3)d^4$ le numérateur de $\frac{3\alpha^2}{d^4} + 2m\frac{\alpha}{d^2} - (m+3)$,
- $B = 2\beta$ le numérateur de $\frac{2\beta}{d^3}$,

- $C = 3\alpha^4 + 4m\alpha^3 d^2 - (6m+18)\alpha^2 d^4 + 12\alpha d^6 - \Delta d^8$
le numérateur de $\frac{3\alpha^4}{d^8} + \frac{4m\alpha^3}{d^6} - (6m+18)\frac{\alpha^2}{d^4} + 12\frac{\alpha}{d^2} - \Delta$,
- $D = \mathrm{pgcd}(A, B)$.

Les nombres premiers qui apportent une contribution locale sont les diviseurs de D. Nous allons maintenant démontrer que le seul nombre premier qui apporte une contribution locale est 2. Pour cela nous effectuons les divisions euclidiennes suivantes :

$$\begin{aligned} 4A^2 &= \left(9\alpha + 3d^2 m\right) B^2 + 4\Delta d^4 \left(\alpha^2 - d^2\alpha + d^4\right) \ , && \text{(I.3)} \\ B^2 &= 4\left(\alpha + d^2(m+1)\right)\left(\alpha^2 - d^2\alpha + d^4\right) - 4d^4\left(3\alpha + d^2 m\right) \ , && \text{(I.4)} \\ 27B^2 &= 4\left(3\alpha + d^2 m - 3d^4\Delta\right)\left(3\alpha + d^2 m\right) + 4d^6\left(2m+3\right)\Delta \ , && \text{(I.5)} \\ 4\Delta &= (2m+3)^2 + 27 \ . && \text{(I.6)} \end{aligned}$$

Soit donc p un nombre premier impair divisant D.
L'équation (I.3) implique que p^2 divise $4\Delta d^4(\alpha^2 - d^2\alpha + d^4)$. Par ailleurs, p divisant β (car $B = 2\beta$), il ne divise pas d. Comme m définit un "simplest cubic field", Δ est sans facteur carré et donc nécessairement

$$p \,|\, (\alpha^2 - d^2\alpha + d^4) \ .$$

En utilisant l'équation (I.4), on déduit alors que p doit diviser $3\alpha + d^2 m$. D'autre part, le résultant de A et B est égal à $d^{12}\Delta^2$ de telle sorte que p divise Δ et donc

$$p | (3\alpha + d^2 m - 3d^4\Delta) \ .$$

Mais alors, en utilisant l'équation (I.5), on montre que p^2 doit diviser $d^6(2m+3)\Delta$, et que donc p divise $(2m+3)$. On conclut finalement en utilisant l'équation (I.6). Celle ci implique que p divise 27, c'est à dire que p vaut nécessairement 3. Mais dans ce cas, 3 divise m et alors Δ n'est pas sans facteur carré, ce qui est contradictoire avec le fait que m définisse un "simplest cubic field". Ainsi 2 est le seul nombre premier divisant D.

Nous pouvons maintenant calculer la contribution locale en 2 que nous noterons C_2.
On a $v_2(B) = 1$ et $C \equiv -(2m+2) \pmod 8$. En appliquant l'algorithme, on obtient le résultat suivant :
- Si m est pair, $C_2 = \log(d)$,
- Si $m \equiv 1 \pmod 4$, $C_2 = \log(d) - \frac{\log(2)}{4}$,
- Si $m \equiv 3 \pmod 4$, $C_2 = \log(d) - \frac{\log(2)}{3}$.

Dans tous les cas, on obtient

$$C_2 \geqslant \log(d) - \frac{\log(2)}{3} \ .$$

Reste maintenant à calculer la contribution archimédienne, que nous noterons C_∞, d'un point rationnel P sur la courbe E_m. Rappelons qu'on note $\psi(P)$ le logarithme elliptique du point P. On pose

$$\begin{aligned} \lambda &= \frac{2\pi}{\omega_1} \ , \\ t &= \lambda \Re e(\psi(P)) \ , \\ q &= \exp\left(2i\pi\frac{\omega_2}{\omega_1}\right) \text{ et} \\ \theta &= \sum_{n=0}^{\infty} \sin\left((2n+1)t\right)(-1)^n q^{\frac{n(n+1)}{2}} \ . \end{aligned}$$

Avec ces notations, la contribution archimédienne vaut alors :

$$C_\infty = \frac{1}{32}\log\left|\frac{16\Delta^2}{q}\right| + \frac{1}{8}\log\left(\frac{\left(\frac{\alpha}{d^2}\right)^3 + m\left(\frac{\alpha}{d^2}\right)^2 - (m+3)\frac{\alpha}{d^2} + 1}{\lambda}\right) - \frac{1}{4}\log|\theta| \ .$$

Rappelons que notre but est de trouver une borne inférieure pour cette quantité. Nous allons donc chercher à minorer chacun des termes apparaissant dans cette expression. Le discriminant de la courbe, $16\Delta^2$, est plus grand que $16m^4$ et cette minoration est bonne assymptotiquement, on ne peut donc pas espérer mieux. En ce qui concerne θ dont on veut une majoration, étant donné que le point P est un point rationnel quelconque, il paraît difficile d'en obtenir une meilleure majoration que la majoration triviale :

$$|\theta| \leqslant \sum_{n=0}^{\infty} q^{\frac{n(n+1)}{2}} \leqslant \frac{1}{1-q} \ .$$

On a également besoin de majorer q. Pour cela on utilise les approximations sur les périodes que nous avons obtenues au paragraphe précédent. On peut donc écrire

$$\begin{aligned} & 2i\pi\tfrac{\omega_2}{\omega_1} && \leqslant \frac{-3.13\ 2\pi}{5.26 + 1.23\log(m)} && \leqslant -\frac{9.47}{\log(m)} && \text{si } m \geqslant 500 \ , \\ \text{d'où} \qquad & q && \leqslant \exp\left(-\frac{9.47}{\log(m)}\right) && \leqslant 1 - \frac{4.86}{\log(m)} && \text{si } m \geqslant 500 \ . \end{aligned}$$

En ce qui concerne le dernier terme, il peut aussi s'écrire $\dfrac{1}{4}\log\left(\dfrac{\beta}{d^3}\right) - \dfrac{1}{8}\log\lambda$. Nous traiterons le cas du premier terme plus tard, et nous le garderons donc tel quel pour le moment. En ce qui concerne $-\frac{1}{8}\log\lambda$, on le minore en utilisant une fois de plus les approximations sur les périodes du paragraphe précédent:

$$\begin{aligned} -\frac{1}{8}\log(\lambda) &= \frac{1}{8}\log\left(\frac{\omega_1}{2\pi}\right) \ , \\ &\geqslant -\frac{\log(2\pi)}{8} + \frac{1}{8}\log\left(\frac{1.91 + 0.99\log(m)}{\sqrt{m}}\right) \ . \end{aligned}$$

On est maintenant en mesure de minorer chaque partie de la composante archimédienne C_∞ pour les valeurs du paramètre m supérieures à 500:

$$\begin{aligned}
\frac{1}{32}\log|16\Delta^2| &\geqslant \frac{\log(m)}{8} + \frac{\log(2)}{8} \ , \\
\frac{1}{32}\log\left|\frac{1}{q}\right| &\geqslant \frac{1}{32}\log\left(\exp\left(\frac{9.47}{\log(m)}\right)\right) \\
&\geqslant \frac{9.47}{32\log(m)} \ , \\
-\frac{1}{4}\log|\theta| &\geqslant -\frac{\log\left(\frac{1}{1-q}\right)}{4} \\
&\geqslant -\frac{\log\left(\frac{\log(m)}{4.86}\right)}{4} \\
&\geqslant \frac{\log(4.86)}{4} - \frac{\log(\log(m))}{4} \ , \\
-\frac{1}{8}\log(\lambda) &\geqslant \frac{1}{8}\log\left(\frac{1}{\sqrt{m}}\right) - \frac{\log(2\pi)}{8} + \frac{1}{8}\log(1.91 + 0.99\log(m)) \\
&\geqslant -\frac{\log(m)}{16} - \frac{\log(2\pi)}{8} + \frac{\log\left(0.99 + \frac{1.91}{\log(m)}\right)}{8} + \frac{\log(\log(m))}{8} \ .
\end{aligned}$$

On peut réunir toutes les constantes intervenant dans ces minorations et minorer leur somme :

$$\frac{\log(2)}{8} - \frac{\log(2\pi)}{8} + \frac{\log(4.86)}{4} \geqslant 0.252 \ .$$

On obtient donc par cette méthode, lorsque $m \geqslant 500$, une borne inférieure pour la contribution archimédienne donnée par :

$$C_\infty \geqslant \frac{\log(m)}{16} + \frac{9.47}{32\log(m)} + \frac{\log\left(\frac{\beta}{d^3}\right)}{4} + \frac{\log\left(0.99 + \frac{1.91}{\log(m)}\right)}{8} - \frac{\log(\log(m))}{8} + 0.252 \ .$$

En lui ajoutant la contribution non archimédienne apportée par le nombre premier 2, on peut écrire

$$\begin{aligned}
\hat{h}(P) \geqslant \frac{\log(m)}{16} + \frac{9.47}{32\log(m)} + \frac{1}{4}\log\left(\frac{\beta}{d^3}\right) + \frac{1}{8}\log\left(0.99 + \frac{1.91}{\log(m)}\right) \\
-\frac{\log(\log(m))}{8} + \log(d) - \frac{\log(2)}{3} + 0.252 \ .
\end{aligned}$$

Finalement, on en déduit une borne inférieure pour la hauteur canonique d'un point rationnel $P = \left[\frac{\alpha}{d^2}, \frac{\beta}{d^3}\right]$ sur la courbe elliptique E_m à condition que m soit plus grand que 500 et définisse un "simplest cubic field" :

$$\frac{\log(m)}{16} + \frac{9.47}{32\log(m)} + \frac{\log(\beta d)}{4} + \frac{\log\left(0.99 + \frac{1.91}{\log(m)}\right)}{8} - \frac{\log(\log(m))}{8} + 0.02 \ . \qquad \text{(I.7)}$$

Nous avons désormais tous les outils nécessaires pour démontrer les derniers résultats annoncés dans le paragraphe I.4.3.

I.5.5 Résultats principaux

Théorème IV *Le point* $[0,1]$ *peut toujours faire partie d'un système de générateurs du groupe de Mordell-Weil de la courbe elliptique* E_m *pour peu que* m *définisse un "simplest cubic field".*

Preuve : Si $m \leqslant 500$, nous avons calculé le groupe de Mordell-Weil de la courbe E_m à l'aide du programme `mwrank` de Cremona [Cre] et l'assertion de ce théorème est vraie.
Si $m \geqslant 500$, on peut utiliser les approximations obtenues dans le paragraphe précédent. On sait déjà que le point $[0,1]$ appartient toujours à $E_m(\mathbb{Q})$ et qu'il n'est pas de torsion. Pour démontrer le théorème IV il suffit de prouver qu'il n'est pas le multiple d'un autre point rationnel.
Soit donc P un tel point sur la courbe E_m et $n \in \mathbb{Z} - \{0, 1, -1\}$ tel que $[0,1] = nP$. Étant donné qu'on a pris un entier n relatif, on peut supposer que P a une ordonnée positive. D'autre part, comme la somme de deux points de $E_m^0(\mathbb{Q})$ est toujours dans $E_m^0(\mathbb{Q})$ et comme $[0,1]$ est dans la partie compacte de la courbe, le point P est nécessairement lui aussi dans la partie compacte de la courbe. En terme de hauteurs canoniques, la condition $[0,1] = nP$ s'exprime par

$$\hat{h}([0,1]) = n^2\, \hat{h}(P) \ .$$

Or grâce au paragraphe précédent, on sait minorer $\hat{h}(P)$ et majorer $\hat{h}([0,1])$. On va donc pouvoir obtenir une borne pour n^2.

Supposons dans un premier temps que P soit un point entier différent du point $[0,1]$. Pour minorer $\hat{h}(P)$, on utilise la formule (I.7) obtenue dans le paragraphe précédent. Dans cette formule, seul le terme $\frac{1}{4}\log(\beta d)$ n'était pas minoré. Comme on a supposé le point P entier, son ordonnée β est forcément supérieure à $\sqrt{2m+3}$, et d vaut 1. On peut donc écrire, lorsque $m \geqslant 500$:

$$\begin{aligned}
\hat{h}(P) &\geqslant \frac{\log(m)}{16} + \frac{\log\sqrt{2m}}{4} + \frac{\log(0.99)}{8} - \frac{\log(\log(m))}{8} + 0.02 \ , \\
\hat{h}(P) &\geqslant \frac{3\log(m)}{16} - \frac{\log(\log(m))}{8} + 0.1 \ , \\
\hat{h}(P) &\geqslant \frac{\log(m)}{6} \ .
\end{aligned}$$

Pour majorer la hauteur canonique de $[0,1]$, on utilise (I.2) car le point $[0,1]$ est entier :

$$\hat{h}([0,1]) \leqslant \frac{32}{25}\log(m) \ .$$

On en conclut donc que pour $m \geqslant 500$,

$$n^2 = \frac{\hat{h}([0,1])}{\hat{h}(P)} \leqslant 6\,\frac{32}{25} \leqslant 8 \ .$$

Comme le point $2P$ appartient à $E_m^0(\mathbb{Q})$, il ne peut être égal au point $[0,1]$ qui appartient à la partie compacte de la courbe. Un tel point P ne peut donc pas exister.

On suppose maintenant que $P = \left[\frac{\alpha}{d^2}, \frac{\beta}{d^3}\right]$ n'est pas un point entier, autrement dit $d \neq 1$. On a déjà remarqué, au début du paragraphe I.5.4 que d était impair et n'était pas un multiple de 3, de telle sorte que le produit βd est supérieur à 5 (rappelons que l'ordonnée de P a été supposée positive). La formule (I.7) nous donne alors

$$\begin{aligned}
\hat{h}(P) &\geqslant \frac{\log(m)}{16} + \frac{\log(0.99)}{8} - \frac{\log(\log(m))}{8} + \frac{\log(5)}{4} \ , \\
\hat{h}(P) &\geqslant \frac{\log(m)}{17} \ .
\end{aligned}$$

Comme dans le cas précédent, on en déduit alors

$$n^2 \leqslant 17\,\frac{32}{25} \leqslant 22 \ .$$

Reste donc à tester si les points $\pm 2P$, $\pm 3P$ et $\pm 4P$ peuvent être égaux au point $[0,1]$. Les points $\pm 2P$ et $\pm 4P$ appartiennent à $E_m^0(\mathbb{Q})$ et ne peuvent donc pas être égaux à $[0,1]$. D'autre part un calcul explicite montre que d^2 divise forcément le dénominateur de l'abscisse des points $\pm 3P$. Ces points ne peuvent donc pas non plus être égaux à $[0,1]$.

Ceci achève donc de prouver qu'il n'est pas possible de trouver un point de $E_m(\mathbb{Q})$ tel que $[0,1]$ en soit un multiple, ce qui prouve bien que le point $[0,1]$ peut toujours faire partie d'un système de générateurs du groupe de Mordell-Weil de la courbe E_m. $\square$

Théorème V *Les seuls points entiers qui soient des multiples positifs du point* $[0,1]$ *sont*

- *Le point* $[0,1]$ *lui-même lorsque* m *est pair.*
- *Le point* $[0,1]$ *et son double* $2[0,1]$ *lorsque* m *est impair.*

Preuve : Lorsque $m \leqslant 500$, les tables obtenues par les méthodes exposées dans la première partie de ce chapitre permettent d'affirmer que ce théorème est vrai. Comme pour le théorème précédent, on utilise les approximations obtenues au paragraphe précédent lorsque $m \geqslant 500$. On démontre dans un premier temps trois lemmes. Pour plus de simplicité dans les énoncés, on ne considérera plus que les multiples positifs dans toute la suite.

Lemme I.5.7 *Les multiples impairs du point* $[0,1]$ *ne sont jamais entiers, en dehors du point* $[0,1]$ *lui-même bien sûr.*

Preuve : Soit donc n un entier strictement positif et $P = (2n+1)[0,1]$ un point entier de $E_m(\mathbb{Q})$. Puisque $[0,1]$ est dans la partie compacte de la courbe et que l'on considère ici des multiples impairs, le point P est également dans la partie compacte de la courbe. Dans ce cas, l'abscisse x_P du point P est inférieure en valeur absolue à $m+1$. On peut alors appliquer l'inégalité (I.2) au point P puisqu'il est entier et cela nous donne une majoration de sa hauteur canonique :

$$\begin{aligned} \hat{h}(P) &\leqslant \frac{32}{25}\log(m) + \frac{\log(m+1)}{2} \ , \\ \hat{h}(P) &\leqslant \frac{45}{25}\log(m) \ . \end{aligned}$$

D'autre part, l'inégalité (I.7) permet d'obtenir une borne inférieure pour la hauteur canonique du point $[0,1]$:

$$\begin{aligned} \hat{h}([0,1]) &\geqslant \frac{\log(m)}{16} + \frac{9.47}{32\log(m)} + \frac{\log\left(0.99 + \frac{1.91}{\log(m)}\right)}{8} - \frac{\log(\log(m))}{8} + 0.02 \ , \\ \hat{h}([0,1]) &\geqslant \frac{\log(m)}{25} \ . \end{aligned}$$

Remarque : Cette hauteur est expérimentalement donnée par :

$$\hat{h}([0,1]) = \frac{\log(m)}{4} + C_2 + o(1) \ ,$$

où C_2 est la contribution locale apportée par le nombre premier 2, comme décrit au paragraphe I.5.4 en prenant $d = 1$.

Finalement, on déduit de ces inégalités que, si $m \geqslant 500$, on a

$$(2n+1)^2 \leqslant 45 \ .$$

Pour compléter la preuve on doit donc regarder si les points $3[0,1]$ et $5[0,1]$ peuvent être des points entiers. Un calcul explicite donne :

$$x(3[0,1]) = -\frac{8m^3 + 40m^2 + 120m + 152}{m^4 + 4m^3 + 22m^2 + 36m + 81} \ ,$$

On peut alors facilement montrer que $|x(3[0,1])| < 1$ dès que le paramètre m est supérieur à 8 ; ainsi le point $3[0,1]$ ne peut pas être entier. Le même raisonnement permet de montrer que $|x(5[0,1])| < 1$ lorsque le paramètre m est supérieur à 29, et donc que le point $5[0,1]$ n'est jamais un point entier. □

Lemme I.5.8 *Le point* $4[0,1]$ *n'est jamais entier.*

Preuve : En appliquant deux fois la loi de duplication, on calcule aisément l'abscisse du point $4[0,1]$:

$$x(4[0,1])=\frac{m^8+8m^7+60m^6+280m^5+1158m^4+3320m^3+7868m^2+11368m+12033}{(4m^3+20m^2+60m+76)^2}$$

- Si m est pair, le numérateur de $x(4[0,1])$ est impair tandis que son dénominateur est pair. Le point $4[0,1]$ ne peut donc pas être entier dans ce cas.

- Si $m \equiv 1 \pmod 4$, on pose $m = 4k+1$ et on reporte cette valeur dans l'expression de $x(4[0,1])$. Le même raisonement que dans le cas précédent entraine alors que le point $4[0,1]$ n'est pas non plus entier dans ce cas.

- Si $m \equiv 3 \pmod 4$, la situation est un peu moins simple. On remplace bien sûr m par $4k+3$ dans l'expression de $x(4[0,1])$. On obtient ainsi une nouvelle expression pour l'abscisse du point $4[0,1]$:

$$\frac{64k^8+512k^7+1920k^6+4384k^5+6672k^4+6944k^3+4844k^2+2080k+426}{(8k^3+28k^2+36k+17)^2} .$$

  Le numérateur $p(k)$ et le dénominateur $q(k)^2$ de cette expression sont alors premiers entre eux pour toutes les valeurs de k. Il est en effet facile de montrer que l'on a

$$u(k)\,p(k)+v(k)\,q(k)=1 ,$$

  avec

$$\begin{aligned} u(k) &= 16k^2+8k-16 , \\ v(k) &= -128k^7-640k^6-1408k^5-1584k^4-648k^3+596k^2+908k+401 . \end{aligned}$$

  Il s'ensuit naturellement que le point $4[0,1]$ n'est jamais un point entier de la courbe elliptique E_m, comme annoncé. □

Lemme I.5.9

$$P \notin E(\mathbb{Z}) \Rightarrow 2P \notin E(\mathbb{Z}) .$$

Preuve : Soit $P = \left[\frac{\alpha}{d^2},\frac{\beta}{d^3}\right]$, avec $(\alpha,d)=(\beta,d)=1$ et $d\neq 1$. En utilisant la loi de duplication, on obtient l'abscisse du point $2P$:

$$x_{2P} = \frac{\alpha^4-2(m+3)\alpha^2d^4-8\alpha d^6+(m^2+2m+9)d^8}{4\beta^2d^2} .$$

Comme α est premier à d, on obtient trivialement que d^2 divise le dénominateur de x_{2P} et donc que $2P$ n'est pas un point entier. □

Remarque : De façon plus générale, si P est un point non entier alors aucun de ses multiples $[n]P$ ne peut être entier. Cela provient de considérations standard sur la filtration

p-adique d'une courbe elliptique sur $\mathbb{Q}_p$ [Hus 78].

Nous pouvons maintenant compléter la preuve du théorème V. On a

$$x(2[0,1]) = \left(\frac{m+1}{2}\right)^2 + 2 \ ,$$

de telle sorte que le point $2[0,1]$ est entier si et seulement si le paramètre m est impair.

Soit désormais P le point $2^p m[0,1]$ avec m impair et $p \geqslant 0$.

- Si $m = 1$, alors
  - soit $p = 0$ et $P = [0,1]$ est toujours entier,
  - soit $p = 1$ et $P = 2[0,1]$ est un point entier si et seulement si le paramètre m est impair,
  - soit $p \geqslant 2$ et alors le point P n'est pas entier en raison des lemmes I.5.8 et I.5.9.

- Si $m > 1$, le point $m[0,1]$ n'est pas un point entier d'après le lemme I.5.7. On peut alors conclure alors que le point P n'est pas un point entier en utilisant une nouvelle fois le lemme I.5.9. □

On déduit alors de façon élémentaire des théorèmes IV et V le corollaire suivant :

Corollaire I.5.10 *Soit m est un entier définissant un "simplest cubic field" et soit E_m la courbe elliptique définie par l'équation*

$$Y^2 = X^3 + mX^2 - (m+3)X + 1 \ .$$

Lorsque le rang de la courbe E_m vaut 1, le point $[0,1]$ forme une base pour le groupe de Mordell-Weil de E_m et l'ensemble $E_m(\mathbb{Z})$ de tous les points entiers de E_m est

- $E_m(\mathbb{Z}) = \{[0,1],[0,-1]\}$ *si m est pair*

- $E_m(\mathbb{Z}) = \{[0,1],[0,-1],2[0,1],2[0,-1]\}$ *si m est impair.*

Chapitre II

Méthodes de Chabauty explicites

Introduction

Comme nous l'avons déjà vu au cours de l'introduction, le nombre de points rationnels sur une courbe de genre supérieur ou égal à 2 définie sur un corps de nombre est fini. Cependant la preuve de ce théorème, due à Faltings [Fal 83], n'est pas explicite et ne permet donc pas de calculer effectivement tous ces points pour une courbe donnée. Pour que ce résultat soit effectif, le principal outil est le théorème beaucoup plus ancien de Chabauty [Cha 41]. Celui ci est cependant conditionné par le fait que le rang de la jacobienne doit être strictement inférieur au genre de la courbe pour pouvoir conclure de façon effective à la finitude du nombre de points rationnels.
Coleman [Col 85] a déduit de la méthode de Chabauty une borne pour le nombre de points rationnels : si $\mathcal{C}$ est une courbe de genre g dont la jacobienne a un rang strictement inférieur à g et si p est un nombre premier strictement supérieur à $2g$ pour lequel la courbe $\mathcal{C}$ a bonne réduction modulo p, alors,

$$|\mathcal{C}(\mathbb{Q})| \leqslant |\mathcal{C}(\mathbb{F}_p)| + 2g - 2 \ .$$

Remarque : Dans le cas des courbes hyperelliptiques, comme dans celui des courbes elliptiques, si p est impair et ne divise pas le discriminant du polynôme définissant la courbe $\mathcal{C}$, cette courbe a bonne réduction modulo p .

Le principal défaut du théorème de Coleman est que dans la plupart des cas non triviaux, il donne une borne non exacte du nombre de points rationnels sur une courbe. Autrement dit, on sait qu'il y a au plus un certain nombre de points rationnels mais on ne peut pas en conclure que les points déjà connus sont les seuls points rationnels.
Pour pallier ce défaut, Flynn a développé une version explicite du théorème de Chabauty pour les courbes de genre 2 dont la jacobienne est de rang 1 [Fly 97]. Cette méthode est basée sur les principes généraux suivants. En genre 2, la loi de groupe formelle est donnée par deux séries formelles en deux variables. En utilisant les propriétés de la surface de Kummer, Flynn exhibe une condition nécessaire devant être satisfaite par les séries

formelles pour qu'un point rationnel existe sur la courbe. Le nombre de zéros p-adiques de telles séries formelles peut alors être borné en utilisant le théorème de Strassman. La borne obtenue est généralement suffisamment fine pour pouvoir écrire exactement tous les points rationnels de la courbe.

Nous n'allons pas exposer plus en détail cette méthode car l'objet de ce chapitre est plutôt la méthode de Chabauty elliptique. Le but de cette méthode est de résoudre le problème suivant : étant donnée une courbe elliptique E de rang r définie sur un corps de nombre $\mathbf{k}$ de degré sur $\mathbb{Q}$ strictement supérieur à r, on veut connaître tous les points rationnels de $E(\mathbf{k})$ ayant une abscisse dans $\mathbb{Q}$. Ce problème étant analogue à celui consistant à trouver tous les points rationnels sur un courbe de genre supérieur à 2, la méthode de Chabauty elliptique est théoriquement entièrement similaire à la méthode de Chabauty classique. Elle est cependant plus simple dans la pratique car elle utilise les outils plus classiques des courbes elliptiques.
Cette méthode a été introduite par Flynn et Wetherell [Fly-Wet 99] et Bruin [Bru 99] afin de pouvoir contourner la méthode de Chabauty classique pour les courbes de genre 2 [Fly 97] lorsque le rang de la jacobienne est supérieur ou égal à 2. Le principe de cette méthode est dans un premier temps de se ramener à une famille de courbes elliptiques définies sur un corps de nombres. Calculer les points rationnels sur la courbe de genre 2 est alors un problème qui se ramène au calcul des points rationnels, dont l'abscisse est dans $\mathbb{Q}$, sur ces courbes elliptiques. En employant une méthode similaire à la méthode employée par Flynn pour les courbes de genre 2 [Fly 97], il est alors possible de calculer de tels points à condition que le rang des courbes elliptiques soit strictement inférieur au degré du corps de nombres sur lequel elles sont définies.

Nous allons dans un premier temps exposer cette méthode dans le détail, puis nous ferons un récapitulatif de diverses façons de ramener le problème des courbes de genre 2 à celui des courbes elliptiques. Ensuite, nous illustrerons cette méthode par un exemple que Flynn et Wetherell n'avaient pas réussi à résoudre [Fly-Wet 99]. Pour terminer ce chapitre, nous proposerons une méthode permettant de résoudre le problème de Chabauty elliptique dans un cas qui n'avait pas encore été traité de manière générale jusqu'à maintenant (on en trouve tout de même quelques exemples dans des cas simples dans [Bru 99]). Nous illustrerons cette généralisation en calculant exactement tous les points rationnels d'une courbe hyperelliptique de genre 4 et de rang 4 définie sur $\mathbb{Q}$.

II.1 La méthode de Chabauty elliptique

Dans ce paragraphe, on considère une courbe elliptique E définie par l'équation :

$$E : y^2 = g_3x^3 + g_2x^2 + g_1x + g_0 \ , \tag{II.1}$$

sur un corps de nombres $\mathbb{Q}(\alpha)$ de degré d sur $\mathbb{Q}$. Comme nous l'avons expliqué précédemment, notre but est de trouver tous les

$$[x, y] \in E(\mathbb{Q}(\alpha)) \text{ avec } x \in \mathbb{Q} \ . \tag{II.2}$$

Rappelons dans un premier temps la loi de groupe formelle d'une courbe elliptique. On introduit le changement de variables défini par

$$z = -\frac{x}{y} \text{ et } w = -\frac{1}{y} \ ,$$

dont la transformation réciproque est donnée par $x = \frac{z}{w}$ et $y = -\frac{1}{w}$. Ce changement de variables envoie le point à l'infini sur le point $[0, 0]$ et l'équation (II.1) devient :

$$w = g_3 z^3 + g_2 z^2 w + g_1 z w^2 + g_0 w^3 \ . \tag{II.3}$$

En effectuant des substitutions récursives grâce à cette équation, il est alors possible d'écrire w comme une série formelle en z à coefficients dans $\mathbb{Z}[g_0, g_1, g_2, g_3]$ dont nous donnons ici les premiers termes :

$$w = w(z) = g_3 \left(z^3 + g_2 z^5 + \left(g_1 g_3 + g_2^2\right) z^7 + \left(g_0 g_3^2 + g_2^3 + 3 g_1 g_2 g_3\right) z^9 + O\left(z^{11}\right)\right) \ . \tag{II.4}$$

Avant de parler de la loi de groupe formelle sur les courbes elliptiques, nous allons exprimer, pour un point $P = [x, y]$ donné, l'inverse de son abscisse ainsi que l'abscisse de sa somme avec un autre point à l'aide de séries formelles en z. Nous aurons en effet besoin de ces séries formelles dans la suite de l'exposé.
Il est possible d'exprimer $x(z) = \frac{z}{w(z)}$ et $y(z) = -\frac{1}{w(z)}$ comme des séries de Laurent mais pas comme des séries formelles. Il est cependant possible d'écrire $\frac{1}{x} = \frac{w(z)}{z}$ comme une série formelle obtenue en divisant l'expression (II.4) par z :

$$\frac{1}{x} = \frac{1}{x(z)} = g_3 \left(z^2 + g_2 z^4 + \left(g_1 g_3 + g_2^2\right) z^6 + \left(g_0 g_3^2 + g_2^3 + 3 g_1 g_2 g_3\right) z^8 + O\left(z^{10}\right)\right) \ . \tag{II.5}$$

D'autre part, si $[x_0, y_0]$ est un autre point de la courbe elliptique E, la loi d'addition sur les courbes elliptiques permet de calculer les coordonnées du point $[x, y] + [x_0, y_0]$ et en particulier son abscisse :

$$\begin{aligned} \text{abscisse}([x, y] + [x_0, y_0]) &= \frac{1}{g_3} \left(\left(\frac{y - y_0}{x - x_0} \right)^2 - g_2 \right) - x - x_0 \ , \\ &= \frac{w(1 + y_0 w)^2 - (g_2 w + g_3 z + g_3 x_0 w)(z - x_0 w)^2}{g_3 w (z - x_0 w)^2} \ , \end{aligned}$$

avec bien sûr $[x, y] = \left[\frac{z}{w}, -\frac{1}{w}\right]$. Si on remplace, dans cette équation, w par l'expression de $w(z)$ obtenue en (II.4), les termes en z^3 s'annulent au numérateur. On peut alors simplifier le numérateur et le dénominateur par $g_3 z^5$ de telle sorte que le dénominateur soit de la forme $1+O(z)$. Ce dénominateur est donc inversible, et l'abscisse du point $[x,y]+[x_0,y_0]$ peut s'écrire comme une série formelle en z à coefficients dans $\mathbb{Z}[g_0,g_1,g_2,g_3,x_0,y_0]$. Les premiers termes de cette série sont alors donnés par

$$\text{abscisse}([x,y]+[x_0,y_0]) = x_0+2y_0z+(3g_3x_0^2+2g_2x_0+g_1)z^2+(4g_3x_0y_0+2g_2y_0)z^3+$$

$$(4g_3^2x_0^2+6g_2g_3x_0^2+2g_1g_3x_0+2g_2^2x_0+g_0g_3+g_3y_0^2+g_1g_2)z^4+O(z^5)\ . \tag{II.6}$$

Revenons désormais à la loi de groupe formelle sur les courbes elliptiques. Soient $[z_1,w(z_1)]$ et $[z_2,w(z_2)]$ deux points de la courbe exprimés à l'aide des coordonnées (z,w). La z-coordonnée de la somme de ces deux points peut alors être écrite comme une série formelle en z_1 et z_2 à coefficients dans $\mathbb{Z}[g_0,g_1,g_2,g_3]$. C'est cette série formelle notée $\mathcal{F}(z_1,z_2)$ qui est appelée loi de groupe formelle. Pour plus de précisions sur cette loi de groupe formelle et pour en calculer les termes jusqu'à n'importe quel degré raisonnable, on se référera au livre de Silverman [Sil 86].

Nous allons maintenant définir le logarithme et l'exponentielle formels. Pour cela on pose $G(z_1,z_2)=\frac{\partial}{\partial z_1}\mathcal{F}(z_1,z_2)$ et on définit le logarithme formel, que l'on notera $\mathrm{Log}(t)$, par $\mathrm{Log}(t)=\int G(0,t)^{-1}dt$. Cette fonction $\mathrm{Log}(t)$ est une série formelle en t à coefficients dans $\mathbb{Q}[g_0,g_1,g_2,g_3]$ dont les premiers termes sont donnés par :

$$\mathrm{Log}\ (t)=t+\frac{1}{3}g_2t^3+\frac{1}{5}\left(g_2^2+2g_1g_3\right)t^5+\frac{1}{7}\left(g_2^3+6g_1g_2g_3+3g_0g_3^2\right)t^7+O\left(t^9\right)\ . \tag{II.7}$$

Cette série formelle satisfait :

$$\mathrm{Log}\left(\mathcal{F}(z_1,z_2)\right)=\mathrm{Log}(z_1)+\mathrm{Log}(z_2)\ .$$

La fonction exponentielle formelle, que nous noterons $\mathrm{Exp}(t)$, peut alors être définie par l'équation $\mathrm{Exp}(\mathrm{Log}(t))=t$. Cette nouvelle fonction $\mathrm{Exp}(t)$ est aussi une série formelle en t à coefficients dans $\mathbb{Q}[g_0,g_1,g_2,g_3]$. Les premiers termes sont donnés par :

$$\mathrm{Exp}(t)=t-\frac{1}{3}g_2t^3+\frac{1}{15}\left(2g_2^2-6g_1g_3\right)t^5-\frac{1}{315}\left(17g_2^3-66g_1g_2g_3+135g_0g_3^2\right)t^7+O\left(t^9\right) \tag{II.8}$$

et cette série formelle vérifie l'équation :

$$\mathcal{F}\left(\mathrm{Exp}(z_1),\mathrm{Exp}(z_2)\right)=\mathrm{Exp}(z_1+z_2)\ .$$

Comme on peut le remarquer dans les équations (II.7) et (II.8), les coefficients de ces séries formelles sont bien des nombres rationnels. Cependant, comme pour le logarithme et l'exponentielle usuels, les dénominateurs intervenant ne deviennent pas arbitrairement grands. On a en effet

$$k!\left(\text{coefficient de } t^k \text{ dans } \mathrm{Log}(t) \text{ ou } \mathrm{Exp}(t)\right)\in\mathbb{Z}[g_0,g_1,g_2,g_3]\ .$$

Nous avons maintenant en mains les outils qui vont nous permettre de décrire la méthode de Chabauty elliptique dont le but est de résoudre le problème (II.2). On a bien sûr besoin pour cela de connaître la structure du groupe de Mordell-Weil $E(\mathbb{Q}(\alpha))$. On suppose donc dans toute la suite qu'on a trouvé son sous-groupe de torsion, son rang ainsi qu'un ensemble de générateurs pour $E(\mathbb{Q}(\alpha))$. Les principes généraux pour ces calculs sont exposés dans le livre de Silverman [Sil 86]. De nombreux chercheurs se sont penchés sur le problème du calcul des générateurs du groupe de Mordell-Weil d'une courbe elliptique définie sur un corps de nombres. Ainsi les articles [Bru 99], [Cre 99], [Dja-Sch-Sma 00], [Sik 95] et [Sim] permettent d'obtenir plus de détails. Pour les calculs pratiques que nous avons eu besoin d'effectuer dans la suite, nous avons utilisé le programme de Simon [Sim] développé pour `pari` [BBBCO].
Dans le cas où le rang de la courbe elliptique est nul, le groupe de torsion $E(\mathbb{Q}(\alpha))_{\text{tors}}$ est fini et il est trivial de répondre au problème (II.2). Il suffit en effet de tester pour chaque point de $E(\mathbb{Q}(\alpha))_{\text{tors}}$ si son abscisse est dans $\mathbb{Q}$.

On suppose désormais que le rang est non nul et qu'il est inférieur à d, le degré du corps de nombres $\mathbb{Q}(\alpha)$ sur lequel E est définie. On entend par là que $\mathbb{Q}(\alpha)$ est engendré par les coefficients g_0, g_1, g_2 et g_3 de la courbe elliptique. Cette condition sur le rang est analogue à la condition sur le rang de la jacobienne dans le théorème de Chabauty et cette analogie entre ce problème et celui qui consiste à trouver tous les points rationnels sur une courbe de genre supérieur à 2 vaut son nom à cette méthode dite de Chabauty elliptique. Comme nous l'avons déjà écrit, nous supposons connue la structure du groupe de Mordell-Weil de la courbe E :

$$E(\mathbb{Q}(\alpha)) = \langle P_1, \ldots, P_r \rangle \bigoplus E(\mathbb{Q}(\alpha))_{\text{tors}} \quad .$$

On choisit maintenant un nombre premier impair p telle que α soit p-entier et on note $\widetilde{\alpha}$ l'image de α dans $\mathcal{O}/p\mathcal{O}$, si $\mathcal{O}$ désigne l'anneau des entiers de $\mathbb{Q}(\alpha)$. On suppose de plus que p satisfait aux conditions suivantes :

1. $[\mathbb{Q}_p(\alpha) : \mathbb{Q}_p] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = d$.
2. L'extension $\mathbb{Q}(\alpha)$ est non ramifiée en p.
3. $|\alpha|_p = 1$.
4. Le corps résiduel de $\mathbb{Q}_p(\alpha)$ est $\mathbb{F}_p((\widetilde{\alpha}))$.
5. La courbe E a bonne réduction en p.
6. $|g_i|_p \leqslant 1$, pour $i = 0, \ldots, 3$.

Cela fait de nombreuses conditions et on peut se demander à juste titre s'il est possible de satisfaire facilement à toutes ces conditions dans la pratique. La première condition est la plus difficile à réaliser. En effet, même s'il est toujours possible de vérifier cette condition lorsque le corps $\mathbb{Q}(\alpha)$ est de degré 2 ou 3, cela n'est plus possible lorsque par exemple le corps est de la forme $\mathbb{Q}\left(\sqrt{a}, \sqrt{b}\right)$. Il est cependant possible de se passer de cette condition comme le font Flynn et Wetherell dans [Fly-Wet 01]. Quant aux autres conditions, elles sont plus simples à remplir. Les conditions 2, 5 et 6 sont des conditions habituelles et peu restrictives. Enfin, les conditions 3 et 4 sont imposées par le fait que α (ou sa réduction) est un générateur pour tous les corps et anneaux que nous avons besoin de considérer.

Nous désignons par $\widetilde{E}$ la réduction de la courbe elliptique modulo p :

$$\widetilde{E} : y^2 = \widetilde{g_3}x^3 + \widetilde{g_2}x^2 + \widetilde{g_1}x + \widetilde{g_0} \ ,$$

où $\widetilde{g_i}$ désigne la réduction modulo p du coefficient g_i. $\widetilde{E}$ est une courbe elliptique sur $\mathbb{F}_p(\widetilde{\alpha})$ puisque p a été supposé de bonne réduction. On note également $\widetilde{P_i}$ la réduction modulo p de P_i et on définit m_i, Q_i et z_i pour $i = 1, \ldots, r$ par

$$\begin{aligned} m_i &= \text{ordre de } \widetilde{P_i} \text{ dans } \widetilde{E}\left(\mathbb{F}_p\left(\widetilde{\alpha}\right)\right) \ , \\ Q_i &= m_i P_i \in E\left(\mathbb{Q}(\alpha)\right) \ , \\ z_i &= z\text{-coordonnée de } Q_i \ , \\ &= -\frac{x_i}{y_i} \text{ si } Q_i = [x_i, y_i] \ , \end{aligned}$$

de telle sorte que chaque point Q_i est dans le noyau de la réduction modulo p. On suit alors la même stratégie que pour la méthode de Chabauty pour les courbes de genre 2 exposée dans [Fly 97]. Soit donc $\mathcal{U}$ l'ensemble fini :

$$\mathcal{U} = \left\{T + k_1P_1 + \cdots + k_rP_r : T \in E(\mathbb{Q}(\alpha))_{\text{tors}}, \left\lfloor -\frac{m_i}{2} \right\rfloor + 1 \leqslant k_i \leqslant \left\lfloor \frac{m_i}{2} \right\rfloor \right\} \ .$$

Ainsi, tout point P appartenant à la courbe elliptique $E(\mathbb{Q}(\alpha))$ peut s'écrire sous la forme

$$P = U + n_1Q_1 + \cdots + n_rQ_r \ ,$$

avec $U \in \mathcal{U}$ et $n_1, \ldots, n_r \in \mathbb{Z}$. Rappelons que la condition qu'on cherche à exprimer est que l'abscisse d'un tel point P soit dans $\mathbb{Q}$. Pour ce faire, nous allons calculer cette abscisse comme une série formelle en $n_1, \ldots, n_r$ à l'aide des outils de la loi de groupe formelle introduits précédemment. Nous pourrons ensuite exprimer qu'une telle série formelle doit être dans $\mathbb{Q}$. En utilisant le logarithme et l'exponentielle formels , on peut écrire la z-coordonnée de $n_1Q_1 + \cdots + n_rQ_r$ comme une série formelle en $n_1, \ldots, n_r$, en effet :

$$z\text{-coordonnée}(n_1Q_1 + \cdots + n_rQ_r) = \operatorname{Exp}(n_1\operatorname{Log}(z_1) + \cdots + n_r\operatorname{Log}(z_r)) \ . \tag{II.9}$$

La condition 6, l'estimation standard $|k!|_p \geqslant p^{-\frac{k-1}{p-1}}$ et le fait que, comme les points Q_i sont dans le noyau de la réduction, $|z_i|_p \leqslant \frac{1}{p}$ permettent de démontrer d'une part que cette série formelle est à coefficients dans $\mathbb{Z}_p[\alpha]$ et d'autre part que ces coefficients tendent vers 0 dans $\mathbb{Z}_p[\alpha]$ quand $k_1 + \cdots + k_r$ tend vers l'infini.

Revenons maintenant au cas du point P. Supposons dans un premier temps que le point U est le point à l'infini. On utilise alors les équations (II.5) et (II.9) afin de définir la série formelle $\theta_\infty \in \mathbb{Z}_p[\alpha][[n_1, \ldots, n_r]]$:

$$\theta_\infty(n_1, \ldots, n_r) = \frac{1}{\text{abscisse}(n_1 Q_1 + \cdots + n_r Q_r)} \ .$$

Supposons maintenant que $U \in \mathcal{U}$ soit un point $[x_0, y_0]$ différent du point à l'infini. Par construction U n'est pas dans le noyau de la réduction, ce qui implique que $|x_0|_p$ et $|y_0|_p$ sont tous deux inférieurs ou égaux à 1. À l'aide des équations (II.6) et (II.9) on définit la série formelle $\theta_U \in \mathbb{Z}_p[\alpha][[n_1, \ldots, n_r]]$:

$$\theta_U(n_1, \ldots, n_r) = \ \text{abscisse}(U + n_1 Q_1 + \cdots + n_r Q_r) \ .$$

Nous pouvons maintenant exploiter ces séries formelles. En effet, la série formelle θ_U (que U soit le point à l'infini ou pas) est à coefficients dans $\mathbb{Z}_p[\alpha]$. On peut donc décomposer cette série formelle suivant les puissances de α :

$$\theta_U = \theta_U^{(0)} + \theta_U^{(1)}\alpha + \cdots + \theta_U^{(d-1)}\alpha^{d-1} \ ,$$

où chaque composante $\theta_U^{(i)}$ est une série formelle en $(n_1, \ldots, n_r)$ à coefficients dans $\mathbb{Z}_p$. De plus les coefficients de ces séries formelles tendent toujours vers 0 dans $\mathbb{Z}_p$ quand $z_1 + \cdots + z_r$ tend vers l'infini. La condition sur la rationalité de l'abscisse du point P se traduit donc par l'annulation de $d-1$ séries formelles en $(n_1, \ldots, n_r)$:

$$\theta_U^{(1)} = \cdots = \theta_U^{(d-1)} = 0 \ .$$

Remarque : La condition sur le rang de la courbe elliptique apparaît ici clairement : cette méthode nous fournit $d-1$ équations (en fait des séries formelles) en r variables $(n_1, \ldots, n_r)$ et il parait donc naturel de supposer $r \leqslant d-1$.

On a donc exprimé le fait que l'abscisse du point P était dans $\mathbb{Q}$ en terme d'annulation de séries formelles. Il nous reste maintenant à connaître les zéros de ces séries formelles. Dans le cas où l'annulation d'une seule série formelle est nécessaire, c'est à dire dans la cas où le rang de la courbe elliptique vaut 1 (quelque soit le degré du corps de nombres), le théorème de Strassman, que l'on peut par exemple trouver dans [Cas 86], permet de borner le nombre de zéros d'une telle série formelle.

Théorème VI *Soit $\theta(X) = c_0 + c_1 X + \ldots$ une série formelle en X à coefficients dans $\mathbb{Z}_p[[X]]$ telle que c_i tend vers 0 dans $\mathbb{Z}_p$. On définit alors ℓ de manière unique par :*

$$\begin{aligned} |c_\ell|_p &\geqslant |c_i|_p \text{ pour tout } i \geqslant 0 \ , \\ |c_\ell|_p &> |c_i|_p \text{ pour tout } i > \ell \ . \end{aligned}$$

Il y a alors au plus ℓ valeurs de x dans $\mathbb{Z}_p$ telles que $\theta(x) = 0$.

Autrement dit le nombre de zéros dans $\mathbb{Z}_p$ d'une telle série formelle est borné par l'indice du coefficient de plus petite valuation p-adique.

Dans les exemples connus jusque là dans la littérature, les courbes elliptiques étaient de rang 0 ou 1 et ce théorème suffisait pour conclure. Il existe aussi quelques exemples où le rang vaut 2 et où l'on peut conclure par des astuces à l'aide du théorème de Strassman [Bru 99]. Dans le cas général Flynn et Wetherell suggèrent d'utiliser un théorème de préparation de Weierstrass en plusieurs variables afin de pouvoir conclure. Nous avons développé cette idée et cela fera l'objet du paragraphe II.4 de ce chapitre.

Supposons donc que l'on sache borner le nombre de solutions $(n_1, \dots, n_r)$ du système

$$\theta_U^{(1)}(n_1, \dots, n_r) = \cdots = \theta_U^{(d-1)}(n_1, \dots, n_r) = 0 \ .$$

Ainsi, pour un élément U donné dans l'ensemble fini $\mathcal{U}$, on peut borner le nombre de r-uplets $(n_1, \dots, n_r)$ tels que le point $U + n_1 Q_1 + \cdots + n_r Q_r$ ait une abscisse dans $\mathbb{Q}$. En appliquant cette stratégie à chacun des points de l'ensemble fini $\mathcal{U}$, on peut donc borner le nombre de points de $E(\mathbb{Q}(\alpha))$ ayant une abscisse dans $\mathbb{Q}$. Il ne reste plus alors qu'à espérer que cette borne corresponde exactement au nombre de points déjà connus ayant cette propriété.
L'inconvénient majeur de cette méthode est qu'elle ne donne qu'une borne sur le nombre de points cherchés. En général, la borne obtenue est assez fine et permet de conclure, cependant plusieurs obstacles peuvent survenir.

- La borne obtenue dans le théorème de Strassman sur le nombre de solutions p-adiques peut ne pas être optimale.

- Il peut exister une solution p-adique à la série formelle qui ne corresponde pas à un point de la courbe elliptique ayant une abscisse dans $\mathbb{Q}$. Dans ce cas la borne obtenue par le théorème de Strassman est optimale mais elle ne permet pas d'obtenir une borne optimale sur le nombre de points recherchés.

- Enfin la borne du théorème de Strassman peut être exacte et correspondre à un point recherché sur la courbe elliptique qu'on ne connaît pas à l'avance, parce qu'il est de hauteur trop grande par exemple.

Il existe cependant des moyens de faire face à ces obstacles. Il est en particulier possible de choisir un autre nombre premier p et de recommencer toute la procédure. On peut alors espérer pouvoir conclure avec ce nouveau choix. Étant donné que l'on travaille avec une certaine précision, le fait de choisir un grand nombre premier p ne complique pas particulièrement les calculs. Par contre il est nécessaire de calculer les points Q_i et plus le nombre premier p est grand, plus l'ordre d'annulation des points P_i modulo p est grand et donc plus les points Q_i sont difficiles à déterminer. On est donc quand même assez

rapidement limité quant au choix du nombre premier p.
D'autre part, même si le théorème de Strassman ne donne pas une borne exacte, il donne des renseignements locaux sur les points recherchés. Cela peut permettre de trouver plus rapidement un point jusque là inconnu car ayant une grande hauteur. Cela peut également permettre de conclure directement en revenant au problème initial et en y traduisant ces renseignements locaux. C'est cette remarque qui nous servira dans l'exemple exposé au paragraphe II.3.

Nous allons maintenant rapidement passer en revue les diverses méthodes connues pour ramener au problème de Chabauty elliptique un problème de calcul de points rationnels sur une courbe de rang supérieur ou égal au genre.

II.2 Quelques techniques de revêtement des courbes de genre 2

Dans ce paragraphe, nous exposons divers moyens pour se ramener du problème de Chabauty classique pour une courbe de genre 2 au problème de Chabauty elliptique dans les cas où la jacobienne de la courbe de genre 2 est de rang supérieur ou égal à 2 et où la méthode de Chabauty classique n'est donc pas applicable. Les deux premières méthodes utilisent des techniques de revêtement.

Le principe de telles méthodes est toujours le suivant : on trouve dans un premier temps une variété abélienne $\mathcal{A}$ qui s'envoie par une isogénie dans $\mathcal{J}$, la jacobienne de la courbe initiale $\mathcal{C}$. On choisit ensuite convenablement un ensemble de plongements de la courbe dans sa jacobienne. Leurs images réciproques par l'isogénie donne un ensemble de courbes sur la variété $\mathcal{A}$ dont les points rationnels recouvrent ceux de la courbe $\mathcal{C}$. Autrement dit, la connaissance de ces points rationnels entraîne la connaissance des points rationnels de $\mathcal{C}$. Bien sûr, si les choses ont été bien faites, le calcul des points rationnels de cette collection de courbes est plus simple que le calcul direct des points rationnels de $\mathcal{C}$. Ces méthodes nécessitent toutefois la connaissance préalable d'un certain homomorphisme μ que nous allons maintenant définir.

On considère une courbe de genre 2 générale définie sur un corps de nombres $\mathbf{k}$ par l'équation

$$\mathcal{C} : Y^2 = F(X) = f_6X^6 + f_5X^5 + \cdots + f_0 = F_1(X)\dots F_k(X) \ , \tag{II.10}$$

où f_6 est supposé non nul, F est sans facteurs multiples et $F_1 \dots F_k$ désignent les facteurs irréductibles de F. On note de plus α_i une racine de F_i pour tout $i \in \{1, \dots, k\}$ et L_i l'extension $\mathbf{k}(\alpha_i)$ de $\mathbf{k}$. On définit alors

$$\begin{array}{rrcl} \mu : & \mathcal{J}(\mathbf{k}) & \longrightarrow & (L_1^*/(L_1^*)^2 \times \cdots \times L_k^*/(L_k^*)^2) / \sim \ , \\ & \{[x_1, y_1], [x_2, y_2]\} & \longmapsto & [(x_1 - \alpha_1)(x_2 - \alpha_1), \dots, (x_1 - \alpha_k)(x_2 - \alpha_k)] \ , \end{array}$$

où $\mathcal{J}(\mathbf{k})$ désigne la jacobienne de la courbe $\mathcal{C}$ définie sur $\mathbf{k}$, $\{[x_1, y_1], [x_2, y_2]\}$ désigne un élément de la jacobienne représenté par un couple de points de la courbe conjugés sur une extension quadratique de $\mathbf{k}$ et $\sim$ est la relation d'équivalence définie par :

$$[a_1, \ldots, a_k] \sim [b_1, \ldots, b_k] \iff a_1 = wb_1, \ldots, a_k = wb_k, \text{ pour un certain } w \in \mathbf{k}^* \ .$$

Le lecteur familier avec le calcul du groupe de Mordell-Weil d'une courbe elliptique ne manquera pas de reconnaître ici une généralisation de l'application μ pour les courbes elliptiques qui permet de calculer le groupe de Selmer d'une courbe elliptique . Cette application est également la base du calcul du groupe de Mordell-Weil pour les jacobiennes de courbes de genre 2 [Sto 01]. Nous pouvons maintenant exposer deux méthodes de revêtement.

II.2.1 Revêtement par isogénies

Nous allons tout d'abord présenter la méthode, réécrite en termes de revêtements, utilisée par Flynn et Wetherell pour les courbes bielliptiques dans l'article où ils exposent la méthode de Chabauty elliptique [Fly-Wet 99] . On appelle courbe bielliptique, une courbe de genre 2 donnée par une équation du type

$$\mathcal{C} : Y^2 = G(X^2) \text{ avec } G(X) = (X - e_1)(X - e_2)(X - e_3) \ , \tag{II.11}$$

Dans les cas où le rang de la jacobienne d'une telle courbe est égal à 0 ou 1, la méthode de Chabauty classique [Fly 97] permet de conclure. Nous supposons donc que ce rang est au moins égal à 2.

Il existe alors des applications $[X, Y] \mapsto [X^2, Y]$ et $[X, Y] \mapsto \left[\frac{1}{X^2}, \frac{Y}{X^3}\right]$ de $\mathcal{C}$ dans les courbes elliptiques E^a et E^b définies par :

$$\begin{aligned} E^a \quad &: \quad Y^2 = G(X) = (X - e_1)(X - e_2)(X - e_3) \ , \\ E^b \quad &: \quad y^2 = x^3 G\left(\frac{1}{x}\right) = (1 - e_1 x)(1 - e_2 x)(1 - e_3 x) \ , \end{aligned}$$

comme décrit dans [Wet 97], si $\mathcal{A}$ désigne le produit des courbes elliptiques E^a et E^b, on a des isogénies $\phi : \mathcal{A} \to \mathcal{J}$ et $\phi' : \mathcal{J} \to \mathcal{A}$ dont la composition est la multiplication par 2. Ces isogénies sont données par :

$$\begin{aligned} \phi \quad &: \quad \{[X, Y], [x, y]\} \mapsto \left\{\left[\sqrt{X}, Y\right], \left[-\sqrt{X}, Y\right]\right\} + \left\{\left[\frac{1}{\sqrt{x}}, \frac{y}{x\sqrt{x}}\right], \left[-\frac{1}{\sqrt{x}}, -\frac{y}{x\sqrt{x}}\right]\right\} \ , \\ \phi' \quad &: \quad \{[X_1, Y_1], [X_2, Y_2]\} \mapsto \left\{[X_1^2, Y_1] + [X_2^2, Y_2], \left[\frac{1}{X_1^2}, \frac{Y_1}{X_1^3}\right] + \left[\frac{1}{X_2^2}, \frac{Y_2}{X_2^3}\right]\right\} \ . \end{aligned}$$

On définit alors un homomorphisme injectif μ_1 qui est un cas particulier de l'homomorphisme μ défini en début de paragraphe.

$$\begin{aligned} \mu_1 : \quad \mathcal{J}(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q})) &\to L_1^*/(L_1^*)^2 \times L_2^*/(L_2^*)^2 \times L_3^*/(L_3^*)^2 \\ \{[X_1, Y_1], [X_2, Y_2]\} &\mapsto [(X_1^2 - e_1)(X_2^2 - e_1), (X_1^2 - e_2)(X_2^2 - e_2), (X_1^2 - e_3)(X_2^2 - e_3)] \end{aligned}$$

où L_i est le corps $\mathbb{Q}(e_i)$.
Supposons désormais que, grâce à une descente, on ait déterminé

$$\mathcal{J}(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q})) = \{D_1, \ldots, D_m\} \ .$$

Soit alors $[X, Y]$ un point quelconque de $\mathcal{C}(\mathbb{Q})$. Il existe nécessairement un $i \in \{1, \ldots, m\}$ tel que $\{[X, Y], \infty^+\} = D_i$ dans $\mathcal{J}(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q}))$ et donc $\mu_1^{(j)}\{([X, Y], \infty^+\}) = \mu_1^{(j)}(D_i)$ pour $j = 1, 2, 3$ si $\mu_1^{(j)}$ est la $j^{\text{ème}}$ composante de l'homomorphisme μ_1. Autrement dit, pour $j = 1, 2, 3$, $X^2 - e_j = \mu_1^{(j)}(D_i)$ dans $L_j^*/(L_j^*)^2$. Comme $G(X^2)$ est également un carré d'après (II.11), il existe des $Y_{i,j}$ appartenant à L_j tels que

$$Y_{i,j}^2 = \mu_1^{(j)}(D_i) \frac{G(X^2)}{X^2 - e_j} \ .$$

En posant $y_{i,j} = XY_{i,j}$ et $x = X^2$, on obtient pour chaque i trois courbes elliptiques données par les équations :

$$y_{i,j}^2 = \mu_1^{(j)}(D_i) \frac{xG(x)}{x - e_j} \text{ pour } j = 1, 2, 3 \ ,$$

Cette collection de courbes elliptiques recouvre $\mathcal{C}(\mathbb{Q})$, autrement dit, la connaissance de tous les points rationnels de ces courbes ayant une abscisse dans $\mathbb{Q}$ entraîne alors la connaissance de tous les points de $\mathcal{C}(\mathbb{Q})$. Cette technique a permis à Wetherell [Wet 97] de résoudre l'un des rares problèmes de Diophante se ramenant au calcul des points rationnels sur une courbe de genre supérieur ou égal à 2 :

Théorème VII (Wetherell [Wet 97]) *Soit $\mathcal{C}$ la courbe de Diophante définie sur $\mathbb{Q}$ par l'équation :*

$$Y^2 = X^6 + X^2 + 1 \ ,$$

alors $\mathcal{C}(\mathbb{Q}) = \left\{\infty^+, \infty^-, [0, \pm 1], \left[\frac{1}{2}, \pm\frac{9}{8}\right], \left[-\frac{1}{2}, \pm\frac{9}{8}\right]\right\}$.
Après une légère modification, cette méthode a aussi permis à Flynn [Fly 01] de calculer tous les points rationnels de la courbe définie par l'équation

$$Y^2 = (X^2 + 15)(X^2 + 45)(X^2 + 135) \ ,$$

ce qui lui permet de démontrer qu'il n'existe pas de polynôme $\mathbb{Q}$-dérivé ayant une racine triple et deux racines simples (un polynôme $\mathbb{Q}$-dérivé est un polynôme défini sur $\mathbb{Q}$ dont toutes les dérivées ont toutes leurs racines dans $\mathbb{Q}$).

II.2.2 Revêtement par la multiplication par 2

Ce paragraphe utilise des idées de Bruin [Bru 99] et des variations de Flynn et Wetherell [Fly-Wet 99], [Fly-Wet 01].
Soit $\mathcal{C}$ une courbe de genre 2 comme définie en (II.10) et soit μ l'homomorphisme défini

précédemment. On suppose dans la suite qu'on connaît un ensemble de représentants de $\mathcal{J}(\mathbf{k})/2\mathcal{J}(\mathbf{k})$. Il est alors facile d'en déduire $\mathcal{J}(\mathbf{k})/\ker(\mu)$ (en effet $2\mathcal{J}(\mathbf{k})$ est soit le noyau de μ, soit d'indice 2 dans $\ker(\mu)$). On peut donc écrire :

$$\mathcal{J}(\mathbf{k})/\ker(\mu) = \{D_1, \dots, D_m\} \ .$$

Soit $[X, Y]$ un point de $\mathcal{C}(\mathbf{k})$, $\{[X, Y], \infty^+\}$ est alors un diviseur rationnel de la jacobienne de $\mathcal{C}$. Il existe donc nécessairement un $i \in \{1, \dots, m\}$ tel que $\mu(\{[X, Y], \infty^+\}) = \mu(D_i)$. De plus, pour tout polynôme de degré pair $G(x)$ divisant $F(x)$, il existe une application induite par μ, que nous noterons μ_G :

$$\begin{array}{rccc} \mu_G : & \mathcal{J}(\mathbf{k}) & \longrightarrow & L_G^*/(L_G^*)^2 \ , \\ & \displaystyle\sum_{j=1}^{\ell} n_j [x_j, y_j] & \longmapsto & \displaystyle\prod_{j=1}^{\ell} G(x_j)^{n_j} \ , \end{array}$$

où L_G est la plus petite extension du corps $\mathbf{k}$ sur laquelle le polynôme G est défini. Il s'ensuit alors que $\mu_G(D_i)G(X)$ doit être un carré de L_G^*. Ainsi, chaque choix du polynôme G de degré pair divisant F donne une courbe hyperelliptique définie sur L_G par l'équation $y^2 = \mu_G(D_i)G(x)$. Sur chacune de ces courbes, il doit y avoir un point rationnel dont l'abscisse est dans le corps de base $\mathbf{k}$. Dans le cas où le degré de G vaut 4, la courbe obtenue de cette manière est une courbe elliptique et on peut espérer lui appliquer la méthode de Chabauty elliptique.

Remarque : Dans le paragraphe II.1 nous avons considéré le problème de Chabauty elliptique sur $\mathbb{Q}$ par souci de simplicité. Cette méthode est en effet valable sur n'importe quel corps de nombres à la condition cependant que celui ci soit suffisamment petit pour pouvoir y effectuer les calculs nécessaires.

Cette technique a été récemment appliquée par Flynn et Wetherell [Fly-Wet 01] pour résoudre l'équation de Serre : $x^4 + y^4 = 17$. Il est en effet démontré dans [Cas-Fly 96] qu'il est pour cela suffisant de trouver tous les points rationnels de la courbe hyperelliptique définie sur $\mathbb{Q}$ par l'équation :

$$Y^2 = (9X^2 - 28X + 18)(X^2 + 12X + 2)(X^2 - 2) \ ,$$

En appliquant cette technique de revêtement à cette courbe, on montre qu'on peut se ramener à trouver les points rationnels sur une courbe elliptique définie sur $\mathbb{Q}(\sqrt{2}, \sqrt{17})$ ayant une abscisse dans $\mathbb{Q}$ et la méthode de Chabauty elliptique permet de conclure.

Théorème VIII (Flynn-Wetherell [Fly-Wet 01]) *Les seuls nombres rationnels x et y vérifiant $x^4 + y^4 = 17$ sont les couples $(\pm 1, \pm 2)$ et $(\pm 2, \pm 1)$.*

Remarque : Ces méthodes de revêtement, sont toutes basées sur le même principe et on peut en imaginer de nouvelles. On pourrait par exemple regarder les revêtements définis par la multiplication par 4. Cependant de telles méthodes n'auraient que peu d'intérêt sans exemple pour les illustrer.

Nous allons maintenant exposer rapidement une dernière méthode permettant de ramener le problème qui consiste à trouver les points rationnels sur une courbe hyperelliptique au problème de Chabauty elliptique.

II.2.3 Utilisation des résultants

Étant donné que nous allons utiliser et détailler cette méthode dans les deux prochains paragraphes, nous n'en donnerons ici qu'une description approximative. C'est une approche plus classique et ne nécessitant pas la connaissance des outils complexes des paragraphes précédents. Le principe est le suivant :
Soit $\mathcal{C}$ une courbe hyperelliptique (non nécessairement de genre 2) définie sur $\mathbb{Q}$ (bien qu'on pourrait prendre un corps de nombres quelconque comme corps de base) par une équation du type

$$\mathcal{C} : Y^2 = F(X) = F_1(X)F_2(X) \ ,$$

où $F(x)$ est sans facteur carré de degré supérieur à 6, $F_1(X)$ et $F_2(X)$ sont des polynômes définis sur une extension $\mathbf{k}$ de $\mathbb{Q}$ et le degré de $F_1(X)$ vaut 3 ou 4.
Dans ces conditions, si $[X, Y]$ est un point de $\mathcal{C}(\mathbb{Q})$, il existe y_1, y_2 et α des éléments de $\mathbf{k}$ tels que l'on ait simultanément

$$\begin{cases} \alpha\, y_1^2 &= F_1(X) \ , \\ \alpha\, y_2^2 &= F_2(X) \ . \end{cases}$$

Il est évident que α peut être choisi sans facteur carré. On peut de plus démontrer (voir par exemple [Bru 99] lemme 2.2.1) qu'on peut choisir α qui divise le résultant des polynômes $F_1(X)$ et $F_2(X)$ de telle sorte que α appartienne à un ensemble fini. Quelques astuces permettent dans un premier temps de réduire cet ensemble fini de valeurs possibles pour α. Ces valeurs de α donnent alors un nombre fini de courbes elliptiques définies sur $\mathbf{k}$ par les équations :

$$E_\alpha \ : \ y^2 = \alpha F_1(X) \ .$$

Ces courbes doivent alors posséder un point de $E_\alpha(\mathbf{k})$ ayant une abscisse dans $\mathbb{Q}$, qui correspond à l'abscisse d'un point rationnel sur la courbe $\mathcal{C}$. On a de cette façon ramené le problème qui consiste à trouver des points rationnels de $\mathcal{C}(\mathbb{Q})$ qui consiste à trouver des points de $E_\alpha(\mathbf{k})$ ayant une abscisse dans $\mathbb{Q}$ pour une famille finie de courbes elliptiques E_α.

C'est cette stratégie qui a permis à Bruin [Bru 99] de résoudre le problème diophantien suivant :

Théorème IX (Bruin [Bru 99]) *Les seuls entiers relatifs x, y et z premiers entre eux, tels que $xyz \neq 0$ et satisfaisant l'équation $x^8 + y^3 = z^2$ sont*

$$(x, y, z) = (\pm 1, 2, \pm 3), \ (\pm 43, 96222, \pm 3004207).$$

II.3 Exemple

Dans ce paragraphe, nous appliquons la méthode de Chabauty elliptique exposée au paragraphe II.1 afin de démontrer le théorème suivant

Théorème X *Soit $\mathcal{C}$ la courbe hyperelliptique définie par l'équation*

$$y^2 = (x^2+1)(x^2+3)(x^2+7) \ .$$

Les points rationnels de cette courbe sont donnés par

$$\mathcal{C}(\mathbb{Q}) = \{\infty^+, \infty^-, [1,8], [1,-8], [-1,8], [-1,-8]\} \ .$$

Cette courbe est une courbe bielliptique. Elle a été introduite par Flynn et Wetherell dans [Fly-Wet 99] avec une cinquantaine d'autres courbes semi-aléatoires afin de tester leur méthode pour trouver les points rationnels sur une courbe bielliptique que nous avons brièvement exposé au paragraphe II.2.1. Cette courbe était la seule pour laquelle Flynn et Wetherell n'avaient pas réussi à conclure. Nous avons donc employé une autre méthode, celle des résultants, pour calculer tous les points rationnels de cette courbe.

Nous allons pour cela travailler sur le corps de nombres $\mathbb{Q}(i)$. Sur ce corps, le polynôme définissant la courbe $\mathcal{C}$ peut être factorisé, de telle sorte que $\mathcal{C}$ puisse être définie par l'équation :

$$y^2 = (x^2+3)(x+i)(x-i)(x^2+7) \ .$$

Supposons maintenant que $[x,y]$ soit un point de $\mathcal{C}(\mathbb{Q})$, alors il existe y_1, y_2 et α des éléments de $\mathbb{Q}(i)$ tels que l'on ait simultanément :

$$\begin{aligned} \alpha y_1^2 &= (x^2+3)(x+i) \ , \\ \alpha y_2^2 &= (x^2+7)(x-i) \ . \end{aligned}$$

Le résultant de $(x^2+3)(x+i)$ et de $(x^2+7)(x-i)$ est égal à $-2^7 3i$ de telle sorte que si $y \neq 0, \infty$, on peut supposer , sans aucune perte de généralité, que α est une $\{2,3\}$-unité sans facteur carré dans $\mathbb{Q}(i)$. Les $\{2,3\}$-unités de $\mathbb{Q}(i)$ sont engendrées par i, $1+i$ et 3. On peut donc écrire toutes les $\{2,3\}$-unités sans facteur carré dans $\mathbb{Q}(i)$, autrement dit toutes les valeurs que α peut prendre :

$$\alpha \in \{1, i, 1+i, 3, 1-i, 3i, 3(1+i), 3(1-i)\}.$$

Nous allons tout d'abord essayer de réduire cet ensemble. Il faut donc tester pour lesquelles de ces valeurs possibles de α, il existe un x dans $\mathbb{Q}$ tel que $\alpha(x^2+3)(x+i)$ et $\alpha(x^2+7)(x-i)$ soient des carrés de $\mathbb{Q}(i)$ simultanément. On peut par exemple regarder le problème localement et il suffit en fait de travailler modulo 9 pour démontrer que cela n'est possible que si $\alpha = 1+i$ ou $\alpha = 1-i$.

Supposons dans un premier temps que $\alpha = 1 - i$, il est naturel de définir les courbes elliptiques suivantes définies sur $\mathbb{Q}(i)$:

$$\begin{array}{rcl} E_1 \; : \; y_1^2 & = & (1-i)(x^2+3)(x+i) \; . \\ E_2 \; : \; y_2^2 & = & (1-i)(x^2+7)(x-i) \; . \end{array}$$

Dans ce cas, on peut résumer la situation de la façon suivante :
Si $[x, y]$ est un point rationnel de $\mathcal{C}(\mathbb{Q})$, il existe deux éléments y_1 et y_2 de $\mathbb{Q}(i)$ tels que le point $[x, y_1]$ appartienne à $E_1(\mathbb{Q}(i))$ et le point $[x, y_2]$ appartienne à $E_2(\mathbb{Q}(i))$. Autrement dit si $[x, y]$ est un point rationnel de $\mathcal{C}(\mathbb{Q})$, il correspond à un point de $E_1(\mathbb{Q}(i))$ ayant une abscisse dans $\mathbb{Q}$ ainsi qu'à un point de $E_2(\mathbb{Q}(i))$ ayant une abscisse dans $\mathbb{Q}$. Ainsi, si on sait appliquer la méthode de Chabauty elliptique sur l'une des deux courbes E_1 ou E_2 définies sur $\mathbb{Q}(i)$, on saura trouver tous les points rationnels sur la courbe $\mathcal{C}$.

Remarque : En ce qui concerne le cas de $\alpha = 1 + i$, après un changement de variables de x en $-x$ et de y en iy, on obtient les conjuguées des courbes E_1 et E_2. Comme notre but est de trouver les points dont l'abscisse est dans $\mathbb{Q}$ et que nous serons seulement intéressés par x^2 (pour trouver les points rationnels de $\mathcal{C}(\mathbb{Q})$), il ne sera pas nécessaire de considérer ce cas.

Nous calculons donc le rang des courbes elliptiques E_1 et E_2 définies sur $\mathbb{Q}(i)$ à l'aide du programme développé par Simon [Sim]. La courbe E_1 est de rang 2 et la méthode de Chabauty elliptique ne peut donc pas lui être appliquée car elle est définie sur le corps $\mathbb{Q}(i)$ de degré 2 sur $\mathbb{Q}$. Heureusement, la courbe E_2 est de rang 1 sur $\mathbb{Q}(i)$ et on peut donc lui appliquer la méthode de Chabauty elliptique afin d'en trouver tous les points d'abscisse dans $\mathbb{Q}$.

Proposition II.3.1 *Soit E_2 la courbe elliptique définie sur $\mathbb{Q}(i)$ par l'équation*

$$E_2 \; : \; y_2^2 = (1-i)(x^2+7)(x-i) \; .$$

Les points rationnels de $E_2(\mathbb{Q}(i))$ ayant une abscisse dans $\mathbb{Q}$ sont exactement le point à l'infini, les points $[-1, \pm 4i]$ et au plus un point P tel que $P = \pm 2[4i-3, 12] + [i, 0] + nQ$ où Q est dans le noyau de la réduction modulo 11.

Remarque : Comme on peut le voir dans cette proposition, la méthode de Chabauty elliptique ne permet pas ici de conclure directement au problème qui consiste à trouver exactement tous les points de $E_2(\mathbb{Q}(i))$ ayant une abscisse dans $\mathbb{Q}$. Cependant les informations fournies suffiront à résoudre le problème initial du théorème X.

Preuve : La première chose à faire pour appliquer la méthode de Chabauty elliptique est de calculer la structure du groupe de Mordell-Weil de la courbe elliptique considérée. Dans le cas qui nous occupe, le groupe de torsion de $E_2(\mathbb{Q}(i))$ est $\{\infty, [i, 0]\}$ et un générateur de la partie libre du groupe de Mordell-Weil est $[4i-3, 12]$.

Choisissons maintenant un nombre premier p qui satisfasse les six conditions exposées au paragraphe II.1. Les nombres premiers 11, 19 et 23 conviennent et nous allons tout d'abord considérer le cas $p = 11$. On note $G = [4i - 3, 12]$ un générateur obtenu à l'aide du programme de Simon [Sim]. Notons $\widetilde{E_2}$ la réduction modulo 11 de la courbe elliptique E_2. L'ordre du point $\widetilde{G}$, réduction de G modulo 11, sur $\widetilde{E_2}$ vaut alors 5. On définit donc, en suivant la méthode de Chabauty elliptique :

- $m = 5$,
- $Q = 5G$,
- z la z-coordonnée de Q $\left(z = -\frac{x}{y} \text{ si } Q = [x, y]\right)$,
- $\mathcal{U} = \{\infty, [i, 0], \pm G, \pm 2G, \pm G + [i, 0], \pm 2G + [i, 0]\}$,

de telle sorte que tout point P de $E_2(\mathbb{Q}(i))$ peut s'écrire sous la forme $P = U + nQ$ pour un certain U dans l'ensemble fini $\mathcal{U}$ et un certain n dans $\mathbb{Z}$. Nous allons maintenant employer quelques astuces classiques pour réduire l'ensemble $\mathcal{U}$.

> D'une part, comme Q est dans le noyau de la réduction modulo 11, $\widetilde{P} = \widetilde{U}$. Ainsi, si P a une abscisse dans $\mathbb{Q}$, alors $\widetilde{U}$ a une abscisse dans $\mathbb{F}_{11}$. Il n'est donc pas nécessaire d'effectuer les calculs qui vont suivre pour les éléments de $\mathcal{U}$ dont la réduction modulo 11 n'a pas une abscisse dans $\mathbb{F}_{11}$. Finalement, seuls le point à l'infini et les points $\pm G + [i, 0]$ et $\pm 2G + [i, 0]$ seront à considérer.
>
> D'autre part, n étant choisi dans $\mathbb{Z}$ et $[i, 0]$ étant un point de 2-torsion, si le calcul a été fait pour $U = G + [i, 0]$ et pour $U = 2G + [i, 0]$, il n'est pas nécessaire de le refaire pour $U = -G + [i, 0]$ et pour $U = -2G + [i, 0]$. Les points U à considérer sont donc finalement le point à l'infini, et les points $G + [i, 0]$ et $2G + [i, 0]$. L'utilisation de cette astuce explique pourquoi l'ensemble $\mathcal{U}$ a été défini de cette façon et non pas par
>
> $$\{T + k_1 P_1 + \cdots + k_r P_r : T \in E(\mathbb{Q}(\alpha))_{\text{tors}}, 0 \leqslant k_i \leqslant m_i - 1\} \quad .$$
>
> ce qui aurait pu paraître plus naturel à priori.

Dans toute la suite, il sera suffisant de travailler modulo 11^5. De plus, grâce au fait que le produit du coefficient de t^k dans $\operatorname{Log}(t)$ ou $\operatorname{Exp}(t)$ et de $k!$ appartient à $\mathbb{Z}[i]$ et grâce à l'estimation standard $|k!|_p \geqslant p^{-\frac{k-1}{p-1}}$, les termes en $O(z^7)$ peuvent être ignorés dans les formules. Soit $\theta_\infty(n)$ l'inverse de l'abscisse du point nQ exprimé comme une série formelle en n et $\theta_U(n)$ l'abscisse du point $U + nQ$ si U n'est pas le point à l'infini exprimé pareillement. Dans tous les cas, on peut séparer la série formelle θ_U en partie réelle et partie imaginaire:

$$\theta_U(n) = \theta_U^{(0)}(n) + \theta_U^{(1)}(n) i.$$

Si l'abscisse du point P est dans $\mathbb{Q}$, alors la partie imaginaire $\theta_U^{(1)}(n)$ doit être nulle. Ainsi, il nous faut déterminer, pour chacun des trois points U quels sont les entiers n tels que

$\theta_U^{(1)}(n) = 0$. On commence par calculer la z-coordonnée de $Q \pmod{11^5}$:

$$z = 11(10763 + 7311i) \pmod{11^5} \ ,$$

puis son logarithme formel :

$$\mathrm{Log}(z) = 11(1446 + 5496i) \pmod{11^5} \ .$$

On remplace maintenant z par $n\mathrm{Log}(z)$ dans l'expression de l'exponentielle formelle et on obtient ainsi la z-coordonnée du point nQ modulo 11^5

$$z\text{-coordonnée}(nQ) = 11(1446 + 5496i)n + 11^3(77 + 15i)n^3 \pmod{11^5} \ .$$

On en déduit alors les séries formelles

$$\begin{aligned}
\theta_\infty(n) &= 11^2(574 + 17i)n^2 + 11^4(8 + 7i)n^4 \pmod{11^5} \ , \\
\theta_{G+[i,0]}(n) &= -1 + 11(45 + 3073i)n + 11^2(382 + 1318i)n^2 + \\
&\qquad 11^3(68 + 16i)n^3 + 11^4(10 + 5i)n^4 \pmod{11^5} \ , \\
\theta_{2G+[i,0]}(n) &= 154608 + 11\,10541i + 11(1484 + 10609i)n + 11^2(445 + 247i)n^2 + \\
&\qquad 11^3(115 + 93i)n^3 + 11^4(7 + 8i)n^4 \pmod{11^5} \ .
\end{aligned}$$

On extrait ensuite de ces séries formelles leur partie imaginaire :

$$\begin{aligned}
\theta_\infty^{(1)}(n) &= 11^2 17n^2 + 11^4 7n^4 \pmod{11^5} \ , \\
\theta_{G+[i,0]}^{(1)}(n) &= 11\,3073n + 11^2 1318n^2 + 11^3 16n^3 + 11^4 5n^4 \pmod{11^5} \ , \\
\theta_{2G+[i,0]}^{(1)}(n) &= 11\,10541 + 11\,10609n + 11^2 247n^2 + 11^3 93n^3 + 11^4 8n^4 \pmod{11^5} \ .
\end{aligned}$$

Nous aimerions désormais savoir, pour combien de valeurs de n ces séries formelles peuvent s'annuler. Nous allons donc appliquer le théorème de Strassman.

– Pour le point à l'infini, nous appliquons le théorème de Strassman à la série formelle

$$\frac{\theta_\infty^{(1)}(n)}{n^2} = 11^2 17 + 11^4 7n^2 \pmod{11^5}$$

si n n'est pas nul. La valuation 11-adique de premier coefficient vaut 2, celle du second coefficient vaut 4 et celle de tous les autres coefficients est supérieure à 5. Ainsi, le coefficient de plus petite valuation 11-adique est le coefficient constant, ce qui signifie, d'après le théorème de Strassman, que $\frac{\theta_\infty^{(1)}(n)}{n^2} = 0$ n'a pas de solution 11-adique et donc n'a pas de solution dans $\mathbb{Z}$. La seule solution possible à $\theta_\infty^{(1)}(n) = 0$ est donc la solution $n = 0$ qui correspond, sur la courbe elliptique, au point à l'infini. Dans le cas où U est le point à l'infini, tout se passe donc bien.

- En ce qui concerne le point $U = G + [i, 0]$, on applique directement le théorème de Strassman à la série formelle $\theta^{(1)}_{G+[i,0]}$. Le coefficient de plus petite valuation 11-adique est le coefficient en n. Le théorème de Strassman permet alors de conclure qu'il existe au plus une solution dans $\mathbb{Z}_{11}$ à l'équation $\theta^{(1)}_{G+[i,0]} = 0$. Or on sait déjà que $n = 0$ est solution de cette équation. Le théorème de Strassman prouve donc que c'est la seule. Cette solution correspond sur la courbe elliptique au point $[-1, -4i]$ qui a bien une abscisse dans $\mathbb{Q}$. Pour ce choix de U aussi, la méthode de Chabauty elliptique s'applique parfaitement.

- Reste maintenant à considérer le cas $U = 2G + [i, 0]$. Les deux premiers coefficients de la série formelle $\theta^{(1)}_{2G+[i,0]}$ sont de valuation 11-adique égale à 1 et tous les autres coefficients ont une valuation 11-adique supérieure à 2 si bien que le théorème de Strassman montre dans ce cas que l'équation $\theta^{(1)}_{2G+[i,0]}(n) = 0$ possède au plus une solution dans $\mathbb{Z}_{11}$. Le problème qui se pose dans ce cas est que nous ne connaissons aucune solution à cette série formelle. Nous ne connaissons pas non plus de point sur $E_2(\mathbb{Q}(i))$ ayant une abscisse dans $\mathbb{Q}$ et de la forme $2G + [i, 0] + nQ$. Autrement dit la borne obtenue par le théorème de Strassman n'est visiblement pas optimale pour ce choix de point U.

La méthode de Chabauty elliptique a ainsi échoué dans ce cas et ne nous a pas permis de trouver tous les points de $E_2(\mathbb{Q}(i))$ ayant une abscisse dans $\mathbb{Q}$. Cependant la méthode nous a tout de même permis de montrer que les points de $E_2(\mathbb{Q}(i))$ ayant une abscisse dans $\mathbb{Q}$ étaient : le point à l'infini, les points $[-1, \pm 4i]$ et au plus un point P_0 (et son opposé) de la forme $P_0 = \pm 2G + [i, 0] + nQ$ avec n dans $\mathbb{Z}$ et $G = [4i - 3, 12]$. □

Remarque : Il est important de noter ici, que la méthode de Chabauty elliptique a non seulement échouée pour le nombre premier 11 mais elle échoue aussi pour les nombres premiers 19 et 23 qui satisfont également aux 6 conditions énoncées dans le paragraphe II.1. En effet, la première chose à faire quand cette méthode échoue est de la recommencer avec un autre nombre premier. En ce qui concerne le nombre premier suivant (31), les calculs sur la courbe elliptique deviennent trop longs et nous n'avons donc pas testé la méthode pour $p = 31$.

Nous pouvons maintenant, grâce à cette proposition, terminer la preuve du théorème X. L'idéal aurait été que la méthode de Chabauty elliptique nous donne tous les points désirés. Ce n'est cependant pas le cas, mais voyons maintenant ce que cette méthode nous permet de déduire sur la courbe hyperelliptique $\mathcal{C}$.
Le point à l'infini sur la courbe elliptique correspond aux points à l'infini sur la courbe $\mathcal{C}$. Les points $[-1, \pm 4i]$ sur la courbe elliptique correspondent aux points $[1, \pm 8]$ et $[-1, \pm 8]$ sur la courbe $\mathcal{C}$. Il ne nous reste plus qu'à prouver que si P_0 est un point de $E_2(\mathbb{Q}(i))$ ayant une abscisse x_0 dans $\mathbb{Q}$ et de la forme $P_0 = \pm 2[4i - 3, 12] + [i, 0] + nQ$ avec n dans $\mathbb{Z}$, alors il ne peut pas correspondre à un point rationnel sur la courbe hyperelliptique $\mathcal{C}$,

c'est à dire qu'un tel x_0 ne peut pas être l'abscisse d'un point rationnel de $\mathcal{C}$. Il est trivial de voir que le point $\pm 2[4i-3, 12]+[i, 0]$ doit avoir une abscisse égale à $-\frac{24}{25}-\frac{143i}{25}$. Comme Q est dans le noyau de la réduction modulo 11, l'abscisse d'un tel point P_0 doit également être égale à $-\frac{24}{25}-\frac{143i}{25}$ modulo 11. C'est à dire que x_0 doit être égal à 3 modulo 11. En remplaçant x par x_0 dans notre équation $y^2=(x^2+1)(x^2+3)(x^2+7)$ définissant la courbe $\mathcal{C}$, on déduit que si x_0 est l'abscisse d'un point de $\mathcal{C}(\mathbb{Q})$ alors l'ordonnée y_0 de ce point doit vérifier $y_0^2 = 6 \pmod{11}$. Le fait que 6 ne soit pas un carré modulo 11 nous permet de montrer qu'un tel x_0 ne peut pas être l'abscisse d'un point de $\mathcal{C}(\mathbb{Q})$. On conclut donc que les seuls points rationnels de $\mathcal{C}$ sont les points à l'infini et les points $[1, 8]$, $[1, -8]$, $[-1, 8]$ et $[-1, -8]$.

II.4 Points rationnels sur les courbes hyperelliptiques et un théorème de préparation de Weierstrass explicite

Comme nous l'avons expliqué dans les paragraphes précédents, la méthode de Chabauty elliptique permet de calculer les points rationnels d'une courbe de genre 2 pour laquelle la méthode de Chabauty classique ne s'applique pas, c'est à dire lorsque le rang de la jacobienne est supérieur au genre de la courbe.
Le principe est de ramener le problème au calcul des points rationnels d'une courbe elliptique définie sur un corps de nombres ayant une abscisse dans $\mathbb{Q}$. L'outil de base de cette méthode est le théorème de Strassman qui permet de borner le nombre de solutions p-adique d'une série formelle en une seule variable quand la courbe elliptique obtenue par cette technique est de rang 1.
Flynn et Wetherell ont donnés plusieurs exemples d'application de cette méthode dans le cas où les courbes elliptiques sont de rang 1, mais n'en donnent aucun quand elles sont de rang supérieur. Dans ce cas, on doit savoir borner les solutions p-adique de systèmes de séries formelle en plusieurs variables. Flynn et Wetherell suggèrent alors l'utilisation du théorème de préparation de Weierstrass. On peut toutefois trouver des exemples d'application de la méthode de Chabauty elliptique dans le cas où la courbe elliptique obtenue est de rang 2 dans [Bru 99]. Cependant, pour ces exemples, le théorème de Strassman est suffisant pour conclure, ce qui n'est pas réalisable en général.

Le but de ce paragraphe est d'écrire une version effective du théorème de préparation de Weierstrass afin de pouvoir appliquer la méthode de Chabauty elliptique dans les cas où la courbe elliptique obtenue est de rang supérieur ou égal à 2. Nous illustrerons cette méthode à l'aide de l'exemple suivant.

II.4.1 Exemple d'une courbe hyperelliptique de genre 4 dont la jacobienne est de rang 4

Théorème XI *Soit $\mathcal{C}$ la courbe hyperelliptique définie sur $\mathbb{Q}$ par l'équation*

$$y^2 = x^9 - 6x^8 + 31x^7 - 81x^6 + 177x^5 - 176x^4 - 9x^3 + 107x^2 + 19x + 1 \ .$$

Alors $\mathcal{C}(\mathbb{Q}) = \{\infty, (1, \pm 8), (0, \pm 1)\}$.

Remarque : La courbe $\mathcal{C}$ est une courbe hyperelliptique de genre 4. En utilisant le programme `magma` de Stoll [Sto 01] (inclus dans les versions supérieures à 2.7 de `magma`), on peut voir que le rang de la jacobienne de cette courbe est égal à 4. Ce rang étant égal au genre de la courbe, on ne peut pas appliquer la méthode de Chabauty standard. Dans ce cas, en effet, seul le théorème de Faltings nous permet d'affirmer que le nombre de points rationnels sur une telle courbe est fini. Ce dernier n'étant pas explicite, nous devons employer une autre technique afin de démontrer le théorème XI.
Nous allons donc utiliser la méthode des résultants (exposée au paragraphe II.2.3) afin de nous ramener à la méthode de Chabauty elliptique. Pour cela nous devons factoriser le polynôme définissant la courbe $\mathcal{C}$ sur un certain corps de nombres.
Soit donc $\mathbf{k}$ le corps de nombres $\mathbb{Q}(\beta)$, où β est une racine du polynôme $x^3 + 2x + 1$. Il est possible de factoriser le polynôme f définissant la courbe $\mathcal{C}$ sur ce corps de nombres de la manière suivante :

$$f(x) \ = \ f_1(x) f_2(x) \ ,$$

avec

$$\begin{aligned} f_1(x) &= x^3 - 2x^2 + (-4\beta^2 - \beta + 1)x + 1 \ . \\ f_2(x) &= x^6 - 4x^5 + (4\beta^2 + \beta + 22)x^4 + (-8\beta^2 - 2\beta - 34)x^3 + \\ & \qquad (37\beta^2 - 15\beta + 83)x^2 + (4\beta^2 + \beta + 18)x + 1 \ . \end{aligned}$$

Soit alors $[X, Y]$ un point rationnel appartenant à $\mathcal{C}(\mathbb{Q})$. Étant donné que $\mathbf{k}$ a un nombre de classes égal à 1, il existe des éléments Y_1, Y_2 et α du corps de nombres $\mathbf{k}$ qui vérifient :

$$\begin{aligned} \alpha \, Y_1^2 &= f_1(X) \ , \\ \alpha \, Y_2^2 &= f_2(X) \ . \end{aligned}$$

Remarquons tout d'abord qu'il n'existe pas de point de Weierstrass sur la courbe $\mathcal{C}$. On peut donc supposer que si $[X, Y]$ est un point appartenant à $\mathcal{C}(\mathbb{Q})$, son ordonnée Y est non nulle. D'autre part, la solution avec Y infini correspond au point à l'infini, bien connu, de la courbe $\mathcal{C}$, autrement dit on supposera aussi que Y n'est pas infini. Le résultant des polynômes $f_1(x)$ et $f_2(x)$ est égal à :

$$\mathrm{Res}(f_1(x), f_2(x)) = (-4 + 3\beta - 2\beta^2)^3(-16 + \beta + 4\beta^2)^3 \ ,$$

de telle sorte que, comme on a supposé Y non nul et fini, sans aucune perte de généralité, on peut choisir α sans facteur carré et divisant le résultant $\mathrm{Res}(f_1(x), f_2(x))$. Autrement dit nous pouvons choisir α appartenant à un système de représentants des $\{2,(-4+3\beta-2\beta^2),(-16+\beta+4\beta^2)\}$-unités de $\mathbf{k}$ modulo les carrés de $\mathbf{k}$. Or, les unités du corps de nombres $\mathbf{k}$ sont engendrées par :

$$U(\mathbf{k}) = \left\langle -1, \beta, 1+\beta, 1+\beta+\beta^2, -4+3\beta-2\beta^2, -16+\beta+4\beta^2 \right\rangle \ .$$

On peut alors calculer explicitement toutes les $\{2,(-4+3\beta-2\beta^2),(-16+\beta+4\beta^2)\}$-unités de $\mathbf{k}$ qui sont sans facteur carré. Il y en a au total 64 et nous ne les avons donc pas écrites ici. Ainsi α peut prendre 64 valeurs. Nous allons, dans un premier temps, réduire le nombre des valeurs possibles pour α. Pour cela, nous regardons pour lesquelles de ces $\{2,(-4+3\beta-2\beta^2),(-16+\beta+4\beta^2)\}$-unités α il existe un nombre rationnel x tel que $\alpha f_1(x)$ et $\alpha f_2(x)$ soient simultanément des carrés dans $\mathbf{k}$ et ce localement. Il suffit en fait de rechercher lesquels de ces α vérifient cette propriété modulo 32. En effet, $\alpha f_1(x)$ et $\alpha f_2(x)$ ne sont jamais simultanément des carrés modulo 32 pour les 63 valeurs de α différentes de 1.

On a ainsi démontré que $\alpha = 1$ est la seule valeur à considérer. On peut donc résumer ce que nous venons de démontrer en écrivant que si $[X, Y]$ est un point rationnel de $\mathcal{C}(\mathbb{Q})$, il existe deux éléments Y_1 et Y_2 dans $\mathbf{k}$ tels que l'on ait simultanément :

$$\begin{aligned} Y_1^2 &= f_1(X) \ , \\ Y_2^2 &= f_2(X) \ . \end{aligned}$$

En particulier, cela signifie que si $[X, Y]$ est un point rationnel sur la courbe $\mathcal{C}$, alors $[X, Y_1]$ est un point rationnel appartenant à la courbe elliptique E définie sur le corps de nombres $\mathbf{k}$ par l'équation :

$$E \ : \ y^2 = f_1(x) = x^3 - 2x^2 + (-4\beta^2 - \beta + 1)x + 1 \ , \tag{II.12}$$

et ayant une abscisse dans $\mathbb{Q}$.
Ainsi la connaissance de tous les points de $E(\mathbf{k})$ ayant une abscisse dans $\mathbb{Q}$ entraînera la connaissance de tous les points rationnels sur la courbe hyperelliptique $\mathcal{C}$.

Notre but est donc de résoudre le problème de Chabauty elliptique pour cette courbe elliptique E définie sur $\mathbf{k}$ un corps de nombres de degré 3 sur $\mathbb{Q}$.
Comme nous l'avons vu dans le paragraphe II.1, si le rang de cette courbe elliptique est égal à 1, la méthode de Chabauty elliptique permet de réduire ce problème à celui de borner le nombre de solutions p-adiques d'une série formelle en une variable. Le théorème de Strassman permet alors de conclure dans la plupart des cas. Dans notre cas cependant, le rang de la courbe elliptique sur $\mathbf{k}$ est égal à 2, si bien que si nous suivons la méthode de Chabauty elliptique, nous devrons borner le nombre de solutions p-adiques d'un système de deux séries formelles en deux variables. Nous avons donc pour cela besoin d'une généralisation du théorème de Strassman pour les systèmes de séries formelles en deux variables. Cette généralisation nous est apportée par le théorème de préparation de Weierstrass, puisque le théorème de Strassman n'en est qu'un cas particulier.

II.4.2 Le théorème de préparation de Weierstrass en 2 variables

Dans ce paragraphe, nous réécrivons dans le cas $n = 2$ le théorème de préparation de Weierstrass en n variables exposé par Sugatani dans [Sug 81].

Comme dans l'article de Sugatani, nous définissons $\mathbb{Z}_p \langle n_1, n_2 \rangle$ l'ensemble des séries formelles en les deux variables n_1 et n_2 dont les coefficients appartiennent à $\mathbb{Z}_p$ et qui peuvent s'écrire sous la forme :

$$f = \sum_{(i,j)=(0,0)}^{\infty} f_{(i,j)} n_1^i n_2^j \ ,$$

avec $f_{(i,j)} \in \mathbb{Z}_p$ et $\left|f_{(i,j)}\right|_p \to 0$ lorsque $i + j \to \infty$.
Cette dernière condition sur les coefficients nous permet alors de définir une norme sur $\mathbb{Z}_p \langle n_1, n_2 \rangle$ donnée par :

$$||f|| = \max_{i\in\mathbb{N}, j\in\mathbb{N}} \left\{ |f_{(i,j)}|_p \right\} \ .$$

Nous pouvons, de la même manière, définir $\mathbb{Z}_p \langle n_2 \rangle$ comme l'ensemble des séries formelles en une seule variable n_2 dont les coefficients sont dans $\mathbb{Z}_p$ et tendent vers 0 dans $\mathbb{Z}_p$. Cela nous permet de définir une norme sur $\mathbb{Z}_p \langle n_2 \rangle$ que nous noterons $||.||_1$ et qui est égale au maximum des normes p-adiques des coefficients. Cette norme est bien définie puisque les coefficients sont supposés tendre vers 0 dans $\mathbb{Z}_p$.
Il devient alors également possible de définir $\mathbb{Z}_p \langle n_2 \rangle \langle n_1 \rangle$ comme l'ensemble des séries formelles en une variable n_1 dont les coefficients appartiennent à $\mathbb{Z}_p \langle n_2 \rangle$ avec la condition supplémentaire que la norme de ces coefficients dans $\mathbb{Z}_p \langle n_2 \rangle$ tende vers 0 lorsque l'indice du coefficient tend vers l'infini.

Nous pouvons alors identifier $\mathbb{Z}_p \langle n_2 \rangle \langle n_1 \rangle$ et $\mathbb{Z}_p \langle n_1, n_2 \rangle$ de telle sorte que n'importe quel élément f de $\mathbb{Z}_p \langle n_1, n_2 \rangle$ puisse s'exprimer sous la forme $f = \sum_{i=0}^{\infty} f_i n_1^i$, avec f_i appartenant à $\mathbb{Z}_p \langle n_2 \rangle$ et $||f_i||_1 \to 0$ lorsque $i \to \infty$.

Avant d'énoncer le théorème de préparation de Weierstrass, nous allons caractériser les unités de $\mathbb{Z}_p \langle n_2 \rangle$ et de $\mathbb{Z}_p \langle n_1, n_2 \rangle$.

- $f = \sum_{j=0}^{\infty} f_j n_2^j \in \mathbb{Z}_p \langle n_2 \rangle$ est une unité de $\mathbb{Z}_p \langle n_2 \rangle$ si et seulement si $|f_0|_p = 1$ et $|f_j|_p < 1$ pour tout $j \neq 0$.
- $f = \sum_{(i,j)=(0,0)}^{\infty} f_{(i,j)} n_1^i n_2^j \in \mathbb{Z}_p \langle n_1, n_2 \rangle$ est une unité de $\mathbb{Z}_p \langle n_1, n_2 \rangle$ si et seulement si $|f_{(0,0)}|_p = 1$ et $|f_{(i,j)}|_p < 1$ pour tout $(i, j) \neq (0, 0)$.

Pour en terminer avec les notations, on dit que $f = \sum f_i n_1^i \in \mathbb{Z}_p \langle n_2 \rangle \langle n_1 \rangle$ est général en n_1 d'ordre s si le coefficient f_s est une unité de $\mathbb{Z}_p \langle n_2 \rangle$ et si tous les coefficients d'indice

i strictement supérieur à s sont de norme strictement inférieure à 1.

Remarque : Nous pouvons dès maintenant remarquer l'analogie entre la définition d'un tel s et la définition de ℓ dans le théorème de Strassman.

Nous pouvons alors énoncer le théorème suivant, qui est un cas particulier du théorème 3.1 de Sugatani [Sug 81] dans le cas où il y a deux variables :

Théorème XII (Sugatani [Sug 81]) *Soit f une série formelle de $\mathbb{Z}_p\langle n_1, n_2\rangle$. On suppose qu'il existe un $s \geqslant 0$ tel que f soit général en n_1 d'ordre s. Il existe alors des fonctions uniques $h, g_0, \ldots, g_{s-1}$ et g_s qui satisfont les conditions suivantes :*

- *h est une unité de $\mathbb{Z}_p\langle n_1, n_2\rangle$ et $h_0(n_2) = 1$.*
- *$g_0, \ldots, g_{s-1}$ sont des éléments de $\mathbb{Z}_p\langle n_2\rangle$ et g_s est une unité de $\mathbb{Z}_p\langle n_2\rangle$.*
- *$f(n_1, n_2) = h(n_1, n_2)\ (g_s(n_2)n_1^s + g_{s-1}(n_2)n_1^{s-1} + \cdots + g_1(n_2)n_1 + g_0(n_2))$.*

Remarque : On pourra aisément reconnaître ici le théorème de préparation de Weierstrass usuel. Ce dernier exprime en effet les mêmes propriétés pour les séries formelles en une seule variable et c'est de ce théorème que se déduit élémentairement le théorème de Strassman (voir par exemple dans [Cas 86] p. 108).

Rappelons que notre but est de borner le nombre de solutions p-adiques de systèmes de deux séries formelles en deux variables. Pour cela nous aurons besoin d'appliquer explicitement ce théorème de préparation de Weierstrass à l'une des séries formelles du système. Il nous sera donc nécessaire dans la suite de savoir calculer les fonctions h_i et g_i qui interviennent dans le théorème XII.

II.4.3 Une version explicite du théorème de préparation de Weierstrass

Dans ce paragraphe, nous allons donner une méthode qui permet de calculer effectivement les fonctions qui apparaissent dans le théorème XII. Par effectivement, nous entendons que si la série formelle f est donnée avec une certaine précision, les séries formelles h_i et g_i doivent pouvoir être calculées avec la même précision.
On se donne donc une série formelle f :

$$f(n_1, n_2) = \sum_{(i,j)=0}^{\infty} f_{(i,j)} n_1^i n_2^j \quad \in \mathbb{Z}_p\langle n_1, n_2\rangle \ ,$$

où $f_{(i,j)}$ tend vers 0 dans $\mathbb{Z}_p$ lorsque $i + j \to \infty$.
Dans le but d'appliquer le théorème de préparation de Weierstrass précédemment exposé,

nous regardons f comme une série formelle en n_1 dont les coefficients, que nous noterons $f_i(n_2)$, sont des séries formelles de $\mathbb{Z}_p\langle n_2\rangle$. Nous supposons de plus que f est général en n_1 d'ordre s, si bien que le coefficient $f_s(n_2)$ de n_1^s est inversible dans $\mathbb{Z}_p\langle n_2\rangle$ et que $||f_i(n_2)||_1 < 1$ pour tout $i \geqslant s+1$.

Notons enfin

$$\begin{aligned} g(n_1,n_2) &= g_0(n_2)+g_1(n_2)n_1+\cdots+g_s(n_2)n_1^s \ , \\ h(n_1,n_2) &= 1+\sum_1^{\infty} h_i(n_2)n_1^i \ , \end{aligned}$$

les fonctions obtenues en appliquant le théorème XII à la série formelle f. Notre but est désormais de calculer ces fonctions avec la même précision que celle donnée initialement pour f. Nous utilisons pour cela l'équation

$$f(n_1,n_2) = g(n_1,n_2)h(n_1,n_2) \ ,$$

L'égalité des termes en n_1^n de cette équation permet d'écrire :

$$h_n(n_2)\ g_0(n_2)+h_{n-1}(n_2)\ g_1(n_2)+\cdots+h_{n-s}(n_2)\ g_s(n_2) = f_n(n_2) \quad \forall n \geqslant 0 \ , \tag{II.13}$$

avec les notations $h_0(n_2)=1$ et $h_n(n_2)=0$ si n est négatif.
Comme h est une unité dans $\mathbb{Z}_p\langle n_1,n_2\rangle$, nous savons que

$$||h_i(n_2)|| < 1 \text{ pour tout } i \geqslant 1 \ .$$

Ainsi, puisque $f_s(n_2)$ est inversible dans $\mathbb{Z}_p\langle n_2\rangle$, l'équation (II.13) prise pour $n=s$ implique que $g_s(n_2)$ est également un élément inversible de $\mathbb{Z}_p\langle n_2\rangle$.
Nous pouvons maintenant énoncer la proposition suivante :

Proposition II.4.1 *Les fonctions h_i peuvent être explicitement calculées à partir des fonctions g_0 ,$g_1,\ldots,g_{s-1}$ et g_s par la formule suivante :*

$$h_n = \sum_{k=0}^{\infty} \frac{(-1)^k}{g_s^{k+1}} \sum_{i_0+i_1+\cdots+i_{s-1}=k} \binom{k}{i_0,i_1,\ldots,i_{s-1}} f_{ind(n,k,s,\mathbf{i})} \prod_{\ell=0}^{s-1} g_\ell^{i_\ell} \ , \tag{II.14}$$

avec

- $\mathbf{i} = (i_0,i_1,\ldots,i_{s-1})$,
- $ind(n,k,s,\mathbf{i}) = n+s+\sum_{\ell=0}^{s-1}(s-\ell)i_\ell$,
- *et* $\binom{k}{i_0,i_1,\ldots,i_{s-1}} = \dfrac{k!}{i_0!i_1!\cdots i_{s-1}!}$ *le coefficient multinomial* .

Preuve : Grâce au théorème XII, nous devons simplement démontrer que les fonctions h_i et g_i ainsi définies satisfont les trois conditions du théorème, car de telles fonctions sont alors uniques. Autrement dit, il est suffisant que ces fonctions satisfassent l'équation (II.13) pour démontrer la proposition. Dans cette optique, nous notons $h_{n,k}$ le $k^{\text{ième}}$ sommant apparaissant dans l'équation (II.14).
On doit donc désormais démontrer que $h_n = \sum_{k=0}^{\infty} h_{n,k}$ vérifie l'équation (II.13), autrement dit:

$$\sum_{k=0}^{\infty}(h_{n,k}\ g_0 + h_{n-1,k}\ g_1 + \cdots + h_{n-s,k}\ g_s) = f_n \quad .$$

Considérons dans un premier temps le premier terme de cette somme (pour $k = 0$) donné par:

$$h_{n,0}g_0 + h_{n-1,0}g_1 + \cdots + h_{n-s+1,0}g_{s-1} + h_{n-s,0}g_s \ , \tag{II.15}$$

Il est trivial de montrer que le dernier terme $h_{n-s,0}g_s$ de cette équation est égal à f_n. Reste donc à prouver que les autres termes s'annulent. On remarque alors que ces termes sont annulés par le terme $h_{n-s,1}\ g_s$ obtenu dans le second terme de la somme infinie (pour $k = 1$). De manière analogue, on démontre facilement que pour un entier positif k donné, le terme $h_{n,k}\ g_0 + h_{n-1,k}\ g_1 + \cdots + h_{n-s+1,k}\ g_{s-1}$ est annulé par le terme $h_{n-s,k+1}\ g_s$. On démontre donc de proche en proche que tous les termes de la somme infinie s'annulent, ce qui achève la preuve de la proposition. □
Ainsi, grâce à cette proposition, si l'on veut obtenir une version explicite du théorème de préparation de Weierstrass, il sera seulement nécessaire de calculer les séries formelles $g_0, \ldots, g_s$. Étant donné que $h_0 = 1$ et que $h_n = 0$ pour tous les indices n négatifs, nous pouvons déduire de l'équation (II.13) que

$$g_0 = f_0 \text{ et} \tag{II.16}$$

$$g_i = f_i - \sum_{j=1}^{i} h_j g_{i-j} \text{ pour } 1 \leqslant i \leqslant s \quad . \tag{II.17}$$

À cette étape, il est possible de calculer les séries formelles g_i par substitution récursive à partir de ces formules en utilisant les formules pour les fonctions h_i précédemment obtenues dans la proposition II.4.1. Cependant ces calculs sont très coûteux. C'est pourquoi nous préférons donner une méthode plus efficace qui permet de calculer les fonctions g_i à la même précision que celle donnée initialement pour les séries formelles f_i.

Supposons donc qu'on a déjà calculé les séries formelles g_i et h_i modulo une certaine puissance de p, par exemple p^{k_0}. Nous allons expliquer comment on peut calculer ces fonctions à la précision supérieure, c'est à dire modulo p^{k_0+1} si les séries formelles f_i sont elles-mêmes connues modulo p^{k_0+1}.

- Nous calculons dans un premier temps l'inverse de g_s modulo p_0^k puisque nous avons vu que g_s était inversible dans $\mathbb{Z}_p\left<n_2\right>$.

– Nous calculons ensuite les séries formelles $h_1, \ldots, h_s$ modulo p^{k_0+1}. Cela est possible car les séries formelles g_ℓ sont connues modulo p^{k_0} et les séries formelles f_i sont connues modulo p^{k_0+1} et divisibles par p de telle sorte que les produits $g_\ell f_i$ sont calculables modulo p^{k_0+1}. Remarquons que les séries formelles f_i ne sont pas toutes divisibles par p, mais par définition de l'entier s, le nombre premier p divise la série formelle f_i de $\mathbb{Z}_p \langle n_2 \rangle$ pour tout $i \geqslant s+1$, or les indices $\mathrm{ind}(n,k,s,\mathbf{i})$ intervenant dans les équations (II.14) sont toujours supérieurs à $s+1$.
D'autre part, la somme sur k des formules (II.14) est finie modulo p^{k_0+1}. Il est en effet possible de minorer l'indice des fonctions f_i y intervenant :

$$\begin{aligned} \mathrm{ind}(n,k,s,\mathbf{i}) &= n+s+\sum_{\ell=0}^{s-1}(s-\ell)i_\ell \ , \\ &\geqslant n+s+\sum_{\ell=0}^{s-1} i_\ell \ , \\ &\geqslant n+s+k \ . \end{aligned}$$

Or par hypothèse, les séries formelles f_i tendent vers 0 dans $\mathbb{Z}_p \langle n_2 \rangle$ lorsque i tend vers l'infini. Ainsi quand k tend vers l'infini, les séries formelles f_i intervenant dans les formules (II.14) tendent vers 0 dans $\mathbb{Z}_p \langle n_2 \rangle$. Autrement dit, elles sont toutes nulles modulo p^{k_0+1} pour k_0 suffisamment grand.

Remarque : Les formules de la proposition II.4.1 permettent en fait de calculer modulo p^{k_0+1} n'importe quelle fonction h_n, mais nous n'aurons besoin dans la suite que des fonctions h_0, $h_1, \ldots$, h_s.

– Nous pouvons alors calculer les séries formelles g_0, $g_1, \ldots$, g_s modulo p^{k_0+1} en utilisant les formules (II.17) pour $i = 0, \ldots, s$. En effet, les fonctions g_j sont connues modulo p^{k_0} par hypothèse et l'étape précédente nous a permis de calculer modulo p^{k_0+1} les fonctions h_i intervenant dans ces formules. En dehors de h_0, toutes ces fonctions h_i sont divisibles par p (car h doit être une unité de $\mathbb{Z}_p \langle n_1, n_2 \rangle$ d'après le théorème XII) si bien que les produits $g_j h_i$ sont calculables modulo p^{k_0+1}.

Cette méthode nous permet donc de calculer très rapidement les séries formelles $g_0, g_1, \ldots$, g_s et h_0, $h_1, \ldots$, h_s avec la même précision que celle donnée initialement pour les séries formelles f_i.

Revenons désormais au problème initial pour lequel ce théorème nous intéresse, à savoir, la méthode de Chabauty elliptique dans le cas où la courbe elliptique est de rang 2 sur un corps de nombres de degré au moins 3.
Dans ce cas, nous obtenons en effet au moins deux séries formelles en deux variables n_1 et n_2. Pour résoudre le problème de Chabauty elliptique, nous cherchons à borner le nombre de solutions p-adiques d'un tel système. Pour trouver une telle borne, nous allons appliquer

le théorème de préparation de Weierstrass à l'une des séries formelles obtenues que nous noterons $f^{(1)}$. Rappelons que les séries formelles obtenues par la méthode de Chabauty elliptique sont des éléments de $\mathbb{Z}_p\langle n_1, n_2\rangle$ comme nous l'avons vu dans le paragraphe II.1. Or la série formelle h obtenue par le théorème XII est une unité de $\mathbb{Z}_p\langle n_1, n_2\rangle$, elle ne peut donc jamais s'annuler si bien que la condition $f^{(1)}(n_1, n_2) = 0$ se transforme, grâce à la troisième condition du théorème XII en :

$$g_0(n_2) + g_1(n_2)n_1 + \cdots + g_s(n_2)n_1^s \;=\; 0\ , \tag{II.18}$$

où $g_0, g_1, \ldots, g_s$ sont les fonctions obtenues par le théorème XII.

Ainsi, la condition d'annulation d'une série formelle est transformée en condition d'annulation d'un polynôme de degré s à coefficients dans $\mathbb{Z}_p\langle n_2\rangle$. Cela signifie en particulier, que pour n_2 fixé, il y a au plus s valeurs de n_1 telles que $f^{(1)}(n_1, n_2)$ puisse être nulle. En appliquant le même principe à la seconde série formelle, notée $f^{(2)}$, donnée par la méthode de Chabauty elliptique, on se retrouve avec un système de deux polynômes en n_1 à coefficients dans $\mathbb{Z}_p\langle n_2\rangle$ dont on cherche les zéros communs. Il est alors naturel de calculer le résultant de ces deux polynômes. Ce résultant est une série formelle de $\mathbb{Z}_p\langle n_2\rangle$. En effet $\mathbb{Z}_p\langle n_2\rangle$ est un anneau et on a le lemme trivial suivant :

Lemme II.4.2 *si $P_a = \sum_{i=0}^{d_a} a_i x^i$ et $P_b = \sum_{i=0}^{d_b} b_i x^i$ sont deux polynômes de $A[x]$ où A est un anneau, le résultant de P_a et P_b est un polynôme de $\mathbb{Z}[a_0, a_1, \ldots, a_{d_a}, b_0, b_1, \ldots, b_{d_b}]$.*

Il nous suffira alors d'appliquer le théorème de Strassman à cette nouvelle série formelle pour déduire une borne sur le nombre de solutions à l'équation $\mathrm{Res}(f^{(1)}, f^{(2)})(n_2) = 0$.
Supposons maintenant que l'on connaît déjà à l'avance les valeurs que doit prendre le paramètre n_2 et que leur nombre correspond à la borne obtenue (ce qui est bien sûr une condition nécessaire au succès de ce type de méthode). On substitue alors ces valeurs de n_2 soit dans l'une des deux équations $f^{(i)} = 0$ soit dans l'un des deux polynômes que l'on en a déduit. Le résultat obtenu est alors une série formelle de $\mathbb{Z}_p\langle n_1\rangle$ à laquelle on applique une nouvelle fois le théorème de Strassman.
Ainsi, pour chaque valeur possible de n_2, on obtient une borne sur le nombre de valeurs que peut prendre le paramètre n_1. Il reste alors à espérer une fois de plus que ces bornes correspondent effectivement aux solutions déjà connues. Nous avons développé un programme `maple` permettant de mettre en pratique cette méthode. Ce programme est présenté dans l'annexe B.1 et disponible par ftp à

`ftp://megrez.math.u-bordeaux.fr/pub/duquesne`.

Afin de pouvoir appliquer cette méthode à la courbe elliptique E, nous allons maintenant calculer les séries formelles en question en suivant la méthode de Chabauty elliptique exposée au paragraphe II.1.

II.4.4 La méthode de Chabauty elliptique pour E

Dans ce paragraphe, on suit la méthode de Chabauty elliptique développée dans le paragraphe II.1 et dans [Fly-Wet 99].
Il est dans un premier temps nécessaire de calculer la structure du groupe de Mordell-Weil de la courbe elliptique E définie sur $\mathbf{k} = \mathbb{Q}(\beta)$ par l'équation (II.12).

1 Calcul de $E(\mathbf{k})$

Nous utilisons pour le calcul explicite du groupe de Mordell-Weil de la courbe E le programme de Simon [Sim]. La courbe $E(\mathbf{k})$ est sans torsion et le programme de Simon nous indique qu'elle est de rang 2 et que $G_1 = [0, 1]$ et $G_2 = [1, 1-\beta^2]$ sont des générateurs de $E(\mathbf{k})/2E(\mathbf{k})$.
Reste maintenant à prouver que G_1 et G_2 sont effectivement des générateurs du groupe de Mordell-Weil de la courbe E. Nous allons pour cela effectuer une descente infinie. Cette méthode est implémentée dans le programme `mwrank` de Cremona [Cre] pour les courbes elliptiques définies sur $\mathbb{Q}$. Elle est cependant plus complexe à mettre en œuvre pour les courbes elliptiques définies sur un corps de nombres. Nous n'allons donc qu'en exprimer les grandes lignes. Ces calculs ont été effectués à l'aide des algorithmes développés par Siksek [Sik 95] et par Silverman pour le calcul de la hauteur canonique [Sil 88].

La première étape consiste à borner la différence entre la hauteur naïve et la hauteur canonique sur E. Le lemme I.3.1 de Silverman exposé au premier chapitre permet d'obtenir une borne égale à 5.86. Cela n'est cependant pas suffisant. Pour obtenir une borne plus fine, on utilise un algorithme de Siksek décrit dans [Sik 95]. On démontre ainsi que pour tout point P dans $E(\mathbf{k})$, on a

$$h(P) - \hat{h}(P) \leqslant 0.217 \ . \tag{II.19}$$

Nous allons maintenant démontrer le lemme suivant :

Lemme II.4.3 *Il n'existe pas de point appartenant à $E(\mathbf{k})$ et ayant une hauteur canonique inférieure à* 0.5.

Preuve : Supposons que P soit un point dont la hauteur canonique est inférieure à 0.5. La hauteur naïve d'un tel point P doit alors être inférieure à 0.717 en vertu de (II.19). Nous devons alors tester quels éléments de $\mathbf{k}$ ayant une hauteur logarithmique inférieure à 0.717 sont les abscisses de points de $E(\mathbf{k})$ ayant une hauteur canonique inférieure à 0.5. Un tel élément peut être représenté par un polynôme f à coefficients entiers de degré n inférieur à 3. Sa hauteur logarithmique est alors égale à $\frac{1}{n}\log(\mu(f))$ où $\mu(f)$ désigne la mesure de Mahler du polynôme f. La condition sur la hauteur logarithmique de l'abscisse de P devient alors une condition sur la mesure de Mahler de son polynôme minimal normalisé. Autrement dit, si $P = [x, y]$ est un point de $E(\mathbf{k})$ et si $\mu(x)$ désigne la mesure de Mahler du polynôme minimal normalisé de x, on a

$$\begin{aligned}\hat{h}(P) \leqslant 0.5 \quad &\Rightarrow \quad h(P) \leqslant 0.717 \\ &\Rightarrow \quad h(x) \leqslant 0.717 \\ &\Rightarrow \quad \mu(x) \leqslant \exp(3 \times 0.717) \leqslant 8.6.\end{aligned}$$

Il n'y a alors qu'un nombre fini de polynômes à coefficients entiers de degré inférieur à 3 dont la mesure de Mahler est inférieure à 8.6 et il est possible de tous les énumérer. Pour chacun de ces polynômes, on peut donc vérifier s'ils proviennent d'un point de la courbe E ayant une hauteur naïve inférieure à 0.717. On démontre de cette manière que G_1 et G_2 sont les seuls points ayant cette propriété (leur hauteur naïve est nulle). La hauteur canonique de ces points est respectivement égale à environ 0.8054 et 0.9715. Nous avons donc démontré qu'il n'existait pas de point de $E(\mathbf{k})$ ayant une hauteur canonique inférieure à 0.5. □

Nous pouvons maintenant démontrer la proposition suivante :

Proposition II.4.4 *Les points G_1 et G_2 sont des générateurs du groupe de Mordell-Weil de la courbe E.*

Preuve : On utilise le raisonnement classique suivant :
si $E(\mathbf{k})$ ne contient aucun point d'ordre infini de hauteur canonique inférieure à λ et si G_1 et G_2 engendrent un sous groupe de $E(\mathbf{k})$ de rang 2, alors l'indice n du groupe engendré par G_1 et G_2 dans $E(\mathbf{k})$ satisfait

$$n \leqslant R(G_1, G_2)^{\frac{1}{2}} \frac{\gamma_2}{\lambda},$$

où $\gamma_2 = \frac{2}{\sqrt{3}}$ et $R(G_1, G_2)$ est le déterminant de la matrice des hauteurs associée à G_1 et G_2. Pour plus de détails sur ce point, on pourra se référera par exemple à l'article de Siksek [Sik 95].

Le lemme II.4.3 permet de montrer qu'on peut choisir $\lambda = \frac{1}{2}$. On peut, d'autre part, borner $R(G_1, G_2)$ par 0.718 en utilisant les algorithmes de Silverman [Sil 88] de telle sorte que l'on ait finalement $n \leqslant 1.96$. Cela signifie que n doit être égal à 1 et donc que G_1 et G_2 sont des générateurs pour $E(\mathbf{k})$. □

Nous pouvons désormais appliquer la méthode de Chabauty elliptique à $E(\mathbf{k})$.

2 Application de la méthode de Chabauty elliptique à $E(\mathbf{k})$

Nous devons tout d'abord choisir un nombre premier p qui satisfasse les six conditions qui permettent d'appliquer la méthode de Chabauty elliptique. Nous choisirons dans ce cas le nombre premier 3 qui satisfait ces conditions. Le point $\widetilde{G_1}$, réduction de G_1 modulo 3, est d'ordre 11 sur la courbe elliptique $\widetilde{E}$, réduction de E modulo 3. De même, l'ordre de $\widetilde{G_2}$ sur $\widetilde{E}$ est 33. Afin de réduire un peu ces ordres, on pose $G_3 = G_1 - 3G_2$. Une nouvelle base pour le groupe de Mordell-Weil de $E(\mathbf{k})$ est alors donnée par les points G_2 et G_3. Cette fois l'ordre de $\widetilde{G_3}$ vaut 1, on définit alors :

- $m_1 = 1$ et $m_2 = 33$ les ordres de $\widetilde{G_2}$ et $\widetilde{G_3}$ modulo 3,
- $Q_1 = G_3$ et $Q_2 = 33G_2$ les plus petits multiples des générateurs qui appartiennent au noyau de la réduction modulo 3,
- $\mathcal{U} = \{\infty, \pm iG_2,\ 1 \leqslant i \leqslant 16\}$,

de telle sorte que tout point P de $E(\mathbf{k})$ s'écrive sous la forme

$$P = U + n_1Q_1 + n_2Q_2\ , \tag{II.20}$$

avec U appartenant à l'ensemble fini $\mathcal{U}$ et n_1 et n_2 appartenant à $\mathbb{Z}$.
Pour chacun des éléments U de $\mathcal{U}$, nous allons donc devoir chercher pour quelles valeurs de n_1 et de n_2, un tel point P peut avoir une abscisse dans $\mathbb{Q}$. La première chose à faire est donc bien sûr de réduire au maximum l'ensemble des U de $\mathcal{U}$ à considérer.

Par construction, les points Q_1 et Q_2 sont dans le noyau de la réduction modulo 3; un point P exprimé comme dans (II.20) doit donc nécessairement vérifier $\widetilde{P} = \widetilde{U}$. Ainsi, si un tel point P a son abscisse dans $\mathbb{Q}$, alors $\widetilde{U}$, la réduction de U modulo 3, doit avoir son abscisse dans $\mathbb{F}_3$. Or ce n'est pas le cas pour la plupart des éléments de l'ensemble fini $\mathcal{U}$. Le calcul de ces éléments modulo 3 montre en effet que les seuls à avoir une abscisse dans $\mathbb{F}_3$ sont

$$U = \infty, G_2, -G_2, 3G_2, -3G_2, 14G_2, -14G_2\ .$$

Dans la suite nous n'aurons donc besoin que de considérer ces valeurs pour U.
D'autre part, comme nous avons choisi n_1 et n_2 dans $\mathbb{Z}$, il n'est bien sûr pas utile de rechercher les points de la forme $-G_2 + n_1Q_1 + n_2Q_2$ ayant une abscisse dans $\mathbb{Q}$ si on connaît déjà ceux de la forme $G_2 + n_1Q_1 + n_2Q_2$. Il n'est donc pas non plus nécessaire de considérer les points $-G_2, -3G_2$ et $-14G_2$.

Pour résumer, on doit maintenant déterminer tous les points de $E(\mathbf{k})$ ayant une abscisse dans $\mathbb{Q}$ et qui peuvent être écrit sous la forme $U + n_1Q_1 + n_2Q_2$ avec $U \in \mathcal{U}'$ et n_1, n_2 dans $\mathbb{Z}$ où $\mathcal{U}'$ désigne l'ensemble $\{\infty, G_2, 3G_2, 14G_2\}$.

Enfin, pour chaque point $Q_i = [x_i, y_i]$, on définit la z-coordonnée de Q_i par $z_i = -\frac{x_i}{y_i}$, et on note $g_3 = 1$, $g_2 = -2$, $g_1 = 1 - \beta - 4\beta^2$ et $g_0 = 1$ les coefficients de la courbe elliptique E.
Nous allons maintenant calculer la z-coordonnée d'un point quelconque P de $E(\mathbf{k})$ de la forme $U + n_1Q_1 + n_2Q_2$ avec $U \in \mathcal{U}'$ en fonction de n_1 et de n_2 On utilise pour cela le logarithme et l'exponentielle formels introduits au paragraphe II.1 (voir [Sil 86] pour les détails).
Remarquons que dans notre cas, il sera suffisant de travailler modulo 3^5. Calculons dans un premier temps z_1 et z_2 modulo 3^5 :

$$\begin{aligned} z_1 &= 240 + 84\beta + 57\beta^2 \qquad \pmod{3^5}\ , \\ z_2 &= 60 + 99\beta + 195\beta^2 \qquad \pmod{3^5}\ . \end{aligned}$$

Nous énonçons maintenant un petit lemme qui nous permet de pouvoir calculer le logarithme et l'exponentielle formels à la précision désirée.

Lemme II.4.5 *Pour calculer Log(t) ou Exp(t) modulo 3^5 quand t est divisible par 3, les termes en $O(t^9)$ peuvent être ignorés dans les formules.*

Preuve : Le produit de $k!$ par le coefficient de t^k dans l'expression de $\mathrm{Log}(t)$ ou de $\mathrm{Exp}(t)$ appartient à $\mathbb{Z}[g_0, g_1, g_2, g_3] = \mathbb{Z}_3[\beta]$ de telle sorte que, si par exemple $\mathrm{Log}(t) = \sum_{k=0}^{\infty} a_k t^k$, alors 3^k divise $k! a_k t^k$ soit

$$v_3(k!) + v_3\left(a_k t^k\right) \geqslant k \ .$$

L'estimation standard $|k!|_p \geqslant p^{-(k-1)/(p-1)}$, permet alors d'en déduire

$$v_3\left(a_k t^k\right) \geqslant k - \frac{k-1}{2} \geqslant \frac{k+1}{2}$$

Autrement dit, si $\frac{k+1}{2} \geqslant 5$ alors le terme $a_k t^k$ est nul modulo 3^5. Cette condition signifie qu'il n'est pas nécessaire de considérer les puissances de t supérieures ou égales à 9. Les puissances intervenant dans $\mathrm{Log}(t)$ et dans $\mathrm{Exp}(t)$ étant toutes impaires, il faudra seulement considérer les puissances inférieures ou égales à 7. □

Étant donné que les points Q_1 et Q_2 sont dans le noyau de la réduction modulo 3, leurs z-coordonnées z_1 et z_2 sont nulles modulo 3. On peut donc calculer $\mathrm{Log}(z_1)$ et $\mathrm{Log}(z_2)$ modulo 3^5 en utilisant le lemme II.4.5

$$\begin{array}{rcll} \mathrm{Log}(z_1) & = & 42 + 48\beta + 39\beta^2 & \pmod{3^5} \ , \\ \mathrm{Log}(z_2) & = & 15 + 117\beta + 15\beta^2 & \pmod{3^5} \ . \end{array}$$

Les puissances de t intervenant dans $\mathrm{Log}(t)$ étant toutes impaires, $\mathrm{Log}(z_1)$ et $\mathrm{Log}(z_2)$ sont toutes deux divisibles par 3. On peut donc appliquer le lemme II.4.5 pour calculer la z-coordonnée de $n_1 Q_1 + n_2 Q_2$ comme une série formelle en n_1 et n_2 :

$$\begin{array}{l} z\text{-coordonnée}(n_1 Q_1 + n_2 Q_2) \ = \ \mathrm{Exp}(n_1 \mathrm{Log}(z_1) + n_2 \mathrm{Log}(z_2)) = \\ \left[(162n_2^2 + 18)n_1^3 + (162n_2^3 + 216n_2)n_1^2 + (81n_2^4 + 81n_2^2 + 39)n_1 + 63n_2^3 + 132n_2\right]\beta^2 + \\ \left[81n_1^5 + (162n_2^2 + 198)n_1^3 + (81n_2^3 + 189n_2)n_1^2 + (162n_2^4 + 216n_2^2 + 48)n_1 + \right. \\ \hfill \left. 162n_2^5 + 63n_2^3 + 117n_2\right]\beta + \\ 162n_1^5 + 162n_2n_1^4 + 36n_1^3 + (81n_2^3 + 162n_2)n_1^2 + (162n_2^2 + 42)n_1 + 45n_2^3 + 15n_2 \quad \pmod{3^5} \ . \end{array}$$

On peut alors en déduire l'inverse de l'abscisse de $n_1 Q_1 + n_2 Q_2$ en utilisant la formule adéquate (II.5). C'est une série formelle en n_1 et n_2, que nous notons θ_∞ et dont les coefficients tendent vers 0 dans $\mathbb{Z}_3[\beta]$. Il est possible de calculer θ_∞ modulo 3^5. En effet, les puissances intervenant dans $\mathrm{Exp}(t)$ étant impaires, la z-coordonnée de $n_1 Q_1 + n_2 Q_2$ est divisible par 3 ; de plus, les coefficients de la formule (II.5) étant dans $\mathbb{Z}_3[\beta]$, il suffit d'en considérer les deux premiers termes. On obtient :

$\theta_\infty(n_1, n_2) =$

$$\left[189n_1^4 + (81n_2^3 + 54n_2)n_1^3 + (162n_2^2 + 108)n_1^2 + (162n_2^3 + 225n_2)n_1 + 189n_2^4 + 54n_2^2\right]\beta^2 +$$
$$\left[54n_1^4 + (162n_2^3 + 162n_2)n_1^3 + 126n_1^2 + (189n_2^3 + 144n_2)n_1 + 189n_2^4 + 126n_2^2\right]\beta +$$
$$27n_1^4 + 81n_2^3n_1^3 + (81n_2^2 + 207)n_1^2 + (27n_2^3 + 117n_2)n_1 + 189n_2^4 + 198n_2^2 \pmod{3^5}\ .$$

Les composantes en β et β^2 de cette série formelle sont des séries formelles notées respectivement $\theta_\infty^{(1)}$ et $\theta_\infty^{(2)}$ appartenant à $\mathbb{Z}_3\langle n_1, n_2\rangle$ qui devront s'annuler si le point $\infty + n_1Q_1 + n_2Q_2$ a une abscisse dans $\mathbb{Q}$. Leurs expressions modulo 3^5 sont alors :

$$\begin{aligned}\theta_\infty^{(1)}(n_1,n_2) &= 54n_1^4 + (162n_2^3 + 162n_2)n_1^3 + 126n_1^2 + (189n_2^3 + 144n_2)n_1 + \\ &\quad 189n_2^4 + 126n_2^2 \pmod{3^5}\ .\end{aligned}$$

$$\begin{aligned}\theta_\infty^{(2)}(n_1,n_2) &= 189n_1^4 + (81n_2^3 + 54n_2)n_1^3 + (162n_2^2 + 108)n_1^2 + (162n_2^3 + \\ &\quad 225n_2)n_1 + 189n_2^4 + 54n_2^2 \pmod{3^5}\ .\end{aligned}$$

Si $\theta_U(n_1,n_2)$ est l'abscisse du point $U + n_1Q_1 + n_2Q_2$ quand $U \neq \infty$, alors θ_U est une série formelle de $\mathbb{Z}_3\langle n_1, n_2\rangle$. De manière analogue, on peut décomposer $\theta_U(n_1,n_2)$ selon ses composantes. Celles qui nous intéressent sont les composantes en β et en β^2 que nous notons respectivement $\theta_U^{(1)}(n_1,n_2)$ et $\theta_U^{(2)}(n_1,n_2)$. Nous les avons calculées modulo 3^5 :

$$\begin{aligned}\theta_{G_2}^{(1)}(n_1,n_2) &= 162n_1^4 + (81n_2^2 + 162n_2 + 9)n_1^3 + (81n_2^3 + 162n_2^2 + 108n_2 + \\ &\quad 234)n_1^2 + (162n_2^4 + 189n_2^3 + 198n_2 + 123)n_1 + 189n_2^4 + \\ &\quad 18n_2^3 + 162n_2^2 + 237n_2 \pmod{3^5}\ .\end{aligned}$$

$$\begin{aligned}\theta_{G_2}^{(2)}(n_1,n_2) &= 162n_1^5 + (162n_2 + 54)n_1^4 + (162n_2^3 + 108n_2 + 36)n_1^3 + (81n_2^3 + \\ &\quad 153)n_1^2 + (27n_2^3 + 162n_2^2 + 216n_2 + 150)n_1 + 45n_2^3 + 33n_2 \pmod{3^5}\ .\end{aligned}$$

$$\begin{aligned}\theta_{3G_2}^{(1)}(n_1,n_2) &= 162n_1^5 + 135n_1^4 + (162n_2^3 + 81n_2^2 + 81n_2 + 207)n_1^3 + (162n_2^3 + \\ &\quad 162n_2^2 + 216n_2 + 225)n_1^2 + (81n_2^4 + 54n_2^3 + 27n_2^2 + 153n_2 + \\ &\quad 105)n_1 + 81n_2^6 + 81n_2^5 + 54n_2^4 + 99n_2^3 + 18n_2^2 + 27n_2 + 138 \pmod{3^5}\ .\end{aligned}$$

$$\begin{aligned}\theta_{3G_2}^{(2)}(n_1,n_2) &= 81n_1^6 + (81n_2^2 + 162n_2 + 9)n_1^3 + (81n_2^3 + 162n_2^2 + 108n_2 + \\ &\quad 234)n_1^2 + (162n_2^4 + 27n_2^3 + 81n_2^2 + 225n_2 + 69)n_1 + 162n_2^6 + \\ &\quad 27n_2^4 + 126n_2^3 + 216n_2^2 + 12n_2 + 93 \pmod{3^5}\ .\end{aligned}$$

$$\begin{aligned}\theta_{14G_2}^{(1)}(n_1,n_2) &= (162n_2 + 108)n_1^4 + (81n_2^3 + 81n_2 + 135)n_1^3 + (162n_2^2 + 54n_2 + \\ &\quad 189)n_1^2 + (81n_2^4 + 162n_2^3 + 54n_2^2 + 108n_2 + 60)n_1 + 162n_2^5 + \\ &\quad 81n_2^4 + 45n_2^3 + 36n_2^2 + 171n_2 + 189 \pmod{3^5}\ .\end{aligned}$$

$$\begin{aligned}\theta^{(2)}_{14G_2}(n_1,n_2) \quad = \quad & 162n_1^5+(81n_2+108)n_1^4+(81n_2^3+81n_2^2+135n_2+126)n_1^3+ \\ & (162n_2^3+81n_2^2+81n_2+99)n_1^2+(189n_2^3+54n_2^2+18n_2+ \\ & 162)n_1+162n_2^5+54n_2^4+108n_2^3+135n_2^2+207n_2+150 \quad \pmod{3^5}\ .\end{aligned}$$

Dans tous ces cas, que U soit le point à l'infini ou non, si le point $U+n_1Q_1+n_2Q_2$ a une abscisse dans $\mathbb{Q}$ alors les deux séries formelles $\theta^{(1)}_U(n_1,n_2)$ et $\theta^{(2)}_U(n_1,n_2)$ doivent être nulles. En d'autres termes, pour chacun des points U de $\mathcal{U}'$, nous devons déterminer quels couples (n_1,n_2) satisfont le système :

$$\theta^{(1)}_U(n_1,n_2)=\theta^{(2)}_U(n_1,n_2)=0\ . \tag{II.21}$$

On connaît déjà de telles solutions, par exemple $(0,0)$ est solution du système (II.21) pour le point à l'infini. Le théorème de préparation de Weierstrass va nous permettre de trouver une borne sur le nombre de telles solutions 3-adiques. Il ne nous restera plus qu'à espérer que la borne ainsi obtenue correspondra aux solutions déjà connues.

II.4.5 Application du théorème de préparation de Weierstrass en 2 variables à la courbe E

Nous avons vu que les seuls points rationnels de $E(\mathbb{Q}(\beta))$ ayant une abscisse dans $\mathbb{Q}$ peuvent s'écrire $\pm U+n_1Q_1+n_2Q_2$ avec $U=\infty, G_2, 3G_2$ ou $14G_2$ et n_1, n_2 appartenant à $\mathbb{Z}$. De plus, pour chacun de ces points U, n_1 et n_2 satisfont un système de deux équations. Considérons dans un premier temps le cas $U=G_2$.

1 Application du théorème de préparation de Weierstrass dans le cas linéaire ($s=1$) pour θ_{G_2}.

Pour qu'un point de la forme $G_2+n_1Q_1+n_2Q_2$ ait son abscisse dans $\mathbb{Q}$, les séries formelles suivantes doivent s'annuler

$$\begin{aligned}\theta^{(1)}_{G_2}(n_1,n_2) \quad = \quad & 162n_1^4+(81n_2^2+162n_2+9)n_1^3+(81n_2^3+162n_2^2+108n_2+ \\ & 234)n_1^2+(162n_2^4+189n_2^3+198n_2+123)n_1+(189n_2^4+ \\ & 18n_2^3+162n_2^2+237n_2) \quad \pmod{3^5}\ ,\end{aligned}$$

$$\begin{aligned}\theta^{(2)}_{G_2}(n_1,n_2) \quad = \quad & 162n_1^5+(162n_2+54)n_1^4+(162n_2^3+108n_2+36)n_1^3+(81n_2^3+ \\ & 153)n_1^2+(27n_2^3+162n_2^2+216n_2+150)n_1+(45n_2^3+33n_2) \quad \pmod{3^5}\ .\end{aligned}$$

Nous allons dans un premier temps appliquer le théorème de préparation de Weierstrass à la série formelle $\theta^{(1)}_{G_2}(n_1,n_2)$. Comme tous les coefficients de cette série formelle sont divisibles par 3, nous considérons plutôt la série formelle :

$$f(n_1,n_2) \quad = \quad \frac{1}{3}\theta^{(1)}_{G_2}(n_1,n_2)$$

$$\begin{aligned} = \; & 54n_1^4+(27n_2^2+54n_2+3)n_1^3+(27n_2^3+54n_2^2+36n_2+78)n_1^2+ \\ & (54n_2^4+63n_2^3+66n_2+41)n_1+(63n_2^4+6n_2^3+54n_2^2+79n_2) \pmod{3^4} \; . \end{aligned}$$

Nous avons vu dans le paragraphe II.1 qu'une telle série formelle a ses coefficients $f_{(i,j)}$ qui convergent vers 0 quand $i+j$ tend vers l'infini, c'est à dire que $f \in \mathbb{Z}_3 \langle n_1, n_2 \rangle$. De plus $f_1(n_2)$ est une unité de $\mathbb{Z}_3 \langle n_2 \rangle$. En effet, le coefficient constant de $f_1(n_2)$ est 41 qui est inversible modulo 3 et tous les autres coefficients de $f_1(n_2)$ sont divisibles par 3. Les autres séries formelles $f_i(n_2)$ pour $i \geqslant 2$ sont également divisibles par 3 ce qui signifie exactement que f est générale en n_1 d'ordre 1. Le théorème de préparation de Weierstrass permet alors de montrer qu'il existe des fonctions uniques h, g_0 et g_1 telles que
- la série formelle h soit une unité de $\mathbb{Z}_3 \langle n_1, n_2 \rangle$ dont le premier coefficient vaut 1,
- la série formelle g_0 appartienne à $\mathbb{Z}_3 \langle n_2 \rangle$,
- la série formelle g_1 soit une unité de $\mathbb{Z}_3 \langle n_2 \rangle$ et
- $f(n_1, n_2) = h(n_1, n_2)\,(g_0(n_2) + g_1(n_2)n_1)$.

Les séries formelles $f_i(n_2)$ étant connues modulo 3^4, nous allons maintenant calculer les séries formelles h, g_0 et g_1 avec la même précision. Nous allons pour cela employer la méthode décrite au paragraphe II.4.3 et B.1.

Si $h(n_1,n_2) = \sum_{i=0}^{\infty} h_i(n_2) n_1^i$ et $f(n_1,n_2) = \sum_{i=0}^{\infty} f_i(n_2) n_1^i$, la proposition II.4.1 et les formules (II.17) s'écrivent dans ce cas de la façon suivante :

$$h_1(n_2) = \sum_{k=0}^{\infty} \frac{(-1)^k}{g_1^{k+1}(n_2)} f_{k+2}(n_2)\; g_0^k(n_2) \; , \tag{II.22}$$

$$g_0(n_2) = f_0(n_2) \; , \tag{II.23}$$

$$g_1(n_2) = f_1(n_2) - g_0(n_2)\; h_1(n_2) \; . \tag{II.24}$$

L'utilisation de (II.23) permet évidemment d'obtenir immédiatement la série formelle g_0 modulo 3^4. Notre objectif est désormais de calculer g_1 modulo 3^4. Les conditions du théorème de préparation de Weierstrass expriment en particulier que la série formelle $h_1(n_2)$ doit être nulle modulo 3. L'équation (II.24) nous permet alors d'en déduire la série formelle $g_1(n_2)$ modulo 3 :

$$\begin{aligned} h_1(n_2) &= 0 \pmod 3 \; , \\ g_0(n_2) &= n_2 \pmod 3 \; , \\ g_1(n_2) &= 2 \pmod 3 \; . \end{aligned}$$

Nous allons maintenant en déduire le calcul de $g_1(n_2)$ modulo 9 :

- Calculons tout d'abord l'inverse de $g_1(n_2)$ qui est évidemment égal à 2 modulo 3.

– Nous devons maintenant calculer $h_1(n_2)$ modulo 9 à l'aide de la formule (II.22). Le calcul de $f(n_1, n_2)$ modulo 3^4 nous permet alors de remarquer que les séries formelles $f_i(n_2)$ sont nulles modulo 9 dès que l'indice i est supérieur ou égal à 4. Seuls les deux premiers termes sont donc à considère (le terme pour $k = 0$ qui fait intervenir $f_2(n_2)$ et le terme pour $k = 1$ qui fait intervenir $f_3(n_2)$) de la somme infinie de la formule (II.22) sont donc à considérer et on a

$$h_1(n_1) = \frac{1}{g_1(n_2)} f_2(n_2) - \frac{1}{g_1^2(n_2)} f_3(n_2) g_0(n_2) \pmod 9 \ .$$

Les séries formelles $f_2(n_2)$ et $f_3(n_2)$ sont divisibles par 3 car f est générale d'ordre 1 si bien que les produits $f_i g_j$ peuvent être calculés modulo 9 :

$$h_1(n_2) = 6n_2 + 3 \pmod 9 \ .$$

– Une fois connue $h_1(n_2)$ modulo 9, la formule (II.24) permet de calculer aisément la série formelle $g_1(n_2)$ modulo 9 :

$$g_1(n_2) = 3n_2^2 + 5 \pmod 9 \ .$$

On obtient donc par cette méthode toutes les fonctions désirées modulo 9. Il est possible de réappliquer cette méthode afin de les connaître modulo 27 puis modulo 3^4. Les fonctions h_i ne servent que d'intermédiaires dans cette méthode puisque celles qui nous intéressent pour la suite sont $g_0(n_2)$ et $g_1(n_2)$:

$$\begin{aligned} g_0(n_2) &= 63n_2^4 + 6n_2^3 + 54n_2^2 + 79n_2 && \pmod{3^4} \ , \\ g_1(n_2) &= 27n_2^5 + 9n_2^3 + 30n_2^2 + 54n_2 + 41 && \pmod{3^4} \ . \end{aligned}$$

On a donc d'après le théorème XII

$$\frac{\theta_{G_2}^{(1)}(n_1, n_2)}{3} = (g_0(n_2) + g_1(n_2)n_1)(1 + \sum_{i=1}^{\infty} h_i(n_2) n_1^i) \ ,$$

avec $||h_i(n_2)|| < 1$ pour tout $i > 0$.
Il s'ensuit alors que la condition $\theta_{G_2}^{(1)}(n_1, n_2) = 0$ implique que $g_0(n_2) + g_1(n_2)n_1 = 0$. La stratégie exposée à la fin du paragraphe II.4.3 suggère alors de faire le même raisonnement avec la seconde série formelle $\theta_{G_2}^{(2)}(n_1, n_2)$ puis de considérer le résultant des deux polynômes ainsi obtenus pour enfin lui appliquer le théorème de Strassman.
Pour notre premier exemple d'application, nous n'allons pas suivre cette suggestion... La situation est en effet particulièrement simple dans ce cas puisque le polynôme obtenu est de degré 1 en n_1. Cela signifie que pour un entier n_2 fixé il y a au plus une solution en n_1 à notre équation. Le théorème XII nous en donne une expression explicite comme une série formelle en n_2 que nous noterons ϕ et dont les coefficients tendent vers 0 dans $\mathbb{Z}_3$:

$$\phi(n_2) = -\frac{g_0(n_2)}{g_1(n_2)} \in \mathbb{Z}_3 \langle n_2 \rangle \ ,$$

Ceci est possible car la série formelle $g_1(n_2)$ est inversible dans $\mathbb{Z}_3\langle n_2\rangle$. On calcule donc cette nouvelle série formelle modulo 3^4 :

$$\phi(n_2) = 54n_2^5 + 45n_2^4 + 72n_2^3 + 27n_2^2 + 4n_2 \qquad (\mathrm{mod}\ 3^4)\ .$$

Dans ce cas, si (n_1, n_2) est une solution au système, alors la série formelle $\psi(n_2)$ obtenue en remplaçant n_1 par $\phi(n_2)$ dans $\theta_{G_2}^{(2)}(n_1, n_2)$ doit être nulle. Étant donné que la série formelle $\theta_{G_2}^{(2)}(n_1, n_2)$ appartient à $\mathbb{Z}_3\langle n_1, n_2\rangle$, cette nouvelle série formelle appartient à $\mathbb{Z}_3\langle n_2\rangle$ et ses premiers termes sont donnés par

$$\psi(n_2) = \theta_{G_2}^{(2)}(\phi(n_2), n_2) = 54n_2^4 + 27n_2^3 + 72n_2^2 + 66n_2 \qquad (\mathrm{mod}\ 3^4)\ .$$

Il ne nous reste alors plus qu'à appliquer le théorème de Strassman à cette série formelle afin de borner le nombre de valeurs que peut prendre n_2. Ce théorème démontre dans ce cas que l'équation $\psi(n_2) = 0$ a au plus une solution 3-adique. Or, nous connaissons déjà une solution à cette équation donnée par $n_2 = 0$ et le théorème de Strassman nous permet donc d'affirmer que c'est la seule solution 3-adique. L'unique entier n_1 correspondant est alors $\phi(0) = 0$. Finalement, nous avons donc montré que $(0, 0)$ est l'unique solution 3-adique au système

$$\theta_{G_2}^{(1)}(n_1, n_2) = \theta_{G_2}^{(2)}(n_1, n_2) = 0\ ,$$

ce qui prouve que G_2 est l'unique point de $E(\mathbf{k})$ de la forme $G_2 + n_1Q_1 + n_2Q_2$ et ayant une abscisse dans $\mathbb{Q}$.

Nous allons maintenant considérer le cas du point à l'infini.

2 Application du théorème de préparation de Weierstrass dans le cas quadratique ($s = 2$) pour θ_∞.

Nous avons vu précédemment que si un point de la forme $\infty + n_1Q_1 + n_2Q_2$ avait son abscisse dans $\mathbb{Q}$, alors les séries formelles suivantes devaient s'annuler :

$$\begin{aligned}\theta_\infty^{(1)}(n_1, n_2) &= 54n_1^4 + (162n_2^3 + 162n_2)n_1^3 + 126n_1^2 + (189n_2^3 + 144n_2)n_1 + \\ &\quad 189n_2^4 + 126n_2^2 \\ &\qquad\qquad (\mathrm{mod}\ 3^5)\ ,\\ \theta_\infty^{(2)}(n_1, n_2) &= 189n_1^4 + (81n_2^3 + 54n_2)n_1^3 + (162n_2^2 + 108)n_1^2 + (162n_2^3 + \\ &\quad 225n_2)n_1 + 189n_2^4 + 54n_2^2 \qquad (\mathrm{mod}\ 3^5)\ .\end{aligned}$$

Remarque : Ces séries formelles ne comportent pas de termes constants, ni de termes en n_1 ou de termes en n_2. En effet, elles sont obtenues en appliquant la formule (II.5) à la z-coordonnée de $n_1Q_1 + n_2Q_2$. Cette formule, qui donne l'inverse de l'abscisse d'un point en fonction de sa z-coordonnée, a son premier terme en z^2 et la z-coordonnée de $n_1Q_1 + n_2Q_2$ n'a pas de terme constant (elle est donnée par l'exponentielle formelle de

$n_1\mathrm{Log}(z_1) + n_2\mathrm{Log}(z_2)$ et l'exponentielle formelle n'a pas de terme constant).

Nous allons, dans un premier temps, appliquer le théorème de préparation de Weierstrass à la série formelle $\theta_\infty^{(1)}(n_1, n_2)$. Comme tous les coefficients de cette série formelle sont divisibles par 9, nous considérons la série formelle :

$$\begin{aligned} f^{(1)}(n_1, n_2) &= \frac{1}{9}\theta_\infty^{(1)}(n_1, n_2) \\ &= 6n_1^4 + (18n_2^3 + 18n_2)n_1^3 + 14n_1^2 + (21n_2^3 + 16n_2)n_1 + 21n_2^4 + 14n_2^2 \pmod{3^3} . \end{aligned}$$

Nous avons vu dans le paragraphe II.1 qu'une telle série formelle a ses coefficients $f_{(i,j)}^{(1)}$ qui convergent vers 0 quand $i + j$ tend vers l'infini, c'est à dire que $f^{(1)} \in \mathbb{Z}_3 \langle n_1, n_2 \rangle$. De plus, le coefficient en n_1^2 de $f^{(1)}$, noté classiquement $f_2^{(1)}(n_2)$, est une unité de $\mathbb{Z}_3 \langle n_2 \rangle$. En effet, le coefficient constant de $f_2^{(1)}(n_2)$ est 14, qui est inversible modulo 3, et tous les autres coefficients de $f_2^{(1)}(n_2)$ sont divisibles par 3. Les autres séries formelles $f_i^{(1)}(n_2)$ pour $i \geqslant 3$ sont également divisibles par 3 ce qui signifie exactement que $f^{(1)}$ est générale en n_1 d'ordre 2.
Le théorème de préparation de Weierstrass permet alors de montrer qu'il existe des fonctions $h^{(1)}$, $g_0^{(1)}$, $g_1^{(1)}$ et $g_2^{(1)}$ uniques, telles que

- la série formelle $h^{(1)}$ soit une unité de $\mathbb{Z}_3 \langle n_1, n_2 \rangle$ dont le premier coefficient vaut 1,
- les séries formelles $g_0^{(1)}$ et $g_1^{(1)}$ appartiennent à $\mathbb{Z}_3 \langle n_2 \rangle$,
- la série formelle $g_2^{(1)}$ soit une unité de $\mathbb{Z}_3 \langle n_2 \rangle$ et
- $f^{(1)}(n_1, n_2) = h^{(1)}(n_1, n_2) \left(g_0^{(1)}(n_2) + g_1^{(1)}(n_2)n_1 + g_2^{(1)}(n_2)n_1^2 \right)$.

Les séries formelles $f_i^{(1)}(n_2)$ étant connues modulo 3^3, nous allons maintenant calculer les séries formelles $g_0^{(1)}(n_2)$, $g_1^{(1)}(n_2)$ et $g_2^{(1)}(n_2)$ avec la même précision. Nous employons pour cela la méthode décrite au paragraphe II.4.3 et dans l'annexe B.1 et nous obtenons :

$$\begin{aligned} g_0^{(1)}(n_2) &= 21n_2^4 + 14n_2^2 && \pmod{3^3} , \\ g_1^{(1)}(n_2) &= 18n_2^5 + 6n_2^3 + 16n_2 && \pmod{3^3} , \\ g_2^{(1)}(n_2) &= 14 && \pmod{3^3} . \end{aligned}$$

Remarque : Le plus petit terme de la série formelle $g_0^{(1)}(n_2)$ est le terme en n_2^2 et $g_1^{(1)}(n_2)$ n'a pas de terme constant. Cela résulte de la remarque précédente concernant la série formelle $\theta_\infty^{(1)}(n_1, n_2)$ et des formules

$$\begin{aligned} g_0^{(1)}(n_2) &= f_0^{(1)}(n_2) , \\ g_1^{(1)}(n_2) &= f_1^{(1)}(n_2) - g_0^{(1)}(n_2)h_1^{(1)}(n_2) , \end{aligned}$$

donnée par (II.17). Cela signifie en particulier que le polynôme $g_0^{(1)}(n_2) + g_1^{(1)}(n_2)n_1 + g_2^{(1)}(n_2)n_1^2$ n'a ni terme constant ni termes linéaires.

Le théorème XII nous permet alors d'écrire :

$$\frac{\theta_\infty^{(1)}(n_1,n_2)}{9} = (g_0^{(1)}(n_2) + g_1^{(1)}(n_2)n_1 + g_2^{(1)}(n_2)n_1^2)(1 + \sum_{i=1}^{\infty} h_i^{(1)}(n_2)n_1^i) \ ,$$

avec $||h_i^{(1)}(n_2)|| < 1$ pour tout $i > 0$.
Il s'ensuit alors que la condition $\theta_\infty^{(1)}(n_1,n_2) = 0$ implique que le polynôme $g_0^{(1)}(n_2) + g_1^{(1)}(n_2)n_1 + g_2^{(1)}(n_2)n_1^2$ doit être nul.

La stratégie exposée à la fin du paragraphe II.4.3 suggère de faire le même raisonnement avec la seconde série formelle $\theta_\infty^{(2)}(n_1,n_2)$ puis de considérer le résultant des deux polynômes ainsi obtenus et de lui appliquer le théorème de Strassman. Nous allons cette fois suivre cette stratégie, du moins sur le fond.

Il n'est en effet pas possible d'appliquer directement le théorème de préparation de Weierstrass à la série formelle $\theta_\infty^{(2)}(n_1,n_2)$ car elle n'est pas générale en n_1. Le coefficient constant et le coefficient linéaire de $\theta_\infty^{(2)}(n_1,n_2)$ (resp. $189n_2^4 + 54n_2^2$ et $162n_2^3 + 225n_2$ modulo 3^5) ne sont pas des unités de $\mathbb{Z}_3\langle n_2\rangle$ et le coefficient de n_1^2 est de valuation 3-adique égale à 3 ainsi que tous les coefficients suivants. Il serait donc nécessaire de diviser cette série formelle par 3^3 pour que l'un de ses coefficients soit une unité de $\mathbb{Z}_3\langle n_2\rangle$. Ceci est impossible car le coefficient en n_1 (qui vaut $162n_2^3 + 225n_2$ modulo 3^5) n'est pas divisible par 3^3.

Nous avons à notre disposition deux astuces pour pallier à ce problème. La première serait de regarder si $\theta_\infty^{(2)}(n_1,n_2)$ est générale en n_2. Il faudrait alors faire de même avec la série formelle $\theta_\infty^{(1)}(n_1,n_2)$ afin d'obtenir au final deux polynômes en n_2 à coefficients dans $\mathbb{Z}_3\langle n_1\rangle$. La seconde astuce est de considérer non pas $\theta_\infty^{(2)}(n_1,n_2)$ seul mais une combinaison linéaire de $\theta_\infty^{(2)}(n_1,n_2)$ et de $\theta_\infty^{(1)}(n_1,n_2)$. En effet cela ne change en rien la condition sur la nullité de ces séries formelles. C'est cette idée que nous allons utiliser ici. Nous considérons donc la série formelle :

$$\begin{aligned} f^{(2)}(n_1,n_2) &= \frac{1}{9}\left(\theta_\infty^{(1)}(n_1,n_2) + \theta_\infty^{(2)}(n_1,n_2)\right) \\ &= 24n_2n_1^3 + (18n_2^2+26)n_1^2 + (14n_2+12n_2^3)n_1 + 15n_2^4 + 20n_2^2 \pmod{3^3} \ . \end{aligned}$$

Cette fois, le coefficient en n_1^2 est une unité de $\mathbb{Z}_3\langle n_2\rangle$ et les coefficients suivants sont tous divisibles par 3 si bien que $f^{(2)}$ est général en n_1 d'ordre 2. On en déduit comme précedemment l'existence de fonctions $h^{(2)}$, $g_0^{(2)}$, $g_1^{(2)}$ et $g_2^{(2)}$ uniques telles que

- la série formelle $h^{(2)}$ soit une unité de $\mathbb{Z}_3\langle n_1,n_2\rangle$ dont le premier coefficient vaut 1,
- les séries formelles $g_0^{(2)}$ et $g_1^{(2)}$ appartiennent à $\mathbb{Z}_3\langle n_2\rangle$,
- la série formelle $g_2^{(2)}$ soit une unité de $\mathbb{Z}_3\langle n_2\rangle$ et

– $f^{(2)}(n_1,n_2) = h^{(2)}(n_1,n_2)\left(g_0^{(2)}(n_2) + g_1^{(2)}(n_2)n_1 + g_2^{(2)}(n_2)n_1^2\right)$.

Les séries formelles $f_i^{(2)}(n_2)$ étant connues modulo 3^3, nous pouvons calculer les séries formelles $g_0^{(2)}(n_2)$, $g_1^{(2)}(n_2)$ et $g_2^{(2)}(n_2)$ avec la même précision :

$$\begin{array}{rcll} g_0^{(2)}(n_2) & = & 15n_2^4 + 20n_2^2 & \pmod{3^3} , \\ g_1^{(2)}(n_2) & = & 18n_2^5 + 6n_2^3 + 14n_2 & \pmod{3^3} , \\ g_2^{(2)}(n_2) & = & 18n_2^4 + 3n_2^2 + 26 & \pmod{3^3} . \end{array}$$

Remarque : On démontre, de manière similaire au cas précédent, que le plus petit terme de la série formelle $g_0^{(2)}(n_2)$ est le terme en n_2^2 et que la série formelle $g_1^{(2)}(n_2)$ n'a pas de terme constant.

La condition initiale $\theta_\infty^{(1)}(n_1,n_2)+\theta_\infty^{(2)}(n_1,n_2) = 0$ implique alors que le polynôme $g_0^{(2)}(n_2)+g_1^{(2)}(n_2)n_1 + g_2^{(2)}(n_2)n_1^2$ doit être nul.

Nous avons donc désormais à chercher pour quelles valeurs de n_2 les deux polynômes en n_1 de degré 2 à coefficients dans $\mathbb{Z}_3\langle n_2\rangle$ ainsi obtenus peuvent être simultanément nuls. Nous calculons pour cela le résultant de ces deux polynômes. D'après le lemme II.4.2 ce résultant est une série formelle de $\mathbb{Z}_3\langle n_2\rangle$ que nous noterons R et qui est donnée modulo 3^3 par :

$$R(n_2) \;=\; 12n_2^6 + 19n_2^4 \pmod{3^3}$$

Remarque : Les remarques précédentes impliquent que les deux polynômes en question n'ont ni terme constant ni terme linéaire si on les considère comme des séries formelles en deux variables. Cela implique de façon élémentaire que leur résultant est divisible par n_2^4 et admet donc $n_2 = 0$ comme zéro quadruple.

Le coefficient de $R(n_2)$ en n_2^4 est de valuation 3-adique nulle tandis que tous les coefficients suivants sont de valuation 3-adique supérieure ou égale à 1. Le théorème de Strassman appliqué à la série formelle $R(n_2)$ permet donc de prouver qu'il y a au plus 4 solutions 3-adiques à l'équation $R(n_2) = 0$. Or on connait déjà les 4 solutions données par $n_2 = 0$. On en déduit donc que $n_2 = 0$ est la seule solution 3-adique à l'équation $R(n_2) = 0$. Ainsi les deux polynômes $g_0^{(1)}(n_2) + g_1^{(1)}(n_2)n_1 + g_2^{(1)}(n_2)n_1^2$ et $g_0^{(2)}(n_2) + g_1^{(2)}(n_2)n_1 + g_2^{(2)}(n_2)n_1^2$ ne peuvent être simultanément nuls que si $n_2 = 0$.
Nous remplacons alors n_2 par 0 dans l'un de ces polynômes, le premier par exemple. Nous avons déjà remarqué que les séries formelles $g_0^{(1)}(n_2)$ et $g_1^{(1)}(n_2)$ ne possédaient pas de terme constant, si bien que $g_0^{(1)}(0) = g_1^{(1)}(0) = 0$. D'autre part $g_2^{(1)}(0) = 14 \pmod{3^3}$ est inversible dans $\mathbb{Z}_3$ et la condition $g_0^{(1)}(0) + g_1^{(1)}(0)n_1 + g_2^{(1)}(0)n_1^2 = 0$ implique alors que n_1 est nécessairement nul également.

Nous avons donc finalement démontré que $(0,0)$ est l'unique solution dans $\mathbb{Z}_3$ (et donc dans $\mathbb{Z}$) au système

$$\theta_\infty^{(1)}(n_1,n_2) = \theta_\infty^{(2)}(n_1,n_2) = 0 \ .$$

Cela prouve bien que le seul point de $E(\mathbb{Q}(\beta))$ de la forme $\infty + n_1Q_1 + n_2Q_2$ et ayant une abscisse dans $\mathbb{Q}$ est le point à l'infini lui même.

II.4.6 Fin de la preuve du théorème XI

De la même façon que pour θ_{G_2}, on démontre que $n_1 = 1, n_2 = 0$ est la seule solution au système

$$\theta^{(1)}_{3G_2}(n_1, n_2) = \theta^{(2)}_{3G_2}(n_1, n_2) = 0 \ .$$

Ainsi le seul point de $E(\mathbb{Q}(\beta))$ de la forme $3G_2 + n_1Q_1 + n_2Q_2$ et ayant une abscisse dans $\mathbb{Q}$ est le point $3G_2 + Q_1 = [0, 1]$.
Enfin, pour montrer que le système

$$\theta^{(1)}_{14G_2}(n_1, n_2) = \theta^{(2)}_{14G_2}(n_1, n_2) = 0$$

n'a aucune solution, il est suffisant d'appliquer le théorème de Strassman à la série formelle $\theta^{(2)}_{14G_2}(n_1, n_2)$ par rapport à l'une des deux variables puisque le terme de plus petite valuation 3-adique est le terme constant. Le théorème de préparation de Weierstrass n'a pas été nécessaire dans ce cas trivial. Il n'y a donc pas de point sur $E(\mathbb{Q}(\beta))$ de la forme $14G_2 + n_1Q_1 + n_2Q_2$.

Cela montre finalement que les seuls points sur $E(\mathbb{Q}(\beta))$ ayant une abscisse dans $\mathbb{Q}$ sont les points ∞, $[1, \pm(1-\beta^2)]$ et $[0, \pm 1]$. Il s'ensuit que les seules abscisses possibles pour un point rationnel sur la courbe $\mathcal{C}$ sont l'infini, 0 et 1.
Cela achève donc la preuve du théorème XI.

II.5 Conclusion et perspectives

La méthode de Chabauty elliptique a ainsi permis de résoudre de nombreuses équations pour lesquelles la méthode de Chabauty usuelle ne permettait pas de conclure. Nous avons également pu nous apercevoir que même lorsque cette méthode ne semblait pas aboutir, de nombreuses astuces permettaient de conclure favorablement. De plus le théorème de préparation de Weierstrass en deux variables nous a permis de généraliser la méthode de Chabauty elliptique au cas où la courbe elliptique considérée était de rang 2 sur un corps de nombres de degré supérieur à 3. Cela nous a donné la possibilité de résoudre de nouvelles équations et nous procure un outil supplémentaire pour la recherche des points rationnels sur les courbes de genre supérieur à 2.

Le théorème de préparation de Weierstrass que nous avons utilisé est exposé dans l'article de Sugatani [Sug 81] non pas pour deux variables mais pour un nombre quelconque de variables. La méthode que nous avons exposée est certainement très facilement généralisable au cas des courbes elliptiques de rang inférieur à n définies sur des corps de nombres de degré supérieur à $n+1$. Nous ne connaissons cependant pas d'exemple où une telle méthode serait nécessaire.

Cette méthode nous ouvre, de plus, de nouvelles perspectives. En effet, la méthode de Chabauty, développée par Flynn [Fly 97], pour les courbes de genre 2 et dont le rang de la jacobienne vaut 1 aboutit à la recherche des solutions p-adiques d'une série formelle en une variable. Le théorème de préparation de Weierstrass en deux variables et la méthode que nous avons décrite permettent de borner le nombre de solutions p-adiques d'un système de deux séries formelles en deux variables. Il est fort probable que ces considérations permettent de pouvoir conclure à une eventuelle méthode de Chabauty pour les courbes de genre 3 analogue à celle de Flynn pour les courbes de genre 2. Cependant l'arithmétique des courbes de genre 3 est encore trop succinte pour envisager une telle méthode. Sans prétendre en arriver jusqu'à ce point, l'objet du chapitre suivant est justement l'étude arithmétique des courbes de genre 3.

Chapitre III

La variété de Kummer

III.1 Surface de Kummer d'une courbe de genre 2

Les outils de la géométrie algébrique, même s'ils sont très puissants du point de vue théorique ne permettent pas actuellement d'effectuer des calculs complexes sur les courbes de genre 2 ou plus dans la pratique. Le meilleur exemple en est sans doute la finitude du nombre de points rationnels. La géométrie algébrique a permis à Faltings de la démontrer mais reste impuissante quant au calcul effectif d'une borne permettant le calcul explicite de tous les points rationnels. C'est la raison pour laquelle Flynn a introduit de nouveaux objets pour travailler sur les jacobiennes de courbes hyperelliptiques de genre 2 [Fly 93]. Nous allons exposer ici en partie ces méthodes. Un exposé plus complet pourra en être trouvé dans le livre de Cassels et Flynn [Cas-Fly 96].

Rappelons que l'on se place sur un corps $\mathbf{k}$ de caractéristique différente de 2 et que l'on considère une courbe $\mathcal{C}$ de genre 2 de la forme

$$\mathcal{C} \ : \ Y^2 = F(X) \ , \tag{III.1}$$

où

$$F(X) = f_0 + f_1 X + \cdots + f_6 X^6 \in \mathbf{k}[X] \ ,$$

est de degré 6 et n'a pas de facteur carré dans $\overline{\mathbf{k}}[X]$.
Rappelons également qu'un élément $\mathcal{X}$ de la jacobienne peut être représenté par une paire de points sur la courbe, c'est à dire

$$\mathcal{X} = \{[x_1, y_1], [x_2, y_2]\} \ .$$

L'élément neutre pour la loi de groupe sur la jacobienne, noté $\mathcal{O}$, est alors donné par la classe des diviseurs vérifiant $x_1 = x_2$ et $y_1 = -y_2$. Flynn introduit les fonctions de $\mathcal{X}$, symétriques en $[x_1, y_1]$ et $[x_2, y_2]$, ayant un pôle seulement en $\mathcal{O}$ et moins grand que $x_1^2 x_2^2$ à l'infini. Ces fonctions forment un espace vectoriel sur $\mathbf{k}$ et Flynn en extrait une base formée de 16 fonctions que nous n'écrirons pas ici mais qui peuvent être trouvée dans son

livre [Cas-Fly 96].
Cette construction permet d'identifier la jacobienne de la courbe $\mathcal{C}$ avec le lieu projectif de ces 16 fonctions dans $\mathbb{P}^{15}$. Cependant, une telle représentation de la jacobienne est trop lourde à manipuler. Cela est d'autant plus ennuyeux que nous nous intéresserons dans la suite de ce chapitre au cas des courbes de genre 3 pour lesquelles cette méthode permet de plonger la jacobienne dans $\mathbb{P}^{63}$.
Flynn a donc imposé une restriction supplémentaire qui consiste à identifier deux points reliés par l'involution hyperelliptique (c'est à dire l'application sur la courbe $\mathcal{C}$ qui à un point $[x, y]$ associe le point $[x, -y]$). Cette restriction est la même que celle que l'on fait dans le cas des courbes elliptiques lorsque l'on décide de ne s'occuper que des abscisses des points en gardant bien en tête qu'elles correspondent à deux points sur la courbe elliptique opposés l'un de l'autre.
Flynn introduit ainsi la surface de Kummer que nous noterons $\mathcal{K}$ dans la suite. Cette surface de Kummer est le lieu projectif dans $\mathbb{P}^3$ de 4 des 16 fonctions précédentes. Nous noterons ces 4 éléments ξ_1, ξ_2, ξ_3 et ξ_4 et nous les appellerons désormais les coordonnées dans $\mathbb{P}^3$ d'un élément de la surface de Kummer. Ce lieu projectif est donné par une quartique explicite en $(\xi_1, \xi_2, \xi_3, \xi_4)$ qui correspond en fait à une traduction de l'équation (III.1).
Il construit ainsi une application, notée κ, du groupe de Mordell-Weil de la jacobienne dans la surface de Kummer, définie de la façon suivante :

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

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

$$F_0(x_1, x_2) = 2f_0 + f_1(x_1 + x_2) + 2f_2 x_1 x_2 + f_3(x_1 + x_2)x_1 x_2 + 2f_4 x_1^2 x_2^2 + f_5(x_1 + x_2)x_1^2 x_2^2 + 2f_3 x_1^3 x_2^3 \ .$$

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, c'est à dire lorsqu'ils sont reliés par l'involution hyperelliptique.
Ainsi, sur la surface 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 surface de Kummer, on a donc perdu la structure de groupe qui constituait pourtant le principal intérêt de la jacobienne.
Il en subsiste cependant des traces. C'est par exemple le cas de la multiplication par 2.

Il parait 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 $\xi_i(\mathcal{B})$). On a en effet le théorème suivant :

Théorème XIII (Flynn [Fly 93]) *Il existe des polynômes explicites B_{ij} biquadratiques en $\xi_i(\mathcal{A})$, $\xi_i(\mathcal{B})$ tels que projectivement, on ait*

$$(\xi_i(\mathcal{A}+\mathcal{B})\xi_j(\mathcal{A}-\mathcal{B}) + \xi_i(\mathcal{A}-\mathcal{B})\xi_j(\mathcal{A}+\mathcal{B}))_{1\leqslant i,j\leqslant 4} = (2B_{ij}(\mathcal{A},\mathcal{B}))_{1\leqslant i,j\leqslant 4} \ .$$

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 $\mathbb{Z}[f_0, \ldots, f_6]$.

Nous allons maintenant expliquer comment Flynn calcule explicitement ces traces de la loi de groupe sur la jacobienne ainsi que ce que l'on peut en faire.

III.1.1 Addition d'un élément d'ordre 2

Comme expliqué précédemment, l'addition d'un élément de 2-torsion est bien définie sur la surface de Kummer. De plus, cette application est linéaire dans $\mathbb{P}^3$ et nous exposons donc dans ce paragraphe la construction de la matrice correspondante. Le programme maple correspondant est donné dans l'annexe B.2 et est disponible par ftp.

Soient donc θ_1 et θ_2 deux racines de $F(X)$. Les points $[\theta_1, 0]$ et $[\theta_2, 0]$ sont des points de Weierstrass de la courbe $\mathcal{C}$ et la classe de diviseurs représentée par $\mathcal{A} = \{[\theta_1, 0], [\theta_2, 0]\}$ est un élément d'ordre 2 sur la jacobienne. Nous cherchons à exprimer l'addition d'un tel élément avec un point général de la surface de Kummer $\mathcal{X} = \{[x_1, y_1], [x_2, y_2]\}$. Posons

$$G(X) = (X - \theta_1)(X - \theta_2), \qquad F(X) = G(X)H(X) \ .$$

On doit trouver le point de la surface de Kummer se situant à l'intersection de la courbe $\mathcal{C}$ et de $Y = M(X)$, où la cubique $M(X)$ doit passer par $\mathcal{A}$ et $\mathcal{X}$. Un rapide calcul permet d'écrire

$$M(X) = G(X)M_0(X) \ ,$$

avec

$$M_0(X) = \frac{X - x_1}{x_2 - x_1}\frac{y_2}{G(x_2)} + \frac{X - u}{x_1 - x_2}\frac{y_1}{G(x_1)} \ .$$

Afin de trouver l'intersection résiduelle de cette cubique avec la courbe $\mathcal{C}$, nous allons devoir calculer $M_0(X)^2$. Dans cette expression, on peut remplacer y_1^2 par $F(x_1)$ et y_2^2 par $F(x_2)$. De plus, on peut éliminer le terme en y_1y_2 en utilisant $\xi_4 = \xi_4(\mathcal{X})$ de telle sorte que:

$$G(x_1)G(x_2)M_0(X)^2 = (X - x_1)(X - x_2)\xi_4 + L \ ,$$

où

$$L = \frac{(X-x_1)^2 G(x_1)H(x_2) + (X-x_2)^2 G(x_2)H(x_1) - (X-x_1)(X-x_2)F_0(x_1,x_2)}{(x_1-x_2)^2} \ ,$$

est un polynôme en X, x_1, x_2 symétrique en x_1, x_2.
En substituant $Y = M(X)$ dans l'équation de $\mathcal{C}$, on déduit que l'abscisse de l'intersection résiduelle doit satisfaire $H(X) = G(X)M_0(X)^2$ c'est à dire

$$\xi_4 G(X) + N = 0 \ ,$$

où

$$N = \frac{G(X)L - H(X)G(x_1)G(x_2)}{(X-x_1)(X-x_2)}$$

est également un polynôme en X, x_1, x_2 quadratique en X et linéaire et symétrique en x_1, x_2. L'équation $\xi_4 G(X) + N = 0$ peut alors s'écrire sous la forme

$$\xi_0^* X^2 - \xi_1^* X + \xi_2^* = 0 \ ,$$

où les ξ_i^* sont des formes linéaires en les ξ_j. Ce polynôme de degré 2 en X donne ainsi les trois premières coordonnées sur la surface de Kummer de l'intersection résiduelle en fonction des coordonnées du point général $\mathcal{X}$. On peut donc écrire

$$\xi_i^* = \sum_{j=1}^{4} w_{ij}\xi_j \qquad (i = 1,2,3) \ ,$$

où les w_{ij} sont données par

$$\left[\begin{array}{cccc} g_2^2h_0 + g_0g_2h_2 - g_0^2h_4 & g_0g_2h_3 - g_0g_1h_4 & g_1g_2h_3 - g_1^2h_4 + 2g_0g_2h_4 & g_2 \\ -g_0g_2h_1 - g_0g_1h_2 + g_0^2h_3 & g_2^2h_0 - g_0g_2h_2 + g_0^2h_4 & g_2^2h_1 - g_1g_2h_2 - g_0g_2h_3 & -g_1 \\ -g_1^2h_0 + 2g_0g_2h_0 + g_0g_1h_1 & -g_1g_2h_0 + g_0g_2h_1 & -g_2^2h_0 + g_0g_2h_2 + g_0^2h_4 & g_0 \end{array}\right] .$$

si g_j et h_j désignent les coefficients de X^j dans G(X) et H(X).

Afin de déterminer la dernière coordonnée, on utilise le fait qu'on est en train d'additionner un élément d'ordre 2. Les ξ_j peuvent donc aussi être exprimés en fonction des ξ_i^* à l'aide des mêmes coefficients w_{ij} à une constante multiplicative près. Autrement dit, les w_{ij} forment une matrice 4×4, notée$\mathbf{W}$, telle que $\mathbf{W}^2$ soit une matrice scalaire. Cela permet d'obtenir la dernière ligne de la matrice :

$$\begin{aligned} w_{41} &= -g_1g_2^2h_0h_1 + g_1^2g_2h_0h_2 + g_0g_2^2h_1^2 - 4g_0g_2^2h_0h_2 - g_0g_1g_2h_1h_2 + g_0g_1g_2h_0h_3 - g_0^2g_2h_1h_3 \\ w_{42} &= g_1^2g_2h_0h_3 - g_1^3h_0h_4 - 2g_0g_2^2h_0h_3 - g_0g_1g_2h_1h_3 + 4g_0g_1g_2h_0h_4 + g_0g_1^2h_1h_4 - 2g_0^2g_2h_1h_4 \\ w_{43} &= -g_0g_2^2h_1h_3 - g_0g_1g_2h_2h_3 + g_0g_1g_2h_1h_4 + g_0g_1^2h_2h_4 + g_0^2g_2h_3^2 - 4g_0^2g_2h_2h_4 - g_0^2g_1h_3h_4 \\ w_{44} &= -g_2^2h_0 - g_0g_2h_2 - g_0^2h_4 \ . \end{aligned}$$

Remarque : La constante c telle que $\mathbf{W}^2 = c\mathbf{I}$ est égale au résultant des polynômes $G(X)$ et $H(X)$.

Ainsi le produit matriciel de cette matrice $\mathbf{W}$ et d'un point général $\mathcal{X}$ de la surface de Kummer donne les coordonnées dans la surface de Kummer de $\mathcal{X} + \{[\theta_1, 0], [\theta_2, 0]\}$.

Nous allons maintenant expliquer brièvement comment Flynn calcule les formes biquadratiques B_{ij} du théorème XIII qui permettent d'avoir une idée de ce qui subsiste de la loi de groupe sur la surface de Kummer.

III.1.2 Les formes biquadratiques

Rappelons que l'objet de ce paragraphe est d'exposer le calcul explicite des formes biquadratiques

$$\left(\xi_i(\mathcal{A}+\mathcal{B})\xi_j(\mathcal{A}-\mathcal{B}) + \xi_i(\mathcal{A}-\mathcal{B})\xi_j(\mathcal{A}+\mathcal{B})\right)_{1\leqslant i,j\leqslant 4} = \left(2B_{ij}(\mathcal{A},\mathcal{B})\right)_{1\leqslant i,j\leqslant 4} \quad ,\text{(III.2)}$$

qui interviennent dans le théorème XIII.
La façon dont Flynn traite ce problème 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 du point de 2-torsion.
Pour être plus précis, si $\mathcal{B} = \{[\theta_1, 0], [\theta_2, 0]\}$ est un point de 2-torsion général et si $\mathbf{W}$ désigne la matrice de l'addition par $\mathcal{B}$ obtenue grâce au paragraphe III.1.1, les formes biquadratiques (III.2) sont projectivement égales à $2\xi_i(\mathbf{W}(\mathcal{A}))\,\xi_j(\mathbf{W}(\mathcal{A}))$. Ceci est une forme quadratique en $(\xi_1(\mathcal{A}), \xi_2(\mathcal{A}), \xi_3(\mathcal{A}), \xi_4(\mathcal{A}))$ et si on regarde les coefficients de chaque produit $\xi_l(\mathcal{A})\xi_m(\mathcal{A})$ comme une forme quadratique en $(\xi_1(\mathcal{B}), \xi_2(\mathcal{B}), \xi_3(\mathcal{B}), \xi_4(\mathcal{B}))$, on peut en déduire facilement les coefficients des B_{ij}.
On peut ainsi déduire les formes biquadratiques B_{ij} pour un $\mathcal{B}$ quelconque à partir du cas particulier des éléments d'ordre 2 car pour un élément d'ordre 2 arbitraire, les 10 produits $\xi_i(\mathcal{B})\xi_j(\mathcal{B})$ sont linéairement indépendants sur $\mathbb{Q}(f_0, \ldots, f_6)$.

Cette condition ne sera plus vérifiée dans le cas des courbes de genre 3 et cette méthode nécessitera donc des modifications. On peut aisément déduire de ces formes biquadratiques l'expression de la loi de duplication sur la surface de Kummer en remplaçant simplement $\mathcal{B}$ par $\mathcal{A}$ dans les formes biquadratiques (III.2). Les expressions explicites de ces formes biquadratiques ainsi que les formules de la loi de duplication 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.

III.1.3 Applications

1 Méthode de Chabauty

Ces traces de la loi de groupe sur la surface de Kummer sont à l'origine de diverses applications concernant les courbes de genre 2. C'est en effet à partir des formes biquadratiques que Flynn a élaboré une méthode de Chabauty explicite pour les courbes de genre 2 dont le rang de la jacobienne est égal à 1 [Fly 97]. Il faut tout de même garder à l'esprit que ce n'est pas le seul outil intervenant dans cette méthode et que sa généralisation aux courbes hyperelliptiques de genre 3 ne permettra sans doute pas d'élaborer une méthode de Chabauty explicite analogue à celle de Flynn précédemment citée. Et ce, même si le théorème de préparation de Weierstrass en deux variables développé au paragraphe II.4 nous a fournit un autre nouvel outil qui pourrait faire progresser une telle méthode.

2 Théorie des hauteurs

Dans un registre tout à fait différent, cela permet de définir une fonction hauteur, explicite et accessible en pratique, sur la jacobienne des courbes de genre 2. 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 2, de prendre la hauteur standard H dans $\mathbb{P}^3(\mathbb{Q})$ des coordonnées de la surface de Kummer ; nous noterons $H_{\mathcal{K}}$ cette fonction. Le théorème XIII permet alors de démontrer que $H_{\mathcal{K}}$ est une bonne fonction hauteur [Fly 95] :

Théorème XIV (Flynn [Fly 95]) *La fonction*

$$\begin{array}{rcccl} H_{\mathcal{K}} & : & \mathcal{J}(\mathbb{Q}) & \longrightarrow & \mathbb{Z}^+ \\ & & \mathcal{A} & \longmapsto & H\left(\xi_1(\mathcal{A}), \xi_2(\mathcal{A}), \xi_3(\mathcal{A}), \xi_4(\mathcal{A})\right) \end{array}$$

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, une telle théorie des hauteurs permet d'obtenir une procédure efficace pour calculer le groupe de torsion de $\mathcal{J}(\mathbb{Q})$. On a en effet la proposition suivante :

Proposition III.1.1 *Si $H_{\mathcal{K}}$ est une fonction hauteur sur $\mathcal{J}(\mathbb{Q})$, alors, avec les notations du théorème XIV, tout élément $\mathcal{A}$ de $\mathcal{J}(\mathbb{Q})$ d'ordre fini satisfait $H_{\mathcal{K}}(\mathcal{A}) \leqslant C_2^{\frac{1}{3}}$.*

3 La descente infinie

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 XIII 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 surface 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 III.1.1. 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 surface de Kummer et τ est l'application qui à $[\xi_1, \xi_2, \xi_3, \xi_4]$ associe $[\xi_1^2, \xi_2^2, \xi_3^2, \xi_4^2]$.
Il en déduit alors 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.

Remarque : Nous avons dans ce paragraphe pris $\mathbb{Q}$ comme corps de base. Ces résultats se généralisent cependant facilement au cas des corps de nombres avec quelques petites modifications [Sil 90], [Fly 95], [Fly-Sma 97].

En dehors de la méthode de Chabauty, les travaux que nous avons effectués sur la variété de Kummer d'une courbe de genre 3 devraient permettre de généraliser plus ou moins bien ces applications.

III.2 La variété de Kummer d'une courbe de genre 3

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

$$\mathcal{C} : Y^2 = F(X) \ ,$$

avec

$$F(X) = f_7 X^7 + \cdots + f_1 X + f_0 \in \mathbf{k}[X] \ ,$$

de degré 7 et sans facteur carré.

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

$$\begin{array}{rcl}
a_0 & = & 1 \\
a_1 & = & x_1 + x_2 + x_3 \\
a_2 & = & x_1 x_2 + x_1 x_3 + x_2 x_3 \\
a_3 & = & x_1 x_2 x_3 \\
c_0 & = & a_0 b_0^2 - f_7 a_1^3 + f_7 a_2 a_1 - f_6 a_1^2 + 3 f_7 a_3 + 2 f_6 a_2 \\
c_1 & = & a_1 b_0^2 + 2 a_0 b_0 b_1 - f_7 a_1^4 + 3 f_7 a_2 a_1^2 - f_6 a_1^3 - f_7 a_2^2 - f_7 a_3 a_1 + 2 f_6 a_2 a_1 - f_5 a_1^2 + 2 f_5 a_2 \\
c_2 & = & a_0 b_1^2 - a_2 b_0^2 + f_7 a_2 a_1^3 - 2 f_7 a_2^2 a_1 + f_6 a_2 a_1^2 + f_7 a_3 a_2 - f_6 a_2^2 + f_5 a_2 a_1 - 3 f_5 a_3 \\
c_3 & = & a_1 b_1^2 + 2 a_2 b_0 b_1 + a_3 b0^2 + f_7 a_2^2 a_1^2 - f_7 a_3 a_1^3 + f_7 a_3 a_2 a_1 - f_7 a_2^3 + f_6 a_2^2 a_1 - f_6 a_3 a_1^2 + \\
 & & f_5 a_2^2 - f_5 a_3 a_1 \ ,
\end{array}$$

avec

$$\begin{array}{rcl}
b_0 & = & (x_1 y_2 - x_2 y_1 - x_3 y_2 + x_3 y_1 - x_1 y_3 + x_2 y_3) / \delta \ , \\
b_1 & = & \left(x_3^2 y_2 - x_3^2 y_1 + x_2^2 y_1 + y_3 x_1^2 - y_2 x_1^2 - y_3 x_2^2\right) / \delta \ , \\
\delta & = & (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \ .
\end{array}$$

Dans ces conditions, l'application

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

définit un plongement de la variété de Kummer dans $\mathbb{P}^7$.
Dans le cas du genre 2, la surface 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 :

$$a_0 c_3 - a_1 c_2 - a_2 c_1 - a_3 c_0 - 2 f_5 a_1 a_3 + f_5 a_2^2 + 2 f_6 a_2 a_3 + 3 f_7 a_3^2 = 0 \ . \qquad \text{(III.3)}$$

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, on perd 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. L'objectif de la fin de ce chapitre est d'étudier ces traces de la loi de groupe. Nous allons, dans un premier temps, calculer la matrice d'addition d'un point de 2-torsion.

III.2.1 Addition d'un point de 2-torsion

Soit $\mathcal{A} = \{[\theta_1, 0], [\theta_2, 0], [\theta_3, 0]\}$ un élément d'ordre 2 de la jacobienne (c'est à dire que θ_1, θ_2 et θ_3 sont des racines de $F(X)$). On pose

$$G(X) = (X - \theta_1)(X - \theta_2)(X - \theta_3) \text{ et } F(X) = G(X)H(X) \ .$$

Dans la suite les g_j et h_j désigneront les coefficients de X^j dans $G(X)$ et $H(X)$.

On veut trouver la matrice correspondant à l'addition de cet élément d'ordre 2 avec un élément quelconque de la jacobienne. Soit donc $\mathcal{X} = \{[x_1, y_1], [x_2, y_2], [x_3, y_3]\}$ un point général de la jacobienne et $[a_0, a_1, a_2, a_3, c_0, c_1, c_2, c_3]$ ses coordonnées dans la variété de Kummer.

Dans un premier temps, nous allons utiliser la loi de groupe définie de façon géométrique comme dans l'introduction pour calculer la somme de cet élément $\mathcal{X}$ et de l'élément $\mathcal{A}$ d'ordre 2 sur la jacobienne. On doit pour cela trouver un polynôme M de degré 4 et un élément γ de $\mathbf{k}$ tels que l'équation

$$(X - \gamma) Y = M(X)$$

passe par les points $[\theta_1, 0], [\theta_2, 0], [\theta_3, 0], [x_1, y_1], [x_2, y_2]$ et $[x_3, y_3]$. Du fait que les trois premiers points ont une ordonnée nulle, la quartique $M(X)$ doit être annulée par θ_1, θ_2 et θ_3. Cette quartique est donc de la forme $G(X)(\alpha X + \beta)$ où α et β sont des éléments de $\mathbf{k}$. En utilisant le système donné par les équations

$$(x_i - \gamma) y_i = G(x_i)(\alpha x_i + \beta) \qquad i = 1, 2, 3 \ ,$$

on montre aisément que $\gamma = \frac{A}{d}, \alpha = \frac{a}{d}$ et $\beta = \frac{b}{d}$ avec

$$\begin{aligned}
A &= y_1 G(x_2) G(x_3) x_1 (x_3 - x_2) + y_2 G(x_1) G(x_3) x_2 (x_1 - x_3) + y_3 G(x_1) G(x_2) x_3 (x_2 - x_1) \\
d &= y_1 G(x_2) G(x_3)(x_3 - x_2) + y_2 G(x_1) G(x_3)(x_1 - x_3) + y_3 G(x_1) G(x_2)(x_2 - x_1) \\
a &= y_2 y_3 G(x_1)(x_2 - x_3) + y_1 y_3 G(x_2)(x_3 - x_1) + y_1 y_2 G(x_3)(x_1 - x_2) \\
b &= x_1 y_2 y_3 G(x_1)(x_2 - x_3) + x_2 y_1 y_3 G(x_2)(x_3 - x_1) + x_3 y_1 y_2 G(x_3)(x_1 - x_2) \ .
\end{aligned}$$

Afin de calculer l'intersection résiduelle de cette courbe et de la courbe $\mathcal{C}$, nous allons devoir élever au carré ces expressions. Nous devrons ensuite en éliminer les termes en y_1, y_2 et y_3 (qui sont toujours des termes quadratiques). Les termes y_i^2 seront bien sûr remplacés par $F(x_i)$, mais nous devons trouver une manière d'éliminer les termes en $y_i y_j$. Dans le cas des courbes de genre 2, on éliminait le terme $y_1 y_2$ en utilisant la dernière coordonnée ξ_4. Dans le cas présent, nous allons devoir exprimer les termes $y_1 y_2, y_1 y_3$ et $y_2 y_3$ en fonction des a_i et des c_i. Nous allons pour cela nous servir de b_0 et b_1 puisque ce sont les seuls termes comportant des y_i. Dans cette optique, on pose

$$\begin{aligned}
H_0 &= -f_7 a_1^3 + f_7 a_2 a_1 - f_6 a_1^2 + 3 f_7 a_3 + 2 f_6 a_2 \ , \\
H_1 &= -f_7 a_1^4 + 3 f_7 a_2 a_1^2 - f_6 a_1^3 - f_7 a_2^2 - f_7 a_3 a_1 + 2 f_6 a_2 a_1 - f_5 a_1^2 + 2 f_5 a_2 \ , \\
H_2 &= f_7 a_2 a_1^3 - 2 f_7 a_2^2 a_1 + f_6 a_2 a_1^2 + f_7 a_3 a_2 - f_6 a_2^2 + f_5 a_2 a_1 - 3 f_5 a_3 \ , \\
H_3 &= f_7 a_2^2 a_1^2 - f_7 a_1^3 a_3 + f_7 a_1 a_2 a_3 - f_7 a_2^3 + f_6 a_2^2 a_1 - f_6 a_3 a_1^2 + f_5 a_2^2 - f_5 a_3 a_1 \ ,
\end{aligned}$$

de telle sorte qu'on ait

$$\begin{aligned}
a_0 b_0^2 &= c_0 - H_0 \ , \\
a_1 b_0^2 + 2 a_0 b_0 b_1 &= c_1 - H_1 \ , \\
a_0 b_1^2 - a_2 b_0^2 &= c_2 - H_2, \\
a_1 b_1^2 + 2 a_2 b_0 b_1 + a_3 b_0^2 &= c_3 - H_3 \ .
\end{aligned}$$

Les termes $y_1 y_2, y_1 y_3$ et $y_2 y_3$ apparaissent dans les expressions de $b_0^2, b_0 b_1$ et b_1^2. Il suffit alors de résoudre un système, après avoir pris soin de remplacer les y_i^2 par $F(x_i)$, pour obtenir le résultat suivant :

$$\begin{pmatrix} 2(x_3-x_2)(x_1-x_3)y_1y_2 \\ 2(x_3-x_2)(x_2-x_1)y_1y_3 \\ 2(x_1-x_3)(x_2-x_1)y_2y_3 \end{pmatrix} = \frac{1}{\delta} \begin{pmatrix} x_1x_2(x_2-x_1) & (x_2+x_1)(x_2-x_1) & x_2-x_1 \\ x_1x_3(x_1-x_3) & (x_1+x_3)(x_1-x_3) & x_1-x_3 \\ x_2x_3(x_3-x_2) & (x_3+x_2)(x_3-x_2) & x_3-x_2 \end{pmatrix} \begin{pmatrix} (c_0-H_0)\delta^2-a_0b_{00} \\ (c_1-H_1)\delta^2-(a_1b_{00}+2a_0b_{01}) \\ (c_2-H_2)\delta^2-(a_0b_{11}-a_2b_{00}) \end{pmatrix} \ ,$$

où b_{00} (resp. b_{01}, b_{11}) désigne la partie de $\delta^2 b_0^2$ (resp. $\delta^2 b_0 b_1, \delta^2 b_1^2$) ne comportant pas les termes en $y_1 y_2, y_1 y_3$ et $y_2 y_3$:

$$\begin{aligned}
b_{00} &= (x_3 - x_2)^2 F(x_1) + (x_1 - x_3)^2 F(x_2) + (x_1 - x_2)^2 F(x_3) \\
b_{01} &= \left(x_2^2 - x_3^2\right)(x_3 - x_2) F(x_1) + \left(x_1^2 - x_3^2\right)(x_3 - x_1) F(x_2) + \left(x_1^2 - x_2^2\right)(x_2 - x_1) F(x_3) \\
b_{11} &= \left(x_2^2 - x_3^2\right)^2 F(x_1) + \left(x_1^2 - x_3^2\right)^2 F(x_2) + \left(x_1^2 - x_2^2\right)^2 F(x_3) \ .
\end{aligned}$$

L'intersection de la courbe définie par l'équation $(dX - A)\, Y = G(X)\,(aX + b)$ et de la courbe $\mathcal{C}$ est alors donnée par

$$(dX - A)^2 F(X) = G(X)^2 (aX + b)^2 \ .$$

Autrement dit, une fois éliminés les éléments d'ordre 2, l'intersection est composée des solutions de l'équation

$$(dX - A)^2 H(X) - G(X)(aX + b)^2 = 0 \ .$$

Dans $(dX - A)^2$ ainsi que dans $(aX + b)^2$, on remplace les y_i^2 par $F(x_i)$ et les $y_i y_j$ par les valeurs exprimées ci-dessus. Posons alors

$$L = (dX - A)^2 H(X) - G(X)(aX + b)^2 \ .$$

Grâce à ces substitutions, L ne contient plus de termes en y_i. De plus L est un polynôme symétrique en x_1, x_2, x_3 et de degré 6 en X.
Nous allons maintenant exprimer le fait que x_1, x_2 et x_3 sont les abscisses de points appartenant à l'intersection de la courbe définie par $(dX - A)\, Y = G(X)\,(aX + b)$ et de la courbe $\mathcal{C}$. Nous posons pour cela

$$N = \frac{(dX - A)^2 H(X) - G(X)(aX + b)^2}{(X - x_1)\,(X - x_2)\,(X - x_3)} \ .$$

Cette fraction rationnelle est donc un polynôme. De plus N est linéaire et symétrique en x_1, x_2, x_3 et de degré 3 en X. En exprimant ce polynôme symmétrique en x_1, x_2 et x_3 à l'aide des fonctions symétriques élémentaires a_i, on obtient un polynôme linéaire en $a_0, a_1, a_2, a_3, c_0, c_1, c_2, c_3$ de degré 3 en X.

Les racines de ce polynôme définissent alors les abscisses des trois derniers points d'intersection entre la courbe $\mathcal{C}$ et la courbe définie par l'équation $(X - \gamma)\, Y = M\,(X)$. La somme de ces trois points est donc un diviseur définissant une classe de diviseurs de $\mathcal{J}(\mathbf{k})$ qui n'est autre que la somme des éléments $\mathcal{X}$ et $\mathcal{A}$. Il ne parait cependant pas aisé de calculer explicitement ces racines. Toutefois, notre but n'est pas de trouver ces racines mais de trouver les coordonnées de cet élément dans la variété de Kummer. Or, et c'est ici qu'apparait l'un des avantages de la variété de Kummer, les 4 premières coordonnées dans la variété de Kummer sont données, au signe près, par les coefficients du polynôme obtenu. Si l'on note $\xi_i(\mathcal{X})$ la $i^{\text{ème}}$ coordonnée de $\mathcal{X}$ dans la variété de Kummer, on peut écrire

$$\xi_i(\mathcal{X} + \mathcal{A}) = \sum_{j=1}^{8} w_{ij}\ \xi_j(\mathcal{X}) \qquad \text{pour } i = 1, 2, 3, 4 \ .$$

Les valeurs des w_{ij} sont données dans l'appendice C et disponible sur le site ftp

`ftp://megrez.math.u-bordeaux.fr/pub/duquesne/`.

Reste à calculer les quatre dernières coordonnées. Comme dans le cas des courbes de genre 2, lorsqu'on additionne un élément d'ordre 2, on peut inversement exprimer les $\xi_j(\mathcal{X})$ en fonction des $\xi_i(\mathcal{X}+\mathcal{A})$ à l'aide des mêmes coefficients. Autrement dit, les w_{ij} forment une matrice 8×8, notée $\mathbf{W}$, dont le carré est une matrice scalaire. Il existe donc une constante c telle que $\mathbf{W}^2 = c\, \mathbf{I}_8$. Cependant, nous allons maintenant voir que, dans ce cas, cette propriété n'est pas suffisante pour calculer de manière unique les lignes manquantes. Regardons désormais la matrice $\mathbf{W}$ comme une matrice par blocs de dimension 4×4 :

$$\mathbf{W} = \begin{pmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{pmatrix}.$$

Les matrices $\mathbf{A}$ et $\mathbf{B}$ sont connues et $\mathbf{B}$ est inversible. Le carré de $\mathbf{W}$ étant une matrice scalaire, on obtient les relations suivantes:

$$\begin{aligned} \mathbf{A}^2 + \mathbf{BC} &= c\,\mathbf{I}_4 \ , && \text{(III.4)} \\ \mathbf{AB} + \mathbf{BD} &= 0 \ , && \text{(III.5)} \\ \mathbf{CA} + \mathbf{DC} &= 0 \ , && \text{(III.6)} \\ \mathbf{CB} + \mathbf{D}^2 &= c\,\mathbf{I}_4 \ . && \text{(III.7)} \end{aligned}$$

Les équations (III.5) et (III.7) permettent de calculer respectivement les matrices $\mathbf{D}$ et $\mathbf{C}$ en fonction des matrices $\mathbf{A}$ et $\mathbf{B}$:

$$\begin{aligned} \mathbf{D} &= -\mathbf{B}^{-1}\mathbf{AB} \ , \\ \mathbf{C} &= c\mathbf{B}^{-1} - \mathbf{B}^{-1}\mathbf{A}^2 \ . \end{aligned}$$

De cette façon, $\mathbf{D}$ est définie de manière unique mais $\mathbf{C}$ dépend de la constante c. D'autre part, on vérifie facilement que ces matrices vérifient les équations (III.4) et (III.6). La condition sur le carré de la matrice $\mathbf{W}$, qui était suffisante dans le cas des courbes de genre 2 n'est donc pas suffisante ici. Afin de déterminer la constante c, nous utilisons le fait que si $\mathbf{W_1}$ (resp. $\mathbf{W_2}$) désigne la matrice de l'addition d'un élément d'ordre 2 $\mathcal{A}_1$ (resp. $\mathcal{A}_2$), alors il existe une constante C telle que

$$\mathbf{W_1}(\mathcal{A}_2) = C\mathbf{W_2}(\mathcal{A}_1) \ ,$$

puisque ces deux termes donnent les coordonnées dans la variété de Kummer de $\mathcal{A}_1 + \mathcal{A}_2$. Si de plus $\mathbf{W_1}^2 = c_1\mathbf{I}_8$ et $\mathbf{W_2}^2 = c_2\mathbf{I}_8$, cette équation donne 8 relations sur les lignes de la matrice $\mathbf{W}$. Les 4 premières relations ne dépendent pas de c_1 et de c_2 et permettent de déterminer la constante C. Les quatres dernières relations permettent alors de déterminer c_1 et c_2. Cela nous permet finalement de montrer que la constante c est égale au coefficient dominant f_7 multiplié par le résultant des polynômes $G(X)$ et $H(X)$. La matrice $\mathbf{W}$ de l'addition d'un point de 2-torsion est ainsi complètement déterminée et ses coefficients sont donnés dans l'appendice C et disponible par ftp. Comme nous l'avons déjà vu dans le cas des courbes de genre 2, le passage à la variété de Kummer ne permet pas de distinguer l'élément $\mathcal{A}$ de l'élément $-\mathcal{A}$ et il est donc impossible de savoir si on a calculé $\mathcal{A}+\mathcal{B}$ ou $\mathcal{A}-\mathcal{B}$. Cependant les $\xi_i(\mathcal{A}+\mathcal{B})\xi_j(\mathcal{A}-\mathcal{B}) + \xi_i(\mathcal{A}-\mathcal{B})\xi_j(\mathcal{A}+\mathcal{B})$ peuvent être déterminés.

III.2.2 Les formes biquadratiques

On s'intéresse désormais au calcul explicite des expressions

$$\xi_i(\mathcal{A}+\mathcal{B})\xi_j(\mathcal{A}-\mathcal{B}) + \xi_i(\mathcal{A}-\mathcal{B})\xi_j(\mathcal{A}+\mathcal{B}).$$

Le corps de base est $\mathbf{k}(f_0, \ldots, f_7)$. Le principe est le même que pour les courbes de genre 2 : on calcule ces expressions pour un élément d'ordre 2 puis on en déduit la formule dans le cas général en utilisant le fait que les produits des coordonnées de $\mathcal{B}$ sont (presque) indépendants sur $\mathbf{k}(f_0, \ldots, f_7)$. Soit donc $\mathcal{B} = \{[\theta_1, 0], [\theta_2, 0], [\theta_3, 0]\}$ un élément d'ordre 2. Notons $s = \theta_1 + \theta_2 + \theta_3, b = \theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3$ et $p = \theta_1\theta_2\theta_3$ les fonctions symétriques élémentaires, les coordonnées de $\mathcal{B}$ dans la variété de Kummer s'écrivent

$$\begin{aligned}
a_0 &= 1 \ , \\
a_1 &= s \ , \\
a_2 &= b \ , \\
a_3 &= p \ , \\
c_0 &= -f_7s^3 + f_7bs - f_6s^2 + 3f_7p + 2f_6b \ , \\
c_1 &= -f_7s^4 + 3f_7bs^2 - f_6s^3 - f_7b^2 - f_7ps + 2f_6bs - f_5s^2 + 2f_5b \ , \\
c_2 &= f_7bs^3 - 2f_7b^2s + f_6bs^2 + f_7bp - f_6b^2 + f_5bs - 3f_5p \ , \\
c_3 &= f_7b^2s^2 - f_7ps^3 + f_7pbs - f_7b^3 + f_6b^2s - f_6ps^2 + f_5b^2 - f_5ps \ .
\end{aligned}$$

Nous devons, dans un premier temps, exprimer les produits deux à deux de ces coordonnées en fonction de s, b et p en tenant compte de la remarque suivante :

Remarque : Les coordonnées sont des fonctions symétriques en θ_1, θ_2 et θ_3 mais comme nous n'allons pas utiliser très longtemps ces notations (puisque nous travaillerons plutôt avec s, b, et p), nous devons exprimer le fait que nous avons choisi trois zéros distincts de $F(X)$. On introduit pour cela les polynômes

$$\begin{aligned}
F_1(\theta_1, \theta_2, \theta_3) &= \frac{\theta_1F(\theta_2) - \theta_2F(\theta_1) - \theta_3F(\theta_2) + \theta_3F(\theta_1) - \theta_1F(\theta_3) + \theta_2F(\theta_3)}{(\theta_1 - \theta_2)(\theta_2 - \theta_3)(\theta_3 - \theta_1)} \\
F_2(\theta_1, \theta_2, \theta_3) &= \frac{F(\theta_2) - F(\theta_3)}{\theta_2 - \theta_3} \\
F_3(\theta_1, \theta_2, \theta_3) &= F(\theta_3)
\end{aligned}$$

Ces polynômes sont symétriques en θ_1, θ_2, θ_3 et doivent être nuls. On peut donc réduire un polynôme symétrique en θ_1, θ_2, θ_3 modulo ces polynômes. On obtient alors un polynôme symétrique en θ_1, θ_2, θ_3 de degré au plus 4 en chaque variable étant donné que $F_1(\theta_1, \theta_2, \theta_3)$ est de degré 5 en chaque variable. Autrement dit, les polynômes en s, b, p que nous considérerons peuvent tous s'écrire comme des formes linéaires en les $s^ib^jp^k$ avec $i + j + k \leqslant 4$.

Contrairement au cas des courbes de genre 2, les produits deux à deux des coordonnées de $\mathcal{B}$ ne sont pas linéairement indépendants en raison de l'équation (III.3). Celle-ci permet en effet d'exprimer (par exemple) le produit a_0c_3 en fonction des autres produits. Cependant cette restriction n'est pas valable seulement pour les éléments d'ordre 2 mais également pour tous les éléments de la jacobienne. On peut donc choisir de ne pas tenir compte du produit a_0c_3 et lorsqu'il intervient de le remplacer en utilisant l'équation (III.3). Les autres produits sont linéairement indépendants, de telle sorte que toute forme linéaire en les $s^ib^jp^k$ avec $i + j + k \leqslant 4$ peut s'écrire de façon unique à l'aide des 35 produits deux à deux des a_i et des c_i excepté le produit a_0c_3.

Soit désormais $\mathcal{A} = \{[x_1, y_1], [x_2, y_2], [x_3, y_3]\}$ un élément quelconque de la jacobienne. Si $\mathbf{W}$ désigne la matrice de l'addition par le l'élément $\mathcal{B}$ d'ordre 2 obtenue au paragraphe précédent, les formes biquadratiques recherchées sont projectivement équivalentes à $2\xi_i(\mathbf{W}(\mathcal{A}))\xi_j(\mathbf{W}(\mathcal{A}))$. Ces expressions sont des formes quadratiques en les coordonnées de $\mathcal{A}$ dans la variété de Kummer. Le coefficient associé à un produit $\xi_l(\mathcal{A})\xi_m(\mathcal{A})$ s'exprime alors à l'aide des coefficients de la matrice $\mathbf{W}$. D'après la remarque précédente, on peut écrire ces coefficients comme des formes linéaires en les $s^ib^jp^k$ avec $i+j+k \leqslant 4$. Si l'on élimine le produit a_0c_3, ces formes linéaires peuvent s'écrire de façon unique en fonction des 35 produits deux à deux des a_i et des c_i car ces 35 produits sont indépendants sur $\mathbf{k}(f_0, \ldots, f_7)$. En d'autres termes, ces coefficients s'écrivent de façon unique comme des formes quadratiques en les a_i et les c_i. Cette unicité nous permet alors d'en déduire que ces formules seront encore valables pour un point $\mathcal{B}$ quelconque. Il existe un moyen simple de vérifier que nous n'avons pas fait d'erreur : les formes biquadratiques ainsi obtenues sont symétriques en $\mathcal{A}$ et $\mathcal{B}$ ce qui n'est pas évident au vu de leur construction. En effet, les $\xi_l(\mathcal{A})\xi_m(\mathcal{A})$ et les $\xi_l(\mathcal{B})\xi_m(\mathcal{B})$ apparaissent de manière complètement indépendante dans ces calculs, or ils sont censés jouer un rôle similaire. On peut désormais énoncer le théorème suivant :

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

$$(\xi_i(\mathcal{A}+\mathcal{B})\xi_j(\mathcal{A}-\mathcal{B}) + \xi_i(\mathcal{A}-\mathcal{B})\xi_j(\mathcal{A}+\mathcal{B}))_{1\leqslant i,j\leqslant 8} = (2B_{ij}(\mathcal{A},\mathcal{B}))_{1\leqslant i,j\leqslant 8} \quad .$$

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 $\mathbb{Z}[f_0, \ldots, f_7]$.

Le programme Maple qui permet de calculer ces formes biquadratiques est donné dans l'annexe B.3 et est disponible par ftp ainsi que les expressions de ces formes.

III.2.3 Conclusion et perspectives

1 Théorie des hauteurs

Comme dans le cas des genres 1 et 2, ces formes biquadratiques permettent d'élaborer une théorie des hauteurs pour les courbes hyperelliptiques de genre 3 définies par un polynôme de degré 7. On définit dans ce cas une hauteur de Kummer $H_{\mathcal{K}}$ sur $\mathcal{J}(\mathbf{k})$ par

$$H_{\mathcal{K}}(\mathcal{X}) = H([a_0(\mathcal{X}), a_1(\mathcal{X}), a_2(\mathcal{X}), a_3(\mathcal{X}), c_0(\mathcal{X}), c_1(\mathcal{X}), c_2(\mathcal{X}), c_3(\mathcal{X})]).$$

Les résultats des paragraphes III.2.1 et III.2.2 permettent de démontrer que $H_{\mathcal{K}}$ définit une fonction hauteur dans $\mathcal{J}(\mathbf{k})$, c'est à dire qu'elle vérifie les trois propriétés énoncées dans le théorème XIV. Nous n'avons cependant pas encore calculé explicitement les constantes C_1 et C_2 qui interviennent dans ces propriétés car il est fort probable que leur taille les rende inexploitables en pratique. Notons tout de même que cela permettrait d'écrire un algorithme pour le calcul du sous-groupe de torsion de $\mathcal{J}(\mathbf{k})$. Nos espoirs reposent sur une version équivalente de la méthode que Flynn emploie pour améliorer la constante C_2 dans le cas des courbes de genre 2.

2 La descente infinie

Cette théorie des hauteurs devrait aussi nous permettre théoriquement d'être en mesure d'effectuer une descente infinie sur de telles courbes, c'est à dire de retrouver $\mathcal{J}(\mathbf{k})$ à partir de $\mathcal{J}(\mathbf{k})/2\mathcal{J}(\mathbf{k})$.
Cette méthode était cependant déjà peu convaincante dans le cas des courbes de genre 2 en raison, une fois de plus, d'une constante C_2 trop grande. Flynn avait alors utilisé l'isogénie de Richelot pour calculer une meilleure borne C_2. Cette méthode ne s'applique malheureusement pas telle quelle pour les courbes de genre 3. En effet, Flynn utilisait le fait que l'image de la jacobienne de la courbe initiale par cette isogénie était la jacobienne d'une courbe facilement exprimable. Dans le cas des courbes de genre 3, on ne peut même pas affirmer que cette image soit la jacobienne d'une courbe hyperelliptique (puisqu'en genre 3 toutes les courbes ne sont pas hyperelliptiques). Il nous a donc fallu avoir une nouvelle approche. Pour le moment, nous avons réussi à calculer les matrices W_2 et W_3, mais nous n'avons encore pas pu trouver la matrice W_1 telle que, comme dans le cas des courbes de genre 2,

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

où $[2]$ désigne la multiplication par 2 sur la variété de Kummer.
L'application $\tau W_2 \tau W_3$ a le même degré et le même noyau que la multiplication par 2. Son espace d'arrivée n'est malheureusement pas $\mathcal{K}$. Il reste donc à trouver la matrice W_1 pour que l'application $W_1 \tau W_2 \tau W_3$ ait son image dans $\mathcal{K}$. Autrement dit, si l'on multiplie l'application $\tau W_2 \tau W_3$ par une matrice inconnue, le résultat doit vérifier les 27 équations qui définissent la variété de Kummer $\mathcal{K}$. Bien qu'il ne s'agisse que d'un système linéaire, les calculs sont bien trop complexes. Certaines astuces nous permettront cependant certainement de résoudre ce problème prochainement.

3 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 ils 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.

Annexe A

Tables des points entiers sur les courbes elliptiques définie par un "simplest cubic field"

Les tables qui vont suivre donnent les calculs que nous avons effectués pour les courbes elliptiques définies sur $\mathbb{Q}$ par un "simplest cubic field", c'est à dire par l'équation

$$y^2 = x^3 + mx^2 - (m+3)x + 1 \ ,$$

où m est un entier positif tel que $m^2 + 3m + 9$ soit sans facteur carré.

Pour les valeurs du paramètre m inférieur à 1000, nous avons calculé un système de générateur du groupe de Mordell-Weil de ces courbes E_m à l'aide du programme `mwrank` développé par Cremona [Cre]. Nous avons ensuite appliqué la méthode des formes linéaires de logarithmes elliptiques exposée au paragraphe I.4 pour calculer tous les points entiers de ces courbes.

Pour plus de clarté, nous avons choisi de présenter ces résultats par rang.

Notons que dans certains cas, le programme `mwrank` n'a pas pu conclure, nous avons alors utilisé la conjecture de Birch et Swinnerton-Dyer pour traiter ces cas. Ils sont indiqués par une étoile dans les tables.

Enfin nous n'avons écrit que les points entiers ayant une ordonnée positive. Il faut donc y rajouter leurs opposés.

A.1 Cas des courbes de rang 1

Lorsque le paramètre m définit une courbe E_m de rang 1, les théorèmes IV et V donnent la base du groupe de Mordell-Weil (le point $[0,1]$) ainsi que tous les points entiers sur E_m (le point $[0,1]$ et son double si m est impair). Il était donc inutile de reporter ici les tables dans leur intégralité. Nous donnons simplement la liste des paramètres m définissant un "simplest cubic field" et dont la courbe elliptique E_m associée est de rang 1.

1 , 2 , 4 , 7 , 8 , 10 , 13 , 14 , 16 , 19 , 20 , 22 , 28 , 31 , 32 , 34 , 35 , 37 , 38 , 40 , 43 , 46 , 47 , 49 , 50 , 52 , 53 , 56 , 58 , 61 , 62 , 65 , 68 , 70 , 73 , 74 , 76 , 77 , 79 , 80 , 82 , 86 , 88 , 89 , 91 , 92 , 94 , 97 , 98 , 104 , 106 , 107 , 109 , 110 , 112 , 115 , 116 , 119 , 121 , 122 , 124 , 125 , 128 , 131 , 134 , 140 , 145 , 148 , 155 , 158 , 160 , 161 , 164 , 167 , 170*, 172 , 173 , 175 , 178 , 182 , 184*, 185 , 190 , 193 , 196 , 197 , 199 , 200 , 202 , 203 , 205 , 206 , 208 , 209 , 211 , 212 , 214 , 215 , 217 , 221 , 224 , 226 , 232 , 233 , 238 , 239 , 241 , 244 , 245 , 247 , 251 , 253 , 254 , 256 , 257 , 259 , 260 , 262*, 265 , 266 , 268 , 272 , 278 , 280*, 281 , 284*, 289 , 290*, 293 , 295 , 296 , 298 , 301*, 302 , 304 , 310*, 313*, 314 , 316 , 317 , 319 , 320 , 322 , 323 , 325 , 326 , 328 , 331 , 332*, 334*, 337 , 338 , 340 , 343 , 344 , 346 , 349 , 352*, 353 , 355 , 361 , 362 , 364 , 367 , 368 , 370*, 373 , 376 , 379 , 380 , 382*, 383 , 385 , 386 , 388 , 392 , 394 , 401 , 403 , 409 , 410 , 412*, 413 , 415 , 416 , 418*, 421 , 422 , 424 , 425 , 427*, 430 , 431 , 436 , 437 , 442*, 443 , 445 , 448 , 449*, 451 , 452 , 454*, 455 , 460*, 463 , 464 , 466 , 467 , 469 , 476 , 478 , 481 , 484 , 485 , 487 , 488 , 490 , 493 , 496*, 497 , 502*, 505*, 506 , 508 , 509 , 514*, 518 , 520 , 521 , 524*, 526 , 527 , 529 , 530 , 536 , 539 , 541 , 547*, 550 , 551 , 553 , 554 , 556*, 560*, 562 , 563 , 566 , 568 , 569 , 572 , 574 , 581 , 586 , 587 , 589 , 590 , 592 , 595 , 596 , 598 , 599 , 601 , 604 , 605 , 608 , 610 , 613 , 614*, 620 , 622 , 623 , 628 , 631 , 632 , 634 , 635 , 638 , 640 , 643 , 646*, 647 , 650 , 652 , 656 , 658 , 659 , 661 , 662 , 664 , 665 , 667 , 670 , 673 , 674 , 676 , 677 , 679 , 680 , 682*, 685 , 686 , 688 , 689 , 692 , 694 , 695 , 697 , 700 , 703 , 706 , 707 , 713 , 715 , 718 , 721 , 725 , 728 , 730 , 731 , 733 , 734*, 736 , 739 , 743 , 746 , 748*, 749 , 751 , 752 , 754 , 755 , 757 , 760 , 761 , 763 , 764 , 766 , 767 , 769 , 770 , 772*, 775 , 778 , 779 , 781 , 782 , 785 , 787 , 788 , 790 , 794*, 797 , 799 , 802 , 805*, 811 , 812 , 814 , 817 , 818 , 820*, 821 , 823 , 826 , 827 , 829 , 830*, 832*, 833 , 836 , 841 , 842*, 847 , 850 , 851 , 853 , 854 , 857 , 859 , 860 , 862 , 863 , 865 , 866 , 868 , 869 , 871 , 872 , 877 , 881 , 883 , 884 , 886 , 889 , 890 , 892*, 893 , 895*, 896 , 898 , 901 , 902 , 905 , 907 , 908 , 910 , 913 , 916 , 917 , 919 , 920 , 922*, 925 , 929 , 931 , 932 , 935 , 937*, 940 , 944*, 946 , 947 , 949 , 950 , 952 , 953 , 955 , 962*, 964*, 965 , 967 , 968 , 971*, 973 , 974 , 976 , 979 , 980 , 986 , 988 , 994 , 997 , 998 , 1000

A.2 Cas des courbes de rang 3

m	Générateurs	points dans $E_{gg}(\mathbb{Z})$	points dans $E^0(\mathbb{Z})$
11	$[-1,5]$ $[0,1]$ $[2,5]$	$[-12,5]$ $[-1,5]$ $[-9,17]$ $[0,1]$ $[-4,13]$	$[2,5]$ $[38,265]$ $[6,23]$ $[3170,178789]$ $[26,157]$ $[7502,650255]$ $[30,191]$
17	$[-12,31]$ $[-4,17]$ $[0,1]$	$[-12,31]$ $[-4,17]$ $[0,1]$	$[3,11]$ $[35,251]$ $[83,829]$
23	$[-1,7]$ $[0,1]$ $[2,7]$	$[-24,7]$ $[-1,7]$ $[-16,47]$ $[0,1]$ $[-9,37]$	$[2,7]$ $[146,1897]$ $[14,83]$ $[42,337]$
25	$[-\frac{8}{9},\frac{181}{27}]$ $[0,1]$ $[3,13]$	$[-12,47]$ $[0,1]$	$[3,13]$ $[51,443]$ $[171,2393]$
26	$[-24,43]$ $[-16,55]$ $[0,1]$	$[-24,43]$ $[-16,55]$ $[0,1]$	
29	$[-28,41]$ $[-4,23]$ $[0,1]$	$[-28,41]$ $[-4,23]$ $[0,1]$	$[11,67]$ $[227,3631]$
44	$[-40,91]$ $[-16,89]$ $[0,1]$	$[-40,91]$ $[-16,89]$ $[0,1]$	
55	$[0,1]$ $[6,43]$ $[126,1693]$	$[-12,83]$ $[0,1]$	$[6,43]$ $[126,1693]$ $[786,22793]$
59	$[-1,11]$ $[0,1]$ $[2,11]$	$[-60,11]$ $[-1,11]$ $[-36,179]$ $[0,1]$ $[-25,151]$	$[2,11]$ $[902,27961]$ $[42,419]$ $[86,1033]$
64	$[-\frac{18696}{289},\frac{186379}{4913}]$ $[-24,157]$ $[0,1]$	$[-24,157]$ $[0,1]$	
67	$[0,1]$ $[\frac{10}{9},\frac{73}{27}]$ $[6,47]$	$[-57,191]$ $[-9,73]$ $[0,1]$	$[6,47]$ $[1158,40529]$
71	$[-52,235]$ $[-4,37]$ $[0,1]$	$[-52,235]$ $[-4,37]$ $[0,1]$	$[14,125]$ $[1298,48025]$
83	$[-1,13]$ $[0,1]$ $[2,13]$	$[-84,13]$ $[-1,13]$ $[-49,293]$ $[0,1]$ $[-36,253]$	$[2,13]$ $[1766,75937]$ $[62,743]$ $[114,1597]$
85	$[0,1]$ $[3,23]$ $[\frac{49995}{49},\frac{11634533}{343}]$	$[-24,193]$ $[0,1]$	$[3,23]$ $[1851,81443]$
95	$[-4,43]$ $[0,1]$ $[\frac{5}{4},\frac{43}{8}]$	$[-84,293]$ $[-4,43]$ $[0,1]$	$[30,331]$ $[2306,112993]$
101	$[0,1]$ $[3,25]$ $[\frac{99}{25},\frac{4393}{125}]$	$[-40,319]$ $[0,1]$	$[3,25]$ $[2603,135355]$
113	$[-4,47]$ $[0,1]$ $[\frac{5}{4},\frac{47}{8}]$	$[-84,463]$ $[-4,47]$ $[0,1]$	$[35,421]$ $[3251,188557]$
118	$[-96,463]$ $[0,1]$ $[\frac{3705}{1156},\frac{1151431}{39304}]$	$[-96,463]$ $[0,1]$	
127	$[-60,499]$ $[-\frac{8}{9},\frac{397}{27}]$ $[0,1]$	$[-60,499]$ $[0,1]$	$[186,3287]$ $[4098,266369]$

m	Générateurs	points dans $E_{gg}(\mathbb{Z})$	points dans $E^0(\mathbb{Z})$
130	$[-72,557]$ $[0,1]$ $[\frac{11025}{16},\frac{1261961}{64}]$	$[-72,557]$ $[0,1]$	
133	$[-24,257]$ $[0,1]$ $[\frac{1675}{441},\frac{353611}{9261}]$	$[-24,257]$ $[0,1]$	$[4491,305387]$
136	$[-\frac{1232}{9},\frac{1315}{27}]$ $[0,1]$ $[\frac{33}{4},\frac{745}{8}]$	$[0,1]$	
137	$[0,1]$ $[\frac{115}{81},\frac{6571}{729}]$ $[3,29]$	$[-40,401]$ $[0,1]$	$[3,29]$ $[4763,333409]$
142	$[-\frac{8}{3249},\frac{215803}{185193}]$ $[0,1]$ $[\frac{9}{4},\frac{161}{8}]$	$[-72,611]$ $[0,1]$	
146	$[-40,419]$ $[-\frac{840}{1681},\frac{728699}{68921}]$ $[0,1]$	$[-40,419]$ $[0,1]$	
149	$[-136,511]$ $[-16,191]$ $[0,1]$	$[-136,511]$ $[-16,191]$ $[0,1]$	$[11,133]$ $[5627,427651]$
151	$[0,1]$ $[\frac{45}{4},\frac{1097}{8}]$ $[66,967]$	$[0,1]$	$[66,967]$ $[5778,444905]$
157*	$[-12,151]$ $[0,1]$ $[3,31]$	$[-84,727]$ $[0,1]$ $[-60,599]$ $[-12,151]$	$[3,31]$ $[6243,499439]$
163	$[-156,443]$ $[-36,413]$ $[0,1]$	$[-156,443]$ $[-36,413]$ $[0,1]$	$[6726,558257]$
166	$[-\frac{412488}{2809},\frac{98513785}{148877}]$ $[-24,293]$ $[0,1]$	$[-24,293]$ $[0,1]$	
169	$[-168,239]$ $[-144,737]$ $[0,1]$	$[-168,239]$ $[-144,737]$ $[0,1]$	$[7227,621521]$
176	$[0,1]$ $[\frac{9}{4},\frac{179}{8}]$ $[\frac{585}{196},\frac{89389}{2744}]$	$[-88,835]$ $[0,1]$	
179	$[-1,19]$ $[0,1]$ $[2,19]$	$[-180,19]$ $[-1,19]$ $[-100,899]$ $[0,1]$ $[-81,811]$	$[2,19]$ $[8102,737281]$ $[146,2627]$ $[222,4441]$
181	$[-96,895]$ $[-\frac{476}{9},\frac{16381}{27}]$ $[0,1]$	$[-96,895]$ $[0,1]$	$[8283,762035]$
187	$[0,1]$ $[\frac{10}{9},\frac{127}{27}]$ $[18,251]$	$[-177,589]$ $[-9,127]$ $[0,1]$	$[18,251]$ $[8838,839609]$
191	$[-\frac{161}{9},\frac{6551}{27}]$ $[0,1]$ $[6,77]$	$[-28,365]$ $[0,1]$	$[6,77]$ $[9218,894145]$
194	$[0,1]$ $[\frac{497}{16},\frac{29401}{64}]$ $[\frac{209}{4},\frac{6509}{8}]$	$[0,1]$	
218	$[-\frac{6696}{169},\frac{1180639}{2197}]$ $[0,1]$ $[\frac{9}{4},\frac{199}{8}]$	$[-88,1013]$ $[0,1]$	
220	$[-\frac{360}{121},\frac{67679}{1331}]$ $[-\frac{8}{9},\frac{521}{27}]$ $[0,1]$	$[0,1]$	

m	Générateurs	points dans $E_{gg}(\mathbb{Z})$	points dans $E^0(\mathbb{Z})$
223	$[0,1]$ $[\frac{198}{169},\frac{14561}{2197}]$ $[6,83]$	$[-33,463]$ $[0,1]$	$[6,83]$ $[12546,1417697]$
227	$[-4,67]$ $[0,1]$ $[\frac{5}{4},\frac{67}{8}]$	$[-172,1291]$ $[-4,67]$ $[0,1]$	$[66,1123]$ $[12998,1494769]$
229	$[-\frac{84}{25},\frac{7211}{125}]$ $[0,1]$ $[75,1301]$	$[0,1]$	$[75,1301]$ $[13227,1534331]$
230	$[-\frac{24}{121},\frac{9983}{1331}]$ $[0,1]$ $[\frac{57}{4},\frac{1721}{8}]$	$[0,1]$	
236	$[0,1]$ $[\frac{57}{16},\frac{2995}{64}]$ $[\frac{665}{4},\frac{26627}{8}]$	$[0,1]$	
242	$[-64,863]$ $[0,1]$ $[\frac{65}{64},\frac{863}{512}]$	$[-64,863]$ $[0,1]$	
248	$[-88,1123]$ $[-\frac{16}{25},\frac{2027}{125}]$ $[0,1]$	$[-88,1123]$ $[0,1]$	
263	$[-1,23]$ $[0,1]$ $[2,23]$	$[-264,23]$ $[-1,23]$ $[-144,1583]$ $[0,1]$ $[-121,1453]$	$[2,23]$ $[17426,2317657]$ $[222,4883]$ $[314,7537]$
274	$[-\frac{1952}{9},\frac{44747}{27}]$ $[-\frac{56}{9},\frac{2969}{27}]$ $[0,1]$	$[0,1]$	
275	$[-12,203]$ $[-\frac{1}{25},\frac{443}{125}]$ $[0,1]$	$[-12,203]$ $[0,1]$	$[26,443]$ $[19046,2647393]$ $[3770,239771]$ $[12630,1434769]$
277	$[-\frac{120}{121},\frac{31219}{1331}]$ $[0,1]$ $[3,41]$	$[-84,1177]$ $[0,1]$	$[3,41]$ $[19323,2705219]$
283	$[0,1]$ $[\frac{70}{9},\frac{3347}{27}]$ $[174,3713]$	$[0,1]$	$[174,3713]$ $[20166,2883737]$
287	$[-\frac{20}{9},\frac{1223}{27}]$ $[0,1]$ $[\frac{22}{9},\frac{863}{27}]$	$[-129,1633]$ $[0,1]$	$[20738,3007009]$
292	$[-240,1751]$ $[0,1]$ $[\frac{2025}{1936},\frac{307691}{85184}]$	$[-240,1751]$ $[0,1]$	
305	$[0,1]$ $[3,43]$ $[\frac{451}{81},\frac{64853}{729}]$	$[-112,1567]$ $[0,1]$	$[3,43]$ $[23411,3605293]$
307	$[0,1]$ $[6,97]$ $[\frac{10126}{441},\frac{3782843}{9261}]$	$[-57,911]$ $[0,1]$	$[6,97]$ $[23718,3676289]$
308	$[-\frac{56}{9},\frac{3151}{27}]$ $[0,1]$ $[\frac{2585}{256},\frac{701059}{4096}]$	$[0,1]$	
311	$[-1,25]$ $[0,1]$ $[2,25]$	$[-312,25]$ $[-1,25]$ $[-169,2027]$ $[0,1]$ $[-144,1873]$	$[2,25]$ $[24338,3821065]$ $[266,6383]$ $[366,9517]$
329	$[0,1]$ $[35,659]$ $[627,19381]$	$[0,1]$	$[35,659]$ $[627,19381]$ $[27227,4519681]$

m	Générateurs	points dans $E_{gg}(\mathbb{Z})$	points dans $E^0(\mathbb{Z})$
341	$[-\frac{5916}{25}, \frac{304277}{125}]$ $[0,1]$ $[11,197]$	$[-28,505]$ $[0,1]$	$[11,197]$ $[29243,5029795]$
350	$[-\frac{10001505232}{29604481}, \frac{197766086856823}{161077981121}]$ $[-24,443]$ $[0,1]$	$[-24,443]$ $[0,1]$	
358	$[-\frac{56}{9}, \frac{3401}{27}]$ $[0,1]$ $[\frac{105609}{21904}, \frac{265247851}{3241792}]$	$[0,1]$	
359	$[-\frac{209}{9}, \frac{11753}{27}]$ $[0,1]$ $[114,2471]$	$[0,1]$	$[114,2471]$ $[32402,5864761]$
365	$[-\frac{204}{121}, \frac{54133}{1331}]$ $[0,1]$ $[3,47]$	$[-112,1793]$ $[0,1]$	$[3,47]$ $[33491,6162343]$
371	$[-\frac{11172}{2209}, \frac{11013395}{103823}]$ $[0,1]$ $[14,265]$	$[-24,457]$ $[0,1]$	$[14,265]$ $[34598,6469825]$
377	$[-12,239]$ $[-\frac{112}{121}, \frac{34579}{1331}]$ $[0,1]$	$[-12,239]$ $[0,1]$	$[35,701]$ $[35723,6787369]$
389	$[-376,1409]$ $[-16,319]$ $[0,1]$	$[-376,1409]$ $[-16,319]$ $[0,1]$	$[27,541]$ $[38027,7453291]$
391	$[-84,1483]$ $[0,1]$ $[\frac{1050}{169}, \frac{249397}{2197}]$	$[-84,1483]$ $[0,1]$	$[34146,6345737]$ $[38418,7568345]$
395	$[-60,1109]$ $[-\frac{4}{25}, \frac{1081}{125}]$ $[0,1]$	$[-60,1109]$ $[0,1]$	$[1890,90341]$ $[39206,7801993]$
400	$[-\frac{491096}{3249}, \frac{443937349}{185193}]$ $[0,1]$ $[\frac{9}{4}, \frac{269}{8}]$	$[-192,2783]$ $[0,1]$	
406	$[-\frac{405384}{2920681}, \frac{40423647713}{4991443829}]$ $[0,1]$ $[\frac{9}{4}, \frac{271}{8}]$	$[-168,2605]$ $[0,1]$	
407	$[0,1]$ $[\frac{26}{25}, \frac{499}{125}]$ $[18,361]$	$[-385,1849]$ $[-25,499]$ $[0,1]$	$[18,361]$ $[41618,8531689]$
428	$[-\frac{118856}{441}, \frac{31580207}{9261}]$ $[-24,493]$ $[0,1]$	$[-24,493]$ $[0,1]$	
434	$[0,1]$ $[\frac{105}{4}, \frac{4423}{8}]$ $[\frac{1073}{4}, \frac{56803}{8}]$	$[0,1]$	
440	$[-\frac{1942344}{7225}, \frac{2170356929}{614125}]$ $[-40,811]$ $[0,1]$	$[-40,811]$ $[0,1]$	
442	$[-\frac{12236547680}{29192409}, \frac{323167351267277}{157726585827}]$ $[-\frac{8}{9}, \frac{737}{27}]$ $[0,1]$	$[0,1]$	
457	$[-240,3551]$ $[-\frac{64592}{441}, \frac{24023539}{9261}]$ $[0,1]$	$[-240,3551]$ $[0,1]$	$[52443,12061889]$
458	$[-40,829]$ $[-\frac{736}{1681}, \frac{1174807}{68921}]$ $[0,1]$	$[-40,829]$ $[0,1]$	
461	$[-12,265]$ $[0,1]$ $[\frac{75609}{8464}, \frac{142216901}{778688}]$	$[-12,265]$ $[0,1]$	$[35,769]$ $[53363,12380215]$

m	Générateurs	points dans $E_{gg}(\mathbb{Z})$	points dans $E^0(\mathbb{Z})$
470	$[-\frac{264}{25}, \frac{29641}{125}]$ $[0, 1]$ $[\frac{1089}{400}, \frac{376687}{8000}]$	$[0, 1]$	
472	$[0, 1]$ $[\frac{721}{36}, \frac{93617}{216}]$ $[\frac{329097}{64}, \frac{197265883}{512}]$	$[0, 1]$	
475	$[-57, 1177]$ $[-\frac{1033676}{27225}, \frac{3616532207}{4492125}]$ $[0, 1]$	$[-57, 1177]$ $[0, 1]$	$[56646, 13538393]$
479	$[-1, 31]$ $[0, 1]$ $[2, 31]$	$[-480, 31]$ $[-1, 31]$ $[-256, 3839]$ $[0, 1]$ $[-225, 3601]$	$[2, 31]$ $[57602, 13882081]$ $[422, 12659]$ $[546, 17473]$
491	$[0, 1]$ $[\frac{26}{25}, \frac{551}{125}]$ $[18, 395]$	$[-465, 2419]$ $[-25, 551]$ $[0, 1]$	$[18, 395]$ $[60518, 14947945]$
494	$[-16, 361]$ $[0, 1]$ $[\frac{17}{16}, \frac{361}{64}]$	$[-456, 2851]$ $[-16, 361]$ $[0, 1]$	
499	$[0, 1]$ $[30, 679]$ $[\frac{1245}{4}, \frac{70807}{8}]$	$[0, 1]$	$[30, 679]$ $[62502, 15688001]$
503	$[0, 1]$ $[\frac{2385}{1024}, \frac{1295783}{32768}]$ $[14, 307]$	$[-33, 727]$ $[0, 1]$	$[14, 307]$ $[63506, 16067017]$
511	$[-\frac{3233}{1521}, \frac{3455135}{59319}]$ $[0, 1]$ $[102, 2515]$	$[0, 1]$	$[102, 2515]$ $[65538, 16843265]$
512	$[-\frac{10608416}{1625625}, \frac{326980417427}{2072671875}]$ $[\frac{17249}{1444}, \frac{14372999}{54872}]$ $[\frac{2625}{4}, \frac{179383}{8}]$	$[0, 1]$	
517	$[-12, 281]$ $[0, 1]$ $[\frac{28569}{64}, \frac{7089629}{512}]$	$[-12, 281]$ $[0, 1]$	$[67083, 17441579]$
523	$[-108, 2213]$ $[-\frac{476}{81}, \frac{105517}{729}]$ $[0, 1]$	$[-108, 2213]$ $[0, 1]$	$[68646, 18053897]$
532	$[-504, 2717]$ $[0, 1]$ $[\frac{796074721}{18714276}, \frac{81638278341983}{80957957976}]$	$[-504, 2717]$ $[0, 1]$	
533	$[-4, 103]$ $[0, 1]$ $[\frac{5}{4}, \frac{103}{8}]$	$[-444, 4217]$ $[-4, 103]$ $[0, 1]$	$[147, 3823]$ $[71291, 19105987]$
535	$[-\frac{396}{25}, \frac{46567}{125}]$ $[0, 1]$ $[66, 1607]$	$[0, 1]$	$[66, 1607]$ $[71826, 19321193]$
538	$[0, 1]$ $[\frac{105}{16}, \frac{9029}{64}]$ $[\frac{43281}{16}, \frac{9858743}{64}]$	$[0, 1]$	
542	$[-280, 4549]$ $[0, 1]$ $[\frac{3145}{36}, \frac{471041}{216}]$	$[-280, 4549]$ $[0, 1]$	
545	$[-40, 911]$ $[-\frac{2604}{121}, \frac{671117}{1331}]$ $[0, 1]$	$[-40, 911]$ $[0, 1]$	$[74531, 20421493]$
548	$[-\frac{32}{9}, \frac{2539}{27}]$ $[0, 1]$ $[\frac{716233}{39204}, \frac{3283579531}{7762392}]$	$[0, 1]$	
557	$[-\frac{952}{121}, \frac{260819}{1331}]$ $[-\frac{8}{9}, \frac{827}{27}]$ $[0, 1]$	$[0, 1]$	$[555, 18499]$ $[77843, 21796039]$

m	Générateurs	points dans $E_{gg}(\mathbb{Z})$	points dans $E^0(\mathbb{Z})$
559	$[-33,769]$ $[0,1]$ $[\frac{1089}{16},\frac{108359}{64}]$	$[-33,769]$ $[0,1]$	$[78402,22030961]$
571	$[-564,1597]$ $[-36,845]$ $[0,1]$	$[-564,1597]$ $[-36,845]$ $[0,1]$	$[81798,23476025]$
575	$[-4,107]$ $[0,1]$ $[\frac{5}{4},\frac{107}{8}]$	$[-444,5107]$ $[-4,107]$ $[0,1]$	$[158,4267]$ $[82946,23971393]$
578	$[0,1]$ $[\frac{465}{64},\frac{83623}{512}]$ $[\frac{33}{4},\frac{1499}{8}]$	$[0,1]$	
583	$[0,1]$ $[6,133]$ $[\frac{2001}{64},\frac{390649}{512}]$	$[-105,2309]$ $[0,1]$	$[6,133]$ $[85266,24982937]$
584	$[-\frac{22392}{49},\frac{1775467}{343}]$ $[0,1]$ $[\frac{705}{16},\frac{69919}{64}]$	$[0,1]$	
616	$[-504,5363]$ $[-\frac{99672408}{147306769},\frac{47354682995765}{1787862255353}]$ $[0,1]$	$[-504,5363]$ $[0,1]$	
617*	$[0,1]$ $[3,61]$ $[11,263]$	$[-220,4399]$ $[-52,1249]$ $[0,1]$	$[3,61]$ $[11,263]$ $[95483,29599729]$
619	$[0,1]$ $[6,137]$ $[\frac{741}{100},\frac{172589}{1000}]$	$[-96,2209]$ $[0,1]$	$[6,137]$ $[96102,29887721]$
625	$[-\frac{110684}{2025},\frac{120142261}{91125}]$ $[0,1]$ $[\frac{8809}{144},\frac{2748221}{1728}]$	$[0,1]$	$[97971,30762893]$
626	$[-616,2045]$ $[-\frac{784}{25},\frac{97189}{125}]$ $[0,1]$	$[-616,2045]$ $[0,1]$	
637	$[-24,607]$ $[0,1]$ $[\frac{51}{25},\frac{4601}{125}]$	$[-24,607]$ $[0,1]$	$[101763,32564159]$
641	$[-4,113]$ $[0,1]$ $[\frac{5}{4},\frac{113}{8}]$	$[-532,5585]$ $[-4,113]$ $[0,1]$	$[147,4115]$ $[103043,33179845]$
644	$[0,1]$ $[\frac{9}{4},\frac{341}{8}]$ $[\frac{4540601}{1600},\frac{10716815149}{64000}]$	$[-304,5623]$ $[0,1]$	
649	$[-\frac{620}{9},\frac{45163}{27}]$ $[0,1]$ $[\frac{21}{4},\frac{967}{8}]$	$[0,1]$	$[105627,34434401]$
653	$[-28,713]$ $[-\frac{3864}{1849},\frac{5161549}{79507}]$ $[0,1]$	$[-28,713]$ $[0,1]$	$[106931,35073367]$
655	$[-12,317]$ $[0,1]$ $[\frac{102}{49},\frac{13189}{343}]$	$[-12,317]$ $[0,1]$	$[107586,35395793]$
668	$[-264,5323]$ $[0,1]$ $[\frac{107793}{64},\frac{41820281}{512}]$	$[-264,5323]$ $[0,1]$	
671	$[-364,6397]$ $[0,1]$ $[1470,68011]$	$[-364,6397]$ $[0,1]$	$[1470,68011]$ $[112898,38046625]$
683	$[-1,37]$ $[0,1]$ $[2,37]$	$[-684,37]$ $[-1,37]$ $[-361,6497]$ $[0,1]$ $[-324,6157]$	$[2,37]$ $[116966,40119337]$ $[614,22103]$ $[762,28957]$

m	Générateurs	points dans $E_{gg}(\mathbb{Z})$	points dans $E^0(\mathbb{Z})$
698	$[-184, 4187]$ $[0, 1]$ $[\frac{1801161}{2500}, \frac{3390648409}{125000}]$	$[-184, 4187]$ $[0, 1]$	
701	$[-\frac{72719240}{670761}, \frac{1457726024971}{549353259}]$ $[0, 1]$ $[3, 65]$	$[-220, 4841]$ $[0, 1]$	$[3, 65]$ $[123203, 43367455]$
704	$[-688, 2839]$ $[-64, 1633]$ $[0, 1]$	$[-688, 2839]$ $[-64, 1633]$ $[0, 1]$	
709	$[-\frac{8079580340}{12383361}, \frac{215852782281031}{43577047359}]$ $[0, 1]$ $[51, 1393]$	$[0, 1]$	$[51, 1393]$ $[126027, 44865611]$
710	$[-\frac{28968}{529}, \frac{17223419}{12167}]$ $[-\frac{328}{49}, \frac{65339}{343}]$ $[0, 1]$	$[0, 1]$	
712*	$[-24, 643]$ $[-\frac{917053654994518824}{115438896848526001}, \frac{8780149282337135578735907293}{39221866025384636526289001}]$ $[0, 1]$	$[-24, 643]$ $[0, 1]$	
719	$[-9, 253]$ $[0, 1]$ $[\frac{10}{9}, \frac{253}{27}]$	$[-633, 5909]$ $[-9, 253]$ $[0, 1]$	$[74, 2071]$ $[129602, 46786321]$
722	$[-\frac{10459303507016}{14741116569}, \frac{4664018507120007911}{1789763185991997}]$ $[0, 1]$ $[\frac{9}{4}, \frac{361}{8}]$	$[-304, 6233]$ $[0, 1]$	
724	$[-288, 6031]$ $[-\frac{840056}{88209}, \frac{7016248331}{26198073}]$ $[0, 1]$	$[-288, 6031]$ $[0, 1]$	
737	$[-\frac{640}{169}, \frac{253547}{2197}]$ $[0, 1]$ $[11, 287]$	$[-72, 1871]$ $[0, 1]$	$[11, 287]$ $[136163, 50380309]$
745	$[-\frac{883217280}{92025649}, \frac{241635529950167}{882802050857}]$ $[0, 1]$ $[3, 67]$	$[-264, 5807]$ $[0, 1]$	$[3, 67]$ $[139131, 52034993]$
758	$[-240, 5479]$ $[0, 1]$ $[\frac{70409}{31684}, \frac{256226161}{5639752}]$	$[-240, 5479]$ $[0, 1]$	
773	$[-348, 7193]$ $[-\frac{80}{9}, \frac{7003}{27}]$ $[0, 1]$	$[-348, 7193]$ $[0, 1]$	$[149771, 58111147]$
784	$[-\frac{272}{9}, \frac{22787}{27}]$ $[0, 1]$ $[\frac{243548171049}{405136384}, \frac{182359644634324309}{8154585137152}]$	$[0, 1]$	
791	$[0, 1]$ $[\frac{78}{49}, \frac{9365}{343}]$ $[\frac{70}{9}, \frac{5543}{27}]$	$[0, 1]$	$[156818, 62256745]$
793	$[-156, 3953]$ $[-\frac{20}{81}, \frac{11431}{729}]$ $[0, 1]$	$[-156, 3953]$ $[0, 1]$	$[3771, 254753]$ $[157611, 62729177]$
796	$[0, 1]$ $[\frac{9}{4}, \frac{379}{8}]$ $[\frac{762049089}{17007376}, \frac{90156083984065}{70138418624}]$	$[-336, 7225]$ $[0, 1]$	
800*	$[-112, 2953]$ $[0, 1]$ $[\frac{333079385}{19945156}, \frac{41240315989531}{89075066696}]$	$[-112, 2953]$ $[0, 1]$	
803	$[-16, 463]$ $[0, 1]$ $[\frac{17}{16}, \frac{463}{64}]$	$[-744, 5767]$ $[-16, 463]$ $[0, 1]$	$[54, 1567]$ $[161606, 65127217]$
806	$[-480, 8689]$ $[0, 1]$ $[\frac{3801}{100}, \frac{1090249}{1000}]$	$[-480, 8689]$ $[0, 1]$	

m	Générateurs	points dans $E_{gg}(\mathbb{Z})$	points dans $E^0(\mathbb{Z})$
808	$[-\frac{667040}{1521}, \frac{501275449}{59319}]$ $[0,1]$ $[\frac{104041}{2916}, \frac{160974323}{157464}]$	$[0,1]$	
809	$[-4,127]$ $[0,1]$ $[\frac{5}{4}, \frac{127}{8}]$	$[-628,8479]$ $[-4,127]$ $[0,1]$	$[219,7009]$ $[164027,66594961]$
815	$[0,1]$ $[6,157]$ $[\frac{116242}{9}, \frac{40863061}{27}]$	$[-145,3769]$ $[0,1]$	$[6,157]$ $[166466,68084593]$
824	$[-\frac{208}{361}, \frac{187949}{6859}]$ $[0,1]$ $[\frac{161}{4}, \frac{9353}{8}]$	$[0,1]$	
830*	$[-40,1139]$ $[0,1]$ $[\frac{17}{4}, \frac{859}{8}]$	$[-184,4693]$ $[-40,1139]$ $[0,1]$	
835	$[-792,5257]$ $[-\frac{4316}{9}, \frac{244711}{27}]$ $[0,1]$	$[-792,5257]$ $[0,1]$	$[174726,73210193]$
839	$[-1,41]$ $[0,1]$ $[2,41]$	$[-840,41]$ $[-1,41]$ $[-441,8819]$ $[0,1]$ $[-400,8401]$	$[2,41]$ $[176402,74265241]$ $[762,30479]$ $[926,38893]$
845	$[-\frac{748}{49}, \frac{155791}{343}]$ $[0,1]$ $[11,307]$	$[-72,2017]$ $[0,1]$	$[11,307]$ $[178931,75866743]$
848	$[-280,6691]$ $[0,1]$ $[\frac{14594441}{2704}, \frac{59974108709}{140608}]$	$[-280,6691]$ $[0,1]$	
856*	$[-24,707]$ $[-\frac{8}{81}, \frac{7075}{729}]$ $[0,1]$	$[-24,707]$ $[0,1]$	
875	$[0,1]$ $[\frac{665}{64}, \frac{150557}{512}]$ $[18,523]$	$[-52,1507]$ $[0,1]$	$[18,523]$ $[10626,1139557]$ $[191846,84220393]$
878	$[-168,4493]$ $[-\frac{204360}{10201}, \frac{619879831}{1030301}]$ $[0,1]$	$[-168,4493]$ $[0,1]$	
880	$[-240,6089]$ $[-\frac{56}{56169}, \frac{18258479}{13312053}]$ $[0,1]$	$[-240,6089]$ $[0,1]$	
899	$[0,1]$ $[\frac{45}{4}, \frac{2593}{8}]$ $[\frac{306}{25}, \frac{44279}{125}]$	$[0,1]$	$[202502,91328401]$
904	$[-\frac{19057104}{851929}, \frac{534153725227}{786330467}]$ $[\frac{23961}{484}, \frac{16120427}{10648}]$ $[\frac{441240320185953}{78423521764}, \frac{998532344570021029255 3}{21961879881834088}]$	$[0,1]$	
914	$[-376,8741]$ $[-\frac{16}{25}, \frac{3877}{125}]$ $[0,1]$	$[-376,8741]$ $[0,1]$	
928	$[-\frac{3080}{9}, \frac{224153}{27}]$ $[0,1]$ $[\frac{1441}{36}, \frac{265753}{216}]$	$[0,1]$	
934	$[0,1]$ $[\frac{1651305}{44944}, \frac{10763018843}{9528128}]$ $[\frac{5073}{4}, \frac{476053}{8}]$	$[0,1]$	
938	$[-\frac{24}{49}, \frac{8989}{343}]$ $[0,1]$ $[\frac{230945}{200704}, \frac{1143374513}{89915392}]$	$[0,1]$	
941	$[-4,137]$ $[0,1]$ $[\frac{5}{4}, \frac{137}{8}]$	$[-732,10615]$ $[-4,137]$ $[0,1]$	$[219,7445]$ $[221843,104709895]$

m	Générateurs	points dans $E_{gg}(\mathbb{Z})$	points dans $E^0(\mathbb{Z})$
943*	$[-129, 3697]$ $[-24, 743]$ $[0, 1]$	$[-660, 11131]$ $[0, 1]$ $[-129, 3697]$ $[-24, 743]$	$[42, 1303]$ $[222786, 105377777]$
956	$[0, 1]$ $[\frac{657}{4}, \frac{43865}{8}]$ $[\frac{3857}{4}, \frac{337945}{8}]$	$[0, 1]$	
958	$[-264, 6973]$ $[0, 1]$ $[\frac{51155497}{24336}, \frac{441416687867}{3796416}]$	$[-264, 6973]$ $[0, 1]$	
959	$[0, 1]$ $[\frac{19154}{2209}, \frac{26350049}{103823}]$ $[14, 421]$	$[-73, 2189]$ $[0, 1]$	$[14, 421]$ $[230402, 110823361]$
961*	$[-12, 385]$ $[-\frac{32}{9}, \frac{3365}{27}]$ $[0, 1]$	$[-12, 385]$ $[0, 1]$	$[75, 2399]$ $[291, 10283]$ $[231363, 111516965]$
970	$[-792, 10603]$ $[-\frac{9522439344}{346146025}, \frac{5540083969000429}{6440046795125}]$ $[0, 1]$	$[-792, 10603]$ $[0, 1]$	
977	$[-\frac{376}{169}, \frac{183899}{2197}]$ $[0, 1]$ $[203, 6959]$	$[0, 1]$	$[203, 6959]$ $[10131, 1067747]$ $[239123, 117170269]$
982	$[-840, 10051]$ $[0, 1]$ $[\frac{4329}{4}, \frac{393281}{8}]$	$[-840, 10051]$ $[0, 1]$	
983	$[-33, 1033]$ $[-\frac{28}{121}, \frac{22343}{1331}]$ $[0, 1]$	$[-33, 1033]$ $[0, 1]$	$[242066, 119338537]$
989	$[-168, 4831]$ $[0, 1]$ $[\frac{5771}{25}, \frac{1006019}{125}]$	$[-168, 4831]$ $[0, 1]$	$[245027, 121533391]$
991	$[0, 1]$ $[6, 173]$ $[\frac{195750}{1681}, \frac{266052421}{68921}]$	$[-156, 4525]$ $[0, 1]$	$[6, 173]$ $[246018, 122270945]$
995	$[-\frac{913}{169}, \frac{406739}{2197}]$ $[0, 1]$ $[18, 557]$	$[-52, 1613]$ $[0, 1]$	$[18, 557]$ $[248006, 123754993]$

A.3 Cas des courbes de rang 5

m	Générateurs	points dans $E_{gg}(\mathbb{Z})$		points dans $E^0(\mathbb{Z})$	
143	$[-33, 353]$	$[-144, 17]$	$[-4, 53]$	$[2, 17]$	$[846, 26603]$
	$[-4, 53]$	$[-124, 557]$	$[-1, 17]$	$[6, 67]$	$[854, 26963]$
	$[0, 1]$	$[-105, 659]$	$[0, 1]$	$[30, 389]$	$[4182, 275027]$
	$[2, 17]$	$[-81, 647]$		$[90, 1369]$	$[5186, 378577]$
	$[6, 67]$	$[-64, 577]$		$[114, 1823]$	$[17342, 2293147]$
		$[-33, 353]$		$[182, 3277]$	$[414290, 266705281]$
		$[-28, 307]$		$[290, 6031]$	
347	$[-84, 1373]$	$[-345, 599]$	$[-12, 229]$	$[6, 103]$	$[14930, 1845349]$
	$[-12, 229]$	$[-292, 2189]$	$[-4, 83]$	$[26, 493]$	$[30278, 5298649]$
	$[-4, 83]$	$[-225, 2501]$	$[0, 1]$	$[98, 2059]$	
	$[0, 1]$	$[-84, 1373]$		$[1190, 46649]$	
	$[6, 103]$	$[-64, 1087]$		$[5070, 373151]$	
419	$[-1, 29]$	$[-420, 29]$	$[-33, 659]$	$[2, 29]$	$[594, 18899]$
	$[0, 1]$	$[-280, 3319]$	$[-1, 29]$	$[6, 113]$	$[44102, 9305521]$
	$[2, 29]$	$[-225, 3149]$	$[0, 1]$	$[14, 281]$	
	$[6, 113]$	$[-196, 2941]$		$[366, 10247]$	
	$[594, 18899]$	$[-64, 1217]$		$[482, 14461]$	
439	$[-105, 1931]$	$[-408, 2311]$		$[42, 911]$	$[30090, 5257489]$
	$[-9, 197]$	$[-276, 3541]$		$[54, 1189]$	$[48402, 10696841]$
	$[0, 1]$	$[-105, 1931]$		$[222, 5699]$	
	$[42, 911]$	$[-9, 197]$		$[270, 7181]$	
	$[270, 7181]$	$[0, 1]$		$[966, 36203]$	
473	$[-60, 1231]$	$[-456, 1937]$	$[-4, 97]$	$[27, 593]$	$[56171, 13368697]$
	$[-16, 353]$	$[-364, 3823]$	$[0, 1]$	$[51, 1157]$	
	$[-4, 97]$	$[-240, 3679]$		$[107, 2567]$	
	$[0, 1]$	$[-60, 1231]$		$[899, 33293]$	
	$[51, 1157]$	$[-16, 353]$		$[2315, 122231]$	
611	$[-9, 233]$	$[-612, 35]$	$[-184, 3817]$	$[2, 35]$	$[1650, 78451]$
	$[-1, 35]$	$[-537, 4655]$	$[-9, 233]$	$[74, 1925]$	$[8502, 811615]$
	$[0, 1]$	$[-324, 5507]$	$[-1, 35]$	$[266, 7867]$	$[93638, 28746865]$
	$[\frac{10}{9}, \frac{233}{27}]$	$[-289, 5203]$	$[0, 1]$	$[546, 18563]$	$[1313274, 1505337995]$
	$[2, 35]$	$[-280, 5111]$		$[686, 24697]$	

Annexe B

Programmes Maple

Nous présentons ici les programmes que nous avons effectués à l'aide de Maple. Le premier programme concerne le théorème de préparation de Weierstrass et la méthode de Chabauty elliptique. Les deux programmes suivants concernent la variété de Kummer d'une courbe hyperelliptique de genre 3 définie par un polynôme de degré 7. Ces programmes sont également disponibles sur le site ftp

`ftp://megrez.math.u-bordeaux.fr/pub/duquesne`.

B.1 Le théorème de préparation de Weierstrass

```
#This maple session computes the functions occuring in the explicit
#Weierstrass preparation theorem explained in chapter II.
#By the way, this program bounds the number of solutions of systems of
#two power series in two variables which is required for some cases for
#the elliptic curve Chabauty method.
#
#Main programs are wpt and ellcha2.
#
#For any given power series f in Z_p<n_1,n_2> modulo p^prec, wpt returns
#a polynomial g in n_1 with coefficients in Z_p<n_2> such that f=g*h
#where h is a unit in Z_p<n_1,n_2> (and so f(n_1,n_2)=0 implies that
#g(n_1,n_2)=0). The polynomial g is given modulo p^prec as a vector
#(the i-th component is the term of degree i-1). Moreover wpt returns
#the new precision to consider. In fact, one of the coefficients of f
#must be invertible modulo p. If this is not the case, f must be divided
#by p and f/p is then known modulo p^{prec-1}.
#
#The program ellcha2 bound the number of solutions of systems of two
#power series f1 and f2 in two variables n1 and n2 given with the
#precision p^prec. The user have to give the known solutions in n_2 with
```

```
#their multiplicity in the resultant of the polynomials g1 and g2
#(obtained by wpt). If  the multiplicity is not known, the program
#will help you. The first result is the number of solution in n2 and
#the second result is the number of solution in n1 for each known
#solution in n2 given in the entries.


with(linalg):
#We first want to compute the fonction hi in terms of the functions gi.
#For this we use proposition II.4.1. In this proposition, we need to
#compute a sum over s-uplet i_0,..,i_{s-1} such that i_0+...+i_{s-1}=k.
#We represent those s-uplets by vectors.
#compnonnul gives the first non zero component of a vector v
compnonnul:=proc(v)
local i,s,t;
s:=vectdim(v):
t:=1:
for i from 1 to s do
    if v[i]=0 then t:=t+1 else break
fi: od:
if t=s+1 then print("zero vector") fi:
t;
end:

#For any given vector v (with the sum of its coordinates equal to k),
#suivant gives vectors of the same form for which the first non zero
#component has been reduced of 1
suivant:=proc(v)
local W,c,i,s,w;
W:={}:
c:=compnonnul(v):
s:=vectdim(v):
for i from c+1 to s do
    w:=v:
    w[c]:=v[c]-1:
    w[i]:=v[i]+1:
    W:=W union {w}:
od:
W:
end:

#finally partition gives all the required s-uplet (the partitions of k)
partition:=proc(s,k)
```

```
local vi,vf,i,S ;
vi:=[seq(0,i=1..s)]:
vf:=[seq(0,i=1..s)]:
vi[1]:=k:
vf[s]:=k:
S:={vi}:
while member(vf,S)=false do
      for i from 1 to nops(S) do
          S:=S union suivant(S[i]):
      od:
od:
S;
end:

#indice computes the index of the fi occuring in the formula
indice:=proc(n,k,s,i)
local ind;
ind:=n+s+sum('(s-(j-1))*i[j]','j'=1..s);
ind;
end:

#multinomial computes the multinomial coefficient occuring in
#(g_0+...+g_{s-1})^k
multinomial:=proc(i,k)
local c,s;
s:=vectdim(i):
c:=k!/product('i[j]!','j'=1..s):
c;
end:

#sommepart computes the finite sum for any given k occuring in the
#formula
sommepart:=proc(f,g,k,n,p,prec)
local sum,s,S,j,i,a,gi,find;
sum:=0:
s:=vectdim(g)-1:
S:=partition(s,k):
for j from 1 to nops(S) do
    i:=S[j]:
    find:=coeff(f,n1,indice(n,k,s,i)) mod p^prec:
    gi:=vector(s,0):
    for a from 1 to s do
        if g[a]=0 and i[a]=0 then
```

```
          gi[a]:=1 else
          gi[a]:=g[a]^(i[a]) mod     p^prec:
        fi:
    od:
    sum:=sum+multinomial(i,k)*find*product('gi[l]','l'=1..s) mod p^prec:
od:
sum;
end:

#inversemodp computes the inverse of a polynomial in n2 modulo p with
#the precision p^prec
inversemodp:=proc(Pol,p,prec)
local P,Pi,a0,a0i,k;
P:=Pol mod p^prec:
a0:=coeff(P,n2,0):
a0i:=1/a0 mod p^prec:
P:=P*a0i mod p^prec:
if ((P-1) mod p) = 0 then
                    else print(Pol,"is not invertible modulo", p^prec):
fi:
Pi:=simplify(a0i*(1+sum('(1-P)^k','k'=1..prec-1))) mod p^prec:
Pi;
end:

#Finally, calculhn computes the function hn with the precision p^prec if
#f and g are given with the precision p^{prec-1}
calculhn:=proc(f,g,h,n,p,prec)
local kmax,s,indmax,hn,k,F;
s:=vectdim(g)-1:
F:=f mod p^prec:
indmax:=degree(f,n1):
kmax:=max(indmax-s-n,0):
hn:=sum('expand((-1)^k *inversemodp(expand(g[s+1]^(k+1)) mod p^prec,
        p,prec)*sommepart(F,g,k,n,p,prec))' ,'k'=0..kmax) mod p^prec:
hn;
end:

#The proposition II.4.1 is now entirely computable, so that we can now
#apply Weierstrass prepareation theorem. explwpt return the polynomial
#g and the function h with the precision p^prec if f is general of
#order s and given with the same precision. explwpt also return test
#which test if f=g*h modulo p^prec
explwpt:=proc(f,s,p,prec)
```

```
local F,i,g,h,k0,j,l,n,indmax,H,G,test;
F:=f mod p^prec:
g:=vector(s+1,0):
indmax:=degree(F,n1):
h:=vector(max(s+1,s+indmax-2*s+1)+1,0):
for i from 1 to s+1 do
    g[i]:=coeff(F,n1,i-1) mod p:
    h[i]:=0:
od:
h[1]:=1:
for k0 from 2 to prec do
    for j from 2 to s+1 do

        h[j]:=sort(calculhn(F,g,h,j-1,p,k0),n2):
        print(h[j]);
    od:
    for j from 1 to s+1 do
    g[j]:=sort(expand(coeff(F,n1,j-1)-sum('h[l]*g[j-l+1]','l'=2..j)), n2)
                                                                  mod p^k0:
    od:
od:
for n from s+1 to s+indmax-2*s+1 do
    h[n+1]:=sort(calculhn(F,g,h,n,p,prec),n2):
od:
H:=expand(sum('h[i]*n1^(i-1)','i'=1..vectdim(h))) mod p^prec:
G:=expand(sum('g[i]*n1^(i-1)','i'=1..s+1)) mod p^prec:
test:=expand(F-G*H) mod p^prec:
[test,evalm(g),evalm(h)]:
end:

#general test if f (given with the precision p^prec) is general in n1
#and give the order and the new precision to consider (in fact, if f
#is divisible by p, this program compute this division so that we
#lose in precision)
general:=proc(f,p,prec)
local F,s1,t,s,newprec;
F:=f:
newprec:=prec:
while (F mod p)=0 do
       F:=simplify(F/p):
       newprec:=newprec-1:
od:
s1:=degree(subs(n2=0,F) mod p,n1):
```

```
if s1=-infinity  then print(f,"is not general in",n1,"try a linear
combination with the other power series or exchange n1 and n2 (in the
two power series)"): break: fi:
[F,newprec,s1]:
end:

#wpt is the weierstrass preparation theorem : given a power series f in
#n1 and n2 with the precision p^prec, wpt apply weierstrass preparation
#theorem for f relatively to n1. It returns g (h is useless but wpt test
#if f=g*h) as a vector with the new precision to consider (if f is
#divisible by p, we lose in precision)
wpt:=proc(f,p,prec)
local F,newprec,s,t,test,g,h,A,B;
A:=general(f,p,prec):
F:=A[1]:newprec:=A[2]:s:=A[3]:
B:=explwpt(F,s,p,newprec):
test:=B[1]:g:=B[2]:h:=B[3]:
if test=0 then else
print("bug, please send your session to duquesne@math.u-bordeaux.fr,
       many thanks."):break:
fi:
[evalm(g),newprec]:
end:

#Finally, ellcha2 bound the number of solutions of systems of two power
#series f1 and f2 in two variables n1 and n2 given with the precision
#p^prec. The user have to give the known solutions of the resultant of
#the polynomial g1 and g2 with their multiplicity. But if this is not
#the case, the program will help you. The first result is the number
#of solutions in n2 and the second result is the number of solutions
#in n1 for each known solution in n2 given in the entries.
ellcha2:=proc(f1,f2,p,prec,sol)
local g1,g2,G1,G2,G1u,G2u,res,newprec,s,S,i,F,sol2,s2,lowdeg;
g1:=wpt(f1,p,prec):
g2:=wpt(f2,p,prec):
newprec:=min(g1[2],g2[2]):
print('modulo',p^newprec):
G1:=sort(sum(g1[1][i]*n1^(i-1),i=1..vectdim(g1[1])) mod p^newprec,n1):
print("first polynomial",G1):
G2:=sort(sum(g2[1][i]*n1^(i-1),i=1..vectdim(g2[1])) mod p^newprec,n1):
print("second polynomial",G2):
res:=sort(resultant(G1,G2,n1) mod p^newprec,n2):
print("resultant",res):
```

```
if (res mod p^newprec)=0 then print("precision too low or resultant
                                     equals to zero") else
  while (res mod p)=0 do
       res:=simplify(res/p):
  od:
  s:=degree(res mod p,n2):
  print("there is at most",s,"solutions in n2"):
  if (vectdim(sol)=s and s<>0) then
     sol2:={}:

     for i from 1 to s do
         if member(sol[i],sol2)=false then sol2:=(sol2 union {sol[i]}):
         fi:
     od:
 s2:=nops(sol2):
     S:=vector(s2,0):
     for i from 1 to s2 do
         F:=subs(n2=sol2[i],f1):
         if (F mod p^newprec)=0 then print("precision too low") else
            while (F mod p)=0 do
              F:=simplify(F/p):
            od:
            S[i]:=degree(F mod p,n1):
            print("for n2 =",sol[i],"there is at most",S[i],"solutions
                  in n1 corresponding to the zeros of",F):
         fi:
     od:
  else
    lowdeg:=ldegree(res):
    if ldegree=0 then
       print("You have to think to indicate all the known solutions for
             n2. If done, this means that elliptic curve Chabauty does
             not work in this case"):break:
    else print("Be careful, 0 can be a multiple zero. In this case it is
               probably of order",lowdeg,"for the resultant. You must in
               dicate it in the entries of the program. For exemple, for
               the point at infinity, 0 is always of order 4"):break:
    fi:
  fi:
fi:
[s,evalm(S)]:
end:
```

B.2 Matrice de l'addition d'un point de 2-torsion

```
#Let X={[x1,y1],[x2,y2],[x3,y3]} be a generic divisor and
#A={[O1,0],[O2,0],[O3,0]}  an element of order 2. We write
#g(x)=(x-O1)(x-O2)(x-O3) and f(x)=g(x)*h(x). This maple session computes
#the matrix which gives addition by the divisor A

h:=x->h4*x^4+h3*x^3+h2*x^2+h1*x+h0:
g:=x->g3*x^3+g2*x^2+g1*x+g0:
f:=g*h:

#As in Stubbs's thesis, we define the coordinates in the Kummer of X.
a0:=1:
a1:=x1+x2+x3:
a2:=x1*x2+x2*x3+x1*x3:
a3:=x1*x2*x3:

#If we define
delta:=(x1-x2)*(x2-x3)*(x3-x1):
H0:=-f7*a1^3+f7*a2*a1-f6*a1^2+3*f7*a3+2*f6*a2:
H1:=-f7*a1^4+3*f7*a2*a1^2-f6*a1^3-f7*a2^2-f7*a3*a1+2*f6*a2*a1-f5*a1^2+
2*f5*a2:
H2:=f7*a2*a1^3-2*f7*a2^2*a1+f6*a2*a1^2+f7*a3*a2-f6*a2^2+f5*a2*a1-3*f5*a3:
H3:=f7*a2^2*a1^2-f7*a1^3*a3+f7*a1*a2*a3-f7*a2^3+f6*a2^2*a1-f6*a3*a1^2+
f5*a2^2-f5*a3*a1:
b0:=(x1*y2-x2*y1-x3*y2+x3*y1-x1*y3+x2*y3)/delta:
b1:=(x3^2*y2-x3^2*y1+x2^2*y1+y3*x1^2-y2*x1^2-y3*x2^2)/delta:

#In our case, we have
f7:=coeff(f(x),x,7):
f6:=coeff(f(x),x,6):
f5:=coeff(f(x),x,5):

#We have
c0:=a0*b0^2+H0:
c1:=a1*b0^2+2*a0*b0*b1+H1:
c2:=a0*b1^2-a2*b0^2+H2:
c3:=a1*b1^2+2*a2*b0*b1+a3*b0^2+H3:

#We first want to find the quartic M and the element gamma such that the
#equation (X-gamma)Y=M(X) passes trought the points [x1,y1], [x2,y2],
#[x3,y3], [O1,0], [O2,0] and [O3,0]. The 3 remaining points in the
#intersection of the curve and (X-gamma)Y=M(X) will give the opposite of
```

```
#the sum of X and A (which is the same in the kummer than the sum of X
#and A). For this, we have to solve the system given by
#(xi-gamma)yi=g(xi)(alpha xi+beta) for i=1,2,3.
#In other words, if we define

System1:=[[x1*G(x1),G(x1),y1],[x2*G(x2),G(x2),y2],[x3*G(x3),G(x3),y3]]:
System2:=[x1*y1,x2*y2,x3*y3]:

#the solution (alpha,beta,gamma) is given by System1^(-1)*System2. If d
#is the determinant of System1, this solution can be written
#(alpha=a/d,beta=b/d,gamma=A/d)

with(linalg):
d:=-det(System1):
sol:=simplify(evalm(d*System1^(-1)&*System2)):
a:=sol[1]:
b:=sol[2]:
A:=sol[3]:

#We have now to compute the squares of these quantities in order to
#compute the residual intersection between (X-gamma)Y=M(X) and the curve.
#But we have to eliminate the term in y, as for example the term in y1y2.
#The term in yi^2 can of course be replaced by f(xi). Let us now express
#the terms in yiyj with the ai and the ci using b0^2, b0b1 and b1^2
#(where y1y2, y1y3 and y2y3 appear). For this, we first compute delta^2*b0^2.
#Note that with our notations, we have
#a0*b0^2=c0-H0,            (1)
#a1*b0^2+2*a0*b0*b1=c1-H1, (2)
#a0*b1^2-a2*b0^2=c2-H2.    (3)
#So that the following must be zero
simplify(a0*b0^2-(c0-H0));
simplify(a1*b0^2+2*a0*b0*b1-(c1-H1));
simplify(a0*b1^2-a2*b0^2-(c2-H2));

#In the following, we prefer keeping the ci in generic form. In the same
#way, we use the function F,G,H instead of f,g,h and we will replace them
#later.
c0:='c0':c1:='c1':c2:='c2':c3:='c3':
b0b0:=simplify(expand(delta^2*b0^2)):

#We then replace yi^2 by F(xi)=G(xi)*H(xi). This can be done using the
#following procedure
replace:=proc(f)
```

```
local f2,f3,f4;
f2:=simplify(f+coeff(f,y1,2)*(G(x1)*H(x1)-y1^2)):
f3:=simplify(f2+coeff(f2,y2,2)*(G(x2)*H(x2)-y2^2)):
f4:=simplify(f3+coeff(f3,y3,2)*(G(x3)*H(x3)-y3^2)):
f4:
end:

b0b0:=replace(b0b0):

#We extract from this the term without any yi
b0b0_y:=subs(y1=0,y2=0,y3=0,b0b0):

#Let us do the same thing for b0b1 and b1^2
b0b1:=simplify(expand(delta^2*b0*b1)):
b0b1:=replace(b0b1):
b0b1_y:=subs(y1=0,y2=0,y3=0,b0b1):

b1b1:=simplify(expand(delta^2*b1^2)):
b1b1:=replace(b1b1):
b1b1_y:=subs(y1=0,y2=0,y3=0,b1b1):

#Let us now consider  equations (1), (2) and (3) as a system whose
#variables are 2*(x3-x2)*(x1-x3)*y1*y2, 2*(x3-x2)*(x2-x1)*y1*y3 and
#2*(x1-x3)*(x2-x1)*y2*y3

System3:=simplify([
[coeff(coeff(a0*b0b0,y1,1),y2,1)/(2*(x3-x2)*(x1-x3)),
 coeff(coeff(a0*b0b0,y1,1),y3,1)/(2*(x3-x2)*(x2-x1)),
 coeff(coeff(a0*b0b0,y2,1),y3,1)/(2*(x1-x3)*(x2-x1))],
[coeff(coeff(a1*b0b0+2*a0*b0b1,y1,1),y2,1)/(2*(x3-x2)*(x1-x3)),
 coeff(coeff(a1*b0b0+2*a0*b0b1,y1,1),y3,1)/(2*(x3-x2)*(x2-x1)),
 coeff(coeff(a1*b0b0+2*a0*b0b1,y2,1),y3,1)/(2*(x1-x3)*(x2-x1))],
[coeff(coeff(a0*b1b1-a2*b0b0,y1,1),y2,1)/(2*(x3-x2)*(x1-x3)),
 coeff(coeff(a0*b1b1-a2*b0b0,y1,1),y3,1)/(2*(x3-x2)*(x2-x1)),
 coeff(coeff(a0*b1b1-a2*b0b0,y2,1),y3,1)/(2*(x1-x3)*(x2-x1))]]):

System4:=simplify([
(c0-H0)*delta^2-a0*b0b0_y,
(c1-H1)*delta^2-(a1*b0b0_y+2*a0*b0b1_y),
(c2-H2)*delta^2-(a0*b1b1_y-a2*b0b0_y)]):

#System3 is a Van der Mond matrix with determinant equals to delta, so
#that we can invert it and then obtain the expression of y1y2, y1y3 and
```

```
#y2y3 in terms of the ai and the ci. Note that, at first, we prefer write
#System4 in a generic form
sol3:=simplify(evalm(System3^(-1)&*[e0,e1,e2])):

#The intersection of the curve and (dX-A)Y=G(X)(aX+b) is then given by
#(dX-A)^2F(X)=G(X)^2(aX+b)^2 which is of degree 9 in X. G(X) is in the
#two terms (it corresponds to the points [O1,0], [O2,0] and [O3,0]). So
#that we define L which is a polynomial in X of degree 6.
L:=(d*X-A)^2*H(X)-G(X)*(a*X+b)^2:

#We replace yi^2 by F(xi)=G(xi)*H(xi) in this expression
L:=replace(L):

#We now replace yiyj thanks to system 3 and 4
Ly1y2:=simplify(coeff(coeff(L,y1,1),y2,1)/(x1-x3)/(x3-x2)/2):
Ly1y3:=simplify(coeff(coeff(L,y1,1),y3,1)/(x2-x1)/(x3-x2)/2):
Ly2y3:=simplify(coeff(coeff(L,y2,1),y3,1)/(x1-x3)/(x2-x1)/2):
L_y:=subs(y1=0,y2=0,y3=0,L):

#So that the following must be 0
simplify(L-Ly1y2*2*(x3-x2)*(x1-x3)*y1*y2-Ly1y3*2*(x3-x2)*(x2-x1)*y1*y3-
Ly2y3*2*(x1-x3)*(x2-x1)*y2*y3-L_y);

L:=simplify(L_y+Ly1y2*sol3[1]+Ly1y3*sol3[2]+Ly2y3*sol3[3]):

#Note that L is divisible by G(x1)G(x2)G(x3). Since we are looking for
#roots of L, we can divide L by G(x1)G(x2)G(x3).
L:=simplify(L/G(x1)/G(x2)/G(x3)):

#We can then write L=P+P0*e0+P1*e1+P2*e2 with
P:=simplify(subs(e0=0,e1=0,e2=0,L)):
P0:=simplify(coeff(L,e0,1)):
P1:=simplify(coeff(L,e1,1)):
P2:=simplify(coeff(L,e2,1)):

#Our goal is now to express that x1, x2 and x3 are in the intersection.
#In other words, L is divisible by (X-x1)(X-x2)(X-x3). For this we have
#to write polynomials G and H with their coefficients

P:=simplify(subs(G=g,H=h,P)/((X-x1)*(X-x2)*(X-x3))):
P0:=simplify(subs(G=g,H=h,P0)/((X-x1)*(X-x2)*(X-x3))):
P1:=simplify(subs(G=g,H=h,P1)/((X-x1)*(X-x2)*(X-x3))):
P2:=simplify(subs(G=g,H=h,P2)/((X-x1)*(X-x2)*(X-x3))):
```

```
#P0, P1 and P2 are very simple. These polynomial are all of degree 3 in
#X, as required. Remember we want to obtain polynomials linear in the ai
#and the ci. As c0 lies only in e0, it is natural to define
p0:=simplify(P0-a3*h4*g(X)):
p1:=simplify(P1-a2*h4*g(X)):
p2:=simplify(P2-a1*h4*g(X)):

#So that p0, p1 and p2 do not depend of the ai. Hence p0 is a good
#candidate to be the coefficient of c0. We have with these notations

N:=subs(G=g,H=h,subs(e0=System4[1],e1=System4[2],e2=System4[3],
P+(p0+a3*h4*g(X))*e0+(p1+a2*h4*g(X))*e1+(p2+a1*h4*g(X))*e2)):

#We can then divide this expression by delta^2 in order to obtain p0 as
#the coefficient of c0.
N:=simplify(N/delta^2):

#But we want this polynomial to be linear in the ai and the ci, and there
#is in this expression a term in a3*c0. To eliminate it, we use the
#relation on the Kummer
#a3*(c0-H0)+a2*(c1-H1)+a1*(c2-H2)=a0*c3*(c3-H3) where
H3:=f7*a2^2*a1^2-f7*a1^3*a3+f7*a1*a2*a3-f7*a2^3+f6*a2^2*a1-f6*a3*a1^2+
f5*a2^2-f5*a3*a1:
coeff_a3c0:=simplify((coeff(N,c0,1)-subs(x1=0,coeff(N,c0,1)))/a3):
#this coefficient is h4*g(X) and is the same for a2*c1 and a1*c2

N:=simplify(N-coeff_a3c0*(a3*(c0-H0)+a2*(c1-H1)+a1*(c2-H2)-a0*(c3-H3))):

#By this way, N contains only linear terms in c0, c1, c2 and c3. The
#remaining terms are linear in the ai
M:=subs(c0=0,c1=0,c2=0,c3=0,N):

#We compute the terms in a0, a1, a2 and a3
ta0:=simplify(subs(x1=0,x2=0,x3=0,M)):
ta1:=simplify(subs(x2=0,x3=0,M-ta0)/x1):
ta2:=simplify(subs(x3=0,M-ta0-ta1*a1)/x1/x2):
ta3:=simplify((M-ta0-ta1*a1-ta2*a2)/a3):

#So that the following must be 0
simplify(N-(ta0*a0+ta1*a1+ta2*a2+ta3*a3+p0*c0+p1*c1+p2*c2+h4*g(X)*c3));

#ta0, ta1, ta2, ta3 are polynomials in X of degree 3 with coefficient in
```

```
#Z[g0,..,g3,h0,..,h4]. Finally N is a polynomial in X of degree 3 and
#is a linear combination of the ai and the ci. The roots of this
#polynomial define the sum of the element X and the divisor A of order 2.
#These roots are of course awful to compute but we are only interested in
#the coordinates in the Kummer of this sum. The first four coordinates
#are projectively equal to the coefficients of the polynomial N.
#If xi_i(X) denotes the (i+1)-th coordinate in the Kummer of X, we can
#write xi_i(X+A)=sum_{j=0}^7  wij*xi_j(X) for i=0..3.
#The coefficient wij are given by
w01:=coeff(ta0,X,3): w11:=-coeff(ta0,X,2):
w02:=coeff(ta1,X,3): w12:=-coeff(ta1,X,2):
w03:=coeff(ta2,X,3): w13:=-coeff(ta2,X,2):
w04:=coeff(ta3,X,3): w14:=-coeff(ta3,X,2):
w05:=coeff(p0,X,3): w15:=-coeff(p0,X,2):
w06:=coeff(p1,X,3): w16:=-coeff(p1,X,2):
w07:=coeff(p2,X,3): w17:=-coeff(p2,X,2):
w08:=coeff(h4*g(X),X,3): w18:=-coeff(h4*g(X),X,2):

w21:=coeff(ta0,X,1): w31:=-coeff(ta0,X,0):
w22:=coeff(ta1,X,1): w32:=-coeff(ta1,X,0):
w23:=coeff(ta2,X,1): w33:=-coeff(ta2,X,0):
w24:=coeff(ta3,X,1): w34:=-coeff(ta3,X,0):
w25:=coeff(p0,X,1): w35:=-coeff(p0,X,0):
w26:=coeff(p1,X,1): w36:=-coeff(p1,X,0):
w27:=coeff(p2,X,1): w37:=-coeff(p2,X,0):
w28:=coeff(h4*g(X),X,1): w38:=-coeff(h4*g(X),X,0):

#We then compute the 4 last lines of the matrix W using that the square
#of W is a scalar matrix. We put

A:=[[w01,w02,w03,w04],
    [w11,w12,w13,w14],
    [w21,w22,w23,w24],
    [w31,w32,w33,w34]]:

B:=[[w05,w06,w07,w08],
    [w15,w16,w17,w18],
    [w25,w26,w27,w28],
    [w35,w36,w37,w38]]:

AA:=simplify(evalm(A^2)):
iB:=evalm(B^(-1)):
DD:=simplify(evalm(-iB&*A&*B)):
```

```
c:=cte*resultant(g(x),h(x),x):
Id:=[[1,0,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,1]]:
cIAA:=c*Id-AA:
C:=simplify(evalm(iB&*cIAA)):

#Finally, we have the matrix W
W:=matrix(8,8):
for i from 1 to 4 do
for j from 1 to 4 do
W[i,j]:=A[i,j];
W[i,j+4]:=B[i,j];
W[i+4,j]:=C[i,j];
W[i+4,j+4]:=DD[i,j]
od
od:

#The following must be the identity matrix
simplify(evalm(W^2/c));

#We have now to compute the constant c. We think it's not far from the
#resultant of g and h. That's the reason why we have chosen c to be
#cte*resultant(g,h). Hence we have to compute cte.
#For this, we use the following remark:
#if Wi is the matrix of the addition of the 2-torsion element Ai, and
#Wi^2=ci*I (the ci are not equal a priori because the constant c depends
#of g and h), there is a constant C such that W1(A2)=C*W2(A1). In the
#following, Ai is defined by the polynomial Gi, and Ki represents its
#coordinates in the Kummer.

#kumcoord computes the Kummer coordinates of an element of 2-torsion
#given by the polynomial G1
kumcoord:=proc(G1,H1)
local a0,a1,a2,a3,b0,b1,c0,c1,c2,c3,f5,f6,f7;
a0:=1:a1:=-coeff(G1(x),x,2)/coeff(G1(x),x,3):
a2:=coeff(G1(x),x,1)/coeff(G1(x),x,3):
a3:=-coeff(G1(x),x,0)/coeff(G1(x),x,3):
b0:=0:b1:=0:
f5:=coeff(G1(x)*H1(x),x,5):
f6:=coeff(G1(x)*H1(x),x,6):
f7:=coeff(G1(x)*H1(x),x,7):
c0:=a0*b0^2-f7*a1^3+f7*a1*a2-f6*a1^2+3*f7*a3+2*f6*a2:
c1:=a1*b0^2+2*a0*b0*b1-f7*a1^4+3*f7*a2*a1^2-f6*a1^3-f7*a2^2-f7*a3*a1+
```

```
2*f6*a2*a1-f5*a1^2+2*f5*a2:
c2:=a0*b1^2-a2*b0^2+f7*a2*a1^3-2*f7*a2^2*a1+f6*a2*a1^2+f7*a3*a2-f6*a2^2+
f5*a1*a2-3*f5*a3:
c3:=a1*b1^2+2*a2*b0*b1+a3*b0^2+f7*a2^2*a1^2-f7*a3*a1^3+f7*a3*a2*a1-
f7*a2^3+f6*a2^2*a1-f6*a3*a1^2+f5*a2^2-f5*a3*a1:
[a0,a1,a2,a3,c0,c1,c2,c3]:
end:

G1:=x->(gg3*x^2+gg2*x+gg1)*(x-e1):
H1:=x->(x-e2)*(hh4*x^3+hh3*x^2+hh2*x+hh1):
K1:=kumcoord(G1,H1):

G2:=x->(gg3*x^2+gg2*x+gg1)*(x-e2):
H2:=x->(x-e1)*(hh4*x^3+hh3*x^2+hh2*x+hh1):
K2:=kumcoord(G2,H2):

#We have
W1:=simplify(subs(
g0=coeff(G1(x),x,0),g1=coeff(G1(x),x,1),g2=coeff(G1(x),x,2),
g3=coeff(G1(x),x,3),h0=coeff(H1(x),x,0),h1=coeff(H1(x),x,1),
h2=coeff(H1(x),x,2),h3=coeff(H1(x),x,3),h4=coeff(H1(x),x,4),
cte=cte1,evalm(W))):
W2:=simplify(subs(g0=coeff(G2(x),x,0),g1=coeff(G2(x),x,1),
g2=coeff(G2(x),x,2),g3=coeff(G2(x),x,3),h0=coeff(H2(x),x,0),
h1=coeff(H2(x),x,1),h2=coeff(H2(x),x,2),h3=coeff(H2(x),x,3),
h4=coeff(H2(x),x,4),cte=cte2,evalm(W))):

W1K2:=simplify(evalm(W1&*K2)):
W2K1:=simplify(evalm(W2&*K1)):

#The constant C (such that W1*K2=C*W2*K1) can be obtained by
C:=evalm(W2K1[2]/W1K2[2]):

#The fifth and sixth line of W1*K2-C*W2*K1 then gives two equations in
#cte1 and cte2

eq1:=simplify(W1K2[5]-C*W2K1[5]):
eq2:=simplify(W1K2[6]-C*W2K1[6]):
System5:=[[coeff(eq1,cte1,1),coeff(eq1,cte2,1)],
          [coeff(eq2,cte1,1),coeff(eq2,cte2,1)]]:
System6:=-[subs(cte1=0,cte2=0,eq1),subs(cte1=0,cte2=0,eq2)]:
sol5:=simplify(evalm(System5^(-1)&*System6)):
```

```
#we then obtain that cte is equal to h4. We can now replace the constant
#cte in the matrix W.

W:=simplify(subs(cte=h4,evalm(W))):

#By this way the matrix W is entirely determined.
```

B.3 Formes biquadratiques

```
#This  program  computes biquadratic forms for hyperelliptic curves of
#genus 3 defined by a polynomial of degree 7. These computations are
#very long and need a lot of memory (I can do them with magma with 1 Go
#of RAM and 2 Go of swap. So that it is much simpler to consider an
#exemple). I choose this one because torsion points are easy to compute
#butthe user can change the function without any problem. Moreover the
#matrix which gives addition by a divisor of order 2 is given by the
#previous program and is denoted W in the following. Be carefull, this
#program is long to execute even with any given f. It took about 45 mn
#on a pentium 433.

f:=x->x*(x-1)*(x-2)*(x-3)*(x-4)*(x-5)*(x-6):i:='i':
for i from 0 to 7 do f.i:=coeff(f(x),x,i); od:

#sym3 transform a symetric polynomial in three variables in a polynomial
#in the elementary symmetric functions s=x1+x2+x3, b=x1*x2+x1*x3+x2*x3
#and p=x1*x2*x3.
s:='s':b:='b':p:='p':
sym3:=proc(P)
local Q,Q1,Q2,Q3,Q4,R,R1,R2,R3,u,v,w,x,y,t1,t2,s12,b12;
Q:=P:
t1:=simplify(Q-subs(x1=s2,x2=x1,s2=x2,Q));
t2:=simplify(Q-subs(x1=s2,x3=x1,x2=x3,s2=x2,Q));
if t1=0 and t2=0 then else print("polynomial is not symmetric"):break:fi:
while Q <> subs(x1=u,x2=v,x3=w,Q) do #test if Q depends of x1, x2 and x3
        R:=subs(x3=0,Q):
while R <> subs(x1=x,x2=y,R) do #test if Q depends of x1, x2
  R1:=subs(x2=0,R);
  R2:=R-subs(x1=x1+x2,R1);
  R3:=simplify(R2/x1/x2);
  R:=subs(x1=s12,R1)+b12*R3
od:
  Q2:=subs(s12=x1+x2+x3,b12=x1*x2+x1*x3+x2*x3,R);
  Q3:=Q-Q2;
  Q4:=simplify(Q3/(x1*x2*x3));
  Q:=subs(s12=s,b12=b,R)+p*Q4 od:
Q
end:

#We first transform the matrix W (constructed with the previous program)
#which gives addition by a divisor of order 2. This matrix is given in
```

```
#terms of the coefficients of g and h, where g is cubic (defining the
#divisor of order 2) and h is of degree 4. We first transform to the
#coefficients of G and those of F=GH, eliminating those of H. We shall
#also put g3=1, g2=-s, g1=b and g0=-p. To eliminate the h's, it is
#convenient to define the procedure subsh.
subsh:=proc(P)
local Q;
Q:=P;
Q:=subs(h0=f3+s*h1-b*h2+p*h3,Q);
Q:=subs(h1=f4+s*h2-b*h3+p*h4,Q);
Q:=subs(h2=f5+s*h3-b*h4,Q);
Q:=subs(h3=f6+s*h4,Q);
Q:=subs(h4=f7,Q);
Q:=simplify(Q);
Q
end:

#Let us now transform the matrix W
for i from 1 to 8 do
for j from 1 to 8 do
W[i,j]:=simplify(subs(g2=-s,g1=b,g0=-p,g3=1,subsh(W[i,j])))
od od:

#We now want g=0 to be a generic divisor of order 2. Since we no longer
#need the original uses of x1, x2, x3, we use them as a triplet of
#distinct zeros of f. We need to express that they are distinct.
B123:=simplify((x1*f(x2)-x2*f(x1)-x3*f(x2)+x3*f(x1)-x1*f(x3)+x2*f(x3))
               /((x1-x2)*(x2-x3)*(x3-x1))):
B23:=simplify((f(x2)-f(x3))/(x2-x3)):

#x1 is a root of f of degree 7. x2 and x3 are other roots of f, so
#satisfies  equation B123 of degree 5 and B23 of degree 6.
#By using B123 and B23 we can reduce a symmetric poly in x1, x2, x3 to
#degree at most 4 in x3. By symmetry it is of degree at most 4 in x1
#and x2 and so of the shape s^i*b^j*p^k, with i+j+k at most 4.
#The following program takes a symmetric function of x1, x2, x3 and
#makes the reduction.
simp:=proc(P)
local Q;
Q:=P;
Q:=rem(Q,B123,x1);
Q:=rem(Q,B23,x2);
Q:=rem(Q,f(x3),x3);
```

```
Q:=simplify(Q);
Q
end:

#Any polynomial in s, b, p is equal to a linear form in the elements
#s^i*b^j*p^k with i+j+k at most 4. We need a routine to do this.
simpsp:=proc(P)
local Q;
Q:=P;
Q:=subs(s=x1+x2+x3,b=x1*x2+x1*x3+x2*x3,p=x1*x2*x3,Q);
Q:=simp(Q);
Q:=sym3(Q);
Q
end:

#Let us now compute the coordinate of {(x1,0),(x2,0),(x3,0)}
a0:=1:
a1:=x1+x2+x3:
a2:=x1*x2+x1*x3+x2*x3:
a3:=x1*x2*x3:
c0:=-f7*s^3+f7*b*s-f6*s^2+3*f7*p+2*f6*b:
c1:=-f7*s^4+3*f7*b*s^2-f6*s^3-f7*b^2-f7*p*s+2*f6*b*s-f5*s^2+2*f5*b:
c2:=f7*b*s^3-2*f7*b^2*s+f6*b*s^2+f7*b*p-f6*b^2+f5*b*s-3*f5*p:
c3:=f7*b^2*s^2-f7*p*s^3+f7*p*b*s-f7*b^3+f6*b^2*s-f6*p*s^2+f5*b^2-f5*p*s:

#We want now to compute the product of all these coordinates
k:=[1,s,b,p,c0,c1,c2,c3]:
remp:=(i,j)->simpsp(k[i]*k[j]):
K2:=matrix(8,8,remp):

#Let us now write these products in the vector V.
V:=[K2[1,1],K2[1,2],K2[1,3],K2[1,4],K2[1,5],K2[1,6],K2[1,7],
            K2[2,2],K2[2,3],K2[2,4],K2[2,5],K2[2,6],K2[2,7],K2[2,8],
                    K2[3,3],K2[3,4],K2[3,5],K2[3,6],K2[3,7],K2[3,8],
                            K2[4,4],K2[4,5],K2[4,6],K2[4,7],K2[4,8],
                                    K2[5,5],K2[5,6],K2[5,7],K2[5,8],
                                            K2[6,6],K2[6,7],K2[6,8],
                                                    K2[7,7],K2[7,8],
                                                            K2[8,8]]:

#the vector V corresponds to the following products
Z:=[A0*A0,A0*A1,A0*A2,A0*A3,A0*C0,A0*C1,A0*C2,
          A1*A1,A1*A2,A1*A3,A1*C0,A1*C1,A1*C2,A1*C3,
```

```
                A2*A2,A2*A3,A2*C0,A2*C1,A2*C2,A2*C3,
                      A3*A3,A3*C0,A3*C1,A3*C2,A3*C3,
                            C0*C0,C0*C1,C0*C2,C0*C3,
                                  C1*C1,C1*C2,C1*C3,
                                        C2*C2,C2*C3,
                                              C3*C3]:

#Hence V[i] is Z[i] expressed with s,b and p. Note that in these vectors
#there is not the product a0c3. That is because of the relation
#a0c3-a1c2-a2c1-a3c0-2f5*a1*a3+f5*a2^2+2*f6*a2*a3+3*f7*a3^2=0
#In fact opposite to the genus 2 case, all the product are not linearly
#independant. Nevertheless, if we replace a0c3 in all the expressions by
#a1c2+a2c1+..., the remaining products are independant. Since this
#relation always occur (not only for divisors of order 2) we can still
#deduce the general case from the 2-torsion case.

#We now need a program (called tryon) to convert a linear form in the
#s^i*b^j*p^k into a quadratic form in a0,a1,a2,a3,c0,c1,c2,c3 (without
#any term in a0c3). For example c3^2 is the only product where p^4 lies.
#Hence the term in c3^2 is given by the term of p^4. We can then look at
#this problem as a system. Let us construct the matrix M of 35
#coefficients in some s^i*b^j*p^k of each of the 35 products in V.
coef:=(cs,cb,cp,es)->(coeff(coeff(coeff(es,s,cs),b,cb),p,cp)):
M:=matrix(35,35,0):
t:=0:
for i from 0 to 4 do
for j from 0 to 4-i do
for l from 0 to 4-i-j do
    t:=t+1:
    for m from 1 to 35 do
M[t,m]:=coef(i,j,l,V[m])
    od:
od od od:
Mi:=evalm(M^(-1)):

tryon:=proc(P)
local Q,R,S,t,i,j,l;
Q:=P:
R:=matrix(35,1):
t:=0:
for i from 0 to 4 do
for j from 0 to 4-i do
for l from 0 to 4-i-j do
```

```
t:=t+1:
R[t,1]:=coef(i,j,l,Q)
od od od:
#R is the vector of coefficients of s^i*b^j*p^l, so that Mi*R is the
#vector of the coefficients of the desired quadratic form in the 35
#products in V.
S:=evalm(Z&*evalm(Mi&*R)):
Q:=simplify(S[1]):
Q
end:

#We now construct the biquadratic forms. Let us first reduce the
#coefficients of the matrix W using simpsp
for i from 1 to 8 do
for j from 1 to 8 do
W[i,j]:=simpsp(W[i,j]) od od:

#Let A be a generic divisor [y1,y2,y3,y4,y5,y6,y7,y8]. Unfortunately
#we cannot make directly the computations of the products Y[i]*Y[j]
#by using Y[i]:=sum('y.j*W[i,j]',j=1..8) because it requires too many
#RAM. We can only compute them for little i and j.
#So, we need to compute the coefficients of these products one by one.
#In other words, we need to compute all the product of the elements of
#the matrix W. We write this in a matrix 8*8 (called WW) which
#coefficients are 8*8 matrices such that WW[i,j][k,l]=W[i,j]*W[k,l].
#The procedure compare is used to do computations of each W[i,j]*W[k,l]
#only one time.
compare:=proc(u,v)
local a;
a:=0:
if u[1]<v[1] then a:=1 fi:
if u[1]=v[1] and u[2]<v[2] then a:=1 fi:
a
end:

#Be carefull, this is a long computation (about 35mn with a pentium 433)
WW:=matrix(8,8,0):
 T:=time():
 for i from 1 to 8 do
   t:=time():
   for j from 1 to 8 do
     WW[i,j]:=matrix(8,8,0):
     for k from 1 to 8 do
```

```
       for l from 1 to 8 do
         if compare([k,l],[i,j])=0 then #cond kl > ij
         WW[i,j][k,l]:=tryon(simpsp(expand(W[i,j]*W[k,l])))
         fi
       od
     od
   od:
 print(i,"time=",time()-t)
 od:
 print("total time=",time()-T);

#Let us now complete the matrix WW by symmetry
for i from 1 to 8 do
for j from 1 to 8 do
for k from 1 to 8 do
for l from 1 to 8 do
    if compare([k,l],[i,j])=1 then
       WW[i,j][k,l]:=WW[k,l][i,j]
    fi
od od od od:

#We can now write the products Y[i]*Y[j] and then deduce the matrix
#Phi of the biquadratic forms. Note that, as we choose to replace the
#term in a0c3, we have to replace the term in y1y8
#if we want the Y[i]*Y[j] to be symmetric
k:='k':i:='i':j:='j':l:='l':
Phi:=matrix(8,8,0):
for i from 1 to 8 do
    for j from 1 to 8 do
phi:=simplify(sum('sum('WW[i,k][j,l]*y.k',k=1..8)*y.l',l=1..8)):
toreplace:=coeff(coeff(phi,y1,1),y8,1):
Phi[i,j]:=simplify(phi-toreplace*y1*y8+toreplace*(y2*y7+y3*y6+
                         y4*y5+2*f5*y2*y4-f5*y3^2-2*f6*y3*y4-3*f7*y4^2))
     od
 od:

#We can now check that these Phi[i,j] actually are symmetric in the y's
#and the ai,ci although they are treated very differently.
test:=matrix(8,8,1):
for i from 1 to 8 do
    for j from 1 to 8 do
temp:=Phi[i,j]:
temp:=subs(A0=t1,A1=t2,A2=t3,A3=t4,C0=t5,C1=t6,C2=t7,C3=t8,
```

```
  y1=s1,y2=s2,y3=s3,y4=s4,y5=s5,y6=s6,y7=s7,y8=s8,temp):
temp:=subs(s1=A0,s2=A1,s3=A2,s4=A3,s5=C0,s6=C1,s7=C2,s8=C3,
                  t1=y1,t2=y2,t3=y3,t4=y4,t5=y5,t6=y6,t7=y7,t8=y8,temp):
test[i,j]:=simplify(Phi[i,j]-temp);
if test[i,j]=0 then else print("mistake",i,j) fi;
    od:
od:

#test must be 0
```

Annexe C

Matrice de l'addition d'un point de 2-torsion pour une courbe hyperelliptique de genre 3

Soit $\mathcal{C}$ une courbe hyperelliptique de genre 3 définie sur un corps de nombres $\mathbf{k}$ par une équation de la forme

$$Y^2 \;=\; F(X) \text{ avec } F \in \mathbf{k}[X] \text{ de degré 7.}$$

Soit $\mathcal{X} = \{[x_1, y_1], [x_2, y_2], [x_3, y_3]\}$ un diviseur générique et $\mathcal{A} = \{[\theta_1, 0], [\theta_2, 0], [\theta_3, 0]\}$ un élément d'ordre 2 de la jacobienne.
On pose

$$G(X) \;=\; (X - \theta_1)(X - \theta_2)(X - \theta_3) \text{ et } F(X) = G(X)H(X),$$

avec les notations

$$\begin{aligned} H(X) &= h_4X^4 + h_3X^3 + h_2X^2 + h_1X + h_0, \\ G(X) &= g_3X^3 + g_2X^2 + g_1X + g_0. \end{aligned}$$

L'addition du point de 2-torsion $\mathcal{A}$ est une application linéaire sur la variété de Kummer (qui est incluse dans $\mathbb{P}^8$). Elle peut donc être représentée par une matrice $\mathbf{W} = (w_{ij})_{1 \leqslant i,j \leqslant 8}$. Autrement dit, si $\xi_i(\mathcal{X})$ désigne la $i^{\text{ème}}$ coordonnée de $\mathcal{X}$ dans la variété de Kummer,

$$\xi_i(\mathcal{X} + \mathcal{A}) = \sum_{j=1}^{8} w_{ij}\xi_j(\mathcal{X}) \text{ pour } i = 1, \ldots, 8.$$

Les 4 premières lignes de cette matrice ont été obtenues en utilisant la définition géométrique de l'addition de $\mathcal{X}$ et de $\mathcal{A}$ tandis que les 4 dernières ont été obtenues entre autres en utilisant le fait que $\mathbf{W}$ est une matrice dont le carré est une matrice scalaire.

$$\begin{aligned}
w_{11} &= -g_0h_2g_2h_4 + h_4h_2g_1^2,\\
w_{12} &= g_1h_4g_2h_2 + g_1^2h_4h_3 - g_0h_2g_3h_4 - g_0h_4g_2h_3,\\
w_{13} &= g_1^2h_4^2 + 2g_1h_4g_2h_3 + g_2^2h_4h_2 - 2h_4g_3h_3g_0 - g_0h_4^2g_2,\\
w_{14} &= 3g_2^2h_4h_3 + 2g_2h_4g_3h_2 - 3g_0h_4^2g_3 + 3g_1h_4^2g_2,\\
w_{15} &= g_0h_4,\\
w_{16} &= -g_1h_4,\\
w_{17} &= g_2h_4,\\
w_{18} &= g_3h_4,
\end{aligned}$$

$$\begin{aligned}
w_{21} &= -h_4g_1h_2g_0 - h_4g_2h_1g_0 + h_3g_2h_2g_0 + g_1^2h_1h_4 - g_1^2h_2h_3 - h_2g_3h_0g_2 + g_2g_3h_1^2,\\
w_{22} &= -g_1h_3g_2h_2 + h_3g_3h_2g_0 - h_3g_3h_0g_2 + h_4g_2g_1h_1 + h_1g_3g_2h_2 + h_1^2g_3^2 - g_1^2h_3^2 - h_4g_2h_2g_0 +\\
&\quad g_2h_3^2g_0 - h_2h_0g_3^2 - h_1g_0g_3h_4 - h_4g_1h_3g_0,\\
w_{23} &= -h_4g_3h_2g_0 + 2h_1g_3^2h_2 - 2g_1^2h_4h_3 - 2h_3h_0g_3^2 - g_0h_4^2g_1 - 2g_1h_3^2g_2 - h_4g_3h_0g_2 + h_1g_2^2h_4 +\\
&\quad h_2^2g_3g_2 - g_2^2h_3h_2 + 2g_3h_3^2g_0,\\
w_{24} &= -3h_4h_0g_3^2 - g_1h_2g_3h_4 - g_0h_4^2g_2 - 2g_1^2h_4^2 + 3h_4g_3h_3g_0 + h_1g_3g_2h_4 + g_2^2h_4h_2 + 3h_2^2g_3^2 -\\
&\quad 6g_1h_4g_2h_3 - 3g_2^2h_3^2,\\
w_{25} &= -g_0h_3 + g_3h_0,\\
w_{26} &= g_1h_3 - h_1g_3 + g_0h_4,\\
w_{27} &= -g_2h_3 + h_2g_3 - g_1h_4,\\
w_{28} &= -g_2h_4,
\end{aligned}$$

$$\begin{aligned}
w_{31} &= -g_1g_0h_1h_4 + h_2g_1h_3g_0 + h_3g_2h_1g_0 - g_2h_2^2g_0 - g_1^2h_1h_3 + g_1^2h_2^2 - h_2g_3h_0g_1 + g_1g_3h_1^2 +\\
&\quad h_2h_0g_2^2 - g_2^2h_1^2 - h_1g_2h_0g_3,\\
w_{32} &= g_1h_2g_3h_1 + g_1h_2^2g_2 + g_1h_3^2g_0 + h_3g_3h_1g_0 - g_2^2h_1h_2 - h_1h_0g_3^2 - g_2h_1g_1h_3 - h_3g_3h_0g_1 -\\
&\quad g_1^2h_1h_4 + g_1^2h_2h_3 - g_3h_2^2g_0 + h_3h_0g_2^2 - g_2g_3h_1^2,\\
w_{33} &= -h_3g_3h_2g_0 - h_2h_0g_3^2 - h_4g_3h_0g_1 + g_2h_3^2g_0 + h_1g_0g_3h_4 + g_1h_2^2g_3 + h_4h_0g_2^2 + 2g_1h_3g_2h_2 -\\
&\quad g_2^2h_1h_3 + h_3g_3h_0g_2 - 2h_4g_2g_1h_1 + 2h_4g_1h_3g_0 - 2h_1g_3g_2h_2 + g_1^2h_3^2 - h_1^2g_3^2,\\
w_{34} &= -3h_1g_3^2h_2 + 3g_1h_2g_3h_3 - h_1g_2^2h_4 - 2h_1g_3g_1h_4 + 2h_4g_3h_0g_2 + 2g_0h_4^2g_1 + 4h_4g_2h_3g_0 -\\
&\quad 3g_2h_1g_3h_3 + 2g_1^2h_4h_3 + 3g_1h_3^2g_2]),\\
w_{35} &= g_0h_2 - g_2h_0,\\
w_{36} &= -g_0h_3 + g_3h_0 - g_1h_2 + g_2h_1,\\
w_{37} &= g_1h_3 - h_1g_3 + g_0h_4,\\
w_{38} &= g_1h_4,
\end{aligned}$$

$$\begin{aligned}
w_{41} &= h_3h_1g_1g_0 - h_2^2g_1g_0 - h_1h_0g_3g_1 + h_1h_0g_2^2,\\
w_{42} &= -g_2h_2^2g_0 - h_2g_3h_0g_1 + h_2h_0g_2^2 + h_1g_2h_0g_3 + g_1g_0h_1h_4 - h_2g_1h_3g_0 + h_3g_2h_1g_0,\\
w_{43} &= h_3g_3h_1g_0 + h_3h_0g_2^2 + 2h_2g_3h_0g_2 - g_1h_3^2g_0 - 2h_3g_2h_2g_0 + 2h_4g_2h_1g_0 - g_3h_2^2g_0 -\\
&\quad h_3g_3h_0g_1 + h_1h_0g_3^2,\\
w_{44} &= 3h_2h_0g_3^2 + h_4h_0g_2^2 - h_4g_3h_0g_1 - 3h_3g_3h_2g_0 + 3h_3g_3h_0g_2 + 3h_1g_0g_3h_4 - 3g_2h_3^2g_0 -\\
&\quad 2h_4g_1h_3g_0,\\
w_{45} &= -g_0h_1 + g_1h_0,\\
w_{46} &= g_0h_2 - g_2h_0,
\end{aligned}$$

$$
\begin{aligned}
w_{47} &= -g_0h_3 + g_3h_0, \\
w_{48} &= -g_0h_4,
\end{aligned}
$$

$$
\begin{aligned}
w_{51} = {} & g_3^2h_0^2h_4g_2 - 2h_1g_3g_0^2h_4^2 - 2g_1h_0g_3^2h_3h_2 + g_2^2h_0g_0h_4^2 - g_2h_0g_1^2h_4^2 - g_0^2h_2h_4^2g_2 - \\
& g_0h_3h_4g_3h_0g_2 - g_3^2h_0h_4h_2g_0 + g_0^2h_3h_4g_3h_2 + 2g_0h_4^2g_3h_0g_1 + 2h_4h_2^2g_1^2g_2 - 4h_4g_3^2h_0h_1g_1 + \\
& g_0^3h_4^3 - h_2^2g_3^2g_2h_0 + g_2^2h_3^2h_2g_0 + g_2^3h_4h_0h_2 - g_1^2h_2h_3^2g_2 + g_1^2h_2^2h_3g_3 - g_2^2g_3h_1^2h_3 + \\
& g_2g_3^2h_1^2h_2 - h_1g_3g_2h_2g_0h_4 - g_2^3h_4h_1^2 + g_2^2h_0h_3h_2g_3 - g_0h_2^2g_3g_2h_3 - g_2h_4g_1h_0g_3h_2 + \\
& g_2h_4g_1g_3h_1^2 + g_1^2h_2g_3h_1h_4 + g_0h_1^2g_3^2h_4 + g_1^2h_0g_3h_3h_4 - 4g_0h_2^2g_3g_1h_4 + 2g_2^2h_4h_0g_3h_1 - \\
& 2g_3^2h_0h_1g_2h_3 + 2g_0h_3^2g_1h_2g_3 + 2g_0h_1g_3h_3^2g_2 + 2h_1^2g_3^2g_1h_3 - 2g_1^2h_3^2h_1g_3 - 2g_2^2h_4g_0h_2^2,
\end{aligned}
$$

$$
\begin{aligned}
w_{52} = {} & g_1h_4^3g_0^2 - g_0^2h_2h_4^2g_3 + g_0^2h_3^2h_4g_3 - g_0^2h_3h_4^2g_2 + g_3^3h_0^2h_4 + 2g_3h_0g_0h_4^2g_2 - 2g_0h_3h_4h_0g_3^2 - \\
& h_4h_1^2g_2^2g_3 - h_1g_3h_3g_2^2h_2 + g_1h_2^2h_3g_2g_3 - 2g_3^2h_0h_3g_2h_2 + 2g_0h_3^2g_2h_2g_3 - g_1h_2g_2^2h_3^2 + \\
& h_2^2g_3^2g_2h_1 - g_2^3h_4h_1h_2 - g_1^2h_3^3g_2 + g_0h_3^3g_2^2 - g_3^3h_0h_2^2 - g_2h_4^2g_1^2h_1 + g_2^3h_4h_0h_3 + \\
& g_1^2h_3^2h_2g_3 - g_0h_2^2g_3^2h_3 + g_2^2h_0g_3h_3^2 - h_1^2g_3^2g_2h_3 + g_1^2h_4^2h_0g_3 - g_1h_4^2g_2^2h_0 + g_0h_4^2h_1g_2^2 + \\
& h_1^2g_3^3h_2 - 6g_3h_4g_0h_2^2g_2 + 2h_1g_3^2h_2g_1h_3 + 2g_2h_4g_1^2h_2h_3 - 2g_3h_4g_1^2h_1h_3 + 2g_3^2h_4g_2h_0h_1 + \\
& 2g_3h_4g_0h_1g_2h_3 + 2g_3h_4^2g_1g_0h_1 - 2g_1h_3^2g_2h_1g_3 + 2g_2h_4g_1h_2g_3h_1 + 2g_2^2h_4g_1h_2^2 - \\
& 2g_3^3h_0h_3h_1 - 2g_3^2h_0h_3^2g_1 + 2g_0h_3^3g_3g_1 + 2g_0h_3^2g_3^2h_1 + 3g_3h_4g_2^2h_0h_2 - 4g_3h_4g_0h_2g_1h_3 - \\
& 2g_2^2h_4g_0h_2h_3 - 4g_3^2h_4g_1h_0h_2,
\end{aligned}
$$

$$
\begin{aligned}
w_{53} = {} & h_4h_2^2g_2^3 - g_0h_4^2h_0g_3^2 + g_0^2h_4^2g_3h_3 - g_0^2h_4^3g_2 + 4h_4g_1h_2g_2^2h_3 + 4h_4h_1g_3^3h_0 - 2h_3^3g_2^2g_1 + \\
& 2h_2^2g_3^3h_1 - 2h_1^2g_3^3h_3 + 2h_3^3g_1^2g_3 + 4h_3^3g_2g_3g_0 - 4g_3^3h_0h_2h_3 - h_4h_1^2g_2g_3^2 + h_2^3g_3^2g_2 + \\
& 2h_3^2g_3h_2g_1g_2 - 2h_1g_3h_3^2g_2^2 - 2h_1g_3^2h_3g_2h_2 + 2h_3g_3^2h_2^2g_1 + g_1^2h_4^3g_0 + h_4^2g_2g_1^2h_2 - h_2g_2^3h_3^2 - \\
& 2h_4^2h_1g_2^2g_1 - g_2h_4g_1^2h_3^2 + g_2^2h_4g_0h_3^2 + g_1h_4^2g_2h_0g_3 + g_1h_4h_2^2g_3g_2 + 2g_1h_4g_0h_3^2g_3 - \\
& g_2^2h_4h_1g_3h_2 - 3g_3h_4^2g_0h_2g_1 + 6g_2^2h_4h_0g_3h_3 - 4g_1h_4g_2h_3h_1g_3 + 8g_3h_4^2g_0h_1g_2 + \\
& 4g_0h_4g_3^2h_3h_1 + 3g_3^2h_4g_2h_0h_2 - 2g_3h_4g_1^2h_2h_3 - 11g_3h_4g_0h_2g_2h_3 - 6g_1h_4g_3^2h_0h_3 - \\
& 3g_0h_4h_2^2g_3^2,
\end{aligned}
$$

$$
\begin{aligned}
w_{54} = {} & -3g_2^3h_3^3 + g_0^2h_4^3g_3 - g_1^2h_3h_4^2g_2 - g_1h_4^2g_0g_3h_3 - 3h_2g_2^2h_3^2g_3 + 6g_3h_3^3g_1g_2 + 6g_3^2h_3^2g_1h_2 - \\
& 6h_1g_3^2g_2h_3^2 + g_1^3h_4^3 - 6h_1g_3^3h_2h_3 + 3h_2^2g_2g_3^2h_3 - 2h_4^2g_3^2h_0g_1 + 7h_4^2g_0h_1g_3^2 + 3g_3^3h_2^3 + \\
& h_4h_1^2g_3^3 + 4h_4^2g_2^2g_3h_0 + 4h_4^2g_1g_2^2h_2 + 3h_4h_2^2g_2^2g_3 + 4h_4g_2^3h_3h_2 - 2h_4^2g_2^3h_1 + 5h_4g_1^2h_3^2g_3 + \\
& 5h_4g_3^3h_0h_2 - 3h_4g_2^2h_3^2g_1 - 6h_4g_1h_3g_3^2h_1 - 5h_4g_0h_3g_3^2h_2 + h_4g_0h_3^2g_3g_2 + h_4^2h_1g_3g_2g_1 + \\
& 11h_4g_3^2h_0g_2h_3 - 3h_4g_2^2h_1g_3h_3 - 5h_4g_1h_2g_3g_2h_3 - 3h_4g_2h_1g_3^2h_2 - 4g_3h_4^2g_0h_2g_2 + \\
& 4g_2^2h_4^2g_0h_3 - 4g_3h_4^2g_1^2h_2,
\end{aligned}
$$

$$
\begin{aligned}
w_{55} = {} & -3h_1g_0g_3h_4 + 2h_4g_2h_2g_0 + h_3g_3h_2g_0 - g_2h_3^2g_0 - h_4h_0g_2^2 + 3h_4g_3h_0g_1 - h_3g_3h_0g_2 + \\
& h_2h_0g_3^2, \\
w_{56} = {} & 4h_4g_3h_2g_0 - 2g_3h_3^2g_0 + h_1g_2^2h_4 - 2g_1h_4g_2h_2 - 2h_4g_3h_0g_2 - g_1h_2g_3h_3 + g_2h_1g_3h_3 + \\
& g_1h_3^2g_2 + 2h_3h_0g_3^2 - h_1g_3^2h_2, \\
w_{57} = {} & g_0h_4^2g_2 - h_4g_3h_3g_0 + g_2^2h_4h_2 + 3h_4h_0g_3^2 - h_1g_3g_2h_4 - g_1h_2g_3h_4 + 2h_3^2g_3g_1 - 2h_1g_3^2h_3 + \\
& h_2^2g_3^2 - g_2^2h_3^2, \\
w_{58} = {} & -(3g_3h_4g_0 - g_1h_4g_2 - 2g_1g_3h_3 + g_2^2h_3)h_4,
\end{aligned}
$$

$$
\begin{aligned}
w_{61} = {} & -h_3^2h_2g_1^3+h_1^3g_3^2g_2+2h_4g_1^2h_1^2g_3+h_4^2g_0^3h_3-h_4^2g_3h_0g_0^2-2h_3h_2g_1^2h_1g_3+2h_1^2g_2g_1g_3h_3- \\
& h_3g_3h_1g_0^2h_4-2h_2g_3h_0g_2g_0h_4+h_3g_3h_0g_1g_0h_4+g_3h_2^2g_0^2h_4-h_4^2g_2h_1g_0^2-h_4g_3^2h_0^2g_1+ \\
& h_1h_0g_3^2g_0h_4+h_4h_0^2g_2^2g_3+h_1^2g_3^2g_1h_2-h_1g_1^2h_3^2g_2-g_0^2h_4^2g_1h_2+2g_0h_4^2g_1g_2h_0-h_2^3g_3g_2g_0+ \\
& g_2^3h_3h_2h_0-g_1h_4g_2^2h_1^2+g_0h_3^2g_2^2h_1-g_3^2h_0h_2^2g_1+g_2^3h_0h_4h_1+2g_1^3h_4h_2^2-g_1^3h_4^2h_0+ \\
& 2h_4g_2g_1^2h_1h_2-3g_1h_2g_3h_1g_0h_4+g_1h_4g_2^2h_0h_2+g_1^2h_2^3g_3-g_2^3h_1^2h_3-g_2^2h_0h_3h_1g_3+ \\
& g_0h_2^2g_3g_1h_3-2g_1h_3g_2h_2g_3h_0-2g_2^2h_1h_2g_0h_4-2g_3^2h_0h_2g_2h_1+2g_0h_3^2g_2g_1h_2- \\
& 3g_1h_4g_2h_0g_3h_1-4g_1h_4g_0h_2^2g_2+2g_0h_2g_3h_3g_2h_1,
\end{aligned}
$$

$$
\begin{aligned}
w_{62} = {} & g_3^2h_0^2h_4g_2-2h_1g_3g_0^2h_4^2-2g_1h_0g_3^2h_3h_2+g_2^2h_0g_0h_4^2-g_2h_0g_1^2h_4^2-g_0^2h_2h_4^2g_2- \\
& g_0h_3h_4g_3h_0g_2-g_3^2h_0h_4h_2g_0+g_0^2h_3h_4g_3h_2+2g_0h_4^2g_3h_0g_1+2h_4h_2^2g_1^2g_2-2h_4g_3^2h_0h_1g_1+ \\
& g_0^3h_4^3-g_1^3h_3^3+h_1^3g_3^3-h_2^2g_3^2g_2h_0+g_2^2h_3^2h_2g_0+g_2^3h_4h_0h_2-g_1^2h_2h_3^2g_2+ \\
& g_1^2h_2^2h_3g_3-g_2^2g_3h_1^2h_3+g_2g_3^2h_1^2h_2-2g_0h_1g_3h_3g_1h_4-3h_1g_3g_2h_2g_0h_4+2g_2h_4^2g_1g_0h_1- \\
& g_2h_4g_1h_0g_3h_2+g_1h_2^3g_2g_3-g_2^3h_1h_2h_3+g_1h_2^2g_3^2h_1-g_2^2h_1g_1h_3^2-g_0h_2^3g_3^2+g_2^3h_0h_3^2- \\
& g_1^3h_1h_4^2+g_2^2h_1h_2g_1h_4+g_2^2h_0h_3g_1h_4-2g_0h_2^2g_3g_1h_4+g_2^2h_4h_0g_3h_1-2g_3^2h_0h_1g_2h_3+ \\
& 2g_0h_3^2g_1h_2g_3-4g_2h_4g_0h_2g_1h_3+2g_0h_1g_3h_3^2g_2-2g_1h_0g_3h_3^2g_2+h_1^2g_3^2g_1h_3-g_1^2h_3^2h_1g_3- \\
& 2g_2^2h_4g_0h_2^2+2g_0h_3^3g_1g_2-2g_3^3h_0h_1h_2+2g_1^3h_2h_3h_4+2g_0h_1g_3^2h_3h_2,
\end{aligned}
$$

$$
\begin{aligned}
w_{63} = {} & g_1h_4^3g_0^2-g_0^2h_2h_4^2g_3+g_0^2h_3^2h_4g_3-g_0^2h_3h_4^2g_2+g_3^3h_0^2h_4+2g_3h_0g_0h_4^2g_2-2g_0h_3h_4h_0g_3^2+ \\
& g_1h_2^3g_3^2+h_4h_1^2g_2^2g_3-h_3^2g_2^3h_1+h_4^2g_0g_1^2h_3+h_2^3g_3g_2^2-4h_1g_3h_3g_2^2h_2+4g_1h_2^2h_3g_2g_3- \\
& 2g_3^2h_0h_3g_2h_2-h_3g_2^3h_2^2+2g_0h_3^2g_2h_2g_3-g_1h_2g_2^2h_3^2+h_2^2g_3^2g_2h_1+2g_2^3h_4h_1h_2-g_1^2h_3^3g_2+ \\
& g_0h_3^3g_2^2-g_3^3h_0h_2^2+g_0h_4h_1g_3^2h_2-g_2h_4^2g_1^2h_1+2g_2^3h_4h_0h_3+g_1^2h_3^2h_2g_3-g_0h_2^2g_3^2h_3+ \\
& g_2^2h_0g_3h_3^2-h_1^2g_3^2g_2h_3+2g_0h_4^2h_1g_2^2+g_3h_4g_1^2h_2^2-g_3^2h_4g_1h_1^2-g_2h_4g_1h_0g_3h_3+h_1^2g_3^3h_2- \\
& g_1^3h_4h_3^2+g_1^3h_4^2h_2-2g_3h_4g_0h_2^2g_2+2h_1g_3^2h_2g_1h_3+2g_2h_4g_1^2h_2h_3-2g_3h_4g_1^2h_1h_3+ \\
& 2g_2h_4g_0h_3^2g_1-g_3h_4g_0h_1g_2h_3-g_3h_4^2g_1g_0h_1-2g_1h_3^2g_2h_1g_3-4g_2h_4g_1h_2g_3h_1+ \\
& g_2^2h_4g_1h_2^2-2g_3^3h_0h_3h_1-2g_3^2h_0h_3^2g_1+2g_0h_3^3g_3g_1+2g_0h_3^2g_3^2h_1-2g_2h_4^2g_0h_2g_1+ \\
& 2g_3h_4g_2^2h_0h_2-2g_3h_4g_0h_2g_1h_3-2g_2^2h_4g_0h_2h_3-3g_3^2h_4g_1h_0h_2,
\end{aligned}
$$

$$
\begin{aligned}
w_{64} = {} & h_4h_2^2g_2^3-g_0h_4^2h_0g_3^2+g_0^2h_4^2g_3h_3-g_0^2h_4^3g_2-2h_4g_1h_2g_2^2h_3-2h_4h_1g_3^3h_0+2h_4g_2^3h_1h_3+ \\
& h_4h_1^2g_2g_3^2+3h_2^3g_3^2g_2+6h_3^2g_3h_2g_1g_2-6h_1g_3h_3^2g_2^2-6h_1g_3^2h_3g_2h_2+6h_3g_3^2h_2^2g_1+ \\
& 3g_1^2h_4^3g_0+h_4^2g_2g_1^2h_2-3h_2g_2^3h_3^2+2h_4^2h_1g_2^2g_1-g_2h_4g_1^2h_3^2+g_2^2h_4g_0h_3^2+3g_1h_4^2g_2h_0g_3+ \\
& g_1h_4h_2^2g_3g_2+4g_1h_4g_0h_3^2g_3+2g_2h_4^2g_0h_3g_1+3g_2^2h_4h_1g_3h_2-3g_3h_4^2g_0h_2g_1+ \\
& 6g_2^2h_4h_0g_3h_3-10g_1h_4g_2h_3h_1g_3+2g_0h_4g_3^2h_3h_1+g_3^2h_4g_2h_0h_2+4g_3h_4g_1^2h_2h_3+ \\
& 3g_3h_4g_0h_2g_2h_3-4g_1h_4g_3^2h_0h_3-6g_1h_4h_1g_3^2h_2+g_0h_4h_2^2g_3^2-4g_3h_4^2g_1^2h_1,
\end{aligned}
$$

$$
\begin{aligned}
w_{65} = {} & 2h_4g_1h_2g_0+g_3h_2^2g_0-h_3g_3h_1g_0-g_1h_3^2g_0+h_1h_0g_3^2-h_3h_0g_2^2+h_3g_3h_0g_1, \\
w_{66} = {} & 2h_4g_2h_2g_0+h_1g_0g_3h_4-h_3g_3h_2g_0-g_2h_3^2g_0-h_4h_0g_2^2-2g_1^2h_2h_4+h_4g_3h_0g_1+h_3g_3h_0g_2+ \\
& g_1^2h_3^2-h_1^2g_3^2+g_2^2h_1h_3-g_1h_2^2g_3+h_2h_0g_3^2, \\
w_{67} = {} & g_0h_4^2g_1+h_4g_3h_2g_0+h_1g_2^2h_4-2h_1g_3g_1h_4+h_4g_3h_0g_2-g_2^2h_3h_2+h_2^2g_3g_2-2g_2h_1g_3h_3+ \\
& 2g_1h_2g_3h_3, \\
w_{68} = {} & -(g_0h_4g_2-g_1^2h_4-2g_3h_2g_1+g_2^2h_2)h_4,
\end{aligned}
$$

$$w_{71} = h_4h_0^2g_2^3 - g_0h_4^2g_1^2h_0 - g_1^3h_4h_3h_0 + h_4g_0^3h_3^2 - h_4^2g_0^3h_2 - 2h_4g_0^2h_3g_3h_0 + h_4g_1^2h_0g_2h_2 + h_4g_3^2h_0^2g_0 + h_4^2g_2h_0g_0^2 + g_0h_2^3g_2^2 + 3g_1^2h_4g_3h_0h_1 + 4g_1h_0g_3^2h_2h_1 + h_3^2h_1g_1^3 - h_2^2g_1^3h_3 + 2g_1^2h_4g_0h_2^2 - h_1^3g_3^2g_1 - h_2^2g_2^3h_0 + h_1^3g_2^2g_3 + h_1g_1^2h_2g_2h_3 - h_1^2g_2g_1g_3h_2 - h_2^3g_2g_1^2 + h_1^2g_2^3h_2 - 3g_2^2h_0h_2h_1g_3 + 4g_2h_0g_3h_1g_1h_3 + g_2h_2^2g_0^2h_4 - 2h_3g_2h_1g_0^2h_4 - h_2g_1h_3g_0^2h_4 - 2h_2h_0g_2^2g_0h_4 + g_1g_0^2h_1h_4^2 + h_1g_2h_0g_3g_0h_4 + h_4g_2^2h_1^2g_0 - 4g_0h_2g_1h_3h_1g_3 - 3g_2^3h_0h_3h_1 - h_4g_2h_1g_0g_1h_2 + h_1g_0^2g_3h_4h_2 - 2h_4g_3h_0^2g_1g_2 + 3h_4g_1h_3g_0g_2h_0 - 4g_0h_1g_2h_3^2g_1 - 3g_1h_4g_2^2h_0h_1 + 3g_0h_2^2g_2g_1h_3 - g_1^2h_2^2h_1g_3 + 3g_0h_2^3g_3g_1 - g_0h_2g_1^2h_3^2 + h_1^2g_2^2g_1h_3 + h_1^2g_3^2h_0g_2 + h_4g_1^3h_1h_2 - g_0h_2g_2^2h_3h_1 - g_0h_1^2g_2h_3g_3 + g_2h_0g_3h_2^2g_1 - g_2^2h_0h_2g_1h_3 + g_0h_2^2g_2h_1g_3 + g_1^2h_0g_3h_2h_3,$$

$$w_{72} = -h_3^2h_2g_1^3 + h_1^3g_3^2g_2 - g_1h_2^3g_2^2 + h_4g_1^2h_1^2g_3 - 3h_2^2g_3g_2^2h_0 + h_1g_2^3h_2^2 + h_4^2g_0^3h_3 - 2g_0h_3^2g_1h_1g_3 - 2g_1h_2^2g_2h_1g_3 + 2g_3^2h_0h_1g_1h_3 + 2g_2^2h_1h_2g_1h_3 + 2g_2^2h_1^2h_2g_3 - h_4^2g_3h_0g_0^2 - 2g_1^2h_2^2g_2h_3 - 2h_3h_2g_1^2h_1g_3 + 2h_1^2g_2g_1g_3h_3 + 2h_4h_1g_1^3h_3 + 3g_2^2h_3h_2^2g_0 - h_3g_3h_1g_0^2h_4 - 2h_2g_3h_0g_2g_0h_4 + 2g_1^2h_4g_0h_2h_3 - 6g_1h_4g_0h_1g_2h_3 + h_3g_3h_0g_1g_0h_4 + g_3h_2^2g_0^2h_4 - h_4^2g_2h_1g_0^2 - h_4g_3^2h_0^2g_1 + h_1h_0g_3^2g_0h_4 + h_4h_0^2g_2^2g_3 - h_1^2g_3^2g_1h_2 + h_1g_1^2h_3^2g_2 - g_0^2h_4^2g_1h_2 + 2g_0h_4^2g_1g_2h_0 + 4h_2^3g_3g_2g_0 - 4g_2^3h_3h_2h_0 - g_1^2h_4^2g_0h_1 - 3g_0h_3^2g_2^2h_1 + 3g_3^2h_0h_2^2g_1 - g_1^3h_4^2h_0 + 2h_4g_2g_1^2h_1h_2 - 5g_1h_2g_3h_1g_0h_4 + 3g_1^2h_4h_0g_3h_2 - 2g_1h_4g_2^2h_0h_2 + g_2g_3h_1^2g_0h_4 - 4g_2^2h_0h_3h_1g_3 + 4g_0h_2^2g_3g_1h_3 - g_0h_1^2g_3^2h_3 - g_2^2h_0h_3^2g_1 + g_0h_2^2g_3^2h_1 + g_1^2h_0g_3h_3^2 + 4g_1h_3g_2h_2g_3h_0 - g_0h_3^3g_1^2 + g_3^3h_0h_1^2 - 2g_3^2h_0h_2g_2h_1 + 2g_0h_3^2g_2g_1h_2 - 3g_1h_4g_2h_0g_3h_1 + 2g_1h_4g_0h_2^2g_2 - 4g_0h_2g_3h_3g_2h_1,$$

$$w_{73} = g_3^2h_0^2h_4g_2 - 2h_1g_3g_0^2h_4^2 + 4g_1h_0g_3^2h_3h_2 + g_2^2h_0g_0h_4^2 - g_2h_0g_1^2h_4^2 - g_0^2h_2h_4^2g_2 - g_0h_3h_4g_3h_0g_2 - g_3^2h_0h_4h_2g_0 + g_0^2h_3h_4g_3h_2 + 2g_0h_4^2g_3h_0g_1 - 2h_4g_3^2h_0h_1g_1 + g_0^3h_4^3 - g_1^3h_3^3 + h_1^3g_3^3 - 5h_2^2g_3^2g_2h_0 + 5g_2^2h_3^2h_2g_0 - g_2^3h_4h_0h_2 - 3g_1^2h_2h_3^2g_2 - g_1^2h_2^2h_3g_3 + g_2^2g_3h_1^2h_3 + 3g_2g_3^2h_1^2h_2 - 8g_0h_1g_3h_3g_1h_4 - 7h_1g_3g_2h_2g_0h_4 - 10g_2^2h_0h_3h_2g_3 + 10g_0h_2^2g_3g_2h_3 - 4g_2h_4^2g_1g_0h_1 - 3g_2h_4g_1h_0g_3h_2 + 2g_2h_4g_1g_3h_1^2 - g_1h_2^3g_2g_3 + g_2^3h_1h_2h_3 - g_1h_2^2g_3^2h_1 + g_2^2h_1g_1h_3^2 + 3g_0h_3^2g_3^2 - 3g_2^3h_0h_3^2 + g_1^3h_1h_4^2 + 4g_1^2h_0g_3h_3h_4 + 3g_2^2h_1h_2g_1h_4 - 3g_2^2h_0h_3g_1h_4 + 2g_0h_2^2g_3g_1h_4 - g_2^2h_4h_0g_3h_1 - 4g_3^2h_0h_1g_2h_3 + 4g_0h_3^2g_1h_2g_3 + 2g_2h_4g_0h_2g_1h_3 - 4g_0h_1g_3h_3^2g_2 + 2g_1h_0g_3h_3^2g_2 + h_1^2g_3^2g_1h_3 - g_1^2h_3^2h_1g_3 + 2g_0h_3^3g_1g_2 - 2g_3^3h_0h_1h_2 - 2g_0h_1g_3^2h_3h_2 + 2g_2^2h_1h_2^2g_3 - 2g_1h_2^2g_2^2h_3 - 6g_2^2h_4g_0h_1h_3 + 4g_2h_4g_1^2h_1h_3,$$

$$w_{74} = g_1h_4^3g_0^2 - g_0^2h_2h_4^2g_3 + g_0^2h_3^2h_4g_3 - g_0^2h_3h_4^2g_2 + g_3^3h_0^2h_4 + 2g_3h_0g_0h_4^2g_2 - 2g_0h_3h_4h_0g_3^2 + h_4h_1^2g_2^2g_3 + 2h_4^2g_0g_1^2h_3 + 3h_1g_3h_3g_2^2h_2 - 3g_1h_2^2h_3g_2g_3 - 18g_3^2h_0h_3g_2h_2 + 18g_0h_3^2g_2h_2g_3 - 3g_1h_2g_2^2h_3^2 + 3h_2^2g_3^2g_2h_1 + g_2^3h_4h_1h_2 - 3g_1^2h_3^3g_2 + 9g_0h_3^3g_2^2 - 9g_3^3h_0h_2^2 - 8g_0h_4h_1g_3^2h_2 + 3g_2h_4^2g_1^2h_1 - 3g_2^3h_4h_0h_3 - 3g_1^2h_3^2h_2g_3 + 9g_0h_2^2g_3^2h_3 - 9g_2^2h_0g_3h_3^2 + 3h_1^2g_3^2g_2h_3 + 3g_1^2h_4^2h_0g_3 - 3g_1h_4^2g_2^2h_0 + g_0h_4^2h_1g_2^2 + 2g_3^2h_4g_1h_1^2 - 4g_2h_4g_1h_0g_3h_3 + 3h_1^2g_3^3h_2 - 2g_1^3h_4h_3^2 - 2g_2h_4g_1^2h_2h_3 - 2g_3^2h_4g_2h_0h_1 + 8g_2h_4g_0h_3^2g_1 - 14g_3h_4g_0h_1g_2h_3 - 12g_3h_4^2g_1g_0h_1 + 4g_2h_4g_1h_2g_3h_1 - 2g_2h_4^2g_0h_2g_1 - 5g_3h_4g_2^2h_0h_2 + 12g_3h_4g_0h_2g_1h_3 - 4g_2^2h_4g_0h_2h_3 - 4g_3^2h_4g_1h_0h_2 + 4g_2^2h_4h_1g_1h_3,$$

$$w_{75} = 3g_1g_0h_1h_4 - g_2h_2^2g_0 + 2h_2g_3h_1g_0 - h_2g_1h_3g_0 + 3h_3g_2h_1g_0 - 2g_1^2h_0h_4 + h_2h_0g_2^2 - 3h_2g_3h_0g_1 + h_1g_2h_0g_3 - 2h_3g_2h_0g_1,$$

$$w_{76} = -2h_4g_1h_2g_0 - 2h_3g_2h_2g_0 + g_1h_3^2g_0 - 3g_3h_2^2g_0 + h_3g_3h_1g_0 - g_1^2h_1h_4 + 2h_4g_2h_0g_1 + g_1h_2g_3h_1 + g_1^2h_2h_3 - g_2^2h_1h_2 + g_1h_2^2g_2 - h_1h_0g_3^2 + 2h_2g_3h_0g_2 - h_3g_3h_0g_1 - g_2g_3h_1^2 + 3h_3h_0g_2^2 - g_2h_1g_1h_3,$$

$$\begin{aligned}
w_{77} &= h_4g_1h_3g_0 - h_4g_2h_2g_0 - h_1g_0g_3h_4 + 3g_2h_3^2g_0 + 3h_3g_3h_2g_0 + h_4g_2g_1h_1 - 2h_4g_3h_0g_1 - \\
&\quad g_1^2h_3^2 + h_1^2g_3^2 - 3h_3g_3h_0g_2 - 3h_2h_0g_3^2 + h_1g_3g_2h_2 - g_1h_3g_2h_2, \\
w_{78} &= (2g_0g_1h_4 + 3g_0h_2g_3 + 3g_0g_2h_3 - g_1^2h_3 - g_1g_2h_2)h_4,
\end{aligned}$$

$$\begin{aligned}
w_{81} &= g_1^2h_2^2g_2h_1 + g_0g_1^2h_2^2h_3 - h_1^2g_2^2g_1h_2 - g_0h_1g_2^2h_2^2 + g_1^3h_2^3 + h_2^2g_1g_2^2h_0 - h_1^3g_2^3 + \\
&\quad 2h_1g_2^3h_0h_2 - 2g_1^3h_1h_3h_2 - h_1^2g_2g_1^2h_3 - h_1^2g_2^2h_0g_3 + 2h_1^3g_2g_1g_3 + h_1^2h_2g_3g_1^2 - 2g_0g_1h_2^3g_2 + \\
&\quad 2g_0h_1^2g_1h_3g_3 - 3g_0^2h_1g_3h_3h_2 + 2g_0h_2g_1h_4g_2h_0 - 2g_3h_0g_0^2h_4h_2 - 2g_0h_2^2g_2g_3h_0 - \\
&\quad 3g_0h_4g_1g_3h_0h_1 + 2g_3h_0^2g_0h_4g_2 - 2g_0^2h_3h_4g_2h_0 - 2g_1^2h_0h_3h_1g_3 - g_0^3h_3^3 + g_3^3h_0^3 + \\
&\quad 2g_2^2h_0h_2g_0h_3 + h_4h_1^2g_1^3 - g_2^2h_0^2h_4g_1 + g_1^2h_0^2g_3h_4 - g_0^2h_2^2g_2h_3 + g_2^2h_0^2h_2g_3 - g_2h_0^2g_3^2h_1 + \\
&\quad g_0^2h_2g_1h_3^2 - g_0^2h_4g_1h_2^2 + g_1h_0g_0^2h_4^2 - g_1^3h_0h_2h_4 + g_1h_0h_1^2g_3^2 - g_0h_1g_1^2h_3^2 - g_2^3h_0^2h_3 + \\
&\quad g_0^2h_2^3g_3 + g_1^3h_0h_3^2 - g_0h_1^3g_3^2 - g_0^3h_1h_4^2 + g_0h_3g_1^2h_4h_0 + g_1h_0g_3h_2g_0h_3 - g_2h_0g_3h_1g_0h_3 - \\
&\quad g_0^2h_4g_1h_1h_3 - 5g_1h_0h_1g_3g_2h_2 + g_1^2h_0h_4g_2h_1 - g_1^2h_0h_3g_2h_2 + g_1h_0g_2^2h_1h_3 - g_0h_1g_1h_2^2g_3 + \\
&\quad g_0h_1^2g_3g_2h_2 - g_0h_1g_1^2h_2h_4 - 3g_0h_1^2h_4g_2g_1 + 5g_0h_1g_1h_3g_2h_2 + 2g_0^2h_1g_2h_3^2 + 2g_0^2h_1^2g_3h_4 - \\
&\quad 2g_1h_0^2g_3^2h_2 + 3g_0^2h_3^2g_3h_0 - 3g_0h_3g_3^2h_0^2 + 2g_0^3h_3h_4h_2 + 3g_1h_0^2g_3h_3g_2 + 3g_3^2h_0h_1g_0h_2 - \\
&\quad 3g_0h_3^2g_1g_2h_0,
\end{aligned}$$

$$\begin{aligned}
w_{82} &= -h_4h_0^2g_2^3 + g_0h_4^2g_1^2h_0 + g_1^3h_4h_3h_0 - h_4g_0^3h_3^2 + h_4^2g_0^3h_2 + 2h_4g_0^2h_3g_3h_0 - h_4g_1^2h_0g_2h_2 - \\
&\quad h_4g_3^2h_0^2g_0 - h_4^2g_2h_0g_0^2 - g_0h_2^3g_2^2 - g_1^2h_4g_3h_0h_1 - 2g_1h_0g_3^2h_2h_1 - h_3^2h_1g_1^3 + h_2^2g_1^3h_3 + \\
&\quad h_1^3g_3^2g_1 + h_2^2g_2^3h_0 - h_1^3g_2^2g_3 - h_1g_1^2h_2g_2h_3 + h_1^2g_2g_1g_3h_2 + h_2^3g_2g_1^2 - h_1^2g_2^3h_2 + g_2^2h_0h_2h_1g_3 - \\
&\quad 2g_2h_0g_3h_1g_1h_3 - g_2h_2^2g_0^2h_4 + 2h_3g_2h_1g_0^2h_4 + h_2g_1h_3g_0^2h_4 + 2h_2h_0g_2^2g_0h_4 - g_1g_0^2h_1h_4^2 - \\
&\quad h_1g_2h_0g_3g_0h_4 - h_4g_2^2h_1^2g_0 + 2g_0h_2g_1h_3h_1g_3 + g_2^3h_0h_3h_1 + h_4g_2h_1g_0g_1h_2 - h_1g_0^2g_3h_4h_2 + \\
&\quad 2h_4g_3h_0^2g_1g_2 - 3h_4g_1h_3g_0g_2h_0 + 2g_0h_1g_2h_3^2g_1 + g_1h_4g_2^2h_0h_1 - g_0h_2^2g_2g_1h_3 + g_1^2h_2^2h_1g_3 - \\
&\quad g_0h_2^3g_3g_1 + g_0h_2g_1^2h_3^2 - h_1^2g_2^2g_1h_3 - h_1^2g_3^2h_0g_2 - h_4g_1^3h_1h_2 + g_0h_2g_2^2h_3h_1 + g_0h_1^2g_2h_3g_3 - \\
&\quad g_2h_0g_3h_2^2g_1 + g_2^2h_0h_2g_1h_3 - g_0h_2^2g_2h_1g_3 - g_1^2h_0g_3h_2h_3 - 2g_1^2h_4g_0h_1h_3,
\end{aligned}$$

$$\begin{aligned}
w_{83} &= h_3^2h_2g_1^3 - h_1^3g_3^2g_2 + 2h_2^2g_3g_2^2h_0 - h_4^2g_0^3h_3 + 2g_0h_3^2g_1h_1g_3 - 2g_3^2h_0h_1g_1h_3 - 2g_2^2h_1^2h_2g_3 + \\
&\quad h_4^2g_3h_0g_0^2 + 2g_1^2h_2^2g_2h_3 - 2h_4h_1g_1^3h_3 - 2g_2^2h_3h_2^2g_0 + h_3g_3h_1g_0^2h_4 + 2h_2g_3h_0g_2g_0h_4 + \\
&\quad 2g_1^2h_4g_0h_2h_3 + 2g_1h_4g_0h_1g_2h_3 - h_3g_3h_0g_1g_0h_4 - g_3h_2^2g_0^2h_4 + h_4^2g_2h_1g_0^2 + h_4g_3^2h_0^2g_1 - \\
&\quad h_1h_0g_3^2g_0h_4 - h_4h_0^2g_2^2g_3 + h_1^2g_3^2g_1h_2 - h_1g_1^2h_3^2g_2 + g_0^2h_4^2g_1h_2 - 2g_0h_4^2g_1g_2h_0 - h_2^3g_3g_2g_0 + \\
&\quad g_2^3h_3h_2h_0 - 2g_1^2h_4^2g_0h_1 - g_1h_4g_2^2h_1^2 + g_0h_3^2g_2^2h_1 - g_3^2h_0h_2^2g_1 + g_2^3h_0h_4h_1 + g_1^3h_4^2h_0 - \\
&\quad 2h_4g_2g_1^2h_1h_2 + g_1h_2g_3h_1g_0h_4 - 2g_1^2h_4h_0g_3h_2 + g_1h_4g_2^2h_0h_2 + g_1^2h_2^3g_3 - g_2^3h_1^2h_3 + \\
&\quad g_2^2h_0h_3h_1g_3 - g_0h_2^2g_3g_1h_3 + 2g_2^2h_1h_2g_0h_4 - g_1h_4g_2h_0g_3h_1,
\end{aligned}$$

$$\begin{aligned}
w_{84} &= -g_3^2h_0^2h_4g_2 + 2h_1g_3g_0^2h_4^2 - g_2^2h_0g_0h_4^2 + g_2h_0g_1^2h_4^2 + g_0^2h_2h_4^2g_2 + g_0h_3h_4g_3h_0g_2 + \\
&\quad g_3^2h_0h_4h_2g_0 - g_0^2h_3h_4g_3h_2 - 2g_0h_4^2g_3h_0g_1 - 2h_4g_3^2h_0h_1g_1 - g_0^3h_4^3 + 3h_2^2g_3^2g_2h_0 - \\
&\quad 3g_2^2h_3^2h_2g_0 + g_2^3h_4h_0h_2 + 3g_1^2h_2h_3^2g_2 + 3g_1^2h_2^2h_3g_3 - 3g_2^2g_3h_1^2h_3 - 3g_2g_3^2h_1^2h_2 + \\
&\quad 4g_0h_1g_3h_3g_1h_4 + 3h_1g_3g_2h_2g_0h_4 - g_2^3h_4h_1^2 + 3g_2^2h_0h_3h_2g_3 - 3g_0h_2^2g_3g_2h_3 + \\
&\quad g_2h_4g_1h_0g_3h_2 - g_2h_4g_1g_3h_1^2 - 3g_1^2h_2g_3h_1h_4 - g_0h_1^2g_3^2h_4 - 2g_1^3h_1h_4^2 - g_1^2h_0g_3h_3h_4 + \\
&\quad 2g_2^2h_4h_0g_3h_1 + 2g_2h_4g_0h_2g_1h_3 + 2g_1^3h_2h_3h_4 + 2g_1^2h_4^2g_0h_2 + 4g_2^2h_4g_0h_1h_3 - \\
&\quad 4g_2h_4g_1^2h_1h_3,
\end{aligned}$$

$$\begin{aligned}
w_{85} &= -h_3h_1g_1g_0 + h_2^2g_1g_0 + h_1h_0g_3g_1 - h_1h_0g_2^2, \\
w_{86} &= g_1g_0h_1h_4 - h_2g_1h_3g_0 - h_3g_2h_1g_0 + g_2h_2^2g_0 + g_1^2h_1h_3 - g_1^2h_2^2 + h_2g_3h_0g_1 - g_1g_3h_1^2 - \\
&\quad h_2h_0g_2^2 + g_2^2h_1^2 + h_1g_2h_0g_3,
\end{aligned}$$

$$
\begin{aligned}
w_{87} &= h_4g_1h_2g_0 + h_4g_2h_1g_0 - h_3g_2h_2g_0 - g_1^2h_1h_4 + g_1^2h_2h_3 + h_2g_3h_0g_2 - g_2g_3h_1^2, \\
w_{88} &= -h_2h_4(g_0g_2 - g_1^2).
\end{aligned}
$$

Bibliographie

[Bak-Dav 69] A. Baker, H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math., Vol. 20 (1969), pp. 129-137.

[BBBCO] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, PARI-GP, version 2.1.0, disponible par ftp://megrez.math.u-bordeaux.fr/pub/pari

[Bru 99] N. Bruin, *On Generalised Fermat Equations*, PhD Dissertation, Leiden (1999).

[Can 87] D. G. Cantor, *Computing on the jacobian of a hyperelliptic curve*, Math. Comp., Vol. 48 (1987), pp.95-101.

[Cas 86] J. W. S. Cassels, *Local Fields*, London Math. Soc. Student Text, Vol. 3, Cambridge University Press (1986).

[Cas-Fly 96] J. W. S. Cassels, E. V. Flynn, *Prolegomena to a middlebrow Arithmetic of Curves of Genus 2*, LMS Lecture Note Series, Vol. 230, Cambridge University Press (1996).

[Cha 41] C. Chabauty, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension*, C. R. A. S. Paris, Vol. 212(1941), pp. 1022-1024.

[Coh 93] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math., Vol. 138, Springer-Verlag (1993).

[Col 85] R. F. Coleman, *Effective Chabauty*, Duke Math. J., Vol. 52 (1985), pp. 765-780.

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

[Cre] J. E. Cremona, *mwrank*, disponible par ftp://euclid.ex.ac.uk/pub/cremona/progs/.

[Cre 99] J. E. Cremona, P. Serf, *Computing the rank of elliptic curves over real quadratic number fields of class number* 1 , Math. Comp., Vol. 68:227 (1999), pp. 1187-1200.

[Dav 95] S. David, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. France, Vol. 62 (1995).

[Dem 68] V. Dem'janenko, *Rational points on a class of algebraic curves*, Amer. Math. Soc. Transl., Vol. 66 (1968), pp. 246-272.

[Dja-Sch-Sma 00] Z. Djabri, E. F. Schaefer, N. P. Smart, *Computing the p-Selmer group of an elliptic curve*, Trans. Amer. Math. Soc., Vol. 352:12 (2000), pp. 5583-5597.

[Duq 01] S. Duquesne, *Integral Points on Elliptic Curves Defined by Simplest Cubic Fields*, Exp. Math., Vol. 10:1 (2001), pp. 91-102.

[Duq 02] S. Duquesne, *Rational Points on Hyperelliptic Curves and an Explicit Weierstrass Preparation Theorem*, Manuscripta Math., à paraitre.

[Fal 83] G. Faltings, *Endlichtkeitssästze für abelsche Varietäten über Zahlenkörpen*, Inv. Math., Vol. 73 (1983), pp 349-366.

[Fly 90] E. V. Flynn, *The jacobian and formal group of a curve of genus 2 over an arbitrary ground field*, Math. Proc. Cam. Phil. Soc., Vol. 107 (1990), pp. 425-441.

[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 97] E. V. Flynn, *A flexible method for applying Chabauty's Thorem*, Compositio Math., Vol. 105 (1997), pp. 79-94.

[Fly 01] E. V. Flynn, *On* $\mathbb{Q}$*-Derived Polynomials*, à paraitre dans Proc. Edinburgh Math. Soc. ???

[Fly-Poo-Sch 97] E. V. Flynn, B. Poonen, E. F. Schaefer, *Cycles of quadratic polynomials andd rational points on a genus-two curve*, Duke Math. J., Vol. 90 (1997), pp.435-463.

[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.

[Fly-Wet 99] E. V. Flynn, J. L. Wetherell, *Finding rational points on bielliptic genus* 2 *curves*, Manuscripta Math., Vol. 100 (1999), pp. 519-533.

[Fly-Wet 01] E. V. Flynn, J. L. Wetherell, *Covering Collections and a Challenge Problem of Serre*, Acta Arith., Vol. 98:2 (2001), pp. 197-205.

[Geb-Pet-Zim 94] J. Gebel, A. Pethö, H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith., Vol. 68:2 (1994), pp.171-192.

[Hus 78] D. Husemöller, *Elliptic curves*, Graduate Texts in Math., Vol. 111, Springer-Verlag (1978)

[Lan 78] S. Lang, *Elliptic curves : Diophantine analysis*, Grundlehren der math. Wissenschaften, Vol. 231, Springer-Verlag (1978).

[Lec 01] O. Lecacheux, *Rang de courbes elliptiques sur* $\mathbb{Q}$ *avec un groupe de torsion isomorphe à* $\mathbb{Z}/5\mathbb{Z}$, C. R. Acad. Sci. Paris Sér. I Math., Vol. 332:1 (2001), pp. 1-6.

[Mes 82] J. F. Mestre, *courbes elliptiques et formules explicites*, Sem. de théorie des nombres de Grenoble (1982).

[Nik-Sma 98] G. Niklasch, N. P. Smart, *Exceptional units in a family of quartic number fields*, Math. Comp., Vol. 67:222 (1998), pp. 759-772.

[Pet 91] A. Pethö, *Complete solutions to families of quartic Thue equations*, Math. Comp., Vol. 57:196 (1991), pp. 777-798

[Sch 95] E. F. Shaefer, *2-descent on the jacobians of hyperelliptic curves*, J. Number Theory, Vol. 51 (1995), pp. 219-232.

[Sha 74] D. Shanks, *The Simplest Cubic Fields*, Math. Comp., Vol. 28 (1974), pp. 1137-1152.

[Shi 90] T. Shioda, *On the Mordell-Weil lattices*, Comment. Math. Univ. St. Paul., Vol. 39:2 (1990), pp. 211-240.

[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 88] J. H. Silverman, *Computing heights on elliptic curves*, Math. Comp., Vol. 51:183 (1988), pp. 339-358.

[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.

[Sim] D. Simon, *Computing the rank of elliptic curves over number fields*, ???

[Sma 94] N. P. Smart, *S-integral points on elliptic curves*, Math. Proc. Cambridge Philos. Soc., Vol. 116:3 (1994), pp.391-399.

[Sma 98] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Math. Soc. Student Text, Vol. 41 (1998).

[Str-Tza 94] R. J. Stroeker, N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith., Vol. 67:2 (1994), pp. 177-196.

[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).

[Sug 81] T. Sugatani, *Rings of convergent power series and Weierstrass preparation theorem*, Nagoya Math. J., Vol. 81 (1981), pp. 73-78.

[Was 87] L. C. Washington, *Class Numbers of the Simplest Cubic Fields*, Math. Comp., Vol. 48:177 (1987), pp. 371-384.

[Wet 97] J. L. Wetherell, *Bounding the Number of Rational Points on Certain Curves of High Rank*, PhD dissertation, University of California at Berkeley (1997).

[Zag 87] D. Zagier, *Large integral points on elliptic curves*, Math. Comp., Vol. 48:177 (1987), pp.425-436. Addendum dans Vol. 51 (1988), p. 375.

Résumé : Cette thèse est constituée de trois parties indépendantes concernant la détermination des points rationnels et entiers sur les courbes algébriques. Nous nous sommes particulièrement intéressé aux aspects algorithmiques de ces problèmes. Dans la première partie, nous avons considéré la famille des courbes elliptiques définies par les "simplest cubic fields". Nous décrivons une méthode pour calculer exactement tous les points entiers sur ces courbes. Une étude expérimentale sur un grand nombre de courbes nous a amené à observer certains phénomènes que nous prouvons par la suite. En particulier, nous donnons explicitement tous les points entiers sur ces courbes lorsque leur rang vaut 1. La deuxième partie concerne le calcul des points rationnels sur les courbes de plus grand genre. Dans le but de calculer ces points lorsque le rang de la jacobienne est supérieur au genre de la courbe, Flynn et Wetherell utilisent le groupe formel d'une courbe elliptique de rang 1. Nous développons une version explicite du théorème de préparation de Weierstrass pour généraliser cette méthode au cas des courbes elliptiques de rang supérieur à 1, ce qui permet de traiter de nouvelles équations diophantiennes. La dernière partie de cette thèse consiste à calculer 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. Ces traces permettent de construire une fonction hauteur sur la jacobienne. Nous pouvons alors espérer d'une part en déduire une procédure effective de calcul du sous-groupe de torsion et d'autre part effectuer des descentes infinies.

Title : Effective Computation of Integral and Rational Points on Curves

Abstract : This thesis consists of three independant parts concerning certain aspects of the study of rational and integral points on curves, with an emphasis on explicit results, using a variety of techniques including computational methods. On the topic of integral points on elliptic curves, we consider the family of elliptic curves defined by simplest cubic fields. We use linear forms in elliptic logarithms to compute all integral points on these curves when the parameter is less than 1000 and using approximations of the canonical height, we find all integral points on these curves when the rank is 1. The second part deals with rational points on curves of higher genus. In order to compute these points when the rank of the jacobian is greater than the genus of the curve, Flynn and Wetherell uses power series for the formal group of elliptic curves when the rank is 1. We use an explicit version of the Weierstrass Preparation Theorem in order to explain how to generalise this technique when the rank is greater than 1. The final topic of this thesis is the Kummer variety of hyperelliptic curves of genus 3 defined by a polynomial of degree 7. We computes traces of the group law in this case. These traces allows us to construct a height function on the jacobian variety. We can then hope to find an effective procedure for finding the torsion subgroup of the jacobian and to perform an infinite descent.

Thèse de **MATHÉMATIQUES PURES**

Mots-Clés :

Algorithme, Chabauty, Courbe Elliptique, Courbe Hyperelliptique, Genre, Jacobienne, Points Entiers, Points Rationnels, Simplest Cubic Fields, Variété de Kummer.

Laboratoire A2X, Université Bordeaux I,
351, Cours de la Libération 33405 TALENCE Cedex.