Journal de Théorie des Nombres
de Bordeaux **15** (2003), 99–113

Points rationnels et méthode de Chabauty elliptique

par Sylvain DUQUESNE

Résumé. La méthode de Chabauty elliptique permet de calculer les points rationnels sur une courbe définie sur un corps de nombres lorsque le théorème de Chabauty ne s'applique pas, c'est à dire lorsque le rang de la jacobienne est supérieur au genre de la courbe. Nous exposons cette méthode et nous la généralisons dans de nouveaux cas en écrivant une version explicite du théorème de préparation de Weierstrass en 2 variables. En particulier nous calculons tous les points rationnels d'une courbe de genre 4 dont le rang de la jacobienne vaut 4.

Abstract. The elliptic curve Chabauty method allows to compute rational points on curves defined over a number field when the rank of the Jacobian is greater than the genus of the curve. We explain this method and generalize it to some new cases. In particular, we are able to compute rational points on a curve of genus 4 and rank 4.

Introduction

D'après le Théorème de Faltings [11], le nombre de points rationnels sur une courbe définie sur un corps de nombre et de genre supérieur ou égal à 2 est fini. La preuve de ce théorème n'étant pas explicite, le calcul des points rationnels est l'un des problèmes les plus importants concernant ces courbes. Il est maintenant bien connu qu'en utilisant la méthode de Chabauty ([4], [5], [12]), il est possible de borner le nombre de points rationnels lorsque le rang de la jacobienne est strictement inférieur au genre de la courbe. Dans la plupart des cas, tous les points rationnels de la courbe peuvent en être déduits. Lorsque le rang de la jacobienne est plus grand ou égal au genre de la courbe, il existe plusieurs méthodes pour calculer les points rationnels ([1], [22], [15] ...). L'une de ces méthodes (la méthode de Chabauty elliptique [14]) consiste à ramener le problème à la recherche

Manuscrit reçu le 3 décembre 2001.

de points rationnels d'une courbe elliptique définie sur un corps de nombres ayant une abscisse dans $\mathbb{Q}$. Nous allons rappeler cette méthode puis la généraliser dans de nouveaux cas. Nous calculerons en particulier les points rationnels d'une courbe de genre 4 dont le rang de la jacobienne vaut également 4.

1. La méthode de Chabauty elliptique

Considérons une courbe elliptique E définie par l'équation :

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

sur un corps de nombres $\mathbb{Q}(\alpha)$ de degré d avec $g_3 \neq 0$. Notre but est de trouver tous les

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

Il est en effet possible, comme nous le verrons dans le paragraphe 2, de ramener le calcul des points rationnels de certaines courbes à ce problème. Rappelons, tout d'abord, que le changement de variables $z = -\frac{x}{y}$ et $w = -\frac{1}{y}$ permet de définir la loi de groupe formelle sur E. Si $[z_1, w_1]$ et $[z_2, w_2]$ sont deux points de E. 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. Des précisions sont données dans [17]. Nous définissons également un logarithme et une exponentielle formels comme des séries formelles à coefficients dans $\mathbb{Q}[g_0, g_1, g_2, g_3]$ qui vérifient :

$$\begin{aligned} \operatorname{Log}\left(\mathcal{F}(z_1, z_2)\right) &= \operatorname{Log}(z_1) + \operatorname{Log}(z_2) \ . \\ \mathcal{F}\left(\operatorname{Exp}(z_1), \operatorname{Exp}(z_2)\right) &= \operatorname{Exp}(z_1 + z_2) \ . \end{aligned}$$

La coordonnée w peut s'écrire comme une série formelle en z. Cela permet d'écrire, d'une part, l'inverse de l'abscisse d'un point P de $E(\mathbb{Q}(\alpha))$ comme une série formelle ϕ de $\mathbb{Z}\left[g_0, g_1, g_2, g_3\right][[z]]$ et d'autre part l'abscisse de la somme de P avec un point $[x, y]$ comme une série formelle ψ de $\mathbb{Z}\left[g_0, g_1, g_2, g_3, x, y\right][[z]]$:

$$\phi(z) = g_3\left(z^2 + g_2z^4 + \left(g_1g_3 + g_2^2\right)z^6 + O\left(z^8\right)\right) \ . \tag{3}$$

$$\begin{aligned} \psi(z) = x + 2yz &+ (3g_3x^2 + 2g_2x + g_1)z^2 \\ &+ (4g_3xy + 2g_2y)z^3 + O(z^4) \ . \end{aligned} \tag{4}$$

Nous supposerons dans la suite que le rang de $E(\mathbb{Q}(\alpha))$ est non nul (le cas du rang nul est trivial à traiter) et qu'il est inférieur à d. Cette condition sur le rang est analogue à la condition sur le rang de la jacobienne dans le théorème de Chabauty et cette analogie vaut son nom à cette méthode dite de Chabauty elliptique. Nous supposerons aussi connue la structure du groupe de Mordell-Weil de la courbe E sur $\mathbb{Q}(\alpha)$:

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

Les principes généraux pour ces calculs sont exposés dans le livre de Silverman [17] et de nombreux chercheurs se sont penchés sur ce problème; les articles [1], [7], [8], [16] et [19] 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 [19] qui permet, après une descente infinie, de connaître effectivement cette structure.

Choisissons maintenant un nombre premier impair p. Nous noterons dans la suite par un $\tilde{}$ la réduction modulo p. Supposons 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. $|g_i|_p \leq 1$, pour $i = 0, \ldots, 3$.

La première condition est la plus difficile à réaliser. En effet, même si elle est toujours vérifiable en degré 2 ou 3, cela n'est, par exemple, plus possible pour le corps $\mathbb{Q}\left(\sqrt{a}, \sqrt{b}\right)$. Il est cependant possible de se passer de cette condition comme [15]. 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) doit être un générateur pour tous les corps et anneaux que nous avons besoin de considérer.

La réduction $\widetilde{E}$ de E modulo p est une courbe elliptique sur $\mathbb{F}_p(\widetilde{\alpha})$ puisque p a été supposé de bonne réduction. Définissons alors, pour $i \in \{1, \ldots, r\}$, m_i l'ordre de $\widetilde{P}_i$ dans $\widetilde{E}\left(\mathbb{F}_p\left(\widetilde{\alpha}\right)\right)$ et $Q_i = m_i P_i \in E\left(\mathbb{Q}(\alpha)\right)$ de telle sorte que chaque point Q_i est dans le noyau de la réduction modulo p. Nous suivons désormais la même stratégie que la méthode de Chabauty pour les courbes de genre 2 exposée dans [12]. Soit donc $\mathcal{U}$ l'ensemble fini :

$$\mathcal{U} = \left\{ T + k_1 P_1 + \cdots + k_r P_r : T \in E(\mathbb{Q}(\alpha))_{\text{tors}}, \left\lfloor -\frac{m_i}{2} \right\rfloor + 1 \leq k_i \leq \left\lfloor \frac{m_i}{2} \right\rfloor \right\}.$$

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

$$P = U + n_1 Q_1 + \cdots + n_r Q_r \ ,$$

avec $U \in \mathcal{U}$ et $n_1, \ldots, n_r \in \mathbb{Z}$. Rappelons que la condition que nous cherchons à exprimer est que l'abscisse d'un tel point P est dans $\mathbb{Q}$. Pour ce faire, nous allons calculer cette abscisse comme une série formelle en

$n_1, \dots, n_r$ à l'aide des outils de la loi de groupe formelle. En utilisant le logarithme et l'exponentielle formels, la z-coordonnée de $n_1Q_1 + \dots + n_rQ_r$ peut s'écrire comme une série formelle en $n_1, \dots, n_r$; en effet :

$$(5) \quad z(n_1Q_1 + \dots + n_rQ_r) = \mathrm{Exp}(n_1\mathrm{Log}(z_1) + \dots + n_r\mathrm{Log}(z_r)) \ .$$

La condition 6 et le fait que les points Q_i soient dans le noyau de la réduction permettent de démontrer que les coefficients de cette série formelle sont dans $\mathbb{Z}_p[\alpha]$ et tendent vers 0 quand $k_1 + \dots + k_r$ tend vers l'infini.

Si U est le point à l'infini, les équations (3) et (5) permettent de définir la série formelle $\theta_\infty \in \mathbb{Z}_p[\alpha][[n_1, \dots, n_r]]$:

$$\theta_\infty(n_1, \dots, n_r) = \frac{1}{\text{abscisse}(n_1Q_1 + \dots + n_rQ_r)} \ .$$

Si $U \in \mathcal{U}$ est un point différent du point à l'infini, les équations (4) et (5) permettent de définir la série formelle $\theta_U \in \mathbb{Z}_p[\alpha][[n_1, \dots, n_r]]$:

$$\theta_U(n_1, \dots, n_r) = \text{ abscisse}(U + n_1Q_1 + \dots + n_rQ_r) \ .$$

De plus, les coefficients de θ_U tendent vers 0 dans $\mathbb{Z}_p[\alpha]$. Notons alors $\theta_U^{(i)}$ la composante de α^i dans θ_U. La condition sur la rationalité de l'abscisse du point P se traduit par l'annulation de $d-1$ séries formelles en $(n_1, \dots, n_r)$:

$$(6) \qquad \theta_U^{(1)}(n_1, \dots, n_r) = \dots = \theta_U^{(d-1)}(n_1, \dots, n_r) = 0 \ .$$

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

Nous avons 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, le théorème de Strassman (voir par exemple [2]) permet de borner le nombre de zéros d'une telle série formelle. Dans les exemples traités 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 des astuces permettent de conclure à l'aide du théorème de Strassman [1]. Dans le cas général, Flynn et Wetherell [14] suggèrent d'utiliser un théorème de préparation de Weierstrass en plusieurs variables afin de pouvoir conclure. Nous avons développé cette idée au paragraphe 3.

Supposons désormais connue une borne du nombre de solutions $(n_1, \dots, n_r)$ au système (6). Ainsi, pour un élément U donné dans l'ensemble fini $\mathcal{U}$, il est possible de borner le nombre de r-uplets $(n_1, \dots, n_r)$ tels que le point $U + n_1Q_1 + \dots + n_rQ_r$ ait une abscisse dans $\mathbb{Q}$. Cette stratégie appliquée

à chacun des points de $\mathcal{U}$ permet 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 tels points déjà connus.
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 zéros p-adiques peut ne pas être optimale.
- Il peut exister un zéro p-adique à la série formelle qui ne corresponde pas à un point de la courbe elliptique. 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 jusque là inconnu, 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, de recommencer toute la procédure et d'espérer pouvoir conclure avec ce nouveau choix. Cependant, les points Q_i seront d'autant plus difficiles à calculer que le nombre premier p est grand. 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. Cela peut également permettre de conclure directement en revenant au problème initial et en y traduisant ces renseignements locaux.

Nous allons maintenant rapidement exposer divers moyens permettant de ramener au problème de Chabauty elliptique un problème de calcul de points rationnels sur une courbe de rang supérieur ou égal au genre.

2. Quelques techniques de revêtement des courbes de genre 2

Le principe de telles méthodes est toujours le suivant : trouver dans un premier temps une variété abélienne $\mathcal{A}$ qui s'envoie par une isogénie dans $\mathcal{J}$, la jacobienne de la courbe initiale $\mathcal{C}$. Choisir 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 $\mathcal{C}$. Le calcul des points rationnels de cette collection de courbes est plus simple que le calcul direct des points rationnels de $\mathcal{C}$.

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 [14] . Une courbe bielliptique est une courbe de genre 2 donnée par une équation du type

(7) $\quad \mathcal{C} : Y^2 = G(X^2)$ avec $G(X) = (X - e_1)(X - e_2)(X - e_3)$.

Dans les cas où le rang de la jacobienne d'une telle courbe est égal à 0 ou 1, la méthode de Chabauty classique [12] 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 :

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

comme décrit dans [22]; lorsque $\mathcal{A}$ désigne le produit des courbes elliptiques E^a et E^b et $\mathcal{J}$ désigne la jacobienne de la courbe $\mathcal{C}$, il existe des isogénies $\phi : \mathcal{A} \to \mathcal{J}$ et $\phi' : \mathcal{J} \to \mathcal{A}$ dont la composition est la multiplication par 2. L'application μ suivante :

$$\begin{aligned} \mathcal{J}(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q})) \quad &\longrightarrow \quad L_1^*/(L_1^*)^2 \times L_2^*/(L_2^*)^2 \times L_3^*/(L_3^*)^2 \\ \{[x, y], [u, v]\} \quad &\longmapsto \quad \big[(x^2 - e_1)(u^2 - e_1), (x^2 - e_2)(u^2 - e_2), \\ &\qquad\qquad (x^2 - e_3)(u^2 - e_3)\big] \end{aligned}$$

où L_i est le corps $\mathbb{Q}(e_i)$, est un homomorphisme injectif d'après la théorie standard des groupes de Selmer. Supposons désormais que, grâce à une descente, un système de représentants de $\mathcal{J}(\mathbb{Q})/\phi(\mathcal{A}(\mathbb{Q}))$ ait été 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 $\mu^{(j)}(\{[X, Y], \infty^+\}) = \mu^{(j)}(D_j)$ pour $j = 1, 2, 3$. Autrement dit, pour $j = 1, 2, 3$, $X^2 - e_j = \mu^{(j)}(D_i)$ dans $L_j^*/(L_j^*)^2$. Comme $G(X^2)$ est également un carré d'après (7), il existe des $Y_{i,j}$ appartenant à L_j tels que

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

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

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

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 [22] 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 1 (Wetherell [22]). *Soit $\mathcal{C}$ la courbe de Diophante définie sur $\mathbb{Q}$ par l'équation :*

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

alors $\mathcal{C}(\mathbb{Q}) = \left\{\infty^+, \infty^-, [0, \pm 1], \left[\frac{1}{2}, \pm\frac{9}{8}\right], \left[-\frac{1}{2}, \pm\frac{9}{8}\right]\right\}$.

2.2. Revêtement par la multiplication par 2. Cette méthode est basée sur les mêmes principes que la méthode précédente. Elle utilise les idées de Bruin [1] et des variations de Flynn et Wetherell [14], [15]. La principale différence avec la méthode précédente est l'utilisation de l'homomorphisme μ lui-même et s'applique, à priori, à une courbe quelconque.

Cette technique a été récemment appliquée par Flynn et Wetherell [15] pour résoudre l'équation de Serre : $x^4 + y^4 = 17$. Il est en effet démontré dans [3] qu'il est pour cela suffisant de trouver tous les points rationnels de la courbe hyperelliptique définie sur $\mathbb{Q}$ par l'équation :

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

Cette technique de revêtement permet de ramener ce problème à trouver les points rationnels sur une courbe elliptique définie sur $\mathbb{Q}(\sqrt{2}, \sqrt{17})$ ayant une abscisse dans $\mathbb{Q}$.

Théorème 2 (Flynn-Wetherell [15]). *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. De nouvelles méthodes peuvent être imaginée, en utilisant par exemple les revêtements définis par la multiplication par 4. Cependant elles n'auraient que peu d'intérêt sans exemple pour les illustrer.

2.3. Utilisation des résultants. Cette dernière méthode est une approche plus classique et ne nécessitant pas la connaissance des outils complexes des précédentes. Le principe est le suivant : soit $\mathcal{C}$ une courbe définie sur $\mathbb{Q}$ par une équation du type

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

où $F(x)$ est sans facteur carré, $F_1(X)$ et $F_2(X)$ sont des polynômes définis sur une extension $\mathbf{k}$ de $\mathbb{Q}$, degré$(F) \geq 6$ et degré$(F_1) = 3$ ou 4. Dans ces conditions, si $[X, Y]$ est un point de $\mathcal{C}(\mathbb{Q})$, et si le groupe des classes de $\mathbf{k}$ est trivial, il existe y_1, y_2 et α des éléments de $\mathbf{k}$ tels que $\alpha y_1^2 = F_1(X)$ et $\alpha y_2^2 = F_2(X)$. Il est évident que α peut être choisi sans facteur carré. De plus α peut être choisi divisant le résultant des polynômes $F_1(X)$ et $F_2(X)$ de telle sorte que α appartienne à un ensemble fini [1]. Quelques astuces permettent de réduire cet ensemble de valeurs possibles pour α. Nous en déduisons 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 $\mathbb{Q}$ correspondant à l'abscisse d'un point rationnel sur la courbe $\mathcal{C}$. Le problème qui consiste à trouver des points rationnels de $\mathcal{C}(\mathbb{Q})$ est ainsi ramené au calcul 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 [1] de résoudre le problème diophantien suivant :

Théorème 3 (Bruin [1])**.** *Les seuls entiers $x, y, z \in \mathbb{Z}$ tels que $(x, y, z) = 1$, $xyz \neq 0$ et satisfaisant l'équation $x^8 + y^3 = z^2$ sont*

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

On peut également utiliser cette méthode pour résoudre le problème diophantien suivant

Théorème 4. *L'ensemble des points rationnels sur la courbe hyperelliptique définie sur $\mathbb{Q}$ par l'équation*

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

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

Cette courbe est une courbe bielliptique. Elle a été introduite par Flynn et Wetherell dans [14] 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 2.1. Cette courbe était la seule pour laquelle Flynn et Wetherell n'avaient pas réussi à conclure. Nous avons donc employé la méthode des résultants pour calculer tous les points rationnels de cette courbe. En fait, on se heurte au meme problème que Flynn et Wetherell, à savoir qu'il est impossible de conclure quant au problème de Chabauty elliptique auquel on se ramène : la borne obtenue est trop grande. Cependant, comme nous l'avons expliqué à la fin de la méthode de Chabauty elliptique, cette méthode donne suffisamment de renseignements locaux pour pouvoir prouver que le défaut dans la borne obtenue par la méthode de Chabauty elliptique ne provient pas de la courbe hyperelliptique de départ et cela permet de conclure la preuve du théorème. On trouvera les détails des calculs dans [9].

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

Le théorème de Strassman permet d'appliquer la méthode de Chabauty elliptique lorsque les courbes elliptiques obtenues sont de rang 1. Nous allons maintenant étudier le cas des courbes de rang supérieur. Nous illustrerons cette méthode à l'aide de l'exemple suivant :

Théorème 5. *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. Le rang de sa jacobienne, calculé grâce au programme `magma` de Stoll [20] est 4. Le théorème de Chabauty ne s'applique donc pas dans ce cas. Nous utilisons donc la méthode des résultants afin de nous ramener à la méthode de Chabauty elliptique. Soit $\mathbf{k}$ le corps de nombres $\mathbb{Q}(\beta)$, où β est une racine du polynôme $x^3 + 2x + 1$. Le polynôme de degré 9 définissant la courbe $\mathcal{C}$ se factorise sur ce corps de nombres. Il vaut $f_1(x)f_2(x)$ avec :

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

La méthode exposée au paragraphe 2.3 permet d'en déduire que si $[X, Y]$ est un point rationnel sur la courbe $\mathcal{C}$, alors il existe $Y_1 \in \mathbf{k}$ tel que $[X, Y_1]$ soit un point rationnel, ayant une abscisse dans $\mathbb{Q}$, sur la courbe elliptique :

$$E \ : \ y^2 = f_1(x) = x^3 - 2x^2 + (-4\beta^2 - \beta + 1)x + 1 \ , \tag{8}$$

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 $\mathcal{C}$. Notre but est donc de résoudre le problème de Chabauty elliptique pour E. Le rang de cette courbe sur $\mathbf{k}$ est 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. Pour cela, nous avons besoin d'une généralisation du théorème de Strassman pour les systèmes de séries formelles en deux variables. Cette généralisation est donnée par le théorème de préparation de Weierstrass.

3.1. 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 [21]. Définissons $\mathbb{Z}_p \langle n_1, n_2 \rangle$ l'ensemble des séries formelles de $Z_p[[n_1, n_2]]$ dont les coefficients $f_{(i,j)}$ tendent vers 0 dans $\mathbb{Z}_p$ lorsque $i + j \to \infty$. Cette condition sur les coefficients permet 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 $\mathbb{Z}_p\langle n_2\rangle$ et le munir d'une norme que nous noterons $||.||_1$. Il devient alors possible de définir $\mathbb{Z}_p\langle n_2\rangle\langle n_1\rangle$ comme l'ensemble des séries formelles de $\mathbb{Z}_p\langle n_2\rangle[[n_1]]$ dont la norme des coefficients tende vers 0 dans $\mathbb{Z}_p\langle n_2\rangle$. 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 $i\to\infty$. Enfin, rappelons que f est une unité de $\mathbb{Z}_p\langle n_2\rangle$ si $|f_0|_p=1$ et $|f_j|_p<1$ pour tout $j\neq 0$ et que f est une unité de $\mathbb{Z}_p\langle n_1,n_2\rangle$ 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, $f=\sum f_i n_1^i\in\mathbb{Z}_p\langle n_2\rangle\langle n_1\rangle$ est dit 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 strictement supérieur à s sont de norme strictement inférieure à 1.

Nous pouvons alors énoncer le théorème suivant, qui est un cas particulier du théorème 3.1 de Sugatani [21] dans le cas où il y a deux variables :

Théorème 6 (Sugatani [21]). *Soit f une série formelle de $\mathbb{Z}_p\langle n_1,n_2\rangle$. Supposons que f soit général en n_1 d'ordre $s\geq 0$. 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 $\mathbb{Z}_p\langle n_2\rangle$.*
- *$f(n_1,n_2)=h(n_1,n_2)\ (g_s(n_2)n_1^s+\cdots+g_1(n_2)n_1+g_0(n_2))$.*

3.2. Une version explicite du théorème de préparation de Weierstrass. Notre but est de borner le nombre de zéros p-adiques communs de deux séries formelles en deux variables. Pour cela nous avons besoin d'une méthode qui permette de calculer effectivement les fonctions qui apparaissent dans le théorème 6. 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. Soient donc

$$\begin{aligned} f(n_1,n_2) &= \sum_{(i,j)=0}^{\infty} f_{(i,j)} n_1^i n_2^j \quad\in\mathbb{Z}_p\langle n_1,n_2\rangle\ , \\ g(n_1,n_2) &= g_0(n_2)+g_1(n_2)n_1+\cdots+g_s(n_2)n_1^s\ , \\ h(n_1,n_2) &= 1+\sum_{n=1}^{\infty} h_n(n_2)n_1^n\ , \end{aligned}$$

les séries formelles du théorème 6. Le terme en n_1^n de l'équation $f(n_1,n_2)=g(n_1,n_2)h(n_1,n_2)$ permet d'écrire pour tout $n\geq 0$:

$$h_n(n_2)g_0(n_2)+h_{n-1}(n_2)g_1(n_2)+\cdots+h_{n-s}(n_2)g_s(n_2)=f_n(n_2)\ , \tag{9}$$

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 $||h_i(n_2)||<1$ pour

tout $i \geq 1$. Ainsi, puisque $f_s(n_2)$ est inversible dans $\mathbb{Z}_p\langle n_2\rangle$, l'équation (9) prise pour $n = s$ implique que $g_s(n_2)$ est inversible dans $\mathbb{Z}_p\langle n_2\rangle$. Ces formules permettent d'énoncer la proposition suivante (prouvée dans [9]).

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

$$(10)\quad h_n = \sum_{k=0}^{\infty} \frac{(-1)^k}{g_s^{k+1}} \sum_{i_0+i_1+\cdots+i_{s-1}=k} \binom{k}{i_0, i_1, \dots, i_{s-1}} f_{ind(n,k,s,\mathbf{i})} \prod_{\ell=0}^{s-1} g_\ell^{i_\ell} \ ,$$

avec

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

D'autre part, étant donné que $h_0 = 1$ et que $h_n = 0$ pour tous les indices n négatifs, nous pouvons déduire de l'équation (9) que

$$(11)\qquad g_0 = f_0,$$

$$(12)\qquad g_i = f_i - \sum_{j=1}^{i} h_j g_{i-j} \text{ pour } 1 \leq i \leq s \ .$$

Il est alors possible de calculer les séries formelles g_i par substitution récursive à partir de ces formules en utilisant la proposition 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 connues les séries formelles g_i et h_i modulo une certaine puissance de p, par exemple p^{k_0}. Nous expliquons comment calculer ces séries modulo p^{k_0+1} si les séries formelles f_i sont connues modulo p^{k_0+1}.

- Nous calculons dans un premier temps l'inverse de g_s modulo p_0^k.
- Nous calculons ensuite les séries formelles $h_1, \dots, h_s$ 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 $i \geq s+1$; or les indices $\mathrm{ind}(n,k,s,\mathbf{i})$ intervenant dans les équations (10) sont toujours supérieurs à $s+1$. D'autre part, la somme sur k des formules (10) est finie modulo p^{k_0+1}. Il est en effet trivial que $\mathrm{ind}(n,k,s,\mathbf{i}) \geq n+s+k$. Comme les séries

formelles f_i tendent vers 0 dans $\mathbb{Z}_p\langle n_2\rangle$ lorsque i tend vers l'infini, elles sont toutes nulles modulo p^{k_0+1} pour k suffisamment grand.

Remarque : Les formules de la proposition 1 permettent de calculer h_n modulo p^{k_0+1}, mais nous n'en aurons besoin que pour $n \leq s$.

- Nous pouvons alors calculer les séries formelles g_0, $g_1, \ldots,$ g_s modulo p^{k_0+1} en utilisant les formules (12) 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 est une unité de $\mathbb{Z}_p\langle n_1, n_2\rangle$) si bien que les produits $g_j h_i$ sont calculables modulo p^{k_0+1}.

3.2.1. *Application à la méthode de Chabauty elliptique.* Nous savons donc maintenant calculer les fonctions intervenant dans le théorème 6 à la précision désirée. Les séries formelles obtenues par la méthode de Chabauty elliptique, notée $f^{(1)}$ et $f^{(2)}$ sont des éléments de $\mathbb{Z}_p\langle n_1, n_2\rangle$. Nous pouvons donc appliquer le théorème 6 à $f^{(1)}$. La série formelle $h^{(1)}$ obtenue par ce théorème 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 6 en :

$$g_0^{(1)}(n_2) + g_1^{(1)}(n_2)n_1 + \cdots + g_s^{(1)}(n_2)n_1^s \quad = \quad 0 \ . \tag{13}$$

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 $f^{(2)}$, nous obtenons un système de deux polynômes de $\mathbb{Z}_p\langle n_2\rangle[n_1]$ dont nous cherchons les zéros communs. Il est alors naturel de calculer le résultant de ces deux polynômes. Ce résultant est une série formelle de $\mathbb{Z}_p\langle n_2\rangle$. Il suffit alors d'appliquer le théorème de Strassman à cette nouvelle série formelle pour déduire une borne sur le nombre de ses zéros. Supposons désormais que les valeurs que doit prendre n_2 sont déjà connues et que leur nombre correspond à la borne obtenue (ce qui est une condition nécessaire au succès de ce type de méthode). En substituant ces valeurs dans l'une des deux équations $f^{(i)}(n_1, n_2) = 0$, nous obtenons une série formelle de $\mathbb{Z}_p\langle n_1\rangle$ à laquelle nous appliquons une nouvelle fois le théorème de Strassman. Ainsi, pour chaque valeur de n_2, nous obtenons une borne sur le nombre de valeurs que peut prendre 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 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 1.

3.3. La méthode de Chabauty elliptique pour E. Dans ce paragraphe, nous suivons la méthode de Chabauty elliptique développée dans le paragraphe 1 et dans [14]. Nous devons d'abord calculer la structure du groupe de Mordell-Weil de E définie sur $\mathbf{k} = \mathbb{Q}(\beta)$ par l'équation (8). Cette courbe est sans torsion et le programme de Simon [19] 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 $E(\mathbf{k})/2E(\mathbf{k})$. Une descente infinie [9] permet de montrer que G_1 et G_2 sont effectivement des générateurs de $E(\mathbf{k})$. Dans ce cas, 3 satisfait les six conditions du paragraphe 1. Le point $\widetilde{G_1}$, réduction de G_1 modulo 3, est d'ordre 11 sur la courbe elliptique $\widetilde{E}$. De même, l'ordre de $\widetilde{G_2}$ sur $\widetilde{E}$ est 33. Afin de réduire ces ordres, posons $G_3 = G_1 - 3G_2$. G_2 et G_3 forment une nouvelle base pour $E(\mathbf{k})$ et l'ordre de $\widetilde{G_3}$ vaut 1. Définissons :

- $m_1 = 1$ 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,
- $\mathcal{U} = \{\infty, \pm iG_2,\ 1 \le i \le 16\}$,

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

$$P = U + n_1Q_1 + n_2Q_2 \ , \tag{14}$$

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 devons chercher les valeurs de n_1 et n_2, pour qu'un tel point P ait son abscisse dans $\mathbb{Q}$. Avant tout, remarquons qu'il est possible de réduire l'ensemble $\mathcal{U}$: comme Q_1 et Q_2 sont dans le noyau de la réduction modulo 3, $\widetilde{U}$ doit avoir son abscisse dans $\mathbb{F}_3$. Les seuls éléments de $\mathcal{U}$ dont la réduction modulo 3 a son abscisse dans $\mathbb{F}_3$ sont ∞, $\pm G_2$, $\pm 3G_2$ et $\pm 14G_2$. D'autre part, comme nous avons choisi n_1 et n_2 dans $\mathbb{Z}$, il ne sera pas nécessaire de faire les calculs pour $-U$ s'ils ont déjà été fait pour U. Nous devons finalement déterminer tous les points de $E(\mathbf{k})$ ayant une abscisse dans $\mathbb{Q}$ et qui peuvent être écrits sous la forme $U + n_1Q_1 + n_2Q_2$ avec n_1, n_2 dans $\mathbb{Z}$ et $U \in \mathcal{U}' = \{\infty, G_2, 3G_2, 14G_2\}$.

Pour chaque $U \in \mathcal{U}'$, nous définissons une série formelle de $\mathbb{Z}_3[\beta]\langle n_1, n_2\rangle$ correspondant soit à l'abscisse du point $U + n_1Q_1 + n_2Q_2$ soit à l'inverse de cette abscisse si U est le point à l'infini. Dans cas, nous obtenons par exemple :

$$\begin{aligned}\theta_\infty(n_1, n_2) \;=\; & \left[27n_1^4 + 54n_2n_1^3 + 27n_1^2 + 63n_2n_1 + 27n_2^4 + 54n_2^2\right] \beta^2 + \\ & \left[54n_1^4 + 45n_1^2 + (27n_2^3 + 63n_2)n_1 + 27n_2^4 + 45n_2^2\right] \beta + \\ & 27n_1^4 + 45n_1^2 + (27n_2^3 + 36n_2)n_1 + 27n_2^4 + 36n_2^2 \pmod{3^4}\end{aligned}$$

Les composantes en β et β^2 de θ_∞ sont des séries formelles de $\mathbb{Z}_3\langle n_1, n_2\rangle$, notées $\theta_\infty^{(1)}$ et $\theta_\infty^{(2)}$, qui doivent s'annuler si le point $\infty + n_1Q_1 + n_2Q_2$ a une abscisse dans $\mathbb{Q}$, d'où le système :

$$\theta_\infty^{(1)}(n_1, n_2) = 27n_1^4 + 54n_2n_1^3 + 27n_1^2 + 63n_2n_1 + 27n_2^4 + 54n_2^2 \pmod{3^4}$$

$$\theta_\infty^{(2)}(n_1, n_2) = 54n_1^4 + 45n_1^2 + (27n_2^3 + 63n_2)n_1 + 27n_2^4 + 45n_2^2 \pmod{3^4}$$

Nous savons déjà que $(0,0)$ est un zéro commun à ces deux séries formelles. Le théorème de préparation de Weierstrass et le programme `maple` que nous avons développé nous ont permis de démontrer que c'était l'unique zéro commun dans $\mathbb{Z}_3$ (et donc dans $\mathbb{Z}$). Cela prouve 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. Pour plus de détails sur ces calculs, voir [9].
Nous démontrons de manière analogue que les seuls points de $E(\mathbb{Q}(\beta))$ de la forme $U + n_1Q_1 + n_2Q_2$ pour $U \in \mathcal{U}'$ et ayant une abscisse dans $\mathbb{Q}$ sont ceux déjà connus. Cette méthode permet donc de montrer 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, ce qui achève la preuve du théorème 5.

4. 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. 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 permet de résoudre de nouvelles équations et procure un outil supplémentaire pour la recherche des points rationnels sur les courbes de genre supérieur à 2. Le théorème de préparation de Weierstrass est également valable en n variables. La méthode que nous avons exposée est donc 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.
D'autre part, cette méthode nous ouvre de nouvelles perspectives. En effet, la méthode de Chabauty, développée par Flynn [12], pour les courbes de genre 2 et dont le rang de la jacobienne vaut 1 aboutit à la recherche des zéros p-adiques d'une série formelle en une variable. Le théorème de préparation de Weierstrass en deux variables et la méthode décrite précédemment permettent de borner le nombre de zéros p-adiques communs de deux séries formelles en deux variables. Il est fort probable que ces considérations permettent de pouvoir conclure à une éventuelle méthode de Chabauty pour les courbes de genre 3 analogue à celle employée par Flynn

pour les courbes de genre 2. Cependant, l'arithmétique des courbes de genre 3 est encore trop succincte pour envisager une telle méthode.

Bibliographie

[1] N. Bruin, *On Generalised Fermat Equations.* PhD Dissertation, Leiden, 1999.

[2] J. W. S. Cassels, *Local Fields.* London Math. Soc. Student Text, Vol. 3, Cambridge University Press, 1986.

[3] 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.

[4] C. Chabauty, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension.* C. R. Acad. Sci. Paris **212**, (1941). 1022–1024

[5] R. F. Coleman, *Effective Chabauty.* Duke Math. J. **52** (1985), 765–780.

[6] J. E. Cremona, *mwrank*, disponible sur http://www.maths.nott.ac.uk/personal/jec/ftp/progs.

[7] J. E. Cremona, P. Serf, *Computing the rank of elliptic curves over real quadratic number fields of class number* 1. Math. Comp. **68** (1999), 1187–1200.

[8] Z. Djabri, E. F. Schaefer, N. P. Smart, *Computing the p-Selmer group of an elliptic curve.* Trans. Amer. Math. Soc. **352** (2000), 5583–5597.

[9] S. Duquesne, *Calculs effectifs des points entiers et rationnels sur les courbes.* Thèse de l'université Bordeaux I, 2001, disponible sur http://www.math.u-bordeaux.fr/~duquesne.

[10] S. Duquesne, *Rational Points on Hyperelliptic Curves and an Explicit Weierstrass Preparation Theorem.* Manuscripta Math. **108** (2002), 191–204.

[11] G. Faltings, *Endlichtkeitssästze für abelsche Varietäten über Zahlenkörpen.* Invent. Math. **73** (1983), 349–366.

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

[13] E. V. Flynn, *On $\mathbb{Q}$-Derived Polynomials.* Proc. Edinb. Math. Soc. **44:1** (2001), 103–110.

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

[15] E. V. Flynn, J. L. Wetherell, *Covering Collections and a Challenge Problem of Serre.* Acta Arith. **98** (2001), 197–205.

[16] S. Siksek, *Infinite descent on elliptic curves.* Rocky Mountain J. Math. **25** (1995), 1501–1538.

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

[18] J. H. Silverman, *Computing heights on elliptic curves.* Math. Comp. **51** (1988), 339–358.

[19] D. Simon, *Computing the rank of elliptic curves over number fields.* LMS J. Comput. Math. **5** (2002), 7–17 (electronic).

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

[21] T. Sugatani, *Rings of convergent power series and Weierstrass preparation theorem.* Nagoya Math. J. **81** (1981), 73–78.

[22] J. L. Wetherell, *Bounding the Number of Rational Points on Certain Curves of High Rank.* PhD dissertation, University of California at Berkeley, 1997.

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