Conjecture de Shafarevitch effective pour les revêtements cycliques

Robin de JONG Gaël RÉMOND

7 septembre 2009

Abstract. — We give an explicit upper bound in terms of K, S, g for the Faltings height of the jacobian of a curve C of genus g, defined over a number field K and with good reduction outside a finite set of places of K under the condition that C can be written as a cyclic cover of prime order of the projective line. The proof rests on the fact that the cross ratios of the branch points of the cover are S-units, thus of bounded height, and give a plane model of C.

1 Introduction

Dans cet article, nous démontrons une version effective de la conjecture de Shafarevitch pour les courbes qui sont revêtements cycliques de degré premier de $\mathbb{P}^1$. Rappelons que Faltings a établi en toute généralité la version qualitative de cette conjecture (voir [F]) :

Théorème 1.1 *Soient K un corps de nombres, S un ensemble fini de places finies de K et g un entier. Alors l'ensemble des classes d'isomorphie de courbes projectives lisses C de genre g sur K ayant bonne réduction en dehors de S est fini.*

Une manière naturelle de quantifier cet énoncé consiste à borner la hauteur d'une telle courbe. Pour cela, plusieurs notions de hauteur peuvent être employées ; ici, pour faire un choix intrinsèque, nous utilisons la hauteur de Faltings stable de la jacobienne de notre courbe, notée $h_{\mathrm{Falt}}(C)$.

En guise de motivation, nous mentionnons encore qu'une majoration de $h_{\mathrm{Falt}}(C)$ dans le théorème 1.1 sans restriction sur C entraînerait une version effective de la conjecture de Mordell (voir [R1]). Toutefois la majoration explicite que nous donnons ci-dessous dans le cas très particulier des revêtements cycliques de degré premier ne semble pas avoir de conséquences dans cette direction (il faudrait connaître une courbe pour laquelle la construction de Kodaira-Parshin fournit une famille de courbes qui soient toutes de tels revêtements).

Pour énoncer notre résultat principal, nous devons quantifier la donnée de K et S. Si nous mesurons classiquement K par son degré $D = [K : \mathbb{Q}]$ et son discriminant absolu $\Delta = |\Delta_{K/\mathbb{Q}}|$, nous introduisons pour S les quantités

$$\Omega = \sum_{\mathfrak{p} \in S} \log N_{K/\mathbb{Q}}(\mathfrak{p}) \; + D \log 4 \qquad \text{et} \qquad \Delta_S = \Delta e^{\Omega^2}.$$

Le terme $D \log 4$ interviendra pour tenir compte des places infinies ; en revanche la définition de Δ_S est purement *ad hoc* (par exemple la quantité Δe^{Ω} serait peut-être plus naturelle).

Théorème 1.2 *Soient K, S, g et C comme dans le théorème 1.1. On suppose de plus qu'il existe un revêtement cyclique $\pi\colon C \to \mathbb{P}^1_K$ de degré premier. Alors*

$$h_{\mathrm{Falt}}(C) \leq 2^{2^{22}9^g} \Delta_S^{2^{15}g^5}.$$

Avec les propriétés de hauteur de h_{Falt}, nous obtenons la finitude de l'ensemble des courbes en question, indépendamment des résultats de Faltings. Ceci concerne en particulier les courbes elliptiques et hyperelliptiques (revêtements de degré 2) ; dans ce cas, l'énoncé qualitatif était connu de Shafarevitch lui-même et de Parshin (voir [O] et les références). Notre démarche s'inspire de cette approche telle que formulée par Oort.

La démonstration repose sur le principe suivant. On considère les points de branchement $P_1, \ldots, P_r$ de π. Ils forment une famille de points de $\mathbb{P}^1(\overline{K})$ stable sous l'action de $\mathrm{Gal}(\overline{K}/K)$. On leur associe ensuite leurs birapports, soit $6\binom{r}{4}$ éléments de $\overline{K}^\times \setminus \{1\}$ sur lesquels agissent les involutions $x \mapsto 1-x$ et $x \mapsto x^{-1}$ ainsi que le groupe $\mathrm{Gal}(\overline{K}/K)$. Pour un tel birapport b, on note $L = K(b)$ et S' l'ensemble fini des places de L formé des places divisant une place de S et de celles divisant $p = \deg \pi$. On montre alors que b est un S'-entier et que L/K n'est pas ramifiée en dehors de S'. Cet argument s'inspire directement du cas des courbes hyperelliptiques traité par Oort (voir [O]). Il se base principalement sur le fait que les points de ramifications de π (dans C) correspondent à des points de p-torsion (dans $\mathrm{Jac}(C)$) et que cette p-torsion s'étend en un schéma étale au-dessus de $\mathrm{Spec}\,\mathcal{O}_{S'}$ (voir partie 2).

Comme $K(b) = K(1-b) = K(b^{-1})$, ce qui précède fait en réalité de $(1-b, b)$ un couple de S'-unités satisfaisant l'équation $x + y = 1$. Cette équation aux S-unités a été largement étudiée et l'on sait grâce à la théorie des formes linéaires de logarithmes borner la hauteur des solutions. De manière précise, nous employons ici une majoration explicite de 2006 due à Győry et Yu (voir [GY]). Elle fait apparaître le régulateur de L que nous majorons à l'aide du discriminant $\Delta_{L/\mathbb{Q}}$ (résultat de Lenstra [Le]) puis nous contrôlons celui-ci en fonction de Δ et Ω en utilisant le fait que L/K n'est ramifiée qu'aux places de S'. Tout ceci conduit à $h(b) \leq \Delta_S^{(8g)^5}$ (voir partie 3).

Pour la dernière étape, nous travaillons uniquement sur $\overline{K}$. Nous pouvons alors opérer un automorphisme de $\mathbb{P}^1$ de sorte que 0, 1 et ∞ soient des points de branchements de π. Les $r-3$ autres se retrouvent alors être parmi les birapports que nous avons étudiés et dont nous avons borné la hauteur. Maintenant, comme le corps de fonctions de $C_{\overline{K}}$ est une extension de Kummer de $\overline{K}(X)$, nous voyons que notre courbe admet un modèle plan (singulier) d'équation affine

$$Y^p = \prod_{i=1}^{r-1} (X - b_i)^{a_i}$$

où $1 \leq a_i \leq p-1$ et les b_i sont les abscisses des points de branchement différents de ∞. Comme $h(b_i) \leq \Delta_S^{(8g)^5}$, on majore immédiatement la hauteur (naïve) de cette équation. Les résultats de [R2] permettent alors de contrôler un plongement de C dans $\mathbb{P}^3_{\overline{K}}$ puis la hauteur thêta de $\mathrm{Jac}(C)$. Finalement, une comparaison due à Bost et David (voir [P]) fait le lien avec la hauteur de Faltings (voir partie 4).

2 Bonne réduction

Nous nous plaçons sous les hypothèses du théorème 1.2. Notons $p = \deg \pi$ et $\sigma\colon C \to C$ un générateur du groupe de Galois de π. Si $Q_1, \ldots, Q_r$ sont les points de ramification de π (dans $C(\overline{K})$), nous écrivons $P_i = \pi(Q_i)$ les points de branchement correspondants. Ils sont deux à deux distincts puisque $\pi^{-1}(P_i)$ est un ensemble

de cardinal $< p$ sur lequel σ (d'ordre p) agit transitivement donc un singleton. Ceci revient à dire que l'indice de ramification de chaque Q_i vaut p et la formule d'Hurwitz donne donc

$$2g-2 = -2p + r(p-1) \iff 2g = (r-2)(p-1).$$

Nous excluons le cas où $g=0$ (puisque $\mathrm{Jac}(C)=0$ on a $h_{\mathrm{Falt}}(C)=0$ et le théorème est trivial) donc la relation précédente fournit $3 \leq r \leq 2g+2$ et $2 \leq p \leq 2g+1$.

Nous utilisons quelques faits élémentaires (et classiques) sur le birapport. Le birapport de quatre éléments distincts a, b, c, d d'un corps k s'écrit

$$\mathrm{Bir}(a,b,c,d) = \frac{c-a}{c-b} \cdot \frac{d-b}{d-a}.$$

On l'étend immédiatement aux points distincts de $\mathbb{P}^1(k) = k \cup \{\infty\}$ (par exemple $\mathrm{Bir}(\infty, b, c, d) = (d-b)/(c-b)$). On obtient toujours un élément de $k \setminus \{0,1\}$. En particulier $\mathrm{Bir}(\infty, 0, 1, x) = x$ pour tout $x \in k \setminus \{0,1\}$. On vérifie aussi facilement que le birapport est invariant par un automorphisme de $\mathbb{P}^1$. On a encore $\mathrm{Bir}(a,b,d,c) = \mathrm{Bir}(a,b,c,d)^{-1}$ et $\mathrm{Bir}(a,c,b,d) = 1 - \mathrm{Bir}(a,b,c,d)$. Enfin $\mathrm{Bir}(a,b,c,d) = \mathrm{Bir}(b,a,d,c) = \mathrm{Bir}(c,d,a,b) = \mathrm{Bir}(d,c,b,a)$, ce qui entraîne que les 24 birapports formés en permutant a, b, c, d prennent au plus 6 valeurs.

Si nous fixons une clôture algébrique et un plongement $K \subset \overline{K}$, nous pouvons voir les points P_i dans $\mathbb{P}^1(\overline{K})$ et former l'ensemble de leurs birapports :

$$\mathcal{B} = \{\mathrm{Bir}(P_i, P_j, P_k, P_\ell) \mid 1 \leq i,j,k,\ell \leq r \text{ deux à deux distincts}\}.$$

Par ce qui précède, $\mathrm{Card}\mathcal{B} \leq 6\binom{r}{4}$ et $\mathcal{B}$ est stable par les involutions $x \mapsto x^{-1}$ et $x \mapsto 1-x$. De plus, comme π est défini sur K, l'ensemble $\{P_1, \ldots, P_r\}$ est stable sous l'action de $\mathrm{Gal}(\overline{K}/K)$ et il en va donc de même de $\mathcal{B}$. En particulier tout élément de $\mathcal{B}$ est de degré au plus $6\binom{r}{4}$. Bien entendu, si $r=3$, l'ensemble $\mathcal{B}$ est vide et l'on peut passer directement à la partie 4.

Pour toute extension finie L de K on note S_L l'ensemble des places de L qui divisent une place de S ou p. L'objectif de cette partie consiste à montrer l'énoncé suivant.

Proposition 2.1 *Pour tout $b \in \mathcal{B}$, l'extension $K(b)/K$ est non ramifiée en dehors de $S_{K(b)}$ et b est un $S_{K(b)}$-entier.*

Bien entendu, pour établir ceci, nous pouvons nous contenter d'exhiber une extension K' de K non ramifiée en dehors de $S_{K'}$, contenant b comme $S_{K'}$-entier. C'est ce que nous faisons en choisissant pour K' la plus petite extension de K sur laquelle tous les points Q_i sont rationnels. Vu la définition, nous avons bien $\mathcal{B} \subset K'$. Fixons ensuite une place finie $v' \notin S_{K'}$ de K' ; notons $\mathcal{O}_{v'}$ son anneau de valuation, $v = v'|_K$ et $\mathcal{O}_v = \mathcal{O}_{v'} \cap K$. Pour conclure, il nous suffit de montrer sous ces hypothèses que $\mathcal{O}_{v'}/\mathcal{O}_v$ n'est pas ramifiée et $\mathcal{B} \subset \mathcal{O}_{v'}$. Ces deux propriétés vont résulter de l'étude de différents modèles sur $\mathcal{O}_v$ et $\mathcal{O}_{v'}$ que nous introduisons maintenant.

Tout d'abord, puisque $v \notin S$, la courbe $C \to \mathrm{Spec}\, K$ s'étend en un morphisme projectif lisse $\mathcal{C} \to \mathrm{Spec}\, \mathcal{O}_v$. De plus le lieu de ramification de π est un sous-K-schéma Y de C et nous considérons son adhérence $\mathcal{Y} \subset \mathcal{C}$ (sous-schémas fermés réduits). Nous notons ensuite $C', Y', \mathcal{C}', \mathcal{Y}'$ l'extension de ces objets à K' ou $\mathcal{O}_{v'}$. Par définition de K', le schéma $Y' \simeq \mathrm{Spec}\,(K')^r$ est l'union des points rationnels $Q_1, \ldots, Q_r$. Écrivons encore J' la jacobienne de C' et $\mathcal{J}'$ son modèle de Néron sur $\mathcal{O}_{v'}$. Nous plongeons C' dans J' à l'aide du point rationnel Q_1 (application $Q \mapsto (Q) - (Q_1)$) et ce morphisme $C' \to J'$ s'étend de manière unique en $\mathcal{C}' \to \mathcal{J}'$ par la propriété de Néron.

Nous pouvons alors énoncer le lemme-clef de cette partie (comparer avec les arguments de Oort, lemmes 2.1 et 2.2, dans le cas hyperelliptique [O]).

Lemme 2.1 *Le morphisme $\mathcal{Y}' \to \operatorname{Spec} \mathcal{O}_{v'}$ est étale.*

Démonstration : Nous avons $\pi^*(P_i) = p(Q_i)$ en termes de diviseurs sur C' donc $p(Q_i) \equiv p(Q_j)$ pour $1 \leq i, j \leq r$. Par suite $p((Q_i) - (Q_1)) = 0$ dans J' pour $1 \leq i \leq r$ et ceci signifie exactement que $Y' \to C' \to J'$ se factorise à travers le sous-schéma J'_p, noyau de la multiplication par p dans J'. Comme Y' et J'_p sont discrets et réduits, l'immersion $a\colon Y' \to J'_p$ est à la fois ouverte et fermée. Maintenant l'hypothèse $v' \notin S_{K'}$ assure que le corps résiduel de $\mathcal{O}_{v'}$ n'est pas de caractéristique p donc $\mathcal{J}'_p$ est étale sur $\mathcal{O}_{v'}$. En particulier, chaque composante connexe de $\mathcal{J}'_p$ est intègre et coïncide donc avec l'adhérence (dans $\mathcal{J}'$) d'un point de J'_p. Ainsi a s'étend en une immersion ouverte et fermée $\mathcal{Y}' \to \mathcal{J}'_p$ (si $\mathcal{Z}'$ est une composante connexe de $\mathcal{J}'_p$, les seuls sous-schémas fermés de $\mathcal{Z}'$ qui induisent un sous-schéma ouvert sur la fibre générique sont $\emptyset$ et $\mathcal{Z}'$). Une immersion ouverte étant étale, il en va de même de $\mathcal{Y}'$. □

Nous pouvons d'ores et déjà déduire de ce lemme la propriété de non-ramification. En effet, il entraîne que $\mathcal{Y}$ est étale sur $\operatorname{Spec} \mathcal{O}_v$ et ceci signifie exactement que, dans chacun des corps résiduels des points de Y, la place v ne se ramifie pas. Or, par définition, K' est le compositum de ces corps donc $\mathcal{O}_{v'}/\mathcal{O}_v$ est effectivement non ramifiée.

Considérons maintenant l'automorphisme $\sigma\colon C \to C$ fixé plus haut. Nous notons par la même lettre son extension en un automorphisme de C', puis de J', de $\mathcal{J}'$ (par propriété de Néron) et enfin de $\mathcal{C}'$ (par restriction à l'adhérence de C' dans $\mathcal{J}'$). Bien entendu, à chaque étape, σ vérifie $\sigma^p = \mathrm{id}$. Notons G le groupe d'automorphismes de $\mathcal{C}'$ engendré par σ.

Lemme 2.2 *Le quotient $\mathcal{C}'/G$ existe et est isomorphe à $\mathbb{P}^1_{\mathcal{O}_{v'}}$.*

Démonstration : Pour l'existence, d'après le théorème 4.12 de [LK], il suffit de vérifier que G agit fidèlement sur la fibre spéciale de $\mathcal{C}'$. Si ce n'était pas le cas, σ induirait l'identité sur cette fibre spéciale $\mathcal{C}'_s$ donc également sur celle de $\mathcal{J}'$ notée $\mathcal{J}'_s$. Ceci est absurde car pour un schéma abélien l'application de restriction $\mathrm{End}(\mathcal{J}') \to \mathrm{End}(\mathcal{J}'_s)$ est toujours injective (voir [La] page 45). Notons donc $\mathcal{P} = \mathcal{C}'/G$ ce quotient et $\mathcal{P}_s$ sa fibre spéciale qui est une courbe lisse de genre g'. Le revêtement $\mathcal{C}'_s \to \mathcal{P}_s$ de groupe G a au moins r points de ramification : ceux de la fibre spéciale du schéma $\mathcal{Y}'$. Par suite la formule d'Hurwitz (il n'y a pas de ramification sauvage) donne

$$2g - 2 = p(2g' - 2) + r'(p - 1) \iff 2pg' + (r' - r)(p - 1) = 0$$

où $r' \geq r$ est le nombre de points de ramification. On conclut $r' = r$ et $g' = 0$. Ainsi $\mathcal{P}$ est une famille de courbes de genre 0 et elle admet une section : il suffit de considérer un point de branchement (en d'autres termes la composée d'une section de $\mathcal{Y}'$ avec $\mathcal{Y}' \to \mathcal{C}' \to \mathcal{P}$). La proposition 3.3 de [LK] assure alors que $\mathcal{P} \simeq \mathbb{P}(\mathcal{E})$ pour un faisceau localement libre $\mathcal{E}$ de rang 2 sur $\operatorname{Spec} \mathcal{O}_{v'}$. Par principalité de $\mathcal{O}_{v'}$, ce faisceau $\mathcal{E}$ est libre donc $\mathcal{P} \simeq \mathbb{P}^1_{\mathcal{O}_{v'}}$. □

Nous déduisons facilement $\mathcal{B} \subset \mathcal{O}_{v'}$ de cet énoncé. Il fournit en effet un morphisme $\mathcal{C}' \to \mathbb{P}^1_{\mathcal{O}_{v'}}$ dont la fibre générique coïncide avec l'extension de π à K' modulo un automorphisme de $\mathbb{P}^1_{K'}$. Comme un tel automorphisme ne modifie pas l'ensemble $\mathcal{B}$, nous pouvons considérer que $P_1, \ldots, P_r$ sont les points de branchement de ce morphisme. Quitte à faire un automorphisme de $\mathbb{P}^1_{\mathcal{O}_{v'}}$ nous supposons même $P_1 = \infty$. Comme les points de branchement sont toujours distincts dans la fibre spéciale (cela vient encore de ce que $\mathcal{Y}'$ est étale et fixé par σ), nous en déduisons que $P_i = (e_i : 1)$ où $e_i \in \mathcal{O}_{v'}$, $i \geq 2$ (car $P_1 = \infty = (1 : 0)$) puis $e_i - e_j \in \mathcal{O}_{v'}^\times$ si $2 \leq i < j$. Alors chaque élément de $\mathcal{B}$ s'écrit

$$\frac{e_i - e_k}{e_i - e_j} \qquad \text{ou} \qquad \frac{e_i - e_k}{e_i - e_j} \cdot \frac{e_\ell - e_j}{e_\ell - e_k}$$

(selon que P_1 apparaît ou non) avec $i \neq j$ et $k \neq \ell$. Ceci entraîne clairement $\mathcal{B} \subset \mathcal{O}_{v'}$ et termine donc la démonstration de la proposition 2.1.

3 S-unités, régulateurs et discriminants

L'objectif de cette partie est d'établir la majoration suivante de la hauteur des éléments de $\mathcal{B}$.

Proposition 3.1 *Pour tout $b \in \mathcal{B}$, on a $h(b) \leq \Delta_S^{(8g)^5}$.*

Nous fixons donc un élément b de $\mathcal{B}$ et notons $L = K(b)$ ainsi que $S' = S_L$. Nous désignons par d, R et h le degré de L (sur $\mathbb{Q}$), son régulateur et son nombre de classes. En vue d'appliquer le résultat de Győry et Yu (voir [GY]) nous écrivons encore s pour le cardinal de $S' \cup \{$ places infinies $\}$, $R_{S'}$ pour le S'-régulateur de L et P pour le maximum des $N_{L/\mathbb{Q}}(\mathfrak{p})$, $\mathfrak{p} \in S'$. Nous abrégeons aussi $\log^\star x = \max(1, \log x)$ pour $x > 0$.

Lemme 3.1 *La hauteur de b est au plus*

$$2^{15}(16sd)^{2s+4} P R_{S'} (1 + \log^\star R_{S'} / \log^\star P).$$

Démonstration : Nous appliquons la proposition 2.1 aux quatre éléments b, b^{-1}, $1-b$ et $(1-b)^{-1}$ de $\mathcal{B}$. Ce sont donc des S'-entiers et donc des S'-unités. Le couple $(b, 1-b)$ appartient à $\{(x,y) \in (\mathcal{O}_{S'}^\times)^2 \mid x+y=1\}$ donc nous pouvons lui appliquer le théorème principal de [GY] avec $\alpha = \beta = 1$ et $H = 4$. Nous obtenons alors la borne de l'énoncé en majorant $\log(2s) \leq \sqrt{2s}$ et $\log^\star(2d) \leq \sqrt{2d}$ puis $7s + 29 \leq 8s + 27$ dans l'exposant de 2. □

Nous estimons maintenant les quantités apparaissant dans cette formule. Notons E un majorant de $[L : K]$. Nous choisissons $E \geq 2$ pour simplifier les calculs (*in fine* nous majorerons E par $6\binom{r}{4}$). On pose $u = E\Omega / \log 2$.

Nous avons facilement $d \leq ED \leq u$ et

$$s \leq 2ED + \sum_{\mathfrak{p} \in S} E \leq 2ED + \sum_{\mathfrak{p} \in S} E \frac{\log N_{K/\mathbb{Q}}(\mathfrak{p})}{\log 2} = u$$

car il y a au plus ED places au-dessus de p, ED au-dessus de ∞ et E au-dessus de chaque place de S. De manière analogue, $P \leq \max(p^{ED}, 2^u)$. Pour le S'-régulateur, nous avons

$$R_{S'} \leq hR \prod_{\mathfrak{p}' \in S'} \log N_{L/\mathbb{Q}}(\mathfrak{p}') \leq hR (\log P)^s$$

où la première inégalité vient du lemme 3 de [BG]. Pour majorer hR, nous employons une estimation de Lenstra (voir théorème 6.5 de [Le]). Elle entraîne

$$hR \leq |\Delta_{L/\mathbb{Q}}|^{1/2} (\log^\star |\Delta_{L/\mathbb{Q}}|)^{ED-1}.$$

La forme faible $hR \leq |\Delta_{L/\mathbb{Q}}|^{ED/2}$ permet de majorer

$$1 + \frac{\log^\star R_{S'}}{\log^\star P} \leq 1 + \log^\star(|\Delta_{L/\mathbb{Q}}|^{ED/2}) + s \frac{\log^\star \log^\star P}{\log^\star P} \leq 2u \log^\star |\Delta_{L/\mathbb{Q}}|.$$

En rassemblant les différents termes, il vient

$$h(b) \leq 2^{16} u (4u)^{4u+8} P (\log P)^u |\Delta_{L/\mathbb{Q}}|^{1/2} (\log^\star |\Delta_{L/\mathbb{Q}}|)^{ED}.$$

Nous faisons alors intervenir $P \leq p^u$, $\log P \leq pu$ et si $x \geq 1$

$$(\log^\star x)^{ED} \leq (ED)^{ED} x^{1/2}$$

(écrire $\log y \leq \sqrt{y}$ pour $y = x^{1/ED}$). Nous aboutissons à

$$h(b) \leq 2^{16} u (4u)^{4u+8} p^{2u} u^{2u} |\Delta_{L/\mathbb{Q}}|$$

puis, en tirant parti de $u \geq 4$, à

$$h(b) \leq (4u)^{9u} p^{2u} |\Delta_{L/\mathbb{Q}}|.$$

Pour majorer le discriminant de L, nous devons faire intervenir le fait que L/K est non ramifiée en dehors de S' (proposition 2.1). Notons pour cela $\mathcal{Q}$ l'ensemble des caractéristiques résiduelles des places de S'. Un résultat de Serre (proposition $4'$ page 129 de [S]) s'écrit avec les présentes notations :

$$\log |\Delta_{L/\mathbb{Q}}| \leq E \log \Delta + D(E-1) \sum_{\ell \in \mathcal{Q}} \log \ell + (\mathrm{Card}\mathcal{Q}) ED \log E.$$

Ici $\mathrm{Card}\mathcal{Q} \leq \sum_{\ell \in \mathcal{Q}} \log \ell + 1 \leq \Omega + \log p$ et donc

$$\log |\Delta_{L/\mathbb{Q}}| \leq E \log \Delta + 2ED(\Omega + \log p) \log E.$$

Nous majorons ensuite (quelque peu brutalement) D par Ω dans cette formule, u par $3E\Omega/2$ et $\Omega \log \Omega$ par Ω^2 pour obtenir

$$\begin{aligned} \log h(b) &\leq 14E\Omega \log 6E + 14E\Omega^2 + 3E\Omega \log p \\ &\quad + E \log \Delta + 2E\Omega^2 \log E + 2E\Omega (\log p)(\log E) \\ &\leq 63E\Omega^2 (\log^\star p)(\log^\star E) + E \log \Delta \\ &\leq 2^6 E (\log \Delta_S)(\log^\star p)(\log^\star E). \end{aligned}$$

Pour terminer la preuve de la proposition 3.1, nous vérifions (élémentairement)

$$2^6 E (\log^\star p)(\log^\star E) \leq (8g)^5$$

à l'aide de $E \leq 6\binom{r}{4}$, $r \leq 2g+2$ et $p \leq 2g+1$.

4 Hauteur de la courbe

Dans cette dernière partie, nous oublions entièrement le corps K pour ne travailler que sur $\overline{K}$. Aussi utilisons-nous les notations $\pi : C \to \mathbb{P}^1$ pour désigner l'extension des objets précédents. Quitte à composer π avec un automorphisme de $\mathbb{P}^1$, nous supposons que 0, 1 et ∞ font partie des $r \geq 3$ points de branchement. Par suite, les $r-3$ autres appartiennent à l'ensemble $\mathcal{B}$. Nous notons aussi $H \geq 1$ la borne que nous avons obtenue pour la hauteur des éléments de $\mathcal{B}$ (voir proposition 3.1).

Le corps des fonctions de C est une extension galoisienne de $\overline{K}(X)$ (corps des fonctions de $\mathbb{P}^1$) de groupe $\mathbb{Z}/p\mathbb{Z}$. Comme $\overline{K}(X)$ contient les racines p-ièmes de l'unité, il s'agit d'une extension de Kummer et donc il existe une fraction rationnelle non nulle $F \in \overline{K}(X)$ telle que le corps des fonctions de C soit isomorphe à

$$\overline{K}(X)[Y]/(Y^p - F(X)).$$

Bien entendu, nous pouvons modifier dans cette assertion F par une puissance p-ième ce qui permet de supposer que F est un polynôme unitaire dont toutes les racines sont de multiplicité au plus $p-1$. Écrivons

$$F(X) = \prod_{i=1}^{t} (X - b_i)^{a_i}$$

où $b_i \in \overline{K}$ et $1 \leq a_i \leq p-1$. Notre courbe C est l'unique courbe projective lisse birationnelle à la courbe affine C_0 d'équation $Y^p = F(X)$ et π se factorise à travers $C_0 \to \mathbb{A}^1$, $(X,Y) \mapsto X$. Ceci entraîne immédiatement que les points de branchement de π sont contenus dans $\{b_1, \ldots, b_t, \infty\}$. Réciproquement chaque b_i correspond à un point de branchement car il est l'image d'un unique point de la normalisée de C_0 (localement pour la topologie étale C_0 est isomorphe à la courbe $Y^p = X^{a_i}$ dont la normalisée est $\mathbb{A}^1$). Par conséquent $b_i \in \mathcal{B} \cup \{0,1\}$ et donc $h(b_i) \leq H$. Ceci montre aussi $t = r-1$.

Notons à présent G le polynôme $Y^p - F(X)$ de $\overline{K}[X,Y]$. Nous estimons son degré

$$\deg G \leq \max(p, (r-1)(p-1)) \leq 2(r-2)(p-1) = 4g$$

et sa hauteur naïve (celle du point projectif formé par ses coefficients, voir [R2])

$$h_\infty(G) = h_\infty(F) \leq (\deg F)\log 2 + \sum_{i=1}^{r-1} a_i h(b_i) \leq 7gH.$$

Par conséquent, le théorème 1.6 de [R2] affirme qu'il existe un plongement de C dans $\mathbb{P}^3_{\overline{K}}$ de degré au plus $8g(2g-1)$ et de hauteur (au sens de la hauteur projective d'un fermé de $\mathbb{P}^3$)

$$h(C) \leq (4g)^{(4g)^3-5}(42gH + 9(4g)^2) \leq (4g)^{(4g)^3}H - 1.$$

Nous pouvons ensuite passer à la hauteur thêta de la jacobienne de C grâce au théorème 1.3 de [R2]. L'entier m y apparaissant est majoré par $4g-2+16g(2g-1) \leq 32g^2$ de sorte que, en écrivant $h_\theta = h_\theta^{(4)}(\mathrm{Jac}(C), \Theta_{\mathrm{sym}})$ la hauteur thêta associée au plongement thêta donné par le diviseur $16\Theta_{\mathrm{sym}}$ (voir encore [R2]), nous avons

$$h_\theta \leq (32g^2)^{640g^2 8^g + 32g^3} H \leq 2^{3360 \cdot g^3 8^g} H$$

(en utilisant $32g^2 \leq 2^{5g}$). Le résultat de [P] compare h_θ (correspondant à $r=4$ dans cet article) et la hauteur de Faltings stable :

$$h_{\mathrm{Falt}}(C) \leq 2h_\theta + 2C_1 \log(2 + \max(1, h_\theta))$$

pour une constante explicite C_1 dont on vérifie facilement qu'elle satisfait $2^{4g-1} \leq C_1 \leq 2^{5g}$. En particulier, si $h_\theta \leq \mathcal{H}$ et $\mathcal{H} \geq 4C_1^2 + 2$ alors $h_{\mathrm{Falt}}(C) \leq 3\mathcal{H}$. Ceci est très largement vérifié pour $\mathcal{H} = 2^{3360 \cdot g^3 8^g} H$. On en déduit $h_{\mathrm{Falt}}(C) \leq 2^{3362 \cdot g^3 8^g} H$. Une élémentaire étude de fonction donne $g^3 8^g \leq 823 \cdot 9^g$ et, comme $3362 \cdot 823 \leq 2^{22}$, cela termine la démonstration du théorème 1.2.

Références

[BG] Y. Bugeaud et K. Győry. Bounds for the solutions of unit equations. *Acta Arith.* 74. 1996. p. 67–80.

[F] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* 73. 1983. p. 349–366.

[GY] K. Győry et K. Yu. Bounds for the solutions of S-unit equations and decomposable form equations. *Acta Arith.* 123. 2006. p. 9–41.

[LK] K. Lønsted et S. Kleiman. Basics on families of hyperelliptic curves. *Compositio Math.* 38. 1979. p. 83–111.

[La] S. Lang. *Complex multiplication.* Grundlehren der Mathematischen Wissenschaften 255. Springer-Verlag. New York. 1983.

[Le] H. Lenstra. Algorithms in algebraic number theory. *Bull. A. M. S.* 26. 1992. p. 211–244.

[O] F. Oort. Hyperelliptic curves over number fields. *Classification of algebraic varieties and compact complex manifolds.* Lect. Notes Math. 412. Springer. Berlin. 1974. p. 211–218.

[P] F. Pazuki. Theta height and Faltings height. arXiv :0907.1458. 24 pages.

[R1] G. Rémond. Hauteurs thêta et construction de Kodaira. *J. Number Th.*. 78. 1999. p. 287–311.

[R2] G. Rémond. Nombre de points rationnels des courbes. 36 pages, soumis.

[S] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Publ. Math. I. H. É. S.* 54. 1981. p. 323–401.

Robin de Jong
Mathematisch Instituut
Universiteit Leiden
PO Box 9512
2300 RA Leiden
Pays-Bas
rdejong@math.leidenuniv.nl

Gaël Rémond
Institut Fourier, UMR 5582
Université Grenoble I
BP 74
38402 Saint-Martin-d'Hères Cedex
France
Gael.Remond@ujf-grenoble.fr