.

NON-TRIVIALITÉ DES POINTS DE HEEGNER
NON-TRIVIALITY OF HEEGNER POINTS
THÉORIE DES NOMBRES/ *NUMBER THEORY*

CHRISTOPHE CORNUT

RÉSUMÉ. Nous donnons ici une nouvelle preuve d'une conjecture de B. Mazur sur la non-trivialité des points de Heegner, en substituant au théorème de M. Ratner qui constituait l'ingrédient principal de notre première preuve [1] un cas démontré de la conjecture d'André-Oort. Conceptuellement plus simple, cette nouvelle approche ne permet toutefois pas de retrouver les renseignements plus fins précédemment obtenus.

We give here a second proof of Mazur's conjecture on higher Heegner points, using a proven case of the André-Oort conjecture as a substitute for the main ingredient of our first proof [1], a theorem of M. Ratner.

1. Soit $\mathbb{E}_{/\mathbb{Q}}$ une courbe elliptique de conducteur N, $\pi : X_0(N) \to \mathbb{E}$ une paramétrisation modulaire, K un corps quadratique imaginaire dans lequel tous les facteurs premiers de N sont décomposés. Soit $\mathcal{N}$ un idéal de O_K tel que $O_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$. Pour tout entier positif c, on note $O_c = \mathbb{Z} + cO_K$ l'ordre de conducteur c de K. Lorsque c est premier à N, $\mathcal{N}_c = \mathcal{N} \cap O_c$ est un idéal inversible de O_c et l'isogénie $\mathbb{C}/O_c \to \mathbb{C}/\mathcal{N}_c^{-1}$ est cyclique de degré N. Le point correspondant de $X_0(N)$ est un *point de Heegner,* dont la théorie de la multiplication complexe montre qu'il est défini sur $K[c]$, *le corps d'ordre* de conducteur c de K.

2. Soit $p \nmid N$ un nombre premier et, pour $n \geq 0$, $x_n = [\mathbb{C}/O_{p^n} \to \mathbb{C}/\mathcal{N}_{p^n}^{-1}] \in X_0(N)(K[p^n])$. Le corps $K[p^\infty] = \cup_{n\geq 0} K[p^n]$ est une extension *finie* de la $\mathbb{Z}_p$-extension anticyclotomique H_∞ de K. Posant $G_0 = \mathrm{Gal}(K[p^\infty]/H_\infty)$, le résultat dont nous allons donner une nouvelle preuve stipule que :

Théorème. *Pour presque tout* $n \geq 0$, $\mathrm{tr}_{G_0}(\pi(x_n))$ *est d'ordre infini dans* $\mathbb{E}(H_\infty)$.

Comme $\mathbb{E}(H_\infty)_{\mathrm{tors}}$ est *fini* (cf. [1, Lemma 4.1]), il suffit de montrer que l'application suivante a des *fibres finies* :

$$(1) \qquad \begin{array}{ccccccc} \mathbb{N} & \to & X_0(N)^{G_0} & \xrightarrow{\pi} & \mathbb{E}^{G_0} & \xrightarrow{\sum} & \mathbb{E} \\ n & \mapsto & (\sigma \cdot x_n)_{\sigma \in G_0} & \longmapsto & (\sigma \cdot \pi(x_n))_{\sigma \in G_0} & \longmapsto & \mathrm{tr}_{G_0}(\pi(x_n)) \end{array}$$

Je remercie Franz Oort, qui le premier m'a indiqué la pertinence de sa conjecture dans le cadre de celle de B. Mazur.

3. Soient $q_1, \ldots, q_g$ les nombres premiers ramifiés dans K qui sont distinct de p et $Q_1, \ldots, Q_g$ les idéaux premiers correspondants de O_K. Les Frobénius des Q_i dans $\mathrm{Gal}(K[p^\infty]/K)$, qui sont d'ordre 2, engendrent un sous-groupe G_1 de $G_0 = \mathrm{Gal}(K[p^\infty]/K)_{\mathrm{tors}}$ dont ils forment une $\mathbb{F}_2$-base. Soient $N' = Nq_1 \cdots q_g$, $\mathcal{N}' = \mathcal{N}\mathcal{Q}_1 \cdots \mathcal{Q}_g$ et pour $n \geq 0$, $x'_n = [\mathbb{C}/O_{p^n} \to \mathbb{C}/\mathcal{N}'^{-1}_{p^n}] \in X_0(N')(K[p^n])$. Les 2^g conjugués de x_n sous l'action de G_1 sont précisément les images de $x_{n'}$ par les 2^g applications de dégénerescence $X_0(N') \to X_0(N)$. Notant $D : X_0(N') \to X_0(N)^{G_1}$ le produit de ces applications, on définit une nouvelle paramétrisation π' de $\mathbb{E}$ par le diagramme commutatif suivant :

$$\begin{array}{ccc} X_0(N)^{G_1} & \xrightarrow{\pi} & \mathbb{E}^{G_1} \\ D \uparrow & & \downarrow \sum \\ X_0(N') & \xrightarrow{\pi'} & \mathbb{E} \end{array}$$

Par construction, $\pi'(x'_n) = \mathrm{tr}_{G_1}(\pi(x_n))$ de sorte que si $\mathcal{R} \subset G_0$ est un système de représentant de G_0/G_1, l'application (1) se réécrit :

$$\begin{array}{ccccccc} \mathbb{N} & \xrightarrow{\Delta} & X_0(N')^{\mathcal{R}} & \xrightarrow{\pi'} & \mathbb{E}^{\mathcal{R}} & \xrightarrow{\sum} & \mathbb{E} \\ n & \longmapsto & \Delta(n) = (\sigma \cdot x'_n)_\sigma & \longmapsto & (\sigma \cdot \pi'(x'_n))_\sigma & \longmapsto & \mathrm{tr}_{G_0}(\pi(x_n)) \end{array} \tag{2}$$

4. La stratégie adoptée dans [1] consistait à étudier la réduction de cette application en des places judicieusement choisies de $K[p^\infty]$. Ici, nous allons démontrer que *si $\mathbb{I}$ est une partie infinie de $\mathbb{N}$, $\Delta(\mathbb{I}) \subset X_0(N')^{\mathcal{R}}(\mathbb{C})$ est dense pour la topologie de Zariski.* Comme les deux dernières flèches de (2) sont dominantes, cela implique bien que les fibres de (1) sont finies, d'où le théorème.

5. Soit donc Z une composante irréductible de l'adhérence de $\Delta(\mathbb{I})$, dont on peut supposer qu'elle contient une infinité des points de $\Delta(\mathbb{I})$. La conjecture d'André-Oort, démontrée dans le cas qui nous intéresse (cf. [4], [2] ou [3])[1], fournit sur Z les informations suivantes : *il existe une partition $\mathcal{R} = \mathcal{R}_1 \amalg \cdots \amalg \mathcal{R}_h$, des sous-variétés $Z_1 \subset X_0(N')^{\mathcal{R}_1}, \ldots, Z_h \subset X_0(N')^{\mathcal{R}_h}$ et des éléments $\beta_\sigma \in GL^+(2, \mathbb{Q})$ pour $\sigma \in \mathcal{R}$ tels que $Z = Z_1 \times \cdots \times Z_h$ et Z_i est l'image de*

$$\begin{array}{ccc} \mathcal{H}^* & \to & (\Gamma_0(N') \setminus \mathcal{H}^*)^{\mathcal{R}_i} \simeq X_0(N')^{\mathcal{R}_i}(\mathbb{C}) \\ \tau & \mapsto & ([\beta_\sigma \cdot \tau])_{\sigma \in \mathcal{R}_i} \end{array}$$

où $\mathcal{H}^* = \{z \in \mathbb{C} \mid \mathrm{im}(z) > 0\} \cup \mathbb{P}^1(\mathbb{Q})$. On veut montrer que $Z = X_0(N')^{\mathcal{R}}$, c'est-à-dire que la partition ci-dessus est triviale ($h = |\mathcal{R}|$).

6. En définitive, on est ramené à établir la propriété suivante : *si deux éléments σ_1 et σ_2 de G_0 sont tels qu'il existe $\beta \in GL^+(2, \mathbb{Q})$ pour lequel il existe une infinité de $n \geq 0$ vérifiant*

$$(\sigma_1 \cdot x'_n, \sigma_2 \cdot x'_n) \in \{([\tau], [\beta \cdot \tau]) \mid \tau \in \mathcal{H}^*\},$$

alors $\sigma_1 \equiv \sigma_2 \mod G_1$ (avec les notations de **5**, $\beta = \beta_{\sigma_1}^{-1}\beta_{\sigma_2}$).

---

[1] La proposition 3.7 et le théorème 4.5 de [4] (ainsi que le théorème 1.2 et la remarque 7.3.2 de [3]) montrent que Z est *une sous-variété de type Hodge* de $X_0(N')^{\mathcal{R}}$. Le résultat ici mentionné résulte alors de la description explicite de ces sous-variétés dans [2].

Or, quitte à multiplier β par un élément de $\mathbb{Q}^*$, on peut supposer que

$$\beta = \begin{pmatrix} x & y \\ z & t \end{pmatrix} \in M_2(\mathbb{Z}) \text{ avec } \mathrm{pgcd}(x, y, z, t) = 1.$$

Si $d = \det \beta$, les courbes elliptiques d'invariants $j(\tau)$ et $j(\beta\tau)$ sont alors liées par une isogénie cyclique de degré d. Notant E_n une courbe elliptique définie sur $K[p^\infty]$ qui, munie d'une structure de niveau ad-hoc, définit le point x'_n, notre hypothèse implique donc que *pour une infinité de $n \geq 0$, il existe une isogénie cyclique de degré d entre $E_n^{\sigma_1}$ et $E_n^{\sigma_2}$.*

7. D'après l'appendice, dont on reprend les notations, une telle isogénie se décompose selon le schéma $(p^n \to p^{n-a_n} \xrightarrow{\mathcal{M}(n)} p^{n-a_n} \to p^n)$ où $\mathcal{M}(n)$ est un idéal de O_K tel que $O_K/\mathcal{M}(n)$ soit cyclique d'ordre d/p^{2a_n}, premier à p^{n-a_n}. En particulier, $a_n = a = v_p(d)/2$ pour $n \gg 0$ et les idéaux $\mathcal{M}(n)$ décrivant un ensemble fini lorsque n varie, on peut supposer que $\mathcal{M}(n) = \mathcal{M}$ est constant. Pour une infinité de n, on obtient donc un diagramme

$$\begin{array}{ccc} E_n^{\sigma_1} & \xrightarrow{d} & E_n^{\sigma_2} \\ p^a \downarrow & & \downarrow p^a \\ E_n^{(1)} & \xrightarrow{d'} & E_n^{(2)} \end{array} \quad \text{avec} \quad \left\{ \begin{array}{lll} E_n^{(1)} & \simeq & (E_n^{\sigma_1})^{O_{p^{n-a}}} \simeq (E_n^{O_{p^{n-a}}})^{\sigma_1} \\ E_n^{(2)} & \simeq & (E_n^{\sigma_2})^{O_{p^{n-a}}} \simeq (E_n^{O_{p^{n-a}}})^{\sigma_2} \\ & \simeq & (E_n^{(1)})^{\mathcal{M}_{p^n}} \end{array} \right.$$

où $d' = d/p^{2a}$ et $\mathcal{M}_{p^n} = \mathcal{M} \cap O_{p^n}$. Si σ est l'élément de $\mathrm{Gal}(K[p^\infty]/K)$ associé à $\mathcal{M}$ par la théorie du corps de classe, la théorie de la multiplication complexe montre alors que $\sigma\sigma_1 = \sigma_2$ sur $K[p^{n-a}]$. Ceci étant valable pour une infinité de n, $\sigma = \sigma_2\sigma_1^{-1}$ dans $\mathrm{Gal}(K[p^\infty]/K)$.

8. En particulier, σ est d'ordre fini, disons r. Cela signifie que l'idéal $\mathcal{M}^r$ de O_K est principal, *engendré par un élément de* $\bigcap_{n \geq 0} O_{p^n} = \mathbb{Z}$. Pour tout idéal premier Q de O_K divisant $\mathcal{M}$, l'idéal conjugué $\overline{Q}$ divise donc également $\mathcal{M}$. Comme $O_K/\mathcal{M}$ est cyclique, on en déduit facilement que $\mathcal{M}$ est produit d'idéaux premiers ramifiés dans $K/\mathbb{Q}$, donc que $\sigma = \sigma_2\sigma_1^{-1} \in G_1$, ce qu'il fallait démontrer.

Appendice

Nous allons ici décrire une *factorisation canonique* des isogénies cycliques entre courbes elliptiques à multiplication complexe par K.

9. Au vu de la théorie analytique des courbes elliptiques, cela revient à étudier les réseaux de K compris entre deux réseaux $a \subset b$ tel que le groupe b/a soit cyclique, disons d'ordre d. On notera cela : $a \subset_d b$.

Soit c_1 et c_2 les conducteurs des ordres de a et b, c'_1 et c'_2 les plus petits entiers $c \geq 1$ (pour l'ordre naturel ou la divisibilité, cela revient au même) tels que $O_c a \subset b$ (resp. $O_c b \subset d^{-1}a$). Comme $O_{c_1} a = a \subset b$ et $O_{c_2} a \subset O_{c_2} b = b$, c'_1 divise c_1 et c_2. De même c'_2 divise c_1 et c_2. Posons $c_1 = d_1 c'_1$ et $c_2 = d_2 c'_2$, de sorte que

$$a \subset_{d_1} O_{c'_1} a \subset_{d/d_1} b \quad \text{et} \quad b \subset_{d_2} O_{c'_2} b \subset_{d/d_2} d^{-1}a.$$

Il en résulte que

$$b \subset_{d/d_1} (d/d_1)^{-1} O_{c_1'} a \subset_{d_1} d^{-1} a \quad \text{et} \quad a \subset_{d/d_2} d_2 O_{c_2'} b \subset b.$$

En particulier, $O_{c_1'} b \subset d^{-1} a$ et $O_{c_2'} a \subset b$, donc $c_1' = c_2' = c$, et avec $d' = d/d_1 d_2$,

$$a \subset_{d_1} O_c a \subset_{d'} d_2 O_c b \subset_{d_2} b.$$

Soit enfin q un nombre premier. Si q divise c, il existe un unique réseau O_c-stable contenant $O_c a$ avec un indice q, et ce réseau est $O_{c/q} a$. Si q divise d', $q^{-1} O_c a \cap d_2 O_c b$ est un tel réseau, de plus contenu dans b. La définition de c montre alors que q ne peut pas diviser à la fois c et d', qui sont donc relativement premiers. Posant $\mathcal{M} = O_K (d_2 b)^{-1} a$, on a alors : $\mathcal{M} \subset_{d'} O_K$, $\mathcal{M}_c = \mathcal{M} \cap O_c$ est O_c-inversible et $d_2 O_c b = \mathcal{M}_c^{-1} O_c a$.

10. Pour décrire commodément le résultat ainsi obtenu en termes de courbes elliptiques, introduisons le formalisme suivant : si $E_{/\mathbb{C}}$ est une courbe elliptique à multiplication complexe par O_f et M un O_f-module, on note E^M le $\mathbb{C}$-préfaisceau en groupe abélien défini par $E^M(S) = \mathrm{Hom}_{O_f}(M, E(S))$ pour tout $\mathbb{C}$-schéma S. C'est un schéma en groupe propre lorsque M est de type fini, et une courbe elliptique lorsque M est un réseau de K.

11. Avec ces conventions, on a démontré :

Lemme. *Toute isogénie cyclique $E_1 \to E_2$ de courbes elliptiques à multiplication complexe par K se factorise de la manière suivante (avec les degrés indiqués) :*

$$\begin{array}{ccc} E_1 & \xrightarrow{d} & E_2 \\ d_1 \downarrow & & \uparrow d_2 \\ E_1^{O_c} & \xrightarrow{d'} & E_1^{\mathcal{M}_c} \simeq E_2^{d_2 O_c} \end{array} \quad \text{avec} \quad \begin{cases} d = d_1 d_2 d' \\ c = c_1/d_1 = c_2/d_2 \\ \mathrm{pgcd}(c, d') = 1 \end{cases}$$

où c_1 et c_2 sont les conducteurs des ordres $\mathrm{End}(E_1)$ *et* $\mathrm{End}(E_2)$ *et $\mathcal{M}_c = \mathcal{M} \cap O_c$ pour un idéal $\mathcal{M} \subset_{d'} O_K$.*

Pour dénoter les principaux invariants associés à cette décomposition, on écrit symboliquement

$$(c_1 \to c \xrightarrow{\mathcal{M}} c \to c_2).$$

Références

[1] Cornut C., *A conjecture of B. Mazur on higher Heegner Points*, à paraître dans Inventiones Math.

[2] Edixoven B., *Special points on products of modular curves*, en préparation.

[3] Edixoven B., Yafaev A., *Subvarieties of Shimura varieties*, soumis. Disponible à : `http ://arXiv.org/abs/math.AG/0105241`.

[4] Moonen B., *Linearity properties of Shimura varieties, II*, Comp. Math. **114** (1998), 3-35.

E-mail address: `cornut@math.harvard.edu`

Science Center, Harvard University, One Oxford Street, Cambridge, MA, 02138, USA. Tel : (617) 495-5960. Fax : (617) 495-5132