

LA TORSION RATIONNELLE DES COURBES ELLIPTIQUES SUR LES CORPS DE NOMBRES

CÉCILE ARMANA

Séminaire étudiant de théorie des nombres de l'IMJ
22 février et 1er mars 2006

Soit E une courbe elliptique sur un corps K .

Si $K = \mathbb{C}$, le groupe abélien des points K -rationnels $E(K)$ est isomorphe à \mathbb{C}/Λ pour un réseau Λ de \mathbb{C} . Le sous-groupe des points d'ordre fini $E(\mathbb{C})_{\text{tors}}$ est alors infini et isomorphe à $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$.

Si K est un corps de nombres, le théorème de Mordell-Weil dit que le groupe abélien $E(K)$ est de type fini, donc isomorphe à $E(K)_{\text{tors}} \times \mathbb{Z}^r$. L'étude de $E(K)$ passe donc par l'étude d'une part de la torsion (qui est finie) et d'autre part du rang r (conjecture de Birch et Swinnerton-Dyer par exemple).

Nous nous intéressons ici à la torsion. En un premier p de bonne réduction de E , la torsion première à p s'injecte dans les points de la réduction \tilde{E} en p : en prenant plusieurs valeurs de p , cela donne une méthode pour borner (et calculer) effectivement la torsion d'une courbe elliptique donnée. Quel résultat peut-on cependant avoir sur la torsion d'une famille (infinie) de courbes elliptiques ? La «conjecture forte» de borne uniforme pour la torsion des courbes elliptiques sur des corps de nombres est la suivante :

Conjecture. *Pour tout entier $d \geq 1$, il existe un entier $C_d \geq 1$ tel que pour tout corps de nombres K de degré d sur \mathbb{Q} , et pour toute courbe elliptique E sur K , $|E(K)_{\text{tors}}| \leq C_d$.*

On parle de conjecture forte, par opposition à la conjecture faible, dans laquelle K est fixé au lieu de d , et la constante dépend de K . Enfin, on ne devrait plus parler de conjecture, puisque c'est désormais un théorème de Merel, dont les idées de démonstration sont l'objet de cet exposé.

Enfin, on peut formuler le problème analogue pour les courbes elliptiques sur un corps de fonctions. Levin [13] a montré que pour tout K corps de fonctions algébrique en une variable, de corps des constantes k , pour toute courbe elliptique sur K (d'invariant j non transcendant sur k), on peut majorer l'ordre de $E(K)_{\text{tors}}$ par une borne effectivement calculable et dépendant uniquement du genre de K .

1 Panorama historique

La paternité de la conjecture, parfois attribuée à Ogg, avait déjà été formulée, sous une forme faible sur \mathbb{Q} , à B. Levi [12] en 1908.

En 1969, Manin [14] démontre une version locale et faible : pour tout corps de nombres K et pour tout premier p , il existe un entier N tel que l'ordre d'un point de p -torsion d'une courbe elliptique sur K ne peut excéder p^N .

En 1976, Mazur [15] démontre la conjecture faible pour $d = 1$. Plus précisément, si E est une courbe elliptique sur \mathbb{Q} , son groupe de torsion est isomorphe à l'un des 15 groupes suivants :

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & \text{pour } 1 \leq m \leq 10, m = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & \text{pour } 1 \leq m \leq 4. \end{array}$$

De plus, chacun de ses groupes est effectivement réalisé. En particulier, cela dit qu'aucune courbe elliptique sur \mathbb{Q} ne peut avoir de point \mathbb{Q} -rationnel d'ordre 11, 13 ou 14.

En 1992, Kamienny [8] démontre la conjecture faible pour les corps quadratiques ($d = 2$). Ses travaux associés à ceux de Kenku et Momose donnent là aussi la liste des groupes de torsion possibles :

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & \text{pour } 1 \leq m \leq 16, m = 18 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & \text{pour } 1 \leq m \leq 6 \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z} & \text{pour } 1 \leq m \leq 2 \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. & \end{array}$$

En 1993, Abramovich [1] ramène la vérification de la conjecture forte pour un d donné à un calcul explicite. Il démontre ainsi la conjecture pour $d \leq 14$.

Enfin, en 1994, Merel [17], suivant les travaux de Mazur et Kamienny, démontre la conjecture forte pour tout entier d . Sa démonstration ne donne pas une borne effective. Cependant, elle donne une majoration des nombres premiers pouvant diviser les ordres des groupes $E(K)_{\text{tors}}$ (en d^{3d^2} , raffiné ensuite en $(1 + 3^{d/2})^2$ par Oesterlé [18]).

En 1995, Parent [19] démontre une version explicite : il donne une borne pour les puissances de nombres premiers qui peuvent diviser la torsion : $p^n \leq 65(3^d - 1)(2d)^6$ pour $p \neq 2, 3$ ⁽¹⁾. Ceci, associé à la borne de Merel-Oesterlé, fournit une borne pour la torsion exponentielle en d . On conjecture qu'il existe une borne polynomiale.

2 Liens avec d'autres conjectures

La conjecture *abc* de Masser-Oesterlé pour un corps de nombres K implique l'existence d'une borne uniforme pour $E(K)_{\text{tors}}$ dépendant de K . Il en est de même pour la conjecture de la hauteur pour les courbes elliptiques sur K (pour ces deux résultats, voir [6]).

Le problème de borne uniforme peut être généralisé aux variétés abéliennes :

Conjecture. *Pour tous entiers $g \geq 1$ et $d \geq 0$, il existe un entier $C_{g,d}$ tel que pour toute variété abélienne A de dimension g sur un corps de nombres K de degré d , $|A(K)|_{\text{tors}} \leq C_{g,d}$.*

Bien entendu, le cas $g = 1$ correspond aux courbes elliptiques. Pour $g > 1$, le problème est ouvert. On ne connaît pas de corps de nombres pour lequel la conjecture est vérifiée. Cependant, il suffirait de démontrer une version faible de la conjecture pour le corps \mathbb{Q} (et pour tout $g \geq 1$) pour avoir la conjecture (pour tout corps de degré au plus d et pour tout $g \geq 1$) : c'est une simple conséquence de la restriction des scalaires à la Weil.

Sur un corps de nombres donné, on connaît des bornes pour des familles de variétés abéliennes vérifiant certaines propriétés. Par exemple, pour celles ayant potentiellement bonne réduction partout, Silverberg [20] établit une borne uniforme (exponentielle en d) qui est une conséquence facile du fait que la torsion première à p s'injecte dans les points rationnels de la réduction modulo p .

¹Pour $p = 2, 3$, on a des formules analogues.

3 Principe de la preuve de Mazur-Kamienny-Merel

Le reste de l'exposé va être consacré à la présentation des grandes lignes de la preuve de la conjecture, et aux différents apports des mathématiciens précédemment cités.

Le langage modulaire fournit un cadre naturel pour étudier le problème. Un point K -rationnel de la courbe modulaire $X_1(N)$ correspond soit à une classe d'isomorphisme de couples (E, P) où E est une courbe elliptique sur K et P un point K -rationnel d'ordre N , soit à une «pointe» (il n'y a qu'un nombre fini de pointes). La borne uniforme pour la torsion des courbes elliptiques sur K revient à dire que pour N suffisamment grand, les seuls points K -rationnels de la courbe modulaire $X_1(N)$ sont les pointes (autre formulation : la courbe modulaire affine $Y_1(N) = \Gamma_1(N) \backslash \mathcal{H}$ n'a pas de points K -rationnels). Depuis les années 80, on sait déjà grâce au théorème de Faltings [4] (ex-conjecture de Mordell) que $X_1(N)(K)$ est fini pour N suffisamment grand.

3.1 Kamienny-Mazur et le problème de p -torsion

Soit un entier $d \geq 1$. On introduit l'ensemble $\Phi(d)$ des classes d'isomorphismes de groupes $E(K)_{\text{tors}}$ avec E courbe elliptique sur un corps de nombres K de degré d . Démontrer la conjecture forte revient à montrer que $\Phi(d)$ est fini pour tout $d \geq 1$.

On introduit l'ensemble $S(d)$ des premiers p tels qu'il existe une courbe elliptique E sur un corps de nombres K de degré d ayant un point K -rationnel d'ordre p . Remarquons que c'est également l'ensemble des premiers p pouvant diviser $E(K)_{\text{tors}}$ (pour un corps K et une courbe elliptique E).

Théorème (Kamienny-Mazur [10]). $\Phi(d)$ est fini si et seulement si $S(d)$ est fini.

Ce théorème permet de ramener la démonstration de la borne uniforme en degré d au problème, plus simple, de la finitude de $S(d)$.

Un mot sur sa démonstration. Un sens est évident. Pour l'autre : pour tout $p \in S(d)$, il suffit de borner l'exposant maximal N tel qu'il puisse exister un corps de nombres K de degré d et une courbe elliptique E/K avec un point d'ordre p^N . Cela revient à démontrer une version forte du théorème de Manin. La démonstration s'appuie alors sur le théorème suivant de Frey, lui-même conséquence d'un théorème de Faltings (conjecture de Lang pour les points rationnels des sous-variétés des variétés abéliennes).

Théorème (Frey [5]). Soit K un corps de nombres, d un entier ≥ 0 et C une courbe géométriquement irréductible, lisse, projective sur K avec $C(K) \neq \emptyset$. On suppose que tout morphisme non constant $C \rightarrow \mathbb{P}_K^1$ est de degré $> 2d$. Alors $C^{(d)}(K)$ est fini.

Une remarque : même si $S(d)$ est donné explicitement, la démonstration du théorème ne permet pas de borner effectivement $\Phi(d)$. L'absence de résultat effectif dans le théorème de Merel est due à cette étape : on borne les premiers pouvant diviser la torsion, mais on ne sait rien des puissances qui interviennent... Le travail de Parent pour obtenir une borne effective a consisté à travailler directement en niveau p^n plutôt qu'en niveau p et à ne pas utiliser ce résultat de Kamienny-Mazur.

3.2 Finitude de $S(1)$, par Mazur

3.2.1 Comportement par réduction

Soit $N \in S(1)$, E la courbe elliptique sur \mathbb{Q} et $P \in E(\mathbb{Q})$ le point d'ordre premier N correspondants. Soit p un nombre premier fixé ($p = 3$ va convenir). Soit \tilde{E} la fibre du modèle de

Néron de E au-dessus de \mathbb{F}_p et $\tilde{P} \in \tilde{E}(\mathbb{F}_p)$ la réduction de P . Si N ne divise pas p , alors \tilde{P} est d'ordre N .

La réduction \tilde{E} est de l'un des types suivants :

- \tilde{E} a bonne réduction : c'est une courbe elliptique sur \mathbb{F}_p , et la borne de Hasse donne $N \leq |\tilde{E}(\mathbb{F}_p)| \leq (1 + p^{1/2})^2$ (majoration indépendante de K et E).
- \tilde{E} a mauvaise réduction additive : on a la suite exacte de schémas en groupes :

$$0 \rightarrow \mathbb{G}_{a, \mathbb{F}_p} \rightarrow \tilde{E} \rightarrow \Phi \rightarrow 0$$

où $\mathbb{G}_{a, \mathbb{F}_p}$ correspond aux points à réduction non singulière et Φ au groupe des composantes connexes. On a $\mathbb{G}_{a, \mathbb{F}_p}(\mathbb{F}_p) \simeq \mathbb{F}_p$ et $\Phi(\mathbb{F}_p)$ de cardinal au plus 4 (classification de Kodaira-Néron, [21] et [22]). Donc $|\tilde{E}(\mathbb{F}_p)|$ divise p , $2p$, $3p$ ou $4p$. Comme N est premier et ne divise pas p , $N \leq 3$.

- \tilde{E} a mauvaise réduction multiplicative : on a la suite exacte de schémas en groupes :

$$0 \rightarrow T \rightarrow \tilde{E} \rightarrow \Phi \rightarrow 0$$

La classification de Kodaira-Néron dit encore :

- ◊ cas non déployé : $T \simeq \mathbb{G}_{m, \mathbb{F}_p}$ (twist) et $\Phi(\mathbb{F}_p)$ est de cardinal $k \leq 4$. Ainsi, $\tilde{E}(\mathbb{F}_p)$, et donc N , divisent $k(p+1)$. On en déduit $N < p$ (si $p \neq 2$).
- ◊ cas déployé : $T \simeq \mathbb{G}_{m, \mathbb{F}_p}$ et $\Phi(\mathbb{F}_p)$ est un groupe cyclique de cardinal $v = -\text{ord}_p(j(E))$. Comme v dépend de E , on ne peut pas *a priori* majorer uniformément l'ordre N de \tilde{P} . Plus précisément, si \tilde{P} est dans la composante neutre \tilde{E}^0 , alors N divise $p-1$. Si \tilde{P} n'est pas dans \tilde{E}^0 , on ne peut pas conclure. L'approche de Mazur consiste à voir que pour N suffisamment grand (en fonction de p premier et de d), ce cas ne se produit pas.

3.2.2 Méthode de Mazur

Soit donc $\tilde{P} \notin \tilde{E}^0$. Notons x le point \mathbb{Q} -rationnel de la courbe modulaire $X_0(N)$ correspondant au couple formé de E et du sous-groupe d'ordre cyclique N engendré par P . On peut supposer que x se spécialise en p en la pointe ∞_p de $X_0(N)_{\mathbb{F}_p}$.

Soit $J_0(N)$ la jacobienne de $X_0(N)$ et le morphisme canonique $f : X_0(N) \rightarrow J_0(N)$ qui à Q associe la classe du diviseur $(Q) - (\infty)$ (et qui envoie ∞ sur 0).

Supposons momentanément que $f(x)$ est de torsion dans la jacobienne. Alors un lemme de spécialisation sur les schémas en groupes dit que $f(x)_p$ et $f(x)$ ont même ordre. Donc $f(x)$ a même ordre que $f(\infty)_p = 0_p$, donc $f(x) = 0$. Supposons également que le genre de $X_0(N)$ soit ≥ 1 , de sorte que f est une injection. On en déduit alors que $x = \infty$ dans $X_0(N)$, ce qui contredit l'interprétation modulaire de x . La preuve serait terminée.

Malheureusement, on ne sait pas dire si $f(x)$ est de torsion. Pour y remédier, on procède de la façon suivante :

1. On remplace $J_0(N)$ par un quotient J de $J_0(N)$ n'ayant qu'un nombre fini de points rationnels : le quotient d'Eisenstein (Mazur) ou le quotient d'enroulement (Merel).
2. Le morphisme f est donc remplacé par la composée

$$f' : X_0(N) \twoheadrightarrow J$$

de f et de la surjection canonique $J_0(N) \twoheadrightarrow J$. Son injectivité n'est plus assurée. Mazur la remplace par la propriété d'être une «immersion formelle» en ∞ (en caractéristique p). Alors, un résultat sur les immersions formelles dit que si $x_p = \infty_p$ et $f'(x) = f'(\infty)$ ($= 0$ ici), on a $x = \infty$ (voir par exemple [19]).

3.2.3 Quotient d'Eisenstein et immersion formelle

Le quotient d'Eisenstein est l'ingrédient fondamental de la preuve de Mazur. C'est un quotient de la jacobienne de $X_0(N)$, défini sur \mathbb{Q} , dont on donne la définition et quelques propriétés.

Soit \mathbb{T} l'anneau d'endomorphismes de $J_0(N)$: il est engendré par les opérateurs de Hecke T_p (p premier $\neq N$) et l'involution d'Atkin-Lehner w_N . L'idéal d'Eisenstein est l'idéal I de \mathbb{T} engendré par les $T_p - (p+1)$ (pour les p premiers $\neq N$) et $w_N + 1$. Soit c la classe du diviseur $(0) - (\infty)$ dans $J_0(N)(\mathbb{Q})$. On démontre que I est l'annulateur de c dans \mathbb{T} .

Soit $\mathbb{T}_I = \varprojlim \mathbb{T}/I^m$ la complétion I -adique de \mathbb{T} . On définit l'idéal γ_I comme le noyau de $\mathbb{T} \rightarrow \mathbb{T}_I$. Soit $\gamma_I J_0(N)$ la sous-variété abélienne de $J_0(N)$ engendrée par les $tJ_0(N)$, pour $t \in \gamma_I$. Le quotient d'Eisenstein est défini comme $J_E = J_0(N)/\gamma_I J_0(N)$. L'un des principaux résultats de l'article de Mazur est :

Théorème (Mazur [15]). *1. (N premier ≥ 5) Le groupe $J_0(N)(\mathbb{Q})_{tors}$ est cyclique engendré par c , d'ordre $n = \text{num}(\frac{N-1}{12})$.*
2. L'application naturelle $J_0(N) \rightarrow J_E$ induit un isomorphisme de $J_0(N)(\mathbb{Q})_{tors}$ sur $J_E(\mathbb{Q})$. En particulier, $J_E(\mathbb{Q})$ est fini.

La démonstration, difficile, utilise une méthode de descente pour borner le rang de $J_E(\mathbb{Q})$, que l'on peut apparenter à la démonstration du théorème de Mordell-Weil faible.

Soient X et Y deux schémas noethériens, $f : X \rightarrow Y$ un morphisme de schémas, x un point de X et $y = f(x)$. On dit que f est une immersion formelle en x si l'homomorphisme d'anneaux $\widehat{\mathcal{O}_{Y,y}} \rightarrow \widehat{\mathcal{O}_{X,x}}$ déduit de f par passage aux complétés des anneaux locaux est surjectif. La condition se traduit également par la surjection de l'application entre cotangents $\text{Cot}_y(Y) \rightarrow \text{Cot}_x(X)$ ([16]). Mazur démontre assez facilement le résultat suivant :

Théorème (Mazur [16]). *Le morphisme $f' : X_0(N) \rightarrow J_E$ est une immersion formelle (en ∞ en caractéristique $\neq 2$).*

La démonstration utilise l'identification de l'espace cotangent à $J_0(N)$ en 0 aux formes cuspidales de poids 2 pour $\Gamma_0(N)$.

Les deux ingrédients étant réunis, on peut appliquer la méthode de Mazur, ce qui donne l'existence de la borne uniforme pour $d = 1$. Plus précisément, on trouve, avec $p = 3$, $S(1) \subset \{2, 3, 5, 7, 13\}$. La démonstration originale de Mazur dans [15] ne faisait pas intervenir cet argument d'immersion formelle. Cette simplification a été introduite un an plus tard dans [16].

3.3 Finitude de $S(d)$, par Kamienny, Merel

3.3.1 Critère de Kamienny pour l'immersion formelle

L'attaque du problème pour d entier quelconque est la même que celle de Mazur pour $d = 1$. Soit $N \in S(d)$, K le corps de nombres de degré au plus d , E la courbe elliptique sur K et $P \in E(K)$ le point d'ordre N correspondants. Soit p un nombre premier distinct de N et \mathfrak{p} une place de K au-dessus de p . La discussion sur les différents cas possibles de la réduction de E en \mathfrak{p} est toujours valide. Dans les cas qui se comportent bien, on obtient $N \leq (p^{d/2} + 1)^2$ (majoration exponentielle en d). Le cas à éliminer reste celui de réduction multiplicative déployée avec \tilde{P} en-dehors de la composante neutre.

Le couple $(E, \langle P \rangle)$ correspond à un point $y \in X_0(N)(K)$. Comme on souhaite se ramener à l'étude de points \mathbb{Q} -rationnels de courbes (ou de quotient de jacobienes), on fait appel à la puissance symétrique d -ème. On a alors :

$$x = \sum_{\sigma: K \hookrightarrow \mathbb{C}} \sigma(y) \in X_0(N)^{(d)}(\mathbb{Q})$$

On applique alors la méthode de Mazur au point x et au morphisme $f_d : X_0(N)^d \rightarrow J$ obtenu par composition du morphisme canonique :

$$\begin{aligned} X_0(N)^{(d)} &\rightarrow J_0(N) \\ (x_1, \dots, x_d) &\mapsto \text{classe de } (x_1) + \dots + (x_d) - d(\infty) \end{aligned}$$

qui envoie $d\infty = (\infty, \dots, \infty)$ sur 0, et de la surjection canonique (J désigne toujours un quotient de $J_0(N)$ tel que $J(\mathbb{Q})$ est fini).

Contrairement au cas $d = 1$, le morphisme f_d n'est pas automatiquement une immersion formelle en $d\infty$. Une condition pour qu'il le soit a été formulée par Kamienny :

Théorème (Critère de Kamienny [9]). *Si les images T'_1, \dots, T'_d des opérateurs de Hecke T_1, \dots, T_d dans \mathbb{T}/γ_I sont linéairement \mathbb{Z} -indépendants, alors f_d est une immersion formelle en $d\infty$.*

Dans cet énoncé, T_1, \dots, T_d désignent les d premiers opérateurs de Hecke. En vérifiant ce critère pour $d = 2$ et N premier > 61 et différent de 71, Kamienny a démontré la borne uniforme pour les courbes elliptiques sur les corps quadratiques.

3.3.2 Quotient d'enroulement : l'apport de Merel

Dans son article [17], Merel utilise à la place du quotient d'Eisenstein de Mazur, un quotient de $J_0(N)$ plus gros qu'il appelle quotient d'enroulement (*winding quotient*). Sa définition fait intervenir la théorie des symboles modulaires, pour laquelle on peut se référer à [2].

Les symboles modulaires sont les éléments du groupe d'homologie singulière relative aux pointes $H_1(X_0(N), \text{ptes}, \mathbb{Z})$. On peut les voir de la façon suivante : prenons deux pointes α et $\beta \in \mathbb{P}^1(\mathbb{Q})$ et un chemin γ les reliant dans $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$; le symbole modulaire $\{\alpha, \beta\}$ est la projection dans $X_0(N)$ du chemin γ , et est indépendant du chemin choisi.

Notons $H_1(X_0(N), \mathbb{Z})$ l'homologie singulière absolue, c'est un sous-groupe de $H_1(X_0(N), \text{ptes}, \mathbb{Z})$: il correspond aux classes de chemins fermés, ayant pour origine et extrémité la même pointe modulo $\Gamma_0(N)$. C'est un groupe abélien libre de rang $2g$ où g est le genre de la courbe $X_0(N)$. Posons $H_1(X_0(N), \mathbb{R}) = H_1(X_0(N), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{R}$.

L'algèbre de Hecke \mathbb{T} agit sur les objets suivants : l'espace de formes paraboliques $S_2(\Gamma_0(N))$, la jacobienne $J_0(N)$ (comme anneau d'endomorphismes), l'homologie absolue $H_1(X_0(N), \mathbb{Z})$. De plus, il existe des relations de comparaison entre ces objets, compatibles à l'action de \mathbb{T} . C'est pour ces raisons que l'élément d'enroulement va être défini comme un élément de l'homologie absolue et non de l'homologie relative.

A un symbole modulaire cuspidal $\{\alpha, \beta\} \in H_1(X_0(N), \mathbb{R})$, on associe une application \mathbb{C} -linéaire :

$$\begin{aligned} S_2(\Gamma_0(N)) &\rightarrow \mathbb{C} \\ f &\mapsto 2\pi i \int_{\alpha}^{\beta} f(z) dz = \int_{\alpha}^{\beta} \omega_f \end{aligned}$$

où ω_f désigne la différentielle holomorphe sur $X_0(N)$ correspondant à f . Elle induit un isomorphisme \mathbb{T} -linéaire de \mathbb{R} -espaces vectoriels :

$$H_1(X_0(N), \mathbb{R}) \simeq \text{Hom}_{\mathbb{C}}(S_2(\Gamma_0(N)), \mathbb{C})$$

A la forme linéaire $f \mapsto -\int_0^\infty \omega_f$ correspond un élément e de $H_1(X, \mathbb{R})$ appelé élément d'enroulement (*winding element*). D'après le théorème de Manin-Drinfeld, on a en fait $e \in H_1X_0(N), \mathbb{Q}$). Pour tout $f \in S_2(\Gamma_0(N))$, on a donc :

$$\int_e \omega_f = - \int_0^\infty \omega_f.$$

L'idéal d'enroulement I_e est alors défini comme l'annulateur de e dans l'algèbre de Hecke \mathbb{T} . Enfin, le quotient d'enroulement J_e est le quotient de $J_0(N)$ par la sous-variété abélienne $I_e J_0(p)$. C'est une variété abélienne sur \mathbb{Q} .

Pour pouvoir appliquer la méthode de Mazur à J_e , il reste à vérifier deux choses : $J_e(\mathbb{Q})$ est fini et f_d est une immersion formelle en l'infini (éventuellement sous certaines hypothèses).

Finitude du groupe de Mordell-Weil. La démonstration de Merel utilise de façon fondamentale le résultat de Kolyvagin-Logachev concernant la conjecture de Birch et Swinnerton-Dyer pour les variétés abéliennes sur un corps de nombres :

Théorème (Kolyvagin-Logachev ⁽²⁾ [11]). *Soit $f \in S_2(\Gamma_0(N))$ une forme propre pour les opérateurs de Hecke et A la variété abélienne quotient de $J_0(N)$ correspondant à f . Si $L_f(1) \neq 0$, alors A n'a qu'un nombre fini de points \mathbb{Q} -rationnels.*

Bien entendu, Mazur ne disposait pas à l'époque de son article de ce résultat, c'est pourquoi il a montré à la main la finitude du groupe de Mordell-Weil de J_E . Le fait que le quotient d'enroulement ait son groupe de Mordell-Weil fini est un résultat bien plus profond que l'énoncé analogue pour le quotient d'Eisenstein. Nous nous contenterons d'utiliser le théorème de Kolyvagin-Logachev comme une boîte noire.

Voyons maintenant comment utiliser ce résultat. On a une isogénie canonique :

$$J_e \rightarrow \prod_{i=1}^s A_{f_i}$$

où les A_{f_i} sont des variétés abéliennes simples sur \mathbb{Q} obtenues à partir de certaines formes primitives f_i . Montrer que $J_e(\mathbb{Q})$ est fini revient à montrer qu'on a $A_{f_i}(\mathbb{Q}) \neq \emptyset$ pour tout i . D'après ce qui précède, il suffit pour cela de prouver que la fonction- L de f_i ne s'annule pas en 1.

Soit f l'une de ses formes. L'expression de la fonction- L comme transformée de Mellin permet de voir que :

$$L(f, 1) = 2\pi \int_0^\infty f(iy)dy = - \int_0^\infty 2\pi i f(\tau)d\tau = - \int_0^\infty \omega_f = \int_e \omega_f.$$

et on montre que pour les formes primitives f_1, \dots, f_s , cette quantité est non nulle (cela vient du fait qu'elles proviennent de J_e).

Lien avec le quotient d'Eisenstein. Le groupe des points complexes de $J_0(N)$ est isomorphe à $H_1(X_0(N), \mathbb{R})/H_1(X_0(N), \mathbb{Z})$. L'élément c correspond alors à la classe de l'élément d'enroulement e dans le quotient. On démontre que l'idéal d'enroulement I_e est contenu dans l'idéal d'Eisenstein

²Leur énoncé original contient une condition supplémentaire sur f qui fut supprimée ensuite indépendamment par Bump, Friedberg, Hoffstein d'une part et M.R. Murty et V.K. Murty d'autre part.

I_E et que J_E est un quotient de J_e . En fait, on peut montrer que J_e est le plus grand quotient de $J_0(N)$ dont la fonction- L ne s'annule pas en $s = 1$. Modulo la conjecture BSD, c'est donc le plus grand quotient de $J_0(N)$ défini sur \mathbb{Q} ayant un nombre fini de points rationnels. Enfin, comme le remarque Oesterlé ([18], remarque 3), comme pour le quotient d'Eisenstein, on a un isomorphisme $J_0(N)(\mathbb{Q})_{\text{tors}} \simeq J_e(\mathbb{Q})$: en particulier, $J_e(\mathbb{Q})$ est également d'ordre $n = \text{num}(\frac{N-1}{12})$.

Immersion formelle. Merel a montré que le critère d'immersion formelle de Kamienny s'exprime dans le cas du quotient d'enroulement de la façon suivante :

Théorème (Critère de Kamienny pour e [17]). *Soit N premier et $d > 1$. Si T_1e, \dots, T_de sont \mathbb{Z} -linéairement indépendants $H_1(X_0(N), \mathbb{Q})$, alors f_d est une immersion formelle en $d\infty$.*

Cela revient à montrer l'indépendance linéaire des images T'_1, \dots, T'_d des opérateurs de Hecke T_1, \dots, T_d dans \mathbb{T}/I_e . Comme $I_e \subset \gamma_I$, c'est une condition plus faible à réaliser que le critère de Kamienny pour le quotient d'Eisenstein.

Pour clore le problème de la borne uniforme en degré d , Merel a démontré ce résultat d'indépendance linéaire de symboles modulaires pour $d \leq 3$ et le niveau $N > d^{3d^2}$ ($N > C.d^6$ chez Parent). Il construit en fait, pour N suffisamment grand, des éléments $x_k \in H_1(X_0(N), \mathbb{Q})$ vérifiant $x_k.T_k(e) \neq 0$ et $x_k.T_i e = 0$ pour $i < k$ (le point désigne le produit d'intersection). Cette construction se fait par un lemme de théorie analytique des nombres, qui se démontre par de l'analyse de Fourier sur $\mathbb{Z}/p\mathbb{Z}$ et une borne sur les sommes de Kloosterman due à Weil (elle-même conséquence de l'hypothèse de Riemann pour les variétés sur les corps finis).

Remarquons qu'à cet endroit, la majoration obtenue est polynomiale en d . Malheureusement, elle est dépassée par la majoration exponentielle obtenue auparavant pour les cas de bonne réduction, réduction additive ou réduction multiplicative non déployée. Hindry et Silverman [7] ont obtenu une borne polynomiale en d pour les courbes elliptiques à bonne réduction partout. C'est en partie pour ces raisons que l'on conjecture l'existence d'une borne polynomiale pour la torsion des courbes elliptiques sur des corps de nombres.

♣ Ce texte s'inspire beaucoup de l'exposé d'Edixhoven [3] au séminaire Bourbaki en mars 1994. Malheureusement, les explications sur l'apport de Merel sont succinctes, car sa démonstration a été annoncée seulement quelques semaines plus tôt. Il existe aussi un texte détaillé d'Oesterlé [18], reprenant la preuve de Merel et améliorant la borne, mais non publié. Enfin, Darmon a écrit une review détaillée de l'article de Merel pour Mathscinet.

Je remercie Nicolas Ratazzi pour sa relecture et pour ses commentaires.

Références

- [1] D. Abramovich. Formal finiteness and the torsion conjecture on elliptic curves. A footnote to a paper : "Rational torsion of prime order in elliptic curves over number fields" [Astérisque No. 228 (1995), 3, 81–100; MR1330929 (96c :11058)] by S. Kamienny and B. Mazur. *Astérisque*, (228) :3, 5–17, 1995. Columbia University Number Theory Seminar (New York, 1992).
- [2] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.
- [3] B. Edixhoven. Rational torsion points on elliptic curves over number fields (after Kamienny and Mazur). *Astérisque*, (227) :Exp. No. 782, 4, 209–227, 1995. Séminaire Bourbaki, Vol. 1993/94.

- [4] G. Faltings. Erratum : “Finiteness theorems for abelian varieties over number fields”. *Invent. Math.*, 75(2) :381, 1984.
- [5] G. Frey. Curves with infinitely many points of fixed degree. *Israel J. Math.*, 85(1-3) :79–83, 1994.
- [6] Gerhard Frey. Links between solutions of $A - B = C$ and elliptic curves. In *Number theory (Ulm, 1987)*, volume 1380 of *Lecture Notes in Math.*, pages 31–62. Springer, New York, 1989.
- [7] Marc Hindry and Joseph Silverman. Sur le nombre de points de torsion rationnels sur une courbe elliptique. *C. R. Acad. Sci. Paris Sér. I Math.*, 329(2) :97–100, 1999.
- [8] S. Kamienny. Torsion points on elliptic curves and q -coefficients of modular forms. *Invent. Math.*, 109(2) :221–229, 1992.
- [9] S. Kamienny. Torsion points on elliptic curves over fields of higher degree. *Internat. Math. Res. Notices*, (6) :129–133, 1992.
- [10] S. Kamienny and B. Mazur. Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, (228) :3, 81–100, 1995. With an appendix by A. Granville, Columbia University Number Theory Seminar (New York, 1992).
- [11] V. A. Kolyvagin and D. Yu. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5) :171–196, 1989.
- [12] B. Levi. Sull’equazione indeterminata del 3° ordine. *Atti del IV congresso internazionale dei matematici, Roma, 6-11 Aprile 1908*, 1908.
- [13] Martin Levin. On the group of rational points on elliptic curves over function fields. *Amer. J. Math.*, 90 :456–462, 1968.
- [14] Ju. I. Manin. The p -torsion of elliptic curves is uniformly bounded. *Izv. Akad. Nauk SSSR Ser. Mat.*, 33 :459–465, 1969.
- [15] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47) :33–186 (1978), 1977.
- [16] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2) :129–162, 1978.
- [17] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3) :437–449, 1996.
- [18] J. Oesterlé. Torsion des courbes elliptiques sur les corps de nombres. Non publié.
- [19] P. Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506 :85–116, 1999.
- [20] A. Silverberg. Points of finite order on abelian varieties. In *p -adic methods in number theory and algebraic geometry*, volume 133 of *Contemp. Math.*, pages 175–193. Amer. Math. Soc., Providence, RI, 1992.
- [21] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
- [22] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

armana@math.jussieu.fr