Points Rationnels et Séries de Dirichlet

Loïc Merel

1 Le problème de la torsion des courbes elliptiques

En 1908, lors du congrès international des mathématiciens, B. Levi a proposé (au vocabulaire près) la conjecture suivante : les points $\mathbf{Q}$-rationnels d'ordre fini d'une courbe elliptique forment un groupe isomorphe à l'un des groupes suivants : $\mathbf{Z}/n\mathbf{Z}$ (avec $n \in \{1,2,3,4,5,6,7,8,10\}$), $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (avec $n \in \{1,2,3,4\}$). La précision de cette conjecture est d'autant plus étonnante que cette formulation précède le théorème de Mordell. Plus de soixante ans plus tard, cette conjecture fut attribuée a A. Ogg jusqu'à la redécouverte récente par N. Schappacher et R. Schoof des travaux de Levi. Bien entendu l'énoncé de Levi est depuis 1977 un théorème de B. Mazur [6].

Comme c'est souvent le cas en arithmétique, un théorème démontré pour les nombres rationnels est un théorème démontré pour seulement un corps de nombres. Mazur a produit en 1978 une seconde preuve de son théorème [7]. Cette dernière preuve peut-être considérée comme le point de départ des travaux ultérieurs sur les points de torsion des courbes elliptiques sur les corps de nombres.

On dispose depuis 1994 du théorème suivant [8] :

Théorème 1 *Soit d un entier > 0. Il existe un nombre fini de groupes, à isomorphisme près, qui sont constitués par la partie de torsion du groupe des points K-rationnels d'une courbe elliptique sur K, où K parcourt les corps de nombres de degré d sur $\mathbf{Q}$.*

Indiquons brièvement comment la recherche s'est developpée à partir de 1978. Les méthodes de Mazur ont été généralisées par S. Kamienny, ce qui a permis de démontrer le théorème ci-dessus pour $d = 2$ (Kamienny [2]), puis pour $d \leq 8$ (Kamienny et Mazur [4]), puis pour $d \leq 14$ (D. Abramovich [1]). La démonstration du cas général repose sur l'approche de Kamienny et Mazur (mais est indépendante de la première preuve de Mazur). Soulignons le rôle central joué (pour $d > 14$) par les travaux de Kolyvagin, Logachev, Gross, Zagier ... en direction de la conjecture de Birch et Swinnerton-Dyer.

Un énoncé plus faible que le théorème (finitude dépendant de K et non seulement du degré d), constituait un problème ouvert au moins depuis les années 60. La dépendance en le degré a été mise en évidence par Kamienny [3]. Comme l'a démontré Abramovich, le théorème est une des multiples conséquence étonnantes de conjectures très générales de S. Lang.

On dispose maintenant de versions précises du théorème 1. Indiquons-en deux dues à J. Oesterlé et P. Parent.

Théorème 2 (Oesterlé) *Soit d un entier > 0. Soit K un corps de nombres de degré d sur $\mathbf{Q}$. Soit E une courbe elliptique sur K munie d'un point K-rationnel d'ordre premier p. Alors on a*

$$p \leq (1 + 3^{\frac{d}{2}})^2.$$

C'est un cas particulier des résultats ultérieurement obtenus par Parent. Il implique, à la suite de remarques d'Abramovich, Frey, Kamienny et Mazur et à l'aide d'un théorème non effectif de G. Faltings le théorème 1. Le théorème suivant se démontre de façon analogue au théorème 2 apour conséquence facile le théorème 1.

Théorème 3 (Parent) *Soit d un entier > 0. Soit K un corps de nombres de degré d sur $\mathbf{Q}$. Soit E une courbe elliptique sur K munie d'un point K-rationnel d'ordre une puissance n d'un nombre premier p. Alors on a*

$$n \leq 129(5^d - 1)(3d)^6.$$

Le théorème d'Oesterlé (malheureusement non publié) donne une idée fidèle des limites des méthodes actuelles. Un examen du principe de la démonstration convainc rapidement que les inégalités numériques obtenues par Oesterlé et Parent n'ont guère de raisons d'être satisfaisantes. Une avancée importante consisterait désormais à établir des des inégalités analogues dépendant polynomialement du degré d. Pour cela on aimerait combiner les méthodes modulaires avec les méthodes issues de la théories des nombres transcendants (voir les travaux de D. Masser, G. Wüstholz, S. David, M. Hindry, F. Pellarin).

Le seul degré d où on dispose d'un analogue satisfaisant du théorème de Mazur est le degré $d = 2$, pour lequel la liste complète des sous-groupes possibles a été établie par Kamienny [2], à l'aide de travaux antérieurs de M. A. Kenku et F. Momose [5].

Nous nous proposons d'évoquer les grandes lignes de la démonstration du théorème 2.

2 Analyse élémentaire

Soit d un entier > 0. Soit K un corps de nombres de degré d sur $\mathbf{Q}$. Soit E une courbe elliptique sur K munie d'un point P qui est K-rationnel et d'ordre premier p.

Considérons un nombre premier auxiliaire l. Soit λ un idéal premier de l'anneau des entiers de K au dessus de l. Des arguments élémentaires (essentiellement le théorème de Hasse-Weil) montrent qu'on a $p \leq (1 + l^{d/2})^2$ ou que E a réduction multiplicative déployée en λ et que P est d'ordre p dans le groupe des composantes de la fibre en p du modèle de Néron de E (Nous dirons que cette dernière situation constitue le cas critique en λ).

La difficulté de la démonstration du théorème est donc concentrée dans le cas totalement critique en l (c'est-à-dire le cas critique en λ pour tout idéal λ au dessus de l). Tout cela a été constaté, notamment par J. Tate, il y a plus de 40 ans.

Oesterlé choisit le nombre premier $l = 3$ pour sa démonstration. La démonstration originale du théorème 1 utilisait une idée de Kamienny, et montrait l'existence d'un nombre premier l (sans donner de valeur précise pour l) borné en fonction de d seulement pour lequel le cas totalement critique est exclu.

3 Courbes modulaires

Considérons la courbe modulaire $X_0(p)$ qui classifie grossièrement les courbes elliptiques généralisées munies d'un sous-groupe cyclique d'ordre p. Le couple $(E/ < P >, E[p]/ < P >)$ définit un point K rationnel de $X_0(p)$ et donc un point $\mathbf{Q}$-rationnel Q de la puissance symétrique d-ième $X_0(p)^{(d)}$ de $X_0(p)$.

On est donc ramené à étudier les points rationnels de $X_0(p)^{(d)}$.

4 De la courbe à sa jacobienne

Après, entre autres, A. Weil, C. Chabauty, A. Parshin, Faltings, R. Coleman, il est classique d'étudier les points rationnels d'une courbe X (resp. de la puissance symétrique d-ième de X) en combinant l'étude de la géomeétrie $\phi : X \longrightarrow A$ (resp. $X^{(d)} \longrightarrow A$), où A est une variété abélienne, avec l'étude du groupe des points rationnels de A (ce qui typiquement consiste à établir la finitude du groupe des points rationnels de A).

Considérons la plus grande variété abélienne quotient J_e de $J_0(p)$ dont la fonction L ne s'annule pas en 1. On considère le morphisme (convenablement normalisé) $X_0(p)^{(d)} \longrightarrow J_e$. Par un théorème de Kolyvagin et Logachev (dont des démonstrations alternatives ont été proposées par K. Kato d'une part et par M. Bertolini et H. Darmon d'autre part) la variété abélienne J_e n'a qu'un nombre fini de points $\mathbf{Q}$-rationnels. C'est un argument de nature profondément arithmétique qui est au centre de la démonstration du théorème 1.

On peut résumer la fin de la démonstration du théorème 2 de la façon suivante. Par des arguments dûs à Kamienny il suffit pour conclure de démontrer que les d premiers opérateurs de Hecke sont linéairement indépendants en caractéristique 3 dans J_e (Le même résultat a été ultérieurement obtenu par M. Baker grâce à des méthodes reposant sur l'intégration p-adique de Coleman).

La démonstration de l'indépendance linéaire cherchée se démontre par la théorie des symboles modulaires. (Un énoncé analogue d'indépendance linéaire en caractéristique 0 a été établi par J. Van der Kam par des méthodes fondées sur la théorie analytique des fonctions L ; Cela suffit pour démontrer le théorème 1 mais pas le théorème 2.)

Références

[1] Abramovich, D. *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"* Columbia University Number Theory Seminar (New York, 1992). Astrisque No. 228 (1995), 3, 5–17.

[2] Kamienny, S. *Torsion points on elliptic curves and q-coefficients of modular forms.* Invent. Math. 109 (1992), no. 2, 221–229.

[3] Kamienny, S. *Torsion points on elliptic curves over fields of higher degree.* Internat. Math. Res. Notices (1992), no. 6, 129–133.

[4] Kamienny, S.; Mazur, B. *Rational torsion of prime order in elliptic curves over number fields.* Columbia University Number Theory Seminar (New York, 1992). Astrisque No. 228 (1995), 3, 81–100.

[5] Kenku, M. A.; Momose, F. *Torsion points on elliptic curves defined over quadratic fields.* Nagoya Math. J. 109 (1988), 125–149.

[6] Mazur, B. *Modular curves and the Eisenstein ideal.* Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186.

[7] Mazur, B. *Rational isogenies of prime degree (with an appendix by D. Goldfeld).* Invent. Math. 44 (1978), no. 2, 129–162.

[8] Merel, L. *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Invent. Math. 124 (1996), no. 1-3, 437–449.

Loïc Merel
UFR de Mathématiques
case 7012
Université Denis Diderot
2, place Jussieu
75251 Paris cedex 05
France
merel@math.jussieu.fr