Introduction au domaine de recherche: courbes elliptiques, courbes modulaires et représentations galoisiennes

Elie Studnia

21 mai 2021

Table des matières

1 Introduction

Les courbes elliptiques sont des objets centraux en théorie des nombres. Elles fournissent par exemple le type le plus « simple » d'équation que l'on ne sache pas résoudre en général, mais possèdent suffisamment de richesse et de variété pour justifier leur étude poussée.

Une courbe elliptique désigne en première approximation l'ensemble des solutions d'une équation cubique en trois variables homogènes. Les équations plus simples sont soit des poynômes (des équations polynomiales en deux variables homogènes), ou des équations de degré au plus deux en trois variables homogènes, appelées coniques, dont l'on sait caractériser les solutions générales.

On peut montrer que l'ensemble des points d'une courbe elliptique a une loi de groupe abélien, ce qui rend (en un certain sens) ces courbes uniques parmi les autres courbes algébriques. Il est alors naturel de s'intéresser à la structure de ce groupe abélien. Ces questions ont été étudiées très tôt au début du XX^{e} siècle, résultant en le théorème de Mordell, qui affirme que le groupe des points d'une courbe elliptique sur un corps de nombres est de type fini. Le sous-groupe constitué des points de torsion peut être étudié à l'aide d'objets modulaires, comme on le verra dans la troisième partie.

En revanche, le *rang* du groupe est beaucoup plus difficile à déterminer : les algorithmes connus de calcul de rang ne terminent que conditionnellement, et la plupart des outils détude du rang se ramènent à l'un des problèmes ouverts les plus célèbres de la théorie des nombres, la *conjecture de Birch et Swinnerton-Dyer*. Celle-ci affirme que le rang d'une courbe elliptique peut se lire directement dans sa *fonction L*, qui est un objet analytique qui regroupe de l'information

sur la courbe *a priori* sans lien direct avec le rang – la structure rationnelle des points de torsion, les solutions de l'équation réduite modulo p.

Ces propriétés des courbes elliptiques font qu'elles apparaissent dans de multiples situations. Par exemple, elles sont au cœur de la démonstration par Wiles [37] du « dernier théorème de Fermat », et d'autres équations diophantiennes peuvent se ramener à des questions portant sur des courbes elliptiques, par exemple la détermination des nombres congruents [36], les nombres entiers qui sont des aires de triangles rectangles avec trois côtés de longueurs rationnelles. On les utilise aussi depuis [27] pour factoriser des entiers. D'autre part, les groupes de points de courbes elliptiques, cette fois sur des corps finis, forment des groupes abéliens très utilisés en cryptographie.

Un autre des intérêts des courbes elliptiques est de permettre la construction de représentations galoisiennes à l'aide de leurs points de torsion, ce qui ouvre la voie à beaucoup d'autres problèmes de théorie des nombres. Que peut-on dire de ces représentations ? Par exemple, sont-elles surjectives ? Peuvent-elles être construites à partir d'objets différents ? C'est cette dernière question qu'étudie en fait Wiles, et qui permet grâce à des travaux antérieurs de montrer le « dernier théorème de Fermat ».

2 Les courbes elliptiques

2.1 Point de vue algébrique

Définition *Une courbe elliptique sur un corps k est la donnée d'une courbe (i.e. d'un schéma de dimension 1) X sur k de genre 1, lisse, projective et géométriquement connexe, et d'un point k-rationnel x sur X. Si K est une extension de k, l'enseble des points de X définis sur K est noté $X(K)$.*

Le *genre* d'une variété lisse réelle compacte de dimension 2 est un invariant géométrique qui correspond en termes simples au nombre de « trous » de la surface. En particulier, cette définition s'applique à une surface de Riemann, c'est-à-dire une variété holomorphe qui est localement isomorphe à un ouvert de $\mathbb{C}$. On peut aussi définir un genre *algébrique* sur les courbes définies sur un corps quelconque, et cette notion coïncide avec l'invariant différentiel.

Cette définition est assez abstraite, mais on peut montrer que toute courbe elliptique sur un corps k se réalise comme le lieu des zéros d'un polynome cubique homogène à trois variables, c'est-à-dire possède un plongement dans $\mathbb{P}^2_k$ dont l'image est de degré 3.

Lorsque k est algébriquement clos de caractéristique différente de 2 ou 3, cette équation peut être mise sous la *forme de Weierstrass* $y^2z = x^3 + axz^2 + bz^3$ (l'hypothèse de lissité signifie alors que $4a^3 + 27b^2 \neq 0$), et le point distingué est le « point à l'infini » $[0 : 1 : 0]$.

Il est naturel de considérer cette forme d'équation dans la mesure où les seules équations algébriques « plus simples » sont des formes quadratiques, dont la théorie est assez bien comprise, en particulier sur $\mathbb{Q}$ ou un corps de nombres en général, ou des polynômes en une variable.

Par exemple, les équations de degré deux dans $\mathbb{P}^2_k$ sont les coniques. Si l'on connaît un point P sur k d'une conique C, on peut établir un k-isomorphisme $\mathbb{P}^1 \to C$ de la façon suivante : étant donné un point $t \in \mathbb{P}^1(k)$, t est un élément de k (ou éventuellement le point à l'infini), et on peut considérer la droite projective $D \subset \mathbb{P}^2_k$ passant par P et de pente t. Comme C est de degré deux, $D \cap C$ consiste en deux points (éventuellement confondus, si D est la tangente) : l'un d'entre eux est P, et on associe l'autre point à t.

C'est une construction similaire qui permet de définir la loi de groupe sur une courbe elliptique.

Si on considère deux points P, Q d'une courbe elliptique X sur un corps k (munie d'un point distingué O), la droite PQ recoupe X en un troisième point R (éventuellement égal à P ou Q si la droite PQ est tangente à X en P ou Q), parce que X est une cubique. On dit alors que $P + Q + R$ est nul (cette appellation prend sens à travers la notion de *diviseur*). On définit la

somme de P et Q comme l'unique point R' tel que $R + R' + O$ soit nul. En particulier, si P, Q sont en fait définis sur une certaine extension K de k (par exemple, K contient les coordonnés de leur plongement dans $\mathbb{P}^2$), alors R est aussi défini sur K.

Proposition 2.1 *Soit X une courbe elliptique sur un corps k. L'application $m : X \times X \to X$ qui à un couple (P, Q) associe $P + Q$ provient d'un morphisme de k-variétés algébriques et fait de X une* variété abélienne *sur k pour laquelle O est le neutre. Plus formellement : $m \circ (m \times \mathrm{id}) = m \circ (\mathrm{id} \times m)$ (associativité), $m(\cdot, O) = m(O, \cdot) = \mathrm{id}$ et il existe un morphisme de variétés algébriques $i : X \to X$ tel que $m(\mathrm{id}, i) = m(i, \mathrm{id})$ est l'application constante égale à O.*

Cette structure dépend du choix du point distingué O, mais pas beaucoup. Plus précisément, changer de point revient à translater la loi de groupe. En d'autres termes, c'est la *soustraction* qui est canoniquement définie (mais qui n'est pas à valeurs dans la courbe elliptique elle-même). Dans toute la suite, on ne se préoccupera pas des questions liées au choix du point de base.

2.2 Une approche plus analytique des courbes elliptiques

Un autre point de vue encore plus concret sur les courbes elliptiques est possible, du moins pour celles qui sont définies sur un sous-corps de $\mathbb{C}$.

Définition *Une courbe elliptique sur $\mathbb{C}$ est le quotient de $\mathbb{C}$ par un réseau, c'est-à-dire un sous-groupe discret de rang 2, muni de sa structure naturelle de variété complexe.*

On peut même raffiner cette définition en notant que si Λ est un réseau, il existe des nombres complexes $\alpha \neq 0$ et β de partie imaginaire strictement positive tels que $\Lambda = \alpha(\mathbb{Z} \oplus \beta\mathbb{Z})$, et alors la paire $(\mathbb{C}, \Lambda)$ est biholomorphiquement équivalente à $(\mathbb{C}, \mathbb{Z} \oplus \beta\mathbb{Z})$ (en divisant par α)

Sur cette définition, l'aspect « groupe » apparaît clairement, puisque c'est le quotient de l'addition de $\mathbb{C}$ (et l'addition est préservée par le biholomorphisme ci-dessus). En revanche, le lien avec la définition algébrique est moins évident. Il utilise la théorie des fonctions elliptiques, développée au XIX^e^ siècle, comme suit.

Proposition 2.2 *Soit Λ un réseau de $\mathbb{C}$. Il existe une fonction*

$$\wp_\Lambda : z \longmapsto \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}$$

méromorphe sur $\mathbb{C}$ et Λ-périodique telle que le corps des fonctions méromorphes sur $\mathbb{C}$ et Λ-périodiques soit $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$.

De plus, la seule relation algébrique sur $\mathbb{C}$ entre $\wp_\Lambda$ et $\wp'_\Lambda$ est

$$(\wp'_\Lambda)^2 = 4(\wp_\Lambda - e_1)(\wp_\Lambda - e_2)(\wp_\Lambda - e_3) = 4\wp_\Lambda^3 - 60G_4(\Lambda)\wp_\Lambda - 140G_6(\Lambda),$$

où u_1, u_2, u_3 représentent les trois éléments non nuls de $(\Lambda/2)/\Lambda$, $e_i = \wp_\Lambda(u_i)$, et $G_n(\Lambda) = \sum_{x \in \Lambda \setminus \{0\}} x^{-n}$ pour $n > 2$.

Les fonctions méromorphes $\wp, \wp'$ jouent le rôle des coordonnées dans le cadre algébrique (c'est-à-dire, dans une forme de Weierstrass, x/z, y/z). Il n'est pas évident *a priori*, mais vrai, que l'addition « algébrique » sur la cubique coïncide avec l'addition naturelle sur $\mathbb{C}/\Lambda$, le point distingué étant 0.

Inversément, pour passer de la définition algébrique à la définition analytique pour une courbe elliptique définite sur $\mathbb{C}$, on munit l'ensemble des solutions complexes de la cubique de sa structure holomorphe naturelle (celle donnée par le plongement dans $\mathbb{P}^2_{\mathbb{C}}$), et on montre que m se relève en une loi de groupe sur son revêtement universel. Grâce au théorème d'uniformisation, on peut montrer que celui-ci est biholomorphe à $\mathbb{C}$ et que le relevé de m est (quitte à translater les coordonnées) $(x, y) \longmapsto x + y$, ce qui implique que la courbe elliptique est bien le quotient de $\mathbb{C}$ par un réseau.

2.3 Quelques résultats « élémentaires » importants

L'approche analytique permet de voir immédiatement le phénomène suivant :

Proposition 2.3 *Si X est une courbe elliptique sur un sous-corps k de $\mathbb{C}$, $n \geq 1$ est entier, l'ensemble $X[n](\mathbb{C})$ des points P de X tels que $n \cdot P = O$ (la multiplication par n est une opération de n'importe quel groupe) est un sous-groupe de $X(\mathbb{C})$ isomorphe à $(\mathbb{Z}/n\mathbb{Z})^2$. De plus, il existe une extension k'/k finie telle que tous les points de $X[n](\mathbb{C})$ soient en fait définis sur k'.*

Les éléments de $X[n](\mathbb{C})$ sont les *points de n-torsion* de X.

Informellement, la structure du groupe des points de n-torsion est assurée par le point de vue analytique : en voyant la courbe elliptique comme le quotient de $\mathbb{C}$ par un réseau R, il est clair que le groupe des points de n-torsion est isomorphe à $(1/n)R/R$ qui est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^2$. L'existence de k' est assuré par l'algébricité du morphisme de multiplication par n : construire des points de n-torsion revient à trouver des solutions à un système d'équations rationnelles à coefficients dans k, ce qui est faisable dans une extension finie de k parce que les solutions existent dans $\mathbb{C}$.

Ceci est en quelque sorte un cas particulier du fait suivant, qui est aussi plus facile à comprendre analytiquement :

Proposition 2.4 *Si $f : X \to Y$ est un morphisme d'une courbe elliptique vers une autre (en particulier, envoyant le point distingué de X sur le point distingué de Y), alors c'est un morphisme de groupes. S'il n'est pas constant, il est surjectif de noyau fini (au sens des schémas, ou du moins des points définis sur une clôture algébrique de k), et on dit que c'est une* isogénie.

En effet, il est facile de voir que les seules applications holomorphes $\mathbb{C} \to \mathbb{C}$ qui envoient un réseau Λ dans un réseau Λ' et 0 sur 0 sont linéaires.

En revanche, la construction analytique des courbes elliptiques est assez peu éclairante sur la question des points *rationnels* de la courbe elliptique. Le théorème le plus élémentaire sur la question est le théorème suivant de Mordell.

Proposition 2.5 (Mordell [31]) *Soit X une courbe elliptique sur un corps de nombres k. Alors $X(k)$ est un groupe abélien de type fini.*

La preuve de ce résultat se décompose en deux étapes. La première partie est le *théorème de Mordell faible*, qui consiste à montrer que $E(k)/2E(k)$ est fini. Cet énoncé est démontré en plongeant $E(k)/2E(k)$ dans un groupe de cohomologie et montrer que son image est contenue dans un sous-groupe particulier, un *groupe de Selmer*, dont on peut montrer la finitude.

La deuxième partie consiste à introduire une *hauteur* h sur la courbe elliptique, qui se comporte comme une approximation d'une norme euclidienne sur $E(\mathbb{Q})$, et dont les »boules fermées « ne contiennent qu'un nombre fini de points de $E(k)$. Si l'on note maintenant $Q_1, \ldots, Q_r$ des représentants de $E(k)/2E(k)$, tout point $P \in E(k)$ de hauteur suffisante s'écrit $P = Q_i + 2R$ pour un $R \in E(k)$ tel que $h(R) < \frac{2h(P)}{3}$ (par « identité du parallélogramme approximative »). En appliquant ce procédé récursivement à R, on s'aperçoit que P est engendré par les Q_i et des points de hauteur bornée, et donc que $E(k)$ est de type fini.

Les objets dits de Selmer, qui correspondent à des classes globales de cohomologie satisfaisant des conditions locales, interviennent dans d'autres résultats sur les points rationnels, dans l'étude des courbes elliptiques ([5] par exemple) ou pour d'autres courbes : par exemple, la méthode de Chabauty-Kim utilise des variétés de Selmer pour y localiser les points rationnels de courbes algébriques (voir [2, 16]).

Les hauteurs sont extrêmement utilisées en géométrie arithmétique, parce qu'elles permettent de traiter les points définis sur des corps de nombres différents de la même façon et de définir une notion entièrement arithmétique de proximité entre eux. Un premier exemple est la formule de Gross-Zagier [21], primordiale dans l'étude des cas connus de la conjecture de Birch et Swinnerton-Dyer, qui fait apparaître la hauteur d'un point rationnel sur certaines courbes elliptiques dans la valeur de la dérivée en $s = 1$.

Mais il existe aussi de nombreux exemples d'applications dans un cadre plus large de géométrie arithmétique, lorsqu'il ne s'agit pas seulement de courbes elliptiques. Elles sont les outils de la preuve du théorème de Faltings [17, 18], qui affirme qu'une courbe de genre au moins 2 définie sur un corps de nombres n'a qu'un nombre fini de points sur n'importe quel corps de nombres, et de résultats uniformes plus récents sur le nombre de points d'une courbe algébrique, par exemple [15] ou le théorème d'équidistribution de [26] (qui n'est encore qu'une prépublication arXiv).

Le théorème de Mordell illustre assez bien le rôle intermédiaire des courbes elliptiques dans les courbes algébriques : les coniques d'un côté (de genre nul) ont de très nombreux points rationnels, et les autres courbes, qui sont de genre au moins 2, n'ont qu'un nombre fini de points définis sur un corps de nombres donné.

Si X est une courbe elliptique sur un corps de nombres k, $X(k)$ est donc isomorphe, en tant que groupe abélien, à un $\mathbb{Z}^r \oplus X(k)_{tors}$. Si, comme nous l'expliquerons plus tard, les groupes de torsion sont assez bien compris, en particulier lorsque $k = \mathbb{Q}$, il est beaucoup plus difficile de décrire le *rang* r de la courbe elliptique.

On ignore, par exemple, s'il existe des courbes elliptiques de rang arbitrairement grand. Le meilleur rang connu sur $\mathbb{Q}$ est au moins 28 (et exactement 28 conditionnellement), apparaissant dans un exemple trouvé par Elkies [24]. Bhargava et Shankar ont montré [5, 6] que le rang « moyen » des courbes elliptiques rationnelles était au plus 7/6 (un de leurs textes [4], apparemment non publié, annonce 0.885), en passant d'ailleurs par une estimation en moyenne sur la taille de groupes de Selmer. Comme il a été précédemment évoqué, la détermination du rang d'une courbe elliptique est l'objet de la *conjecture de Birch et Swinnerton-Dyer*. Pour l'énoncer, on associe à une courbe elliptique E sur $\mathbb{Q}$ une certaine fonction holomorphe $L(E, s)$ définie sur $\{s \in \mathbb{C},\, \mathrm{Re}\, s > \frac{3}{2}\}$. Lorsque la conjecture a été formulée, il était conjecturé que cette fonction L pouvait s'étendre en une fonction entière, ce qui est maintenant connu comme une conséquence immédiate du *théorème de modularité* dont nous reparlerons.

Conjecture 2.6 (Birch et Swinnerton-Dyer) *r est l'ordre d'annulation en $s = 1$ de $L(E, s)$ (le « rang analytique » de la courbe).*

Kolyvagin [25] a montré que la conjecture était vraie pour toute courbe elliptique rationnelle modulaire (cette condition est en fait vide d'après le théorème de modularité, mais ce n'était pas encore démontré) dont la fonction L s'annule en 1 avec ordre au plus 1. Un texte de Bhargava, Skinner et Zhang [7] montre qu'une forte proportion (légèrement moins de s deux tiers) de courbes elliptiques est de rang analytique au plus 1 et vérifie donc la conjecture. Mais il ne semble pas y avoir de progrès sur les cas $r \geq 2$ de la courbe, car il n'existe plus de méthode connue pour construire des points rationnels sur la courbe elliptique.

3 Formes modulaires et applications aux courbes elliptiques

3.1 Formes et courbes modulaires

On appelle $\mathbb{H}$ le *demi-plan de Poincaré*, c'est l'ensemble des nombres complexes de partie imaginaire strictement positive. Le groupe $GL_2^+(\mathbb{R})$ des matrices de $\mathbb{R}$ à déterminant strictement positif agit transitivement sur $\mathbb{H}$ par $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \frac{az+b}{cz+d}$.

Pour $n \geq 1$, on a un morphisme de réduction modulo n de $SL_2(\mathbb{Z})$ vers $SL_2(\mathbb{Z}/n\mathbb{Z})$: les sous-groupes $\Gamma(n), \Gamma_1(n), \Gamma_0(n)$ en sont respectivement le noyau, l'image réciproque des matrices triangulaires supérieures avec 1 sur la diagonale, et l'image réciproque des matrices triangulaires supérieures.

Les quotients $Y(n) = \Gamma(n)\backslash\mathbb{H}, Y_1(n) = \Gamma_1(n)\backslash\mathbb{H}, Y_0(n) = \Gamma_0(n)\backslash\mathbb{H}$ sont des surfaces de Riemann (l'action de $SL_2(\mathbb{Z})$ a des points fixes, donc cette assertion n'est pas complètement évidente). Leur intérêt est de paramétrer certaines classes de courbes elliptiques « enrichies » de structures supplémentaires.

Pour justifier l'utilisation de ces groupes, on peut remarquer que $SL_2(\mathbb{Z}) \cdot z$ est, pour $z \in \mathbb{H}$, l'ensemble des $y \in \mathbb{H}$ tels qu'il existe un biholomorphisme $(\mathbb{C}, \mathbb{Z} \oplus \mathbb{Z}z) \to (\mathbb{C}, \mathbb{Z} \oplus \mathbb{Z}y)$.

Proposition 3.7 *Les points de $Y_0(n)$ paramètrent les classes d'équivalence (à biholomorphisme près) de paires (E, G), où E est une courbe elliptique complexe et $G \subset E(\mathbb{C})$ est un sous-groupe cyclique d'ordre n. Plus précisément, la classe de $\tau \in \mathbb{H}$ représente la courbe elliptique $\mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z})$ et le sous-groupe cyclique engendré par $[1/n]$.*

Les points de $Y_1(n)$ paramètrent les classes d'équivalence à biholomorphisme près de paires (E, P), où E est une courbe elliptique complexe et $P \in E(\mathbb{C})$ est un point d'ordre n. Plus précisément, la classe de $\tau \in \mathbb{H}$ représente la paire $(\mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z}), 1/n)$.

Les points de $Y(n)$ paramètrent les classes d'équivalence à biholomorphisme près de triplets (E, P, Q), où E est une courbe elliptique complexe et $P, Q \in E(\mathbb{C})$ forment une base de $E[n](\mathbb{C})$. Plus précisément, la classe de $\tau \in \mathbb{H}$ représente le triplet $(\mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z}), 1/n, \tau/n)$.

On compactifie ces surfaces de Riemann en leur ajoutant un nombre fini de *pointes* : les surfaces obtenues sont notées $X_0(n), X_1(n), X(n)$. On peut en fait définir un tel X_Γ pour tout sous-groupe $\Gamma \leq SL_2(\mathbb{Z})$ qui contient un $\Gamma(N)$ (Γ est alors un *sous-groupe de congruence*).

Une manière commode de travailler sur la surface de Riemann X_G (appelée *courbe modulaire*) est de considérer ses r-différentielles holomorphes, pour $r \geq 1$. Ces différentielles s'écrivent $f(z)(dz)^r$, où f est holomorphe sur $\mathbb{H}$, vérifie certaines conditions de croissance à l'infini (ou aux pointes en général), et telle que si $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$,

$$f\left(\frac{az+b}{cz+d}\right) = \frac{1}{(cz+d)^{r+1}} f(z).$$

Ces fonctions sont des *formes modulaires* de poids $r+1$ pour le groupe de congruence G.

En réalité, tous ces objets sont algébriques en nature, c'est-à-dire que les problèmes de classification sur des sous-corps de $\mathbb{C}$ qui donnent naissance à $X_0(n), X_1(n), X(n)$ (par exemple) peuvent être représentés par des courbes algébriques sur un corps de nombres, égal à $\mathbb{Q}$ pour $X_0(n)$ et $X_1(n)$.

Ceci peut se faire en considérant les corps de fonctions méromorphes de $X_0(n)$ et $X_1(n)$, dans lesquels figurent l'*invariant j*, qui est la fonction holomorphe et $SL_2(\mathbb{Z})$-invariante sur $\mathbb{H}$, défini par

$$j_{an}(\tau) = 1728 \frac{(60G_4)^3}{(60G_4)^3 - 27(140G_6)^2}(\mathbb{Z} + \tau\mathbb{Z}).$$

On peut donc le voir comme une fonction qui associe un nombre complexe à une courbe elliptique. Cette application à un pendant algébrique j_{alg}, qui à une courbe elliptique E d'équation $y^2 = x^3 + ax + b$ associe $1728\frac{4a^3}{4a^3+27b^2}$ – ainsi, $j_{alg}(\mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z})) = j_{an}(\tau)$ – et cette quantité ne dépend pas du choix de l'équation représentant E. Il existe des formules plus complexes valables dans n'importe quel corps, de sorte que toute courbe elliptique E définie sur un corps k possède un invariant $j_{alg}(E)$ sur k, et que tout élément de k puisse s'écrire $j_{alg}(E)$, pour une courbe elliptique E sur k.

Proposition 3.8 *Si E, F sont deux courbes elliptiques sur un corps k avec $j_{alg}(E) = j_{alg}(F)$, alors il existe une extension finie k'/k telle que $E_{k'}$ et $F_{k'}$ soient isomorphes.*

Par exemple, le corps des fonctions de $X_0(n)$ comme courbe algébrique définie sur le corps k de caractéristique nulle est alors $k(j_{an}, j_{an}(n\cdot))$, qui est de degré de transcendance 1 sur k. Un k-point de cette courbe est donc soit une pointe, soit la donnée d'une isogénie $E \to F$ (définie sur la clôture algébrique $\overline{k}$ de k) de courbes elliptiques définies sur k, à isomorphisme sur $\overline{k}$ près. On peut montrer que cela revient à se donner une k-isogénie de courbes elliptiques $E' \to F$, où E' est définie sur k et isomorphe sur $\overline{k}$ à E.

Similairement, les points de $X_1(n)$ définis sur k sont des pointes, ou des paires (E, P), où E est une courbe elliptique définie sur k et P est un point de $E(k)$ d'ordre n, à $\overline{k}$-isomorphisme près.

3.2 Applications à l'étude des points de torsion

Avec cette réinterprétation, on peut ramener nombre de questions sur des courbes elliptiques à des problèmes de points rationnels sur ces courbes modulaires. Voici quelques conséquences, démontrées par Mazur dans [28, 29] :

Théorème 3.9 *Soit E une courbe elliptique sur $\mathbb{Q}$. Alors la partie de torsion de $E(\mathbb{Q})$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ avec $n \leq 12, n \neq 11$ ou $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ avec $m \leq 4$.*

Théorème 3.10 *Si E, F sont deux courbes elliptiques définies sur $\mathbb{Q}$ et isogènes sur $\mathbb{Q}$, par une isogénie de degré n premier (le* degré *d'une isogenie peut être vu comme le nombre de points complexes dans son noyau), alors $n \leq 19$ ou $n \in \{37, 43, 67, 163\}$.*

Au cœur de la preuve de Mazur, et en fait au cœur de la plupart des arguments impliquant des objets modulaires, figurent les *opérateurs de Hecke*. Ils peuvent être définis à plusieurs niveaux : directement en termes de formes modulaires, ou comme des *correspondances* des courbes modulaires, c'est-à-dire en termes simples, des constructions associant à chaque point de la courbe modulaire une combinaison linéaire formelle de points de celle-ci.

Par exemple, si $n \geq 1$ est entier et p est un nombre premier ne divisant pas n, l'opérateur de Hecke T_p d'indice p sur $X_1(n)$ associe à une paire (E, P) $(P \in E[p](\mathbb{C}))$ la somme formelle $\sum_C (E/C, P \bmod C)$, où C parcourt les sous-groupes cycliques d'ordre p de $E(\mathbb{C})$. On peut définir un opérateur de Hecke sur $X_0(n), X_1(n)$ d'indice p pour chaque nombre premier p, avec une modification de la définition lorsque p ne divise pas n.

Rappelons que la *jacobienne* d'une courbe C paramètre les diviseurs de C de degré nul à équivalence linéaire près. Lorsque C est une courbe algébrique, J peut être construite en tant que variété algébrique elle aussi : c'est alors une variété abélienne. Les opérateurs de Hecke, qui commutent deux à deux, peuvent alors être réalisés comme des endomorphismes de la jacobienne $J_0(n)$ de $X_0(n)$, et on peut montrer en fait que tout endomorphisme de $J_0(n)$ a un multiple (au sens de la loi de groupe) engendré par les opérateurs de Hecke.

Mazur définit alors *le quotient d'Eisenstein* J, qui est le quotient de $J_0(n)$ (n est premier) par l'idéal engendré par les $1 + l - T_l$, pour l premier différent de n, et de $1 - T_n$. Mazur montre ensuite que J possède un nombre fini de points rationnels. La partie suivante de la preuve est géométrique : il étudie le comportement du morphisme $X_0(n) \to J$ sur $\mathbb{Z}$, pour établir qu'un point rationnel de $X_0(n)$ qui n'est pas une pointe correspond à une courbe elliptique rationnelle E dont l'équation se comporte suffisamment bien modulo 3. D'après un « lemme de spécialisation », l'existence d'un point rationnel d'ordre premier $n > 7$ sur une telle courbe elliptique rationnelle se traduit en l'existence d'un point d'ordre n sur la réduction de la courbe elliptique modulo 3. Mais on peut vérifier que n'importe quelle courbe elliptique sur $\mathbb{F}_3$ a au plus 7 points modulo 3.

À travers une étude plus systématique de l'algèbre de Hecke (engendrée par les opérateurs de Hecke), que l'on peut voir agir sur les formes modulaires, les jacobiennes des courbes modulaires, ou même encore l'homologie singulière des courbes modulaires, on peut étudier la torsion de courbes elliptiques définies sur des corps de nombres généraux. On peut citer le résultat de Merel et Oesterlé [30], rendu explicite par Parent [32].

Théorème 3.11 (Parent) *Soit E une courbe elliptique sur un corps de nombres K, de degré d sur $\mathbb{Q}$. Si un point $P \in E(K)$ est d'ordre $q = p^r$ (p nombre premier), alors $q \leq 65(3^d - 1)(2d)^6$ si $p \geq 5$, $q \leq 65(5^d - 1)(2d)^6$ si $p = 3$, et $q \leq 129(3^d - 1)(3d)^6$ si $p = 2$.*

4 Représentations galoisiennes et modularité

4.1 Module de Tate d'une courbe elliptique

Définition *Soient k un corps, p un nombre premier distinct de la caractéristique de k, E une courbe elliptique sur k. Le* module de Tate *de E est $T_pE = \varprojlim E[p^n](\overline{k})$. C'est un $\mathbb{Z}_p$-module libre de rang 2.*

De façon un peu plus concrète, T_pE est l'ensemble des suites $(P_n)_{n\geq 1}$ de points de E définis sur $\overline{k}$, tels que $p \cdot P_{n+1} = P_n$ et P_1 soit de p-torsion sur E. Un entier p-adique z transforme une suite (P_n) en $((z \bmod p^n)P_n)_{n\geq 1}$.

Le module de Tate d'une courbe elliptique E définie sur un corps de nombres K est un $\mathbb{Z}_p$-module libre de rang 2 qui contient beaucoup d'information arithmétique sur E. En effet, il est équipé d'une action naturelle du groupe de Galois absolu G_K de K, c'est-à-dire le groupe d'automorphismes de la clôture algébrique de K. En choisissant une base de T_pE, on obtient un morphisme de groupes $G_K \to GL_2(\mathbb{Z}_p)$, pour n'importe quel nombre premier p. Étudier ce morphisme, c'est à la fois une façon de mieux comprendre G_K et ses représentations, et aussi de comprendre la structure K-rationnelle du groupe de torsion de la courbe elliptique.

4.2 Fonction L de la courbe et modularité des courbes elliptiques

Définition *Soit K un corps de nombres et $\mathfrak{p}$ un idéal premier de son anneau des entiers O_K. Soit $O_{\overline{K}}$ l'anneau des entiers de $\overline{K}$ et soit $\mathfrak{q}$ un idéal premier de $O_{\overline{K}}$ tel que $\mathfrak{q} \cap O_K = \mathfrak{p}$. Le* groupe de décomposition *en $\mathfrak{q}$ est le groupe $G_{\mathfrak{q},K}$ des K-automorphismes σ de $\overline{K}$ tels que $\sigma(\mathfrak{q}) = \mathfrak{q}$. Un $\sigma \in G_{\mathfrak{q},K}$ induit alors un $O_K/\mathfrak{p}$-automorphisme du corps résiduel $O_{\overline{K}}/\mathfrak{q}$ (qui est algébriquement clos).*

Autrement dit, on a un morphisme $G_{\mathfrak{q},K} \to G_{O_K/\mathfrak{p}}$ (le second groupe étant l'adhérence du sous-groupe engendré par le morphisme $x \longmapsto x^{|O_K/\mathfrak{p}|}$, le Frobenius*), et le groupe d'inertie en $\mathfrak{q}$ en est le noyau, noté $I_{\mathfrak{q},K}$. Un* Frobenius *de K en $\mathfrak{p}$ est un élément de $G_{\mathfrak{q},K}$ dont l'image dans $G_{O_K/\mathfrak{p}}$ est le Frobenius.*

Grâce à cette définition, nous pouvons définir la fonction L d'une courbe elliptique.

Proposition 4.12 *Soit E une courbe elliptique sur $\mathbb{Q}$. Soient ℓ, p deux nombres premiers distincts. On choisit un Frobenius en ℓ, noté $F_{\mathfrak{l}}$ pour un certain idéal $\mathfrak{l}$ de $\overline{\mathbb{Z}}$. On considère le sous-module $M_{\mathfrak{l},p}$ de T_pE des points fixes par l'action de $I_{\mathfrak{l},\mathbb{Q}}$. Le polynôme $P_{\ell,E}(X) = \det(I - X(F_{\mathfrak{l}})_{|M_{\mathfrak{l},p}})$ est à coefficients entiers et ne dépend que de ℓ, pas des autres choix (en particulier pas de p).*

Si E est une courbe elliptique sur $\mathbb{Q}$, sa fonction L est définie par

$$L(E,s) = \prod_p P_{p,E}(p^{-s})^{-1}.$$

Cette définition s'inscrit dans un cadre beaucoup plus géneral de définition de fonctions L pour des représentations galoisiennes : on considère le produit de polynômes caractéristiques de Frobenius du groupe de Galois absolu. Mais ici, il y a une recette plus concrète permettant de produire les $P_{p,E}$.

Proposition 4.13 *Soit E une courbe elliptique sur $\mathbb{Q}$. Si un nombre premier impair p est de « bonne réduction » (une condition vérifiée pour tout nombre premier p sauf un nombre fini que l'on sait déterminer), on peut considérer la courbe elliptique E_p qui est la réduction modulo p de E. Alors $P_{p,E} = 1 - a_pX + pX^2$, avec $a_p = 1 + p - |E_p(\mathbb{F}_p)|$.*

Pour les nombres premiers de « mauvaise réduction », il y a un autre critère assez explicite permettant de déterminer $P_{p,E}$, sur lequel nous ne nous attarderons pas.

Théorème 4.14 (Hasse) *On a, dans la situation qui précède, $|a_p| \leq 2\sqrt{p}$.*

En particulier, le produit définissant $L(E,s)$ est absolument convergent pour $D = \{s \in \mathbb{C},\ \mathrm{Re}\, s > \frac{3}{2}\}$.

En réalité, la fonction $L(E,s)$ possède un prolongement entier sur $\mathbb{C}$ et une équation fonctionnelle de la forme $L(E,s) \leftrightarrow L(E,2-s)$. Cela découle du *théorème de modularité*, suggéré par Taniyama puis précisé par Shimura et Weil.

Théorème 4.15 (Wiles, Taylor, Breuil, Conrad, Diamond [37, 14, 12, 11]) *Soit E une courbe elliptique sur $\mathbb{Q}$. Il existe un entier N directement calculable à partir de la courbe (le* conducteur

de la courbe, qui mesure en bref l'étendue de la « mauvaise réduction »), et un morphisme surjectif de courbes sur $\mathbb{Q}$ de $X_0(N)$ sur E. Il existe une forme modulaire $f(z) = \sum_{n=1}^{\infty} a_n e^{2in\pi z}$ de poids 2 pour $\Gamma_0(N)$, propre pour tous les opérateurs de Hecke, telle que $L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ pour tout nombre complexe $s \in D$.

Le membre droit de l'égalité est la *fonction L* de la forme modulaire f. Malgré son apparence complexe, cette quantité est en réalité plus facile à étudier et à manipuler que la fonction L d'une courbe elliptique, parce que f satisfait de bonnes propriétés analytiques (qui permettent par exemple de montrer très facilement que sa fonction L est entière).

Grâce à des travaux de Hellegouarch, Frey [20], puis Serre [35] et Ribet [33], le théorème de modularité implique le célèbre « grand théorème de Fermat ». L'idée de l'argument est la suivante : soit p un nombre premier et considérons trois entiers strictement positifs a, b, c tels que $a^p + b^p = c^p$. On considère alors la courbe elliptique d'équation $y^2 = x(x - a^p)(x + b^p)$ (dite *courbe de Frey*). Serre et Ribet ont montré que la fonction L d'une telle courbe elliptique ne pouvait provenir d'une forme modulaire de poids 2.

On peut aussi déduire ces théorèmes d'un résultat de modularité « modulo p » conjecturé par Serre en 1985 [35] et prouvé par Kharé et Wintenberger.

Théorème 4.16 (Khare, Wintenberger, [22, 23]) *Soient k un corps fini de caractéristique p, ρ une représentation de $G_{\mathbb{Q}}$ sur un k-espace vectoriel de dimension 2. On suppose que la conjugaison complexe agit avec déterminant -1 (la représentation est* impaire*). Alors, on peut attribuer un poids k, un conducteur N et un caractère ϵ à ρ. Il existe une forme modulaire $f(z) = \sum_{n \geq 1} a_n e^{2in\pi z}$ pour $\Gamma_1(N)$ de poids k et de caractère ϵ, propre pour tous les opérateurs de Hecke, à coefficients entiers algébriques, telle que pour tout nombre premier q ne divisant pas pN, un Frobenius en q agit avec trace a_p et déterminant $p^{k-1}\epsilon(p)$ (comme plus haut, ces quantités ne dépendent pas des choix faits pour définir le Frobenius).*

Les théorèmes de modularité ont beaucoup progressé depuis l'article de Wiles. Ainsi, on sait maintenant que les courbes elliptiques sur un corps réel quadratique sont modulaires [19], et des articles plus récents encore [10, 1] (pas encore parus dans des journaux) suggèrent des résultats analogues (avec des définitions de modularité plus élaborées et un énoncé plus faible de *modularité potentielle*) à des corps de nombres beaucoup plus généraux et à des objets de dimension supérieure.

Introduire des courbes de Frey permet en fait de ramener d'autres problèmes arithmétiques à des courbes elliptiques. On peut par exemple étudier de cette façon des équations ternaires ressemblant à celle de Fermat [13]. On peut aussi reformuler l'une des conjectures majeures de la théorie des nombres, la *conjecture ABC* en termes de courbes elliptiques. Ainsi, le deuxième des énoncés suivants implique le premier.

Conjecture 4.17 (Conjecture ABC de Masser-Oesterlé) *Soit $\epsilon > 0$. Il existe une constante K telle que, pour tous entiers non nuls a, b, c premiers entre eux avec $a + b = c$, on ait $\max(|a|, |b|, |c|) \leq K r^{1+\epsilon}$, où r est le radical de abc, c'est-à-dire le produit des nombres premiers distincts divisant abc.*

Conjecture 4.18 (Conjecture du degré modulaire) *Soit $\epsilon > 0$. Il existe $K > 0$ telle que pour toute courbe elliptique E définie sur $\mathbb{Q}$ de conducteur N, il existe un morphisme surjectif de courbes algébriques $X_0(N) \to E$ de degré au plus $KN^{2+\epsilon}$.*

4.3 Une question d'uniformité de Serre

On revient à la représentation galoisienne donnée par les modules de Tate d'une courbe elliptique E sur un corps de nombres K. Serre a montré le résultat suivant.

Théorème 4.19 (Serre, [34]) *Si on considère le produit des représentations pour chaque nombre premier p, on obtient un morphisme de groupes $\mu : G_K \to \prod_p GL_2(\mathbb{Z}_p)$. Si E est* sans multiplication complexe *(une condition facile à vérifier et vraie dans la plupart des cas – cela revient à*

exiger, si E est définie sur $\mathbb{C}$ par le réseau $\mathbb{Z} \oplus \tau\mathbb{Z}$, que τ n'est pas algébrique de degré deux sur $\mathbb{Q}$), alors μ est d'image ouverte. En particulier, comme $\prod_p GL_2(\mathbb{Z}_p)$ est compact, l'image de μ est d'indice fini.

Une conséquence (très faible) de ce théorème est l'énoncé suivant :

Corollaire 4.20 *Soit E une courbe elliptique rationnelle sans multiplication complexe. Il existe un $B_E > 0$ tel que si $p > B_E$ est un nombre premier, l'action de $G_\mathbb{Q}$ sur $E[p]$ soit surjective (c'est-à-dire que tout automorphisme de $E[p]$ est réalisé par l'action d'un élément de $G_\mathbb{Q}$).*

Serre a alors posé la « question d'uniformité » suivante : est-il possible que B_E ne dépende en fait pas de E ? Cette question est actuellement toujours ouverte, même si de nombreux cas ont été résolus.

Le programme de preuve pour les cas connus est le suivant : on connaît les sous-groupes maximaux stricts de $GL_2(\mathbb{F}_p)$. Si l'action $G_\mathbb{Q}$ sur la p-torsion de la courbe elliptique n'est pas surjective, alors son image est contenue (à conjugaison près) dans un sous-groupe maximal strict de $GL_2(\mathbb{F}_p)$. On peut définir une courbe modulaire, qui paramètre (en un certain sens) les courbes elliptiques pour lesquelles l'action de Galois est contenue dans chacun de ces sous-groupes, et en construire une version algébrique. Il reste alors à trouver les points rationnels de ces courbes qui ne sont pas des pointes ou des courbes à multiplication complexe.

Les sous-groupes maximaux de $GL_2(\mathbb{F}_p)$ sont de type suivant (à conjugaison près) :

— des sous-groupes exceptionnels, d'image projective contenue dans S_4, A_4 ou A_5.

— le sous-groupe de Borel, c'est-à-dire le groupe des matrices triangulaires supérieures.

— le normalisateur Γ_s d'un sous-groupe de Cartan déployé constitué des matrices diagonales et anti-diagonales.

— le normalisateur Γ_{ns} d'un sous-groupe de Cartan non déployé, engendré par $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ et les $\begin{bmatrix} a & rb \\ b & a \end{bmatrix}$, avec $a, b \in \mathbb{F}_p$ variables non tous deux nuls, et $r \in \mathbb{F}_p$ fixé qui n'est pas un carré.

Serre avait déjà résolu le cas des sous-groupes exceptionnels, comme expliqué au début de [28]. Le travail de Mazur sur les isogénies de courbes elliptiques montre que le cas du sous-groupe de Borel est exclu si $p > 37$, car les points rationnels sur $X_0(p)$ (pour $p > 37$) qui ne soient pas des pointes sont des courbes elliptiques à multiplication complexe. En effet, si l'action de $G_\mathbb{Q}$ est contenue dans un sous-groupe de Borel, la courbe elliptique possède un sous-groupe cyclique d'ordre p stable par $G_\mathbb{Q}$, et donc une isogénie rationnelle d'ordre p vers son quotient par ce sous-groupe.

Comment construire des courbes modulaires correspondant aux normalisateurs des sous-groupes de Cartan ? Dans le cas déployé, on s'intéresse au quotient $Y_s(p) = \Gamma_s(p)\backslash\mathbb{H}$, où $\Gamma_s(p)$ est le sous-groupe des matrices de $SL_2(\mathbb{Z})$ dont la réduction modulo p est diagonale ou anti-diagonale. Si τ représente la paire $(\mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z}, \{1/p\mathbb{Z}, \tau/p\mathbb{Z}\})$, $Y_s(p)$ paramètre les paires $(E, \{A, B\})$, où E est une courbe elliptique complexe et A, B sont deux sous-groupes cycliques d'ordre p distincts. Un point rationnel de cette courbe correspond donc à une courbe elliptique rationnelle E munie de deux sous-groupes cycliques $A, B \subset E[p]$ distincts tels que l'action de $G_\mathbb{Q}$ préserve la paire $\{A, B\}$, et cela revient à exiger que l'image de $G_\mathbb{Q}$ soit dans Γ_s.

Dans le cas non-deployé, on peut considérer, comme dans [16], l'ensemble des classes d'isomorphisme des (E, ϕ), où E est une courbe elliptique et ϕ est un endomorphisme de $E[p]$ tel que $\phi^2 = r$, où r est un élément fixé de $\mathbb{F}_p\backslash\mathbb{F}_p^2$, qui peut s'écrire comme $Y_{ns}(p) = \Gamma_{ns}(p)\backslash\mathbb{H}$, où $\Gamma_{ns}(p)$ est le sous-groupe de $SL_2(\mathbb{Z})$ constitué des matrices dont la réduction modulo p est un $\begin{bmatrix} a & rb \\ b & a \end{bmatrix}$. La courbe modulaire dont on cherche les points rationnels est alors le quotient $Y_{ns}(p)^+$ de $Y_{ns}(p)$ par l'involution $(E, \phi) \longmapsto (E, -\phi)$.

Déterminer la réponse à la question d'uniformité dans le cas des sous-groupes de Cartan est plus difficile. Les travaux de Bilu, Parent et Rebolledo dans [8] (qui montre l'existence d'une borne uniforme) puis [9] (pour $p \geq 11$ distinct de 13) prouvent le cas déployé de la conjecture. Le cas $p = 13$ a finalement été complètement étudié dans [3] en utilisant la méthode de Chabauty-Kim quadratique (la jacobienne de la courbe modulaire correspondante a pour genre $g = 3$ et un groupe de points rationnels de rang $r = 3$; la méthode de Chabauty originale requiert que $r < g$ pour pouvoir fonctionner).

Le cas non déployé reste ouvert. Le théorème de Faltings assure qu'à chaque niveau assez grand, il y a au plus un nombre fini de courbes elliptiques rationnelles pour lesquelles l'action de Galois sur la p-torsion est contenue dans le normalisateur d'un sous-groupe de Cartan non-déployé. Plus récemment, Dogra et Le Fourn [16] ont montré que la méthode de Chabauty-Kim quadratique pouvait s'appliquer à la courbe modulaire $X_{ns}^{+}(p)$ (qui est la compactification de $Y_{ns}^{+}(p)$ que nous avons déjà mentionnée), et en particulier donnent une borne calculable pour le nombre de points, mais c'est insuffisant.

En fait, les méthodes utilisées dans les autres cas par Mazur, Serre, et Bilu-Parent-Rebolledo sont d'inspiration ressemblant la méthode de Chabauty, et requièrent pour fonctionner, d'après des conjectures à la Birch et Swinnerton-Dyer, la non-annulation de la fonction L de la jacobienne de la courbe, ou au moins d'un de ses facteurs. Mais dans le cas dans le cas non déployé, tous les facteurs de cette fonction L s'annulent. Les auteurs de [16] montrent qu'il y a suffisamment de facteurs de la fonction L qui s'annulent à l'ordre exactement 1 pour pouvoir appliquer une version raffinée de la méthode de Chabauty.

Références

[1] P. Allen, F. Calegari, A. Caraiani, T. Gee, D. Helm, B. Le Hung, J. Newton, P. Scholze, R. Taylor, and J. Thorne. Potential Automorphy over CM fields. Soumis.

[2] J. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points, I : p -adic heights. *Duke Math. J.*, 167(11) :1981–2038, 08 2018.

[3] J. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty–Kim for the split Cartan modular curve of level 13. *Ann. of Math.*, 189(3) :885–944, 2019.

[4] M. Bhargava and A. Shankar. The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1, 2013.

[5] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. of Math.*, 181(1) :191–242, 2015.

[6] M. Bhargava and A. Shankar. Binary quartic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. of Math.*, 181(2) :587–621, 2015.

[7] M. Bhargava, C. Skinner, and W. Zhang. A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture, 2014.

[8] Y. Bilu and P. Parent. Serre's uniformity problem in the split Cartan case. *Ann. of Math.*, 173(1) :569–584, 2011.

[9] Y. Bilu, P. Parent, and M. Rebolledo. Rational points on $X_0^{+}(p^r)$. *Ann. Inst. Fourier (Grenoble)*, 63(3) :957–984, 2013.

[10] G. Boxer, F. Calegari, T. Gee, and V. Pilloni. Abelian Surfaces over totally real fields are potentially modular. Soumis.

[11] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the Modularity of Elliptic Curves Over $\mathbf{Q}$: Wild 3-Adic Exercises. *J. Amer. Math. Soc.*, 14, 2001.

[12] B. Conrad, F. Diamond, and R. Taylor. Modularity of certain potentially Barsotti-Tate Galois representations. *J. Amer. Math. Soc.*, 12(2) :521–567, 1999.

[13] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's Last Theorem. *J. Reine Angew. Math.*, 490 :81–100, 1997.

[14] F. Diamond. On deformation rings and Hecke rings. *Ann. of Math.*, 144(1) :137–166, 1996.

[15] V. Dimitrov, Z. Gao, and P. Habegger. Uniformity in Mordell-Lang for curves. *Ann. of Math.*, page À paraître.

[16] N. Dogra and S. Le Fourn. Quadratic Chabauty for modular curves and modular forms of rank one, 2019.

[17] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3) :349–366, 1983.

[18] G. Faltings. Erratum : Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 75(2) :381, 1984.

[19] N. Freitas, B. Le Hung, and S. Siksek. Elliptic curves over real quadratic fields are modular. *Invent. Math.*, 201(1) :159–206, 2015.

[20] G. Frey. On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2. In J. Coates and S-T. Yau, editors, *Elliptic curves, modular forms and Fermat's Last Theorem*, pages 79–98. International Press, Cambridge, 1997.

[21] B. Gross and D. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2) :225–320, 1986.

[22] C Khare and J.-P. Wintenberger. Serre's modularity conjecture (I). *Invent. Math.*, 178(3) :485–504, 2009.

[23] C Khare and J.-P. Wintenberger. Serre's modularity conjecture (II). *Invent. Math.*, 178(3) :505–586, 2009.

[24] Z. Klagsbrun, T. Sherman, and J. Weigandt. The Elkies curve has rank 28 subject only to GRH. *Math. Comp.*, 88(316) :837–846, 2019.

[25] V Kolyvagin. Finiteness of $E(\mathbf{Q})$ and $\text{Ø}(E, \mathbf{Q})$ for a subclass of Weil curves. *Mathematics of the USSR-Izvestiya*, 32(3) :523–541, 1989.

[26] L. Kühne. Equidistribution in Families of Abelian Varieties and Uniformity, 2021.

[27] H. W. Lenstra. Factoring integers with elliptic curves. *Ann. of Math.*, 126(3) :649–673, 1987.

[28] B. Mazur. Modular curves and the Eisenstein ideal. *Publ. Math. Inst. Hautes Études Sci.*, 47 :33–186, 1977.

[29] B. Mazur and D. Goldfeld. Rational isogenies of prime degree. *Invent. Math.*, 44(2) :129–162, 1978.

[30] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124 :437–449, 1996.

[31] L. Mordell. On the rational solutions of the indeterminate equation of the third and fourth degrees. *Proc. Camb. Phil. Soc.*, 21 :179–192, 1922.

[32] P. Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 1999(506) :85–116, 1999.

[33] K. A. Ribet. On modular representations of $\overline{\mathbf{Q}}/\mathbf{Q}$ arising from modular forms. *Invent. Math.*, 100(1) :431–476, 1990.

[34] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math*, 15(4) :259–331, 1971.

[35] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1) :179–230, 1987.

[36] J. B. Tunnell. A classical Diophantine problem and modular forms of weight 3/2. *Invent. Math.*, 72(2) :323–334, 1983.

[37] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. of Math.*, 141(3), 1995.