RAPPORT DE STAGE DE DEUXIÈME ANNÉE : PROBLÈME DU NOMBRE DE CLASSES 1

ELIAS CAEIRO

Table des matières

Déroulement du stage

J'ai effectué mon stage à l'université de McGill à Montréal de début mars à début juillet 2024, sous la direction d'Henri Darmon. Je les remercie pour m'avoir accueilli pendant ces 4 mois.

Toutes les deux semaines, le jeudi, avaient lieu deux exposés d'une heure et demie dans le cadre du séminaire de théorie de nombres Québec-Vermont (QVNTS), entre lesquels tous les participants étaient conviés à déjeuner dans un restaurant de raviolis chinois ! Cela m'a permis de m'introduire à un large éventail de problèmes contemporains de recherche en théorie des nombres. De plus, comme Henri a de nombreux étudiants, il organisait aussi son propre séminaire hebdomadaire le jeudi, puis il déjeunait avec ses étudiants les semaines où QVNTS n'avait pas lieu. Cela m'a permis de bien m'intégrer et de garder un contact hebdomadaire avec mon encadrant. Henri était également toujours disposé à libérer du temps pour discuter de l'avancée du stage avec moi, répondre à mes questions souvent bien naïves, et s'assurer que mon stage se passe bien ; je ne saurais assez l'en remercier.

J'ai travaillé sur le projet initial du stage de mars à avril, et en mai nous avons rédigé et soumis l'article [CD24]. En juin, j'ai assisté à des conférences de théorie des nombres sur des thèmes variés, et ai eu le privilège de donner deux exposés sur cet article : un à l'institut Fields de Toronto à l'occasion de la seizième conférence CNTA, et un à l'université d'Édimbourg à l'occasion d'un colloque sur le douzième problème de Hilbert.

Il va sans dire que tout cela aurait été impossible sans le soutien constant de mon encadrant Henri Darmon. Je le remercie chaleureusement pour m'avoir offert cette formidable expérience de découverte arithmétique. Sa générosité et son enthousiasme frappants seront sans aucun doute sources d'inspiration pour moi durant de longues années à venir.

Enfin, je souhaiterais également exprimer ma gratitude envers mon tuteur Gaëtan Chenevier pour m'avoir mis en contact avec Henri Darmon et pour m'avoir soutenu avant le début du stage.

Introduction

On sait depuis Kummer que les anneaux d'entiers de corps de nombres ne sont pas toujours factoriels. En d'autres termes, si K est une extension finie de $\mathbb{Q}$, il se peut que son anneau des entiers $\mathcal{O}_K$ ne vérifie pas la propriété de la factorisation unique [1]. Kummer montra cependant que tout idéal fractionnaire [2] non nul de $\mathcal{O}_K$ peut s'écrire de manière unique (à réordonnement des facteurs près) comme un produit d'idéaux premiers ; on dit que $\mathcal{O}_K$ est un *anneau de Dedekind*. On peut ainsi définir le quotient

$$\mathrm{Cl}(K) := I_K/P_K$$

où I_K est le groupe (pour la multiplication) des idéaux fractionnaires non nuls de K, et P_K est le sous-groupe des idéaux principaux. Il s'agit d'un groupe abélien fini mesurant à quel point $\mathcal{O}_K$ est loin d'être factoriel : il est trivial si et seulement si $\mathcal{O}_K$ est factoriel. Son cardinal h_K est appelé le nombre de classes de K.

Il est naturel de se demander s'il existe une infinité de corps de nombres K de nombre de classes 1, c'est-à-dire pour lesquels $\mathcal{O}_K$ est factoriel. Cette question reste aujourd'hui très ouverte, mais il semble particulièrement intéressant de commencer par le cas où K est un corps quadratique, c'est-à-dire de la forme $\mathbb{Q}(\sqrt{D})$ pour un unique entier sans facteur carré D. Dans ce cas, on conjecture que la réponse est positive si $D > 0$ et on sait qu'elle est négative si $D < 0$. La détermination de l'ensemble des entiers sans facteur carré $D < 0$ tels que $h_{\mathbb{Q}(\sqrt{D})} = 1$ est communément appelée le « problème du nombre de classes 1 » et a fait l'objet de nombreux travaux lors du vingtième siècle, jusqu'à sa résolution par Heegner [He52] (voir aussi [St69]), Baker [Ba66] et Stark [St69] dans les années 60.

Théorème 1 (Heegner-Baker-Stark)**.** *Soit $D < 0$ un entier négatif sans facteur carré. Alors, $h_{\mathbb{Q}(\sqrt{D})} = 1$ si et seulement si*

$$-D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$

Les démonstrations données par Heegner, Baker et Stark reposent toutes sur la théorie de la multiplication complexe. Le projet de mon stage était d'obtenir un analogue de ce théorème à partir d'un analogue conjectural de la multiplication complexe au cas des discriminants positifs, appelée « multiplication réelle », développée par mon encadrant Henri Darmon et ses collaborateurs depuis les années 2000. On redonne ainsi une démonstration, conditionnelle mais très directe, du résultat suivant, démontré par des méthodes entièrement différentes.

1. Càd que tout élément peut s'écrire d'une unique manière comme un produit d'éléments premiers (ou irréductibles), à multiplication par une unité et à réordonnement des facteurs près.

2. Càd un sous $\mathcal{O}_K$-module M de K tel qu'il existe $N \in \mathbb{N}^*$ pour lequel $M \subseteq N^{-1}K$.

Théorème 2 (Biró [Bi03a, Bi03b], Byeon–Kim–Lee [BLK07])**.** *Soit D un entier sans facteur carré de la forme n^2+4, n^2-4, ou $4n^2+1$, pour un certain $n \in \mathbb{N}$. Alors, $h_{\mathbb{Q}(\sqrt{D})} = 1$ si et seulement si*

$$D \in \{-3, 5, 13, 17, 21, 29, 37, 53, 77, 101, 117, 179, 197, 437, 677\}.$$

Il est remarquable que les théorèmes 1 et 2 puissent se démontrer (en partie conjecturalement) en faisant intervenir des courbes elliptiques, et c'est ce que nous nous proposons d'expliquer ici.

L'organisation du rapport est la suivante. Dans la section 1, on explique cette dichotomie derrière le cas $D > 0$ et le cas $D < 0$, et pourquoi on pourrait s'attendre aux théorèmes 1 et 2. Dans la section 2, on introduit les courbes elliptiques et la courbe modulaire. Dans la section 3, on rappelle la théorie de la multiplication complexe et on explique comment elle a permis la résolution du problème du nombre de classes 1. Dans la section 4, on fait le lien entre multiplication complexe et courbes modulaires. Dans la section 5, on présente la théorie conjecturale de multiplication réelle de Darmon [Da01], et on explique comment en déduire le théorème 2. Enfin, dans la dernière section 6, on explique comment adapter cette démonstration du théorème 2 pour donner une nouvelle démonstration du théorème 1. Une annexe présente les notions de base de géométrie algébrique utilisées. On a tâché d'inclure de nombreuses références pour aider le lecteur intéressé à approfondir les notions présentées.

On pourra notamment consulter les références [Co78, Co13] pour plus de détails sur l'arithmétique des corps quadratiques, [Si09, Si94] pour l'arithmétique des courbes elliptiques, [Da04] pour tout le texte, [La87] pour la théorie de la multiplication complexe, [Se97, Appendix A] pour la fin de la section 3, [CD24] pour la section 5 et [Ca] pour la section 6.

1. Théorème de Siegel

Un *ordre quadratique* est un sous-anneau d'un corps quadratique qui est aussi de rang 2 comme $\mathbb{Z}$-module. Ceux-ci sont en bijection avec les *discriminants*, c'est-à-dire les entiers $D \in \mathbb{Z}$ qui sont congrus à 0 ou 1 modulo 4 et ne sont pas des carrés parfaits. Cette bijection associe a un discriminant D l'ordre

$$\mathcal{O}_D = \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right]$$

et à un ordre $\mathcal{O}$ son discriminant $D_{\mathcal{O}} = \det(\mathrm{Tr}(e_i e_j)_{i,j=1,2})$, où $\mathcal{O} = \mathbb{Z}e_1 + \mathbb{Z}e_2$ et $\mathrm{Tr} : K \to \mathbb{Q}$ est la trace du corps des fractions K de $\mathcal{O}$. Par exemple, si d est un entier sans facteur carré, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ est de discriminant d si $d \equiv 1 \pmod 4$ et $4d$ sinon.

Le *conducteur* d'un ordre $\mathcal{O} = \mathcal{O}_D$ est le plus grand $f \in \mathbb{N}$ tel que $f^2 \mid D$ et $D_0 = D/f^2$ est encore un discriminant. Un discriminant est dit *fondamental* s'il est de conducteur 1 ; cela revient à ce que l'ordre soit maximal, i.e. soit l'anneau des entiers de son corps des fractions.

À un corps quadratique K de discriminant $D = D_{\mathcal{O}_K}$ est associé un caractère de Dirichlet χ_D de conducteur D, induit par le symbole de Kronecker $\left(\frac{\cdot}{D}\right)$ [3]. La formule du nombre de classes de Dirichlet [Ne99, Chapter VII, Corollary 5.11] affirme alors que

$$L(1, \chi_D) = \alpha \frac{R_D h_D}{\sqrt{|D|}}$$

où $\alpha \in \left[\frac{1}{2}, 4\right]$ [4] et R_D est le *régulateur* de $\mathcal{O}_D$, qu'on peut définir comme le volume du groupe des unités $\mathcal{O}_D^\times$ quotienté par sa torsion. Explicitement, R_D vaut 1 si $D < 0$, et $\log|\varepsilon_D|$ si $D > 0$, où ε_D est *l'unité fondamentale* de $\mathcal{O}_D$, c'est-à-dire un générateur du groupe abélien $\mathcal{O}_D^\times/\{\pm 1\} \simeq \mathbb{Z}$.

Il transparaît de ce théorème et de la philosophie de l'hypothèse de Riemann que $R_D h_D$ devrait être de l'ordre de grandeur de $\sqrt{D}$. C'est essentiellement ce que démontra Siegel (voir [Go74] pour une démonstration analytique d'une page).

Théorème 3 (Siegel [Si68])**.** *Soit D un discriminant fondamental. Lorsque $|D| \to +\infty$, on a*

$$\log(R_D h_D) \sim \log\sqrt{|D|}.$$

3. Par exemple, si $D \equiv 1 \pmod 4$ et m est premier avec D, on a $\chi_D(m) = 1$ si m est un carré modulo D et $\chi_D(m) = -1$ sinon.

4. La formule exacte est $\alpha = 2^r(2\pi)^s/w$ où w est le nombre de racines de l'unité de K (c'est-à-dire 4 si $D = -4$, 6 si $D = -3$ et 2 sinon) et (r, s) vaut $(2, 0)$ si $D > 0$ et $(0, 1)$ si $D < 0$.

Malheureusement, la démonstration de Siegel n'est pas effective car Siegel ne disposait pas de région sans zéros de $L(s, \chi_D)$ suffisamment bonne et fut embêté par l'existence potentielle de ce qu'on appelle aujourd'hui les *zéros de Siegel*. Le théorème ne permet donc pas de résoudre le problème du nombre de classes 1, mais il explique pourquoi il n'y a qu'un nombre fini de discriminants tels que dans les théorèmes 1 et 2 : si $D < 0$, son régulateur vaut 1, et si D est de la forme $n^2 \pm 4$ ou $4n^2 + 1$, il admet l'unité évidente $\varepsilon = \frac{n+\sqrt{n^2 \pm 4}}{2}$ ou $\varepsilon = n + \sqrt{4n^2 + 1}$. Dans tous les cas $R_D = O(\sqrt{D})$ et on a donc $\log(h_D) \sim \log \sqrt{|D|} \to +\infty$.

2. Courbes elliptiques et modulaires

La démonstration du problème du nombre de classes 1 telle que nous allons l'expliquer est très géométrique. Le lecteur trouvera ainsi un rappel de la notion de variété algébrique (géométriquement réduite) sur un corps k en annexe.

Commençons par définir les courbes elliptiques.

Définition 4 (Groupe algébrique)**.** *Un* groupe algébrique *sur un corps k est une variété algébrique G sur k muni d'un point rationnel $e \in X(k)$ ainsi que d'un morphisme $m : G \times G \to G$ munissant $\overline{G} = G_{\overline{k}}$ d'une structure de groupe pour lequel e est l'élément neutre.*

Par exemple, le groupe additif $\mathbb{G}_a := \mathbb{A}^1_k \simeq k$ muni de l'addition et le groupe multiplicatif $\mathbb{G}_m := \mathbb{A}^1_k \setminus \{0\} \simeq k^\times$ muni de la multiplication sont des groupes algébriques. Il en va de même du groupe général linéaire GL_n, vu par exemple comme ouvert de $\mathbb{A}^{n^2}_k$ défini par l'inéquation $\det \neq 0$.

Si K est une extension quadratique de k, le groupe des éléments de norme 1 de K est également un groupe algébrique sur k, comme on peut le voir en le plongeant dans $\mathrm{SL}_{2,k}$ en choissant une base. Il devient isomorphe à $\mathbb{G}_m$ sur K : on dit que c'est une *tordue quadratique* de $\mathbb{G}_m$. Par exemple, pour $k = \mathbb{R}$ et $K = \mathbb{C}$, le tore $S^1 \simeq \mathbb{R}/\mathbb{Z}$ est un groupe algébrique réel.

Définition 5 (Variété abélienne)**.** *Une* variété abélienne *est une variété projective lisse connexe qui est aussi un groupe algébrique. Une* courbe elliptique *est une variété abélienne de dimension* 1.

Sur un corps algébriquement clos, les seuls groupes algébriques lisses connexes de dimension 1 sont les courbes elliptiques, $\mathbb{G}_a$ et $\mathbb{G}_m$. Sur un corps parfait, la théorie de la descente montre que les seuls groupes algébriques lisses de dimension 1 sont les courbes elliptiques, $\mathbb{G}_a$, $\mathbb{G}_m$ et ses tordues quadratiques. [5]

5. En effet, on a $\mathrm{Aut}(\mathbb{G}_{m,\overline{k}}) = \{\pm 1\}$ (où Aut désigne le groupe d'automorphismes de groupes algébriques) et, si k est parfait, $\mathrm{Aut}(\mathbb{G}_{a,\overline{k}}) = \overline{k}^\times$. Ainsi, les tordues de $\mathbb{G}_{a,k}$ s'identifient (voir annexe) à

On peut montrer [Si09, Chapter III, Proposition 3.1] [6] à l'aide du théorème de Riemann-Roch que toute courbe elliptique peut s'écrire comme cubique plane $y^2 = x^3 + ax + b$ (avec comme élément neutre le point à l'infini $e = [0 : 1 : 0] \in \mathbb{P}^2_k$), où le polynôme $f(x) = x^3 + ax + b$ est sans racine multiple, i.e. son discriminant $\Delta = -4a^3 - 27b^2$ est non nul. Une telle équation est appelée *équation de Weierstrass*. Par ailleurs, la loi de groupe d'une variété abélienne est automatiquement commutative. L'*invariant* j d'une courbe elliptique E sous forme de Weierstrass est $j(E) = \frac{-4 \cdot 1728 a^3}{\Delta}$, il ne dépend pas de l'équation de Weierstrass choisie. Sur un corps algébriquement clos k, il caractérise uniquement la classe d'isomorphisme de E et induit une bijection entre les classes d'isomorphisme de courbes elliptiques et $\mathbb{A}^1_k$ ([Si09, Chapter III, Proposition 1.4]).

Sur $\mathbb{C}$, l'uniformisation complexe via la fonction $\wp$ de Weierstrass [Si09, Chapter VI] montre que les courbes elliptiques peuvent s'écrire, en tant que surfaces de Riemann et groupes de Lie, comme quotients de $\mathbb{C}$ par un réseau Λ. Quitte à effectuer une homothétie, on peut supposer Λ de la forme $[1, \tau] := \mathbb{Z} + \tau\mathbb{Z}$ pour $\tau \in \mathfrak{H}$, et l'invariant j de $E = \mathbb{C}/\Lambda$ est alors $j(\tau)$ où $j : \mathfrak{H} \to \mathbb{C}$ est l'invariant j holomorphe usuel.

Un morphisme de courbes elliptiques est un morphisme de variétés envoyant l'élément neutre sur l'élément neutre, c'est alors automatiquement un morphisme de groupes. Deux courbes elliptiques sont dites *isogènes* s'il existe un morphisme non nul entre elles (une « isogénie »).

Un des intérêts principaux des courbes elliptiques en arithmétique est qu'elles sont sources de *représentations galoisiennes*. En effet, si E est une courbe elliptique sur $\mathbb{Q}$ et $N \geq 1$ est un entier, on peut considérer sa N-torsion $E[N]$. Grâce à l'uniformisation complexe, on sait que $E[N]$ est isomorphe à $(\mathbb{Z}/N\mathbb{Z})^2$ comme groupe abélien. Or, on sait également que le groupe de Galois $G_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ agit par automorphismes dessus, et on obtient ainsi une représentation $G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ après choix d'une base de la N-torsion.

Il existe une courbe algébrique paramétrisant les courbes elliptiques avec représentation galoisienne triviale : la courbe modulaire. On trouvera une démonstration complète du résultat suivant, dans un autre langage, dans [DR73] (ou une construction dans le même langage mais sans démonstration de la proposition dans [DS05, Chapter 7]).

Proposition 6. *Pour tout $N \geq 1$, il existe une courbe lisse et affine $Y(N)$ sur $\mathbb{Q}(\mu_n)$ telle que, pour tout corps k contenant $\mathbb{Q}(\mu_n)$, les k-points $Y(N)(k)$ s'identifient canoniquement aux classes de $\overline{k}$-isomorphisme de paires $(E, (P, Q))$ où E est une courbe elliptique sur k et (P, Q) est une base de $E[N](k)$ (une « structure de niveau N »).*

$H^1(G_k, \overline{k}^\times) = 0$ (d'après le théorème 90 de Hilbert [Ne99, Chapter IV, Proposition 3.8]) tandis que celles de $\mathbb{G}_{m,k}$ s'identifient à $H^1(G_k, \{\pm 1\}) = \mathrm{Hom}(G_k, \{\pm 1\})$, c'est-à-dire aux extensions quadratiques de k.

6. Une courbe elliptique est bien de genre 1 puisque son fibré cotangent est trivial (par homogénéité) donc ses sections globales sont de dimension $g = 1$.

Esquisse de démonstration. Par souci de simplicité, on considérera plutôt le problème de module suivant : une courbe $Y_0(N)$ paramétrisant les paires (E, H) où $H \subseteq E[N](k)$ est un sous-groupe cyclique d'ordre N. Il revient au même de considérer les morphismes $E \to E' := E/H$ qui sont des N-isogénies cycliques. La construction de $Y_0(N)$ est la suivante. Considérons la fonction analytique $j : \mathfrak{H} \to \mathbb{C}$. L'extension $\mathbb{Q}(j(\tau), j(N\tau))|\mathbb{Q}(j(\tau))$ est galoisienne de groupe de Galois $\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(N) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/B$ où B est l'ensemble des matrices triangulaires supérieures modulo N et $\Gamma_0(N)$ est la préimage de B par l'application de réduction modulo N. Le polynôme minimal de $j(N\tau)$ est

$$\Phi_N(x, j) = \prod_{\alpha \in M_2(\mathbb{Z})/\,\mathrm{SL}_2(\mathbb{Z}), \det(\alpha) = N} x - j \circ \alpha.$$

Alors, $Y_0(N)$ est la courbe affine plane définie par l'équation $\Phi_N(x, y) = 0$. En effet, comme toute courbe elliptique et structure de niveau sont définis sur un corps de type fini [7], on peut supposer k plongé dans $\mathbb{C}$. Alors, un k-point $(x, y) \in k^2$ de $Y_0(N)$ correspond à un $\tau \in \mathfrak{H}$ tel que $j(\tau) = x$ et $j(\alpha\tau) = y$. Le point τ correspond alors à la courbe E et le point $\alpha\tau$ à la courbe E'. L'isogénie cyclique $E \to E'$ correspond alors à la multiplication par $c\tau + d$, où $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Voir [La87, Chapter 5] pour plus de détails. □

Remarque 7. En particulier, $Y_0(N)$ est déjà définie sur $\mathbb{Q}$, pas seulement sur $\mathbb{Q}(\mu_n)$. En général, on dispose d'un critère simple pour calculer le corps de définition d'une courbe modulaire (sur laquelle elle reste solution du problème du module) à l'aide de la notion de « pointe », que l'on n'a pas introduite.

Remarque 8. Lorsque $N \geq 2$, les points de $Y(N)$ correspondent aux classes d'isomorphisme sur k de courbes elliptiques avec structure de niveau N, c'est un espace de module *fin*. La raison est que le problème de module alors considéré est *rigide* : deux courbes elliptiques avec structure de niveau sont isomorphes sur $\overline{k}$ si et seulement si elles le sont sur k. Lorsque $N = 1$, il n'existe pas de tel espace de module car le problème de module n'est plus rigide : une courbe elliptique peut avoir des tordues non triviales. Il ne peut donc pas exister d'espaces de module fin : la courbe $Y(1) = \mathbb{A}^1_k$ est alors seulement un espace de module *grossier* et il faut introduire la notion de « champ » pour obtenir un espace de module fin.

Remarque 9. On peut montrer que le corps des fonctions méromorphes de la surface de Riemann $\mathfrak{H}/\Gamma_0(N)$, c'est-à-dire les fonctions $\Gamma_0(N)$-invariantes sur $\mathfrak{H}$, est $\mathbb{C}(j(\tau), j(N\tau))$. En fait, $\mathfrak{H}/\Gamma_0(N) \simeq Y_0(N)(\mathbb{C})$: cela correspond à l'application $\tau \mapsto (\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z}), \langle \tau/N \rangle)$. Lorsque $N = 1$, $Y_0(1) = \mathbb{A}^1_k$ correspond à l'isomorphisme $\mathfrak{H}/\,\mathrm{SL}_2(\mathbb{Z}) \xrightarrow{j} \mathbb{C}$.

7. Par exemple le corps engendré par les coefficients d'une équations de Weierstrass et les coordonnées de la structure de niveau.

La catégorie des variétés quasi-projectives sur un corps k admet les quotients par des groupes finis d'automorphismes [8]. Explicitement, si X est affine et correspond à l'algèbre de fonctions A, X/G correspond à l'algèbre de fonctions invariantes A^G. De plus, on peut montrer que, en tant qu'espace topologique, X/G est le quotient de l'espace topologique X par le groupe d'automorphismes G. En particulier, un point rationnel de X/G correspond à un point géométrique x (modulo l'action de G) tel que $G_k \cdot x \subseteq G \cdot x$.

Le groupe $G = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ agit par automorphismes sur $Y(N)$ en agissant sur la base (P, Q). Si H est un sous-groupe de G, l'observation précédente montre que $Y_H := Y(N)/H$ paramétrise des courbes elliptiques avec représentation galoisienne prescrite.

Théorème 10. *Pour tout sous-groupe $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, il existe une courbe Y_H définie sur $\mathbb{Q}(\mu_n)$ paramétrisant les courbes elliptiques E dont la représentation galoisienne de niveau N est à image dans H.*

Plus formellement, si k est une extension de $\mathbb{Q}(\mu_n)$, $Y_H(k)$ s'identifie aux paires $(E, (P, Q))$ où E est une courbe elliptique sur k et (P, Q) est une structure de niveau N telle que la représentation

$$\rho_{E,N} : G_k \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

est à image dans H, modulo la relation d'équivalence suivante : deux paires $(E_1, S_1), (E_2, S_2)$ sont identifiées s'il existe un isomorphisme $\varphi : E_1 \to E_2$ sur $\overline{k}$ tel que $\varphi(S_1)$ diffère de $\varphi(S_2)$ par un élément de H.

Dans la suite, on n'utilisera pas Y_H mais plutôt une compactification canonique X_H [9] paramétrisant cette fois-ci des courbes elliptiques « généralisées ». Les points de $X \setminus Y$ sont appelés des « pointes ».

3. Multiplication complexe

Une courbe elliptique sur un corps k de caractéristique 0 a un anneau d'endomorphisme qui est, soit réduit à $\mathbb{Z}$ (tous les endomorphismes sont de la forme $x \mapsto nx$ pour un $n \in \mathbb{Z}$), soit un ordre quadratique imaginaire (c'est-à-dire un ordre quadratique de discriminant négatif). En effet, puisque toute variété algébrique et tout endomorphisme sont définis sur un corps de type fini, on peut supposer k de type fini sur $\mathbb{Q}$. Il se plonge alors dans $\mathbb{C}$ et on s'est ainsi ramenés au cas $k = \mathbb{C}$. Mais alors, toute courbe elliptique E est de la forme

8. Au sens où un morphisme $X/G \to Y$ correspond à un morphisme $X \to Y$ qui envoie les éléments de G sur l'identité.

9. Pouvant par exemple être définie comme la normalisation de $X(1) := \mathbb{P}^1_k$ dans Y_H via le morphisme fini $Y_H \to Y(1) \subseteq X(1)$, ou, de manière équivalente, comme l'unique courbe projective lisse sur $\mathbb{Q}$ de même corps des fonctions que Y_H.

$E_\tau := \mathbb{C}/[1,\tau]$ pour un $\tau \in \mathfrak{H}$ et $\mathrm{End}(E)$ s'identifie [10] à

$$\{\alpha \in \mathbb{C} \mid \alpha[1,\tau] \subseteq [1,\tau]\}.$$

En particulier, si $\mathrm{End}(E)$ est plus grand que $\mathbb{Z}$, il existe un $\alpha = u + v\tau$ avec $u, v \in \mathbb{Z}$, $v \neq 0$ tel que $\alpha\tau \in [1,\tau]$ et donc τ est quadratique (et imaginaire car il appartient à $\mathfrak{H}$, on dit que τ est un point « CM »). Réciproquement, si τ est CM, $\mathrm{End}(E)$ s'identifie à l'ordre quadratique

$$\mathcal{O}_\tau := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) - \{0\} \;\middle|\; \frac{a\tau + b}{c\tau + d} = \tau \right\} \cup \{0\}$$

plongé dans le corps quadratique imaginaire $\mathbb{Q}(\tau)$ via [11] $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto c\tau + d$.

Définition 11 (Multiplication complexe)**.** *Une courbe elliptique E sur un corps k de caractéristique 0 est à* multiplication complexe *par l'ordre quadratique $\mathcal{O}$ si $\mathrm{End}(E) \simeq \mathcal{O}$. Elle est à multiplication complexe si elle est à multiplication complexe pour un certain ordre quadratique, i.e. $\mathrm{End}(E) \neq \mathbb{Z}$.*

Afin d'énoncer dans toute sa généralité le lien entre courbes elliptiques CM et le problème du nombre de classes 1, étendons la définition du groupe de classes aux ordres quadratiques non maximaux. Dans ce cas, $\mathcal{O}$ n'est plus un anneau Dedekind et les idéaux fractionnaires (non nuls) ne sont alors plus tous inversibles. De manière générale, dans un anneau noethérien intègre, un idéal est inversible si et seulement si il est projectif. On définit donc $\mathrm{Cl}(\mathcal{O})$ comme le groupe de Picard [12] de $\mathcal{O}$: le quotient du groupe (pour la multiplication) des idéaux fractionnaires projectifs par celui des idéaux principaux. Le nombre de classes $h(\mathcal{O})$ est comme précédemment le cardinal de $\mathrm{Cl}(\mathcal{O})$.

Remarque 12. On peut donner une description plus commode des idéaux inversibles de $\mathcal{O} = \mathcal{O}_D$ [Co13, Proposition 7.22] : si $\mathcal{O}$ est de conducteur f avec $D = f^2 D_0$, tous les idéaux inversibles de $\mathcal{O}_D$ sont, modulo un idéal principal, la restriction d'un idéal $\mathfrak{a}$ de $\mathcal{O}_{D_0}$ premier avec f. De la sorte, on obtient la description suivante du groupe de classes

$$\mathrm{Cl}(D) := \mathrm{Cl}(\mathcal{O}_D) \simeq I_{K,f}/P_{K,f}$$

où $K = \mathbb{Q}(\sqrt{D})$ est le corps des fractions de $\mathcal{O}$, $I_{K,f} \subseteq I_K$ désigne le sous-groupe des idéaux fractionnaires premiers avec f et $P_{K,f} \subseteq P_K$ le sous-groupe des idéaux principaux premiers avec f et engendrés par un élément congru à un entier rationnel modulo f.

10. Un morphisme $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ de courbes elliptiques sur $\mathbb{C}$ se relève au revêtement fondamental $\mathbb{C} \to \mathbb{C}/\Lambda_2$ et provient donc de la multiplication par un élément $\alpha \in \mathbb{C}$.

11. Une matrice ρ fixe τ par transformations de Möbius si et seulement si le vector $(\tau, 1)$ est propre. Le plongement ci-dessus revient à associer sa valeur propre à ρ.

12. En général, le groupe de Picard d'un anneau est le groupe dont les éléments sont les classes d'isomorphisme de modules projectifs de rang 1 (aussi appelés « modules inversibles ») et la loi est induite par le produit tensoriel. Ici, tous les modules inversibles sont isomorphes à des idéaux, et un idéal est isomorphe au module trivial si et seulement si il est principal, d'où notre définition.

En particulier, la suite exacte courte

$$0 \to P_K(f)/P_{K,f} \to \mathrm{Cl}(D) \to \mathrm{Cl}(D_0) \to 0,$$

où $P_K(f)$ est le groupe des idéaux principaux premiers avec f, permet de calculer très facilement h_D en fonction de h_{D_0} et f.

Proposition 13. *Toute courbe elliptique CM est définie sur $\overline{\mathbb{Q}}$. De plus, si D est un discriminant, l'ensemble $\mathrm{Ell}(D)$ des classes d'isomorphisme (sur $\overline{\mathbb{Q}}$ ou $\mathbb{C}$) de courbes elliptiques à multiplication complexe par $\mathcal{O}_D$ est munie d'une action canonique de $\mathrm{Cl}(D)$, simplement transitive. En particulier, il y a h_D classes d'isomorphisme de telles courbes.*

Démonstration. Par l'application $\tau \mapsto E_\tau$, $\mathrm{Ell}(D)$ s'identifie à l'ensemble $\mathrm{CM}(D)$ des points $\tau \in \mathfrak{H}$ CM de discriminant D, c'est-à-dire dont le polynôme minimal à coefficients dans $\mathbb{Z}$ est de discriminant D, modulo l'action de $\mathrm{SL}_2(\mathbb{Z})$. [13] Si $\tau \in \mathrm{CM}(D)$, par construction $[1, \tau]$ est un $\mathcal{O}_\tau \simeq \mathcal{O}_D$ idéal fractionnaire inversible (d'inverse $N(\tau)^{-1}[1, \overline{\tau}]$), et on obtient tous les idéaux fractionnaires inversibles à homothétie près ainsi [14]. Très concrètement, la bijection entre $\mathrm{Cl}(D)$ et $\mathrm{Ell}(D)$ est donc $\mathfrak{a} \mapsto \mathbb{C}/\mathfrak{a}$.

En particulier, toute courbe elliptique CM est définie sur $\overline{\mathbb{Q}}$. En effet, si E est à multiplication complexe par un ordre $\mathcal{O}$, il en va de même pour σE, de j-invariant $\sigma(j(E))$, pour tout automorphisme $\sigma \in \mathrm{Aut}(\mathbb{C}|\mathbb{Q})$. Le fait que l'action de $\mathrm{Aut}(\mathbb{C}|\mathbb{Q})$ sur $j(E)$ soit à image finie signifie que $j(E)$ est algébrique, i.e. E est définie sur $\overline{\mathbb{Q}}$.

L'action de $\mathrm{Cl}(\mathcal{O}_D)$ sur les courbes elliptiques CM peut être décrite ainsi : une courbe elliptique CM E correspond à un idéal inversible $\mathfrak{a}$ tel que $E \simeq \mathbb{C}/\mathfrak{a}$. Alors, on pose

$$\mathfrak{b} \star E := \mathbb{C}/\mathfrak{b}^{-1}\mathfrak{a}.$$

□

En particulier, l'invariant j d'une courbe elliptique CM est algébrique (c'est d'ailleurs même un entier algébrique [Si09, Chapter II, Section 6]). Mais on a bien mieux : on peut décrire entièrement l'extension qu'il engendre. Afin d'énoncer précisément ce résultat, faisons quelques rappels de théorie du corps de classes.

Si K est un corps de nombres, il existe une unique extension abélienne (non ramifiée) H telle que l'application d'Artin [15] induise un isomorphisme . Cette extension est caractérisée par les propriétés équivalentes suivantes et est appelée « corps de classes de Hilbert »de K (voir [Ne99, Chapter Vi, Proposition 6.8]) :

13. Au passage, on retrouve ainsi la bijection entre l'ensemble $\mathrm{BQF}(D)$ des formes quadratiques binaires primitives de discriminant D modulo l'action de $\mathrm{SL}_2(\mathbb{Z})$ et $\mathrm{Cl}(D)$.

14. Si $\mathfrak{a}$ est un idéal inversible de base orientée u, v, i.e. telle que $\mathrm{Im}(u/v) > 0$, $\tau = u/v$ convient.

15. Explicitement, le morphisme d'Artin $I_K \to \mathrm{Gal}(H|K)$ envoie un idéal premier $\mathfrak{p}$ sur l'unique $\sigma \in \mathrm{Gal}(H|K)$ tel que $\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{p}}$ pour tout $x \in \mathcal{O}_H$.

(i) H est l'extension abélienne non ramifiée partout (y compris à l'infini) maximale de K.

(ii) H est l'unique extension finie de K telle qu'un idéal premier de K soit totalement décomposé dans H si et seulement si il est principal (dans K).

Signalons également, même si l'on n'en aura pas besoin, que tout idéal de K devient principal dans H. Il existe également une variante pour les ordres non maximaux, donnant toujours un isomorphisme canonique $\mathrm{Gal}(H|K) \simeq \mathrm{Cl}(\mathcal{O})$. Dans ce cas, H est appelé le « corps de classes d'anneau » de $\mathcal{O}$.

Théorème 14 (Premier théorème de la multiplication complexe)**.** *Soit $D < 0$ un discriminant et $K = \mathbb{Q}(\sqrt{D})$. Soit E une courbe elliptique à multiplication complexe par $\mathcal{O}_D$. Alors, $K(j(E))$ est le corps de classes d'anneau de $\mathcal{O}_D$. De plus, l'isomorphisme de réciprocité d'Artin $\mathrm{rec} : \mathrm{Cl}(D) \to \mathrm{Gal}(H|K)$ est réalisé par la loi de réciprocité dite « de Shimura »*

$$j(\mathfrak{a} \star E) = \mathrm{rec}(\mathfrak{a})(j(E)).$$

Esquisse de démonstration. La première étape clé, que l'on admettra (voir [Si94, Chapter II, Proposition 2.5]), est de vérifier que l'action de $\mathrm{Cl}(D)$ sur $\mathrm{Ell}(D)$ commute avec l'action de $G_{\mathbb{Q}}$. Comme l'action de $\mathrm{Cl}(D)$ est de plus simplement transitive, on obtient un morphisme $G_K \to \mathrm{Cl}(D)$ découpant l'extension $L = K(j(E))$. En particulier, cette extension est abélienne de groupe de Galois un sous-groupe de $\mathrm{Cl}(D)$. Pour montrer que L est le corps de classes de Hilbert, il suffit de démontrer la loi de réciprocité de Shimura puisqu'elle implique immédiatement qu'un idéal premier de K est totalement décomposé dans L si et seulement il est principal. Par multiplicativité, il suffit de le faire lorsque $\mathfrak{a} = \mathfrak{p}$ est premier. On peut supposer $\mathfrak{p}$ au dessus d'un premier rationnel scindé p puisque le cas inerte est trivial, et on peut également supposer $\mathfrak{p}$ suffisamment grand pour que tous les éléments de $\mathrm{Ell}(D)$ aient bonne réduction modulo un premier $\mathfrak{P}$ de L au dessus de $\mathfrak{p}$. On doit vérifier que $j(\mathfrak{p} \star E) = \mathrm{rec}(\mathfrak{p})(j(E))$, i.e. que, modulo $\mathfrak{p}$, $j(E)^p \equiv j(\mathfrak{p} \star E)$. On dispose d'une isogénie canonique de degré p

$$E_{\mathbb{C}} \simeq \mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{p}^{-1}\mathfrak{a} \simeq (\mathfrak{p} \star E)_{\mathbb{C}}.$$

Le point clé, que l'on peut voir à l'aide de formes différentielles, est que, lorsque l'on réduit cette isogénie modulo p, elle est inséparable. Comme elle est de degré p, il ne peut s'agir que du Frobenius Fr_p à automorphisme près : on a ainsi $(\mathfrak{p} \star E) \pmod{\mathfrak{P}} \simeq \mathrm{Fr}_p(E \pmod{\mathfrak{P}})$. En passant aux j-invariants, on trouve exactement la congruence voulue. Voir [Si94, Chapter II, Section 4] pour plus de détails. □

Corollaire 15. *Toutes les courbes elliptiques à multiplication complexe par $\mathcal{O}_D$ sont conjuguées, et leur j-invariant est de degré exactement h_D.*

Remarque 16. On dispose également d'un deuxième théorème de la multiplication complexe qui décrit les corps de classes de rayon $\mathfrak{a}$ d'un corps quadratique imaginaire : essentiellement, cela revient à ajouter au corps de classes de Hilbert $H = K(j(E))$ les

coordonnées x des points de $\mathfrak{a}$-torsion de E, cf. [Si94, Chapter II, Section 5]. Ces résultats sont à placer dans le cadre de la « théorie du corps de classes explicite » et du douzième problème de Hilbert, visant à construire explicitement des extensions abéliennes par adjonction de valeurs spéciales de certaines fonctions analytiques particulières.

Pour terminer, expliquons comment démontrer le théorème 1. La clé est le résultat suivant. Notons qu'il s'applique bien aux discriminants de nombre de classes 1 d'après le lemme suivant.

Lemme 17. *Soit $D < 0$ un discriminant de nombre de classes 1 et $N < \frac{|D|}{4}$ un entier premier avec le conducteur de D. Alors, N est « non déployé » dans $\mathbb{Q}(\sqrt{D})$ au sens où aucun de ses facteurs premiers n'est un carré modulo D.*

Démonstration. On peut bien évidemment supposer N premier. Supposons que N est un carré modulo D. Étant premier avec le conducteur de D, il est alors représenté par une forme quadratique binaire primitive de discriminant D. Comme $h_D = 1$, modulo $\mathrm{SL}_2(\mathbb{Z})$, il est donc représenté par la forme principale $x^2 - \frac{D}{4}y^2$ ou $x^2 - xy - \frac{D-1}{4}y^2$ selon la congruence de D modulo 4. Dans les deux cas, comme $D < 0$, il vaut au moins $-\frac{D}{4} = \frac{|D|}{4}$. [16] □

Proposition 18. *Soit E une courbe elliptique à multiplication complexe par $\mathcal{O}_D$, définie sur $L = \mathbb{Q}(j(E))$. Supposons N non déployé dans $\mathbb{Q}(\sqrt{D})$. Alors, il existe (à conjugaison près) un sous-groupe H_N de $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, dépendant uniquement de N, tel que la représentation galoisienne $\rho_{E,N} : G_L \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ soit à image dans H_N.*

Démonstration. La clé est que la classe d'isomorphisme de l'algèbre $A = \mathcal{O}_D/N\mathcal{O}_D$ est uniquement déterminée par la condition d'inertie. En effet, supposons N sans facteur carré pour simplifier [17]. Alors,

$$A \simeq \prod_{p|N} \mathcal{O}_D/p\mathcal{O}_D \simeq \prod_{p|N} \mathbb{F}_{p^2}.$$

Cette algèbre est munie d'une involution canonique ι, produit des involutions canoniques sur chacun des $\mathbb{F}_{p^2}$. Soit E est une courbe elliptique à multiplication complexe par $\mathcal{O}_D$. Le A-module $E[N]$ étant cyclique (on peut le voir sur les $\mathbb{C}$-points), il s'identifie à A via le choix d'un générateur x_0. Par ailleurs, le choix d'une base de A comme $\mathbb{Z}/N\mathbb{Z}$-module permet de voir $H_0 := A^\times \curvearrowright A$ comme un sous-groupe de

16. Si D est fondamental, cet argument peut être raccourci comme suit : si p est scindé dans $\mathbb{Q}(\sqrt{D})$. Si le groupe de classes vaut 1, c'est donc la norme d'un élément $\frac{u+v\sqrt{D}}{2}$: en particulier, $p = \frac{u^2+|D|v^2}{4} \geq \frac{|D|}{4}$.

17. En général, $\mathcal{O}_D/p^n\mathcal{O}_D$ est l'unique $\mathbb{Z}/p^n\mathbb{Z}$-algèbre étale se réduisant à $\mathbb{F}_{p^2}$ modulo p. Explicitement, elle est obtenue via le lemme de Hensel en relevant un élément primitif de $\mathbb{F}_{p^2}$.

$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Alors, $H_N := H_0 \cup \iota H_0$ convient. En effet, si $\sigma \in G_L$ est un automorphisme de $\overline{L}$, il existe $g \in A^\times$ tel que $\sigma(x_0) = gx_0$. Alors, σ agit sur $E[N] \simeq A \simeq (\mathbb{Z}/N\mathbb{Z})^2$ comme l'élément g si σ fixe $\sqrt{D}$, et comme l'élément $\iota(g)$ sinon. □

Avant d'expliquer la démonstration du théorème 1, faisons un petit rappel de théorie du genre qui décrit les éléments d'ordre 2 du groupe de classe.

Proposition 19 (Gauss). *Soit $D < 0$ un discriminant. Alors, le groupe des éléments d'ordre 2 de $\mathrm{Cl}(D)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^{\mu+\varepsilon-1}$ où μ est le nombre de facteurs premers distincts de D et ε vaut 0 si $D \equiv 1 \pmod 4$, et $\varepsilon \in \{0,1,2\}$ selon la classe de congruence de $D/4$ modulo 8 sinon.*

Esquisse de démonstration. Par souci de simplicité, donnons uniquement la démonstration lorsque D est fondamental, voir [Co13, Theorem 3.15] pour une démonstration complète. Tout facteur premier p de D se ramifie dans $K = \mathbb{Q}(\sqrt{D})$ et fournit donc un élément $\mathfrak{p}$ d'ordre 2 tel que $\mathfrak{p}^2 = (p)$. On a ainsi 2^μ éléments d'ordre divisant 2. Comme on dispose de la relation linéaire

$$\prod \mathfrak{p}^{v_p(D)} = (\sqrt{D}) \equiv 0 \pmod{\mathrm{Cl}(D)},$$

on obtient seulement $2^{\mu-1}$ classes distinctes d'ordre divisant 2 dans $\mathrm{Cl}(D)$, et on vérifie que ces classes exhaustent les éléments d'ordre 2. □

Esquisse de démonstration du théorème 1. On suit [Se97, Section A.5]. Fixons un entier $N \geq 1$ quelconque. Si $D < 0$ est de nombre de classes 1, il existe une unique courbe elliptique E_D à multiplication complexe par $\mathcal{O}_D$ et celle-ci est définie sur $\mathbb{Q}$ (d'après la proposition 13). Si $|D| > 4N$ est de plus fondamental, il doit être premier d'après la proposition 19 et le lemme 17 montre que E_D fournit un point rationnel de la courbe Y_{H_N} de la proposition 18, dont on vérifie que le corps de définition est $\mathbb{Q}$. On s'est ainsi ramenés à trouver tous les points rationnels sur la courbe $Y_{H_N} \subseteq X_{H_N}$; il suffit ensuite de vérifier ceux correspondant à une courbe elliptique à multiplication complexe.

Un calcul de revêtements ramifiés avec $X_{H_N} \to X(1)$ permet de calculer le genre de X_{H_N} en fonction de N, et même, avec plus de travail, de trouver des équations explicites. On s'est ainsi ramenés à un problème complétement diophantien, qu'on peut résoudre de diverses manières (par des méthodes p-adiques, par approximation diophantienne, par descente, ...). On dispose également d'un avantage supplémentaire : l'invariant j d'une courbe elliptique à multiplication complexe étant toujours entier, on peut en fait se limiter à la recherche de points entiers, ce qui permet de travailler avec des courbes de genre 1 ou même de genre 0 avec plus de trois pointes, plutôt que de devoir être en genre > 1. Voir [Ba09] pour l'exemple de $N = 9$ et [Ke85] pour

$N = 7$, tous deux de genre 0. On pourra également trouver la démonstration originale de Heegner en niveau 24, rédigée dans un langage sans courbes modulaires, dans [Sh14]. □

4. Modularité et points de Heegner

Nous allons à présent expliquer comment la théorie de la multiplication complexe permet de produire des points rationnels sur des courbes elliptiques. Commençons par un rappel sur la réduction des courbes elliptiques.

Soit E une courbe elliptique sur $\mathbb{Q}$. Il existe alors (voir [BLR90]) un modèle lisse $\mathcal{E}$ de E sur $\mathbb{Z}$, appelé « modèle de Néron » de E satisfaisant la propriété universelle suivante : si $\mathcal{X}$ est une variété algébrique sur $\mathbb{Z}$ et X est la variété correspondante sur $\mathbb{Q}$, tout morphisme $X \to E$ sur $\mathbb{Q}$ provient d'un morphisme $\mathcal{X} \to \mathcal{E}$ sur $\mathbb{Z}$.

En particulier, en prenant $\mathcal{X} = \mathcal{E} \times \mathcal{E}$ et $m : X \to E$ la multiplication, on voit que $\mathcal{E}$ est encore un groupe algébrique (sur $\mathbb{Z}$). L'avantage de $\mathcal{E}$ est que, désormais, on peut le réduire modulo un nombre premier p pour obtenir un groupe algébrique E_p sur $\mathbb{F}_p$. La classification des groupes algébriques lisses de dimension 1 sur $\mathbb{F}_p$ fournit trois cas de figures possibles :

(i) E_p est une courbe elliptique, i.e. E_p est projective. On dit que E a « bonne réduction » en p.

(ii) E_p est isomorphe à $\mathbb{G}_a$. On dit que E a « réduction additive ».

(iii) E_p est isomorphe à $\mathbb{G}_m$ sur $\mathbb{F}_{p^2}$. On dit que E a « réduction multiplicative ». Si E_p est isomorphe à $\mathbb{G}_m$ sur $\mathbb{F}_p$, la réduction est dite « déployée », et « non déployée »sinon.

On définit également $a_p = p + 1 - |E_p(\mathbb{F}_p)|$ [18] si E a bonne réduction en p, $a_p = 0$ si E a réduction additive, et $a_p = 1$ ou -1 selon que E a réduction multiplicative déployée ou non déployée. Tout ceci marche *verbatim* sur un corps de nombres K plus général que $\mathbb{Q}$, en remplaçant le premier p par un idéal premier $\mathfrak{p}$ (et $a_\mathfrak{p} = N(\mathfrak{p}) + 1 - |E_\mathfrak{p}(\mathcal{O}_K/\mathfrak{p})|$).

Définition 20 (Fonction L)**.** *La* fonction L de Hasse-Weil *d'une courbe elliptique E sur un corps de nombres K est la fonction analytique*

$$L(E,s) = \prod_{\mathfrak{p}\notin S} \left(1 - a_\mathfrak{p} N(\mathfrak{p})^{-s} + N(\mathfrak{p})^{1-2s}\right)^{-1} \prod_{\mathfrak{p}\in S} \left(1 - a_\mathfrak{p} N(\mathfrak{p})^{-s}\right)^{-1} =: \sum_{\mathfrak{n}\in I_K^\circ} \frac{a_\mathfrak{n}}{N(\mathfrak{n})^s}$$

où $I_K^\circ \subseteq I_K$ désigne l'ensemble des idéaux entiers de $\mathcal{O}_K$ et S désigne l'ensemble des premiers de mauvaise réduction.

18. Il s'agit de la trace du Frobenius sur le premier groupe de cohomologie de E_p.

Il découle de l'hypothèse de Riemann sur les corps finis que le produit est convergeant pour $\mathrm{Re}(s) > \frac{3}{2}$. Le théorème de modularité (anciennement « conjecture de Shimura–Taniyama–Weil ») affirme que, si E est défini sur $\mathbb{Q}$, $L(E,s)$ est la fonction L d'une forme modulaire, et prédit même son niveau.

Définition 21 (Conducteur). *Le conducteur d'une courbe elliptique E sur $\mathbb{Q}$ est $N = \prod_p p^{n_p}$ où $n_p = 0$ si E a bonne réduction en p, $n_p = 1$ si E a réduction multiplicative, et $n_p = 2$ si E a réduction additive et $p \geq 5$ (voir* [Si09, Appendix A] *pour la recette en 2 et 3).*

Théorème 22 (Wiles [Wi95], Taylor–Wiles [TW95], Breuil–Conrad–Diamond–Taylor [BCDT01]). *Soit E une courbe elliptique sur $\mathbb{Q}$ de fonction L*

$$L(E,s) = \sum_{n\geq 1} \frac{a_n}{n^s}$$

et de conducteur N. Alors, $f(\tau) = \sum_{n\geq 1} a_n q^n$ est une forme modulaire de poids 2 et niveau $\Gamma_0(N)$ où $q = e^{2i\pi\tau}$.

Remarque 23. Si E est à multiplication complexe, on peut montrer [Si94, Chapter II, Theorem 10.5] à l'aide de la théorie de la multiplication complexe que $L(E,s)$ est produit de deux fonctions L de Hecke, de sorte que la forme modulaire associée est une forme modulaire *CM*, connues déjà depuis Hecke.

En d'autres termes, f est une forme différentielle holomorphe sur la courbe modulaire $X_0(N)$. Nous allons utiliser la forme suivante du théorème de modularité, découlant du théorème du modularité et du théorème d'isogénie de Faltings, cf. [Da04, Chapter 2, Sections 5–6].

Théorème 24. *Soit E une courbe elliptique sur $\mathbb{Q}$ de conducteur N. Alors, il existe un morphisme surjectif $\varphi_E : X_0(N) \to E$ de courbes algébriques sur $\mathbb{Q}$.*

Supposons E unique dans sa classe d'isogénie sur $\mathbb{Q}$ pour simplifier. Analytiquement, ce morphisme est facile à décrire : il envoie un élément $\tau \in \mathfrak{H}/\Gamma_0(N)$ sur l'intégrale

$$c\int_{i\infty}^{\tau} 2i\pi f(\tau) \in \mathbb{C}/\Lambda_E \simeq E(\mathbb{C})$$

pour un certain scalaire $c \in \mathbb{Q}^\times$ appelé *constante de Manin*[19].

Le grand avantage de ce théorème est que la théorie de la multiplication nous fournit une famille explicite de points de $X_0(N)$ définis sur $\overline{\mathbb{Q}}$, qu'on peut ensuite envoyer sur E pour obtenir des points de E. On appelle ces points des *points de Heegner*.

19. On conjecture que $c = 1$ tout le temps et ceci est démontré lorsque N est sans facteur carré (E est *semistable*).

Commençons par remarquer que, si $D < 0$ est un discriminant premier avec N, il existe des points CM de discriminant D si et seulement si N est *déployé* dans $\mathbb{Q}(\sqrt{D})$, i.e. tous ses facteurs premiers sont des carrés modulo D. On appelle cette hypothèse « l'hypothèse de Heegner ».

En effet, dans ce cas N peut s'écrire comme une norme idéale $\mathfrak{n}\overline{\mathfrak{n}}$ sur $\mathbb{Q}(\sqrt{D})$, et on a ainsi une isogénie N-cyclique $E \to \mathfrak{n} \star E$ pour tout $E \in \mathrm{Ell}(D)$, c'est-à-dire un point de $X_0(N)$. Par la théorie de la multiplication complexe, ce point est défini sur le corps de classes d'anneau H_D de $\mathcal{O}_D$.

La formule de Gross–Zagier fait le lien entre les points de Heegner sur E et sa fonction L. Elle donne une formule explicite pour la dérivée $L'(E/\mathbb{Q}(\sqrt{D}), 1)$ en termes de la hauteur du point de Heegner, mais pour simplifier et éviter d'avoir à définir la hauteur canonique, on formule simplement le théorème sous cette forme.

Théorème 25 (Gross–Zagier [GZ84])**.** *Soit E une courbe elliptique sur $\mathbb{Q}$ de conducteur N et $D < 0$ un discriminant satisfaisant l'hypothèse de Heegner. Alors, pour tout point CM τ de discriminant D sur $X_0(N)$, $L'(E/\mathbb{Q}(\sqrt{D}), 1) = 0$ si et seulement si*

$$\mathrm{Tr}_{H_D|\mathbb{Q}(\sqrt{D})}(\varphi(\tau)) \in E(\mathbb{Q}(\sqrt{D}))$$

est un point de torsion.

On peut montrer par un calcul sur $\mathbb{F}_p$ que, si E est définie sur $\mathbb{Q}$

$$L(E/\mathbb{Q}(\sqrt{D}), s) = L(E/\mathbb{Q}, s)L(E^{(D)}/\mathbb{Q}, s)$$

où $E^{(D)}$ est la *D-ème tordue quadratique* de E. Explicitement, si E est donnée par l'équation de Weierstrass $y^2 = f(x)$, $E^{(D)}$ est donnée par l'équation $Dy^2 = f(x)$.[20] En particulier, on peut s'assurer que $L'(E/\mathbb{Q}(\sqrt{D}), 1) = 0$ indépendamment de D en choissant E telle que $L(E/\mathbb{Q}, 1) = L'(E/\mathbb{Q}, 1) = 0$. Par ailleurs, on peut vérifier cette condition pour une courbe spécifique en choisissant un discriminant D tel que $L(E^{(D)}/\mathbb{Q}, 1) \neq 0$ et en vérifiant que le point de Heegner du théorème 25 est de torsion. On dira que E est *de rang analytique* ≥ 2 si cette condition est vérifiée.

Corollaire 26. *Soit E une courbe elliptique de rang analytique ≥ 2 et soit $\tau \in \mathfrak{H}$ un point CM de discriminant de nombre de classes 1 satisfaisant l'hypothèse de Heegner. Alors, $\varphi_E(\tau) \in E(\mathbb{Q}(\tau))$ est un point de torsion.*

Ce corollaire paraît prometteur au premier abord puisque, pour presque tout discriminant D, les points de torsion de E sur $\mathbb{Q}(\sqrt{D})$ sont les mêmes que ceux de E sur $\mathbb{Q}$ et on peut déterminer effectivement les discriminants exceptionnels ; en pratique, il n'y en

20. Si $\mathrm{End}_{\overline{k}}(E) \neq \mathcal{O}_{-4}, \mathcal{O}_{-3}$, on a $\mathrm{Aut}_{\overline{k}}(E) = \mathrm{End}_{\overline{k}}(E)^\times = \{\pm 1\}$ et toutes les tordues de E sont quadratiques. En effet, $H^1(G_k, \mathrm{Aut}(E)) = \mathrm{Hom}(G_k, \{\pm 1\})$ s'identifie aux extensions quadratiques de k.

a pas. Ainsi, si on choisit E de torsion triviale sur $\mathbb{Q}$, le corollaire 26 nous dit qu'on peut détecter les discriminants de nombre de classes 1 en analysant la fibre $\varphi^{-1}(0_E)$.

Malheureusement, ceci vaut seulement pour les discriminants satisfaisant l'hypothèse de Heegner, et le lemme 17 nous dit que seul les discriminants de valeur absolue au plus $4N$ ont une chance de la satisfaire... On verra dans les deux prochaines sections comment corriger ce problème pour obtenir une démonstration des théorèmes 1 et 2.

5. Multiplication réelle

L'idée de base de la multiplication réelle telle qu'introduite dans l'article [Da01] est de remplacer le rôle de la place à l'infini par la place en p, i.e. remplacer $\mathbb{C}$ par $\mathbb{C}_p$ pour obtenir un analogue des points de Heegner pour les corps quadratiques réels, appelés « points de Stark–Heegner » [21].

Malheureusement, les propriétés algébriques de ces points sont très mal connues et en grande partie conjecturales à ce jour. Leur construction procède donc par voie analytique. Soit E une courbe elliptique de conducteur N, qu'on supposera unique dans sa classe d'isogénie pour simplifier. Sur $\mathbb{C}$, les points de Heegner étaient définis via une application

$$\varphi_E : (\mathfrak{H}_\infty/\Gamma_0(N))^{\mathrm{CM}} \to \mathbb{C}_\infty/\Lambda_E \simeq E(\mathbb{C}_\infty)$$

obtenue en intégrant une forme différentielle associée à E. Nous allons définir des analogues de chacun des termes apparaissant dans cet énoncé.

Tout d'abord, l'analogue du demi-plan de Poincaré $\mathfrak{H}_\infty$, composante connexe supérieure de $\mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R})$, est le demi-plan de Drinfeld $\mathfrak{H}_p := \mathbb{P}^1(\mathbb{C}_p) - \mathbb{P}^1(\mathbb{Q}_p)$ (connexe pour $p \neq \infty$). Il est muni d'une structure canonique d'espace analytique p-adique qui permet de parler de fonctions analytiques $\mathfrak{H}_p \to \mathbb{C}_p$ (cf. [BC92, Chapitre I], ainsi que [Bo14] pour les bases de géométrie analytique p-adique).

Pour parler du membre de droite, il nous faut disposer d'une uniformisation p-adique analogue à $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda_E \simeq \mathbb{C}/[1, \tau_E]$, obtenue via la fonction $\wp$ de Weierstrass. Telle quelle, cette uniformisation ne peut pas être valide pour $\mathbb{C}_p$ puisque $\mathbb{C}_p$ n'admet aucun réseau discret ($\mathbb{Z}$ est dense dans $\mathbb{Z}_p$). L'idée clé de Tate fût de remplacer cette unformisation additive par une version multiplicative : en passant à l'exponentielle $q = e^{2\pi\tau}$, puisque $\mathbb{C}^\times \simeq \mathbb{C}/\mathbb{Z}$, on a aussi un isomorphisme

$$E(\mathbb{C}) \simeq \mathbb{C}/[1, \tau_E] \simeq \mathbb{C}^\times/q_E^{\mathbb{Z}}.$$

21. Nommés ainsi en raison d'un sentiment que « les points de Stark–Heegner sont aux points de Heegner ce que les unités de Stark sont aux unités elliptiques ».

Cette fois-ci, l'isomorphisme est donné par certaines fonctions analytiques $(X, Y) : \mathbb{C}^\times \to E(\mathbb{C})$, séries entières à coefficients entiers en q. On peut alors espérer obtenir une uniformisation p-adique de la forme

$$\mathbb{C}_p/q_E^{\mathbb{Z}} \xrightarrow{\sim} E(\mathbb{C}_p)$$

où q_E est tel que $j(q_E) = j(E)$. Pour pouvoir évaluer X et Y en q_E, il faut que $|j(E)|_p^{-1} = |q_E|_p < 1$, ce qui se trouve être équivalent à ce que E ait réduction multiplicative en p. Réciproquement, Tate montra que les fonctions X et Y fournissent bien une uniformisation p-adique

$$E(\mathbb{C}_p) \simeq \mathbb{C}_p/q_E^{\mathbb{Z}}$$

lorsque E a réduction multiplicative en p, voir [Si94, Chapter 5, Sections 3–4]. Un grand avantage de cette uniformisation, contrairement au cas complexe, est qu'elle est compatible avec l'action galoisienne, mais on n'en aura pas besoin ici. On suppose donc que E a réduction multiplicative en p.

Enfin, le sous-groupe de congruence $\Gamma_0(N)$ de $\mathrm{SL}_2(\mathbb{Z})$ est quant à lui remplacé par le sous-groupe de congruence

$$\Gamma_0^{(p)}(M) := \left\{ \rho = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}[1/p]) \;\middle|\; c \equiv 0 \pmod{N}, \det(\rho) = \pm 1 \right\}$$

de $\mathrm{GL}_2(Z[1/p])$, où $M = N/p$ est la partie « modérée » du conducteur N, c'est-à-dire la partie première à p de N.

Ainsi, nous allons construire une application

$$J_E : (\mathfrak{H}_p/\Gamma_0^{(p)}(M))^{\mathrm{RM}} \to \mathbb{C}_p^\times/q_E^{\mathbb{Z}} \simeq E(\mathbb{C}_p).$$

Les éléments de l'image seront appelés des points de Stark–Heegner. Nous définirons la notion de point RM du quotient $\mathfrak{H}_p/\Gamma_0^{(p)}(M)$ plus tard, mais pour l'instant $\mathfrak{H}_p^{\mathrm{RM}}$ désigne simplement les éléments de $\mathfrak{H}_p$ engendreant une extension quadratique réelle de $\mathbb{Q}$.

Cette application est obtenue à partir d'un « symbole modulaire » construit (en partie conjecturalement) dans [Da01], c'est-à-dire une fonction de $\mathbb{P}^1(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q})$ vers $\mathscr{A}_{\mathfrak{H}_p}/q_E^{\mathbb{Z}}$, où $\mathscr{A}_{\mathfrak{H}_p}$ désigne les fonctions holomorphes sur $\mathfrak{H}_p$, notée suggestivement comme une intégrale multiplicative indéfinie

$$J_E\{r, s\}(\tau) = \prod_r^\tau \int_r^s \omega_E$$

et satisfaisant les propriétés habituelles de transitivité d'intégrales

(1) Pour tout $r \in \mathbb{P}^1(\mathbb{Q})$ et $\tau \in \mathfrak{H}_p$,

$$\prod_r^\tau \int_r^r \omega_E = 1.$$

(2) Pour tous $r, s, t \in \mathbb{P}^1(\mathbb{Q})$ et $\tau \in \mathfrak{H}_p$,
$$\oint_r^\tau \int_r^s \omega_E \times \oint_s^\tau \int_s^t \omega_E \times \oint_t^\tau \int_t^r \omega_E \times = 1.$$

(3) Pour tous $r, s \in \mathbb{P}^1(\mathbb{Q})$ et $\tau_1, \tau_2 \in \mathfrak{H}_p$, le quotient
$$\oint_r^{\tau_2} \int_r^s \omega_E \div \oint_r^{\tau_1} \int_r^s \omega_E = \oint_{\tau_1}^{\tau_2} \int_r^s \omega_E$$
est égal à l'intégrale multiplicative définie, définie explicitement comme l'intégrale sur $\mathbb{P}^1(\mathbb{Q}_p)$ d'une mesure p-adique associée à τ_1, τ_2, r, s et E.

ainsi que la relation de $\Gamma_0^{(p)}(M)$-invariance
$$\oint_{\gamma r}^{\gamma\tau} \int_{\gamma r}^{\gamma s} \omega_E = \oint_r^\tau \int_r^s \omega_E$$
pour tout $\gamma \in \Gamma_0^{(p)}(M)$, $r, s \in \mathbb{P}^1(\mathbb{Q})$ et $\tau \in \mathfrak{H}_p$.

À partir d'un tel symbole modulaire, on définit une classe de cohomologie [22], toujours noté abusivement $J_E \in H^1(\Gamma_0^{(p)}(M), \mathscr{A}_{\mathfrak{H}_p})$ par la formule
$$J_E(\gamma) := J_E\{t, \gamma t\}$$
où $t \in \mathbb{P}^1(\mathbb{Q})$ est un point de base quelconque.

Revenons enfin aux points de Stark–Heegner. Soit $\tau \in \mathfrak{H}_p^{\mathrm{RM}}$ un point RM, c'est-à-dire un point RM $\tau \in \mathbb{C}_p^{\mathrm{RM}}$ tel que p est inerte ou ramifié dans $\mathbb{Q}(\tau)$. Alors, l'anneau
$$\mathcal{O}_\tau := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}[1/p]) - \{0\} \;\middle|\; \frac{a\tau + b}{c\tau + d} \right\} \cup \{0\}$$
s'identifie à un $\mathbb{Z}[1/p]$-ordre quadratique de même discriminant que τ, et $\mathrm{End}_{\Gamma_0^{(p)}(M)} \tau$ à un sous-groupe du groupe des unités $\mathcal{O}_\tau^\times \simeq \{\pm 1\} \times \mathbb{Z}$. On peut montrer que ce sous-groupe est non trivial si et seulement si τ satisfait l'« hypothèse de Heegner » suivante : M est déployé dans $\mathbb{Q}(\tau)$. On note ainsi $(\mathfrak{H}_p/\Gamma_0^{(p)}(M))^{\mathrm{RM}}$ les points RM de $\mathfrak{H}_p$ satisfaisant l'hypothèse de Heegner, modulo $\Gamma_0^{(p)}$.

Si $\tau \in \mathfrak{H}_p^{\mathrm{RM}}$ satisfait l'hypothèse de Heegner, on note γ_τ l'unique générateur du stabilisateur modulo $\{\pm 1\}$ dont l'image dans $\mathbb{Q}(\tau)$ est > 1 [23], qu'on appelle *automorphe fondamental* de τ.

Nous sommes enfin en mesure de définir les points de Stark–Heegner.

22. Rappelons que si G est un groupe agissant sur un groupe abélien A, $H^1(G, A)$ désigne le groupe des « cocycles » $f : G \to A$, c'est-à-dire satisfaisant la relation $f(gh) = f(g) + gf(h)$, modulo les « cobords », c'est-à-dire les cocycles de la forme $f_a(g) = ga - a$ pour un $a \in A$.

23. Après choix d'un plongement $\overline{\mathbb{Q}} \to \mathbb{C}_p$ pour pouvoir parler de positivité.

Définition 27 (Points de Stark–Heegner)**.** *Soit E une courbe elliptique sur $\mathbb{Q}$ à réduction multiplicative en p et soit $\tau \in (\mathfrak{H}_p/\Gamma_0^{(p)}(M))^{\mathrm{RM}}$ un point RM. Alors, le point de Stark–Heegner associé à τ est*

$$J_E[\tau] := J_E(\gamma_\tau) \in \mathbb{C}_p^\times/q_E^{\mathbb{Z}} \simeq E(\mathbb{C}_p).$$

Conjecture 28 (Darmon [Da01])**.** *Soit E une courbe elliptique sur $\mathbb{Q}$ à réduction multiplicative en p et soit $\tau \in (\mathfrak{H}_p/\Gamma_0^{(p)}(M))^{\mathrm{RM}}$ un point RM.*

(i) Le point local $J_E[\tau] \in E(\mathbb{C}_p)$ est en fait un point global défini sur le corps de classe d'anneau H_τ de $\mathcal{O}_\tau$.

(ii) (Formule de Gross–Zagier) Le point $\mathrm{Tr}_{H_\tau|\mathbb{Q}(\tau)}(J_E[\tau]) \in E(\mathbb{Q}(\tau))$ est de torsion si et seulement si $L'(E/\mathbb{Q}(\tau), 1) = 0$.

Corollaire 29. *Soit E une courbe elliptique de rang analytique ≥ 2 à réduction multiplicative et soit $\tau \in \mathfrak{H}_p$ un point RM de discriminant de nombre de classes 1 satisfaisant l'hypothèse de Heegner. Alors, $J_E[\tau] \in E(\mathbb{Q}(\tau))$ est un point de torsion.*

L'hypothèse de Heegner est un peu embêtante, comme dans le cas imaginaire, à cause du résultat suivant (voir [CD24, Lemma 1] pour la démonstration).

Lemme 30. *Soit D un discriminant de nombre de classes 1 de la forme n^2-4, n^2+4, ou $4n^2+1$ pour un certain $n \geq 0$ et soit $N < n-2$ un entier positif premier avec le conducteur de D. Alors, N est non déployé dans $\mathbb{Q}(\sqrt{D})$, i.e. aucun de ses facteurs premiers n'est un carré modulo D.*

Heureusement, on peut s'en débarasser en prenant $M = 1$, i.e. $N = p$!

Esquisse de démonstration conditionnelle du théorème 2. Fixons une courbe elliptique E de conducteur premier p, unique dans sa classe d'isogénie sur $\mathbb{Q}$ et sans torsion quadratique. Commençons par supposer que D est un discriminant de la forme $n^2 \pm 4$, non divisible par p, et (sans perte de généralité) que $n > p+2$. Alors, le lemme 30 montre que $\frac{n+\sqrt{D}}{2} \in \mathfrak{H}_p$ et le corollaire 29 implique

$$J_E\left[\frac{n+\sqrt{D}}{2}\right] = 1 \in \mathbb{C}_p^\times/q_E^\times.$$

Or, $\gamma_D = \left(\begin{smallmatrix} n & \pm 1 \\ 1 & 0 \end{smallmatrix}\right)$ stabilise $\tau_D = \frac{n+\sqrt{D}}{2}$ donc

$$J_E\{0,\infty\}(\tau_D) = J_E\{0,\gamma_D 0\}(\tau_D) = 1$$

puisque c'est une puissance de $J_E[\tau_D]$. On s'est ainsi ramenés à résoudre l'équation $J_E\{0,\infty\}(\tau) = 1$ pour $\tau \in \mathfrak{H}_p$. De plus, les τ_D appartiennent tous à l'*affinoïde standard* $\mathfrak{H}_p^\circ \subseteq \mathfrak{H}_p$, défini comme la préimage de $\mathbb{P}^1(\overline{\mathbb{F}}_p) - \mathbb{P}^1(\mathbb{F}_p)$ selon l'application de

réduction

$$\mathrm{red}_p : \mathbb{P}^1(\mathbb{C}_p) \to \mathbb{P}^1(\overline{\mathbb{F}}_p).$$

L'avantage est que la fonction $\Phi_E = J_E\{0,\infty\}|_{\mathfrak{H}_p^\circ}$ peut être normalisée pour envoyer $\mathfrak{H}_p^\circ$ sur $\mathcal{O}_{\mathbb{C}_p}^\times$, nous débarassant ainsi de l'ambiguïté de $q_E^{\mathbb{Z}}$. On cherche à trouver tous les zéros de RM $\tau \in \mathfrak{H}_p^\circ$ de $\Phi_E - 1$: si on de la chance, il suffit de majorer le nombre de zéros quadratiques $\tau \in \mathbb{Q}_{p^2}$ (où $\mathbb{Q}_{p^2}$ est l'extension non ramifiée de degré 2 de $\mathbb{Q}_p$) et que cette borne soit atteinte. Or, une telle majoration est précisément fournie par le nombre de zéros dans $\mathbb{F}_{p^2}$ de la réduction

$$\mathrm{red}_p(\Phi_E - 1) \in \mathbb{F}_p(X),$$

une fonction rationnelle dont les zéros et les pôles sont dans $\mathbb{F}_p$.

Pour conclure, la plupart des choix de courbes E permettent de résoudre le problème : par exemple, l'unique courbe de conducteur $p = 389$ et rang 2 convient et permet de résoudre le problème pour les discriminants non divisibles par 389. En faisant la même chose pour E de conducteur $p = 433$, on obtient ainsi le résultat pour tous les discriminants, fondamentaux ou non, grâce à la théorie du genre (une variante du lemme 19 pour les discriminants positifs).

Pour D de la forme $4n^2 + 1$, la même stratégie fonctionne en remarquant qu'on a cette fois-ci

$$J_E\{-1/2,\infty\}\left(\frac{2n-1+\sqrt{D}}{2}\right) = J_E\left[\frac{D+\sqrt{D}}{2}\right]^{m_D} = 1.$$

Voir [CD24] pour plus de détails. □

Remarque 31. On a ainsi démontré le théorème 2 pour tous les discriminants, pas seulement les fondamentaux. Remarquons qu'il est crucial dans cette approche de considérer les discriminants non fondamentaux même si on ne souhaite établir le théorème uniquement dans le cas fondamental, sinon la majoration n'est pas atteinte.

Lorsque $D < 0$, la théorie du genre (lemme 19) montre qu'un discriminant de nombre de classes 1 est de la forme $-2^\varepsilon p$ avec p premier et $\varepsilon \leq 2$. Comme $h_D \mid h_{Df^2}$ pour tous D et f (cf. la remarque 12), on peut se restreindre au cas fondamental. En revanche, pour $D > 0$, la théorie du genre est un peu différente et il est possible que $h_{f^2D} = h_D = 1$ pour une infinité de f. Le théorème 2 pour les discriminants non fondamentaux ne semble donc pas découler formellement de la version fondamentale.

6. Courbes de Shimura

Enfin, dans cette dernière section, on explique comment corriger l'approche de la section 4 pour démontrer le théorème 1. La raison pour laquelle cette approche échouait était que l'hypothèse de Heegner était incompatible avec le fait d'être de nombre de classes 1.

En effet, le lemme 17 montre que les petites valeurs N sont non déployées plutôt que déployées dans des corps quadratiques imaginaires de nombre de classes 1. On pourra consulter [Da04, Chapter 4], [Da04, Chapter 6] et [Zh01, Section 1] pour plus de détails et de références sur les courbes de Shimura.

Pour résoudre ce problème, nous allons définir d'autres points de Heegner de sorte que l'hypothèse de Heegner devienne cette fois « N est non déployée dans $\mathbb{Q}(\sqrt{D})$ ». Pour ce faire, nous allons remplacer la paramétrisation $X_0(N) \to E$ par une paramétrisation $X \to E$ par une *courbe de Shimura* plutôt qu'une courbe modulaire.

Expliquons rapidement ce qu'est une courbe de Shimura. Tandis que les courbes modulaires paramétrisaient les courbes elliptiques avec structure de niveau, les courbes de Shimura paramétrisent, elles, des surfaces abéliennes à multiplication quaternionique, sans structure de niveau pour nous. Ici, une surface abélienne est une variété abélienne de dimension 2. On dit qu'une surface abélienne S est *à multiplication quaternionique* par un ordre $\mathcal{O}$ dans une algèbre quaternionne sur $\mathbb{Q}$ s'il existe un plongement $\mathcal{O} \to \mathrm{End}(S)$.

Fixons donc une algèbre quaternionne $A = A_{p,q}$ sur $\mathbb{Q}$ (voir [Vo21] pour la théorie des algèbres quaternionnes), disons qui est ramifiée en deux nombres premiers p et q et choisissons un ordre maximal $\mathcal{O} = \mathcal{O}_{p,q}$ dans A. En d'autres termes, pour ℓ premier ou $\ell = \infty$, $A \otimes \mathbb{Q}_\ell$ est isomorphe à $M_2(\mathbb{Q}_\ell)$ si et seulement si $\ell \neq p, q$; sinon, il s'agit d'une algèbre à division sur $\mathbb{Q}_\ell$. Sur $\mathbb{C}$, la courbe de Shimura $X_{p,q}$ paramétrisant les surfaces abéliennes à multiplication quaternionnique par $\mathcal{O}_{p,q}$ s'identifie à la surface de Riemann compacte

$$\mathfrak{H}/\iota(\mathcal{O}_{p,q}^1)$$

où $\mathcal{O}_{p,q}^1$ désigne les éléments de norme (réduite) 1 de $\mathcal{O}_{p,q}$ et ι est un déploiement $A_{p,q} \hookrightarrow A_{p,q} \otimes_{\mathbb{Q}} \mathbb{R} \simeq M_2(\mathbb{R})$, de sorte que $\iota(A_{p,q}^1)$ soit un sous-groupe de $\mathrm{SL}_2(\mathbb{R})$.

Si E est de conducteur pq, la correspondance de Jacquet–Langlands combinée au théorème de modularité montre l'existence d'un morphisme surjectif $\varphi_{p,q} : X_{p,q} \to E$ de courbes algébriques sur $\mathbb{Q}$, obtenue en intégrant la forme modulaire quaternionique associée à E.

On dispose toujours d'une notion de « point CM » sur $X_{p,q}$, correspondant au surfaces abéliennes isogènes au produit d'une courbes elliptique à multiplication complexe avec elle-même. En particulier, les points CM sont encore définis sur le corps de classes de Hilbert et la formule de Gross–Zagier 25 est un théorème de Zhang [Zh01] dans ce cadre. Sur $\mathbb{C}$, les points CM correspondent aux points de $\mathfrak{H}$ dont le stabilisateur sous $\iota(\mathcal{O}_{p,q})$ est un ordre quadratique imaginaire.

Mais cette fois-ci, l'existence de points CM de discriminant D équivaut à ce que $N = pq$ soit non déployé dans $\mathbb{Q}(\sqrt{D})$! Ainsi, il suffit d'analyser la fibre $\varphi_{p,q}^{-1}(0_E)$ pour démontrer

le théorème 1 (encore une fois, pour E de rang analytique ≥ 2, sans torsion, et unique dans sa classe d'isogénie).

Comme dans la section 5, nous allons majorer le nombre de points quadratiques de la fibre sur $\mathbb{Q}_p$. En faisant les calculs, cette majoration sera atteinte pour E de rang 2 et conducteur $2 \cdot 223$ et $p = 223$, et on aura ainsi démontré le théorème 1. Mentionnons simplement le théorème clé nous permettant de faire ces calculs, dont la démonstration est expliquée dans [BC92].

Théorème 32 (Čerednik [Če76], Drinfeld [Dr76])**.** *La courbe de Shimura $X_{p,q}$ est isomorphe comme espace analytique sur $\mathbb{Q}_{p^2}$ au quotient*

$$\mathfrak{H}_p/\iota(\mathcal{O}_{q,\infty}[1/p]^1)$$

où ι est un déploiement $A_{q,\infty} \hookrightarrow A_{q,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq M_2(\mathbb{Q}_p)$.

De plus, les points CM correspondent toujours aux points de $\mathfrak{H}_p$ dont le stabilisateur sous $\iota(\mathcal{O}_{q,\infty}[1/p])$ est un $\mathbb{Z}[1/p]$-ordre quadratique imaginaire.

Comme tout à l'heure, on a une fonction analytique $\psi_E : \mathfrak{H}_p \to \mathbb{C}_p^\times/q_E^{\mathbb{Z}}$ (donnée par intégration contre la forme modulaire quaternionique rigide analytique associée à E) et on souhaite calculer sa fibre en 1. Il se trouve que presque tous les point CM de discriminant 1 tombent dans l'affinoïde standard $\mathfrak{H}_p^\circ$ et que $\Phi_E := \psi_E|_{\mathfrak{H}_p^\circ}$ peut être normalisé de sorte que son image soit contenue dans $\mathcal{O}_{\mathbb{C}_p}^\times$. Alors, le nombre de zéros de $\Phi_E - 1$ dans $\mathbb{Q}_{p^2}$ est majoré par le nombre de zéros de $\mathrm{red}_p(\Phi_E) - 1$ dans $\mathbb{F}_{p^2}$. Les détails seront exposés dans [Ca].

Références

[Ba66] Alan Baker. *Linear forms in the logarithms of algebraic numbers.*Mathematika **13** (1966), 204–216. ↑ii.

[Ba09] Burcu Baran. *A modular curve of level 9 and the class number one problem.* J. Number Theory **129** (2009) 715–728. ↑10.

[Bi03a] András Biró. *Yokoi's conjecture.* Acta Arithmetica **106** (2003) 85–104. ↑iii.

[Bi03b] András Biró. *Chowla's conjecture.* Acta Arithmetica **107** (2003) 179–194. ↑iii.

[Bo14] Siegfried Bosch. *Lectures on formal and rigid geometry.* Lecture Notes in Mathematics **2105**, Springer-Verlag (2014). ↑14.

[BLR90] Siegfried Bosch, Werner Lütkebohmert et Michel Raynaud. *Néron models.* A Series of Modern Surveys in Mathematics **21**, Springer-Verlag (1990). ↑11.

[BC92] Jean-François Boutot et Henri Cayarol. *Uniformisation p-adique des courbes de Shimura : les théorèmes de Čerednik et de Drinfeld.* Courbes modulaires et courbes de Shimura (Orsay, 1987/1988), Astérisque **196-197** (1991) 45–198. ↑14, 20.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond et Richard Taylor. *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises.* J. Amer. Math. Soc. **14** (2001) no. 4, 843–939. ↑12.

[BLK07] Dongho Byeon, Jungyun Lee et Myoungil Kim. *Mollin's conjecture.* Acta Arithmetica **126** (2007) 99–114. ↑iii.

[Ca] Elias Caeiro. *The class number one problem via p-adic uniformisation of Shimura curves.* En cours de préparation. ↑iii, 20.

[CD24] Elias Caeiro et Henri Darmon. *The Heegner–Stark theorem and Stark–Heegner points.* Prépublication (2024). ↑i, iii, 17, 18.

[Če76] I.V. Čerednik. *Uniformisation of algebraic curves by discrete arithmetic subgroups of $PGL_2(k_w)$ with compact quotients.* Math. U.S.S.R Sbornik **29** (1976) no. 1, 123–165. ↑20.

[Co78] Harvey Cohn. *A Classical Invitation to Algebraic Numbers and Class Fields.* Universitext, Springer-Verlag (1978). ↑iii.

[Co13] David A. Cox. *Primes of the form $x^2 + ny^2$*, 2nd ed. Wiley (2013). ↑iii, 6, 10.

[Da01] Henri Darmon. *Integration on $\mathfrak{H}_p \times \mathfrak{H}$ and arithmetic applications.* Ann. of Math. (2) **154** (2001) no. 3, 589–639. ↑iii, 14, 15, 17.

[Da04] Henri Darmon. *Rational points on modular elliptic curves* CBMS Regional Conference Series in Mathematics **101**, AMS Press (2004). ↑iii, 12, 19.

[DR73] Pierre Deligne et Michael Rapoport. *Les schémas de modules des courbes elliptiques.* Modular functions of one variable II, Lecture Notes in Mathematics **349**, Springer-Verlag (1973), 143–316. ↑3.

[DS05] Fred Diamond et Jerry Shurman. *A first course in modular forms.* Graduate Texts in Mathematics **228**, Springer-Verlag (2005). ↑3.

[Dr76] Vladimir G. Drinfeld. *Coverings of p-adic symmetric regions.* Func. Anal. App.**10** (1976) no. 2, 107–115. ↑20.

[Go74] Dorian M. Goldfeld. *A simple proof of Siegel's theorem.* Proc. Natl. Acad. Sci. U.S.A. **74** (1974) no.4, 1055. ↑1.

[GW20] Ulrich Görtz et Torsten Wedhorn. *Algebraic Geometry I : Schemes.* Springer Studium Mathematik – Master, Springer-Verlag (2020). ↑22.

[GZ84] Benedict H. Gross et Don B. Zagier. *Heegner points and derivatives of L-series.* Invent. Math. **84** (1986) no. 2, 225–320. ↑13.

[He52] Kurt Heegner. *Diophantische analysis und modulfunktionen.* Math Z. **56** (1952), 227–253. ↑ii.

[Ke85] Monsur A. Kenku. *A note on the integral points of a modular curve of level* 7. Mathematika **32** (1985) 45–48. ↑10.

[La87] Serge Lang. *Elliptic Functions.* Graduate Texts in Mathematics **112**, Springer-Verlag (1987). ↑iii, 4.

[Ne99] Jürgen Neukirch. *Algebraic Number Theory.* Grundlehren der mathematischen Wissenschaften **322**, Springer-Verlag (1999). ↑1, 3, 7, 24.

[Se97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem.* Aspects of mathematics, Springer-Verlag (1997). ↑iii, 10.

[Sh14] Igor R. Shafarevich. *On the problem on the 10th discriminant.* St. Petersbourg Math. J. **25** (2014) no. 4, 699–711. ↑11.

[Si68] Charles L. Siegel. *Beweise des Starkschen Satzes.* Invent. Math. **5** (1968) 180–191. ↑1.

[Si09] Joseph H. Silverman. *The arithmetic of elliptic curves*, 2nd ed. Graduate Texts in Mathematics **106**, Springer-Verlag (2009). ↑iii, 3, 7, 12.

[Si94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, 2nd ed. Graduate Texts in Mathematics **151**, Springer-Verlag (1994). ↑iii, 8, 9, 12, 15.

[St69] Harold M. Stark. *A complete determination of the complex quadratic fields of class-number one.* Mich. Math. J. **14** (1967), 1–27. ↑ii.

[St69] Harold M. Stark. *On the "gap" in a theorem of Heegner.* J. Number Theory **1** (1969) 16–27. ↑ii.

[TW95] Richard Taylor et Andrew Wiles. *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) **141** (1995) no. 3, 553–572. ↑12.

[Vo21] John Voight. *Quaternion algebras.* Graduate Texts in Mathematics **288**, Springer-Verlag (2021). ↑19.

[We16] Torsten Wedhorn. *Manifolds, sheaves, and cohomology.* Springer Studium Mathematik – Master, Springer-Verlag (2016). ↑23.

[Wi95] Andrew Wiles. *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141** (1995) no. 3, 441–551. ↑12.

[Zh01] Shou-Wu Zhang. *Heights of Heegner points on Shimura curves.* Ann. of Math. (2) **153** (2001) no. 2, 183–290. ↑19.

Annexe : variétés algébriques

Par souci de minimisation, nous présentons la notion de variété selon un point de vue plus classique que celui des schémas de Grothendieck. On pourra consulter [GW20] pour le point de vue moderne des schémas, et [GW20, Section 14.20] pour l'équivalence avec notre point de vue (cf. [GW20, Theorem 14.86]).

Fixons un corps k et commençons par le supposer algébriquement clos. Une partie $X \subseteq k^n$ est dite *algébrique* si elle est le lieu d'annulation commune d'une famille de polynômes. On munit k^n de la topologie dont les fermés sont les ensembles algébriques, appelée *topologie de Zariski*, et on munit les sous-ensembles de k^n de la topologie induite. Une fonction $\varphi : X \to k$ est *régulière* en un point $x \in X$ s'il existe des fonctions polynomiales $f : X \to k$ et $g : X \to k$ telles que $g(x) \neq 0$ et $\varphi = f/g$ sur l'ouvert défini par le lieu de non annulation de g.

Il découle du Nullstellensatz de Hilbert qu'une fonction $\varphi : X \to k$ définie sur un ensemble algébrique X est régulière partout si et seulement si elle est polynomiale. Étant donné un ouvert U de X, on note $\mathcal{O}_X(U)$ l'ensemble des fonctions régulières $U \to k$. La donnée de l'espace topologique X et de la collection de fonctions régulières $\mathcal{O}_X$ est appelé une *variété affine*. On note $\mathbb{A}^n_k$ la variété affine k^n, appelée *espace affine n-dimensionnel*. Un morphisme de variétés affines $X \to Y$ est une application $X \to Y \subseteq k^m$ induite par m fonctions régulières sur X.

Le Nullstellensatz fournit également une anti-équivalence de catégories entre les variétés affines sur k et les algèbres réduites [24] de type fini sur k : à une variété X on associe son algèbre de fonctions régulières $A = \mathcal{O}_X(X)$, et à une algèbre A on associe la variété

24. Càd sans nilpotents

$\operatorname{Spm} A$ dont les points sont l'ensemble des idéaux maximaux de A muni de la topologie de Zariski [25]

Nous allons définir les variétés algébriques comme un type particulier d'espaces annelés.

Définition 33 (Faisceau)**.** *Soit X un espace topologique. Un* faisceau de fonctions $\mathcal{F}$ *sur X est la donnée, pour tout ouvert U de X, d'un ensemble $\mathcal{F}(U)$ de fonctions $U \to k$. Ces fonctions doivent être définies localement, au sens, si $f : U \to k$ est une fonction telle que tout point $x \in U$ admette un voisinage ouvert V pour lequel $f|_V \in \mathcal{F}(V)$, alors, $f \in \mathcal{F}(U)$.*

Définition 34 (Espace annelé)**.** *Un* espace annelé *est une paire $(X, \mathcal{O}_X)$ ou X est un espace topologique et $\mathcal{O}_X$ un faisceau de fonctions sur X (appelé* faisceau structural*). Un morphisme d'espaces annelés $(X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ est la donnée d'une application continue $\varphi : X \to Y$ et d'un morphisme de Y-faisceaux $\varphi_* : \mathcal{O}_Y \to \varphi_*\mathcal{O}_X$ où $\varphi_*\mathcal{O}_X$ désigne le faisceau sur Y défini par $V \mapsto \mathcal{O}_X(\varphi^{-1}(V))$.* [26]

Définition 35 (Variété algébrique)**.** *Une* variété algébrique *sur un corps algébriquement clos k est un espace annelé $(X, \mathcal{O}_X)$ qui est, localement pour la topologie de X, une variété affine. Un morphisme de variétés algébriques $X \to Y$ est un morphisme d'espaces annelés $\varphi : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ telle que, pour tous ouverts affines $V \subseteq Y$ et $U \subseteq \varphi^{-1}(V)$, $\varphi|_U : (U, \mathcal{O}_U) \to (V, \mathcal{O}_V)$ soit un morphisme de variétés affines.*

Remarque 36. On peut de la même manière définir une (pré)variété différentielle comme un espace annelé localement isomorphe à un ouvert de $\mathbb{R}^n$ muni de son faisceau de fonctions C^∞ vers $\mathbb{R}$, cf. [We16].

L'exemple le plus simple de variété algébrique qui ne soit pas affine est celle de l'espace projective $\mathbb{P}^n_k$, obtenu comme recollement de $n+1$ espaces affines $\mathbb{A}^n_k$ comme en géométrie différentielle. Si X est une variété algébrique et $Z \subseteq X$ une partie localement fermée, la restriction des (faisceaux de) fonctions de X à Z muni Z d'une unique structure de sous-variété. Une sous-variété fermée d'un espace projectif est dite *projective*, et une sous-variété localement fermée d'un espace projective est *quasi-projective*.

L'avantage de travailler avec un corps algébriquement clos est que le Nullstellensatz nous dit qu'on peut retrouver une variété affine X à partir de son algèbre de fonctions $A = \mathcal{O}_X(X)$: les points de X s'identifient aux idéaux maximaux de A (à un point $x \in X$ correspond l'idéal $\mathfrak{m}_x$ des fonctions s'annulant en x). Si k n'est pas algébriquement clos,

25. Ou, plus explicitement, on écrit A comme quotient de $k[t_1, \dots, t_n]$ par un idéal $I = (f_1, \dots, f_r)$ en prenant des générateurs de A de sorte que $\operatorname{Spm} A$ s'identifie aux lieux des zéros communs $V(I) \subseteq \mathbb{A}^n_k$ ed $f_1, \dots, f_r$.

26. Intuitivement, φ_* correspond à composer par φ à droite : si f est une fonction sur $V \subseteq Y$, $f \circ \varphi$ est une fonction sur $\varphi^{-1}(V)$.

cela devient totalement faux et une telle approche ne peut pas donner de bonne catégorie de variétés algébriques.

Afin de résoudre cette difficulté, nous définirons donc une variété algébrique sur un corps k comme une variété algébrique sur la clôture algébrique $\overline{k}$ munie d'une « donnée de descente » qui nous assurera que la variété est bien définie sur k. La philosophie à retenir est que les équations définissant une variété sont plus importantes que les solutions de ces équations.

L'intuition est la suivante : X est une variété affine sur k, disons définie par des équations $f_1, \ldots, f_r$, la variété affine $\overline{X} = V(f_1, \ldots, f_r)$ sur $\overline{k}$ dispose d'une action galoisienne canonique et on retrouve les zéros communs dans k des f_i comme les points de $\overline{X}$ invariant sous l'action galoisienne. Nous définissons ainsi une variété algébrique sur k comme la donnée d'une variété algébrique sur $\overline{k}$ munie d'une action galoisienne localement de cette forme.

Définition 37 (Variété algébrique)**.** *Une* variété algébrique X *sur un corps* k *est la donnée d'une variété algébrique* $\overline{X}$ *sur* $\overline{k}$ *munie d'une action galoisienne, c'est-à-dire un morphisme continu* $G_k = \mathrm{Gal}(\overline{k}|k) \to \mathrm{Aut}((\overline{X}, \mathcal{O}_{\overline{X}}))$ [27] *qui est, localement pour la topologie de* X*, donnée par l'action galoisienne canonique sur* $\mathrm{Spm}(A \otimes_k \overline{k})$ *pour une algèbre de type finie* A *sur* k*. Un morphisme de variétés algébriques sur* k *est un morphisme de variétés algébriques sur* $\overline{k}$ *commutant avec l'action galoisienne.*

En particulier, une fonction régulière sur k, c'est-à-dire une fonction $X \to \mathbb{A}^1_k$, correspond à une fonction régulière sur $\overline{X}$ invariante sous G_k, i.e. $\mathcal{O}_X(U) = \mathcal{O}_{\overline{X}}(\overline{U})^{G_k}$. De cette manière, il découle du théorème 90 de Hilbert [Ne99, Chapter IV, Proposition 3.8] qu'on a toujours une correspondance entre les variétés affines sur k et les algèbres géométriquement réduites [28] de type fini sur k.

Un *point rationnel* de X est un élément de $\overline{X}$ dont l'orbite sous G_k est un singleton. Plus généralement, un point de X est une orbite galoisienne d'éléments de $\overline{X}$, c'est-à-dire un élément du quotient ensembliste X/G_k. De la sorte, si A est l'algèbre de fonctions sur X, les points de X s'identifient toujours aux idéaux maximaux de A. De plus, si $x \in X$ est un point correspondant à un idéal maximal $\mathfrak{m}$ de A, le corps de définition de X s'identifie à l'extension finie $K = A/\mathfrak{m}$ de k. Si K est une extension de k, on notera X_K la variété algébrique sur K déduite de X, et $X(K)$ les points rationnels de X_K. Par exemple, $\overline{X} = X_{\overline{k}}$ et $\overline{X} = X(\overline{k})$ comme ensemble.

Il est à noter que certaines variétés peuvent n'avoir aucun point rationnel : c'est par exemple le cas de la variété définie par l'équation $x^2 + y^2 = -1$ sur $\mathbb{R}$ (ayant pour algèbre

27. Dans la catégorie des espaces annelés plutôt que les $\overline{k}$-variétés.
28. Càd les k-algèbres A telles que $A \otimes_k \overline{k}$ soit réduite.

de fonctions $\mathbb{R}[x,y]/(x^2+y^2-1)$). Par opposition à « rationnel », on utilisera l'adjectif « géométrique » pour désigner tout ce qui se passe sur la clôture algébrique. Par exemple, un point géométrique de X est simplement un point de $\overline{X}$, et X est géométriquement connexe si et seulement si $\overline{X}$ est connexe.

Signalons également qu'il existe une notion de dimension pour les variétés algébriques (coïncidant avec la notion usuelle sur $\mathbb{C}$) qui nous permet ainsi de parler de « courbes » et de « surfaces » algébriques.

Définition 38 (Espace irréductible)**.** *Un espace topologique est irréductible s'il est non vide et ne peut pas s'écrire comme l'union de deux fermés stricts.*

Définition 39 (Dimension)**.** *Soit X une variété algébrique sur un corps k. Sa* dimension *est la longueur maximale d d'une chaîne de fermés irréductibles*

$$X_0 \subset \cdots \subset X_d.$$

Une courbe *est une variété de dimension* 1*, une* surface *de dimension* 2*.*

Il existe aussi une notion de *lissité* pour les variétés algébriques. Elle est définie de sorte qu'une variété algébrique sur $\mathbb{C}$ soit lisse si et seulement si c'est une (pré)variété différentielle : un point $x \in X$ est dit *lisse* ou *non singulier* s'il existe un voisinage affine $U \subseteq \mathbb{A}^n_k$ défini par des équations $f_1, \ldots, f_r \in k[t_1, \ldots, t_n]$ tel que la matrice jacobienne

$$J = \left(\frac{\partial f_i}{\partial x_j}\right)$$

soit de rang $\dim U =: \dim_x X$.

Une variété algébrique est dite lisse si elle est lisse partout. On peut montrer qu'une variété lisse sur un corps algébriquement clos est une union disjointe de composantes irréductibles ; ainsi, une variété lisse connexe sur un corps quelconque est géométriquement irréductible.

Enfin, une *forme tordue* d'une k-variété X est une k-variété Y qui devient isomorphe à X sur $\overline{k}$. Il revient au même de changer l'action galoisienne sur $\overline{X}$. Si $\rho : G_k \to \mathrm{Aut}_{\overline{k}}(\overline{X})$ est un cocycle continu, c'est-à-dire qu'il vérifie $\rho(\sigma\tau) = \rho(\sigma)^\tau \circ \rho(\sigma)$, où l'action de G_k sur $\mathrm{Aut}(\overline{X})$ est obtenue par conjugaison, alors on peut tordre l'action $\cdot$ de G_k sur $(\overline{X}, \mathcal{O}_{\overline{X}})$ par ρ pour obtenir une nouvelle action $\star$

$$\sigma \star x := \rho(\sigma)(\sigma x),\ \sigma \star f := \rho(\sigma)_*(\sigma \cdot f),$$

$x \in \overline{X}$ et $f \in \mathcal{O}_{\overline{X}}(U)$. Réciproquement, si Y est une forme de X et $\varphi : Y_{\overline{k}} \to X_{\overline{k}}$ est un isomorphisme,

$$\rho(\sigma) := \varphi^\sigma \circ \varphi^{-1} \in \mathrm{Aut}(\overline{X})$$

définit un cocycle. De la sorte, l'ensemble des classes d'isomorphismes formes tordues de X s'identifie à l'ensemble de cohomologie $H^1(G_k, \mathrm{Aut}(\overline{X}))$, quotient des cocycles $G_k \to \mathrm{Aut}(\overline{X})$ par la relation d'équivalence $\rho \sim \rho'$ s'il existe $\varepsilon \in \mathrm{Aut}(\overline{X})$ tel que $\varepsilon^{\sigma}\rho(\sigma) = \rho'(\sigma)\varepsilon$ pour tout $\sigma \in G_k$.