MÉMOIRE DE TROISIÈME ANNÉE
THÉORÈME DE TORSION DE MAZUR

EMMANUEL LECOUTURIER

Contents

1. Courbes modulaires 4
2. Formes modulaires 5
3. Algèbre de Hecke 7
4. Idées de la preuve du théorème de torsion de Mazur 8
5. Le cas de la 11-torsion 13
6. Quelques généralisations et problèmes ouverts 16
References 17

Les équations diophantiennes (équations dont les solutions sont des nombres entiers ou rationnels) sont un exemple classique et difficile de problème en théorie des nombres. Une cas particulier important d'équations diophantiennes est la recherche de solutions à coordonnées entières ou rationnelles d'équations polynomiales, c'est-à-dire la recherche de points rationnels sur des variétés algébriques. On peut ordonner les variétés algébriques par leur dimension.

Citons par exemple le dernier théorème de Fermat, qui affirme la non existence de points rationnels non triviaux sur la courbe algébrique $x^n + y^n = 1$. Un autre exemple (cette fois facile) est celui des triplets pythagoriciens : trouver tous les triplets $(x, y, z) \in \mathbb{Z}^3$ tels que $x^2 + y^2 = z^2$. Quitte à multiplier par un même entier les variables, on peut supposer $\mathrm{pgcd}(x, y, z) = 1$. Les solutions sont alors $(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2)$ où $(u, v) \in \mathbb{Z}^2$. Une manière élégante de le voir est la suivante. Le problème revient à trouver les points rationnels sur la courbe algébrique $x^2 + y^2 = 1$ (un cercle). Remarquons que le point $P_0 = (x, y) = (1, 0)$ est solution. Alors si $t \in \mathbb{Q}$, considérons la droite de pente t passant par P. Son intersection avec le cercle est un point P à coordonnées rationnelles, et on voit facilement que tous les points rationnels sont obtenus de cette manière. On calcule facilement $P = (\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1})$, et en écrivant $t = \frac{u}{v}$ on retrouve les triplets pythagoriciens.

Pourquoi est-ce que ce dernier problème est facile ? Parce que le cercle est une courbe algébrique de genre 0 (isomorphe à la droite projective). Plus le genre d'une courbe est élevé, plus le problème de trouver les points rationnels sur la courbe est difficile. Le premier cas difficile est celui du genre 1. Le cas du genre > 1 est fondamentalement différent (il y a un nombre fini de points rationnels, par un théorème de Faltings). Notons que le genre de la courbe de Fermat est de genre $\frac{(n-1)(n-2)}{2}$.

Définition 1. Une **courbe elliptique** sur un corps k est une courbe projective lisse connexe de genre 1, possédant un point à coordonnées dans k.

Il y a plusieurs définitions du genre sur un corps quelconque. Le genre g est lié au degré du diviseur canonique apparaissant dans le théorème de Riemann-Roch. Ce théorème permet d'exhiber des fonctions rationnelles non triviales sur notre courbe. En particulier si E est une courbe elliptique et que k est de caractéristique différente de 2 et 3, il existe une équation plane de la forme $y^2 = x^3 + ax + b$ où $a, b \in k$ et $\Delta := -16(4a^3 + 27b^2) \neq 0$ (cette condition sur Δ assure que la courbe est non singulière ; en réalité il faudrait écrire l'équation de E sous une forme homogène $zy^2 = x^3 + axz^2 + bz^3$). On cherche donc toutes les solutions rationnelles de $y^2 = x^3 + ax + b$. Noter qu'il y a déjà le point à l'infini $(x, y, z) = (0, 1, 0)$.

Il existe aussi une définition de courbe elliptique sur un anneau quelconque. Formellement, une courbe elliptique E sur un anneau A est un schéma propre et lisse sur $\mathrm{Spec}(A)$ muni d'une section $e : Spec(A) \to E$, et tel que les fibres sont des courbes elliptiques (sur un corps). Par exemple, on peut penser intuitivement à une courbe elliptique sur $\mathbb{Q}[t]$ comme une famille de courbe elliptique paramètrée par t (e.g. $E : y^2 = x^3 + t$ est une courbe elliptique sur $\mathbb{Q}[t, t^{-1}]$; en $t = 0$ la courbe dégénère en la cubique cuspidale $y^2 = x^3$ qui n'est pas lisse et donc pas une courbe elliptique). Cette notion de courbe elliptique sur un anneau quelconque est très importante car même pour étudier les courbes elliptiques sur $\mathbb{Q}$, on a souvent besoin de parler de courbes elliptiques plus générales. En particulier si E est une courbe elliptique sur $\mathbb{Q}$ et p un nombre premier, on dit que E a **bonne réduction** en p si E se prolonge

en une courbe elliptique sur $\mathbb{Z}_{(p)}$ (on inverse tous les nombres premiers à p). Cela revient à dire qu'on peut trouver une équation $y^2 = x^3 + ax + b$ pour E avec a, $b \in \mathbb{Z}_{(p)}$ et Δ non divisible par p.

En fait l'ensemble des solutions rationnelles (noté $E(\mathbb{Q})$ si E désigne notre courbe elliptique) a une structure naturelle de groupe (abélien). Plus précisément, E a une structure de groupe algébrique (il y a une multiplication $m : E \times E \to E$ et un inverse $i : E \to E$ qui satisfont aux relations usuelles pour les groupes et qui sont des applications polynomiales en les coordonnées). Une preuve directe utilise le théorème de Riemann-Roch.

Le premier résultat intéressant sur $E(\mathbb{Q})$ est :

Théorème 1 (Théorème de Mordell)**.** Soit E une courbe elliptique sur $\mathbb{Q}$. Alors $E(\mathbb{Q})$ est un groupe abélien de type fini. On peut donc écrire $E(\mathbb{Q}) = E_{tors}(\mathbb{Q}) \oplus \mathbb{Z}^r$ où $r \in \mathbb{N}$ est le appelé le **rang** de E et $E_{tors}(\mathbb{Q})$ est la torsion de $E(\mathbb{Q})$.

Idée de preuve. (cf. [8] Chap. IV pour une preuve complète et les rappels de cohomologie galoisienne) Nous montrons quelque chose de plus faible (souvent appelé théorème de Mordell faible) : pour tout entier $n \geq 1$, le groupe $E(\mathbb{Q})/nE(\mathbb{Q})$ est fini. Notons que la finitude de la torsion de $E(\mathbb{Q})$ est facile, car découle de la finitude de ce groupe sur les corps p-adiques (cf [12] Proposition 3.1).

On a une suite exacte :

$$0 \to E(\overline{\mathbb{Q}})[n] \to E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}}) \to 0$$

où la flèche $E(\overline{\mathbb{Q}}) \to E(\overline{\mathbb{Q}})$ est la multiplication par n et $\overline{\mathbb{Q}}$ est une clôture algébrique fixée de $\mathbb{Q}$. Notons $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ le groupe de Galois absolu de $\mathbb{Q}$. En prenant les $G_{\mathbb{Q}}$-invariants de cette suite exacte on obtient

$$E(\mathbb{Q})/nE(\mathbb{Q}) \hookrightarrow Sel^n(E/\mathbb{Q})$$

où

$$Sel^n(E/\mathbb{Q}) := Ker(H^1(G_{\mathbb{Q}}, E(\overline{\mathbb{Q}})[n]) \to \prod_{p \text{ premier}} H^1(G_{\mathbb{Q}_p}, E(\overline{\mathbb{Q}}_p)))$$

On peut montrer que $Sel^n(E/\mathbb{Q})$ est fini, ce qui montre que $E(\mathbb{Q})/nE(\mathbb{Q})$ est fini. Essentiellement cela vient du fait que E a bonne réduction partout sauf en un nombre fini de nombres premiers, ce qui implique que les classes de cohomologie provenant de $E(\mathbb{Q})/nE(\mathbb{Q})$ sont non ramifiées en dehors de ces nombres premiers et des nombres premiers divisant n. Cette restriction sur la ramification est suffisante pour assurer la finitude de $Sel^n(E/\mathbb{Q})$ (penser à $H^1(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z}) = \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ qui est infini, mais les classes non ramifiées en dehors de p_1, ..., p_n correspondent aux rationnels dont les facteurs premiers sont parmi p_1, ..., p_n, et il y en a un nombre fini modulo les carrés).

Remarque. Ce théorème se généralise à toute extension finie K de $\mathbb{Q}$, par la même méthode.

Remarque. Pour une courbe elliptique donnée, on sait calculer $Sel^n(E/\mathbb{Q})$, mais on ne sait pas calculer $E(\mathbb{Q})/nE(\mathbb{Q})$. Cependant on sait calculer $E_{tors}(\mathbb{Q})$.

Le théorème de torsion de Mazur donne la liste des possibilités pour le groupe $E_{tors}(\mathbb{Q})$.

Théorème 2 (Théorème de torsion de Mazur, 1977)**.** Quand E décrit les courbes elliptiques sur $\mathbb{Q}$, $E_{tors}(\mathbb{Q})$ décrit exactement les groupes suivants :

- $\mathbb{Z}/n\mathbb{Z}$ pour $1 \leq n \leq 10$ ou $n = 12$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ pour $n = 2, 4, 6, 8$.

De plus chaque possibilité apparaît une infinité de fois.

La preuve est longue et utilise des outils de géométrie algébrique moderne (en particulier une étude de certains schémas en groupe et de leur cohomologie fppf). Je vais donc seulement donner les grandes lignes. Je suis le plan du cours d'Andrew Snowden ([13]), que je recommande d'ailleurs au lecteur intéressé.

Remarque. Ce théorème peut paraître anecdotique, mais il est crucial dans la preuve du théorème de Fermat. Nous y reviendrons rapidement dans la section 5.

1. Courbes modulaires

Nous allons définir une courbe algébrique affine dont les points correspondent aux courbes elliptiques munies d'une donnée supplémentaire (typiquement un point de torsion). Le théorème de Mazur se reformulera alors en disant que les seuls points rationnels sur une certaine courbe sont les pointes (les points rationnels évidents) Je vais d'abord donner l'énoncé exact puis expliquer intuitivement sa signification.

Théorème 3 (Existence de la courbe modulaire)**.** Soit $N \geq 3$ un entier. Il existe un (unique) schéma affine $Y_1(N)$ lisse sur $Spec(\mathbb{Z}[\frac{1}{N}])$ tel que pour tout schéma S sur $Spec(\mathbb{Z}[\frac{1}{N}])$, on a

$$Y_1(N)(S) = \{(E, P),\ E \text{ est une courbe elliptique sur } S \text{ et } P \text{ est un point d'ordre N de } E(S)\}/\text{isomorphisme}$$

Concrètement, on peut imaginer $Y_1(N)$ comme un sous-ensemble d'un espace affine $\mathbb{A}^d$ défini par des équations polynomiales à coefficients dans $\mathbb{Z}[\frac{1}{N}]$ et dont les points correspondent naturellement aux courbes elliptiques munies d'un point de N-torsion (modulo isomorphisme). Ici «naturellement» veut dire que pour **tout anneau** A dans lequel N est inversible, se donner un point de $Y_1(N)$ à coordonnées dans A revient à se donner une courbe elliptique sur A avec un point de N-torsion (à coordonnées dans A). Intuitivement, se donner une famille de courbes elliptiques munies d'un point de N-torsion paramètrées par une variété S revient à se donner une flèche $S \to Y_1(N)$. Cette dernière propriété est beaucoup plus forte que de simplement dire que les points (disons à coefficients dans $\mathbb{C}$) de $Y_1(N)$ sont en bijection avec les courbes elliptiques + N-torsion sur $\mathbb{C}$.

Notons aussi qu'on suppose $N \geq 3$ dans le théorème. En fait pour $N = 1, 2$ la courbe $Y_1(N)$ n'existe pas. Voici une preuve pour $N = 1$: supposons par l'absurde que $Y_1(1)$ existe. Soient E_1 et E_2 deux courbes elliptiques non isomorphes sur $\mathbb{Q}$ qui deviennent isomorphes sur $\overline{\mathbb{Q}}$ (il en existe, par exemple $y^2 = x^3 + 1$ et $dy^2 = x^3 + 1$ où $d \in \mathbb{N}$ n'est pas un carré – ces deux courbes sont isomorphes sur une extension quadratique de $\mathbb{Q}$). Alors E_2 et E_2 définissent le même point dans $Y_1(1)(\overline{\mathbb{Q}})$ mais des points différents dans $Y_1(1)(\mathbb{Q})$. C'est une contradiction car $Y_1(1)(\mathbb{Q}) \hookrightarrow Y_1(1)(\overline{\mathbb{Q}})$. En fait le vrai problème est l'existence d'automorphismes non triviaux d'une courbe elliptique sur $\mathbb{Q}$ (multiplication par -1). Pour une discussion plus détaillée de ce problème d'automorphismes, cf. [13] Lecture 14.

Le théorème de Mazur implique :

Théorème 4. Pour N premier, $N \geq 11$, $Y_1(N)(\mathbb{Q}) = \emptyset$.

En fait c'est l'essentiel du théorème de Mazur. Nous allons le prouver plus tard pour $N = 11$.

Un dernier point important sur la courbe modulaire : on peut la compactifier de manière naturelle. Plus précisément il existe une courbe naturelle $X_1(N)$ projective et lisse sur $\mathrm{Spec}(\mathbb{Z}[\frac{1}{N}])$ telle que $Y_1(N) \subset X_1(N)$ soit une immersion ouverte (i.e. $Y_1(N)$ est un ouvert de $X_1(N)$). On peut donner à $X_1(N)$ une interprétation d'espace de module : $X_1(N)$ paramètre des courbes elliptiques généralisées (essentiellement une courbe elliptique généralisée sur une variété S est une courbe projective sur S donc les fibres sont soit des courbes elliptiques soit des «courbes elliptiques dégénérées» comme par exemple une courbe nodale $y^2 = x^2(x + 1)$). Pour plus de détails sur la compactification, cf. [13] Lecture 15.

Il existe une autre courbe modulaire intéressante : $X_0(N)$. Nous ne donnons pas la définition formelle car c'est un peu technique. On veut paramétrer les classes d'isomorphisme de couples (E, C) où E est une courbe elliptique (sur une variété algébrique quelconque S) et C est un sous-groupe de E cyclique d'ordre N. On aimerait trouver une courbe $Y_0(N)$ sur $\mathbb{Z}[\frac{1}{N}]$ dont les points correspondent naturellement à ces couples (E, C). Malheureusement une telle courbe n'existe pas à cause de l'automorphisme «multiplication par -1» de (E, C) (noter que si on remplace C par un point d'ordre $N \geq 3$, $-P \neq P$ donc la multiplication par -1 dans E ne préserve pas P, c'est pourquoi $Y_1(N)$ existe mais pas $Y_0(N)$). Cependant il existe un analogue assez proche de l'espace de module («coarse moduli space» en anglais) qu'on note $Y_0(N)$. Sur un corps k, $Y_0(N)(k)$ est en bijection (naturelle en un certain sens) avec les (classes d'isomorphismes de) couples (E, C) sur k. Mais on n'a pas la propriété sur des anneaux plus généraux (i.e. en famille). On peut compactifier $Y_0(N)$ en une courbe $X_0(N)$ (correspondant moralement aux courbes elliptiques généralisées avec une structure de niveau).

2. Formes modulaires

Nous allons maintenant introduire un objet fondamental lié à la courbe modulaire. Notons qu'on peut regarder $Y_1(N)(\mathbb{C})$ comme une courbe algébrique sur $\mathbb{C}$, et donc comme une surface de Riemann.

Définition 2. Une forme modulaire de poids 2 et de niveau $N \geq 3$ est une forme différentielle méromorphe sur $X_1(N)(\mathbb{C})$ et holomorphe sur $Y_1(N)(\mathbb{C})$. On note $M_2(\Gamma_1(N))$ l'ensemble des formes modulaires de poids 2 et de niveau N.

On a une description plus concrète de ce qu'est une forme modulaire (et c'est souvent la définition adoptée en premier). Notons que $Y_1(N)(\mathbb{C})$ paramètre les courbes elliptiques munies d'un point de N-torsion sur $\mathbb{C}$. Rappelons aussi qu'une courbe elliptique sur $\mathbb{C}$ est une surface de Riemann de genre 1, donc un tore complexe. Autrement dit, en tant que surface de Riemann on peut voir une courbe elliptique comme $E = \mathbb{C}/\Lambda$ où Λ est un réseau de $\mathbb{C}$. Tout réseau est (quitte à faire une homothétie) de la forme $\Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau$ où $\tau \in \mathbb{H} := \{z \in \mathbb{C}, \mathrm{Im}(z) > 0\}$. Notons $\Gamma_1(N)$ le sous-groupe de $SL_2(\mathbb{Z})$

constitué des matrices congrues à une matrice unipotente modulo N. On a une action de $SL_2(\mathbb{Z})$ sur $\mathbb{H}$ par homographies : $\begin{pmatrix} a & b \\ c & c \end{pmatrix} \cdot z = \dfrac{az+b}{cz+d}$.

Proposition 1. L'application $\mathbb{H} \to Y_1(N)(\mathbb{C})$ donnée par $\tau \mapsto (E, P) = (\mathbb{C}/\Lambda_\tau, \frac{1}{N})$ induit un isomorphisme de surfaces de Riemann $\Gamma_1(N)\backslash\mathbb{H} \simeq Y_1(N)(\mathbb{C})$.

Soit $\pi : \mathbb{H} \to Y_1(N)(\mathbb{C})$ la projection naturelle. Une forme modulaire ω (par défaut de poids 2) de niveau N est donc telle que $\pi^*(\omega) = f(z)dz$ où $f : \mathbb{H} \to \mathbb{C}$ est holomorphe et $f(z)dz$ est invariante par l'action de $\Gamma_1(N)$. Autrement dit, si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$, $f(\frac{az+b}{cz+d})d(\frac{az+b}{cz+d}) = f(z)dz$. D'où :

Proposition 2. Une forme modulaire est une forme différentielle ω est telle que $\pi^*(\omega) = f(z)dz$ où $f : \mathbb{H} \to \mathbb{C}$ est une fonction holomorphe vérifiant $\forall z \in \mathbb{H}, \forall \gamma = \begin{pmatrix} a & b \\ c & c \end{pmatrix} \in \Gamma_1(N), f(\frac{az+b}{cz+d}) = (cz+d)^2 f(z)$.

On identifie ω et f (on appelle donc f une forme modulaire). Comme $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$, on a $f(z+1) = f(z)$, donc f se développe en série de Fourier $f(z) = \sum_{n\geq 0} a_n q^n$ où $q = e^{2i\pi z}$.

Remarque. Il y a aussi des formes modulaires de poids $k \geq 1$ qui vérifient $\forall z \in \mathbb{H}, \forall \gamma = \begin{pmatrix} a & b \\ c & c \end{pmatrix} \in \Gamma_1(N), f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$.

Posons $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. L'action de $SL_2(\mathbb{Z})$ s'étend à $\overline{\mathbb{H}}$. On peut munir $\Gamma_1(N)\backslash\overline{\mathbb{H}}$ d'une structure de surface de Riemann naturelle.

Proposition 3. On a un isomorphisme naturel de surface de Riemann $\Gamma_1(N)\backslash\overline{\mathbb{H}} \simeq X_1(N)(\mathbb{C})$.

Si f est une forme modulaire, $f(z)dz$ induit une forme méromorphe sur $X_1(N)(\mathbb{C})$, dont les éventuels pôles sont situés aux pointes de $X_1(N)(\mathbb{C})$, c'est-à-dire aux points de $X_1(N)(\mathbb{C}) - Y_1(N)(\mathbb{C})$. Il y a un nombre fini de pointes (elles sont en bijection avec les orbites de $\mathbb{P}^1(\mathbb{Q})$ sous l'action de $\Gamma_1(N)$). Par exemple si N est premier il y a $N-1$ pointes.

Définition 3. On dit qu'une forme modulaire f est **cuspidale** si $f(z)dz$ est holomorphe sur tout $X_1(N)(\mathbb{C})$. On note $S_2(\Gamma_1(N))$ l'ensemble des formes modulaires cuspidales (de poids 2 et de niveau N).

Concrètement, f est cuspidale si quand on écrit $f = \sum_{n\geq 0} a_n q^n$ en série de Fourier au voisinage de chaque pointe, on a $a_0 = 0$ (par défaut on écrit souvent $f = \sum_{n\geq 0} a_n q^n$ pour le développement en série de Fourier en la pointe ∞). Par exemple au voisinage de l'infini, $q = e^{2i\pi z}$, donc $\frac{dq}{q} = 2i\pi \cdot dz$, donc $f(z)dz = \frac{1}{2i\pi} \cdot (\frac{a_0}{q} + \sum_{n\geq 1} a_n q^{n-1})dq$ est holomorphe en ∞ (qui correspond à $q = 0$) si et seulement si $a_0 = 0$ (q est un paramètre local en l'infini).

Proposition 4. L'ensemble $M_2(\Gamma_1(N))$ est un $\mathbb{C}$-espace vectoriel de dimension finie. De plus on peut donner des formules explicites pour la dimension de $M_2(\Gamma_1(N))$ et de $S_2(\Gamma_1(N))$.

Preuve. Cela découle du théorème de Riemann–Roch.

Il existe un moyen de construire des formes modulaires non cuspidales explicites (on connaît leur développement de Fourier en l'infini). Donnons un exemple qui sera utilisé plus tard.

Proposition 5. Soit $N \geq 3$ un nombre premier. Si $n \geq 1$ est un entier, notons $\sigma_1'(n) = \sum'_{d|n} d$ où la somme est restreinte aux d premiers à N. Alors $E_2 := \frac{N-1}{24} + \sum_{n\geq 1} \sigma_1'(n)q^n$ est une forme modulaire de poids 2 et niveau N. On appelle E_2 une série d'Eisenstein.

Il existe une action naturelle de $(\mathbb{Z}/N\mathbb{Z})^\times$ sur $M_2(\Gamma_1(N))$ et $S_2(\Gamma_1(N))$. On peut la voir de la façon suivante. Soit $\Gamma_0(N)$ le sous-groupe de $SL_2(\mathbb{Z})$ constitué des matrices triangulaires modulo N. On a $\Gamma_1(N) \subset \Gamma_0(N)$. L'application $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ donné par $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \pmod N$ induit un isomorphisme $\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$. On a une action de $\Gamma_0(N)$ sur les formes modulaires donnée par $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f(z) = (cz+d)^{-2} f(\frac{az+b}{cz+d})$. Dire que $f \in M_2(\Gamma_1(N))$ revient à dire que f est invariante par $\Gamma_1(N)$. Cela induit une action de $\Gamma_0(N)/\Gamma_1(N) = (\mathbb{Z}/N\mathbb{Z})^\times$ sur $M_2(\Gamma_1(N))$. Si $d \in \mathbb{Z}$ est premier à N, On note $\langle d \rangle$ l'opérateur de $M_2(\Gamma_1(N))$ qui agit par $\overline{d}$ (la réduction de d modulo N) via l'action décrite ci-dessus. Noter que $\langle d \rangle$ préserve $S_2(\Gamma_1(N))$. Si $\mathrm{pgcd}(d, N) > 1$, on pose $\langle d \rangle = 0$.

Notons finalement qu'il y a un isomorphisme naturel de surface de Riemann $\Gamma_0(N)\backslash\overline{\mathbb{H}} \simeq X_0(N)(\mathbb{C})$.

3. Algèbre de Hecke

Nous allons construire des opérateurs fondamentaux qui agissent sur les objets mis en jeu (courbes modulaires, formes modulaires...).

Soit $J_1(N)$ la jacobienne de $X_1(N)$. C'est une variété abélienne sur $\mathbb{Z}[\frac{1}{N}]$ (i.e. une variété algébrique lisse propre sur $\mathbb{Z}[\frac{1}{N}]$ qui possède une loi de groupe – nécessairement commutative – compatible à la structure de variété). Elle a la propriété que si A est une autre variété abélienne sur $\mathbb{Z}[\frac{1}{N}]$, alors tout morphisme $X_1(N) \to A$ se factorise uniquement par $J_1(N)$. Intuitivement on peut penser à la jacobienne d'une courbe X comme paramétrant les fibrés en droite sur X, ou aussi que ses points sont les diviseurs de Weil (relatifs) de degré 0 sur X. Par exemple, $J_0(N)(\overline{\mathbb{Q}}) = Pic^0(X) := \{\sum_{x\in X} \lambda_x x, \lambda_x \text{ est nul pour presque tout } x \text{ et } \sum \lambda_x = 0\}/\{\text{les diviseurs principaux}\}$. Pour la définition précise (et le théorème d'existence de la Jacobienne), cf.[13] Lecture 10. Voir aussi [3].

Soit $n \geq 1$ un entier. On définit un endomorphisme T_n de $J_1(N)$ en termes d'espace de module : $T_n((E, P)) = \sum_C (E/C, (P+C)/C)$ où la somme est sur les sous-groupes cycliques d'ordre n de E tels que $C \cap \langle P \rangle = 0$ où $\langle P \rangle$ est le sous-groupe engendré par P. Noter que T_n ne définit pas un endomorphisme de $X_1(N)$ mais seulement de sa Jacobienne (en fait T_n peut être vu comme une correspondance de $X_1(N)$). Soit $\mathbb{T}_N$ la sous algèbre de $End(J_1(N))$ engendrée par les T_n. C'est l'*algèbre de Hecke* de niveau N et poids 2. La proposition suivante est remarquable.

Proposition 6. L'algèbre $\mathbb{T}_N$ est commutative.

On a aussi une action de $\mathbb{T}_N$ sur $S_2(\Gamma_1(N))$. En effet, $S_2(\Gamma_1(N))$ est l'ensemble des formes différentielles holomorphes sur $X_1(N)$, donc s'identifie à l'espace cotangent de $J_1(N)$ (si on voit la Jacobienne comme une surface de Riemann, on a une description $J_1(N) = H^1(X_1(N), \Omega^1)^\wedge / H_1(X_1(N), \mathbb{Z})$, cf. [3]). Concrètement, si $f = \sum_{n\geq 0} a_n q^n$ est une forme modulaire, $T_m(f) = \sum_{n\geq 0} b_n q^n$ où $b_n = \sum_{d|\mathrm{pgcd}(m,n)} d \cdot a_{mn/d^2}(\langle d \rangle f)$.

Définition 4. On dit que $f \in M_2(\Gamma_1(N))$ est une forme propre si $f \neq 0$ et pour tout $n \geq 1$, il existe $\lambda_n \in \mathbb{C}$ tel que $T_n(f) = \lambda_n \cdot f$.

Remarque. Si $f = \sum_{n\geq 1} a_n q^n$ est une forme propre, nécessairement $a_1 \neq 0$ et $\lambda_n = a_n/a_1$. On normalise souvent f pour avoir $a_1 = 1$ (on dit que f est une forme propre normalisée) ; on a alors $\lambda_n = a_n$.

Remarque. Il n'existe pas nécessairement une base de formes propres pour $S_2(\Gamma_1(N))$, mais c'est vrai si on suppose seulement que $T_n(f) = \lambda_n \cdot f$ pour $\mathrm{pgcd}(n, N) = 1$, car alors ces opérateurs de Hecke sont auto-adjoints pour un produit scalaire sur $S_2(\Gamma_1(N))$.

Il est important de voir $S_2(\Gamma_1(N))$ comme dual de l'algèbre de Hecke.

Proposition 7. La forme bilinéaire $S_2(\Gamma_1(N)) \times \mathbb{T}_N \to \mathbb{C}$ donnée par $(f, T) \mapsto a_1(T(f))$ est un accouplement parfait. De plus une forme f est propre si et seulement si la forme linéaire $\phi_f : \mathbb{T}_N \to \mathbb{C}$ est un morphisme d'anneau. On note I_f le noyau de ϕ_f.

Remarque. Ce point de vue est avantageux pour étudier les formes modulaires à coefficients dans d'autres anneaux que $\mathbb{C}$, par exemple dans $\overline{\mathbb{F}}_p$. Il est aussi pratique pour calculer l'espace des formes modulaires : il suffit de comprendre l'algèbre de Hecke.

4. Idées de la preuve du théorème de torsion de Mazur

Nous allons donner les grandes lignes de la preuve du fait qu'une courbe elliptique sur $\mathbb{Q}$ n'a pas de point de N-torsion si N est un nombre premier ≥ 11. Le cas $N = 11$ sera traité plus tard, de manière plus élémentaire, et le cas $N = 13$ nécessite un travail supplémentaire (ce cas a été prouvé par Mazur-Tate dans [5] avant le théorème de Mazur). On suppose donc que N est premier et est ≥ 17. Cette section nécessite plus de prérequis en géométrie algébrique et théorie des nombres que les autres (par faute de place). Je suis [13] Lecture 1.

On a un morphisme naturel $X_1(N) \to X_0(N)$ sur $\mathbb{Z}[\frac{1}{N}]$. Moralement ce morphisme provient en termes de modules de l'application $(E, P) \to (E, \langle P \rangle)$ où P est un point d'ordre N et $\langle P \rangle$ est le sous-groupe engendré par P. En termes de surfaces de Riemann, ce morphisme correspond à l'application naturelle $\Gamma_1(N)\backslash\overline{\mathbb{H}} \to \Gamma_0(N)\backslash\overline{\mathbb{H}}$. L'application $X_1(N) \to X_0(N)$ est finie (au sens de la géométrie algébrique ; en particulier les fibres sont finies) de degré $\frac{N-1}{2}$ (ce qui correspond au fait que $\Gamma_1(N)/\pm\Gamma_0(N) \simeq (\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$, qui est d'ordre $\frac{N-1}{2}$ car N est premier). Il suffit donc de montrer que $X_0(N)(\mathbb{Q})$ est fini.

C'est un fait général que si X est une courbe (disons sur $\mathbb{Q}$) de genre $g \geq 1$ avec un point rationnel, alors on a une immersion fermée $X \hookrightarrow Jac(X)$ où $Jac(X)$ est la Jacobienne de X (si P_0 est un point

rationnel sur X, on envoie $P \in X$ sur $P - P_0$ en termes de diviseurs). Avec notre hypothèse $N \geq 17$, on a toujours $g(X_0(N)) \geq 2$ (il y a une formule explicite pour le genre – le genre est quadratique en N).

Remarque. Un théorème de Faltings (postérieur au théorème de Mazur) dit que si C est une courbe de genre $g \geq 2$ sur $\mathbb{Q}$ alors $C(\mathbb{Q})$ est fini.

On a donc $X_0(N) \hookrightarrow J_0(N)$ (où $J_0(N) := Jac(X_0(N))$). De plus on sait que $dim(J_0(N)) = g(X_0(N)) \geq 2$ et que $J_0(N)(\mathbb{Q})$ est un groupe abélien de type fini (généralisation du théorème de Mordell aux variétés abéliennes de dimension ≥ 2). Si $J_0(N)(\mathbb{Q})$ est fini, on a terminé. Mais ce n'est bien sûr pas toujours le cas. On va trouver un quotient A de $J_0(N)$ tel que $A(\mathbb{Q})$ est fini et l'application $X_0(N) \to A$ est non constante (donc finie car $X_0(N)$ est une courbe). Cela entraînera que $X_0(N)(\mathbb{Q})$ est fini. Il s'agit donc de trouver un quotient A ni trop petit pour que l'application $X_0(N) \to A$ retienne de l'information géométrique sur $X_0(N)$, ni trop gros pour que $A(\mathbb{Q})$ soit fini.

Voici un critère (très restrictif en fait) pour qu'une variété abélienne ait un nombre fini de points.

Théorème 5. Soient N et p deux nombres premiers avec N impair. Soit A une variété abélienne sur $\mathbb{Q}$. Supposons que :

- A a bonne réduction en dehors de N,
- A a réduction torique en N,
- $A[p](\overline{\mathbb{Q}})$, en tant que représentation de $G_{\mathbb{Q}}$, a une filtration de Jordan-Hölder dont les quotients sont de dimension un et, soit triviaux, soit χ_p où χ_p est le caractère cyclotomique modulo p.

Alors $A(\mathbb{Q})$ est fini.

Expliquons intuitivement ce que signifient ces hypothèses. La première signifie que les équations définissant A (a priori a coefficients rationnels) peuvent se récrire avec des coefficients dans $\mathbb{Z}$ et tels que si on réduit ces équations modulo un nombre premier différent de N, la variété obtenue est lisse (autrement dit A s'étend en un schéma propre et lisse sur $\mathbb{Z}[\frac{1}{N}]$). La deuxième signifie que la réduction modulo N du modèle de Néron de A est un produit de groupes multiplicatifs $\mathbb{G}_m$ après extension des scalaires. En gros, on peut trouver des équations pour A à coefficients dans $\mathbb{Z}$ telles que quand on les réduit modulo N, on obtient une variété isomorphe à $(\mathbb{A}^1_{\overline{\mathbb{F}}_N} \backslash \{0\})^n$ sur $\overline{\mathbb{F}}_N$ (noter que cette courbe n'est pas projective). Pour la dernière hypothèse, rappelons seulement que $\chi_p : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ est un caractère tel que si $g \in G_{\mathbb{Q}}$, on a $g(\zeta_p) = \zeta_p^{\chi_p(g)}$ où ζ_p est n'importe quelle racine primitive p-ième de l'unité. Cette dernière hypothèse est vraiment cruciale et restrictive.

Donnons rapidement l'idée de la preuve (cf. [13] pour les détails). Comme dans la preuve du théorème de Mordell, on a une injection $A(\mathbb{Q})/p^n A(\mathbb{Q}) \hookrightarrow H^1(G_{\mathbb{Q},Np}, A(\overline{\mathbb{Q}})[p^n])$ où $G_{\mathbb{Q},Np}$ est le groupe de Galois de l'extension maximale de $\mathbb{Q}$ non ramifiée en dehors de N et p. Malheureusement ce groupe de cohomologie (qui est fini) n'est pas borné uniformément en n. Soit $\mathcal{A}$ le modèle de Néron de A. C'est un schéma lisse sur $\mathbb{Z}$ qui possède une loi de groupe abélien, et dont la restriction à $\mathbb{Z}[\frac{1}{N}]$ est égal à A. C'est en un certain sens le meilleur modèle de A sur $\mathbb{Z}$. Soit $G_n = \mathcal{A}[p^n]$: c'est un schéma en groupe fini plat sur $\mathbb{Z}$. On peut montrer que $A(\mathbb{Q})/p^n A(\mathbb{Q}) \hookrightarrow H^1_{\text{fppf}}(Spec(\mathbb{Z}), G_n)$ (en fait ce n'est pas exact, il faut considérer la composante connexe de l'identité dans A, mais c'est un détail peu important). Ici *fppf* veut dire qu'on

considère la cohomologie de G_n pour une certaine topologie (de Grothendieck) appelée topologie *fppf*. Cette cohomologie détecte le fait que G_n est fini et plat sur $\mathbb{Z}$ et est donc plus fine que la cohomologie galoisienne (qui ne considère que la fibre générique de G_n). On peut montrer que $H^1_{\text{fppf}}(Spec(\mathbb{Z}), G_n)$ est borné uniformément. La preuve utilise le fait que G_n possède une filtration dont les quotients sont bien connus (il y a quatre possibilités, qui sont des extensions à $Spec(\mathbb{Z})$ de la fibre générique de $\mathbb{Z}/p\mathbb{Z}$ ou μ_p). C'est là qu'on utilise la troisième hypothèse.

Il reste à voir comment trouver un quotient A de $J_0(N)$ qui vérifie les trois hypothèses du théorème. Les deux premières sont automatiques car $J_0(N)$ lui-même les vérifie ($J_0(N)$ a bonne réduction en N par existence de $X_0(N)$ sur $\mathbb{Z}[\frac{1}{N}]$, et a réduction torique en N, ce qui n'est pas évident, cf. [13] Lecture 19). Voyons comment satisfaire la troisième hypothèse. On va utiliser le lien entre les formes modulaires et les représentations galoisiennes.

Théorème 6 (Deligne)**.** Soit $f = \sum_{n\geq 1} a_n q^n \in S_2(\Gamma_0(N))$ une forme propre (normalisée : $a_1 = 1$). Alors pour tout nombre premier p, il existe une unique représentation continue $\rho_f : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{Q}}_p)$ irréductible telle que pour tout nombre premier $\ell \nmid Np$, ρ_f est non ramifiée en ℓ, $Tr(\rho_f(Frob_\ell)) = a_\ell$ et $det(\rho_f(Frob_\ell)) = \ell$.

Remarque. Les a_n sont des entiers algébriques (cela découle du fait que ce sont des valeurs propres des opérateurs de Hecke, qui sont donnés par des matrices à coefficients entiers dans une certaine base).

Si f est une forme propre, on rappelle que $\phi_f : \mathbb{T}_N \to \mathbb{C}$ est le morphisme d'algèbre correspondant. Soit $I_f = Ker(\phi_f)$ (cf. Prop. 7). On pose $A_f = J_0(N)/I_f J_0(N)$ (c'est une variété abélienne sur $\mathbb{Q}$). Si N est premier, $J_0(N)$ est isogène (comprendre presque isomorphe) à $\oplus_f A_f$ où la somme est sur les formes propres normalisées pour $\Gamma_0(N)$. La représentation galoisienne ρ_f attachée à f par le théorème de Deligne provient de $\varprojlim_n A_f[p^n](\overline{\mathbb{Q}})$. En fait quitte à faire un changement de base, ρ_f prend ses valeurs dans $GL_2(\overline{\mathbb{Z}}_p)$. Si on réduit cette représentation modulo l'idéal maximal de $\overline{\mathbb{Z}}_p$, on obtient une représentation galoisienne $\overline{\rho}_f : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_p)$ (cette représentation dépend du choix du réseau $(\overline{\mathbb{Z}}_p)^2$ stable par ρ_f mais la semisimplification de $\overline{\rho}_f$ n'en dépend pas). Alors $\overline{\rho}_f$ correspond à $A_f[p](\overline{\mathbb{Q}})$. Même si ρ_f est irréductible, il se peut que $\overline{\rho}_f$ soit réductible. Dans ce cas la condition sur la trace et le déterminant de ρ_f impose que $\overline{\rho}_f^{ss} = \begin{pmatrix} 1 & 0 \\ 0 & \chi_p \end{pmatrix}$ où χ_p est le caractère cyclotomique modulo p et $\overline{\rho}_f^{ss}$ est la semisimplification de $\overline{\rho}_f$. Autrement dit il existe un idéal premier $\mathfrak{p}$ au-dessus de p dans $\overline{\mathbb{Z}}$ tel que $a_\ell \equiv \ell + 1$ modulo $\mathfrak{p}$ pour tout ℓ premier ne divisant pas Np.

Rappelons que $E_2 = \frac{N-1}{24} + \sum_{n\geq 1} \sigma'_1(n) q^n$ est dans $M_2(\Gamma_0(N))$, et que si $\ell \neq N$ est premier, $\sigma'_1(\ell) = \ell + 1$. Donc E_2 vérifie la congruence cherchée. Mais $E_2 \notin S_2(\Gamma_0(N))$ car E_2 ne s'annule pas en l'infini (sa valeur en l'infini est son coefficient constant $\frac{N-1}{24}$). Pour simplifier supposons que $p \geq 5$. Alors si p divise $N-1$, E_2 est cuspidale modulo p (c'est-à-dire qu'il existe $f \in S_2(\Gamma_0(N))$ dont les coefficients de la q-développement en l'infini sont congrus aux coefficients de E_2). En effet, le coefficient constant en l'infini est clairement nul modulo p, et automatiquement son coefficient constant en l'autre pointe de $X_0(N)$ l'est aussi par la formule des résidus : la somme des valeurs aux pointes est nulle (et il y a deux pointes dans $X_0(N)$ car N est premier). Donc $E_2(z)dz$ est une forme différentielle méromorphe sur $X_0(N)(\mathbb{C})$

qui a des pôles aux pointes, mais la réduction de cette forme différentielle sur $X_0(N)_{\overline{\mathbb{F}}_p}$ est holomorphe, donc provient d'une forme différentielle holomorphe sur $X_0(N)_{\mathbb{C}}$, i.e. d'une forme modulaire cuspidale.

Intuitivement on va donc choisir $A = \oplus_f A_f$ où la somme porte sur les $f \in S_2(\Gamma_0(N))$ congrues à E_2 modulo p. Formellement, on note I l'idéal de $\mathbb{T}$ engendré par les $T_\ell - (\ell+1)$, l'involution d'Atkin-Lehner w_N. Soit $\mathfrak{P} = I + (p)$: c'est l'unique idéal maximal de $\mathbb{T}$ contenant I et de caractéristique résiduelle p. Notons $I_0 = \cap_{n\geq 0}\mathfrak{P}^n$. Alors on pose $A = J_0(N)/I_0J_0(N)$. Moralement, si on écrit $\mathbb{T}$ comme produit d'anneaux associés aux formes propres $f \in S_2(\Gamma_0(N))$ (ce qui est forcément faux car $Spec(\mathbb{T})$ est connexe, mais c'est vrai si on tensorise par $\mathbb{Q}$), I_0 correspond au produit des formes **non** congrues à E_2, et A correspond aux A_f avec f congrue à E_2 modulo **un** idéal maximal au-dessus de p de l'anneau des entiers du corps des coefficients K_f de f (c'est le corps engendré par les coefficients de la q-expansion de f). En fait A ne vérifie pas toujours la troisième condition (cruciale) du théorème 5. Cela correspond au fait qu'en général $K_f \neq \mathbb{Q}$ donc il peut y avoir certains idéal au-dessus de p pour lesquels f est congrue à E_2 et certains pour lesquels f ne l'est pas. Et on ne peut pas sélectionner ces idéaux premiers dans la décomposition $A = \oplus A_f$. Cependant une modification de la preuve du théorème 5 nous permet de montrer que A est de rang nul (cf [13] Lecture 21).

Expliquons pourquoi on peut deviner à l'avance que A est de rang nul. Il s'agit de voir que A_f est de rang nul pour toute f congrue à E_2. Par la généralisation de la conjecture de Birch et Swinnerton-Dyer aux variétés abéliennes, cela devrait être équivalent à ce que $\int_0^\infty f(z)dz \neq 0$ (et en fait on sait maintenant qu'il suffit que $\int_0^\infty f(z)dz \neq 0$).

Considérons le point $P = (0) - (\infty) \in J_0(N)$ (vu comme un diviseur sur $X_0(N)$). Notons que les pointes 0 et ∞ sont les deux seules pointes sur $X_0(N)$ car N est premier (autrement dit, $\Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q})$ est constitué des deux orbites $\Gamma_0(N)0$ et $\Gamma_0(N)\infty$).

Proposition 8. Supposons que le genre de $X_0(N)$ est ≥ 1 (cela revient à supposer $N \geq 11$). Le point P est d'ordre fini un diviseur de $N-1$. De plus P est non nul.

Preuve. Par définition de $J_0(N)$, un diviseur est nul dans $J_0(N)$ si et seulement si il est de la forme $div(f)$ pour une fonction rationnelle f sur $J_0(N)$ ($div(f)$ est la somme des zéros de f moins la somme des pôles de f, avec multiplicité).

Soit $f(z) = \frac{\Delta(z)}{\Delta(Nz)}$ où $\Delta \in S_{12}(SL_2(\mathbb{Z}))$ est l'unique forme cuspidale de poids 12 et niveau 1 (elle correspond, en termes modulaires, au discriminant d'une courbe elliptique, c'est-à-dire que $\Delta(z)$ est le discriminant de $E = \mathbb{C}/(\mathbb{Z} + z\cdot\mathbb{Z})$ pour $z \in \mathbb{H}$). On sait que Δ ne s'annule pas sur $\mathbb{H}$ (par exemple car le discriminant d'une courbe elliptique est non nul par définition). Donc f n'a pas de pôle ni de zéro sur $\mathbb{H}$. Un calcul immédiat montre que si $g(z) \in S_k(SL_2(\mathbb{Z}))$, alors $g(Nz) \in S_k(\Gamma_0(N))$. Donc f est bien une fonction rationnelle sur $X_0(N)$ (en tant que quotient de deux «fonctions» homogènes de degré 12 sur $X_0(N)$). On sait que Δ admet un q-développement $q + \sum_{n\geq 2}\tau(n)q^n$ pour des nombres $\tau(n)$ (entiers en fait – ce qui compte ici c'est que le coefficient devant q est non nul). Donc f a un pôle d'ordre $N-1$ en l'infini. Comme $deg(div(f)) = 0$, $div(f) = (N-1)P$. Cela montre que P est d'ordre un diviseur de $N-1$. Montrons que P est non nul. On sait que l'application $X_0(N) \to J_0(N)$ (donnée par $x \mapsto (x) - (\infty)$) est injective (c'est le théorème d'Abel–Jacobi). Donc l'image de la pointe 0 (qui est P) est non nulle.

Remarque. En fait on peut montrer que l'ordre de P est égal au numérateur du rationnel réduit égal à $\frac{N-1}{12}$. L'existence de P est remarquable (cf. la conjecture de Manin–Mumford).

Le fait que P est non nul signifie que la forme linéaire $S_2(\Gamma_0(N)) \to \mathbb{C}$ donnée par $f \mapsto \int_0^\infty f(z)dz$ est non nulle (si l'on interprète la Jacobienne de X comme la surface de Riemann $H^0(X(\mathbb{C}), \Omega^1)^\vee / H_1(X, \mathbb{Z})$). On peut en déduire que si f est congrue à E_2, $\int_0^\infty f(z)dz \neq 0$ (cf. [6] Proposition 1).

Donnons une dernière motivation pour le choix de A. Un calcul montre que l'idéal d'Eisenstein I annule P. On en déduit que P est d'ordre p dans A. Cela est intéressant car on peut alors essayer de faire une p-descente dans A (comme dans la preuve du théorème de Mordell). On mettra cette idée en application dans le cas $N = 11$.

Concluons cette section en expliquant rapidement le lien entre les courbes elliptiques et le théorème de Fermat. Nous nous référons à [11]. Soient A, B, C trois entiers premiers entre eux tels que $A + B = C$. Considérons alors la courbe elliptique $E_{A,B,C}$ sur $\mathbb{Q}$ donnée par $y^2 = x(x - A)(x + B)$. On l'appelle souvent «courbe de Frey» même si Hellegouarch a introduit cette courbe avant Frey, en 1969. Nous supposerons dans ce qui suit $A \equiv -1 \pmod 4$ et $B \equiv 0 \pmod{32}$.

Proposition 9. La courbe $E_{A,B,C}$ a bonne réduction en dehors de ABC, et a réduction multiplicative aux nombres premiers divisant ABC. Son j-invariant est $2^8 \frac{(C^2-AB)^3}{A^2B^2C^2}$.

Proposition 10. Soit $p \geq 5$ un nombre premier et $E = E_{A,B,C}$. La représentation galoisienne $\rho : G_\mathbb{Q} \to GL_2(\mathbb{F}_p)$ provenant de $E[p]$ est irréductible.

Preuve (cf [11] Proposition 6)**.** Raisonnons par l'absurde. La représentation ρ est alors de la forme $\begin{pmatrix} 1 & * \\ 0 & \chi_p \end{pmatrix}$ ou $\begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}$ (cela découle de la semi-stabilité de E). Dans le premier cas on a un point de $E(\mathbb{Q})$ d'ordre p. Comme E a 4 points de 2-torsion, $E(\mathbb{Q})_{tors} \geq 4p \geq 20$ ce qui contredit le théorème de Mazur. Dans le second cas, on a seulement un sous-groupe $C \subset E$ d'ordre p qui est globalement stable par $G_\mathbb{Q}$. On peut considérer $E' = E/C$ qui possède un point rationnel d'ordre p et 4 points de 2-torsion sur $\mathbb{Q}$, ce qui contredit à nouveau le théorème de Mazur.

Supposons par l'absurde qu'on a une solution $a^p + b^p = c^p$ à l'équation de Fermat avec $abc \neq 0$ (et p premier ≥ 5). Posons $A = a^p$, $B = b^p$ et $C = c^p$ (on suppose sans difficulté que $A \equiv -1 \pmod 4$ et $B \equiv 0 \pmod{32}$).

Proposition 11. La représentation ρ de la proposition précédente est non ramifiée en dehors de 2 et p. De plus elle est peu ramifiée en p (au sens de Serre [11] section 2.4), et modérément ramifiée en 2.

Corollaire 1. Il existe une forme modulaire cuspidale propre $f \in S_2(\Gamma_0(2))$ telle que la représentation $\overline{\rho}_f$ modulo p associée à f par Deligne est égale à la représentation ρ ci-dessus.

La preuve de ce corollaire est très difficile. Pour résumer, cela découle de la modularité des courbes elliptiques semi-stables sur $\mathbb{Q}$, démontrée par Wiles, puis du travail d'optimisation du niveau de Ribet ([10]) (historiquement Ribet a d'abord prouvé que la conjecture de Taniyama implique Fermat puis Wiles

a prouvé la conjecture de Taniyama pour les courbes elliptiques semi-stables). On a directement une contradiction car $S_2(\Gamma_0(2))$ est nul.

Remarque. Plusieurs variantes du théorème de Fermat ont été démontrées par Serre en utilisant la même méthode ([11] section 4.3).

5. Le cas de la 11-torsion

Le but de cette section est de prouver qu'une courbe elliptique sur $\mathbb{Q}$ n'a pas de point de 11-torsion (non nul). Ce cas a été prouvé par Billing et Mahler en 1940 ([1]) de manière complètement explicite et élémentaire.

On sait que $X_0(11)$ et $X_1(11)$ ont pour genre 1 avec un point rationnel (la pointe ∞). Plus précisément, la théorie générale nous dit que $X_1(11)$ et $X_0(11)$ sont des courbes elliptiques (dont l'élément neutre est par convention ∞) avec bonne réduction en dehors de 11, et que l'application naturelle $X_1(11) \to X_0(11)$ est une isogénie de degré 5 (autrement dit cette flèche est surjective et le noyau est de cardinal 5, disons au niveau des $\overline{\mathbb{Q}}$-points). On veut montrer que les seuls points de $X_1(11)(\mathbb{Q})$ sont les 5 pointes rationnelles (il y a 5 autres pointes non rationnelles, qui sont définies sur $\mathbb{Q}(\zeta_{11})$). Il suffit de montrer que $X_0(11)(\mathbb{Q})$ est constitué des 5 pointes (on a vu à la fin de la section précédente que la pointe 0 donnait un point d'ordre 5 sur $X_0(11)$). Notons pour simplifier $X = X_0(11)$.

Premièrement, trouvons une équation cubique explicite (sur $\mathbb{Q}$) pour X. Toute courbe elliptique possède intrinsèquement un j-invariant, qui fournit un revêtement (ramifié) $j : X \to \mathbb{P}^1$, c'est-à-dire que j est une fonction rationnelle sur X. Notons F le corps des fonctions rationnelles (définies sur $\mathbb{Q}$) sur X : F est une extension finie de $\mathbb{Q}(j)$ (le corps des fractions rationnelles en une indéterminée j). Si $\tau \in \mathbb{H}$, notons $j_{11}(\tau) = j(11\tau)$. On vérifie immédiatement que, comme j est invariante sous l'action de $SL_2(\mathbb{Z})$, j_{11} est invariante sous l'action de $\Gamma_0(11)$ (i.e. $j_{11}(\frac{a\tau+b}{c\tau+d}) = j_{11}(\tau)$ pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$). Autrement dit, $j_{11} \in F$.

Proposition 12. Il existe un polynôme irréductible P à coefficients dans $\mathbb{Q}(j)$ tel que $P(j_{11}) = 0$. On a $F = \mathbb{Q}(j, j_{11})$.

Preuve. On a une application $X \to \mathbb{P}^1 \times \mathbb{P}^1$ donnée par $\tau \mapsto (j(\tau), j_{11}(\tau))$. Intuitivement, en termes modulaires, si (E, C) est un «point» de $X_0(11)$, on associe $(j(E), j(E/C))$ (on peut quotienter une courbe elliptique par un sous-groupe fini, cela donne à nouveau une courbe elliptique, même sur un anneau quelconque). Cette application n'est pas injective mais donne un isomorphisme entre un ouvert (nécessairement dense au sens de la topologie de Zariski) de X et une courbe de $\mathbb{P}^1 \times \mathbb{P}^1$. Cette courbe est définie par «$P(x, y) = 0$» pour un $P \in \mathbb{Q}[X, Y]$, ce qui fournit le P de l'énoncé. Le fait que $F = \mathbb{Q}(j, j_{11})$ vient du fait que le corps des fonctions rationnelles de X est le même que celui de tout ouvert.

Il reste à calculer P. Il y a des algorithmes pour calculer les «polynômes modulaires» (comme P), mais les coefficients deviennent extrêmement gros très rapidement. Il y a une autre approche plus efficace en pratique pour calculer l'équation de X. Cette approche est expliquée en détails dans [14], et ne nécessite pas de prérequis. On trouve finalement :

Proposition 13. Une équation cubique pour X est $y^2 + y = x^3 - x^2 - 10x - 20$.

Il s'agit maintenant de calculer $X(\mathbb{Q})$. On a un algorithme pour calculer $X(\mathbb{Q})_{tors}$ (cf. [12] VII Application 3.2). On trouve que $X(\mathbb{Q})_{tors} \simeq \mathbb{Z}/5\mathbb{Z}$ et explicitement,

$$X(\mathbb{Q})_{tors} = \{\infty, (5,5), (16,-61), (16,60), (5,-6)\}$$

Il reste à prouver que X est de rang nul, ce qui est loin d'être évident. Une approche est de faire une 2-descente, c'est-à-dire d'appliquer la preuve du théorème de Mordell présentée ci-dessus pour $n = 2$, mais ce n'est pas le plus naturel et reste hautement calculatoire. C'est cependant faisable (c'est ce que font Billing et Mahler). Ici on a un point d'ordre 5 dans X, donc il est plus naturel de faire une 5-descente. Essayons. On applique la suite exacte longue de cohomologie à

$$0 \to X[5] \to X \to X \to 0$$

(ici on considère les $\overline{\mathbb{Q}}$-points). On obtient $X(\mathbb{Q})/5X(\mathbb{Q}) \hookrightarrow H^1(G_{\mathbb{Q},11,5}, X[5])$ où $G_{\mathbb{Q},11,5}$ désigne le groupe de Galois de la plus grande extension non ramifiée en dehors de 5 et 11 de $\mathbb{Q}$.

Proposition 14. En tant que $G_{\mathbb{Q}}$-module, on a $X[5] = \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$ ($\mathbb{Z}/5\mathbb{Z}$ est vu comme un $G_{\mathbb{Q}}$-module trivial).

Preuve. On sait que $X[5]$ est un $\mathbb{F}_5[G_{\mathbb{Q}}]$-module qui est de dimension 2 en tant que $\mathbb{F}_5$-espace vectoriel. On a une suite exacte $0 \to \mathbb{Z}/5\mathbb{Z} \to X[5] \to \mu_5 \to 0$ de $\mathbb{F}_5[G_{\mathbb{Q}}]$-modules. Il s'agit de voir que cette suite exacte est scindée. En termes matriciels, $X[5]$ correspond à une représentation $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_5)$ donnée par $\rho = \begin{pmatrix} 1 & c \\ 0 & \chi_5 \end{pmatrix}$ où $c : G_{\mathbb{Q}} \to \mathbb{F}_5$ est un cocycle de $H^1(G_{\mathbb{Q}}, \mu_5)$ (écrire la condition $\rho(gg') = \rho(g)\rho(g')$ et identifier les coefficients en haut à droite). Il s'agit de voir que ce cocycle est nul dans $H^1(G_{\mathbb{Q}}, \mu_5)$. On va montrer que ce cocycle est non ramifié en tous les nombres premiers q. C'est évident pour $q \neq 5, 11$. Il va falloir travailler séparément pour $q = 5$ et $q = 11$.

Cas $q = 5$.
Notons qu'on a plus d'information sur $X[5]$: c'est un schéma fini plat sur $\mathbb{Z}[\frac{1}{11}]$, donc a fortiori sur $\mathbb{Z}_5$. On a la suite de schémas en groupes finis plats sur $\mathbb{Z}_5$:

$$0 \to G^0 \to X[5] \to G^{\text{ét}} \to 0$$

où G^0 est connexe et $G^{\text{ét}}$ est étale. Il faut y penser comme dans le cas d'un groupe de Lie G : on a $0 \to G^0 \to G \to G/G^0 \to 0$ où G^0 est la composante connexe de l'identité. Noter que μ_5 est connexe (sa fibre spéciale en 5 est $Spec(\mathbb{F}_5[x]/(x^5 - 1))$ qui est un point car $x^5 - 1 = (x-1)^5$ modulo 5) et que $\mathbb{Z}/5\mathbb{Z}$ est étale (c'est 5 copies disjointes de la base $\mathbb{Z}_5$). Ici, G^0 est distinct de $X[5]$ car $X[5]$ contient une copie de $\mathbb{Z}/5\mathbb{Z}$. Donc $G^0(\overline{\mathbb{Q}})$ est un $\mathbb{F}_5$-espace vectoriel de rang 1 (sinon les fibres génériques de $X[5]$ et G^0 seraient identiques, donc $G^0 = X[5]$ par les résultats de Raynaud [9]). Il fournit le scindage cherché, donc c est non ramifié en 5.

Cas $q = 11$.
On peut scinder facilement la suite exacte $0 \to \mathbb{Z}/5\mathbb{Z} \to X[5] \to \mu_5 \to 0$ localement en 11, en posant X^0

l'ensemble des points de $X[5](\overline{\mathbb{Q}})$ qui ne se réduisent pas sur le noeud modulo 11 (c'est un sous-groupe propre d'ordre 5 de $X(\overline{\mathbb{Q}})$). Ce groupe est distinct de $\mathbb{Z}/5\mathbb{Z}$ car les pointes se réduisent sur le noeud modulo 11.

On a donc prouvé que partout localement c est nul (i.e. la suite est partout localement scindée). Il reste à montrer que c est globalement nul. On a $\rho_{|G_{\mathbb{Q}(\zeta_5)}} = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ donc on obtient (en prenant le noyau de c) une extension E partout non ramifiée abélienne de degré divisant 5 de $\mathbb{Q}(\zeta_5)$. Comme le groupe des classes de $\mathbb{Q}(\zeta_5)$ est trivial, la théorie du corps des classes nous dit que $E = \mathbb{Q}(\zeta_5)$, donc que c est trivial.

Remarque. Il y a une autre preuve plus directe (je remercie Maarten Derickx pour me l'avoir mentionnée). Considérons le morphisme $X_1(11) \to X_0(11)$ (notons que $X_1(11)$ est aussi une courbe elliptique). C'est un morphisme de degré 5 non ramifié. La courbe $X_1(11)$ a 10 pointes : cinq au-dessus de chacune des deux pointes de $X_0(11)$. Les pointes au-dessus de ∞ sont définies sur $\mathbb{Q}$ et celles au-dessus de 0 ne le sont pas (elles sont définies sur $\mathbb{Q}(\zeta_5)$). On prend ∞ pour origine de la loi de groupe de $X_1(11)$. Le groupe engendré par les cinq pointes au-dessus de ∞ dans $X_1(11)$ est $\mathbb{Z}/5\mathbb{Z}$ (en tant que $G_{\mathbb{Q}}$-module), et est le noyau du morphisme $X_1(11) \to X_0(11)$. Le groupe engendré par la pointe 0 de $X_1(11)$ est cyclique d'ordre 25. L'image de ce groupe par notre morphisme donne une section $\mu_5 \hookrightarrow X_0(11)[5]$.

Donc on a $H^1(G_{\mathbb{Q},11,5}, X[5]) = H^1(G_{\mathbb{Q},11,5}, \mathbb{Z}/5\mathbb{Z}) \oplus H^1(G_{\mathbb{Q},11,5}, \mu_5)$. On a $H^1(G_{\mathbb{Q},11,5}, \mathbb{Z}/5\mathbb{Z}) = Hom(G_{\mathbb{Q},11,5}, \mathbb{Z}/5\mathbb{Z})$ est un $\mathbb{F}_5$-espace vectoriel dont les droites sont en bijection avec les extensions de $\mathbb{Q}$ non triviales non ramifiées en dehors de 5 et 11 et de groupe de Galois $\mathbb{Z}/5\mathbb{Z}$. Il y a une telle extension non triviale, qui est $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ (c'est un exercice en théorie du corps de classe). La suite exacte de Kummer nous donne que $H^1(G_{\mathbb{Q},11,5}, \mu_5)$ est un $\mathbb{F}_5$-espace vectoriel de dimension 2 (correspondant aux classes 11 et 5 dans $\mathbb{Q}^\times/(\mathbb{Q}^\times)^5$). Au final, $H^1(G_{\mathbb{Q},11,5}, X[5])$ est de dimension 3. Mais cela nous donne seulement que le rang de $X(\mathbb{Q})$ est plus petit que 2. Il s'agit d'utiliser plus d'informations sur X. On sait que X a bonne réduction en dehors de 11. Il faut tenir compte de la structure intégrale de X dans la cohomologie. Autrement dit, il faut remplacer la suite exacte de cohomologie galoisienne par une suite exacte de cohomologie *fppf* (dont on a déjà vaguement parlé dans la section 6). Comme tout ceci est technique, nous donnons juste les arguments rapidement sans justification.

Soit $\mathcal{X}$ le modèle de Néron de X sur $\mathbb{Z}$. Soit $\mathcal{X}^0$ la composante connexe de 0 dans $\mathcal{X}$.

Proposition 15. On a $\mathcal{X}[5] = \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$ (sur $\mathbb{Z}$).

Proposition 16. On a une suite exacte de faisceaux *fppf* sur $\mathbb{Z}$:

$$0 \to \mathcal{X}^0[5] \to \mathcal{X}^0 \to \mathcal{X}^0 \to 0 \ .$$

Proposition 17. On a $H^1_{fppf}(\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}) = H^1_{fppf}(\mathbb{Z}, \mu_5) = 0$. Par conséquent, $H^1_{fppf}(\mathbb{Z}, \mathcal{X}^0[5]) = 0$.

Corollaire 2. La multiplication par 5 $\mathcal{X}^0(\mathbb{Z}) \to \mathcal{X}^0(\mathbb{Z})$ est surjective.

Notons que $\mathcal{X}^0(\mathbb{Z}) = X^0(\mathbb{Q})$ où $X^0(\mathbb{Q})$ est l'ensemble des points de $X(\mathbb{Q})$ qui se ne se réduisent pas sur la singularité modulo 11 (X a un noeud modulo 11, et on remarque que les pointes de $X[5](\mathbb{Q})$ se

réduisent sur ce noeud). Donc $Card(X^0(\mathbb{Q})) = 0$. Donc tous les points de $X(\mathbb{Q})$ se réduisent sur le noeud modulo 11.

Proposition 18. On a $Card(X(\mathbb{Q})/X^0(\mathbb{Q})) = 5$.

Preuve. Mazur montre que le nombre de composantes connexes modulo N de $J_0(N)$ est num($\frac{N-1}{12}$).

On a donc ce qu'on voulait depuis le début :

Corollaire 3. On a $X(\mathbb{Q}) = X(\mathbb{Q})[5] = \mathbb{Z}/5\mathbb{Z}$.

6. Quelques généralisations et problèmes ouverts

Soit $d \geq 1$ un entier et $S(d)$ l'ensemble des nombres premiers p tels qu'il existe une courbe elliptique sur une extension K de degré plus petit que d de $\mathbb{Q}$ avec un K-point de p-torsion.

Théorème 7 (Merel [6])**.** L'ensemble $S(d)$ est fini. On a $S(d) \subset [1, (1 + 3^{\frac{d}{2}}])$.

Corollaire 4 (Mazur et Kamienny [4])**.** Pour tout entier $d \geq 1$, il existe une constante $B(d)$ telle que pour tout corps K de degré d sur $\mathbb{Q}$, pour toute courbe elliptique E sur K, on a $\mathrm{Card}(E(K)_{\mathrm{tors}}) \leq B(d)$.

Remarque. Parent ([**?**], Corollaire 1.8) donne une majoration explicite sur p^r si il existe une courbe elliptique avec un point de p^r-torsion sur un corps de nombre de degré d.

Théorème 8. On a :

- $S(1) = \{2, 3, 5, 7\}$ (Mazur)
- $S(2) = \{2, 3, 5, 7, 13\}$ (Kamienny, Kenku, Momose)
- $S(3) = \{2, 3, 5, 7, 11, 13\}$ (Parent)
- $S(4) = \{2, 3, 5, 7, 11, 13, 17\}$ (Kamienny, Stein, Stoll)

Voici un problème de Serre lié à la torsion des courbes elliptiques.

Théorème 9 (Serre)**.** Si E est une courbe elliptique sur $\mathbb{Q}$ sans multiplication complexe, soit $\rho_{E,N} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_N)$ la représentation galoisienne (à conjugaison près) correspondant à $E[N](\overline{\mathbb{Q}})$. Il existe une constante C_E (dépendant *a priori* de E) telle que pour tout $N > C_E$, $\rho_{E,N}$ est surjective.

Question 1. Peut-on choisir C_E indépendamment de E ? Peut-on choisir $C_E = 37$?

Question 2. La torsion des variétés abéliennes sur $\mathbb{Q}$ de dimension $d > 1$ est-elle bornée en fonction de d ?

Question 3. Le nombre de points d'une courbe de genre 2 sur $\mathbb{Q}$ est-il borné (indépendamment de la courbe) ?

Question 4. Existe-t-il des courbes elliptiques sur $\mathbb{Q}$ de rang arbitrairement grand ?

Pour cette dernière question, mentionnons un théorème spectaculaire de Bhargava.

Théorème 10. On ordonne les courbes elliptiques par leur hauteur. Il y a une proportion positive de courbes elliptiques sur $\mathbb{Q}$ de rang 0. Le rang moyen des courbes elliptiques sur $\mathbb{Q}$ est < 1.

Question 5. Est-ce qu'en proportion la moitié des courbes elliptiques sur $\mathbb{Q}$ ont rang 0 et la moitié ont rang 1 ?

References

[1] G. Billing and K. Mahler. On exceptional points on cubic curves. *J. London Math. Soc.*, 15:32–43, 1940.

[2] Frank Calegari and Matthew Emerton. On the ramification of Hecke algebras at Eisenstein primes. *Invent. Math.*, 160(1):97–144, 2005.

[3] Conrad. *The shimura construction in weight* 2. Ribet/Stein, 2001.

[4] S. Kamienny and B. Mazur. Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, (228):3, 81–100, 1995. With an appendix by A. Granville, Columbia University Number Theory Seminar (New York, 1992).

[5] B. Mazur and J. Tate. Points of order 13 on elliptic curves. *Invent. Math.*, 22:41–49, 1973/74.

[6] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[7] Loïc Merel. L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$. *J. Reine Angew. Math.*, 477:71–115, 1996.

[8] J. S. Milne. *Elliptic curves*. BookSurge Publishers, Charleston, SC, 2006.

[9] Michel Raynaud. Schémas en groupes de type $(p, \dots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[10] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

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

[12] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[13] Andrew Snowden. Math 679 / elliptic curves. `http://asnowden.com/679/`.

[14] Weston. The modular curves $X_0(11)$ and $X_1(11)$. `http://swc.math.arizona.edu/aws/2001/01Weston1.pdf`.