COURBES ELLIPTIQUES, MODULARITÉ ET LE DERNIER THÉORÈME DE FERMAT

OLIVIER DE GAAY FORTMAN, JANUARY 7, 2021

Contents

0. Introduction

Cette note a pour premier but de donner une idée de la démonstration de Wiles du théorème de modularité pour les courbes elliptiques semistables sur les nombres rationnels, et pour deuxième objectif de démontrer pourquoi ce théorème implique le Dernier Théorème de Fermat. Dans [7], Wiles montre ce résultat:

Theorem 0.1 (Wiles, [7])**.** *Chaque courbe elliptique semi-stable sur $\mathbb{Q}$ est modulaire.*

Avant Wiles, Ribet avait déjà montré dans [4] que Théorème 0.1 impliquerait le Dernier Théorème de Fermat:

Corollary 0.2. *Il n'y a pas d'entiers non nuls a, b, c, n avec $n > 2$ tels que $a^n + b^n = c^n$.*

Le théorème suivant était connu:

Theorem 0.3 (Eichler-Shimura)**.** *Soit $f = \sum c(n)q^n$ une forme modulaire pour $\Gamma_0(N)$ de poids 2, nouvelle et normalisée. Si $c(n) \in \mathbb{Z}$ pour chaque $n \in \mathbb{Z}$, il existe une courbe elliptique E_f avec conducteur N avec la même serie de Dirichlet, i.e. $L(E_f, s) = L(f, s)$.*

Ensemble, Théorèmes 0.1 et 0.3 impliquent en effet le théorème de modularité:

Theorem 0.4 (Modularité)**.** *Une série L de Dirichlet $\sum c(n)n^{-s}$ avec $c(n) \in \mathbb{Z}$ est égale à la série L d'une courbe elliptique semi-stable $E/\mathbb{Q}$ avec conducteur N si et seulement si elle est égale à la série L d'une forme f modulaire pour $\Gamma_0(N)$ nouvelle normalisée.* □

Le point clé de la preuve du Théorème 0.1 est le Théorème 6.3 dans la Section 6, qui est à son tour basé sur l'idée suivante. Soit S un ensemble non-vide et fini de nombres premiers et soit $l \in S$. Soit K_S la limite du systéme des corps de nombres K avec $K/\mathbb{Q}$ non-ramifié sur p pour chaque $p \notin S$, et définir $G_S = \mathrm{Gal}(K_S/\mathbb{Q})$. Fixe une représentation

$$\rho_0 : G_S \to \mathrm{GL}_2(\mathbb{F}_l). \tag{1}$$

Soit $\mathcal{A}$ la catégorie des anneaus noethériens locaux complets $(R, \mathfrak{m})$ qui satisfont $R/\mathfrak{m} = \mathbb{F}_l$.

Definition 0.5. Deux homomorphismes $\rho_1, \rho_2 : G_S \to \mathrm{GL}_2(R)$ sont *équivalents* si $\rho_1 = M\rho_2 M^{-1}$ pour une matrice $M \in \mathrm{Ker}(\mathrm{GL}_2(R) \to \mathrm{GL}_2(\mathbb{F}_l))$. Une *déformation* de ρ_0 est une classe d'équivalence $[\rho]$ de représentations $\rho : G_S \to \mathrm{GL}_2(R)$ telles que $\rho \equiv \rho_0 \mod \mathfrak{m}$.

Avec la Définition 0.5, la représentation ρ_0 de (1) nous donne un foncteur

$$F(\rho_0) : \mathcal{A} \to \mathrm{Set}, \quad R \mapsto \{\text{classes d'équivalence } [\rho] \text{ de déformations } \rho : G_S \to \mathrm{GL}_2(R) \text{ de } \rho_0\}.$$

Mazur a montré (cf. [3], V.8) que pour un certain ensemble $*$ de conditions sur représentations $\rho : G_S \to \mathrm{GL}_2(R)$, le foncteur

$$F(\rho_0)^* : \mathcal{A} \to \mathrm{Set}, \quad R \mapsto \{\text{classes d'équivalence } [\rho] \text{ de } *\text{-déformations } \rho : G_S \to \mathrm{GL}_2(R) \text{ de } \rho_0\}$$

est représentable par un anneau noethérien local complet $\tilde{R}$, qui admet donc une représentation universelle $\tilde{\rho} : G_S \to \mathrm{GL}_2(\tilde{R})$. Si on suppose que ρ_0 est *modulaire* (cf. Section 4) Hida et autres (cf. [3], V.8) ont montré que pour un certain ensemble $*$ de conditions sur représentations $\rho : G_S \to \mathrm{GL}_2(R)$, le foncteur

$$F(\rho_0)^*_M : \mathcal{A} \to \mathrm{Set}, \quad R \mapsto \{\text{classes } [\rho] \text{ de } *\text{-déformations } \textit{modulaires } \rho : G_S \to \mathrm{GL}_2(R) \text{ de } \rho_0\}$$

est représentable par un anneau noethérien local complet $\mathbb{T}$, admettant une représentation universelle $\rho_{\mathbb{T}} : G_S \to \mathrm{GL}_2(\mathbb{T})$. Comme $\tilde{R}$ est universal pour toutes classes de $*$-déformations, il existe un homomorphisme d'anneaux locaux unique $\delta : \tilde{R} \to \mathbb{T}$ tel que $\delta(\tilde{\rho}) \sim \rho_{\mathbb{T}}$. Finalement, si on fait des conditions $*$ aussi fortes que possible mais qui sont satisfaites par la représentation $\rho_{E,l} : G_S \to \mathrm{Aut}_{\mathbb{Z}_l}(T_l E)$ pour une courbe elliptique semi-stable E sur $\mathbb{Q}$ (cf. Section 6), et si on suppose que $\rho_0 : G_S \to \mathrm{GL}_2(\mathbb{F}_l)$ soit modulaire, on a le fait clé suivant:

Theorem 0.6 (Wiles, cf. [3], V.8.7)**.** *L'homomorphisme $\delta : \tilde{R} \to \mathbb{T}$ est un isomorphisme. Autrement dit, chaque déformation ρ de ρ_0 qui satisfait les conditions $*$ est modulaire.* □

Avec ce théorème on peut démontrer le Théorème 0.1 comme suit. On suppose d'abord que la représentation $\bar{\rho}_{E,3} : G_S \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[3]) \cong \mathrm{GL}_2(\mathbb{F}_3)$ est irréductible. Comme la conjecture de Serre (cf. Conjecture 4.5) est vraie (cf. Théorème 4.7), $\bar{\rho}_{E,3}$ est modulaire. Par le Théorème 0.6, la représentation $\rho_{E,3} : G_S \to \mathrm{Aut}_{\mathbb{Z}_3}(T_3 E) \cong \mathrm{GL}_2(\mathbb{Z}_3)$ est modulaire, et donc la courbe elliptique E est modulaire. Si $\bar{\rho}_{E,3}$ n'est pas irréductible, on peut montrer que $\bar{\rho}_{E,5}$ est irréductible. D'après Lemme 6.7 dans Section 6, il existe une courbe elliptique semi-stable E' sur $\mathbb{Q}$ telle que $E'(K_S)[5] \cong E(K_S)[5]$ comme modules Galoissiens, et telle que la représentation $\bar{\rho}_{E',3} : G_S \to \mathrm{Aut}(E'(K_S)[3])$ est irréductible. Ce dernier fait montre (avec les arguments précédents) que E' est modulaire, donc aussi que $\rho_{E',5} : G_S \to \mathrm{Aut}_{\mathbb{Z}_5}(T_5 E')$ est modulaire, ce qui implique que $\bar{\rho}_{E',5} : G_S \to \mathrm{Aut}(E'(K_S)[5])$ est modulaire. Comme $E'(K_S)[5] \cong E(K_S)[5]$, la représentation $\bar{\rho}_{E,5} : G_S \to \mathrm{Aut}(E(K_S)[5])$ est modulaire. Par le

Théorème 0.6, $\rho_{E,5} : G_S \to \mathrm{Aut}_{\mathbb{Z}_5}(T_5 E)$ est modulaire, donc E est modulaire.

Pour plus de détails sur cette preuve, voir Section 6. Une esquisse de la preuve du Dernier Théorème de Fermat est donné dans la Section 7. Les références utilisées sont [3] et [7].

1. Théorie Galoissienne Infinie

Definition 1.1. Soit F un corps, Ω/F une extension algébrique. Alors l'extension Ω/F est *Galoisienne* si elle est normale et séparable. Le *groupe de Galois* de Ω sur F est le groupe $\mathrm{Gal}(\Omega/F) = \mathrm{Aut}_F(\Omega)$.

Corollary 1.2. *Le corps Ω est Galois sur F si et seulement si Ω est la limite inductive d'un système d'extensions Galoisiennes finies sur F.* □

Proposition 1.3 (Topologie de Krull)**.** *Soit Ω/F Galoissienne, $G = Gal(\Omega/F)$. Pour chaque ensemble fini $S \subset \Omega$, note $G(S) = \cap_{s\in S} G_s$. Alors il existe une structure de groupe topologique sur G qui satisfait (et est unique pour) la propriété suivante: les $G(S)$ forment une base de ouverts autour de $1 \in G$. De plus, les $G(S)$ pour S stable sur G forment une base d'ouverts de 1 de sous-groupes ouverts normaux, et on a une isomorphisme de groupes topologiques*

$$Gal(\Omega/F) \to \varprojlim Gal(E/F).$$

□

On a le théorème fondamental de la théorie Galoisienne infinie:

Theorem 1.4. *Soit Ω de Galois sur F avec groupe de Galois G. L'application*

$$\{\text{sous-groupes fermés de } G\} \to \{\text{corps intermédiares } F \subset M \subset \Omega\},$$

défini par $H \mapsto \Omega^H$ est une bijection avec application inverse $M \mapsto Gal(\Omega/M)$. □

2. Le Frobenius

Theorem 2.1 (Dedekind)**.** *Soit K un corps de nombres, $I \subset \mathcal{O}_K$ un idéal. Alors il existe une decomposition unique*

$$I = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i(\mathfrak{p}_i|I)} \subset \mathcal{O}_K$$

où les $\mathfrak{p}_i$ sont des idéaux premiers. □

Definition 2.2. Soit p un nombre premier et $S(p) = \{\mathfrak{p} \in \mathrm{Spec}\mathcal{O}_K : e(\mathfrak{p}|p\mathcal{O}_K) \geqslant 1\}$. On dit que p est *non-ramifié dans K* si $e(\mathfrak{p}|p) = 1$ pour chaque $\mathfrak{p} \in S(p)$.

Soit $K/\mathbb{Q}$ Galoisienne avec groupe de Galois G, $p \in \mathbb{Z}$ premier, $\mathfrak{p} \subset \mathcal{O}_K$ un idéal premier tel que $\mathfrak{p}|p\mathcal{O}_K$. Soit $G(\mathfrak{p}) = \mathrm{Stab}_G(\mathfrak{p}) = \{g \in G : g \cdot \mathfrak{p} = \mathfrak{p}\}$. Alors G agit sur $\mathcal{O}_K$, de là $G(\mathfrak{p})$ agit sur $\mathcal{O}_K/\mathfrak{p} =: k(\mathfrak{p})$. On admet le lemme suivant:

Lemma 2.3. *L'application $f : G(\mathfrak{p}) \to \mathrm{Gal}(k(\mathfrak{p})/\mathbb{F}_p)$ est surjective. De plus, f est un isomorphisme si et seulement si p est non-ramifié dans K.* □

Suppose que $p \in \mathrm{Spec}\mathbb{Z}$ est non-ramifié dans K. Alors il existe un unique élément $F_\mathfrak{p} \in G(\mathfrak{p})$ tel que $f(F_\mathfrak{p}) = [x \mapsto x^p] \in \mathrm{Gal}(k(\mathfrak{p})/\mathbb{F}_p)$. L'élément $F_\mathfrak{p}$ s'appelle l'élément de Frobenius à $\mathfrak{p}$. Pour un autre $\mathfrak{q} \in \mathrm{Spec}\mathcal{O}_K$ qui divise p il existe un $\sigma \in G$: $\sigma\mathfrak{p} = \mathfrak{q}$, d'où $F_\mathfrak{q} = \sigma F_\mathfrak{p} \sigma^{-1}$. De plus, cette construction s'éteind sur les extensions Galoisiennes infinies.

Notation 2.4. Soit S un ensemble non-vide et fini de nombres premiers. On note K_S la limite du système des corps de nombres K avec $K/\mathbb{Q}$ non-ramifié sur p pour chaque $p \notin S$. Remarquez que $K_S/\mathbb{Q}$ est une extension Galoisienne infinie; définir

$$G_S = \mathrm{Gal}(K_S/\mathbb{Q}). \tag{2}$$

Pour chaque $p \notin S$, on peut définir un élément de Frobenius, bien défini à conjugaison près:

$$F_p \in G_S. \tag{3}$$

Proposition 2.5. *Soit $E/\mathbb{Q}$ une courbe elliptique, l un nombre premier, et*

$$S = \{p \in \mathrm{Spec}\mathbb{Z} : E \text{ a mauvaise réduction sur p } \} \cup \{l\} \subset \mathrm{Spec}\mathbb{Z}.$$

Alors l'application canonique $E(K_S)[l^n] \to E(\bar{\mathbb{Q}})[l^n]$ est un isomorphisme $\forall n \in \mathbb{Z}_{\geqslant 1}$.

Proof. Soit $P \in E(\bar{\mathbb{Q}})[l^n]$. On veut montrer qu'il existe une extension Galoisienne finie $K/\mathbb{Q}$ avec $P \in E(K)[l^n]$ telle que chaque $p \notin S$ est non-ramifié dans K. Utilisons Lemme 2.3: on est réduit à montrer qu'il existe une extension Galoisienne finie $K/\mathbb{Q}$ avec $P \in E(K)[l^n]$ telle que pour chaque $p \notin S$ et $\mathfrak{p} \in \mathcal{O}_K : \mathfrak{p}|p$, l'application $G(\mathfrak{p}) \to \mathrm{Gal}(k(\mathfrak{p})/\mathbb{F}_p)$ est injective. Soit K une extension Galoisienne finie telle que $P \in E(K)[l^n]$, $H = \mathrm{Ker}(\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}\langle P \rangle)$, $L = K^H$ et $G = \mathrm{Gal}(L/\mathbb{Q})$. Alors $P \in (E(K)[l^n])^H = (E(K)[l^n])^{\mathrm{Gal}(K/L)} = E(L)[l^n]$. Soit $p \notin S$ et $\mathfrak{p} \in \mathcal{O}_L$ tel que $\mathfrak{p}|p$. Soit $\sigma \in \mathrm{Ker}(G(\mathfrak{p}) \to \mathrm{Gal}(k(\mathfrak{p})/\mathbb{F}_p))$. L'application de réduction $r : E(L)[l^n] \to E(k(\mathfrak{p}))[l^n]$ est injective, donc $r(P) = r(\sigma(P))$ implique que $P = \sigma(P)$; mais $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q})/\mathrm{Gal}(K/K^H) = \mathrm{Gal}(K/\mathbb{Q})/H \to \mathrm{Aut}\langle P \rangle$ est injective, et $\sigma = \mathrm{id}$. □

3. Modules de Tate

Definition 3.1. Pour une courbe elliptique E sur un corps K et un nombre premier l, on définit le *module de Tate* $T_l E$ de E/K comme

$$T_l E = T_l E_{\bar{K}} = \varprojlim_n E(\bar{K})[l^n]. \tag{4}$$

Corollary 3.2. *Pour une courbe elliptique E sur $\mathbb{Q}$ et un nombre premier l, le module de Tate $T_l E$ est un $\mathbb{Z}_l$-module libre de rang 2, et*

$$T_l E/l^n T_l E = E(K_S)[l^n] = E(\bar{\mathbb{Q}})[l^n] \qquad \forall n \in \mathbb{Z}_{\geqslant 1}. \tag{5}$$

□

Soit E, l, S comme dans Proposition 2.5. Définissez G_S comme dans Notation 2.4. L'action de G_S sur chaque $E(\bar{\mathbb{Q}})[l^n]$ définit une action sur $\varprojlim_n E(\bar{\mathbb{Q}})[l^n] = T_l E$, i.e. un homomorphisme continu (i.e. une *représentation*)

$$\rho_{E,l} : G_S \to \mathrm{Aut}_{\mathbb{Z}_l}(T_l E) \cong \mathrm{GL}_2(\mathbb{Z}_l). \tag{6}$$

On admet le lemme suivant:

Lemma 3.3. *Soit E une courbe elliptique sur $\mathbb{F}_p$. Rappeler que $a_p := p + 1 - N_p$, où $N_p = \#E(\mathbb{F}_p)$. Alors la trace de l'endomorphisme de Frobenius $\varphi_p : T_l E \to T_l E$ satisfait*

$$\mathrm{Tr}(\varphi_p | T_l E) = a_p.$$

□

Proposition 3.4. *Soit E, l, S comme dans Proposition 2.5. Soit $p \in \mathrm{Spec}\mathbb{Z} : p \notin S$. Soit $F_p \in Gal(K_S/\mathbb{Q})$ comme dans Équation (3). Alors $Tr(\rho_{E,l}(F_p)|T_l E) = a_p$.*

Proof. Comme $p \notin S$, la réduction E_p de E est une courbe elliptique sur $\mathbb{F}_p$, et le morphisme de réduction $E \to E_p$ induit un isomorphisme de groupes abéliens $T_l E \to T_l E_p$, équivariant pour le homomorphisme $\phi : \mathrm{Gal}(K_S/\mathbb{Q}) \to \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ (qui est induit par les homomorphismes $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(k(\mathfrak{p})/\mathbb{F}_p)$ pour des corps de nombres $K/\mathbb{Q}$ non-ramifiés en dehors de S et $\mathfrak{p} \in \mathrm{Spec}\mathcal{O}_K : \mathfrak{p}|p$). Mais $\phi(F_p) = [x \mapsto x^p] = \varphi_p$ donc Lemme 3.3 montre que

$$\mathrm{Tr}(\rho_{E,l}(F_p)|T_l E) = \mathrm{Tr}(\varphi_p | T_l E_p) = a_p$$

□

4. Modularité

Definition 4.1. Pour un ensemble S non-vide et fini de nombres premiers, une représentation $\rho : G_S \to \mathrm{GL}_2(\mathbb{Z}_l)$ est *modulaire* si $\mathrm{Tr}(\rho(F_p)|\mathbb{Z}_l^2) \in \mathbb{Z}\ \forall p \notin S$ et ils existent $k, N \in \mathbb{N}$ et une forme modulaire parabolique $f = \sum_{n \geqslant 1} c(n) q^n \in S_{2k}(\Gamma_0(N)) :\ \mathrm{Tr}(\rho(F_p)|\mathbb{Z}_l^2) = c(p),\ \forall p \notin S$.

Corollary 4.2. *Pour qu'une courbe elliptique $E/\mathbb{Q}$ soit modulaire, il faut et il suffit que il existe un nombre premier l tel que la représentation*

$$\rho_{E,l} : G_S \to \mathrm{Aut}_{\mathbb{Z}_l}(T_l E)$$

est modulaire. Si c'est le cas, alors $\rho_{E,l}$ est modulaire pour chaque nombre premier l. □

Definition 4.3. Un homomorphisme continu $\rho_0 : G_S \to \mathrm{GL}_2(\mathbb{F}_l)$ est modulair si $\exists k, N \in \mathbb{N}, f = \sum_{n \geqslant 1} c(n) q^n \in S_{2k}(\Gamma_0(N))$ tels que $\mathrm{Tr}(\rho_0(F_p)|\mathbb{F}_l^2) \equiv c(p) \mod l,\ \forall p \notin S$.

Definition 4.4. Soit S un ensemble fini non-vide de nombres premiers, $c = \mathrm{conj} \in G_S = \mathrm{Gal}(K_S/\mathbb{Q})$ la conjugaison complexe. Une représentation $\rho_0 : G_S \to \mathrm{GL}_2(\mathbb{F}_l)$ est *impaire* si $\det \rho(c) = -1$, et *irréductible* s'il n'existe pas un élément non nul $v \in \mathbb{F}_l^2$ avec $\rho(G_S) \cdot \langle v \rangle = \langle v \rangle$.

Conjecture 4.5 (Serre)**.** *Si $\rho_0 : G_S \to GL_2(\mathbb{F}_l)$ est impaire et irréductible, ρ_0 est modulaire.*

Example 4.6. Soit $E/\mathbb{Q}$ une courbe elliptique, l et S comme dans Proposition 2.5. Pour chaque $n \in \mathbb{Z}_{\geqslant 1}$ on a le couplage de Weil ([6], III.8)

$$e_{l^n} : E(\bar{\mathbb{Q}})[l^n] \times E(\bar{\mathbb{Q}})[l^n] \to \mu_{l^n}(\bar{\mathbb{Q}})$$

qui est alternée, bilinéaire, non dégénérée est Galois équivariante ([6], III, 8.1). Par conséquent, $\bigwedge^2 E(\bar{\mathbb{Q}})[l^n] \cong \mu_{l^n}(\bar{\mathbb{Q}}) = \langle \zeta_{l^n} \rangle$; comme $c\zeta_{l^n} = \zeta_{l^n}^{-1}$, la représentation $\rho_{E,l} : G_S \to \mathrm{Aut}_{\mathbb{Z}_l}(T_l E)$ est impaire. Mais $\rho_{E,l}$ n'est pas forcément irréductible: si il existe un élément $P \in E(\mathbb{Q})[l]$, alors $\rho_{E,l}$ ne l'est pas.

Theorem 4.7 (Langlands, Tunnell)**.** *La conjecture de Serre est vraie pour $l = 3$.*

Esquisse de la preuve. On a un plongement $\mathrm{GL}_2(\mathbb{F}_3) \hookrightarrow \mathrm{GL}_2(\mathbb{C})$ ce qui induit un diagramme commutatif

$$\begin{array}{ccccc} G_S & \twoheadrightarrow & \mathrm{GL}_2(\mathbb{F}_3) & \hookrightarrow & \mathrm{GL}_2(\mathbb{C}) \\ \downarrow & & \downarrow & & \downarrow \\ S_4 & = & \mathrm{PGL}_2(\mathbb{F}_3) & \hookrightarrow & \mathrm{PGL}_2(\mathbb{C}). \end{array}$$

Il suffit de montrer que une représentation $\rho : G_S \to \mathrm{GL}_2(\mathbb{C})$ est modulaire si $\pi(\rho(G_S)) = S_4 \subset \mathrm{PGL}_2(\mathbb{C})$, pour $\pi : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{PGL}_2(\mathbb{C})$. Soit $G \subset \mathrm{GL}_2(\mathbb{C})$ un sous groupe fini. Un théorème de Klein dit que $\pi(G)$ est cyclique, diédral, A_4, S_4 ou A_5. Langlands a montré que $\rho : G_S \to \mathrm{GL}_2(\mathbb{C})$ est modulaire si $\pi(\rho(G_S)) = A_4$, et Tunnell si $\pi(\rho(G_S)) = S_4$. □

5. Déformations de Représentations

Notation 5.1. Soit f une eigenforme associée au sous groupe de congruence $\Gamma_1(N) \subset \mathrm{SL}_2(\mathbb{Z})$ de poids $k \geqslant 2$ et charactère χ (voir [1] ou [5]). Alors, si T_n est l'operateur de Heche associé à l'entier n, il existe un entier algébrique $c(n, f)$ tel que $T_n f = c(n, f)f$. Soit K_f le corps de nombres engendré sur $\mathbb{Q}$ par les $\{c(n, f)\}$ et les valeurs de χ, et soit $\mathcal{O}_f \subset K_f$ son anneau des entiers. Pour an idéal premier λ de $\mathcal{O}_f$, soit $\mathcal{O}_{f,\lambda}$ la completion de $\mathcal{O}_f$ sur λ.

Theorem 5.2 (Eichler & Shimura, Deligne, c.f. [7], 0.1)**.** *Pour chaque premier $l \in \mathbb{Z}$ et chaque premier $\lambda | l$ de $\mathcal{O}_f$, il existe une représentation continue*

$$\rho_{\lambda,f} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_{f,\lambda})$$

non-ramifiée en dehors des premiers p divisant Nl et telle que, pour chaque premier $p \nmid Nl$,

$$Tr(\rho_{f,\lambda}(F_p)) = c(p, f), \quad \det\rho_{\lambda,f}(F_p) = \chi(p)p^{k-1}.$$

□

Definition 5.3. Soit

$$\rho_0 : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\bar{\mathbb{F}}_l) \tag{7}$$

une représentation continue telle que $\det \rho_0$ est impair.

(1) On dit que ρ_0 est *modulaire* si ρ_0 et $\rho_{\lambda,f}$ sont isomorphes sur $\bar{\mathbb{F}}_l$ pour certains f, λ et un plongement $\mathcal{O}_f/\lambda \to \bar{\mathbb{F}}_l$.

(2) Si $\mathcal{O}$ est l'anneau des entiers d'un corps local, on dit que

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O})$$

est un *relèvement* de ρ_0 si, pour un certain plongement du corps residuel de $\mathcal{O}$ dans $\bar{\mathbb{F}}_l$, les représentations $\bar{\rho}$ et ρ_0 sont isomorphes sur $\bar{\mathbb{F}}_l$.

(3) Supposons que ρ_0 est modulaire. Une relévement ρ de ρ_0 est *modulaire* si $\rho \cong \rho_{f,\lambda}$ sur $\overline{K_{f,\lambda}}$ pour certains f, λ.

Definition 5.4. (1) On dit que ρ_0 est *ordinaire* sur l si il existe un sous espace vectorielle de dimension 1 de $\bar{\mathbb{F}}_l^2$, stable sur le groupe de decomposition sur l, telle que l'action sur l'espace quotient et non-ramifiée et disctincte de l'action sur la sous espace.

(2) On dit que ρ_0 est *plate* sur l si comme représentation d'un groupe de decomposition sur l, ρ_0 est équivalente à une représentation obtenue à partir d'un schéma en groupes sur $\mathbb{Z}_l$ plat et fini: $\det \rho_0$ restreint à un groupe d'inertie est le caractère cyclotomique.
(3) On dit que ρ est *ordinaire* sur l si, vue comme représentation vers $\bar{\mathbb{Q}}_l^2$, il existe une sous-espace vectorielle de dimension 1 de $\bar{\mathbb{Q}}_l^2$ stable sous le groupe de decomposition sur l et telle que l'action sur l'espace quotient et non-ramifiée.

6. La Preuve de Wiles

Definition 6.1. Soit M un groupe abélien fini, et $\rho : G \to \mathrm{Aut}(M)$ un homomorphisme continu. Le noyeau H de ρ est un sous-groupe ouvert de G, donc $L = \bar{\mathbb{Q}}^H$ est une extension finie de $\mathbb{Q}$. On dit que ρ est *non-ramifié* sur p si p est non-ramifié dans L.

Conditions 6.2. Soit $\rho_0 : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\bar{\mathbb{F}}_l)$ une représentation impaire.

I. La représentation ρ_0 est irréductible.
II. La représentation ρ_0 est ordinaire ou plate.
III. La représentation ρ_0 est absolument irréductible lorsqu'elle est restreinte à $\mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}} l})$.
IV. Si $q \equiv -1 \mod l$ est non-ramifié dans ρ_0, alors soit $\rho_0|_{D_q}$ est réductible sur la clôture algébrique (où D_q est le groupe de decomposition sur q) soit $\rho_0|I_q$ est absolument irréductible (où I_q est un groupe d'inertie sur q).

Theorem 6.3 ([7], 0.2, 3.3)**.** *Soit $\rho_0 : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\bar{\mathbb{F}}_l)$ une représentation impaire, modulaire et satisfaisant les Conditions 6.2. Alors chaque relèvement irréductible*

$$\rho : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O})$$

qui est non-ramifié en dehors d'un emsemble fini de premiers est modulair. □

Rappelons-nous les résultats suivants:

Theorem 6.4 (Mazur, cf. [6], 7.5)**.** *Si $E/\mathbb{Q}$ est une courbe elliptique, alors $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/N\mathbb{Z}$ avec $1 \leqslant N \leqslant 12 : N \neq 11$ ou $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ avec $1 \leqslant N \leqslant 4$.* □

Theorem 6.5 ([6], III, 6.4b)**.** *Soit K un corps avec $m \neq 0$ dans K. Alors $E(\bar{K})[m] = \mathbb{Z}/m \times \mathbb{Z}/m$ pour chaque courbe elliptique E sur K.* □

Theorem 6.6 (cf. [3], V.9.1, V.9.2)**.** *Soit l un nombre premier.*

(1) *Une courbe elliptique $E/\mathbb{Q}$ a bonne réduction sur un nombre premier $p \neq l$ si et seulement si la représentation $\rho_{l^n} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[l^n])$ est non-ramifié $\forall n$.*
(2) *Une courbe elliptique $E/\mathbb{Q}$ a bonne réduction sur l si et seulement si la représentation $\rho_{l^n} : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[l^n])$ est plate $\forall n$.* □

Preuve du Théorème 0.1. Par le Théorème 6.5, $E(\bar{\mathbb{Q}})[3] = \mathbb{Z}/3 \times \mathbb{Z}/3$, donc $\mathrm{Aut}(E(\bar{\mathbb{Q}})[3]) \cong \mathrm{GL}_2(\mathbb{F}_3)$. On conclut que la représentation $\rho_{E,3} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{Z}_3}(T_3E) \cong \mathrm{GL}_2(\mathbb{Z}_3)$ est un relèvement de $\bar{\rho}_{E,3} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[3]) \cong \mathrm{GL}_2(\mathbb{F}_3)$. Supposons d'abord que $\bar{\rho}_{E,3} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[3])$ est irréductible. Par l'Exemple 4.6, $\bar{\rho}_{E,3}$ est toujours impaire, donc par le Théorème 4.7, $\bar{\rho}_{E,3}$ est modulaire. De plus, ce n'est pas dûr de montrer, utilisant le hypothese de la semi-stabilité de E, que le fait que $\bar{\rho}_{E,3}$ est irréductible

implique que $\bar{\rho}_{E,3}$ restreint à $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$ est absolument irréductible. Mais pour une courbe elliptique semi-stable E sur $\mathbb{Q}$ et sa représentation $\bar{\rho}_{E,3} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[3])$, si $q \equiv -1 \mod 3$, soit $\rho|_{D_q}$ est réductible sur la clôture algébrique soit $\rho|_{I_q}$ est absolument irréductible. Comme $E/\mathbb{Q}$ a bonne réduction sur l pour un nombre infini de nombres premiers l, la représentation $\bar{\rho}_{E,3} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[3])$ est non-ramifié en dehors d'un nombre fini de premiers par le Théorème 6.6. Alors le Théorème 6.3 implique que $\rho_{E,3} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{Z}_3}(T_3E)$ est modulaire, donc E est modulaire par le Corollaire 4.2.

Si $\bar{\rho}_{E,3}$ n'est pas irréductible, $\bar{\rho}_{E,5} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[5])$ est irréductible - sinon, une courbe elliptique isogène à E aura points rationnels d'ordres 3 et 15, donc un point rationnel d'ordre 15, ce qui est impossible d'après le Théorème 6.4. On prétend qu'il suffit de montrer que $\bar{\rho}_{E,5} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[5])$ soit modulaire et que sa restriction à $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{-5}))$ soit absolument irréductible. En effet, raisonnant comme avant, le Théorème 6.3 impliquerait que $\rho_{E,5} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{Z}_5}(T_5E)$ soit modulaire, donc E aussi par le Corollaire 4.2.

Montrons-nous alors que $\bar{\rho}_{E,5} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[5])$ restreint à $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{-5}))$ est absolument irréductible et que $\bar{\rho}_{E,5}$ est modulaire. Ce premier fait est une conséquence du fait que $\bar{\rho}_{E,5}$ est irréductible. Pour le deuxième, on utilise le lemme suivant:

Lemma 6.7. *Il existe une courbe elliptique E' sur $\mathbb{Q}$ telle que*

(i) $E'(K_S)[5] \cong E(K_S)[5]$ *comme modules Galoissiens*
(ii) *la représentation* $\bar{\rho}_{E',3} : G_S \to \mathrm{Aut}(E'(K_S)[3]) \cong GL_2(\mathbb{F}_3)$ *est irréductible*
(iii) E' *(ou un 'twist quadratique' de* E'*) a réduction semi-stable sur* 5.

La courbe E' du Lemme 6.7 satisfait toutes les conditions nécessaires pour appliquer le Théorème 6.3. Par conséquent, E' est modulaire et donc $\bar{\rho}_{E',5} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E'(\bar{\mathbb{Q}})[5])$ est aussi modulaire. Comme $E'(K_S)[5] \cong E(K_S)[5]$ par le Lemme 6.7.(i), on voit bien que $\bar{\rho}_{E,5} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[5])$ est modulaire, ce que nous voulions démontrer. □

Preuve du Lemme 6.7. Soit $X(5)_{/\mathbb{Q}}$ la courbe dont les points non cuspidaux classifient les courbes elliptiques avec la structure de niveau 5 pleine. Soit L le corps de décomposition de $\bar{\rho}_{E,5}$ et considérons le twist $X(\rho)_{/\mathbb{Q}}$ de $X(5)_{/\mathbb{Q}}$ défini par la classe de cohomologie de $H^1(\mathrm{Gal}(L/\mathbb{Q}), \mathrm{Aut}\, X(5)_{/L})$ donnée par

$$\bar{\rho}_{E,5} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[5]) \cong \mathrm{GL}_2(\mathbb{F}_5) \subset \mathrm{Aut}\, X(5)_{/L}.$$

Alors E correspond à un point rationel de $X(\rho)_{/\mathbb{Q}}$ et donc aussi d'un composant irréductible C de $X(\rho)_{/\mathbb{Q}}$. Cette courbe C est lisse parce que $X(\rho)_{/\bar{\mathbb{Q}}} = X(5)_{/\bar{\mathbb{Q}}}$ est lisse, et son genre est zéro puisque la même chose est vraie pour les composants irréductibles de $X(5)_{/\bar{\mathbb{Q}}}$. Un point rationel x de C n'est pas cuspidal et corréspond à une courbe elliptique E_x sur $\mathbb{Q}$ avec un isomorphisme $E_x(\bar{\mathbb{Q}})[5] \cong E(\bar{\mathbb{Q}})[5]$ comme modules Galoissiens [2], VI, 3.2. Maintenant, il reste qu'à montrer qu'on peut choisir le point x sur C tel que E_x satisfait les conditions (ii) et (iii) de l'énoncé (pour cela, voir le dernier paragraphe du preuve du 5.2 dans [7]). □

7. Le Dernier Théorème de Fermat

Fixe une représentation continue irréductible

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}), \tag{8}$$

où $\mathbb{F}$ est un corps fini de caractéristique $l \geqslant 3$. Suppose ρ est modulaire de poids N. Suppose de plus que p est un nombre premier qui divise exactement N (on écrit $p||N$), et restreigner ρ à un groupe de décomposition de G pour p. On peut voir cette restriction comme une représentation ρ_p de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Definition 7.1. ρ est *finie* sur p s'il existe un schéma en $\mathbb{F}$-espaces vectorielles H sur $\mathbb{Z}_p$ plat et fini, pour lequel l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ sur la $\mathbb{F}$-espace vectorielle $H(\bar{\mathbb{Q}}_p)$ est ρ_p.

Theorem 7.2 (Ribet, [4], 1.1)**.** *Sous les hypothèses précédentes, suppose de plus que ρ est finie sur $p : p||N$. Si $p \not\equiv 1 \mod l$ ou N est premier à l, alors ρ est modulaire de poids N/p.*

Proof of Corollary 0.2. Suppose que (a, b, c) est un triple d'entiers non nuls relativement premiers qui satisfont l'équation

$$a^l + b^l + c^l = 0 \tag{9}$$

avec $l \geqslant 5$ (le cas $l = 3$ était démontré par Euler). En permutant (a, b, c) on peut supposer b est pair et $a \equiv 3 \mod 4$. Définir E comme la courbe elliptique sur $\mathbb{Q}$ avec l'équation

$$y^2 = x(x - a^l)(x + b^l). \tag{10}$$

On peut calculer que le discriminant de E est $\Delta = 16a^{2l}b^{2l}c^{2l}$, et que son conducteur est $N = \prod_{p|abc} p$. Donc E est semi-stable, et *a posteriori* E est modulaire à cause du Théorème 0.1. Alors il existe une forme modulaire f pour $\Gamma_0(N)$ de poids 2, nouvelle et normalisée, avec $L(f, s) = L(E, s)$ (cf. Théorème 0.4). Considérons la représentation

$$\bar{\rho}_{E,l} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\bar{\mathbb{Q}})[l]) \cong \mathrm{GL}_2(\mathbb{F}_l). \tag{11}$$

Cette représentation est irréductible à cause de [5], 4.1.6, et finie sur chaque $p \neq 2$, $p|N$ à cause du [5], 4.1.9 et 4.1.12. Supposer que N est divisible par l. Alors $\bar{\rho}_{E,l}$ est finie sur $p = l$, et comme $l \not\equiv 1 \mod l$, le Théorème 7.2 implique que $\bar{\rho}_{E,l}$ est modulaire de niveau N/l. On conclut que $\bar{\rho}_{E,l} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_l)$ est modulaire pour un certain niveau N_0 qui divise N et qui est premier à l: en effet, soit $N_0 = N$ si l ne divise pas N et $N_0 = N/l$ si l divise N. Maintenant soit $2 \neq p \neq l$ un nombre premier tel que $p|N_0$. Parce que $\bar{\rho}_{E,l} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_l)$ est finie sur $p \neq 2$, que $p|N$, que $\bar{\rho}_{E,l}$ modulaire de niveau N_0, et que N_0 est premier à l, le Théorème 7.2 implique que $\bar{\rho}_{E,l}$ est modulaire de niveau N_0/p. Comme b est pair, $2|N_0$; en répétant cette procédure, on trouve que $\bar{\rho}_{E,l}$ est modulaire d'un niveau $M : 2|M|N$ tel qu'il n'existe pas un nombre premier $p \neq 2$ tel que $p|M$. Autrement dit, $\bar{\rho}_{E,l}$ est modulaire de niveau 2, ce qui est absurde parce que $S_2(\Gamma_0(2)) = \{0\}$. (En effet, on a un isomorphisme $S_2(\Gamma_0(M)) \cong H^0(X_0(M), \Omega^1_{X_0(M))})$ pour chaque M ([3], III.3.3) et le genre de $X_0(2)$ est 0: appliquer la formule de genre de Hurwitz à l'application quotient $X_0(2) \to X_0(1)$ sachant que le genre de $X_0(1)$ est 0 ([3], V.1.9)). □

References

[1] Fred Diamond and Jerry Shurman. *A first course in modular forms*. Graduate texts in mathematics. New York: Springer, 2005. ISBN: 978-1-4419-2005-8.

[2] Vladimir Drinfeld. "Two-dimensional l-adic representations of the fundamental group of a curve over a finite field and automorphic forms on GL(2)". In: *Amer. J. Math.* 105.1 (1983), pp. 85–114. ISSN: 0002-9327. DOI: 10.2307/2374382. URL: https://doi.org/10.2307/2374382.

[3] James Milne. *Elliptic Curves*. Kea books. BookSurge Publishers, 2006. ISBN: 9781419652578. URL: https://books.google.fr/books?id=g-urAAAACAAJ.

[4] Kenneth Ribet. "On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms". In: *Invent. Math.* 100.2 (1990), pp. 431–476. ISSN: 0020-9910. DOI: 10.1007/BF01231195. URL: https://doi.org/10.1007/BF01231195.

[5] Jean-Pierre Serre. "Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$". In: *Duke Math. J.* 54.1 (1987), pp. 179–230. DOI: 10.1215/S0012-7094-87-05413-5. URL: https://doi.org/10.1215/S0012-7094-87-05413-5.

[6] Joseph Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Dordrecht: Springer, 2009. DOI: 10.1007/978-0-387-09494-6. URL: https://cds.cern.ch/record/1338326.

[7] Andrew Wiles. "Modular Elliptic Curves and Fermat's Last Theorem". In: *Annals of Mathematics* 141.3 (1995), pp. 443–551. ISSN: 0003486X. URL: http://www.jstor.org/stable/2118559.