La Conjecture de Shimura-Taniyama-Weil est enfin Démontrée

Henri Darmon*

September 9, 2007

Le 23 juin 1993, Andrew Wiles révèle sa stratégie pour démontrer la conjecture de Shimura-Taniyama-Weil. Sa démonstration subséquente de cette conjecture—pour certaines courbes elliptiques, dites semi-stables, sur le corps $\mathbb{Q}$ des nombres rationnels—suffit déjà à démontrer le dernier théorème de Fermat, grâce aux travaux antérieurs de Gerhard Frey, Jean-Pierre Serre et Kenneth Ribet. Mais la conjecture de Shimura-Taniyama-Weil reste à démontrer dans le cas général. Six ans après, elle succombe enfin aux efforts de Christophe Breuil, Brian Conrad, Fred Diamond, et Richard Taylor.

La Conjecture

La conjecture de Shimura-Taniyama-Weil relie les *courbes elliptiques*—courbes définies par une équation du troisième degré en deux variables de la forme $y^2 = x^3 + ax + b$, où a and b sont des nombres rationnels—aux *formes modulaires*—objets, définis ci-dessous, provenant d'un domaine des mathématiques en apparence très éloigné des courbes elliptiques.

Une fois munie d'un "point à l'infini" qui joue le rôle de l'élément neutre, toute courbe elliptique E possède une loi de groupe naturelle compatible à sa structure de courbe algébrique. (On dit aussi que E est un *groupe algébrique*.) Géométriquement, la somme de deux points P et Q sur E s'obtient en traçant la droite passant par P et Q. En général cette droite coupe E en un troisième

*Henri Darmon est professeur adjoint de mathématiques à l'Université McGill et membre du CICMA (Centre Interuniversitaire en Calcul Mathématique Algébrique) et du CRM (Centre de Recherches Mathématiques). e-mail: darmonmath.mcgill.ca.

point R. On définit la somme de P et Q comme la réflection de R autour de l'axe des abscisses.

C'est cette loi de groupe qui justifie en grande partie l'interêt des courbes elliptiques. En effet, parmi toutes les *courbes projectives* (définies par une équation en deux variables, et compactifiées par l'ajout de points à l'infini convenables) les courbes elliptiques sont les seules à être munies d'une telle loi, dont on démontre qu'elle est forcément commutative.

Après un changement de variables approprié, destiné à mettre l'équation de E sous une forme aussi simple que possible, cette équation peut être réduite modulo un nombre premier p quelconque. Si l'équation réduite n'a pas de singuliarités sur le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ à p éléments, on dit que E a *bonne réduction* en p. Par exemple la courbe elliptique définie par l'équation

$$y^2 = x^3 - x^2 + 1/4, \text{ ou de manière équivalente, } y^2 + y = x^3 - x^2, \tag{1}$$

a bonne réduction en p pour tout p différent de 11.

Soit N_p le nombre de solutions (sur $\mathbb{F}_p$) de l'équation réduite et posons $a_p(E) = p - N_p$. La suite $\{a_p(E)\}_p$ (où p parcourt les nombres premiers de bonne réduction) est un invariant arithmétique naturel de la courbe. La table 1 donne quelques termes de la suite $a_p(E)$ pour la courbe elliptique décrite par l'équation (1).

p	2	3	5	7	11	13	17	19	23	29	31	$\cdots$	10007
N_p	4	4	4	9	–	9	19	19	24	29	24	$\cdots$	9989
$a_p(E)$	-2	-1	1	-2	–	4	-2	0	-1	0	7	$\cdots$	18

Table 1. La suite $a_p(E)$ pour la courbe elliptique (1).

Les suites arithmétiques de ce genre, et la découverte des lois qui les régissent, figurent parmi les préoccupations majeures de la théorie des nombres. Considérons par exemple le cas plus simple de l'équation du second degré à une variable $x^2 - d = 0$, où d est un entier. Les premiers qui ne divisent pas $2d$ représentent les nombres premiers de bonne réduction pour cette équation, et pour un tel p l'entier N_p est alors égal à 2 ou 0, suivant que d est un carré ou non modulo p. Grâce à la loi de réciprocité quadratique de Gauss, on sait que cette propriété de p ne dépend que de la classe de congruence de p modulo $4d$, et que la suite N_p est donc périodique de période $4d$.

Dans le cas des courbes elliptiques, la suite $a_p(E)$ obéit une loi du même genre, mais bien plus subtile. Ce n'est que dans les années 50 qu'elle fut formulée, de manière conjecturale, grâce aux travaux de Shimura, Taniyama, et Weil. Cette loi repose sur la notion de *forme modulaire de poids deux*—c'est-à-dire, une fonction analytique, définie sur le demi-plan de Poincaré $\{z \in \mathbb{C} \text{ avec } \mathrm{Im}(z) > 0\}$, satisfaisant certaines conditions de croissance au bord ainsi qu'une équation fonctionnelle de la forme

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z), \quad \text{pour tout } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

où Γ est un certain "sous-groupe de congruence" de $\mathbf{SL}_2(\mathbb{Z})$. Le prototype d'un sous-groupe de congruence, suffisant pour la formulation de la conjecture de Shimura-Taniyama-Weil, est le groupe $\Gamma_0(N)$ des matrices de déterminant 1 de la forme $\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}$, où a, b, c et d appartiennent à $\mathbb{Z}$. Une *forme modulaire de poids deux* sur $\Gamma_0(N)$ (dite aussi *de niveau* N) est, en particulier, invariante par la translation $z \mapsto z+1$. On peut donc la représenter par une *série de Fourier*

$$f(z) = \sum_{n=0}^{\infty} a_n(f) q^n, \quad \text{où } q = e^{2\pi i z}.$$

On s'interesse particulièrement aux "formes paraboliques", satisfaisant une condition plus forte de croissance au bord, qui implique en particulier que $a_0(f) = 0$. Soit E une courbe elliptique quelconque, définie sur $\mathbb{Q}$. La conjecture de Shimura-Taniyama-Weil affirme alors qu'il existe un entier $N \geq 1$ et une forme parabolique f de poids deux et de niveau N, normalisée pour que $a_1(f) = 1$, telle que

$$a_p(E) = a_p(f),$$

pour tous les premiers p de bonne réduction pour E. La courbe E est alors dite *modulaire*.

La conjecture prédit aussi la valeur du niveau N: il s'agirait du "conducteur" de E, une quantité qui mesure la complexité diophantienne de l'équation minimale associée à E. Il est seulement divisible par les nombres premiers de mauvaise réduction de E. Si p divise N, mais non p^2, alors on dit que E est *semi-stable* en p. En particulier, E est semistable en tout p si et seulement si N est sans facteurs carrés. Dans ce cas on dit simplement que E est *semi-stable*.

Par exemple, la courbe elliptique décrite par l'équation (1) est de conducteur 11. On remarque par ailleurs que l'espace des formes modulaires paraboliques de niveau 11 est de dimension un, engendré par la fonction

$$\begin{aligned} q \prod_{n=1}^{\infty} & (1-q^n)^2 \cdot (1-q^{11n})^2 \\ = \; & q - \mathbf{2q^2} - \mathbf{q^3} + 2q^4 + \mathbf{q^5} + 2q^6 - \mathbf{2q^7} \\ & - 2q^9 - 2q^{10} + \mathbf{q^{11}} - 2q^{12} + \mathbf{4q^{13}} + 4q^{14} \\ & - q^{15} - 4q^{16} - \mathbf{2q^{17}} + 4q^{18} + 2q^{20} + 2q^{21} \\ & - 2q^{22} - \mathbf{q^{23}} - 4q^{25} - 8q^{26} + 5q^{27} - 4q^{28} \\ & + 2q^{30} + \mathbf{7q^{31}} + \cdots + \mathbf{18q^{10007}} + \cdots \end{aligned}$$

Le lecteur notera que le coefficient de q^p coincide avec le nombre $a_p(E)$ de la table 1, obtenu par un calcul entièrement différent.

Au début de Juin 1993, la conjecture de Shimura-Taniyama-Weil semble poser une barrière infranchissable, ce qui explique la surprise avec laquelle est accueillie l'annonce par Wiles d'une démonstration de la modularité de toute les courbes elliptiques semi-stables. Démonstration publiée en 1994, dans une série de deux articles [W] et [TW], le second en collaboration avec Taylor. Peu après, Diamond [Di1] montre que l'on peut se passer de l'hypothèse de semi-stabilité en tous les premiers sauf 3 and 5. Ce résultat est amélioré en 1998 par Conrad, Diamond, et Taylor [CDT], qui réussissent à démontrer la conjecture de Shimura-Taniyama-Weil pour toutes les courbes elliptiques dont le conducteur n'est pas divisible par 27. Enfin, au début de l'été de 1999, la démonstration complète de la conjecture de Shimura-Taniyama-Weil est annoncée par Breuil, Conrad, Diamond, et Taylor.

L'importance de la conjecture

Le travail de Breuil, Conrad, Diamond, et Taylor met terme à un parcours—allant de la formulation de la conjecture de Shimura-Taniyama-Weil, à sa démonstration éventuelle—qui figure parmi les plus belles réussites de la théorie des nombres du vingtième siècle. En effet, l'importance de la conjecture de Shimura-Taniyama-Weil se manifeste à bien des niveaux, dont on mentionnera trois:

Le dernier théorème de Fermat

Tout d'abord, la conjecture de Shimura-Taniyama-Weil implique le dernier théorème de Fermat. Ce fait peut paraître surprenant au premier abord, car l'équation $x^n + y^n = z^n$ n'est pas du troisième dégré et n'a donc pas de rapport évident avec les courbes elliptiques. C'est Frey qui a eu l'idée d'associer à une solution non triviale (a, b, c) de l'équation $x^p + y^p = z^p$ une courbe elliptique $E_{a,b,c}$ (appelée maintenant "courbe de Frey"), donnée par l'équation $y^2 = x(x - a^p)(x + b^p)$. Si a, b et c sont premiers entre eux, on peut les réarranger et changer leurs signes pour que le conducteur de E soit le produit des premiers divisant abc. En particulier E est semi-stable. Ribet, guidé par des conjectures de Serre, montre qu'une telle courbe elliptique ne peut être associée à une forme modulaire de la manière prédite par la conjecture de Shimura-Taniyama-Weil. Cette conjecture implique donc le dernier théorème de Fermat.

Parce que la courbe de Frey est semi-stable, le résultat original de [W] et [TW] est suffisant pour démontrer le dernier théorème de Fermat. Le résultat de Breuil, Conrad, Diamond, et Taylor n'apporte donc rien de nouveau sur l'équation de Fermat proprement dite. Il implique par contre d'autres résultats de même nature. Ainsi, si $n \geq 3$, un cube parfait ne peut s'exprimer comme la somme de deux puissances n-ièmes relativement premières entre elles, ce qui généralise le résultat d'Euler pour le cas $n = 3$. Comme dans le cas du dernier théorème de Fermat, l'article [DM] se sert d'une solution de l'équation $x^p + y^p = z^3$ avec $\gcd(x, y, z) = 1$ pour construire une courbe elliptique dont l'existence contredirait la conjecture de Shimura-Taniyama-Weil. Dans beaucoup de cas—quand 3 ne divise pas ab—le conducteur de cette courbe est divisible par 27; le résultat de Breuil, Conrad, Diamond, et Taylor est donc indispensable pour conclure la démonstration.

L'Arithmétique des Courbes Elliptiques

L'importance de la conjecture de Shimura-Taniyama-Weil va bien plus loin que ne le laisse deviner son rôle dans l'étude de l'équation de Fermat. En effet elle occupe une place fondamentale dans la théorie des courbes elliptiques.

Un théorème de Mordell affirme que le groupe, $E(\mathbb{Q})$ des points d'une courbe elliptique E à coordonnées rationnelles est un groupe abélien de type fini. Il est donc isomorphe en tant que groupe abstrait à $\mathbb{Z}^r \oplus T$, où T est fini. On sait déterminer explicitement le groupe de torsion T. L'entier

$r \geq 0$, appelé le *rang* de E sur $\mathbb{Q}$, est un invariant plus subtil: on ne connaît présentement aucun algorithme pour le calculer...

Dans les années soixante, Birch et Swinnerton-Dyer pressentent que l'invariant r devrait pouvoir se mesurer par le comportement asymptotique de la suite $N_p(E)$, où encore $a_p(E)$, lorsque p varie. Ils attachent à cette suite une fonction génératrice, appelée *série-L*; il s'agit (grosso modo) d'une fonction de la variable complexe s définie initialement par le produit Eulérien

$$L(E,s) := \prod_{p \nmid N} (1 - a_p(E)p^{-s} + p^{1-2s})^{-1}.$$

Ce produit converge lorsque la partie réelle de s est strictement plus grande que $3/2$. La conjecture de Shimura-Taniyama-Weil permet d'identifier la série $L(E,s)$ avec la série L attachée à une forme modulaire de poids deux. Grâce aux travaux de Hecke, on sait qu'une telle série L admet un prolongement analytique à tout le plan complexe. En particulier, on peut parler du comportement de $L(E,s)$ au voisinage de $s = 1$. Notons que formellement,

$$L(E,1) = \prod_p \frac{p}{N_p + 1}.$$

On pourrait s'attendre à ce que les entiers $N_p(E)$ pour une courbe E de grand rang aient tendance à être plus grands en moyenne, et que ceci se reflète dans le comportement analytique de $L(E,s)$ au voisinage de $s = 1$. Forts de cette intuition, Birch et Swinnerton–Dyer conjecturent que la fonction $L(E,s)$ admet en $s = 1$ un *zéro d'ordre* r:

$$\mathrm{ord}_{s=1} L(E,s) = r.$$

Cette conjecture revêt une importance fondamentale pour l'arithmétique des courbes elliptiques. Elle est encore loin d'être résolue, même si les travaux de Gross-Zagier et Kolyvagin montrent qu'elle est vraie lorsque $\mathrm{ord}_{s=1}(L(E,s)) \leq 1$.

Grâce à la théorie de la multiplication complexe, la modularité de E permet aussi de construire des points sur E à coordonnées algébriques, définies sur des extensions abélienne de corps quadratiques imaginaires. De telles constructions jouent d'ailleurs un rôle important dans l'étude de la conjecture de Birch et Swinnerton–Dyer, à travers les travaux de Gross-Zagier et de Kolyvagin notamment.

Le Programme de Langlands

Soit F un corps, muni éventuellement d'une topologie naturelle, et soit $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ le groupe de Galois absolu de $\mathbb{Q}$, muni de sa topologie de groupe profini. Une *représentation galoisienne* est un homomorphisme continu

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathbf{GL}_n(F).$$

(Les cas où $F = \mathbb{C}$, $\bar{\mathbb{Q}}_\ell$, ou $\bar{\mathbb{F}}_\ell$ sont particulièrement intéressants.)

Le travail de Wiles s'inscrit dans un programme plus large dont le but est de jeter un pont entre les représentations galoisiennes et les formes automorphes— des objets apparaissant dans la théorie des représentations (de dimension infinie) des groupes adéliques, et qui généralisent la notion de forme modulaire. Vu sous cette angle, la conjecture de Shimura-Taniyama-Weil fait partie d'un vaste édifice conjectural élaboré par Langlands, et fondé sur des travaux antérieurs de Tate, Shimura, Taniyama, et de bien d'autres. La méthode de Wiles a donné, tant aux arithméticiens qu'aux théoriciens des représentations, une nouvelle méthode puissante et versatile pour s'attaquer au programme de Langlands. Ainsi l'impact des idées de Wiles commence à se faire sentir dans des aspects divers de ce programme:

Les représentations complexes de dimension deux de $G_{\mathbb{Q}}$: Emil Artin a attaché à une représentation galoisienne $\rho : G_{\mathbb{Q}} \longrightarrow \mathbf{GL}_n(\mathbb{C})$ une fonction L, $L(\rho, s)$, et a conjecturé qu'elle admet un prolongement analytique à tout le plan complexe. Grâce aux travaux de Deligne et Serre, le programme de Langlands relie de telles représentations, quand $n = 2$, à certaines "formes paraboliques de poids un" sur un groupe légèrement différent de $\Gamma_0(N)$. Cette relation implique le prolongement analytique de $L(\rho, s)$, tout comme la modularité d'une courbe elliptique implique le prolongement analytique de sa fonction L grâce aux travaux de Hecke. Avant Wiles, les seuls cas de la conjecture d'Artin qui pouvaient être attaqués de façon générale étaient ceux où l'image de ρ est résoluble, grâce aux travaux de Langlands et Tunnell. Pour les représentations de dimension deux, le seul cas à rester ouvert est donc celui, dit *icosaédral*, où l'image naturelle de ρ dans $\mathbf{PGL_2}(\mathbb{C})$ est isomorphe à A_5, le groupe des rotations préservant les sommets d'un icosaèdre régulier.

En s'appuyant sur la méthode de Wiles, Taylor a mis sur pied une nouvelle stratégie [Ta] pour démontrer la conjecture d'Artin dans le cas icosaédral. Le programme de Taylor a été partiellement mené à bien dans une série

d'articles (en collaboration avec Kevin Buzzard, Mark Dickinson, et Nicholas Shepherd–Barron), et a permis d'établir la conjecture d'Artin pour une infinité de représentations galoisiennes icosaédrales.

Généralisations aux corps de nombres. Les méthodes de Wiles ont été beaucoup simplifiée par Diamond, Fujiwara, Skinner et Wiles lui-même. Fujiwara, Skinner, et Wiles ont ainsi réussi à étendre le résultat de Wiles au cas où le corps $\mathbb{Q}$ est remplacé par un corps totalement réel K. En particulier, ceci a permis la démonstration d'une généralisation de la conjecture de Shimura-Taniyama-Weil pour un grand nombre de courbes elliptiques définies sur de tels corps.

Généralisations en dimension n. Michael Harris et Taylor se sont récemment penchés sur des généralisations du résultat principal de [W] et surtout de [TW] aux des réprésentations de $G_{\mathbb{Q}}$ de dimension n.

Le travail de Breuil, Conrad, Diamond, et Taylor

L'espace $S_2(N)$ des formes paraboliques de poids deux sur $\Gamma_0(N)$ est un espace vectoriel complexe de dimension finie, muni de l'action d'une famille naturelle d'opérateurs auto-adjoints commutant entre eux, appelés "opérateurs de Hecke". Une *forme primitive normalisée sur* $\Gamma_0(N)$ est un vecteur propre simultané pour ces opérateurs, normalisé de telle sorte que son premier coefficient de Fourier soit égal à 1, et qui ne provient pas de l'espace des formes paraboliques sur $\Gamma_0(D)$ pour un $D \neq N$ divisant N. Une construction d'Eichler et Shimura associe à une telle forme primitive normalisée de niveau N, ayant des coefficients de Fourier *rationels*, une courbe elliptique définie sur $\mathbb{Q}$ de conducteur N. La conjecture initiale de Shimura-Taniyama-Weil affirme que cette construction fournit une bijection entre l'espace des formes primitives normalisées sur $\Gamma_0(N)$ à coefficients de Fourier rationnels et l'ensemble des courbes elliptiques de conducteur N à *isogénie près.* Ilsemble difficile de fournir des estimations *a priori* pour la cardinalité de ces ensembles en fonction de N; en fait les questions de rationalité des coefficients de Fourier des vecteurs propres des opérateurs de Hecke semblent très subtiles et difficiles à attaquer de front.

Mais en général, les coefficients de Fourier d'une forme primitive nor-

malisée f sont des *nombres algébriques*, définis sur une une extension finie $K_f \subset \bar{\mathbb{Q}}$ de $\mathbb{Q}$. Soit ℓ un nombre premier et $\iota : \bar{\mathbb{Q}} \longrightarrow \bar{\mathbb{Q}}_\ell$ un plongement de $\bar{\mathbb{Q}}$ dans une clôture algébrique du corps $\mathbb{Q}_\ell$ des nombres ℓ-adiques. Par une généralisation de la construction d'Eichler-Shimura, f donne lieu à une représentation galoisienne ℓ-adique

$$\rho_f : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbf{GL_2}(\bar{\mathbb{Q}}_\ell)$$

vérifiant $\mathrm{trace}(\rho_f(\mathrm{Frob}_p)) = \iota(a_p(f))$, pour tout les premiers p ne divisant pas $N\ell$. Ici Frob_p désigne l'"élément de Frobenius" en p. Un notion de *conducteur* peut être définie pour une représentation galoisienne ℓ-adique. On sait grâce aux travaux de Carayol, Deligne, Igusa, Langlands, et Shimura, que le conducteur de ρ_f est égal au niveau de f.

Quand f est vecteur propre des opérateurs de Hecke avec des coefficients de Fourier rationels, associé à une courbe elliptique E_f par la construction originale d'Eichler-Shimura, alors ρ_f s'obtient en considérant l'action naturelle de $G_\mathbb{Q}$ sur l'espace des points de ℓ^n-torsion de $E_f(\bar{\mathbb{Q}})$, en faisant tendre n vers l'infini.

Il apparaît donc naturel d'énoncer une version plus générale de la conjecture de Shimura-Taniyama-Weil qui remplacerait les courbes elliptiques par des représentations de dimension deux de $G_\mathbb{Q}$ à coefficients dans $\bar{\mathbb{Q}}_\ell$. Cette version plus générale a l'avantage d'éviter les subtilités associées au corps de définition des coefficients de Fourier des vecteurs propres des opérateurs de Hecke.

On s'attend à ce que les représentations galoisiennes ℓ-adiques qui "proviennent de la géométrie"—par exemple, celles qui s'obtiennent à partir de formes modulaires par la construction d'Eichler-Shimura—puissent être caractérisées par leur restriction à un "groupe de décomposition" $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ en ℓ, ou même à un "groupe d'inertie" en ℓ. Ce principe a été dégagé et rendu précis au cours des dernières décennies grâce aux travaux d'Alexandre Grothendieck, Pierre Cartier, Jean Dieudonné, et finalement Jean-Marc Fontaine et son école. Ces travaux ont mené à la notion de "représentation potentiellement semi-stable", notion qui fournit une clef de la généralisation de la conjecture de Shimura-Taniyama-Weil aux représentations galoisiennes ℓ-adiques. Autour de 1990, Fontaine et Mazur ont conjecturé que la construction ℓ-adique d'Eichler-Shimura fournit une bijection entre l'ensemble $\Lambda_{mod}(N)$ des vecteurs propres normalisés des opérateurs de Hecke de niveau

N (ayant des coefficients de Fourier dans $\bar{\mathbb{Q}}_\ell$) et l'ensemble $\Lambda_{gal}(N)$ des classes d'isomorphie des représentations galoisiennes ℓ-adiques de conducteur N qui sont potentiellement semi-stables en ℓ. En simplifiant de facon sans doute excessive, la démonstration de Wiles se résume à une comparaison de la cardinalité de ces deux ensembles, que l'on trouve ainsi être en bijection.

L'outil principal pour contrôler la taille de $\Lambda_{mod}(N)$ est fourni par la théorie des "anneaux de Hecke" et des congruences entre formes modulaires, un riche panoplie de techniques développée par Mazur, Hida, et Ribet, et exploitée par Ribet pour déduire le dernier théorème de Fermat de la conjecture de Shimura-Taniyama-Weil.

L'ensemble $\Lambda_{gal}(N)$ représente sans doute le terme le plus subtil de l'équation, celui pour lequel on dispose *a priori* du moins d'informations explicites. Il y a deux ingrédients majeurs pour estimer la cardinalité de $\Lambda_{gal}(N)$ et la comparer à la cardinalité de $\Lambda_{mod}(N)$.

• La théorie du "changement de base", et en particulier les travaux de Langlands et Tunnell sur le changement de base dans le cas résoluble.

• La théorie des déformations galoisiennes initiée par by Mazur et Hida.

Le second ingrédient, développé par Wiles, est extrêmement général et versatile, et a été façonné en un outil puissant dans l'étude arithmétique des formes automorphes. Le premier ingrédient, par contre, n'est disponible que lorsque l'image de ρ_f est un groupe (pro-)*résoluble*. La théorie des nombres a développé dans le dernier siècle tout un arsenal de techniques pour comprendre les extensions abéliennes et résolubles des corps de nombres, comme en atteste la théorie du Corps de Classes qui fournit une description précise de toutes les extensions abéliennes d'un corps de nombres, ainsi que du comportement des éléments de Frobenius dans ces extensions. L'étude des extensions non résolubles dans le même esprit s'avère plus difficile.

Malheureusement, l'image de ρ_f est rarement résoluble. Mais elle l'est lorsque le nombre premier ℓ est égal à 3, par un accident de la théorie des groupes: le groupe $\mathbf{GL}_2(\mathbb{F}_3)$, et donc aussi $\mathbf{GL}_2(\mathbb{Z}_3)$, est résoluble, une propriété qui cesse d'être vraie dès que 3 est remplacé par un nombre premier plus grand. C'est pour cette raison qu'il est indispensable dans la stratégie de Wiles de travailler avec le premier $\ell = 3$.

Le dernier obstacle pour compléter le programme de Wiles et obtenir une démonstration complète la conjecture de Shimura-Taniyama-Weil provenait

d'une difficulté technique: les représentations galoisiennes 3-adiques de conducteur N, quand 27 divise N, ont un comportement compliqué quand elles sont restreintes à un sous-groupe d'inertie en 3—et une description précise de ce comportement s'avère nécessaire pour contrôler l'ensemble $\Lambda_{gal}(N)$ quand $\ell = 3$. Pour surmonter ces difficultés, il a été nécessaire de développer de nouveaux outils pour étudier les représentations 3-adiques de $G_{\mathbb{Q}}$ qui sont "hautement ramifiées" en 3. Une partie de ces outils ont été fournis par les travaux de Breuil généralisant la théorie de Fontaine.

Bibliographie

[CDT] Conrad, Brian; Diamond, Fred; Taylor, Richard. *Modularity of certain potentially Barsotti-Tate Galois representations*. J. Amer. Math. Soc. **12** (1999), no. 2, 521–567.

[DM] Darmon, Henri; Mérel, Loïc. *Winding quotients and some variants of Fermat's last theorem*. J. Reine Angew. Math. **490** (1997), 81–100.

[Di1] Diamond, Fred. *On deformation rings and Hecke rings*. Ann. of Math. (2) **144** (1996), no. 1, 137–166.

[Ta] Taylor, Richard. *Icosahedral Galois representations*. Olga Taussky-Todd: in memoriam. Pacific J. Math. 1997, Special Issue, 337–347.

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

[W] Wiles, Andrew. *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) **141** (1995), no. 3, 443–551.