# LA CONJECTURE DE SHIMURA-TANIYAMA-WEIL

*par*

Christophe Breuil

## 1. Introduction

"*Toute courbe elliptique sur* $\mathbb{Q}$ *est modulaire*" : la conjecture de Shimura-Taniyama-Weil est devenue un théorème en 1999. Sa démonstration est due au mathématicien anglais Andrew Wiles et à ses continuateurs ([**12**], [**11**], [**4**], [**2**], [**1**], voir [**8**] pour une preuve plus récente et plus courte), mais elle est basée sur les travaux antérieurs de nombreux mathématiciens. Ce résultat exprime un lien très profond, conjecturé pendant presque 45 ans, entre deux objets mathématiques : d'une part les *courbes elliptiques sur* $\mathbb{Q}$, et d'autre part les *formes modulaires de poids* 2. Les premières sont de nature arithmético-géométrique et les secondes de nature arithmético-analytique. Dans cet article, nous introduisons les courbes elliptiques, puis les formes modulaires. Nous formulons ensuite précisément la conjecture (l'appellation "conjecture" est

demeurée même s'il s'agit désormais d'un théorème). Enfin, nous présentons un bref historique et donnons une idée de la preuve.

## 2. Courbes elliptiques

**2.1. Définition.** — La géométrie arithmétique moderne puise en partie sa source dans l'étude des équations polynômiales :

$$P(X,Y)=0 \tag{1}$$

où $P(X,Y)=\sum_{i,j} A_{i,j}X^iY^j$ est un polynôme à deux variables $X$ et $Y$ et à coefficients $A_{i,j}$ dans le corps des rationnels $\mathbb{Q}$. Le cas le plus simple est celui d'une droite $P(X,Y)=A_{1,0}X+A_{0,1}Y+A_{0,0}$ (degré 1). Puis vient le cas des coniques (degré 2) : ellipses (par exemples cercles), paraboles et hyperboles.

On peut ainsi s'intéresser aux solutions $(X,Y)$ de (1) dans n'importe quel corps contenant $\mathbb{Q}$ comme par exemple le corps $\mathbb{C}$ des nombres complexes, ou bien celui $\mathbb{R}$ des réels, ou encore $\mathbb{Q}$ lui-même. On peut essayer de décrire les propriétés géométriques de la courbe formée par les solutions dans $\mathbb{C}$ ou $\mathbb{R}$ (singularités, composantes connexes, etc.) et, ce qui est beaucoup plus difficile en général, les propriétés arithmétiques des solutions dans $\mathbb{Q}$ (nombre de ces solutions, taille, etc.). Une telle étude géométrique et arithmétique des droites et des coniques est bien comprise. Le cas qui vient immédiatement après est celui des *cubiques*, c'est-à-dire du degré 3, que l'on peut ramener, après un changement de variable convenable, à l'étude des équations :

$$Y^2-X^3-AX-B=0 \tag{2}$$

avec $A$ et $B$ dans $\mathbb{Q}$. Lorsque $X^3 + AX + B = 0$ n'a pas de racine double dans $\mathbb{C}$ (ou, de manière équivalente, dans $\mathbb{R}$), les solutions $(X, Y)$ dans $\mathbb{R} \times \mathbb{R}$ de (2) sont de la forme :

Figure 1 Figure 2

et lorsque $X^3 + AX + B = 0$ a une racine double, voire triple :

Figure 3 Figure 4

Les deux premiers cas correspondent à des cubiques dites *lisses*, aussi appelées *courbes elliptiques* et les deux derniers à des cubiques dites *singulières*. L'étude arithmétique de ces cubiques avec singularités est bien comprise et s'apparente un peu à celle des coniques. Nous les oublions dans la suite. L'étude arithmétique des courbes elliptiques est, en revanche, bien plus riche.

**2.2. Loi de groupe commutatif.** — Soit $E$ une courbe elliptique définie sur $\mathbb{Q}$, c'est-à-dire la donnée d'une équation comme en (2) avec $X^3 + AX + B = 0$ sans racine double. Il est un fait remarquable que l'ensemble des solutions de (2) dans un corps contenant $\mathbb{Q}$ est alors naturellement muni d'une structure de *groupe commutatif*. Expliquons la pour le corps $\mathbb{R}$.

Notons $E(\mathbb{R})$ l'ensemble des solutions $(X, Y)$ de (2) dans $\mathbb{R} \times \mathbb{R}$. En fait, il est très pratique en géométrie algébrique de remplacer l'équation (2) par l'équation "homogénéisée" :

$$Y^2Z - X^3 - AXZ^2 - BZ^3 = 0 \tag{3}$$

et de définir plutôt $E(\mathbb{R})$ comme l'ensemble des *classes d'équivalence* de triplets $(X, Y, Z) \in \mathbb{R}^3 - \{(0, 0, 0)\}$ solution de (3) pour la relation d'équivalence $(X, Y, Z) \sim (\lambda X, \lambda Y, \lambda Z)$ où $\lambda \in \mathbb{R} - \{0\}$. Les classes d'équivalence des triplets $(X, Y, Z)$ solutions de (3) avec

$Z \neq 0$ correspondent exactement aux solutions de (2) en associant à une telle classe les coordonnées $(X/Z, Y/Z)$. Mais on a maintenant en plus un "point à l'infini" dans $E(\mathbb{R})$ correspondant à la classe du triplet $(0, 1, 0)$.

L'ensemble $E(\mathbb{R})$ est alors muni d'une loi de groupe commutatif d'élément neutre le point à l'infini comme suit. Soient $P$, $Q$ deux points de $E(\mathbb{R})$. Si $P$ et $Q$ sont tous deux différents du point à l'infini, et donc correspondent à deux points sur la courbe de la Figure 1, traçons la droite $(PQ)$ les joignant. Si cette droite n'est pas verticale, elle coupe toujours la courbe en un troisième point $R$ car la courbe a une équation de degré 3. On définit alors $P \oplus Q$ comme le point symétrique de $R$ par rapport à l'axe des $X$ (il est bien sur la courbe car elle est symétrique par rapport à l'axe des $X$). Si $(PQ)$ est verticale, on définit $P \oplus Q$ comme le point à l'infini. Il est clair que $P \oplus Q = Q \oplus P$ (commutativité). Si l'un des points, $Q$ disons, est le point à l'infini, on remplace la droite $(PQ)$ par la droite verticale passant par $P$ et on raisonne de même : on voit que le symétrique de $R$ est alors le point $P$ de départ de sorte que $P \oplus \infty = P$ (l'infini est l'élément neutre). L'opposé de $P$ est son symétrique par rapport à l'axe des $X$ et l'axiome d'associativité se démontre aussi sans difficultés.

On définit de la même manière l'ensemble des solutions complexes $E(\mathbb{C})$ ou rationnelles $E(\mathbb{Q})$ que l'on munit d'une loi de groupe commutatif d'élément neutre la classe du triplet $(0, 1, 0)$.

La structure des groupes $E(\mathbb{C})$, $E(\mathbb{R})$ et $E(\mathbb{Q})$ est bien connue. Le groupe $E(\mathbb{C})$ est isomorphe à $\mathbb{C}/\Lambda$ où $\mathbb{C}$ est ici muni de sa loi de groupe additif et $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}$ est un réseau de $\mathbb{C}$ appelé *réseau des périodes*. Le groupe $E(\mathbb{R})$ est isomorphe au sous-groupe multiplicatif de $\mathbb{C} - \{0\}$ des nombres complexes de module 1 s'il

est connexe (Figure 1) ou au produit de ce sous-groupe par $\mathbb{Z}/2\mathbb{Z}$ sinon (Figure 2). En 1922, le mathématicien anglais Louis Mordell a démontré que le groupe $E(\mathbb{Q})$ est engendré par un nombre fini de points de $E(\mathbb{Q})$. Cela entraîne qu'il est de la forme $E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r$ où $r$ est un entier positif ou nul, le *rang* de $E(\mathbb{Q})$, et $E(\mathbb{Q})_{\text{tor}}$ un groupe abélien fini, le groupe des *points de torsion* de $E(\mathbb{Q})$ (c'est un produit de $\mathbb{Z}/n\mathbb{Z}$). On ne connait pas l'ensemble des entiers $r$ qui sont le rang d'une courbe elliptique (on ne sait même pas s'il est infini ou non). Par contre on connait tous les groupes qui peuvent être de la forme $E(\mathbb{Q})_{\text{tor}}$, il n'y en a qu'un nombre fini.

**2.3. Conducteur.** — À une courbe elliptique $E$ définie sur $\mathbb{Q}$, on peut associer un entier $N_E \geq 1$ qui mesure ses singularités "*modulo* $p$" pour tout nombre premier $p$.

Reprenons l'équation (2) et posons $\Delta = -16(4A^3 + 27B^2)$. On dit que (2) est une équation *minimale de* $E$ *en dehors de* 2 *et* 3 si $A$ et $B$ sont dans $\mathbb{Z}$ et si : ou bien $\Delta$ (dans $\mathbb{Z}$ aussi) n'est divisible par aucun entier de la forme $p^{12}$, ou bien $A$ n'est divisible par aucun entier de la forme $p^4$ où $p$ est ici un nombre premier différent de 2 et 3. En remplaçant $X$ par $u^2X$ et $Y$ par $u^3Y$ dans (2) pour $u \in \mathbb{Q} - \{0\}$ convenable et en divisant l'équation nouvelle obtenue par $u^6$ (ce qui change $\Delta$ en $u^{-12}\Delta$ et $A$ en $u^{-4}A$), on peut toujours se ramener à une équation minimale de $E$ (en dehors de 2 et 3).

Fixons une telle équation minimale $Y^2 - X^3 - AX - B = 0$. Soit $p$ un nombre premier différent de 2 et 3, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ l'unique corps à $p$ éléments et $\overline{A}$, $\overline{B} \in \mathbb{F}_p$ les classes de $A$ et $B$ modulo $p$. On définit un entier $n_E(p) \geq 0$ comme suit :

- $n_E(p) = 0$ si le polynôme $X^3 + \overline{A}X + \overline{B} \in \mathbb{F}_p[X]$ n'a pas de racine double (dans une clôture algébrique de $\mathbb{F}_p$) ou, ce qui est équivalent, si l'entier $\Delta$ n'est pas divisible par $p$

- $n_E(p) = 1$ si le polynôme $X^3 + \overline{A}X + \overline{B}$ a une racine double qui n'est pas triple

- $n_E(p) = 2$ sinon.

La définition de $n_E(2)$ et $n_E(3)$ et un peu plus compliquée (par exemple $n_E(3)$ peut aller jusqu'à 5) et nous ne la donnerons pas. Notons que $n_E(p) = 0$ pour tous les nombres premiers sauf un ensemble fini d'entre eux. On pose alors :

$$N_E = \prod_p p^{n_E(p)} \in \mathbb{N}.$$

Cet entier s'appelle le *conducteur* de la courbe elliptique. On peut montrer qu'il est toujours supérieur ou égal à 11. D'après sa définition et la discussion du §2.1, remarquons que la puissance de $p$ qui le divise, au moins pour $p \neq 2, 3$, mesure le "degré de singularité" de la cubique modulo $p$ d'équation :

$$Y^2 - X^3 - \overline{A}X - \overline{B} = 0. \tag{4}$$

Notons que, si $p$ ne divise pas $\Delta$, cette cubique est une courbe elliptique *définie sur* $\mathbb{F}_p$.

**2.4. Fonction $L$.** — À une courbe elliptique $E$ définie sur $\mathbb{Q}$, on peut associer une fonction $L_E(s)$ de la variable complexe qui est un analogue en "dimension 1" de la fonction zêta de Riemann.

Fixons une équation minimale (en dehors de 2 et 3) de $E$ comme au §2.3. Pour $p$ premier différent de 2 et 3 tel que $n_E(p) = 0$, notons $E(\mathbb{F}_p)$ l'ensemble des solutions $(X, Y)$ de (4) dans $\mathbb{F}_p \times \mathbb{F}_p$. En fait, comme au §2.2, on définit $E(\mathbb{F}_p)$ en "homogénéisant" (4) et en rajoutant le point à l'infini $(0, 1, 0)$. L'ensemble $E(\mathbb{F}_p)$ est alors encore un groupe commutatif d'élément neutre le point à l'infini, mais cette fois il est *fini*. On peut également définir $E(\mathbb{F}_2)$ et $E(\mathbb{F}_3)$ (nous ne le ferons pas). En 1933, le mathématicien allemand Helmut Hasse a montré les bornes suivantes pour le cardinal de $E(\mathbb{F}_p)$ :

$$p + 1 - 2\sqrt{p} \leq \text{cardinal de } E(\mathbb{F}_p) \leq p + 1 + 2\sqrt{p}. \tag{5}$$

Pour $p$ premier tel que $n_E(p) \leq 1$, on pose :

- $a_p = p + 1 -$ cardinal de $E(\mathbb{F}_p)$ si $n_E(p) = 0$

- $a_p = 1$ si $n_E(p) = 1$ et si $E$ a *réduction multiplicative déployée en* $p$ (si $p \neq 2, 3$, cela veut dire que l'équation $Y^2 = X^3 + \overline{A}X + \overline{B}$ a des tangentes au point double de pentes dans $\mathbb{F}_p$, ce qui revient aussi à dire que la racine double $\lambda$ de $X^3 + \overline{A}X + \overline{B} = 0$ est telle que $3\lambda$ est un carré dans $\mathbb{F}_p$)

- $a_p = -1$ si $n_E(p) = 1$ et si $E$ a *réduction multiplicative non déployée en* $p$ (si $p \neq 2, 3$, cela veut dire que l'équation $Y^2 = X^3 + \overline{A}X + \overline{B}$ a des tangentes au point double de pentes non dans $\mathbb{F}_p$).

L'une des fonctions les plus étudiées des mathématiques est la fonction *zêta de Riemann* $\zeta(s) = \prod_p \frac{1}{1-\frac{1}{p^s}} = \sum_{n=1}^{+\infty} \frac{1}{n^s}$ (la deuxième égalité s'obtenant en écrivant $\frac{1}{1-\frac{1}{p^s}} = \sum_{n=0}^{+\infty} \frac{1}{p^{ns}}$, en développant

formellement le produit de ces sommes et en utilisant la décomposition des entiers en nombres premiers). À une courbe elliptique $E$, on associe une fonction analogue très importante $L_E(s)$ de la variable complexe $s$ appelée *fonction de Hasse-Weil* (des noms de Hasse (déjà cité) et du mathématicien français André Weil). Sa formule est, comme précédemment, donnée par un produit :

$$L_E(s) = \left( \prod_{\{p|n_E(p)=0\}} \frac{1}{1 - \frac{a_p}{p^s} + \frac{p}{p^{2s}}} \right) \left( \prod_{\{p|n_E(p)=1\}} \frac{1}{1 - \frac{a_p}{p^s}} \right).$$

En écrivant encore toutes les fractions comme une somme infinie et en développant formellement le produit, on obtient aussi une formulation :

$$L_E(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s} \tag{6}$$

où les $a_n$ sont dans $\mathbb{Z}$ et valent les précédents $a_p$ lorsque $n = p$. En utilisant les bornes $-2\sqrt{p} \leq a_p \leq 2\sqrt{p}$ lorsque $n_E(p) = 0$ déduites de (5), on peut montrer que la fonction $L_E(s)$ converge lorsque la partie réelle de $s$ est $> 3/2$ et qu'elle est même *analytique en* $s$ sur ce domaine. En fait, $L_E(s)$ se prolonge analytiquement (et donc de façon unique) sur $\mathbb{C}$ *tout entier*, mais ceci est une conséquence de la conjecture de Shimura-Taniyama-Weil qui dit que $L_E(s)$ peut également s'obtenir à partir d'une forme modulaire. Nul ne connaît, à ce jour, une preuve directe de l'existence du prolongement analytique de la fonction $L_E(s)$ sans passer par les formes modulaires.

## 3. Formes modulaires

**3.1. Définition.** — Soit $\mathbb{H} \subset \mathbb{C}$ l'ensemble des nombres complexes $z$ de partie imaginaire strictement positive. On appelle $\mathbb{H}$ le *demi-plan de Poincaré*. Le groupe $\mathrm{SL}_2(\mathbb{Z})$ des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $a, b, c, d$ dans $\mathbb{Z}$ et $ad - bc = 1$ opère à gauche sur $\mathbb{H}$ par la formule $z \mapsto \frac{az+b}{cz+d}$. Pour $N \in \mathbb{N} - \{0\}$, notons $\Gamma_0(N)$ le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $N$ divise $c$. Il opère également sur $\mathbb{H}$ via l'action de $\mathrm{SL}_2(\mathbb{Z})$. Notons que $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$.

Les formes modulaires sont certaines fonctions holomorphes sur $\mathbb{H}$ vérifiant une équation fonctionnelle liée au choix d'un groupe $\Gamma_0(N)$. Leur définition, donnée ci-dessous en poids 2, est peu éclairante quant à leur formidable richesse.

On appelle *forme modulaire de poids* 2 *et niveau* $N$ une fonction analytique (ou holomorphe) $f : \mathbb{H} \to \mathbb{C}$ vérifiant les deux propriétés suivantes :

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),\ f\Big(\frac{az+b}{cz+d}\Big) = (cz+d)^2 f(z) \tag{7}$$

(8) $f$ est holomorphe aux pointes.

Expliquons la propriété (8). En appliquant (7) à $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$, on obtient $f(z+1) = f(z)$. Comme $f$ est holomorphe et périodique de période 1, la théorie des séries de Fourier nous permet d'écrire $f(z) = \sum_{n=-\infty}^{+\infty} a_n e^{2i\pi nz}$ pour des coefficients $a_n \in \mathbb{C}$ (où $e^{2i\pi nz} = \cos(2\pi nz) + i\sin(2\pi nz)$). Plus généralement, si

$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, la fonction $f\,|_\gamma\,(z) = \frac{1}{(cz+d)^2} f\big(\frac{az+b}{cz+d}\big)$ est holomorphe périodique de période un diviseur de $N$ (par exemple 1 si $\gamma \in \Gamma_0(N)$). Elle s'écrit ainsi :

$$f\,|_\gamma\,(z) = \sum_{n=-\infty}^{+\infty} a_n(\gamma) e^{\frac{2i\pi}{N} nz} \tag{9}$$

pour des $a_n(\gamma)$ dans $\mathbb{C}$. On dit que $f$ est *holomorphe aux pointes* si $a_n(\gamma) = 0$ pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ et tout $n < 0$.

En particulier, une forme modulaire s'écrit :

$$f(z) \;=\; \sum_{n=0}^{+\infty} a_n e^{2i\pi nz}. \tag{10}$$

On dit qu'une forme modulaire $f$ est *parabolique* si $a_0(\gamma) = 0$ dans (9) pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. On dit qu'une forme modulaire parabolique est *normalisée* si de plus $a_1 = 1$ dans (10).

**3.2. Exemples.** — Notons $M(2, N)$ l'ensemble des formes modulaires de poids 2 et niveau $N$ et $S(2, N) \subset M(2, N)$ le sous-ensemble de celles qui sont paraboliques.

Si $f \in M(2, N)$ et si $\lambda \in \mathbb{C}$, il est facile de vérifier sur (7) et (8) qu'on a encore $\lambda f \in M(2, N)$. Si $f$ et $g$ sont deux formes modulaires dans $M(2, N)$, on a de même $f + g \in M(2, N)$. Ceci reste vrai en remplaçant $M(2, N)$ par $S(2, N)$. Ainsi, $M(2, N)$ et $S(2, N)$ sont naturellement munis d'une structure de $\mathbb{C}$-espace vectoriel. On peut montrer que leur dimension est *finie*.

Les premiers exemples de formes modulaires, comme la série $\Theta^4$ de l'exemple 1 ci-dessous, furent étudiés dès la première moitié du dix-huitième siècle. En général, il n'est pas facile de se donner explicitement une forme modulaire dans $M(2,N)$ et encore moins dans $S(2,N)$.

Exemple 1 : Soit $\Theta : \mathbb{H} \to \mathbb{C}$, $z \mapsto 1 + 2\sum_{n=1}^{+\infty} e^{2i\pi n^2 z}$, alors la fonction $\Theta^4$ est dans $M(2,4)$ et n'est pas parabolique.

Exemple 2 : Soit $\eta : \mathbb{H} \to \mathbb{C}$, $z \mapsto e^{\frac{2i\pi z}{24}} \prod_{n=1}^{+\infty}(1 - e^{2i\pi nz})$. Alors la fonction $\eta(z)^2\eta(11z)^2$ est dans $S(2,11)$. En fait, on a $S(2,11) = \mathbb{C}\eta(z)^2\eta(11z)^2$.

## 4. La conjecture

**4.1. Énoncé.** — Il existe plusieurs formulations équivalentes de la conjecture de Shimura-Taniyama-Weil, insistant soit sur l'aspect géométrique, soit sur l'aspect analytique. Nous privilégions ici une formulation explicite plutôt analytique, pouvant par exemple se tester sur ordinateur.

Soit $E$ une courbe elliptique définie sur $\mathbb{Q}$. Rappelons que l'on a associé à $E$ un entier $N_E$, son conducteur (§2.3) et une fonction de la variable complexe $L_E(s) = \sum_{n=1}^{+\infty} \frac{a_n}{n^s}$, sa fonction de Hasse-Weil (§2.4).

**Théorème 4.1 (ex-conjecture de Shimura-Taniyama-Weil)**

*Soit $E$ une courbe elliptique définie sur $\mathbb{Q}$. Alors la fonction $\sum_{n=1}^{+\infty} a_n e^{2i\pi nz}$ est une forme modulaire parabolique normalisée de poids 2 et niveau $N_E$.*

Une courbe $E$ étant donnée, un ordinateur peut calculer facilement $N_E$ et les premiers coefficients $a_n$ de $L_E(s)$ à partir de l'équation de $E$. Comme $S(2, N_E)$ est de dimension finie (§3.2), l'ordinateur peut alors aisément vérifier que la fonction $\sum_{n=1}^{+\infty} a_n e^{2i\pi nz}$ est bien dans $S(2, N_E)$. Bien entendu, ceci ne constitue aucunement une preuve puisqu'il y a une infinité de courbes elliptiques !

Exemple : La courbe elliptique d'équation $Y^2 - X^3 + 3^3.2^4X - 3^3.2^4.19 = 0$ (minimale en dehors de 2 et 3) donne la forme modulaire $\eta(z)^2\eta(11z)^2$ de l'exemple 2 du §3.2.

Il faut comprendre que l'énoncé 4.1 est véritablement "miraculeux" car il n'y a *a priori* aucune raison pour que la fonction $\sum_{n=1}^{+\infty} a_n e^{2i\pi nz}$ vérifie les conditions (7) et (8) du §3.1 avec $N = N_E$. Heuristiquement, c'est même étrange car il est très facile de se donner une courbe elliptique sur $\mathbb{Q}$ : il suffit de considérer une équation (2) et il est donc très facile d'obtenir la fonction $\sum_{n=1}^{+\infty} a_n e^{2i\pi nz}$ (au moins si l'on ne cherche pas à la calculer explicitement). En revanche, on sait qu'il n'est pas facile de se donner une forme modulaire dans $S(2, N_E)$.

Le Théorème 4.1 a d'abord été démontré par Wiles (aidé de son ancien élève et compatriote Richard Taylor) en 1994 pour les courbes elliptiques $E$ telles que $N_E$ n'a pas de facteur carré (on dit que la courbe est *semi-stable*), cf. [**12**], [**11**]. Il a introduit à cet effet les principales idées nouvelles de démonstration qui ont été reprises et amplifiées par ses successeurs. L'article [**4**] a ensuite peu après étendu le résultat aux courbes elliptiques telles que ni 9 ni 25 ne divisent $N_E$, puis l'article [**2**] en 1997 aux courbes telles que 27 ne divise pas $N_E$. Enfin, en 1999, l'article [**1**] a démontré le cas général. D'article en article, les démonstrations requièrent une technique mathématique de plus en plus pointue.

Mentionnons deux corollaires de ce théorème. Le premier, très médiatique, et qui découle déjà de la modularité des courbes elliptiques semi-stables démontrée par Wiles, est le Grand Théorème de Fermat ($a^n + b^n + c^n$ n'a pas de solution dans $\mathbb{Z}$ telle que $abc \neq 0$ si $n > 2$). Le principe est de construire à partir d'une solution (pour $n = p$ premier et $p > 3$) une courbe elliptique dont on montre en utilisant des résultats du mathématicien français Jean-Pierre Serre et du mathématicien américain Kenneth Ribet qu'elle ne peut être modulaire. Pour plus de détails sur ce sujet, nous renvoyons le lecteur par exemple à l'article [**7**].

Le deuxième corollaire est le fait, très important, que la fonction de Hasse-Weil $L_E(s)$ peut se prolonger analytiquement sur $\mathbb{C}$ et satisfaît même une équation fonctionnelle reliant $L_E(2-s)$ et $L_E(s)$. Cette conséquence est fondamentale car elle montre que $L_E(s)$ est bien définie au voisinage de $s = 1$ (notons que $1 \leq 3/2$, cf. §2.4) et permet d'énoncer une autre conjecture mythique sur les courbes elliptiques qui est la *conjecture de Birch & Swinnerton-Dyer* (du nom des mathématiciens anglais Brian Birch et Peter Swinnerton-Dyer) prédisant, sous sa forme faible, que $L_E(s)$ a en $s = 1$ un *zéro d'ordre exactement* $r$, où $r$ est le rang de $E(\mathbb{Q})$ (cf. §2.2).

**4.2. Bref historique.** — C'est en septembre 1955, lors d'une conférence à Tokyo et Nikko, que le mathématicien japonais Yutaka Taniyama a émis l'hypothèse que toute fonction de Hasse-Weil $L_E(s)$ comme au §2.4 pouvait donner naissance à une forme automorphe (objet mathématique généralisant les formes modulaires), sans prédire toutefois si la forme automorphe était ou non simplement une forme modulaire. La suggestion de Taniyama fut précisée et acquit le statut de conjecture dans les années soixante avec les travaux du mathématicien japonais Goro Shimura et ceux

de Weil. En particulier, Weil identifia le niveau de la forme modulaire cherchée au conducteur $N_E$ de la courbe elliptique. La conjecture s'appela pendant longtemps conjecture de Taniyama-Weil.

**4.3. Stratégie de la preuve.** — Il est malheureusement impossible de donner ici autre chose qu'un synopsis grossier de la preuve. L'introduction avec précision des multiples autres notions utilisées demanderait à elle seule des dizaines de pages. Nous renvoyons le lecteur qui désirerait en savoir davantage aux articles d'exposition plus ardus [**6**], [**3**], [**10**], [**9**] et [**5**].

Soit $p$ un nombre premier. Pour relier une courbe elliptique à une forme modulaire, il existe un troisième objet mathématique : une *représentation* du groupe Galois$(\overline{\mathbb{Q}}/\mathbb{Q})$. Ici, $\overline{\mathbb{Q}}$ est le sous-corps de $\mathbb{C}$ formé des nombres complexes racines d'un polynôme à coefficients dans $\mathbb{Q}$ et Galois$(\overline{\mathbb{Q}}/\mathbb{Q})$ le groupe abstrait des automorphismes de corps de $\overline{\mathbb{Q}}$ qui laissent fixes les éléments de $\mathbb{Q}$.

Soit $E$ une courbe elliptique sur $\mathbb{Q}$. Le groupe Galois$(\overline{\mathbb{Q}}/\mathbb{Q})$ agit naturellement sur le sous-groupe $E[p^n](\mathbb{C})$ des points de $E(\mathbb{C})$ qui, additionnés $p^n$ fois à eux-mêmes par la loi du §2.2, redonnent le point à l'infini, i.e. l'élément neutre (ces points sont dits de $p^n$-*torsion*). En effet, les coordonnées de ces points sont en fait dans $\overline{\mathbb{Q}}$ et Galois$(\overline{\mathbb{Q}}/\mathbb{Q})$ les permuttent entre eux en agissant sur leurs coordonnées. Comme on peut montrer que $E[p^n](\mathbb{C})$ est un $\mathbb{Z}/p^n\mathbb{Z}$-module libre de rang 2, on obtient ainsi un morphisme de groupes $\rho_{E,n} : \text{Galois}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ où le groupe de droite est celui des matrices $2\times 2$ à coefficients dans $\mathbb{Z}/p^n\mathbb{Z}$ de déterminant inversible dans l'anneau $\mathbb{Z}/p^n\mathbb{Z}$. En passant à la limite sur $n$, on en déduit une représentation $p$-*adique* :

$$\rho_E : \text{Galois}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}_p)$$

où $\mathbb{Z}_p$ désigne les nombres entiers $p$-adiques. En faisant varier $E$, on obtient ainsi un ensemble $\mathcal{R} = \{\rho_E\}$ de représentations $p$-adiques de Galois$(\overline{\mathbb{Q}}/\mathbb{Q})$.

Pour tout entier positif non nul $N$, l'espace vectoriel $S(2, N)$ est muni d'une collection d'endomorphismes canoniques $T_\ell$ pour tout nombre premier $\ell$ appelés *opérateurs de Hecke*. Il se trouve que l'on peut aussi associer à certaines formes modulaires de poids 2 et de coefficients $a_n \in \mathbb{Z}$ (dans (10)) une représentation $p$-adique $\rho_f$ : Galois$(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_p)$ : ce sont les $f$ qui sont *vecteurs propres* de tous les opérateurs $T_\ell$. En faisant varier $f$ (sous les conditions précédentes), on obtient ainsi un deuxième ensemble $\mathcal{T} = \{\rho_f\}$ de représentations $p$-adiques de Galois$(\overline{\mathbb{Q}}/\mathbb{Q})$.

On peut alors montrer que l'on a une inclusion naturelle $\mathcal{T} \subseteq \mathcal{R}$ et que la conjecture de Shimura-Taniyama-Weil est *équivalente* au fait que cette inclusion est une *bijection*. Autrement dit, il suffit de choisir un nombre premier $p$ et de montrer que les représentations $\rho_E$ sont toutes de la forme $\rho_f$.

Malheureusement, montrer directement $\mathcal{T} = \mathcal{R}$, même pour des petites valeurs de $p$, semble hors de portée. L'idée de Wiles est alors de découper les ensembles $\mathcal{T}$ et $\mathcal{R}$ en sous-ensembles plus petits et de montrer que l'on a une bijection sur *chacun* de ces sous-ensembles lorsque $p = 3$. Pour tout entier $N$ positif non nul et toute représentation $\overline{\rho}$ : Galois$(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$, on peut ainsi considérer le sous-ensemble $\mathcal{R}(N, \overline{\rho}) \subset \mathcal{R}$ des $\rho_E$ telles que $N_E = N$ et $\rho_E$ modulo 3 redonne $\overline{\rho}$ (i.e. $\rho_{E,1} = \overline{\rho}$), et le sous-ensemble $\mathcal{T}(N, \overline{\rho}) \subseteq \mathcal{R}(N, \overline{\rho})$ des $\rho_f$ telles que $f$ est de niveau $N$ et $\rho_f$ modulo 3 redonne $\overline{\rho}$. Bien sûr, si on prend $N$ et $\overline{\rho}$ quelconques, ces sous-ensembles sont en général tous les deux vides. Pour avoir une chance qu'ils soient non vides, il ne faut pas prendre $N$

n'importe comment par rapport à $\overline{\rho}$ (il faut que $\overline{\rho}$ soit "non ramifiée en dehors de $N$ et 3"). Pour un tel choix de $(N,\overline{\rho})$, on peut alors déduire de résultats du mathématicien américain Jerrold Tunnel et du mathématicien canadien Robert Langlands que l'on a toujours $\mathcal{T}(N,\overline{\rho})\neq\emptyset$.

On montre ensuite qu'il existe une $\mathbb{Z}_3$-algèbre $\mathbb{T}(N,\overline{\rho})$ (engendrée par des opérateurs de Hecke) et une représentation :

$$\rho_{\mathbb{T}} : \mathrm{Galois}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}(N,\overline{\rho}))$$

telle que *toute* représentation $\rho_f$ dans $\mathcal{T}(N,\overline{\rho})$ s'obtient en composant $\rho_{\mathbb{T}}$ avec une surjection $\mathbb{T}(N,\overline{\rho})\twoheadrightarrow\mathbb{Z}_3$ et que, de plus, *toute* surjection $\mathbb{T}(N,\overline{\rho})\twoheadrightarrow\mathbb{Z}_3$ conduit à une représentation dans $\mathcal{T}(N,\overline{\rho})$ en composant avec $\rho_{\mathbb{T}}$. Comme $\mathcal{T}(N,\overline{\rho})\neq 0$, on voit que $\mathbb{T}(N,\overline{\rho})\neq 0$. On montre aussi qu'il existe une autre $\mathbb{Z}_3$-algèbre $R(N,\overline{\rho})$ (introduite par le mathématicien américain Barry Mazur) et une représentation :

$$\rho_R : \mathrm{Galois}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(R(N,\overline{\rho}))$$

telle que *toute* représentation $\rho_E$ dans $\mathcal{R}(N,\overline{\rho})$ (par exemple une représentation $\rho_f$) s'obtient en composant $\rho_R$ avec une surjection $R(N,\overline{\rho})\twoheadrightarrow\mathbb{Z}_3$. Par contre, on ignore *a priori* que toutes les surjections $R(N,\overline{\rho})\twoheadrightarrow\mathbb{Z}_3$ conduisent à des représentations dans $\mathcal{R}(N,\overline{\rho})$, c'est-à-dire provenant d'une courbe elliptique (on ne le sait qu'*a posteriori*). Des arguments généraux fournissent une surjection canonique de $\mathbb{Z}_3$-algèbres $R(N,\overline{\rho})\twoheadrightarrow\mathbb{T}(N,\overline{\rho})$.

Pour montrer $\mathcal{T}(N,\overline{\rho})=\mathcal{R}(N,\overline{\rho})$, c'est-à-dire la conjecture de Shimura-Taniyama-Weil, on voit donc par ce qui précède qu'il suffit de montrer que la surjection $R(N,\overline{\rho})\twoheadrightarrow\mathbb{T}(N,\overline{\rho})$ est en fait un *isomorphisme*. C'est ce qu'a réussi à démontrer Wiles, et après lui ses successeurs, par une comparaison fine de la "taille" des $\mathbb{Z}_3$-algèbres

non nulles $R(N, \overline{\rho})$ et $\mathbb{T}(N, \overline{\rho})$. La preuve utilise, outre de l'algèbre commutative non triviale, une grande partie de l'arithmétique moderne : cohomologie galoisienne, théorie de Hodge $p$-adique, congruences entre formes modulaires, etc.

## Références


[1] C. Breuil, B. Conrad B., F. Diamond F. & R. Taylor R., *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercices*, in Journal of the American Mathematical Society, volume 14, numéro 4, p. 843, 2001.

[2] B. Conrad B., F. Diamond F. & R. Taylor R., *Modularity of certain potentially Barsotti-Tate Galois representations*, in Journal of the American Mathematical Society, volume 12, numéro 2, p. 521, 1999.

[3] H. Darmon, *A proof of the full Shimura-Taniyama-Weil conjecture is announced*, in Notices of the American Mathematical Society, volume 46, numéro 11, p.1397, 1999.

[4] F. Diamond, *On deformation rings and Hecke rings*, in Annals of Mathematics, volume 144, numéro 2, p. 137, 1996.

[5] B. Edixhoven, *Rational elliptic curves are modular (after Breuil, Conrad, Diamond, Taylor)*, Séminaire Bourbaki numéro 871, in Astérisque 276, p.161, 2002.

[6] G. Faltings, *The proof of Fermat's last Theorem by R. Taylor and A. Wiles*, in Notices of the American Mathematical Society, volume 42, numéro 7, p.743, 1995.

[7] C. Goldstein, *Le théorème de Fermat enfin démontré*, in La Recherche Hors-Série numéro 2, p.21, 1999.

[8] M. Kisin, *Moduli of finite flat group schemes and modularity*, à paraître.

[9] J. Oesterlé, *Travaux de Wiles (et Taylor...) II*, Séminaire Bourbaki numéro 804, in Astérisque, volume 237, p.333, 1996.

[10] J.-P. Serre, *Travaux de Wiles (et Taylor...) I*, Séminaire Bourbaki numéro 803, in Astérisque, volume 237, p.319, 1996.

[11] R. Taylor & A. Wiles, *Ring theoretic properties of certain Hecke algebras*, in Annals of Mathematics, volume 141, numéro 2, p. 553, 1995.

[12] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, in Annals of Mathematics, volume 141, numéro 2, p. 443, 1995.

---

C. Breuil, C.N.R.S., Institut des Hautes Études Scientifiques, 35 route de Chartres, 91440 Bures-sur-Yvette, France • *E-mail :* breuil@ihes.fr