# Familles de formes modulaires et le théorème de Fermat

Cours de DEA, 2001

A.A.Pantchichkine, 1 semestre (2001/2002)

**vendredi le 12 octobre 2001, Salle17, IF,**

§**0. Préhistoire.** Pierre de Fermat (1601–1665) à soulevé son probème célèbre (c.1637) dans la marge d'une traduction des "Arithmétiques" de Diophante: "Décomposer un cube en deux autre cubes, une quatrième puissance, et généralement, une puissance quelconque, en deux puissances de même nom au-dessus de la second puissance, est une chose impossible et j'en ai assurément trouvé l'admirable démonstration. La marge trop exiguë ne la contiendrait pas".

*En langage moderne:*

$$\text{pour} \quad n > 2 \quad \begin{cases} x^n + y^n = z^n \\ x, y, z \in \mathbf{Z} \end{cases} \implies xyz = 0 \qquad (FLT(n))$$

("Fermat's Last Theorem").

*Cas* $n = 4$ (Fermat lui-même dans une lettre à Huygens)

*cas* $n = 3$ (Euler en1753);

*cas* $n = 5$ (Dirichlet, Legendre, c.1825);

*cas* $n = 7$ (G.Lamé, 1839; $n = 14$ a déjà été fait par Dirichlet en 1832);

*"premier cas"*, $FLT\mathrm{I}(p)$ pour les nombres premiers $p$ avec $q = 2p + 1$ premier aussi (Sophie Germain dans une lettre à Gauss en 1820):

$$\begin{cases} x^p + y^p = z^p \\ x, y, z \in \mathbf{Z} \end{cases} \implies \quad xyz \equiv 0 (\mathrm{mod} p) \qquad (FLT\mathrm{I}(p)).$$

*Le 11 mars 1847 G.Lamé* informait l'Académie des Sciences de Paris d'une démonstration complète à la base de l'identité

$$x^p + y^p = (x + y)(x + \zeta y) \cdot \ldots \cdot (x + \zeta^{p-1} y), \quad \zeta = \zeta_p = \exp(2\pi i/p), p \neq 2$$

admettant la factorialité de l'anneau $\mathbf{Z}[\zeta_p]$.
Immédiatement J.Liouville dit: "N'y a-t-il pas là une lacune à remplir?" (et dans quelques mois A.Cauchy publia une note sur la non-factorialité de $\mathbf{Z}[\zeta_{23}]$).

*E.Kummer en 1847* a defini un *p régulier*:

$$\text{pout tout idéal} \quad I \subset \mathbf{Z}[\zeta_p] \quad \Big(I^p \text{ principal} \implies I \text{ principal}\Big).$$

(en langage moderne), et il a démontré FLT($p$) pour tout $p$ régulier (la Médaille d'Or de l'Académie des Sciences en 1850). Le plus petit nombre premier irrégulier est $p = 37$, voir [10].

**§1. Survol de la démonstration de Wiles**

*Par l'absurde:* si $a^p + b^p = c^p, abc \neq 0$, avec un premier $p \geq 5$, on montre l'existence d'une fonction holomorphe non-nulle $f = f_{a,b,c} : H \to \mathbf{C}$ remarquable: cette fonction construite à partir d'une solution primitive $(a, b, c)$ possède trop de symétries qui impliquent $f \equiv 0$, une contradiction.

*Ce sont les symétries suivantes:* la différentielle holomorphe $\omega_f = f(z)dz$ est invariante par l'action $z \mapsto \dfrac{\alpha z + \beta}{\gamma z + \delta}$ de tout $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ dans le sous groupe

$$\Gamma_0(2) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; \gamma \equiv 0 \bmod 2 \right\}$$

d'indice 3 de $\mathrm{SL}_2(\mathbf{Z})$, et la différentielle $\omega_f$ est régulière sur la surface de Riemann compacte

$$X_0(2) = \Gamma_0(2)\backslash\overline{H},\ \ \overline{H} = H \cup \mathbf{Q} \cup i\infty,\ \ H = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}.$$

En particuler,

$$\forall\sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0(2),\ \ f\left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) = (\gamma z + \delta)^2 f(z),\ \ \text{et}\ \ f(0) = f(i\infty) = 0.$$

Mais $\dim_{\mathbf{C}} \Omega^1(X_0(2)) = \mathrm{genre}(X_0(2)) = 0$ car $X_0(2) \cong S$ (la sphère de Riemann).

On obtient l'existence d'une telle fonction $f$ non-nulle à partir de la courbe de Frey $E = E_{a^p,b^p,c^p} : y^2 = x(x - a^p)(x + b^p)$, où l'on suppose sans réstriction de généralité que $a^p \equiv -1 \bmod 4$, 2 divise $b$, en deux étapes:

I) *Modularité de la série géneratrice $g$ de toute courbe elliptique $E$ semistable* (voir ci-dessous);

II) *L'existence d'une forme modulaire $f$ d'un niveau minimal $N_0 = N(E, p)$*; $f$ congrue à $g$ modulo un ideal convenable $\lambda_p$ et $N_0 = 2$ pour les courbes de Frey.

I) On observe tout d'abord que *le discriminant* du polynôme cubique $P_3(x) = x(x - a^p)(x + b^p)$ est $(abc)^{2p} \neq 0$ donc la courbe projective $E$ de l'équation affine $y^2 = P_3(x)$ est lisse de genre 1, avec un point rationnel à l'infinie. Considérons la *série génératrice*: pour tout nombre premier $l$ posons

$$N_l(E) = \sharp\left\{(x, y) \in \mathbf{F}_l^2 \mid y^2 \equiv P_3(x) \bmod l\right\},\ \ b_l = b_l(E) = l - N_l(E),$$
$$g = g_{E,S} = \sum_{n\geq 1} b_n e^{2\pi i n z}\ \ \text{avec}\ \ \sum_{n\geq 1} b_n n^{-s} = \prod_{l\notin S}(1 - b_l + l^{1-2s})^{-1},$$

pour un ensemble fini $S$ de nombres premiers contenant tous les diviseurs premiers du discriminant de $P_3$. On voit bien que $g$ est convergente donc elle est une fonction holomorphe sur le demi-plan de Poincaré $H$, et que

$$N_l(E) = l + \sum_{x \bmod l} \left(\frac{x}{l}\right),\ \ \left(\frac{x}{l}\right)\ \text{est le symbole de Legendre.}$$

**La conjecture STW (de Shimura, Taniyama, Weil)** dit:
I) pour toute courbe elliptique $E : y^2 = P_3(x)$ sur $\mathbf{Q}$ la série génératrice $g$ possède beaucoup de symétries:

$$\forall E \forall S \exists N \in \mathbf{N}^* \quad g = g_{E,S} \text{ est une forme modulare de poids 2 et de niveau } N$$

(pour le sous-groupe de congruence

$$\Gamma_0(N) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \;\middle|\; \gamma \equiv 0 \bmod N \right\} \subset \mathrm{SL}_2(\mathbf{Z})),$$

i.e. $\omega_g = g(z)dz$ est une différentielle régulière dans $\Omega^1(X_0(N))$ sur la surface de Riemann compacte $X_0(N) = \Gamma_0(N)\backslash\overline{H}$. Notation: $g \in S_2(N)$, ceci signifie

$$\forall \sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0(N), \quad g\left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) = (\gamma z + \delta)^2 g(z), \quad \text{et} \quad \forall x \in \mathbf{Q} \cup i\infty, f(x) = 0 \ .$$

où $S_2(N) \cong \Omega^1(X_0(N)$ est un espace vectoriel complexe de dimension $\dim S_2(N) =$ genre$(X_0(N))$.
II) Si l'ensemble exceptionnel $S$ est *minimal*, le nombre $N$ coïncide avec le *conductuer minimal* de la courbe $E$.

*Exemple.* Soit

$$E : y^2 + y = x^3 - x^2 \Longleftrightarrow y^2 = x^3 - x^2 + \frac{1}{4}, \quad S = \{11\}$$

alors

$$g = q \prod_{m \geq 1} (1 - q^m)^2 (1 - q^{11m})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \ldots \in S_2(11)$$

| $l$ | 2 | 3 | 5 | 7 | 11 | 13 | $\cdots$ |
|---|---|---|---|---|---|---|---|
| $N_l$ | 4 | 4 | 4 | 9 | – | 9 | $\cdots$ |
| $b_l$ | $-2$ | $-1$ | 1 | $-2$ | – | 4 | $\cdots$ |

Cette conjecture célèbre généralise *la loi de réciprocité* de Gauss: soit $d \in \mathbf{Z}$,

$$N_l(d) = \sharp \left\{ x \in \mathbf{F}_l \mid x^2 \equiv d \bmod l \right\} \Rightarrow N_l(d) = 1 + \left(\frac{d}{l}\right) = \begin{cases} 2, & d \in (\mathbf{F}_l^\times)^2 \\ 1, & d \equiv 0 \bmod l \\ 0, & d \notin (\mathbf{F}_l)^2 \end{cases},$$

alors $N_l(d)$ ne dépend que de $l \bmod 4|d|$ et la série génératrice

$$g = \sum_{n \geq 1} b_n e^{2\pi i n z} \quad \text{avec} \quad \sum_{n \geq 1} b_n n^{-s} = \prod_l \left(1 - \left(\frac{d}{l}\right) l^{-s}\right)^{-1}$$

se trouve dans l'espace vectoriel complexe de dimension finie formée par les fonctions avec les cofficients de Fourier $n \mapsto d_n$ périodiques modulo $4|d|$.

*Démonstration complète* de la conjecture STW générale a été trouvé en 1999 par Ch.Breuil, B.Conrad, F.Diamond et R.Taylor (see [17]). En 1994 A.Wiles l'a démontré pour une partie importante des courbes elliptiques formée par les courbes *semistables*, ce que suffisait pour FLT car si l'on admet l'existence des courbes de Frey, elles doivent être semistables: on va expliquer cette notion dans un instant. Selon un résultat de K.Ribet (1986) conjecturé déjà en automn 1984 par G.Frey, les courdes de Frey ne sont jamais modulaires (a cause de symétries excessives de ses séries génératrices) donc STW semistable implique FLT par la contradiction avec la non-modularité des courbes de Frey.

Signalons que la STW générale est nécessaire, par exemple, pour montrer

$$a^p + b^p = c^3 \Longrightarrow abc = 0 \quad \text{pour} \quad p \geq 5$$

(à l'aide d'une courbe analogue à la courbe de Frey, mais qui n'est pas semistable dans ce cas).

II) *L'existence d'une forme modulaire $f$ d'un niveau minimal $N_0 = N(E,p)$.* La démonstration du théorème de Ribet (qu'on ne discute pas en détail dans ce cours), associe à toute courbe $E$ (de bonne réduction $\bmod p$) le *conducteur d'Artin* $N_0 = N(E,p)$ de la repésentation galoisienne "elliptique"

$$\rho_{p,E} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{F}_p)$$

(sur les points d'ordre $p$ de $E$).

**Théorème de Ribet (pour les représentations elliptiques).** Soit $E$ une courbe elliptique de bonne réduction $\bmod p$ (dont la réduction $\bmod p$ est aussi elliptique $(E \bmod p)_{/\mathbf{F}_p}$). Si la série génératrice

$$g = g_{E,S} = \sum_{n \geq 1} b_n q^n \in \mathbf{Z}[[q]]$$

est modulaire ($g \in S_2(N)$ pour un $N$) alors il existe une forme modulaire $f \in S_2(N_0)$,

$$f = \sum_{n \geq 1} a_n q^n \in \mathcal{O}_{\overline{\mathbf{Q}}}[[q]]$$

à coefficients dans les nombres algébriques entiers $\mathcal{O}_{\overline{\mathbf{Q}}} \subset \overline{\mathbf{Q}} \subset \mathbf{C}$ telle que

$$f \in S_2(N_0) \quad \text{et} \quad \forall l \notin S, a_l \equiv b_l \bmod \lambda_p$$

pour un idéal maximal $\lambda_p \subset \mathcal{O}_{\overline{\mathbf{Q}}}$ contenant $p$ (en particuler, $f \not\equiv 0$).

**Corollaire.** Si $p \geq 5$, la courbe de Frey $E = E_{a^p,b^p,c^p} : y^2 = x(x-a^p)(x+b^p)$ avec $a^p \equiv -1 \bmod 4$, 2 divise $b$, n'est pas modulaire.

*En effet*, dans ce cas le conductuer d'Artin se calcule facilement, $N_0 = 2$, mais $S_2(2) \cong \Omega^1(X_0(2)) = 0$ donc $f \equiv 0$, contradiction avec le théoreme.

**Modularité des courbes elliptiques semistables.** Le but de mon cours: explquer la démonstration de Wiles de ce résultat.

*Définition.* Une courbe ellptique $E$ sur $\mathbf{Q}$ est dite *semistable* si l'on peut choisir son équation $\Phi(x,y)=0$ de telle faccon que

$\Phi(x,y)\in\mathbf{Z}[x,y]$ et

$\forall\ l$ premier les points singuliers de la réduction $\overline{\Phi}(x,y)\in\mathbf{F}_l[x,y]$ sont *simples*

(c'est à dire, la partie quadratique de $\overline{\Phi}(x,y)$ autour de tout point singulier $(x_0,y_0)$ est *non-dégénérée*; rapellons que pour un point singulier $(x_0,y_0)$

$$\overline{\Phi}(x_0,y_0)=\overline{\Phi}'_x(x_0,y_0)=\overline{\Phi}'_y(x_0,y_0)=0.$$

*Exemples.* a) Soit $E$ une courbe elliptique d'équation $y^2=x(x-a^p)(x+b^p)$ avec un nombre premier $p\geq 5$, alors la substitution $x=4X, y=8Y+4X$ donne l'équation suivante

$$Y^2+XY=X^3+\gamma X^2+\delta X,\quad \gamma=\frac{b^p-a^p-1}{4},\delta=-\frac{a^pb^p}{16}$$

d'où $E$ est semistable pour $l=2$ si $a^p\equiv -1 \bmod 4$, $2|b$: $(X,Y)=(0,0)$ est un seul point singulier $\bmod 2$ avec la partie quadratique

$$\begin{cases} Y^2+XY, & \text{si 8 divise } a^p+1\\ X^2+XY+Y^2, & \text{si 8 ne divise pas } a^p+1.\end{cases}$$

D'autre part, si $l\neq 2$, $a^p+b^p=c^p$ et $l|abc$ alors il n'y a qu'un seul point singuler $(x,y)=(\alpha,0)$ pour l'équation d'origine $y^2=P_3(x)$, où $\alpha$ est une racine *simple* du polynôme cubique $P_3(x)=x(x-a^p)(x+b^p)$; la partie quadratique $y^2-\varepsilon x^2$ avec $\varepsilon=P''(\alpha)\neq 0$ est donc non-dégénérée.

b) La courbe elliptique modulaire $X_0(15): y^2=x(x+3^2)(x-4^2)$ est semistable, mais $E: y^2=x(x-3^2)(x+4^2)$ n'est pas semistable.

**Théorème 1.1 (STW semistable, A.Wiles, 1994).** Toute courbe elliptique semistable est modulaire.

**Corollaire.** Il n'existe pas de courbes de Frey $E=E_{a^p,b^p,c^p}$ et l'assertion $FLT(p)$ est vraie pour tout nombre premier $p\geq 5$.

*Plan de démonstration* du théorème 1.1.

I) *Modularité modulo p* (avec $p=3,5$). Soit $E: y^2=P_3(x)$ une courbe elliptique semistable, on peut supposer $P_3(x)\in\mathbf{Z}[x]$, et soit $g=g_{E,S}=\sum_{n\geq 1}b_nq^n\in\mathbf{Z}[[q]]$ sa série génératrice,

$$b_l=l-N_l(E)=-\sum_{x \bmod l}\left(\frac{x}{l}\right),\quad \left(\frac{x}{l}\right)\ \text{est le symbole de Legendre.}$$

On construit une forme modulaire $h=\sum_{n\geq 1}c_nq^n\in\mathcal{O}_{\overline{\mathbf{Q}}}[[q]]$ avec $c_l\equiv b_l \bmod \lambda_p$ pour tous les $l\notin S$ avec un ensemble fini exceptionnel $S$, où $\lambda_p\subset\mathcal{O}_{\overline{\mathbf{Q}}}$ un idéal maximal contenant $p$. Ce problème a été résolu uniquement pour $p = 3$ (le théorme de Tunnell-Langlands-Serre) sous la condition d'irréductibilité modulo 3 pour la représentation

$$\rho_{3,E} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{F}_3)$$

(sur les points d'ordre 3 de $E$). Cette condition n'est pas toujours satisfaite, et elle a beaucoup enquêté A.Wiles. En mai 1993 A.Wiles a trouvé un moyen de contourner cette condition à l'aide d'une famille $E_t$ avec toutes les représentations $\rho_{5,E_t}$ isomorphes, dans laquelle il y a une courbe $E' = E_{t_0}$ avec $\rho_{3,E'}$ irréductible, ce que permet de remplacer $E$ par $E'$ dans le raisonnement.

II) *Relèvement modulaire:* toute série $\tilde{h} = \sum_{n \geq 1} \tilde{c}_n q^n \in \mathcal{O}[[q]]$ à coefficients dans une extension finie $\mathcal{O}$ de $\mathbf{Z}_p$ (d'idéal maximal $\lambda$), satisfaisante certaines *conditions nécessaires* de modulatité, avec la propriété

$$\forall l \notin S, \tilde{c}_l \equiv c_l \bmod \lambda$$

est *automatiquement* une forme modulaire (on l'appele un *relèvement* de $h \bmod \lambda$, ou une *déformation admissible* de $h$). On donne ces conditions nécessaires et la formulation du théorème de Ribet en termes d'irréductibilité absolue de rerésentations galoisiennes attachées aux formes modulaires. Autrement dit, on montre que toute relèvement admissible de $h \bmod \lambda$ est modulaire.

III) *Application du relèvement modulaire:* on montre que les conditions d'irréductibilité absolue sont satisfaites pour la représentation galoisienne

$$\rho_{p,E} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathbf{F}_p)$$

soit avec $p = 3$ soit avec $p = 5$.

IV) *Fin de démonstration : passage de $p = 3$ à $p = 5$.* Posons $\tilde{h} = g$ (la série génératrice); par I) elle est une déformation admissible d'une forme modulaire $h \bmod 3$ (sous les conditions d'irréductibilité pour $p = 3$), et II) implique que dans ce cas $g$ est une forme modulaire. Sinon, III) dit que les conditions d'irréductibilité sont satisfaites pour $p = 5$, de plus, II) implique que $g' = g_{E',S}$ est une forme modulaire. Par la construction de $E'$ la série $g' \bmod 5 = g \bmod 5 \in \mathbf{F}_5[[q]]$ satisfait de nouveau aux conditions II) de relèvement modulaire (avec $p = 5$) donc $g$ et modulaire dans tous les deux cas.

### Références bibliographiques


1. Wiles, Andrew, Modular elliptic curves and Fermat's Last Theorem. Ann. Math., II. Ser. 141, No.3, 443-551 (1995)

2. Taylor, Richard; Wiles, Andrew, Ring-theoretic properties of certain Hecke algebras. Ann. Math., II. Ser. 141, No.3, 553-572 (1995)

3. Serre, Jean-Pierre, Travaux de Wiles (et Taylor,...). I. (The works of Wiles (and Taylor,...). I.). Séminaire Bourbaki. Volume 1994/95. Exposés 790-804. Paris: Societe Mathématique de France, Astérisque. 237, 319-332, Exp. No.803 (1996)

4. Oesterlé, Joseph, Travaux de Wiles (et Taylor, ...). II. [Works of Wiles (and Taylor ...). II] Séminaire Bourbaki, Vol. 1994/95. Astérisque No. 237 (1996), Exp. No. 804, 5, 333–355

5. Ribet, K.A., On modular representations of Gal($\overline{\mathbf{Q}}/\mathbf{Q}$) arising from modular forms. Invent. Math. 100, No.2, 431-476 (1990)

6. Frey, Gerhard, Links between stable elliptic curves and certain diophantine equations. Ann. Univ. Sarav., Ser. Math. 1, No.1, 40 p. (1986)

7. Serre, Jean-Pierre, Sur les representations modulaires de degre 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$). Duke Math. J. 54, 179-230 (1987)

8. Darmon, Henri; Diamond, Fred; Taylor, Richard, Fermat's Last Theorem. Bott, Raoul (ed.) et al., Current developments in mathematics, 1995. Lectures of a seminar, held in Boston, MA, USA, May 7-8, 1995. Cambridge, MA: International Press. 1-107 (1995).

9. Cornell, Gary (ed.); Silverman, Joseph H.(ed.); Stevens, Glenn (ed.), Modular forms and Fermat's last theorem. Papers from a conference, Boston, MA, USA, August 9–18, 1995

10. Borevich Z.I., Shafarevich I.R., Number Theory. 3$^{\text{rd}}$ Ed., Moscow, Nauka, 1985, 503 p.

11. Manin, Yu.I.; Panchishkin, A.A., Introduction to number theory. Number theory I: fundamental problems, ideas and theories. Transl. from the Russian by A. A. Panchishkin. Berlin: Springer-Verlag. Encycl. Math. Sci. 49, 303 p. (1995)

12. Hellegouarch, Yves, Invitation aux mathématiques de Fermat-Wiles. Enseignement des Mathématiques. Paris: Masson. vii, 397 p. (1997)

13. van der Poorten, Alfred J., Notes on Fermat's last theorem. Canadian Mathematical Society Series of Monographs and Advanced Texts. New York, NY: Wiley

14. Hida, Haruzo, Elementary theory of $L$-functions and Eisenstein series. London Mathematical Society Student Texts, 26. Cambridge University Press, Cambridge, 1993. xii+386 pp.

15. Serre, Jean-Pierre, Formes modulaires et fonctions zeta p-adiques. Modular Functions one Variable III, Proc. internat. Summer School, Univ. Antwerp 1972, Lecture Notes Math. 350, 191-268 (1973)

16. Serre, Jean-Pierre, Cours d'arithmétique. 2me ed. Le Mathématicien. Paris: Presses Universitaires de France. 188 p. (1977)

17. Darmon H., A proof of the full Shimura-Taniyama-Weil conjecture is announced. Notices of the AMS, December 1999, 1397-1401.