Formes modulaires

1 Fonctions de réseaux

Exercice 1. *Soit F une fonction sur l'ensemble $\mathcal{R}$ des réseaux de $\mathbb{C}$ à valeurs complexes de poids $k \in \mathbb{Z}$, i.e. telle que $F(\lambda\Gamma) = \lambda^{-2k}F(\Gamma)$ pour tout réseau $\Gamma \in \mathcal{R}$ et tout $\lambda \in \mathbb{C}^\times$. Montrez qu'il existe une fonction modulaire f de poids $2k$ et de niveau 1, i.e. $f_{|2kA} = f$ pour tout $A \in SL_2(\mathbb{Z})$, telle que*

$$F(\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2) = \omega_2^{-2k} f(\frac{\omega_1}{\omega_2})$$

Étant donné un réseau Λ de $\mathbb{C}$, on pose pour tout entier $m \geq 3$:

$$G_m(\Lambda) := \sum_{\omega\in\Lambda}{}' \frac{1}{\omega^m} = \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^m}$$

Une fois noté que $G_m(\Lambda)$ est nul pour m impair, $G_{2k}(\Lambda)$ est appelée **la série d'Eisenstein d'indice 2k** de Λ. On a vu dans la feuille 2, que ces séries convergent pour $k \geq 2$ et que le développement de Laurent de la fonction de Weierstrass $\mathfrak{P}$ à l'origine est

$$\mathfrak{P}_\Gamma(z) = \frac{1}{z^2} + 3G_4(\Gamma)z^2 + 5G_6(\Gamma)z^4 + 7G_8(\Gamma)z^6 + \cdots$$

et que pour tout $z \in \mathbb{C}/\Gamma$, les points $(\mathfrak{P}_\Gamma(z), \mathfrak{P}'_\Gamma(z))$ décrivent la cubique d'équation

$$Y^2 = 4X^3 - g_4X - g_6$$

où $g_4 := 60G_4(\Lambda)$ et $g_6 = 140G_6(\Lambda)$. Le discriminant est alors $\Delta(\Lambda) = g_4^3 - 27g_6^3$ et l'invariant modulaire $j(\Lambda)$, appelé ainsi car deux courbes elliptiques sur $\mathbb{C}$ sont birationnellement équivalentes si et seulement si elles ont le même j, est $j(\Lambda) = 1728\frac{g_4^3}{\Delta}$.

Exercice 2. *Décrivez les fonctions modulaires attachées aux fonctions de réseaux G_{2k}, Δ et j. Montrez que G_{2k} et Δ sont des formes modulaires avec Δ parabolique. Qu'en est-il de j?*

2 Formes modulaires de niveau 1

Pour un entier k, on note $\mathcal{M}(1,k)$ (resp. $\mathcal{C}(1,k)$) le $\mathbb{C}$-espace vectoriel des formes modulaires de poids k (resp. paraboliques de poids k). On rappelle les résultats suivants du cours:

- $\mathcal{M}(1,k)$ est nul pour k impair;
- $\mathcal{M}(1,2k) = \mathcal{C}(1,2k) \oplus \mathbb{C}.G_{2k}$;
- $\mathcal{M}(1,2k) = 0$ pour $k < 0$ et $k = 2$;
- pour $k = 0, 2, 3, 4, 5$, $\mathcal{M}(1,2k) = \mathbb{C}G_{2k}$ et $\mathcal{C}(1,2k) = 0$;
- la multiplication par Δ définit un isomorphisme de $\mathcal{M}(1,2k-12)$ sur $\mathcal{C}(1,2k)$.

Exercice 1. *Montrez que $\mathbb{M}(1,2k)$ admet pour base la famille des monômes $G_2^\alpha G_3^\beta$ avec α, β des entiers positifs ou nuls tels que $2\alpha + 3\beta = 2k$ où*

$$G_k(\tau) = \zeta(k) \sum_{\substack{(c,d)\\ c\wedge d=1}} \frac{1}{(c\tau+d)^k}$$

sont les séries d'Eisenstein introduites plus haut. On introduit alors $E_k(\tau) = \frac{1}{2}\sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ c\wedge d=1}} \frac{1}{(c\tau+d)^k}$*, montrez que l'on peut l'écrire sous la forme*

$$E_k(\tau) = \frac{1}{2}\sum_{\gamma\in P_+\backslash SL_2(\mathbb{Z})} j(\gamma,\tau)^{-k}$$

où $j(\gamma,\tau)$ *est le facteur d'automorphie habituel et* $P_+ = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} :\ n\in\mathbb{Z}\}$.

Exercice 2. *En partant de la formule classique*

$$\pi\mathrm{cotg}(\pi z) = \frac{1}{z} + \sum_{m=1}^{\infty}(\frac{1}{z+m} + \frac{1}{z-m})$$

montrez que pour tout $k \geq 2$*, on a*

$$\sum_{m\in\mathbb{Z}} \frac{1}{(m+z)^k} = \frac{1}{(k-1)!}(-2i\pi)^k \sum_{n=1}^{\infty} n^{k-1}q^n$$

où $q = e^{2i\pi z}$ *et en déduire que pour tout* $k \geq 1$*,*

$$G_{2k}(z) = 2\zeta(2k) + 2\frac{(2i\pi)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n$$

où on note $\sigma_k(n) = \sum_{d|n} d^k$.

On pose alors $E_{2k}(z) = \frac{G_{2k}(z)}{2\zeta(2k)}$*, montrez que*

$$E_{2k}(z) = 1 + (-1)^k\frac{4k}{B_k}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n$$

où B_k *est le* k*-ème nombre de Bernouilli défini par*

$$\frac{x}{e^x-1} = \sum_{k=1}^{\infty}(-1)^{k+1}B_k\frac{x^{2k}}{(2k)!}$$

avec $\zeta(2k) = \frac{2^{2k-1}}{(2k)!}B_k\pi^{2k}$.

Exercice 3. *Montrez que*

$$(2\pi)^{-12}\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

L'application $n\mapsto\tau(n)$ *s'appelle la fonction de Ramanujan. Montrez que* $\tau(n) = O(n^6)$.
Remarque: Deligne a en fait montré la célèbre conjecture de Ramanujan-Peterson: si p *est premier on a* $|\tau(p)| \leq 2p^{11/2}$.

Exercice 4. *Montrez les égalités suivantes:*

$$\sigma_7(n) = \sigma_3(n) + 120\sum_{m=1}^{n-1}\sigma_3(m)\sigma_3(n-m)$$

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040\sum_{m=1}^{n-1}\sigma_3(m)\sigma_5(n-m)$$

Exercice 5. *Montrez les congruences suivantes*

$$\begin{aligned}
&\tau(n) \equiv \sigma_{11}(n) \mod 691\\
&p^7 \equiv p^3 \mod 120\\
&11p^9 \equiv 21p^5 - 10p^3 \mod 5040\\
&p^9 \equiv 11p^5 - 10p^3 \mod 2640
\end{aligned}$$

3 Formes modulaires de niveau quelconque

Soit N un entier positif, on notera avec une barre la réduction modulo N d'un élément de $\mathbb{Z}$, $\mathbb{Z}^2$ ou de $GL_2(\mathbb{Z})$ selon le cas. On pose $\epsilon_N = \frac{1}{2}$ si $N = 1, 2$ et $\epsilon_N = 1$ sinon.
Séries d'Eisenstein: pour $k \geq 3$ et $v \in \mathbb{Z}^2$, on définit

$$E_k^{\bar{v}} = \epsilon_N \sum_{\substack{(c,d)\equiv v \mod N \\ c\wedge d=1}} \frac{1}{(c\tau+d)^k} = \sum_{\gamma\in(P_+\cap\Gamma(N))\backslash\Gamma(N)\delta} j(\gamma,\tau)^{-k}$$

où $\delta \in \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ est tel que $\overline{(c,d)} = \bar{v}$.

Exercice 1. - *Montrer que pour $\gamma \in SL_2(\mathbb{Z})$, on a*

$$(E_k^{\bar{v}})_{|k}\gamma(\tau) = E_k^{\overline{v\gamma}}(\tau)$$

et en déduire que $E_k^{\bar{v}} \in \mathcal{M}(N,k)$.

- Montrez que

$$\lim_{\mathrm{Im}\,\tau\to\infty} E_k^{\bar{v}}(\tau) = \begin{cases} (\pm 1)^k \text{ si } \bar{v} = \pm\overline{(0,1)}, \text{ sauf si } k \text{ est impair et } N = 1,2 \\ 0 \text{ sinon} \end{cases}$$

- On introduit pour $k \geq 3$ pair ou $N > 2$, $\mathcal{E}(N,k)$ le sous-espace vectoriel de $\mathcal{M}(N,k)$ engendré par les $E_k^{\bar{v}}$. Soit alors $\mathcal{I} := \{\bar{v} = \overline{(c,d)}\}$ un ensemble tel que les $-d/c$ représentent les cusps de $\Gamma(N)$. Montrez alors que $\{E_k^{\bar{v}}, \bar{v} \in \mathcal{I}\}$ est une base de $\mathcal{E}(N,k)$.
Indication: *utilisez que pour k impair et $N = 1, 2$, $\mathcal{M}(N,k) = \mathcal{C}(N,k)$ et que sinon la dimension de $\mathcal{M}(N,k)/\mathcal{C}(N,k)$ est égale au nombre de de cusps de $\Gamma(N)$.*

On introduit les séries d'Eisenstein non normalisées

$$G_k^{\bar{v}}(\tau) = {\sum_{(c,d)\equiv v \mod N}}' \frac{1}{(c\tau+d)^k}$$

Exercice 2. *Montrer que*

$$G_k^{\bar{v}}(\tau) = \frac{1}{\epsilon_N} \sum_{n\in(\mathbb{Z}/N\mathbb{Z})^\times} \zeta_+^n(k) E_k^{n^{-1}\bar{v}}(tau)$$

où $\zeta_+^n(k) = \sum_{\substack{m=1 \\ m\equiv n \mod N}}^{\infty} \frac{1}{m^k}$ est la fonction zêta d'Hurwitz. En déduire que

$$E_k^{\bar{v}}(\tau) = \epsilon_N \sum_{n\in(\mathbb{Z}/N\mathbb{Z})^\times} \zeta_+^n(k,\mu) G_k^{n^{-1}\bar{v}}(\tau)$$

où μ est la fonction de Moebius et $\zeta_+^n(k,\mu) = \sum_{\substack{m=1 \\ m\equiv n \mod N}}^{\infty} \frac{\mu(m)}{m^k}$. En déduire que $\{G_k^{\bar{v}}, \bar{v} \in \mathcal{I}\}$ est une base de $\mathcal{E}(N,k)$.

Le développement en série de Fourier de $G_k^{\bar{v}}$ se calcule aisément et donne

$$G_k^{\bar{v}}(\tau) = \delta(\bar{c}_v)\zeta^{\bar{d}_v}(k) + \frac{(-2i\pi)^k}{(k-1)!N^k} \sum_{n=1}^{\infty} \sigma_{k-1}^{\bar{v}}(n) q_N^n$$

avec $q_N = e^{2i\pi N}$, $\delta(\bar{c}_v) = 1$ si $\bar{c}_v = \bar{0}$ et 0 sinon, $\zeta^{\bar{d}_v} = \sum'_{d\equiv d_v \mod N} d^{-k}$, et
$\sigma_{k-1}^{\bar{v}}(n) = \sum_{\substack{m|n \\ n/m\equiv c_v \mod N}} sgn(m) m^{k-1} e^{2i\pi d_v m/N}$.

Étant donné deux caractères de Dirichlet ψ modulo u et ϕ modulo v avec $uv = N$ et $(\psi\phi)(-1) = (-1)^k$, on considère

$$G_k^{\psi,\phi}(\tau) = \sum_{c=0}^{u-1}\sum_{d=0}^{v-1}\sum_{e=0}^{u-1}\psi(c)\bar{\phi}(d)G_k^{\overline{(cv,d+ev)}}(\tau)$$

ainsi que $E_k^{\psi,\phi}(\tau) = \frac{v^k(k-1)!}{g(\phi)(-2i\pi)^k}G_k^{\psi,\phi}(\tau)$. Alors $G_k^{\psi,\phi} \in \mathcal{M}(N,k,\psi\phi)$. Pour $k \geq 3$, on introduit $A_{n,k}$ l'ensemble des triplets (ψ,ϕ,t) tels que ψ,ϕ sont des caractères de Dirichlet primitifs modulo u et v avec $(\psi\phi)(-1) = (-1)^k$ et t un entier positif tel que $tuv|N$. Alors

$$\{E_k^{\psi,\phi}(t\tau) :\ (\psi,\phi,t) \in A_{N,k},\ \psi\phi = \xi\}$$

est une base de $\mathcal{E}(N,k,\xi)$.

En poids 2, on peut définir des séries d'Eisenstein via la fonction $\mathfrak{P}$ de Weierstrass; en poids 1 on utilise la fonction σ de Weierstrass

$$\sigma_\Lambda(z) = z\prod_{\omega\in\Lambda}{}'(1-\frac{z}{\omega})e^{z/\omega+(z/\omega)^2/2}$$

Afin de réunir toutes ces situations en une, on introduit les séries d'Eisenstein non holomorphes

$$G_k^{\bar{v}}(\tau,s) = \sum_{(c,d)\equiv v \mod N}{}' \frac{y^s}{(c\tau+d)^k|c\tau+d|^{2s}}$$

Ces séries convergent absolument pour $\mathrm{Re}(k+2s) > 2$ définissant alors un élément de $\mathcal{M}(N,k)$ et possèdent un prolongement méromorphe à tout le plan complexe. Pour $\mathrm{Re}(s+2k) \leq 2$, ces prolongements ne sont plus définis par la série mais donnent encore, d'après le théorème de prolongement analytique, des formes modulaires. En particulier pour $s = 0$, on retrouve les séries d'Eisenstein "classiques": pour $k \geq 3$ on retrouve les séries classiques mais pour $k \leq 2$, on obtient quelque chose de nouveau.

Exercice 3. *Soit $\theta^{2k}(z) = \sum_n r_{2k}(n)q^n$. En remarquant que pour $k \leq 3$, $\mathcal{C}(4,k)$ est nul, montrez que $r_{2k}(n) = \delta_k(n)$ où $\delta_k(n)$ est une fonction arithmétique qui met en jeu des sommes de diviseurs de n, d'ordre de grandeur$n^{k/2-1}$ et que pour $k \geq 4$, on a $r_{2k}(n) = \delta_k(n) + O_\epsilon(n^{\frac{k-1}{2}+\epsilon})$ pour tout $\epsilon > 0$ alors que $\delta_k(n)$.*

Séries de Poincaré: comme on l'a vu les séries d'Eisenstein ne donnent pas des formes paraboliques. Pour en construire on s'inspire de la construction précédente en introduisant

$$P_k(z;m) := \sum_{\gamma\in\Gamma_\infty\backslash\Gamma}\frac{e(m\gamma z)}{j(\gamma,z)^k}$$

où $m \geq 0$ est entier. Pour $m = 0$ on retrouve les séries d'Eisenstein. En particulier pour $m > 0$, les séries de Poincaré sont dominées par les séries d'Eisenstein qui s'annulent en tous les cusps non équivalents à ∞; en outre pour $m > 0$, elles s'annulent aussi en ∞ de sorte qu'elles sont des élément de $\mathcal{C}(N,k)$.

Exercice 4. *Soit $f(z) = \sum_{n=1}^\infty a_n q^n \in \mathcal{C}(N,k)$. Montrez que*

$$< P_k(z;m), f >= \frac{\bar{a}_m}{(4\pi m)^{k-1}}\Gamma(k-1)$$

et en déduire que les $P_k(z;m)$ engendrent $\mathcal{C}(N,k)$.

Ainsi pour évaluer les coefficients de Fourier, il suffit de le faire pour les séries de Fourier. Ces calculs introduisent alors les sommes de Kloosterman.

4 Opérateurs de Hecke

Pour n un entier, on note $T(n)$ la correspondance sur l'ensemble des réseaux $\mathcal{R}$ définit par

$$T(n)\Gamma = \sum_{[\Gamma:\Gamma']=n} \Gamma'$$

Les $T(n)$ sont des endomorphismes du groupe abélien $\mathbb{Z}[\mathcal{R}]$. On note aussi pour $\lambda \in \mathbb{C}^\times$, R_λ l'opérateur d'homothétie. On rappelle alors les relations suivantes:

$$\begin{cases} R_\lambda R_\mu = R_{\lambda\mu} \\ R_\lambda T(n) = T(n) R_\lambda \\ T(m)T(n) = T(mn) \text{ si } m \wedge n = 1 \\ T(p^n)T(p))T(p^{n+1} + pT(p^{n-1})R_p \ p \text{ premier} \end{cases}$$

Étant donné une fonction faiblement modulaire de poids $2k$, il lui correspond une fonction F de poids $2k$ sur $\mathcal{R}$, on définit alors $T(n)f$ comme la fonction sur $\mathcal{H}$ associée à la fonction $n^{2k-1}T(n)F$ sur $\mathcal{R}$ (le coefficient n^{2k-1} permet d'avoir des formules sans dénominateurs). On peut alors montrer que si f est une forme modulaire (resp. forme parabolique) alors il en est de même de $T(n)f$.

Soit $f(z) = \sum_{n=0}^{\infty} c(n)q^n$ une forme modulaire de poids $2k > 0$ non nulle propres pour tous les $T(n)$, alors $c(1)$ est non nul et si on normalise f de telle sorte que $c(1) = 1$ alors la valeur propre associée est égale à $c(n)$.

Exercice 1. *Montrez que G_{2k} (resp. Δ) est une fonction propre des $T(n)$ de valeurs propres les $\sigma_{2k-1}(n)$ (resp. $\tau(n)$). Que pouvez-vous en déduire d'intéressant?*

On note $\mathcal{D}^* = \{\tau \in \mathcal{H} : \ \mathrm{Re}(\tau) \leq 1/2, \ |\tau| \geq 1\} \cup \{\infty\}$. Pour $\Gamma \subset SL_2(\mathbb{Z})$ un sous-groupe de congruence, soient $\{\alpha_j\}$ un ensemble de représentant de $\{\pm I\}\Gamma\backslash SL_2(\mathbb{Z})$. Pour $f, g \in \mathcal{M}(N,k)$ tels que fg s'annule en tous les cusps, alors on définit

$$< f, g >_\Gamma = \frac{1}{V_\Gamma} \sum_j \int_{\mathcal{D}^*} f(\alpha_j\tau)\overline{g(\alpha_j\tau)}(\mathrm{Im}(\tau))^k d\mu(\tau)$$

où $d\mu(\tau) = \frac{dx\ dy}{y^2}$. On remarque alors que les $T(n)$ sont autoadjoints et comme ils commutent entre eux, ils sont alors simultanément diagonalisables avec des valeurs propres réelles.

Exercice 2. *Montrez que les coefficients de Fourier des fonctions paraboliques propres pour les opérateurs de Hecke, ont des coefficients de Fourier qui sont des entiers algébriques.*

Exercice 3. *- Soit $P_+(N) := P_+ \cap \Gamma(N)$; montrez que $\mathcal{D}_N^* = \{\tau \in \mathcal{H}^* : \ 0 \leq \mathrm{Re}(\tau) \leq N\} \cup \{\infty\}$ est un domaine fondamental de $P_+(N)\backslash\mathcal{H}^*$.*

- Soit alors α_i (resp. β_i) un système de représentants de $P_+(N)\backslash\Gamma(N)$ (resp. de $\Gamma(N)\backslash SL_2(\mathbb{Z})$). Montrez que pour tout $f \in \mathcal{C}(N,k)$, on a

$$\int_{\mathcal{D}_N^*} f(\tau)(\mathrm{Im}(\tau))^{k+s} d\mu(\tau) = 0$$

et en déduire que $< f, E_k^{\overline{(0,1)}}(\tau, s) >= 0$ pour tout $\mathrm{Re}(s + 2k) > 2$.

- Conclure que $\mathcal{M}(N,k) = \mathcal{C}(N,k) \oplus \mathcal{E}(N,k)$, la décomposition étant orthogonale.

5 Fonctions L d'une forme modulaire

Soit $f(z) = \sum_{n=0}^{\infty} c_n q^n \in \mathcal{M}(1, 2k)$. La fonction $n \mapsto c_n$ ayant tendance à être multiplicative il est naturel, au moins depuis Euler, de lui associer **la série de Dirichlet**

$$L(f, s) := \sum_{n=1}^{\infty} c_n n^{-s}.$$

Exercice 1. *Montrez que $L(f,s)$ converge pour $\mathrm{Re}(s) > 2k$ et que si f est propre pour les opérateurs de Hecke, elle est égale au produit eulérien*

$$\prod_p \frac{1}{1 - c_p p^{-s} + p^{2k-1-2s}}$$

Montrez alors que

$$L(E_k, s) = \prod_p \frac{1}{(1-p^{2k-1-s})(1-p^{-s})} = \zeta(s-2k+1)\zeta(s)$$

$$L(\Delta, s) = \prod_p \frac{1}{1 - \tau(p)p^{-s} + p^{11-2s}}$$

Lorsque $f \in \mathcal{M}(N, 2k)$, on définit

$$L(f,s) = \prod_{p|N} \frac{1}{1-c_p p^{-s}} \prod_{p \not| N} \frac{1}{1 - c_p p^{-s} + p^{2k-1-2s}}$$

En utilisant la transformation de Mellin $M\psi(s) := \int_0^\infty \psi(t) t^{s-1} dt$

$$M(\sum_{n=1}^\infty c_n e^{-nt}) = \Gamma(s) \sum_{n=1}^\infty \frac{c_n}{n^s}$$

on montre que si $f \in \mathcal{M}(1, 2k)$ (resp. $f \in \mathcal{C}(1, 2k)$) alors $L(f,s)$ admet un prolongement méromorphe (resp. holomorphe) à $\mathbb{C}$ avec un seul pôle simple en $s = 2k$ de résidu $\frac{(2i\pi)^{2k}}{(k-1)!} c_0$. En outre ce prolongement méromorphe satisfait à l'équation fonctionnelle

$$(2\pi)^{-s}\Gamma(s)L(f,s) = (-1)^k (2\pi)^{s-2k}\Gamma(2k-s)L(f, 2k-s)$$

Pour $f \in \mathcal{M}(N, 2k)$, la fonction $L(f,s)$ converge toujours absolument et uniformément pour $\mathrm{Re}(s) \geq 2k + \epsilon$ pour tout $\epsilon > 0$ et possède un prolongement méromorphe à $\mathbb{C}$ avec au plus un pôle simple en $s = 2k$. Cependant elle ne possède pas en général une équation fonctionnelle car on n'a plus de symétrie pour $f(it)$ lorsque l'on passe de t à $1/t$. Ce qui remplace cette symétrie est **l'involution de Fricke**

$$w_N : f(\tau) \mapsto w_N f(\tau) := N^{-k} \tau^{-2k} f(\frac{-1}{N\tau})$$

qui agit sur $\mathcal{C}(N, 2k)$ parce que $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$ normalise $\Gamma_0(N)$. Cette involution permet de décomposer $\mathcal{C}(N, 2k)$ en une somme directe de deux sous-espaces propres $\mathcal{C}(N, 2k)^\pm$ tels que si $f \in \mathcal{C}(N, 2k)^\epsilon$ alors

$$(2\pi)^{-s} N^{s/2} \Gamma(s) L(f,s) = \epsilon(-1)^k N^{\frac{2k-s}{2}} \Gamma(2k-s) L(f, 2k-s)$$

On remarquera aussi que w_N stabilise le sous-espace des formes nouvelles.

Étant donnée une courbe elliptique E définie sur $\mathbb{Q}$, on pose alors pour tout premier p:

$$a_p = \begin{cases} p + 1 - N_p \text{ si } E \text{ a bonne réduction en } p \\ 1 \text{ si } E \text{ admet deux tangentes au point double, rationnelles sur } \mathbb{F}_p \\ -1 \text{ si } E \text{ admet un point double isolé dans } \mathbb{F}_p \\ 0 \text{ si } E \text{ admet une réduction additive} \end{cases}$$

où N_p désigne le nombre de points de la courbe réduite modulo p dans $\mathbb{P}^2(\mathbb{F}_p)$. Pour $\mathrm{Re}(s) > 3/2$, on définit alors la fonction L de E par le produit infini

$$L(E,s) = \prod_{\text{mauvais } p} \frac{1}{1 - a(p)p^{-s}} \prod_{\text{bons } p} \frac{1}{1 - a(p)p^{-s} + p^{1-2s}}$$

Hasse a alors conjecturé que $L(E,s)$ admettait un prolongement analytique dans $\mathbb{C}$ tout entier et que

$$\Lambda(E,s) := N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$$

où N_E est le conducteur de E, vérifiait l'équation fonctionnelle

$$\Lambda(E,2-s) = \pm\Lambda(E,s)$$

Théorème (Eichler, Shimura) Soit $N \geq 1$ et soit $f \in \mathcal{C}(N,2)^{new}$ une forme nouvelle propre pour les opérateurs de Hecke. Alors il existe une courbe elliptique E définie sur $\mathbb{Q}$ telle que la transformée de Mellin de f soit $N^{-s/2}\Lambda(E,s)$.

Les courbes elliptiques construite à partir de formes paraboliques nouvelles de Hecke, sont appelées des **courbes de Weil**. Ainsi si E est une courbe de Weil, elle vérifie la conjecture de Hasse. La fameuse conjecture de Shimura-Taniyama-Weil est alors la suivante:

Soit E une courbe elliptique sur $\mathbb{Q}$, on désigne par $L(E,s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ et $f_E(\tau) = \sum_{n\geq 1} a(n)q^n$ la transformée de Mellin inverse de $(2\pi)^{-s}\Gamma(s)L(E,s)$. Alors f_E appartient à $\mathcal{C}(N,2)^{new}$ où N désigne le conducteur de E et f_E est une forme propre pour les opérateurs de Hecke.

En 1994, Wiles a prouvé un cas particulier de cette conjecture, si E est semi-stable, résultat qui a été généralisé à toutes les courbes elliptiques par Breuil, Conrad, Diamond et Taylor. On savait depuis Serre que la conjecture de Shimura-Taniyama-Weil impliquait le grand théorème de Fermat, le principe étant le suivant. On veut associer à tout point primitif (a,b,c) de la courbe de Fermat $x^p + y^p + z^p$, une cubique de Weierstrass $E_{a,b,c}$ de telle sorte que la cubique soit lisse, i.e. une courbe elliptique, si et seulement si (a,b,c) n'est pas une solution triviale de l'équation de Fermat, i.e. $abc \neq 0$. Cette simple condition conduit à chercher $E_{a,b,c}$ sous la forme

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

avec puisque α, β, γ ne peuvent être définis qu'à une translation près, les conditions

$$\beta - \gamma = a^p, \quad \gamma - \alpha = b^p, \quad \alpha - \beta = c^p$$

de telle sorte que le discriminant soit $(abc)^{2p} \neq 0$. On prend alors $\gamma = 0$ et donc l'équation

$$y^2 = x(x-a^p)(x+b^p)$$

La courbe obtenue est alors semi-stable. Ainsi si on possédait une solution non triviale à l'équation de Fermat, en utilisant le résultat de Wiles et un cas particulier de la conjecture de Serre prouvé par Mazur-Ribet (et désormais en toute généralité par Wintenberger et Khare), on obtiendrait une forme f non nulle de $\mathcal{C}(2,2)$ alors que cet espace est nul.