La paramétrisation modulaire des courbes elliptiques

Notes pour le séminaire Jouve-Pazuki

Bruno Winckler

7 mars 2012

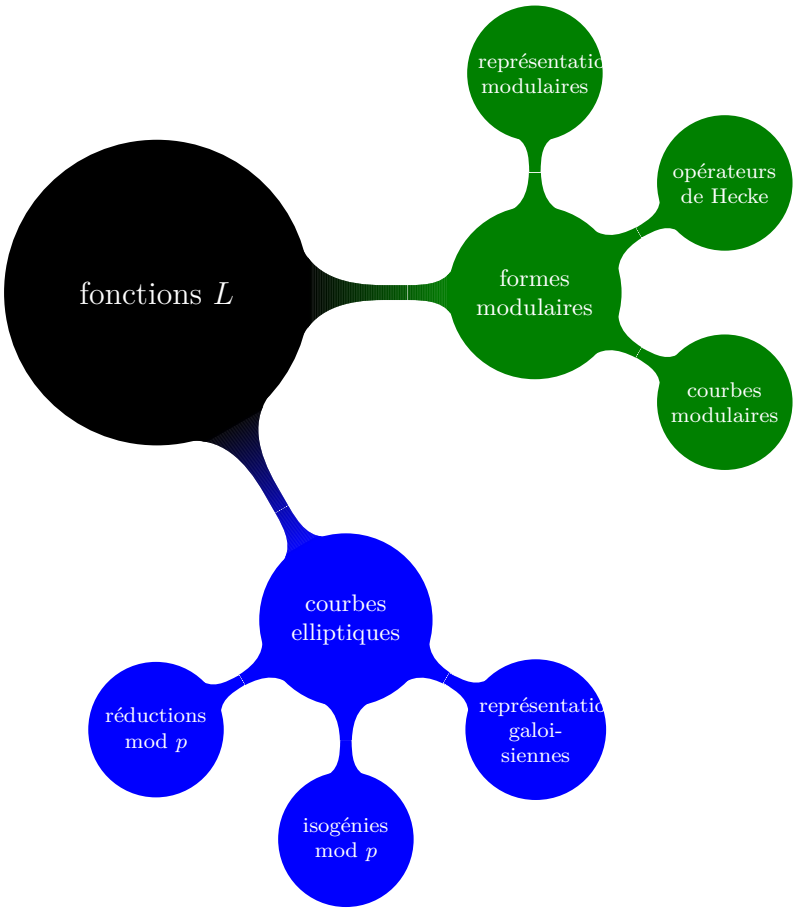
fonctions L
formes modulaires
représentatio modulaires
opérateurs de Hecke
courbes modulaires
courbes elliptiques
réductions mod p
représentatio galoi- siennes
isogénies mod p

Table des matières

Introduction

L'objectif de cet exposé d'une heure est de modestement présenter quelques aspects de la théorie des formes modulaires, et quelques applications de ce domaine qui peut paraître mystérieux d'un point de vue extérieur. On entend souvent parler pour la première fois des formes modulaires pour évoquer la démonstration du théorème de Fermat. Quand on s'intéresse un peu plus à ces objets, des fonctions de la variable complexe aux nombreuses symétries, on peut se demander où est le rapport, sans compter que l'énoncé « toute courbe elliptique rationnelle est modulaire » (qui revêt beaucoup de noms différents dans cet exposé et la littérature) n'est pas forcément des plus parlants, même avec toutes les cartes en main pour le comprendre. Je vais faire de mon mieux pour exposer, en une heure, le minimum syndical pour comprendre cet énoncé, et l'appliquer à quelques problèmes arithmétiques. Pour les besoins de la cause, je ferai plusieurs raccourcis et quelques imprécisions que les spécialistes ne manqueront pas de remarquer. Je fournis une bibliographie détaillée pour ceux qui désirent combler les trous et gommer les imperfections.

1 Formes modulaires de poids 2

1.1 Les courbes et formes modulaires

Soit N un entier naturel non nul. On appellera, quelque peu à tort, sous-groupe de congruence principal de niveau N le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ défini par

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}); \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}.$$

En particulier, $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$. Ces groupes agissent sur le demi-plan de Poincaré $\mathcal{H} = \{z \in \mathbb{C}; \Im(z) > 0\}$ par homographies, et même sur $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$.

Définition 1.1 (Courbes modulaires) *On note $X_0(N) = \Gamma_0(N) \backslash \mathcal{H}^*$, et on appelle ces courbes les courbes modulaires de niveau N.*

Les $X_0(N)$ sont des surfaces de Riemann compactes (et l'ajout de $\mathbb{P}^1(\mathbb{Q})$ est là pour que ce soit compact, justement). Les orbites de points de $\mathbb{P}^1(\mathbb{Q})$ sous $\Gamma_0(N)$ sont appelées *pointes* de $X_0(N)$. On peut démontrer qu'il y en a toujours un nombre fini ; pour $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$, il y en a même qu'une seule, car l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur la droite projective rationnelle est transitive. Sur le site `https://www.math.lsu.edu/~verrill/`, vous trouverez tout ce qu'on a envie de savoir sur ces courbes modulaires : leur genre, le nombre de points, à quoi ressemblent les domaines fondamentaux, *etc.*

Définition 1.2 (Formes modulaires (de poids 2)) *Soit N un entier naturel non nul. On appelle forme modulaire de niveau N (sous-entendu dans cet exposé : parabolique de poids 2 pour $\Gamma_0(N)$) une 1-forme différentielle holomorphe de $\Omega^1(X_0(N))$.*

Une telle forme se tire en arrière en $f(\tau)\mathrm{d}\tau$ sur le demi-plan de Poincaré, où f est une fonction holomorphe vérifiant quelques propriétés intéressantes : très grossièrement, comme $f(\tau)\mathrm{d}\tau$ est issue d'une 1-forme sur $X_0(N)$, elle doit être invariante sous l'action de Γ pour être bien définie. Autrement dit, pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, en notant $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$, on devrait avoir

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z\right) \mathrm{d}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z\right) = f(z)\mathrm{d}z.$$

Un calcul direct donne

$$\mathrm{d}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z\right) = \frac{\mathrm{d}z}{(cz+d)^2},$$

donc f vérifie

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N), \forall z \in \mathcal{H}, f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z).$$

On demande également que f soit « holomorphe aux pointes ». Grossièrement, ceci signifie que si on fait le développement « au voisinage d'une pointe » en série, alors ce développement commence aux puissances positives. Plus précisément : soit $f(\tau)\mathrm{d}\tau$ une forme modulaire pour Γ, et soit h le plus petit entier strictement positif tel que $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ soit dans Γ (il existe forcément un tel h). Alors $f(z+h) = f(z)$ par modularité, et f est une fonction h-périodique, donc admet un développement en série de Fourier (qui sera très important pour la suite) :

$$f(\tau) = \sum_n a_n e^{2i\pi\tau/h} = \sum_n a_n q_h^n,$$

et on dit que f est holomorphe en ∞ si n débute après 0. En fait, pour les formes modulaires au sens où je les ai introduites, n débute même après 1, f s'annulant aux pointes. Mais on ne veut pas que f soit holomorphe uniquement en ∞, mais en toutes les pointes, donc que $z \mapsto f\left(\frac{az+b}{cz+d}\right)$ soit holomorphe en ∞ pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$; en effet, pour tout rationnel, il existe une matrice de $\mathrm{SL}_2(\mathbb{Z})$ qui envoie ce rationnel sur ∞, donc le problème de l'holomorphie aux pointes se ramène en un problème d'holomorphie en ∞. Résumons :

Définition 1.3 (Formes modulaires (de poids 2), le retour) *Soit N un entier naturel non nul. On appelle forme modulaire de niveau N (sous-entendu dans cet exposé : parabolique de poids 2 pour $\Gamma_0(N)$) une fonction $f : \mathcal{H} \to \mathbb{C}$ holomorphe sur $\mathcal{H}$, qui vérifie :*

- $\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \forall z \in \mathcal{H}, f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$;
- *pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, l'application $z \mapsto f\left(\frac{az+b}{cz+d}\right)$ est holomorphe en ∞ (au sens donné dans le paragraphe précédent), et le terme constant de son développement est nul.*

Est-ce qu'il existe des fonctions si symétriques ? Je traite cette question dans la prochaine section.

1.2 Calcul de la dimension de l'espace vectoriel des formes modulaires

L'ensemble des formes modulaires (au sens très réduit que j'ai donné) de niveau N est un espace vectoriel sur $\mathbb{C}$, qu'on note $S_2(N)$ traditionnellement, de dimension finie. En effet, comme $X_0(N)$ est une courbe, elle a un genre (fini), et ce genre donne la dimension de $S_2(N)$. On peut le calculer explicitement. Tout d'abord :

Proposition 1.4 *Il n'existe pas de forme modulaire de niveau 1.*

Ébauche de preuve. Soit f une forme modulaire de niveau 1, vue comme fonction holomorphe sur $\mathcal{H}$. En intégrant $\frac{1}{2\pi i}\frac{f'}{f}$ sur un contour intelligent sur le bord d'un domaine fondamental de $X_1(1)$ (selon que f ait des zéros ou non sur ce bord), on trouve que

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{z \neq i,\rho} v_z(f) = \frac{1}{6},$$

où $v_z(f)$ désigne l'ordre d'annulation de f en z, $\rho = \exp(2i\pi/3)$, et la somme porte sur les éléments z du domaine fondamental choisi ; il y a bien un nombre fini de zéros pour f dans un domaine fondamental de $X_1(1)$, donc cette expression a un sens. Il est impossible d'écrire $\frac{1}{6}$ comme somme d'entiers positifs et de multiples de $\frac{1}{2}$ et $\frac{1}{3}$, donc il n'existe pas de forme modulaire pour $\mathrm{SL}_2(\mathbb{Z})$. □

Grâce à la formule de Riemann-Hurwitz, on en déduit le genre de tous les espaces $\Gamma_0(N)$. En effet, la projection naturelle $\mathcal{H}^* \to X_1(1)$ se factorise évidemment, pour donner une flèche $X_0(N) \to X_1(1)$. Le degré de cette application est l'indice de $\Gamma_0(N)$ dans $\mathrm{SL}_2(\mathbb{Z})$, et il reste à calculer la ramification de cette application. Pour la comprendre, il faudrait examiner en détail la géométrie de ces surfaces de Riemann, ce que je n'ai pas fait. La ramification dépend des pointes de $X_0(N)$, de ses points « elliptiques » (des points dont le stabilisateur sous l'action de $\Gamma_0(N)$ n'est pas trivial). En tout cas, on trouve :

Proposition 1.5 (Dimension de $S_2(N)$) *L'espace des formes modulaires de niveau N a une dimension explicitement calculable qui dépend de N et des nombres premiers qui le divisent.*

– *elle est nulle si, et seulement si* $N \in \{1,2,3,4,5,6,7,8,9,10,12,13,16,18,22,25,28,60\}$ *;*
– *supposons que* N *est un nombre premier. Alors la dimension de* $S_2(N)$ *est* $\left[\frac{N+1}{12}\right] - 1$ *si* $N \equiv 1 \mod 12$*, et* $\left[\frac{N+1}{12}\right]$ *sinon.*

Bref, pour certains N, il existe bien des formes modulaires. Ceci peut étonner, parce que des formes modulaires sont des fonctions vérifiant un très grand nombre de symétries !

Remarque. Si f est une forme modulaire pour un niveau N, elle est modulaire pour tout niveau multiple de N. De plus, si M est un autre entier naturel non nul, alors $z \mapsto f(Mz)$ est une forme modulaire de niveau NM, comme on le vérifie simplement. Ainsi, dans $S_2(N)$, il y a des formes provenant de tous les $S_2(d)$ pour d divisant M. Ceci motive la notion de forme modulaire ancienne : pour tout d divisant N/M, l'application $z \mapsto f(dz)$ est modulaire de niveau dM, donc de niveau N (car dM divise N). On note $S_2(\Gamma_1(N))^{\text{old}}$ l'espace vectoriel engendré par les formes modulaires pour $\Gamma_1(N)$ qui proviennent de niveaux plus petits par ces moyens : c'est l'espace des formes modulaires *anciennes* de niveau N.

Il est bien beau de montrer qu'il existe des formes modulaires si on n'est pas capable d'en exhiber. Le moyen le plus simple serait de considérer des fonctions qui sont une sorte de « moyenne » d'éléments, de sorte que faire agir un sous-groupe de congruence Γ sur la fonction ne ferait que « translater » les éléments de cette moyenne, qui serait alors plus ou moins invariante sous cette action. Cette idée mène aux séries d'Eisenstein, dont les plus simples sont de la forme

$$E_k(z) = \frac{(k-1)!}{2(2\pi i)^k} \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(mz+n)^k},$$

dont on voit immédiatement qu'elles vérifient $E_k\left(\frac{az+b}{cz+d}\right) = (cz+d)^k E_k(z)$ pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathrm{SL}_2(\mathbb{Z})$ (il y a juste à le vérifier pour $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, puisqu'ils engendrent le groupe $\mathrm{SL}_2(\mathbb{Z})$) ; la constante devant la somme est là pour des soucis de normalisation. Cependant, elles ne sont pas nulles en l'infini, et de toute façon c'est le cas où $k = 2$ qui nous intéresserait, et dans ce cas la fonction n'est pas holomorphe en ∞. Cependant, elle n'est pas loin de l'être[*]. En effet, son développement en ∞ est

$$E_2(\tau) = \frac{1}{8\pi\Im(z)} - \frac{1}{24} + \sum_{n=1}^{\infty} \sigma_1(n) q^n,$$

où σ_1 est la somme des diviseurs de n. La démonstration de cette égalité est intéressante, mais n'est pas le sujet de cet exposé. Alors, si on considère la fonction $z \mapsto 4E_2(4z) - E_2(z)$, la remarque précédente montre qu'elle vérifie la loi de transformation pour $\Gamma_0(4)$; il ne manquerait plus qu'elle s'annule en

∗. En fait, pour $k = 2$, c'est encore pire : la série ne converge pas absolument. En fait, on peut rajouter dans la somme un $\frac{1}{|mz+n|^s}$, histoire de faire converger la série absolument, puis faire tendre s vers 0.

l'infini pour être modulaire[†]. Je vais y remédier très bientôt.

Une autre façon de produire des 1-formes invariantes est en utilisant les fonctions θ : j'appelle fonction θ de dimension l la fonction

$$\theta(\tau, l) = \sum_{\vec{n} \in \mathbb{Z}^l} e^{\pi i ||\vec{n}||\tau}.$$

Grâce aux propriétés mirifiques de l'exponentielle, notamment vis-à-vis sa transformée de Fourier, la formule de Poisson permet de prouver que $\theta(i/t, l) = t^{l/2}\theta(it, l)$ pour $t > 0$, et donc $\theta(-1/\tau, l) = (-i\tau)^{l/2}\theta(\tau, l)$ pour tout $\tau \in \mathcal{H}$ par prolongement analytique. Ceci ressemble fortement à la propriété d'invariance des formes modulaires. En outre, la fonction $\theta(\tau,1)^4$ vérifie la relation

$$\theta\left(\frac{\tau}{4\tau+1},1\right)^4 = \theta\left(-\frac{1}{4(-1/4\tau-1)},1\right)^4,$$

puis

$$\theta\left(\frac{\tau}{4\tau+1},1\right)^4 = -4\left(\frac{1}{4\tau}+1\right)\theta\left(-\frac{1}{4\tau}-1,1\right)^4 = 4\left(\frac{1}{4\tau}+1\right)(-2i\tau)\theta\left(\tau,1\right)^4.$$

Comme il est clair, et implicitement utilisé dans le calcul ci-dessus, que $\theta(\cdot,1)^4$ est également 1-périodique, on en déduit que cette fonction vérifie la propriété d'invariance des formes modulaires pour le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ engendré par $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ et $\begin{pmatrix}1 & 0\\ 4 & 1\end{pmatrix}$, c'est-à-dire $\Gamma_0(4)$. Elle est de plus holomorphe aux pointes, essentiellement parce qu'elle converge très vite. Malheureusement, elle ne s'annule pas aux pointes, elle y vaut 1.

Cependant, en combinant tout ce que j'ai raconté, on peut produire une forme modulaire pour $\Gamma_0(4)$: comme la fonction $z \mapsto 4E_2(4z) - E_2(z)$ vaut $\frac{-3}{24}$ aux pointes, la fonction $f : z \mapsto 4E_2(4z) - E_2(z) + \frac{3}{24}\theta(z,1)^4$ s'annule aux pointes, et vérifie la propriété de transformation, désirée. Ouf, on a fourni une forme modulaire pour $\Gamma_0(4)$! À ceci près que j'avais dit plus haut qu'il n'y avait pas de telle forme modulaire non nulle... Donc $f = 0$, et tous les coefficients de son développement de Fourier en l'infini sont nuls. On a donné les coefficients du développement de la série E_2 plus haut, et ceux de la fonction $\theta(\cdot,1)^4$ sont les $r_4(n)$, qui désignent le nombre de façons d'écrire n comme somme de quatre carrés d'entiers. Bref, on a démontré :

$$r_4(n) = 8 \sum_{d|n, 4\nmid d} d.$$

C'est le théorème de Jacobi. Plus généralement, le fait que les formes modulaires forment des espaces vectoriels de dimension finie, tout en ayant une infinité de coefficients de Fourier, fournit des contraintes fortes sur ces coefficients, et des relations inattendues.

†. En fait, selon la terminologie classique (et universellement acceptée en dehors de cet exposé), c'est bien une forme modulaire, et je suis désolé pour les habitués de la théorie qui risquent d'être perturbés par mon choix.

1.3 Les opérateurs de Hecke et formes primitives

Un problème est de trouver une base canonique pour l'espace des formes modulaires de niveau N. Comme les formes modulaires au sens de cet exposé n'ont pas vraiment une expression simple, au contraire des séries d'Eisenstein, on a besoin de méthodes plus sophistiquées.

L'espace vectoriel $S_2(N)$ peut être muni d'un produit scalaire, appelé produit scalaire de Petersson, défini comme suit : pour deux formes modulaires f et g,

$$\langle f, g\rangle = \frac{1}{V(X_0(N))}\int_{X_0(N)} f(\tau)\mathrm{d}\tau \wedge \overline{g(\tau)\mathrm{d}\tau} = \frac{1}{V(X_0(N))}\int_{X_0(N)} f(\tau)\overline{g(\tau)}\mathrm{d}x\mathrm{d}y,$$

où l'intégrale est prise sur un domaine fondamental de $X_0(N)$, et $V(X_0(N))$ désigne le volume de ce domaine fondamental. Cette intégrale ne dépend pas du domaine fondamental choisi et converge bien, comme on peut le pressentir en voyant le développement en ∞ des formes modulaires, car l'exponentielle décroît très vite au voisinage de ∞.

On peut montrer qu'il existe des opérateurs linéaires sur $S_2(N)$, que je ne décrirai pas précisément et qu'on appelle opérateurs de Hecke. Pour n entier naturel, on note T_n ces opérateurs. Tout ce qui est à savoir sur ces opérateurs est qu'ils commutent deux à deux, sont des endomorphismes normaux, simultanément diagonalisables dans une base de vecteurs propres, des relations de récurrence et de multiplicativité lient ces opérateurs entre eux, et enfin les coefficients de Fourier des images d'une forme modulaire par ces opérateurs sont effectivement calculables.

Rappelons que l'espace des formes anciennes de niveau N désigne l'espace vectoriel des formes modulaires issues d'un niveau inférieur à N. Son orthogonal pour le produit scalaire de Petersson, noté $S_2(N)^{\mathrm{new}}$, est appelé espace vectoriel des formes modulaires *nouvelles* de niveau N. Les sous-espaces vectoriels $S_2(N)^{\mathrm{old}}$ et $S_2(N)^{\mathrm{new}}$ sont stables sous l'action des opérateurs de Hecke pour tout n entier naturel, et on peut encore en déduire l'existence d'une base orthogonale de vecteurs propres pour les opérateurs de Hecke sur ces sous-espaces.

Définition 1.6 (Forme primitive) *On appelle forme primitive de niveau N une forme modulaire non nulle nouvelle de niveau N qui est forme propre pour tous les opérateurs de Hecke, et telle que $a_1(f) = 1$.*

Le résultat suivant est très important.

Théorème 1.7 *Si f est une forme primitive de niveau N, alors $T_n f = a_n(f)f$: autrement dit, les valeurs propres des T_n sont les coefficients de Fourier des formes propres. De plus, si une autre forme modulaire vérifie les mêmes propriétés que f et a les mêmes valeurs propres que f pour les T_n, alors ces deux formes modulaires diffèrent d'une constante multiplicative (cette propriété s'appelle la propriété* multiplicité Un*, puisque ça énonce que les sous-espaces propres des T_n sont tous de dimension un).*

Par exemple, si $\eta = q_{24}\prod_{n=1}^{\infty}(1-q^n)$, alors la fonction $\varphi(\tau) = \eta(\tau)^2\eta(11\tau)^2$ est une forme primitive. D'ailleurs, comme $S_2(11)$ est de dimension un d'après les formules de dimension données, c'est la seule forme primitive, et toutes les formes modulaires lui sont proportionnelles. Pour avoir une base de tout $S_2(N)$, il suffit maintenant de considérer l'ensemble des formes primitives de niveaux plus bas :

Théorème 1.8 *L'ensemble des $z \mapsto f(nz)$, où f est une forme primitive de niveau M et nM divise N, est une base de $S_2(N)$.*

Les conséquences de l'action des opérateurs de Hecke sont nombreuses et importantes pour les coefficients de Fourier d'une forme primitive de niveau N : ils vérifient une relation de récurrence proche de celles vérifiées par les opérateurs de Hecke, ce sont des entiers algébriques de degré borné par le genre de $X_0(N)$ (le corps de nombres engendré par ces coefficients est souvent noté K_f), en conjuguant ces coefficients par un automorphisme de Galois on obtient encore une forme primitive, *etc.* En particulier, si $X_0(N)$ est une courbe elliptique, alors les coefficients de l'unique forme primitive de niveau N sont des entiers.

La relation de récurrence vérifiée par les T_{p^r} en induit une autre pour les coefficients de Fourier d'une forme primitive de niveau N. Ceci se synthétise dans la proposition suivante.

Théorème 1.9 *Soit f une forme primitive de niveau N. Posons $L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$; c'est la fonction L de f. Alors, L admet le produit eulérien suivant :*

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

2 Courbes elliptiques et modularité

2.1 Prérequis sur les courbes elliptiques

Cette section sur les courbes elliptiques ne se veut pas exhaustif. Pour plus de détails, il faudrait voir un vrai cours dessus, ou mon mémoire de M1 pour un exposé naïf.

Définition 2.1 *Une courbe elliptique E sur $\mathbb{Q}$ est la donnée d'une équation $E : y^2 = x^3+ax+b$, avec a et b des rationnels, telle que $\Delta = -2^4(4a^3+27b^2) \neq 0$ (ceci signifie que le polynôme en x à droite de l'égalité est séparable), et d'un point O dit point à l'infini. Plus précisément, E désigne le lieu dans $\mathbb{P}^2$ de l'équation homogène $Y^2Z = X^3 + aXZ + bZ^3$ associée à l'équation affine ci-dessus, et $O = [0,1,0]$. Une telle équation est appelée équation de Weierstrass.*

Une définition équivalente est qu'une courbe elliptique est une courbe lisse et de genre 1.

Si K est une extension de $\mathbb{Q}$, alors $E(K)$ est l'ensemble des points (x,y) dans K^2 vérifiant l'équation de Weierstrass qui définit E. On peut définir une loi de groupe sur $E(K)$ par le procédé de cordes et tangentes. Si P et Q sont deux points de $E(K)$, les coordonnées de $P+Q$ sont des fractions rationnelles en celles de P et Q, et $P+Q+R = O$ si, et seulement ces trois points sont alignés. Les points vérifiant $[2]P = P+P = O$ sont exactement les points dont l'abscisse est racine du polynôme X^3+aX+b. Muni de cette loi de groupe, $E(K)$ est un groupe abélien de type fini dans le cas où K est un corps de nombres, c'est-à-dire isomorphe à $\mathbb{Z}^r \times G$, où G est un groupe fini : c'est le théorème de Mordell-Weil. Déterminer r, et plus généralement des générateurs d'une courbe elliptique, est un problème très délicat.

Théorème 2.2 *Soit E une courbe elliptique sur $\mathbb{Q}$. Il existe un réseau $\Lambda \subseteq \mathbb{C}$ unique à homothétie près, qu'on peut écrire $\mathbb{Z} + \tau\mathbb{Z}$, tel que $\mathbb{C}/\Lambda$ et $E(\mathbb{C})$ soient isomorphes (c'est même un isomorphisme de groupes de Lie complexes). On peut rendre cet isomorphisme explicite.*

On peut toujours écrire une courbe elliptique sur $\mathbb{Q}$ sous la forme

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

où cette fois tous les coefficients a_i sont entiers, quitte à faire un changement de coordonnées. Si une courbe elliptique a deux telles écritures, leurs discriminants (qui s'écrivent explicitement à l'aide des coordonnées a_i) sont proportionnels, reliés par une puissance douzième d'un entier. On appelle discriminant minimal de la courbe le plus petit choix possible de discriminant. Une fois une courbe elliptique sous cette forme, on peut la réduire modulo p (et plus généralement la considérer sur « le » corps fini $\mathbb{F}_q$), et observer si on obtient encore une courbe elliptique (c'est-à-dire si elle est encore lisse). Comme dans le cas des courbes sur $\mathbb{Q}$, le discriminant nous dit si la courbe reste elliptique après réduction : si $\Delta \equiv 0 \mod p$, alors ce n'est plus une courbe elliptique, et on parle de mauvaise réduction. Sinon, on parle de bonne réduction ; on constate que les nombres premiers de mauvaise réduction sont *exactement* les nombres premiers qui divisent le discriminant.

Dans le cas de mauvaise réduction en p, on peut montrer qu'il n'y a qu'un point singulier, et soit c'est une pointe (un point de rebroussement) et on parle de réduction additive en p (la plus pénible dans bien des cas), soit c'est un nœud (il y a deux tangentes en ce point) et on parle de réduction multiplicative en p. Le type de réduction peut parfaitement se lire algébriquement sur l'équation ci-dessus qui définit la courbe elliptique (par exemple, si on écrit un modèle de Weierstrass minimal, sauf peut-être en 2 ou 3, sous la forme $y^2 = x^3 - 27c_4x - 54c_6$, alors la réduction est additive si p divise à la fois c_4 et Δ). Le discriminant ne contient pas, *a priori*, ces informations sur la réduction dans sa décomposition en facteurs premiers. C'est pourquoi on introduit la notion de conducteur N d'une courbe elliptique qui contient toute l'information. En gros, il est défini par $N = \prod_p p^{\alpha_p}$, où $\alpha_p = 0$ en cas de bonne réduction modulo p, $\alpha_p = 1$ en cas de mauvaise réduction multiplicative modulo p, et 2 si la réduction est additive modulo un nombre premier supérieur ou égal à 5 (les cas de réduction additive en 2 ou 3 sont plus compliqués).

Lorsque p ne divise pas le discriminant minimal, on note

$$a_p(E) = p + 1 - \mathrm{card}(E(\mathbb{F}_p)).$$

Si E n'a pas bonne réduction modulo p, on pose à la place $a_p(E) = 0$, 1 ou -1 selon les cas. Une fois toutes ces informations recueillies, on peut définir la fonction L d'une courbe elliptique de la façon suivante : on pose

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

On sait montrer que $|a_p(E)| \leq 2\sqrt{p}$ pour tout p, et ceci implique la convergence du produit pour $\Re(s) > 3/2$.

2.2 Théorème de Taylor-Wiles

L'objectif de cette section est d'éclaircir un minimum l'affirmation que

« toute courbe elliptique rationnelle est modulaire. »

Un lien entre les courbes elliptiques et les formes primitives existait déjà bien avant la conjecture de Taniyama-Shimura qui a débouché sur le théorème de Wiles. En effet, soit f une forme primitive de niveau N, dont les coefficients de Fourier sont des entiers. La forme différentielle $2i\pi c f(z)\mathrm{d}z$, pour c un entier, est holomorphe, donc l'intégrale

$$\tilde{\varphi}(\tau) = 2i\pi c \int_{\infty}^{\tau} f(z)\mathrm{d}z$$

est indépendante du chemin choisi, et définit une fonction $\tilde{\varphi} : \mathcal{H} \to \mathbb{C}$. De plus, si $\gamma \in \Gamma_0(N)$, on pose

$$\omega(\gamma) = \tilde{\varphi}(\gamma\tau) - \tilde{\varphi}(\tau),$$

et cette fonction ne dépend pas de τ. Elle définit ce qu'on appelle une période de f. On peut montrer que $\omega : \Gamma_0(N) \to \mathbb{C}$ est un homomorphisme de groupes, et son image est contenue dans un réseau Λ de $\mathbb{C}$ (c'est un résultat de Drinfeld, qu'il a démontré dans son adolescence). Ainsi, on a une application :

$$\varphi \ : \begin{cases} X_0(N) & \to & \mathbb{C}/\Lambda \\ \tau & \mapsto & c\sum_{n\geq 1} \frac{a(n)}{n} q^n \end{cases} .$$

Il existe un isomorphisme entre $\mathbb{C}/\Lambda$ et une courbe elliptique E_f, ce qui donne finalement, après composition, une flèche $X_0(N) \to E_f(\mathbb{C})$. On pouvait associer une courbe elliptique E_f à une forme primitive par d'autres moyens, qui permettent de montrer plus naturellement que $L(f,s) = L(E,s)$, mais la méthode fait appel à des outils de géométrie algébrique que je tais pour les besoins de l'exposé. Il était alors naturel, même si c'est plus facile de le dire *a fortiori*, de se demander si réciproquement, étant donnée une courbe elliptique E, je peux trouver une flèche $X_0(N) \to E(\mathbb{C})$, une forme primitive f qui lui est naturellement associée, *etc.* Autrement dit, Eichler et Shimura ont montré que l'application $f \mapsto E_f$, qui à une forme primitive à coefficients de Fourier entiers associe une classe d'isogénie de courbes elliptiques rationnelles, est bien définie (et injective, par ailleurs, mais ce n'est pas évident du tout), et on se demande à présent si l'application est surjective. C'est l'objet de la conjecture de Taniyama-Shimura, nettement plus délicate à montrer.

Il existe plusieurs versions équivalentes du théorème de Taylor-Wiles, ou théorème modulaire, ou théorème de modularité (ou théorème de Taniyama-Shimura-Weil-Wiles-Taylor, ou...). Je mets les deux versions les plus simples, dans un souci d'auto-contenance.

Théorème 2.3 (Modularité, version L) *Soit E une courbe elliptique sur $\mathbb{Q}$ de conducteur N. Il existe alors une forme primitive f de niveau N telle que $L(f,s) = L(E,s)$. En particulier, $a_p(f) = a_p(E)$ pour tout p.*

Ce résultat est spectaculaire parce que les $a_p(E)$ sont des données locales sur la courbe elliptique E. Rien ne permettait de présager qu'ils pourraient être issus,

en quelque sorte, d'un objet défini globalement, à savoir une forme modulaire. Une application simple de ce résultat est le prolongement méromorphe de la fonction L d'une courbe elliptique. On sait démontrer que la fonction L d'une forme primitive admet une équation fonctionnelle ; c'est même assez facile, à l'aide de la transformée de Mellin et des symétries des formes modulaires. Le fait que cette fonction L soit aussi celle d'une courbe elliptique implique que $L(E, s)$ vérifie la même équation fonctionnelle et le même prolongement. C'est important, parce qu'une conjecture centrale en théorie des nombres, la conjecture de Birch et Swinnerton-Dyer, suggère que le résidu en 1 de la fonction L d'une courbe elliptique contient des informations sophistiquées sur la structure de groupe de la courbe. En particulier, l'ordre d'annulation de la fonction L donnerait son rang. Mais avant d'avoir le théorème modulaire, on n'était même pas sûr que la fonction L de E soit définie autour de 1.

Théorème 2.4 (Modularité, version uniformisation) *Soit E une courbe elliptique sur $\mathbb{Q}$. Il existe alors un morphisme holomorphe surjectif $X_0(N) \to E(\mathbb{C})$, appelé paramétrisation modulaire de E, où N est le conducteur de E.*

Ainsi, la compréhension de $X_0(N)$ permet, en théorie, de comprendre toutes les courbes elliptiques. La forme primitive associée à la courbe elliptique est ici quelque peu masquée. Pour l'exhiber, soit on passe par le morphisme

$$\mathrm{Jac}(X_0(N)) \to E,$$

qui induit un morphisme surjectif sur une des sous-variétés irréductibles qui composent la jacobienne, dont on montre (grâce à un théorème d'Eichler et Shimura) qu'elle est naturellement associée à une forme primitive, soit on considère la tirée en arrière de la 1-forme différentielle invariante de E par ce morphisme holomorphe. Cette tirée en arrière est de la forme $2i\pi c_E f(z)\mathrm{d}z$, où f est une forme primitive, et c_E la constante de Manin, conjecturalement égale à ± 1 dans le cas où la courbe est forte (c'est-à-dire qu'on ne peut pas factoriser notre morphisme *via* une isogénie $E' \to E$ où E' est une autre courbe elliptique).

Pour montrer l'équivalence des deux versions, on aurait besoin de la version qui utilise les représentations galoisiennes. Je n'en parlerai pas. Essayons plutôt de voir un aperçu (très léger) de la surpuissance du théorème modulaire dans les prochaines sections.

3 Applications

3.1 Le Dernier Théorème de Fermat, et autres problèmes diophantiens

Ça va devenir vrai dans cette section dans quelques instants. On va commencer par illustrer le théorème de Taylor-Wiles avec son application la plus célèbre :

Théorème 3.1 (Le Dernier Théorème de Fermat) *Soit n un entier supérieur ou égal à trois. Si (a, b, c) est un triplet d'entiers vérifiant $a^n + b^n = c^n$, alors $abc = 0$.*

Il n'est pas difficile de voir qu'on peut se ramener à traiter le cas $n = 4$ et le cas où n est un nombre premier impair. Par des méthodes de théorie algébrique des nombres, on sait traiter les premiers cas, et on peut donc supposer que $n = \ell \geq 5$ est un nombre premier. On peut supposer qu'une solution hypothétique (a, b, c) est primitive, c'est-à-dire que a, b et c sont premiers entre eux. Remarquons que les symétries de l'équation permettent de supposer que $a \equiv -1 \mod 4$ et $b \equiv 0 \mod 2$.

L'idée qui a germé dans l'esprit de Hellegouarch puis de Frey ‡ est de considérer les courbes qui portent désormais leur nom : si (a, b, c) est un triplet d'entiers vérifiant $a + b + c = 0$, on considère la courbe elliptique $E_{a,b,c}$ d'équation affine $y^2 = x(x - a)(x + b)$. On vérifie que son discriminant *minimal* est $\frac{(abc)^2}{2^8}$. La courbe est alors elliptique si, et seulement si $abc \neq 0$. S'il existait une solution non triviale à l'équation de Fermat, c'est-à-dire ne vérifiant pas $abc = 0$, alors la courbe E_{a^ℓ,b^ℓ,c^ℓ} serait elliptique, et Serre fit remarquer dans une lettre envoyée à Hellegouarch que cette courbe serait bien trop bizarre pour être modulaire (dans le métier, on dit qu'elle est très peu ramifiée ; c'est une notion plus ou moins liée à la réduction de la courbe), ce qui contredirait la conjecture de Taniyama-Shimura. On va préciser tout ceci.

Tout d'abord, le conducteur de E_{a^ℓ,b^ℓ,c^ℓ} est $N = \mathrm{rad}(abc)$, où $\mathrm{rad}(n)$ est le produit des nombres premiers qui divisent n (on retient que 2 divise N). Le théorème modulaire assure l'existence d'une forme primitive de niveau N de même fonction L que E_{a^ℓ,b^ℓ,c^ℓ}. *A priori*, on n'est pas très avancés à présent, car on ne sait rien du radical de abc, donc des formes primitives d'un tel niveau. Heureusement, un théorème de Ribet permet de diminuer le niveau de la forme primitive associée : parmi les nombres premiers qui divisent N, certains ne « comptent pas vraiment » et on peut les « enlever » ; rigoureusement, ces nombres premiers p correspondent à des nombres premiers pour lesquels la représentation galoisienne induite par la ℓ-torsion de la courbe elliptique est non ramifiée modulo p (où ℓ est un nombre premier *fixé*), ou plus vulgairement : la ℓ-torsion de la courbe elliptique « se réduit bien » modulo p. Comme je n'ai pas parlé de représentation galoisienne jusqu'à présent, il ne serait pas correct de commencer maintenant, je vais donc reformuler ceci uniquement en fonction des coefficients de Fourier de la forme primitive associée.

Définition 3.2 *En gardant les mêmes notations, soit ℓ un nombre premier. On définit N_ℓ par la formule*

$$N_\ell = \frac{N}{\prod_p p},$$

*où le produit est indexé par les nombres premiers p tels que $v_p(N) = 1$ (*i.e. *$p|N$ mais $p^2 \nmid N$; géométriquement, ceci signifie que E a réduction multiplicative) et $\ell | v_q(\Delta_{min})$.*

On a le choix du nombre premier ℓ. Souvent, ce sera un nombre premier dont dépend l'équation ; je donnerai la stratégie générale plus tard, là on s'occupe de Fermat. Alors, voici le résultat qui nous intéresse :

Théorème 3.3 (Théorème d'abaissement du niveau, Ribet) *Soit E une courbe elliptique sur $\mathbb{Q}$, et soit $\ell \geq 5$ un nombre premier. Supposons qu'il n'existe*

‡. Apparemment ? Hellegouarch lui-même ne sait pas si quelqu'un a eu cette idée avant lui.

*pas d'isogénie de degré ℓ de E dans une autre courbe elliptique (*i.e.*, en substance, un morphisme de groupes entre deux courbes elliptiques dont le noyau est isomorphe à $\mathbb{Z}/\ell\mathbb{Z}$) sur $\mathbb{Q}$. Il existe alors une forme primitive f de niveau N_ℓ dont E « provient » modulo ℓ (*i.e. $a_p(E) \equiv a_p(f) \mod \lambda$, *où λ est un idéal premier de K_f au dessus de ℓ) pour presque tout p.*

On a donc besoin de savoir déterminer quand il n'existe pas de ℓ-isogénie. Le théorème de Mazur qui suit aide beaucoup, mais il y en a d'autres :

Théorème 3.4 *Soit E une courbe elliptique sur $\mathbb{Q}$ de conducteur N. Alors E n'a pas d'isogénie de degré ℓ si au moins une des conditions suivantes est remplie :*

- *$\ell \geq 17$ et $j(E)$ n'est pas un demi-entier ;*
- *$\ell \geq 11$ et N est* quadratfrei *;*
- *$\ell \geq 5$, N est* quadratfrei*, et $E[2](\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ (c'est en particulier le cas pour la courbe de Fermat, car O, $(a^\ell,0)$, $(0,0)$ et $(b^\ell,0)$ sont de 2-torsion).*

Ceci étant dit, on peut démontrer le théorème de Fermat dans la marge, je vous laisse admirer le travail.

Soit (a,b,c) une solution non triviale. La courbe E_{a^ℓ,b^ℓ,c^ℓ} est alors elliptique, donc modulaire de niveau le radical de abc. Le théorème de Ribet permet d'abaisser le niveau en divisant par les nombres premiers impairs divisant le conducteur. Ainsi, cette courbe provient d'une forme primitive de $S_2(\Gamma_0(2)) = \{0\}$: contradiction. □

Voici la stratégie générale pour attaquer une équation diophantienne avec la méthode utilisée pour le Dernier Théorème de Fermat :

- les coefficients de E dépendent de l'équation diophantienne ;
- le discriminant minimal Δ de E peut être écrit sous la forme $\Delta = C \cdot D^\ell$, où D dépend de la solution de l'équation diophantienne, C ne dépend que de l'équation en elle-même mais pas de la solution, et ℓ est un nombre premier inconnu apparaissant dans l'équation diophantienne ;
- si p divise D, alors E a réduction multiplicative en p (ce qui se traduit par le fait que $v_p(N) = 1$, où N est le conducteur de E).

Alors, le conducteur sera divisible par les nombres premiers divisant C et D, mais la condition ci-dessus assure que les nombres premiers divisant D peuvent être enlevées quand on abaisse jusqu'au niveau N_ℓ. En bref, N_ℓ sera divisible uniquement par des nombres premiers divisant C, qui ne dépendent que de l'équation. Sans connaître les solutions de l'équation diophantienne, on pourra alors en déduire un nombre fini de possibilités pour N_ℓ, et la condition de congruence sur les formes primitives donnée dans le théorème de Ribet affine encore les possibilités. À partir de là, on travaille un peu plus. En fait, le Dernier Théorème de Fermat est une application particulièrement simple, façon de parler, du théorème modulaire, puisqu'aucune forme primitive ne peut être associée à une solution hypothétique, et il n'y a donc pas de solution. Je vais esquisser un autre exemple où une forme primitive existe, ce qui nécessitera un peu de travail.

Considérons l'équation diophantienne

$$a^2 + 7 = b^p,$$

où a et b sont des entiers, b étant pair, et p un nombre premier supérieur ou égal à 11. On peut supposer, sans perte de généralité, que $a \equiv 1 \mod 4$. On associe à cette équation la courbe de Frey

$$E_a : y^2 = x^3 + ax^2 + \frac{a^2+7}{4}x,$$

dont le discriminant minimal est

$$\Delta = \frac{-7b^{2p}}{2^{12}},$$

et le conducteur

$$N_a = 14 \prod_{q|b, q\neq 2,7} q.$$

Le théorème de Ribet nous dit alors que E provient modulo p d'une forme primitive de niveau 14. Heureusement, il n'y a qu'une seule telle forme f, à coefficients entiers (ce qui n'est pas forcément le cas quand une forme primitive est associée à E_a modulo p !), et qui correspond à la courbe elliptique

$$E_f : y^2 + xy + y = x^3 + 4x - 6,$$

de conducteur 14. D'après le sens que j'ai donné plus haut à cette relation entre E_a et f, on a, pour l un nombre premier différent de 2 et 7 :

$$\text{si } l \nmid b, \text{ alors } a_l(E_a) \equiv a_l(E_f) \mod p, \text{ et}$$

$$\text{si } l|b, \text{ alors } a_l(E_f) \equiv 0, 2l+2 \mod p.$$

En reformulant ceci, on a le lemme suivant :

Lemme 3.5 *Soit $p \geq 11$ un nombre premier, et soit $l \neq 2, 7$ un nombre premier vérifiant $a_l(E_f) \not\equiv 0, 2l+2 \mod p$ et $a_l(E_f) \not\equiv a_l(E_a) \mod p$ pour tout $a \in \mathbb{F}_l$ satisfaisant $a^2 + 7 \in \mathbb{F}_l^{*p}$. Alors, il n'y a pas de solution à l'équation $a^2 + 7 = b^p$ pour ce choix de p.*

Il ne reste alors plus qu'à choisir des nombres premiers l jusqu'à ce que ça marche, ce qui est un peu plus facile puisque ça revient à compter des points sur des corps finis, et c'est purement algorithmique. Ceci a permis de prouver que les seules solutions sont pour $p = 3, 5$ et 7 (si on autorise les puissances non premières, on a aussi $p = 4$ et 15. Plus précisément, les triplets (a, b, p) solutions sont $(\pm 1, 2, 3)$, $(\pm 5, 2, 5)$, $(\pm 181, 2, 15)$, $(\pm 181, 32, 3)$, $(\pm 181, 8, 5)$, $(\pm 3, \pm 2, 4)$ et $(\pm 11, 2, 7)$.

3.2 Lien avec la conjecture *abc*

Je présente un autre exemple d'application du théorème de Wiles à un problème d'arithmétique actuel :

Conjecture 1 (Conjecture *abc*) *Pour tout $\varepsilon > 0$, il existe $C > 0$ tel que si a, b, c sont des entiers premiers entre eux vérifiant $a + b + c = 0$, alors on a :*

$$\max(|a|, |b|, |c|) \leq C \cdot \mathrm{rad}(abc)^{1+\varepsilon}.$$

Parmi les résultats qu'impliquerait la justesse de cette conjecture, on a presque trivialement le théorème de Faltings pour les courbes de Fermat d'équation homogène : $uX^m + vY^m + wZ^m = 0$, et bien plus fort encore. Le texte qui suit est tiré partiellement de mon mémoire ; vous pourrez y trouver les détails.

On reconsidère une courbe de Frey : si $a+b+c=0$, je considère $E_{a,b,c}$. Son discriminant minimal est $\Delta = \frac{(abc)^2}{2^8}$: La courbe $E_{a,b,c}$ est donc elliptique si, et seulement si $abc \neq 0$, ce qu'on suppose être le cas. Cette courbe est alors modulaire, paramétrée par $\phi : X_0(N) \to E_{a,b,c}$. Soit f la forme primitive associée à ϕ *via* $\phi^*(\mathrm{d}z) = 2\pi i c f(z)\mathrm{d}z$. On peut relier le degré de ϕ à f grâce au produit scalaire de Petersson :

$$4\pi^2||f||^2 = 2\pi^2 i \int_{X_0(N)} f(\tau)\mathrm{d}\tau \wedge \overline{f(\tau)\mathrm{d}\tau} = \frac{i}{2c^2}\int_{X_0(N)} \phi^*(\mathrm{d}z)\wedge\overline{\phi^*(\mathrm{d}z)},$$

d'où :

$$4\pi^2||f||^2 = \frac{i}{2c^2}(\deg(\phi))\int_{E_f}\mathrm{d}z\wedge\overline{\mathrm{d}z} = \frac{1}{c^2}(\deg(\phi))\int_{E_f}\mathrm{d}x\mathrm{d}y = \frac{1}{c^2}(\deg(\phi))\mu(E_f),$$

où $\mu(E_f)$ désigne le volume de E_f. Alors,

$$\ln(\deg(\phi)) = \ln(4\pi^2c^2) + 2\ln(||f||) - \ln(\mu(E_f)).$$

La quantité $\ln(\mu(E_f))$ est particulièrement intéressante. En effet,

$$\mu(E_f) = \int_{E_f}\mathrm{d}x\mathrm{d}y = \frac{2}{i}\int_{E_f}\mathrm{d}z\wedge\overline{\mathrm{d}z} = 2\pi e^{-2h(E_f)},$$

où les habitués des courbes elliptiques reconnaitront en $h(E_f)$ la hauteur de Faltings de E_f. Pour me simplifier la vie, je note $E = E_f$ dans la suite des calculs. Bref,

$$\ln(\deg(\phi)) = 2\ln(2\pi|c|) + 2\ln(||f||) + 2h(E), \tag{1}$$

et une inégalité sur $\max(|a|,|b|,|c|)$ apparaîtra après estimation de chaque terme du membre de droite. Dans les estimations suivantes, toutes les constantes c_i qui apparaîtront, ainsi que les constantes implicites dans les notations de Landau, sont indépendantes de N et de a, b, c, mais éventuellement de ε.

On sait montrer que $\ln(2\pi|c|) = O(1)$. Pour le terme $2\ln(||f||)$, j'utilise un résultat classique qui lie $||f||$ à la fonction $L(\mathrm{Sym}^2(f),\cdot)$ à l'aide de la méthode de Rankin-Selberg :

$$L(\mathrm{Sym}^2(f),2) = 288\prod_{p^2|N}\left(1-\frac{1}{p^2}\right)\frac{||f||^2}{N}. \tag{2}$$

Je rappelle que si $f = \sum_{n\geq 1} a_n q^n$ est une forme primitive de niveau N, alors

$$L(\mathrm{Sym}^2(f),s) = \zeta^{(N)}(s)\sum_{n=1}^{\infty}\frac{a_{n^2}}{n^s},$$

où $\zeta^{(N)}$ est la fonction ζ de Riemann dont il manque les facteurs eulériens correspondant aux facteurs premiers de N. Selon les auteurs, c'est $\zeta^{(N)}(2s)$ qui apparaît, et cela change l'axe de symétrie de l'équation fonctionnelle vérifiée par $L(\mathrm{Sym}^2(f),\cdot)$.

De ceci, après calculs, on tire l'inégalité :

$$||f||^2 \leq C \cdot N \cdot L(\mathrm{Sym}^2(f),2), \tag{3}$$

où $C > 0$ est indépendante de N.

Grâce au théorème de Phragmén-Lindelhöf, version Rademacher, on sait estimer la taille de notre fonction L. On a :

$$L(\mathrm{Sym}^2(f),2) = O((\ln(N)^3)).$$

Ainsi, $||f||^2 \leq c_2 N(\ln(N))^3$, où c_2 est une certaine constante positive. Il reste à évaluer $h(E)$. Une approche va me permettre de faire le lien entre la conjecture *abc* et le degré de ϕ, une autre va me permettre de borner ce fameux degré.

Je ne définirai pas la hauteur de Faltings précisément ici. Ce qui importe est qu'ici, on a

$$h(E) = \frac{1}{12}\left(\ln(|\Delta|) - \ln(|\Delta(\tau_\infty)|(\Im(\tau_\infty))^6)\right),$$

où $\tau_\infty \in \mathcal{H}$ est tel que $E(\mathbb{C}) = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau_\infty)$.

Grâce à des estimations traditionnelles sur Δ et le j-invariant modulaire, on finit par obtenir une première inégalité importante :

$$\ln(\max(|a|,|b|,|c|)) + O(\ln(\ln(\max(|a|,|b|,|c|)))) = \ln(\deg(\phi)) - \ln(||f||^2) + O(1).$$

Il ne reste plus qu'à exploiter l'égalité (1). Comme on sait montrer que $\ln(||f||^2) \geq (1-\varepsilon)\ln(N)$, on a, pour c_1 une certaine quantité positive :

$$\begin{aligned}\ln(\max(|a|,|b|,|c|) + O(\ln(\ln(\max(|a|,|b|,|c|))) &\leq \ln(\deg(\phi)) - \ln(||f||^2) + c_1 \\ &\leq \ln(\deg(\phi)) + (\varepsilon - 1)\ln(N) + c_1.\end{aligned}$$

Si on suppose $\deg(\phi) \leq N^{2+\varepsilon}$ (conjecture de Szpiro), on obtient alors, pour un certain $c_2 > 0$,

$$\max(|a|,|b|,|c|) \leq c_2 N^{1+\varepsilon},$$

Comme $N = \mathrm{rad}(abc)$, on reconnait là la conjecture *abc*. Réciproquement, la justesse de la conjecture *abc* entraine la justesse de la conjecture de Szpiro, en vertu de

$$\ln(\max(|a|,|b|,|c|) + O(\ln(\ln(\max(|a|,|b|,|c|)))) \geq \ln(\deg(\phi)) - \ln(N) - \ln(\ln(N)) + O(1).$$

4 Bibliographie

– Pour comprendre la paramétrisation modulaire, *A first course in modular forms* de Diamond et Shurman est un bon ouvrage qui se suffit presque à lui-même. Dans ce livre sont démontrées presque toutes les équivalences entre les différentes formulations du théorème modulaire. La géométrie des courbes modulaires, les calculs de dimension, et l'action des opérateurs de Hecke est détaillée. Les auteurs traitent du cas général de courbes modulaires.

– Si on veut la preuve qu'il n'existe pas de forme modulaire non nulle de niveau 1, il faut se tourner vers le *Cours d'arithmétique* de Serre. À noter qu'il traite uniquement des formes modulaires de niveau 1, mais de tout poids, chose dont je n'ai pas parlé ici.
– Concernant les courbes elliptiques, on peut soit se rediriger vers mon mémoire de M1 (disponible sur mon site Internet), soit lire le cours élémentaire de Hindry sur les courbes elliptiques, dans son livre *Arithmétique*. Il y démontre le théorème de Mordell-Weil très simplement, sans cohomologie galoisienne et tout ce qui va avec ; si on veut de la cohomologie, il faut plutôt se tourner vers *The arithmetic of elliptic curves*, de Silverman, qui parle un peu plus des propriétés profondes des courbes elliptiques, explique le lien entre ramification et réduction, et prouve d'ailleurs tous les résultats que j'ai évoqués sur la réduction.
– Au sujet de la construction de la paramétrisation modulaire de E_f, en partant d'une forme primitive f, je me suis documenté avec la thèse de Delaunay, *Formes modulaires et invariants de courbes elliptiques définies sur* $\mathbb{Q}$.
– Pour la résolution de problèmes diophantiens à l'aide de la paramétrisation modulaire, un bon point de départ est l'article *Diophantine equations after Fermat's Last Theorem* de Siksek, puis le livre de Cohen intitulé *Number theory* pour des exemples beaucoup plus musclés. Cependant, pour tout ce qui tourne autour de l'abaissement du niveau, rien ne me semble mieux que l'article *From the Taniyama-Shimura conjecture to Fermat's Last Theorem* de Ribet lui-même.
– Concernant la conjecture *abc* et le lien avec le degré de Szpiro, mon mémoire de M2 résume un peu la situation, le livre de Hindry cité ci-dessus aussi. Je donne plus de références dans ce même mémoire.