La méthode des graphes. Exemples et applications.

J.-F. Mestre.
Ed.

February 18, 2004

1 Introduction

Soit $S_k(N, \varepsilon)$ l'espace des formes paraboliques de poids k, de niveau N et de caractère ε, où k et N sont des entiers ≥ 1, et ε un caractère de Dirichlet mod N. Il existe plusieurs manières d'en construire une base. On peut par exemple utiliser la formule des traces de Selberg: notons $\mathrm{Tr}(n)$ la trace de T_n, le n^{ienne} opérateur de Hecke. La fonction

$$f = \sum_{n=1}^{\infty} \mathrm{Tr}(n) q^n$$

appartient alors à $S_k(N, \varepsilon)$. L'ensemble des $f_i = T_i f$ engendre cet espace et cela permet théoriquement d'en obtenir une base. Par exemple, si N est premier, si $\varepsilon = 1$, et si $k = 2$, l'ensemble des f_i, $1 \leq i \leq g$, où g est le genre de $X_0(N)$, est une base de $S_2(N, 1)$.

Mais même dans ce cas, qui est le plus favorable, les calculs deviennent rapidement insurmontables: sur un ordinateur de taille moyenne, on ne peut guère espérer traiter des niveaux N plus gros que 5000 (toujours avec N premier, poids 2 et caractère trivial): en effet, le calcul de $\mathrm{Tr}(n)$ nécessite la connaissance de nombreux nombres de classes de corps quadratiques imaginaires - dont le discriminant est de l'ordre de grandeur de n – et, pour avoir la base $f_1, f_2, \ldots, f_g$, il faut calculer $\mathrm{Tr}(n)$ pour $n \leq g^2$.

Nous décrivons dans le paragraphe suivant une méthode, la "méthode des graphes", reposant sur des résultats de Deuring et Eichler, et développeée par J. Oesterlé et moi-même, qui permet d'obtenir plus rapidement (au moins dans le cas N premier) une base de $S_2(N, 1)$.

Dans le second paragraphe, nous indiquons comment cette méthode a permis de montrer que certaines courbes elliptiques définies sur $\mathbf{Q}$ sont des courbes de Weil (ce qui, en l'occurrence, par l'obtention d'une courbe de Weil adéquate, donne tous

les corps quadratiques imaginaires de nombres de classes 3, à l'aide d'un résultat de Goldfeld et des travaux récents de Gross et Zagier).

Le troisième paragraphe est consacré à la vérification d'une conjecture de Serre dans certains cas particuliers, vérification qui a été possible grâce à la méthode exposée dans le premier paragraphe. On sait que cette conjecture, si elle est vraie, a de nombreuses conséquences (la conjecture de Shimura-Taniyama-Weil, ainsi que le théorème de Fermat, en découleraient en particulier).

2 La méthode des graphes

2.1 Définitions et notations

Dans ce qui suit, p désigne un nombre premier, N_1 un entier positif premier à p. On pose $N = pN_1$.

Soit

$$M_N = \oplus_S \mathbf{Z}[S]$$

où S décrit l'ensemble des points supersinguliers de $X_0(N_1)$ en caractéristique p, c'est-à-dire l'ensemble des couples (E, C) formés d'une courbe elliptique définie sur $\overline{\mathbb{F}}_p$ munie d'un groupe cyclique C d'ordre N_1. Deux tels couples sont identifiés s'ils sont, dans un sens évident, $\overline{\mathbb{F}}_p$-isomorphes.

Posons

$$\alpha_S = \frac{|\operatorname{Aut}(S)|}{2},$$

où $\operatorname{Aut}(S)$ désigne le groupe des $\overline{\mathbb{F}}_p$-automorphismes de S. On a toujours $\alpha_S \leq 12$, et même, si p ne divise pas 6, $\alpha_S \leq 3$.

On peut alors définir un produit scalaire sur M_N par $\langle S, S\rangle = \alpha_S$ et $\langle S, S'\rangle = 0$ si $S \neq S'$. Soit $\operatorname{Eis} = \sum \alpha_S^{-1}[S]$, et soit

$$M_N^0 = \Big\{ \sum x_S[S] : \sum x_S = 0 \Big\}$$

l'orthogonal de Eis.

Pour tout entier $n \geq 1$ premier à p, on définit un opérateur T_n sur M par:

$$T_n(E, C) = \sum_{C_n} (E/C_n, (C + C_n)/C_n),$$

où C_n parcourt les sous-groupe d'ordre n de E dels que $C \cap C_n = \{0\}$.

Pour tout entier q divisant N_1 et premier à $q' = N_1/q$, on définit de même des involutions W_q par:

$$W_q(E, C) = (E/q'C, (E_q + C)/q'C),$$

où E_q est le groupe des points d'ordre q de E.

Enfin, on définit une involution W_p par $W_p = -\mathrm{Frob}_p$, où Frob_p est l'endomorphisme de M_N qui transforme (E, C) en (E^p, C^p). (Le fait qu'il s'agit d'une involution reflète le fait que les points supersinguliers sont définis sur $\mathbb{F}_{p^2}$.)

Ces divers opérateurs possédent les propriétés suivantes: l'ensemble des W_q et des T_n, n premier à N, engendre un semi-groupe commutatif d'opérateurs hermitiens par rapport au produit scalaire $\langle \cdot, \cdot \rangle$. Les T_n commutent entre eux pour tout n premier à p. Si $q = q_1 q_2$, q_1 et q_2 premiers entre eux, et si $n = n_1 n_2$, n_1 et n_2 premiers entre eux et premiers à p, on a $W_q = W_{q_1} W_{q_2}$ et $T_n = T_{n_1} T_{n_2}$.

Par ailleurs, pour tout d divisant N_1, on a un morphisme ϕ_d de M_N vers $M_{N/d}$ qui transforme (E, C) en (E, dC). Ce morphisme commute aux T_n, n premier à N, et aux W_q, pour q divisant N/d. Pour d divisant N_1 et premier à N_1/d, on a la formule

$$T_d \phi_d = \phi_d (T_d + W_d)$$

2.2 Un isomorphisme avec $S_2(N)$

On considère ici l'espace $S_2(N)$ des formes paraboliques de poids 2 sur le groupe $\Gamma_0(N)$, muni de sa structure naturelle de $\mathbf{T}$-module, où $\mathbf{T}$ est l'algèbre de Hecke [1].

Théorème 2.1. Il existe un isomorphisme, compatible avec l'action des opérateurs de Hecke, entre l'espace vectoriel $M_N^0 \otimes \mathbf{C}$ et le sous-espace de $S_2(N)$ engendré par les newforms de niveau N et les oldforms provenant des formes paraboliques de poids 2 et de niveau pd, d divisant N_1.

Remark 2.2. Supposons N (ou N_1, cela revient au même) sans facteur carré. On peut alors déterminer facilement le sous-espace de M_N^0 correspondant aux newforms de $S_2(N)$: il s'agit du sous-espace formé des x tels que, pour tout d divisant N_1, on ait

$$\phi_d(x) = \phi_d(W_d(x)) = 0.$$

En particulier, si $N = pq$, q premier, c'est le sous-espace de M_{pq} intersection du noyau de ϕ_q et de $\phi_q W_q$.

2.3 Rapport avec les algèbres de quaternions

Les matrices des opérateurs T_n agissant sur M_N ne sont rien d'autre que les matrices de Brandt classiques [15], construites d'ordinaire à partir d'algèbres de quaternions.

En effet, soit $B_{p,\infty}$ l'algèbre de quaternions sur $\mathbf{Q}$ ramifiée en p et l'infini, soit $\mathcal{O}$ un ordre d'Eichler de niveau N_1 (défini par Eichler [6] dans le cas où N_1 est sans facteur carré, et défini dans le cas géneral par Pizer [14]), et soient $I_1, I_2, \ldots, I_h$ des représentants des classes d'idéaux à gauche de $\mathcal{O}$.

Soient $\mathcal{O}_i$ les ordres à droite (i.e., normalisateurs à droite) des idéaux I_i, et e_i le nombre des unités de $\mathcal{O}_i$. La matrice de Brandt $B(n) = (b_{i,j}^{(n)})$ a lors comme terme général

$$b_{i,j}^{(n)} = e_j^{-1} \cdot |\{\alpha : \alpha \in I_j^{-1} I_i,\, \mathrm{Nor}(\alpha)\,\mathrm{Nor}(I_j)/\,\mathrm{Nor}(I_i) = n\}|,$$

où Nor est la norme sur $B_{p,\infty}$ (la norme d'un idéal étant le pgcd des normes de ses éléments non nuls).

Dans le langage des courbes supersingulières en caractéristique p, on peut donner de ces matrices, où plus exactement de leurs transposées l'interprétation suivante:

Soit S un point supersingulier comme en I.1, c'est-à-dire une courbe elliptique supersingulière E définie sur $\overline{\mathbb{F}}_p$ munie d'un groupe C cyclique d'ordre N_1. L'anneau des endomorphismes $\mathcal{O}_1$ de S est un ordre d'Eichler de niveau N_1. A tout autre point supersingulier $S' = (E', C')$, associons l'ensemble $I_{S,S'}$ des homomorphismes de S vers S', i.e. l'ensemble des homomorphismes α de E sur E' qui envoient C sur C'. C'est de manière évidente un idéal à droite sur $\mathcal{O}_1$, et l'idéal inverse n'est autre que $I_{S',S}$. On peut alors montrer que tout idéal à droite de $\mathcal{O}_1$ est obtenu de cette manière, et que tout ordre d'Eichler de niveau N_1 est anneau d'endomorphismes d'un point supersingulier S. Il est alors clair que le term général $b_{i,j}^{(n)}$ de la n^{ieme} matrice de Brandt est le nombre d'isogénies de S_i vers S_j (les points supersinguliers étant convenablement indexés), deux telles isogénies étant identifiées si elles diffèrent par un automorphisme de S_j. On retrouve donc la matrice de l'opérateur T_n agissant sur le module M_N.

D'autre part, si à tout couple de points supersinguliers (S, S') on associe la fonction

$$\theta_{S,S'}(q) = \sum_{\alpha} q^{\deg \alpha}$$

où α parcourt les morphsimes de S vers S', on retrouve les fonctions θ classiquement associées aux idéaux d'ordres de quaternions, ou, si l'on préfère, aux formes quadratiques entières définies positives à 4 variables.

Il est alors facile de montrer que, si $\sum x_S[S]$ est un élément de $M_N \otimes \mathbf{C}$ vecteur propre de tous les opérateurs de Hecke, et si $f(q)$ est la forme modulaire correspondante, on a, pour tout S':

$$x_{S'} f(q) = \sum_{S} x_S \theta_{S,S'}$$

ce qui permet en théorie de trouver à partir des x_S les coefficients a_n de f. En pratique, malheureusement, le calcul d'un a_n demande la connaissance de toutes les isogénies de degré n arrivant vers S', et il ne semble pas y avoir d'algorithme simple pour cela.

Néanmoins, dans certains cas, il existe une autre méthode pour calculer les coefficients de f qui ce prête plus facilement au calcul:

supposons donc ici N premier (donc égal à p) ou N de la forme pq, où q est premier et $X_0(q)$ de genre 0 (donc $q = 2, 3, 5, 7$ ou 13).

Dans l'appendice, nous donnons dans chacun de ces cas une équation de $X_0(q)$ de la forme $xy = p^k$, ainsi que l'action de opérateurs de Hecke T_2 et T_3 sur $X_0(q)$, qui est donnée par une équation étonnament simple comparée à celle des polynômes modulaires $\Phi_2(j, j')$ et $\Phi_3(j, j')$ (qui donnent l'action de T_2 et T_3 sur $X_0(1)$, paramétré par l'invariant modulaire j, cf. le paragraphe 2.4).

Posons $u = x$ si $N = pq$ et $u = j$ si $N = p$. Le développement de Fourier de u au voisinage de l'infini est alors $1/q + \cdots$. Soit $f(q) = \sum a_n q^n$ une newform normalisée de niveau N et poids 2 correspondant à un vecteur $\sum x_S[S]$ de $M_N^0 \otimes K$, où K est l'extension de $\mathbf{Q}$ engendrée par les a_n. Il existe alors un idéal premier $\wp$ de K au-dessus de p tel qu'on a:

$$\Big(\sum x_S u(S)\Big) f(q)\frac{dq}{q} \equiv \sum x_S \frac{du}{u - u(S)} \pmod{\wp}. \tag{1}$$

(Il s'agit d'une congruence entre séries de Laurent en q).

Supposons par exemple que f corresponde à une courbe de Weil de conducteur N, donc que les a_n soient dans $\mathbf{Z}$. Les x_S sont alors dans $\mathbf{Z}$, et on peut montrer que $\sum x_S u(S) \neq 0$. On connait donc les a_n mod p pour tout n. Mais l'inégalité de Hasse $|a_l| < 2\sqrt{l}$ pour l premier montre qu'en fait on les connait exactement pour $n < p^2/16$.

2.4 Construction explicite du réseau M_N

Dans ce paragraphe, nous supposons pour simplifier que N est impair. Supposons connu un modèle explicite de la courbe $X_0(N_1)$, ainsi que l'action de l'opérateur de Hecke T_2 sur ce modèle (cf. Appendice).

Il nous fait d'abord trouver un point supersingulier. Notons qu'ils sont tous définis sur $\mathbb{F}_{p^2}$. Par exemple, supposons pour simplifier $N = p$. On cherche d'abord si p est inerte dans l'un des 9 corps quadratiques imaginaires de nombre de classes 1. Si oui, on peut prendre pour valeur de j initiale l'invariant modulaire de la courbe à multiplications complexes par l'anneau des entiers du corps correspondant. Si non, on peut connaître une liste des polynômes minimaux des invariants modulaires de courbes elliptiques à multiplications complexes par des corps quadratiques imaginaires de petit nombre de classes, et appliquer la même méthode. Il faut ici résoudre dans $\mathbb{F}_{p^2}$ une équation polynomiale, ce qui se fait en $\log p$ opérations – tout au moins probabilistiquement. Supposons enfin que toutes ces tentatives aient échouées; il reste la possibilité d'énumérer toutes les valeurs de $\mathbb{F}_p$ jusqu'à en trouver une supersingulière. On sait qu'il en existe toujours dans $\mathbb{F}_p$, mais malheureusement en assez petit nombre – de l'ordre de grandeur du nombre de classes de $\mathbf{Q}(\sqrt{-p})$, soit environ $\sqrt{p}$.

Supposons donc connu un point supersingulier S_1. La connaissance de l'action de T_2 sur le modèle donné de $X_0(N_1)$ nous permet d'obtenir les trois points super-

singuliers S_2, S_3 et S_4 (non forcément distincts) liés à S_1 par une 2-isogénie. Il s'agit de résoudre un polynôme de degré 3 sur $\mathbb{F}_{p^2}$, ce qui requiert l'extraction de racines cubiques et de racines carrées, opérations ne nécessitant que $O(\log p)$ opérations. Parfois, on peut d'ailleurs éviter cette résolution: supposons ici encore $N = p$, et que l'on ait, par exemple, $p \equiv 2 (\mathrm{mod}\ 3)$. Alors p est inert dans $\mathbf{Q}(\sqrt{-3})$, donc $j = 0$ est une valeur supersingulière, et on sait que les trois isogénies de degré 2 envoient la courbe d'invariant nul sur la courbe à multiplications complexes par $\mathbf{Z}[\sqrt{-3}]$, dont l'invariant est $j = 54000$.

De toutes manières, on a au plus une seule fois à résoudre une équation du troisième degré: en effet, une fois connu S_2, on cherche à partir de S_i, $i \geq 2$, les trois points supersinguliers qui lui sont reliés, mais *on en connaˆît déjà un*, et donc il ne reste à résoudre qu'une équation du second degré, donc à extraire une racien carrée sur $\mathbb{F}_{p^2}$, ce qui est rapide (les méthodes probabilistes demandant $O(\log p)$ opérations, par un algorithme très simple à mettre en oeuvre).

Pour montrer que l'on obtient ainsi, de proche en proche, tous les points supersinguliers de M_N, il suffit de montrer que le graphe de T_2 (et plus généralement de T_n) est connexe. Mais, comme me l'a fait remarquer J.-P. Serre, la valeur propre $a_2 = 3$ de T_2 sur M_N de multiplicité égale au nombre de composantes connexes du graphe de T_2. Or, dans M_N, l'espace M_N^0 correspondant aux formes paraboliques est de codimension 1, donc 3 est valeur propre simple de T_2 dans M_N, (car, pour une forme parabolique, on a $|a_2| < 2\sqrt{2}$) et le graphe de T_2 est donc connexe.

En conclusion, en un algorithme en $O(N \log N)$ opérations, on a donc trouvé tous les points supersinguliers et la matrice de Brandt B_2 associée. L'un des intérêts de cette matrice est d'être très creuse: dans chque ligne (et chaque colonne) il y a au plus trois termes non nuls, qui sont des entiers dont la somme est 3. Cela permet, étant donné une valeur propre, de trouver assez rapidement, si N n'est pas trop grand, les vecteurs propres correspondants.

2.5 Exemples

1. Prenons par exemple $N = p = 37$. Comme 37 est inerte dans le corps quadratique imaginaire $\mathbf{Q}(\sqrt{-2})$, on peut prendre comme premier sommet de notre graphe la courbe E_1 à multiplications complexes par $\mathbf{Z}[\sqrt{-2}]$, dont l'invariant modulaire est $j_1 = 8000 \equiv 8 \mathrm{mod}\ 37$; il nous faut à présent trouver les invariants des courbes 2-isogènes à celle-ci, c'est-à-dire résoudre l'équation $\Phi_2(x, 8000) \equiv 0 (\mathrm{mod}\ 37)$. Or $\sqrt{-2}$ est un endomorphisme de degré 2 de E_1, donc j_1 est racine (sur $\mathbf{Q}$) du polynôme $\Phi_2(x, 8000)$. En divisant ce polynôme par $x - 8000$, on trouve donc un polynôme du second degré dont les racines sont j_2 et j_3, les invariants des deux autres courbes E_2 et E_3 reliées à E_1 par une isogénie de degré 2. Soit $\omega \in \mathbb{F}_{p^2}$ tel que $\omega^2 = -2$. On trouve alors $j_2 = 3 + 14\omega$ et $j_3 = 3 - 14\omega$.

Une autre méthode pour trouver j_2 et j_3 consiste à remarquer que 37 est également inerte dans le corps $K = \mathbf{Q}(\sqrt{-15})$, dont le nombre de classes est 2. Le polynôme du second degré donnant les valeurs des invariants modulaires des 2 courbes à multiplications complexes par l'anneau des entiers de K est $x^2 + 191025x - 121287375$, dont les racines engendrent $\mathbf{Q}(\sqrt{5})$, donc modulo 37 sont conjuguées dans $\mathbb{F}_{37^2}$. On retrouve ainsi j_2 et j_3.

Pour N premier congru à 1 mod 12, le nombre de courbes supersingulières mod N est égal à $(N-1)/12$. Pour $N = 37$, on a donc trouvé les 3 courbes supersingulières voulues. Il reste à trouver l'action de T_2 sur E_2 (on en déduira par conjugaison l'action sur E_3). Il n'est pas possible qu'il y ait 2 isogénies de E_2 sur E_1, car alors il y aurait 5 isogénies de degré 2 partant de E_1. Il n'est pas non plus possible qu'il y ait une 2-isogénie de E_2 sur E_2.

En effet, s'il existe une 2-isogénie d'une courbe elliptique d'invariant j sur elle-même, cet invariant est racine de l'équation $\Phi_2(x, x) = 0$, équation de degré 4 qui s'écrit

$$(x - 1728)(x - 8000)(x + 3375)^2$$

.

(Pour le voir, on peut faire le calcul à partir l'équation de $\Phi_2(j, j')$ ci-dessus. On peut aussi chercher quelles sont les courbes à multiplications complexes qui admettent un endomorphisme de degrè 2, c'est-à-dire quels sont les corps quadratiques imaginaires qui contiennent un élément de norme 2. On trouve, à multiplication par une unité du corps près, les éléments $1 + i$, $\sqrt{-2}$, $\frac{1+\sqrt{-7}}{2}$ and $\frac{1-\sqrt{-7}}{2}$, qui sont les endomorphismes de degré 2 des courbes d'invariant $j = 1728, j = 8000$, et pour les deux derniers, $j = -3375$.)

Par suite, modulo p, le graphe de T_2 ne peut contenir de boucle d'une courbe supersingulière sur elle-même que si cette courbe est définie sur $\mathbb{F}_p$ (et, plus précisément, est l'une des 3 courbes décrites ci-dessus). Par conséquent, il y a 2 isogénies reliant E_2 à E_3, et le graphe de T_2 agissant sur M_{37} est complètement déterminé.

Pour calculer les vecteurs propres correspondants, on peut évidemment diagonaliser la matrice $(3, 3)$ de T_2, mais il y a encore plus simple:

l'involution $W_{37} = -\mathrm{Frob}_{37}$ découpe M_{37} de manière évidente en deux sous-espaces propres orthogonaux, l'un, engendré par $u_1 = [E_2] - [E_3]$, associé à la valeur propre 1, l'autre, associé à la valeur propre -1, engendré par $\mathrm{Eis} = [E_1] + [E_2] + [E_3]$ et par le produit vectoriel de u_1 et Eis, soit $u_2 = 2[E_1] - [E_2] - [E_3]$. On en déduit donc, sans recours à coefficients dans $\mathbf{Q}$, et donc le fait que $J_0(37)$, la jacobienne de $X_0(37)$, est isogène au produit de 2 courbes elliptiques (ce qui est bien connu, voir par exemple [9]). La formule (1) ci-dessue permet alors d'obtenir les 83 premiers termes de leur fonction L.

2. $p - 37, N = 2 \cdot 37$.

Pour étudier $X_0(74)$, on utilise le morphisme ϕ_2 de M_{74} vers M_{37} défini plus haut. Les fibres de chacun des trois points supersinguliers $[E_1], [E_2]$ et $[E_3]$ de $X_0(1)\text{mod } 37$ sont formées de trois points supersinguliers distincts de $X_0(2)\text{mod } 2$. D'une manière générale, notons que si $S_1, S_2, \ldots, S_k$ sont les points supersinguliers de $X_0(qM)\text{mod } p$ au-dessus d'un point supersingulier S de $X_0(M)\text{mod } p$ (p et q premiers et premiers à l'entier M), on a la formule

$$\frac{q+1}{\operatorname{Aut} S} = \sum_1^k \frac{1}{\operatorname{Aut} S_i}.$$

L'équation de $X_0(2)$ utilisée ici est celle décrite dans l'appendice:

$$uv = 2^{12},$$

l'involution W_2 échangeant u et v. Rappelons d'autre part que $W_{37} = -\operatorname{Frob}_{37}$, et que $j = (u+16)^3/u$ (où j est l'invariant de la courbe E, image du point (E, C) de $X_0(2)$ par le morphisme "oubli" de $X_0(2)$ sur $X_0(1)$). De l'équation $j = j_1 = 8$, on tire les valeurs des trois points supersinguliers au-dessus de E_1, de coordonnées $u_1 = (-1+\omega)/2, u_2 = (-1-\omega)/2 = W_2(u_1)$ et $u_3 = 27 = W_2(u_2)$. (Ici encore, il était possible de deviner la valeur de u_3, car il est clair d'après l'action de $T(2)$ sur $X_0(1)\text{mod } 37$ faite précédemment que l'un des points au-dessus de E_1 doit être invariant par W_2; or les 2 solutions de $u^2 = 2^{12}$ sont $u = u_1$ et $u = -u_1$. En les remplaçant dans l'équation donnat j, on voit qu'il s'agit de u_1. Pour trouver u_2 et u_3, il suffit de résoudre une équation du second degré.)

On calcule ensuite $u_4 = W_2(u_1) = 2^{12}/u_1 = -5 - 5\omega$, et on trouve que l'invariant $j(u_4)$ correspondant est $j_2 = 3 + 14\omega$. On résoud l'équation du second degré donnant les 2 autres points au-dessus de j_2, d'òu $u_5 = 15 + 17\omega$ et $u_6 = 16 - 12\omega$. Notons alors $u_7 = W_2(u_2) = \bar{u}_4, u_8 = W_2(u_5) = \bar{u}_5$ et $u_9 = W_2(u_6) = \bar{u}_6$ les abscisses des trois points supersinguliers au-dessus de E_3 ($x \longrightarrow \bar{x}$ étant l'automorphisme non trivial de $\mathbb{F}_{p^2}$.) Nous avons ainsi la liste de tous les points supersinguliers de $X_0(2)\text{mod } 37$.

Comme il a été dit plus haut, l'espace M_{74}^{new} correspondant aux newforms est l'intersection du noyau de ϕ_2 et de $\phi_2 W_2$. Si on note $[u_i]$, $i = 1, \ldots, 9$ les générateurs de M_{74} correspondant aux points supersinguliers d'abscisse u_i, un examen facile de l'action de W_{37} et W_2 montre que M_{74}^{new} est somme directe de deux sous-espaces de dimension 2, l'un G_1, engendré par $e_1 = [u_1] - [u_2] - [u_4] + [u_7] - [u_9]$ et $e_2 = [u_5] - [u_6] - [u_8] + [u_9]$, sur lequel $W_{37} = -W_2 = 1$, l'autre, G_2, engendré par $e_3 = [u_1] + [u_2] - 2[u_3] + [u_4] - [u_6] + [u_7] - [u_9]$, sur lequel $W_2 = -W_{37} = 1$.

En utilisant l'équation de T_3 agissant sur $X_0(2)$ (cf. l'appendice) on montre alors que la matrice de T_3 agissant sur G_1 (resp. G_2) dans la base (e_1, e_2) (resp. (e_3, e_4))) est $\begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$, de polynôme caractéristique $x^2 + x - 1$ (resp. $\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}$, de polynôme caractéristique $x^2 - 3x - 1$).

On en déduit que $J_0^{new}(74)$ est isogène à un produit de 2 variétés abéliennes simples, A_1 (resp. A_2), à multiplications réelles par l'anneau des entiers de $\mathbf{Q}(\sqrt{5})$, (resp. $\mathbf{Q}(\sqrt{13})$.)

Si $\lambda = \frac{-1+\sqrt{5}}{2}$ et $\mu = \frac{3+\sqrt{13}}{2}$, les vecteurs $v_1 = e_1 + (\lambda+1)e_2, v_2 = e_1 - \lambda e_2, v_3 = \mu e_3 + e_4$ et $v_4 = (3-\mu)e_3 + e_4$ correspondent aux 4 newforms f_1, f_2, f_3, f_4 de poids 2 et de niveau 74. En utilisant la congruence (1), on peut alors, comme ci-dessus, obtenir la valeur des 83 premiers coefficients de ces newforms. Par exemple, pour f_1, la liste des premières valeurs de a_l est

l	2	3	5	7	11	13
a_l	1	$\frac{-1+\sqrt{5}}{2}$	$\frac{1-3\sqrt{5}}{2}$	$-1+\sqrt{5}$	$\frac{-5-\sqrt{5}}{2}$	$\frac{1+3\sqrt{5}}{2}$

alors que pour f_3 on trouve

l	2	3	5	7	11	13
a_l	-1	$\frac{3+\sqrt{13}}{2}$	$-1-\sqrt{13}$	$\frac{1-\sqrt{13}}{2}$	$\frac{-1-\sqrt{13}}{2}$	$\frac{-1+\sqrt{13}}{2}$

3 Application à la recherche de courbes de Weil

Soit $f = \sum a_n q^n$ une newform de poids 2 et de niveau N, dont les coefficients a_n sont dans $\mathbf{Z}$. Elle correspond donc à une courbe de Weil forte $\mathcal{E}$ de conducteur N. Malheureusement, les coefficients a_n ne donnent que peu de renseignements sur $\mathcal{E}$, et ne permettent pas d'obtenir simplement une équation de $\mathcal{E}$. (Dans [10], on décrit une méthode due à Serre qui permet parfois d'en trouver une, mais cela n'a rien de systématique.) Nous donnons ci-après une méthode qui, au moins dans le cas où $N = p$ est premier, résoud ce problème.

On suppose donc désormais N premier. D'après les paragraphes précédents, à la newform f est associé un vecteur $v_f = \sum x_S[S]$, $x_S \in \mathbf{Z}$, vecteur propre des opérateurs de Hecke définis dans le paragraph 2.1. Le théorème 1 ne décrit pas l'isomorphisme (d'ailleurs non canonique) entre $S_2(N)$ et $M_N^0 \otimes \mathbf{C}$. Mais supposons connus les premiers termes a_n de f (a_2 suffit en général). La construction du paragraphe 2.4 hous donne simultanément les valeurs supersingulières mod N et le graphe de T_2 agissant sur M_N. Nous pouvons donc déterminer l'espace propre V_2 associé à la valeur propre a_2. S'il est de dimension 1, nous avons v_f, ou tout au moins l'espace qu'il engendre. Sinon, on applique T_3 sur V_2 (qui est expérimentalement de petite

dimension – pour les conducteurs < 80000, $\dim V_2$ ne dèpasse pas 6), jusqu'à trouver un espace de dimension 1, correspondant aux mêmes valeurs propres des opérateurs T_l que f. Choisissons dans cet espace un vecteur $r_f = \sum x_E[E]$, les étant dans $\mathbf{Z}$ et premiers entre eux; $w - f$ est donc déterminé au signe près.

Pour aller plus loin, il nous faut à présent une interprétation géométrique de ces x_E

Soient donc $\Delta = \pm N^\delta$ le discriminant d'un modèle minimal de Weierstrass de $\mathcal{E}$, $\phi : X_0(N) \longrightarrow \mathcal{E}$ un revêtement minimal de $\mathcal{E}$, et $n = \deg \phi$.

D'après Deligne-Rapoport [5], il existe un modèle $X_0(N)_{/\mathbf{Z}}$ de $X_0(N)$ défini sur $\mathbf{Z}$ dont la réduction modulo N est la réunion de deux droites projectives, l'une, C_∞, classifiant les courbes elliptiques en caractéristique N munies du schéma en groupes noyau du Frobenius (donc correspondant à des isogénies inséparables), l'autre, C_0, classifiant les courbes munies du "Verschiebung". Ces deux droites se coupent aux points supersinguliers. Quant à la courbe $\mathcal{E}$, la réduction modulo N de son modèle de Néron a une composante neutre $\mathcal{E}^0_{/\mathbb{F}_N}$ isomorphe sur $\mathbb{F}_{N^2}$ au groupe multiplicatif G_m. On peut montrer que le revêtement ϕ se prolonge à $X_0(N)_{/\mathbf{Z}} - \S$, où $\S$ est l'ensemble des points supersinguliers en caractéristique N, et définit par spécialisation et restriction une application régulière de $C_\infty - S$ sur $\mathcal{E}^0_{/\overline{\mathbb{F}}_N}$, d'où une fonction rationnelle ϕ sur C_∞, dont les pôles et les zéros appartiennent à $\mathcal{E}$. Le diviseur $\sum \lambda_E[E]$ o de ϕ, E parcourant les courbes supersingulières mod N, est donc un élément de M^0_N, défini au signe près (dépendant du choix de l'isomorphisme de $\mathcal{E}^0_{/\mathbb{F}_N}$ sur G_m.)

Proposition 3.1. *Avec les notations ci-dessus, le diviseur* $(\Phi) = \sum \lambda_E[E]$ *est égal á* $\pm r_f$.

Il n'est pas très difficile de voir que (Φ) est proportionnel à r_f. Par contre, le fait que les l_E sont premiers entre eux se déduit du beau résultat que Ribet vient d'obtenir[1], à savoir que, si l est un nombre premier distinct de 2 et 3, toute forme parabolique mod l de poids 2 et de niveau Np, où Np est sans facteur carré, dont la représentation mod l associée est irréductible et n ramifiée en p, provient d'une forme parabolique mod l de poids 2 et de niveau N (ce résultat avait été conjecturé par Serre, dans une lettre qu'il m'avait adressée en août 1985. On en déduit en particulier que la conjecture de Taniyama-Weil implique le grand théorème de Fermat).

Pour prouver la proposition précédente, on montre d'abord que δ est relié aux λ_E par la formule

$$\delta = \gcd(\lambda_E \omega_E - \lambda_F \omega_F)$$

où ω_E est le nombre d'automorphismes de E. Supposons qu'un nombre premier l divise le pgcd des λ_E. Il divise alors δ, et on en déduit que p n'est pas ramifié dans le corps des points d'ordre l de $\mathcal{E}$. Si l est premier à 6, le théorème de Ribet implique que la forme modulaire f associée à $\mathcal{E}$ est congrue mod l à une forme modulaire

[1] K.Ribet, *Lectures on Serre's conjectures*, MSRI, Fall 1986

de poids 2 et de niveau 1, qui ne peut être que la série d'Eiseinstein. La courbe $\mathcal{E}$ étant semi-stable, cela implique d'après [16], p.306, que $\mathcal{E}$ ou une courbe qui lui est $\mathbf{Q}$-isogène possède un point fini d'ordre l. Si $l = 2$ ou 3, on a le même résultat grâce à [4], Appendice. Or on connaˆît explicitement les courbes de conducteur premier possédant de la torsion [11], à savoir les courbes $11A$ et $11B$ de [19], qui ont un point d'ordre 5, les courbes $17A, 17B$ et $17C$ (un point d'ordre 4), $17D$ (d'ordre 2), $19A$ et $19B$ (d'ordre 3), $37B$ et $37C$ (d'ordre 3), et les courbes de Setzer-Neumann [18], qui est égal au nombre de points d'ordre fini rationnels sur $\mathbf{Q}$ des courbes considérées, et on vérifie que les λ_E sont premiers entre eux. En dehors de ces cas, les courbes $\mathcal{E}$ n'ont pas de torsion sur $\mathbf{Q}$, et sont seules dans leur classe d'isogénie sur $\mathbf{Q}$; on a donc $\delta = 1$, et les λ_E sont premiers entre eux. Ceci démontre la proposition. Notons qu'en cours de démonstration on a montré que le théorème de Ribet implique également le résultat suivant:

Théorème 3.2. Soit E une courbe de Weil forte de conducteur premier N. La valuation de son discriminant en N est alors égale au nombre de points de torsion de $E(\mathbf{Q})$.

Nous énonçons à présent sans démonstration le théorème qui permet d'obtenir explicitement une équation de $\mathcal{E}$ une fois connus les λ_E.

Théorème 3.3. SoitLet $\mathcal{E}$ une courbe de Weil forte de conducteur premier N, et $\sum \lambda_E[E]$ l'élément de M_N^0 associé à $\mathcal{E}$ par la construction ci-dessus. Il existe une équation de $\mathcal{E}$

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$$

avec c_4 et c_6 dans $\mathbf{Z}$, tels que, si $H = \sup(\sqrt{|c_4|}, \sqrt[3]{|c_6|})$, on a, avec les notations ci-dessus L

1. $H \leq \frac{8n}{\sqrt{N}-2}(\log(H^6/1728) + b)$, où $b = (\Gamma(1/3)/\Gamma(2/3))^3 = 7.74316962\ldots$.
2. Soit $\Delta' = (c_4^3 - c_6^2)/1728$. Alors $\Delta' = \Delta$ si $\mathcal{E}$ est supersingulière en 2, et $\Delta' = \Delta$ ou $2^{12}\Delta$ sinon.
3. $c_4 \equiv (\sum \lambda_E j_E)^4 \text{mod } N$.
4. $c_6 \equiv -(\sum \lambda_E j_E)^6 \text{mod } N$.
5. $n\delta = \lambda_E^2 \omega_E$.

Si les λ_E sont connus, 5 permet d'obtenir n, et 1 d'obtenir une borne de H donc de c_4 et c_6. Par 2, on connait $c_4^3 - c_6^2 = 1728\Delta'$, ce qui permet de trouver c_4 et c_6. Les congruences 3 et 4 permettent de diminuer notablement le nombre de calculs. On a donc ainsi trouvé une équation de la courbe de Weil forte correspondant à la newform f initiale.

En fait, cette méthode permet aussi de prouver qu'une courbe elliptique de conducteur N premier assez petit est de Weil. Supposons en effet donnée une telle courbe, par exemple par son équation. Nous pouvons alors calculer le nombre de ses points N_l mod l pour $l = 2, 3, \ldots$. On cherche ensuite, par la méthode des graphes, si $a_2 = 3 - N_2$ est valeur propre de T_2 agissant sur M_N. Si non, la conjecture de Taniyama-Weil est fausse. Si oui, on continue avec T_3 agissant sur l'espace propre trouvé, s'il n'est pas de dimension 1, jusqu'à trouver un espace propre de dimension 1 pour les opérateurs de Hecke, à valeurs propres entières. S'il n'existe pas, on a un contre-exemple à la conjecture de Taniyama-Weil. S'il existe, on calcule une équation de la courbe de Weil correspondante. Si cette courbe se révèle être isogène à la courbe initiale, on a fini. Sinon, la courbe initiale n'est pas de Weil.

En particulier, cela a permis de montrer que la courbe elliptique d'équation

$$y^2 + y = x^3 - 7x + 6$$

de conducteur 5077, est une courbe de Weil.

Cette courbe semble être la plus petite courbe (lorsqu'on ordonne les courbes par conducteurs croissants) ayant un groupe de Mordell-Weil de rang ≥ 3 [3]. Son intérêt est le suivant:

Soit $f(z) = \sum a_n q^n$ ($q = e^{2\pi i z}$), une newform de poids 2 et de conducteur N, et $L(s) = \sum a_n n^{-s}$, la fonction L associée. Si l'ordre en 1 de L est ≥ 3, Goldfeld a montré qu'il existe une constante C_f calculable telle que

$$\log p < C_f h(-p),$$

où p est un nombre premier $\equiv 3 (\mathrm{mod}\ 4)$ et premier à N et $h(-p)$ le nombre de classes du corps quadratique imaginaire de discriminant $-p$. On a des formules analogues, mais plus compliquées, dans le cas des corps quadratiques imaginaires de discriminant non premier (voir [13] par exemple).

Si la conjecture de Birch et Swinnerton-Dyer est vraie, toute courbe de Weil dont le groupe de Mordell-Weil sur $\mathbf{Q}$ est de rang ≥ 3 devrait fournir de telles formes modulaires, mais jusqu'aux travaux de Gross et Zagier [8], on n'avait aucun moyen de vérifier que la dérivée en 1 de la fonction L d'une courbe de Weil est effectivement nulle. Les résultats de Gross et Zagier permettent par contre d'écrire $L'(1)$ comme un produit d'un facteur non nul aisément calculable et de la hauteur de Néron-Tate d'un point de Heegner (cf. [8] pour les détails). Il est alors possible, en minorant la hauteur des points rationnels de la courbe et en majorant $L'(1)$ par un calcul approché, de montrer que L est d'ordre ≥ 3 en $s = 1$. (Dans toute ce qui précéde, on a considéré des courbes de Weil impaires, c'est-à-dire dont la fonction L a un ordre impair en 1 – ou, si l'on préfère, dont le signe de l'équation fonctionnelle est -1.)

On a plusieurs moyens de construire des courbes de Weil doint le groupe de Mordell-Weil est de rang ≥ 3 (et qui sont donc de bons candidats pour la question

précédente: par la méthode de Gross-Zagier, on peut calculer $L'(1)$. Si $L'(1)$ est nul, on a une fonction L qui permet d'obtenir une majoration de la valeur absolue du discriminant des corps quadratiques imaginaires de nombre de classes donné; s'il est non nul, la conjecture de Birch et Swinnerton-Dyer est fausse! Il va sans dire que jusqu'à présent, on s est toujours trouvé dans le premier cas...) On peut par exemple chercher des courbes à multiplications complexes de rang 3 (on sait a priori qu'elles sont de Weil), mais la constant C_f est alors très grande. On peut aussi tordre une courbe de Weil (par exemple la courbe $37C$ de [19] jusqu'à obtenir une courbe de rang 3 (en l'occurrence, pour la courbe $37C$, on peut tordre par $\mathbf{Q}(\sqrt{-139})$, comme le montrent Gross et Zagier [8]). Ceci conduit à une constante C_f de l'odre de grandeur de 7000.

On peut enfin choisir une courbe elliptique quelconque définie sur $\mathbf{Q}$, de rang 3, et tenter de montrer que c'est une courbe de Weil. C'est ce qui a été fait dans [10] pour la courbe ci-dessus de conducteur 5077, en employant la formule des traces. Mais le calcul a été très long (5 ehures sur l'ordinateur employé, un IBM 4341). Le méthode des graphes a permis de le faire en environ 5 secondes sur le même ordinateur.

Pour cette courbe, on a $C_f < 50$: tout corps quadratique imaginaire de discriminant d, avec $|d| > e^{150}$ a donc un nombre de classes ≥ 4. D'autre part, il n'existe pas de corps quadratique imaginaire de discriminant d et de nombre de classes 3 pour $907 < |d| < 10^{2500}$ [12]. Par suite (après examen d'une table donnant les nombres de classes des premiers corps quadratiques):

Théorème 3.4. Les corps quadratiques imaginaires de nombre de classes 3 sont les seize corps de discriminant $-23, -31, -59.-83, -107, -139, -211, -283, -307, -331, -379, -499, -54$

4 Application à une conjecture de Serre

Soit ρ une représentation contique de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ dans $\mathrm{GL}_2(V)$, où V est un espace vectoriel de dimension 2 sur un corps fini $\mathbb{F}_q$ de caractéristique p. On suppose cette représentation impaire, c'est-à-dire que l'image $\rho(c)$ de la conjugaison complexe c, vue comme élément de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, a comme valeurs propres -1 et 1. Dans ce qui suit, on pose $G = Im\rho$.

Dans [17], Serre définit le niveau, le caractère et le poids d'une telle représentation:

1. Le niveau.

   Soit l un nombre premier premier à p. On note G_i, $i = 0, \ldots$ les groupes de ramification de ρ en l. Soit

   $$n(l) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \mathrm{codim} V^{G_i},$$

   où g_i est l'ordre de $G_i|$.

Le conducteur de la représentation ρ est alors défini comme étant

$$N = \prod_{l \neq p} l^{n(l)}.$$

2. Le caractère.

   Le déterminant de ρ fournit un caractère de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ dans $\mathbb{F}_q^*$,dont le conducteur divise pN. Par suite, on peut écrire

   $$\det \rho = \varepsilon \chi^{k-1},$$

   où χ est le caractère cyclotomique de conducteur p et où ε est un caractère $(\mathbf{Z}/N\mathbf{Z})^* \longrightarrow \mathbb{F}_q^*$. L'entier k est défini mod $(p-1)$,et le fait que la représentation est impaire implique que $\varepsilon(-1) = (-1)^k$.

   Par définition, ε est le caractère de la représentation ρ.

3. Le poids.

   L'entier k est défini mod $(p-1)$. Je renvoie à l'article de Serre pour la définition du poids $k \in \mathbf{Z}$ de la représentation ρ. Alors que le conducteur N ne dépend que du comportement de ρ aux places premières à p, la définition du poids ne fait intervenir que les propriétés locales en p de la représentation ρ.

La conjecture de Serre peut alors s'énoncer ainsi:

Conjecture 4.1. *Soit ρ une représentation comme ci-dessus, de poids k, de niveau N et de caractère ε. Supposons cette représentation irréductible. Elle provient alors d'une forme parabolique mod p de poids k, niveau N caractère ε.*

Cette conjecture, si elle était vraie, aurait de nombreuses conséquences: elle implique notamment la conjecture de Taniyama-Weil, et le grand théorème de Fermat.

Beaucoup de telles représentations ρ sont modulaires, soit par constructions, soit parce qu'elles entrent dans le cadre de conjectures classiques (Langlands, Artin, ...) qui entrainent la conjecture (parfois sulement sous une forme faible, c'est-à-dire avec un poids ou un conducteur plus grands que ceux définis dans [17].)

Pour vérifier (ou infirmer) la conjecture de Serre, il faut trouver des extensions $K/\mathbf{Q}$, de groupe de Galois un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_q)$ à déterminant impair si $p \neq 2$. Il n'est en général pas difficile de calculer, pour l premier et pas trop grand, la trace a_l de Frob_l dans $\mathrm{GL}_2(\mathbb{F}_q)$: si $P(x)$ est un polynôme dont les racines engendrent K, la décomposition de $P \mathrm{mod}\ l$ suffit souvent.

Il est par contre beaucoup plus ardu de trouver la forme modulaire mod p, si elle existe, qui correspond à la représentation ρ donnée par le corps K: le discriminant de K est souvent gros, donc aussi le conducteur de ρ, qui lui est intimement lié, et il n'est alors pas possible de mener les calculs à bien

4.1 Le cas $SL_2(\mathbb{F}_4)$

Un cas troublant est celui où $p = 2$, car, du fait que $-1 \equiv 1 (\text{mod } 2)$, toute représentation est alors impaire.

Les représentations de $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ dans $\text{GL}_2(\mathbb{F}_2) = S_3$ (même totalement réelles, cf. [17]) proviennent de formes modulaires de poids 1, le groupe S_3 pouvant être réalisé comme un sous-groupe de $\text{GL}_2(\mathbf{C})$. On peut alors espérer que par multiplication par des séries d'Eiseinstein convenables, on obtienne une forme modulaire de poids et de niveau prédits par la conjecture de Serre (cf. [17] pour des exemples).

Pour obtenir des cas plus intéressants en caractéristique 2, on considère des représentations à valeurs dans $\text{GL}_2(\mathbb{F}_4)$. L'isomorphisme $A_5 \simeq \text{SL}_2(\mathbb{F}_4)$ permet d'en obtenir plusieurs exemples. Soit donc une extension K de $\mathbf{Q}$ de Galois A_5. Comme A_5 se plonge dans $PGL_2(\mathbf{C})$, si le corps n'est pas totalement réel, la représentation ρ associée provient encore d'une forme modulaire de poids 1 (modulo la conjecture d'Artin; cf. [2]). Supposons par contre que K soit totalement réel; aucune des conjectures classiques ne nous permet alors de soupçonner ρ de provenir d'une forme modulaire, même de poids ou de niveau éléve. C'est ce cas que nous étudions en détail dans ce qui suit. La méthode des graphes a ici été indispensable, les formes modulaires recherchées ayant de trop gros conducteurs pour être étudiées à l'aide de la formule des traces de Eichler-Selberg.

Soit donc $P(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5$ un polynôme à coefficients dans $\mathbf{Q}$ de degré 5, de discriminant D. Pour que le corps des racines de P soit A_5, il faut et il suffit que P soit irréductible, que D soit un carré, et qu'il existe un nombre premier l ne divisant pas D tel que $P\text{mod } l$ ait exactement 2 racines dans $\mathbb{F}_l$ (cette dernière condition assurant que le groupe est bien A_5 tout entier).

Il est clair que $\varepsilon = 1$. Si p divise D, p premier à 30, $n(p) = 1$ si it seulment si l'inertie en p est d'ordre 2, et donc si le polynôme P a des racines au plus doubles mod p. Quant au poids k, il est 2 ou 4 suivant la ramification de K en 2. Pour simplifier les calculs, nous avons limité la recherche d'exemples aux représentations de niveau premier et de poids 2.

D'autre part, bien qu'il s'agisse de représentations dans $SL_2(\mathbb{F}_4)$, le coefficient a_2 de la forme modulaire cherchée, si elle existe, peut ne pas être dans $\mathbb{F}_4$, mais dans $\mathbb{F}_{16}$. Cela provient du fait que le coefficient a_l d'une forme modulaire mod l est égal à une valeur propre de Frob_l, et non à sa trace. Or, si une matrice de $SL_2(\mathbb{F}_4)$ est d'ordre 5, ses valeurs propres sont dans $\mathbb{F}_{16}$, et non dans $\mathbb{F}_4$.

Les exemples traités ci-dessous ont éte obtenus en faisant tout d'abord une recherche systématique sur ordinateur (l'IBM 4341 de l'ENS, rue d'Ulm) de polynômes convenables (totalement réels, de type A_5, dont le conducteur de la représentation associée est un nombre premier N, et dont le poids est 2.

Ensuite, pour chachun de ces polynômes P, on a calculé la valeur propre a_2 correspondante (dans $\mathbb{F}_16$), et on a cherché s'il existe une forme modulaire mod 2 de niveau N et de poids 2 telle que T_2 ait a_2 comme valeur propre. Dans tous les cas

considérés, on a alors trouvé un espace propre de dimension 1 ou 2. En employant les opérateurs T_3 et T_5, on a alors calculé les coefficients a_3 et a_5, et vérifié qu'ils ont la valeur prédite par le type de décomposition de P en 3 et 5.

Évidemment, cela ne prouve pas vraiment que la représentation ρ associée à P est modulaire: nous avons seulement exhibé une forme modulaire mod 2 du bon niveau et du bon poids dont les termes a_2, a_3 et a_5 conviennent. Mais c'est une bonne présomption de la véracité de la conjecture de Serre dans les cas considérés: une recherche extensive sur de nombreux nombres premiers N des coefficients a_2 de formes modulaires de poids 2 et de niveau N montre en effet qu'il est rare qu'ils soient dans des corps de petit degré. (En fait, il semble que 2, et plus généralement les petits nombres premiers, soient les plus "inertes" possibles dans les corps intervenant dans l'algèbre de Hecke des formes modulaires, corps qui eux-mêmes paraissent en général être du plus gors degré possible, compte tenu des contraintes du type involutions d'Atkin-Lehner, premiers d'Eiseinstein, etc. Il arrive évidemment qu'il y ait des petits facteurs, – correspondant par exemple aux courbes elliptiques de conducteur premier – mais c'est apparemment rare.)

4.2 Quelques exemples

1. $P(x) = x^5 - 10x^3 + 2x^2 + 19x - 6$.

   Le discriminant de P est $(2^3887)^2$. Ce polynôme est irréductible mod 5, donc irréductible sur $\mathbf{Q}$. Ses racines sont toutes réelles (on peut par exemple appliquer l'algorithme de Sturm). On a

   $$P(x) \equiv x(x-1)(x^3+x^2-1) \bmod 3,$$

   ce qui fournit un cycle d'ordre 3; le groupe de Galois de K, le corps des racines de P, est donc A_5.

   Du fait que $P(x) \equiv (x-462)(x-755)^2(x-788)^2 \bmod 887$[2] on déduit que le conducteur N de la représentation associée à P est $N = 887$. On peut également montrer que 3 est "peu ramifié" au sens de [17], donc le poids de ρ est 2. Un examen facile de la réduction de P mod 2 montre que les coefficients a_2, a_3 et a_5 de la forme modulaire mod 2 de niveau 887 qui doit correspondre via la conjecture de Serre à ρ sont 1, 1 et j (où $j \in \mathbb{F}_4$ vérifie $j^2 + j + 1 = 0$).

   On applique alors la méthode des graphes: l'espace des formes modulaires mod 2 de poids 2 et niveau 887 est de dimension 73, et le calcul montre que l'espace propre G_1 de T_2 correspondant à la valeur propre 1 est de dimension 2; T_3 agit comme l'identité sur G_1, et j et j^2 sont les valeurs propres de T_5 agissant sur G_1, d'où une base de G_1 formée de $f_1 = q + q^2 + q^3 + q^4 + jq^5 + \cdots$ et

[2] correction from original: $P(x) \equiv (x-446)(x-126)^2(x-538)^2 \bmod 887$

$f_2 = q + q^2 + q^3 + q^4 + j^2q^5 + \cdots$, vecteurs propres des opérateurs de Hecke. Ceci corrobore parfaitement la conjecture.

2. $P(x) = x^5 - 23x^3 + 55x^2 - 33x - 1$.

   Then $D = 13613^2, P(x) \equiv (x - 6308)(x - 2211)^2(x - 8248)^2 \bmod 13613$, $N = 13613$; P étant irréductible mod 2, Frob_2 est un cycle d'ordre 5, et $a_2 = \zeta_5$, une racine cinquième de l'unitè, vue comme élément de $\mathbb{F}_{16}$. La calcul montre alors que, dans l'espace des formes modulaires mod 2 de niveau 13613 et de poids 2, qui est de dimension 1134, ζ_5 est valeur propre simple de T_2. Les coefficients a_3 et a_5 sont respectivement égaux à $1 + \zeta_5^2 + \zeta_5^3 = j$ et à $\zeta_5^2 + \zeta_5^3 = j^2$, qui sont bien les traces de Frob_3 et Frob_5 dans $\mathrm{SL}_2(\mathbb{F}_4)$.

3. Énonçons rapidement les autres polynômes trouvés; dans chaque cas, il existe une forme modulaire de poids 2 et du bon niveau, dont les premiers termes a_n correspondent à ceux prédits par la conjecture de Serre.

$$P(x) = x^5 + x^4 - 16x^3 - 7x^2 + 57x - 35, N = 8311, \sqrt{D} = N$$

$$P(x) = x^5 + 2x^4 - 43x^3 + 29x^2 + 2x - 3, N = 8447, \sqrt{D} = 2^2N$$

$$P(x) = x^5 + x^4 - 13x^3 - 14x^2 + 18x + 14, N = 15233, \sqrt{D} = 2N$$

$$P(x) = x^5 + x^4 - 37x^3 + 67x^2 + 21x + 1, N = 24077, \sqrt{D} = 2^2N$$

5 Appendice: Les courbes $X_0(p)$ de genre 0

Dans [5], il est montré que, si p est un nombre premier, la courbe $X_0(p)$ sur $\mathbf{Z}_p$ est formellement isomorphe à la courbe d'équation $xy = p^k$ au voisinage de tout point se réduisant mod p en un point supersingulier S, k étant la moitié du nombre d'automorphismes de S.

Si $X_0(p)$ est de genre 0 (i.e., $p = 2, 3, 5, 7$, et 13) on a en fait un tel modèle sur $\mathbf{Z}$, donné par la fonction

$$x = \left(\frac{\eta(z)}{\eta(pz)}\right)^{\frac{24}{p-1}}, \tag{2}$$

où $\eta(z) = q^{1/24}\prod_{i=1}^{\infty}(1 - q^n)$ and $q = e^{2\pi iz}$.

Ceci découle de Fricke [7], qui donne également, pour chacune des valeurs de p ci-dessus, l'expression du morphisme oubli $j : X_0(p) \longrightarrow X_0(1)$, qui à tout point (E, C) de $X_0(p)$ associe le point (E) de $X_0(1)$, paramétré par l'invariant modulaire j.

Dans ce qui suit, nous rappelons ces équations, et donnons également l'expression des correspondances T_2 et T_3 sur ces courbes. La variable x est celle donnée par

l'équation (2), l'involution W_p échange x et y et le diviseur de x est $(0)-(\infty)$, où 0 et ∞ sont les deux pointes de $X_0(p)$.

1. $p=2$ Les èquations données par Fricke (légèrement modifiées pour donner un modèle de $X_0(2)$ sur $\mathbf{Z}$) sont:

$$xy = 2^{12}$$

$$j = \frac{(x+16)^3}{x}$$

T_2 est donné par:

$$y^2 - y(x^2 + 2^4 3x) - 2^{12}x = 0$$

(A tout point x est associée par T_2 la somme formelle des points de coordonnées y racines de ce polynôme.)

T_3 est donné par:

$$x^4+y^4-x^3y^3-2^3 3^2 x^2y^2(x+y)-2^2 3^2 5^2 xy(x^2+y^2)+2\cdot 3^2 1579 x^2y^2-2^{15}3^2xy(x+y)-2^{24}xy = 0$$

2. $p=3$.

$$xy = 3^6$$

$$j = \frac{(x+27)(x+3)^3}{x}$$

$$T_2 : x^3 + y^3 - 2^3 3xy(x+y) - x^2y^2 - 3^6 xy = 0$$

$$T_3 : y^3 - y^2(x^3 + 2^2 3^2 x^2 + 2\cdot 3^2 5y) - 3^6 yx(x + 2^2 3^2) - 3^{12}x = 0$$

3. $p=5$.

$$xy = 5^3$$

$$j = \frac{(x^2+10x+5)^3}{x}$$

$$T_2 : x^3 + y^3 - x^2y^2 - 2^3 xy(x+y) - 7^2 xy = 0$$

$$T_3 : x^4+y^4-x^3y^3-2\cdot 3^2 x^2y^2(x+y)-3^4 xy(x^2+y^2)-2\cdot 3^2 23 x^2y^2-2250xy(x+y)-5^6 xy = 0$$

4. $p=7$.

$$xy = 7^2$$

$$j = \frac{(x^2+13x+49)(x^2+5x+1)^3}{x}$$

$$T_2 : x^3 + y^3 - x^2y^2 - 2^3 xy(x+y) - 7^2 xy = 0$$

$$T_3 : x^4+y^4-x^3y^3-2^2 3x^2y^2(x+y)-2\cdot 3\cdot 7xy(x^2+y^2)-3\cdot 53 x^2y^2-2^2 3\cdot 7^2 xy(x+y)-7^4 xy = 0$$

5. $p = 13$.

$$xy = 13$$

$$j = \frac{(x^2+5x+13)(x^4+7x^3+20x^2+19x+1)^3}{x}$$

$$T_2 : x^3+y^3-x^2y^2-2^2xy(x+y)-13xy = 0$$

$$T_3 : x^4+y^4-x^3y^3-2\cdot 3x^2y^2(x+y)-3\cdot 5xy(x^2+y^2)-3\cdot 11x^2y^2-2\cdot 3\cdot 13xy(x+y)-13^2xy = 0$$

Les polynômes ci-dessus donnat T_2 et T_3 sont donc d'écriture plus simple que les équations modulaires classiques $\Phi_2(j,j')$ et $\Phi_3(j,j')$ (qui correspondent à l'action de T_2 et T_3 sur $X_0(1)$). A titre de comparaison, nous rappelons leur expression:

$$\begin{aligned}\Phi_2(j,j') &= j^3+j'^3-j^2j'^2+2^4 3\cdot 31jj'(j+j')-2^4 3^4 5^3(j^2+j'^2)\\ &\quad +3^4 5^3 4027jj'+2^8 3^7 5^6(j+j')-2^{12}3^9 5^9\end{aligned}$$

$$\begin{aligned}\Phi_3(j,j') &= j^4+j'^4-j^3j'^3-2^2 3^3 9907jj'(j^2+j'^2)+2^3 3^2 31j^2j'^2(j+j')\\ &\quad -2^{16}5^3 3^5 17\cdot 263jj'(j+j')+2^{15}3^2 5^3(j^3+j'^3)+2\cdot 3^4 13\cdot 193\cdot 6367j^2j'^2\\ &\quad -2^{31}5^6 22973jj'+2^{30}3^3 5^6(j^2+j'^2)+2^{45}3^3 5^9(j+j')\end{aligned}$$

References

[1] A.O.L. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134-160.

[2] J.P. Buhler, *Icosahedral Galois Representations*, Springer Lecture Notes **654** (1978).

[3] J.P. Buhler, B. Gross, D. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3*, Math. Of Comp. **44** (1985), 473-481.

[4] A. Brumer, K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), 716-743.

[5] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques*, Springer Lecture Notes **349** (1973), 143-316.

[6] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren*, J. reine angew. Math. **195** (1956), 127-151.

[7] R. Fricke, Lehrbuch der Algebra, III, Braunschweig, F. Vieweg & Sohn, 1928.

[8] B. Gross, D. Zagier, *Points de Heegner et dérivées de fonctions L*, C. R. Acad. Sc. Paris **297** (1983), 85-87.

[9] B. Mazur, P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1-61.

[10] J. -F. Mestre, *Courbes de Weil de conducteur* 5077, C.R. Acad. Sc. Paris **300** (1985), 509-512.

[11] I. Miyawaki, *Elliptic curves of prime power conductor with* $\mathbf{Q}$*-rational points of finite order*, Osaka Math. J. **10** (1973), 309-323.

[12] H.L. Montgomery, P. J. Weinberger, *Notes on small class numbers*, Acta Arithm. **24** (1973), 529-542.

[13] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Se'm. Bourbaki, Juin 1984.

[14] A. Pizer, *On the arithmetic of quaternion algebras II*, J. Math. Soc. Japan **28** (1976), 676-688.

[15] A. Pizer, *An algorithm for copmuting modular forms on* $\Gamma_0(N)$, J. of Alg. **64** (1980), 340-390.

[16] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[17] J.-P. Serre, *Sur les représentations modulaires de degré 2 de Gal*($\overline{\mathbf{Q}}/\mathbf{Q}$), à paraˆître dans Duke Math. J.

[18] C. B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. **10** (1975), 367-378.

[19] Tables, *Modular Functions of One Variable IV*, Springer Lecture Notes **476** (1975), 33-52.