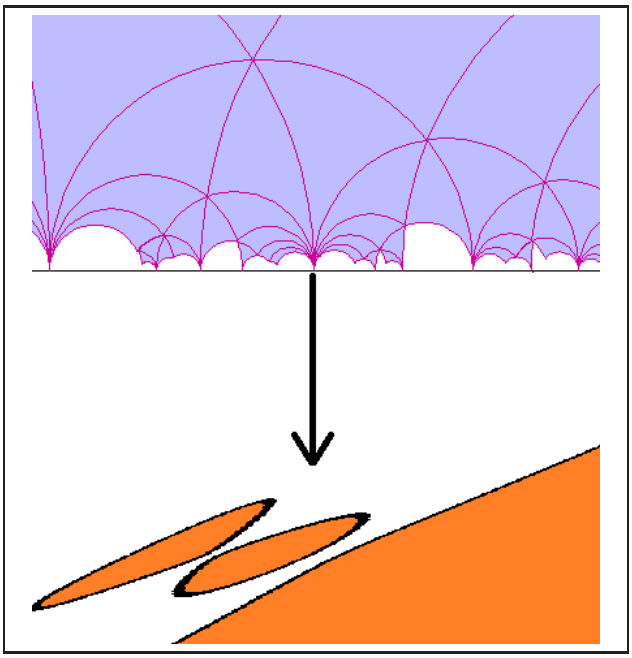
La paramétrisation modulaire pour les courbes de genre supérieur à deux

Bruno Winckler
sous la direction de Fabien Pazuki



2 octobre 2010

Table des matières

Introduction

L'objectif de ce stage de ce recherche était de parfaire mes connaissances en théorie des nombres, plus particulièrement dans l'univers des formes modulaires qui avait déjà attisé ma curiosité. À cet effet, Fabien Pazuki m'a soufflé l'idée d'étudier *Finiteness results for modular curves of genus at least 2*, un article publié conjointement par Matthew H. Baker, Enrique González-Jiménez, Josep González et Björn Poonen. J'espère, ici, éclairer le problème qu'ils étudient et quelques idées qui jaillissent de cet article, tout en explorant des problèmes dans son adhérence.

Au commencement était une courbe elliptique sur $\mathbb{Q}$ de conducteur N, nommée E ; Andrew Wiles et d'autres mathématiciens ont démontré que cette courbe est nécessairement modulaire, c'est-à-dire qu'il existe un morphisme non constant $\phi : X_0(N) \to E$, où $X_0(N)$ est le compactifié du quotient du demi-plan de Poincaré $\mathcal{H}$ par le sous-groupe des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $PSL_2(\mathbb{Z})$ telles que N divise c (qui agit sur $\mathcal{H}$ par homographies). On dit alors que $\phi : X_0(N) \to E$ est une paramétrisation modulaire de E. Ce résultat est suffisamment fécond, comme j'essaye de l'illustrer très partiellement dans une première section en le reliant à la conjecture *abc*, pour qu'on puisse légitimement se demander s'il s'étend à des courbes de genre supérieur (on préférera alors $X_1(N)$ à $X_0(N)$). La situation est en fait radicalement différente, puisqu'on sait montrer que certaines courbes ne sont pas modulaires. De plus, le résultat suivant est soupçonné :

Conjecture 1 *Pour tout $g \geq 2$, l'ensemble des courbes modulaires sur $\mathbb{Q}$ de genre g est fini, à $\mathbb{Q}$-isomorphisme près.*

Même si cette proposition n'est toujours pas démontrée, plusieurs résultats vont en ce sens : je montrerai par exemple qu'il y a un nombre fini, à $\mathbb{Q}$-isomorphisme près, de courbes modulaires *nouvelles*, adjectif que je définirai en temps voulu.

Je remercie Fabien Pazuki pour cette initiation à la paramétrisation modulaire et tout ce qui s'en rapproche, mais aussi pour sa sympathie et sa disponibilité malgré les contretemps. Merci également à Pierre Parent, Guillaume Ricotta, Qing Liu et Mladen Dimitrov pour leurs éclaircissements décisifs, ainsi qu'à Pierre Charollois et Patrice Philippon pour avoir contribué à mon enterrement de vie d'étudiant.

1 Le cas des courbes elliptiques

1.1 Conjecture *abc* et paramétrisation modulaire

Il est difficile d'être exhaustif, mais je présente tout de même un exemple d'application du théorème de Wiles à un problème d'arithmétique actuel :

Conjecture 2 (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 lien entre la conjecture *abc* et la paramétrisation modulaire n'est pas si surprenant, si on connait les courbes de Frey : si $a + b + c = 0$, je note $E_{a,b,c}$ la courbe elliptique d'équation affine

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

Son discriminant est $\Delta = \frac{1}{2^8}a^2(-b)^2(a+b)^2 = \frac{(abc)^2}{2^8}$: La courbe $E_{a,b,c}$ est donc elliptique si, et seulement si $abc \neq 0$, ce qui est le cas. Cette courbe est alors modulaire, paramétrée par $\phi : X_0(N) \to E$. Soit f la forme primitive de poids 2 associée à ϕ *via* $\phi^*(\mathrm{d}z) = 2\pi i c_E f(z)\mathrm{d}z$, où c_E est un entier non nul, appelé constante de Manin et conjecturalement égal à ± 1 quand la courbe E est forte. On peut relier le degré de ϕ à f grâce au produit scalaire de Petersson :

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

d'où :

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

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

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

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

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

où les habitués des courbes elliptiques reconnaitront en $h(E)$ la hauteur de Faltings de E. Bref,

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

et une inégalité sur $\max(|a|, |b|, |c|)$ apparaîtra après estimation de chaque terme du membre de droite.

1.2 Estimations du degré de ϕ

Évaluation de $2\ln(2\pi|c_E|)$ À défaut d'affirmer que $c_E^2 = 1$ comme le suggère Manin, on sait tout de même montrer que $\ln(2\pi|c_E|)$ est borné : d'après [Maz], si p divise c_E, alors p^2 divise $4N$. On sait montrer que N égale $\mathrm{rad}(abc)$; c'est, en fait, un des intérêts de la manœuvre. En particulier, N est *quadrafrei*, donc si p divise c_E, alors $p = 2$. Or, un résultat de [A&U] montre que si 4 divise c_E, alors 4 divise N. Là encore, ceci permet de prouver que c_E égale au plus ± 2. Bref, $\ln(2\pi|c_E|) = O(1)$.

Évaluation de $2\ln(||f||)$ Pour ce terme, 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 $L(\mathrm{Sym}^2(f), \cdot)$.

Bref, comme

$$\prod_{p^2|N} \left(1 - \frac{1}{p^2}\right)^{-1} \leq \prod_{p\leq N} \left(1 - \frac{1}{p^2}\right)^{-1} < \infty,$$

le produit convergeant car $\ln\left(1 - \frac{1}{p_n^2}\right) \simeq -\frac{1}{p_n^2} \simeq -\frac{1}{n^2 \ln(n)^2}$ est le terme général d'une série convergente, on a l'inégalité :

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

où $C > 0$ est indépendante de N.

Le théorème de Phragmén-Lindelhöf, version Rademacher (voir [M&M]), fournit

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

l'énoncé général portant sur les fonctions L admettant des « bons » produits eulériens, pour assurer qu'on a alors $|L(\sigma+it)| \leq \left(A(|t|+2)^d\right)^{(2-\sigma)/2} \left(\ln(A(|t|+2)^d)^d\right)$ où d est le degré maximal des polynômes dans l'écriture des facteurs eulériens et A un coefficient apparaissant dans l'équation fonctionnelle. Ici $d = 3$ et $\ln(A) = O(\ln(N))$, d'où l'inégalité que je soumets. Ainsi, $||f||^2 \leq c_2 N(\ln(N))^3$, où c_2 est une certaine constante positive.

Évaluation de $h(E)$ Voici l'occasion de parler plus en détails de la hauteur de Faltings de 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.

Une façon de définir $h(E)$ est par le degré du fibré $\omega_{\mathscr{E}}$, où $\mathscr{E}$ est un modèle de Néron pour $E/\mathbb{Q}$. C'est-à-dire, en prenant $t \in \omega_{\mathscr{E}}$ non nul :

$$h(E) = \ln(\mathrm{card}(\omega/\mathbb{Z}t)) - \ln(||t||_\infty).$$

En calculant chacun des termes, on trouve

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

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

Pour évaluer cette quantité, commençons par le terme archimédien : on remarque d'une part que, pour τ_∞ dans le domaine fondamental

$$D = \{\tau \in \mathcal{H} || \Re(\tau)| \leq \frac{1}{2}, |\tau| \geq 1\},$$

on a $\Im(\tau) \geq \frac{\sqrt{3}}{2}$ et $|q| \leq \exp(-\pi\sqrt{3})$, donc

$$\left|\prod_{n=1}^{\infty}(1-q^n)\right|$$

est borné, avec une minoration large différente de 0. Alors, $\ln(|\Delta(\tau)|) = \ln(|q|) + O(1)$.

Or $-\ln(|q|) = -\ln(\max(|j(\tau)|, 1)) + O(1)$. En effet, le q-développement de $j(\tau)$ donne $\ln(|j(\tau)|) = \ln(|1/q|) + O(1)$ pour $\Im(\tau) \geq 1$, et $\ln(|j(\tau)|) = O(1)$ sinon ; cette distinction est nécessaire à cause de l'annulation de j en $\exp(2i\pi/3)$. Ceci permet d'écrire

$$-\ln(|\Delta(\tau)|) = \ln(\max(|j(\tau)|, 1)) + O(1).$$

Combiné à l'égalité $\ln(|q|) = -2\pi\Im(\tau)$, on obtient

$$\ln(\Im(\tau)) = \ln(\ln(\max(|j(\tau)|, e))) + O(1),$$

puis, en remarquant que $j(\tau_\infty) = j_E$:

$$12h(E) = \ln(|\Delta|) + (\ln(\max(|j_E|, 1)) - 6\ln(\ln(\max(|j_E|, e))) + O(1)).$$

À présent, posons $\gamma = \frac{\Delta}{\beta}$, où β est le dénominateur de la fraction irréductible $\frac{\alpha}{\beta}$ de j_E : on l'appelle discriminant instable minimal. On sait que $H_\mathbb{Q}(j_E) = |\beta| \cdot \max(|j_E|, 1)$. On peut alors réécrire l'équation précédente ainsi :

$$\ln(|\beta|) + \ln(\max(|j_E|, 1)) = \ln(H_\mathbb{Q}(j_E)) = h(j_E).$$

D'où

$$12h(E) = h(j_E) + \ln(\gamma) + O(\ln(h(j_E))).$$

Comme $\Delta = \frac{(abc)^2}{2^8}$ et $j_E = \frac{2^8(a^2+b^2+ab)^3}{(abc)^2}$, et que a^2+b^2+ab est premier avec abc, on voit que $\beta = \frac{(abc)^2}{2^k}$ pour un certain entier naturel $k \in [\![0,8]\!]$. Ainsi, $\gamma = 2^{k-8}$, qui est borné quand le conducteur varie.

Il est aisé de vérifier que a^2+b^2+ab est premier avec abc : si p divise abc et a^2+b^2+ab, il divise par exemple a. Alors, il divise également b, donc il divise c : absurde, car a, b et c sont supposés premiers entre eux pour les besoins de la cause. Bref, $h(j_E) = 3\ln(a^2+b^2+ab)+O(1)$. Un calcul lourd mais sans mystère montre que $\ln(a^2+b^2+ab) = 2\ln(\max(|a|,|b|,|c|)) + O(1)$; grâce à tout ceci, on a déjà 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 $\ln(||f||^2) \geq (1-\varepsilon)\ln(N)$ d'après [H&L] (théorème 0.2, page 5), 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

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

On connait déjà une version exponentielle de « l'inégalité *abc* » : dans [S&Y], cette version est démontrée à l'aide d'une estimation p-adique pour des formes linéaires à base de logarithme de nombres algébriques. En tout cas, grâce à $\ln(\max(|a|,|b|,|c|)) = N^d + O(1)$, on obtient $\ln(\deg(\phi)) \leq c_3 N^d$ (encore une fois $c_3 > 0$), avec les mêmes raisonnements qu'ici.

J'ai donc exhibé ici une des études possibles liées à la paramétrisation modulaire des courbes elliptiques, qui confronte la théorie des hauteurs, l'étude des fonctions L et de l'arithmétique visiblement (et à tort) élémentaire *via* la conjecture *abc*. La paramétrisation modulaire mène à bien d'autres applications mathématiques : par exemple, une application frappante réside dans la démonstration du dernier théorème de Fermat (avec l'étude d'une courbe de Frey E_{a^p,b^p,c^p}), et l'approche se généralise à des équations diophantiennes variées ; [Sik] illustre bien le propos.

Il était également possible, dans mon approche, de relier directement $\deg(\phi)$ à $L(\mathrm{Sym}^2(f),2)$; on a en effet, d'après [Wat],

$$L(\mathrm{Sym}^2(f),2) = 2\pi\mu(E_f) \prod_{p^2|N} U_p(2) \frac{\deg(\phi)}{N c_E^2}$$

où les $U_p(2)$ sont des facteurs eulériens qui ne sont pas sans rappeler la formule précédente, liant $L(\mathrm{Sym}^2(f), 2)$ et $||f||$. Watkins l'utilise pour montrer que $\deg(\phi) \gg N^{7/6-\varepsilon}$, et qu'on peut bien s'attendre à avoir une borne polynomiale sur le degré de ϕ, ce qui entrainerait la justesse de la conjecture *abc*.

2 Le cas du genre supérieur à 2

Dorénavant, on préférera parler de paramétrisation modulaire pour un morphisme $X_1(N) \to X$ plutôt que $X_0(N) \to X$, où $X_1(N) = \mathcal{H}/\Gamma_1(N)$, $\Gamma_1(N)$ étant le sous-groupe de $\Gamma_0(N)$ des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ où a et d sont congrus à 1 modulo N. Il est clair qu'être modulaire pour $X_0(N)$ implique être modulaire pour $X_1(N)$. Toutes les courbes elliptiques sur $\mathbb{Q}$ restent donc modulaires pour $X_1(N)$.

2.1 Modularité des courbes : contre-exemple

Pour un genre plus grand que celui des courbes elliptiques, la situation est radicalement différente : certaines courbes ne sont pas modulaires. Par exemple, soit E une courbe hyperelliptique sur $\mathbb{Q}$, définie par le modèle affine :

$$y^2 = \prod_{i=0}^{42}(x - i).$$

C'est une courbe hyperelliptique de genre 21. Supposons qu'elle soit modulaire, paramétrée par $\phi : X_1(N) \to E$. Je note g et G le genre et la gonalité de $X_1(N)$, où la gonalité de $X_1(N)$ désigne le plus petit degré possible d'un morphisme $X_1(N) \to \mathbb{P}^1_{\mathbb{C}}$. On sait que g et G sont reliés par la formule

$$\frac{21}{200}(g-1) \leq G.$$

L'idée derrière cette formule est la suivante : comme la métrique de Poincaré sur $X_1(N)$ est le *pullback* de $\frac{\mathrm{d}x^2+\mathrm{d}y^2}{y^2}$ sur $X_1(1)$, on a

$$\mathscr{A}(X_1(N)) = [PSL_2(\mathbb{Z}) : \Gamma_1(N)]\mathscr{A}(X_1(1)) = [PSL_2(\mathbb{Z}) : \Gamma_1(N)]\frac{\pi}{3},$$

où $\mathscr{A}(X)$ désigne l'aire d'un domaine fondamental de X. Les propriétés conformes des homothéties de $\mathbb{P}^1$, combinées à un argument de point fixe, permettent de prouver que

$$\lambda_1\mathscr{A}(X_1(N)) \leq 2\mathscr{A}_c(X_1(N)) \leq 8\pi \cdot G,$$

où $\mathscr{A}_c(X_1(N))$ est la borne inférieure de l'ensemble des $\int_{X_1(N)} f^*\mathrm{d}\mu_0$ pour $f : X_1(N) \to \mathbb{P}^1$ une application conforme non constante, $\mathrm{d}\mu_0$ une mesure SO_3-invariante, et λ_1 est la première valeur propre non nulle de la partie discrète du

spectre du laplacien de $X_1(N)$, conjecturalement supérieure à $\frac{1}{4}$, dont on sait seulement qu'elle est supérieure à $\frac{21}{100}$. De tout ceci, on déduit

$$\frac{7}{800}[PSL_2(\mathbb{Z}) : \Gamma_1(N)] \leq G.$$

Or, la formule de Gauss-Bonnet donne ici

$$g - 1 = \frac{[PSL_2(\mathbb{Z}) : \Gamma_1(N)]}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2} \leq \frac{[PSL_2(\mathbb{Z}) : \Gamma_1(N)]}{12},$$

où ε_i représente le nombre de points elliptiques de périodes i si $i \neq \infty$, et le nombre de pointes de $X_1(N)$ sinon. Donc $\frac{21}{200}(g-1) \leq G$. Pour le détail, voir [Abr].

Bref, comme $X_1(N) \stackrel{\phi}{\to} X \to \mathbb{P}^1$ définit un morphisme non constant de degré $2\deg(\phi)$, on a $G \leq 2\deg(\phi)$. De plus, la formule de Riemann-Hurwitz donne l'inégalité $\deg(\phi) \leq \frac{g-1}{20}$, donc on obtient, en combinant ce qu'on a :

$$\frac{21}{200}(g-1) \leq 2\frac{g-1}{20} \Rightarrow 20 \leq \frac{400}{21} < \frac{420}{21} = 20,$$

ce qui est absurde.

Ce même raisonnement montre qu'une courbe hyperelliptique nouvelle est nécessairement de genre $g \leq 20$.

2.2 Le cadre

Il est temps, pour être dans de bonnes conditions, de définir le cadre de la paramétrisation modulaire en genre supérieur. En plus des objets $X_0(N)$ et $X_1(N)$ déjà introduits, on aura souvent besoin du point de vue « jacobien » de la situation, qu'on traitera à l'aide de $J_1(N) = \mathrm{Jac}(X_1(N))$. On sait qu'un morphisme $X_1(N) \to X$ induit des morphismes $J_1(N) \to \mathrm{Jac}(X)$ et $\mathrm{Jac}(X) \to J_1(N)$ duaux, le premier permettant de voir $\mathrm{Jac}(X)$ comme un quotient de $J_1(N)$.

Définissons $J_1(N)_{\mathrm{old}}$ comme étant la somme dans $J_1(N)$ des images des morphismes $J_1(M) \to J_1(N)$ induits par les $\begin{cases} \mathcal{H} & \to & \mathcal{H} \\ z & \mapsto & d \cdot z \end{cases}$ où $M|N$ et $d|\frac{N}{M}$, $M \neq N$. On dit que X est modulaire nouvelle si l'image de $\mathrm{Jac}(X) \to J_1(N)$ est contenue dans $J_1(N)_{\mathrm{new}}$: $J_1(N)_{\mathrm{new}}$ est l'unique sous-variété abélienne de $J_1(N)$ telle que $J_1(N) = J_1(N)_{\mathrm{old}} + J_1(N)_{\mathrm{new}}$ où $J_1(N)_{\mathrm{old}} \cap J_1(N)_{\mathrm{new}}$ est fini. On voit alors que si X est nouvelle, alors il y a un morphisme $J_1(N)^{\mathrm{new}} \to \mathrm{Jac}(X)$, où $J_1(N)^{\mathrm{new}} = J_1(N)/J_1(N)_{\mathrm{old}}$. Par exemple, les différents travaux sur les courbes elliptiques montrent qu'en plus d'être modulaires, elles sont modulaires nouvelles.

Dans le contexte, Ω dénote le faisceau des 1-formes sur une courbe X en présence. Alors, $H^0(X, \Omega)$ est classiquement l'ensemble des sections globales,

et on appelle genre de X la dimension sur k de cet espace vectoriel. Si on a un morphisme $\phi : X_1(N) \to X$, on note $S_2(X)$ le sous-ensemble des formes paraboliques f de niveau N telles que $f(z)\mathrm{d}z$ provient d'une forme différentielle sur X grâce à ϕ^*.

Dans tout ce mémoire, les formes modulaires sont de poids 2. La notation New_N désigne l'ensemble des formes primitives de poids 2 et de niveau N, c'est-à-dire l'ensemble des formes paraboliques nouvelles et propres pour les opérateurs de Hecke T_n tels que n est premier avec N.

Sauf mention contraire, k désigne toujours un corps de caractéristique nulle. Enfin, tous les résultats de finitude sont à $\mathbb{Q}$-isomorphisme près.

2.3 Résultats préliminaires

Le premier résultat de la section sera utilisé fréquemment pour nos théorèmes de finitude. Il permet de caractériser une courbe à l'aide du développement tronqué de ses différentielles, généralement des formes modulaires dans ce mémoire.

Lemme 2.1 *Soit $g \geq 2$ un entier. Il existe alors un entier $B \geq 1$ dépendant de g tel que pour tous éléments w_1, w_2, ..., w_g dans $k[[q]]/q^B$, il existe au plus une courbe X sur k telle que, pour un certain point $P \in X(k)$ et $q \in \hat{\mathcal{O}}_{X,P}$ un paramètre uniformisant analytique, les $w_1 dq$, ..., $w_n dq$ soient les développements modulo q^B d'une base de $H^0(X, \Omega)$.*

On peut même expliciter B en fonction de g, comme on va le voir dans la preuve.

Preuve. Soient X, P, q et w_i tels que dans l'énoncé du lemme, et $\omega_i = w_i \mathrm{d}q \in H^0(X, \Omega)$. Il s'agit de montrer que X est déterminée par les w_i quand $B = \max(8g - 7, 6g + 1)$.

Comme $B > 8g - 8$, les w_i déterminent l'ensemble des relations polynômiales homogènes de degré 4 satisfaites par les ω_i. En effet, le théorème de Riemann-Roch assure qu'un élément non nul de $H^0(X, \Omega^{\otimes 4})$ a $8g - 8$ zéros, donc son développement en un point s'annule au plus à l'ordre $8g - 8$, si bien que $F(w_1, \ldots, w_g) \equiv 0 \mod q^B$ implique $F(\omega_1, \ldots, \omega_g) = 0$. Or...

Théorème 2.2 *Soit X une courbe de genre $g \geq 2$ sur un corps k de caractéristique nulle. Alors l'image X' de l'application canonique $X \to \mathbb{P}^{g-1}$ est le lieu commun des zéros des polynômes homogènes de degré 4 qui s'annulent sur X'.*

L'application canonique $X \to \mathbb{P}^{g-1}$ est celle déterminée par le système linéaire canonique.

Preuve. Si X est hyperelliptique, birationnelle à $y^2 = f(x)$ où f est séparable, alors $\{\frac{x^i \mathrm{d}x}{y} | 0 \leq i \leq g - 1\}$ forme classiquement une base de $H^0(X, \Omega)$. Alors, l'image de l'application canonique est l'intersection de la courbe normale

rationnelle* avec $\{t_i t_j - t_{i'} t_{j'} | i + j = i' + j'\}$, où les t_i sont les coordonnées homogènes dans $\mathbb{P}^{g-1}$. Si X n'est pas hyperelliptique et de genre 3, alors son modèle canonique est une quartique plane. Dans les autres cas, le théorème de Petri (voir [ACGH], page 131) dit exactement que l'image de $X \to \mathbb{P}^{g-1}$ est le lieu commun des zéros de polynômes homogènes de degré 2 ou 3, donc de polynômes homogènes de degré 4, si on les prend parmi leurs multiples. □

Bref, ce théorème dit que les w_i caractérisent l'image X' de l'application canonique. Si X n'est pas hyperelliptique, d'après [Har], $X \to \mathbb{P}^{g-1}$ est un plongement, donc les w_i caractérisent X. Il reste donc à traiter le cas hyperelliptique.

En s'inspirant de l'élimination de Gauss, on peut supposer que $0 = \mathrm{ord}_q(w_1) < \cdots < \mathrm{ord}_q(w_g) \leq 2g-2$, et que le premier coefficient de chaque w_i est 1. À présent, j'ai besoin du lemme suivant :

Lemme 2.3 *Soit X une courbe hyperelliptique de genre g sur un corps k, et supposons que $P \in X(k)$. Soit $(\omega_1, \ldots, \omega_g)$ une base de $H^0(X, \Omega)$ telle que $\mathrm{ord}_P(\omega_1) < \cdots < \mathrm{ord}_P(\omega_g)$. Alors $x = \frac{\omega_{g-1}}{\omega_g}$ et $y = \frac{\mathrm{d}x}{\omega_g}$ engendrent le corps de fonctions $K(X)$, et il existe un unique polynôme F séparable de degré au plus $2g+2$ tel que $y^2 = F(x)$. Si P est un point de Weierstrass, alors $\deg(F) = 2g+1$ et $\mathrm{ord}_P(\omega_i) = 2i-2$ pour tout i, sinon $\deg(F) = 2g+2$ et $\mathrm{ord}_P(\omega_i) = i-1$ pour tout i. Il est possible de remplacer chaque ω_i par une combinaison linéaire de $\omega_i, \omega_{i+1}, \ldots, \omega_g$, afin d'avoir $\omega_i = \frac{x^{g-i}\mathrm{d}x}{y}$ pour tout $1 \leq i \leq g$.*

Un point de Weierstrass $P \in X$ est un point tel qu'il existe une forme différentielle s'annulant à l'ordre au moins g en P, où g est le genre de la courbe X. Il est équivalent, par le théorème de Riemann-Roch, de dire que $l(jP) = l((j-1)P)$ pour tous les entiers j entre 1 et g.

Preuve. On le démontre directement en utilisant les résultats du chapitre 3, section 6 de [Gol]. □

Voici comment utiliser ce lemme : si P est un point de Weierstrass, alors $w_i = q^{2i-2}(1 + \cdots + O(q^{B-2i+2}))$. En définissant x et y comme dans le lemme, on a

$$y = \frac{\mathrm{d}x}{w_g \mathrm{d}q} = -2q^{-(2g+1)}(1 + \cdots + O(q^{B-2g+2})),$$

et $y^2 = 4q^{-(4g+2)}(1 + \cdots + O(q^{B-2g+2}))$. Comme $B \geq 6g+1$, on a $-(4g+2) + (B-2g+2) > 0$, et il y a donc un unique polynôme F tel que $y^2 = F(x)$, ce qui définit donc une unique courbe hyperelliptique vérifiant les propriétés demandées. Si P n'est pas un point de Weierstrass, on procède de même, et $B \geq 3g+2$ est suffisant. □

Dans le cas où q n'est pas un paramètre uniformisant analytique, on peut tout de même obtenir un résultat proche, en ajustant la preuve. En effet, on

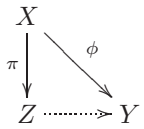
∗. C'est-à-dire l'image du plongement classique $\mathbb{P}^1 \to \mathbb{P}^{g-1}$, qui à $a = (a_0, a_1)$ associe $(M_0(a), \ldots, M_N(a))$, où les M_i sont les monômes de degré $g-1$ en les variables X_0, …, X_{g-1}, et $N = \binom{n+g-1}{n} - 1$.

peut démontrer qu'on peut remplacer q par un élément $q' \in \hat{\mathcal{O}}_{X,P}$ de la forme $q' = c_e q^e + c_{e+1} q^{e+1} + \cdots$ avec $c_e \neq 0$, tel que $w_1 \mathrm{d}q'$, …, $w_g \mathrm{d}q'$ soient les développements modulo q'^{eB} d'une base de $H^0(X, \Omega)$.

Enfin, on aura besoin d'induire des automorphismes d'une courbe $X_1(N)$ sur une courbe X à plusieurs reprises. C'est l'objet du prochain lemme qui, on le verra, est typique du genre supérieur à 2.

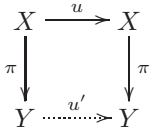
Lemme 2.4 (Descente des morphismes) *Soient X, Y et Z trois courbes sur k, et supposons que le genre de Y est supérieur à 2. Alors :*

(i) Si deux morphismes non constants $\pi : X \to Z$ et $\phi : X \to Y$ vérifient $\phi^*(H^0(Y, \Omega)) \subseteq \pi^*(H^0(Z, \Omega))$, alors il existe un morphisme non constant $u' : Z \to Y$ tel que le diagramme



commute.

(ii) Si $\pi : X \to Y$ est un morphisme non constant et u un automorphisme de X tel que u^* laisse stable $\pi^*(H^0(Y, \Omega))$, alors il existe un unique automorphisme u' de Y tel que le diagramme



commute.

Preuve. La conclusion de (i) est équivalente à l'affirmation $\phi^*(K(Y)) \subseteq \pi^*(K(Z))$. Pour la prouver, il suffit de voir que toute fonction de $\phi^*(K(Y))$ s'écrit comme quotient de *pullbacks* de différentielles méromorphes sur Z.

Si Y n'est pas hyperelliptique, alors $K(Y)$ est engendré par des quotients de différentielles de $H^0(Y, \Omega)$, donc l'inclusion $\phi^*(H^0(Y, \Omega)) \subseteq \pi^*(H^0(Z, \Omega))$ fournit ce qu'il nous faut. Si Y est hyperelliptique, c'est plus subtile : on a $K(Y) = k(x, y)$ avec $y^2 = f(x)$ pour f un polynôme séparable. Alors, le corps engendré par les quotients de différentielles dans $H^0(Y, \Omega)$ est $k(x)$, si bien que $\phi^*(k(x)) \subseteq \pi^*(k(Z))$. L'élément $\phi^*(y)$ est également dans $\pi^*(k(Z))$, parce que $y = \frac{x\mathrm{d}x}{x\mathrm{d}x/y}$ et $x\mathrm{d}x/y$ est dans $H^0(Y, \Omega)$.

À présent, si on applique (i) à $\pi : X \to Y$ et $\pi \circ u : X \to Y$ qui vérifient bien les hypothèses, on obtient l'existence de $u' : Y \to Y$ tel que $u' \circ \pi = \pi \circ u$. Comme le genre de Y est supérieur ou égal à 2, la formule de Riemann-Hurwitz dans le cas séparable fournit $\deg(u') = 1$ et u' est un automorphisme. L'unicité provient

de l'injection $\mathrm{Hom}(K(X), K(X)) \hookrightarrow \mathrm{Mor}_k(X, X)$, d'image les morphismes dominants de X dans X. $\square$

On remarque que dans la démonstration, la caractéristique nulle n'intervient que pour la formule de Riemann-Hurwitz, qui nécessite que les morphismes soient séparables. Dans la suite du mémoire, j'induirai des automorphismes entre des courbes sur $\mathbb{F}_p$ grâce à cette observation.

Enfin, le dernier résultat, très important, concerne les éléments de $S_2(X)$ pour X une courbe modulaire. Dans la preuve de ce lemme, j'utiliserai le fait que $\mathrm{End}(A_f)$ soit, essentiellement, l'ensemble des multiplications par un élément de $\mathbb{Q}_f$ (le corps engendré par les coefficients de Fourier de f). C'est un résultat dû à Shimura et Ribet. Plus précisément, $\mathrm{End}(A_f) \otimes \mathbb{Q} = \mathbb{Q}_f$.

Lemme 2.5 *Soit X une courbe modulaire sur $\mathbb{Q}$. Alors $S_2(X)$ a une base T stable par $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ formée de formes paraboliques de la forme*

$$h(q) = \sum_{d|N/M} c_d f(q^d)$$

pour un certain M divisant N, et $f \in \mathrm{New}_M$, où $c_d \in \mathbb{Q}_f$ ne dépend que de f et d.

Preuve. En multipliant l'application quotient $J_1(N) \to \mathrm{Jac}(X)$ par un entier convenable, on peut supposer qu'elle se factorise *via* l'isogénie

$$J_1(N) \to \bigoplus_{M|N} \bigoplus_{f \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\backslash \mathrm{New}_M} A_f^{n_f}.$$

Comme $\mathrm{Jac}(X)$ est un quotient de $J_1(N)$, elle s'écrit comme produit de variétés abéliennes $A_f^{n_f}$. Les formes différentielles sur $\mathrm{Jac}(X)$ s'obtenant par somme directe des formes différentielles sur chaque variété simple qui compose $\mathrm{Jac}(X)$, je peux supposer que cette jacobienne est $\mathbb{Q}$-simple et donc isomorphe à un certain A_f. Alors, l'application quotient $J_1(N) \to \mathrm{Jac}(X)$ n'est rien d'autre que la composition de $J_1(N) \to A_f$ avec un homomorphisme $A_f \to \mathrm{Jac}(X)$. De

$$X_1(N) \hookrightarrow J_1(N) \to A_f \xrightarrow{c} \mathrm{Jac}(X),$$

où $c = (c_d)_{d|N/M} \in \mathrm{End}(A_f)^{n_f}$, je déduis que la 1-forme sur $\mathrm{Jac}(X) \simeq A_f$ correspondant à f donne $\sum_{d|N/M} c_d f(q^d) \frac{\mathrm{d}q}{q}$ sur $X_1(N)$. Alors, $H^0(\mathrm{Jac}(X), \Omega)$ a une base formée de cette 1-forme et de ses conjuguées, et les *pullbacks* de ces conjuguées sont de la même forme. $\square$

Enfin, pour les besoins de la cause, je donne l'action de quelques opérateurs sur les formes différentielles de $X_1(N)$. Je rappelle que si χ est un caractère, le conducteur de χ est le plus petit entier M divisant N tel que χ se factorise par $(\mathbb{Z}/M\mathbb{Z})^*$. Si la valuation en p de $\mathrm{cond}(\chi)$ est strictement inférieure à celle de N, on écrit χ' le caractère de $(\mathbb{Z}/(N/p)\mathbb{Z})^*$ induit par χ.

Proposition 2.6 *Soit $f = \sum_{n=1}^{\infty} a_n q^n$ une forme primitive de niveau N et de caractère χ. Alors :*

(i) Si $v_p(N) \geq 2$ et $v_p(N) > v_p(\mathrm{cond}(\chi))$, alors $a_p = 0$.

(ii) Si $v_p(N) = 1$ et $v_p(N) > v_p(\mathrm{cond}(\chi)) = 0$, alors $a_p^2 = \chi'(p)$.

(iii) Si $v_p(N) = 1$ et χ est trivial, alors $f|W_p = -a_p f$.

Preuve. La preuve de ces formules, essentiellement calculatoire, se trouve dans [A&L] et [Li]. □

2.4 Quelques résultats de finitude

Théorème 2.7 *Pour tout $g \geq 2$, l'ensemble des courbes modulaires nouvelles de genre g est fini.*

Preuve. Soit $g \geq 2$, et X une courbe nouvelle de niveau N et genre g, paramétrée par le morphisme $\phi : X_1(N) \to X$. En adaptant la preuve du lemme 2.5 à l'isogénie

$$J_1(N)^{\mathrm{new}} \to \bigoplus_{f \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\backslash \mathrm{New}_N} A_f,$$

on voit qu'il existe une base T de $S_2(X)$ stable par $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ formée de formes primitives de niveau N.

Soit $f = q + \sum_{n=2}^{\infty} a_n q^n$ un élément de T. Il existe $\omega \in H^0(X_{\mathbb{C}}, \Omega)$ tel que $\phi^*(\omega) = f\frac{\mathrm{d}q}{q}$, quantité qui ne s'annule pas en ∞, donc ϕ est non ramifié en ∞. Alors, le paramètre uniformisant q en ∞ sur $X_1(N)$ en reste un en $\pi(\infty)$ sur X.

Soit $\mathbb{Q}_f$ le corps engendré par les coefficients de Fourier de f. Il vérifie

$$[\mathbb{Q}_f : \mathbb{Q}] = \dim(A_f) \leq \dim(J) = g.$$

De plus, chaque a_n est un entier algébrique de degré au plus g, et de norme archimédienne bornée (par $\sigma_0(n)\sqrt{n}$), si bien que par un résultat classique ([Win2], page 26), il n'y a qu'un nombre fini de possibilités pour chaque a_n, donc pour f modulo q^B, où B est l'entier du lemme 2.1, et donc pour $\{f \mod q^B | f \in T\}$ qui est de cardinal $\dim(\phi^*(H^0(X, \Omega))) = g$, car ϕ^* est injective. Chaque possibilité donne lieu à une unique courbe X par le lemme 2.1. □

Les coefficients des formes primitives de T ne sont pas dans $\mathbb{Q}$ mais dans $\mathbb{Q}_f$, et pourtant on peut quand même conclure de la même manière, à savoir avec l'unicité d'une certaine courbe sur $\mathbb{Q}$. Pour ce faire, il faut ajouter un complément à la preuve du lemme 2.1 : soit K un corps contenant les coefficients de toutes les formes primitives de T. Alors, l'espace vectoriel sur K engendré par T est stable sous l'action de $\mathrm{Gal}(K/\mathbb{Q})$. On a juste à remplacer T par une base sur $\mathbb{Q}$ de cet espace vectoriel, et appliquer le lemme tel qu'on le connait.

Le fait que les courbes concernées soient nouvelles est utilisé de manière décisive ici. D'une part, pour avoir une base de formes primitives pour $S_2(X)$, ce qui permet de limiter le nombre de possibilités pour leurs coefficients, et d'autre

part pour être certain que ϕ est non ramifié en ∞. Ainsi, si on veut adapter la preuve précédente à des courbes modulaires qui ne sont pas nouvelles, il faut quelques restrictions supplémentaires. Voici un résultat qu'on peut obtenir, avec une démonstration sensiblement proche :

Théorème 2.8 *Soit S un sous-ensemble de $\mathbb{N}^*$ fixé. Pour tout $g \geq 2$, l'ensemble des courbes modulaires de genre g et de niveau contenu dans S est fini si $S = \text{Épars}_{B(g)}$, où Épars_m est l'ensemble des entiers positifs dont le rapport des diviseurs (positifs) consécutifs est toujours strictement supérieur à m.*

Ce théorème généralise en un certain sens le résultat plus classique suivant :

Théorème 2.9 (Théorème de de Franchis-Severi) *Soit k un corps de nombres ou $\bar{\mathbb{Q}}$, et soit X une courbe sur k. Alors l'ensemble des paires (Y, π) où Y est une courbe sur k de genre au moins 2 et $\pi : X \to Y$ est un morphisme est fini, à k-isomorphisme près ((Y, π) et Y', π' sont isomorphes si, et seulement si il existe un isomorphisme $Y \to Y'$ dont la composition avec π donne π').*

Preuve du théorème 2.8. Cette fois, le lemme 2.5 nous assure l'existence d'une base T dont les formes modulaires sont de la forme $h = \sum_{d|N/M} c_d f(q^d)$ où f est une forme primitive de niveau $M|N$, et $c_d \in \mathbb{C}$. Si je note e la valeur minimale de $\text{ord}_q(g)$ pour g dans T, on a même $h = \sum_{d|N/M, d \geq e} c_d f(q^d)$. La forme $g\text{d}q/q$ est la tirée en arrière d'une différentielle qui ne s'annule pas en $\phi(\infty)$, donc e est en fait l'indice de ramification de $X_1(N) \to X$. La remarque qui suit la preuve du lemme 2.1 montre que l'ensemble $\{h \mod q^{eB} | h \in T\}$ caractérise X : notre paramètre q « devenant » q^e sur X, on voit que e doit correspondre à l'indice de ramification de $X_1(N) \to X$.

Comme $N \in \text{Épars}_B$, on a $d > eB$ pour tout d divisant N tel que $d > e$. Si $c_e = 0$, alors $h = 0 \mod q^{eB}$. On peut donc supposer, quitte à normaliser, que $c_e = 1$. Alors, « l'éparsement » de N permet de s'assurer que $a_n(h(q)) = a_n(f(q^e))$ pour tout $n \in [\![1, eB]\!]$. C'est-à-dire : $a_n(h) = a_{n/e}(f)$ si $e|n$, et $a_n(h) = 0$ sinon. Comme f est une forme primitive, on peut montrer de la même manière que pour le théorème 2.7 qu'il y a un nombre fini de choix pour les $a_n(h)$ tels que $n \leq eB$ et $e|n$, et donc un nombre fini de choix pour $\{h \mod q^{eB} | h \in T\}$, d'où un nombre fini de X possibles. □

À l'image du dernier théorème, l'essentiel des résultats de finitude s'obtiennent en fixant une condition sur le niveau, le genre, ou la gonalité, par exemple. Voici d'autres résultats qu'on peut déduire, modulo une ou plusieurs restrictions :

Théorème 2.10 *Pour tout $G \geq 2$, l'ensemble des courbes modulaires nouvelles de genre au moins 2 et de gonalité au plus G est fini.*

Preuve. En suivant le même raisonnement que dans le contre-exemple en début de section, on arrive sans peine à l'inégalité $g \leq \frac{200}{21} G + 1$. Ce résultat,

lié au théorème 2.7, fait de ce théorème une évidence. □

Enfin, on sait que la conjecture sur le nombre de courbes modulaires à genre fixé est vraie, si on impose que les courbes modulaires en question soient des quotients de $X_1(N)$ par un sous-groupe du groupe d'automorphismes (sur $\bar{\mathbb{Q}}$) engendré par les opérateurs diamants $\langle d \rangle$ et les involutions d'Atkin-Lehner W_M. En effet, le quotient de $X_1(N)$ par ce sous-groupe (que je note $G(N)$) est égal au quotient de $X_0(N)$ par le groupe des involutions d'Atkin-Lehner, et je note ce quotient $X^*(N)$. On connait le genre de $X_0(N)$, il est de l'ordre de $N^{1+o(1)}$ quand $N \to \infty$. D'après ce qu'on vient de montrer, sa gonalité est au moins $N^{1+o(1)}$. De plus, le degré de $X_0(N) \to X^*(N)$ est $2^{\mathrm{card}(\{p|N\})}$, donc de l'ordre de $N^{o(1)}$ (en fait, on a même $\mathrm{card}(\{p|N\}) \sim \ln(\ln(N))$). Ainsi, la gonalité de $X^*(N)$ tend vers l'infini quand $N \to \infty$, donc son genre également. Ceci étant dit, si on fixe $g \geq 2$, on voit aisément qu'il y a un nombre fini de $X^*(N)$ de genre g. De même, si $X = X_1(N)/\Gamma$ où $\Gamma \subseteq G(N)$, le genre de cette courbe, étant supérieur à celui de $X^*(N)$, tend vers l'infini quand $N \to \infty$. Il y a donc un nombre fini de courbes $X_1(N)/\Gamma$ à genre fixé et Γ fixé. Comme $G(N)$ est fini (de cardinal au plus $2^{\mathrm{card}(\{p|N\})}\varphi(N)^{\varphi(N)}$, où φ est l'indicatrice d'Euler), il y a un nombre fini de choix pour Γ, et donc un nombre fini de courbes $X_1(N)/\Gamma$ à genre fixé.

2.5 Propriétés des courbes modulaires

Pour mieux comprendre les courbes modulaires, une possibilité est d'étudier leur niveau et de trouver des restrictions sur ce dernier en fonction du genre des courbes ; c'est par exemple ce qui permet de conclure si on remplace $X_1(N)$ par des courbes de Fermat. En particulier, on a des résultats sur les diviseurs premiers du niveau, en fonction du genre de la courbe. Dans cette optique, il est compréhensible qu'on s'intéresse aux réductions modulo p d'une courbe modulaire, à condition de voir ce qu'on entend par réduction modulo p ; pour une courbe elliptique ou hyperelliptique, la démarche peut paraître naturelle, si on peut réduire modulo p les coefficients. Mais plus généralement, voici comment procéder : si A est un anneau de valuation discrète et de corps de fraction K, et X une courbe sur K, alors X admet une bonne réduction en A si X admet un modèle projectif lisse sur A, un modèle étant une courbe $\mathcal{X}$ sur A telle que $\mathcal{X} \times_A K \simeq X$. Si $A = \mathbb{Z}_{(p)}$ et $K = \mathbb{Q}$, on reconnait la réduction modulo p classique.

Lemme 2.11 *Soit A un anneau de valuation discrète de corps de fraction K. Supposons que $f : X \to Y$ soit un morphisme fini entre courbes projectives lisses et géométriquement intégrales sur K, la courbe Y étant de genre $g \geq 1$. Si X admet un modèle projectif lisse $\mathcal{X}$ sur A, alors Y admet un modèle projectif lisse $\mathcal{Y}$ sur A, et f s'étend un morphisme fini $\mathcal{X} \to \mathcal{Y}$ sur A.*

C'est l'objet de l'article [L&L].

Lemme 2.12 *Soit X une courbe hyperelliptique sur $\mathbb{Q}$ modulaire nouvelle de niveau N et de genre g. Si p ne divise pas N, alors $(p-1)(g-1) < 2(p^2+1)$.*

Preuve. Si p ne divise pas N, alors $X_1(N)$ a bonne réduction en p, de même pour X par le lemme précédent, et $\phi : X_1(N) \to X$ induit un morphisme sur $\mathbb{F}_p$ entre les courbes correspondantes, que je note toujours de la même manière. En composant avec le plongement canonique $X \to \mathbb{P}^1$, les automorphismes de $X_1(N)$ peuvent induire des automorphismes de X puis de $\mathbb{P}^1$ d'après la proposition 4.3, toujours sur $\mathbb{F}_p$. C'est ce que je fais de $\langle -p \rangle$.

$$\begin{array}{ccccc} X_1(N) & \xrightarrow{\phi} & X & \longrightarrow & \mathbb{P}^1 \\ {\scriptstyle \langle -p \rangle}\downarrow & & \downarrow & & \downarrow \\ X_1(N) & \longrightarrow & X & \longrightarrow & \mathbb{P}^1 \end{array}$$

Soit n le nombre de solutions à l'équation $\mathrm{Frob}_p^2(x) = \langle -p \rangle x$. Tous les points supersinguliers de $X_1(N)(\bar{\mathbb{F}}_p)$ vérifient cette équation : un point supersingulier est associé à une courbe elliptique supersingulière E, et on a le résultat suivant :

Lemme 2.13 *Sous les mêmes hypothèses, une telle courbe est toujours isomorphe à une courbe elliptique sur $\mathbb{F}_{p^2}$ telle que $\mathrm{Frob}_p^2 = -p$.*

Preuve. En effet, on sait qu'une courbe elliptique est supersingulière si, et seulement si la multiplication par $-p$ est purement inséparable. La multiplication par $-p$ étant une isogénie de degré p^2, on a le diagramme commutatif suivant, d'après [Sil] :

$$\begin{array}{ccc} E & \xrightarrow{-p} & E \\ & {\scriptstyle \mathrm{Frob}_p^2} \searrow & \uparrow {\scriptstyle \sim} \\ & & E^{(p^2)} \end{array} ,$$

où $E^{(p^2)}$ est obtenue en élevant à la puissance p^2 les coefficients d'une équation de Weierstrass de E ; l'idée est que si K est une clôture séparable de $[-p]^*(k(E))$ dans $k(E)$, alors $k(E)/K$ est purement inséparable de degré p^2, donc $k(E)^{(p^2)} \subseteq K$. Considérer le Frobenius donne l'égalité $K = [-p]^*(k(E)^{(p^2)})$, d'où l'emboîtement $[-p]^*(k(E)) \subseteq [-p]^*(k(E)^{(p^2)}) \subseteq k(E)$, auquel on fait correspondre les applications du diagramme ci-dessus. Comme $E \simeq E^{(p^2)}$, on a $j(E) = j(E)^{(p^2)}$ et donc $j(E) \in \mathbb{F}_{p^2}$. Il existe donc une courbe elliptique E' sur $\mathbb{F}_{p^2}$ et supersingulière de même j-invariant que E, donc isomorphe à E. Là encore, on peut dresser un diagramme commutatif :

$$\begin{array}{ccc} E' & \xrightarrow{-p} & E' \\ & {\scriptstyle \mathrm{Frob}_p^2} \searrow & \uparrow {\scriptstyle \lambda} \\ & & E' \end{array} ,$$

où λ est un automorphisme de E'. Alors, $\mathrm{Frob}_p^2 = \lambda^{-1} \circ [-p] = [-p] \circ \lambda^{-1}$.

Soit $\sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_{p^2})$ le générateur de ce groupe de Galois, et le morphisme de groupes $\xi : \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_{p^2}) \to \mathrm{Aut}(E')$ défini par $\sigma \mapsto \lambda^{-1}$. Comme $\xi \in H^1(\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_{p^2}), \mathrm{Aut}(E'))$, le théorème X.2.2 et la proposition X.5.3 dans [Sil] permettent de construire une courbe elliptique E'' sur $\mathbb{F}_{p^2}$ telle que $\varphi : E'' \otimes \bar{\mathbb{F}}_p \to E' \otimes \bar{\mathbb{F}}_p$ soit un isomorphisme vérifiant $\xi(\tau) = \varphi^\tau \circ \varphi^{-1}$ pour tout $\tau \in \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_{p^2})$, où $\varphi^\tau(P) = \varphi(P^{\tau^{-1}})^\tau$ pour tout P, ce qu'on peut réécrire $\varphi^\sigma(P) = \pi'' \circ \varphi \circ (\pi')^{-1}(P)$.

Par conséquent,

$$\lambda^{-1}(P) = \xi(\sigma)(P) = \mathrm{Frob}_p^2 \circ \varphi \circ (\mathrm{Frob}_p^2)^{-1}(P) \circ \varphi^{-1}(P),$$

où on prend garde au sens des différents Frobenius (notamment concernant leurs espaces de départ et d'arrivée), et pour P sur la courbe E', on a $\mathrm{Frob}_p^2(P) = [-p] \circ \lambda^{-1}(P) = [-p] \circ \mathrm{Frob}_p^2 \circ \varphi \circ (\mathrm{Frob}_p^2)^{-1} \circ \varphi^{-1}(P)$, d'où, en utilisant le fait que $-p$ commute :

$$\mathrm{Frob}_p^2(P) = [-p](P),$$

pour tout P sur la courbe E''. Le résultat voulu en découle. □

Or, on sait dénombrer le nombre de courbes elliptiques supersingulières :

Lemme 2.14 *Soit p un nombre premier ne divisant pas N, π l'application naturelle (sur $\bar{\mathbb{Q}}$) de $X_1(N)$ dans $X_1(1)$. Alors $X_1(N)$ a une bonne réduction en toute place au dessus de p, et le nombre de $\bar{\mathbb{F}}_p$-points associés à des points supersinguliers de $X_1(1)$ par l'application de réduction est au moins $\frac{(p-1)\deg(\pi)}{12}$.*

Bref, $n \geq \frac{(p-1)\deg(\pi)}{12}$. De plus, $\mathrm{Frob}_p^2(x) = \langle -p \rangle x$ sur $X_1(N)(\bar{\mathbb{F}}_p)$ induit une solution sur X puis sur $\mathbb{P}^1$. Un résultat de théorie de l'intersection sur $\mathbb{P}^1 \times \mathbb{P}^1$ assure que, les fonctions $x \mapsto (x, \mathrm{Frob}_p^2)$ et $x \mapsto (x, \langle -p \rangle x)$ étant respectivement de bidegrés $(1, p^2)$ et $(1, 1)$, il y a $1 \cdot 1 + p^2 \cdot 1 = p^2 + 1$ points d'intersection entre ces courbes. Bref, $n \leq (2\deg(\phi))(p^2 + 1)$.

Résumons. On a :

$$\frac{(p-1)\deg(\pi)}{12} \leq (2\deg(\phi))(p^2 + 1). \tag{4}$$

De plus, on a vu que le genre g_1 de $X_1(N)$ vérifie :

$$g_1 - 1 \leq \frac{\deg(\pi)}{12}. \tag{5}$$

Enfin, la formule de Riemann-Hurwitz donne, une fois de plus, l'inégalité $\deg(\phi) \leq \frac{g_1 - 1}{g - 1}$. Ces trois inégalités donnent naissance à l'inégalité $(p-1)(g-1) < 2(p^2 + 1)$. □

Corollaire 2.15 *Soit X une courbe hyperelliptique modulaire nouvelle de niveau N et de genre g. Si $g > 10$, alors $6|N$. Si $g > 13$, alors $30|N$.*

Preuve. Il suffit de prendre $p = 2, 3$ puis 5 dans le lemme précédent. □

Si X est dominée par $X_0(N)$, alors $\langle -p \rangle$ est l'automorphisme trivial, donc la borne $(2\deg(\phi))(p^2+1)$ peut être remplacée par $(\deg(\phi))\mathrm{card}(X(\mathbb{F}_p^2))$ dans la preuve précédente (X a bien bonne réduction en p). Ceci donne l'inégalité

$$(p-1)(g-1) < \mathrm{card}(X(\mathbb{F}_{p^2})). \tag{6}$$

Toujours si X est hyperelliptique, on peut établir le théorème suivant :

Théorème 2.16 *Soit X une courbe hyperelliptique modulaire nouvelle de genre $g \geq 3$ et de niveau N. Si $\mathrm{Jac}(X)$ est un quotient de $J_0(N)$, alors $g \leq 10$. Si, de plus, 3 divise N, alors X égale la courbe $X_0(39)$ de genre 3.*

Pour ce théorème et ceux qui suivent, les conditions de divisibilité sur le niveau N sont essentiellement pour permettre de profiter de l'effet des involutions d'Atkin-Lehner sur les coefficients des formes différentielles qui nous intéressent, ou pour profiter des identités du lemme 2.6. Le lemme 2.12 aura bien sûr son utilité.

Preuve. Si 3 ne divise pas N, alors le lemme 2.12 implique $g < 11$. Supposons donc que 3 divise N, et que $\mathrm{Jac}(X)$ est un quotient de $J_0(N)$. Par le lemme de descente des morphismes, $X_1(N) \to X$ se factorise à travers $X_0(N) \to X$.

Soit $\{f^{(1)}, \ldots, f^{(g)}\}$ une base de formes primitives de $S_2(X)$, qu'on écrit sous la forme $f^{(j)} = 1 + \sum_{n\geq 2} a_n^{(j)} q^n$. Alors, on remarque que les $a_3^{(j)}$ ne peuvent pas être indépendants de j, sinon on aurait $\det((a_i^{(j)})_{1\leq i,j\leq g}) = 0$ et $\det((a_{2i-1}^{(j)})_{1\leq i,jg}) = 0$; ce n'est pas possible, car ce sont des matrices de changement de base. En effet :

Lemme 2.17 *Avec les mêmes notations, soit $P = \phi(\infty)$, où ϕ est la paramétrisation modulaire. Il existe une unique base $(h_1, \ldots, h_g)$ de $S_2(X)$ telle que pour tout $j \in [\![1, g]\!]$:*

$$h_j \equiv \begin{cases} q^j & \mod q^{g+1} \quad \textit{si } P \textit{ n'est pas un point de Weierstrass} \\ q^{2j-1} + \sum_{i=j}^{g-1} C_{j,2i} q^{2i} & \mod q^{g+1} \quad \textit{sinon.} \end{cases}$$

Preuve. On utilise le lemme 2.3 ; le fait que ϕ ne soit pas ramifiée en ∞, comme on l'a déjà justifié dans la preuve du théorème 2.7, permet d'effectivement utiliser les résultats du lemme, d'où l'existence d'une base de formes paraboliques $(h'_1, \ldots, h'_g)$ pour $S_2(X)$ qui satisfont

$$h'_j \equiv \begin{cases} q^j & \mod q^{j+1} \quad \text{si } P \text{ n'est pas un point de Weierstrass} \\ q^{2j-1} & \mod q^{j+1} \quad \text{sinon.} \end{cases}$$

Pour avoir précisément l'énoncé du lemme, il suffit d'utiliser le pivot de Gauss sur cette base. □

Bref, en particulier il existe au moins un j tel que $a_3^{(j)} \neq 0$, et par conséquent 9 ne divise pas N d'après le lemme 2.6. Par ce même lemme, $a_3^{(j)} \in \{-1, 1\}$. Alors, l'involution W_3 d'Atkin-Lehner est bien définie sur $X_0(N)$, et $f^{(j)}|W_3 = -a_3^{(j)} f^{(j)}$ pour tout j.

Posons $X' = X/\langle W_3 \rangle$, où W_3 est en fait l'automorphisme de X induit par W_3 sur $X_0(N)$, toujours grâce au lemme de descente des morphismes. X' est également modulaire nouvelle de niveau N, et $S_2(X')$ est engendrée par les $f^{(j)}$ tels que $a_3^{(j)} = -1$; en effet, si π est la surjection canonique $X \to X/\langle W_3 \rangle$ et $\phi : X_1(N) \to X$ la paramétrisation modulaire, alors

$$S_2(X') = \phi^*(\pi^*(H^0(X', \Omega))) = \phi^*(H^0(X, \Omega)^{\langle W_3 \rangle}).$$

Il y a au moins un tel $f^{(j)}$, sinon $a_3^{(j)} = 1$ pour tout j, et le lemme précédent prouve encore que ce n'est pas possible. On en déduit que X' est de genre au plus 2. De même, si $X'' = X/\langle wW_3 \rangle$, alors $S_2(X'')$ est engendré par les $f^{(j)}$ tels que $a_3^{(j)} = 1$, et encore une fois le genre de X'' est au plus 2. Or la somme de ces genres égale $g \geq 3$, donc au moins l'un de ces genres égale 2. Bref, X est hyperelliptique modulaire nouvelle, de genre 3 ou 4, et de même niveau qu'une certaine courbe modulaire nouvelle de genre 2. Or, l'ensemble des courbes modulaires nouvelles de genre 2 est fini et calculable (on peut trouver des tables dans [GJ&G] ou l'article que j'étudie, par exemple), et on déduit des tables que X est la courbe hyperelliptique d'équation affine

$$y^2 = (x^4 - 3x^3 - 4x^2 - 2x - 1)(x^4 + 5x^3 + 8x^2 + 6x + 3),$$

et c'est la seule courbe modulaire nouvelle de genre 3 et de niveau divisible par 3. Comme $X_0(39)$ vérifie ceci, on en déduit que $X = X_0(39)$. □

Je compte démontrer deux autres résultats de ce genre, où cette fois, ce sont les diviseurs premiers du niveau qui renseignent sur le genre, et je n'ai pas besoin de supposer que X est hyperelliptique :

Théorème 2.18 *Pour tout nombre premier p, l'ensemble des courbes modulaires nouvelles de genre au moins 2, dont la jacobienne est un quotient de $J_0(N)^{\mathrm{new}}$ avec $p|N$ est fini.*

Si la jacobienne d'une courbe modulaire nouvelle est un quotient de $J_0(N)^{\mathrm{new}}$, on dit que la courbe est de « caractère trivial », par analogie avec les formes primitives de caractère trivial qui sont en fait modulaires pour $\Gamma_0(N)$.

Théorème 2.19 *Soit X une courbe modulaire nouvelle de genre g au moins 2, de niveau N et de caractère trivial. Alors :*

(i) Si $2|N$, alors $g \leq 16$.

(ii) $4|N$ si, et seulement si X est hyperelliptique et $\pi(\infty)$ un point de Weierstrass.

(iii) Si $6|N$, alors $g \leq 5$.

(iv) Si $12|N$*, alors* $g = 2$*.*
(v) Si $18|N$*, alors* $g \leq 4$*.*
(vi) 36 ne divise pas N*.*

Pour commencer, je précise ce qu'on peut entendre par « caractère trivial ».

Lemme 2.20 *Soit* X *une courbe modulaire nouvelle de genre* $g \geq 2$*, et soit* $N \geq 1$ *un entier. Alors, les propositions suivantes sont équivalentes :*
(i) Il existe un morphisme $X_0(N) \to X$ *tel que* $S_2(X) \subseteq S_2(X_0(N))^{\mathrm{new}}$*.*
(ii) Il existe un morphisme $X_1(N) \to X$ *tel que* $S_2(X) \subseteq S_2(X_0(N))^{\mathrm{new}}$*.*
(iii) La jacobienne de X *est un quotient de* $J_0(N)^{\mathrm{new}}$*.*

Preuve. Montrons que $(iii) \Rightarrow (ii) \Rightarrow (i) \Rightarrow (iii)$. Comme X est modulaire nouvelle, il existe un entier M et un morphisme $\phi : X_1(M) \to X$ tel que $S_2(X) = \phi^*(H^0(X, \Omega)) \subseteq S_2(X_1(M)^{\mathrm{new}})$. Alors, $\mathrm{Jac}(X)$ est, par un raisonnement qu'on a déjà croisé, isogène à un produit de variétés abéliennes de la forme A_f où f est primitive de niveau M. Par hypothèse, $\mathrm{Jac}(X)$ est un quotient de $J_0(N)^{\mathrm{new}}$, donc également isogène à un produit de variétés abéliennes de la forme $A_{f'}$ où f' est primitive de niveau N et de caractère trivial. Par la proposition 4.1, $N = M$ et $S_2(X) \subseteq S_2(X_0(N))^{\mathrm{new}}$. Donc (iii) implique (ii).

(ii) implique (i) grâce au lemme 2.4, et (i) implique (iii) clairement (en comparant les H^0). □

Ceci étant dit, c'est le lemme suivant qui est à la base de la démonstration du théorème 2.18.

Lemme 2.21 *Soit* X *une courbe sur* k *de genre* $g > 0$ *et* q *un paramètre analytique local uniformisant en* $P \in X(k)$*. Écrivons* $\omega_1, \ldots, \omega_g \in H^0(X, \Omega)$ *sous la forme* $\omega_i = \left(1 + \sum_{j=2}^{\infty} a_j^{(i)} q^j\right) \frac{\mathrm{d}q}{q}$*. Soit* $m \geq 2$ *un entier, et supposons que* $a_m^{(i)} = a_m^{(i')}$ *pour tous* i*,* $i' \in [\![1, g]\!]$*. Alors il existe une fonction rationnelle de degré* m*, définie sur* k*, dont les seuls pôles sont en* P*.*

Preuve. Soit $l(D)$ la dimension de l'espace vectoriel $L(D)$ formé de 0 et de l'ensemble des fonctions rationnelles sur X dont le diviseur est supérieur ou égal à $-D$, et soit K un diviseur canonique sur X. Par hypothèse, si $\omega = \sum_{j=2}^{\infty} a_j q^j \frac{\mathrm{d}q}{q}$ est une combinaison linéaire des ω_i, alors $a_m = 0$, ce qui signifie qu'aucune différentielle régulière sur X ne s'annule exactement à l'ordre $m - 1$ en P. En d'autres termes, $l(K - (m-1)P) = l(K - mP)$, ce qui est équivalent à $l(mP) - l((m-1)P) = 1$ d'après le théorème de Riemann-Roch. Alors, tout $f \in L(mP) \setminus L((m-1)P)$ convient. □

Corollaire 2.22 *En conservant les mêmes notations que dans le lemme précédent, on a les résultats suivants :*
(i) Si $a_2^{(i)} = a_2^{(i')}$ *pour tous* $i, i' \in [\![1, g]\!]$*, alors soit* $g = 1$*, soit* X *est hyperelliptique et* P *un point de Weierstrass.*
(ii) Si $a_2^{(i)} = a_2^{(i')}$ *et* $a_3^{(i)} = a_3^{(i')}$ *pour tous* $i, i' \in [\![1, g]\!]$*, alors* $g = 1$*.*

(iii) Si $g \geq 2$ et si toute différentielle de $H^0(X, \Omega)$ s'annulant en P s'annule à l'ordre au moins r en P, alors $r \leq 2$, le cas d'égalité étant si, et seulement si X est hyperelliptique et P un point de Weierstrass.

Preuve. Si on démontre (i) et (ii), alors (iii) découle aussitôt. Le point (i) découle presque immédiatement du lemme : sous ces hypothèses, il existe une fonction rationnelle de degré 2, définie sur k, avec un pôle en P uniquement. Si le genre est supérieur à 2, cette fonction définit un morphisme $X \to \mathbb{P}^1$ de degré 2, donc X est hyperelliptique. Que P soit un point de Weierstrass découle également de cette fonction.

Il reste à prouver (ii). En répétant l'argument du lemme précédent, on obtient des fonctions rationnelles dans $L(2P) \setminus L(P)$ et $L(3P) \setminus L(2P)$, puis dans $L(mP) \setminus L((m-1)P)$ en faisant des produits des fonctions ici exhibées, car 2 et 3 sont premiers entre eux. Par récurrence, on obtient $l(mP) \geq m$ pour tout $m \geq 1$. Le théorème de Riemann-Roch, pour $m > 2g - 2$, donne $l(mP) = \deg(mP) - g + 1 < m$, sauf si $g = 1$, d'où le résultat. □

Proposition 2.23 *Soit X une courbe modulaire nouvelle de niveau N et de caractère trivial. Si p est un nombre premier divisant N, alors la $\mathbb{Q}$-gonalité de X est au plus p^2.*

Preuve. La valeur de a_{p^2} est la même pour chaque forme primitive $f \in \mathrm{New}_N$: il s'agit de 0 ou 1, selon que p^2 divise N ou non ; ceci découle facilement des formules de la proposition 2.6 et de l'identité formelle classique

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p (1 - a_p p^{-s} + \chi(p) p^{1-2s})^{-1},$$

dont on déduit $a_{p^2} = a_p^2$ ici.

Comme q sert de paramètre analytique uniformisant en l'image P de ∞ par $X_1(N) \to X$ comme dans la preuve du théorème 2.7, le lemme précédent s'applique, et la fonction rationnelle de degré p^2 exhibée ainsi donne le résultat voulu. □

Le théorème 2.18 en découle, en combinant la proposition précédente au théorème 2.10.

Preuve du théorème 2.19. Cette preuve nécessite de la concentration, parce qu'on navigue d'un point à l'autre de ce théorème sans cesse, et elle est relativement longue.

Encore une fois, $S_2(X)$ est engendré par des formes primitives pour $\Gamma_0(N)$, que je note $f_1, \ldots, f_g$.

Je commence par démontrer la condition nécessaire de (ii) : encore une fois, q sert de paramètre analytique uniformisant en $\phi(\infty)$. Si 4 divise N, alors $a_2(f_i) = 0$ pour tout i en utilisant le lemme 2.6. La courbe X est donc hyperelliptique

et P est un point de Weierstrass, par le corollaire 2.22. J'admets la réciproque pour plus de lisibilité : l'idée est que sous ces hypothèses, alors on peut montrer par le calcul que $a_{2n}(f^{(1)}) = 0$, pour tout n, et par contraposée, des relations du même acabit que celles du lemme 2.6 impliquent $v_2(N) \geq 2$.

Supposons que X n'est pas hyperelliptique, puisque dans le cas hyperelliptique on a d'ores et déjà $g \leq 10$. On peut supposer de plus que 4 ne divise pas N, puisqu'on vient de traiter le cas où 4 divise N. Alors, l'involution d'Atkin-Lehner W_2 existe sur X.

Soit $X' = X/\langle W_2 \rangle$, et soit P' l'image de P par la projection canonique $X \to X'$. Comme $f_i|W_2 = -a_2(f_i)f_i$, on a $a_2(f_i') = -1$ pour tout i, où les f_i' sont les formes paraboliques qui engendrent $S_2(X')$. Alors, si une différentielle régulière sur X' s'annule en P', elle s'annule au moins à l'ordre 2. Ceci prouve que X' est une courbe elliptique : si le genre de X' dépassait strictement 1, alors on pourrait utiliser le corollaire 2.22 pour prouver que X' est hyperelliptique et que P' est un point de Weierstrass, et le point (ii) du théorème 2.19 (qu'on a déjà prouvé) impliquerait que 4 divise N, alors qu'on a supposé le contraire. Si le genre de X' était 0, alors $X/\langle W_2 \rangle = \mathbb{P}^1$ montrerait que X est hyperelliptique, comme on le voit en annexe : c'est absurde. Bref, X est un revêtement de degré 2 de la courbe elliptique X'. La majoration du genre provient de l'inégalité (6) : si 3 ne divise pas N, alors :

$$(3-1)(g-1) < \mathrm{card}(X(\mathbb{F}_9)) \leq 2\mathrm{card}(X'(\mathbb{F}_9)) \leq 2(9+1+2\sqrt{9}) = 32,$$

donc $g \leq 16$. Si 3 divise N, alors en particulier 6 divise N, et on a juste à démontrer le point (iii) du théorème, que je démontre bientôt.

Pour démontrer (v), supposons que 18 divise N. D'après (i), X revêt une courbe elliptique X' avec un morphisme de degré 2. Comme 9 divise N, on a $a_3(f_i) = 0$ pour tout i, donc le lemme 2.21 montre qu'il existe un morphisme $X \to \mathbb{P}^1$ de degré 3. L'inégalité de Castelnuovo-Severi, qui s'énonce ainsi :

$$g \leq (d_1-1)(d_2-1) + d_1 g_1 + d_2 g_2$$

où les g_i et d_i sont respectivement les genres de courbes C_i et les degrés (premiers entre eux) de morphismes $C \to C_i$, permet de montrer que $g \leq 4$ si on l'applique aux morphismes $X \to X'$ et $X \to \mathbb{P}^1$. Cette inégalité est prouvée dans [Acc].

Prouvons à présent (iii), comme promis : la preuve déjà faite de (v) et tout ce qui précède permet de se restreindre au cas où $v_3(N) = 1$, $v_2(N) = 1$ et X non hyperelliptique. Comme avant, X revêt la courbe elliptique $X' = X/\langle W_2 \rangle$, avec un morphisme de degré 2.

Soit $w_j(f_i)$ la valeur propre de W_j pour les formes primitives f_i, avec $j \in \{2,3,6\}$, $i \in [\![1,g]\!]$. Comme à l'accoutumée, on a $w_2(f_i) = -a_2(f_i)$, $w_3(f_i) = -a_3(f_i)$, et $w_6(f_i) = a_6(f_i)$ par multiplicativité. Soit g_j le genre des $X/\langle W_j \rangle$. On a $g = \{i | w_j(f_i) = 1\}$. Comme $X/\langle W_2 \rangle$ est de genre 1, tous les $w_2(f_i)$ sont égaux à -1 sauf un, égal à 1. Soit f la forme primitive correspondante. L'identité $w_2 w_3 = w_6$, ainsi que le fait que les w_2 sont -1 pour toutes les formes sauf une, assurent que $g_3 + g_6$ égale soit $g-1$, soit $g+1$, selon que $f|W_3$ égale $-f$ ou f. Les deux cas sont à traiter séparément.

Si $f|W_3 = -f$, la courbe $X/\langle W_3\rangle$ ne peut pas être de genre au moins 2. Si tel était le cas, tous les w_2 de $S_2(X/\langle W_3\rangle)$ étant égaux à -1, et par le lemme 2.6 (ou plutôt, par contraposée de ce lemme), 4 diviserait N, or on a supposé le contraire. Donc $g_3 \leq 1$, et de meme $g_6 \leq 1$. Comme g_3+g_6 égale $g-1$, on a $g \leq 3$. Si $f|W_3 = f$, alors $g_3 \geq 1$. Comme $f|W_6 = f$, on a aussi $g_6 \geq 1$. Supposons d'abord que $g_3 = 1$. Alors $w_2(f_j) = w_3(f_j)$ pour tout j, donc il existe une fonction rationnelle sur X dans $L(3P) \setminus L(2P)$, en suivant la preuve du lemme 2.21. Tous les a_4 sont égaux à $+1$, toujours grâce au fait que $a_2 \in \{-1, 1\}$, il y a donc également une fonction dans $L(4P) \setminus L(3P)$. Ceci permet de trouver des fonctions dans $L(mP) \setminus L((m-1)P)$ pour tout $m \geq 6$ en faisant le produit de ces fonctions, si bien que les entiers pour lesquels $L(mP) = L((m-1)P)$ sont contenus dans $\{1, 2, 5\}$. Or, le théorème de Riemann-Roch permet de prouver que l'ensemble des entiers j pour lesquels $L(jP) = L((j-1)P)$ est de cardinal g, donc $g \leq 3$ (c'est ce qu'on appelle les *Weierstrass gap sequences*). Supposons à présent que $g_6 = 1$. Alors $w_2(f_j) = w_6(f_j)$ pour tout j, donc $w_3(f_j) = 1$ pour tout j. Le corollaire 2.22 assure l'existence d'une fonction dans $L(3P) \setminus L(2P)$, et on peut déduire de même que $g \leq 3$. Dans le cas général, on applique ce raisonnement à $X/\langle W_3\rangle$ au lieu de X, profitant du fait que $(X/\langle W_3\rangle)/\langle W_6\rangle$ est de genre 1 (sa seule forme primitive est f). On trouve dans ce cas $g_3 \leq 3$. De même, comme est de genre 1, on conclut que $g_6 \leq 3$. En bref, comme $g_3 + g_6 = g + 1$ dans ce cas, on a $g \leq 5$ comme voulu.

Il nous reste à prouver (vi) et (iv). Pour (vi), supposons que 36 divise N. Alors $a_2(f_i) = a_3(f_i) = 0$ pour tout i. Comme pour prouver (ii), il s'ensuit que toute différentielle sur X s'annule au moins à l'ordre 3 en P, ce qui contredit le corollaire 2.22. Pour prouver (iv), supposons que 12 divise N. Alors X est hyperelliptique, d'après (ii). Le théorème 2.16 montre que $g = 2$, comme convenu. Ouf! □

3 Comparaisons de cas

3.1 Différences avec le genre 1

Dans les sections précédentes, on a plusieurs fois eu besoin de supposer que le genre est supérieur à celui d'une courbe elliptique pour démontrer quelques résultats. Je vais essayer de voir dans quelle mesure les situations sont différentes dès qu'on passe à un genre supérieur.

Par exemple, on pourrait penser que le théorème 2.7 suffirait à avoir la finitude pour toutes les courbes modulaires, en imaginant que toute courbe modulaire est nouvelle à un certain niveau, comme dans le cas des courbes elliptiques qui sont modulaires nouvelles de niveau leur conducteur. Malheureusement, ce n'est pas le cas :

Proposition 3.1 *Il est faux de penser que les courbes modulaires de genre supérieur à 2 sont nouvelles à un certain niveau.*

Preuve. Il suffit de considérer $X = X_1(11^2)$.

Le genre de X est connu (et calculé dans [D&S], par exemple), et tout ce qui m'importe ici est que

$$0 < \underbrace{2g(X_1(11))}_{=\dim(J_1(11^2)_{\mathrm{old}})} < \underbrace{g(X_1(11^2))}_{=\dim(J_1(11^2))}.$$

La dimension de $J_1(11^2)_{\mathrm{old}}$ est justifiée par une étude de la décomposition en facteurs simples de $J_1(N)$: on a

$$J_1(N) \sim \bigoplus_{M|N} \bigoplus_{f \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\backslash \mathrm{New}_M} A_f^{\sigma_0(N/M)}, \tag{7}$$

et

$$J_1(N)^{\mathrm{new}} \sim \bigoplus_{f \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\backslash \mathrm{New}_N} A_f. \tag{8}$$

En examinant ces isogénies pour $N = 11$ et $N = 11^2$, on en déduit les formules de dimension ci-dessus (il faut se rappeler qu'il n'existe pas de forme primitive de poids 2 et de niveau 1). Bref, ce qui importe est que les jacobiennes en question ne sont pas triviales, et on peut donc utiliser la proposition 4.1 pour montrer que $J_1(11^2)^{\mathrm{new}}$ ne peut être quotient de $J_1(N)^{\mathrm{new}}$ que pour $N = 11^2$. Alors, X ne peut pas être nouvelle, car $J_1(11^2)_{\mathrm{old}}$ ne peut pas être quotient de $J_1(11^2)^{\mathrm{new}}$: il suffit de comparer leurs facteurs premiers, toujours à l'aide des isogénies ci-dessus. □

Il peut être intéressant de remarquer que même si $J_1(11^2)_{\mathrm{old}}$ ne peut pas être quotient de $J_1(11^2)^{\mathrm{new}}$, la dimension de $J_1(11^2)_{\mathrm{old}}$, qui égale 2, divise bien celle de $J_1(11^2)^{\mathrm{new}}$, qui égale 526 ; ce n'était donc pas suffisant pour conclure.

Voici d'autres propositions à l'encontre de l'intuition née du genre 1 :

Proposition 3.2 *Si X est une courbe modulaire, alors le plus petit niveau de X et le conducteur de $\mathrm{Jac}(X)$ n'ont pas nécessairement les mêmes diviseurs premiers.*

Pour une courbe elliptique, en revanche, c'est le cas, les différents travaux sur la modularité d'une courbe elliptique montrent que le plus petit niveau est le conducteur de E, or $E = \mathrm{Jac}(E)$.

Preuve de la proposition. Considérons $X = X_0(22)$. Alors le plus petit niveau pour lequel X est modulaire est évidemment $22 = 2{\cdot}11$. Par contre, le conducteur de $\mathrm{Jac}(X)$ est 11^2. □

Proposition 3.3 *Si $\mathrm{Jac}(X)$ est un quotient $\mathbb{Q}$-simple de $J_1(N)^{\mathrm{new}}$ et $X(\mathbb{Q}) \neq \emptyset$, alors X n'est pas nécessairement une courbe modulaire nouvelle de niveau N (il y a même une infinité de contre-exemples).*

Pour une courbe elliptique, si $\mathrm{Jac}(E)$ est un quotient $\mathbb{Q}$-simple de $J_1(N)^{\mathrm{new}}$, donc isogène à un certain A_f, alors il existe un morphisme $A_f \to E$, ce qui est

équivalent à la donnée d'un morphisme $J_1(N) \to E$, et donc à la modularité de E grâce au plongement d'Albanese $X_1(N) \to J_1(N)$, donné par $P \mapsto (P)-(\infty)$.

Ébauche de preuve de la proposition. Soit a un entier non nul, et X_a la courbe hyperelliptique de genre 2 d'équation affine $y^2 = x^5+ax^3-4x$. On a $X_a(\mathbb{Q}) \neq \emptyset$, car $(0,0) \in X_a(\mathbb{Q})$. On sait décrire le groupe $\mathrm{Aut}(X_a)$ (qui est isomorphe à D_8), et sa connaissance nous permet de prouver que $\mathrm{End}(\mathrm{Jac}(X_a))\otimes\mathbb{Q} = \mathbb{Q}(\sqrt{2})$, donc $\mathrm{Jac}(X_a)$ est $\mathbb{Q}$-simple. On vérifie à présent que cette jacobienne est un quotient de $J_1(N)$, donc nécessairement de $J_1(N)^{\mathrm{new}}$ grâce à sa simplicité : si u est un générateur bien choisi de $\mathrm{Aut}(X_a)$ et différent de l'involution hyperelliptique (en tant qu'automorphisme sur $\mathbb{Q}(i)$), alors $\mathrm{Jac}(X_a)$ est la restriction de Weil de la courbe elliptique $E_a = X_a/\langle u\rangle$, décrite par

$$y^2 = x^3 + 27(3a - 20i)x - 108(28 + 9ai)(1 - i).$$

En étudiant la représentation $\rho_{E_a,3}$ déduite de l'action du groupe de Galois absolu sur le $\mathbb{Q}_3$-module de Tate associé à E_a, on peut montrer que E_a est modulaire, donc $\mathrm{Jac}(X_a)$ également. Bref, $\mathrm{Jac}(X_a)$ est quotient de $J_1(N)^{\mathrm{new}}$ pour un certain N dépendant de a. Comme le j-invariant $j_a = \frac{64(3a-20i)^3(a-4i)}{(a^2+16)^2}$ est non constant, la famille des X_a n'est pas isotriviale. Alors, par le théorème 2.7, il n'y a qu'un nombre fini de X_a qui sont modulaires nouvelles. □

3.2 Domination par les courbes de Fermat

Il existe un analogue de notre conjecture pour les courbes de Fermat, la N-ième courbe de Fermat X_N (sur k) étant la courbe lisse d'équation homogène $x^N + y^N = z^N$ dans le plan projectif. Alors, on sait prouver que la conjecture est vraie en remplaçant les $X_1(N)$ par les X_N :

Théorème 3.4 *Pour tout corps k et tout entier $g \geq 2$, l'ensemble des courbes sur k de genre g dominées par un certain X_N (pour $N \geq 1$) est fini.*

La clé de la preuve réside dans le fait qu'ici, on sait lier le genre de la courbe dominée et un « niveau » de la courbe. Par niveau, j'entends un entier N tel que X_N paramètre X. Alors, grâce au théorème de Franchis-Severi (théorème 2.9), on arrive à conclure. Je vais considérer $k = \mathbb{C}$ uniquement, dont la validité du prochain lemme dépend, et qui permet d'écrire $\mathrm{Jac}(X) = H^0(X,\Omega)^*/H_1(X,\mathbb{Z})$.

Pour cette preuve, j'introduis quelques notations d'usage qui ne sont pas sans rappeler le cadre modulaire : soit J_N la jacobienne de X_N, et je définis $J_{N,\mathrm{old}}$ comme la somme des images des morphismes $J_M \to J_N$ induits par les $\begin{cases} X_N & \to & X_M \\ [x,y,z] & \mapsto & [x^{N/M}, y^{N/M}, z^{N/M}] \end{cases}$ où $M|N$ et $d|\frac{N}{M}$, et je pose $J_N^{\mathrm{new}} = J_N/J_{N,\mathrm{old}}$. Il est possible de voir X_M comme le quotient de X_N par un certain sous-groupe d'automorphismes stable par $\mathrm{Gal}(\bar{k}/k)$, et on note ce sous-groupe $\Gamma_{N,M}$.

Preuve du théorème 3.4. Lier le niveau au genre nécessite un lemme :

Lemme 3.5 *Si $N > 180$, alors tout quotient k-simple de J_N^{new} est de dimension au moins $\varphi(N)/8$, où φ est l'indicatrice d'Euler.*

Preuve. D'après [Aok], J_N^{new} est isogène à un produit (fini) de variétés abéliennes A_S de dimension $\varphi(N)/2$. Ce même article montre que si N n'est pas dans une certaine partie de $\mathbb{N}$ majorée par 180, alors pour tout S : $A_S = B_S^{W_S}$, où B_S est une variété abélienne simple, et $W_S \leq 4$. C'est pourquoi la dimension est au moins $\frac{\varphi(N)/2}{4}$. $\square$

D'où, comme je l'annonçais :

Lemme 3.6 *Il existe une fonction $g \mapsto M(g)$ telle que pour toute courbe X de genre $g \geq 2$ sur k dominée par X_N pour $N \geq 1$, alors X est également dominée par $X_{M'}$ pour un certain $M' \leq M(g)$.*

Preuve. On considère $m > 180$ tel que $\varphi(n) > 8g$ pour tout $n > m$; c'est possible car $\varphi(n) \to \infty$ quand $n \to \infty$. Posons $M = m!$, et supposons que X soit une courbe telle que décrite dans le lemme. Il suffit alors de prendre $M' = M \wedge N$: par le lemme précédent, la composition $\text{Jac}(X) \to J_N \to J_{m'}^{\text{new}}$ est triviale dès que $m'|N$ et $m' \geq m$, donc l'image de $\text{Jac}(X) \to J_N$ est contenue dans une sous-variété abélienne de J_N isogène à $\prod_{m'|N, m' \leq m} J_{m'}^{\text{new}}$, elle-même contenue dans l'image de $J_{M'} \to J_N$. Le lemme 2.4 s'applique ici, l'hypothèse se vérifiant à l'aide des isomorphismes $H^0(\text{Jac}(X), \Omega) = H^0(X, \Omega)$ et $T_0(\text{Jac}(X)) = H^0(X, \Omega)$ décrits dans [H&S] (page 117), et on en déduit que le morphisme $X_N \to X$ se factorise à travers $X_{M'}$. $\square$

Revenons à la preuve du théorème : il n'y a plus qu'à appliquer le théorème de de Franchis-Severi à $X_{M'}$ où $M' \leq M(g)$ pour obtenir une liste finie de courbes dominées par les courbes de Fermat sur k, et on est certain de contenir toutes celles de genre g. $\square$

4 Annexe : résultats «classiques»

Proposition 4.1 *Soient f et f' deux formes primitives de niveaux respectifs N et N'. Alors, $A_f \overset{\mathbb{Q}}{\sim} A_{f'}$ si, et seulement si $N = N'$ et $f = f'^{\tau}$ pour $\tau \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.*

Preuve. Si $f = f'^{\tau}$ (et donc $N = N'$), il est clair que $A_f \overset{\mathbb{Q}}{\sim} A_{f'}$ par construction de A_f ; en fait, on a même une bijection

$$\begin{array}{ccc} \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\backslash \text{New}_N & \to & \{\mathbb{Q}\text{-quotients simples de } J_1(N)^{\text{new}}\}/\mathbb{Q}\text{-isogénie} \\ f & \mapsto & A_f \end{array} .$$

Réciproquement, supposons que A_f (à isogénie près) détermine f (à conjugaison près). Soit l un nombre premier, et $V_f = \varprojlim_n A_f[l^n]$ le $\mathbb{Q}_l$-module de Tate associé à A_f ; je note $\bar{V_f}$ le $\bar{\mathbb{Q}}_l$-module obtenu par extension des scalaires. On sait, grâce à [Rib], que

$$\bar{V_f} = \oplus_\sigma V_{f,\sigma},$$

où les $V_{f,\sigma}$ sont des $\bar{\mathbb{Q}}_l[\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$-modules irréductibles indexés par les plongements $\sigma : \mathbb{Q}_f \hookrightarrow \bar{\mathbb{Q}}_l$. Pour $p \not| lN$, la trace de Frob_p sur $V_{f,\sigma}$ égale $\sigma(a_p)$.

Si f' est une autre forme primitive telle que $A_f \overset{\mathbb{Q}}{\sim} A_{f'}$, alors $V_f \simeq V_{f'}$ et $\bar{V_f} \simeq \bar{V_{f'}}$. Le module $V_{f,\sigma}$ est, par conséquent, isomorphe à une des composantes irréductibles $V_{f',\sigma'}$, donc $\sigma(a_p) = \sigma'(a'_p)$ en considérant la trace du Frobenius, et ce pour presque tout p. Bref, comme les deux formes sont primitives, $f = f'^{\sigma^{-1}\sigma'}$, d'où le résultat. □

Définition 4.2 (Courbe hyperelliptique) *Une courbe X est dite hyperelliptique si son genre est supérieur à 2, et s'il existe un morphisme fini $X \to \mathbb{P}^1$ de degré 2.*

Il est intéressant de remarquer que toutes les courbes de genre 2 sont hyperelliptiques : en effet, le diviseur canonique définit un système linéaire complet de degré 2 et de dimension 1, sans points de base.

Une courbe hyperelliptique X a pour image dans $\mathbb{P}^2$ une courbe d'équation affine $y^2 = f(x)$, où f est un polynôme séparable de degré $2g+1$ ou $2g+2$. Pour voir ceci, on peut par exemple se rappeler que si $\pi : X \to \mathbb{P}^1$ est de degré 2, alors $[K(X) : K(\mathbb{P}^1)] = 2$, or $K(\mathbb{P}^1) = k(x)$, une extension purement transcendante de k. De l'algèbre élémentaire conduit alors, du moins si $\mathrm{car}(k) \neq 2$, à $K(X) = k(x,y)$ avec $y^2 = f(x)$, où f est sans facteur carré. La formule de Riemann-Hurwitz appliquée à $(x,y) \mapsto x$ fournit :

$$2g - 2 = -4 + \sum_{P \in X} (e_P - 1),$$

ou encore : $2g+2 = \sum_{P\in X}(e_P - 1)$. Les points de branchement sont les racines de f et éventuellement l'infini, selon que f soit de degré impair ou non. Bref, $\sum_{P\in X} e_P = \deg(f)$ ou $\deg(f)+1$, d'où le résultat.

Proposition 4.3 *Soit X une courbe hyperelliptique. Tout automorphisme de X induit un automorphisme de $\mathbb{P}^1$.*

Preuve. Je rappelle qu'un résultat de [Har] (page 343) assure qu'il n'existe qu'un seul morphisme $f : X \to \mathbb{P}^1$ de degré 2 pour une courbe hyperelliptique. À ce morphisme de degré 2, on peut naturellement associer une involution w de X (et réciproquement, une involution de X définit un morphisme de degré 2), définie par $w(z) = z'$ où $z' \in f^{-1}(\{f(z)\})$, et $z' \neq z$ si z n'est pas un point de branchement ; on l'appelle involution hyperelliptique. La formule de Riemann-Hurwitz appliquée à la projection canonique $X \to X/\langle w\rangle$ montre que $X/\langle w\rangle$ est de genre nul (on vérifie facilement que la ramification de ce morphisme est la même que pour f, ce qui donne $\sum_P (e_P - 1) = 2g+2$; le reste en découle), et isomorphe à $\mathbb{P}^1$. Par unicité du morphisme $X \to \mathbb{P}^1$ de degré 2, l'involution hyperelliptique est la seule à vérifier ceci.

À présent, si g est un automorphisme de X, alors $f \circ g : X \to \mathbb{P}^1$ est de degré 2, donc $f \circ g = f$ par unicité, ce qui signifie que g permute les points de ramification de f. Donc gwg^{-1} est encore une involution qui laisse fixe les points de ramification de $X \to \mathbb{P}^1$. Cette approche permet de voir, comme

précédemment, que $X/\langle gwg^{-1}\rangle = \mathbb{P}^1$, et donc que $wg = gw$ par unicité de w. Bref, g commute avec w, donc laisse stable les orbites de $X/\langle w\rangle$ et induit un automorphisme de $X/\langle w\rangle = \mathbb{P}^1$. $\square$

Références

[A&U] Ahmed Abbes and Emmanuel Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. 103 (1996), no. 3, 269–286.

[Abr] Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices, (20) :1005-1011, 1996.

[Acc] Robert D. M. Accola, *Topics in the theory of Riemann surfaces*. Springer-Verlag, Berlin, 1994.

[ACGH] E. Arbarello, M. Cornalba, P. A. Griffiths et J. Harris, *Geometry of algebraic curves, Vol. I.*, Springer-Verlag, New York, 1985.

[Aok] Noboru Aoki, *Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves.*, Amer. J. Math, 113(5) :779–833, 1991.

[A&L] A. O. L. Atkin et Wen Ch'ing Winnie Li, *Twists of newforms and pseudo-eigenvalues of W-operators*, Invent. Math., 48(3) :221–243, 1978.

[BGJGP] Matthew H. Baker, Enrique GonzÍez-Jiménez, Josep González, and Björn Poonen, *Finiteness results for modular curves of genus at least 2*, Amer. J. Math. 127 (2005), no. 6, 1325–1387.

[D&S] Fred Diamond et Jerry Shurman, *A first course in modular forms*, 436 pages, Springer-Verlag, 2007.

[Edx] Bas Edixhoven, *Modular parametrizations at primes of bad reduction*, en préparation.

[GJ&G] Enrique González-Jiménez et Josep González, *Modular curves of genus 2*, `http://arxiv.org/PS_cache/math/pdf/0105/0105232v1.pdf`.

[Gol] David Goldschmidt, *Algebraic functions and projective curves*, Springer-Verlag, 2002.

[Har] Robin Hartshorne, *Algebraic Geometry*, 512 pages, Springer-Verlag, 1977.

[Hd1] Marc Hindry, *Arithmétique*, 327 pages, Calvage & Mounet, 2008.

[H&L] Jeffrey Hoffstein et Paul Lockhart, *Coefficients of Maass forms and the Siegel zero*, Annals of Math., (2) 140 (1994), no. 1, pp. 161–181.

[H&S] Marc Hindry et Joseph Silverman, *Diophantine geometry : an introduction*, Springer, 558 pages, 2000.

[Li] Wen Ch'ing Winnie Li, *Newforms and functional equations*, Math. Ann., 212 :285–315, 1975.

[L&L] Qing Liu et Dino Lorenzini, *Models of curves and finite covers*, Compositio Math., 118(1) :61–102, 1999.

[Maz] Barry Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. 44 (1978), no. 2, 129–162.

[M&M] Liem Mai et Ram Murty, *The Phragmén-Lindelöf Theorem and Modular Elliptic Curves*, Contemporary Math., 166 (1994), pp. 335–340.

[Mur] Ram Murty, *Bounds for congruence primes*, in Automorphic forms, automorphic representations, and arithmetic (ed. Doran et al.), American Mathematical Society, Proc. Symp. Pure Math. 66, 1999, 177–182.

[Rib] Kenneth A. Ribet, *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann., 253(1) :43–62, 1980.

[Sik] Samir Siksek, *Diophantine equations after Fermat's last theorem.*

[Sil] Joseph Silverman, *The arithmetic of elliptic curves*, Springer-Verlag New York Inc., 514 pages, 2009.

[S&Y] C. L. Stewart et Kunrui Yu, *On the conjecture abc, II.*

[Wat] Mark Watkins, *Explicit lower bounds on the modular degree of an elliptic curve.*

[Win] Bruno Winckler, *Recueil de blagues mathématiques et autres curiosités*, 115 pages, 2008.

[Win2] Bruno Winckler, *Les courbes elliptiques ; théorème de Mordell-Weil*, 40 pages, 2009.

[Win3] Bruno Winckler, *Paramétrisation modulaire pour les courbes de genre supérieur à 2*, 31 pages, 2010.

[Wit] Olivier Wittenberg, *Variétés abéliennes sur les corps finis : théorème de Tate et classification de Honda-Tate*, 11 pages, 2001.