Courbes elliptiques, représentations galoisiennes et l'équation $x^2 + y^3 = z^5$

par

Steve Thiboutot

Novembre 1996

Département de Mathématiques et Statistiques

Université McGill, Montréal

Canada

Mémoire présenté à la Faculté des Études Supérieures de l'Université McGill pour l'obtention du grade de maître ès sciences (M.Sc.)

©Steve Thiboutot, 1996

Remerciements

Ce mémoire n'aurait jamais vu le jour sans les idées de mon directeur de recherche, M. Henri Darmon. Ses nombreux conseils et explications, ainsi que son support m'ont été indispensables et j'aimerais le remercier sincèrement. Les travaux antérieurs de M. Frits Beukers ont été essentiels et je le remecie grandement pour m'avoir calculé les polynômes qu'on retrouve dans l'appendice A. Je tiens aussi à exprimer ma reconnaissance envers M. Karl Rubin pour m'avoir donné une copie du fichier contenant les polynômes de l'appendice B. Le support financier du Conseil de recherches en sciences naturelles et en génie du Canada m'a permis de me concentrer sur mon projet et je les remercie grandement.

Merci enfin à ma conjointe, Julie, pour qui j'exprime toute ma gratitude et, de façon générale, à tous mes parents et amis, dont le support m'a été essentiel au cours de l'élaboration de ce travail.

Résumé

L'équation diophantienne

$$x^2 + y^3 = z^5 \tag{1}$$

admet un nombre infini de solutions entières avec $\text{pgcd}(x, y, z) = 1$. Appelons (F, G, H) une *famille paramétrée de solutions* de (1) si F, G et H sont des polynômes homogènes non nuls appartenant à $\mathbf{Q}[s, t]$ satisfaisant $\text{pgcd}(F, G, H) = 1$ et $F(s, t)^2 + G(s, t)^3 = H(s, t)^5$ pour tout s, t appartenant à $\mathbf{Z}$. Les solutions entières de (1) s'écrivent comme une union disjointe de familles paramétrées de solutions. Un théorème de Beukers nous dit que ce nombre N de familles paramétrées de solutions est fini. Cependant, seul quelques familles paramétrées de solutions de (1) sont connues. En établissant un lien entre les représentations galoisiennes mod 5 provenant de certaines courbes elliptiques et les familles paramétrées de solutions de (1), on construit de nouvelles familles paramétrées de solutions et on indique une méthode pour établir une borne supérieure pour N.

Abstract

The diophantine equation

$$x^2 + y^3 = z^5 \tag{1}$$

has an infinite number of integer solutions with $\gcd(x, y, z) = 1$. Call (F, G, H) a *parametrised solutions* of (1) if F, G, and H are non-trivial homogeneous polynomials in $\mathbf{Q}[s, t]$ with $\gcd(F, G, H) = 1$ and $F(s, t)^2 + G(s, t)^3 = H(s, t)^5$ for all s, $t \in \mathbf{Z}$. The integer solutions of (1) may be written as a disjoint union of parametrised solutions. A theorem of Beukers states that the number N of such parametrised solutions is finite. However, only few parametrised solutions of (1) are known. Establishing a link between the mod 5 Galois representations coming from some elliptic curves and the parametrised solutions of (1), we find new parametrised solutions and indicate a way to find a bound for N.

Tables des matières

Remerciements ii

Résumé iii

Abstract iv

1 Introduction 2

2 Préliminaires 4

2.1 Courbes elliptiques 4

2.2 Formes modulaires 15

2.3 La Conjecture de Shimura-Taniyama 19

2.4 Représentations galoisiennes 21

2.5 Théorème de Ribet et Dernier Théorème de Fermat 30

3 L'équation $x^2 + y^3 = z^5$ 33

3.1 Les travaux de Beukers sur l'équation $x^2 + y^3 = z^5$ 33

3.2 Lien entre familles paramétrées de solutions de $x^2 + y^3 = z^5$ et représentations galoisiennes 37

3.3 Construction de familles paramétrées de solutions 41

3.4 Liste des familles paramétrées de solutions 48

3.5 Borne supérieure pour le nombre de familles paramétrées de solutions 51

Appendice A 60

Appendice B **62**

Bibliographie **66**

Chapitre 1

Introduction

Soient p, q, $r \in \mathbf{Z}_{\geq 2}$ et A, B, $C \in \mathbf{Z}$, $ABC \neq 0$. Considérons l'équation diophantienne

$$Ax^p + By^q + Cz^r = 0, \tag{1.1}$$

où x, y, $z \in \mathbf{Z}$ sont des inconnus satisfaisant $\text{pgcd}(x, y, z) = 1$ et $xyz \neq 0$. Un tel triplet d'entiers (x, y, z) sera appelé une solution primitive de l'équation (1.1).

On distingue trois cas pour l'équation (1.1): le cas *hyperbolique*, le cas *euclidien* et le cas *sphérique*.

Le cas *hyperbolique* survient lorsque $1/p+1/q+1/r < 1$. Dans ce cas, en utilisant le théorème de Faltings, Darmon et Granville [DG] ont montré que l'équation (1.1) admet un nombre fini de solutions primitives.

Lorsque $1/p + 1/q + 1/r = 1$, le cas *euclidien*, on peut énumérer les triplets $\{p, q, r\}$ possibles: $\{3, 3, 3\}$, $\{2, 4, 4\}$ et $\{2, 3, 6\}$. Dans ce cas, les solutions primitives de l'équation (1.1) correspondent aux points rationnels de certaines courbes elliptiques.

Quant au cas *sphérique*, $1/p + 1/q + 1/r > 1$, les triplets $\{p, q, r\}$ sont $\{2, 2, k\}$ avec $k \geq 2$, $\{2, 3, 3\}$, $\{2, 3, 4\}$ et $\{2, 3, 5\}$. Dans ce cas, un nouveau phénomène se produit dans l'étude des solutions primitives de l'équation (1.1): celui des familles paramétrées de solutions. On appelle famille paramétrée la donnée d'un triplet (F, G, H), où F, G, $H \in \mathbf{Q}[X, Y]$ sont trois polynômes homogènes non nuls avec

$\mathrm{pgcd}(F,G,H)=1$ tels que $AF(s,t)^p+BG(s,t)^q+CH(s,t)^r=0$ pour tout $(s,t)\in \mathbf{Z}^2$.

Beukers [Be] démontre le théorème suivant:

Théorème 1 *Considérons l'équation (1.1) dans le cas sphérique.*

a) Si l'équation (1.1) admet une solution, alors elle en admet une infinité.

b) Il existe un nombre fini de familles paramétrées de solutions tel que chaque solution de l'équation (1.1) peut être obtenue à partir de l'une d'elles par spécialisation en des valeurs entières.

Dans ce présent travail, on traite un cas particulier du cas *sphérique*. Fixons $p=2$, $q=3$, $r=5$, $A=B=1$ et $C=-1$. On a alors $1/p+1/q+1/r=31/30>1$. Puisque l'équation

$$x^2+y^3=z^5$$

admet au moins une solution (on peut prendre $(x,y,z)=(3,-2,1)$), par le théorème 1, elle en admet une infinité. De plus, ses solutions primitives sont engendrées par un nombre fini de familles paramétrées de solutions. Par contre, la démonstration de Beukers n'indique pas de méthode pour compter de telles familles paramétrées de solutions. Une question naturelle qu'on peut se poser est de savoir combien de familles paramétrées de solutions, à une certaine équivalence près, possède l'équation $x^2+y^3=z^5$. En établissant un lien entre les familles paramétrées de solutions de cette équation et les représentations du groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ dans $\mathbf{GL}_2(\mathbf{F}_5)$, on construit de nouvelles familles paramétrées de solutions pour l'équation $x^2+y^3=z^5$, non parues dans l'article de Beukers [Be], et on indique une méthode pour trouver une borne supérieure pour ce nombre de familles.

Chapitre 2

Préliminaires

2.1 Courbes elliptiques

Une courbe elliptique E (définie sur un corps k), notée E/k, est une courbe projective non singulière de genre 1 qui possède un point k-rationnel $\mathcal{O}$. On montre, plus concrètement, que toute courbe elliptique E/k est donnée par une équation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \ ,$$

où $(a_1, a_2, a_3, a_4, a_6)$ appartient à k^5 (cf. [Si1], Chap. III, prop. 3.1). Il est bon de remarquer que les coefficients a_i ne sont pas uniques et il existe une infinité de quintuplets $(a_1, a_2, a_3, a_4, a_6)$ dans k^5 définissant une même courbe E/k. La courbe donnée par l'équation ci-haut intersecte toujours la droite à l'infini en un point unique qu'on prend pour définir notre point rationnel ($\mathcal{O} = [0, 1, 0]$). Cette équation est le modèle (ou équation) de Weierstrass associé à E. Pour faciliter la notation, on utilise les coordonnées non homogènes, $x = X/Z$ et $y = Y/Z$. Avec ces nouvelles coordonnées, la courbe E s'écrit

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

tout en n'oubliant pas le point supplémentaire "à l'infini" $\mathcal{O} = [0, 1, 0]$.

L'intérêt des courbes elliptiques vient du fait qu'elles sont munies d'une structure de groupe commutatif, où $\mathcal{O}$ joue le rôle de l'élément neutre pour l'addition. En

d'autres mots, on dit que les courbes elliptiques sont des variétés abéliennes de dimension un. Pour chaque corps K, on définit $E(K)$, l'ensemble des points de E définis sur K. Ainsi, pour une même courbe elliptique E, on obtient généralement différents groupes $E(K)$ pour différentes extensions K de k.

L'opération qui définit la structure de groupe sur $E(k)$ est communément appelée "chord and tangent operation". Lorsque E/k est donnée par un modèle de Weierstrass, un point P de $E(k)$ est donné par un couple (x, y) défini sur k qui satisfait l'équation. Trois points distincts de $E(k)$ s'additionnent pour donner $\mathcal{O}$ si et seulement s'ils sont colinéaires. L'addition entre deux points de $E(k)$ peut être décrite par deux quotients de polynômes à coefficients dans k donnant les coefficients x et y du point résultant.

Exemple 2 Soit $E : y^2 = x^3 - 4x^2 + 16$. On peut montrer que $E(\mathbf{Q})$ possède seulement 5 points $\{\mathcal{O}, (0, \pm 4), (4, \pm 4)\}$. Cependant, sur l'extension $\mathbf{Q}(\sqrt{-2})$ de $\mathbf{Q}$, $E(\mathbf{Q}(\sqrt{-2}))$ contient aussi le point $P = (8 + 4\sqrt{-2}, 12 + 16\sqrt{-2})$. On démontre que P est un point d'ordre infini et donc $E(\mathbf{Q}(\sqrt{-2}))$ contient un nombre infini de points. Remarquez comment le corps K peut modifier la structure de groupe de $E(K)$.

Dans le reste de cette section, on explique brièvement quelques concepts reliés aux courbes elliptiques. À partir de maintenant, on suppose que nos courbes elliptiques sont définies sur $\mathbf{Q}$ bien que la majorité des concepts restent valides sur des corps plus généraux.

Morphismes: Il existe différents types de morphismes entre courbes elliptiques. Étant donné qu'une telle courbe est toujours munie d'un point rationnel particulier, il est naturel de regarder d'abord les morphismes respectant cette propriété.

Définition 3 *Soient E et E' des courbes elliptiques. Une isogénie entre E et E' est un morphisme non nul*

$$\phi : E \longrightarrow E'$$

satisfaisant $\phi(\mathcal{O}) = \mathcal{O}'$. Les courbes E et E' sont dites isogènes, s'il existe une isogénie entre elles.

Exemple 4 Soit E une courbe elliptique. Pour chaque $m \in \mathbf{Z} \setminus \{0\}$, l'application *multiplication par* m

$$[m] : E \longrightarrow E$$

est une isogénie. Si $m > 0$, alors

$$[m](P) = \underbrace{P + P \cdots + P}_{m \text{ fois}};$$

si $m < 0$, alors $[m](P) = [-m](-P)$.

Remarque 5 L'application *multiplication par* m est aussi un homomorphisme de groupes. Ceci est une propriété générale des isogénies: toute isogénie est un homomorphisme de groupe (cf. [Si1], Chap. III, thm. 4.8).

Puisque les courbes elliptiques ont une structure de groupe, on peut définir l'endomorphisme de E donné par la translation par un point donné.

Définition 6 *Soit* $E/\mathbf{Q}$ *une courbe elliptique et* $Q \in E(\mathbf{Q})$. *L'application translation par* Q *se définit par*

$$\begin{array}{rccc} \tau_Q : & E & \longrightarrow & E \\ & P & \longmapsto & P + Q. \end{array}$$

L'application τ_Q est clairement un automorphisme de E car τ_{-Q} constitue son inverse mais elle n'est pas une isogénie sauf pour $Q = \mathcal{O}$.

Soit maintenant

$$\varphi : E \longrightarrow E'$$

un morphisme quelconque entre les courbes elliptiques E et E'. Alors, l'application

$$\phi = \tau_{-\varphi(\mathcal{O})} \circ \varphi$$

est une isogénie entre E et E' car $\phi(\mathcal{O}) = \mathcal{O}'$. Le morphisme φ peut donc s'écrire

$$\varphi = \tau_{\varphi(\mathcal{O})} \circ \phi$$

et donc tout morphisme non-nul entre courbes elliptiques est une composition d'une isogénie et d'une translation.

Discriminant et j-invariant: On attache quelques quantités à une courbe elliptique E. La non singularité d'une courbe elliptique E est détectée par la valeur non nulle du *discriminant* Δ de E. Si la courbe E est donnée par une équation de Weierstrass, le discriminant de ce modèle est donné par un polynôme en a_i, qu'on peut retrouver par exemple dans [Si1] (cf. Chap. III, §1).

Si la courbe E est donnée sous la forme $y^2 = f(x)$, où

$$f(x) = x^3 + ax^2 + bx + c,$$

alors le discriminant de ce modèle est précisement $\Delta = 16 \cdot Disc(f)$, où $Disc(f)$ est le discriminant de f. On rappelle que le discriminant de

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = (x - \alpha_1) \cdots (x - \alpha_n)$$

est défini par

$$Disc(f) = \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j)^2.$$

On remarque que l'équation $y^2 = f(x)$ est non-singulière (et donc définit une courbe elliptique) si et seulement si $f(x)$ n'admet pas de zéro multiple.

On note que le discriminant d'une courbe elliptique E dépend de son modèle. Parmis toutes les équations de $E/\mathbf{Q}$ ayant des coefficients entiers, il en existe une qu'on appelle équation minimale; cette équation donne lieu au plus petit discriminant entier possible. Ce discriminant est appelé *discriminant minimal* de E et noté Δ_{min}.

Exemple 7 Soient A, B, C trois entiers non nuls, premiers entre eux deux à deux, et tels que

$$A + B + C = 0.$$

Considérons la *courbe de Frey* $E_{A,B}$ d'équation

$$y^2 = x(x - A)(x + B).$$

Le discriminant de $x(x-A)(x+B)$ est $(AB(A+B))^2 = (ABC)^2$ et le discriminant de la courbe $E_{A,B}$ est donc $\Delta = 2^4 \cdot (ABC)^2$. Si de plus, $A \equiv -1 \pmod 4$ et $B \equiv 0$

(mod 32), on montre que

$$y^2 + xy = x^3 + \frac{B - A - 1}{4}x^2 - \frac{AB}{16}x$$

est une équation minimale de la courbe $E_{A,B}$ et son discriminant (minimal) correspondant est

$$\Delta_{\min} = \frac{(ABC)^2}{2^8}$$

(cf. [Se4], section 4.2).

Exemple 8 Soit (a, b, c) une solution primitive de $x^2 + y^3 = z^5$ et considérons la courbe elliptique

$$E : y^2 = x^3 + 27bx - 54a.$$

On a $Disc(f) = -2^2 3^9 (a^2 + b^3)$, où $f(x) = x^3 + 27bx - 54a$. Le discriminant de l'équation ci-dessus est donc $\Delta = -2^6 3^9 c^5$.

Remarque 9 Soient $E/\mathbf{Q}$ une courbe elliptique donnée par une équation de Weierstrass, Δ son discriminant et $ord_p(\Delta)$ l'exposant de p qui apparaît dans la décomposition de Δ en produit de facteurs premiers. On dit que le modèle de la courbe elliptique E est minimal en un premier p, si $ord_p(\Delta)$ est minimal sous la condition que les a_i $(i = 1, \ldots, 4, 6)$ sont dans $\mathbf{Z}$. Étant donné que $\text{pgcd}(A, B, C) = 1$, on peut montrer que la courbe E de l'exemple précédent est minimale en p, pour tout $p > 3$. Ainsi, le discriminant minimal de la courbe E de l'exemple 8 est toujours de la forme $\Delta_{min} = \pm 2^s 3^t p_1^5 \cdots p_k^5$, où $\{p_1, \ldots, p_k\}$ sont les diviseurs premiers de c différents de 2 et 3.

Si $E/\mathbf{Q}$ est une courbe elliptique donnée par une équation de Weierstrass, le *j-invariant* de la courbe E, noté $j(E)$ ou simplement j, est défini par un quotient de polynômes en a_i, qu'on peut trouver par exemple dans [Si1], Chap. III, §1. Le j-invariant d'une courbe elliptique E ne dépend pas du choix du quintuplet $(a_1, a_2, a_3, a_4, a_6)$ pour définir la courbe E. Ainsi, deux courbes elliptiques définies sur $\mathbf{Q}$ isomorphes sur $\overline{\mathbf{Q}}$ ont le même j-invariant. Réciproquement, deux courbes elliptiques sur $\mathbf{Q}$ ayant le même j-invariant sont isomorphes sur $\overline{\mathbf{Q}}$ (cf. [Si1], Chap. III, prop. 1.4).

Exemple 10 Lorsque la courbe E est donnée par

$$y^2 = x^3 + ax + b,$$

le j-invariant de la courbe E est donné par

$$j = \frac{4 \cdot (12a)^3}{(4a^3 + 27b^2)}.$$

Ainsi, si $A^2 + B^3 = C^5$, la courbe E de l'exemple 8 a pour j-invariant

$$j = \frac{1728B^3}{C^5}.$$

Réduction modulo p: Étant donné une courbe elliptique $E/\mathbf{Q}$, donnée par une équation minimale, et un nombre premier p, il est possible de réduire cette équation modulo p et d'obtenir une équation définie sur le corps fini $\mathbf{F}_p$. Si cette équation définit une courbe elliptique $\widetilde{E_p}$ sur $\mathbf{F}_p$, alors on dit que p est un nombre premier de *bonne réduction*, contrairement aux autres nombres premiers qu'on appelle ceux de *mauvaise réduction*. Les nombres premiers de mauvaise réduction d'une courbe elliptique $E/\mathbf{Q}$ sont précisement ceux qui divisent le discriminant minimal Δ_{min} de E; pour un tel p, la courbe $\widetilde{E_p}$ a un point singulier.

On répartit les nombres premiers de mauvaise réduction en deux catégories: ceux ayant réduction *multiplicative* et les autres ayant réduction *additive*. On dit qu'une courbe elliptique $E/\mathbf{Q}$ a réduction multiplicative (resp. additive) en p si le point singulier de la courbe $\widetilde{E_p}$ est un noeud (resp. une pointe). En d'autres mots, la courbe E a réduction multiplicative (resp. additive) en p si la courbe $\widetilde{E_p}$ admet deux tangentes distinctes (resp. confondues) au point singulier.

Par exemple, soient $E/\mathbf{Q}$ une courbe, donnée par une équation de la forme $y^2 = f(x)$, et un nombre premier $p \geq 5$. Alors, la courbe a bonne réduction en p si et seulement si f n'admet pas de zéro multiple modulo p. Les nombres premiers de réduction multiplicative correspondent aux p tels que f a un zéro double modulo p.

Soit maintenant p un nombre premier de bonne réduction. Le groupe $\widetilde{E_p}(\mathbf{F}_p)$ est l'ensemble des points sur $\widetilde{E_p}$ à coefficients dans $\mathbf{F}_p$; il s'agit donc d'un groupe abélien fini. On rappelle que le nombre de points sur la droite projective $\mathbf{P}_1$ sur $\mathbf{F}_p$

est $p+1$. Un argument heuristique laisse croire que $\#(\widetilde{E_p}(\mathbf{F}_p))$ est assez proche de $p+1$. Il est donc naturel de définir l'entier $a_p(E) = a_p$

$$a_p := p + 1 - \#(\widetilde{E_p}(\mathbf{F}_p)).$$

Le prochain théorème a d'abord été conjecturé par E. Artin dans sa thèse et démontré par Hasse dans les années 30.

Théorème 11 *Soit E une courbe elliptique définie sur le corps fini $\mathbf{F}_p$. Alors,*

$$\mid p + 1 - \#(E(\mathbf{F}_p)) \mid \leq 2\sqrt{p}.$$

Preuve: voir [Si1], Chap. V, §1.

En anticipant quelque peu la conjecture de Shimura-Taniyama, ces entiers a_p auront un lien direct avec les formes modulaires.

Il existe des propriétés arithmétiques des courbes elliptiques qui sont conservées par une isogénie définie sur $\mathbf{Q}$.

Théorème 12 *Soient $E/\mathbf{Q}$ et $E'/\mathbf{Q}$ deux courbes elliptiques isogènes sur $\mathbf{Q}$.*

a) Les courbes E et E' ont le même ensemble de nombres premiers de mauvaise réduction.

b) Si p est un nombre premier de bonne réduction, alors

$$\#(\widetilde{E_p}(\mathbf{F}_p)) = \#(\widetilde{E_p}'(\mathbf{F}_p)).$$

La démonstration de a) est une conséquence directe du critère de Néron-Ogg-Shafarevich (cf. [Si1], Chap. VII, §7) et pour b) voir l'exercice 5.4 dans [Si1].

Le conducteur: Le *conducteur* d'une courbe elliptique $E/\mathbf{Q}$ est un entier positif N divisible précisement par les nombres premiers p de mauvaise réduction. Il est défini comme suit:

$$N = \prod_p p^{f_p} \quad \text{, où}$$

$$f_p = \begin{cases} 0 & \text{si } E \text{ a bonne réduction en } p \\ 1 & \text{si } E \text{ a réduction multiplicative en } p \\ 2+\delta_p & \text{si } E \text{ a réduction additive en } p \end{cases}$$

et δ_p est un entier non négatif ($\delta_p = 0$ si $p \geq 5$ et δ_p est borné par 3 et 6 pour $p = 2$ et 3 respectivement (cf. [Si2], Chap. IV, thm. 10.4)).

La courbe $E/\mathbf{Q}$ est dite *semi-stable en* p si p^2 ne divise pas son conducteur N. Cela signifie que la courbe $E/\mathbf{Q}$ a, soit bonne réduction en p, dans le cas où p ne divise pas N, soit mauvaise réduction en p de type multiplicatif lorsque p divise exactement N. Si la courbe elliptique $E/\mathbf{Q}$ est semi-stable en tout nombre premier p, c'est-à-dire que N est sans facteur carré, alors la courbe $E/\mathbf{Q}$ est dite *semi-stable*.

Il existe un algorithme, dû à Tate, permettant de calculer le conducteur d'une courbe elliptique $E/\mathbf{Q}$ (cf. [Si2]). Toute la difficulté réside dans le calcul des exposants de 2 et 3. Pour les autres nombres premiers, le calcul se fait sans difficulté. Par exemple, si $E/\mathbf{Q}$ est donnée par une équation de la forme $y^2 = f(x)$, où $f \in \mathbf{Z}[x]$, alors les entiers f_p ($p \neq 2, 3$) sont déterminés en considérant le polynôme $f(x)$ sur le corps $\mathbf{F}_p$.

1. Si $f(x)$ a trois zéros distincts modulo p, alors E a bonne réduction et $f_p = 0$.

2. Si $f(x)$ a un zéro double modulo p, alors E a réduction multiplicative en p et $f_p = 1$.

3. Si $f(x)$ a un zéro triple modulo p, alors il faut être plus attentif. Il se pourrait que le modèle ne soit pas minimal et que la courbe soit en fait semi-stable en p. Si ce n'est pas le cas, alors E a réduction additive et $f_p = 2$.

Exemple 13 Soient A, B et C trois entiers non nuls, premiers entre eux deux à deux, tels que

$$A + B + C = 0$$

et soit $E_{A,B}$ la courbe de Frey d'équation

$$y^2 = x(x - A)(x + B).$$

Puisque A et B sont copremiers entre eux, la fonction $f(x) = x(x-A)(x+B)$ n'admet pas de zéro triple modulo p.

Considérons d'abord un nombre premier $p \neq 2, 3$. La courbe $E_{A,B}$ a mauvaise réduction en p si et seulement si p divise ABC, et cette mauvaise réduction est de type multiplicatif.

Si de plus $A \equiv -1 \pmod 4$ et $B \equiv 0 \pmod{32}$, l'équation

$$y^2 + xy = x^3 + \frac{B-A-1}{4}x^2 - \frac{AB}{16}x$$

fournit un modèle minimal pour la courbe $E_{A,B}$. En considérant cette équation sur $\mathbf{F}_2$ et $\mathbf{F}_3$, si 3 divise ABC, on vérifie qu'on obtient une cubique ayant un point double en $(0,0)$ à tangentes distinctes. Lorsque A et B satisfont les congruences ci-haut, la courbe $E_{A,B}$ est donc semi-stable et son conducteur est donné par

$$N = \prod_{p|ABC} p.$$

Exemple 14 Soit (a, b, c) une solution primitive de $x^2 + y^3 = z^5$. On considère

$$E : y^2 = x^3 + 27bx - 54a$$

et on sait que le discriminant de E est $\Delta = -2^6 3^9 c^5$. On montre que le conducteur N de E est de la forme $2^s 3^t p_1 \cdots p_k$, où $\{p_1, \ldots p_k\}$ sont les diviseurs premiers $\neq 2, 3$ de c.

Soit p un diviseur premier de c $(p > 3)$ et supposons que

$$f(x) = x^3 + 27bx - 54a$$

a un zéro triple modulo p. Alors,

$$f(x) = (x-\alpha)^3 \qquad (\text{mod } p)$$

et en comparant les coefficients de x^2 et x, on déduit que

$$a \equiv b \equiv 0 \qquad (\text{mod } p).$$

Ceci contredit l'hypothèse $\text{pgcd}(a,b,c) = 1$ et puisque $p \mid c$, E a mauvaise réduction en p (la courbe E est minimale en p, voir remarque 9). Ainsi,

$$N = 2^s 3^t p_1 \cdots p_k,$$

où $\{p_1 \ldots p_k\}$ sont les diviseurs premiers $\neq 2, 3$ de c.

Tordues: Une courbe elliptique $E'/\mathbf{Q}$ isomorphe sur $\overline{\mathbf{Q}}$ à $E/\mathbf{Q}$ mais non necéssairement isomorphe sur $\mathbf{Q}$ est appelée une *tordue* de E. Donc les tordues d'une courbe E sont toutes les courbes elliptiques ayant le même j-invariant que E. On sait caractériser l'ensemble des tordues d'une courbe E.

Théorème 15 *Soit $E/\mathbf{Q}$ une courbe elliptique de j-invariant j.*

a) Si $j \neq 1728$ et $j \neq 0$, alors les tordues de E sont isomorphes à E sur une extension quadratique de $\mathbf{Q}$.

b) Si $j = 0$, alors E est donnée par une équation de la forme $y^2 = x^3 + k$ avec $k \in \mathbf{Z}$ et $E' : y^2 = x^3 + k'$ est isomorphe à E sur $\mathbf{Q}(\sqrt[6]{\frac{k}{k'}})$.

c) Si $j = 1728$, alors E est donnée par une équation de la forme $y^2 = x^3 + kx$ avec $k \in \mathbf{Z}$ et $E' : y^2 = x^3 + k'x$ est isomorphe à E sur $\mathbf{Q}(\sqrt[4]{\frac{k}{k'}})$.

Preuve:

a) Soit E' une tordue de E et $\psi : E' \to E$ un isomorphisme. Soit $\sigma \in \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ et considérons $\psi^\sigma \circ \psi^{-1}$. L'application $\psi^\sigma \circ \psi^{-1}$ est un automorphisme de E. Puisque $j \neq 0, 1728$, on a $\text{Aut}(E) = \pm 1$. Par conséquent, $\psi^\sigma = \pm\psi \ \forall \sigma \in \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. L'application qui à σ associe $\varepsilon(\sigma) \in \{1, -1\}$ tel que $\psi^\sigma = \varepsilon(\sigma)\psi$ est un homomorphisme de $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ dans $\{1, -1\}$, qui découpe une extension quadratique K de $\mathbf{Q}$. L'isomorphisme ψ est défini sur K.

b) L'isomorphisme entre les courbes E et E' est donné par

$$(x, y) \longmapsto (\sqrt[3]{\frac{k}{k'}}x, \sqrt{\frac{k}{k'}}y).$$

c) L'isomorphisme entre les courbes E et E' est donné par

$$(x, y) \longmapsto (\sqrt{\frac{k}{k'}}x, \sqrt[4]{\frac{k}{k'}}^3 y).$$

□

Soit maintenant $E/\mathbf{Q}$ une courbe elliptique ayant un j-invariant $j \neq 1728$ et $j \neq 0$. Si $E/\mathbf{Q}$ a un modèle de la forme $y^2 = f(x)$, alors pour tout d ($d \neq 0, 1$) sans facteur carré, il existe une tordue, notée $E * d$, ayant un modèle de la forme $dy^2 = f(x)$. L'isomorphisme entre E et $E * d$, défini sur $\mathbf{Q}(\sqrt{d})$, est obtenu par

$$(x, y) \longmapsto (x, \sqrt{d}y).$$

Dans bien des cas, on peut déterminer aisément la conducteur de la courbe $E*d$.

Théorème 16 *Soient $E/\mathbf{Q}$ une courbe elliptique de conducteur N, d ($\neq 0, 1$) un entier sans facteur carré et D le discriminant de $\mathbf{Q}(\sqrt{d})$. Le conducteur N_d de la courbe $E*d$ est seulement divisible par les nombres premiers divisant ND. De plus, si D^2 ne divise pas N, alors $N_d = ppcm(N, D^2)$; si D^2 divise N, N_d peut être plus petit que N.*

Ce résultat est mentionné dans [Cr], p.82. Le théorème suivant donne une méthode pour obtenir les coefficients a_p de $E * d$ à partir de ceux de E.

Théorème 17 *Soient $E/\mathbf{Q}$ une courbe elliptique, d ($\neq 0, 1$) un entier sans facteur carré et p un nombre premier de bonne réduction non ramifié dans $\mathbf{Q}(\sqrt{d})$. Alors,*

$$a_p(E * d) = \chi(p)a_p(E),$$

où χ est le caractère quadratique associé à $\mathbf{Q}(\sqrt{d})$.

Preuve: Soit p un nombre premier non ramifié dans $\mathbf{Q}(\sqrt{d})$. Si $\chi(p) = 1$, alors d est un résidu quadratique mod p et les courbes E et $E*d$ sont isomorphes sur $\mathbf{F}_p$; ainsi, $\#(E(\mathbf{F}_p)) = \#(E * d(\mathbf{F}_p))$ et donc $a_p(E) = a_p(E * d)$. Si $\chi(p) = -1$, alors d et $\frac{1}{d}$ sont non résidus quadratiques mod p. Ainsi, pour $x \in \mathbf{F}_p$, soit $f(x)$, soit $\frac{1}{d}f(x)$ est résidu quadratique mod p. Donc, si $\chi(p) = -1$, $\#(E(\mathbf{F}_p)) + \#(E*d(\mathbf{F}_p)) = 2(p+1)$ et $a_p(E) = -a_p(E * d)$. □

Exemple 18 Soit E la courbe elliptique donnée par l'équation

$$y^2 = x^3 + 24x - 16.$$

Cette courbe a pour conducteur $N = 864$ et pour j-invariant $j = 2^9 3$. Soit maintenant E', la courbe elliptique donnée par l'équation:

$$E' : y^2 = x^3 + 6x + 2.$$

Il est possible de calculer les valeurs des a_p en utilisant, par exemple, GP-pari et voici les résultats pour $5 \leq p \leq 61$:

p	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61
$a_p(E)$	-2	1	-2	1	-6	-5	6	-8	8	-5	-8	-4	-10	-4	14	3
$a_p(E')$	2	-1	-2	-1	-6	-5	-6	8	-8	5	-8	-4	10	4	14	-3

On vérifie que $a_p(E') = \left(\frac{-2}{p}\right) a_p(E)$, où $\left(\frac{-2}{p}\right)$ est le symbole de Legendre. On note que $\left(\frac{-2}{p}\right)$ est exactement le caractère quadratique $\chi(p)$ associé à $\mathbf{Q}(\sqrt{-2})$. Ainsi, d'après ces données, le théorème 17 laisserait croire que $E' = E * -2$ (ou tout au moins que ces deux courbes sont isogènes). La dernière égalité est effectivement vraie et l'isomorphisme, défini sur $\mathbf{Q}(\sqrt{-2})$, entre E et E' est donné par

$$(x, y) \longmapsto (-2x, -2\sqrt{-2}y).$$

L'équation $y^2 = x^3 + 6x + 2$ est le modèle minimal de $-2y^2 = x^3 + 24x - 16$. Le discriminant de $\mathbf{Q}(\sqrt{-2})$ étant -8, le conducteur de E' est 1728, par le théorème 16. Puisque la courbe E' est isomorphe à E, le j-invariant j' de E' est $j' = 2^9 3$.

2.2 Formes modulaires

On rappelle brièvement la définition et quelques concepts reliés aux formes modulaires considérées dans ce papier. Soit N un entier positif; on définit le sous-groupe $\Gamma_0(N)$ de $\mathbf{SL}_2(\mathbf{Z})$ comme étant

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z}) \ : \ c \equiv 0 \pmod{N} \right\}.$$

On rappelle que tout sous-groupe Γ de $\mathbf{SL}_2(\mathbf{Z})$ agit sur le demi-plan complexe supérieur $\mathcal{H}$ de la façon suivante:

$$\Gamma \times \mathcal{H} \longrightarrow \mathcal{H} : \quad \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau \right) \longmapsto \frac{a\tau + b}{c\tau + d}.$$

Les formes modulaires utilisées dans ce papier sont des formes paraboliques de poids deux sur $\Gamma_0(N)$, où N est dit le niveau de la forme modulaire. Celles-ci sont des fonctions f définies sur $\mathcal{H}$ satisfaisant

1. $f(\tau) = (c\tau + d)^{-2} f(\gamma\tau)$ pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, $\tau \in \mathcal{H}$ et
2. f est une fonction holomorphe sur $\mathcal{H}$ dont la valeur de f tend vers zéro à l'infini de façon exponentielle.

En particulier, pour $\gamma = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, $f(\tau) = f(\tau + k)$ et donc f peut s'écrire comme une série de Fourier $\sum_{n=1}^{\infty} c_n q^n$, où $q := e^{2\pi i z}$ et $c_n \in \mathbf{C}$.

En prenant le quotient de $\mathcal{H}$ par $\Gamma_0(N)$, on obtient $\mathcal{H}/\Gamma_0(N)$, une surface de Riemann non compacte, notée habituellement $Y_0(N)$. On appelle $X_0(N)$ la compactification de $Y_0(N)$ (cf. [Sh], Chap. 1).

Théorème 19 *La surface de Riemann $X_0(N)$ est une courbe algébrique sur $\mathbf{C}$.*

Ce théorème est un cas particulier du théorème d'existence de Riemann (cf. [Fo], Chap. 2): toute surface de Riemann est isomorphe à l'ensemble des points $(x, y) \in \mathbf{C}^2$, où x et y satisfont une équation polynomiale $f(x, y) = 0$.

L'ensemble des formes paraboliques de poids deux sur $\Gamma_0(N)$ est un espace vectoriel sur $\mathbf{C}$ que l'on note $S(N)$. L'espace $S(N)$ peut-être identifié à l'espace des formes différentielles holomorphes sur $X_0(N)$. En effet, si f est une forme parabolique de $S(N)$, on vérifie que l'expression $f(\tau)\mathrm{d}\tau$ est invariante sous l'action de $\Gamma_0(N)$ et la condition à l'infini satisfaite par la forme f entraîne l'holomorphicité de $f(\tau)\mathrm{d}\tau$. Le théorème de Riemann-Roch (cf. [Ki], section 6.3) entraîne alors

Proposition 20 *L'espace $S(N)$ est de dimension finie. Sa dimension est égale au genre de $X_0(N)$.*

Le genre de $X_0(N)$ peut se calculer grâce à la formule de Riemann-Hurwitz (cf. [Kn], thm. 9.10).

Théorème 21 *La dimension de $S(N)$ est*

$$g = 1 + \frac{\mu(N)}{12} - \frac{\mu_2(N)}{4} - \frac{\mu_3(N)}{3} - \frac{\mu_\infty(N)}{2},$$

où

$$\mu(N) = N \prod_{p|N} (1 + \tfrac{1}{p})$$

$$\mu_2(N) = \begin{cases} 0 & \text{si } 4 \mid N \\ \prod_{p|N} (1 + \left(\frac{-1}{p}\right)) & \text{autrement} \end{cases}$$

$$\mu_3(N) = \begin{cases} 0 & \text{si } 2|N \text{ ou } 9|N \\ \prod_{p|N} (1 + \left(\frac{-3}{p}\right)) & \text{autrement} \end{cases}$$

$$\mu_\infty(N) = \sum_{d|N} \varphi(pgcd(d, \tfrac{N}{d})).$$

La fonction φ est la fonction d'Euler et $\left(\frac{-1}{p}\right)$, $\left(\frac{-3}{p}\right)$ sont des symboles de Legendre.

Exemple 22 Pour $N = 11$, le théorème 21 donne que la dimension de $S(11)$ est un. On montre que

$$f(q) := q \prod_{n=1}^{\infty} (1 - q^n)^2 \cdot (1 - q^{11n})^2$$

est une forme parabolique de niveau 11 et donc f est une fonction génératrice de l'espace $S(11)$. On remarque que les coefficients de Fourier de f sont rationnels et même entiers. Ceci n'est pas un accident d'après le théorème suivant.

Théorème 23 *L'espace $S(N)$ a une base constituée de formes paraboliques à coefficients de Fourier entiers.*

Preuve: voir [DDT], section 1.4.

L'espace $S(N)$ est équipé d'une famille d'endomorphismes appelés *opérateurs de Hecke* T_n ($n \geq 1$). Traditionnellement, l'action des opérateurs T_n sur f est notée

par $f\,|\,T_n$. Les T_n peuvent s'écrire en fonction des opérateurs T_p indexés par les facteurs premiers de n. Si $f = \sum c_n q^n$, alors l'action des opérateurs T_p sur f est donnée par

$$T_p : f = \sum c_n q^n \longmapsto \begin{cases} \sum c_{pn} q^n + p \sum c_n q^{pn} & \text{si } (p, N) = 1 \\ \sum c_{pn} q^n & \text{si } p \mid N. \end{cases}$$

On appelle f *fonction propre* de $S(N)$ si $f = \sum c_n q^n$ est une forme parabolique non nulle qui est vecteur propre pour tous les T_n $(n \geq 1)$. La fonction f est dite *fonction propre normalisée*, si de plus elle satisfait $c_1 = 1$. Si f est une telle fonction propre, on a que $f|T_n = c_n f$, c'est-à-dire que ses coefficients de Fourier et ses valeurs propres coïncident pour tout $n \geq 1$. Ainsi, le corps engendré par les coefficients c_n est une extension finie de $\mathbf{Q}$, par le théorème 23. De plus, les c_n sont toujours des entiers algébriques et il arrive qu'ils soient de simples entiers rationnels.

Bien qu'il soit souvent possible de diagonaliser les opérateurs T_n dans $S(N)$, il arrive d'en être incapable. Donc, les fonctions propres normalisées ne forment pas toujours une base de l'espace vectoriel $S(N)$. Le problème apparaît seulement lorsque n et N ne sont pas copremiers entre eux. On introduit le concept de "newforms" pour remédier à ce problème. On remarque d'abord que l'espace $S(N)$ est équipé d'un produit scalaire hermitien que l'on nomme le *produit scalaire de Petersson*; on retrouve la définition de ce produit scalaire, par exemple, dans [DDT], section 1.1.

Définition 24 *Une forme modulaire f de niveau N est appelée une "oldform" de niveau N si elle est une combinaison linéaire de fonctions de la forme $g(d\tau)$, où g est une forme modulaire de niveau strictement divisant N. Une "newform" de niveau N est une fonction propre normalisée qui est orthogonale à toutes les "oldforms" de niveau N selon le produit scalaire de Petersson. L'espace des "oldforms" de niveau N est noté $S^{\text{old}}(N)$ et celui des "newforms" de niveau N est noté $S^{\text{new}}(N)$.*

On a

$$S(N) = S^{\text{old}}(N) \oplus S^{\text{new}}(N).$$

De plus, $S^{\text{new}}(1) = \emptyset$ et

$$S^{\text{old}}(N) \simeq \bigoplus_{\substack{d|N \\ d \neq N}} (S^{\text{new}}(d))^{\sigma_0(\frac{N}{d})}, \tag{2.1}$$

où $\sigma_0(x)$ dénote le nombre de diviseurs de x. A. Atkin et J. Lehner ont montré que l'espace $S(N)$ a une base constituée de transformations de "newforms" de $S(M)$, où M parcourt les diviseurs de N.

2.3 La Conjecture de Shimura-Taniyama

La conjecture de Shimura-Taniyama est une conjecture célèbre, entre autres par le lien qu'elle a avec la démonstration du dernier théorème de Fermat. Les travaux de Eichler et Shimura ont d'abord mené au théorème suivant:

Théorème 25 (Eichler-Shimura) *Soit $f = \sum c_n q^n$ une fonction propre normalisée de l'espace S(N) ayant des coefficients de Fourier rationnels. Alors, il existe une courbe elliptique E_f définie sur $\mathbf{Q}$ associée à f, ayant les propriétés suivantes:*

a) Le conducteur de E_f est égal à N. En particulier, E_f a bonne réduction en p si p ne divise pas N.

b) Si p ne divise pas N, on a $\#(E_f(\mathbf{F}_p)) = p + 1 - c_p$.

Références: [DDT], section 1.7.

En d'autres mots, le théorème de Eichler-Shimura assure l'existence d'une application $f \mapsto E_f$, où f et E_f satisfont les propriétés du théorème. Étant donné que des courbes isogènes sur $\mathbf{Q}$ ont même conducteur et coefficients a_p (voir théorème 12), la courbe E_f est définie seulement à isogénie près.

La conjecture de Shimura-Taniyama peut maintenant s'énoncer ainsi:

Conjecture de Shimura-Taniyama. *L'application*

$$\left\{ \begin{array}{c} \text{"Newforms" de poids 2 sur } \Gamma_0(N) \\ \text{à coefficients de Fourier rationnels} \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{Classes d'isogénie de courbes} \\ \text{elliptiques définies sur } \mathbf{Q} \\ \text{et de conducteur } N \end{array} \right\}$$

est une bijection.

Bien qu'à ce jour, la conjecture de Shimura-Taniyama soit presque démontrée, elle demeure encore une conjecture. Cependant, Andrew Wiles a démontré cette conjecture pour les courbes elliptiques semi-stables et ceci était suffisant pour compléter la preuve du dernier théorème de Fermat. Dans ce papier, nous aurons à utiliser cette conjecture dans des conditions particulières où elle n'est pas démontrée. Ainsi, nous n'aurons autre choix que de la supposer vraie. Ceci ne semble pas être une grande restriction étant donné la confiance des mathématiciens à pouvoir démontrer prochainement la conjecture telle qu'énoncée ci-haut.

Définition 26 *Une courbe elliptique $E/\mathbf{Q}$ est dite modulaire si la courbe E est isogène sur $\mathbf{Q}$ à E_f, pour une "newform" $f \in S(N)$.*

On illustre la conjecture de Shimura-Taniyama par un exemple.

Exemple 27 Soit E la courbe elliptique

$$E : y^2 + y = x^3 - x^2.$$

Son conducteur est égal à 11. Pour tout nombre premier $p \neq 11$, la courbe E a bonne réduction et il est possible de calculer les coefficients $a_p(E)$. Voici quelques valeurs, calculées à l'ordinateur.

p	2	3	5	7	11	13	17	19	23	29	31
a_p	-2	-1	1	-2	-	4	-2	0	-1	0	7

La conjecture de Shimura-Taniyama prédit qu'il existe une "newform" $f \in S(11)$ à coefficients de Fourier rationnels, telle que f est appliquée sur E. Or, la dimension de l'espace vectoriel $S(11)$ est un et $S(11)$ est engendré par

$$\begin{aligned} q\prod_{n=1}^{\infty}(1-q^n)^2\cdot(1-q^{11n})^2 &= q\mathbf{-2q^2-q^3}+2q^4\mathbf{+q^5}+2q^6\mathbf{-2q^7} \\ &\quad -2q^9-2q^{10}\mathbf{+q^{11}}-2q^{12}\mathbf{+4q^{13}}+4q^{14} \end{aligned}$$

$$
\begin{aligned}
& - q^{15} - 4q^{16} \mathbf{-2q^{17}} + 4q^{18} + 2q^{20} + 2q^{21} \\
& - 2q^{22} \mathbf{-q^{23}} - 4q^{25} - 8q^{26} + 5q^{27} - 4q^{28} \\
& + 2q^{30} \mathbf{+7q^{31}} + \cdots \\
= & \sum_{n=1}^{\infty} c_n q^n
\end{aligned}
$$

(voir exemple 22). On remarque que les coefficients $a_p(E)$ coïncident avec les coefficients de Fourier c_p.

Cet exemple illustre le lien qu'il existe entre les coefficients $a_p(E)$ d'une courbe elliptique $E/\mathbf{Q}$ et les coefficients de Fourier de la forme modulaire associée. La conjecture de Shimura-Taniyama énonce qu'il existe une telle relation avec toutes les courbes elliptiques définies sur $\mathbf{Q}$, à savoir si $E/\mathbf{Q}$ est une courbe elliptique de conducteur N, alors on conjecture qu'il existe une "newform" $f = \sum c_n q^n$ dans $S(N)$ telle que $c_p = a_p(E)$ pour tout p, p ne divisant pas N. On note que les coefficients de Fourier c_n de f, pour $(n, N) = 1$, sont des entiers rationnels.

2.4 Représentations galoisiennes

a) Représentations galoisiennes associées aux courbes elliptiques

Soit $E/\mathbf{Q}$ une courbe elliptique, et soit $n \geq 1$. On considère $E[n]$, le sous-groupe de $E(\mathbf{C})$ constitué des points de E d'ordre divisant n, où de façon équivalente, le noyau de l'application *multiplication par* n définie dans l'exemple 4. On rappelle que la loi d'addition de 2 points sur $E(\mathbf{C})$ est donnée par des fonctions rationnelles à coefficients dans $\mathbf{Q}$. De ce fait, on voit que $E[n]$ est un sous-groupe de $E(\overline{\mathbf{Q}})$ et que $E[n]$ est stable sous l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur $E(\overline{\mathbf{Q}})$. Pour la même raison, pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, l'automorphisme défini par $P \mapsto P^\sigma$, où $P \in E[n]$, est en fait un automorphisme de groupe de $E[n]$, c'est-à-dire $(P + Q)^\sigma = P^\sigma + Q^\sigma$,

pour P, $Q \in E[n]$. Ainsi, l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ donne lieu à un homomorphisme (continu) ρ_n^E, défini par

$$\rho_n^E : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longmapsto \mathrm{Aut}(E[n]).$$

Proposition 28 *Soit E une courbe elliptique et $n \geq 1$.*

$$E[n] \simeq (\mathbf{Z}/n\mathbf{Z})^2.$$

Preuve: Lorsque la courbe E est considérée sur le corps des complexes $\mathbf{C}$, alors $E(\mathbf{C}) \simeq C/L$, où L est un réseau, c'est-à-dire $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbf{Z}\}$ (cf. [Si1], Chap. VI). L'isomorphisme entre $(\mathbf{Z}/n\mathbf{Z})^2$ et $E[n]$ est alors donné par

$$(a_1, a_2) \longrightarrow \frac{a_1}{n}\omega_1 + \frac{a_2}{n}\omega_2.$$

□

L'isomorphisme de la proposition 28 n'est pas canonique et dépend du choix des générateurs ω_1 et ω_2, où de façon équivalente d'une base de $E[n]$. Ainsi, pour chaque choix d'une telle base, on a $\mathrm{Aut}(E[n]) \simeq \mathbf{GL}_2(\mathbf{Z}/n\mathbf{Z})$. Ayant fixé une base de $E[n]$, on obtient une représentation de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ qu'on appelle la représentation de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ fournie par les points de n-division de la courbe elliptique E. Il est souhaitable de fixer à prime abord une base de $E[n]$ et de voir ρ_n^E prenant ses valeurs dans $\mathbf{GL}_2(\mathbf{Z}/n\mathbf{Z})$. Du fait de la base de $E[n]$ choisie, on définit, de cette façon, une représentation à conjugaison près, notée encore ρ_n^E.

Par la théorie de Galois, le noyau de ρ_n^E correspond à une extension finie K_n de $\mathbf{Q}$ contenue dans $\overline{\mathbf{Q}}$. Concrètement K_n est la plus petite extension de $\mathbf{Q}$ contenant toutes les coordonnées des points de $E[n]$; si $E[n] = \{(x_1, y_1), \ldots, (x_{n^2}, y_{n^2})\}$, alors $K_n = \mathbf{Q}(x_1, \ldots, x_{n^2}, y_1, \ldots, y_{n^2})$ et K_n est habituellement notée $\mathbf{Q}(E[n])$. Ainsi, en prenant le quotient de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ par le noyau de ρ_n^E, on obtient une représentation de $\mathrm{Gal}(\mathbf{Q}(E[n])/\mathbf{Q})$ qui est injective et en particulier, on peut identifier le groupe $\mathrm{Gal}(\mathbf{Q}(E[n])/\mathbf{Q})$ à un sous-groupe de $\mathbf{GL}_2(\mathbf{Z}/n\mathbf{Z})$. À l'avenir, on s'intéressera seulement au cas où n est un nombre premier ℓ, auquel cas $\mathbf{Z}/n\mathbf{Z}$ est le corps fini $\mathbf{F}_\ell$.

Exemple 29 Soit E la courbe elliptique

$$E : y^2 = x^3 - x^2 + x - 1 = (x^2 + 1)(x - 1)$$

et soit

$$\rho_2^E : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}_2(\mathbf{F}_2),$$

la représentation associée à ses points d'ordre 2. Les points d'ordre 2 de E correspondent aux points (x, y) de E, où $y = 0$. Alors,

$$E[2] = \{\mathcal{O}, (1, 0), (i, 0), (-i, 0)\}$$

et on a $\mathbf{Q}(E[2]) = \mathbf{Q}(i)$. Le groupe de Galois $\mathrm{Gal}(\mathbf{Q}(E[2])/\mathbf{Q})$ contient donc deux éléments $\{\sigma_0, \sigma_1\}$ correspondant respectivement à l'identité et à la conjugaison complexe. Pour connaître la représentation $\mathrm{Gal}(\mathbf{Q}(E[2])/\mathbf{Q}) \longrightarrow \mathbf{GL}_2(\mathbf{F}_2)$, on choisit une base $\{P, Q\}$ de $E[2]$ et on regarde l'action de σ_i $(i = 0, 1)$ sur P et Q. On rappelle que si $P = (x, y)$, on définit l'action de Galois par

$$P^\sigma = (x^\sigma, y^\sigma).$$

On a

$$\begin{array}{rcccccl} P^{\sigma_1} & = & (1^{\sigma_1}, 0^{\sigma_1}) & = & (1, 0) & = & P \\ Q^{\sigma_1} & = & (i^{\sigma_1}, 0^{\sigma_1}) & = & (-i, 0) & = & P + Q \end{array}$$

et donc

$$\sigma_0 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\sigma_1 \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Ainsi, la représentation ρ_2^E est donnée par

$$\rho_2^E(\sigma) = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \text{si } i^\sigma = i \\ \\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & \text{si } i^\sigma = -i. \end{cases}$$

Le caractère cyclotomique χ_ℓ d'ordre ℓ est défini en considérant l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur le groupe μ_ℓ des racines $\ell^{\text{ième}}$ de l'unité de $\overline{\mathbf{Q}}$. Cette action de groupe donne lieu a un homomorphisme

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(\mu_\ell)$$

et puisque μ_ℓ est un groupe d'ordre ℓ, son groupe d'automorphismes est isomorphe à $(\mathbf{Z}/\ell\mathbf{Z})^\times = \mathbf{F}_\ell^\times$. Ceci mène au caractère cyclotomique

$$\chi_\ell : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{F}_\ell^\times.$$

L'introduction du caractère χ_ℓ se justifie par la proposition suivante:

Proposition 30 *Si $E/\mathbf{Q}$ est une courbe elliptique, alors le déterminant de ρ_ℓ^E est le caractère cyclotomique χ_ℓ.*

Preuve: Cette proposition est une conséquence directe de l'accouplement e_ℓ de Weil et de ses propriétés (cf. [Si1], Chap. III, §8). En effet,

$$e_\ell : E[\ell] \times E[\ell] \longrightarrow \mu_\ell$$

est

a) bilinéaire:

$$\begin{aligned} e_\ell(P_1 + P_2, Q) &= e_\ell(P_1, Q) \cdot e_\ell(P_2, Q) \\ e_\ell(P, Q_1 + Q_2) &= e_\ell(P, Q_1) \cdot e_\ell(P, Q_2); \end{aligned}$$

b) alternée: $e_\ell(P, P) = 1$, en particulier $e_\ell(P, Q) = e_\ell(Q, P)^{-1}$;

c) Galois invariant: pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$,

$$e_\ell(P, Q)^\sigma = e_\ell(P^\sigma, Q^\sigma)$$

(cf. [Si1], Chap. III, prop. 8.1). Soient $\{P, Q\}$ une base de $E[\ell]$ et $\zeta = e_\ell(P, Q)$. Supposons que

$$\begin{aligned} P^\sigma &= a(\sigma)P + c(\sigma)Q \\ Q^\sigma &= b(\sigma)P + d(\sigma)Q. \end{aligned}$$

Alors,

$$\rho_\ell^E : \sigma \longmapsto \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$$

et

$$\begin{aligned} \zeta^\sigma &= e_\ell(P,Q)^\sigma \\ &= e_\ell(P^\sigma, Q^\sigma) \\ &= e_\ell(a(\sigma)P + c(\sigma)Q) \cdot e_\ell(b(\sigma)P + d(\sigma)Q) \\ &= e_\ell(P,Q)^{a(\sigma)d(\sigma) - b(\sigma)c(\sigma)} \\ &= \zeta^{\det(\rho_\ell^E(\sigma))} \end{aligned}$$

□

Dans l'étude de l'équation $x^2 + y^3 = z^5$, il faudra distinguer les cas où la représentation ρ_ℓ^E est irréductible et réductible. On dit que la représentation ρ_ℓ^E est réductible lorsque la courbe E possède un sous-groupe d'ordre ℓ qui est stable sous l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Un exemple typique est lorsque le groupe $E[\ell]$ contient un point d'ordre ℓ défini sur $\mathbf{Q}$. Soit ρ_ℓ^E une représentation réducible et soit P le point dans $E[\ell]$ qui engendre le sous-groupe de $E(\overline{\mathbf{Q}})$ stable par l'action de Galois. Si Q est un point de $E[\ell]$ à l'extérieur de la droite engendrée par P alors, les points P et Q forment une base de l'espace $E[\ell]$. Étant donné que le point P est stable sous l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, on voit qu'en utilisant la base $\{P, Q\}$, l'image d'un automorphisme $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ par la représentation ρ_ℓ^E est de la forme

$$\sigma \longmapsto \begin{pmatrix} a(\sigma) & b(\sigma) \\ 0 & c(\sigma) \end{pmatrix},$$

c'est-à-dire les matrices de l'image de la représentation ρ_ℓ^E sont triangulaires. Ceci caractérise les représentations réductibles. Si $b(\sigma) = 0$ pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, on dit que la représentation est totalement réductible.

Voici un théorème profond démontré par Mazur.

Théorème 31 (Mazur) *Soit $E/\mathbf{Q}$ une courbe elliptique. Si $\ell > 163$ est un nombre premier, alors la représentation ρ_ℓ^E est irréductible. Si la courbe E est semi-stable, alors ρ_ℓ^E est irréductible pour tout $\ell > 7$ et irréductible pour tout $\ell > 3$ si de plus tous ses points d'ordre 2 sont définis sur $\mathbf{Q}$.*

Preuve: voir [Ma].

On dit que ρ_ℓ^E est ramifié en un nombre premier p si l'extension $K_p/\mathbf{Q}$ est ramifiée en p.

Théorème 32 *Soient $E/\mathbf{Q}$ une courbe elliptique de conducteur N, ℓ un nombre premier et ρ_ℓ^E la représentation de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *fournie par les points de ℓ-division de E. Supposons que p est un nombre premier ne divisant pas ℓN. Alors, ρ_ℓ^E est non ramifiée en p. De plus,*

a) $Trace(\rho_\ell^E(Frob_p)) \equiv a_p \pmod{\ell}$, et

b) $Det(\rho_\ell^E(Frob_p)) \equiv p \pmod{\ell}$.

Preuve: voir [Se1], Chap. 4, §1.3.

Ainsi, à partir de la représentation ρ_ℓ^E, il est possible de récupérer les coefficients a_p de E modulo ℓ.

Maintenant, soit $\Delta = \Delta_{min}$ le discriminant minimal d'une courbe elliptique $E/\mathbf{Q}$. Soit $ord_p(\Delta)$ la valuation de Δ en p définie comme dans la remarque 9. Voici un résultat permettant de caractériser les nombres premiers ($\neq \ell$) ramifiés de ρ_ℓ^E.

Théorème 33 *Soit $p \neq \ell$ un nombre premier tel que E soit semi-stable en p. Alors, la représentation ρ_ℓ^E est non ramifiée en p si et seulement si $ord_p(\Delta) \equiv 0 \pmod{\ell}$.*

Preuve: Ce résultat est une application de la théorie de la courbe de Tate (cf. [Si2], Chap. V, §3). La démonstration qui suit est empruntée de [Ri1]. On regarde la ramification de ρ_ℓ^E en p en considérant la courbe E définie sur l'extension maximale non ramifiée de $\mathbf{Q}_p$, notée $\mathbf{Q}_p^{\mathrm{nr}}$. Par définition, la représentation ρ_ℓ^E est non ramifiée en p si $\mathbf{Q}_p^{\mathrm{nr}}(E[\ell]) = \mathbf{Q}_p^{\mathrm{nr}}$. La théorie de la courbe de Tate fournit un isomorphisme

$$E(\overline{\mathbf{Q}}_p) \simeq \overline{\mathbf{Q}}_p^{\times}/q^{\mathbf{Z}},$$

avec $|q| < 1$, compatible à l'action de $\mathrm{Gal}(\overline{\mathbf{Q}_p}/\mathbf{Q}_p^{\mathrm{nr}})$. Ainsi, l'extension $\mathbf{Q}_p^{\mathrm{nr}}(E[\ell])$ de $\mathbf{Q}_p^{\mathrm{nr}}$ est obtenue en ajoutant à $\mathbf{Q}_p^{\mathrm{nr}}$ les racines $\ell^{\text{ième}}$ de q (les racines $\ell^{\text{ième}}$ de

l'unité appartiennent déjà à $\mathbf{Q}_p^{\mathrm{nr}}$, car $\ell \neq p$). Puisque $\ell \neq p$, on note que q est une puissance $\ell^{\text{ième}}$ dans $\mathbf{Q}_p^{\mathrm{nr}}$ si et seulement si ℓ divise la valuation de q, c'est-à-dire $\mathrm{ord}_p(q) \equiv 0 \pmod{\ell}$. Puisque la valuation de q coïncide avec la valuation du déterminant minimal $\Delta_{\min}$ de E ($\Delta_{\min} = q \prod_{n \geq 1} (1-q^n)^{24}$), on obtient le résultat. □

Exemple 34 Soit (a, b, c) une solution primitive de $x^2 + y^3 = z^5$ et soit la courbe

$$E : y^2 = x^3 + 27bx - 54a.$$

On vérifie que la représentation ρ_5^E est non ramifiée à l'extérieur de $\{2, 3, 5\}$. En effet, soit $\ell = 5$. On sait par l'exemple 8 que le discriminant de E est $\Delta = -2^6 3^9 c^5$ et qu'il est minimal pour tout $p > 3$ (voir remarque 9). De plus, on sait que pour tout $p > 3$ de mauvaise réduction (c'est-à-dire, $p \mid c$), $p \parallel N$, où N est le conducteur de la courbe E (voir exemple 14). Par le théorème 33, on conclut que ρ_5^E est non ramifiée à l'extérieur de $\{2, 3, 5\}$.

Remarque 35 Le principe de démonstration du théorème 33 se généralise sans dificulté au cas ou on remplace $\mathbf{Q}_p$ par le corps de fractions d'un anneau de valuation discrète quelconque. Ainsi on a

Théorème 36 *Soit R un anneau de valuation discrète de caractéristique 0, m son idéal maximal, $k = R/m$ son corps résiduel et K son corps de fractions. Soit E une courbe elliptique définie sur K, ayant bonne réduction ou réduction multiplicative modulo m. Soit $\Delta \in R$ le discriminant minimal de E sur R. Notons par ρ_ℓ^E : $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$ la représentation galoisienne sur les points d'ordre ℓ de E, et supposons que ℓ est différent de char(k). Alors ρ_ℓ^E est non ramifiée en m si et seulement si ℓ divise la valuation de Δ.*

Nous aurons à nous servir plus tard de ce résultat dans le cas où la courbe est définie sur le corps de fonction $\mathbf{Q}(t)$.

b) Représentations galoisiennes associées aux formes modulaires

Dans cette section, on s'intéresse seulement aux formes modulaires qui sont des fonctions propres normalisées. Si la forme modulaire $f \in S(N)$ a des coefficients de Fourier c_n rationnels, il est possible de lui associer une courbe elliptique $E = E_f$ satisfaisant $a_p(E) = c_p$, pour p ne divisant pas N (voir théorème 25) et de considérer la famille de représentations ρ_ℓ^E, où ℓ parcourt les nombres premiers ℓ. Étant donné que la représentation ρ_ℓ^E provient initialement de la fonction f, il est tentant de nommer cette application ρ_ℓ^f. Cependant, un obstacle apparaît avec cette écriture; la courbe elliptique E est seulement définie à isogénie près et la représentation ρ_ℓ^E dépend du choix de la courbe E. Il faut donc modifier quelque peu la représentation ρ_ℓ^E de façon qu'elle soit indépendante du choix de la courbe E. Pour bien définir la représentation ρ_ℓ^f, on introduit la *semi-simplification* de ρ_ℓ^E.

On distingue deux cas bien différents: représentations irréductibles et réductibles. Lorsque la représentation ρ_ℓ^E est irréductible, sa semi-simplification est ρ_ℓ^E elle-même. Si la représentation ρ_ℓ^E est réductible (la cas où les matrices sont triangulaires), ρ_ℓ^E se décompose en deux représentations ρ_1, ρ_2 de dimension un et la semi-simplification de ρ_ℓ^E est la somme directe de ρ_1 et ρ_2. En définissant

$$\rho_\ell^f := \text{semi-simplification de } \rho_\ell^E,$$

on démontre que la représentation ρ_ℓ^f est indépendante du choix de la courbe E choisie. Les propriétés arithmétiques de la forme modulaire $f = \sum c_n q^n \in S(N)$ sont reflétées dans la représentation ρ_ℓ^f.

Théorème 37 *Soit p un nombre premier ne divisant pas ℓN, où N est le niveau de la fonction propre normalisée $f = \sum c_n q^n$. Alors, la représentation ρ_ℓ^f est non ramifiée en p. De plus,*

a) $Trace(\rho_\ell^f(Frob_p)) \equiv c_p \ (mod\ \ell)$ *et*

b) $Det(\rho_\ell^f(Frob_p)) \equiv p \ (mod\ \ell)$.

Preuve: Soit la courbe E_f associée à f par le théorème 25 de Eichler-Shimura. La représentation ρ_ℓ^f est la semi-simplification de $\rho_\ell^{E_f}$. Par sa construction, ρ_ℓ^f a les même fonctions trace et déterminant que $\rho_\ell^{E_f}$. Le résultat s'obtient en utilisant le théorème 25 de Eichler-Shimura et le théorème 32 appliqué à la courbe E_f. □

Il est possible de généraliser ce processus aux fonctions propres normalisées $f = \sum c_n q^n \in S(N)$ n'ayant pas necéssairement des coefficients de Fourier rationnels. Si K_f dénote l'extension de $\mathbf{Q}$ engendrée par les coefficients c_n de f, alors ces coefficients appartiennent à l'anneau des entiers $\mathcal{O}_f$ de K_f (§2.2). Désormais, les représentations provenant de la forme modulaire f ne seront plus indexées par des nombres premiers, mais par les idéaux premiers de $\mathcal{O}_f$. Si λ est un idéal premier de $\mathcal{O}_f$ au-dessus de ℓ, alors le corps résiduel $\mathbf{F}_\lambda$ associé à λ est une extension finie de $\mathbf{F}_\ell$.

En analogie avec le cas où la fonction f possède des coefficients de Fourier rationnels, il est possible de définir une représentation $\rho_\lambda^f : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_\lambda)$ (cf. [Sh], Chap. 7). Cette représentation est aussi caractérisée à isomorphisme près par le théorème suivant:

Théorème 38 *Soit p un nombre premier ne divisant pas ℓN, où N est le niveau de la forme modulaire $f = \sum c_n q^n$. Alors, la représentation ρ_λ^f est non ramifiée en p. De plus,*

a) $Trace(\rho_\lambda^f(Frob_p)) \equiv c_p \ (mod\ \lambda)$ et

b) $Det(\rho_\lambda^f(Frob_p)) \equiv p \ (mod\ \lambda)$.

Preuve: voir [Sh].

Définition 39 *On dit qu'une représentation ρ est modulaire (de niveau N), si l'on peut trouver*

i) une fonction propre normalisée $f(\in S(N))$ et

ii) un idéal premier λ dans l'anneau $\mathcal{O}_f$

tels que la représentation ρ_λ^f soit isomorphe à ρ. Dans ce cas, on dit que ρ et f sont associées.

2.5 Théorème de Ribet et Dernier Théorème de Fermat

Cette section est consacrée à un théorème de Kenneth A. Ribet qui nous sera indispensable dans l'étude de l'équation $x^2 + y^3 = z^5$. On se contentera d'en énoncer un cas particulier, suffisant pour nos applications. Bien qu'il nous soit impossible d'expliquer la démonstration, nous verrons comment ce théorème implique le fameux dernier théorème de Fermat.

Soit $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_\ell)$ $(\ell > 2)$ une représentation et supposons qu'elle provienne d'une courbe elliptique $E/\mathbf{Q}$, c'est-à-dire que $\rho = \rho_\ell^E$. Soient $\Delta_{\min} = \Delta$ le discriminant minimal de la courbe E et N son conducteur. On peut écrire la conducteur N sous la forme

$$N = N_1 N_2$$

où N_1 et N_2 satisfont les conditions suivantes:

1. $\mathrm{pgcd}(N_1, N_2) = 1$,
2. $\mathrm{ord}_p(N_1) \geq 1$ pour tout $p \mid N_1$ et
3. N_2 est sans facteur carré.

On définit maintenant $N(\rho) = N_1 \prod_{\substack{p \mid N_2 \\ \ell \nmid \mathrm{ord}_p(\Delta)}} p$.

Théorème 40 (Ribet) *Supposons que la représentation ρ provienne d'une courbe elliptique modulaire et que ρ soit irréductible. Alors, il existe une "newform" normalisée de niveau $N(\rho)$ associée à ρ.*

Remarques sur le théorème de Ribet

(1) La conclusion du théorème signifie qu'il existe une "newform" normalisée $f \in S(N(\rho))$ et un idéal premier λ de $\mathcal{O}_f$ tels que ρ soit isomorphe à ρ_λ^f (voir définition 39).

(2) L'hypothèse que la représentation ρ provienne d'une certaine courbe elliptique, n'intervient pas dans l'énoncé plus général du théorème de Ribet. Cependant, elle sera suffisante pour notre application.

(3) C'est précisément en applicant ce théorème qu'on supposera la conjecture de Shimura-Taniyama; l'hypothèse que la courbe elliptique E soit modulaire est un élément crucial dans cet énoncé du théorème de Ribet.

Voici maintenant une application intéressante de ce théorème qui permet de démontrer le célèbre dernier théorème de Fermat. Il est bon de remarquer qu'on n'a pas besoin de supposer la conjecture de Shimura-Taniyama pour assurer la modularité des courbes elliptiques utilisées dans la démonstration du dernier théorème de Fermat. On utilise seulement des courbes elliptiques semi-stables et sous cette hypothèse, la conjecture de Shimura-Taniyama est complètement démontrée par Wiles!

Exemple (Dernier théorème de Fermat)

Voici d'abord l'énoncé du dernier théorème de Fermat.

Dernier théorème de Fermat *L'équation*

$$a^n + b^n + c^n = 0$$

n'a aucune solution avec $a, b, c \in \mathbf{Z}$, $abc \neq 0$ *et* $n \geq 3$.

Puisque le résultat est connu pour $n = 3$ et 4, on remarque qu'il est suffisant de montrer le théorème lorsque n est un nombre premier $\ell \geq 5$. En effet, si $n = \ell q$ et $(a^q)^\ell + (b^q)^\ell + (c^q)^\ell = 0$, alors pour $A = a^q, B = b^q$ et $C = c^q$, $A^\ell + B^\ell + C^\ell = 0$.

Ainsi, on suppose qu'il existe une solution $a^\ell + b^\ell + c^\ell = 0$ satisfaisant les conditions du théorème. En divisant l'équation par le plus grand commun diviseur à la puissance ℓ de a, b et c, on peut supposer qu'ils sont sans facteur commun.

De plus, en permutant les lettres, on peut toujours supposer que $b \equiv 0 \pmod 2$ et $a \equiv -1 \pmod 4$.

Empruntant la stratégie de Frey, on considère la courbe de Frey E_{a^ℓ,b^ℓ} donnée par l'équation

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

Le discriminant minimal de la courbe E_{a^ℓ,b^ℓ} est

$$\Delta_{\min} = \Delta = \frac{(abc)^{2\ell}}{2^8}$$

(voir exemple 7). La courbe E_{a^ℓ,b^ℓ} est semi-stable et son conducteur est donné par

$$N = \prod_{p|abc} p$$

(voir exemple 13). Puisque tous les points d'ordre 2 de la courbe E_{a^ℓ,b^ℓ} sont définis sur $\mathbf{Q}$, le théorème 31 de Mazur assure l'irréductibilité de la représentation $\rho = \rho_\ell^{E_{a^\ell,b^\ell}}$. De plus, la courbe E_{a^ℓ,b^ℓ} étant semi-stable, elle est modulaire (par Wiles) et on peut donc utiliser le théorème de Ribet.

Selon les notation utilisées au début de la section, le conducteur de la courbe E_{a^ℓ,b^ℓ} s'écrit $N = N_1 N_2$, où

$$N_1 = 1 \text{ et } N_2 = \prod_{p|abc} p.$$

Pour connaître $N(\rho)$, il suffit de vérifier si ℓ divise ou non $\mathrm{ord}_p(\Delta)$ pour $p \mid abc$. Or,

$$\mathrm{ord}_p(\Delta) = \begin{cases} 2\ell \cdot \mathrm{ord}_p(abc) - 8 \equiv -8 \pmod \ell & \text{si } p = 2 \\ 2\ell \cdot \mathrm{ord}_p(abc) \equiv 0 \pmod \ell & \text{si } p \neq 2. \end{cases}$$

Puisque $\ell \geq 5$, on a $\mathrm{ord}_2(\Delta) \not\equiv 0 \pmod \ell$ et $N(\rho) = 2$. D'après le théorème de Ribet, la représentation ρ provient d'une fonction propre normalisée de niveau 2. Or, il n'existe pas de forme modulaire de niveau 2, ce qui constitue une contradiction.

Chapitre 3

L'équation $x^2 + y^3 = z^5$

3.1 Les travaux de Beukers sur l'équation $x^2+y^3 = z^5$

Pour faire l'étude de l'équation $x^2 + y^3 = z^5$, on est amené à considérer le groupe icosaédral. Tout ceci vient de la merveilleuse analyse de l'icosaèdre de Klein dans [Kl]. On rappelle que l'icosaèdre est un polygone régulier possédant 20 faces (à 3 côtés), 30 arêtes et 12 sommets. Soit **S** la sphère qui circonscrit l'icosaèdre. On peut projeter le centre de gravité des arêtes, sommets et faces du polygone sur **S** et obtenir, ce qu'on appellera arête-points, sommet-points et face-points respectivement. Soit **G** le groupe des rotations de la sphère **S** qui envoient l'icosaèdre sur lui-même. L'ordre de ce groupe est 2 fois le nombre d'arêtes, c'est-à-dire 60. On montre que ce groupe est isomorphe au groupe A_5 des permutations paires de 5 lettres. Si on suppose que le diamètre de **S** est égal à un, les 12 sommet-points sont envoyés, par la projection stéréographique, sur les 12 points suivants de $\mathbf{P}^1(\mathbf{C})$:

$$\frac{u}{v} = 0, \infty, \left(\frac{-1 \pm \sqrt{5}}{2}\right)\varepsilon^j$$

où $\varepsilon = e^{2\pi i/5}$ $(j = 1, \ldots, 5)$. Ceux-ci sont les zéros du polynôme

$$f(u, v) = uv(u^{10} - 11u^5v^5 - v^{10}).$$

Les 20 face-points correspondent aux zéros du polynôme de degré 20 déterminé par

$$g = \frac{-1}{121}\det(\text{hessienne}(f))$$

où la matrice hessienne de f se définit par

$$\begin{pmatrix} \frac{\partial^2 f}{\partial u^2} & \frac{\partial^2 f}{\partial u \partial v} \\ \frac{\partial^2 f}{\partial v \partial u} & \frac{\partial^2 f}{\partial v^2} \end{pmatrix}.$$

Ainsi, $g(u,v) = u^{20} + 228u^{15}v^5 + 494u^{10}v^{10} - 228u^5v^{15} + v^{20}$. Et finalement, le déterminant de la matrice jacobienne

$$\begin{pmatrix} \frac{\partial f}{\partial u} & \frac{\partial f}{\partial v} \\ \frac{\partial g}{\partial u} & \frac{\partial g}{\partial v} \end{pmatrix}$$

est de degré 30. Les zéros du polynôme

$$h(u,v) = \frac{-1}{20}\det(\text{jacobienne}(f,g)) =$$

$$u^{30} - 522u^{25}v^5 - 10005u^{20}v^{10} - 10005u^{10}v^{20} + 522u^5v^{25} + v^{30}$$

correspondent, quant à eux, aux trente arête-points de l'icosaèdre.

Le groupe $\mathbf{G}$ peut être vu comme un sous-groupe fini de $\mathbf{GL}_2(\mathbf{C})$. On peut alors définir une action naturelle de $\mathbf{G}$ sur l'anneau des polynômes $\mathbf{C}[X_1, X_2]$. Soient $g \in \mathbf{G}$ et $f(X_1, X_2) \in \mathbf{C}[X_1, X_2]$; l'action se définit comme suit: $g \cdot f(X_1, X_2) = f((g(X_1, X_2)^t)^t)$. Un théorème de E. Noether stipule que l'anneau des $\mathbf{G}$-invariants, noté $\mathbf{C}[X_1, X_2]^{\mathbf{G}}$, est une $\mathbf{C}$-algèbre de type fini. Dans notre cas, les polynômes f, g et h décrits ci-haut sont précisement les générateurs des invariants du groupe icosaédral. Ces mêmes polynômes satisfont la célèbre identité de Klein

$$h^2 + 1728f^5 = g^3.$$

Pour étudier l'équation $x^2 + y^3 = z^5$, Beukers considère l'application $\varphi : \mathbf{C}^2 \longrightarrow \mathbf{C}^3$ donnée par

$$(u,v) \longmapsto (ih(u,v), g(u,v), (1728)^{\frac{1}{5}} f(u,v))$$

où $i = \sqrt{-1}$. Celle-ci est une application quotient pour l'action de $\mathbf{G}$ et par l'identité de Klein, on voit que l'image de φ est l'ensemble des (x,y,z) satisfaisant l'équation $x^2 + y^3 = z^5$.

Beukers s'intéresse aux matrices $m \in \mathbf{GL}_2(\overline{\mathbf{Q}})$ telles que $\varphi \circ m$ est défini sur $\mathbf{Q}$. Une telle matrice est appelée une $\mathbf{Q}$-matrice. On vérifie facilement que $\varphi \circ m$ est une famille paramétrée de $x^2 + y^3 = z^5$. Inversement, il note que toute famille paramétrée de degré 60 est de la forme $\varphi \circ m$, pour un certain $m \in \mathbf{GL}_2(\overline{\mathbf{Q}})$. On remarque que si m est une $\mathbf{Q}$-matrice, alors pour tout $g \in \mathbf{G}$ et $r \in \mathbf{GL}_2(\mathbf{Q})$, $g \circ m \circ r$ est aussi une $\mathbf{Q}$-matrice. En effet, pour $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, $\sigma(\varphi \circ (g \circ m \circ r)) = \sigma(\varphi \circ m \circ r) = \sigma(\varphi \circ m) \circ r = \varphi \circ m \circ r = \varphi \circ (g \circ m \circ r)$. On obtient ainsi une relation d'équivalence entre $\mathbf{Q}$-matrices; m' est équivalente à m si $m' = g \circ m \circ r$ pour un certain $g \in \mathbf{G}$, $r \in \mathbf{GL}_2(\mathbf{Q})$.

On dira que deux familles paramétrées de solutions (F, G, H) et (F', G', H') sont *équivalentes* s'il existe une matrice $\gamma \in \mathbf{GL}_2(\mathbf{Q})$ telle que $F \circ \gamma = F'$, $G \circ \gamma = G'$ et $H \circ \gamma = H'$. Par la remarque faite ci-haut, on a

Théorème 41 *Deux* $\mathbf{Q}$*-matrices équivalentes donnent lieu à des familles paramétrées équivalentes. Ainsi, on a une surjection*

$$\left\{ \begin{array}{c} \textit{Familles d'équivalence} \\ \textit{de } \mathbf{Q}\textit{-matrices} \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \textit{Familles d'équivalence de} \\ \textit{familles paramétrées de} \\ \textit{solutions (de degré 60)} \end{array} \right\}$$

Beukers démontre le résultat suivant:

Proposition 42 *Soit* $\mathbf{x}$ *une solution primitive de l'équation* $x^2 + y^3 = z^5$*. Alors, il existe une* $\mathbf{Q}$*-matrice* m *et* $\mathbf{s} \in \mathbf{Q}^2$ *tel que* $\mathbf{x} = (\varphi \circ m)(\mathbf{s})$*. La classe d'équivalence de* m *est uniquement déterminée par la solution* $\mathbf{x}$*.*

Preuve: voir [Be], prop. 2.2.

Cette proposition est d'une grande importance pour notre étude. En fait, elle dit que l'ensemble des solutions de l'équation $x^2 + y^3 = z^5$ s'écrit comme une union disjointe de familles paramétrées.

On remarque qu'il existe une méthode explicite pour construire une $\mathbf{Q}$-matrice m associée à une solution $\mathbf{x}$, à partir de $\mathbf{u} \in \varphi^{-1}(\mathbf{x})$ quelconque. Soit la matrice jacobienne suivante

$$J = \begin{pmatrix} \frac{\partial f}{\partial u} & \frac{\partial f}{\partial v} \\ \frac{\partial g}{\partial u} & \frac{\partial g}{\partial v} \end{pmatrix}.$$

Le déterminant de la matrice J, évaluée en $\mathbf{u}$, est $-20h(\mathbf{u})$ qui est différent de zéro et on vérifie que la matrice inverse $J^{-1}(\mathbf{u})$ est une $\mathbf{Q}$-matrice pour $\mathbf{x}$.

Exemple 43 Soit la solution $(1,-1,0)$ de l'équation $x^2+y^3=z^5$. On vérifie que $\mathbf{u}=(0,(-1)^{1/20}) \in \varphi^{-1}(1,-1,0)$. Alors, la matrice

$$m = J^{-1}(\mathbf{u}) = \begin{pmatrix} \frac{(-1)^{9/20}}{2\cdot 54^{1/5}} & 0 \\ 0 & \frac{-(-1)^{1/20}}{20} \end{pmatrix}$$

est une $\mathbf{Q}$-matrice pour la solution $(1,-1,0)$. On a

$$(\varphi \circ m)(12s,20t) = (F(s,t),G(s,t),H(s,t)),$$

où

$$\begin{aligned} F(s,t) &= 8916100448256s^{30} + 323208641124928s^{25}t^5 - 43011966868480s^{20}t^{10} \\ &\quad -207463680s^{10}t^{20} - 75168s^5t^{25} + t^{30}, \\ G(s,t) &= -429981696s^{20} + 680804352s^{15}t^5 - 10243584s^{10}t^{10} - 32832s^5t^{15} - t^{20}, \\ H(s,t) &= 12st(20736s^{10} + 1584s^5t^5 - t^{10}). \end{aligned}$$

Finalement, $\varphi \circ m(0,20) = (1,-1,0)$.

Remarque 44 À l'avenir, on utilisera les formes non homogènes de F, G et H pour définir une famille paramétrée (F,G,H). Ainsi, une famille paramétrée de l'équation $x^2+y^3=z^5$ sera donnée par trois polynômes non nuls F, G, $H \in \mathbf{Q}[t]$ satisfaisant $\mathrm{pgcd}(F,G,H)=1$ et $F(t)^2+G(t)^3=H(t)^5$ pour tout $t \in \mathbf{Q}$. Si $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\mathbf{Q})$,

$$\gamma(t) = \frac{at+b}{ct+d}$$

et l'équivalence entre familles paramétrées de solutions est définie de la même façon qu'auparavant.

3.2 Lien entre familles paramétrées de solutions de $x^2 + y^3 = z^5$ et représentations galoisiennes

Avant de montrer le lien qu'il existe entre les familles paramétrées de solutions pour l'équation $x^2 + y^3 = z^5$ et les représentations galoisiennes, on doit énoncer un théorème qui nous sera utile. On fait d'abord une brève digression sur le corps de fonctions $\overline{\mathbf{Q}}(t)$.

On rappelle que le corps de fonctions $\mathbf{Q}(t)$ est défini par

$$\left\{ \frac{f(t)}{g(t)} : f, g \in \mathbf{Q}[T] \text{ et } g \text{ non identiquement nul} \right\}.$$

Par exemple, la fonction rationnelle

$$\frac{1-t}{2+t}$$

est un élément bien défini de $\mathbf{Q}(t)$. Le corps $\overline{\mathbf{Q}}(t)$ est défini de façon similaire: où les fonctions f et g appartiennent maintenant à l'anneau des polynômes $\overline{\mathbf{Q}}[T]$. L'anneau des entiers de $\overline{\mathbf{Q}}(t)$ peut se définir simplement comme étant l'anneau des polynômes $\overline{\mathbf{Q}}[T]$. Ainsi, les idéaux premiers de l'anneau des entiers de $\overline{\mathbf{Q}}(t)$ sont les polynômes irréductibles à coefficients dans $\overline{\mathbf{Q}}$. Étant donné que $\overline{\mathbf{Q}}$ est algébriquement clos, les polynômes irréductibles de $\overline{\mathbf{Q}}[T]$ sont les polynômes de degré un. Les idéaux engendrés par les polynômes constants sont bien sur l'anneau $\overline{\mathbf{Q}}[T]$ tout entier et ne sont pas intéressants. En excluant les idéaux (0) et (1), tout idéal premier de $\overline{\mathbf{Q}}[T]$ peut donc s'écrire $(t - \alpha)$, où $\alpha \in \overline{\mathbf{Q}}$.

Théorème 45 *Soit L une extension finie de $\overline{\mathbf{Q}}(t)$. Si l'anneau des entiers de L est non ramifié en $(t - \alpha)$ pour tout $\alpha \in \overline{\mathbf{Q}}$, alors $L = \overline{\mathbf{Q}}(t)$.*

Le lecteur remarquera que ce théorème est analogue à un théorème bien connu: il n'existe pas d'extension non triviale de $\mathbf{Q}$ qui soit non ramifiée en tous les nombres premiers p. Nous sommes présentement prêts pour le théorème principal de cette section.

Soit $(A(t), B(t), C(t))$ une famille paramétrée de l'équation $x^2+y^3 = z^5$. Définissons

$$E_t : y^2 = x^3 + 27B(t)x - 54A(t) \tag{3.1}$$

une courbe elliptique sur $\mathbf{Q}(t)$, c'est-à-dire pour chaque valeur de $t \in \mathbf{Q}$, E_t est une courbe elliptique définie sur $\mathbf{Q}$ si $\Delta(E_t) \neq 0$. La courbe E_t peut donc être vue comme une famille de courbes elliptiques.

Remarque 46 Le discriminant minimal $\Delta_{\min}$ de la courbe

$$E : y^2 = x^3 + 27bx - 54a$$

déterminé dans la remarque 9 se calcule de façon similaire pour la courbe E_t définie par l'équation (3.1).

Par analogie avec l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ sur les points d'ordre n d'une courbe elliptique $E/\mathbf{Q}$, le groupe de Galois $\mathrm{Gal}(\overline{\mathbf{Q}(t)}/\mathbf{Q}(t))$ agit sur les points d'ordre n de la courbe E_t. Ainsi, soit

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}(t)}/\mathbf{Q}(t)) \longrightarrow \mathbf{GL}_2(\mathbf{F}_5)$$

la représentation fournie par les points de 5-division de la courbe E_t. Ayant fixé le choix de la courbe E_t, le théorème principal de cette section s'énonce ainsi:

Théorème 47 *Il existe une injection*

$$\left\{ \begin{array}{c} \textit{Familles paramétrées de} \\ \textit{solutions de} \\ x^2 + y^3 = z^5 \\ \textit{à équivalence près} \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \textit{Représentations} \\ \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_5) \\ \textit{à conjugaison près} \end{array} \right\}.$$

Avant d'en faire la démonstration, voici un résultat de K. Rubin et A. Silverberg (thm. 5.1 dans [RS]).

Théorème 48 *Soit une courbe elliptique $E/\mathbf{Q}$ d'équation*

$$y^2 = x^3 + ax + b.$$

Définissons

$$a(t) = a\sum_{k=0}^{20}\binom{20}{k}\alpha_k t^k, \qquad b(t) = b\sum_{k=0}^{30}\binom{30}{k}\beta_k t^k$$

où, $\alpha_k, \beta_k \in \mathbf{Q}[J]$*, avec* $J = 1 - j(E)/1728 = 27b^2/(4a^3 + 27b^2)$ *sont des polynômes donnés dans l'appendice B. Soit* E_t*, une courbe elliptique sur* $Q(t)$ *définie par*

$$y^2 = x^3 + a(t)x + b(t).$$

Alors, pour tout $t \in \mathbf{Q}$ *tel que* E_t *est non singulière,* $\rho_5^{E_t} \simeq \rho_5^E$*. De plus, si* $ab \neq 0$ *et* E' *est une courbe elliptique sur* $\mathbf{Q}$ *telle que* $\rho_5^{E'} \simeq \rho_5^E$*, alors* $E' \simeq_{\mathbf{Q}} E_{t_0}$ *pour un certain* $t_0 \in \mathbf{Q}$*.*

Preuve: voir [RS].

Lemme 49 *Soit* E_t *une courbe elliptique définie sur* $\mathbf{Q}(t)$ *et soit* $\Delta(t)$ *son discriminant minimal. Si la représentation mod 5, définie par* E_t*, est constante, alors* $\Delta(t) = df(t)^5$*, où* $d \in \mathbf{Q}$ *et* $f \in \mathbf{Q}[t]$*.*

Preuve: Soit $\alpha \in \overline{\mathbf{Q}}$ tel que $\Delta(\alpha) = 0$. Il suffit de montrer que $\mathrm{ord}_{(t-\alpha)}\Delta(t) \equiv 0 \pmod 5$. On considère E_t sur $\overline{\mathbf{Q}}((t-\alpha))$, c'est-à-dire les séries formelles de $t-\alpha$ à coefficients dans $\overline{\mathbf{Q}}$.
(On rappelle que toute série formelle non nulle de $\overline{\mathbf{Q}}((t-\alpha))$ s'écrit

$$f(t) = \sum_{i \geq m_0} a_i (t-\alpha)^i$$

avec $m_0 \in \mathbf{Z}$, $a_i \in \overline{\mathbf{Q}}$ et $a_{m_0} \neq 0$. On définit la valuation $\nu(f) = \mathrm{ord}_{(t-\alpha)}f(t)$ de f comme étant l'entier m_0. Le corps $\overline{\mathbf{Q}}((t-\alpha))$ est un corps local dont l'anneau de valuation est $\overline{\mathbf{Q}}[[t-\alpha]]$, c'est-à-dire l'ensemble des séries formelles à exposant ≥ 0. Son corps résiduel est $\overline{\mathbf{Q}}$.)

Puisque $\overline{\mathbf{Q}}$ est algébriquement clos, la courbe E_t, considérée sur $\overline{\mathbf{Q}}((t-\alpha))$, a réduction multiplicative déployée et la théorie de Tate fournit un isomorphisme entre $E_t(\overline{\mathbf{Q}}((t-\alpha)))$ et $\overline{\mathbf{Q}}((t-\alpha))^\times/q^{\mathbf{Z}}$, où $\nu(q) > 0$ (cf. [Si2], Chap. V).

L'hypothèse que la représentation mod 5 est constante équivaut à dire que les points d'ordre 5 de $E_t(\overline{\mathbf{Q}(t)})$ sont dans $\overline{\mathbf{Q}}(t) \hookrightarrow \overline{\mathbf{Q}}((t-\alpha))$. L'isomorphisme donné

par la théorie de Tate entraîne que q est une puissance $5^{\text{ième}}$ et donc $\nu(q) \equiv 0 \pmod 5$. Puisque la valuation de q coïncide avec la valuation de Δ, on a $\nu(\Delta) \equiv 0 \pmod 5$, c'est-à-dire $\text{ord}_{(t-\alpha)}\Delta(t) \equiv 0 \pmod 5$. □

Preuve du théorème 47: En utilisant le théorème 48 et le lemme 49, il est facile de montrer que la courbe

$$E_t : y^2 = x^3 + 27B(t)x - 54A(t)$$

provenant d'une famille paramétrée $(A(t), B(t), C(t))$, donne lieu a une représentation $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_5)$ définie à conjugaison près. Au lieu de faire appel à ces deux résultats, voici une démonstration directe de l'existence de l'application.

Soit L l'extension finie de $\mathbf{Q}(t)$ sur lequel sont définis les points de 5-division de la courbe E_t définie par (3.1). On vérifie qu'il n'y a pas de premier propre $p(t)$ dans l'anneau des entiers de $\mathbf{Q}(t)$, c'est-à-dire l'anneau des polynômes $\mathbf{Q}[T]$, qui se ramifie dans l'anneau des entiers de L.

En effet, supposons que $p(t)$ se ramifie dans l'anneau des entiers de L, c'est-à-dire $p(t)$ divise le discriminant de L. Le discriminant de L est seulement divisible par les premiers qui divisent le discriminant minimal de E_t. En d'autres mots, E_t a mauvaise réduction en $p(t)$. Mais alors, la courbe E_t a réduction multiplicative en $p(t)$ et $p(t)$ divise le discriminant avec multiplicité 5 (voir l'exemple 8 et la remarque 46). En utilisant le théorème 36, pour la courbe E_t, la représentation ρ est non ramifiée en $p(t)$ ce qui contredit notre hypothèse.

Soit maintenant le corps L', l'union du corps L et de $\overline{\mathbf{Q}}(t)$. Alors, L' est une extension de $\overline{\mathbf{Q}}(t)$ et $L \subset L'$. Puisque l'anneau des entiers de $\overline{\mathbf{Q}}(t)$ est non ramifié en $(t-\alpha)$ $\forall \alpha \in \overline{\mathbf{Q}}$ et que l'anneau des entiers de L est non ramifié pour tout idéal propre de $\mathbf{Q}[T]$, alors l'anneau des entiers de L' est aussi non ramifié en $(t-\alpha)$ $\forall \alpha \in \overline{\mathbf{Q}}$. Par le théorème 45, $L' = \overline{\mathbf{Q}}(t)$ et $L \subset \overline{\mathbf{Q}}(t)$. Ainsi, on a $\text{Gal}(\overline{\mathbf{Q}(t)}/\overline{\mathbf{Q}}(t)) \subset \text{Gal}(\overline{\mathbf{Q}(t)}/L) = \ker \rho$ et la représentation ρ "ne dépend pas de t".

Pour montrer l'injectivité, on fait appel au théorème 48 et au lemme 49. Soient

(a,b,c) et (a',b',c') deux solutions primitives de $x^2+y^3=z^5$ et les courbes

$$\begin{aligned} E: &\quad y^2 = x^3 + 27bx - 54a \\ E': &\quad y^2 = x^3 + 27b'x - 54a' \end{aligned}$$

telles que $\rho_5^E \simeq \rho_5^{E'}$. Soit

$$E_t : y^2 = x^3 + 27b(t)x - 54a(t),$$

où $a(t) = a\sum_{k=0}^{30}\binom{30}{k}\beta_k t^k$ et $b(t) = b\sum_{k=0}^{20}\binom{20}{k}\alpha_k t^k$ sont les polynômes obtenus par le théorème 48.

Le discriminant minimal de la courbe E_t est de la forme $\pm 2^u 3^v(a(t)^2+b(t)^3)$ (voir l'exemple 8 et la remarque 9). En utilisant le lemme 49 et ses notations avec la courbe E_t, on a $a(t)^2+b(t)^3 = f(t)^5$ et $d = \pm 2^u 3^v$; on pose $c(t) = f(t)$.

Par le théorème 48, il existe un $t_0 \in \mathbf{Q}$ tel que $E_{t_0} \simeq_{\mathbf{Q}} E'$. En fait, $E_{t_0} = E'$. En effet, les courbes E_{t_0} et E' sont données par

$$\begin{aligned} E_{t_0}: &\quad y^2 = x^3 + 27b(t_0)x - 54a(t_0) \quad \text{et} \\ E': &\quad y'^2 = x'^3 + 27b'x' - 54a'. \end{aligned}$$

Puisque $E_{t_0} \simeq_{\mathbf{Q}} E'$, il existe un $u \in \mathbf{Q}^\times$ tel que $x = u^2x'$ et $y = y^3y'$, c'est-à-dire $u^4b' = b(t_0)$ et $u^6a' = a(t_0)$ (cf. [Si1] p.50). On a

$$c(t_0)^5 = a(t_0)^2 + b(t_0)^3 = (u^6a')^2 + (u^4b')^3 = u^{12}(a'^2+b'^3) = u^{12}c'^5$$

et puisque $u \in \mathbf{Q}, u = \pm 1$ et $E_{t_0} = E'$.

Puisque $(a,b,c) = (a(0),b(0),c(0))$ et $(a',b',c') = (a(t_0),b(t_0),c(t_0))$, ces deux solutions sont dans une même famille paramétrée. □

3.3 Construction de familles paramétrées de solutions

Dans la prochaine section, on donne une liste des familles paramétrées de solutions de l'équation $x^2+y^3=z^5$ qui nous sont connues jusqu'à ce jour. Cette liste est

constituée de familles paramétrées de solutions trouvées par Beukers ainsi que celles qu'on a concues par une nouvelle méthode. Les familles paramétrées de solutions de Beukers proviennent de toutes les solutions (a, b, c) trouvées à l'ordinateur dont $|c| \leq 10000$ et $|b| \leq 3000000$. Dans cette section, on explique une méthode pour trouver de nouvelles familles paramétrées de solutions qui donneront lieu à des représentations mod 5 irréductibles.

D'après la section précédente, à toute famille paramétrée de l'équation $x^2 + y^3 = z^5$, on peut associer une représentation galoisienne $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_5)$. Par la construction dans la démonstration du théorème 47, il est facile de construire la représentation mod 5 à partir d'une famille paramétrée $(A(t), B(t), C(t))$ de l'équation $x^2 + y^3 = z^5$. En effet, il suffit de prendre n'importe quelle solution particulière (a, b, c) de la famille $(A(t), B(t), C(t))$ et de considérer la courbe elliptique d'équation

$$y^2 = x^3 + 27bx - 54a.$$

En prenant la représentation de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ fournie par les points de 5-division de cette courbe elliptique, on obtient la représentation mod 5 cherchée, définie à conjugaison près.

Maintenant, que fait-on si on veut construire la famille paramétrée à partir d'une représentation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_5)$? On suppose, dans cette section, que la représentation ρ est irréductible. Premièrement, on remarque que toutes les représentations irréductibles associées aux familles paramétrées de solutions de l'équation $x^2 + y^3 = z^5$ satisfont les hypothèses du théorème de Ribet.

En effet, toute représentation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_5)$ considérée provient d'une courbe elliptique E donnée par l'équation

$$y^2 = x^3 + 27bx - 54a,$$

où $a^2 + b^3 = c^5$ est une solution primitive. La courbe E a un déterminant minimal $\Delta_{\min} = \pm 2^s 3^t p_1 \cdots p_k$ et un conducteur $N = 2^\alpha 3^\beta p_1 \cdots p_k$, où $\{p_1, \ldots p_k\}$ sont les diviseurs de c, exceptés possiblement 2 et 3. Pour utiliser le théorème de Ribet, on doit trouver la valeur de $N(\rho)$. Voici d'abord un lemme qui nous aidera à calculer

$N(\rho)$.

Lemme 50 *Soit (a,b,c) une solution primitive de $x^2+y^3=z^5$ et on soit la courbe elliptique E d'équation*

$$y^2 = x^3 + 27bx - 54a$$

et de discriminant minimal $\Delta_{\min}$. Si $p=2$ ou 3, alors $\mathrm{ord}_p(\Delta_{\min}) \not\equiv 0 \pmod 5$.

Preuve: On sait que le discriminant de E est $\Delta = 2^6 3^9 c^5$ (voir l'exemple 8). La courbe minimale de E est obtenue par un changement de coordonnées

$$x = u^2 x' + r \quad \text{et} \quad y = u^3 y' + u^2 s x' + t$$

où $u \in \mathbf{Z} \setminus \{0\}$ et $r,s,t, \in \mathbf{Z}$ (cf. [Si1], Chap. VII, prop. 1.3). Avec ces nouvelles coordonnées, le discriminant minimal de E est donné par $\Delta_{\min} = u^{-12}\Delta$. Puisque a et b sont copremiers, les seules valeurs possibles de u sont 1, 2, 3 ou 6 (ceci se voit en regardant les quantités c_4, c_6 et Δ). On a donc

$$\mathrm{ord}_2(\Delta_{min}) = \begin{cases} 6 & \text{si } u = 1,3 \\ 11 & \text{si } u = 2,6 \end{cases} \quad \text{et} \quad \mathrm{ord}_3(\Delta_{\min}) = \begin{cases} 9 & \text{si } u = 1,2 \\ 2 & \text{si } u = 3,6 \end{cases}$$

Dans tous les cas, si $p \in \{2,3\}$, $\mathrm{ord}_p(\Delta_{\min}) \not\equiv 0 \pmod 5$. □

Avec ce lemme, il est maintenant facile de trouver le valeur de $N(\rho)$. Puisque $\mathrm{ord}_p(\Delta_{\min}) \not\equiv 0 \pmod 5$ pour $p = 2$ et 3, et que $\mathrm{ord}_p(\Delta_{\min}) \equiv 0 \pmod 5$ pour les autres nombres premiers p (on remarque que la courbe E est semi-stable pour ces p), $N(\rho) = 2^\alpha 3^\beta$, où α et β sont les exposants de 2 et 3 respectivement du conducteur N de E. De plus, les exposants α et β sont bornés par 8 et 5 respectivement (§1.1).

Ainsi, par le théorème de Ribet, toute représentation irréductible $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_5)$, associée à une famille paramétrée $(A(t), B(t), C(t))$ de l'équation $x^2 + y^3 = z^5$, peut être obtenue à partir d'une "newform" f de niveau divisant $2^8 3^5$. On dira alors que la fonction f est associée à la famille paramétrée $(A(t), B(t), C(t))$.

On énonce ce résultat sous forme de théorème bien qu'il soit une conséquence directe du théorème 47 et du théorème de Ribet.

Théorème 51 *Si la famille paramétrée $(A(t), B(t), C(t))$ de l'équation $x^2+y^3 = z^5$ donne lieu à une représentation irréductible, alors il existe une "newform" normalisée f mod 5 de niveau divisant $2^8 3^5$ associée à $(A(t), B(t), C(t))$.*

Corollaire 52 *Soient $(A(t), B(t), C(t))$ et $(A'(t), B'(t), C'(t))$ deux familles paramétrées de l'équation $x^2 + y^3 = z^5$ qui donnent lieu à des représentations irréductibles et soient f et f' leur "newform" normalisée mod 5 de niveau divisant $2^8 3^5$ associée. Si les familles $(A(t), B(t), C(t))$ et $(A'(t), B'(t), C'(t))$ sont équivalentes, alors $f \equiv f'$ (mod 5).*

Ce résultat donne un critère pour vérifier que deux solutions particulières de l'équation $x^2 + y^3 = z^5$ n'appartiennent pas à la même famille paramétrée.

Voici d'abord une première application de ce résultat qui est utile pour déterminer des familles paramétrées de solutions non mentionnées par Beukers dans [Be].

Soit (a, b, c) une solution primitive de l'équation $x^2+y^3 = z^5$. Alors, $(-a, b, c)$ est aussi une solution primitive. Bien que cette dernière solution soit obtenue de façon banale à partir de la première, ces deux solutions n'appartiennent pas en général à la même famille paramétrée. Si $(A(t), B(t), C(t))$ est la famille paramétrée de la solution (a, b, c), celle de $(-a, b, c)$ est simplement $(-A(t), B(t), C(t))$. Cependant, les polynômes $(A(t), B(t), C(t))$ et $(-A(t), B(t), C(t))$ ne sont pas en général $\mathbf{GL}_2(\mathbf{Q})$-équivalents, c'est-à-dire il n'existe pas necéssairement une matrice $\gamma \in \mathbf{GL}_2(\mathbf{Q})$ telle que $(A(\gamma(t)), B(\gamma(t)), C(\gamma(t)))$ soit égale à $(-A(t), B(t), C(t))$.

En effet, soient

$$\begin{aligned} E &: y^2 = x^3 + 27bx - 54a \text{ et} \\ E' &: y^2 = x^3 + 27bx + 54a \end{aligned}$$

les courbes elliptiques construites à partir des solutions (a, b, c) et $(-a, b, c)$. Ces deux courbes sont des tordues l'une de l'autre sur $\mathbf{Q}(i)$; l'application

$$(x, y) \longmapsto (-x, iy)$$

est un isomorphisme entre E et E'. Les coefficients $a_p(E')$ sont égaux à $\left(\frac{-1}{p}\right) a_p(E)$,

c'est-à-dire

$$a_p(E') = \begin{cases} a_p(E) & \text{si } p \equiv 1 \pmod 4 \\ -a_p(E) & \text{si } p \equiv -1 \pmod 4, \end{cases}$$

(voir théorème 17). Si f et f' sont les "newforms" normalisées de niveau divisant $2^8 3^5$ associées à E et E' respectivement, il résulte, en regardant leur série de Fourier, que $f = f'$ seulement si $a_p(E) = 0$ pour $p \equiv -1 \pmod 4$. En général, on a $f \neq f'$. En utilisant le corollaire 52, on conclut que les solutions (a, b, c) et $(-a, b, c)$ ne sont, en général, pas dans la même famille paramétrée.

On a montré le théorème suivant:

Théorème 53 *Soit (a, b, c) une solution primitive de l'équation $x^2 + y^3 = z^5$ et soit la courbe elliptique E d'équation*

$$y^2 = x^3 + 27bx - 54a.$$

La solution $(-a, b, c)$ appartient à la même famille paramétrée de solutions que (a, b, c) seulement si

$$a_p(E) = 0 \qquad \textit{pour} \qquad p \equiv -1 \textit{ (mod 4).}$$

Après avoir construit toutes les familles paramétrées de solutions associées aux solutions $(-a, b, c)$, où (a, b, c) sont les solutions particulières trouvées par Beukers, on aimerait construire de nouvelles familles paramétrées de solutions. Ces familles ne donneront que des solutions primitives satisfaisant $|b| > 10000$ ou $|c| > 3000000$.

On note d'abord que l'on peut construire une famille paramétrée à partir d'une de ses solutions particulières (cf. [Be]). Ainsi, pour trouver une nouvelle famille paramétrée, il suffit de trouver une solution particulière qui donne lieu à une "newform" normalisée de niveau divisant $2^8 3^5$ qui n'apparaît pas dans la liste constituée de "newforms" normalisées provenant de familles paramétrées de solutions déjà connues. Ceci peut se faire sans difficulté; si on a une solution primitive (a, b, c) de l'équation $x^2 + y^3 = z^5$, on calcule les coefficients a_p de la courbe elliptique

$$E : y^2 = x^3 + 27bx - 54a$$

(à l'aide de l'ordinateur, par exemple PARI) et on identifie avec les tables disponibles (table de Cremona, par exemple) la fonction propre normalisée associée (de niveau divisant $2^8 3^5$) à l'aide des coefficients $a_p(E)$.

Par le théorème 51, il est donc naturel d'essayer de construire une solution primitive de l'équation $x^2 + y^3 = z^5$ à partir d'une "newform" normalisée f de niveau divisant $2^8 3^5$.

Lorsque la fonction f a niveau N et admet des coefficients de Fourier rationnels, le théorème 25 de Eichler-Shimura conclut qu'il existe une courbe elliptique E_f de conducteur N associée à f. Il est tentant alors de rendre le modèle de la courbe E_f de la forme

$$y^2 = x^3 + 27bx - 54a$$

pour une certaine solution primitive $a^2 + b^3 = c^5$. L'obstacle avec cette méthode est que le conducteur de la courbe E_f est $N = 2^\alpha 3^\beta$ ($\alpha \leq 8$, $\beta \leq 5$) et il est indépendant du modèle (sur $\mathbf{Q}$) de la courbe. Puisque le conducteur de la courbe

$$E : y^2 = x^3 + 27bx - 54a$$

($a^2 + b^3 = c^5$) est divisible précisement par $\{\text{diviseurs premiers de } c\} \bigcup \{2, 3\}$, la courbe E_f peut seulement donner lieu à une solution (a, b, c), où c est de la forme $2^s 3^t$. En utilisant les mêmes idées que dans la démonstration du lemme 50, on montre que $s \in \{0, 1, 2\}$ et $t \in \{0, 1\}$ et donc, ces solutions donneront lieu à des familles paramétrées de solutions trouvées par Beukers.

On utilise les travaux de Rubin et Silverberg pour remédier à ce problème. Dans [RS], à partir d'une courbe elliptique E définie sur $\mathbf{Q}$, les auteurs donnent explicitement l'ensemble des courbes elliptiques $E'/\mathbf{Q}$ satisfaisant $\rho_5^E \simeq \rho_5^{E'}$.

Soit une "newform" normalisée f à coefficients de Fourier rationnels de niveau divisant $2^8 3^5$ et soit E_f, la courbe elliptique associée par le théorème 25 de Eichler-Shimura. Les résultats de Rubin et Silverberg nous fournissent les courbes elliptiques $E/\mathbf{Q}$ ayant la même représentation mod 5 que celle de E_f. Parmi ces courbes E, on regarde celles qui sont susceptibles d'avoir un modèle de la forme

$$y^2 = x^3 + 27bx - 54a \tag{3.2}$$

pour une certaine solution primitive (a, b, c). Il est malheureusement trop difficile de vérifier directement s'il existe une courbe E ayant un tel modèle. On a cependant recours aux j-invariants associés aux courbes elliptiques E pour déterminer s'il peut exister une courbe ayant un modèle de la forme (3.2). En effet, on a vu qu'une courbe elliptique ayant un modèle de la forme (3.2), où $a^2+b^3 = c^5$, a un j-invariant égal à $\frac{1728b^3}{c^5}$ (voir exemple 10). En regardant les j-invariants des courbes E, il est possible de voir s'il en existe de la forme $\frac{1728b^3}{c^5}$. Si tel est le cas et si $c^5 - b^3$ est un carré, on obtient une solution primitive de l'équation $x^2 + y^3 = z^5$.

Cette méthode admet par contre des limites.

(1) La fonction qui exprime le j-invariant de la famille des courbes elliptiques E, donnée par le théorème de Rubin et Silverberg, est un quotient de polynômes dans $\mathbf{Q}[J]$, où J est le j-invariant de la courbe E_f. Étant donné la complexité de cette fonction, on a pas d'autre choix que de spécialiser cette fonction en des valeurs particulières. Il nous est donc difficile de trouver, a priori, les courbes elliptiques E ayant un j-invariant de la forme

$$\frac{1728b^3}{c^5}.$$

(2) En calculant le j-invariant d'une courbe elliptique, on considère la classe d'isomorphisme de la courbe. Ainsi, soit la courbe elliptique E_f et soit une courbe E satisfaisant $\rho_5^{E_f} \simeq \rho_5^E$, $j(E) = \frac{1728b^3}{c^5}$ et $c^5 - b^3 = a^2$. La courbe d'équation

$$E' : y^2 = x^3 + 27bx - 54a$$

est isomorphe à la courbe E (puisqu'elles ont le même j-invariant) mais la représentation ρ_5^E n'est pas en général isomorphe à $\rho_5^{E'}$. Si tel est le cas, la courbe E' est une tordue de E sur une extension non triviale de $\mathbf{Q}$. La "newform" f' de niveau divisant $2^8 3^5$ associée à E' sera alors une tordue de la fonction f.

Malgré ces inconvénients, on trouve une nouvelle famille paramétrée.

Exemple 54 Les notations utilisées dans cet exemple sont celles de Cremona dans [Cr]. Soit f la "newform" 288A de niveau $2^5 3^2$. La courbe elliptique E_f (=288A1)

d'équation

$$E_f : y^2 = x^3 + 3x$$

est associée à la fonction f par le théorème de Eichler-Shimura. On utilise le théorème 5.5 dans [RS] avec $D = -3$. Si $j(t)$ est le j-invariant de la courbe elliptique E_t (selon les notations de [RS]), alors on vérifie que

$$j(\frac{1}{6}) = \frac{1728 \cdot (-469957964531)^3}{(4546613)^5}.$$

De plus, $(4546613)^5 - (-469957964531)^3 = (325173797539747828)^2$; cette solution est une solution primitive de l'équation $x^2 + y^3 = z^5$. Si

$$\begin{aligned} a &= 325173797539747828, \\ b &= -4699579646531, \\ c &= 4546613 \text{ et} \end{aligned}$$

$$E : y^2 = x^3 + 27bx - 54a,$$

en calculant les coefficients $a_p(E)$, on vérifie que la "newform" normalisée associée à E est 288A. Bien qu'on obtienne la même forme modulaire (288A) au départ et à l'arrivée, ceci n'a généralement pas lieu (voir remarque (2) ci-haut).

3.4 Liste des familles paramétrées de solutions

Dans cette section, on donne une liste des familles paramétrées de solutions de l'équation $x^2 + y^3 = z^5$ qui nous sont connues jusqu'à ce jour. Cette liste n'est pas complète et on croit qu'elles sont beaucoup plus nombreuses que celles mentionnées ici.

Les polynômes $A(t)$ et $B(t)$ d'une famille paramétrée $(A(t), B(t), C(t))$ sont déterminés à partir du polynôme $C(t)$ (cf. [Be]). Si $c(s,t)$ dénote l'homogénisation du polynôme $C(t)$, alors les polynômes homogènes $a(s,t)$ et $b(s,t)$ associés aux polynômes $A(t)$ et $B(t)$ respectivement sont donnés par

$$b = \lambda \begin{vmatrix} c_{ss} & c_{st} \\ c_{st} & c_{tt} \end{vmatrix} \qquad \text{et} \qquad a = \mu \begin{vmatrix} c_s & c_t \\ b_s & b_t \end{vmatrix}$$

où $c_s = \frac{\partial c(s,t)}{\partial s}$ et $c_{st} = \frac{\partial^2 c(s,t)}{\partial s \partial t}$, etc. et λ, $\mu \in \mathbf{Q}$. Les polyômes $A(t)$ et $B(t)$ sont obtenus simplement en déshomogénisant les polynômes $a(s,t)$ et $b(s,t)$. Pour connaître les polynômes $A(t), B(t)$ et $C(t)$ d'une famille paramétrée, il est donc suffisant de donner le polynôme $C(t)$ ainsi que les constantes λ et μ.

En vertu du théorème 51, on donne la "newform" mod 5 de niveau divisant $2^8 3^5$ associée à chaque famille paramétrée (donnant lieu à une représentation mod 5 irréductible). Les notations uilisées sont celles de Cremona dans [Cr]. Lorsque la famille paramétrée donne lieu à une représentation réductible, on inscrit "réductible" au lieu de la "newform".

Pour chaque famille paramétrée, le tableau qui suit donne une solution primitive (a,b,c) qui provient de la famille paramétrée, le numéro du polynôme $C(t)$ donné dans l'appendice A, les valeurs λ et μ correspondantes et la "newform" associée.

a	b	c	$C(i)$	$\frac{1}{\lambda}$	$\frac{1}{\mu}$	forme
1	-1	0	C(1)	17424	-240	réductible
-1					240	réductible
0	1	1	C(2)	17424	240	288E
1	0	1	C(3)	4356	120	1728A
-1					-120	1728W
3	-2	1	C(4)	17424	240	1728Z
-3					-240	1728Q
10	-7	-3	C(5)	17424	240	96B
-10					-240	96A
39151	-1153	-6	C(6)	17424	240	24A
-39151					-240	48A
7792	-393	7	C(7)	17424	240	1728AA
-7792					-240	1728R
411	-41	10	C(8)	17424	240	216A
-411					-240	432H
654	127	19	C(9)	17424	240	1728D
-654					-240	1728I

a	b	c	$C(i)$	$\frac{1}{\lambda}$	$\frac{1}{\mu}$	forme
1	-1226	-55	C(10)	17424	-240	réductible
36599					240	1728Z
-36599					-240	1728N
12092581	-52684	57	C(11)	4356	120	réductible
-12092581					-120	réductible
647992	-5879	185	C(12)	17424	240	864D
-647992					-240	864A
1506463	-16514	-295	C(13)	17424	240	576F
2730128	12931	395	C(14)	17424	240	1728Y
-2730128					-240	1728O
3353687	-29158	-423	C(15)	17424	240	192B
-3353687					-240	192A
4387861	29396	537	C(16)	4356	-120	réductible
-4387861					120	réductible
5574720	51701	701	C(17)	17424	240	864D
-5574720					-240	864A
4942947	53831	710	C(18)	17424	240	216B
-4942947					-240	432D
168454745	-251382	1657	C(19)	17424	240	1728H
-168454745					-240	1728C
128301258	-322343	-1763	C(20)	17424	-240	864K
-128301258					240	864C
184589480	-442143	-2207	C(21)	17424	-240	864I
-184589480					240	864L
-888155653	-894906	2353	C(22)	17424	240	576G
74330984303	-16061281	16908	C(23)	17424	240	réductible
-74330984303					-240	réductible
325173797539747828	-469957964531	4546613	C(24)	17424	-240	288A

Remarque 55 Les solutions $(\pm 74330984303, -16061281, 16908)$ ont été obtenues à partir de la famille paramétrée $C(23)$, mentionnée par Don Zagier (cf. [Be]).

3.5 Borne supérieure pour le nombre de familles paramétrées de solutions

On rappelle que toute représentation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_5)$ apparaissant dans le théorème 47 provient d'une courbe elliptique

$$E : y^2 = x^3 + 27bx - 54a$$

pour une certaine solution primitive (a, b, c) de l'équation $x^2 + y^3 = z^5$. De plus, cette représentation est non ramifiée à l'extérieur de $\{2, 3, 5\}$ (voir exemple 34). Étant donné le théorème 47, pour trouver une borne supérieure pour le nombre de familles paramétrées de solutions, il suffit d'estimer le nombre de représentations $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_5)$ non ramifiées à l'extérieur de $\{2, 3, 5\}$ provenant de certaines courbes elliptiques.

Soit N cette estimation et divisons N en trois termes

$$N = N_{\text{irréd.}} + N_{\text{tot. réd.}} + N_{\text{triang.}},$$

où $N_{\text{irréd.}}$, $N_{\text{tot. réd.}}$ et $N_{\text{triang.}}$ correspondent aux estimations de représentations qui sont irréductibles, totalement réductibles et réductibles mais non totalement réductibles (c.-à-d. que les matrices sont triangulaires). On distingue d'abord les représentations irréductibles et réductibles.

a) Représentations irréductibles

Lorsque la représentation ρ est irréductible, le théorème de Ribet indique que ρ provient d'une "newform" normalisée de niveau divisant $2^8 3^5$. Avant de poursuivre, voici d'abord une remarque.

En partant d'une courbe elliptique

$$E : y^2 = x^3 + 27bx - 54a$$

où $a^2 + b^3 = c^5$, on associe, par la conjecture de Shimura-Taniyama, une "newform" $f \in S(N)$ à coefficients de Fourier rationnels, où N est le conducteur de la courbe

E ($N = 2^\alpha 3^\beta p_1 \cdots p_k$ où $\{p_1, \ldots, p_k\}$ sont les diviseurs premiers ($\neq 2, 3$) de c et $\alpha \leq 8$, $\beta \leq 5$). Si la représentation $\rho = \rho_5^E$ fournie par les points de 5-division de la courbe E est irréductible alors elle est isomorphe à la semi-simplification ρ_5^f de ρ_5^E (§2.4). Le théorème de Ribet indique qu'il existe une "newform" normalisée f' de niveau plus petit, plus précisement $f' \in S(2^\alpha 3^\beta)$, et un idéal λ de $\mathcal{O}_f$ tels que ρ soit isomorphe à $\rho_\lambda^{f'}$. Bien que la forme modulaire du départ f ait des coefficients de Fourier rationnels, la fonction $f' \in S(2^\alpha 3^\beta)$ ne possède pas necéssairement des coefficients de Fourier rationnels. Donc, en abaissant le niveau de la forme modulaire par le théorème de Ribet, on perd la propriété que les coefficients de Fourier de la nouvelle forme modulaire, obtenue par le théorème de Ribet, ait des coefficients de Fourier rationnels.

Voici un exemple, tiré de [Da], qui illustre ce phénomène.

Exemple 56 La courbe elliptique

$$E : y^2 + xy = x^3 - x^2 - 10x - 12$$

est une courbe modulaire de conducteur $N = 2 \cdot 23$ et discriminant $\Delta_{\min} = -2^{10} \cdot 23$. Puisque la représentation $\rho = \rho_5^E$ fournie par les points de 5-division de E est irréductible, le théorème de Ribet indique que la représentation ρ est modulaire de niveau 23, c'est-à-dire que la représentation ρ provient d'une "newform" $f \in S(23)$. Or, il n'existe pas de fonction propre normalisée f dans $S(23)$ ayant des coefficients de Fourier rationnels. En effet, si f avait des coefficients de Fourier rationnels, il existerait, par le théorème de Eichler-Shimura, une courbe elliptique $E_f/\mathbf{Q}$ de conducteur 23 mais il n'existe pas de telle courbe elliptique définie sur $\mathbf{Q}$.

Il est possible de calculer la fonction propre normalisée $f \in S(23)$ obtenue par le théorème de Ribet (cf. [Da], section 3, exemple 3). Cette forme modulaire a ses coefficients de Fourier dans $\mathbf{Z}[\sqrt{5}]$ et le début de son expansion s'écrit

$$\begin{aligned} f \;=\; & q - \overline{\omega} q^2 - \sqrt{5} q^3 - \omega q^4 - 2\overline{\omega} q^5 - (2 + \overline{\omega}) q^6 + 2\omega q^7 - \sqrt{5} q^8 \\ & + 2q^9 + 2(1 + \overline{\omega}) q^{10} - 2(1 + \omega) q^{11} + (2 + \omega) q^{12} + 3q^{13} + 2q^{14} \\ & - 2(3 - \omega) q^{15} - 3\overline{\omega} q^{16} + 2(1 + \overline{\omega}) q^{17} - \overline{\omega} q^{18} - 2q^{19} + \ldots \end{aligned}$$

où $\omega = \frac{1+\sqrt{5}}{2}$ est le nombre d'or et $\overline{\omega}$ est son conjugué complexe. Puisque la représentation $\rho^f_{(\sqrt{5})}$ est isomorphe à ρ^E_5, les coefficients de Fourier $c_p(f)$ de f sont congruents aux coefficients $a_p(E)$ de E modulo $(\sqrt{5})$ $(p \neq 2, 23)$ (théorème 32 et 38). On vérifie les premières valeurs dans la tableau suivant:

p	2	3	5	7	11	13	17	19
$a_p(E)$	-	0	4	-4	2	-2	-2	-2
$c_p(f)$	$-\overline{\omega}$	$-\sqrt{5}$	$-1+\sqrt{5}$	$1+\sqrt{5}$	$-3-\sqrt{5}$	3	$3-\sqrt{5}$	-2

Calcul de $N_{\text{irréd.}}$*:* Pour estimer le nombre de représentations irréductibles ρ : $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_5)$ provenant d'une certaine courbe elliptique

$$E : y^2 = x^3 + 27bx - 54a$$

où $a^2 + b^3 = c^5$, on calcul le nombre de "newforms" de $S(N)$, où N divise $2^8 3^5$. Puisque ces formes modulaires de $S(N)$ sont linéairement indépendantes, leur nombre est au plus égal à la dimension de l'espace $S^{\text{new}}(N)$. On calcul la dimension de cet espace en calculant la dimension de $S(N)$, par le théorème 21, et la dimension de $S^{\text{old}}(N)$ récursivement, utilisant l'équation (2.1), page 19. La dimension de $S^{\text{new}}(N)$ est alors la différence de la dimension de $S(N)$ avec la dimension de $S^{\text{old}}(N)$. On retrouve les valeurs de ces dimensions pour les diviseurs de $2^8 3^5$ dans le tableau suivant:

N	$S_2(N)$	$S_2^{\text{old}}(N)$	$S_2^{\text{new}}(N)$	N	$S_2(N)$	$S_2^{\text{old}}(N)$	$S_2^{\text{new}}(N)$
2	0	0	0	$2 \cdot 3^3$	4	2	2
2^2	0	0	0	$2^2 \cdot 3^3$	10	9	1
2^3	0	0	0	$2^3 \cdot 3^3$	25	21	4
2^4	0	0	0	$2^4 \cdot 3^3$	55	47	8
2^5	1	0	1	$2^5 \cdot 3^3$	121	105	16
2^6	3	2	1	$2^6 \cdot 3^3$	253	221	32
2^7	9	5	4	$2^7 \cdot 3^3$	529	465	64
2^8	21	15	6	$2^8 \cdot 3^3$	1081	953	128
3	0	0	0	3^4	4	2	2
$2 \cdot 3$	0	0	0	$2 \cdot 3^4$	16	12	4
$2^2 \cdot 3$	0	0	0	$2^2 \cdot 3^4$	37	33	4
$2^3 \cdot 3$	1	0	1	$2^3 \cdot 3^4$	85	73	12
$2^4 \cdot 3$	3	2	1	$2^4 \cdot 3^4$	181	159	22
$2^5 \cdot 3$	9	7	2	$2^5 \cdot 3^4$	385	337	48
$2^6 \cdot 3$	21	17	4	$2^6 \cdot 3^4$	793	701	92
$2^7 \cdot 3$	49	41	8	$2^7 \cdot 3^4$	1633	1441	192
$2^8 \cdot 3$	105	89	16	$2^8 \cdot 3^4$	3313	2937	376
3^2	0	0	0	3^5	19	7	12
$2 \cdot 3^2$	0	0	0	$2 \cdot 3^5$	64	52	12
$2^2 \cdot 3^2$	1	0	1	$2^2 \cdot 3^5$	136	124	12
$2^3 \cdot 3^2$	5	4	1	$2^3 \cdot 3^5$	289	253	36
$2^4 \cdot 3^2$	13	11	2	$2^4 \cdot 3^5$	595	523	72
$2^5 \cdot 3^2$	33	28	5	$2^5 \cdot 3^5$	1225	1081	144
$2^6 \cdot 3^2$	73	64	9	$2^6 \cdot 3^5$	2485	2197	288
$2^7 \cdot 3^2$	161	141	20	$2^7 \cdot 3^5$	5041	4465	576
$2^8 \cdot 3^2$	337	299	38	$2^8 \cdot 3^5$	10153	9001	1152
3^3	1	0	1				

Théorème 57 *Il existe au plus 3432 familles paramétrées de solutions de l'équation $x^2 + y^3 = z^5$ donnant lieu à des représentations mod 5 irréductibles.*

On pose alors

$$N_{\text{irréd.}} = 3432.$$

Voici quelques remarques sur ce résultat.

(1) Cette borne s'avère quelque peu grossière. En effet, puisque les représentations qu'on considère proviennent de certaines courbes elliptiques, elles prennent leurs valeurs dans le groupe $\mathbf{GL}_2(\mathbf{F}_5)$. Or, parmis les "newforms" f qu'on a comptées, certaines d'entre elles donnent lieu à des représentations ρ_λ^f prenant leurs valeurs dans $\mathbf{GL}_2(\mathbf{F}_\lambda)$ qui est strictement plus grand que $\mathbf{GL}_2(\mathbf{F}_5)$ (§2.4). Ces "newforms" normalisées ne peuvent pas être obtenues à partir d'une solution de $x^2 + y^3 = z^5$ et ne devraient donc pas être comptées. Ceci peut se faire en étudiant l'anneau des entiers sur lequel sont définis les coefficients de Fourier de la forme modulaire f et fera l'un des objets d'une étude ultérieure.

(2) Toutes les familles paramétrées de solutions de l'équation $x^2 + y^3 = z^5$ trouvées jusqu'à ce jour donnent lieu à des "newforms" de niveau inférieur ou égal à $1728 = 2^6 \cdot 3^3$. Une question qu'on peut se poser est la suivante:

Question 58 *Existe-il des familles paramétrées de solutions de l'équation $x^2+y^3 = z^5$ donnant lieu à des "newforms" de niveau minimal plus grand que 1728?*

Si la réponse à cette question s'avérait être "non", la valeur de $N_{\text{irréd.}}$ serait considérablement améliorée; elle passerait de 3432 à 92. Cette question mérite qu'on s'y penche et fera aussi l'un des objets d'une étude future.

b) Représentations réductibles

On a vu dans la section §2.4 que si $\rho : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}_2(\mathbf{F}_5)$ provient d'une courbe elliptique E et est réductible, alors dans une base de $E[5]$ judicieusement choisie,

la représentation ρ s'écrit

$$\rho : \sigma \longmapsto \begin{pmatrix} \psi_1(\sigma) & c(\sigma) \\ 0 & \psi_2(\sigma) \end{pmatrix}.$$

Étant donné que ρ est un homomorphisme, il satisfait $\rho(\sigma\tau) = \rho(\sigma)\rho(\tau)$ et cette condition se traduit en termes matriciels par

$$\begin{pmatrix} \psi_1(\sigma\tau) & c(\sigma\tau) \\ 0 & \psi_2(\sigma\tau) \end{pmatrix} = \begin{pmatrix} \psi_1(\sigma)\psi_1(\tau) & \psi_1(\sigma)c(\tau) + c(\sigma)\psi_2(\tau) \\ 0 & \psi_2(\sigma)\psi_2(\tau) \end{pmatrix} \tag{3.3}$$

pour tout σ, $\tau \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. On voit que ψ_1 et ψ_2 sont des homomorphismes et on pose $\psi = \frac{\psi_2}{\psi_1}$. Puisque le déterminant de la représentation ρ est le caractère cyclotomique χ_5, c'est-à-dire $\psi_1 \cdot \psi_2 = \chi_5$ (voir la proposition 30), le nombre d'homomorphismes

$$\psi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{F}_5^\times$$

est égal au nombre de possibilités d'homomorphismes ψ_1 et ψ_2.

Le corps K découpé par l'homomorphisme ψ, c'est-à-dire le corps fixé par le noyau de ψ, est une extension abélienne de $\mathbf{Q}$ (de degré 1, 2 ou 4) puisque $\mathbf{F}_5^\times$ est commutatif.

Théorème 59 (Kronecker-Weber) *Toute extension finie abélienne de* $\mathbf{Q}$ *est contenue dans un corps cyclotomique.*

Preuve: voir [Wa], Chap. 14.

Par ce théorème, le corps K est contenu dans $\mathbf{Q}(\zeta_n)$ pour un certain n.

Proposition 60 *Le nombre premier p se ramifie dans $\mathbf{Q}(\zeta_n)$ si et seulement si p divise n.*

Preuve: voir [Wa], prop. 2.3.

Étant donné que la représentation ρ est non ramifiée à l'extérieur de $\{2, 3, 5\}$, le corps K est contenu dans $\mathbf{Q}(\zeta_{2^a 3^b 5^c})$ pour un certain a, b et $c \in \mathbf{Z}_{>0}$.

Ainsi, puisque l'homomorphisme

$$\psi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{F}_5^\times$$

est non ramifié en dehors de 2,3 et 5, il se factorise à travers le quotient de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ à $\mathrm{Gal}(\mathbf{Q}(\zeta_{2^a3^b5^c})/\mathbf{Q})$. Par abus de notation, on notera

$$\psi : \mathrm{Gal}(\mathbf{Q}(\zeta_{2^a3^b5^c})/\mathbf{Q}) \longrightarrow \mathbf{F}_5^\times$$

l'homomorphisme obtenu par passage au quotient.

Comment déterminer les entiers a, b et c?

Proposition 61 $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$

Preuve: voir [FT], Chap. VI, thm. 44.

Proposition 62 *Soit* $n = 2^\alpha p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. *Alors,*

$$(\mathbf{Z}/n\mathbf{Z})^\times \simeq \begin{cases} C_{2^{\alpha-1}} \times C_{(p_1-1)p_1^{\alpha_1-1}} \times \cdots C_{(p_s-1)p_s^{\alpha_s-1}} & si\ \alpha \leq 2 \\ C_2 \times C_{2^{\alpha-2}} \times C_{(p_1-1)p_1^{\alpha_1-1}} \times \cdots \times C_{(p_s-1)p_s^{\alpha_s-1}} & si\ \alpha > 2, \end{cases}$$

où C_a *dénote le groupe cyclique d'ordre* a.

Par la combinaison de ces deux propositions,

$$\mathrm{Gal}(\mathbf{Q}(\zeta_{2^a3^b5^c})/\mathbf{Q}) \simeq \begin{cases} C_{2^{a-1}} \times C_{2.3^{b-1}} \times C_{4.5^{c-1}} & \text{si } a \leq 2 \\ C_2 \times C_{2^{a-2}} \times C_{2.3^{b-1}} \times C_{4.5^{c-1}} & \text{si } a > 2. \end{cases}$$

Puisque l'opération de groupe sur $\mathbf{F}_5^\times$ est d'ordre 4 et que ψ est un homomorphisme, le groupe $\mathrm{Gal}(\mathbf{Q}(\zeta_{2^a3^b5^c})/\mathbf{Q})$ ne peut contenir d'élément d'ordre 3 et 5; donc $b = c = 1$. De plus, on peut prendre $a = 4$ car le groupe multiplicatif défini sur $\mathbf{F}_5^\times$ est isomorphe à C_4 et tout homomorphisme de C_{2^a} $(a > 2)$ dans C_4 se factorise à travers un homomorphisme de C_4 dans C_4.

Pour connaître le nombre de possibilités d'homomorphismes ψ_1 et ψ_2, on est donc amené à compter le nombre d'homomorphismes

$$\psi : \mathrm{Gal}(\mathbf{Q}(\zeta_{240})/\mathbf{Q}) \longrightarrow C_4.$$

Puisque la groupe de Galois $\mathrm{Gal}(\mathbf{Q}(\zeta_{240})/\mathbf{Q})$ est isomorphe à $C_4 \times C_4 \times C_2 \times C_2$, par la proposition 62, on compte 64 possibilités pour l'homomorphisme ψ.

Calcul de $N_{\text{tot. réd.}}$*:* Lorsque la représentation ρ est totalement réductible, $c(\sigma) = 0$ pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. La représentation ρ s'écrit donc

$$\rho : \sigma \longmapsto \begin{pmatrix} \psi_1(\sigma) & 0 \\ 0 & \psi_2(\sigma) \end{pmatrix}$$

pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Les repésentations considérées sont cependant définies seulement à conjugaison près. Puisque que les matrices

$$\begin{pmatrix} \psi_1(\sigma) & 0 \\ 0 & \psi_2(\sigma) \end{pmatrix} \qquad \text{et} \qquad \begin{pmatrix} \psi_2(\sigma) & 0 \\ 0 & \psi_1(\sigma) \end{pmatrix}$$

sont conjuguées et que $\psi_1 \neq \psi_2$ (sinon la surjectivité de χ_5 serait altérée), on a

$$N_{\text{tot. réd.}} = 32.$$

Calcul de $N_{\text{triang.}}$*:* On fixe maintenant l'homomorphisme ψ_1 ou de façon équivalente l'homomorphisme ψ. La fonction

$$\frac{c}{\psi_1} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{F}_5$$

satisfait

$$\frac{c}{\psi_1}(\sigma\tau) = \frac{c}{\psi_1}(\sigma) \cdot \psi(\tau) + \frac{c}{\psi_1}(\tau).$$

Dénotons toujours par K, le corps découpé par l'homomorphisme

$$\psi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{F}_5^{\times}.$$

La fonction $\frac{c}{\psi_1}$ restreinte à $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$ est maintenant un homomorphisme car si σ, $\tau \in \mathrm{Gal}(\overline{\mathbf{Q}}/K)$, alors

$$\psi(\tau) = 1 \qquad \text{et donc} \qquad \frac{c}{\psi_1}(\sigma\tau) = \frac{c}{\psi_1}(\sigma) + \frac{c}{\psi_1}(\tau).$$

Ainsi, pour chaque homomorphisme ψ fixé, la fonction

$$c : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{F}_5$$

donne lieu à un homomorphisme

$$\frac{c}{\psi_1} : \mathrm{Gal}(\overline{\mathbf{Q}}/K) \longrightarrow \mathbf{F}_5$$

noté $\frac{c}{\psi_1}$ par abus de notation.

Soit maintenant L le corps découpé par l'homomorphisme $\frac{c}{\psi_1} : \mathrm{Gal}(\overline{\mathbf{Q}}/K) \to \mathbf{F}_5$. Le corps L est une extension abélienne de K (de degré 1 ou 5). En utilisant la théorie du corps de classes sur K, on peut calculer les extensions possibles L et estimer ainsi le nombre d'homomorphismes $\frac{c}{\psi_1}$. Ce calcul sera exécuté ultérieurement pour but de publication.

Appendice A

$$C(1) = 12t^{11} + 19008t^6 - 248832t,$$

$$C(2) = t^{12} - 12t^{11} + 132t^{10} - 880t^9 + 1980t^8 + 3168t^7 - 32736t^6 + 101376t^5 - 245520t^4 + 461120t^3 - 394944t^2 + 46848t + 150592,$$

$$C(3) = t^{12} - 55t^9 - 165t^6 + 275t^3 + 25,$$

$$C(4) = t^{12} - 132t^{10} - 1320t^9 - 5940t^8 - 19008t^7 - 47520t^6 - 57024t^5 + 71280t^4 + 380160t^3 + 513216t^2 + 362880t + 191808,$$

$$C(5) = -3t^{12} - 12t^{11} + 132t^{10} + 1980t^8 + 3168t^7 - 3168t^6 - 12672t^5 + 39600t^4 + 10560t^3 + 61248t^2 + 26112t - 27072,$$

$$C(6) = -6t^{12} - 12t^{11} + 12672t^{10} - 457380t^9 + 8437770t^8 - 98630136t^7 + 788874768t^6 - 4452512328t^5 + 17822147310t^4 - 49714538940t^3 + 92201264496t^2 - 102450626388t + 51726152718,$$

$$C(7) = 7t^{12} - 12t^{11} - 3696t^{10} - 64680t^9 - 582120t^8 - 3326400t^7 - 13020480t^6 - 35925120t^5 - 69854400t^4 - 93139200t^3 - 79833600t^2 - 38361600t - 7257600,$$

$$C(8) = 10t^{12} - 12t^{11} - 264t^{10} - 1540t^9 - 990t^8 - 3960t^7 - 10560t^6 + 3960t^5 + 24750t^4 + 47300t^3 + 6600t^2 + 7500t + 10150,$$

$$C(9) = 19t^{12} + 60t^{11} + 528t^{10} + 440t^9 - 3960t^8 - 6336t^7 - 10560t^6 - 12672t^5 - 31680t^4 - 14080t^3 + 16896t^2 + 7680t + 5632,$$

$$C(10) = -55t^{12} + 312t^{11} + 660t^{10} - 11000t^9 + 49500t^8 - 126720t^7 + 203808t^6 - 221760t^5 + 198000t^4 - 176000t^3 + 137280t^2 - 66432t + 11840,$$

$$C(11) = 57t^{12} - 204t^{11} - 14916t^{10} - 159555t^9 - 902385t^8 - 3263040t^7 - 8103645t^6 - 14227290t^5 - 17728425t^4 - 15395325t^3 - 8881125t^2 - 3063675t - 478650,$$

$$
\begin{aligned}
C(12) &= 185t^{12} + 144t^{11} - 2046t^{10} - 9680t^9 - 13365t^8 - 15840t^7 - 20724t^6 - 9504t^5 + \\
&\quad 8415t^4 + 16720t^3 + 6930t^2 + 1776t + 701, \\
C(13) &= -295t^{12} - 204t^{11} + 3630t^{10} - 5500t^9 + 12375t^8 - 3960t^7 - 4092t^6 - 3960t^5 + \\
&\quad 12375t^4 - 5500t^3 + 3630t^2 - 204t - 295, \\
C(14) &= 395t^{12} + 1836t^{11} + 6072t^{10} + 5720t^9 - 11880t^8 - 31680t^7 - 40128t^6 - 38016t^5 - \\
&\quad 31680t^4 - 14080t^3 + 1536t + 512, \\
C(15) &= -423t^{12} - 816t^{11} + 3828t^{10} - 1320t^9 + 9900t^8 + 6336t^7 - 3168t^6 - 6336t^5 + \\
&\quad 7920t^4 + 2112t^2 + 384t - 192, \\
C(16) &= -3t^{11} + 297t^6 + 243t, \\
C(17) &= 701t^{12} - 1776t^{11} + 6930t^{10} - 16720t^9 + 8415t^8 + 9504t^7 - 20724t^6 + 15840t^5 - \\
&\quad 13365t^4 + 9680t^3 - 2046t^2 - 144t + 185, \\
C(18) &= 710t^{12} - 1116t^{11} + 5808t^{10} - 11220t^9 - 2970t^8 + 11880t^7 - 14256t^6 + 7128t^5 - \\
&\quad 8910t^4 + 5940t^3 - 324t + 162, \\
C(19) &= 1657t^{12} + 804t^{11} - 9834t^{10} - 31020t^9 - 31185t^8 - 26136t^7 - 22572t^6 - 7128t^5 + \\
&\quad 4455t^4 + 5940t^3 + 1782t^2 + 324t + 81, \\
C(20) &= 25t^{12} - 4950t^{10} + 57200t^9 - 334125t^8 + 1235520t^7 - 3129060t^6 + 5559840t^5 - \\
&\quad 6826545t^4 + 5445440t^3 - 2411046t^2 + 305136t + 107749, \\
C(21) &= 64t^{12} - 2112t^{10} + 10560t^9 - 23760t^8 + 38016t^7 - 47520t^6 + 28512t^5 + 17820t^4 - \\
&\quad 47520t^3 + 32076t^2 - 11340t + 2997, \\
C(22) &= 64t^{12} + 384t^{11} + 2112t^{10} + 7040t^9 + 7920t^8 - 6336t^7 - 32736t^6 - 50688t^5 - \\
&\quad 61380t^4 - 57640t^3 - 24684t^2 - 1464t + 2353, \\
C(23) &= 12(256t^{11} - 1584t^6 - 81t), \\
C(24) &= 125t^{12} + 1650t^{10} - 7425t^8 - 5940t^6 - 13365t^4 + 5346t^2 + 729.
\end{aligned}
$$

Appendice B

$$
\begin{aligned}
\alpha_0 &= 1, \\
\alpha_1 &= 1, \\
\alpha_2 &= 1 - J, \\
\alpha_3 &= 1 - 3J - 2J^2, \\
\alpha_4 &= 1 - 6J - (139J^2 + 48J^3)/17, \\
\alpha_5 &= 1 - 10J - (355J^2 + 272J^3 + 36J^4)/17, \\
\alpha_6 &= 1 - 15J - (725J^2 + 957J^3 + 256J^4)/17, \\
\alpha_7 &= 1 - 21J - (1295J^2 + 2667J^3 + 1294J^4 - 156J^5)/17, \\
\alpha_8 &= 1 - 28J - (2114J^2 + 6412J^3 + 5335J^4 - 832J^5 - 432J^6)/17, \\
\alpha_9 &= 1 - 36J - (3234J^2 + 13860J^3 + 18399J^4 - 1440J^5 - 3320J^6 - 864J^7)/17, \\
\alpha_{10} &= 1 - 45J - (51810J^2 + 303534J^3 + 599577J^4 + 37395J^5 - 114352J^6 - 109872J^7 - \\
&\quad 10368J^8)/187, \\
\alpha_{11} &= 1 - 55J - (6600J^2 + 51414J^3 + 142527J^4 + 30795J^5 - 7622J^6 - 48952J^7 - 19008J^8)/17, \\
\alpha_{12} &= 1 - 66J - (8965J^2 + 90684J^3 + 336633J^4 + 116658J^5 + 84163J^6 - 148080J^7 - \\
&\quad 117776J^8 - 24192J^9)/17, \\
\alpha_{13} &= 1 - 78J - (11869J^2 + 152724J^3 + 731445J^4 + 313326J^5 + 533299J^6 - 274416J^7 - \\
&\quad 559508J^8 - 35232J^9 - 108864J^{10})/17, \\
\alpha_{14} &= 1 - 91J - (15379J^2 + 247247J^3 + 1483053J^4 + 657345J^5 + 2089633J^6 + \\
&\quad 174677J^7 - 3066512J^8 + 1027280J^9 - 585216J^{10} - 373248J^{11})/17,
\end{aligned}
$$

$$\alpha_{15} = 1 - 105J - (19565J^2 + 386841J^3 + 2837263J^4 + 1071135J^5 + 6664879J^6 + 5206179J^7 - 16810714J^8 + 5968812J^9 + 3457408J^{10} - 4435776J^{11} - 746496J^{12})/17,$$

$$\alpha_{16} = 1 - 120J - (24500J^2 + 587496J^3 + 5166538J^4 + 1140360J^5 + 18887284J^6 + 34450584J^7 - 75167809J^8 + 492672J^9 + 50776288J^{10} - 11536896J^{11} - 17024256J^{12})/17,$$

$$\alpha_{17} = 1 - 136J - 1780J^2 - 51128J^3 - 530426J^4 + 18824J^5 - 2913092J^6 - 9751240J^7 + 15122369J^8 + 9456832J^9 - 13418768J^{10} - 10084288J^{11} + 10920960J^{12} + 248832J^{13},$$

$$\alpha_{18} = 1 - 153J - 2172J^2 - 73908J^3 - 892290J^4 + 354978J^5 - 7213804J^6 - 38920356J^7 + 37171977J^8 + 60303087J^9 + 16401120J^{10} - 170087328J^{11} + 107379712J^{12} - 9504000J^{13} + 2985984J^{14},$$

$$\alpha_{19} = 1 - 171J - 2622J^2 - 104652J^3 - 1453386J^4 + 1267110J^5 - 17046952J^6 - 135295884J^7 + 46284513J^8 + 174262509J^9 + 683618766J^{10} - 1401592464J^{11} + 584002432J^{12} + 150976512J^{13} - 125203968J^{14} + 35831808J^{15},$$

$$\alpha_{20} = 1 - 190J - 3135J^2 - 145464J^3 - 2300862J^4 + 3364140J^5 - 38641174J^6 - 421126184J^7 - 124394691J^8 - 171099294J^9 + 5923508469J^{10} - 8685664368J^{11} + 3654839008J^{12} - 1176272128J^{13} + 2234836224J^{14} - 1636319232J^{15} + 429981696J^{16},$$

$$\beta_0 = 1,$$

$$\beta_1 = 2,$$

$$\beta_2 = 3 + J,$$

$$\beta_3 = 4 + (19J + 9J^2)/7,$$

$$\beta_4 = 5 + (34J + 35J^2 + 8J^3)/7,$$

$$\beta_5 = 6 + 2(325J + 583J^2 + 251J^3 + 24J^4)/91,$$

$$\beta_6 = 7 + (845J + 2511J^2 + 1751J^3 + 80J^4)/91,$$

$$\beta_7 = 8 + (143J + 703J^2 + 777J^3 + 29J^4 - 92J^5)/13,$$

$$\beta_8 = 9 + (156J + 1294J^2 + 2188J^3 + 373J^4 - 656J^5 - 144J^6)/13,$$

$$\beta_9 = 10 + 2(858J + 12474J^2 + 30624J^3 + 13371J^4 - 13218J^5 - 7352J^6 - 864J^7)/143,$$

$$\beta_{10} = 11 + (10725J + 293502J^2 + 991914J^3 + 795711J^4 - 418767J^5 - 507056J^6 - 145104J^7 - 6912J^8)/1001,$$

$$\beta_{11} = 12 + (715J + 43197J^2 + 191862J^3 + 238350J^4 - 38937J^5 - 154575J^6 - 85688J^7 - 9648J^8)/91,$$

$$\beta_{12} = 13 + (286J + 67617J^2 + 380028J^3 + 662241J^4 + 107310J^5 - 371057J^6 - 392744J^7 - 82128J^8)/91,$$

$$\beta_{13} = 14 - 2(13J - 3949J^2 - 27247J^3 - 62547J^4 - 29529J^5 + 21233J^6 + 54379J^7 + 18752J^8 + 272J^9)/7,$$

$$\beta_{14} = 15 - 13J + 1667J^2 + 13783J^3 + 39933J^4 + 30969J^5 + 2289J^6 - 46099J^7 - 25792J^8 + 16J^9 - 384J^{10},$$

$$\beta_{15} = 16 - 25J + 2403J^2 + 23351J^3 + 82799J^4 + 89049J^5 + 56857J^6 - 113347J^7 - 108843J^8 + 2636J^9 - 400J^{10} - 1728J^{11},$$

$$\beta_{16} = 17 - 40J + 3388J^2 + 38088J^3 + 161510J^4 + 221704J^5 + 261980J^6 - 217864J^7 - 413231J^8 + 8160J^9 + 13856J^{10} - 5120J^{11} - 6912J^{12},$$

$$\beta_{17} = 18 - 2(204J - 16388J^2 - 210392J^3 - 1047914J^4 - 1746512J^5 - 3098964J^6 + 827832J^7 + 4966321J^8 + 76324J^9 - 221744J^{10} - 208640J^{11} + 138240J^{12} + 82944J^{13})/7,$$

$$\beta_{18} = 19 - (7293J - 578340J^2 - 8387868J^3 - 48371358J^4 - 94627338J^5 - 232655540J^6 - 39750828J^7 + 403291863J^8 + 21122997J^9 + 4631136J^{10} - 39873120J^{11} - 15169792J^{12} + 20535552J^{13} + 5971968J^{14})/91,$$

$$\beta_{19} = 20 - (9633J - 772293J^2 - 12538860J^3 - 82740972J^4 - 185352258J^5 - 605974486J^6 - 355084236J^7 + 1160500848J^8 + 62864553J^9 + 135215763J^{10} - 49421136J^{11} - 223421024J^{12} + 8802816J^{13} + 88259328J^{14} + 11943936J^{15})/91,$$

$$\beta_{20} = 21 - (135850J - 11177529J^2 - 201583008J^3 - 1507200042J^4 - 3793336548J^5 - 16085890314J^6 - 16289869336J^7 + 34526209575J^8 - 115646454J^9 + 6254997315J^{10} + 7271447016J^{11} - 9059068128J^{12} - 9447997952J^{13} + 4309426944J^{14} + 2956621824J^{15} + 143327232J^{16})/1001,$$

$$
\begin{aligned}
\beta_{21} &= 22 - 2(12155J - 1036431J^2 - 20623911J^3 - 173266890J^4 - 482501922J^5 - \\
&\quad 2609714030J^6 - 3819754718J^7 + 6424335879J^8 - 713141385J^9 + 514831629J^{10} + \\
&\quad 3595587861J^{11} + 842148056J^{12} - 5075106016J^{13} - 771525120J^{14} + \\
&\quad 1741181184J^{15} + 398628864J^{16})/143, \\
\\
\beta_{22} &= 23 - (2717J - 241637J^2 - 5274533J^3 - 49434846J^4 - 150402366J^5 - \\
&\quad 1024787914J^6 - 1990883498J^7 + 3001464713J^8 - 643759567J^9 - 756531393J^{10} + \\
&\quad 1861304607J^{11} + 3842211568J^{12} - 2807570272J^{13} - 3699388928J^{14} + \\
&\quad 1539989248J^{15} + 733224960J^{16} + 95551488J^{17})/13, \\
\\
\beta_{23} &= 24 - (3289J - 306383J^2 - 7298797J^3 - 75837417J^4 - 249391530J^5 - \\
&\quad 2119805718J^6 - 5192588698J^7 + 7733724470J^8 - 1794609707J^9 - 5491442763J^{10} - \\
&\quad 914927913J^{11} + 21236689467J^{12} + 6768088108J^{13} - 29438790944J^{14} + \\
&\quad 2230554752J^{15} + 6841353984J^{16} - 64447488J^{17} + 429981696J^{18})/13, \\
\\
\beta_{24} &= 25 - (27508J - 2691414J^2 - 69656972J^3 - 797964461J^4 - 2810102280J^5 - \\
&\quad 29555919908J^6 - 88134506104J^7 + 140455145235J^8 - 14346704572J^9 - \\
&\quad 142183615222J^{10} - 260123244540J^{11} + 399412791773J^{12} + 936124288336J^{13} - \\
&\quad 946299684336J^{14} - 473425872896J^{15} + 547643666176J^{16} - 98786414592J^{17} + \\
&\quad 21054173184J^{18} + 10319560704J^{19})/91, \\
\\
\beta_{25} &= 26 - 2(16250J - 1672790J^2 - 46845480J^3 - 588768145J^4 - 2202248390J^5 - \\
&\quad 28462011020J^6 - 100668298880J^7 + 182231986895J^8 + 33247831470J^9 - \\
&\quad 151971650150J^{10} - 746058724600J^{11} - 190714623295J^{12} + 3012941752670J^{13} - \\
&\quad 514345504280J^{14} - 3596959091232J^{15} + 2435460930560J^{16} - 251308367360J^{17} - \\
&\quad 186907392000J^{18} + 94506393600J^{19} + 10319560704J^{20})/91, \\
\\
\beta_{26} &= 27 - (2925J - 317110J^2 - 9574210J^3 - 131440975J^4 - 518385385J^5 - \\
&\quad 8182082100J^6 - 33639132540J^7 + 71920859125J^8 + 42059449675J^9 + \\
&\quad 4271199130J^{10} - 406685281010J^{11} - 813284452425J^{12} + 1760449216785J^{13} + \\
&\quad 1947869739440J^{14} - 4664750038576J^{15} + 2012915893760J^{16} + 529629981440J^{17} - \\
&\quad 550520156160J^{18} + 53527080960J^{19} + 54607675392J^{20})/7, \\
\\
\beta_{27} &= 28 - (3393J - 387585J^2 - 12574890J^3 - 187829730J^4 - 775884645J^5 - \\
&\quad 14874579435J^6 - 69941089620J^7 + 180444466800J^8 + 190496524455J^9 +
\end{aligned}
$$

$$322135166745J^{10} - 866597775210J^{11} - 5136257200890J^{12} + 2346424807005J^{13} + 21274535872755J^{14} - 27633870852984J^{15} + 5269341610512J^{16} + 6800561464320J^{17} - 1157611621120J^{18} - 2744861644800J^{19} + 1276230463488J^{20} - 36118462464J^{21})/7,$$

$$\beta_{28} = 29 - 558J + 67167J^2 + 2334780J^3 + 37807605J^4 + 162579870J^5 + 3767209215J^6 + 19990254960J^7 - 62788004865J^8 - 97644174930J^9 - 275678461035J^{10} - 41617916820J^{11} + 3082666356735J^{12} + 3336703533090J^{13} - 20112039551475J^{14} + 18083589754536J^{15} - 111802681872J^{16} - 1969309527552J^{17} - 6598483313920J^{18} + 6267833026560J^{19} - 1241189609472J^{20} - 345848610816J^{21} + 61917364224J^{22},$$

$$\beta_{29} = 30 - 2(319J - 40455J^2 - 1502577J^3 - 26291835J^4 - 117028485J^5 - 3263140755J^6 - 19323907125J^7 + 73950146595J^8 + 152153088525J^9 + 584372990475J^{10} + 997418209005J^{11} - 4647934166985J^{12} - 17313700710615J^{13} + 51936991371855J^{14} - 37264352503815J^{15} + 11006357460336J^{16} - 40907186783280J^{17} + 70497975516672J^{18} - 48386143673600J^{19} + 16757644677120J^{20} - 5284334702592J^{21} + 2190756741120J^{22} - 371504185344J^{23}),$$

$$\beta_{30} = 31 - 725J + 96831J^2 + 3833307J^3 + 72261243J^4 + 331155495J^5 + 11067601035J^6 + 72453438615J^7 - 336492552195J^8 - 857661126255J^9 - 4157244533475J^{10} - 12492099396495J^{11} + 16171895675145J^{12} + 209687940471405J^{13} - 463497334953255J^{14} + 381320123560029J^{15} - 593972413014240J^{16} + 1373115281994864J^{17} - 1561862739489152J^{18} + 786960405859072J^{19} - 346886836346 88J^{20} - 191303639101440J^{21} + 142267828764672J^{22} - 55354123616256J^{23} + 8916100448256J^{24}.$$

Bibliographie

[Be] F. Beukers, *The diophantine equation* $Ax^p + By^q = Cz^r$, preprint nr.912 University of Utrecht (April 1995). À apparaître dans Duke Math. Journal.

[Cr] J. Cremona, *Algorithms for modular elliptic curves*, Cambridge Univ. Press, Cambridge (1992).

[Da] H. Darmon, *Serre's conjectures*, dans: *Seminar on Fermat's Last Theorem*, V. Kumar Murty ed., CMS conference proceedings Volume 17, pp. 135-155.

[DDT] H. Darmon, F. Diamond, R, Taylor, *Fermat's Last Theorem*, Current Developments in Mathematics **1**, 1995, International Press, pp. 1-157.

[DG] H. Darmon, A. Granville, *On the equations* $x^p + y^q = z^r$ *and* $z^m = F(x, y)$, Bulletin of the London Math. Society, no 129, **27** part6, November 1995, pp. 513-544.

[Fo] O. Forster, *Lectures on Riemann Surfaces*, Springer-Verlag, New York, Berlin, Heidelberg, 1981.

[FT] A. Frölich, M. J. Taylor, *Algebraic number theory*, Cambridge Univ. Press, Cambridge, 1991.

[Hi] F. Hirzebruch, *The icosahedron*, dans: Collected papers, vol.II (Springer, Berlin, 1987), 656-661.

[Ki] F. Kirwan, *Complex Algebraic Curves*, LMS Student Texts **23**, Cambridge Univ. Press, Cambridge, 1993.

[Kl] F. Klein, *Lectures on the icosahedron and the solutions of equations of the fifth degree*, London, K. Paul, Trench, Trubner (1913).

[Kn] A. W. Knapp, *Elliptic Curves*, Princeton Univ. Press, Princeton, 1992.

[Ma] B. Mazur, *Rational isogenies of prime degree*, Inv. Math. **44** (1978), 129-162.

[Ri1] K. A. Ribet, *From the Taniyama-Shimura conjecture to Fermat's Last Theorem*, Ann. Fac. Sci. Toulouse Math. **11** (1990), 116-139.

[Ri2] K. A. Ribet, *Galois representations and modular forms*, Bulletin of the AMS, vol. 32, number 4, October 1995, 375-402.

[RS] K. Rubin, A. Silverberg, *Families of elliptic curves with constant mod p representations*, dans: *Elliptic curves, modular forms, and Fermat's Last Theorem (Hong Kong, December 1994)*, Coates and Yau, eds. International Press, Cambridge (1995), 148-161.

[Se1] J.-P. Serre, *Abelian ℓ-adic Representations and Elliptic Curves*, New York: W.A. Benjamin 1968.

[Se2] J.-P. Serre, *Extensions icosaédriques*, dans: Oeuvres, Collected Papers, vol. III (Springer-Verlag, Berlin, 1985) pp. 550-554.

[Se3] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[Se4] J.-P. Serre, *Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$)*, Duke Math. J. **54** (1987), 179-230.

[Si1] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol.106, Springer-Verlag, Berlin and New York, 1986.

[Si2] J. H. Silverman, *Advanced Topics in the arithmetic of elliptic curves*, Graduate Texts in Math. vol.151, Springer-Verlag, Berlin and New York, 1994.

[ST] J. H. Silverman, J. T. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Math., Springer-Verlag, Berlin and New York, 1992.

[Sh] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princeton, NJ, 1971.

[Wa] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer-Verlag, New York, Brlin, Heidelberg, 1982.