Université Paris VI
Pierre et Marie Curie

Mémoire de Master $2^{\text{ème}}$ année

Nicolas Billerey

Sur l'équation $x^5 + y^5 = dz^p$

Directeur : Alain Kraus

Mémoire soutenu le 20 juin 2005

SUR L'ÉQUATION $x^5 + y^5 = dz^p$

par

Nicolas Billerey

Introduction

Soient d un entier naturel sans puissances cinquièmes et p un nombre premier ≥ 7. On se propose dans ce mémoire de faire quelques remarques sur l'étude de l'équation diophantienne ternaire

$$x^5 + y^5 = dz^p. \tag{1}$$

On dira qu'un triplet d'entiers $(a, b, c) \in \mathbf{Z}^3$ est une *solution* de l'équation (1) si $a^5 + b^5 = dc^p$, qu'elle est *propre* si l'on a $\mathrm{pgcd}(a, b, c) = 1$, et qu'elle est *non triviale* si $abc \neq 0$. On note $S_p(d)$ l'ensemble des solutions propres non triviales de l'équation (1). Une conséquence de la conjecture *abc* est la suivante :

Conjecture. — *Supposons que d ne soit pas la somme de deux puissances cinquièmes d'entiers relatifs non nuls. Alors, il existe une constante $c(d)$, qui ne dépend que de d, telle que si $p > c(d)$, l'ensemble $S_p(d)$ est vide.*

Les travaux de G. Frey, K. A. Ribet, J.-P. Serre et A. Wiles sur les représentations modulaires, permettent parfois d'aborder ce type de problèmes (*cf.* **[Fre86]**, **[Rib90]**, **[Ser87]** et **[Wil95]**). La méthode maintenant fréquemment utilisée à ce sujet est souvent appelée la méthode modulaire. Elle exploite les propriétés modulaires de certaines courbes elliptiques ainsi que les propriétés galoisiennes de leurs points de p-torsion. Plus précisément, à une hypothétique solution de l'équation étudiée, on associe une courbe elliptique dite *courbe de Frey* ou *courbe de Hellegouarch-Frey*, dont la représentation galoisienne dans ses points de p-torsion est liée à l'existence d'une forme modulaire parabolique

de poids et de niveau précis, qui « essentiellement » ne dépend pas de la solution considérée. Si par exemple une telle forme n'existe pas, on obtient alors une contradiction à l'existence de telles solutions. Il en est ainsi pour l'équation de Fermat classique $x^n + y^n = z^n$ $(n \geq 3)$.

L'étude de l'équation (1) ne semble pas avoir été entreprise dans la littérature. Signalons qu'un résultat figurant dans [**Kra02**] entraîne que, p étant donné, l'ensemble des entiers d sans puissances cinquièmes et sans diviseurs premiers congrus à 1 modulo 5, pour lesquels $S_p(d)$ soit non vide, est fini. Dans ce mémoire, nous mettrons en œuvre la méthode modulaire et certaines de ses variantes pour l'étude de l'équation (1). On montre notamment qu'elle permet de conclure à la vacuité de $S_p(d)$ pour $p \geq 7$, ou seulement pour une infinité de p, dans certains cas où d est de la forme $2^\alpha.3^\beta.5^\gamma$ avec $0 \leq \alpha, \beta, \gamma \leq 4$.

Ce mémoire est constitué de cinq parties et d'un appendice :

- La première concerne l'énoncé des principaux résultats obtenus.
- Dans la deuxième partie, on associe à tout élément $(a, b, c) \in S_p(d)$ une courbe elliptique $E(a, b)$ définie sur $\mathbf{Q}$ permettant de mettre en œuvre la méthode modulaire. On étudie son type de réduction en chaque nombre premier, et on détermine son conducteur.
- La troisième partie consiste en la description de la représentation $\rho_p^{a,b}$ donnant l'action du groupe de Galois absolu de $\mathbf{Q}$ sur le groupe des points de p-torsion de $E(a, b)$.
- La quatrième partie est consacrée à des rappels sur la méthode modulaire et une de ses variantes, appelée méthode symplectique dans [**HK02**].
- La dernière partie regroupe les démonstrations des résultats obtenus. Elles utilisent les propriétés de modularité de la représentation $\rho_p^{a,b}$.

La construction de la courbe $E(a, b)$ est dûe à H. Darmon. Dans l'appendice, on décrit le procédé qu'il a utilisé pour obtenir cette courbe elliptique, en vue d'une étude éventuelle de l'équation (1).

Je remercie mon directeur de mémoire, Alain Kraus, pour ses conseils durant mon travail et pour le temps qu'il m'a consacré.

Table des matières

1. Énoncés des résultats

Soient d un entier naturel non nul sans puissances cinquièmes et p un nombre premier ≥ 7. Les résultats décrits ici concernent les entiers d de la forme

$$d = 2^\alpha.3^\beta.5^\gamma, \quad \text{avec } 0 \leq \alpha, \beta, \gamma \leq 4.$$

Dans le cas particulier où $d = 1$, en utilisant la méthode modulaire « classique », on obtient l'énoncé suivant :

Théorème 1.1. — *Soit (a, b, c) un élément de $S_p(1)$, alors c est impair. Autrement dit, la puissance p-ième d'un nombre pair non nul ne peut s'écrire comme la somme de deux puissances cinquièmes d'entiers premiers entre eux.*

Pour quinze valeurs de d sur les cent vingt-cinq envisagées ci-dessus, par la même méthode que celle utilisée dans le théorème 1, on obtient une réponse complète quant à la description de $S_p(d)$:

Théorème 1.2. — *Supposons que d soit de la forme*

$$d = 2^\alpha.5^\gamma \quad \textit{avec } \alpha \in \big\{2, 3, 4\big\} \quad \textit{et} \quad 0 \leq \gamma \leq 4.$$

Alors, $S_p(d)$ est vide.

Pour certaines valeurs de d, nous obtenons une réponse partielle en démontrant que $S_p(d)$ est vide seulement pour un ensemble de nombres premiers p de densité > 0. En utilisant la méthode symplectique, on obtient à ce sujet l'énoncé suivant :

Théorème 1.3. — *Posons $d = 2^\alpha.3^\beta.5^\gamma$ et supposons que l'on soit dans l'un des cas ci-dessous :*

1. $(\alpha, \beta, \gamma) \in \big\{(3, 1, \geq 1), (3, 4, \geq 1), (4, 2, \geq 1)\big\}$ *et* $p \equiv 5$ *ou* $7 \pmod{12}$.
2. $(\alpha, \beta, \gamma) \in \big\{(3, 2, \geq 1), (4, 1, \geq 1), (4, 4, \geq 1)\big\}$ *et* $p \equiv 7, 11, 13$ *ou* $17 \pmod{24}$.
3. $(\alpha, \beta, \gamma) \in \big\{(3, 1, 0), (3, 4, 0), (4, 2, 0), (4, 3, 0)\big\}$ *et* $p \equiv 5$ *ou* $19 \pmod{24}$.
4. $(\alpha, \beta, \gamma) = (4, 3, \geq 1)$ *et* $p \equiv 3$ *ou* $5 \pmod{8}$.

Alors, $S_p(d)$ est vide.

Remarque. Il existe d'autres méthodes de résolution de l'équation (1), notamment la *méthode de réduction*, dont le principe consiste à identifier la réduction modulo certains nombres premiers de la courbe de Frey considérée (*cf.* [**HK02**, p.176] et [**Kra98**]). Cette méthode devrait permettre de conclure, pour certaines valeurs de d, le nombre premier p étant donné, à la vacuité de $S_p(d)$. Elle n'est pas exposée dans ce mémoire par manque de temps et fera l'objet de travaux ultérieurs.

2. La courbe elliptique $E(a,b)$

2.1. Définition. — Soient d un entier naturel non nul sans puissances cinquièmes et p un nombre premier ≥ 7. Considérons un élément (a,b,c) de $S_p(d)$. À un tel triplet on associe l'équation de Weierstraß $E(a,b)$ définie sur $\mathbf{Q}$:

$$y^2 = x^3 - 5(a^2+b^2)x^2 + 5\left(\frac{a^5+b^5}{a+b}\right)x \tag{2}$$

Les coefficients standard associés à cette équation sont les suivants (*cf.* [**Tat75**]) :

$$\begin{cases} a_1 = 0, & a_2 = -5(a^2+b^2), \\ a_3 = 0, & a_4 = 5\left(\frac{a^5+b^5}{a+b}\right), \\ a_6 = 0, & \\ b_2 = -20(a^2+b^2), & b_4 = 10\left(\frac{a^5+b^5}{a+b}\right), \\ b_6 = 0, & b_8 = -25\left(\frac{a^5+b^5}{a+b}\right)^2. \end{cases}$$

et

$$\begin{cases} c_4 &= 2^4.5\left(5(a^2+b^2)^2 - 3\frac{a^5+b^5}{a+b}\right) = 2^4.5(2a^4+3ba^3+7a^2b^2+3ab^3+2b^4), \\ c_6 &= 2^5.5^2(a^2+b^2)\left(2.5(a^2+b^2)^2 - 3^2\frac{a^5+b^5}{a+b}\right) \\ &= 2^5.5^2(a^6+9a^5b+12a^4b^2+18a^3b^3+12a^2b^4+9ab^5+b^6), \\ \Delta &= 2^4.5^3(a+b)^2(a^5+b^5)^2. \end{cases}$$

Puisque (a,b,c) appartient à $S_p(d)$, $E(a,b)$ représente une courbe elliptique définie sur $\mathbf{Q}$.
Notations.

1. Si ℓ est un nombre premier, on note v_ℓ la valuation ℓ-adique de $\mathbf{Z}$.
2. L'élément $(a,b,c) \in S_p(d)$ étant donné, on notera souvent E au lieu de $E(a,b)$ si cela ne prête pas à confusion.

2.2. Calcul du conducteur de E. — Considèrons un élément (a, b, c) de $S_p(d)$. Posons

$$r = \prod_{\ell | cd, \ell \neq 2,5} \ell,$$

où ℓ parcourt l'ensemble des diviseurs premiers de cd autres que 2 et 5.

Remarques préliminaires.

1. Les entiers a, b et c sont premiers entre eux deux à deux : cela résulte du fait que a, b et c sont premiers entre eux dans leur ensemble et que d est sans puissances cinquièmes.
2. Supposons d impair. Si a ou b est pair (mais pas les deux), alors c est impair. Si a et b sont impairs, alors c est pair.
3. Si d est pair, alors ab est impair.
4. Compte-tenu des deux remarques précédentes, on peut supposer, ce que l'on fera dans toute la suite, que l'on est dans l'un des cas suivants :
   (a) d est impair et ac est pair : si c est impair, alors ab est pair et l'on suppose que c'est a qui est pair.
   (b) d est pair et ab impair.

On démontre les résultats suivants :

Proposition 2.1. — *Supposons d* impair. *Alors, on a :*

1. $N_E = 2^4.5^2.r$ *si* $v_2(a) = 1$;
2. $N_E = 2^3.5^2.r$ *si* $v_2(a) \geq 2$;
3. $N_E = 2.5^2.r$ *si a est impair.*

Proposition 2.2. — *Supposons d* pair. *Alors :*

1. *Si c est* pair, *on a* $N_E = 2.5^2.r$.
2. *Si c est* impair, *alors :*
   (a) *si* $v_2(d) = 2$, *on a* $N_E = 5^2.r$;
   (b) *si* $v_2(d) = 3$ *ou* 4, *on a* $N_E = 2.5^2.r$;
   (c) *si* $v_2(d) = 1$, *on a* $N_E = 2^4.5^2.r$.

La démonstration des propositions 2.1 et 2.2 fait l'objet des § 2.2.1 à 2.2.4. Elle nécessite l'étude du type de réduction de E en chaque nombre premier.

2.2.1. Étude de la réduction de E en dehors de $\{2, 5\}$. — Soit ℓ un nombre premier distinct de 2 et 5. Si ℓ ne divise pas cd, alors d'après l'égalité (1) et le fait que $a + b$ divise $a^5 + b^5$, ℓ ne divise pas Δ et E a donc bonne réduction en ℓ.

Supposons que ℓ divise cd. Dans ce cas, ℓ divise a^5+b^5. On distingue alors deux cas suivant que $a+b$ est ou non divisible par ℓ.

2.2.1.1. Supposons que ℓ divise $a+b$.— Dans ce cas, $a \equiv -b \pmod{\ell}$ et

$$\frac{a^5+b^5}{a+b} = a^4 - a^3b + a^2b^2 - ab^3 + b^4 \equiv 5.b^4 \pmod{\ell}.$$

Par ailleurs, $(a^2+b^2)^2 \equiv 4.b^4 \pmod{\ell}$, donc $c_4 \equiv 2^4.5^2.b^4 \pmod{\ell}$, et on en déduit $v_\ell(c_4) = 0$. En effet, si ℓ divise c_4, alors ℓ divise b et a, et ceci contredit la remarque 1. L'équation (2) est donc minimale en ℓ et E a réduction multiplicative en ℓ, d'où $v_\ell(N_E) = 1$.

2.2.1.2. Supposons que ℓ ne divise pas $a+b$.— On a

$$\frac{a^5+b^5}{a+b} \equiv 0 \pmod{\ell}$$

car ℓ divise a^5+b^5 sans diviser $a+b$. Vérifions que ℓ ne divise pas a^2+b^2. Dans le cas contraire, on aurait :

$$\frac{a^5+b^5}{a+b} = a^4 - a^3b + a^2b^2 - ab^3 + b^4 \equiv b^4 + ab^3 - b^4 - ab^3 + b^4 \equiv b^4 \pmod{\ell},$$

et donc b serait divisible par ℓ, ainsi que a, ce qui est exclu, d'où l'assertion. On en déduit que $v_\ell(c_4) = 0$. Par suite, l'équation (2) est minimale en ℓ et E a réduction multiplicative. On a donc $v_\ell(N_E) = 1$.

Ceci achève le calcul de l'exposant de ℓ dans N_E.

2.2.2. Étude de la réduction de E en 5. — Comme dans le § précédent, on distingue deux cas.

2.2.2.1. Supposons que 5 ne divise pas $a+b$.— Dans ce cas, $\frac{a^5+b^5}{a+b} \equiv 1 \pmod{5}$ car $a^5+b^5 \equiv a+b \pmod{5}$. D'où :

$$(v_5(c_4), v_5(c_6), v_5(\Delta)) = (1, \geq 2, 3).$$

Le type de Kodaira de E est donc III (*cf.* tableau I, p.126 de [**Pap93**]) et l'on a ainsi $v_5(N_E) = 2$.

2.2.2.2. Supposons que 5 divise $a+b$.— Alors $a^2+b^2 \equiv -2ab \pmod{25}$, donc :

$$\begin{aligned} \tfrac{a^5+b^5}{a+b} &= a^4 - a^3b + a^2b^2 - ab^3 + b^4 \equiv a^2(a^2 - ab + b^2) - ab^3 + b^4 \\ &\equiv (-b^2 - 2ab)(-3ab) - ab^3 + b^4 \equiv 3ab^3 + 6a^2b^2 - ab^3 + b^4 \\ &\equiv b^2(b^2 + 6a^2 + 2ab) \equiv 5a^2b^2 \pmod{25}. \end{aligned}$$

Et donc $5(a^2+b^2)^2 - 3\frac{a^5+b^5}{a+b} \equiv 5a^2b^2 \pmod{25}$. On en déduit :

$$v_5(c_4) = 2, \text{ et de même } v_5(c_6) = 3.$$

Or d'après le résultat ci-dessus on a :

$$v_5(a^5 + b^5) = v_5(a + b) + 1.$$

Il en résulte que l'on a $v_5(\Delta) = 5 + 4v_5(a + b) \geq 9$. Le type de Kodaira de E est donc I_ν^* où $\nu = 4v_5(a + b) - 1$ et l'on obtient $v_5(N_E) = 2$ (*cf. loc. cit.*).

Il résulte de l'étude faite ci-dessus que l'invariant modulaire de E est entier en 5 si et seulement si 5 ne divise pas $a + b$.

2.2.3. Étude de la réduction de E en 2 si d est impair. — On est amené à distinguer deux cas suivant la parité de a.

2.2.3.1. Supposons a pair.— On a alors :

$$v_2(c_4) \geq 5, \quad v_2(c_6) = 5, \quad v_2(\Delta) = 4.$$

En fait, on a plus précisément $(v_2(a), v_2(c_4)) \in \{(1, \geq 6), (\geq 2, 5)\}$. En effet,

$$\begin{aligned} \frac{c_4}{2^4} \equiv 2 + 3ab^3 &\equiv 2 + 3ab \pmod 4 \\ &\equiv \begin{cases} 0 \pmod 4 & \text{si} \quad v_2(a) = 1 \\ 2 \pmod 4 & \text{si} \quad v_2(a) \geq 2. \end{cases} \end{aligned} \tag{3}$$

Il convient donc de séparer les cas $v_2(a) = 1$ et $v_2(a) \geq 2$.

1. On suppose $v_2(a) = 1$. On est dans le cas 3 ou 5 de Tate (*cf.* tableau IV, p.129 de [**Pap93**]). D'après la proposition 1, p.124 de *loc. cit.* appliquée avec $r = t = 1$, on est dans un cas ≥ 4 si et seulement si

   $$5\left(\frac{a^5 + b^5}{a + b}\right) - 5(a^2 + b^2) \equiv 0 \pmod 4,$$

   ce qui équivaut à

   $$a^4 - a^3b + a^2b^2 - ab^3 + b^4 - (a^2 + b^2) \equiv 0 \pmod 4.$$

   Or on a $a^4 - a^3b + a^2b^2 - ab^3 + b^4 - (a^2 + b^2) \equiv -ab \pmod 4$ et comme $v_2(a) = 1$, l'entier ab n'est pas multiple de 4. On est donc dans le cas 3 de Tate et l'on a $v_2(N_E) = 4$.
2. On suppose $v_2(a) \geq 2$. On a alors :

   $$v_2(c_4) = 5, \quad v_2(c_6) = 5, \quad v_2(\Delta) = 4.$$

   On est donc dans le cas 3 ou 4 de Tate. On déduit alors de la congruence $a^4 - a^3b + a^2b^2 - ab^3 + b^4 - (a^2 + b^2) \equiv -ab \pmod 4$, que l'on est dans le cas 4 de Tate et l'on a $v_2(N_E) = 3$.

2.2.3.2. Supposons a impair.— Dans ce cas, d'après la remarque 4, b est impair et c est pair. On a ainsi $\frac{a^5+b^5}{a+b} \equiv 1 \pmod 2$, $a^2+b^2 \equiv 2 \pmod 4$ et l'égalité $v_2(a^5+b^5) = v_2(a+b)$. Compte-tenu de l'égalité (1), il en résulte que l'on a

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, \geq 32).$$

Vérifions que l'équation (2) n'est pas minimale en 2. On étudie pour cela la congruence de $\frac{c_6}{2^6}$ modulo 4 (*cf.* [**Kra89**, p.77]). On constate que l'on a

$$\frac{c_6}{2^5} \equiv 4ab + 2 \pmod 8,$$

autrement dit,

$$\frac{c_6}{2^6} \equiv 2ab + 1 \pmod 4.$$

Puisque ab est impair, on a $ab \equiv \pm 1 \pmod 4$, et l'on obtient la congruence $\frac{c_6}{2^6} \equiv -1 \pmod 4$. Notre assertion résulte alors du corollaire du th. 2 de *loc. cit.*. On en déduit que E a réduction multiplicative en 2 et l'on a donc $v_2(N_E) = 1$.

2.2.4. Étude de la réduction de E en 2 si d est pair. — Dans ce cas, a et b sont impairs et comme au § précédent, on a $v_2(c_4) = 4$, $v_2(c_6) = 6$. D'après l'égalité $v_2(\Delta) = 4(1 + v_2(d) + pv_2(c))$, on obtient ainsi

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (4, 6, \geq 8).$$

Plus précisément, on a

$$\begin{cases} v_2(\Delta) = 8 & \text{si} \quad v_2(d) = 1 \text{ et si } c \text{ est impair,} \\ v_2(\Delta) = 12 & \text{si} \quad v_2(d) = 2 \text{ et si } c \text{ est impair,} \\ v_2(\Delta) > 12 & \text{si} \quad v_2(d) = 3 \text{ ou } 4, \text{ ou bien si } c \text{ est pair.} \end{cases}$$

On distingue donc les cas où $v_2(\Delta) = 8$ et $v_2(\Delta) \geq 12$.

2.2.4.1. Supposons $v_2(\Delta) \geq 12$.— On a comme ci-dessus les congruences

$$\frac{c_6}{2^6} \equiv 2ab + 1 \equiv -1 \pmod 4.$$

Par suite, l'équation (2) n'est pas minimale en 2. Si l'on a $v_2(d) = 2$ et si c est impair, la courbe E a donc bonne réduction en 2, *i.e.* on a $v_2(N_E) = 0$. Par ailleurs, si $v_2(d) = 3$ ou 4, ou bien si c est pair, E a donc réduction multiplicative en 2 et l'on a $v_2(N_E) = 1$.

2.2.4.2. Supposons $v_2(\Delta) = 8$.— On a

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (4, 6, 8)$$

et l'on est dans le cas 6, 7 ou 8 de Tate. D'après la prop. 3 p.124 de **[Pap93]**, on est amené à déterminer si la congruence

$$-5^2\left(\frac{a^5+b^5}{a+b}\right)^2 + 2.3.5.r^2\left(\frac{a^5+b^5}{a+b}\right) - 2^2.5.r^3(a^2+b^2) + 3r^4 \equiv 0 \pmod{32}$$

a ou non une solution $r \in \mathbf{Z}$. On vérifie que $r = 1$ convient. D'après la prop. 3 de *loc. cit.*, il existe $t \in \mathbf{Z}$ tel que

$$5\left(\frac{a^5+b^5}{a+b}\right) - 5(a^2+b^2) + 1 \equiv t^2 \pmod{8}.$$

et l'on vérifie que $t = 2$ convient. Posons

$$u = 5\left(\frac{a^5+b^5}{a+b}\right) - 5(a^2+b^2) - 3.$$

Vérifions que l'on a $v_2(u) = 3$. Les entiers a^2 et b^2 sont congrus à 1 ou 9 modulo 16, de sorte que l'on a $a^2 \equiv b^2 \pmod{16}$ ou $b^2 \equiv 9a^2 \pmod{16}$. Par ailleurs, on a $v_2(d) = 1$ et c est impair. D'après l'égalité (1), on a donc la congruence $a \equiv b \pmod 4$, autrement dit, on a $ab \equiv 1, 5 \pmod 8$.

1. Supposons $a^2 \equiv b^2 \pmod{16}$. Dans ce cas, on vérifie que l'on a

   $$u \equiv 2 + 6ab \pmod{16}.$$

   D'après l'hypothèse faite, on a $ab \equiv 1 \pmod 8$, ce qui entraîne notre assertion.
2. Supposons $b^2 \equiv 9a^2 \pmod{16}$. On obtient alors

   $$u \equiv 2(1 - ab) \pmod{16}.$$

   Par ailleurs, on a dans ce cas $ab \equiv 5 \pmod 8$, d'où le résultat.

Il en résulte que l'on est dans le cas 6 de Tate, puis que $v_2(N_E) = 4$.

Cela termine la démonstration des propositions 1 et 2.

3. La représentation $\rho_p^{a,b}$

Soient p un nombre premier et (a, b, c) un élément de $S_p(d)$. Notons $\overline{\mathbf{Q}}$ la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$ et $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ le groupe de Galois absolu de $\mathbf{Q}$. Soit $E[p]$ le sous-groupe de $E(\overline{\mathbf{Q}})$ constitué des points de p-division de la courbe elliptique $E = E(a, b)$. C'est un $\mathbf{F}_p$-espace vectoriel de dimension 2

sur lequel le groupe $G_{\mathbf{Q}}$ opère continûment. Par le choix d'une base de $E[p]$ sur $\mathbf{F}_p$, on en déduit un homomorphisme de groupes

$$\rho_p^{a,b} : G_{\mathbf{Q}} \longrightarrow \mathbf{GL}_2(\mathbf{F}_p).$$

À une telle représentation J.-P. Serre associe un *poids* k qui est un entier ≥ 2 et un *conducteur* $N(\rho_p^{a,b})$ qui est un entier ≥ 1, premier à p, qui divise le conducteur N_E de E (*cf.* [**Ser87**, §1]). Dans les paragraphes suivants, on démontre que $\rho_p^{a,b}$ est irréductible et on détermine les entiers k et $N(\rho_p^{a,b})$.

3.1. Irréductibilité de $\rho_p^{a,b}$. —

Proposition 3.1. — *La représentation $\rho_p^{a,b}$ est irréductible.*

Démonstration. La courbe elliptique E possède un point d'ordre 2 rationnel sur $\mathbf{Q}$. Par suite, si $\rho_p^{a,b}$ était réductible, le groupe $E(\overline{\mathbf{Q}})$ posséderait un sous-groupe d'ordre $2p$ stable par $G_{\mathbf{Q}}$, de sorte que la courbe modulaire $Y_0(2p)$ aurait un point rationnel sur $\mathbf{Q}$. Or si $p \geq 11$, B. Mazur et M. A. Kenku ont démontré que l'ensemble $Y_0(2p)(\mathbf{Q})$ est vide (*cf.* [**Ken82**], notamment le th.1 p.199), d'où le résultat dans ce cas. Supposons maintenant $p = 7$ et $\rho_7^{a,b}$ réductible. La courbe elliptique E correspond alors à un point rationnel sur $\mathbf{Q}$ de la courbe modulaire $Y_0(14)$. Or celle-ci a deux points rationnels sur $\mathbf{Q}$ qui correspondent à deux classes de $\overline{\mathbf{Q}}$-isomorphisme de courbes elliptiques d'invariants $j = -15^3$ ou 255^3 (*cf.* [**Cre**] et [**Lig75**]) : ce sont en effet les invariants modulaires des courbes notées 49A1 et 49A2 dans les tables de [**Cre**] et elles possèdent un sous-groupe d'ordre 14 stable par $G_{\mathbf{Q}}$. On a donc $j = c_4^3/\Delta$, ce qui entraîne l'existence de $t \in \mathbf{Q}$ tel que l'on ait (en posant $t = a/b$)

$$2^8 \frac{(2t^4 + 3t^3 + 7t^2 + 3t + 2)^3}{(t+1)^2(t^5+1)^2} = -15^3 \quad \text{ou} \quad 255^3.$$

On vérifie que cela conduit à une contradiction, d'où la proposition.

3.2. Calcul de k. —

On va démontrer le résultat suivant :

Proposition 3.2. — *On a $k = 2$ si p ne divise pas d et $k = p + 1$ sinon.*

Démonstration. Supposons que p ne divise pas d. Si p ne divise pas c, alors E a bonne réduction en p et l'on a $k = 2$ d'après la prop. 5 p.191 de [**Ser87**]. Si p divise c, puisque l'on a $p \geq 7$, la courbe E a réduction multiplicative en p (*cf.* §2.2.1). Posons

$$\Phi(a,b) \quad = \quad a^4 - a^3b + a^2b^2 - ab^3 + b^4.$$

On a les égalités

$$\Delta = 2^4.5^3(a+b)^4\Phi(a,b)^2 \quad \text{et} \quad (a+b)\Phi(a,b) = dc^p. \tag{4}$$

Les entiers $a+b$ et $\Phi(a,b)$ étant premiers entre eux en dehors de 5, il en résulte que p divise $v_p(\Delta)$, ce qui entraîne de nouveau $k = 2$ (*cf. loc. cit.*).

Supposons que p divise d. La courbe E a alors réduction de type multiplicatif en p (*cf.* §2.2.1) et l'on déduit des égalités (4) que p ne divise pas $v_p(\Delta)$. Cela conduit à $k = p+1$, d'où le résultat.

3.3. Calcul de $N(\rho_p^{a,b})$. — Posons

$$r' = \prod_{\ell \mid d, \ell \neq 2,5,p} \ell,$$

où ℓ parcourt les diviseurs premiers de d distincts de $2, 5$ et p. Le conducteur cherché est donné dans les deux énoncés suivants :

Proposition 3.3. — *Supposons d* impair. *Alors :*

1. $N(\rho_p^{a,b}) = 2^4.5^2.r'$, *si* $v_2(a) = 1$;
2. $N(\rho_p^{a,b}) = 2^3.5^2.r'$, *si* $v_2(a) \geq 2$;
3. $N(\rho_p^{a,b}) = 2.5^2.r'$, *si a est impair.*

Proposition 3.4. — *Supposons d* pair. *Alors :*

1. *si c est* pair, *on a* $N(\rho_p^{a,b}) = 2.5^2.r'$;
2. *si c est* impair, *alors :*
   (a) *si* $v_2(d) = 2$, *on a* $N(\rho_p^{a,b}) = 5^2.r'$;
   (b) *si* $v_2(d) = 3$ *ou* 4, *on a* $N(\rho_p^{a,b}) = 2.5^2.r'$;
   (c) *si* $v_2(d) = 1$, *on a* $N(\rho_p^{a,b}) = 2^4.5^2.r'$.

Démonstration. Puisque $N(\rho_p^{a,b})$ divise N_E, pour tout nombre premier ℓ qui ne divise pas $10r$, on a $v_\ell\big(N(\rho_p^{a,b})\big) = 0$.

Considérons un diviseur premier ℓ de N_E distinct de $2, 5$ et p. Vérifions que l'on a $v_\ell\big(N(\rho_p^{a,b})\big) = 1$ si ℓ divise d et $v_\ell\big(N(\rho_p^{a,b})\big) = 0$ sinon. D'après les propositions 1 et 2, la courbe E a réduction multiplicative en ℓ. Démontrons alors que l'on a l'équivalence :

$$p \text{ divise } v_\ell(\Delta) \iff \ell \text{ ne divise pas } d, \tag{5}$$

ce qui prouvera notre assertion (*cf.* [**Kra97**, p.28]). L'égalité

$$\Delta = 2^4.5^3.(a+b)^2.d^2.c^{2p},$$

entraîne la congruence $v_\ell(\Delta) \equiv 2v_\ell(a+b) + 2v_\ell(d) \pmod{p}$.

Supposons que ℓ divise $a+b$. Dans ce cas, on a $v_\ell\big(\Phi(a,b)\big) = 0$. D'après l'égalité $(a+b)\Phi(a,b) = dc^p$, on a donc $v_\ell(a+b) \equiv v_\ell(d) \pmod p$. On en déduit que $v_\ell(\Delta) \equiv 4v_\ell(d) \pmod p$. Puisque l'on a $0 \leq v_\ell(d) \leq 4$, on obtient l'équivalence (5) dans ce cas. Si ℓ ne divise pas $a+b$, on a $v_\ell(\Delta) \equiv 2v_\ell(d) \pmod p$ d'où encore l'équivalence annoncée.

La courbe E ayant réduction de type additif en 5, on a $v_5\big(N(\rho_p^{a,b})\big) = 2$ (*loc. cit.*).

Il reste à déterminer l'exposant de 2 dans $N(\rho_p^{a,b})$. Dans le cas où E a réduction de type additif en 2, *i.e.* si $v_2(N_E) \geq 2$, on a $v_2(N_E) = v_2\big(N(\rho_p^{a,b})\big)$ (*loc. cit.*). Notons $\Delta(E)$ le discriminant minimal de E. Il s'agit alors de démontrer le résultat suivant :

Lemme 3.5. — *Supposons que E ait réduction de type multiplicatif en 2. Alors, p ne divise pas $v_2\big(\Delta(E)\big)$.*

Démonstration. On est dans l'un des cas suivants :

1. les entiers d et a sont impairs (et c est pair) ;
2. les entiers d et c sont pairs ;
3. l'entier d est pair, c est impair et l'on a $v_2(d) = 3$ ou 4.

Supposons que l'on soit dans le premier cas. On déduit de l'étude faite à l'alinéa 2.2.3.2 page 10 que l'on a

$$\Delta(E) = \frac{\Delta}{2^{12}}.$$

Puisque ab est impair, on a $v_2(a+b) = v_2(a^5+b^5)$. On en déduit que

$$v_2\big(\Delta(E)\big) \quad = \quad 4 + 4v_2(a^5+b^5) - 12,$$

autrement dit,

$$v_2\big(\Delta(E)\big) \quad = \quad -8 + 4pv_2(c) \equiv -8 \pmod p.$$

Dans les deux cas suivants, l'étude faite dans l'alinéa 2.2.4.1 page 10 entraîne que l'on a de nouveau $\Delta(E) = \frac{\Delta}{2^{12}}$, de sorte que

$$v_2\big(\Delta(E)\big) = -8 + 4\big(v_2(d) + pv_2(c)\big) \equiv -8 + 4v_2(d) \pmod p.$$

D'où le lemme.

Compte-tenu du fait que $N(\rho_p^{a,b})$ est premier à p, cela termine la démonstration des propositions 3.3 et 3.4.

4. La méthode modulaire

On considère dans ce chapitre une courbe elliptique $A/\mathbf{Q}$ définie sur $\mathbf{Q}$, de conducteur N_A.

4.1. Courbes elliptiques et formes modulaires. — Pour tout nombre premier ℓ, on définit un entier $a_\ell(A)$ par :

$$\begin{cases} a_\ell(A) = -1 \text{ si } A \text{ a réduction de type multiplicatif déployée en } \ell \\ a_\ell(A) = +1 \text{ si } A \text{ a réduction de type multiplicatif non déployée en } \ell \\ a_\ell(A) = 0 \text{ si } A \text{ a réduction de type additif en } \ell \\ a_\ell(A) = \ell + 1 - |\widetilde{A}(\mathbf{F}_\ell)| \text{ si } A \text{ a bonne réduction en } \ell, \end{cases}$$

où $|\widetilde{A}(\mathbf{F}_\ell)|$ est le nombre de points sur $\mathbf{F}_\ell$ de la courbe elliptique $\widetilde{A}/\mathbf{F}_\ell$ déduite de A par réduction modulo ℓ.

Par ailleurs, la fonction définie par $s \mapsto L(A,s) = \sum_{n\geq 1} a_n(A) n^{-s}$ désigne la fonction L de Hasse-Weil de A.

Définition 4.1. — On dit que la courbe elliptique $A/\mathbf{Q}$ est *modulaire* si la fonction définie sur le demi-plan de Poincaré $\mathbf{H}$ par :

$$\tau \mapsto \sum_{n\geq 1} a_n(A) q^n, \quad \text{avec } q = e^{2i\pi\tau},$$

est une forme modulaire parabolique de poids 2 pour le sous-groupe de congruences $\Gamma_0(N_A)$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z})$ avec $c \equiv 0 \pmod{N_A}$.

Il a été démontré que toute courbe elliptique sur $\mathbf{Q}$ est *modulaire* : c'est l'ancienne conjecture de Taniyama-Weil, devenue un théorème dû à Wiles, ainsi que Taylor, Conrad, Diamond et Breuil (*cf.* **[Wil95]** pour le cas semi-stable et **[BCDT01]** pour le cas général).

Considérons alors un nombre $p \geq 5$ et $\rho_p^A : G_\mathbf{Q} \longrightarrow \mathbf{GL}_2(\mathbf{F}_p)$ la représentation donnant l'action de $G_\mathbf{Q}$ sur le groupe $A[p]$ des points de p-torsion de A, moyennant le choix d'une base de $A[p]$. Supposons que ρ_p^A soit irréductible de poids 2 et de conducteur $N(\rho_p^A)$. D'après les travaux de Ribet (*cf.* **[Rib90]**), il existe une *newform* de poids 2 et de niveau $N(\rho_p^A)$ (au sens de **[AL70]**)

$$f = q + \sum_{n\geq 2} a_n(f) q^n,$$

et une place $\mathfrak{P}$ de $\overline{\mathbf{Q}}$ de caractéristique résiduelle p telles que, pour tout nombre premier ℓ, on ait :

$$(6)\quad \begin{cases} a_\ell(f) \equiv a_\ell(A) \pmod{\mathfrak{P}} & \text{si } \ell \text{ ne divise pas } pN_A \\ a_\ell(f) \equiv \pm(\ell+1) \pmod{\mathfrak{P}} & \text{si } \ell \text{ divise } N_A \text{ et } \ell \text{ ne divise pas } pN(\rho_p). \end{cases}$$

Par ailleurs, dans le cas où les coefficients $a_n(f)$ sont dans $\mathbf{Z}$, la newform f correspond à une courbe elliptique $F/\mathbf{Q}$ de conducteur $N(\rho_p^A)$ et l'on a pour tout $n \geq 1$:

$$(7)\qquad a_n(f) \;=\; a_n(F).$$

La courbe elliptique $F/\mathbf{Q}$ est unique à isogénie près. Les représentations ρ_p^F et ρ_p^A sont alors isomorphes et l'on a en particulier :

$$a_\ell(A) \;\equiv\; a_\ell(F) \pmod{p},$$

pour tout nombre premier ℓ ne divisant pas N_A.

La méthode modulaire consiste à appliquer ces résultats en prenant pour A la courbe elliptique $E(a,b)$ associée à un élément (a,b,c) de $S_p(d)$ et à contredire l'existence de f.

4.2. La variante modulaire symplectique. — Supposons que l'on soit dans le cas où les coefficients $a_n(f)$ sont dans $\mathbf{Z}$, les congruences (7) étant réalisées. La méthode symplectique repose sur le lemme 4.2 suivant ([**HK02**, p.180]) : notons $\Delta(A)$ (resp. $\Delta(F)$) le discriminant minimal de A (resp. de F).

Lemme 4.2. — *Soient ℓ_1 et ℓ_2 deux nombres premiers distincts, autres que p. Supposons que A et F aient réduction de type multiplicatif en ℓ_i et que p ne divise pas $v_{\ell_i}\big(\Delta(A)\big)$, auquel cas p ne divise pas non plus $v_{\ell_i}\big(\Delta(F)\big)$ ($i = 1, 2$). Alors, les classes modulo p de $v_{\ell_1}\big(\Delta(A)\big)v_{\ell_2}\big(\Delta(A)\big)$ et $v_{\ell_1}\big(\Delta(F)\big)v_{\ell_2}\big(\Delta(F)\big)$ diffèrent multiplicativement par un carré de $\mathbf{F}_p$.*

Ce résultat a été obtenu en comparant symplectiquement les modules galoisiens $A[p]$ et $F[p]$, *i.e.* en examinant s'ils sont ou non isomorphes de façon compatible aux accouplements de Weil (*cf. loc. cit.*). En prenant pour A la courbe elliptique $E(a,b)$ comme ci-dessus, ce résultat permet parfois de contredire l'existence d'une telle courbe elliptique F. Lorsque la méthode aboutit on obtient une densité > 0 de nombres premiers p pour lesquelles, d étant fixé, l'ensemble $S_p(d)$ est vide.

5. Conséquences sur l'équation $x^5 + y^5 = dz^p$

Considérons pour toute la suite de ce chapitre, un entier d de la forme

$$d = 2^\alpha.3^\beta.5^\gamma, \quad \text{où } \alpha, \beta, \gamma = 0, \ldots, 4,$$

un nombre premier $p \geq 7$ et un élément (a, b, c) de $S_p(d)$. Sous les hypothèses faites dans les théorèmes 1.1, 1.2 et 1.3, on démontre que l'existence de (a, b, c) conduit à une contradiction. On commence par le lemme préliminaire suivant :

Lemme 5.1. — *Soit ℓ un nombre premier non congru à 1 modulo 5 et divisant $a^5 + b^5$. Alors, ℓ divise $a + b$.*

Démonstration. Supposons que ℓ ne divise pas $a + b$. Puisque ℓ divise $a^5 + b^5$, ℓ ne divise pas ab. Soit b' l'inverse de $-b$ modulo ℓ. On a $a^5 \equiv (-b)^5 \pmod{\ell}$, d'où $(ab')^5 \equiv 1 \pmod{\ell}$. Par suite, l'ordre de ab' dans le groupe multiplicatif $\mathbf{F}_\ell^*$ est 1 ou 5. Or la congruence $ab' \equiv 1 \pmod{\ell}$ conduit à $a + b \equiv 0 \pmod{\ell}$ donc à une contradiction. On en déduit donc que l'ordre de ab' dans $\mathbf{F}_\ell^*$ est 5. D'où $\ell \equiv 1 \pmod{5}$ et le lemme par contraposition.

Rappelons que pour tout entier $n \geq 1$, le $\mathbf{C}$-espace vectoriel $S_2^+(n)$ formé des newforms de poids 2 et de niveau n est de dimension finie $g^+(n)$ sur $\mathbf{C}$. On utilisera dans la suite le calcul de $g^+(n)$, que l'on peut par exemple trouver dans [**HK02**]. Il y a exactement $g^+(n)$ newforms qui sont normalisées (*i.e.* celles dont le q-développement est de la forme $q + a_2q^2 + \cdots$) et elles constituent une base de $S_2^+(n)$.

5.1. Démonstration du th.1.1. — On suppose ici que l'on a $d = 1$ (*i.e.* $\alpha = \beta = \gamma = 0$) et que c est pair. L'entier a est impair. D'après l'étude faite dans le paragraphe 3, la représentation $\rho_p^{a,b}$ est irréductible de poids 2 et de conducteur 50. Il existe donc une newform normalisée $f \in S_2^+(50)$ telle que, en prenant pour A la courbe elliptique $E = E(a, b)$, les congruences (6) soient réalisées. On a $g^+(50) = 2$, de sorte qu'il y a exactement deux telles newforms. Elles correspondent aux courbes elliptiques sur $\mathbf{Q}$ de conducteur 50 :

$$y^2 + xy + y = x^3 - x - 2,$$

$$y^2 + xy + y = x^3 + x^2 - 3x + 1,$$

notées respectivement 50A1 et 50B1 dans les tables [**Cre**]. On va alors contredire les congruences (6) avec le nombre premier $\ell = 3$. On remarque pour cela que l'on a

$$\begin{cases} a_3(\text{A1}) = +1, \\ a_3(\text{B1}) = -1, \end{cases}$$

et $a_3(f) = a_3(\text{A1})$ ou $a_3(\text{B1})$, d'après l'égalité (7).

Par ailleurs, la courbe elliptique E a réduction semi-stable en 3 (prop. 2.1). Supposons que E ait réduction multiplicative en 3. Puisque 3 divise N_E, mais pas $50p = pN(\rho_p^{a,b})$, on déduit des congruences (6) que l'on a

$$\pm 1 \quad \equiv \quad \pm 4 \pmod{p},$$

ce qui conduit à une contradiction car $p \geq 7$. La courbe E a donc bonne réduction en 3 et l'application de réduction induit un morphisme de groupes injectif (*cf.* **[Sil86**, p.176]) :

$$E(\mathbf{Q})[2] \hookrightarrow \widetilde{E}(\mathbf{F}_3).$$

Puisque E a point d'ordre 2 rationnel sur $\mathbf{Q}$, on en déduit que $|\widetilde{E}(\mathbf{F}_3)|$ est pair. D'après les congruences (6), on a donc

$$\pm 1 \quad \equiv \quad 4 - |\widetilde{E}(\mathbf{F}_3)| \pmod{p},$$

ce qui conduit de nouveau à une contradiction. Cela termine la démonstration du théorème 1.1.

5.2. Démonstration du th.1.2. — On distingue deux cas suivant la valeur de $v_2(d)$.

5.2.1. Supposons $v_2(d) = 2$. — D'après la prop.3.4, on a :

$$N(\rho_p^{a,b}) \quad = \quad \begin{cases} 50 & \text{si } c \text{ est pair} \\ 25 & \text{si } c \text{ est impair .} \end{cases}$$

Or $g^+(25) = 0$, donc l'entier c est pair. La réprésentation $\rho_p^{a,b}$ « provient » donc d'une newform normalisée de $S_2^+(50)$. Or on vient de voir que cela est impossible (*cf.* §5.1). On obtient ainsi une contradiction, d'où le résultat.

5.2.2. Supposons $v_2(d) = 3$ *ou* 4. — Dans ce cas, on a $N(\rho_p^{a,b}) = 50$, ce qui entraîne, comme ci-dessus, le résultat. (*cf.* §5.1).

5.3. Démonstration du th.1.3. — On suppose ici que d s'écrit

$$d = 2^\alpha.3^\beta.5^\gamma, \quad \text{avec } \alpha = 3 \text{ ou } 4 \text{ et } 1 \leq \beta \leq 4,\ 0 \leq \gamma \leq 4.$$

On a alors :

$$N(\rho_p^{a,b}) \quad = \quad 150.$$

On a $g^+(150) = 3$ et une base de $S_2^+(150)$ correspond aux trois classes d'isogénie de courbes elliptiques sur $\mathbf{Q}$ de conducteur 150. Ainsi $\rho_p^{a,b}$ est isomorphe à la représentation de $G_{\mathbf{Q}}$ dans les points de p-torsion de l'une des courbes notées

150A1, 150B1 et 150C1 dans les tables de [**Cre**]. Par ailleurs, E a réduction multiplicative en 2 et 3 (*cf.* le §3.3). Soit $\Delta(E)$ le discriminant minimal de E. D'après le lemme 3.5 et sa démonstration, on a donc :

$$\begin{aligned} v_2\big(\Delta(E)\big) &\equiv -8 + 4v_2(d) \pmod{p} \\ &\equiv -8 + 4\alpha \pmod{p} \\ &\equiv \begin{cases} 4 \pmod{p} & \text{si } \alpha = 3 \\ 8 \pmod{p} & \text{si } \alpha = 4. \end{cases} \end{aligned}$$

D'après le lemme 5.1, 3 divise $a + b$, donc 3 ne divise pas $(a^5 + b^5)/(a + b)$, d'où $v_3(a + b) = v_3(a^5 + b^5)$ qui est congru à $v_3(d)$, modulo p. On a ainsi

$$v_3\big(\Delta(E)\big) \equiv 4\beta \pmod{p}.$$

Les entiers $v_2\big(\Delta(E)\big)$ et $v_3\big(\Delta(E)\big)$ ne sont donc pas divisibles par p. On distingue alors deux cas suivant la valeur de l'entier α.

On rappelle que l'invariant modulaire de E est entier en 5 si et seulement si 5 ne divise pas $a + b$ (*cf.* alinéa 2.2.2.2 page 8).

5.3.1. Supposons $\alpha = 3$. — On est amené à distinguer deux cas selon que 5 divise on non $a + b$.

5.3.1.1. Supposons que 5 *divise* $a+b$. — Démontrons que l'on a les assertions suivantes :

$$\begin{cases} 3 \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 1 \text{ ou } 4 \\ 6 \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 2 \\ 1 \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 3. \end{cases}$$

D'après l'hypothèse faite, E a potentiellement réduction multiplicative en 5, autrement dit, E a réduction additive en 5 et son invariant modulaire n'est pas entier en 5. Soit $\mathbf{Q}(E[p])$ le corps laissé fixe par le noyau de $\rho_p^{a,b}$. On a $p \neq 5$, par suite l'indice de ramification en 5 de $\mathbf{Q}(E[p])/\mathbf{Q}$ est 2 ou $2p$, d'après [**CK02**, p.7]. Par ailleurs, les courbes notées 150A1 et 150B1 dans [**Cre**] ont réduction additive en 5 et leurs invariants modulaires sont entiers en 5. Les valuations de leurs discriminants minimaux en 5 sont respectivement 3 et 9. Leur défaut de semi-stabilité en 5 (qui est mesuré par l'ordre d'un certain groupe fini Φ_5) est donc d'ordre 4 ([**?**, p.312]). L'indice de ramification en 5 des extensions de $\mathbf{Q}$ engendrées par leurs points de p-torsion vaut donc 4 (*loc. cit.*). Puisque l'on a $p \neq 2$, cela entraîne que $\rho_p^{a,b}$ est isomorphe à ρ_p^F, où F est la courbe elliptique notée 150C1 dans [**Cre**]. On applique alors le résultat du lemme 4.2 avec les

courbes E et F, et les nombres premiers $\ell_1 = 2$, $\ell_2 = 3$. Il vient :

$$3 \pmod p \equiv \beta \pmod p \pmod{(\mathbf{F}_p^*)^2},$$

d'où les assertions ci-dessus.

5.3.1.2. Supposons que 5 *ne divise pas* $a + b$. — Dans ce cas, vérifions que l'on a :

$$\text{(8)} \qquad \begin{cases} 2 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 1 \text{ ou } 4 \\ 1 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 2 \\ 6 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 3. \end{cases}$$

L'invariant modulaire de E est entier en 5. Puisque l'on a $v_5\big(\Delta(E)\big) = 3$, l'indice de ramification en 5 de l'extension $\mathbf{Q}(E[p])/\mathbf{Q}$ est 4. Or la courbe elliptique notée 150C1 a un invariant modulaire non entier en 5. Comme ci-dessus, on en déduit que $\rho_p^{a,b}$ est isomorphe à ρ_p^F, où F est l'une des courbes elliptiques notées 150A1 et 150B1 dans [**Cre**]. D'après le lemme 4.2, on obtient :

$$2 \pmod p \equiv \beta \pmod p \pmod{(\mathbf{F}_p^*)^2},$$

d'où les conditions (8).

5.3.1.3. Démonstration du th. 1.3 si $\alpha = 3$. — Supposons $\gamma \geq 1$. Dans ce cas, 5 divise $a + b$. Par hypothèse, on a $\beta \in \big\{1, 2, 4\big\}$. Par ailleurs, on a les équivalences :

$$3 \pmod p \notin (\mathbf{F}_p^*)^2 \iff p \equiv 5 \text{ ou } 7 \pmod{12},$$

et

$$\begin{aligned} 6 \pmod p \notin (\mathbf{F}_p^*)^2 &\iff \begin{cases} p \equiv 1 \text{ ou } 7 \pmod 8 \text{ et } p \equiv 5 \text{ ou } 7 \pmod{12} \\ \text{ou} \\ p \equiv 3 \text{ ou } 5 \pmod 8 \text{ et } p \equiv 1 \text{ ou } 11 \pmod{12}, \end{cases} \\ &\iff p \equiv 7, 11, 13 \text{ ou } 17 \pmod{24}, \end{aligned}$$

d'où le résultat dans ce cas.

Supposons $\gamma = 0$. On a alors $\beta = 1$ ou 4. De l'équivalence

$$2 \pmod p \notin (\mathbf{F}_p^*)^2 \iff 3 \text{ ou } 5 \pmod 8,$$

on déduit :

$$\begin{aligned} 3 \pmod p \notin (\mathbf{F}_p^*)^2 \text{ et } 2 \notin (\mathbf{F}_p^*)^2 &\iff p \equiv 5 \text{ ou } 7 \pmod{12} \\ &\quad \text{et } p \equiv 3 \text{ ou } 5 \pmod 8 \\ &\iff p \equiv 5 \text{ ou } 19 \pmod{24}. \end{aligned}$$

Compte-tenu des deux alinéas précédents, cela prouve le th. 1.3 si $\alpha = 3$.

5.3.2. Supposons $\alpha = 4$. — La démarche est identique à celle du § précédent : seules les congruences obtenues diffèrent. On explicitera donc les calculs sans répéter exhaustivement les raisonnements.

5.3.2.1. Supposons que 5 *divise* $a + b$. — La représentation $\rho_p^{a,b}$ est alors isomorphe à ρ_p^F, où F est la courbe elliptique notée 150C1 dans **[Cre]**. On déduit du lemme 4.2 les congruences :

$$3 \pmod p \equiv 2\beta \pmod p \pmod{(\mathbf{F}_p^*)^2}.$$

Autrement dit, on a :

$$\begin{cases} 6 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 1 \text{ ou } 4 \\ 3 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 2 \\ 2 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 3. \end{cases}$$

5.3.2.2. Supposons que 5 *ne divise pas* $a + b$. — On sait qu'alors $\rho_p^{a,b}$ est isomorphe à ρ_p^F, où F est l'une des courbes elliptiques notées 150A1 et 150B1 dans **[Cre]**. On obtient dans ce cas :

$$\beta \pmod p \in (\mathbf{F}_p^*)^2.$$

5.3.2.3. Démonstration du th. 1.3 si $\alpha = 4$. — En distinguant comme ci-dessus les cas où $\gamma = 0$ et $\gamma \geq 1$, on constate que les congruences explicitées dans le §5.3.1.3 entraînent directement le résultat. Ceci achève la démonstration du th.1.3.

Appendice A

Comment la courbe $E(a, b)$ a-t-elle été construite ?

Dans cet appendice, on décrit le procédé suivi par H. Darmon (*cf.* **[Kra99**, p. 329]) pour obtenir la courbe $E(a, b)$ associée à un élément $(a, b, c) \in S_p(d)$.

Soit $\sqrt{5}$ est une racine carrée de 5. On pose :

$$\omega = \frac{-1+\sqrt{5}}{2} \quad \text{et} \quad \overline{\omega} = \frac{-1-\sqrt{5}}{2},$$

de sorte que l'on a

$$a^5 + b^5 = (a+b)(a^2 + \omega ab + b^2)(a^2 + \overline{\omega} ab + b^2).$$

Il s'agit alors de construire, à partir de (a, b, c), une courbe de Frey, au sens par exemple de la définition donnée dans *loc. cit.* page 320. L'idée est de trouver deux entiers algébriques A et B dans $\mathbf{Q}\big(\sqrt{5}\big)$ tels que A, B et $A+B$ soient « essentiellement » des puissances p-ièmes. Tel est le cas avec :

$$A = \omega(a^2 + \overline{\omega} ab + b^2) \quad \text{et} \quad B = \overline{\omega}(a^2 + \omega ab + b^2),$$

pour lesquels on a $A + B = -(a+b)^2$.

On considère ensuite la courbe elliptique $\mathcal{F}$ définie sur $\mathbf{Q}\big(\sqrt{5}\big)$ par :

$$\mathcal{F} : Y^2 = X(X-A)(X+B).$$

Une équation de $\mathcal{F}$ est donc :

$$Y^2 = X^3 - \sqrt{5}(a^2+b^2)X^2 + \left(\frac{a^5+b^5}{a+b}\right)X. \tag{9}$$

La courbe $E(a,b)$ est alors la tordue quadratique de $\mathcal{F}$ sur $\mathbf{Q}\big(\sqrt{5}\big)$ par une racine carrée $\sqrt[4]{5}$ de $\sqrt{5}$. En effet, le changement de variables

$$X = \frac{x}{\sqrt{5}} \quad \text{et} \quad Y = \frac{y}{\big(\sqrt[4]{5}\big)^3}$$

transforme l'équation (9) en l'équation (2) de $E(a,b)$.

Références

[AL70] A. O. L. Atkin & J. Lehner – « Hecke Operators on $\Gamma_0(m)$ », *Math. Ann.* **185** (1970), p. 134–160.

[BCDT01] C. Breuil, B. Conrad, F. Diamond & R. Taylor – « On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercices », *J. Amer. Math. Soc.* **14** (2001), p. 843–939.

[CK02] É. Cali & A. Kraus – « Sur la p-différente du corps des points de ℓ-torsion des courbes elliptiques, $\ell \neq p$ », *Acta Arith.* **104** (2002), p. 1–21.

[Cre] J. E. Cremona – *Algorithms for modular elliptic curves*, disponible à l'adresse suivante :
http ://www.ma.utexas.edu/users/tornaria/cnt/.

[Fre86] G. Frey – « Links between stable elliptic curves and certain diophantine equations », *Ann. Univ. Sarav. Ser. Math.* **1** (1986), p. 1–40.

[HK02] E. Halberstadt & A. Kraus – « Courbes de Fermat : résultats et problèmes », *J. reine angew. Math.* **548** (2002), p. 167–234.

[Ken82] M. A. Kenku – « On the Number of **Q**-isomorphism Classes of Elliptic Curves in Each **Q**-Isogeny Class », *J. Number Theory* **15** (1982), no. 2, p. 199–202.

[Kra89] A. Kraus – « Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique », *Acta Arith.* **54** (1989), p. 75–80.

[Kra97] ———, « Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique », *Dissertationes Math.* **364** (1997).

[Kra98] ———, « Sur l'équation $a^3+b^3 = c^p$ », *Experiment. Math.* **7** (1998), no. 1, p. 1–13.

[Kra99] ———, « On the equation $x^p + y^q = z^r$: A Survey », *The Ramanujan Journal* **3** (1999), no. 3, p. 315–333.

[Kra02] ———, « Une question sur les équations $x^m - y^m = Rz^n$ », *Compositio Math.* **132** (2002), p. 1–26.

[Lig75] G. Ligozat – « Courbes modulaires de genre 1 », *Bull. Soc. Math. de France* **43** (1975).

[Pap93] I. Papadopoulos – « Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3 », *J. Number Theory* **44** (1993), no. 2, p. 119–152.

[Rib90] K. A. Ribet – « On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms », *Invent. Math.* **100** (1990), p. 431–476.

[Ser87] J.-P. Serre – « Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ », *Duke Math. J.* **54** (1987), p. 179–230.

[Sil86] J. H. Silverman – *The Arithmetic of Elliptic Curves*, GTM, vol. 106, Springer-Verlag, 1986.

[Tat75] J. Tate – « Algorithm for determining the type of a singular fiber in an elliptic pencil », in *Modular functions of one variable, Lect. Notes in Math.* **273** (1975), p. 33–52.

[Wil95] A. Wiles – « Modular elliptic curves and Fermat's Last Theorem », *Ann. of Math.* **141** (1995), no. 3, p. 443–551.

Nicolas Billerey • *E-mail :* billerey@math.jussieu.fr