Équations de Fermat de type $(5, 5, p)$

Nicolas Billerey,
Université Paris 6, Projet théorie des nombres, UMR 7586,
Case 247, 4, place Jussieu, Institut de Mathématiques,
75252 PARIS, FRANCE
billerey@math.jussieu.fr

Résumé

Soient p un nombre premier ≥ 7 et d un entier naturel sans puissances cinquièmes. Nous mettons en œuvre les différentes méthodes modulaires connues pour l'étude de l'équation diophantienne $x^5 + y^5 = dz^p$. Nous montrons en particulier qu'elle n'admet aucune solution propre et non triviale pour $p \geq 7$ ou pour une infinité de nombres premiers, dans certains cas où d est de la forme $2^\alpha \cdot 3^\beta \cdot 5^\gamma$. Pour $d = 3$, on énonce un critère permettant de vérifier, notamment, que tel est le cas lorsque p est $\leq 10^6$.

Let p be a prime number ≥ 7 and d be a positive integer fifth power free. We use the known modular methods for the study of the diophantine equation $x^5 + y^5 = dz^p$. We prove that this equation has no non trivial proper solution for $p \geq 7$ or for infinitely many prime numbers, in some cases where d is of the shape $2^\alpha \cdot 3^\beta \cdot 5^\gamma$. For $d = 3$, we give a criterion which allows us to verify that this holds if p is less than 10^6.

Introduction

Soient d un entier naturel sans puissances cinquièmes et p un nombre premier ≥ 7. On s'intéresse dans cet article à l'équation diophantienne suivante :

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

Suivant la terminologie de H. Darmon et A. Granville ([5]), on dira qu'un triplet d'entiers $(a, b, c) \in \mathbb{Z}^3$ est une solution de l'équation (1) si l'on a $a^5 + b^5 = dc^p$, qu'elle est propre si a, b et c sont premiers entre eux et qu'elle est non triviale si abc est non nul.

Notons $S_p(d)$ l'ensemble des solutions propres et non triviales de l'équation (1). On se propose dans cet article de démontrer quelques résultats concernant l'ensemble $S_p(d)$. Une conséquence de la conjecture abc est la suivante :

Conjecture 1 *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 l'on a $p > c(d)$, alors l'équation (1) n'admet aucune solution propre et non triviale.

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. [7], [17], [19] et [22]). 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 (1), on associe ici une courbe elliptique sur $\mathbb{Q}$, dont la construction est dûe à H. Darmon ([4]), dite *courbe de Frey* ou *courbe de Hellegouarch-Frey* et dont la représentation galoisienne dans ses points de p-torsion est liée à l'existence d'une forme modulaire de poids et de niveau précis, qui « essentiellement » ne dépendent pas de la solution considérée. On est alors confronté au problème de démontrer que l'existence d'une telle forme modulaire conduit à une contradiction. Une étude de la ramification du corps des points de p-torsion de la courbe de Frey permet parfois d'y parvenir.

Signalons qu'un résultat figurant dans [13] 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 cet article, nous mettons en œuvre la méthode modulaire et certaines de ses variantes pour l'étude de l'équation (1). Elle permet de montrer que $S_p(d)$ est vide pour $p \geq 7$, ou seulement pour une infinité de p, dans certains cas où d est de la forme $2^\alpha \cdot 3^\beta \cdot 5^\gamma$ avec $0 \leq \alpha, \beta, \gamma \leq 4$.

On énonce par ailleurs un critère, analogue à celui obtenu par A. Kraus concernant l'équation $x^3 + y^3 = z^p$ (cf. [12]), permettant souvent de montrer que $S_p(3)$ est vide pour un nombre premier p fixé. On démontre qu'il s'applique également aux petites valeurs de p (notamment $p = 7$). On le vérifie numériquement, à l'aide d'un programme PARI pour tous les nombres premiers p compris entre 7 et 10^6.

Remerciements. Je remercie A. Kraus, pour ses nombreux conseils et D. Bernardi pour son aide sur le logiciel de calculs PARI.

1 Énoncés des résultats

Soit p un nombre premier ≥ 7. Les résultats décrits ici concernent les entiers d de la forme

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

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 entier 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 1.1, on obtient une réponse complète quant à la description de $S_p(d)$:

Théorème 1.2 *Supposons que d soit de la forme*

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

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, décrite dans [8], on obtient à ce sujet l'énoncé suivant :

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

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

Énonçons maintenant les résultats obtenus concernant le cas où $d = 3$. Pour tout nombre premier $p \geq 7$, on démontre un critère qui permet souvent de prouver que $S_p(3)$ est vide. Considérons pour cela un nombre premier q congru à 1 modulo p. Posons $q = np + 1$. Le groupe $\mu_n(\mathbb{F}_q)$ des racines n-ièmes de l'unité de $\mathbb{F}_q$ est d'ordre n. On définit deux sous-ensembles $A(n,q)$ et $B(n,q)$ de $\mu_n(\mathbb{F}_q)$ de la façon suivante.

1. Soit $\widetilde{A}(n,q)$ le sous-ensemble de $\mu_n(\mathbb{F}_q)$ formé des éléments ζ pour lesquels :

   $$405 + 62500\zeta \text{ est un carré dans } \mathbb{F}_q.$$

   À un tel élément ζ, on associe le plus petit entier $\delta_{1,\zeta} \geq 0$ tel que

   $$\delta_{1,\zeta}^2 \pmod{q} = 405 + 62500\zeta.$$

   On définit $A(n,q)$ comme étant le sous-ensemble de $\widetilde{A}(n,q)$ constitué des éléments ζ pour lesquels l'un au moins des entiers

   $$-225 + 10\delta_{1,\zeta} \quad \text{et} \quad -225 - 10\delta_{1,\zeta}$$

   est un carré modulo q. À tout élément $\zeta \in A(n,q)$, on associe alors la cubique sur $\mathbb{F}_q$ suivante :

   $$F_{1,\zeta} : y^2 = x^3 + \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x. \tag{2}$$

Son discriminant vaut $6480\zeta^2 = 2^4 \cdot 3^4 \cdot 5\zeta^2$, qui est non nul car on a $q \geq 7$. Par suite, $F_{1,\zeta}$ est une courbe elliptique sur $\mathbb{F}_q$. On note $n_{1,q}(\zeta)$ le nombre de points rationnels sur $\mathbb{F}_q$ de $F_{1,\zeta}$ et l'on pose

$$a_q(\zeta) = q + 1 - n_{1,q}(\zeta). \tag{3}$$

2. Soit $\widetilde{B}(n,q)$ le sous-ensemble de $\mu_n(\mathbb{F}_q)$ formé des éléments ζ pour lesquels :

$$405 + 20\zeta \text{ est un carré dans } \mathbb{F}_q.$$

À un tel élément ζ, on associe le plus petit entier $\delta_{2,\zeta} \geq 0$ tel que

$$\delta_{2,\zeta}^2 \pmod q = 405 + 20\zeta.$$

On définit $B(n,q)$ comme étant le sous-ensemble de $\widetilde{B}(n,q)$ constitué des éléments ζ pour lesquels l'un au moins des entiers

$$-225 + 10\delta_{2,\zeta} \quad \text{et} \quad -225 - 10\delta_{2,\zeta}$$

est un carré modulo q. À tout élément $\zeta \in B(n,q)$, on associe alors la cubique sur $\mathbb{F}_q$ suivante :

$$F_{2,\zeta} : y^2 = x^3 + \delta_{2,\zeta} x^2 + 5\zeta x. \tag{4}$$

Son discriminant $2^4 \cdot 3^4 \cdot 5^3\zeta^2$ est non nul car on a $q \geq 7$. Par suite, $F_{2,\zeta}$ définit une courbe elliptique sur $\mathbb{F}_q$. On note $n_{2,q}(\zeta)$ le nombre de points rationnels sur $\mathbb{F}_q$ de $F_{2,\zeta}$ et l'on pose

$$b_q(\zeta) = q + 1 - n_{2,q}(\zeta). \tag{5}$$

Les notations étant celles utilisées dans les tables de [3] (à ceci près que les lettres minuscules ont été remplacées ici par des lettres majuscules), on considère les trois ensembles de courbes elliptiques suivants :

$$\begin{aligned} \mathcal{E}_1 &= \{150\text{C}1, 600\text{A}1, 600\text{F}1, 1200\text{J}1\}; \\ \mathcal{E}_2 &= \{150\text{A}1, 600\text{C}1, 1200\text{N}1\}. \end{aligned}$$

Si F est l'une des courbes des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$ et si ℓ est un nombre premier ≥ 7, alors F a bonne réduction en ℓ. On pose

$$a_\ell(F) = \ell + 1 - |\widetilde{F}(\mathbb{F}_\ell)|,$$

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

Le critère que l'on obtient est le suivant :

Théorème 1.4 *Soit p un nombre premier ≥ 7. Supposons que les deux conditions suivantes soient satisfaites :*

1. *pour toute courbe elliptique F appartenant à $\mathcal{E}_1$, il existe un entier $n \geq 2$ tel que :*
   (a) *l'entier $q = np + 1$ est premier.*
   (b) *On a $a_q(F)^2 \not\equiv 4 \pmod{p}$.*
   (c) *Pour tout ζ dans $A(n, q)$, on a*
   $$a_q(\zeta)^2 \equiv a_q(F)^2 \pmod{p}.$$
2. *Pour toute courbe elliptique F appartenant à $\mathcal{E}_2$, il existe un entier $n \geq 2$ tel que :*
   (a) *l'entier $q = np + 1$ est premier.*
   (b) *On a $a_q(F)^2 \not\equiv 4 \pmod{p}$.*
   (c) *Pour tout ζ dans $B(n, q)$, on a*
   $$b_q(\zeta)^2 \equiv a_q(F)^2 \pmod{p}.$$

Alors, $S_p(3)$ est vide.

En utilisant ce critère et un résultat de L. Dirichlet concernant le cas où $p = 5$ ([6]), on obtient l'énoncé suivant :

Proposition 1.5 *Si l'on a $5 \leq p \leq 10^6$, alors $S_p(3)$ est vide.*

Le critère du théorème 1.4 s'applique pour des valeurs de p considérablement plus grandes que 10^6. Ainsi $S_p(3)$ est vide lorsque $p = 15485863$ qui est le millionième nombre premier : on vérifie en effet que $n = 10$ satisfait aux conditions du théorème 1.4 (pour toute courbe F des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$). De même, $S_p(3)$ est vide pour $p = 1000000007$. Il suffit de prendre $n = 44$.

On donne en Appendice un tableau de valeurs d'entiers n satisfaisant aux conditions du théorème 1.4 pour les nombres premiers compris entre 11 et 150, ainsi que quelques explications heuristiques sur l'efficacité de ce critère pour les « grands » nombres premiers.

2 La courbe elliptique E

On considère un élément (a, b, c) de $S_p(d)$. À un tel triplet on associe l'équation de Weierstrass E définie sur $\mathbb{Q}$:

$$y^2 = x^3 - 5(a^2 + b^2)x^2 + 5\left(\frac{a^5 + b^5}{a + b}\right)x. \tag{6}$$

Ses invariants standard (c_4, c_6, Δ) sont les suivants (cf. [21]) :

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

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

Notations.

1. On pose
$$r = \prod_{\ell | cd, \ell \neq 2,5} \ell,$$
où ℓ parcourt l'ensemble des diviseurs premiers de cd autres que 2 et 5.
2. Si ℓ est un nombre premier, on note v_ℓ la valuation ℓ-adique de $\mathbb{Q}$.
3. On pose
$$\phi(a, b) = \frac{a^5 + b^5}{a + b} = a^4 - a^3 b + a^2 b^2 - ab^3 + b^4. \tag{7}$$
4. On note Δ_m le discriminant minimal de E.

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.

Proposition 2.1 *L'équation (6) est minimale en dehors de* 2. *Elle est minimale en* 2, *auquel cas on a* $\Delta_m = \Delta$, *sauf dans les trois 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* c *est impair et l'on a* $v_2(d) = 2$, 3 *ou* 4.

Dans chacun de ces trois cas, on a alors :

$$\Delta_m = \frac{\Delta}{2^{12}}.$$

Soit N_E le conducteur de E.

Proposition 2.2 *Supposons* d *impair. On a :*

1. $N_E = 2^4 \cdot 5^2 r$ *si* $v_2(a) = 1$;
2. $N_E = 2^3 \cdot 5^2 r$ *si* $v_2(a) \geq 2$;
3. $N_E = 2 \cdot 5^2 r$ *si* a *est impair.*

Proposition 2.3 *Supposons d pair.*

1. *Si c est* pair, *on a $N_E = 2 \cdot 5^2 r$.*
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 $N_E = 2 \cdot 5^2 r$;*
   (c) *si $v_2(d) = 1$, on a $N_E = 2^4 \cdot 5^2 r$.*

Les démonstrations de ces propositions font l'objet des paragraphes 2.1 à 2.5.

2.1 Lemmes préliminaires

Les trois lemmes suivants interviennent dans la suite à plusieurs reprises.

Lemme 2.4 *Soit ℓ un nombre premier divisant $a+b$. On a alors*

$$\phi(a,b) \equiv 5a^2b^2 \pmod{\ell^2}. \tag{8}$$

Démonstration : Si ℓ un nombre premier divisant $a+b$, on a

$$a^2 + b^2 \equiv -2ab \pmod{\ell^2}.$$

Or

$$\phi(a,b) = (a^2+b^2)^2 - ab(a^2+b^2+ab), \tag{9}$$

d'où

$$\phi(a,b) \equiv 5a^2b^2 \pmod{\ell^2}$$

et le lemme 2.4

Lemme 2.5 *Les entiers $a+b$ et $\phi(a,b)$ sont premiers entre eux en dehors de 5. De plus, si 5 divise $a+b$, alors $v_5(\phi(a,b)) = 1$ et $v_5(a+b) = v_5(d) + pv_5(c) - 1$.*

Démonstration : Soit ℓ un nombre premier divisant $a+b$ et $\phi(a,b)$. Si $\ell \neq 5$, on a $5a^2b^2 \not\equiv 0 \pmod{\ell}$ car ℓ ne divise pas ab. Donc ℓ ne divise pas $\phi(a,b)$ (lemme 2.4). Si $\ell = 5$, la congruence (8) ci-dessus implique $v_5(\phi(a,b)) = 1$. L'égalité $(a+b)\phi(a,b) = dc^p$ entraîne alors le lemme.

Lemme 2.6 *Soit ℓ un nombre premier non congru à 1 modulo 5 et divisant $a^5 + b^5$. Alors, ℓ divise $a+b$.*

Démonstration : 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 $\mathbb{F}_\ell^*$ est 1 ou 5. La congruence $ab' \equiv 1 \pmod{\ell}$ conduit à $a+b \equiv 0 \pmod{\ell}$. Si ℓ ne divise pas $a+b$, on en déduit donc que l'ordre de ab' dans $\mathbb{F}_\ell^*$ est 5 puis $\ell \equiv 1 \pmod{5}$. D'où le lemme.

2.2 Étude de la réduction de E en dehors de $\{2, 5\}$

On démontre le résultat suivant :

Lemme 2.7 *Soit ℓ un nombre premier distinct de 2 et 5. La courbe E est semi-stable en ℓ et l'on a*

$$v_\ell(N_E) = \begin{cases} 1 & \text{si } \ell \text{ divise } cd, \\ 0 & \text{sinon.} \end{cases}$$

L'équation (6) définit un modèle minimal en ℓ de E et $\Delta_m = \Delta$. On a de plus,

$$v_\ell(\Delta_m) \equiv \begin{cases} 4v_\ell(d) \pmod p & \text{si } \ell \text{ divise } a+b, \\ 2v_\ell(d) \pmod p & \text{si } \ell \text{ ne divise pas } a+b. \end{cases} \tag{10}$$

En particulier,

$$p \text{ divise } v_\ell(\Delta_m) \Longleftrightarrow \ell \text{ ne divise pas } d. \tag{11}$$

Démonstration : D'après l'égalité,

$$\Delta = 2^4.5^3(a+b)^2(a^5+b^5)^2,$$

on a $v_\ell(\Delta) = 2v_\ell(a+b) + 2v_\ell(a^5+b^5)$. Or

$$a^5 + b^5 = dc^p,$$

donc $v_\ell(a^5+b^5) = v_\ell(d) + pv_\ell(c)$. D'où

$$v_\ell(\Delta) \equiv 2v_\ell(a+b) + 2v_\ell(d) \pmod p. \tag{12}$$

Si ℓ ne divise pas cd, alors d'après l'égalité $a^5+b^5 = dc^p$ 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.

1. Supposons que ℓ divise $a+b$. Alors, $\phi(a,b) \equiv 5a^4 \pmod \ell$, d'après le lemme 2.4. On en déduit

   $$c_4 \equiv 2^4.5^2a^4 \pmod \ell$$

   d'où $v_\ell(c_4) = 0$. L'équation (6) est donc minimale en ℓ et E a réduction multiplicative en ℓ, d'où $v_\ell(N_E) = 1$ et $v_\ell(\Delta_m) = v_\ell(\Delta)$.
   Puisque ℓ divise $a+b$, ℓ ne divise pas $\phi(a,b)$ (lemme 2.5). On en déduit

   $$v_\ell(a+b) \equiv v_\ell(d) \pmod p.$$

   La congruence (12) entraîne alors la condition (10). L'équivalence (11) en résulte vu que l'on a $0 \leq v_\ell(d) \leq 4$.

2. Supposons que ℓ ne divise pas $a+b$. On a $\phi(a,b) \equiv 0 \pmod \ell$ car ℓ divise a^5+b^5 sans diviser $a+b$. D'après l'égalité (9), ℓ ne divise pas a^2+b^2 car ℓ ne divise pas ab. On en déduit que $v_\ell(c_4) = 0$. Par suite, l'équation (6) est minimale en ℓ et E a réduction multiplicative en ℓ, d'où $v_\ell(N_E) = 1$. D'après la congruence (12), on a $v_\ell(\Delta_m) \equiv 2v_\ell(d) \pmod p$ et l'on conclut comme ci-dessus.

2.3 Étude de la réduction de E en 5

On démontre le résultat suivant :

Lemme 2.8 *La courbe E a mauvaise réduction de type additif en 5 et l'on a $v_5(N_E) = 2$. L'équation (6) est minimale en 5. L'invariant modulaire j de E est entier en 5 si et seulement si 5 ne divise pas $a + b$.*

De plus, p divise $v_5(j)$ si et seulement si l'une des deux conditions suivantes est satisfaite :

1. *on a $a + b \not\equiv 0 \pmod 5$,*
2. *on a $a + b \equiv 0 \pmod 5$ et $(p, v_5(d)) \in \{(7, 3), (11, 4)\}$.*

Démonstration : On distingue deux cas.

1. Supposons que 5 ne divise pas $a + b$. Dans ce cas, $\phi(a, b) \equiv 1 \pmod 5$ 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 [16]) et l'on a ainsi $v_5(N_E) = 2$. L'égalité $j = c_4^3/\Delta$ entraîne alors $v_5(j) = 0$.
2. Supposons que 5 divise $a + b$. On a alors (lemme 2.4)
$$a^2 + b^2 \equiv -2ab \pmod{25} \quad \text{et} \quad \phi(a, b) \equiv 5a^2b^2 \pmod{25}.$$
On a donc :
$$\frac{c_4}{5} \equiv 2^4.5a^2b^2 \pmod{25} \quad \text{et} \quad \frac{c_6}{5^2} \equiv 2^6.5(ab)^3 \pmod{25},$$
d'où les égalités :
$$v_5(c_4) = 2 \quad \text{et} \quad v_5(c_6) = 3.$$
On en conclut que la courbe E a mauvaise réduction de type additif en 5 et que l'équation (6) est minimale en 5. 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.*).
D'après le lemme 2.5, on a :
$$v_5(a^5 + b^5) = v_5(a + b) + 1,$$
d'où $v_5(\Delta) = 5 + 4v_5(a + b) \geq 9$ et l'inégalité $v_5(j) < 0$.
De l'égalité
$$v_5(\Delta) = 5 + 4(v_5(d) + pv_5(c) - 1),$$
il vient :
$$v_5(j) = 6 - v_5(\Delta) \equiv 5 - 4v_5(d) \pmod p.$$
Autrement dit,
$$v_5(j) \equiv \begin{cases} 5 \pmod p & \text{si } v_5(d) = 0, \\ 1 \pmod p & \text{si } v_5(d) = 1, \\ -3 \pmod p & \text{si } v_5(d) = 2, \\ -7 \pmod p & \text{si } v_5(d) = 3, \\ -11 \pmod p & \text{si } v_5(d) = 4. \end{cases}$$
Cela établit le lemme.

2.4 Étude de la réduction de E en 2 si d est impair

On démontre le résultat suivant :

Lemme 2.9 *Supposons d impair. La courbe E a mauvaise réduction en* 2.

1. *Si a est pair, E a réduction de type additif en* 2. *On a*

$$v_2(N_E) = \begin{cases} 4 & si\ v_2(a) = 1, \\ 3 & si\ v_2(a) \geq 2. \end{cases}$$

2. *Si a est impair, E a réduction de type multiplicatif en* 2 *et l'on a alors* $v_2(N_E) = 1$.

L'équation (6) est minimale en 2 *si et seulement si a est pair.*

Démonstration : On est amené à distinguer deux cas suivant la parité de a.

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, on a

$$\begin{aligned} \frac{c_4}{2^4} \equiv 2 + 3ab^3 &\equiv 2 + 3ab \pmod 4 \\ &\equiv \begin{cases} 0 \pmod 4 & \text{si} \quad v_2(a) = 1 \\ 2 \pmod 4 & \text{si} \quad v_2(a) \geq 2. \end{cases} \end{aligned} \tag{13}$$

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

(a) Supposons $v_2(a) = 1$. On est dans le cas 3 ou 5 de Tate (cf. tableau IV, p.129 de [16]). 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 $v_2(N_E) = 4$.

(b) Supposons $v_2(a) \geq 2$. 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. Supposons a impair. Dans ce cas, d'après la remarque préliminaire 4, b est impair et c est pair. On a ainsi $\phi(a,b) \equiv 1 \pmod 2$, $a^2+b^2 \equiv 2 \pmod 4$ 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 (6) n'est pas minimale en 2. On étudie pour cela la congruence de $c_6/2^6$ modulo 4 ([10, p.77]). On constate que l'on a

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

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

Cela termine la démonstration du lemme 2.9.

2.5 Étude de la réduction de E en 2 si d est pair

On démontre le résultat suivant :

Lemme 2.10 *Supposons d pair.*

1. *Si c est impair et si $v_2(d) = 2$, E a bonne réduction en 2, auquel cas on a $v_2(N_E) = 0$.*
2. *Si c est impair et si $v_2(d) = 1$, E a mauvaise réduction de type additif en 2 et l'on a $v_2(N_E) = 4$.*
3. *Supposons c pair ou bien que l'on ait $v_2(d) = 3$ ou 4. Alors E a réduction de type multiplicatif en 2 et l'on a $v_2(N_E) = 1$.*

L'équation (6) est minimale en 2 si et seulement si c est impair et $v_2(d) = 2$.

Démonstration : Puisque d est pair, les entiers a et b sont impairs. On a donc $\phi(a,b) \equiv 1 \pmod 2$ et $v_2(a+b) = v_2(a^5+b^5)$. Il en résulte que l'on a

$$v_2(c_4) = 4, \quad v_2(c_6) = 6, \quad v_2(\Delta) = 4(1 + v_2(d) + pv_2(c)).$$

En particulier, on a

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

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 $v_2(\Delta) \geq 12$.

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 (6) 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 réduction multiplicative en 2 et l'on a $v_2(N_E) = 1$.

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 proposition 3 p.124 de [16], on est amené à déterminer si la congruence

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

a ou non une solution $r \in \mathbb{Z}$. On vérifie que $r = 1$ convient. D'après la proposition 3 de *loc. cit.*, il existe $t \in \mathbb{Z}$ 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 $ab \equiv 1$ ou $5 \pmod 8$.

   (a) 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.

   (b) 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 l'assertion.

Il en résulte que l'on est dans le cas 6 de Tate, puis que $v_2(N_E) = 4$. D'où le lemme 2.10.

Les propositions 2.1, 2.2 et 2.3 résultent alors des lemmes 2.7 à 2.10.

3 La représentation ρ_p^E

Soit p un nombre premier ≥ 7 et (a, b, c) un élément de $S_p(d)$. Notons $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ et $\mathrm{G}_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ le groupe de Galois absolu de $\mathbb{Q}$. Soit $E[p]$ le sous-groupe de $E(\overline{\mathbb{Q}})$ constitué des points de p-torsion de la courbe elliptique E. C'est un $\mathbb{F}_p$-espace vectoriel de dimension 2 sur lequel $\mathrm{G}_{\mathbb{Q}}$ opère continûment. Par le choix d'une base de $E[p]$ sur $\mathbb{F}_p$, on en déduit un homomorphisme de groupes

$$\rho_p^E : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathbf{GL}_2(\mathbb{F}_p).$$

À une telle représentation J.-P. Serre associe un poids k qui est un entier ≥ 2 et un conducteur $N(\rho_p^E)$ qui est un entier ≥ 1, premier à p, qui divise le conducteur N_E de E (cf. [19]).

Proposition 3.1 *La représentation ρ_p^E est irréductible.*

Démonstration : La courbe E a un point d'ordre deux rationnel sur $\mathbb{Q}$. Par suite, si ρ_p^E était réductible, le groupe $E(\overline{\mathbb{Q}})$ possèdrait un sous-groupe d'ordre $2p$ stable par $\mathrm{G}_{\mathbb{Q}}$, de sorte que la courbe modulaire $Y_0(2p)$ aurait un point rationnel sur $\mathbb{Q}$. Or, si $p \geq 11$, B. Mazur et M. A. Kenku ont démontré que l'ensemble $Y_0(2p)(\mathbb{Q})$ est vide (cf. [9]). D'où le résultat dans ce cas.

Supposons maintenant $p = 7$ et ρ_7^E réductible. La courbe modulaire $Y_0(14)$ est la courbe elliptique notée 14A1 dans les tables de [3] ([15, p.45]). Elle possède exactement deux points rationnels sur $\mathbb{Q}$ qui correspondent aux deux classes de $\overline{\mathbb{Q}}$-isomorphisme de courbes elliptiques d'invariants $j = -15^3$ et 255^3. Ce sont en effet les invariants modulaires des courbes notées 49A1 et 49A2 dans les tables de [3] et elles ont bien un sous-groupe d'ordre 14 stable par $\mathrm{G}_{\mathbb{Q}}$. La courbe elliptique E correspond donc à un point rationnel sur $\mathbb{Q}$ de la courbe modulaire $Y_0(14)$. En particulier, on a $j = -15^3$ ou 255^3. En posant $t = a/b$, on en déduit que t est une solution rationnelle de l'équation :

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

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

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 (lemme 2.7) et l'on a $k = 2$ d'après la proposition 5 p.191 de [19]. Si p divise c, puisque l'on a $p \geq 7$, la courbe E a réduction multiplicative en p (*loc. cit.*). Par ailleurs, p divise $v_p(\Delta_m)$ (*loc. cit.*), ce qui entraîne de nouveau $k = 2$.

Supposons que p divise d. D'après le lemme 2.7, la courbe E a alors réduction de type multiplicatif en p et p ne divise pas $v_p(\Delta_m)$. Cela conduit à $k = p + 1$, d'où le résultat.

Calcul de $N(\rho_p^E)$. Posons

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

où ℓ parcourt les diviseurs premiers de d distincts de $2, 5$ et p. Le conducteur $N(\rho_p^E)$ de ρ_p^E est donné dans les deux énoncés suivants :

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

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

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

1. $N(\rho_p^E) = 2.5^2 r'$*, si* $v_2(d) = 3$ *ou* 4 *;*
2. $N(\rho_p^E) = 5^2 r'$*, si* $v_2(d) = 2$ *;*
3. $N(\rho_p^E) = 2.5^2 r'$*, si* $v_2(d) = 1$ *et c est pair.*
4. $N(\rho_p^E) = 2^4.5^2 r'$*, si* $v_2(d) = 1$ *et c est impair.*

Avant de démontrer ces propositions, on commence par le résultat suivant.

Lemme 3.5 *Supposons que E ait réduction de type multiplicatif en* 2*. Alors,*

$$v_2(\Delta_m) \equiv -8 + 4v_2(d) \pmod{p}. \tag{14}$$

En particulier, p divise $v_2(\Delta_m)$ si et seulement si c est pair et $v_2(d) = 2$.

Démonstration : Puisque E a réduction de type multiplicatif en 2, on est dans l'un des cas suivants (lemmes 2.9 et 2.10) :

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

Dans chacun des trois cas ci-dessus, l'entier ab est impair donc

$$v_2(a + b) = v_2(a^5 + b^5).$$

D'après la proposition 2.1, on a :

$$\Delta_m = \frac{\Delta}{2^{12}}.$$

On en déduit

$$v_2(\Delta_m) = 4 + 4v_2(a^5 + b^5) - 12.$$

Or $v_2(a^5 + b^5) = v_2(d) + pv_2(c) \equiv v_2(d) \pmod{p}$. D'où la congruence (14). L'équivalence du lemme s'en déduit immédiatement car on a $0 \leq v_2(d) \leq 4$.

Démontrons à présent les propositions 3.3 et 3.4. Puisque $N(\rho_p^E)$ divise N_E, pour tout nombre premier ℓ qui ne divise pas $10r$, on a $v_\ell(N(\rho_p^E)) = 0$.

Considérons un diviseur premier ℓ de N_E distinct de $2, 5$ et p. D'après le lemme 2.7 et [11, p.28], on a

$$v_\ell(N(\rho_p^E)) = \begin{cases} 1 & \text{si } \ell \text{ divise } d, \\ 0 & \text{sinon.} \end{cases}$$

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

Il reste à déterminer l'exposant de 2 dans $N(\rho_p^E)$. La valeur de l'exposant de 2 dans le conducteur N_E est donnée dans les propositions 2.2 et 2.3. Dans le cas où E a réduction de type additif en 2, i.e. si $v_2(N_E) \geq 2$, on a $v_2(N(\rho_p^E)) = v_2(N_E)$ (*loc. cit.*). Si E a réduction multiplicative en 2, alors d'après le lemme 3.5, $v_2(N(\rho_p^E)) = v_2(N_E)$ sauf si c est pair et $v_2(d) = 2$ auquel cas on a $v_2(N(\rho_p^E)) = v_2(N_E) - 1$, i.e. $v_2(N(\rho_p^E)) = 0$.

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

4 Démonstrations des résultats

On suppose pour toute la suite qu'il existe un élément $(a, b, c) \in S_p(d)$ où p est un nombre premier ≥ 7. Soit E la courbe d'équation (6) attachée à la solution (a, b, c).

Notations. Si n est un entier ≥ 1, on note $\mathcal{S}_2^+(n)$ le $\mathbb{C}$-espace vectoriel formé des newforms paraboliques de poids 2 pour le sous-groupe $\Gamma_0(n)$ au sens de [1].

La représentation ρ_p^E est irréductible, de poids 2 et de conducteur $N(\rho_p^E)$. D'après les travaux de K. Ribet (cf. [17]), il existe alors une newform

$$f = q + \sum_{n \geq 2} a_n(f) q^n \in \mathcal{S}_2^+(N(\rho_p^E)) \quad \text{avec} \quad q = e^{2i\pi\tau},$$

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

$$\begin{cases} a_\ell(f) \equiv a_\ell(E) \pmod{\mathfrak{P}} & \text{si } \ell \text{ ne divise pas } pN_E, \\ a_\ell(f) \equiv \pm(\ell + 1) \pmod{\mathfrak{P}} & \text{si } \ell \text{ divise } N_E \text{ et ne divise pas } pN(\rho_p^E). \end{cases} \tag{15}$$

Par ailleurs, dans le cas où les coefficients $a_n(f)$ sont dans $\mathbb{Z}$, la newform f correspond à une courbe elliptique $A/\mathbb{Q}$ de conducteur $N(\rho_p^E)$ unique à isogénie près. Notons respectivement

$$L_E(s) = \sum_{n \geq 1} a_n(E) n^{-s} \quad \text{et} \quad L_A(s) = \sum_{n \geq 1} a_n(A) n^{-s}$$

les fonctions L de Hasse - Weil de E et A.

Les représentations ρ_p^E et ρ_p^A sont alors isomorphes et l'on a en particulier :

$$a_\ell(E) \equiv a_\ell(A) \pmod{p}, \tag{16}$$

pour tout nombre premier ℓ ne divisant pas N_E (cf. [14]). Il s'agit de contredire l'existence de f.

Soit $\mathbb{Q}(E[p])/\mathbb{Q}$ l'extension de $\mathbb{Q}$ engendrée par les coordonnées des points de p-torsion de E. C'est une extension galoisienne de $\mathbb{Q}$. On note e son indice de ramification en 5.

Le lemme suivant intervient dans les paragraphes 4.3 et 4.4.

Lemme 4.1 *1. Si 5 divise $a+b$, on a :*

$$e = \begin{cases} 2 & \text{si } (p, v_5(d)) = (7,3) \text{ ou } (11,4), \\ 2p & \text{sinon.} \end{cases} \tag{17}$$

2. Si 5 ne divise pas $a+b$, on a $e = 4$.

Démonstration : Si 5 divise $a+b$, la courbe 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 (lemme 2.8). L'égalité (17) résulte alors du lemme 2.8 et de [2, p.7].

Si 5 ne divise pas $a+b$, l'invariant modulaire j de E est entier en 5 (lemme 2.8). La courbe E a donc potentiellement bonne réduction en 5. La valuation en 5 de son discriminant minimal vaut 3 (cf. §2.3). Le défaut de semi-stabilité en 5 de E (qui est mesuré par l'ordre d'un certain groupe fini Φ_5) est donc d'ordre 4 ([18, p.312]), d'où le résultat.

4.1 Démonstration du théorème 1.1

On suppose ici que l'on a $d = 1$ et que c est pair. L'entier a est impair. D'après l'étude faite dans la partie 3, la représentation ρ_p^E est irréductible de poids 2 et de conducteur 50. Or une base du $\mathbb{C}$-espace vectoriel $\mathcal{S}_2^+(50)$ correspond aux deux courbes elliptiques sur $\mathbb{Q}$ de conducteur 50 notées 50A1 et 50B1 dans [3] et d'équations respectives :

$$\begin{aligned} 50\text{A1} : y^2 + xy + y &= x^3 - x - 2, \\ 50\text{B1} : y^2 + xy + y &= x^3 + x^2 - 3x + 1. \end{aligned}$$

On va alors contredire les congruences (15) avec le nombre premier $\ell = 3$. On remarque pour cela que l'on a

$$\begin{cases} a_3(50\text{A1}) &= +1, \\ a_3(50\text{B1}) &= -1. \end{cases}$$

Par ailleurs, la courbe elliptique E a réduction semi-stable en 3 (lemme 2.7). Supposons que E ait réduction multiplicative en 3. Puisque 3 divise N_E, mais pas $50p = pN(\rho_p^E)$, on déduit des congruences (15) que l'on a

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

ce qui conduit à une contradiction car $p \geq 7$. La courbe E a donc bonne réduction en 3. Puisque E a un point d'ordre 2 rationnel sur $\mathbb{Q}$, $a_3(E)$ est pair et l'inégalité $|a_3(E)| < 2\sqrt{3}$ ([20, th.1.1, p.131]) entraîne $a_3(E) = 0$ ou ± 2. D'après les congruences (15), on a donc

$$\pm 1 \equiv a_3(E) \pmod{p},$$

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

4.2 Démonstration du théorème 1.2

On a $r' = 1$. On distingue deux cas suivant la valeur de $v_2(d)$.

1. Supposons $v_2(d) = 2$. D'après la proposition 3.4, on a $N(\rho_p^E) = 25$. Or l'espace $\mathcal{S}_2^+(25)$ est réduit à 0. D'où le théorème dans ce cas.
2. Supposons $v_2(d) = 3$ ou 4. Dans ce cas, on a $N(\rho_p^E) = 50$, ce qui entraîne, par le même argument que celui utilisé dans le §4.1, le résultat.

4.3 Démonstration du théorème 1.3

Supposons que l'on soit dans le cas où les coefficients $a_n(f)$ sont dans $\mathbb{Z}$. Les congruences (16) sont réalisées. On utilise ici la méthode symplectique reposant sur le lemme suivant ([8, p.180]). Notons $\Delta_m(A)$ le discriminant minimal de A.

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

On suppose ici que d s'écrit

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

D'après la proposition 3.4, on a alors :

$$N(\rho_p^E) \quad = \quad 150.$$

Une base de $\mathcal{S}_2^+(150)$ correspond aux trois classes d'isogénie de courbes elliptiques sur $\mathbb{Q}$ de conducteur 150. Ainsi ρ_p^E est isomorphe à la représentation de $\mathrm{G}_\mathbb{Q}$ dans les points de p-torsion de l'une des courbes notées 150A1, 150B1 et 150C1 dans les tables de [3]. Par ailleurs, E a réduction multiplicative en 2 et 3 (lemmes 2.7 et 2.10) et d'après le lemme 3.5, on a donc :

$$v_2(\Delta_m) \equiv \begin{cases} 4 \pmod{p} & \text{si } \alpha = 3 \\ 8 \pmod{p} & \text{si } \alpha = 4. \end{cases} \tag{18}$$

D'après le lemme 2.6, 3 divise $a+b$ et d'après le lemme 2.7, on a donc :

$$v_3(\Delta_m) \equiv 4\beta \pmod{p}. \tag{19}$$

Les entiers $v_2(\Delta_m)$ et $v_3(\Delta_m)$ ne sont pas divisibles par p.

On distingue alors deux cas suivant la valeur de l'entier α.

4.3.1 Supposons $\alpha = 3$

On distingue deux cas selon que 5 divise on non $a+b$.

1. Supposons que 5 divise $a+b$. Démontrons que l'on a les assertions suivantes :
$$\begin{cases} 3 \pmod{p} \in (\mathbb{F}_p^*)^2 & \text{si } \beta = 1 \text{ ou } 4, \\ 6 \pmod{p} \in (\mathbb{F}_p^*)^2 & \text{si } \beta = 2. \end{cases} \tag{20}$$
D'après le lemme 4.1, l'indice de ramification en 5 de l'extension $\mathbb{Q}(E[p])/\mathbb{Q}$ est 2 ou $2p$. Or les courbes notées 150A1 et 150B1 dans [3] 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. L'indice de ramification en 5 des extensions de $\mathbb{Q}$ engendrées par leurs points de p-torsion vaut donc 4 ([18, p.312]). Puisque l'on a $p \neq 2$, cela entraîne que ρ_p^E est isomorphe à ρ_p^A, où A est la courbe elliptique notée 150C1 dans [3]. On applique alors le résultat du lemme 4.2 avec les courbes E et A, et les nombres premiers $\ell_1 = 2$, $\ell_2 = 3$. On a $v_2(\Delta_m(A)) = 4$ et $v_3(\Delta_m(A)) = 3$. D'après (18) et (19), on obtient ainsi :
$$3 \pmod{p} \equiv \beta \pmod{p} \pmod{(\mathbb{F}_p^*)^2},$$
d'où les assertions (20).
2. Supposons que 5 ne divise pas $a+b$. Dans ce cas, vérifions que l'on a :
$$\begin{cases} 2 \pmod{p} \in (\mathbb{F}_p^*)^2 & \text{si } \beta = 1 \text{ ou } 4 \\ 6 \pmod{p} \in (\mathbb{F}_p^*)^2 & \text{si } \beta = 3. \end{cases} \tag{21}$$
L'invariant modulaire de E est entier en 5. D'après le lemme 4.1, l'indice de ramification en 5 de l'extension $\mathbb{Q}(E[p])/\mathbb{Q}$ est 4. Or la courbe elliptique notée 150C1 a un invariant modulaire non entier en 5. Comme ci-dessus, on en déduit que ρ_p^E est isomorphe à ρ_p^A, où A est l'une des courbes elliptiques notées 150A1 et 150B1 dans [3]. On a $v_2(\Delta_m(A)) = 2$ et $v_3(\Delta_m(A)) = 1$. D'après le lemme 4.2 et les congruences (18) et (19), on obtient :
$$2 \pmod{p} \equiv \beta \pmod{p} \pmod{(\mathbb{F}_p^*)^2},$$
d'où les assertions (21).

Démontrons le théorème 1.3 si $\alpha = 3$. Supposons $\gamma \geq 1$. Dans ce cas, d'après le lemme 2.6, 5 divise $a + b$. Par hypothèse, on a $\beta \in \{1, 2, 4\}$. Par ailleurs, on a les équivalences :

$$3 \pmod p \notin (\mathbb{F}_p^*)^2 \iff p \equiv 5 \text{ ou } 7 \pmod{12}, \tag{22}$$

et

$$6 \pmod p \notin (\mathbb{F}_p^*)^2 \iff p \equiv 7, 11, 13 \text{ ou } 17 \pmod{24}, \tag{23}$$

d'où le résultat dans ce cas.

Supposons $\gamma = 0$, i.e. 5 ne divise pas d. On a alors $\beta = 1$ ou 4. Et, d'après ce qui précède, 2 (mod p) ou 3 (mod p) appartient à $(\mathbb{F}_p^*)^2$ suivant que 5 divise ou non $a + b$.

De l'équivalence

$$2 \pmod p \notin (\mathbb{F}_p^*)^2 \iff p \equiv 3 \text{ ou } 5 \pmod 8, \tag{24}$$

on déduit :

$$3 \pmod p \notin (\mathbb{F}_p^*)^2 \text{ et } 2 \pmod p \notin (\mathbb{F}_p^*)^2 \iff p \equiv 5 \text{ ou } 19 \pmod{24}. \tag{25}$$

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

4.3.2 Supposons $\alpha = 4$

La démarche est identique à celle du paragraphe précédent : seules les congruences obtenues diffèrent. On explicitera donc les calculs sans répéter exhaustivement les raisonnements.

1. Supposons que 5 divise $a + b$. La représentation ρ_p^E est alors isomorphe à ρ_p^A, où A est la courbe elliptique notée 150C1 dans [3]. On déduit du lemme 4.2 les congruences :

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

   Autrement dit, on a :

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

2. Supposons que 5 ne divise pas $a + b$. On sait qu'alors ρ_p^E est isomorphe à ρ_p^A, où A est l'une des courbes elliptiques notées 150A1 et 150B1 dans [3]. On obtient dans ce cas :

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

Démontrons alors le théorème 1.3 si $\alpha = 4$.

Supposons $\gamma = 0$, i.e. 5 ne divise pas d. Alors par hypothèse $\beta = 2$ ou 3. D'après les alinéas ci-dessus, 2 (mod p) ou 3 (mod p) appartient à $(\mathbb{F}_p^*)^2$. D'où le résultat dans ce cas, d'après la congruence (25).

Supposons $\gamma \geq 1$. Alors 5 divise $a + b$ et $\beta \in \{1, 2, 3, 4\}$. Si $\beta = 1$ ou 4, on a le résultat avec la congruence (23). Les cas où $\beta = 2$ et $\beta = 3$ se déduisent respectivement des congruences (22) et (24).

Ceci achève la démonstration du théorème 1.3.

4.4 Démonstration du théorème 1.4

On rappelle que p est un nombre premier ≥ 7, (a, b, c) est un élément de $S_p(3)$ et que E la courbe d'équation (6) attachée à (a, b, c).

D'après la proposition 3.3, on a :

$$N(\rho_p^E) = \begin{cases} 150 & \text{si } a \text{ est impair;} \\ 600 & \text{si } v_2(a) \geq 2; \\ 1200 & \text{si } v_2(a) = 1. \end{cases}$$

Les newforms appartenant aux espaces $\mathcal{S}_2^+(150)$, $\mathcal{S}_2^+(600)$ et $\mathcal{S}_2^+(1200)$ sont toutes à coefficients entiers relatifs. Elles correspondent donc à des courbes elliptiques. Il y a en trois de conducteur 150, neuf de conducteur 600 et dix-neuf de conducteur 1200, soit trente-et-une courbes au total. Par commodité pour le lecteur, on donne en Appendice la liste des équations de ces courbes elliptiques ainsi que la valeur des invariants dont on aura besoin.

On considère les deux ensembles de courbes elliptiques suivants, avec les notations des tables de [3] :

$$\begin{aligned} \mathcal{F}_1 &= \{150\text{C1}, 600\text{A1}, 600\text{F1}, 1200\text{E1}, 1200\text{G1}, 1200\text{J1}, 1200\text{P1}\}; \\ \mathcal{F}_2 &= \{150\text{A1}, 150\text{B1}, 600\text{C1}, 600\text{H1}, 1200\text{B1}, 1200\text{I1}, 1200\text{M1} \\ &\quad 1200\text{N1}, 1200\text{Q1}, 1200\text{S1}\}. \end{aligned}$$

Le lemme suivant décrit les isomorphismes possibles entre ρ_p^E et les représentations ρ_p^A où A est l'une des trente-et-une courbes elliptiques de conducteur 150, 600 et 1200.

Lemme 4.3 *1. Si 5 divise $a + b$, alors il existe A dans $\mathcal{F}_1$ tel que ρ_p^E soit isomorphe à ρ_p^A ;*

2. Si 5 ne divise pas $a+b$, alors il existe A dans $\mathcal{F}_2$ tel que ρ_p^E soit isomorphe à ρ_p^A.

Démonstration : La représentation ρ_p^E est isomorphe à la représentation ρ_p^A d'une courbe elliptique A de conducteur 150, 600 ou 1200. Définissons l'ensemble suivant :

$$\begin{aligned} \mathcal{G} = \{&150\text{A1}, 150\text{B1}, 600\text{B1}, 600\text{C1}, 600\text{D1}, 600\text{E1}, 600\text{G1}, 600\text{H1}, 600\text{I1}, \\ &1200\text{A1}, 1200\text{B1}, 1200\text{C1}, 1200\text{D1}, 1200\text{F1}, 1200\text{H1}, 1200\text{I1}, 1200\text{K1}, \\ &1200\text{L1}, 1200\text{M1}, 1200\text{N1}, 1200\text{O1}, 1200\text{Q1}, 1200\text{R1}, 1200\text{S1}\}. \end{aligned}$$

D'après le tableau 2 de l'Appendice, l'ensemble $\mathcal{G}$ (resp. $\mathcal{F}_1$) correspond précisément aux courbes de conducteur 150, 600 et 1200 ayant un invariant modulaire j entier en 5 (resp. non entier en 5).

On rappelle que la courbe E a réduction additive en 5 (lemme 2.8).

1. Supposons tout d'abord que 5 divise $a+b$. D'après le lemme 4.1, l'indice de ramification en 5 de l'extension $\mathbb{Q}(E[p])/\mathbb{Q}$ est $2p$ (car $v_5(d) \neq 3, 4$). Or les courbes de l'ensemble $\mathcal{G}$ ont toutes réduction additive en 5 et leur invariant modulaire est entier en 5. Leur défaut de semi-stabilité en 5 est alors d'ordre 2, 3, 4 ou 6 (cf. le tableau 2). En particulier, ρ_p^E n'est isomorphe à la représentation modulo p d'aucune des courbes de l'ensemble $\mathcal{G}$. Autrement dit, ρ_p^E est isomorphe à ρ_p^A où A est une courbe de l'ensemble $\mathcal{F}_1$.
2. Supposons que 5 ne divise pas $a+b$. L'invariant modulaire de E est entier en 5 (lemme 2.8). D'après le lemme 4.1, l'indice de ramification en 5 de l'extension $\mathbb{Q}(E[p])/\mathbb{Q}$ est 4. Or les courbes A de l'ensemble $\mathcal{F}_1$ ont toutes réduction additive en 5 et leur invariant modulaire n'est pas entier en 5. L'indice de ramification en 5 de l'extension $\mathbb{Q}(A[p])/\mathbb{Q}$ est alors $2p$ (cf. tableau 2). En particulier, ρ_p^E n'est isomorphe à la représentation modulo p d'aucune de ces courbes.

   Par ailleurs, parmi les courbes de l'ensemble $\mathcal{G}$, seules celles de l'ensemble $\mathcal{F}_2$ ont un défaut de semi-stabilité en 5 d'ordre 4. On en déduit que dans ce cas, ρ_p^E est isomorphe à ρ_p^A où A est une courbe de l'ensemble $\mathcal{F}_2$.

Ceci achève la démonstration du lemme 4.3.

Remarque. Parmi les courbes des ensembles $\mathcal{F}_1$ et $\mathcal{F}_2$ du début du paragraphe, les courbes suivantes ont le même invariant modulaire j :

- 150C1 et 1200P1,
- 600A1 et 1200E1,
- 600F1 et 1200G1,
- 150A1, 150B1, 1200M1 et 1200Q1,
- 600C1, 600H1, 1200B1 et 1200I1,
- 600D1 et 1200A1,
- 1200N1 et 1200S1.

Leur invariant modulaire étant différent de 0 et de 1728, elles sont donc isomorphes sur une extension quadratique de $\mathbb{Q}$. L'ensemble $\mathcal{E}_1$ (resp. $\mathcal{E}_2$) du théorème 1.4 est un ensemble de représentants des classes d'isomorphisme des courbes de l'ensemble $\mathcal{F}_1$ (resp. $\mathcal{F}_2$).

En particulier, pour toute courbe A de l'ensemble $\mathcal{F}_1$ (resp. $\mathcal{F}_2$), il existe une unique courbe F de l'ensemble $\mathcal{E}_1$ (resp. $\mathcal{E}_2$) de même invariant modulaire que A. On a alors pour tout nombre premier ℓ :

$$a_\ell(A)^2 = a_\ell(F)^2. \tag{26}$$

Montrons à présent le théorème 1.4. D'après le lemme 4.3, ρ_p^E est isomorphe à ρ_p^A où A est une courbe des ensembles $\mathcal{F}_1$ et $\mathcal{F}_2$. On note F l'unique courbe elliptique des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$ de même invariant modulaire que A. Soit alors n un entier ≥ 2 tel que le couple (F, n) vérifie la condition 1 du théorème 1.4

si A appartient à $\mathcal{F}_1$ et la condition 2 si A appartient à $\mathcal{F}_2$. On a le résultat suivant.

Lemme 4.4 *La courbe E a bonne réduction en q. Autrement dit, q ne divise pas c.*

DÉMONSTRATION : Supposons que ce ne soit pas le cas. Dans ce cas, q divise c et d'après le lemme 2.7, la courbe E a réduction multiplicative en q. Comme A a bonne réduction en q, il vient d'après [14, prop.3(iii)] :

$$a_q(A) \equiv \pm(q+1) \equiv \pm 2 \pmod{p}.$$

Or, d'après (26), on a $a_q(A)^2 = a_q(F)^2$. C'est en contradiction avec les hypothèses du thèorème. D'où le lemme.

Désignons par $\overline{a}$ et $\overline{b}$ les réductions de a et b modulo q. On distingue à présent deux cas.

1. Supposons que 5 divise $a+b$, i.e. $F \in \mathcal{E}_1$. D'après les lemmes 2.5 et 2.6, il existe c_1 et c_2 deux entiers tels que :

   $$5(a+b) = 3c_1^p, \quad \phi(a,b) = 5c_2^p \quad \text{et} \quad c = c_1 c_2.$$

   De plus d'après le lemme 4.4, q ne divise pas c, ainsi

   $$u = c_1^p \pmod{q} \in \mu_n(\mathbb{F}_q) \quad \text{et} \quad v = c_2^p \pmod{q} \in \mu_n(\mathbb{F}_q).$$

   On a alors :

   $$5(\overline{a}+\overline{b}) = 3u \quad \text{et} \quad \phi(\overline{a},\overline{b}) = 5v.$$

   En posant

   $$\overline{a}' = \frac{\overline{a}}{u}, \quad \overline{b}' = \frac{\overline{b}}{u} \quad \text{et} \quad \zeta = \frac{v}{u^4},$$

   on obtient :

   $$5(\overline{a}'+\overline{b}') = 3 \quad \text{et} \quad \phi(\overline{a}',\overline{b}') = 5\zeta. \tag{27}$$

   On en déduit que $\overline{b}'$ est racine du polynôme

   $$P_{1,\zeta}(X) = X^4 - \frac{6}{5}X^3 + \frac{18}{25}X^2 - \frac{27}{125}X + \frac{81}{3125} - \zeta \in \mathbb{F}_q[X].$$

   Avec les notations de la partie 1, l'égalité $P_{1,\zeta}(\overline{b}') = 0$ entraîne alors

   $$\zeta \in \widetilde{A}(n,q).$$

   Choisissons $\alpha_{1,\zeta}$ une racine carrée de $-225 + 10\delta_{1,\zeta}$ et $\beta_{1,\zeta}$ une racine carrée de $-225 - 10\delta_{1,\zeta}$ dans une clôture algébrique $\overline{\mathbb{F}_q}$ de $\mathbb{F}_q$. Les racines de $P_{1,\zeta}$ dans $\overline{\mathbb{F}_q}$ sont :

   $$\frac{3}{10} + \frac{\alpha_{1,\zeta}}{50}, \quad \frac{3}{10} - \frac{\alpha_{1,\zeta}}{50}, \quad \frac{3}{10} + \frac{\beta_{1,\zeta}}{50}, \quad \frac{3}{10} - \frac{\beta_{1,\zeta}}{50}.$$

Il en résulte que $\overline{b}'$ est l'un de ces éléments. On en déduit que $\alpha_{1,\zeta}$ ou $\beta_{1,\zeta}$ est dans $\mathbb{F}_q$ et que $\zeta \in A(n,q)$. Par ailleurs, on a (formule (27))

$$\overline{a}' = \frac{3}{5} - \overline{b}'.$$

D'où :

$$\{\overline{a}', \overline{b}'\} = \left\{\frac{3}{10} + \frac{\alpha_{1,\zeta}}{50}, \frac{3}{10} - \frac{\alpha_{1,\zeta}}{50}\right\} \quad \text{ou} \quad \{\overline{a}', \overline{b}'\} = \left\{\frac{3}{10} + \frac{\beta_{1,\zeta}}{50}, \frac{3}{10} - \frac{\beta_{1,\zeta}}{50}\right\}.$$

On a donc respectivement

$$\overline{a}'^2 + \overline{b}'^2 = \frac{\delta_{1,\zeta}}{125} \quad \text{ou} \quad \overline{a}'^2 + \overline{b}'^2 = -\frac{\delta_{1,\zeta}}{125}.$$

Explicitons à présent l'équation de la courbe sur $\mathbb{F}_q$ déduite de (6) par réduction modulo q. Compte tenu de ce qui précède, il s'agit de l'équation

$$y^2 = x^3 - 5u^2(\overline{a}'^2 + \overline{b}'^2)x^2 + 5u^4\phi(\overline{a}', \overline{b}')x$$

qui est isomorphe sur $\mathbb{F}_q$ à la courbe d'équation

$$y^2 = x^3 - 5(\overline{a}'^2 + \overline{b}'^2)x^2 + 5\phi(\overline{a}', \overline{b}')x. \tag{28}$$

Si $\overline{a}'^2 + \overline{b}'^2 = -\frac{\delta_{1,\zeta}}{125}$, il s'agit de la courbe la courbe $F_{1,\zeta}$ d'équation

$$y^2 = x^3 + \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x. \tag{29}$$

Si $\overline{a}'^2 + \overline{b}'^2 = \frac{\delta_{1,\zeta}}{125}$, il s'agit de la tordue quadratique de $F_{1,\zeta}$ par $\sqrt{-1}$, notée $F'_{1,\zeta}$. Elle a pour équation

$$y^2 = x^3 - \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x. \tag{30}$$

Posons alors

$$a'_q(\zeta) = q + 1 - n'_{1,q}(\zeta) \tag{31}$$

où $n'_{1,q}(\zeta)$ le nombre de points rationnels sur $\mathbb{F}_q$ de $F'_{1,\zeta}$. On a

$$a'_q(\zeta) = \pm a_q(\zeta).$$

Il en résulte l'égalité

$$a_q(E)^2 = a_q(\zeta)^2. \tag{32}$$

D'après la congruence (16) et l'égalité (26), on en déduit que :

$$a_q(\zeta)^2 \equiv a_q(F)^2 \pmod{p}.$$

C'est en contradiction avec la condition $1(c)$ du théorème 1.4.

2. Supposons que 5 ne divise pas $a+b$. Comme ci-dessus, il existe alors c_1 et c_2 deux entiers tels que :

$$a+b=3c_1^p, \quad \phi(a,b)=c_2^p \quad \text{et} \quad c=c_1c_2.$$

D'après le lemme 4.4, q ne divise pas c, ainsi :

$$u=c_1^p \pmod q \in \mu_n(\mathbb{F}_q) \quad \text{et} \quad v=c_2^p \pmod q \in \mu_n(\mathbb{F}_q).$$

On a alors :

$$\overline{a}+\overline{b}=3u \quad \text{et} \quad \phi(\overline{a},\overline{b})=v.$$

En posant

$$\overline{a}'=\frac{\overline{a}}{u}, \quad \overline{b}'=\frac{\overline{b}}{u} \quad \text{et} \quad \zeta=\frac{v}{u^4},$$

on obtient :

$$\overline{a}'+\overline{b}'=3 \quad \text{et} \quad \phi(\overline{a}',\overline{b}')=\zeta. \tag{33}$$

On en déduit que $\overline{b}'$ est racine du polynôme

$$P_{2,\zeta}(X)=X^4-6X^3+18X^2-27X+\frac{81-\zeta}{5}\in\mathbb{F}_q[X].$$

Avec les notations de la partie 1, l'égalité $P_{2,\zeta}(\overline{b}')=0$ entraîne alors

$$\zeta\in\widetilde{B}(n,q).$$

Choisissons $\alpha_{2,\zeta}$ une racine carrée de $-225+10\delta_{2,\zeta}$ et $\beta_{2,\zeta}$ une racine carrée de $-225-10\delta_{2,\zeta}$ dans $\overline{\mathbb{F}_q}$. Les racines de $P_{2,\zeta}$ dans $\overline{\mathbb{F}_q}$ sont alors :

$$\frac{3}{2}+\frac{\alpha_{2,\zeta}}{10}, \quad \frac{3}{2}-\frac{\alpha_{2,\zeta}}{10}, \quad \frac{3}{2}+\frac{\beta_{2,\zeta}}{10}, \quad \frac{3}{2}-\frac{\beta_{2,\zeta}}{10}.$$

Il en résulte que $\overline{b}'$ est l'un de ces éléments. On en déduit que $\alpha_{2,\zeta}$ ou $\beta_{2,\zeta}$ est dans $\mathbb{F}_q$ et que $\zeta\in B(n,q)$. Par ailleurs, on a (formule (33))

$$\overline{a}'=3-\overline{b}'.$$

D'où :

$$\{\overline{a}',\overline{b}'\}=\left\{\frac{3}{2}+\frac{\alpha_{2,\zeta}}{10},\frac{3}{2}-\frac{\alpha_{2,\zeta}}{10}\right\} \quad \text{ou} \quad \{\overline{a}',\overline{b}'\}=\left\{\frac{3}{2}+\frac{\beta_{2,\zeta}}{10},\frac{3}{2}-\frac{\beta_{2,\zeta}}{10}\right\}.$$

On a donc respectivement

$$\overline{a}'^2+\overline{b}'^2=\frac{\delta_{2,\zeta}}{5} \quad \text{ou} \quad \overline{a}'^2+\overline{b}'^2=-\frac{\delta_{2,\zeta}}{5}.$$

Explicitons à présent l'équation de la courbe sur $\mathbb{F}_q$ déduite de (6) par réduction modulo q. Il s'agit de l'équation

$$y^2=x^3-5u^2(\overline{a}'^2+\overline{b}'^2)x^2+5u^4\phi(\overline{a}',\overline{b}')x$$

qui est isomorphe sur $\mathbb{F}_q$ à la courbe d'équation

$$y^2 = x^3 - 5(\overline{a}'^2 + \overline{b}'^2)x^2 + 5\phi(\overline{a}', \overline{b}')x.$$

Si $\overline{a}'^2 + \overline{b}'^2 = \frac{\delta_{2,\zeta}}{5}$, il s'agit de la courbe $F_{2,\zeta}$ d'équation

$$y^2 = x^3 + \delta_{2,\zeta}x^2 + 5\zeta x. \tag{34}$$

Si $\overline{a}'^2 + \overline{b}'^2 = -\frac{\delta_{2,\zeta}}{5}$, il s'agit de la tordue quadratique de $F_{2,\zeta}$ par $\sqrt{-1}$, notée $F'_{2,\zeta}$. Elle a pour équation

$$y^2 = x^3 - \delta_{2,\zeta}x^2 + 5\zeta x. \tag{35}$$

Posons alors comme ci-dessus

$$b'_q(\zeta) = q + 1 - n'_{2,q}(\zeta) \tag{36}$$

où $n'_{2,q}(\zeta)$ le nombre de points rationnels sur $\mathbb{F}_q$ de $F'_{2,\zeta}$. On a, à nouveau

$$b'_q(\zeta) = \pm b_q(\zeta),$$

puis

$$a_q(E)^2 = b_q(\zeta)^2. \tag{37}$$

D'après la congruence (16) et l'égalité (26), on en déduit que :

$$b_q(\zeta)^2 \equiv a_q(F)^2 \pmod{p},$$

ce qui contredit la condition $2(c)$ du théorème 1.4.

On aboutit ainsi à une contradiction à l'existence de $(a, b, c) \in S_p(3)$. Par suite, $S_p(3)$ est vide. Cela termine la démonstration du théorème 1.4.

4.5 Démonstration de la proposition 1.5

Il s'agit de montrer que l'équation $x^5 + y^5 = 3z^p$ n'admet pas de solution propre et non triviale pour $5 \leq p \leq 10^6$. C'est connu pour $p = 5$ (cf. [6]).

L'équation $x^5 + y^5 = 3z^7$. On suppose que l'on a $p = 7$. Pour toute courbe elliptique A de $\mathcal{F}_1$ et $\mathcal{F}_2$, il s'agit de montrer que ρ_7^E n'est pas isomorphe à ρ_7^A (lemme 4.3). Pour certaines de ces courbes A, on utilise pour cela la remarque suivante qui est une conséquance directe de la démonstration du théorème 1.4.

Remarque. Soit A l'une des courbes elliptiques de $\mathcal{F}_1$ (resp. de $\mathcal{F}_2$). Soit F l'unique courbe de $\mathcal{E}_1$ (resp. de $\mathcal{E}_2$) ayant le même invariant modulaire que A. Si l'on démontre l'existence d'un entier $n \geq 2$ pour lequel la condition 1 (resp. la condition 2) du théorème 1.4 est satisfaite, alors les représentations ρ_7^E et ρ_7^A ne sont pas isomorphes.

En utilisant cette remarque, on parvient à éliminer directement les courbes suivantes :

$$150\text{A1}, 150\text{B1}, 150\text{C1}, 600\text{A1}, 600\text{F1}, 1200\text{E1},$$
$$1200\text{G1}, 1200\text{P1}, 1200\text{M1}, 1200\text{N1}, 1200\text{Q1}, 1200\text{S1}.$$

En effet, si $A \in \{150\text{C1}, 1200\text{P1}\}$, le couple $(F, n) = (150\text{C1}, 16)$ vérifie la condition 1 du théorème 1.4. On en déduit, comme au paragraphe précédent, que ρ_7^E et ρ_7^A ne sont pas isomorphes. De même :

- si $A \in \{600\text{A1}, 1200\text{E1}\}$, le couple $(F, n) = (600\text{A1}, 16)$ vérifie la condition 1 du théorème.
- Si $A \in \{600\text{F1}, 1200\text{G1}\}$, le couple $(F, n) = (600\text{F1}, 16)$ vérifie la condition 1 du théorème.
- Si $A \in \{150\text{A1}, 150\text{B1}, 1200\text{M1}, 1200\text{Q1}\}$, le couple $(F, n) = (150\text{A1}, 4)$ vérifie la condition 2 du théorème.
- Si $A \in \{1200\text{N1}, 1200\text{S1}\}$, le couple $(F, n) = (1200\text{N1}, 6)$ vérifie la condition 2 du théorème.

Il reste à montrer que ρ_7^E n'est pas isomorphe à ρ_7^A où A est l'une des courbes

$$1200\text{J1},\ 600\text{C1},\ 600\text{H1},\ 1200\text{B1} \text{ et } 1200\text{I1}.$$

Supposons que ρ_7^E soit isomorphe à ρ_7^A où $A = 1200\text{J1}$. D'après le lemme 4.4, E a bonne réduction en $q = 43$ car

$$a_q(1200\text{J1}) = 4 \not\equiv \pm 2 \pmod 7. \tag{38}$$

De plus, d'après le lemme 4.3, 5 divise $a+b$. Déterminons les équations possibles de la courbe de Frey réduite modulo 43. On a

$$\mu_6(\mathbb{F}_{43}) = \{1 \pmod{43}, 6 \pmod{43}, 7 \pmod{43}, 36 \pmod{43}, 37 \pmod{43}, 42 \pmod{43}\},$$

puis

$$\widetilde{A}(6, 43) = \{6 \pmod{43}, 7 \pmod{43}, 36 \pmod{43}, 37 \pmod{43}, 42 \pmod{43}\}$$

et

$$A(6, 43) = \{6 \pmod{43}, 7 \pmod{43}\}.$$

Avec les notations du paragraphe précédent, on a donc $\zeta = 6 \pmod{43}$ ou $\zeta = 7 \pmod{43}$.

Supposons que $\zeta = 6 \pmod{43}$. Alors, toujours avec les notations du paragraphe précédent, on a que $\overline{b}'$ est racine du polynôme

$$\begin{aligned} P_{1,6}(X) &= X^4 + 16X^3 - X^2 - 4X + 22 \\ &= (X+2)(X+6)(X^2+8X+9) \in \mathbb{F}_{43}[X]. \end{aligned}$$

D'où $\overline{b}' = -2 \pmod{43}$ ou $-6 \pmod{43}$ et

$$(\overline{a}', \overline{b}') = (37 \pmod{43}, -2 \pmod{43})$$

ou

$$(\overline{a}', \overline{b}') = (41 \pmod{43}, -6 \pmod{43}).$$

La courbe de Frey réduite modulo 43 est alors isomorphe sur $\mathbb{F}_{43}$ à la courbe $F'_{1,6}$ d'équation (cf. (28) et (30))

$$y^2 = x^3 - 28x^2 + 21x. \tag{39}$$

Supposons que $\zeta = 7 \pmod{43}$. Alors, on a que $\overline{b}'$ est racine du polynôme

$$\begin{aligned} P_{1,7}(X) &= X^4 + 16X^3 - X^2 - 4X + 21 \\ &= (X+23)(X+28)(X^2+8X+22) \in \mathbb{F}_{43}[X]. \end{aligned}$$

D'où $\overline{b}' = 20 \pmod{43}$ ou $15 \pmod{43}$ et

$$(\overline{a}', \overline{b}') = (15 \pmod{43}, 20 \pmod{43})$$

ou

$$(\overline{a}', \overline{b}') = (20 \pmod{43}, 15 \pmod{43}).$$

La courbe de Frey réduite modulo 43 est alors isomorphe sur $\mathbb{F}_{43}$ à la courbe $F_{1,7}$ d'équation (cf. (28) et (29))

$$y^2 = x^3 + 14x^2 + 3x. \tag{40}$$

Il en résulte que (39) et (40) sont les deux seules équations possibles pour la réduite de la courbe de Frey modulo 43. En particulier, on a $a_q(E) = a'_q(6) = -8$ ou $a_q(E) = a_q(7) = 10$ (cf (3) et (31)). D'après l'égalité (38) ci-dessus et la congruence (16), on a donc :

$$4 \equiv -8 \pmod{7} \quad \text{ou} \quad 4 \equiv 10 \pmod{7}.$$

On en déduit une contradiction. Les représentations ρ_7^E et ρ_7^A où $A = 1200\text{J}1$ ne sont donc pas isomorphes.

On procède de même pour éliminer les isomorphismes entre ρ_7^E et ρ_7^A où $A = 600\text{C}1, 1200\text{B}1$ et $1200\text{I}1$. On explicite donc certains calculs sans répéter exhaustivement les raisonnements.

Supposons que ρ_7^E soit isomorphe à ρ_7^A où A est la courbe 1200B1 ou la courbe 1200I1. Posons $n = 10$ et $q = 71$. On a

$$a_{71}(1200\text{B}1) = a_{71}(1200\text{I}1) = 4.$$

Donc, d'après le lemme 4.4, la courbe E a bonne réduction en q. On vérifie qu'il y a quatre équations possibles pour la réduite de E modulo 71. Il s'agit des

courbes suivantes (cf. (5) et (36) et les équations (34) et (35)) :

$$\begin{aligned} F'_{2,5} : y^2 &= x^3 - 24x^2 + 25x \quad \text{et } b'_{71}(5) = 0, \\ F_{2,5} : y^2 &= x^3 + 24x^2 + 25x \quad \text{et } b_{71}(5) = 0, \\ F'_{2,57} : y^2 &= x^3 - 14x^2 + x \quad \text{et } b'_{71}(57) = -8, \\ F'_{2,70} : y^2 &= x^3 - 32x^2 + 66x \quad \text{et } b'_{71}(70) = -4. \end{aligned}$$

Par ailleurs, on a les congruences

$$a_{71}(E) \equiv b'_{71}(5),\ b_{71}(5),\ b'_{71}(57) \text{ ou } b'_{71}(70) \pmod 7.$$

D'où il résulte

$$4 \equiv 0,\ 3 \text{ ou } 6 \pmod 7.$$

On en déduit une contradiction : les représentations ρ_7^E et ρ_7^A où $A = 1200\text{B}1$ ou 1200I1 ne sont pas isomorphes.

De même, les représentations ρ_7^E et ρ_7^A, où A est la courbe 600C1, ne sont pas isomorphes. D'après le lemme 4.4, la courbe E a bonne réduction en $q = 197$ car $a_{197}(600\text{C}1) = 6$. Comme par ailleurs 5 ne divise pas $a + b$, on a onze équations possibles pour la courbe E réduite modulo 197 (cf. équations (34) et (35)). De plus,

$$\begin{array}{llll} b_{197}(104) = 4, & b'_{197}(113) = 14, & b_{197}(113) = 14, & b'_{197}(120) = 10, \\ b_{197}(120) = 10, & b'_{197}(178) = -12, & b_{197}(196) = 8, & b'_{197}(77) = -18, \\ b_{197}(77) = -18, & b'_{197}(87) = 2, & b'_{197}(87) = 2. & \end{array}$$

On conclut comme ci-dessus que les représentations ρ_7^E et ρ_7^A, où $A = 600\text{C}1$ ne sont pas isomorphes.

En revanche, pour la courbe $A = 600\text{H}1$ il n'existe aucun entier n tel que $6 < n < 1000$ pour lequel la méthode ci-dessus s'applique. Elle s'applique cependant avec $n = 6$, pourvu que l'on sache montrer que E a bonne réduction en $q = 43$, ce que le lemme 4.3 ne nous permet pas d'affirmer car

$$a_{43}(600\text{H}1) = -12 \equiv 2 \pmod 7.$$

Pour montrer que E a bonne réduction en 43, on utilise alors le résultat suivant.

Lemme 4.5 *Soient q un nombre premier et A une courbe elliptique sur $\mathbb{Q}$ ayant bonne réduction en q. Supposons que ρ_7^E soit isomorphe à ρ_7^A et que q vérifie les deux conditions suivantes :*

1. *on a $q \equiv 1 \pmod 7$ et $q \not\equiv 1 \pmod 5$.*
2. *On a*
$$a_q(A) \not\equiv 2\left(\frac{5}{q}\right) \pmod 7,$$
où $\left(\frac{5}{q}\right)$ est le symbole de Legendre.

Alors, E a bonne réduction en q.

DÉMONSTRATION : Supposons que E ait mauvaise réduction en q. Puisque l'on a $q \neq 2, 5$, la courbe E a réduction de type multiplicatif en q (lemme 2.7). On a donc :

$$a_q(E) = \left(\frac{-c_6}{q}\right).$$

L'hypothèse $q \not\equiv 1 \pmod 5$ entraîne que q divise $a + b$ (lemme 2.6). Par suite, on a :

$$-c_6 = 2^6 \cdot 5^3 a^6 \pmod q,$$

d'où l'on déduit que l'on a

$$\left(\frac{-c_6}{q}\right) = \left(\frac{5}{q}\right).$$

Les représentations ρ_7^E et ρ_7^A étant isomorphes et A ayant bonne réduction en q, on a ([14, prop.3(iii)]) :

$$a_q(E)a_q(A) \equiv q + 1 \pmod 7,$$

et compte tenu de la congruence $q \equiv 1 \pmod 7$, on obtient

$$a_q(E)a_q(A) \equiv 2 \pmod 7.$$

On a donc

$$a_q(A) \equiv 2\left(\frac{5}{q}\right) \pmod 7,$$

ce qui contredit la condition 2. D'où le lemme.

Déduisons-en que ρ_7^E et ρ_7^A, pour $A = 600\text{H}1$, ne sont pas isomorphes. Supposons le contraire. La courbe E a bonne réduction en $q = 43$. En effet, on a

$$a_{43}(A) = -12 \equiv 2 \pmod 7. \tag{41}$$

Puisque $\left(\frac{5}{43}\right) = -1$, on a

$$2 \equiv a_{43}(A) \not\equiv 2\left(\frac{5}{43}\right) \pmod 7,$$

d'où l'assertion d'après le lemme 4.5.

Par ailleurs, avec les notations de la partie 1, on a $B(6, 43) = \{42 \pmod{43}\}$ et l'on vérifie que l'on a une seule courbe possible pour la réduction de E modulo 43. Elle a pour équation (cf. (35)) :

$$F'_{2,42} : y^2 = x^3 - 16x^2 + 38x.$$

On en déduit avec les formules (16), (36) et (41) que l'on a

$$2 \equiv a_{43}(A) \equiv b'_{43}(42) \equiv -1 \pmod 7.$$

On obtient ainsi une contradiction et le fait que ρ_7^E et ρ_7^A, pour $A = 600\text{H}1$, ne sont pas isomorphes.

Remarque. La même démonstration (appliquée à nouveau à $q = 43$) permettrait de redémontrer que les représentations ρ_7^E et ρ_7^A où $A = 1200\text{I}1$ ne sont pas isomorphes.

On a donc montré que $S_7(3)$ est vide.

L'équation $x^5 + y^5 = 3z^p$, pour $p \geq 11$. Pour $p \geq 11$, on utilise le critère énoncé dans le théorème 1.4 et le programme `Fermat` disponible à l'adresse `www.math.jussieu.fr/~billerey`.

Pour tout nombre premier p tel que $11 \leq p \leq 10^6$, et pour toute courbe elliptique F des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$, on trouve un entier $n \geq 2$ tel que le couple (F, n) vérifie la condition 1 du théorème 1.4 si F appartient à $\mathcal{E}_1$ et la condition 2 si F appartient à $\mathcal{E}_2$.

On obtient ainsi la proposition 1.5.

Remarque. On a indiqué dans le tableau 1 de l'Appendice A, les premières valeurs d' entiers n trouvés pour chaque courbe elliptique de $\mathcal{E}_\infty$ et $\mathcal{E}_\in$.

Appendices

A—Tableau de valeurs

On a vu au §4.4 que si $q = np+1$ est un nombre premier congru à 1 modulo p et si E a bonne réduction en q, on est dans l'un des cas suivants (cf. (32) et (37)) :

1. il existe un élément $\zeta \in A(n, q)$ tel que
$$a_q(E) \equiv \pm a_q(\zeta) \pmod{p}.$$
2. Il existe un élément $\zeta \in B(n, q)$ tel que
$$a_q(E) \equiv \pm b_q(\zeta) \pmod{p}.$$

Il en résulte qu'il existe au plus $4n$ valeurs possibles pour la classe de $a_q(E)$ modulo p car les ensembles $A(n, q)$ et $B(n, q)$ sont de cardinal $\leq n$. Plus p est grand et n petit et plus la *probabilité* (en un sens heuristique) qu'une congruence de la forme
$$a_q(E)^2 \equiv a_q(F)^2 \pmod{p},$$
où F est l'une des courbes elliptiques des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$, soit réalisée, est faible.

Cela porte à croire que, pour une courbe F des ensembles $\mathcal{E}_1$ ou $\mathcal{E}_2$ donnée, l'existence d'un entier n satisfaisant aux conditions du théorème 1.4 est d'autant plus probable que p est grand. De plus, on constate que pour les petites valeurs de

p, on est souvent obligé de choisir une valeur de n pour chaque courbe elliptique, ce qui est « rarement » nécessaire lorsque p est grand (disons $p > 10000$).

Dans le tableau 1, on a on a indiqué dans la première colonne la liste des nombres premiers p compris entre 11 et 150. Les courbes elliptiques inscrites sur la première ligne sont celles des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$. Pour un nombre premier p et une courbe elliptique F comme ci-dessus, on lit dans la case correspondante un entier n tel que le couple (F, n) vérifie la condition 1 du théorème 1.4 si F appartient à $\mathcal{E}_1$ et la condition 2 si F appartient à $\mathcal{E}_2$.

Ces valeurs ont été obtenues à l'aide du programme `Fermat` disponible à l'adresse `www.math.jussieu.fr/~billerey`.

	150C1	600A1	600F1	1200J1	150A1	600C1	1200N1
11	2	2	2	2	2	2	2
13	4	4	4	4	6	4	4
17	6	6	6	6	14	8	14
19	10	24	24	10	22	22	12
23	2	2	2	2	2	2	2
29	2	2	2	2	2	2	2
31	10	10	22	22	10	10	42
37	4	4	4	4	4	4	6
41	2	2	2	2	2	2	2
43	4	4	4	4	10	4	4
47	6	6	6	6	6	6	6
53	2	2	2	2	2	2	2
59	12	18	18	12	12	18	12
61	12	6	12	6	12	6	6
67	4	4	4	4	4	4	4
71	8	8	8	8	8	8	8
73	4	4	6	4	4	4	6
79	4	4	18	18	18	4	4
83	2	2	2	2	2	2	2
97	4	4	4	4	4	4	4
101	8	6	6	6	8	36	6
103	6	12	10	12	10	10	6
107	6	6	6	6	6	6	6
109	30	10	10	10	10	10	10
113	14	2	14	2	2	2	2
127	4	18	4	4	4	4	4
131	2	2	8	2	2	2	2
137	6	6	6	6	6	6	6
139	4	4	4	4	4	4	4
149	8	8	8	8	8	8	8

TAB. 1 – Tableau des premières valeurs d'entiers n vérifiant les conditions du théorème 1.4.

B—Courbes de conducteur 150, 600 et 1200

Les notations du tableau 2 sont celles des tables de [3]. Pour un représentant F de chaque classe d'isogénie de courbes de conducteur 150, 600 ou 1200, on donne successivement :

- un quintuplet $[a_1, a_2, a_3, a_4, a_6]$ tel que

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

  soit une équation minimale de Weierstrass de F,
- l'invariant modulaire j_F de F,
- la valuation en 5, $v_5(j_F)$, de l'invariant modulaire j_F de F,
- la valuation en 5, $v_5(\Delta_m(F))$, du discriminant minimal de F,
- l'indice de ramification e en 5 de l'extension $\mathbb{Q}(F[p])/\mathbb{Q}$ engendrée par les coordonnées des points de p-torsion de la courbe F. Si $v_5(j_F) \geq 0$, c'est le dénominateur de $v_5(\Delta_m(F))/12$ et si $v_5(j_F) < 0$, compte tenu du fait que p ne divise pas $v_5(j_F)$, on a $e = 2p$ (cf. [2]).

courbe	équation	j_F	$v_5(j_F)$	$v_5(\Delta_m(F))$	e
150A1	$[1,0,0,-3,-3]$	$-24389/12$	0	3	4
150B1	$[1,1,0,-75,-375]$	$-24389/12$	0	9	4
150C1	$[1,1,1,37,281]$	$357911/2160$	-1	7	$2p$
600A1	$[0,-1,0,-383,3012]$	$24918016/45$	-1	7	$2p$
600B1	$[0,-1,0,7,-3]$	$5120/3$	1	2	6
600C1	$[0,-1,0,32,-68]$	$27436/27$	0	3	4
600D1	$[0,1,0,17,38]$	$2048/3$	0	6	2
600E1	$[0,1,0,-233,1563]$	$-8780800/2187$	2	4	3
600F1	$[0,-1,0,92,-188]$	$21296/15$	-1	7	$2p$
600G1	$[0,-1,0,-5833,207037]$	$-8780800/2187$	2	10	6
600H1	$[0,1,0,792,-6912]$	$27436/27$	0	9	4
600I1	$[0,1,0,167,-37]$	$5120/3$	1	8	3
1200A1	$[0,-1,0,17,-38]$	$2048/3$	0	6	2
1200B1	$[0,-1,0,792,6912]$	$27436/27$	0	9	4
1200C1	$[0,-1,0,167,37]$	$5120/3$	1	8	3
1200D1	$[0,-1,0,-233,-1563]$	$-8780800/2187$	2	4	3
1200E1	$[0,1,0,-383,-3012]$	$24918016/45$	-1	7	$2p$
1200F1	$[0,1,0,7,3]$	$5120/3$	1	2	6
1200G1	$[0,1,0,92,188]$	$21296/15$	-1	7	$2p$
1200H1	$[0,1,0,-5833,-207037]$	$-8780800/2187$	2	10	6
1200I1	$[0,1,0,32,68]$	$27436/27$	0	3	4
1200J1	$[0,-1,0,-8,-1488]$	$-1/15$	-1	7	$2p$
1200K1	$[0,-1,0,27,-243]$	$20480/243$	1	2	6
1200L1	$[0,-1,0,-333,3537]$	$-40960/27$	1	8	3
1200M1	$[0,-1,0,-48,192]$	$-24389/12$	0	3	4
1200N1	$[0,-1,0,-333,-2088]$	$131072/9$	0	9	4
1200O1	$[0,1,0,-13,23]$	$-40960/27$	1	2	6
1200P1	$[0,1,0,592,-16812]$	$357911/2160$	-1	7	$2p$
1200Q1	$[0,1,0,-1208,21588]$	$-24389/12$	0	9	4
1200R1	$[0,1,0,-133,563]$	$-102400/3$	2	4	3
1200S1	$[0,1,0,-13,-22]$	$131072/9$	0	3	4

TAB. 2 – Classes d'isogénie des courbes elliptiques de conducteur 150, 600 et 1200

Références

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

[2] É. Cali et A. Kraus. Sur la p-différente du corps des points de ℓ-torsion des courbes elliptiques, $\ell \neq p$. *Acta Arith.*, 104 :1–21, 2002.

[3] J. E. Cremona. *Algorithms for modular elliptic curves.* Disponible à

l'adresse suivante :
http ://www.ma.utexas.edu/users/tornaria/cnt/cremona.html.

[4] H. Darmon. Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation. *C. R. Math. Rep. Acad. Sci. Canada*, 19(1) :3–14, 1997.

[5] H. Darmon et A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27 :513–544, 1995.

[6] L. Dirichlet. Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré. *J. reine angew. Math.*, 3 :354–375, 1828.

[7] G. Frey. Links between stable elliptic curves and certain diophantine equations. *Ann. Univ. Sarav. Ser. Math.*, 1 :1–40, 1986.

[8] E. Halberstadt et A. Kraus. Courbes de Fermat : résultats et problèmes. *J. reine angew. Math.*, 548 :167–234, 2002.

[9] M. A. Kenku. On the Number of $\mathbf{Q}$-isomorphism Classes of Elliptic Curves in Each $\mathbf{Q}$-Isogeny Class. *J. Number Theory*, 15(2) :199–202, 1982.

[10] A. Kraus. Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique. *Acta Arith.*, 54 :75–80, 1989.

[11] A. Kraus. Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique. *Dissertationes Math.*, 364, 1997.

[12] A. Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7(1) :1–13, 1998.

[13] A. Kraus. Une question sur les équations $x^m - y^m = Rz^n$. *Compositio Math.*, 132 :1–26, 2002.

[14] A. Kraus et J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293 :259–275, 1992.

[15] G. Ligozat. *Courbes modulaires de genre* 1. Société Mathématique de France, 1975. Bull. Soc. Math. France, Mém. 43.

[16] I. Papadopoulos. Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3. *J. Number Theory*, 44(2) :119–152, 1993.

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

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

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

[20] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, 1992.

[21] 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 :33–52, 1975.

[22] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. of Math.*, 141(3) :443–551, 1995.

Paris, le 18/07/2006.