Canad. J. Math. Vol. **58** (1), 2006 pp. 115–153

Quelques résultats sur les équations $ax^p + by^p = cz^2$

W. Ivorra et A. Kraus

Abstract. Let p be a prime number ≥ 5 and a, b, c be non zero natural numbers. Using the works of K. Ribet and A. Wiles on the modular representations, we get new results about the description of the primitive solutions of the diophantine equation $ax^p + by^p = cz^2$, in case the product of the prime divisors of abc divides 2ℓ, with ℓ an odd prime number. For instance, under some conditions on a, b, c, we provide a constant $f(a, b, c)$ such that there are no such solutions if $p > f(a, b, c)$. In application, we obtain information concerning the $\mathbb{Q}$-rational points of hyperelliptic curves given by the equation $y^2 = x^p + d$ with $d \in \mathbb{Z}$.

Introduction

Soient p un nombre premier supérieur ou égal à 5 et a, b, c trois entiers naturels non nuls premiers entre eux deux à deux. On s'intéresse dans ce travail à l'étude de l'équation diophantienne

$$ax^p + by^p = cz^2. \tag{1}$$

Nous dirons qu'une solution $(x, y, z) \in \mathbb{Z}^3$ de l'équation (1) est propre si l'on a l'égalité $\mathrm{pgcd}(x, y, z) = 1$ et qu'elle est non triviale si xyz est non nul. On désigne par $S_p(a, b, c)$ l'ensemble des solutions propres non triviales de l'équation (1). H. Darmon et A. Granville ont démontré vers 1993, en utilisant le théorème de Faltings sur la finitude de l'ensemble des points rationnels des courbes de genre au moins deux, que $S_p(a, b, c)$ est fini (*cf.* [11]). Notre objectif principal est de décrire $S_p(a, b, c)$ dans certains cas particuliers, à travers les deux conjectures ci-dessous et le problème énoncé plus loin. Nous donnerons par ailleurs, en application des résultats obtenus, des informations concernant la recherche des points rationnels sur $\mathbb{Q}$ des courbes hyperelliptiques de la forme $y^2 = x^p + d$, où d est un entier.

Conjecture 1 *Supposons que les trois entiers $a + b$, $a - b$ et $b - a$ n'appartiennent pas à $c\mathbb{Z}^2$. Alors, il existe une constante $f(a, b, c)$ telle que l'on ait l'implication :*

$$p > f(a, b, c) \Longrightarrow S_p(a, b, c) \text{ est vide.}$$

Conjecture 2 *Supposons que l'un des entiers $a + b$, $a - b$ et $b - a$ appartienne à $c\mathbb{Z}^2$. Alors, il existe une constante $g(a, b, c)$ telle que, pour tout $p > g(a, b, c)$, l'on ait l'implication :*

$$(x, y, z) \in S_p(a, b, c) \Longrightarrow xy = \pm 1.$$

Reçu par la rédaction le novembre 11, 2003; revu le decembre 24, 2004.
Classification (AMS) par sujet: 11G.

Ces conjectures sont des conséquences de la conjecture (*abc*), avec la conclusion souhaitée si l'on a $p > \alpha + \beta \log(abc)$, où α et β sont deux constantes absolues > 0. L'étude de la conjecture 2 est en fait plus difficile que celle de la conjecture 1. La raison en est que si $a - b$, $a + b$ ou $b - a$ est dans $c\mathbb{Z}^2$, et si $ab \neq 1$, il existe un point «évident» $(x, y, z) \in S_p(a, b, c)$ tel que $xy = \pm 1$.

La méthode, aujourd'hui classique, que nous utiliserons pour aborder ces conjectures est la méthode modulaire, qui repose sur les travaux de G. Frey, K. Ribet, J.-P. Serre et A. Wiles sur les représentations modulaires (*cf.* [13, 35, 37, 43]). Sans rentrer ici dans les détails, elle consiste à associer à tout élément de $S_p(a, b, c)$ une courbe elliptique sur $\mathbb{Q}$, appelée parfois courbe de Hellegouarch–Frey ou courbe de Frey, et à exploiter les propriétés galoisiennes de ses points de p-torsion. Signalons que, dans notre contexte, on peut associer à chaque élément de $S_p(a, b, c)$ deux courbes elliptiques définies sur $\mathbb{Q}$, qui ne sont pas isogènes en général, et qui permettent chacune la mise en œuvre de la méthode. Nous rappellerons son principe et certains de ses compléments au §4. Afin d'optimiser nos résultats, nous avons utilisé simultanément ces deux courbes dans les démonstrations (*cf.* l'alinéa 2 des remarques 3). Cette approche permet par ailleurs de relier les conjectures 1 et 2 à d'autres plus centrales en théorie des nombres. Par exemple, elles se déduisent de la conjecture suivante concernant la comparaison galoisienne des points de torsion des courbes elliptiques (*cf.* [10] et le §4) :

Conjecture 3 *Soient E une courbe elliptique définie sur $\mathbb{Q}$ et A_E l'ensemble des nombres premiers p possédant la propriété suivante : il existe une courbe elliptique sur $\mathbb{Q}$, non isogène à E sur $\mathbb{Q}$, dont le module galoisien des points de p-torsion soit isomorphe à celui de E. Alors, l'ensemble A_E est fini.*

On ne connait aucune courbe elliptique $E/\mathbb{Q}$ pour laquelle la conjecture 3 soit démontrée. Signalons que les seuls résultats partiels déjà prouvés à ce sujet concernent le cas où E a des multiplications complexes.

Dans toute la suite nous nous préoccuperons de la situation où le produit des diviseurs premiers de *abc* divise 2ℓ, où ℓ est un nombre premier impair. Précisons maintenant le contenu de ce travail.

Sur la conjecture 1

Le premier résultat la concernant est dû à H. Darmon qui, en 1993, a démontré que $S_p(1, 4, 1)$ est vide si $p \geq 17$ (*cf.* [9, prop. 2.5]). Il se trouve dans [23] un résumé du fait que si ℓ est un nombre premier congru à 3 modulo 8, autre que 3, l'ensemble $S_p(1, \ell, 1)$ est vide si p est assez grand en fonction de ℓ ; ce résultat n'a pas été rédigé par la suite. M. Bennett et C. Skinner en 2002 ont prouvé la conjecture 1 pour certains triplets d'entiers (a, b, c), pour lesquels *abc* est de la forme $2^\alpha \ell_1^\beta \ell_2^\gamma$, où ℓ_1 et ℓ_2 sont des nombres premiers inférieurs à 80 (*cf.* [3]). Par ailleurs, on peut trouver dans [17] des résultats sur les ensembles $S_p(a, b, c)$ si *abc* est une puissance de 2. Ils ont été obtenus indépendamment par Bennett et Skinner dans [3]. Par exemple, la conjecture 1 est vraie si *ab* est une puissance de 2 et $c = 1$. Ce sont à notre connaissance les seuls travaux déjà publiés sur cette conjecture.

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

On considère ici un nombre premier impair ℓ. En utilisant les résultats démontrés dans [18], on prouve ici la conjecture 1, de façon effective, dans certains cas particuliers où le produit des diviseurs premiers de abc divise 2ℓ (théorèmes 1.1 et 1.2).

À titre indicatif, considérons un entier $m \geq 1$. Explicitons l'énoncé de la conjecture 1 pour les triplets de la forme $(1, \ell^m, 1)$: si $\ell^m + 1 \in \mathbb{Z}^2$ on vérifie que $m = 1$ et $\ell = 3$, et si $\ell^m - 1 \in \mathbb{Z}^2$ on a $m = 1$ (*cf.* [18, Lemme 3]). Par suite, si la condition suivante est satisfaite :

$$(m = 1,\ \ell \neq 3 \text{ et } \ell - 1 \text{ n'est pas un carré}) \quad \text{ou bien} \quad m \geq 2,$$

la conjecture 1 affirme que $S_p(1, \ell^m, 1)$ est vide si p est assez grand en fonction de ℓ et m. Comme cas particulier du théorème 1.1, on obtient l'énoncé ci-dessous dans lequel on pose

$$f(\ell) = \begin{cases} 18 + 2\dfrac{\log \ell}{\log 2} & \text{si } \ell < 2^{96}, \\ 435 + 10\dfrac{\log \ell}{\log 2} & \text{si } \ell \geq 2^{96}. \end{cases}$$

Théorème *Supposons que l'une des quatre conditions suivantes soit réalisée :*

(1) *on a* $\ell \equiv 1 \bmod 8$ *et les deux assertions suivantes sont satisfaites :*
   (i) *les entiers* $\ell - 1$, $\ell - 8$ *et* $\ell + 8$ *ne sont pas des carrés ;*
   (ii) *pour tout* k *tel que* $7 \leq k < f(\ell)$, *les entiers* $\ell - 2^k$ *et* $\ell + 2^k$ *ne sont pas des carrés.*

(2) *On a* $\ell \equiv 3 \bmod 8$ *et* $\ell \neq 3$.

(3) *On a* $\ell \equiv 5 \bmod 8$ *et* $\ell - 1$ *n'est pas un carré.*

(4) *On a* $\ell \equiv 7 \bmod 8$ *et pour tout* k *tel que* $7 \leq k < f(\ell)$, *l'entier* $2^k - \ell$ *n'est pas un carré.*

Alors, pour tout nombre premier p *tel que*

$$p > m \quad et \quad p > \left(\sqrt{8(\ell+1)} + 1\right)^{2(\ell-1)}, \tag{2}$$

l'ensemble $S_p(1, \ell^m, 1)$ *est vide.*

Si l'une des conditions précédentes est satisfaite par ℓ, la conjecture 1 est ainsi démontrée pour $(1, \ell^m, 1)$. En particulier, si l'on a $\ell \equiv 3$ ou $5 \bmod 8$, la conjecture 1 est vraie pour le triplet $(1, \ell, 1)$. Dans les cas où l'on a $m \geq 2$ ou bien si ℓ est congru à 1 ou 7 modulo 8, on obtient des conditions qui sont conjecturalement superflues pour assurer la conclusion du théorème. Néanmoins, elles s'avèrent assez efficaces en pratique (*cf.* remarques 1).

Pour tout entier $n \geq 0$, on obtient plus généralement dans le théorème 1.1 des conditions portant sur ℓ qui entraînent que $S_p(2^n, \ell^m, 1)$ et $S_p(2^n\ell^m, 1, 1)$ sont vides si p est assez grand. On dispose aussi d'un énoncé analogue concernant les ensembles $S_p(1, \ell^m, 2)$ (théorème 1.2). Par exemple, $S_p(1, \ell^m, 2)$ est vide si l'on a $\ell \equiv 5 \bmod 8$ et si p est assez grand.

Pour certains triplets (a, b, c) pour lesquels on ne sait pas démontrer la conjecture 1, on apporte dans le théorème 1.3 une réponse partielle en démontrant l'existence d'un ensemble $\mathcal{P}$ de nombres premiers p de densité > 0 (dépendant de a, b, c),

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

tels que $S_p(a,b,c)$ soit vide. On utilise pour cela un complément de la méthode modulaire, appelé méthode symplectique dans [15] (*cf.* §4.2). Tel est, par exemple, le cas des triplets $(1,\ell^m,1)$ si $\ell \equiv 7 \bmod 8$, $\ell \neq 7$ et si m est impair. Lorsque ℓ n'est pas trop grand, on peut expliciter un tel ensemble $\mathcal{P}$. On pourra trouver au §7 des exemples illustrant cette situation, notamment si $\ell = 23$ (la condition 4 du théorème n'est pas vérifiée si $\ell = 23$: on a $2^{11} - 23 = 45^2$).

Sur la conjecture 2

Comme on le signalait au début, son étude s'avère plus difficile que celle de la conjecture 1. Si (a,b,c) est un triplet d'entiers vérifiant les hypothèses de la conjecture 2, il existe un point (x,y,z) satisfaisant l'équation (1) tel que $xy = \pm 1$. Ce point est dans $S_p(a,b,c)$ si z est non nul. Comme il est expliqué dans le §2, on peut lui associer deux courbes elliptiques définies sur $\mathbb{Q}$ (y compris si $z = 0$, mais on ne se placera pas dans cette situation). Dans chacun des cas où la conjecture 2 a été démontrée, ces courbes possèdent des multiplications complexes. On ne dispose d'aucun exemple dans le cas contraire, notamment s'il existe un nombre premier impair qui divise ab. Nous n'aborderons pas cette situation.

Les travaux déjà publiés sur la conjecture 2 sont les suivants :

(1) En 1997, H. Darmon et L. Merel l'ont prouvée si $a = b = c = 1$ (*cf.* [12]). Ils ont démontré que $S_p(1,1,1)$ est vide si $p \geq 7$. Il en est de mÃłme si $p = 5$ (*cf.* [34]).
(2) On peut trouver dans [17] une démonstration du fait que, pour tout $p \geq 7$, l'on a $S_p(1,1,2) = \{(1,1,-1),(1,1,1)\}$ et $S_p(8,1,1) = \{(1,1,3),(1,1,-3)\}$.
(3) M. Bennett et C. Skinner dans [3] ont aussi traité les cas où $a = b = 1$ et $c \in \{2,3,5,6,10,11,13,17\}$, en montrant que $S_p(1,1,c)$ est vide si $p \geq 7$ ne divise pas c (*cf.* [3, Th. 1.1])(le cas où p divise c semble avoir été omis).

On fournit au §6 une preuve du fait que l'on a

$$S_p(4,1,3) = \{(1,-1,1),(1,-1,-1)\} \quad \text{si } p \geq 7.$$

Une démonstration analogue permet de prouver que

$$S_p(64,1,7) = \{(1,-1,3),(1,-1,-3)\} \quad \text{si } p \geq 11.$$

Ces égalités se démontrent en utilisant, entre autres, des propriétés arithmétiques des courbes elliptiques sur $\mathbb{Q}$ à multiplications complexes (*cf.* [32, 12] ; voir aussi [14]). Nous ne savons pas décrire l'ensemble $S_7(64,1,7)$; il semble que les arguments utilisés dans ce travail ne permettent pas de conclure (*cf.* la proposition 3.1 et le §4).

Sur les ensembles $S_p(a,b,c)$ avec (p,a,b,c) fixé

Considérons un triplet d'entiers naturels non nuls (a,b,c) et un nombre premier $p \geq 5$ fixés. On s'intéressera au problème suivant :

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Problème Comment démontrer que $S_p(a, b, c)$ est vide, si tel est le cas ?

Un nombre premier $p \geq 7$ étant donné, signalons qu'un cas particulier de l'étude faite dans [26] est celui de la description des ensembles $S_p(1, 1, c)$ pour les entiers $c \geq 3$ sans facteurs carrés vérifiant la condition suivante :

$$\text{pour tout diviseur premier } \ell \text{ de } c, \text{ on a } \ell \not\equiv 1 \bmod p.$$

On démontre dans [26], en utilisant les résultats de [11], que l'ensemble des entiers $c \geq 3$ sans facteurs carrés vérifiant cette condition, pour lesquels $S_p(1, 1, c)$ est non vide, est fini. En fait, on démontre dans [19] qu'il n'existe pas de tels entiers c si $p \in \{7, 11, 13, 17\}$; ce dernier résultat a été obtenu par la méthode dite de Chabauty elliptique.

Pour aborder ce problème, outre la méthode modulaire classique, on utilisera ici la méthode symplectique et un autre de ses compléments appelé méthode de réduction dans [15]. La méthode de réduction a aussi été utilisée pour la résolution de certaines équations ternaires dans [25]. On rappelera au §4.1 son principe dans le cadre considéré ici. On l'illustrera à travers des exemples numériques au §7. Elle permet par exemple de démontrer que $S_p(1, 7, 1)$ est vide si l'on a $11 \leq p < 10^4$. De mÃłme, $S_{11}(1, 11^m, 1)$ est vide pour tout $m \leq 10$.

Sur les points rationnels des courbes $y^2 = x^p + d\,(d \in \mathbb{Z})$

Soient p un nombre premier ≥ 5 et d un entier sans puissances p-ièmes. En application des résultats obtenus dans ce travail, on peut parfois déterminer les points rationnels sur $\mathbb{Q}$ de la courbe hyperelliptique, de genre $\frac{p-1}{2}$, d'équation

$$C_{d,p} : y^2 = x^p + d.$$

En fait, si $S_p(1, |d|, 1)$ est vide, alors si $(x, y) \in C_{d,p}(\mathbb{Q})$, on a $xy = 0$ (lemme 8.1). Il résulte par exemple du théorème énoncé précédemment que pour tout nombre premier ℓ, si l'on a :

$$(\ell \equiv 3 \bmod 8, \ell \neq 3) \quad \text{ou bien} \quad (\ell \equiv 5 \bmod 8 \text{ et } \ell - 1 \text{ n'est pas un carré}),$$

les ensembles $C_{\ell,p}(\mathbb{Q})$ et $C_{-\ell,p}(\mathbb{Q})$ sont vides dès que p est plus grand qu'une constante dépendant de ℓ. À titre indicatif, si $\ell = 11$ tel est le cas pour tout $p \geq 7$. On abordera une discussion, utilisant la méthode de réduction, concernant l'ensemble $C_{-3,p}(\mathbb{Q})$.

1 Énoncé des résultats sur la conjecture 1

Considérons un nombre premier impair ℓ fixé. Rappelons que l'on note

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

$$f(\ell) = \begin{cases} 18 + 2\dfrac{\log \ell}{\log 2} & \text{si } \ell < 2^{96}, \\ 435 + 10\dfrac{\log \ell}{\log 2} & \text{si } \ell \geq 2^{96}. \end{cases}$$

Introduisons la terminologie suivante :

(1) Nous dirons que ℓ vérifie la propriété (A) si les deux conditions suivantes sont réalisées :
   (i) on a $\ell \equiv 1 \bmod 8$;
   (ii) pour tout k tel que $7 \leq k < f(\ell)$, les entiers $\ell - 2^k$ et $\ell + 2^k$ ne sont pas des carrés.

(2) Nous dirons que ℓ vérifie la propriété (B) si les deux conditions suivantes sont réalisées :
   (i) on a $\ell \equiv 7 \bmod 8$;
   (ii) pour tout k tel que $7 \leq k < f(\ell)$, l'entier $2^k - \ell$ n'est pas un carré.

(3) Nous dirons que ℓ vérifie la propriété (C) si les deux conditions suivantes sont réalisées :
   (i) on a $\ell \equiv 7 \bmod 8$;
   (ii) pour tout entier impair k tel que $1 \leq k \leq 164969$, l'entier $\ell^k + 2$ n'est pas un carré.

Étant donnés deux entiers $m \geq 1$ et $n \geq 0$, le résultat qui suit fournit des conditions suffisantes, portant sur le couple (ℓ, n), pour que les ensembles $S_p(2^n, \ell^m, 1)$ et $S_p(2^n\ell^m, 1, 1)$ soient vides si p est assez grand en fonction de ℓ, m et n.

Théorème 1.1 *Soit n un entier naturel. Supposons que le couple (ℓ, n) vérifie l'une des quatre conditions suivantes :*

(1) *ℓ vérifie la propriété* (A) *et l'une des assertions suivantes est satisfaite :*
   (i) *on a $n \geq 7$;*
   (ii) *on a $n = 6$ et $\ell - 64$ n'est pas un carré ;*
   (iii) *on a $n \in \{4, 5\}$ et les entiers $\ell - 16$, $\ell - 32$ et $\ell + 32$ ne sont pas des carrés ;*
   (iv) *on a $n \in \{0, 3\}$ et les entiers $\ell - 1$, $\ell - 8$ et $\ell + 8$ ne sont pas des carrés ;*
   (v) *on a $n = 2$ et pour tout $k \in \{4, 5, 6\}$, $\ell - 2^k$ et $\ell + 2^k$ ne sont pas des carrés ;*
   (vi) *on a $n = 1$ et les entiers $2\ell - 1$ et $2\ell^2 - 1$ ne sont pas des carrés.*

(2) *On a $\ell \equiv 3 \bmod 8$ et l'une des assertions suivantes est satisfaite :*
   (i) *on a $n \geq 6$;*
   (ii) *on a $n \in \{0, 2, 3, 4, 5\}$ et $\ell \neq 3$;*
   (iii) *on a $n = 1$ et $\ell - 2$ n'est pas un carré.*

(3) *On a $\ell \equiv 5 \bmod 8$ et l'une des assertions suivantes est satisfaite :*
   (i) *on a $n \geq 6$;*
   (ii) *on a $n \in \{4, 5\}$ et $\ell \neq 5$;*
   (iii) *on a $n \in \{0, 3\}$ et $\ell - 1$ n'est pas un carré ;*
   (iv) *on a $n = 2$ et $\ell - 4$ n'est pas un carré ;*
   (v) *on a $n = 1$ et les entiers $2\ell - 1$ et $2\ell^2 - 1$ ne sont pas des carrés.*

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

(4) ℓ *vérifie la propriété* (B) *et l'une des assertions suivantes est satisfaite :*
   (i) *on a* $n \neq 1$ *;*
   (ii) *on a* $n = 1$ *et* ℓ *vérifie la propriété* (C).

Alors, pour tout entier $m \geq 1$ *et tout nombre premier* p *tels que*

$$p > \mathrm{Max}(m, n+6) \quad et \quad p > \left(\sqrt{32(\ell+1)} + 1\right)^{8(\ell-1)}, \tag{3}$$

les ensembles $S_p(2^n, \ell^m, 1)$ *et* $S_p(2^n\ell^m, 1, 1)$ *sont vides.*

En ce qui concerne les ensembles $S_p(1, \ell^m, 2)$, avec $m \geq 1$, on a l'énoncé suivant :

Théorème 1.2 *Supposons que l'une des quatre conditions suivantes soit réalisée :*

(1) *on a* $\ell \equiv 1 \bmod 8$ *et les entiers* $\frac{\ell^2+1}{2}$, $\frac{\ell+1}{2}$ *et* $\frac{\ell-1}{2}$ *ne sont pas des carrés ;*
(2) *on a* $\ell \equiv 3 \bmod 8$ *et* $\frac{\ell-1}{2}$ *n'est pas un carré ;*
(3) *on a* $\ell \equiv 5 \bmod 8$ *;*
(4) *on a* $\ell \equiv 7 \bmod 8$, $\ell \neq 23$ *et les entiers* $\frac{\ell^2+1}{2}$ *et* $\frac{\ell+1}{2}$ *ne sont pas des carrés.*

Alors, pour tout entier $m \geq 1$ *et tout nombre premier* p *tels que*

$$p > m \quad et \quad p > \left(8\sqrt{\ell+1} + 1\right)^{16(\ell-1)}, \tag{4}$$

l'ensemble $S_p(1, \ell^m, 2)$ *est vide.*

Les théorèmes 1.1 et 1.2 affirment que la conjecture 1 est vraie pour certains triplets d'entiers de la forme $(2^n, \ell^m, 1)$, $(2^n\ell^m, 1, 1)$ et $(1, \ell^m, 2)$. On en déduit par exemple le résultat suivant :

Corollaire

(1) *Si* $\ell \equiv 3$ *ou* $5 \bmod 8$, *la conjecture* 1 *est vraie pour les triplets* $(1, \ell, 1)$ *et* $(1, \ell, 2)$.
(2) *Si* $\ell \equiv 3 \bmod 8$, *la conjecture 1 est vraie pour le triplet* $(2, \ell, 1)$.

Dans certains cas où le théorème 1.1 ne permet pas de conclure, pour $n \in \{0, 1, 3, 5\}$ et $\ell \equiv 1$ ou $7 \bmod 8$, le résultat qui suit apporte une réponse partielle à la conjecture 1. On note r le nombre de classes de $\mathbb{Q}$-isogénie de courbes elliptiques sur $\mathbb{Q}$ de conducteur 2ℓ ayant au moins un point d'ordre 2 sur $\mathbb{Q}$.

Théorème 1.3 *Supposons* $n \in \{0, 1, 3, 5\}$ *et que le couple* (ℓ, n) *vérifie l'une des deux conditions suivantes :*

(1) *On a* $\ell \equiv 1 \bmod 8$ *et l'une des assertions suivantes est satisfaite :*
   (i) *on a* $n = 1$ *et les entiers* $2\ell - 1$ *et* $2\ell^2 - 1$ *ne sont pas des carrés ;*
   (ii) *on a* $n \in \{0, 3\}$ *et les entiers* $\ell - 1$, $\ell - 8$ *et* $\ell + 8$ *ne sont pas des carrés ;*
   (iii) *on a* $n = 5$ *et les entiers* $\ell - 16$, $\ell - 32$ *et* $\ell + 32$ *ne sont pas des carrés.*
(2) *On a* $\ell \equiv 7 \bmod 8$ *et l'une des assertions suivantes est satisfaite :*
   (i) *on a* $n = 1$ *et* ℓ *vérifie la propriété* (C) *;*
   (ii) *on a* $n \in \{0, 3\}$ *et* $\ell \neq 7$ *;*
   (iii) *on a* $n = 5$ *et* $\ell \neq 7, 23, 31$.

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Alors, pour tout entier naturel impair m, il existe deux ensembles $\mathcal{P}$ et $\mathcal{P}'$ de nombres premiers (dépendant de ℓ, m et n), dont les densités sont > 0, tels que pour tout p dans $\mathcal{P}$ (resp. $\mathcal{P}'$), l'ensemble $S_p(2^n, \ell^m, 1)$ (resp. $S_p(2^n\ell^m, 1, 1)$) soit vide.

Si δ est la plus petite des densités de $\mathcal{P}$ et $\mathcal{P}'$, on a :

$$\delta \geq \begin{cases} \dfrac{1}{4^r} & \text{si } n = 0, \\ \dfrac{1}{2^r} & \text{si } n \in \{1, 3, 5\}. \end{cases}$$

Remarques 1 (1) Les propriétés (A), (B) et (C) sont souvent réalisées en pratique. En effet, il y a 2384 nombres premiers congrus à 1 modulo 8 plus petits que 10^5 et il y en a 1812 qui vérifient la propriété (A). Il y a 2399 nombres premiers plus petits que 10^5 congrus à 7 modulo 8. Il y en a 2256 qui vérifient la propriété (B) et 2333 qui vérifient la propriété (C). Les propriétés (B) et (C) sont toutes les deux satisfaites pour 2201 d'entre eux.

(2) Supposons $\ell \equiv 7 \bmod 8$. Dans ce cas, on a $r = 1$ si ℓ n'est pas un nombre de Mersenne, i.e. n'est pas de la forme $2^t - 1$; on a $r \leq 2$ sinon. Cela résulte de [4, théorème 2] et du [18, théorème 1], tout au moins si ℓ est distinct de 7 et 23.

2 Courbes elliptiques

Considérons trois entiers naturels non nuls a, b, c et un nombre premier $p \geq 5$. On suppose, pour toute la suite, que la condition ci-dessous est satisfaite :

a, b et c sont premiers entre eux deux à deux.

Soit (x, y, z) un élément de $S_p(a, b, c)$. On va lui associer deux courbes elliptiques E_1 et E_2 définies sur $\mathbb{Q}$, ayant chacune au moins un point d'ordre 2 sur $\mathbb{Q}$, dont on va décrire les propriétés de réduction. Pour simplifier cette étude, on suppose de plus, dans ce paragraphe, que les quatre conditions suivantes sont réalisées :

(C_1) b est impair.
(C_2) c est sans facteurs carrés.
(C_3) Si cz est impair, on choisit z de sorte que l'on ait $cz \equiv -1 \bmod 4$.
(C_4) Les entiers ax et by sont premiers entre eux.

Pour tout nombre premier ℓ, on note désormais v_ℓ la valuation ℓ-adique de $\mathbb{Q}$.

Remarque 2 La condition (C_4) est la seule contraignante pour démontrer les résultats que l'on a en vue. On devra en tenir compte dans la suite. Notons cependant que si pour tout nombre premier ℓ divisant ab, on a

$$v_\ell(ab) \equiv 1 \bmod 2 \quad \text{et} \quad v_\ell(ab) < p, \tag{5}$$

alors, la condition (C_4) est satisfaite.

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

2.1 La courbe E_1

Soit E_1 la courbe d'équation de Weierstrass

$$Y^2 = X^3 + (2cz)X^2 + (acx^p)X. \tag{6}$$

Les invariants standard qui lui sont associés sont (*cf.* [42, p. 36]) :

$$c_4 = 2^4c(4cz^2 - 3ax^p), \quad c_6 = 2^6c^2z(9ax^p - 8cz^2), \quad \Delta = 2^6(a^2bc^3)(x^2y)^p.$$

Puisque Δ est non nul, E_1 est une courbe elliptique définie sur $\mathbb{Q}$. On note N_{E_1} son conducteur.

Lemme 2.1 *Soit ℓ un nombre premier impair.*

(1) *Si ℓ ne divise pas $abcxy$, E_1 a bonne réduction en ℓ.*
(2) *Si ℓ divise $abxy$, E_1 a réduction multiplicative en ℓ, et l'on a $v_\ell(N_{E_1}) = 1$.*
(3) *Si ℓ divise c, E_1 a réduction additive en ℓ, et l'on a $v_\ell(N_{E_1}) = 2$.*
(4) *L'équation* (6) *est minimale en ℓ.*

Démonstration (1) L'assertion 1 résulte du fait que ℓ ne divise pas Δ.

(2) Supposons que ℓ divise c_4 et que ℓ divise $abxy$. Si ℓ divise ax, alors ℓ divise cz puis by, ce qui contredit la condition (C_4). Ainsi ℓ divise by. D'après (C_4), ℓ ne divise pas c, d'où la congruence $4cz^2 \equiv 3ax^p \bmod \ell$. D'après l'égalité $ax^p + by^p = cz^2$, on a $ax^p \equiv cz^2 \bmod \ell$, d'où $ax \equiv 0 \bmod \ell$ et une contradiction. Cela prouve l'assertion 2.

(3) On suppose que ℓ divise c. La condition (C_4) entraîne que ℓ ne divise pas $abxy$. Puisque c est sans facteurs carrés, on a ainsi $v_\ell(\Delta) = 3$, et l'équation (6) est donc minimale en ℓ. Puisque ℓ divise c_4, E_1 a réduction additive en ℓ. Si $\ell \neq 3$, on a $v_\ell(N_{E_1}) = 2$ (*cf.* [42, p. 46]). Si $\ell = 3$, cette égalité résulte de l'algorithme de Tate (*cf.* [42, p. 47–48] : en suivant ses notations, on a $a_3 = a_6 = 0$, $a_4 = acx^p$, $b_2 = 8cz$ et $b_8 = -a^2c^2x^{2p}$. Par suite, ℓ divise a_3, a_4 et b_2, ℓ^2 divise a_6 et c étant sans facteurs carrés (condition (C_2)), ℓ^3 ne divise pas b_8. Le type de Kodaira de E_1 en 3 est donc III, d'où l'assertion 3.

(4) L'assertion 4 est une conséquence de ce qui précède. D'où le lemme. ∎

En ce qui concerne le type de réduction de E_1 en 2, on a l'énoncé suivant :

Lemme 2.2

(1) *Si c est pair, E_1 a réduction additive en 2, et l'on a $v_2\big(N_{E_1}\big) = 8$.*
(2) *Si a est pair, E_1 a réduction additive en 2, et l'on a*

$$v_2(N_{E_1}) = \begin{cases} 7 & \text{si } v_2(a) = 1 \text{ et } x \text{ est impair,} \\ 6 & \text{sinon.} \end{cases}$$

(3) *Supposons ac impair.*

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

(3.1) *Supposons y pair.*
Si $p = 5$ *et* $v_2(y) = 1$, E_1 *a réduction additive en* 2 *et l'on a* $v_\ell(N_{E_1}) = 3$.
Si $p \geq 7$ *ou* $v_2(y) \geq 2$, E_1 *a réduction multiplicative en* 2 *et l'on a* $v_2 N_{E_1} = 1$.

(3.2) *Si y est impair,* E_1 *a réduction additive en* 2, *et l'on a*

$$v_2(N_{E_1}) = \begin{cases} 6 & \text{si } x \text{ est pair,} \\ 6 & \text{si } acx \equiv 1 \bmod 4, \\ 5 & \text{si } acx \equiv -1 \bmod 4. \end{cases}$$

(4) *L'équation* (6) *est minimale en* 2 *si et seulement si* E_1 *a réduction additive en* 2.

Comme conséquence directe des lemmes 2.1 et 2.2, on obtient :

Corollaire 2.3 *Soit* Δ_{E_1} *le discriminant minimal de* E_1. *On a*

$$\Delta_{E_1} = \begin{cases} 2^6(a^2bc^3)(x^2y)^p & \text{si } E_1 \text{ a réduction additive en 2,} \\ 2^{-6}(a^2bc^3)(x^2y)^p & \text{sinon.} \end{cases} \tag{7}$$

Démonstration du lemme 2.2 Les invariants standard b_2, b_4, b_6 et b_8 associés à l'équation (6) sont (*cf.* [42]) :

$$b_2 = 8cz, \quad b_4 = 2acx^p, \quad b_6 = 0, \quad b_8 = -a^2c^2x^{2p}.$$

(1) Si c est pair, $abxy$ est impair (condition (C_4)). Puisque c est sans facteur carré (condition (C_2)), on a donc $v_2(c_4) = 5$, $v_2(c_6) \geq 8$ et $v_2(\Delta) = 9$. D'après [33, tableau IV, p. 129], on a alors $v_2\big(N_{E_1}\big) = 8$. D'où l'assertion (1).

(2) Supposons a pair. Dans ce cas, $bcyz$ est impair (condition (C_4)).

Supposons x pair. On a alors $v_2(c_4) = 6$, $v_2(c_6) = 9$ et $v_2(\Delta) \geq 18$. Le tableau IV de [33] entraîne alors $v_2(N_{E_1}) = 6$.

Supposons x impair. On a

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = \begin{cases} (5, 7, 8) & \text{si } v_2(a) = 1, \\ (\geq 6, 8, 10) & \text{si } v_2(a) = 2, \\ (6, \geq 9, 12) & \text{si } v_2(a) = 3, \\ (6, 9, \geq 14) & \text{si } v_2(a) \geq 4. \end{cases}$$

Le tableau IV de [33] entraîne le résultat si $v_2(a) \neq 3$.

Supposons $v_2(a) = 3$. Il s'agit de démontrer que le type de Néron de E_1 est I_2^*. On utilise pour cela l'algorithme de Tate (*cf.* [42, p. 49]). Les conditions intervenant dans cet algorithme sont réalisées. Avec ses notations, on a

$$P(T) = T^3 + czT^2 + \frac{acx^p}{4}T.$$

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Le polynôme P a dans $\mathbb{F}_2$ une racine simple ($T = 1$) et une racine double ($T = 0$), car cz est impair. Il s'agit alors de décider si le polynôme $czX^2 + \frac{acx^p}{8}X$ a deux racines distinctes modulo 2, ce qui est le cas, car $v_2(a) = 3$ et cxz est impair. D'où l'assertion.

(3) On suppose ac impair.
(3.1) Supposons y pair. Dans ce cas, $acxz$ est impair (condition (C_4)). On a donc

$$v_2(c_4) = 4, \quad v_2(c_6) = 6, \quad \text{et} \quad v_2(\Delta) \geq 11.$$

Suivant la terminologie employée dans [33], on est dans un cas de Tate ≥ 7. On utilise la proposition 4 de [33]. D'après la condition (C_3), on a $cz \equiv 3$ ou $7 \mod 8$ et par ailleurs, on a

$$ax^p \equiv cz^2 \mod 32.$$

On en déduit que l'entier $r = 1$ vérifie la congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \mod 32.$$

La congruence $2cz + 3 - s^2 \mod 4$ étant satisfaite avec $s = 1$, il en résulte que l'on est dans un cas de Tate ≥ 8.

Supposons $p = 5$ *et* $v_2(y) = 1$. Compte tenu du fait que b est impair (condition (C_1)), on a $\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (4, 6, 11)$, de sorte que le type de Kodaira de E_1 est II* et l'on a $v_2(N_{E_1}) = 3$.

Supposons $p \geq 7$ *ou bien* $v_2(y) \geq 2$. Dans ce cas, on a $v_2(c_4) = 4$, $v_2(c_6) = 6$, $v_2(\Delta) \geq 13$, et l'on déduit de ce qui précède que l'équation (6) n'est pas minimale en 2, ce qui entraîne le résultat.

(3.2) Supposons y impair.

Si x est pair, cz est impair (condition (C_4)). On a ainsi $v_2(c_4) = 6$, $v_2(c_6) = 9$ et $v_2(\Delta) \geq 16$. Il en résulte que $v_2(N_{E_1}) = 6$.

Supposons x impair. Puisque ax^p et by^p sont impairs, z est pair. On a donc $v_2(c_4) = 4$, $v_2(c_6) \geq 7$ et $v_2(\Delta) = 6$. On est dans le cas 3 ou 4 de Tate. On utilise [33, proposition 1] avec $r = 1$ et $t = 0$, ce qui entraîne le résultat.

(4) L'assertion 4 est une conséquence de l'étude des cas précédents. Cela termine la démonstration du lemme 2.2. ∎

2.2 La courbe E_2

Soit E_2 la courbe d'équation de Weierstrass :

$$Y^2 = X^3 + (2cz)X^2 + (bcy^p)X. \tag{8}$$

Les invariants standard associés à ce modèle sont

$$c_4 = 2^4c(4cz^2 - 3by^p), \quad c_6 = 2^6c^2z(9by^p - 8cz^2), \quad \Delta = 2^6(ab^2c^3)(xy^2)^p.$$

On a $\Delta \neq 0$, donc E_2 est une courbe elliptique sur $\mathbb{Q}$. Notons N_{E_2} son conducteur. Les démonstrations des deux lemmes qui suivent étant identiques à celles des lemmes 2.1 et 2.2, sont omises ici.

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Lemme 2.4 *Soit ℓ un nombre premier impair.*

(1) *Si ℓ ne divise pas abcxy, E_2 a bonne réduction en ℓ.*
(2) *Si ℓ divise abxy, E_2 a réduction multiplicative en ℓ, et l'on a $v_\ell(N_{E_2}) = 1$.*
(3) *Si ℓ divise c, E_2 a réduction additive en ℓ, et l'on a $v_\ell(N_{E_2}) = 2$.*
(4) *L'équation* (8) *est minimale en ℓ.*

Lemme 2.5

(1) *Si c est pair, E_2 a réduction additive en* 2*, et l'on a $v_2(N_{E_2}) = 8$.*
(2) *Supposons a pair.*
  (2.1) *Supposons x pair.*
    Si $p = 5$, $v_2(a) = 1$ et $v_2(x) = 1$, E_2 a bonne réduction en 2*.*
    Si $p \geq 7$, ou $v_2(a) \geq 2$, ou $v_2(x) \geq 2$, E_2 a réduction multiplicative en 2*, et l'on a $v_2\big(N_{E_2}\big) = 1$.*
  (2.2) *Supposons x impair. Dans ce cas, E_2 a réduction additive en* 2 *sauf si $v_2(a) \geq 6$.*
    Si $v_2(a) = 1$, on a $v_2(N_{E_2}) = 7$.
    Si $v_2(a) = 2$, on a

$$v_2(N_{E_2}) = \begin{cases} 4 & \text{si } acx \equiv 4 \mod 16 \\ 2 & \text{si } acx \equiv 12 \mod 16. \end{cases}$$

    Si $v_2(a) = 3$, on a $v_2(N_{E_2}) = 5$.
    Si $v_2(a) \in \{4, 5\}$, on a $v_2(N_{E_2}) = 3$.
    Si $v_2(a) = 6$, E_2 a bonne réduction en 2*.*
    Si $v_2(a) \geq 7$, E_2 a réduction multiplicative en 2 *et l'on a $v_2(N_{E_2}) = 1$.*
(3) *Supposons ac impair.*
  (3.1) *Si y est pair, E_2 a réduction additive en* 2*, et l'on a $v_2(N_{E_2}) = 6$.*
  (3.2) *Supposons y impair et x pair.*
    Si $p = 5$ et $v_2(x) = 1$, E_2 a réduction additive en 2 *et l'on a $v_2(N_{E_2}) = 3$.*
    Si $p \geq 7$ ou $v_2(x) \geq 2$, E_2 a réduction multiplicative en 2 *et l'on a $v_2(N_{E_2}) = 1$.*
  (3.3) *Si xy est impair, E_2 a réduction additive en* 2*, et l'on a*

$$v_2(N_{E_2}) = \begin{cases} 5 & \text{si } acx \equiv 1 \bmod 4, \\ 6 & \text{si } acx \equiv -1 \bmod 4. \end{cases}$$

(4) *L'équation* (8) *est minimale en* 2 *si et seulement si E_2 a réduction additive en* 2*.*

On en déduit le résultat suivant :

Corollaire 2.6 *Soit Δ_{E_2} le discriminant minimal de E_2. On a*

$$\Delta_{E_2} = \begin{cases} 2^6(ab^2c^3)(xy^2)^p & \text{si } E_2 \text{ a réduction additive en } 2, \\ 2^{-6}(ab^2c^3)(xy^2)^p & \text{sinon.} \end{cases} \tag{9}$$

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

3 Représentations galoisiennes

Soient a, b et c trois entiers naturels non nuls, premiers entre eux deux à deux, et p un nombre premier ≥ 7. On considère un élément $(x, y, z) \in S_p(a, b, c)$ vérifiant les conditions (C_1)–(C_4) du §2. Pour $i \in \{1, 2\}$, soit E_i la courbe elliptique associée à (x, y, z) définie par l'équation (6) ou (8). Soient $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ contenue dans $\mathbb{C}$ et $E_i[p]$ le sous-groupe des points de p-torsion de $E_i(\overline{\mathbb{Q}})$. Le groupe de Galois $G_{\mathbb{Q}}$ de $\overline{\mathbb{Q}}$ sur $\mathbb{Q}$ agit sur $E_i[p]$ et cette action fournit une représentation de dimension 2 sur $\mathbb{Z}/p\mathbb{Z}$

$$\rho_p^{E_i} : G_{\mathbb{Q}} \to \mathrm{Aut}(E_i[p]).$$

Proposition 3.1 *Pour $i \in \{1, 2\}$, on a les assertions suivantes :*

(1) *si $p \geq 11$, $\rho_p^{E_i}$ est irréductible ;*

(2) *si $p = 7$, $\rho_p^{E_i}$ est réductible si et seulement si on a*

$$(a, b, c) = (64, 1, 7) \quad \textit{et} \quad (x, y, z) = (1, -1, -3).$$

Dans ce cas, les conducteurs de E_1 et E_2 sont respectivement $2^6.7^2$ et 7^2.

Démonstration La courbe E_i a un point d'ordre 2 rationnel sur $\mathbb{Q}$. Par suite, si $\rho_p^{E_i}$ est réductible, il existe un sous-groupe de $E_i(\overline{\mathbb{Q}})$ d'ordre $2p$ stable par $G_{\mathbb{Q}}$.

(1) Pour tout nombre premier $p \geq 11$, la courbe modulaire $Y_0(2p)$ n'a pas de points rationnels sur $\mathbb{Q}$ (*cf.*[20]), d'où l'assertion 1.

(2) Supposons $p = 7$. La courbe modulaire $Y_0(14)$ est la courbe elliptique notée 14A1 dans les tables de [7] [29, p. 45]. On en déduit que $Y_0(14)$ possède exactement deux points rationnels sur $\mathbb{Q}$. Ils correspondent à deux classes de $\overline{\mathbb{Q}}$-isomorphisme de courbes elliptiques sur $\mathbb{Q}$ d'invariants modulaires -15^3 et 255^3 : en effet, ce sont les invariants modulaires respectivement des courbes notées 49A1 et 49A2 dans [7] et elles ont un sous-groupe d'ordre 14 stable par Galois.

Notons j_{E_i} l'invariant modulaire de E_i. Si $(a, b, c) = (64, 1, 7)$ et $(x, y, z) = (1, -1, -3)$, on vérifie que l'on a $j_{E_1} = -15^3$ et $j_{E_2} = 255^3$, donc $\rho_p^{E_1}$ et $\rho_p^{E_2}$ sont réductibles.

Inversement, supposons $\rho_7^{E_i}$ réductible. On a donc $j_{E_i} \in \{-15^3, 255^3\}$. Il existe ainsi un entier d sans facteurs carrés tel que E_i soit isomorphe sur $\mathbb{Q}$ à la tordue quadratique de la 49A1 ou 49A2 par $\sqrt{d}$; notons respectivement $F_{1,d}$ et $F_{2,d}$ ces tordues quadratiques. Vérifions que l'on a

$$d \in \{\pm 1, \pm 2\}.$$

Supposons pour cela qu'il existe un nombre premier impair ℓ qui divise d. Dans ce cas, $F_{1,d}$ et $F_{2,d}$ ont réduction additive en ℓ et l'exposant de ℓ dans leurs discriminants minimaux vaut 6 ou 9 (ce dernier cas se produisant si $\ell = 7$). Par ailleurs, d'après les lemmes 2.1 et 2.4, l'exposant de ℓ dans le discriminant minimal Δ_{E_i} de E_i est 3, d'où une contradiction et l'assertion. En calculant les discriminants minimaux et les conducteurs de $F_{1,d}$ et $F_{2,d}$, on en déduit que l'on a

$$(\Delta_{E_i}, N_{E_i}) \in \left\{ (\pm 7^3, 7^2), (\pm 2^{12}.7^3, 2^4.7^2), (\pm 2^{18}.7^3, 2^6.7^2) \right\}.$$

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Il résulte alors des assertions 1 des lemmes 2.2 et 2.5 que c est impair. D'après les lemmes 2.1 et 2.4 on a donc $c = 7$ et $b = 1$.

On a $\Delta_{E_1} \neq \pm 7^3$ car E_1 a mauvaise réduction en 2 (lemme 2.2). Par suite, E_1 a réduction additive en 2 et d'après la formule (7) on a

$$\Delta_{E_1} = 2^6(a^2bc^3)(x^2y)^7 \in \left\{\pm 2^{12}.7^3, \pm 2^{18}.7^3\right\}.$$

Supposons $\Delta_{E_1} = \pm 2^{12}.7^3$. Compte tenu de l'égalité $ax^7 + y^7 = 7z^2$ et de la condition (C_3), cela implique $a = 8$ et $(x, y, z) = (1, -1, 1)$, ce qui conduit à $j(E_1) = -64$ et à une contradiction. On a donc $\Delta_{E_1} = \pm 2^{18}.7^3$, ce qui entraîne que xy est impair puis $a = 64$ et $(x, y, z) = (1, -1, -3)$.

Supposons $\Delta_{E_2} = \pm 7^3$. Dans ce cas, E_2 a bonne réduction en 2 et d'après la formule (9), on obtient

$$2^{-6}a(xy^2)^7 = \pm 1,$$

ce qui entraîne $a = 64$ et $(x, y, z) = (1, -1, -3)$. Supposons $\Delta_{E_2} \neq \pm 7^3$. Dans ce cas, E_2 a réduction additive en 2 et l'on a

$$\Delta_{E_2} = 2^6(ab^2c^3)(xy^2)^7 \in \left\{\pm 2^{12}.7^3, \pm 2^{18}.7^3\right\}.$$

L'égalité $\Delta_{E_2} = \pm 2^{12}.7^3$ conduit de nouveau à $a = 64$ et $(x, y, z) = (1, -1, -3)$ (en fait, cette situation ne peut pas se produire car si $a = 64$ et si x est impair, E_2 a bonne réduction en 2). Si l'on a $\Delta_{E_2} = \pm 2^{18}.7^3$, on obtient $a(xy^2)^7 = \pm 2^{12}$, d'où

$$(a, x, y) \in \left\{(32, 2, \pm 1), (2^{12}, 1, \pm 1)\right\},$$

ce qui contredit l'égalité $ax^7 + y^7 = 7z^2$.

On a ainsi dans tous les cas la condition annoncée. D'où la proposition. ■

Si $p = 5$, il est plus difficile d'obtenir un énoncé analogue à la proposition 3.1 permettant de décider à priori si $\rho_p^{E_i}$ est ou non irréductible. Cela est dû au fait que la courbe modulaire $Y_0(10)$ est isomorphe sur $\mathbb{Q}$ à la droite projective $\mathbb{P}^1$. Néanmoins, il y a des situations simples, dans lesquelles on peut conclure (*cf.* §8).

On suppose désormais que la condition suivante est réalisée :

(C_5) *ab* est sans puissances p-ièmes. Autrement dit, pour tout nombre premier ℓ, on a

$$v_\ell(ab) < p.$$

Pour $i \in \{1, 2\}$, soit k le poids de $\rho_p^{E_i}$ défini par Serre dans [37] : il est le mÃłme pour E_1 et E_2, comme on le constate ci-dessous tout au moins si p ne divise pas c, ce qui est le cas qui nous intéressera dans la suite :

Proposition 3.2

(1) *Si p divise ab, on a* $k = p + 1$.
(2) *Si p ne divise pas abc, on a* $k = 2$.

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Démonstration (1) Si p divise ab, E_i a réduction multiplicative en p (lemmes 2.1 et 2.4). D'après la condition (C_5), p ne divise pas $v_p(ab)$, *i.e.*, p ne divise pas $v_p(j_{E_i})$. La proposition 5 de [37] implique alors $k = p + 1$.

(2) Supposons que p ne divise pas abc. Si p ne divise pas xy, E_i a bonne réduction en p. Si p divise xy, E_i a réduction multiplicative en p et dans ce cas, p divise $v_p(j_{E_i})$. Cela entraîne $k = 2$ (*cf.* [37]); d'où le résultat. ∎

Soit $N(\rho_p^{E_i})$ le conducteur de $\rho_p^{E_i}$ défini par Serre dans [37]. C'est un entier premier à p qui divise N_{E_i}. Il est donné dans les deux énoncés suivants, qui résultent directement des lemmes 2.1 2.2, 2.4, et 2.5, des corollaires 2.3 et 2.6, et par exemple de la proposition de [22, p. 28].

Proposition 3.3 *On a*

$$N(\rho_p^{E_1}) = 2^t \prod_{\substack{\ell \mid ab, \\ \ell \neq 2,p}} \ell \prod_{\substack{\ell \mid c, \\ \ell \neq 2,p}} \ell^2,$$

où t est l'entier défini ci-dessous.

(1) *Si c est pair, on a $t = 8$.*

(2) *Si a est pair, on a*

$$t = \begin{cases} 7 & \text{si } v_2(a) = 1 \text{ et } x \text{ est impair,} \\ 6 & \text{sinon.} \end{cases}$$

(3) *Supposons ac impair.*

(3.1) *Supposons y pair.*
Si $p = 5$ et $v_2(y) = 1$, on a $t = 3$.
Si $p \geq 7$ ou $v_2(y) \geq 2$, on a $t = 1$.

(3.2) *Si y est impair, on a*

$$t = \begin{cases} 6 & \text{si } x \text{ est pair,} \\ 6 & \text{si } acx \equiv 1 \bmod 4, \\ 5 & \text{si } acx \equiv -1 \bmod 4. \end{cases}$$

Proposition 3.4 *On a*

$$N(\rho_p^{E_2}) = 2^t \prod_{\substack{\ell \mid ab \\ \ell \neq 2,p}} \ell \prod_{\substack{\ell \mid c \\ \ell \neq 2,p}} \ell^2,$$

où t est l'entier défini ci-dessous.

(1) *Si c est pair, on a $t = 8$.*

(2) *Supposons a pair.*

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

(2.1) *Supposons x pair.*
Si $p = 5$, *on a*

$$t = \begin{cases} 0 & \text{si } v_2(a) = 1, \\ 1 & \text{sinon.} \end{cases}$$

Si $p \geq 7$, *on a*

$$t = \begin{cases} 0 & \text{si } v_2(a) = 6, \\ 1 & \text{sinon.} \end{cases}$$

(2.2) *Supposons x impair.*
Si $v_2(a) = 1$, *on a* $t = 7$.
Si $v_2(a) = 2$, *on a*

$$t = \begin{cases} 4 & \text{si } acx \equiv 4 \bmod 16, \\ 2 & \text{si } acx \equiv 12 \bmod 16. \end{cases}$$

Si $v_2(a) = 3$, *on a* $t = 5$.
Si $v_2(a) \in \{4, 5\}$, *on a* $t = 3$.
Si $v_2(a) = 6$, *on a* $t = 0$.
Si $v_2(a) \geq 7$, *on a* $t = 1$.

(3) *Supposons ac impair.*

(3.1) *Si y est pair, on a* $t = 6$.
(3.2) *Supposons y impair et x pair.*
Si $p = 5$ *et* $v_2(x) = 1$, *on a* $t = 3$.
Si $p \geq 7$ *ou* $v_2(x) \geq 2$, *on a* $t = 1$.
(3.3) *Si xy est impair, on a*

$$t = \begin{cases} 5 & \text{si } acx \equiv 1 \bmod 4, \\ 6 & \text{si } acx \equiv -1 \bmod 4. \end{cases}$$

4 La méthode modulaire

Cette méthode est maintenant bien connue et a été exposée dans de nombreux travaux, (*cf.* par exemple [38]). Rappelons en quoi elle consiste dans notre contexte.

Étant donnés deux entiers naturels non nuls k et N, avec k pair, on note $S_k(\Gamma_0(N))$ le $\mathbb{C}$-espace vectoriel des formes modulaires paraboliques de poids k pour le sous-groupe de congruence $\Gamma_0(N)$. Soit $S_k^+(N)$ le sous-$\mathbb{C}$-espace vectoriel de $S_k(\Gamma_0(N))$ engendré par les newforms au sens d'Atkin–Lehner (*cf.* [1]). C'est un espace vectoriel de dimension finie $g_k^+(N)$ sur $\mathbb{C}$. Une newform f de $S_k^+(N)$ possède un développement en série de Fourier

$$f = \sum_{n \geq 1} a_n(f) q^n \quad \text{où } q = \exp(2\pi i \tau),\ \operatorname{Im}(\tau) > 0.$$

Dans le cas où f est normalisée, *i.e.*, si $a_1(f) = 1$, les $a_n(f)$ sont des entiers algébriques, et l'extension $\mathbb{Q}(f)$ de $\mathbb{Q}$ obtenue en adjoignant à $\mathbb{Q}$ les coefficients $a_n(f)$

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

est une extension finie de $\mathbb{Q}$ qui est totalement réelle. Pour tout nombre premier ℓ ne divisant pas N, $a_\ell(f)$ est valeur propre de l'opérateur de Hecke T_ℓ opérant sur $S_k^+(N)$. Il existe exactement $g_k^+(N)$ newforms normalisées. Elles forment une base de $S_k^+(N)$.

Soient p un nombre premier ≥ 5 et a, b et c trois entiers naturels non nuls premiers entre eux deux à deux. On suppose qu'il existe un élément (x, y, z) de $S_p(a, b, c)$ tel que $xy \neq \pm 1$, les conditions (C_1)–(C_5) du §2 étant satisfaites. En vue de prouver la conjecture 1 ou 2 pour le triplet (a, b, c), ou de résoudre le problème énoncé dans l'introduction, notre objectif est de démontrer, dans certains cas particuliers, que ces hypothèses conduisent à une contradiction.

Dans ce qui suit, l'indice i désigne l'un des entiers 1 ou 2 : on a $i \in \{1, 2\}$. Considérons la courbe elliptique $E_i/\mathbb{Q}$ associée à (x, y, z) et à (a, b, c) comme dans le paragraphe 2. Soient $\rho_p^{E_i}$ la représentation de $G_\mathbb{Q}$ dans $\mathrm{Aut}(E_i[p])$, k son poids et $N(\rho_p^{E_i})$ son conducteur : ils sont donnés dans les propositions 3.2–3.4. Soit

$$L(E_i, s) = \sum_{n \geq 1} \frac{a_n(E_i)}{n^s},$$

la fonction L de Hasse–Weil de E_i. Il est maintenant démontré que E_i est modulaire (*cf.* [5, 43]). Supposons que $\rho_p^{E_i}$ soit irréductible. Dans ce cas, il existe une newform normalisée f_i de $S_k^+(N(\rho_p^{E_i}))$,

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

et une place $\mathfrak{P}_i$ de $\overline{\mathbb{Q}}$ de caractéristique résiduelle p telles que, pour tout nombre premier ℓ, on ait (*cf.* par exemple [38, 2]) :

$$a_\ell(f_i) \equiv a_\ell(E_i) \bmod \mathfrak{P}_i, \quad \text{si } \ell \text{ ne divise pas } pN_{E_i}, \tag{10}$$

$$a_\ell(f_i) \equiv \pm(\ell + 1) \bmod \mathfrak{P}_i, \quad \text{si } \ell \text{ divise } N_{E_i} \text{ et } \ell \text{ ne divise pas } pN(\rho_p^{E_i}). \tag{11}$$

Pour démontrer que l'existence du point (x, y, z) envisagé conduit à une contradiction, il suffit donc de prouver, en considérant au choix $\rho_p^{E_1}$ ou $\rho_p^{E_2}$, qu'il n'existe pas de tel couple $(f_1, \mathfrak{P}_1)$ ou $(f_2, \mathfrak{P}_2)$, pour lequel les congruences (10) et (11) soient satisfaites. En pratique, ce choix est dicté par les conducteurs de ces représentations.

Dans certaines situations, f_i « correspond » à une courbe elliptique sur $\mathbb{Q}$ de conducteur $N(\rho_p^{E_i})$. En effet, supposons que les deux conditions suivantes soient satisfaites :

(i) on a $k = 2$;
(ii) pour tout $n \geq 1$ le coefficient $a_n(f_i)$ appartient à $\mathbb{Z}$.

Dans ce cas, il existe une courbe elliptique $F_i/\mathbb{Q}$, de conducteur $N(\rho_p^{E_i})$, telle que pour tout $n \geq 1$ on ait

$$a_n(f_i) = a_n(F_i),$$

où $a_n(F_i)$ est le n-ième coefficient de la fonction de L de F_i. La courbe F_i est unique à $\mathbb{Q}$-isogénie près. Le $G_\mathbb{Q}$-module $F_i[p]$ des points de p-torsion de F_i est isomorphe à

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

$E_i[p]$ et l'on a (*cf.* [27, proposition 3]) :

$$a_\ell(F_i) \equiv a_\ell(E_i) \bmod p, \quad \text{pour tout } \ell \text{ premier ne divisant pas } N_{E_i}. \tag{12}$$

En fait, les conditions (i) et (ii) sont réalisées si p est assez grand, de sorte que $\rho_p^{E_i}$ « provient » alors, au sens précédent, d'une courbe elliptique sur $\mathbb{Q}$ de conducteur $N(\rho_p^{E_i})$. Plus précisément, pour tout entier $n \geq 1$, posons

$$\begin{gathered}\mu(n) = n \prod_{\substack{l \mid n \\ l \text{ premier}}} \left(1 + \frac{1}{l}\right), \quad F(n) = \left(\sqrt{\frac{\mu(n)}{6}} + 1\right)^{2g_2^+(n)}, \\ G(n) = \left(\sqrt{\frac{\mu(\mathrm{ppcm}(4,n))}{6}} + 1\right)^2.\end{gathered} \tag{13}$$

Proposition 4.1 *Pour $i = 1$ ou $i = 2$, supposons que l'on ait*

$$abc \not\equiv 0 \bmod p \quad \textit{et} \quad p > \mathrm{Max}\left(F\left(N(\rho_p^{E_i})\right), G\left(N(\rho_p^{E_i})\right)\right).$$

Alors, il existe une courbe elliptique $F_i/\mathbb{Q}$, de conducteur $N(\rho_p^{E_i})$ et ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, telle que les $G_{\mathbb{Q}}$-modules $E_i[p]$ et $F_i[p]$ soient isomorphes.

Démonstration Puisque p ne divise pas abc, on a $k = 2$ (prop. 3.2). D'après l'inégalité $p > F\left(N(\rho_p^{E_i})\right)$, il existe une courbe elliptique $F_i/\mathbb{Q}$, de conducteur $N(\rho_p^{E_i})$, telle que les $G_{\mathbb{Q}}$-modules $E_i[p]$ et $F_i[p]$ soient isomorphes (*cf.* [24, théorème 3]). Par ailleurs, en utilisant l'inégalité $p > G(N(\rho_p^{E_i}))$ et le fait que E_i possède un point d'ordre 2 sur $\mathbb{Q}$, on déduit, de la mÃłme façon que dans la démonstration de [24, théorème 4], que pour tout nombre premier ℓ ne divisant pas $2N(\rho_p^{E_i})$, on a $a_\ell(F_i) = a_\ell(E_i)$, puis $a_\ell(F_i) \equiv \ell + 1 \bmod 2$. Compte tenu du théorème de densité de Chebotarev, cela entraîne que F_i a un point d'ordre 2 rationnel sur $\mathbb{Q}$. D'où le résultat. ∎

Lorsqu'il n'existe pas de courbes elliptiques sur $\mathbb{Q}$, de conducteur $N(\rho_p^{E_i})$ et ayant au moins un point d'ordre 2 sur $\mathbb{Q}$, ce résultat permet d'obtenir la contradiction souhaitée, tout au moins si p est assez grand. Nous l'utiliserons pour démontrer les théorèmes 1.1 et 1.2. La proposition 4.1 permet par ailleurs de démontrer que la conjecture 3 énoncée dans l'introduction entraîne les conjectures 1 et 2.

S'il existe des courbes elliptiques sur $\mathbb{Q}$ de conducteurs $N(\rho_p^{E_1})$ et $N(\rho_p^{E_2})$ ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, il est plus difficile d'obtenir une contradiction à l'existence de (x, y, z). On dispose néanmoins de deux méthodes, présentées ci-dessous, qui permettent parfois d'y parvenir.

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

4.1 La méthode de réduction

On conserve les hypothèses faites et les notations utilisées précédemment. En particulier, pour $i \in \{1, 2\}$, il existe un couple $(f_i, \mathfrak{P}_i)$ vérifiant les congruences (10) et (11). La méthode de réduction permet d'éliminer certains couples $(f, \mathfrak{P})$ comme ci-dessus parmi ceux susceptibles de vérifier ces congruences.

Considérons un nombre premier q satisfaisant les deux conditions suivantes :

(i) on a $q \equiv 1 \bmod p$;
(ii) E_1 et E_2 ont bonne réduction en q.

La condition (ii) signifie que q ne divise pas $abcxy$ (lemmes 2.1 et 2.4). Par suite, E_1 a bonne réduction en q si et seulement si tel est le cas de E_2. Par exemple, la condition (ii) est satisfaite si pour $i = 1$ ou $i = 2$:

(iii) q ne divise pas abc et $a_q(f_i) \not\equiv \pm 2 \mod \mathfrak{P}_i$.

Notons ici que nous ne disposons pas *a priori* de critères simples utilisant seulement l'égalité (1), permettant de décider si la condition (ii) est réalisée.

Si u est un entier, notons $\bar{u}$ son image dans $\mathbb{F}_q$. On pose $q = np + 1$ où $n \geq 1$. Pour toute courbe elliptique $\widetilde{E}/\mathbb{F}_q$, posons par ailleurs

$$a(\widetilde{E}) = 1 + q - \left|\widetilde{E}(\mathbb{F}_q)\right|,$$

où $|\widetilde{E}(\mathbb{F}_q)|$ est le cardinal de $\widetilde{E}(\mathbb{F}_q)$.

Considérons l'ensemble R_q des triplets $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$ vérifiant les égalités suivantes :

$$\alpha^n = \beta^n = 1 \quad \text{et} \quad \bar{a}\alpha + \bar{b}\beta = \bar{c}\gamma^2. \tag{14}$$

À chaque élément $\xi = (\alpha, \beta, \gamma) \in R_q$, on associe les équations de Weierstrass sur $\mathbb{F}_q$

$$\widetilde{E_{1,\xi}} : Y^2 = X^3 + (2\bar{c}\,\gamma)X^2 + (\overline{ac}\,\alpha)X,$$
$$\widetilde{E_{2,\xi}} : Y^2 = X^3 + (2\bar{c}\,\gamma)X^2 + (\overline{bc}\,\beta)X.$$

Puisque q ne divise pas abc et que $\alpha\beta$ n'est pas nul, $\widetilde{E_{1,\xi}}$ et $\widetilde{E_{2,\xi}}$ sont des courbes elliptiques sur $\mathbb{F}_q$.

Lemme 4.2 *Il existe un élément $\xi \in R_q$ tel que l'on ait*

$$a_q(f_i) \equiv a(\widetilde{E_{i,\xi}}) \mod \mathfrak{P}_i. \tag{15}$$

Démonstration Puisque q ne divise pas xy, on a $(\bar{x}^p)^n = (\bar{y}^p)^n = 1$ et l'on a l'égalité $\bar{a}\bar{x}^p + \bar{b}\bar{y}^p = \bar{c}\bar{z}^2$, de sorte que le triplet

$$\xi = (\bar{x}^p, \bar{y}^p, \bar{z})$$

vérifie les égalités (14), *i.e.*, ξ appartient à R_q. Soit $\widetilde{E}_i$ la courbe elliptique sur $\mathbb{F}_q$ déduite de E_i par réduction modulo q. On a $\widetilde{E}_i = \widetilde{E_{i,\xi}}$, d'où l'on déduit que $a_q(E_i) = a(\widetilde{E_{i,\xi}})$. La congruence (10) entraîne alors le résultat. ∎

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

La méthode de réduction consiste en pratique à sélectionner un nombre premier q congru à 1 modulo p satisfaisant la condition (iii). On explicite ensuite tous les éléments ξ de R_q et on calcule les entiers $a(\widetilde{E_{i,\xi}})$ correspondants. Si aucun de ces entiers ne vérifie la congruence (15), le couple $(f_i, \mathfrak{P}_i)$ ne satisfait pas les congruences (10) et (11) et est ainsi écarté. On notera que cette méthode utilisée avec un nombre premier $q \not\equiv 1 \bmod p$ ne permet pas de conclure.

4.2 La méthode symplectique

Pour $i = 1$ ou $i = 2$, considérons un couple $(f_i, \mathfrak{P}_i)$ vérifiant les congruences (10) et (11). On suppose que f_i « correspond » à une courbe elliptique $F_i/\mathbb{Q}$ de conducteur $N(\rho_p^{E_i})$ (auquel cas on peut prendre $\mathfrak{P}_i = p\mathbb{Z}$). Les $G_{\mathbb{Q}}$-modules $F_i[p]$ et $E_i[p]$ sont isomorphes. Afin d'écarter cette situation, la méthode envisagée ici consiste à utiliser le résultat suivant, obtenu à partir d'un critère permettant de décider si les modules $E_i[p]$ et $F_i[p]$ sont ou non symplectiquement isomorphes (*cf.* [15]). On note Δ_{F_i} le discriminant minimal de F_i.

Proposition 4.3 *Soient ℓ_1 et ℓ_2 deux nombres premiers distincts, autres que p. Supposons que les deux conditions suivantes soient réalisées (pour $i = 1$ ou $i = 2$) :*

(i) *E_i et F_i ont réduction de type multiplicatif en ℓ_1 et ℓ_2 ;*

(ii) *on a $v_{\ell_1}(\Delta_{E_i})v_{\ell_2}(\Delta_{E_i}) \not\equiv 0 \bmod p$, auquel cas $v_{\ell_1}(\Delta_{F_i})v_{\ell_2}(\Delta_{F_i}) \not\equiv 0 \bmod p$.*

Alors,

$$v_{\ell_1}(\Delta_{E_i})v_{\ell_2}(\Delta_{E_i}) \mod p \quad \text{et} \quad v_{\ell_1}(\Delta_{F_i})v_{\ell_2}(\Delta_{F_i}) \mod p,$$

diffèrent multiplicativement par un carré de $\mathbb{F}_p$.

5 Démonstrations des théorèmes

On pose

$$C(\ell) = \left(\sqrt{32(\ell+1)} + 1\right)^{8(\ell-1)}.$$

5.1 Démonstration du théorème 1.1

On distingue deux cas suivant que n est nul ou non. Si $n = 0$, il suffit de démontrer le théorème énoncé dans l'introduction, compte tenu du fait que

$$D(\ell) := \left(\sqrt{8(\ell+1)} + 1\right)^{2(\ell-1)} < C(\ell).$$

Pour certaines autres valeurs de n, quant à l'effectivité du théorème 1.1, on peut diminuer sensiblement la constante $C(\ell)$ comme dans le cas où $n = 0$. Les constantes obtenues étant néanmoins loin d'Ãłtres optimales, nous ne les avons pas explicitées dans l'énoncé du théorème 1.1 afin d'en simplifier sa présentation.

5.1.1 Cas où $n = 0$

Démontrons le lemme suivant :

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Lemme 5.1 *Soient M un entier naturel non nul et p un nombre premier tels que*

$$p > \mathrm{Max}(M, D(\ell)).$$

Soit (u, v, w) un élément de $S_p(1, \ell^M, 1)$. Alors, ℓ divise u.

Démonstration Supposons que ℓ ne divise pas u. Les conditions (C_1), (C_2), (C_4) et (C_5) des §2 et 3 sont alors satisfaites par (u, v, w) et $(1, \ell^M, 1)$. Quitte à changer w en son opposé, on peut supposer que la condition (C_3) l'est aussi. Soient E_1 et E_2 les courbes elliptiques associées à (u, v, w) et $(1, \ell^M, 1)$ comme dans le §2. L'inégalité $p > D(\ell)$ entraîne

$$p \geq 11 \quad \text{et} \quad p \neq \ell.$$

Par suite, $\rho_p^{E_1}$ et $\rho_p^{E_2}$ sont irréductibles (prop. 3.1) et l'on est dans l'un des quatre cas suivants (prop. 3.3 et 3.4) :

(i) v est pair et $N(\rho_p^{E_1}) = 2\ell$;
(ii) u est pair et $N(\rho_p^{E_2}) = 2\ell$;
(iii) v est impair, on a $u \equiv -1 \bmod 4$ et $N(\rho_p^{E_1}) = 32\ell$;
(iv) v est impair, on a $u \equiv 1 \bmod 4$ et $N(\rho_p^{E_2}) = 32\ell$.

Par ailleurs, on a (*cf.* [15, 24]) :

$$g_2^+(32\ell) = \ell - 1 \quad \text{et} \quad g_2^+(2\ell) < \ell - 1.$$

Dans chacun des cas ci-dessus, on vérifie que l'on a l'inégalité (*cf.* (13))

$$\mathrm{Max}\left(F\left(N(\rho_p^{E_i})\right), G\left(N(\rho_p^{E_i})\right)\right) \leq D(\ell) \quad (\text{avec } i = 1 \text{ ou } i = 2).$$

Puisque l'on a $p \neq \ell$, on déduit alors de la proposition 4.1 qu'il existe une courbe elliptique sur $\mathbb{Q}$ de conducteur 2ℓ ou 32ℓ possédant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$. Si l'on a $\ell \geq 31$, compte tenu des hypothèses faites sur ℓ, les corollaires des théorèmes 1 et 5 de [18] entraînent une contradiction à l'existence d'une telle courbe elliptique. Si l'on a $\ell < 31$, on obtient directement une contradiction en utilisant les tables de [7]. D'où le lemme. ∎

Le théorème se déduit comme suit : considérons un entier $m \geq 1$ et un nombre premier p vérifiant les égalités (2) et supposons qu'il existe un élément (x, y, z) de $S_p(1, \ell^m, 1)$. D'après le lemme 5.1, ℓ divise x. Les entiers x, y et z étant premiers entre eux, on en déduit que ℓ ne divise pas y. L'inégalité $m < p$ entraîne alors que m est pair et que $2v_\ell(z) = m$. Posons $x = \ell^\alpha x_1$, $z = \ell^{\frac{m}{2}} z_1$ avec $\alpha \geq 1$ et $v_\ell(x_1) = v_\ell(z_1) = 0$. On a

$$y^p + \ell^{p-m}(\ell^{\alpha-1}x_1)^p = z_1^2.$$

Il en résulte que $(y, \ell^{\alpha-1}x_1, z_1)$ appartient à $S_p(1, \ell^{p-m}, 1)$. Par ailleurs, on a $1 \leq m < p$, d'où les inégalités $p > p - m > 0$. Puisque ℓ ne divise pas y, le lemme 5.1, utilisé avec $M = p - m$, conduit alors à une contradiction. D'où le théorème 1.1 si $n = 0$.

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Remarques 3 (1) Soient p un nombre premier ≥ 7 distinct de ℓ et m un entier naturel non nul tels que $m < p$. Soit (u, v, w) un élément de $S_p(1, \ell^m, 1)$ tel que ℓ ne divise pas u. Il résulte de la démonstration du lemme 5.1 que l'on peut associer à (u, v, w) une courbe elliptique F sur $\mathbb{Q}$, ayant un point d'ordre 2 sur $\mathbb{Q}$, telle que l'on ait $N(\rho_p^F) = 2\ell$ si uv est pair et $N(\rho_p^F) = 32\ell$ sinon. On prend pour F la courbe E_1 ou E_2 comme dans les cas (i), (ii), (iii) et (iv) ci-dessus. La représentation ρ_p^F est irréductible (prop. 3.1) et de poids 2 (prop. 3.2). On utilisera cette remarque dans la suite de ce travail.

(2) Dans la démonstration du lemme 5.1, il est possible de ne faire intervenir qu'une seule des courbes elliptiques E_1 et E_2. Dans ce cas, les propositions 3.3 et 3.4 montrent alors que, sous les hypothèses du lemme, on a $N(\rho_p^{E_i}) = 2\ell$, 32ℓ ou bien 64ℓ pour $i = 1$ et 2. Avec les arguments utilisés dans ce travail, il est alors nécessaire, pour obtenir une contradiction, de supposer que ℓ vérifie les conditions du corollaire du théorème 6 de [18]. Ces conditions sont sensiblement plus fortes que celles se trouvant dans l'énoncé du théorème. C'est la raison pour laquelle on a été amené à considérer les deux courbes E_1 et E_2 dans la démonstration de ce lemme.

5.1.2 Cas où $n \geq 1$

On utilise dans ce cas le résultat suivant :

Lemme 5.2 *Soient M un entier naturel non nul et p un nombre premier tels que*

$$p > \mathrm{Max}(M, n+6) \quad \textit{et} \quad p > C(\ell).$$

Pour tout $s = (u, v, w) \in \mathbb{Z}^3$, on a les assertions suivantes :

(i) *si $s \in S_p(2^n, \ell^M, 1) \cup S_p(2^{p-n}, \ell^M, 1)$, alors ℓ divise u ou v est pair ;*
(ii) *si $s \in S_p(2^n\ell^M, 1, 1) \cup S_p(2^{p-n}\ell^M, 1, 1)$, alors ℓ divise v ou v est pair.*

Démonstration Soit $s = (u, v, w)$ un élément appartenant à l'un des quatre ensembles envisagés ci-dessus. Les conditions (C_1), (C_2) et (C_5) sont satisfaites et quitte à changer w en $-w$, la condition (C_3) l'est aussi. Il s'agit de démontrer que la condition (C_4) n'est pas vérifiée.

On suppose le contraire. On désigne indifféremment par E_2 la courbe elliptique associée à s et l'un des triplets $(2^n, \ell^M, 1)$, $(2^{p-n}, \ell^M, 1)$, $(2^n\ell^M, 1, 1)$ et $(2^{p-n}\ell^M, 1, 1)$, définie par l'équation (8). L'inégalité $p > C(\ell)$ entraîne $p \geq 11$ et $p \neq \ell$. On est amené à distinguer les deux cas ci-dessous.

(1) Supposons $s \in S_p(2^n, \ell^M, 1) \cup S_p(2^n\ell^M, 1, 1)$. La représentation $\rho_p^{E_2}$ est irréductible et l'on a (prop. 3.4) :

$$N(\rho_p^{E_2}) = \begin{cases} 2\ell & \text{si } u \text{ est pair et } n \neq 6, \\ \ell & \text{si } u \text{ est pair et } n = 6, \end{cases}$$

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

et si u est impair

$$N(\rho_p^{E_2}) = \begin{cases} 128\ell & \text{si } n = 1, \\ 4\ell \text{ ou } 16\ell & \text{si } n = 2, \\ 32\ell & \text{si } n = 3, \\ 8\ell & \text{si } n \in \{4, 5\}, \\ \ell & \text{si } n = 6, \\ 2\ell & \text{si } n \geq 7. \end{cases}$$

On vérifie par ailleurs que l'on a

$$g_2^+(128\ell) = 4(\ell - 1) \quad \text{et} \quad g_2^+\big(N\big(\rho_p^{E_2}\big)\big) \leq 4(\ell - 1).$$

Il en résulte l'inégalité

$$\text{Max}\big(F\big(N(\rho_p^{E_2})\big), G\big(N(\rho_p^{E_2})\big)\big) \leq C(\ell). \tag{16}$$

D'après la proposition 4.1, il existe donc une courbe elliptique de conducteur $N(\rho_p^{E_2})$ ayant au moins un point d'ordre 2 sur $\mathbb{Q}$. Les hypothèses faites sur le couple (ℓ, n) entraînent alors une contradiction : dans le cas où $\ell \geq 31$, cela résulte de B. Setzer (*cf.* [39, théorème 2]) et des corollaires des théorèmes 1 à 5 et 7 de [18] (dans le cas où $n = 1$, on notera que si $2\ell^2 - 1$ est un carré on a $\ell \equiv 1 \bmod 4$ (*cf.* [18, lemme 3])). Si $\ell \leq 31$, on le constate en utilisant les tables de [7, 8] (on utilise cette dernière référence si $n = 1$ et $\ell = 19$).

(2) Supposons $s \in S_p(2^{p-n}, \ell^M, 1) \cup S_p(2^{p-n}\ell^M, 1, 1)$. Par hypothèse, on a $p - n \geq 7$. On a ainsi $N(\rho_p^{E_2}) = 2\ell$ (prop. 3.4). L'inégalité (16) est satisfaite. Comme ci-dessus, on déduit de la proposition 4.1 l'existence d'une courbe elliptique sur $\mathbb{Q}$ de conducteur 2ℓ et ayant au moins un point d'ordre 2 sur $\mathbb{Q}$. Les hypothèses faites sur le couple (ℓ, n) conduisent de nouveau à une contradiction. En effet, si ℓ vérifie la propriété (A) ou (B), il n'existe pas de telles courbes elliptiques et il en est de mÃłme si ℓ est congru à 3 ou 5 modulo 8 (*cf.* [7, 18]). D'où le lemme. ∎

Considérons alors un entier $m \geq 1$ et un nombre premier p vérifiant les égalités (3). Supposons qu'il existe un élément

$$(x, y, z) \in S_p(2^n, \ell^m, 1) \cup S_p(2^n\ell^m, 1, 1).$$

(1) Supposons que (x, y, z) appartienne à $S_p(2^n, \ell^m, 1)$. D'après l'assertion (i) du lemme 5.2, il existe deux entiers naturels α et β tels que l'on ait

$$x = \ell^\alpha x_1, \quad y = 2^\beta y_1 \quad \text{avec } (\alpha, \beta) \neq (0, 0),\ x_1 \not\equiv 0 \bmod \ell,\ y_1 \not\equiv 0 \bmod 2.$$

On distingue alors plusieurs cas.

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Supposons $\alpha = 0$. Dans ce cas, on a $\beta \geq 1$ et x est impair. De l'inégalité $p > n$, on déduit que n est pair et que $z = 2^{\frac{n}{2}} z_1$, où z_1 est impair. On a l'égalité

$$2^{p-n}\ell^m(2^{\beta-1}y_1)^p + x^p = z_1^2,$$

d'où il résulte que $(2^{\beta-1}y_1, x, z_1)$ appartient à $S_p(2^{p-n}\ell^m, 1, 1)$. Puisque x est impair et que ℓ ne divise pas x, l'assertion (ii) du lemme 5.2 entraîne ainsi une contradiction.

Supposons $\beta = 0$. On a $\alpha \geq 1$, m est pair et l'on a $z = \ell^{\frac{m}{2}} z_1$, avec z_1 non divisible par ℓ. On a

$$2^n\ell^{p-m}(\ell^{\alpha-1}x_1)^p + y^p = z_1^2,$$

et $(\ell^{\alpha-1}x_1, y, z_1)$ appartient à $S_p(2^n\ell^{p-m}, 1, 1)$. Compte tenu du fait que y est impair et que ℓ ne divise pas y, l'assertion (ii) du lemme 5.2, utilisée avec $M = p - m$, conduit de nouveau à une contradiction.

Supposons $\alpha\beta \neq 0$. Dans ce cas, on a $z = 2^{\frac{n}{2}}\ell^{\frac{m}{2}} z_1$, avec z_1 impair et non divisible par ℓ. On a

$$2^{p-n}(2^{\beta-1}y_1)^p + \ell^{p-m}(\ell^{\alpha-1}x_1)^p = z_1^2,$$

et $(2^{\beta-1}y_1, \ell^{\alpha-1}x_1, z_1)$ appartient à $S_p(2^{p-n}, \ell^{p-m}, 1)$. Par ailleurs, l'hypothèse faite entraîne que ℓ ne divise pas y et que x est impair. On obtient ainsi une contradiction (assertion (i) du lemme 5.2).

(2) Si (x, y, z) appartient à $S_p(2^n\ell^m, 1, 1)$, il existe, d'après le lemme 5.2, deux entiers naturels α et β tels que l'on ait

$$y = 2^\alpha \ell^\beta y_1, \quad \text{avec } (\alpha, \beta) \neq (0, 0),\ y_1 \not\equiv 0 \bmod \ell,\ y_1 \not\equiv 0 \bmod 2.$$

On vérifie, comme ci-dessus, que l'on obtient dans chacun des cas une contradiction.

Cela termine la démonstration du théorème 1.1.

5.2 Démonstration du théorème 1.2

Posons

$$H(\ell) = \left(8\sqrt{\ell + 1} + 1\right)^{16(\ell-1)}.$$

Lemme 5.3 *Soient M un entier naturel non nul et p un nombre premier tels que*

$$p > \mathrm{Max}(M, H(\ell)).$$

Soit (u, v, w) un élément de $S_p(1, \ell^M, 2)$. Alors, ℓ divise u.

Démonstration On suppose que ℓ ne divise pas u, les conditions (C_1)–(C_5) étant satisfaites par (u, v, w) et $(1, \ell^M, 2)$. Soit E_2 la courbe elliptique associée à ces triplets par l'équation (8). On a $p \geq 11$ et $p \neq \ell$, $\rho_p^{E_2}$ est irréductible et l'on a $N(\rho_p^{E_2}) = 256\ell$ (prop. 3.4). On a $g_2^+(256\ell) = 8(\ell - 1)$, d'où l'inégalité

$$\mathrm{Max}\left(F\left(N(\rho_p^{E_2})\right), G\left(N(\rho_p^{E_2})\right)\right) \leq H(\ell).$$

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Il existe donc une courbe elliptique sur $\mathbb{Q}$ de conducteur 256ℓ ayant au moins un point d'ordre 2 rationnel sur $\mathbb{Q}$ (prop. 4.1). Si $\ell \geq 31$, le corollaire du théorème 8 de [18] entraîne une contradiction (on notera que si $\ell \equiv 1 \bmod 8$ et si $\frac{\ell+1}{2}$ n'est pas un carré, tel est aussi le cas de $\frac{\ell^2-1}{2}$; la mÃłme conclusion vaut si $\ell \equiv 3, 7 \bmod 8$ et si $\frac{\ell-1}{2}$ n'est pas un carré). Si $\ell < 31$, on obtient une contradiction en utilisant [7, 8]. D'où le résultat. ∎

Considérons alors un entier $m \geq 1$ et un nombre premier p vérifiant l'inégalité (4). Supposons qu'il existe un élément (x, y, z) de $S_p(1, \ell^m, 2)$. D'après le lemme 5.3, ℓ divise x. Puisque l'on a $m < p$, l'entier m est pair et $2v_\ell(z) = m$. Posons $x = \ell^\alpha x_1$ et $z = \ell^{\frac{m}{2}} z_1$ où l'on a $v_\ell(x_1) = v_\ell(z_1) = 0$. On a l'égalité

$$y^p + \ell^{p-m}(\ell^{\alpha-1}x_1)^p = 2z_1^2,$$

d'où l'on déduit que $(y, \ell^{\alpha-1}x_1, z_1)$ appartient à $S_p(1, \ell^{p-m}, 2)$. L'entier y n'est pas divisible par ℓ. Par suite, le lemme 5.3, utilisé avec $M = p - m$, entraîne une contradiction. D'où le théorème 1.2.

5.3 Démonstration du théorème 1.3

Soient m un entier naturel impair et p un nombre premier. On suppose qu'il existe un élément

$$(x, y, z) \in S_p(2^n, \ell^m, 1) \cup S_p(2^n\ell^m, 1, 1),$$

les conditions (C_1)–(C_5) étant réalisées (*cf.* la condition (5)). Il s'agit de démontrer que p n'appartient pas à un ensemble convenable de nombres premiers de densité > 0. On suppose pour cela, ce qui n'est pas restrictif, que l'on a

$$p > \mathrm{Max}(m, C(\ell)). \tag{17}$$

On choisit un système de représentants $\{A_1, \ldots, A_r\}$ des r classes de $\mathbb{Q}$-isogénie de courbes elliptiques sur $\mathbb{Q}$ de conducteur 2ℓ ayant au moins un point d'ordre 2 sur $\mathbb{Q}$; notons Δ_{A_i} le discriminant minimal de A_i.

On distingue deux cas suivant que n est nul ou non.

5.3.1 Cas où $n = 0$

On peut supposer que (x, y, z) appartient à $S_p(1, \ell^m, 1)$. D'après les remarques 3, on peut associer à (x, y, z) une courbe elliptique F ayant un point d'ordre 2 sur $\mathbb{Q}$ telle que l'on ait $N(\rho_p^F) = 2\ell$ ou 32ℓ. D'après les hypothèses faites sur ℓ, il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ de conducteur 32ℓ ayant au moins un point d'ordre 2 sur $\mathbb{Q}$ (*cf.* [7] et cor. du th. 5 de [18]). On déduit alors de la proposition 4.1, de (17) et de l'alinéa 1 des remarques 3 que xy est pair et que l'une des assertions suivantes est vérifiée :

(i) y est pair et il existe $h \in \{1, \ldots, r\}$ tel que le module $A_h[p]$ soit isomorphe à $E_1[p]$;

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

(ii) y est impair, x est pair et il existe $k \in \{1, \dots, r\}$ tel que $A_k[p]$ soit isomorphe à $E_2[p]$.

Si y est pair, E_1 a réduction multiplicative en 2 et en ℓ (lemmes 2.1 et 2.2). D'après le corollaire 2.3, on a dans ce cas :

$$\Delta_{E_1} = 2^{-6}\ell^m(x^2y)^p.$$

Par ailleurs, si y est impair et x est pair, E_2 a aussi réduction multiplicative en 2 et en ℓ (lemmes 2.4 et 2.5) et l'on a (cor. 2.6) :

$$\Delta_{E_2} = 2^{-6}\ell^{2m}(xy^2)^p.$$

Pour tout $i \in \{1, \dots, r\}$, posons

$$n_i = -6m\, v_2(\Delta_{A_i})v_\ell(\Delta_{A_i}) \quad \text{et} \quad t_i = 2n_i.$$

En utilisant la proposition 4.3, avec $\ell_1 = 2$ et $\ell_2 = \ell$, on déduit de l'assertion (i) ou (ii) que l'on a :

$$\left(\frac{n_h}{p}\right) = 1 \quad \text{ou} \quad \left(\frac{t_k}{p}\right) = 1. \tag{18}$$

Considérons alors l'ensemble $\mathcal{P}_1$ des nombres premiers q tels que

$$\left(\frac{n_i}{q}\right) = -1 \quad \text{pour tout } i \in \{1, \dots, r\},$$

et l'ensemble $\mathcal{P}_2$ des nombres premiers q tels que

$$\left(\frac{t_i}{q}\right) = -1 \quad \text{pour tout } i \in \{1, \dots, r\}.$$

Posons $\mathcal{P} = \mathcal{P}_1 \cap \mathcal{P}_2$. D'après la condition (18), p n'appartient pas à $\mathcal{P}$. Tout revient alors à démontrer que $\mathcal{P}$ est de densité $1/2^s$ pour un certain entier $s \leq 2r$. D'après le théorème de densité de Chebotarev, il suffit pour cela de vérifier que $\mathcal{P}$ n'est pas vide. Soit S l'ensemble des nombres premiers q vérifiant les deux conditions suivantes :

(1) on a $q \equiv 7 \bmod 8$;
(2) on a $(u/q) = 1$ pour tout diviseur premier impair u divisant le produit des n_i : par exemple $q \equiv -1 \bmod u$ pour ces nombres premiers u.

L'ensemble S est contenu dans $\mathcal{P}_1$. Par ailleurs, si q est dans S, 2 est un carré dans $\mathbb{F}_q$ et l'on a l'égalité

$$\left(\frac{t_i}{q}\right) = \left(\frac{n_i}{q}\right) \quad \text{pour tout } i \in \{1, \dots, r\}.$$

Par suite, S est aussi contenu dans $\mathcal{P}_2$. Puisque S est non vide, cela prouve notre assertion. D'où le théorème si $n = 0$.

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

5.3.2 Cas où $n \in \{1, 3, 5\}$

Posons $t := (x, y, z)$. Soit E_2 la courbe elliptique associée à t et l'un des triplets $(2^n, \ell^m, 1)$ et $(2^n\ell^m, 1, 1)$. D'après la proposition 3.4, on a $N\big(\rho_p^{E_2}\big) = 2\ell$, 8ℓ, 32ℓ ou 128ℓ. Il résulte des hypothèses faites sur ℓ et des propositions 3.4 et 4.1, que l'on a $N\big(\rho_p^{E_2}\big) = 2\ell$ (*cf.* [7, 8] et cor. des th. 3, 5 et 7 de [18]). La courbe E_2 a donc réduction multiplicative en 2 et ℓ, et l'on a :

$$\Delta_{E_2} = \begin{cases} 2^{n-6}\ell^{2m}(xy^2)^p & \text{si } t \in S_p(2^n, \ell^m, 1), \\ 2^{n-6}\ell^m(xy^2)^p & \text{si } t \in S_p(2^n\ell^m, 1, 1). \end{cases}$$

Pour tout $i \in \{1, \dots, r\}$, posons

$$n_i = \begin{cases} 2m(n-6)\, v_2(\Delta_{A_i})v_\ell(\Delta_{A_i}) & \text{si } t \in S_p(2^n, \ell^m, 1), \\ m(n-6)v_2(\Delta_{A_i})v_\ell(\Delta_{A_i}) & \text{si } t \in S_p(2^n\ell^m, 1, 1). \end{cases}$$

On déduit des propositions 4.1 et 4.3 l'existence de $h \in \{1, \dots, r\}$ tel que

$$\left(\frac{n_h}{p}\right) = 1.$$

Par suite, p n'appartient pas à l'ensemble des nombres premiers q tels que

$$\left(\frac{n_i}{q}\right) = -1 \quad \text{pour tout } i \in \{1, \dots, r\},$$

dont on vérifie qu'il est de densité $1/2^s$ avec $s \leq r$. D'où le théorème 1.3.

6 Description de $S_p(4, 1, 3)$

Étant donnés trois entiers non nuls a, b et c, premiers entre eux, on supposera pour toute la suite, sans autre précision, que les éléments de $S_p(a, b, c)$ que l'on considérera vérifient la condition (C_3). Étant donné $s \in S_p(a, b, c)$, les conditions (C_1)–(C_5) étant implicitement satisfaites, on notera désormais $E_1(s)$ et $E_2(s)$ les courbes elliptiques associées à s et (a, b, c) respectivement par les équations (6) et (8), sans préciser le triplet (a, b, c), ou plus simplement E_1 et E_2 si le contexte ne prÃłte pas à confusion. Par ailleurs, pour toute courbe elliptique $E/\mathbb{Q}$ on notera Δ_E son discriminant minimal, j_E son invariant modulaire, ρ_p^E la représentation donnant l'action de $G_\mathbb{Q}$ sur le groupe $E[p]$ des points de p-torsion de E et $a_n(E)$ le n-ième coefficient de la fonction L de Hasse–Weil de E.

Rappelons le résultat bien connu suivant, qui est une conséquence de la théorie de la courbe de Tate (*cf.* [40, p. 355]) :

Lemme 6.1 *Soient $A/\mathbb{Q}$ une courbe elliptique et ℓ, p deux nombres premiers distincts. Supposons que A ait en ℓ réduction additive et que $v_\ell(j_A) < 0$. Soit n_ℓ l'ordre de l'image par ρ_p^A d'un sous-groupe d'inertie en ℓ de $G_\mathbb{Q}$. On a $n_\ell = 2$ si p divise $v_\ell(j_A)$ et $n_\ell = 2p$ sinon.*

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Soit p un nombre premier ≥ 7. On va démontrer que l'on a

$$S_p(4,1,3) = \{(1,-1,1),(1,-1,-1)\}. \tag{19}$$

On considère un élément $t := (x,y,z)$ de $S_p(4,1,3)$.

(1) Prouvons que y est impair. Supposons que y soit pair. Posons $n = v_2(y)$. Il existe deux entiers impairs y_1 et z_1, premiers entre eux, tels que l'on ait $y = 2^n y_1$ et $z = 2z_1$. On a l'égalité

$$2^{p-2}(2^{n-1}y_1)^p + x^p = 3z_1^2,$$

autrement dit, $s := (2^{n-1}y_1, x, z_1)$ appartient à $S_p(2^{p-2},1,3)$. La représentation $\rho_p^{E_2(s)}$ est irréductible de poids 2 (prop. 3.1 et 3.2) et l'on a (prop. 3.4) :

$$N\big(\rho_p^{E_2(s)}\big) = \begin{cases} 18 & \text{si } n \geq 2 \text{ ou } p \geq 11, \\ 72 & \text{si } n = 1 \text{ et } p = 7. \end{cases}$$

On a $g_2^+(18) = 0$ et $g_2^+(72) = 1$. Par suite, on a $n = 1$, $p = 7$ et $\rho_7^{E_2(s)}$ est isomorphe à ρ_7^E, où E est la courbe elliptique notée 72A1 dans les tables de [7]. La courbe E a réduction additive en 3, et l'on a $v_3(j_E) = -1$. D'après le lemme 6.1, l'image par ρ_7^E d'un sous-groupe d'inertie en 3 de $G_{\mathbb{Q}}$ est d'ordre 14. Par ailleurs, $E_2(s)$ a réduction additive en 3 et $j_{E_2(s)}$ est entier en 3. Le défaut de semi-stabilité de $E_2(s)$ en 3 étant d'ordre 4 ou 12 (lemme 2.4 et [21, p. 356]), cela conduit à une contradiction. D'où notre assertion.

Les conditions (C_1)–(C_5) sont donc satisfaites par t et $(4,1,3)$.

(2) L'entier x est impair : en effet, dans le cas contraire, $\rho_p^{E_2(t)}$ serait irréductible de poids 2 et de conducteur 18, ce qui n'est pas car $g_2^+(18) = 0$.

(3) Prouvons maintenant l'égalité (19). Puisque x est impair, on a :

$$N\big(\rho_p^{E_2(t)}\big) = \begin{cases} 36 & \text{si } x \equiv 1 \bmod 4, \\ 144 & \text{si } x \equiv -1 \bmod 4. \end{cases}$$

On a $g_2^+(36) = 1$ et $g_2^+(144) = 2$. Par ailleurs, il existe deux classes de $\mathbb{Q}$-isogénie de courbes elliptiques de conducteur 144 (*cf.* [7, p. 124]). On en déduit que $\rho_p^{E_2(t)}$ est isomorphe à ρ_p^F, où F est une courbe elliptique de conducteur 36 ou 144. On peut supposer que F est l'une des trois courbes elliptiques notées 36A1, 144A1 et 144B1 dans les tables de [7]. Le cas où F est la courbe 144B1 ne peut se produire : on le vérifie en utilisant le lemme 6.1, en remarquant que l'invariant modulaire de la 144B1 n'est pas entier en 3. Ainsi, $\rho_p^{E_2(t)}$ est isomorphe à ρ_p^F, où F est l'une des courbes 36A1 et 144A1. Ces courbes sont à multiplications complexes par l'anneau d'entiers de $\mathbb{Q}(\sqrt{-3})$. Il en résulte que l'image de $\rho_p^{E_2(t)}$ est contenue dans le normalisateur d'un sous-groupe de Cartan C de $\mathrm{Aut}(E_2(t)[p])$ (*cf.* [36]).

Supposons $p \equiv 1 \bmod 3$. Dans ce cas, C est déployé. Si l'on a $p \geq 17$, les conducteurs de F et $E_2(t)$ sont égaux (*cf.* [14]) ; puisque xy est impair, le lemme 2.4 entraîne alors $xy = \pm 1$, puis $x = 1$, $y = -1$, et le résultat. Supposons $p = 13$. La courbe $E_2(t)$

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

correspond alors à un point de la courbe modulaire $X_0(26)$ rationnel sur $\mathbb{Q}(\sqrt{-3})$. Par ailleurs, la jacobienne $J_0(26)$ de $X_0(26)$ est isogène sur $\mathbb{Q}$ au produit des courbes elliptiques notées 26A1 et 26B1 dans les tables de [7]. Les tordues quadratiques de ces courbes par $\sqrt{-3}$ sont de rang 0 sur $\mathbb{Q}$. En particulier, $J_0(26)$ possède un quotient non trivial de rang 0 sur $\mathbb{Q}(\sqrt{-3})$. Compte tenu du fait que xy est impair, il résulte alors de [30, corollaire 4.3] que l'on a de nouveau $xy = \pm 1$. Le mÃłme argument vaut si $p = 7$, car la tordue quadratique par $\sqrt{-3}$ de la courbe elliptique $Y_0(14)$, notée 14A1 dans [7], est aussi de rang 0 sur $\mathbb{Q}$.

Supposons $p \equiv 2 \bmod 3$. Dans ce cas, C est non déployé et $E_2(t)$ ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, $j_{E_2(t)}$ appartient à $\mathbb{Z}[1/p]$ (*cf.* [12]). Par ailleurs, on a

$$j_{E_2(t)} = \frac{2^4.3^3.(4z^2 - y^p)^3}{(xy^2)^p}.$$

On vérifie que xy et $6(4z^2 - y^p)$ sont premiers entre eux. Par suite, xy est une puissance de p. Si p divise xy, la courbe $E_2(t)$ a réduction multiplicative en p et l'on a $a_p(E_2(t)) = \pm 1$. On en déduit que $a_p(F) \equiv \pm 1 \bmod p$. Cela conduit à une contradiction, car on a $a_p(F) = 0$. D'où le résultat dans ce cas et l'égalité (19).

7 Exemples numériques

Nous allons illustrer dans ce paragraphe la méthode modulaire et ses compléments afin de résoudre le problème énoncé dans l'introduction dans certains cas particuliers. On explicitera par ailleurs numériquement le théorème 1.3 sur quelques exemples. Pour chacun d'entre eux, les calculs nécessaires ont été réalisés à l'aide du logiciel PARI (*cf.* [2]) et du programme metmod (*cf.* [31]).

Exemple 1 On considère l'équation

$$x^p + 7y^p = z^2.$$

On ne sait pas démontrer l'existence d'une infinité de nombres premiers p pour lesquels $S_p(1, 7, 1)$ soit vide. Signalons que J.-L. Lesage avait démontré qu'il n'existe pas de solutions avec $y = -1$ si $p > 10^{16}$ (*cf.* [28]), et que Y. Bugeaud, M. Mignotte et S. Siksek ont étendu récemment ce résultat aux nombres premiers $p \geq 11$. En revanche, si l'on se donne p explicitement, la méthode de réduction est un moyen efficace de prouver que $S_p(1, 7, 1)$ est vide.

Considérons un nombre premier $p \geq 11$. Soit (x, y, z) un élément de $S_p(1, 7, 1)$. D'après l'alinéa 1 des remarques 3, la représentation ρ_p^F est irréductible de poids 2 et $N(\rho_p^F) = 14$ ou 224 selon xy est pair ou non. On a $g_2^+(14) = 1$ et $g_2^+(224) = 6$. Il existe deux classes de $\mathbb{Q}$-isogénie de courbes elliptiques de conducteur 224. Par ailleurs, à conjugaison près par un élément de $G_{\mathbb{Q}}$, il existe deux newforms normalisées f et g de $S_2^+(224)$ dont les q-développements sont à coefficients dans $\mathbb{Q}(\sqrt{5})$. On peut supposer que $a_3(f) = 1 + \sqrt{5}$ et $a_3(g) = -1 + \sqrt{5}$. En utilisant les congruences (10) et (11) avec $\ell = 3$, on vérifie alors que, lorsque $N(\rho_p^F) = 224$,

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

la représentation ρ_p^F ne provient pas de f ni de g. Par suite, ρ_p^F est isomorphe à ρ_p^E, où E est l'une des courbes elliptiques notées 14A1, 224A1 et 224B1 dans les tables de [7].

En utilisant la méthode de réduction, on constate que :

$$S_p(1,7,1) \text{ est vide si l'on a } 11 \leq p < 10^4.$$

Afin de vérifier cette assertion, pour chacune des courbes E ci-dessus et chaque nombre premier p, on a explicité le plus petit entier $n(E) \geq 1$ tel que les conditions suivantes soient satisfaites (*cf.* le lemme 4.2) :

(i) $q = n(E)p + 1$ est premier ;
(ii) $a_q(E) \not\equiv \pm 2 \mod p$;
(iii) pour $i = 1$ et $i = 2$, on a :

$$a_q(E) \not\equiv \widetilde{a(E_i, \xi)} \mod p \quad \text{pour tout} \quad \xi \in R_q.$$

Compte tenu du fait que les courbes 224A1 et 224B1 se déduisent l'une de l'autre par torsion quadratique par $\sqrt{-1}$, il suffit d'expliciter $n(E)$ pour les courbes 14A1 et 224A1. À titre indicatif, on détermine $n(E)$ dans le tableau ci-dessous, pour les nombres premiers $p < 80$.

p	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79
n(14A1)	2	10	8	10	2	60	48	4	2	4	6	60	12	6	28	18	4	34
n(224A1)	2	12	66	12	2	2	46	6	62	4	6	2	12	6	30	12	4	4

Pour les nombres premiers $p < 10^4$, le plus grand entier $n(E)$ utilisé est $n(E) = 102$ si E est la courbe $14A1$ et $p = 211$, et $n(E) = 76$ si E est la courbe $224A1$ et $p = 5227$.

Exemple 2 On démontre ici l'assertion suivante :

$$S_{11}(1, 11^m, 1) \quad \text{est vide si l'on a } 1 \leq m \leq 10. \tag{20}$$

On utilise pour cela la méthode de réduction qui est la seule qui nous a permis de conclure. Supposons qu'il existe un élément $(x, y, z) \in S_{11}(1, 11^m, 1)$.

(1) Vérifions que 11 divise x. On suppose le contraire. Les conditions (C_1)–(C_5) sont alors satisfaites. Les représentations $\rho_{11}^{E_1}$ et $\rho_{11}^{E_2}$ sont irréductibles, de poids 12, et l'on est dans l'un des cas suivants :

(i) y est pair et $N(\rho_{11}^{E_1}) = 2$;
(ii) on a $x \equiv -1 \mod 4$, y est impair et $N(\rho_{11}^{E_1}) = 32$;
(iii) x est pair et $N(\rho_{11}^{E_2}) = 2$;
(iv) on a $x \equiv 1 \mod 4$, y est impair et $N(\rho_{11}^{E_2}) = 32$.

On a $g_{12}^+(2) = 0$ et $g_{12}^+(32) = 11$. Par suite, on est dans l'un des cas (ii) et (iv). Il existe ainsi une newform normalisée $f \in S_{12}^+(32)$ et une place $\mathfrak{P}$ de $\overline{\mathbb{Q}}$ de caractéristique résiduelle 11 telles que les congruences (10) et (11) soient satisfaites avec E_1 ou E_2. En utilisant les tables de Stein, on constate que f est l'un des éléments

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

notés $32k12A1, \ldots, 32k12E1$ (*cf.* [41]). On vérifie alors que cela n'est possible que si f est la newform $32k12A1$. La méthode de réduction utilisée avec

$$q = \begin{cases} 23 & \text{si } m \in \{1,4,5,6,7,10\}, \\ 67 & \text{si } m \in \{3,8\}, \\ 331 & \text{si } m \in \{2,9\}, \end{cases}$$

permet alors d'écarter cette newform. D'où une contradiction et le fait que 11 divise x.

(2) Comme dans la démonstration du théorème 1.1 (si $n = 0$), on déduit de là l'existence de deux entiers u et v tels que (y, u, v) appartienne à $S_{11}(1, 11^{11-m}, 1)$. Puisque 11 ne divise pas y, l'alinéa précédent entraîne une contradiction. D'où l'assertion (20).

Exemple 3 On poursuit ici l'exemple 2, si $m = 1$, en précisant que :

$$S_p(1, 11, 1) \text{ est vide si } p \geq 7.$$

On peut supposer $p \neq 11$ (exemple 2). Supposons qu'il existe $(x, y, z) \in S_p(1, 11, 1)$. Dans ce cas, la représentation ρ_p^F est de poids 2, et l'on a $N(\rho_p^F) = 22$ ou 352 selon que xy est pair ou non (*cf.* remarques 3). On a $g_2^+(22) = 0$ et $g_2^+(352) = 10$. Puisque $g_2^+(22) = 0$, on a donc $N(\rho_p^F) = 352$. Si l'on a $p \geq 13$, en utilisant les tables de Stein, on contredit alors directement les congruences (10) et (11) avec le nombre premier $\ell = 3$ ou $\ell = 5$. Si $p = 7$, la méthode de réduction permet de conclure.

Exemple 4 Bennett et Skinner (*cf.* [3]) ont démontré que $S_p(1, 5, 2)$ est vide dès que l'on a $p \geq 11$. Vérifions ici que $S_7(1, 5, 2)$ est vide. Supposons qu'il existe un élément de $S_7(1, 5, 2)$. La représentation $\rho_7^{E_1}$ correspondante est irréductible de poids 2 et de conducteur $2^8.5$. Soient $f \in S_2^+(1280)$ et $\mathfrak{P}$ une place de $\overline{\mathbb{Q}}$ au-dessus de 7, vérifiant (10) et (11). On a $g_2^+(1280) = 32$. On obtient directement une contradiction sauf si f est l'une des newforms notées $1280A1$, $1280D1$, $1280E1$, $1280I1$, $1280J1$ ou $1280N1$ dans les tables de Stein. On élimine ensuite ces newforms en utilisant la méthode de réduction : avec le nombre premier $q = 43$ si f est la $1280A1$ ou $1280D1$, et avec $q = 29$ dans les autres cas. D'où l'assertion.

Exemple 5 On va préciser le théorème 1.3 si $\ell = 23$ et $n = 0$. Soient m un entier naturel impair et p un nombre premier tels que $p \geq 11$, $p \neq 23$ et $m < p$. Vérifions que :

(21) $S_p(1, 23^m, 1)$ est vide si $-15m$ et $-30m$ ne sont pas des carrés dans $\mathbb{F}_p$.

On considère pour cela un élément $(x, y, z) \in S_p(1, 23^m, 1)$. La représentation ρ_p^F est de poids 2, et l'on a $N(\rho_p^F) = 46$ ou 736 selon que xy est pair ou non. On a $g_2^+(46) = 1$ et $g_2^+(736) = 22$. On ne peut pas avoir $N(\rho_p^F) = 736$: on utilise les tables de Stein et on contredit les congruences (10) et (11). Soit E la courbe notée 46A1

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

dans [7]. On en déduit que ρ_p^E est isomorphe à $\rho_p^{E_1}$ ou $\rho_p^{E_2}$. On a $\Delta_E = -2^{10}.23$. La proposition 4.3 entraîne alors (21).

À titre indicatif, si $m = 1$ on en déduit que :

$$S_p(1, 23, 1) \text{ est vide si } p \equiv 7, 41, 71, 73, 89, 97, 103, 119 \bmod 120 \text{ et } p \neq 7.$$

Par ailleurs, en utilisant la méthode de réduction, on constate que :

$$S_p(1, 23, 1) \text{ est vide si l'on a } 13 \leq p < 10^4 \text{ et } p \neq 23.$$

Pour le vérifier, on procède comme dans l'exemple 1 ci-dessus avec la courbe E. Avec ses notations, le plus grand entier $n(E)$ utilisé si $p < 10^4$ est 96 pour $p = 5641$. Notons que $(2, -1, 45)$ appartient à $S_{11}(1, 23, 1)$. On ne sait pas décider si $S_7(1, 23, 1)$ est vide ou non.

Exemple 6 On explicite ici le théorème 1.3 pour $\ell = 19249$, qui est congru à 1 modulo 8, et $n = 1$. L'entier ℓ ne vérifie pas la propriété (A) : on a $\ell - 2^{10} = 135^2$. Par suite, ℓ ne vérifie pas les hypothèses faites dans le théorème 1.1. Néanmoins, dès que p est assez grand, par exemple si $p > C(\ell)$, on a les implications suivantes :

$$p \equiv 11, 13, 17, 19 \bmod 20 \Longrightarrow S_p(2, \ell, 1) \text{ est vide,} \tag{22}$$

$$p \equiv 3, 17, 21, 27, 29, 31, 33, 39 \bmod 40 \Longrightarrow S_p(2\ell, 1, 1) \text{ est vide.} \tag{23}$$

En effet, soit $t := (x, y, z)$ un élément de $S_p(2, \ell, 1) \cup S_p(2\ell, 1, 1)$ où $p \geq 7$ et $p \neq \ell$. La représentation $\rho_p^{E_2}$ associée à t et $(2, \ell, 1)$ ou $(2\ell, 1, 1)$ est de poids 2 et l'on a $N(\rho_p^{E_2}) = 2\ell$ si x est pair et 128ℓ sinon. D'après [18], il existe une unique classe de $\mathbb{Q}$-isogénie de courbes elliptiques sur $\mathbb{Q}$ de conducteur 2ℓ ayant un point d'ordre 2 sur $\mathbb{Q}$. Cette classe est représentée par la courbe elliptique $E/\mathbb{Q}$ d'équation minimale (*cf.* [18]) :

$$Y^2 + XY + Y = X^3 - X^2 - 396X - 2929.$$

On a $\Delta_E = 2^8\ell$. Par ailleurs, il n'existe pas de courbes elliptiques sur $\mathbb{Q}$ de conducteur 128ℓ ayant un point d'ordre 2 sur $\mathbb{Q}$ (*cf.* [18]). On en déduit que si $p > C(\ell)$ les représentations ρ_p^E et $\rho_p^{E_2}$ sont isomorphes (prop. 4.1). D'après le corollaire 2.6, on a

$$\Delta_{E_2} = \begin{cases} 2^{-5}\ell^2(xy^2)^p & \text{si } t \in S_p(2, \ell, 1), \\ 2^{-5}\ell(xy^2)^p & \text{si } t \in S_p(2\ell, 1, 1). \end{cases}$$

La proposition 4.3 entraîne alors les implications (22) et (23). On obtient ainsi des ensembles de nombres premiers p de densité $1/2$ pour lesquels $S_p(2, \ell, 1)$ et $S_p(2\ell, 1, 1)$ sont vides.

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

8 Sur les points rationnels des courbes $y^2 = x^p + d$

Étant donnés un nombre premier $p \geq 5$ et un entier non nul d, on désigne par $C_{d,p}$ la courbe définie sur $\mathbb{Q}$ d'équation

$$C_{d,p} : y^2 = x^p + d.$$

C'est une courbe hyperelliptique lisse de genre $\frac{p-1}{2}$. Comme conséquence des résultats obtenus dans les paragraphes précédents, on se propose ici de faire quelques remarques sur la description des points rationnels sur $\mathbb{Q}$ des courbes $C_{d,p}$. Dans ce qui suit, on note ε l'un des entiers -1 et 1.

8.1 Lien entre $S_p(1, d, 1)$ et $C_{d,p}(\mathbb{Q})$, $C_{-d,p}(\mathbb{Q})$ $(d > 0)$

On considère un entier $d \geq 1$ et un nombre premier $p \geq 5$.

Lemme 8.1 *Soit (x, y) un point de $C_{\varepsilon d,p}(\mathbb{Q})$. Supposons qu'il n'existe pas d'éléments $(\alpha, \beta, \gamma) \in S_p(1, d, 1)$ tels que $\varepsilon\beta$ soit un carré. Alors, on a $xy = 0$.*

Démonstration Il existe des entiers u, v, w tels que $\text{pgcd}(u, v) = 1$, $\text{pgcd}(w, v) = 1$ et

$$x = \frac{u}{v^2} \quad \text{et} \quad y = \frac{w}{v^p}.$$

On en déduit l'égalité

$$w^2 = u^p + d(\varepsilon v^2)^p. \tag{24}$$

Si xy est non nul, on a $uw \neq 0$ et $(u, \varepsilon v^2, w)$ appartient alors à $S_p(1, d, 1)$, ce qui contredit l'hypothèse faite. D'où le lemme. ∎

Corollaire 8.2 *Soit (x, y) un point de $C_{\varepsilon d,p}(\mathbb{Q})$. Si $S_p(1, d, 1)$ est vide, on a $xy = 0$.*

Il résulte par ailleurs de la démonstration du lemme 8.1 que la description de $S_p(1, d, 1)$ permet la détermination des ensembles $C_{-d,p}(\mathbb{Q})$ et $C_{d,p}(\mathbb{Q})$.

8.2 Applications

Soient ℓ un nombre premier impair et m, n deux entiers naturels. Posons $d = 2^n \ell^m$. En application des résultats obtenus on peut parfois décrire les ensembles $C_{\varepsilon d,p}(\mathbb{Q})$. Le théorème 1.1 et le corollaire 8.2 entraînent le résultat suivant :

Corollaire 8.3 *Soit (x, y) un point de $C_{\varepsilon d,p}(\mathbb{Q})$. Supposons $m \geq 1$ et que (ℓ, n) vérifie l'une des quatre conditions de l'énoncé du théorème* 1.1. *Alors, si p est assez grand, par exemple si p vérife les inégalités* (3), *on a $xy = 0$.*

Dans le cas où $m = 0$, on déduit de [17, théorème 1] l'énoncé suivant :

Corollaire 8.4 *Supposons $m = 0$, $p \geq 7$ et $n < p$. Soit (x, y) un point de $C_{\varepsilon d,p}(\mathbb{Q})$.*

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

(1) *Si n est distinct de* 1, 3, $p-3$ *et* $p-1$, *on a* $xy=0$.
(2) *L'ensemble* $C_{-8,p}(\mathbb{Q})$ *est vide et l'on a* $C_{8,p}(\mathbb{Q})=\{(1,-3),(1,3)\}$.
(3) *Si* $n=p-3$, $C_{-d,p}(\mathbb{Q})$ *est vide et l'on a* $C_{d,p}(\mathbb{Q})=\{(2,-3.2^{\frac{p-3}{2}}),(2,3.2^{\frac{p-3}{2}})\}$.

8.3 Sur l'ensemble $C_{-3,p}(\mathbb{Q})$

Parmi les nombres premiers ℓ congrus à 3 modulo 8, l'entier $\ell=3$ est le seul pour lequel on ne dispose d'aucune information sur la description de $S_p(1,\ell,1)$. Que peut-on néanmoins démontrer quant à la détermination $C_{-3,p}(\mathbb{Q})$ et $C_{3,p}(\mathbb{Q})$? L'étude de $C_{3,p}(\mathbb{Q})$ s'avère plus difficile que celle de $C_{-3,p}(\mathbb{Q})$; cela est dû au fait que les points $(1,-2)$ et $(1,2)$ appartiennent à $C_{3,p}(\mathbb{Q})$ et l'on est dans ce cas dans une situation analogue à celle de la conjecture 2. Nous ne savons pas décider si ce sont les seuls points de $C_{3,p}(\mathbb{Q})$. En revanche, on dispose de quelques informations sur $C_{-3,p}(\mathbb{Q})$, que l'on va décrire dans ce qui suit.

On ne sait pas prouver que $C_{-3,p}(\mathbb{Q})$ est vide pour une infinité de p. Néanmoins, le nombre premier p étant donné, la méthode de réduction permet de démontrer assez facilement que $C_{-3,p}(\mathbb{Q})$ est vide, y compris si $p=5$. Par exemple :

(25) $\qquad C_{-3,p}(\mathbb{Q})$ est vide si l'on a $5\leq p<10^4$.

Pour vérifier cette assertion, on procède comme suit : supposons $C_{-3,p}(\mathbb{Q})$ non vide. D'après l'égalité (24), il existe des entiers non nuls u, v et w, premiers entre eux dans leur ensemble, tels que l'on ait $w^2=u^p-3v^{2p}$ et $s:=(u,-v^2,w)$ appartient à $S_p(1,3,1)$.

Afin de démontrer que $C_{-3,5}(\mathbb{Q})$ est vide, on est amené à prouver l'énoncé suivant :

Lemme 8.5 *La représentation $\rho_5^{E_1(s)}$ est irréductible.*

Démonstration Supposons le contraire. Dans ce cas $E_1(s)$ possède un sous-groupe C d'ordre 5 stable par $G_{\mathbb{Q}}$. Posons $K=\mathbb{Q}(\sqrt{-3})$. Soit Δ le discriminant de $E_1(s)$ définie par l'équation (6). On a

$$\Delta=-3.2^6.(uv)^{10}.$$

Par suite, $E_1(s)$ a tous ses points d'ordre 2 rationnels sur K. Il en résulte que $E_1(s)$ contient un sous-groupe isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2\times C$ stable par le groupe de Galois de $\overline{\mathbb{Q}}$ sur K.

Considérons alors la courbe modulaire Y qui paramètre les classes d'isomorphisme de couples $(E,(\mathbb{Z}/2\mathbb{Z})^2\times H)$, où E est une courbe elliptique et $(\mathbb{Z}/2\mathbb{Z})^2\times H$ un sous-module galoisien de E, H étant un sous-groupe stable d'ordre 5. La compactifiée lisse de Y est une courbe elliptique X définie sur $\mathbb{Q}$. Un modèle de X est la complétée projective de l'équation

$$y^2=x^3+x^2+4x+4,$$

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

qui est la courbe notée 20A1 dans [7]. [16]). Elle possède exactement six points rationnels sur $\mathbb{Q}$, qui sont des pointes, et qui forment ainsi le complémentaire de Y dans X.

On déduit de ce qui précède que le couple $(E_1(s), (\mathbb{Z}/2\mathbb{Z})^2 \times C)$ correspond à un point de $Y(K)$. Par ailleurs, la tordue quadratique de X par $\sqrt{-3}$ est une courbe elliptique de rang 0 sur $\mathbb{Q}$. Par suite, $X(K)$ est de rang 0. On vérifie alors que l'on a $X(K) = X(\mathbb{Q})$: en effet, Y a bonne réduction en les deux places de K au-dessus de 7 et le nombre de points de la réduite de X modulo une de ces places est égal à 6. On en déduit que $Y(K)$ est vide, d'où une contradiction et le lemme. ■

D'après la proposition 3.1 et le lemme 8.5, $\rho_p^{E_1(s)}$ est irréductible pour tout $p \geq 5$. Son poids vaut 2. Par ailleurs, l'égalité $w^2 = u^p - 3v^{2p}$ entraîne $u \equiv 1 \bmod 2$. On en déduit que v est impair : sinon v est pair et l'on a alors $N\left(\rho_p^{E_1(s)}\right) = 6$ (prop. 3.3), ce qui conduit à une contradiction car $g_2^+(6) = 0$. Ainsi uv est impair, et cela entraîne $u \equiv -1 \bmod 4$. Il en résulte que l'on a

$$N\left(\rho_p^{E_1(s)}\right) = 96.$$

On a $g_2^+(96) = 2$. Par suite, $\rho_p^{E_1(s)}$ est isomorphe à ρ_p^E, où E est l'une des courbes elliptiques notée 96A1 et 96B1 dans [7]. Ces courbes elliptiques se déduisant l'une de l'autre par torsion quadratique par $\sqrt{-1}$, on peut supposer que E est la 96A1. Elle possède tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$. La méthode de réduction permet alors de contredire cette situation si l'on a $5 \leq p < 10^4$. D'où l'assertion (25).

Pour les nombres premiers p tels que $2p+1$ soit premier, on a l'énoncé ci-dessous. On note E la courbe 96A1 et $F/\mathbb{Q}$ la courbe elliptique, de conducteur 768, d'équation

$$y^2 = x^3 - 4x^2 - 2x.$$

Lemme 8.6 *Supposons que $q := 2p+1$ soit un nombre premier et que l'une des conditions suivantes soit réalisée :*

(1) *on a $p \equiv 3 \bmod 4$;*
(2) *on a $a_q(F)^2 \neq a_q(E)^2$.*

Alors, $C_{-3,p}(\mathbb{Q})$ est vide.

Démonstration On suppose que $C_{-3,p}(\mathbb{Q})$ est non vide. Il existe alors des entiers u, v et w tels que $s := (u, -v^2, w)$ appartienne à $S_p(1, 3, 1)$.

Vérifions que $E_1(s)$ a bonne réduction en q. Comme ci-dessus, on peut supposer que $\rho_p^{E_1(s)}$ est isomorphe à ρ_p^E. Puisque E a bonne réduction en q, il suffit donc de vérifier que l'on a (condition (iii) du §4.1) :

$$a_q(E) \not\equiv \pm 2 \bmod p. \tag{26}$$

Si n_q désigne le nombre de points sur $\mathbb{F}_q$ de la réduite de E modulo q, on a $a_q(E) = q + 1 - n_q$ *i.e.*, $a_q(E) = 2(p+1) - n_q$. La courbe E ayant tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$, l'entier n_q est divisible par 4. Par suite, on a

$$a_q(E) \equiv 0 \bmod 4. \tag{27}$$

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

D'après l'inégalité $|a_q(E)| \leq 2\sqrt{q}$ (*cf.* [40, p. 131]), on a $|a_q(E) \pm 2| \leq 2(\sqrt{q}+1)$, d'où l'on déduit que $|a_q(E) \pm 2| < p$ (cette inégalité est aussi vraie si $p = 11$ car $a_{23}(E) = 0$). Cela entraîne (26) : en effet, dans le cas contraire, on aurait $a_q(E) = \pm 2$, ce qui contredit (27). D'où notre assertion.

Il en résulte que q ne divise pas uv. De l'égalité $u^p - 3v^{2p} = w^2$, on déduit alors que -1 ou -2 est un carré dans $\mathbb{F}_q$. Puisque 4 ne divise pas $q-1$ on obtient que

$$-2 \text{ est un carré dans } \mathbb{F}_q. \tag{28}$$

Par ailleurs, on en déduit les congruences,

$$u^p \equiv 1 \bmod q \quad \text{et} \quad w^2 \equiv -2 \bmod q. \tag{29}$$

(1) Si $p \equiv 3 \bmod 4$, on a $q \equiv 7 \bmod 8$, ce qui contredit (28). D'où le résultat dans ce cas.

(2) Supposons réalisée la condition 2 de l'énoncé. Soit $\sqrt{w}$ une racine carrée de w dans $\overline{\mathbb{Q}}$. En posant $\alpha = wx$ et $\beta = \sqrt{w}^3 y$, on constate que $E_1(s)$ est isomorphe sur $\mathbb{Q}(\sqrt{w})$ à la courbe elliptique $A/\mathbb{Q}$ d'équation

$$\beta^2 = \alpha^3 + 2w^2\alpha^2 + u^p w^2 \alpha.$$

Le discriminant de A est $-2^6.3.(uv)^{2p}.w^6$. D'après (29), q ne divise pas w. Ainsi, A a bonne réduction en q, et $E_1(s)$ ayant aussi bonne réduction en q, on a donc

$$a_q(A) = \pm a_q(E_1(s)). \tag{30}$$

Il résulte de (29) que les courbes elliptiques sur $\mathbb{F}_q$ déduites de F et A par réduction sont les mêmes. On a ainsi

$$a_q(A) = a_q(F). \tag{31}$$

Par ailleurs, les représentations $\rho_p^{E_1(s)}$ et ρ_p^E étant isomorphes, on a (formule (12))

$$a_q(E) \equiv a_q(E_1(s)) \bmod p.$$

On déduit alors de (30) et (31) que l'on a

$$a_q(E) \equiv \pm a_q(F) \bmod p.$$

Afin de démontrer que $C_{3,p}(\mathbb{Q})$ est vide, on peut supposer, compte tenu de (25), que $p > 31$. L'inégalité $|a_q(E) \pm a_q(F)| \leq 4\sqrt{q}$ entraîne alors $|a_q(E) \pm a_q(F)| < p$, puis $a_q(E) = \pm a_q(F)$. D'où une contradiction et le lemme. ∎

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Il y a conjecturalement une infinité de nombres premiers $p \equiv 3 \bmod 4$ tels que $2p + 1$ soit premier. Ceux plus petits que 500 sont

$$\{3, 11, 23, 83, 131, 179, 191, 239, 251, 359, 419, 431, 443, 491\}.$$

Par ailleurs, la conclusion du lemme est aussi vraie si $p = 3$. En effet, la courbe elliptique d'équation $y^2 = x^3 - 3$, de conducteur 972, n'a pas de points rationnels sur $\mathbb{Q}$ (autre que le point à l'infini) (*cf.* [7, p. 249]). La conique d'équation $y^2 = x^2 - 3$ a une infinité de points rationnels sur $\mathbb{Q}$. En revanche, la courbe $y^2 = x^4 - 3$ n'en possède pas, comme on peut le vérifier en remarquant qu'elle est birationnellement équivalente à la courbe elliptique notée 576F2 dans [7]. Au vue des résultats obtenus, il semble donc naturel de conjecturer que pour tout entier $n \geq 3$, la courbe d'équation $y^2 = x^n - 3$ n'a pas de points rationnels sur $\mathbb{Q}$. Signalons qu'il se trouve dans [6] une démonstration du fait qu'elle ne possède pas de points entiers.

8.4 Tordues quadratiques de $C_{d,p}$

Les résultats obtenus dans ce travail permettent parfois la détermination des points rationnels sur $\mathbb{Q}$ de certaines tordues quadratiques de courbes $C_{d,p}$. Il s'agit de courbes sur $\mathbb{Q}$ ayant une équation de la forme $ey^2 = x^p + d$ où e est un entier sans facteurs carrés. Les théorèmes 1.1 et 1.2 permettent notamment d'obtenir des résultats dans cette direction si $e = 2$. On se limitera ici à indiquer le résultat suivant qui est une conséquence de la description de l'ensemble $S_p(4, 1, 3)$ (égalité (19)).

Proposition 8.7 *Soient p un nombre premier ≥ 7 et $C_p/\mathbb{Q}$ la courbe d'équation*

$$3y^2 = x^p + 4.$$

On a $C_p(\mathbb{Q}) = \{(-1, -1), (-1, 1)\}$.

Démonstration Soit (x, y) un point de $C_p(\mathbb{Q})$.

Supposons $v_3(y) \geq 0$. Il existe des entiers non nuls u, v et w tels que $\text{pgcd}(u, v) = 1$ et $\text{pgcd}(w, v) = 1$ avec $x = \frac{u}{v^2}$ et $y = \frac{w}{v^p}$. On a $3w^2 = u^p + 4v^{2p}$, de sorte que (v^2, u, w) appartient à $S_p(4, 1, 3)$. Cela conduit à $(x, y) \in \{(-1, -1), (-1, 1)\}$.

Supposons $v_3(y) < 0$. Dans ce cas, il existe deux entiers naturels r, s et des entiers u, v, w, non nuls, vérifiant les conditions suivantes :

(i) $\text{pgcd}(u, v) = 1$ et $\text{pgcd}(w, v) = 1$;
(ii) 3 ne divise pas uvw ;
(iii) $2r - 1 = sp$;
(iv) on a les égalités $x = \frac{u}{3^s v^2}$ et $y = \frac{w}{3^r v^p}$.

On a $w^2 = u^p + 4(3^s v^2)^p$, et l'élément $(3^s v^2, u, w)$ appartient à $S_p(4, 1, 1)$, ce qui conduit à une contradiction (*cf.* [17, th. 1]). D'où le résultat. ∎

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press

Références

[1] A. O. L. Atkin et J. Lehner, *Hecke operators on* $\Gamma_0(m)$. Math. Ann. **185**(1970), 134–160.
[2] C. Batut, D. Bernardi, K. Belabas, H. Cohen, et M. Olivier, *User's guide to PARI-GP (version 2.0.12).* Lab A2X, Université de Bordeaux I, Bordeaux, 1998.
[3] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms.* Canad. J. Math. **56**(2004), 23–54.
[4] F. Beukers, *On the generalized Ramanujan-Nagell equation. I.* Acta Arith. **38**(1981), 389–410.
[5] C. Breuil, B. Conrad, F. Diamond, et R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild* 3*-adic exercises.*, J. Amer. Math. Soc. **14**(2001), 843–939.
[6] J. H. E. Cohn, *The diophantine equation* $x^2 + 3 = y^n$. Glasgow Math. J. **35**(1993), 203–206
[7] J. E. Cremona, *Algorithms for modular elliptic curves.* Second edition, Cambridge University Press, Cambridge, 1997.
[8] ———, Elliptic curves data, disponible à : http://www.maths.nott.ac.uk/personal/jec/ftp/data/
[9] H. Darmon, *The equations* $x^n + y^n = z^2$ *and* $x^n + y^n = z^3$. Intern. Math. Res. Notices **10**(1993), 263–274.
[10] ———, *Serre's conjectures.* CMS Conf. Proc. 17, American Mathematical Society, Providence, RI, 1995 pp. 135–153.
[11] 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**(1995), 513–543.
[12] H. Darmon et L. Merel, *Winding quotients and some variants of Fermat's last theorem.* J. Reine Angew. Math. **490**(1997), 81–100.
[13] G. Frey, *Links between stable elliptic curves and certain Diophantine equations.* Ann. Univ. Sarav. Ser. Math. **1**(1986), 1–40.
[14] E. Halberstadt et A. Kraus, *Sur les modules de torsion des courbes elliptiques.* Math. Ann. **310**(1998), 47–54.
[15] ———, *Courbes de Fermat : résultats et problèmes.* J. Reine Angew. Math. **548**(2002), 167–234.
[16] E. Halberstadt, manuscrit (2003).
[17] W. Ivorra, *Sur les équations* $x^p + 2^\beta y^p = z^2$ *et* $x^p + 2^\beta y^p = 2z^2$. Acta. Arith. **108**(2003), 327–338.
[18] ———, *Courbes elliptiques sur* $\mathbb{Q}$*, ayant un point d'ordre* 2 *rationnel sur* $\mathbb{Q}$*, de conducteur* $2^N p$. Dissertationes Math. **429**(2004).
[19] ———, Équations diophantiennes ternaires de type $(p, p, 2)$ et courbes elliptiques, Chap. IV, Thèse Université Paris VI, 2004.
[20] M. A. Kenku, *On the number of* $\mathbb{Q}$*-isomorphism classes of elliptic curves in each* $\mathbb{Q}$*-isogeny class.* J. Number Theory **15**(1982), 199–202.
[21] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive.* Manuscripta Math. **69**(1990), 353–385.
[22] ———, *Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique.* Dissertationes Math. **364**(1997).
[23] ———, *Sur l'équation* $La^p + b^p = c^2$. Huitièmes rencontres arithmétiques de Caen, Université de Caen, 6-7 juin 1997.
[24] ———, *Majorations effectives pour l'équation de Fermat généralisée.* Canad. J. Math. **49**(1997), 1139–1161.
[25] ———, *Sur l'équation* $a^3 + b^3 = c^p$. Experiment. Math. **7**(1998), 1–13.
[26] ———, *Une question sur les équations* $x^m - y^m = Rz^n$. Compositio Math. **132**(2002), 1–26.
[27] A. Kraus et J. Oesterlé, *Sur une question de B. Mazur,* Math. Ann. **293**(1992), 259–275.
[28] J.-L. Lesage, *Différence entre puissances et carrés d'entiers.* J. Number Theory **73**(1998), 390–425.
[29] G. Ligozat, *Courbes modulaires de genre* 1. Bull. Soc. Math. France **43**(1975).
[30] B. Mazur, *Rational isogenies of prime degree.* Invent. Math. **44**(1978), 129–162.
[31] Metmod, disponible à : http://www.math.jussieu.fr/∼ivorra.
[32] F. Momose, *Rational points on the modular curves* $X_{\text{split}}(p)$. Compositio Math. **52**(1984), 115–137.
[33] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3. J. Number Theory **44**(1993), 119–152.
[34] B. Poonen, *Some Diophantine equations of the form* $x^n + y^n = z^m$. Acta Arith. **86**(1998), 193–205.
[35] K. Ribet, *On modular representations of* $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms.* Invent. Math. **100**(1990), 431–476.
[36] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. **15**(1972), 259–331.
[37] ———, *Sur les représentations modulaires de degré 2 de* $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Math. J. **54**(1987), 179–230.

[38] ———, *Travaux de Wiles (et Taylor,...). I.* . Séminaire Bourbaki 1994/95, Astérisque **237**(1996) 319–332.
[39] B. Setzer, *Elliptic curves of prime conductor.* J. London Math. Soc. (2) **10**(1975), 367–378.
[40] J. Silverman, *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 106, Springer-Verlag, 1986.
[41] W. Stein, *Modular forms database,* disponible à l'adresse: http://modular.fas.harvard.edu/Tables/
[42] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil.* In: Modular Functions of One Variable IV, Lecture Notes in Math. 476, Springer, Berlin, 1975, pp. 33-52.
[43] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141**(1995), 443–551.

Institut de Mathématiques
Université Paris VI
Équipe de Théorie des Nombres
UMR 7586 du CNRS
175 Rue du Chevaleret
Paris 75013
France
e-mail: ivorra@math.jussieu.fr
e-mail: kraus@math.jussieu.fr

https://doi.org/10.4153/CJM-2006-006-9 Published online by Cambridge University Press