Can. J. Math. Vol. **49** (6), 1997 pp. 1139–1161

MAJORATIONS EFFECTIVES POUR L'ÉQUATION DE FERMAT GÉNÉRALISÉE

ALAIN KRAUS

RÉSUMÉ. Soient A, B et C trois entiers non nuls premiers entre eux deux à deux, et p un nombre premier. Comme conséquence des travaux de A. Wiles et F. Diamond sur la conjecture de Taniyama-Weil, on explicite une constante $f(A,B,C)$ telle que, sous certaines conditions portant sur A, B et C, l'équation $Ax^p + By^p + Cz^p = 0$ n'a aucune solution non triviale dans $\mathbb{Z}$, si p est $> f(A,B,C)$. On démontre par ailleurs, sans condition supplémentaire portant sur A, B et C, que cette équation n'a aucune solution non triviale dans $\mathbb{Z}$, si p divise xyz, et si p est $> f(A,B,C)$.

0. **Introduction.** Ce travail concerne la conjecture suivante :

CONJECTURE (F). *Soient A, B et C trois entiers non nuls, premiers entre eux deux à deux, et p un nombre premier. Il existe une constante $f(A,B,C)$, telle que si p est $> f(A,B,C)$, l'équation*

$$Ax^p + By^p + Cz^p = 0, \tag{1}$$

n'a pas de solution x, y, z dans $\mathbb{Z}$, avec xyz distinct de 0, 1 et -1 et $\operatorname{pgcd}(x,y,z) = 1$.

La conjecture (F) est une conséquence de la conjecture (abc) (*cf.* [20], 3). Elle résulte aussi de conjectures générales de G. Frey sur la comparaison galoisienne des modules des points de p-torsion des courbes elliptiques (*cf.* [12], et [4], p. 148).

Les résultats déjà démontrés sur la conjecture (F) utilisent ceux obtenus par A. Wiles et F. Diamond sur la conjecture de Taniyama-Weil ([30] et [9]). Il semble que ce soient les suivants :

(1) Soient α un entier ≥ 0 et L un nombre premier appartenant à l'ensemble

$$\{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}.$$

Soit p un nombre premier ≥ 11, et distinct de L. L'équation $x^p + y^p + L^\alpha z^p = 0$ n'a alors aucune solution x, y, z dans $\mathbb{Z}$ avec xyz non nul (*cf.* [26], 1.4, et [24] p. 202, th. 2).

(2) Soient L un nombre premier *impair* qui ne soit ni un nombre de Fermat ni un nombre de Mersenne. Soient α un entier ≥ 1, et β un entier ≥ 0. Alors la conjecture (F) est maintenant démontrée, de façon non effective, pour l'équation

$$x^p + 2^\beta y^p + L^\alpha z^p = 0$$

Reçu par les éditeurs le 16 décembre 1996.
Classification (AMS) par sujet : 11G.

(*cf.* [11], p. 54 ; si $\beta = 0$, voir aussi [24], p. 204, alinéa (4)). Des résultats analogues non effectifs peuvent aussi être obtenus dans d'autres cas particuliers à partir d'un résultat de G. Frey, sur les représentations galoisiennes définies par les points de p-torsion des courbes elliptiques (*cf.* [11], p. 53, prop. 6.2).

(3) Soient p un nombre premier ≥ 3 et α un entier vérifiant $2 \leq \alpha < p$. K. Ribet a prouvé que l'équation $x^p + 2^\alpha y^p + z^p = 0$ n'a pas de solution x, y, z dans $\mathbb{Z}$ avec xyz non nul (*cf.* [21], th. 3).

(4) Récemment il H. Darmon et L. Merel ont prouvé la conjecture (F) pour l'équation $x^p + 2y^p + z^p = 0$ avec $f(1, 2, 1) = 2$ (*cf.* [5]), complétant ainsi les résultats obtenus par P. Dénes et K. Ribet sur cette équation (*cf.* [8] et [21]).

Toujours en utilisant les travaux de A. Wiles et F. Diamond sur la conjecture de Taniyama-Weil, nous démontrons dans cet article, dans des cas particuliers, la conjecture (F) de façon *effective* (*cf.* §2). À titre indicatif, supposons par exemple que $R = ABC$ soit impair. Posons $N = 2\,\mathrm{rad}(R)$, où $\mathrm{rad}(R)$ est le produit des nombres premiers qui divisent R. Supposons de plus qu'il n'existe pas de courbe elliptique sur $\mathbb{Q}$ de conducteur N ayant tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$. Alors la conjecture (F) est vraie pour l'équation (1), avec pour $f(A, B, C)$ une constante explicite ne dépendant que de l'indice du sous-groupe de congruence $\Gamma_0(N)$ dans $\mathrm{SL}_2(\mathbb{Z})$, et de la dimension de l'espace vectoriel engendré par les *newforms* de poids 2 pour $\Gamma_0(N)$ (*cf. loc. cit.* et l'appendice I) ; si $R = L^\alpha$, où α est un entier ≥ 0, et où L est un nombre premier impair qui ne soit ni un nombre de Fermat ni un nombre de Mersenne, on peut prendre

$$f(1, 1, L^\alpha) = \left(\sqrt{\frac{L+1}{2}} + 1\right)^{\frac{L+11}{6}}.$$

Si L appartient à l'ensemble $\{37, 41, 43, 47\}$, la constante $f(1, 1, L^\alpha) = 7$ convient (*cf.* §6).

Nous obtenons par ailleurs un énoncé effectif relatif au *deuxième cas* de la conjecture (F). Plus précisément, on détermine une constante $f(A, B, C)$, telle que si l'on a l'inégalité $p > f(A, B, C)$, l'équation (1) n'a pas de solution x, y, z dans $\mathbb{Z}$, avec xyz non nul et divisible par p.

Le plan de ce travail est le suivant :

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

1. **Notations.** Étant donné un entier $n \geq 1$, on notera pour toute la suite :
   - $\Gamma_0(n)$ le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ formé des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que n divise c ;
   - $\mu(n)$ l'indice de $\Gamma_0(n)$ dans $\mathrm{SL}_2(\mathbb{Z})$. On a
   $$\mu(n) = n \prod_{\substack{l \mid n \\ l \text{ premier}}} \left(1 + \frac{1}{l}\right). \tag{2}$$
   - $S_2(n)$ le $\mathbb{C}$-espace vectoriel des formes modulaires paraboliques de poids 2 et de caractère trivial pour $\Gamma_0(n)$;
   - $g_0(n)$ la dimension du $\mathbb{C}$-espace vectoriel $S_2(n)$. Les formules donnant $g_0(n)$ se trouvent par exemple dans [27], pp. 23–25 ;
   - $S_2^{\mathrm{new}}(n)$ le sous-espace vectoriel de $S_2(n)$ engendré par les *newforms* au sens des définitions qui figurent dans [2] (voir aussi [23], pp. 199–201) ;
   - $g_0^+(n)$ la dimension du $\mathbb{C}$-espace vectoriel $S_2^{\mathrm{new}}(n)$. On détermine dans l'appendice I $g_0^+(n)$ en fonction des $g_0(d)$ où d parcourt l'ensemble des diviseurs de n.

Si l est un nombre premier, on notera par ailleurs $v_l(n)$ l'exposant de l dans la décomposition de n en facteurs premiers, et $\mathrm{rad}'(n)$ le produit des nombres premiers *impairs* divisant n, *i.e.*, le plus grand entier impair sans facteur carré qui divise n.

2. **Énoncé des résultats sur la conjecture (F).** Soient A, B et C trois entiers *non nuls, premiers entre eux deux à deux*. Posons $R = ABC$ et désignons par N l'entier défini de la façon suivante :

$$N = \begin{cases} 2\,\mathrm{rad}'(R) & \text{si } v_2(R) = 0 \text{ ou } v_2(R) \geq 5 \\ 2^5\,\mathrm{rad}'(R) & \text{si } v_2(R) = 1 \\ 2^3\,\mathrm{rad}'(R) & \text{si } v_2(R) = 2 \text{ ou } 3 \\ \mathrm{rad}'(R) & \text{si } v_2(R) = 4. \end{cases} \tag{3}$$

On pose :

$$F(N) = \left(\sqrt{\frac{\mu(N)}{6}} + 1\right)^{2\, g_0^+(N)}. \tag{4}$$

THÉORÈME 1. *Soit p un nombre premier $> \mathrm{Max}\big(F(N), 3\big)$. Supposons que p ne divise pas R et que l'on ait $v_l(R) < p$ pour tout nombre premier l. Supposons de plus que l'une des conditions suivantes soit réalisée :*

(a) on a $v_2(R) = 0$ ou $v_2(R) \geq 4$, et il n'existe pas de courbe elliptique définie sur $\mathbb{Q}$ de conducteur N, ayant tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$;

(b) on a $v_2(R) = 1$, et il n'existe pas de courbe elliptique définie sur $\mathbb{Q}$ de conducteur N ni $N/16$, ayant tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$;

(c) on a $v_2(R) = 2$ ou 3, et il n'existe pas de courbe elliptique définie sur $\mathbb{Q}$ de conducteur N ni $N/4$, ayant tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$.

L'équation $Ax^p + By^p + Cz^p = 0$ n'a alors aucune solution x, y, z dans $\mathbb{Z}$ avec $xyz \neq 0$.

Rappelons qu'un nombre premier n'est pas un nombre de Fermat ni un nombre de Mersenne s'il ne s'écrit pas sous la forme $2^n \pm 1$. Le théorème 1 permet d'expliciter une version effective du résultat (2) signalé dans l'introduction :

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

COROLLAIRE 1. *Soient L un nombre premier impair qui ne soit ni un nombre de Fermat ni un nombre de Mersenne et p un nombre premier tels que*

$$p > \left(\sqrt{8(L+1)}+1\right)^{2^{(L-1)}}.$$

Soient α et β deux entiers ≥ 0, avec α non multiple de p. L'équation $x^p + 2^\beta y^p + L^\alpha z^p = 0$ n'a alors aucune solution x, y, z dans $\mathbb{Z}$ avec $xyz \neq 0$.

Dans le cas où $\beta = 0$ (*cf.* [24], p. 202, th. 2) ou $\beta = 4$ (*cf.* [11], p. 54), nous obtenons les deux énoncés suivants :

COROLLAIRE 2. *Soient L un nombre premier impair qui ne soit ni un nombre de Fermat ni un nombre de Mersenne et p un nombre premier tels que*

$$p > \left(\sqrt{\frac{L+1}{2}}+1\right)^{\frac{L+11}{6}}.$$

Si α est un entier ≥ 0, l'équation $x^p + y^p + L^\alpha z^p = 0$ n'a aucune solution x, y, z dans $\mathbb{Z}$ avec $xyz \neq 0$.

COROLLAIRE 3. *Soient L un nombre premier impair distinct de 17 et p un nombre premier ≥ 5, distinct de L, tels que*

$$p > \left(\sqrt{\frac{L+1}{6}}+1\right)^{\frac{L+1}{6}}.$$

Si α est un entier ≥ 0, l'équation $x^p + 16y^p + L^\alpha z^p = 0$ n'a aucune solution x, y, z dans $\mathbb{Z}$ avec $xyz \neq 0$.

L'énoncé qui suit fournit une version effective du *deuxième cas* de la conjecture (F) :

THÉORÈME 2. *Soit p un nombre premier $> \mathrm{Max}\big(F(N), 5\big)$. Supposons que p ne divise pas R et que l'on ait $v_l(R) < p$ pour tout nombre premier l. L'équation $Ax^p + By^p + Cz^p = 0$ n'a alors aucune solution x, y, z dans $\mathbb{Z}$, avec $xyz \neq 0$ et divisible par p.*

3. **Représentations modulaires et courbes elliptiques.**

On reprend les notations introduites dans le paragraphe 1.

3.1 *Énoncé des résultats.* Considérons dans ce paragraphe une courbe elliptique E définie sur $\mathbb{Q}$ et p un nombre premier ≥ 5 *fixés*. Soient $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ et $E_p(\bar{\mathbb{Q}})$ le sous-groupe des points de p-torsion de $E(\bar{\mathbb{Q}})$; c'est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension 2. Le groupe $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ opère sur $E_p(\bar{\mathbb{Q}})$ et son action est donnée par un homomorphisme

$$\rho_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}\big(E_p(\bar{\mathbb{Q}})\big).$$

À une telle représentation, J.-P. Serre associe un poids k qui est un entier ≥ 2, et un conducteur $N(\rho_p)$ qui est un entier ≥ 1 premier à p ([24], §1). Supposons désormais que les conditions suivantes soient réalisées :

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

(a) la courbe E est *modulaire* ;
(b) la représentation ρ_p est *irréductible* ;
(c) le poids k de ρ_p est 2.

Soient N_E le conducteur de E, et $\sum a_n(E)n^{-s}$ la fonction L de Hasse-Weil de E. La condition (a) signifie que la fonction définie sur le demi-plan de Poincaré par

$$\tau \longmapsto \sum_{n=1}^{\infty} a_n(E)q^n \qquad \text{où } q = e^{2i\pi\tau},$$

appartient à $S_2(N_E)$. Cette condition est réalisée si E a réduction semi-stable en 3 et 5 (*cf.* [30] et [9]). Si p est ≥ 11, la condition (c) signifie que E a réduction semi-stable en p et que l'exposant de p dans le discriminant minimal de E est multiple de p (*cf.* [24], p. 191, prop. 5, et [17], th. 1).

Identifions désormais $\bar{\mathbb{Q}}$ à un sous-corps de $\mathbb{C}$. Il est maintenant démontré que les conditions (a), (b) et (c) entraînent le fait que ρ_p, dans la terminologie de [26], soit modulaire de poids 2 et de caractère trivial pour $\Gamma_0\big(N(\rho_p)\big)$ (*cf.* [26], p. 6, *Remarques* (2)) ; cela signifie qu'il existe une forme modulaire parabolique

$$f = \sum a_n q^n$$

dans $S_2\big(N(\rho_p)\big)$, normalisée par $a_1 = 1$, fonction propre des opérateurs de Hecke T_l pour l ne divisant pas $pN(\rho_p)$, et une place $\wp$ de $\bar{\mathbb{Q}}$ de caractéristique résiduelle p, telles que pour tout nombre premier l, l'on ait

$$a_l \equiv a_l(E) \bmod \wp, \qquad \text{si } l \text{ ne divise pas } pN_E, \tag{5}$$

$$a_l \equiv \pm(l+1) \bmod \wp, \qquad \text{si } l \text{ divise } N_E \text{ et } l \text{ ne divise pas } pN(\rho_p). \tag{6}$$

En fait f est une *newform* de $S_2^{\text{new}}\big(N(\rho_p)\big)$ (*cf.* [24], p. 197, alinéa (5)).

Nous allons énoncer un critère pour que les coefficients a_n de f puissent être choisis dans $\mathbb{Z}$. Si tel est le cas, cela signifie qu'il existe une courbe elliptique modulaire E' définie sur $\mathbb{Q}$, de conducteur $N(\rho_p)$, dont la fonction L de Hasse-Weil soit $\sum a_n n^{-s}$. Pour tout nombre premier l sauf un nombre fini, on a alors la congruence

$$a_l \equiv a_l(E) \bmod p,$$

et d'après la condition (b), les représentations de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ définies par les points de p-torsion de E et E' sont isomorphes (*cf.* par exemple [18], prop. 3).

Étant donné un entier $n \geq 1$, posons (*cf.* (4)) :

$$F(n) = \left(\sqrt{\frac{\mu(n)}{6}} + 1\right)^{2\, g_0^+(n)}. \tag{7}$$

Nous obtenons le résultat suivant :

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

THÉORÈME 3. *Soit p un nombre premier ≥ 5. Supposons que E soit modulaire et que ρ_p soit irréductible de poids 2. Alors, si p est tel que*

$$p > F\big(N(\rho_p)\big),$$

il existe une courbe elliptique modulaire E' définie sur $\mathbb{Q}$, de conducteur $N(\rho_p)$, telle que les sous-groupes des points de p-torsion de $E(\bar{\mathbb{Q}})$ et $E'(\bar{\mathbb{Q}})$ soient isomorphes de façon compatible à l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

REMARQUES. (1) Le conducteur de ρ_p divise toujours le conducteur N_E de E ([24], ou [17], II, prop.). Le théorème 3 n'a donc d'intérêt que si $N(\rho_p)$ est un diviseur strict de N_E (si $N(\rho_p) = N_E$, la courbe E satisfait à la conclusion du théorème).

(2) Soit n un entier ≥ 1. On a l'inégalité

$$F(n) \leq \mu(n)^{g_0^+(n)}.$$

(3) Soit n un entier ≥ 2. Posons $g(n) = n\,(1 + \log\,\log n)$. En utilisant le lemme de [16], on peut démontrer l'inégalité

$$F(n) \leq g(n)^{1+\frac{g(n)}{5}}.$$

Énonçons maintenant un résultat qui précise le théorème 3 lorsque la courbe E possède *tous ses points d'ordre* 2 *rationnels sur* $\mathbb{Q}$, et qui est la situation que l'on rencontrera dans la suite. Étant donné un entier $n \geq 1$, on note

$$G(n) = \left(\sqrt{\frac{\mu\big(\mathrm{ppcm}(4,n)\big)}{6}} + 1\right)^2, \tag{8}$$

$$H(n) = \mathrm{Max}\big(F(n), G(n)\big). \tag{9}$$

THÉORÈME 4. *Conservons les hypothèses du théorème 3. Supposons de plus que E possède tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$. Alors, si p est tel que*

$$p > H\big(N(\rho_p)\big),$$

il existe une courbe elliptique modulaire E' définie sur $\mathbb{Q}$, de conducteur $N(\rho_p)$, ayant tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$, telle que les sous-groupes des points de p-torsion de $E(\bar{\mathbb{Q}})$ et $E'(\bar{\mathbb{Q}})$ soient isomorphes de façon compatible à l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

3.2 *Démonstration du théorème 3.* Démontrons d'abord le lemme préliminaire suivant :

LEMME 1. *Soient M un entier ≥ 1 et $f = \sum_{n\geq 1} a_n q^n$ une newform de $S_2^{\mathrm{new}}(M)$ normalisée par $a_1 = 1$. Supposons que pour tout nombre premier $l \leq \mu(M)/6$, a_l appartienne à $\mathbb{Z}$. Alors pour tout entier n, a_n appartient à $\mathbb{Z}$.*

DÉMONSTRATION. Les coefficients a_n de f appartiennent à l'anneau d'entiers d'un corps de nombres (*cf.* [23], p. 203, (iii)). Pour tout élément de σ de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, $\sum \sigma(a_n)q^n$

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

est le q-développement à l'infini d'une newform ${}^{\sigma}f$ de $S_2^{\text{new}}(M)$ (*cf. loc. cit.* (i)). Puisque a_l appartient à $\mathbb{Z}$ pour tout nombre premier $l \leq \mu(M)/6$, on a en fait ${}^{\sigma}f = f$ pour tout σ de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, autrement dit tous les a_n sont dans $\mathbb{Z}$ (*cf.* [7], p. 252, 4. et 5. A, ou la prop. 1 de l'appendice II). D'où le lemme.

Prouvons maintenant le théorème 3. D'après hypothèses faites, il existe une *newform* $f = \sum a_n q^n$ de $S_2^{\text{new}}\big(N(\rho_p)\big)$, normalisée par $a_1 = 1$, et une place $\wp$ de $\bar{\mathbb{Q}}$ de caractéristique résiduelle p, telles que les congruences (5) et (6) soient satisfaites. Supposons désormais qu'il existe des entiers n pour lesquels les coefficients a_n de f ne soient pas dans $\mathbb{Z}$, et que l'on ait $p > F\big(N(\rho_p)\big)$. D'après le lemme 1, il existe alors un nombre premier

$$l \leq \frac{\mu\big(N(\rho_p)\big)}{6}$$

tel que a_l n'appartienne pas à $\mathbb{Z}$. Nécessairement l ne divise pas $N(\rho_p)$, car sinon, f étant une newform normalisée de $S_2^{\text{new}}\big(N(\rho_p)\big)$, a_l serait 0 ou ± 1. Par ailleurs, l est distinct de p ; en effet, l'existence de f implique $g_0^+\big(N(\rho_p)\big) \geq 1$, de sorte que l'on a

$$F\big(N(\rho_p)\big) > \frac{\mu\big(N(\rho_p)\big)}{6},$$

et par hypothèse, on a $p > F\big(N(\rho_p)\big)$. D'après les congruences (5) et (6), on est donc dans l'un des deux cas suivants :

(i) on a $a_l \equiv a_l(E) \bmod \wp$ si l ne divise pas N_E

(ii) on a $a_l \equiv \pm(l+1) \bmod \wp$ si l divise N_E.

Considérons alors l'extension K de $\mathbb{Q}$ engendrée par les coefficients a_n de f ; le corps K est une extension finie de $\mathbb{Q}$ et les a_n appartiennent à l'anneau des entiers de K (*cf.* [23], p. 203, (iii)). Il résulte des congruences ci-dessus que p divise la norme de K sur $\mathbb{Q}$ de $a_l - a_l(E)$ ou de $a_l \pm (l+1)$ (qui est dans $\mathbb{Z}$), suivant que l'on soit dans le cas (i) ou (ii). Puisque a_l n'est pas dans $\mathbb{Z}$, a_l est distinct de $a_l(E)$ et de $\pm(l+1)$. Ainsi p est majoré par la valeur absolue de la norme de K sur $\mathbb{Q}$ de $a_l - a_l(E)$ ou de $a_l \pm (l+1)$. Par ailleurs, K est un corps de nombres totalement réel dont le degré sur $\mathbb{Q}$ est $\leq g_0^+\big(N(\rho_p)\big)$, et pour tout plongement σ de K dans $\mathbb{R}$, on a l'inégalité $|\ \sigma(a_l)\ | \leq 2\sqrt{l}$ (*cf.* [6], p. 302, th. 8.2). Puisque l'on a $|\ a_l(E)\ | \leq 2\sqrt{l}$ ([28], p. 131, th. 1.1), on obtient dans les deux cas (i) et (ii) ci-dessus, l'inégalité

$$p \leq \left(\sqrt{l}+1\right)^{2\, g_0^+\left(N(\rho_p)\right)}.$$

Mais l étant $\leq \mu\big(N(\rho_p)\big)/6$, cela entraîne $p \leq F\big(N(\rho_p)\big)$, ce qui contredit l'hypothèse faite sur p. Cela termine la démonstration du théorème 3.

3.3 *Démonstration du théorème 4.* Supposons que l'on ait $p > H\big(N(\rho_p)\big)$. Soit E' une courbe elliptique de conducteur $N(\rho_p)$, satisfaisant à la conclusion du théorème 3. Désignons par $\sum a_n(E')n^{-s}$ la fonction L de Hasse-Weil de E'. Étant donné un nombre premier q en lequel E a bonne réduction (et donc aussi E'), notons $n_q(E)$ le nombre de points sur $\mathbb{F}_q$ de la courbe elliptique sur $\mathbb{F}_q$ déduite de E par réduction modulo

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

q, et $n_q(E')$ son analogue en ce qui concerne la courbe elliptique E'. Posons $M(\rho_p) = \mathrm{ppcm}\big(4, N(\rho_p)\big)$.

Nous allons démontrer l'assertion suivante :

$(*)$ pour tout nombre premier l qui ne divise pas $2N(\rho_p)$, 4 divise $n_l(E')$.

En effet, supposons qu'il existe un nombre premier l qui ne divise pas $2N(\rho_p)$, tel que 4 ne divise pas $n_l(E')$. D'après le corollaire de l'appendice II, on peut supposer que l'on a

$$l \leq \frac{\mu\big(M(\rho_p)\big)}{6}. \tag{10}$$

Prouvons que E a bonne réduction en l. Supposons le contraire, autrement dit que E ait mauvaise réduction en l. D'après l'inégalité (10) et le fait que p soit $> G\big(N(\rho_p)\big)$, l est distinct de p. Par ailleurs, p est ≥ 5 (par hypothèse) et l divise le conducteur de E sans diviser $N(\rho_p)$. On déduit de là que la réduction de E en l est de type multiplicatif (*cf.* [17], II, prop.). Les représentations de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ définies par les points de p-torsion de E et E' étant isomorphes, et l^2 ne divisant pas $N_E N(\rho_p)$, on a donc :

$$a_l(E') \equiv \pm(l+1) \bmod p \qquad (cf.\ [18], \text{prop. } 3). \tag{11}$$

Puisque $|a_l(E')| \leq 2\sqrt{l}$, on a l'inégalité $|a_l(E') \pm (l+1)| \leq (\sqrt{l}+1)^2$. Or $a_l(E')$ est distinct de $\pm(l+1)$. D'après (11), p est donc $\leq (\sqrt{l}+1)^2$, ce qui conduit à l'inégalité $p \leq G\big(N(\rho_p)\big)$ (*cf.* (10)). Cela contredit l'hypothèse faite sur p et démontre le fait que E a bonne réduction en l.

Puisque le conducteur de E' divise celui de E, E' a aussi bonne réduction en l, et l'on a donc

$$a_l(E) \equiv a_l(E') \bmod p \qquad (cf.\ [18], \text{prop. } 3).$$

On déduit de là que $a_l(E) = a_l(E')$: en effet, si $a_l(E) \neq a_l(E')$, on a les inégalités $p < 4\sqrt{l} < (\sqrt{l}+1)^2 \leq G\big(N(\rho_p)\big)$, ce qui n'est pas. On a donc $n_l(E) = n_l(E')$, et d'après l'hypothèse faite sur l, 4 ne divise pas $n_l(E)$. Mais cela conduit à une contradiction car E possède tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$ (*cf.* [28], p. 176, prop. 3.1). Cela démontre notre assertion $(*)$.

Pour tout nombre premier l, sauf un nombre fini, 4 divise $n_l(E')$. Cela entraîne que E' est liée, par une isogénie définie sur $\mathbb{Q}$ de degré ≤ 2, à une courbe elliptique E'' sur $\mathbb{Q}$ *ayant tous ses points d'ordre 2 rationnels sur* $\mathbb{Q}$: en effet, E' possède un point P d'ordre 2 sur $\mathbb{Q}$ (*cf.* [25], IV-6), et si P est le seul point d'ordre 2 de $E'(\mathbb{Q})$, la courbe elliptique $E'' = E'/<P>$ convient. Comme p est distinct de 2, les représentations de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de p-torsion de E' et E'' sont isomorphes. La courbe elliptique E'' satisfait donc à la conclusion de l'énoncé du théorème 4, ce qui termine sa démonstration.

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

4. **Courbe de Frey.** Soient A, B et C trois entiers *non nuls, premiers entre eux deux à deux*, et p un nombre premier ≥ 5 *fixés*. On pose

$$R = ABC.$$

On suppose que les deux conditions suivantes sont réalisées :

(c_1) on a $v_p(R) = 0$;

(c_2) pour tout nombre premier l on a $v_l(R) < p$.

Soient a, b et c trois entiers *non nuls, premiers entre eux deux à deux*, tels que :

$$Aa^p + Bb^p + Cc^p = 0. \tag{12}$$

Les entiers Aa^p, Bb^p et Cc^p sont aussi non nuls et premiers entre eux deux à deux. Supposons *pour toute la suite*, ce qui n'est pas restrictif, que l'on ait

$$Aa^p \equiv -1 \bmod 4 \quad \text{et} \quad Bb^p \equiv 0 \bmod 2. \tag{13}$$

On a ainsi $v_2(R) = v_2(B)$ et $v_2(abc) = v_2(b)$.

Considérons alors la courbe elliptique E, dite de Frey, associée à l'égalité (12). Il s'agit de la courbe elliptique d'équation

$$y^2 = x(x - Aa^p)(x + Bb^p). \tag{14}$$

Rappelons quelques propriétés de la courbe E utiles pour la suite. Les invariants standards c_4 et Δ associés à l'équation (14) sont (*cf.* [29], p. 36) :

$$c_4 = 16\left(A^2a^{2p} + B^2b^{2p} + AB(ab)^p\right) \quad \text{et} \quad \Delta = 16R^2(abc)^{2p}. \tag{15}$$

Le modèle (14) est donc *minimal* en tout nombre premier *impair*, et E a réduction *semi-stable* en dehors de 2. En fait E a réduction semi-stable en 2 si et seulement si 16 divise Bb^p (*cf.* [20], I, 1, et (13)). Soit $\Delta_{\min}(E)$ le discriminant minimal de E ; on a

$$\Delta_{\min}(E) = \begin{cases} \Delta & \text{si 16 ne divise pas } Bb^p \\ \Delta/2^{12} & \text{si 16 divise } Bb^p \end{cases} \tag{16}$$

(*cf. loc. cit.*). Si n est un entier ≥ 1, rappelons que l'on désigne par $\mathrm{rad}'(n)$ le plus grand entier impair sans facteur carré qui divise n. Si N_E est le conducteur de E, on a le résultat suivant :

LEMME 2. *(a) Si $v_2(R) = 0$ ou $v_2(R) \geq 5$, on a $N_E = 2\ \mathrm{rad}'(\Delta)$.*

(b) Si $1 \leq v_2(R) \leq 4$, et si b est pair, on a $N_E = 2\ \mathrm{rad}'(\Delta)$.

(c) Si $1 \leq v_2(R) \leq 4$, et si b est impair, on a

$$N_E = \begin{cases} 2^5\ \mathrm{rad}'(\Delta) & \text{si } v_2(R) = 1 \\ 2^3\ \mathrm{rad}'(\Delta) & \text{si } v_2(R) = 2 \text{ ou } 3 \\ \mathrm{rad}'(\Delta) & \text{si } v_2(R) = 4. \end{cases}$$

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

DÉMONSTRATION. Si l est un nombre premier impair qui divise Δ, on a $v_l(N_E) = 1$ car E a réduction multiplicative en l. Déterminons maintenant $v_2(N_E)$. Si b est pair, ce qui est en particulier le cas si R est impair, ou bien si l'on a $v_2(R) \geq 5$, la courbe E a réduction de type multiplicatif en 2 (car 32 divise alors Bb^p) et l'on a $v_2(N_E) = 1$. Le cas où $1 \leq v_2(R) \leq 4$ et où b est impair résulte directement de l'étude faite dans [10]. D'où le lemme.

Notons ρ_p la représentation de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ définie par le sous-groupe des points de p-torsion de $E(\bar{\mathbb{Q}})$ et $N(\rho_p)$ son conducteur.

LEMME 3. *(a) Si $v_2(R) = 0$ ou $v_2(R) \geq 5$, on a $N(\rho_p) = 2\ \mathrm{rad}'(R)$.*
(b) Si $v_2(R) = 4$, on a $N(\rho_p) = \mathrm{rad}'(R)$.
(c) Si $1 \leq v_2(R) \leq 3$, et si b est pair, on a $N(\rho_p) = 2\ \mathrm{rad}'(R)$.
(d) Si $1 \leq v_2(R) \leq 3$, et si b est impair, on a

$$N(\rho_p) = \begin{cases} 2^5\ \mathrm{rad}'(R) & \text{si } v_2(R) = 1 \\ 2^3\ \mathrm{rad}'(R) & \text{si } v_2(R) = 2 \text{ ou } 3. \end{cases}$$

DÉMONSTRATION. (1) Soit l un nombre premier *impair distinct* de p. Vérifions que

$$v_l\big(N(\rho_p)\big) = \begin{cases} 0 & \text{si } l \text{ ne divise pas } R \\ 1 & \text{si } l \text{ divise } R. \end{cases} \tag{17}$$

En effet, si l ne divise pas Δ, E a bonne réduction en l, et l'on a $v_l\big(N(\rho_p)\big) = 0$. Supposons que l divise Δ. D'après les formules (15) et (16) on a

$$v_l\big(\Delta_{\min}(E)\big) = 2v_l(R) + 2pv_l(abc).$$

La courbe E a en l réduction de type multiplicatif. D'après la condition (c_2), l'exposant de l dans $\Delta_{\min}(E)$ est multiple de p si et seulement si l ne divise pas R. Cela entraîne (17) (*cf.* [24], p. 201, (4.1.12), ou [17], II, prop.).

(2) Déterminons maintenant $v_2\big(N(\rho_p)\big)$. Remarquons d'abord que si 16 divise Bb^p, *i.e.*, si E a réduction semi-stable en 2, on a la congruence

$$v_2\big(\Delta_{\min}(E)\big) \equiv 2v_2(R) - 8 \bmod p \qquad (\textit{cf.} \text{ formules (15) et (16)}).$$

Puisque l'on a $v_2(R) < p$ (condition (c_2)), on déduit dans ce cas que p divise $v_2\big(\Delta_{\min}(E)\big)$ si et seulement si l'on a $v_2(R) = 4$.

(2.1) Supposons $v_2(R) = 0$ ou $v_2(R) \geq 5$. La courbe E a réduction multiplicative en 2 (lemme 2). Par ailleurs, p ne divise pas $v_2\big(\Delta_{\min}(E)\big)$; on a donc

$$v_2\big(N(\rho_p)\big) = 1. \tag{18}$$

(2.2) Supposons $v_2(R) = 4$. Si b est pair, E a réduction multiplicative en 2 (*loc. cit.*) et p divise $v_2\big(\Delta_{\min}(E)\big)$. Si b est impair, E a bonne réduction en 2 (*loc. cit.*). Dans les deux cas on a donc :

$$v_2\big(N(\rho_p)\big) = 0. \tag{19}$$

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

(2.3) Supposons $1 \leq v_2(R) \leq 3$ et b pair. La courbe E a en 2 réduction de type multiplicatif, et p ne divise pas $v_2\big(\Delta_{\min}(E)\big)$; on a donc

$$v_2\big(N(\rho_p)\big) = 1. \tag{20}$$

(2.4) Supposons $1 \leq v_2(R) \leq 3$ et b impair. La courbe E a réduction de type additif en 2 et l'on a (*cf.* [17], II, prop.) :

$$v_2\big(N(\rho_p)\big) = v_2(N_E). \tag{21}$$

Le lemme 3 résulte alors de la condition (c_1), des formules (17) à (21) et de l'assertion (c) du lemme 2.

LEMME 4. *La représentation ρ_p est irréductible.*

DÉMONSTRATION. Si E est semi-stable, cette assertion résulte directement de la proposition 6 de [24], p. 201 (on a $p \geq 5$). Supposons que E ne soit pas semi-stable. On a alors $1 \leq v_2(R) \leq 3$ (*cf.* le lemme 2), et l'équation (14) est un modèle minimal de E. Le triplet $\big(v_2(R), v_2(\Delta), v_2(c_4)\big)$ est (1,6,4), (2,8,4) ou (3,10,4). La courbe E a potentiellement bonne réduction en 2. Soit Φ_2 le groupe, défini par J.-P. Serre dans [22], p. 311, mesurant le défaut de semi-stabilité de E en 2. D'après le corollaire p. 357 de [15], on constate que l'ordre de Φ_2 est dans tous les cas distinct de 2, 3, 4, et 6 : il est d'ordre 8 ou 24. Cela entraîne que ρ_p est irréductible (*cf.* [22], p. 313, prop. 23, (b)). D'où le lemme 4.

LEMME 5. *Le poids de ρ_p est 2.*

DÉMONSTRATION. Puisque p est $\neq 2$, E a réduction semi-stable en p. Par ailleurs, p ne divise pas R (condition (c_1)), et donc l'exposant de p dans le discriminant minimal de E est multiple de p. Cela implique le lemme (*cf.* [24], p. 191, prop. 5).

5. **Démonstrations des résultats sur la conjecture (F).**

5.1 *Démonstration du théorème 1.*

Considérons trois entiers non nuls a, b et c tels que $Aa^p + Bb^p + Cc^p = 0$. On peut supposer que a, b et c sont premiers entre eux. Puisque l'on a $v_l(R) < p$ pour tout nombre premier l, les entiers a, b et c sont alors premiers entre eux deux à deux. Quitte à effectuer une permutation convenable sur le triplet (Aa^p, Bb^p, Cc^p), on peut par ailleurs supposer que les congruences (13) sont réalisées. Soient E la courbe de Frey associée à l'égalité ci-dessus comme dans le paragraphe 4, ρ_p la représentation de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de p-torsion de $E(\bar{\mathbb{Q}})$ et $N(\rho_p)$ son conducteur. Par hypothèse p est ≥ 5 et les conditions (c_1) et (c_2) du paragraphe 4 sont satisfaites.

Vérifions d'abord que l'on a

$$F(N) \geq F\big(N(\rho_p)\big). \tag{22}$$

En effet, si $v_2(R) = 4$, on a $N(\rho_p) = N$ (lemme 3 et formule (3)). Si $v_2(R)$ est distinct de 4, $N(\rho_p)$ est *pair* et appartient à $\{N, N/4, N/16\}$ (*cf. loc. cit.*). On a par conséquent

$$\mu(N) \geq \mu\big(N(\rho_p)\big), \tag{23}$$

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

et d'après la remarque (a) de l'appendice I, on a

$$g_0^+(N) \geq g_0^+\big(N(\rho_p)\big). \tag{24}$$

D'où l'inégalité (22) ((23) et (24)).

On est alors amené à distinguer plusieurs cas :

(1) supposons que l'on ait $g_0^+(N) \geq 2$. On a alors les inégalités

$$F(N) \geq \left(\sqrt{\frac{\mu(N)}{6}} + 1\right)^4 \geq \left(\sqrt{\frac{\mu\big(N(\rho_p)\big)}{6}} + 1\right)^4 \geq \left(\sqrt{\frac{\mu\big(4N(\rho_p)\big)}{6}} + 1\right)^2,$$

la dernière inégalité ayant lieu car, sous l'hypothèse (1), $N(\rho_p)$ est ≥ 2. D'où, par définition de la constante $G\big(N(\rho_p)\big)$ (formule (8)) :

$$F(N) \geq G\big(N(\rho_p)\big). \tag{25}$$

D'après les inégalités (22) et (25), on a donc

$$F(N) \geq H\big(N(\rho_p)\big), \tag{26}$$

(*cf.* formule (9)). Par ailleurs, la représentation ρ_p est irréductible et de poids 2 (lemmes 4 et 5) et E est modulaire (*cf.* [30] et [9] : E est semi-stable en 3 et 5). Le théorème 1 dans ce cas résulte alors du théorème 4.

La représentation ρ_p est modulaire de poids 2 et de niveau $N(\rho_p)$ (*cf.* le paragraphe 3) : soit $f = \sum a_n(f)q^n$ une newform normalisée de $S_2^{\text{new}}\big(N(\rho_p)\big)$ qui est associée à ρ_p comme dans *loc. cit.*

(2) Supposons que l'on ait $g_0^+(N) = 0$. D'après la formule (24) on a $g_0^+\big(N(\rho_p)\big) = 0$. Il n'existe donc pas de newform de poids 2 et de niveau $N(\rho_p)$, ce qui contredit l'existence de f et prouve le théorème sous l'hypothèse (2).

(3) Supposons que l'on ait $v_2(R) \neq 4$ et $g_0^+(N) = 1$. Puisque N est un entier de la forme $2u$, $8u$ ou $32u$, où u est un entier impair sans facteur carré, N appartient à l'ensemble :

$$\{14, 24, 30, 32, 34, 40, 42, 46, 70, 78\}$$

(*cf.* la remarque (c) de l'appendice I). Par hypothèse il n'existe pas de courbe elliptique sur $\mathbb{Q}$ de conducteur N ayant tous ses points d'ordre 2 sur $\mathbb{Q}$ (conditions (a), (b) et (c) du théorème 1). Par ailleurs, une courbe elliptique sur $\mathbb{Q}$ de conducteur N étant modulaire, la liste des courbes elliptiques de conducteur N qui se trouvent dans les tables de [3] est exhaustive, et l'on a en fait

$$N \in \{14, 34, 46\}.$$

On déduit de là que $N(\rho_p) = N$ (lemme 3 et formule (3)). Mais p étant par hypothèse $> F(N)$, on a ainsi $p \geq 11$. Par ailleurs, on a (*cf.* [24], p. 203, lemme 1) :

$$a_3(f) \equiv \begin{cases} 0 \bmod \wp & \text{si } E \text{ a bonne réduction en 3} \\ \pm 4 \bmod \wp & \text{si } E \text{ a réduction multiplicative en 3,} \end{cases} \tag{27}$$

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

$$a_5(f) \equiv \begin{cases} \pm 2 \bmod \wp & \text{si } E \text{ a bonne réduction en 5} \\ \pm 6 \bmod \wp & \text{si } E \text{ a réduction multiplicative en 5,} \end{cases} \tag{28}$$

où $\wp$ est une place de $\bar{\mathbb{Q}}$ de caractéristique résiduelle p. Il résulte alors du lemme 2 de *loc. cit.*, et des congruences (27) et (28), que f ne peut exister. D'où le théorème dans ce cas.

(4) Supposons enfin que l'on ait $v_2(R) = 4$ et $g_0^+(N) = 1$. On a $N = N(\rho_p)$ (lemme 3 et formule (3)). Par les mêmes arguments que ceux utilisés dans l'alinéa (3) précédent, N étant impair sans facteur carré, on constate que l'on a

$$N \in \{11, 19\}.$$

Supposons $N = 11$. On a $F(11) = (\sqrt{2}+1)^2$ et donc p est ≥ 7. On a dans ce cas $a_3(f) = -1$ (*cf.* [3], p. 244) et les congruences (27) entraînent que f n'existe pas. Si $N = 19$, on doit avoir $a_3(f) = -2$ (*cf. loc. cit.*) et là encore f ne peut exister.

Cela termine la démonstration du théorème 1.

5.2 *Démonstration des corollaires 1, 2 et 3.*

Prouvons d'abord le lemme suivant :

LEMME 6. *Soient k un entier ≥ 0 et q un nombre premier impair. Supposons qu'il existe une courbe elliptique définie sur $\mathbb{Q}$, de conducteur $2^k q$, ayant tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$. Alors q est un nombre de Fermat ou un nombre de Mersenne. Si de plus $k = 0$, on a $q = 17$.*

DÉMONSTRATION. Considérons une courbe elliptique E définie sur $\mathbb{Q}$ possédant tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$. Soit (W) un modèle entier minimal de E :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{W}$$

En effectuant le changement de variables

$$\begin{cases} X = 4x \\ Y = 8y + 4(a_1x + a_3), \end{cases}$$

on obtient comme nouveau modèle de E :

$$Y^2 = X^3 + b_2X^2 + 8b_4X + 16b_6, \tag{W'}$$

où b_2, b_4 et b_6 sont les invariants standards associés à (W) (*cf.* [29], 1, (1.2) et (1.6)). Le modèle (W') est entier et minimal en dehors de 2 . Dans ce modèle les coordonnées des points de 2-torsion de E sont dans $\mathbb{Z}$. Il existe donc a et b dans $\mathbb{Z}$ tels que

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

soit un modèle *entier* de E *minimal en dehors de* 2. Soient $c_4(W)$ et $\Delta(W)$ les invariants standards associés à (W). On a

$$c_4(W) = a^2 + b^2 + ab \quad et \quad \Delta(W) = \frac{\big(ab(a+b)\big)^2}{2^8}. \tag{29}$$

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

Supposons que le conducteur de E soit $2^k q$. Le produit des nombres premiers qui divisent $ab(a+b)$ divise donc $2q$ et est divisible par q. Par ailleurs, E ayant réduction semi-stable en tout nombre premier l *impair*, si l divise a, alors l ne divise pas b. On déduit de là l'existence d'entiers r, s, t et u, avec $s \geq 1$, tels que l'on ait

$$\pm 2^r \pm q^s 2^t + 2^u = 0. \tag{30}$$

On a nécessairement $r = t$ ou $t = u$; en effet, dans le cas contraire, on aurait $r = u$, ce qui entraîne $s = 0$ et conduit à une contradiction. Il existe donc un entier n tel que l'on ait $q^s = 2^n \pm 1$, ce qui entraîne le fait que q soit un nombre de Fermat ou de Mersenne.

Supposons de plus que l'on ait $k = 0$. Dans ce cas E a bonne réduction en 2. On doit donc avoir $v_2\big(ab(a+b)\big) = 4$ (*cf.* (29)). Cela entraîne que $q \in \{3, 5, 7, 17\}$ (*cf.* (30)), ce qui prouve le lemme, car il n'existe pas de courbe elliptique sur $\mathbb{Q}$ de conducteur 3, 5 ni 7.

Posons alors

$$A_L = \left(\sqrt{8(L+1)} + 1\right)^{2(L-1)},\ B_L = \left(\sqrt{\frac{L+1}{2}} + 1\right)^{\frac{L+11}{6}}$$
$$\text{et} \quad C_L = \left(\sqrt{\frac{L+1}{6}} + 1\right)^{\frac{L+1}{6}}.$$

Rappelons que $g_0(L)$ (resp. $g_0(2L)$) désigne la dimension du $\mathbb{C}$-espace vectoriel $S_2(L)$ (resp. $S_2(2L)$).

(1) Prouvons maintenant le corollaire 1. On peut supposer $0 \leq \beta < p$ et $1 \leq \alpha < p$. Puisque par hypothèse p est $> A_L$, on a $p \neq L$ et $p \geq 5$. Par ailleurs, on a (formule (3))

$$N = \begin{cases} 2L & \text{si } \beta = 0 \text{ ou } \beta \geq 5 \\ 32L & \text{si } \beta = 1 \\ 8L & \text{si } \beta = 2 \text{ ou } 3 \\ L & \text{si } \beta = 4. \end{cases}$$

D'après le lemme 6, L n'étant pas un nombre premier de Fermat ni de Mersenne, il n'existe pas de courbe elliptique sur $\mathbb{Q}$, de conducteur N ni $2L$, possédant tous ses points d'ordre 2 rationnels sur $\mathbb{Q}$. Les hypothèses du théorème 1 sont donc satisfaites. Il s'agit alors de vérifier l'inégalité

$$F(N) \leq A_L,$$

ce qui d'après le théorème 1, prouvera le corollaire 1. On remarque pour cela que l'on a

$$F(N) \leq \left(\sqrt{\frac{\mu(32L)}{6}} + 1\right)^{2d_L},$$

où $d_L = \mathrm{Max}\big(g_0^+(L), g_0^+(2L), g_0^+(8L), g_0^+(32L)\big)$. Tout revient alors à démontrer que l'on a $d_L = L - 1$. Par hypothèse L est ≥ 5. On a $g_0^+(L) = g_0(L)$ et $g_0^+(2L) = g_0(2L) - 2g_0(L)$

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

(*cf.* th. de l'appendice I). En utilisant les propositions 1.40 et 1.43 de [27], on vérifie alors que l'on a

$$g_0^+(2L) = \begin{cases} \frac{L+11}{12} & \text{si } L \equiv 1 \bmod 12 \\ \frac{L-5}{12} & \text{si } L \equiv 5 \bmod 12 \\ \frac{L+5}{12} & \text{si } L \equiv 7 \bmod 12 \\ \frac{L-11}{12} & \text{si } L \equiv 11 \bmod 12. \end{cases} \tag{31}$$

De même on constate que

$$g_0^+(8L) = \begin{cases} \frac{L+1}{4} & \text{si } L \equiv 3 \bmod 4 \\ \frac{L-1}{4} & \text{si } L \equiv 1 \bmod 4, \end{cases}$$

et que $g_0^+(32L) = L - 1$. On a donc $d(L) = L - 1$; d'où le corollaire 1.

(2) Démonstration du corollaire 2 : on peut supposer $0 < \alpha < p$. On a $p \neq L$, $p \geq 5$ et $N = 2L$ (formule (3)). D'après les formules (31) on a $F(N) \leq B_L$. Le corollaire 2 se déduit alors directement du lemme 6 et du théorème 1.

(3) Démonstration du corollaire 3 : là encore on peut supposer $0 < \alpha < p$ (*cf.* par exemple [21], th. 3). On a $N = L$ et $g_0^+(L) = g_0(L) \leq \frac{L+1}{12}$ (*cf.* [27], prop. 1.40 et 1.43). D'où $F(N) \leq C_L$ et le corollaire 3 (*cf.* le lemme 6 et le th. 1).

5.3 *Démonstration du théorème 2.* On utilise le lemme suivant :

LEMME 7. *Soit A un courbe elliptique définie sur $\mathbb{Q}$ ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$. Soient l un nombre premier impair en lequel A a bonne réduction, et $\sum a_n n^{-s}$ la fonction L de Hasse-Weil de A. On a $a_l \neq \pm 1$.*

DÉMONSTRATION. Soit n_l le nombre de points sur $\mathbb{F}_l$ de la courbe elliptique déduite de A par réduction modulo l. On a $a_l = 1 + l - n_l$. Supposons $a_l = \pm 1$. On a alors $n_l = l$ ou $l + 2$. Or A ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, et l étant impair, 2 divise n_l, ce qui conduit à une contradiction. D'où le lemme.

Démontrons maintenant le théorème 2. Considérons trois entiers a, b et c non nuls vérifiant $Aa^p + Bb^p + Cc^p = 0$, avec a, b et c premiers entre eux deux à deux, tels que p divise abc, et que les congruences (13) soient réalisées (cela n'est pas restrictif). Soient E la courbe de Frey associée à cette égalité (*cf.* §4), ρ_p la représentation de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ dans les points de p-torsion de $E(\bar{\mathbb{Q}})$ et $N(\rho_p)$ son conducteur. Par hypothèse on a $p \geq 7$, et les conditions (c_1) et (c_2) du paragraphe 4 sont satisfaites.

(1) Supposons $g_0^+(N) \geq 2$. La représentation ρ_p étant irréductible et de poids 2 (lemmes 4 et 5) et E étant modulaire, le couple (E, p) satisfait aux hypothèses du théorème 4. Par ailleurs on a $F(N) \geq H\big(N(\rho_p)\big)$ (formule (26)). Il existe donc une courbe elliptique E' définie sur $\mathbb{Q}$, de conducteur $N(\rho_p)$, ayant tous ses points d'ordre 2 sur $\mathbb{Q}$, telle que les $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules des points de p-torsion de E et E' soient isomorphes (th. 4). La courbe E' a bonne réduction en p, car p ne divise pas $N(\rho_p)$. Par ailleurs, E a en p réduction de type multiplicatif, car p divise abc. On déduit de là que l'on a

$$a_p(E') \equiv \pm 1 \bmod p, \tag{32}$$

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

où $a_p(E')$ est la trace de l'endomorphisme de Frobenius de la courbe elliptique déduite de E' par réduction modulo p (*cf.* [18], prop. 3 (iii)). Or on a $\mid a_p(E') \pm 1 \mid \leq 2\sqrt{p}+1 < p$ (p est ≥ 7 par hypothèse) ; d'où l'égalité $a_p(E') = \pm 1$, ce qui contredit le lemme 7. D'où le théorème 2 sous l'hypothèse (1).

La représentation ρ_p est modulaire de poids 2 et de niveau $N(\rho_p)$; soit $f = \sum a_n(f)q^n$ une newform normalisée de $S_2^{\text{new}}\big(N(\rho_p)\big)$ associée à ρ_p comme dans le paragraphe 3.

(2) Si $g_0^+(N) = 0$: on a $g_0^+\big(N(\rho_p)\big) = 0$ (inégalité (24)) et f n'existe pas, ce qui prouve en particulier le théorème 2 dans ce cas (*cf.* dém. du th. 1, 2).

(3) Supposons $g_0^+(N) = 1$. On a donc $g_0^+\big(N(\rho_p)\big) \leq 1$, et l'on peut supposer que $g_0^+\big(N(\rho_p)\big) = 1$. D'après la remarque (c) de l'appendice I, et le lemme 3, $N(\rho_p)$ appartient à l'ensemble

$$\{11, 14, 15, 17, 19, 21, 24, 30, 32, 33, 34, 40, 42, 46, 70, 78\}.$$

Si $N(\rho_p) = 11$ ou 19, f n'existe pas (*cf.* dém. du th. 1, 4). Si $N(\rho_p)$ est distinct de 11 et 19, $\sum a_n(f)n^{-s}$ est la fonction L d'une courbe elliptique E' ayant au moins un point d'ordre 2 sur $\mathbb{Q}$ (*cf.* [3], pp. 90-96). La congruence (32) est encore satisfaite, ce qui contredit de nouveau le lemme 7.

Cela termine la démonstration du théorème 2.

6. **Exemples.** On se propose dans ce paragraphe de préciser l'énoncé du corollaire 2 du théorème 1 pour quelques nombres premiers L. La méthode suivie est analogue à celle utilisée par J.-P. Serre pour démontrer le théorème 2, p. 202, de [24].

On reprend les notations du paragraphe 1. Par ailleurs, si n est un entier ≥ 1 et l un nombre premier qui ne divise pas n, on note $H_l(n)$ le polynôme caractéristique de l'opérateur de Hecke $T_l|_{S_2^{\text{new}}(n)}$ agissant sur $S_2^{\text{new}}(n)$. Dans la démonstration du théorème 5 ci-dessous, on a utilisé la formule des traces de Selberg pour $S_2(n)$ qui se trouvent dans [13], ainsi que la méthode des graphes qui est présentée dans [19]. La formule des traces pour $S_2(n)$ ainsi que celles permettant de déterminer $H_l(n)$ (*cf.* [13] et l'appendice I), ont été implantées sur ordinateur par E. Halberstadt, à l'aide du logiciel de calculs PARI.

THÉORÈME 5. *Soient p un nombre premier ≥ 11, α un entier ≥ 0, et L un nombre premier distinct de p appartenant à l'ensemble*

$$\{37, 41, 43, 47\}.$$

L'équation $x^p + y^p + L^\alpha z^p = 0$ n'a alors aucune solution x, y, z dans $\mathbb{Z}$ avec xyz non nul.

DÉMONSTRATION. On peut supposer $0 < \alpha < p$. Soient a, b et c trois entiers non nuls premiers entre eux deux à deux vérifiant l'égalité $a^p + b^p + L^\alpha c^p = 0$. Soient E la courbe de Frey associée à cette égalité comme au paragraphe 4, $\sum a_n(E)n^{-s}$ sa fonction L de Hasse-Weil, et ρ_p la représentation donnant l'action de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur $E_p(\overline{\mathbb{Q}})$. Le poids de ρ_p est 2 et son niveau est $2L$. Puisque E est modulaire, il existe une newform

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

$f = \sum a_n(f)q^n$ de $S_2^{\text{new}}(2L)$, normalisée par $a_1(f) = 1$, et une place $\wp$ de $\bar{\mathbb{Q}}$ au-dessus de p, telles que pour tout nombre premier $l \neq p$ en lequel E a bonne réduction, l'on ait

$$a_l(f) \equiv a_l(E) \bmod \wp. \tag{33}$$

Nous allons maintenant démontrer que f n'existe pas.

(1) Supposons $L = 37$. On a $g_0^+(74) = 4$ et $H_3(74) = (X^2 - 3X - 1)(X^2 + X - 1)$. Le $\mathbb{C}$-espace $S_2^{\text{new}}(74)$ est donc engendré par quatre newforms normalisées, deux conjuguées sur $\mathbb{Q}(\sqrt{5})$ et deux autres conjuguées sur $\mathbb{Q}(\sqrt{13})$. Le coefficient $a_3(f)$ est donc une unité de $\mathbb{Q}(\sqrt{5})$ ou de $\mathbb{Q}(\sqrt{13})$; d'après le lemme 1 de [24], on a donc

$$a_3(f) \equiv \pm 4 \bmod \wp.$$

En considérant les normes de $\mathbb{Q}(\sqrt{13})$ sur $\mathbb{Q}$ de $a_3(f) \pm 4$, on constate que f ne peut être rationnelle sur $\mathbb{Q}(\sqrt{13})$ (car p est $\neq 3$). Par ailleurs, la norme de $\mathbb{Q}(\sqrt{5})$ sur $\mathbb{Q}$ de $a_3(f) \pm 4$ est 11 ou 19. On a donc nécessairement $p = 11$ ou $p = 19$. Par ailleurs on a $H_5(74) = (X^2 - X - 11)(X^2 + X - 3)$. On déduit de là que $a_5(f)$ est racine de $X^2 - X - 11$. Puisque l'on a

$$a_5(f) \equiv \pm 2 \ \text{ ou } \ \pm 6 \bmod \wp,$$

cela entraîne en fait $p = 19$.

Il reste à démontrer que f n'existe pas si $p = 19$. On utilise pour cela la méthode des graphes (*cf.* [19]). Elle permet d'expliciter les premiers coefficients des q-développements à l'infini des deux newforms normalisées de $S_2^{\text{new}}(74)$ qui sont à coefficients dans l'anneau d'entiers A de $\mathbb{Q}(\sqrt{5})$ (*cf. loc. cit.*, p. 227). Posons $w = \frac{1+\sqrt{5}}{2}$. On constate alors que les coefficients a_l, pour l premier compris entre 2 et 37, du q-développement $\sum a_n q^n$ d'une de ces deux newforms, sont donnés par le tableau suivant :

l	2	3	5	7	11	13	17	19	23	29	31	37
a_l	1	$-1+w$	$2-3w$	$-2+2w$	$-2-w$	$-1+3w$	$-2+4w$	$2-4w$	$1-3w$	$-5+7w$	$8+w$	-1

Soit $\wp_{19}$ l'idéal de A engendré par $4w - 1$. C'est l'un des deux idéaux de A au-dessus de 19. On vérifie que pour tout nombre premier $l \neq 2, 37$, compris entre 2 et 37, l'on a $a_l \equiv l+1 \bmod \wp_{19}$, et que par ailleurs -2.38 est dans $\wp_{19}$. Il résulte de la proposition 2 de l'appendice II, que cette congruence est valable pour tous les nombres premiers $l \neq 2, 37$. On déduit de là que pour tout nombre premier $l \neq 2, 37$,

$$a_l(f) \equiv l + 1 \bmod P,$$

où P est l'un des idéaux de A au-dessus de 19. Il résulte alors de la congruence (33) que

$$a_l(E) \equiv l + 1 \bmod 19,$$

pour presque tout nombre premier l. Mais cela contredit le fait que ρ_{19} soit irréductible (*cf.* [25], IV-6). Cela démontre le théorème si $L = 37$.

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

(2) Supposons $L = 41$. On a $g_0^+(82) = 3$ et $H_3(82) = (X+2)(X^2-2)$. Le coefficient $a_3(f)$ est donc -2 ou est racine du polynôme $X^2 - 2$. On constate alors directement que l'on ne peut avoir $a_3(f) \equiv 0$ ou $\pm 4 \bmod \wp$, car p est ≥ 11. D'où le rèsultat dans ce cas.

(3) Supposons $L = 43$. La démonstration du théorème dans ce cas est analogue à celle du cas (1) ci-dessus. On a $g_0^+(86) = 4$ et $H_7(86) = (X^2-20)(X-2)^2$. Par ailleurs, on a

$$a_7(f) \equiv 0 \text{ ou } \pm 4 \text{ ou } \pm 8 \bmod \wp,$$

(cela se prouve comme le lemme 1 de [24]). On déduit de là que l'on doit avoir $p = 11$, et que f est l'une des deux newforms normalisées de $S_2^{\text{new}}(86)$ dont les q-développements à l'infini sont à coefficients dans l'anneau d'entiers A de $\mathbb{Q}(\sqrt{5})$. Posons encore $w = \frac{1+\sqrt{5}}{2}$. En utilisant de nouveau la méthode des graphes, on constate que les coefficients a_l, pour l premier compris entre 2 et 43, du q-développement à l'infini $\sum a_n q^n$ d'une de ces deux newforms, sont donnés par le tableau suivant :

l	2	3	5	7	11	13	17	19	23	29	31	37	41	43
a_l	1	w	$-1-w$	$2-4w$	$-4+4w$	$-2+4w$	$-w$	$5+w$	$3-3w$	$-2-3w$	$6+w$	$-2-w$	$-1-3w$	-1

Pour tous les nombres premiers $l \neq 2, 43$, compris entre 2 et 43, on a la congruence $a_l \equiv l+1 \bmod \wp_{11}$, où $\wp_{11}$ est l'idéal de A engendré par $3+2w$. L'idéal $\wp_{11}$ contient -2.44. Pour tout nombre premier $l \neq 2, 43$, on a donc $a_l(f) \equiv l+1 \bmod P$, où P est un idéal de A au-dessus de 11 (prop. 2 de l'appendice II) ; d'où $a_l(E) \equiv l+1 \bmod 11$ pour presque tout l premier, ce qui conduit encore à une contradiction, et prouve que f n'existe pas.

(4) Si $L = 47$, on a $g_0^+(94) = 3$ et $H_3(94) = X(X^2-8)$. La congruence $a_3(f) \equiv 0$ ou $\pm 4 \bmod \wp$, entraîne que $a_3(f) = 0$, et que les coefficients du q-développement de f à l'infini sont dans $\mathbb{Z}$. Par ailleurs, on a $H_5(94) = X(X^2-4X+2)$; d'où $a_5(f) = 0$ qui ne peut être congru modulo $\wp$ à ± 2 ou à ± 6, car p est ≥ 11. D'où le résultat dans ce cas, et le théorème.

7. **Appendice I : Sur la partie new de $S_2(N)$.** On reprend les notations introduites dans le paragraphe 1. Étant donnés un entier $n \geq 1$ et un entier k premier à n, on note par ailleurs :

- $T_k|_{S_2(n)}$ le k-ième opérateur de Hecke agissant sur $S_2(n)$. Le sous-espace $S_2^{\text{new}}(n)$ de $S_2(n)$ est stable par $T_k|_{S_2(n)}$. On note $T_k|_{S_2^{\text{new}}(n)}$ cet opérateur agissant sur $S_2^{\text{new}}(n)$ par restriction ;
- $\text{Tr}(T_k|_{S_2(n)})$ la trace de $T_k|_{S_2(n)}$;
- $\text{Tr}(T_k|_{S_2^{\text{new}}(n)})$ la trace de $T_k|_{S_2^{\text{new}}(n)}$.

Considérons désormais un entier $N \geq 1$ *fixé*. On détermine ici $g_0^+(N)$, et pour tout entier $k \geq 1$ premier à N, $\text{Tr}(T_k|_{S_2^{\text{new}}(N)})$ en termes des $\text{Tr}(T_k|_{S_2(d)})$, où d parcourt les diviseurs de N ; ils se trouvent dans [13] les formules permettant de calculer $\text{Tr}(T_k|_{S_2(d)})$.

Soit $\lambda\colon \mathbb{N}^* \longrightarrow \mathbb{N}$ la fonction arithmétique définie par les conditions suivantes :

(a) on a $\lambda(1) = 1$;

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

(b) on a $\lambda(mn) = \lambda(m)\lambda(n)$ si m et n sont deux entiers ≥ 1 premiers entre eux (*i.e.*, λ est une fonction multiplicative) ;

(c) si p est un nombre premier, on a $\lambda(p) = -2$, $\lambda(p^2) = 1$ et $\lambda(p^r) = 0$ si r est ≥ 3.

THÉORÈME. *Soit k un entier ≥ 1 premier à N. On a les égalités :*

$$\mathrm{Tr}(T_k|_{S_2^{\mathrm{new}}(N)}) = \sum_{d|N} \mathrm{Tr}(T_k|_{S_2(d)})\ \lambda\left(\frac{N}{d}\right), \tag{1}$$

$$g_0^+(N) = \sum_{d|N} g_0(d)\ \lambda\left(\frac{N}{d}\right). \tag{2}$$

DÉMONSTRATION. Pour tout entier $d \geq 1$ soit R_d l'opérateur qui à une fonction g sur le demi-plan de Poincaré associe la fonction $\tau \longmapsto g(d\tau)$. Étant donnés deux entiers d et $M \geq 1$ tels que $dM|N$, désignons par $S(d, M)$ le sous-espace vectoriel de $S_2(N)$ engendré par les éléments $R_d(f)$, où f parcourt $S_2^{\mathrm{new}}(M)$. D'après théorème 2.5. de [2] on a l'égalité

$$S_2(N) = \bigoplus_{dM|N} S(d, M). \tag{3}$$

Démontrons d'abord l'égalité (2). Soit σ_0 la fonction qui à un entier $n \geq 1$ associe le nombre des diviseurs de n. D'après la formule (3) on a

$$g_0(N) = \sum_{M|N} g_0^+(M)\ \sigma_0\left(\frac{N}{M}\right).$$

Autrement dit la fonction g_0 est le produit de convolution des fonctions $n \longmapsto g_0^+(n)$ et σ_0 (*cf.* [1], p. 29) : avec les notations de *loc. cit.*, on a $g_0 = g_0^+ * \sigma_0$. La fonction σ_0 possède un inverse σ_0^{-1} pour cette opération qui est donné par l'égalité

$$\sigma_0^{-1} = \mu * \mu,$$

où μ est la fonction de Möbius usuelle (*cf. loc. cit.*, p. 24, 2.2 et p. 39 th. 2.20). Tout revient alors à démontrer que l'on a

$$\mu * \mu = \lambda.$$

La fonction σ_0^{-1} est multiplicative (car σ_0 l'est) (*loc. cit.* p. 36, th. 2.16), et par hypothèse il en est de même de λ. Il suffit donc de vérifier la formule ci-dessus pour les puissances de nombres premiers, ce qui résulte directement des définitions.

En ce qui concerne la formule (1) la démonstration est analogue : les espaces $S(d, M)$ et $S_2^{\mathrm{new}}(M)$ sont isomorphes via R_d de façon compatible à l'action des opérateurs de Hecke. On déduit de là l'égalité

$$\mathrm{Tr}(T_k|_{S_2(N)}) = \sum_{dM|N} \mathrm{Tr}(T_k|_{S_2^{\mathrm{new}}(M)}),$$

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

i.e.,

$$\mathrm{Tr}(T_k|_{S_2(N)}) = \sum_{M\,|\,N} \mathrm{Tr}(T_k|_{S_2^{\mathrm{new}}(M)})\ \sigma_0\left(\frac{N}{M}\right).$$

La formule (1) résulte alors de nouveau du fait que $\sigma_0^{-1} = \lambda$. D'où le théorème.

REMARQUE. La fonction $n \longmapsto g_0^+(n)$ possède les propriétés suivantes :

(a) si N est un entier pair ≥ 2, on a $g_0^+(4N) \geq g_0^+(N)$;

(b) on a $g_0^+(N) = 0$ si et seulement si N appartient à l'ensemble

$$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60\}\,;$$

(c) on a $g_0^+(N) = 1$ si et seulement si N appartient à l'ensemble

$$\{11, 14, 15, 17, 19, 20, 21, 24, 27, 30, 32, 33, 34, 36, 40, 42,$$
$$44, 45, 46, 48, 49, 52, 64, 70, 72, 76, 78, 100, 108, 180\}.$$

Ces assertions sont utilisées dans la démonstration des théorèmes 1 et 2. Leur preuve, qui m'a été généreusement communiquée par E. Halberstadt, est trop longue pour être décrite ici.

8. **Appendice II : Sur les congruences modulo un idéal des formes modulaires.** Considérons un corps de nombres K et N un entier ≥ 1. Notons O_K l'anneau des entiers de K. On conserve les notations du paragraphe 1 ; en particulier si n est un entier $n \geq 1$, $\mu(n)$ est l'indice de $\Gamma_0(n)$ dans $\mathrm{SL}_2(\mathbb{Z})$ (*cf.* formule (2)).

PROPOSITION 1. *Soient k un entier ≥ 0, χ un caractère de Dirichlet de conducteur N et f une forme modulaire de poids k et de caractère χ pour $\Gamma_0(N)$, dont le développement de Taylor à l'infini $\sum_{n\geq 0} a_n q^n$ est à coefficients dans O_K. Soit J un idéal de O_K. Alors, si a_n appartient à J pour tout $n \leq \mu(N)k/12$, a_n appartient à J pour tout n.*

Si $K = \mathbb{Q}$, cet énoncé est essentiellement celui de la prop. de [18] p. 273, à ceci près qu'il convient de remplacer la constante $\big(\mu(N) - 1\big)k/12$ par $\mu(N)k/12$ (on obtient un contre-exemple à la prop. de *loc. cit.* en prenant pour f la forme modulaire de poids 2 pour $\Gamma_0(4)$ introduite dans la démonstration de la prop. 2 ci-dessous) ; la ligne 15 en haut de la p. 274 de [18] comporte une erreur : avec les notations de *loc. cit.*, il faut changer $\big(\mu(N) - i\big)m$ par $\big(\mu(N) - i\big)(m - l)$. En tenant compte de cette rectification on obtient la prop. 1 si $K = \mathbb{Q}$. Le cas où l'on remplace $\mathbb{Q}$ par K se démontre alors, à des modifications mineures près, par les mêmes arguments.

PROPOSITION 2. *Soit f une newform normalisée de $S_2^{\mathrm{new}}(N)$ dont le développement de Taylor à l'infini $\sum_{n\geq 1} a_n q^n$ est à coefficients dans O_K. Soient P un idéal premier de O_K et m un entier ≥ 1. Posons $M = \mathrm{ppcm}(4, N)$. Supposons réalisées les conditions suivantes :*

(i) pour tout nombre premier $l \leq \mu(M)/6$ ne divisant pas $2N$, on a

$$a_l \equiv l + 1 \bmod P^m\,;$$

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

(ii) pour tout nombre premier $l \leq \mu(M)/6$ *divisant* $2N$ *tel que* l^2 *ne divise pas* $4N$, $(l+1)(a_l - 1)$ *appartient à* P^m.

Alors, pour tout nombre premier l *qui ne divise pas* $2N$, *on a* $a_l \equiv l + 1 \bmod P^m$.

On déduit de la proposition 2 le résultat suivant :

COROLLAIRE. *Soit E une courbe elliptique modulaire définie sur* $\mathbb{Q}$ *de conducteur* N. *Étant donné un nombre premier* l *qui ne divise pas* N, *soit* n_l *le nombre de points sur* $\mathbb{F}_l$ *de la courbe elliptique sur* $\mathbb{F}_l$ *déduite de E par réduction modulo* l. *Posons* $M = \text{ppcm}(4, N)$. *Les conditions suivantes sont équivalentes :*

(i) pour tout nombre premier $l \leq \mu(M)/6$ *qui ne divise pas* $2N$, 4 *divise* n_l ;

(ii) pour tout nombre premier l *qui ne divise pas* $2N$, 4 *divise* n_l.

DÉMONSTRATION DU COROLLAIRE. Supposons que la condition (i) soit réalisée. Notons $\sum a_n(E)n^{-s}$ la fonction L de Hasse-Weil de E. Puisque E est modulaire, le q-développement $\sum a_n(E)q^n$ est une newform de $S_2^{\text{new}}(N)$. Considérons un nombre premier $l \leq \mu(M)/6$. Si l ne divise pas $2N$, on a $a_l(E) = 1 + l - n_l$, et l'hypothèse faite entraîne la congruence $a_l(E) \equiv l + 1 \bmod 4$. Supposons maintenant que l divise $2N$ et que l^2 ne divise pas $4N$. Dans ce cas l est impair, E a en l réduction de type multiplicatif, et l'on a $a_l(E) = \pm 1$. Ainsi 4 divise $(l+1)(a_l(E) - 1)$; les conditions (i) et (ii) de la proposition 2 sont donc satisfaites avec $K = \mathbb{Q}$, $P = 2\mathbb{Z}$ et $m = 2$. D'où le corollaire.

8.1 *Démonstration de la proposition 2.* Elle est analogue à celle de la prop. 4 p. 263 de [18]. Étant donné un entier $n \geq 1$, on note R_n l'opérateur qui à une fonction h sur le demi-plan de Poincaré H associe la fonction $\tau \longmapsto h(n\tau)$, et $\sigma_1(n)$ la somme des diviseurs de n.

Considérons la fonction g définie sur H par

$$\tau \longmapsto \sum_{\substack{n \geq 1 \\ n \text{ impair}}} \sigma_1(n) q^n \quad \text{avec } q = e^{2\pi i \tau}.$$

La fonction g est une forme modulaire de poids 2 et de caractère trivial pour le groupe $\Gamma_0(4)$, et est fonction propre de *tous* les opérateurs de Hecke (*cf.* [14], p. 145, 10 et p. 174, 2). La série de Dirichlet L_g associée à g définie par

$$L_g(s) = \sum_{\substack{n \geq 1 \\ n \text{ impair}}} \sigma_1(n) n^{-s},$$

possède donc un produit eulérien qui est donné par l'égalité

$$L_g(s) = \prod_{\substack{p \text{ premier} \\ \text{impair}}} \frac{1}{1 - (p+1)p^{-s} + p^{1-2s}} \qquad (\textit{cf. loc. cit.}, \text{ p. 160, prop. 36 et p. 163}).$$

Rappelons que la série de Dirichlet L_f associée à f possède aussi un produit eulérien qui est donné par

$$L_f(s) = \prod_{\substack{p \text{ premier} \\ (p,N)=1}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{\substack{p \text{ premier} \\ p \mid N}} \frac{1}{1 - a_p p^{-s}} \qquad (\textit{cf. loc. cit.}).$$

https://doi.org/10.4153/CJM-1997-056-2 Published online by Cambridge University Press

On a $a_p = \pm 1$ si p divise N et p^2 ne divise pas N, et $a_p = 0$ si p^2 divise N.

Considérons alors un nombre premier $l \leq \mu(M)/6$. Soit i l'exposant de l dans N. Définissons des opérateurs V_l et V_l' de la façon suivante (*cf.* dém. de la prop. 4 de [18]) :

(i) si $l = 2$ et $i = 0$, on pose $V_2 = 1 - a_2R_2 + 2R_4$ et $V_2' = 1$;
(ii) si $l = 2$ et $i = 1$, on pose $V_2 = 1 - a_2R_2$ et $V_2' = 1$;
(iii) si $l = 2$ et $i \geq 2$, on pose $V_2 = V_2' = 1$;
(iv) si $l \neq 2$ et $i = 0$, on pose $V_l = V_l' = 1$;
(v) si $l \neq 2$ et $i = 1$, on pose $V_l = 1$ et $V_l' = 1 - (l + 1 - a_l)R_l$;
(vi) si $l \neq 2$ et $i \geq 2$, on pose $V_l = 1$ et $V_l' = 1 - (l + 1)R_l + lR_{l^2}$.

Notons F et G les fonctions définies par

$$F = \left(\prod_{l \leq \mu(M)/6} V_l\right)(f) \qquad \text{et} \qquad G = \left(\prod_{l \leq \mu(M)/6} V_l'\right)(g).$$

Ce sont des formes modulaires de poids 2 pour $\Gamma_0(M)$. Les séries de Dirichlet associées à F et G possèdent des produits eulériens dont les facteurs en les nombres premiers $\leq \mu(M)/6$ sont des séries de Dirichlet à coefficients congrus modulo P^m. Les développements de Taylor de F et G sont donc congrus modulo P^m en degrés $\leq \mu(M)/6$; ils sont donc congrus modulo P^m (prop. 1). Par ailleurs, si l est un nombre premier $> \mu(M)/6$, les coefficients d'indice l des développements de F et G sont respectivement a_l et $l + 1$. Cela entraîne le résultat.

RÉFÉRENCES

1. T. M. Apostol, *Introduction to Analytic Number Theory*. Undergraduate Texts in Math., Springer-Verlag, 1976.
2. A. O. L. Atkin et J. Lehner, *Hecke operators on* $\Gamma_0(N)$. Math. Ann. **185**(1970), 134–160.
3. J. E. Cremona, *Algorithms for modular elliptic curves*. Cambridge University Press, 1992.
4. H. Darmon, *Serre's conjectures*. Seminar on Fermat's Last Theorem (Ed.: V. Kumar Murty), CMS Conference Proceedings **17**(1995), 135–153.
5. H. Darmon et L. Merel, *Winding quotients and some variants of Fermat's last Theorem*. J. Crelle **490**(1997).
6. P. Deligne, *La conjecture de Weil. I*, Publ. Math. I.H.E.S. **43**(1973), 273–307.
7. ———, *Représentations l-adiques*. S.M.F, Astérisque, **127**(1985), 249–255.
8. P. Dénes, *Über die Diophantische Gleichung* $x^l + y^l = cz^l$. Acta Math. **88**(1952), 241–251.
9. F. Diamond, *On deformation rings and Hecke rings*. Ann. of Math. **144**(1996), 137–166.
10. F. Diamond et K. Kramer, *Modularity of a family of elliptic curves*. Math. Res. Lett. **2**(1995), 299–304.
11. G. Frey, *Links between solutions of* $A - B = C$ *and elliptic curves*. Lecture Notes in Math. **1380** 1989, 31–62.
12. ———, *On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2*. Dans : Elliptic Curves, Modular Forms, & Fermat's Last Theorem (Rédacteurs : J. Coates et S. T. Yau), International Press, 1995.
13. H. Hijikata, *Explicit formula of the traces of Hecke operators for* $\Gamma_0(N)$. J. Math. Soc. Japan **26**(1974), 56–82.
14. N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*. Graduate Texts in Math. **97**, Springer-Verlag, 1984.
15. A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*. Manuscripta Math. **69**(1990), 353–385.
16. ———, *Une remarque sur les points de torsion des courbes elliptiques*. C.R. Acad. Sci. Paris t. **321** Série I(1995), 1143–1146.

17. ———, *Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique*. Dissertationes Math. **364**(1997), 39 pp.
18. A. Kraus et J. Oesterlé, *Sur une question de B. Mazur*. Math. Ann. **293**(1992), 259–275.
19. J.-F. Mestre, *La méthode des graphes. Exemples et applications*. Taniguchi Symp., Kyoto, 1986, 217–242.
20. J. Oesterlé, *Nouvelles approches du "théorème de Fermat"*. Sém. Bourbaki **694**, 1987–88.
21. K. Ribet, *On the equation* $a^p + 2^\alpha b^p + c^p = 0$. Acta Arith., à paraître.
22. J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15**(1972), 259–331.
23. ———, *Modular forms of weight one and Galois representations.* Algebraic Number Theory (Rédacteur : A. Fröhlich), New York, Academic Press, 1977, 193–268.
24. ———, *Sur les représentations modulaires de degré 2 de Gal* $(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54**(1987), 179–230.
25. ———, *Abelian l-Adic Representations and Elliptic Curves*. Advanced book classics series, Addison-Wesley, 1989 (publié originalement en 1968 par W. A. Benjamin, Inc.).
26. ———, *Travaux de Wiles (et Taylor, . . .), I*. Sém. Bourbaki **803**, 1994–95.
27. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Publ. Math. Soc. Japan **11**, Princeton Univ. Press, 1971.
28. J. Silverman, *The Arithmetic of Elliptic Curves*. Graduate Texts in Math. **106**, Springer-Verlag, 1986.
29. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*. Dans : Modular Functions of One Variable IV, Lecture Notes in Math. **476**(1975), 33–52.
30. A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*. Ann. of Math. **141**(1995), 443–551.

Université de Paris VI
Institut de Mathématiques, Case 247
4, place Jussieu
75252 Paris Cedex 05
France