ACTA ARITHMETICA
108.4 (2003)

# Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$

par

Wilfrid Ivorra (Montreuil)

**Introduction.** Soient $p$ un nombre premier $\geq 5$ et $\beta$ un entier tels que $0 \leq \beta \leq p-1$. On s'intéresse dans cet article à l'étude des équations

$$x^p + 2^\beta y^p = z^2, \tag{1}$$

$$x^p + 2^\beta y^p = 2z^2. \tag{2}$$

Soient $a$ et $b$ deux entiers *relatifs* et $c$ un entier *naturel*. Nous dirons que $(a,b,c)$ est une solution de l'équation (1) si l'on a $a^p + 2^\beta b^p = c^2$, que cette solution est *propre* si l'on a $\mathrm{pgcd}(a,b,c) = 1$ et qu'elle est *non triviale* si $abc$ est non nul. Nous définissons de même le fait pour $(a,b,c)$ d'être une solution propre non triviale de l'équation (2). On notera $S_0(\beta,p)$ l'ensemble des solutions propres non triviales de l'équation (1) et $S_1(\beta,p)$ son analogue pour l'équation (2).

En 1993, H. Darmon a étudié l'équation (1) dans le cas où $\beta = 0$ ; il a démontré que $S_0(0,p)$ est vide si $p \geq 17$ et $p \equiv 1 \bmod 4$ (cf. [9]). En 1997, H. Darmon et L. Merel ont ensuite prouvé que $S_0(0,p)$ est vide pour tout $p \geq 7$ ([11]), et B. Poonen a étendu ce résultat au cas où $p = 5$ ([19]). Par ailleurs, les travaux de N. Bruin en 1999 permettent de prouver que l'on a (cf. [5] et [6]) :

$$S_0(1,5) = \{(-1,1,1)\}, \quad S_0(2,5) = \{(2,1,6)\}, \quad S_0(3,5) = \{(1,1,3)\},$$
$$S_0(4,5) = \{(2,-1,4)\}, \quad S_1(0,5) = \{(-1,3,11),(3,-1,11),(1,1,1)\}.$$

De plus, $S_1(\beta,5)$ est vide si $\beta$ est non nul. On le vérifie facilement si $\beta$ est pair ; si $\beta$ est impair, cela se déduit directement des égalités ci-dessus. On pourra trouver en Appendice quelques indications sur la démonstration de ces résultats.

Lorsque l'on a $p \geq 7$, en utilisant les travaux de Wiles et Ribet sur les représentations modulaires ([20] et [25]), on détermine dans ce travail les ensembles $S_0(\beta,p)$ si $\beta$ est distinct de 1 et $p-1$, ainsi que les ensem-

2000 *Mathematics Subject Classification*: 11D41.

bles $S_1(\beta,p)$. On donne quelques résultats partiels concernant $S_0(1,p)$ et $S_0(p-1,p)$.

Par ailleurs, en 1997, Y. Bugeaud s'est intéressé à l'existence de certains quadruplets d'entiers $(x,y,m,n)$ vérifiant l'égalité

$$x^2-2^m=y^n,$$

pour lesquels il obtient un énoncé de finitude et une majoration de $n$ de l'ordre de $10^6$ ([7]). Les résultats que l'on démontre sur l'équation (1) permettent de déterminer ces quadruplets dans le cas où $m\geq 2$.

Je remercie N. Bruin, Y. Bugeaud et A. Kraus pour les conversations que j'ai eues avec eux pendant ce travail, ainsi que M. Bennett et C. Skinner pour m'avoir signalé qu'ils avaient obtenu par ailleurs les résultats présentés ici ([3]).

**1. Énoncé des résultats.** Soient $p$ un nombre premier supérieur ou égal à 7 et $\beta$ un entier naturel vérifiant les inégalités $0\leq\beta\leq p-1$.

THÉORÈME 1. (a) *Si $\beta$ est distinct de* 1, 3, $p-3$ *et* $p-1$, *l'ensemble $S_0(\beta,p)$ est vide.*

(b) $S_0(3,p)=\{(1,1,3)\}$.

(c) $S_0(p-3,p)=\{(2,1,3\cdot 2^{(p-3)/2})\}$.

(d) *Si $(a,b,c)$ est un élément de $S_0(1,p)$, l'entier $ab$ est impair.*

(e) *Si $(a,b,c)$ est un élément de $S_0(p-1,p)$, on a $a\equiv 2 \bmod 4$.*

Comme conséquence de ce résultat, on obtient l'énoncé suivant :

COROLLAIRE. *Soit $S$ l'ensemble des quadruplets $(x,y,m,n)\in\mathbb{Z}^4$ vérifiant les conditions suivantes* :

(i) $x^2-2^m=y^n$ ;

(ii) $x\geq 1$ *et* $y$ *est distinct de* 0 *et* $\pm 1$ ;

(iii) $\operatorname{pgcd}(x,y)=1$ ;

(iv) $m\geq 2$ *et* $n\geq 3$.

*Alors, $S$ est égal à* $\{(13,-7,9,3),(71,17,7,3)\}$.

THÉORÈME 2. (a) *Si $\beta$ est non nul, l'ensemble $S_1(\beta,p)$ est vide.*

(b) $S_1(0,p)=\{(1,1,1)\}$.

**2. Démonstration du théorème 1.** On considère un élément $(a,b,c)$ de $S_0(\beta,p)$. Compte tenu des résultats de [11] rappelés dans l'introduction, on supposera désormais que l'on a $\beta\geq 1$.

Étant donné un entier $n$, on notera $v_2(n)$ la valuation 2-adique de $n$.

**2.1.** *Cas où a est impair.* Démontrons l'énoncé suivant :

PROPOSITION 1. *Supposons a impair. Alors, l'une des conditions suivantes est vérifiée* :

(a) $\beta = 1$ *et* $b$ *est impair*;
(b) $\beta = 3$ *et* $(a, b, c) = (1, 1, 3)$.

On considère pour cela la courbe elliptique $E_0$ sur $\mathbb{Q}$ d'équation de Weierstrass

$$y^2 = x^3 + 2cx^2 + a^p x. \tag{3}$$

Les invariants standard $c_4$, $c_6$ et $\Delta$ associés à cette équation sont ([24, p. 36]) :

$$c_4 = 2^4(4c^2 - 3a^p), \quad c_6 = 2^6 c(9a^p - 8c^2), \quad \Delta = 2^{6+\beta} a^{2p} b^p.$$

On désigne par $N_{E_0}$ le conducteur de $E_0$.

LEMME 1. (a) *Soit $\ell$ un nombre premier impair. L'équation* (3) *est minimale en $\ell$. Si $\ell$ ne divise pas $ab$, $E_0$ a bonne réduction en $\ell$. Si $\ell$ divise $ab$, $E_0$ a réduction multiplicative en $\ell$.*

(b) *Supposons b impair. Si $\beta$ est distinct de* 1 *et* 3, *on a $v_2(N_{E_0}) \leq 4$. De plus*,

$$v_2(N_{E_0}) = \begin{cases} 7 & \text{si } \beta = 1, \\ 5 & \text{si } \beta = 3. \end{cases}$$

(c) *Si b est pair, on a $v_2(N_{E_0}) \leq 4$.*

*Démonstration.* Par définition, si $\ell$ ne divise pas $ab$, $E_0$ a bonne réduction en $\ell$. Si $\ell$ divise $ab$, le fait que les entiers $a$, $b$ et $c$ soient premiers entre eux entraîne que $\ell$ ne divise pas $c_4$, puis l'assertion (a). Par ailleurs, si $b$ est impair, on a ($a$ étant impair)

$$v_2(\Delta) = 6 + \beta, \quad v_2(c_4) = 4, \quad v_2(c_6) = 6.$$

La classification qui se trouve dans le tableau IV de [18] implique alors directement l'assertion (b). De même, si $b$ est pair, on a

$$v_2(\Delta) = 6 + \beta + pv_2(b), \quad v_2(c_4) = 4, \quad v_2(c_6) = 6,$$

et le tableau IV de [18] entraîne l'assertion (c). D'où le lemme.

Soit $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ contenue dans $\mathbb{C}$. Notons $E_0[p]$ le sous-groupe des points de $p$-torsion de $E_0(\overline{\mathbb{Q}})$. C'est un espace vectoriel de dimension 2 sur $\mathbb{Z}/p\mathbb{Z}$ sur lequel le groupe de Galois $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ opère de façon naturelle. Soit

$$\varrho_p^{E_0} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E_0[p])$$

la représentation ainsi obtenue. Soient $k$ et $N(\varrho_p^{E_0})$ le poids et le conducteur de $\varrho_p^{E_0}$ respectivement, qui sont définis par J.-P. Serre dans [22].

LEMME 2. (a) $k = 2$.

(b) *Supposons $b$ impair. Si $\beta$ est distinct de 1 et 3, il existe un entier $s \leq 4$ tel que $N(\varrho_p^{E_0}) = 2^s$. De plus,*

$$N(\varrho_p^{E_0}) = \begin{cases} 2^7 & si\ \beta = 1, \\ 2^5 & si\ \beta = 3. \end{cases}$$

(c) *Supposons $b$ pair. Il existe un entier $s \leq 4$ tel que $N(\varrho_p^{E_0}) = 2^s$.*

*Démonstration.* D'après le lemme 1, l'exposant de $p$ dans le discriminant minimal de $E_0$ est multiple de $p$. La proposition 5 p. 191 de [22] implique alors $k = 2$. Les assertions (b) et (c) sont des conséquences directes du lemme 1 et de la proposition p. 28 de [14].

LEMME 3. *La représentation $\varrho_p^{E_0}$ est irréductible.*

*Démonstration.* On suppose que $\varrho_p^{E_0}$ est réductible.

(1) Supposons $p = 11$ ou $p \geq 17$. D'après le corollaire 4.4 de [17], $E_0$ a potentiellement bonne réduction en tout nombre premier impair. Le lemme 1 montre alors que $a = \pm 1$ (puisque $a$ est impair) et que $b = \pm 2^r$ où $r$ est un entier. On obtient ainsi $2^{\beta + rp} = c^2 \pm 1$. Cela entraîne $r = 0$, $ab = \pm 1$ et $c \in \{1, 3\}$. Il en résulte que l'on a $\beta = 1$ ou $\beta = 3$ et donc que $N_{E_0}$ est égal à 128 ou 32 (lemme 1), ce qui conduit à une contradiction (cf. [8, p. 111 et p. 122]) et prouve le lemme dans ce cas.

(2) Supposons $p = 13$ ; puisque $E_0$ possède un point d'ordre 2 rationnel sur $\mathbb{Q}$, il existe un sous-groupe de $E_0(\overline{\mathbb{Q}})$ d'ordre 26 stable par $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Par ailleurs, la jacobienne de la courbe modulaire $X_0(26)$ est isogène sur $\mathbb{Q}$ à un produit de deux courbes elliptiques de rang 0 sur $\mathbb{Q}$. Si $\ell$ est un nombre premier impair, $E_0$ a donc potentiellement bonne réduction en $\ell$ ([17, cor. 4.3]). Cela conduit à $ab = \pm 1$, et l'on conclut comme ci-dessus.

(3) Si $p = 7$, la courbe modulaire $X_0(14)$ est une courbe elliptique de rang 0 sur $\mathbb{Q}$ ([16, th. 5.1.1]), ce qui entraîne de nouveau une contradiction. D'où le lemme.

Terminons maintenant la preuve de la proposition 1. Étant donné un entier $n \geq 1$, notons $S_2(\Gamma_0(n))$ le $\mathbb{C}$-espace vectoriel des formes modulaires paraboliques de poids 2 pour le sous-groupe de congruence $\Gamma_0(n)$. Désignons par $S_2^+(n)$ le sous-espace vectoriel de $S_2(\Gamma_0(n))$ engendré par les *newforms* au sens de [1] ; c'est un espace vectoriel de dimension finie $g_0^+(n)$ sur $\mathbb{C}$ ; on pourra trouver dans [15] la détermination de $g_0^+(n)$.

La représentation $\varrho_p^{E_0}$ étant irréductible de poids 2 et $E_0$ étant modulaire (cf. [12] et [25]), il existe une newform $f$ de $S_2^+(N(\varrho_p^{E_0}))$ dont le développement de Taylor à l'infini est

$$\tau \mapsto q + \sum_{n \geq 2} a_n(f) q^n \quad \text{où } q = \exp(2\pi i \tau),$$

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

$$a_\ell(f) \equiv a_\ell(E_0) \bmod \mathfrak{P} \qquad \text{si } \ell \text{ ne divise pas } pN_{E_0}. \tag{4}$$

(On pourra consulter à ce sujet la remarque 2, p. 325 de [23].)

Supposons que $\beta$ soit distinct de 1 et 3. D'après le lemme 2, il existe un entier $s \leq 4$ tel que $N(\varrho_p^{E_0}) = 2^s$. On a $g_0^+(2^s) = 0$, d'où une contradiction, et le fait que $(a, b, c)$ n'existe pas dans ce cas.

Si $\beta = 1$, l'assertion (c) du lemme 2 et le même argument que celui utilisé ci-dessus entraînent que $b$ est impair.

Supposons $\beta = 3$. Comme ci-dessus $b$ est impair ; on a $N(\varrho_p^{E_0}) = 32$ et $g_0^+(32) = 1$. La newform $f$ correspond donc à la courbe elliptique $E$ de conducteur 32 d'équation

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

qui est celle notée $32A2$ dans les tables de [8]. C'est une courbe à multiplications complexes par l'anneau d'entiers de $\mathbb{Q}(i)$.

Soit $\varrho_p^E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p])$ la représentation donnant l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur le sous-groupe des points de $p$-torsion de $E(\overline{\mathbb{Q}})$. Il résulte de la condition (4) que $\varrho_p^{E_0}$ et $\varrho_p^E$ ont des semi-simplifiées isomorphes. Puisqu'elles sont irréductibles, elles sont donc isomorphes. L'image de $\varrho_p^{E_0}$ est donc contenue dans le normalisateur d'un sous-groupe de Cartan $C$ de $\mathrm{Aut}(E_0[p])$ (cf. [21]).

(1) Supposons que $C$ soit déployé. On a alors $p \equiv 1 \bmod 4$. Si l'on a $p \geq 17$, le théorème 1 de [13] implique $N_{E_0} = 32$. L'entier $b$ étant impair, on déduit de là que $ab = \pm 1$ (lemme 1), puis $(a, b, c) = (1, 1, 3)$. On a la même conclusion si $p = 13$ (cf. [11, p. 89, deuxième alinéa de la démonstration de la prop. 4.2]).

(2) Supposons que $C$ soit non déployé. L'image de $\varrho_p^{E_0}$ est alors le normalisateur de $C$ (cf. [21, prop. 12]). La courbe elliptique $E_0$ possède un point d'ordre 2 rationnel sur $\mathbb{Q}$. L'invariant modulaire $j$ de $E_0$ appartient donc à $\mathbb{Z}[1/p]$ ([11, th. 8.1]). On a l'égalité

$$j = \frac{8(4c^2 - 3a^p)^3}{(a^2 b)^p}.$$

Les entiers $8(4c^2 - 3a^p)^3$ et $ab$ sont premiers entre eux. On déduit de là que $ab$ est au signe près une puissance de $p$, puis que $p$ divise $ab$ ou bien que $ab = \pm 1$.

Supposons que $p$ divise $ab$. Dans ce cas, $E_0$ a mauvaise réduction de type multiplicatif en $p$. Soit $I$ un sous-groupe d'inertie en $p$ de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (qui est bien défini à conjugaison près). L'ordre de $\varrho_p^{E_0}(I)$ est $p - 1$ ou $p(p - 1)$ (cf. [21, prop. 13]). Par ailleurs, $E$ a par hypothèse bonne réduction de hauteur 2 en $p$, donc l'ordre de $\varrho_p^E(I)$ est $p^2 - 1$ ([21, prop. 12]). Cela contredit le

fait que $\varrho_p^E$ et $\varrho_p^{E_0}$ sont isomorphes ; ainsi $p$ ne divise pas $ab$. Par conséquent, $ab = \pm 1$ et l'on a de nouveau $(a, b, c) = (1, 1, 3)$.

Cela termine la démonstration de la proposition 1.

**2.2.** *Cas où a est pair.* On va démontrer dans ce cas l'énoncé suivant :

PROPOSITION 2. *Supposons a pair. Alors, l'une des conditions suivantes est vérifiée* :

(a) $\beta = p - 1$ *et* $v_2(a) = 1$ ;
(b) $\beta = p - 3$ *et* $(a, b, c) = (2, 1, 3 \cdot 2^{(p-3)/2})$.

*Démonstration.* On remarque d'abord que $c$ est pair et par suite $b$ est impair. Il existe donc un entier impair $c_1 \geq 1$ tel que l'on ait $c^2 = 2^\beta c_1^2$. Par ailleurs, il existe un entier $r \geq 1$ et un entier impair $a_1$ tels que $a = 2^r a_1$. On a $2^{rp-\beta} a_1^p + b^p = c_1^2$. Soient $u$ et $t$ des entiers tels que $rp - \beta = up + t$ avec $1 \leq t \leq p - 1$. On a l'égalité

$$b^p + 2^t (2^u a_1)^p = c_1^2.$$

Les entiers $b$, $a_1$ et $c_1$ sont non nuls et premiers entre eux. On déduit de là que $(b, 2^u a_1, c_1)$ appartient à $S_0(t, p)$. Puisque $b$ est impair, il résulte de la proposition 1 que l'on est dans l'un des deux cas suivants :

(1) $t = 1$, auquel cas $u = 0$ (prop. 1), puis $r = 1$. Cela conduit à $\beta = p - 1$ et $v_2(a) = 1$.

(2) $t = 3$. Dans ce cas, on a $(b, 2^u a_1, c_1) = (1, 1, 3)$ (prop. 1). On obtient ainsi $b = 1$. De plus, on a $u = 0$, puis $r = 1$ et par suite $\beta = p - 3$. On déduit ensuite que $a = 2$ et que $c = 3 \cdot 2^{(p-3)/2}$. D'où la proposition.

Le théorème 1 est alors une conséquence directe des propositions 1 et 2.

REMARQUES. (1) Nous donnons une description incomplète de $S_0(1, p)$. Cela tient au fait que si $(a, b, c)$ appartient à $S_0(1, p)$ et si $a$ est impair, on a $N(\varrho_p^{E_0}) = 2^7$ (prop. 1 et lemme 1). Les courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^7$ n'étant pas à multiplications complexes, les arguments que l'on utilise dans ce travail semblent insuffisants pour déterminer $S_0(1, p)$.

Cela étant, la conjecture ci-dessous concernant la comparaison galoisienne des points de torsion des courbes elliptiques entraîne que $S_0(1, p) = \{(-1, 1, 1)\}$ dès que $p$ est assez grand (cf. par exemple [10, p. 148]) :

CONJECTURE. *Soit $A$ une courbe elliptique définie sur $\mathbb{Q}$. Soit $P$ l'ensemble des nombres premiers $p$ pour lesquels il existe une courbe elliptique sur $\mathbb{Q}$, non isogène à $A$ sur $\mathbb{Q}$, dont le module galoisien des points de $p$-torsion soit isomorphe à celui de $A$. Alors, $P$ est fini.*

(2) On est confronté à la même situation si $\beta = p - 1$. En effet, si $(a, b, c)$ appartient à $S_0(p - 1, p)$ l'équation (3) n'est pas minimale en 2 : on a $v_2(a) = 1$, $v_2(c^2) = p - 1$, et si l'on pose $a = 2a_1$, $c^2 = 2^{p-1} c_1^2$, $p = 4t + r$ avec

$r = 1$ ou 3, le changement de variables $x = 2^{2t}X$, $y = 2^{3t}Y$ transforme (3) en le modèle

$$Y^2 = X^3 + 2^{(r+1)/2}c_1X^2 + 2^r a_1^p X,$$

qui est minimal. On déduit de là que $v_2(N_{E_0}) = 7$ et l'on a encore $N(\varrho_p^{E_0}) = 2^7$.

**3. Démonstration du corollaire.** Soit $(a, b, m, n)$ un élément de $S$. Puisque $a$ et $b$ sont premiers entre eux, $a$ et $b$ sont impairs. Par ailleurs, $n$ est impair ([7, p. 3205, sect. 4]).

Soit $p$ un diviseur premier de $n$. Posons $n = rp$ et $m = tp + u$, avec $0 \le u \le p - 1$. On a l'égalité

$$(b^r)^p + 2^u(2^t)^p = a^2,$$

autrement dit, $(b^r, 2^t, a)$ est un élément de $S_0(u, p)$.

Si $p \ge 7$, il résulte du théorème 1 que l'on est dans l'un des cas suivants :

(i) $u = 1$, $t = 0$, d'où $m = 1$ ;
(ii) $u = 3$ et $(b^r, 2^t, a) = (1, 1, 3)$, d'où $b = 1$ ;
(iii) $u = p - 3$ et $(b^r, 2^t, a) = (2, 1, 3 \cdot 2^{(p-3)/2})$, d'où $b = 2$ ;
(iv) $u = p - 1$ et $b$ est pair.

Cela conduit à une contradiction.

Si $p = 5$, les résultats issus des travaux de N. Bruin, rappelés dans l'introduction, montrent que l'on a

$$(u, b^r, 2^t, a) \in \{(1, -1, 1, 1), (2, 2, 1, 6), (3, 1, 1, 3), (4, 2, -1, 4)\},$$

d'où $b \in \{\pm 1, 2\}$, et l'on obtient de nouveau une contradiction.

Si $p = 3$, on a $(b^r)^3 - a^2 = -2^m$, et la table 4a, p. 125 de [4] entraîne alors que l'on a

$$(a, b^r, m) \in \{(13, -7, 9), (71, 17, 7)\},$$

ce qui implique $r = 1$ puis $n = 3$. D'où le corollaire.

**4. Démonstration du théorème 2.** On considère un élément $(a, b, c)$ de $S_1(\beta, p)$.

Démontrons l'assertion (a) du théorème :

PROPOSITION 3. $\beta = 0$.

*Démonstration.* Supposons que l'on ait $\beta \ge 1$. On a alors

$$a \equiv 0 \bmod 2, \quad b \equiv 1 \bmod 2, \quad \beta = 2v_2(c) + 1. \tag{5}$$

Posons $a = 2^r a_1$ où $a_1$ impair et $r \ge 1$, et $c = 2^{(\beta-1)/2}c_1$. On a l'égalité

$$2^{rp-\beta}a_1^p + b^p = c_1^2. \tag{6}$$

Il existe deux entiers naturels $q$ et $u$ tels que l'on ait $rp - \beta = qp + u$ et $1 \leq u \leq p-1$. L'égalité (6) s'écrit

$$b^p + 2^u(2^q a_1)^p = c_1^2.$$

Le triplet $(b, 2^q a_1, c_1)$ appartient donc à $S_0(u,p)$. Puisque $b$ est impair, la proposition 1 implique $u = 1$ ou $u = 3$. Par ailleurs, on a la congruence $\beta \equiv -u \bmod p$. On déduit de là que $\beta = p - u$, ce qui contredit le fait que $\beta$ soit impair. D'où le résultat.

Prouvons maintenant l'assertion (b). Il résulte de la proposition 3 que l'on a

$$ab \equiv 1 \bmod 2. \tag{7}$$

On considère la courbe elliptique $E_1$ sur $\mathbb{Q}$ d'équation de Weierstrass

$$y^2 = x^3 + 4cx^2 + 2b^p x. \tag{8}$$

Les invariants standard $c_4$, $c_6$ et $\Delta$ associés à cette équation sont (cf. [24]) :

$$c_4 = 2^5(8c^2 - 3b^p), \quad c_6 = 2^8 c(9b^p - 16c^2), \quad \Delta = 2^9 a^p b^{2p}.$$

Soit $N_{E_1}$ le conducteur de $E_1$.

Lemme 4. (a) *Soit $\ell$ un nombre premier. L'équation* (8) *est minimale en $\ell$. Si $\ell$ ne divise pas $2ab$, $E_1$ a bonne réduction en $\ell$. Si $\ell$ divise $ab$, $E_1$ a réduction multiplicative en $\ell$.*

(b) $v_2(N_{E_1}) = 8$.

*Démonstration.* La condition (7) implique la minimalité de l'équation (8) en 2. Si $\ell$ est un diviseur premier de $ab$, $\ell$ ne divise pas $c_4$ car $a$, $b$ et $c$ sont premiers entre eux ; d'où l'assertion (a). Par ailleurs, on a

$$v_2(c_4) = 5, \quad v_2(c_6) \geq 8, \quad v_2(\Delta) = 9,$$

ce qui entraîne l'assertion (b) ([18, tableau IV]).

Notons $E_1[p]$ le sous-groupe des points de $p$-torsion de $E_1(\overline{\mathbb{Q}})$ et $\varrho_p^{E_1}$ la représentation donnant l'action de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur $E_1[p]$. Soient $k$ et $N(\varrho_p^{E_1})$ le poids et le conducteur de $\varrho_p^{E_1}$ respectivement.

Lemme 5. *$k = 2$ et $N(\varrho_p^{E_1}) = 2^8$.*

La preuve de ce lemme est identique à celle du lemme 2.

Lemme 6. *La représentation $\varrho_p^{E_1}$ est irréductible.*

*Démonstration.* On suppose que $\varrho_p^{E_1}$ est réductible. Comme dans la démonstration du lemme 3, cette condition entraîne que $E_1$ a potentiellement bonne réduction en tout nombre premier impair. D'après (7), cela implique $ab = \pm 1$, puis $(a,b,c) = (1,1,1)$. On déduit de là que $N_{E_1} = 2^8$, ce qui conduit à une contradiction (cf. [8, p. 139]). D'où le lemme.

On déduit alors des lemmes 5 et 6 l'existence d'une newform $f$ de $S_2^+(2^8)$ dont le développement de Taylor à l'infini est

$$\tau \mapsto q + \sum_{n\geq 2} a_n(f) q^n \quad \text{où } q = \exp(2\pi i \tau),$$

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

$$a_\ell(f) \equiv a_\ell(E_1) \bmod \mathfrak{P} \qquad \text{si } \ell \text{ ne divise pas } 2pab, \tag{9}$$

$$a_\ell(f) \equiv \pm(\ell+1) \bmod \mathfrak{P} \qquad \text{si } \ell \text{ divise } ab \text{ et } \ell \neq p \tag{10}$$

(la condition (10) s'obtient en utilisant la théorie de la courbe de Tate qui fournit une description de la restriction de $\varrho_p^{E_1}$ à un sous-groupe de décomposition en $\ell$).

On a $g_0^+(2^8) = 6$. On est donc dans l'un des cas suivants :

(i) la newform $f$ correspond à l'une des quatre classes d'isogénie de courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^8$ (cf. [8, p. 139]) ;

(ii) les coefficients $a_n(f)$ appartiennent à un corps quadratique $K_f$.

Le cas (ii) ne convient pas : en effet, on vérifie que le polynôme caractéristique de l'opérateur de Hecke $T_3$ agissant sur $S_2^+(2^8)$ est

$$X^2(X-2)(X+2)(X^2-8).$$

Il en résulte que $K_f = \mathbb{Q}(\sqrt{2})$, et que l'on a $a_3(f) = \pm 2\sqrt{2}$. Par ailleurs, $E_1$ ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, on déduit des congruences (9) et (10) que l'on a

$$a_3(f) \equiv 0, \pm 2 \bmod \mathfrak{P} \qquad \text{si 3 ne divise pas } ab,$$

$$a_3(f) \equiv \pm 4 \bmod \mathfrak{P} \qquad \text{si 3 divise } ab.$$

Cela entraîne une contradiction et prouve notre assertion.

Comme me l'a fait remarquer le referee de cet article, on peut aussi démontrer que le cas (ii) ne convient pas en utilisant le fait que $f$ est à multiplications complexes par $\mathbb{Q}(\sqrt{-2})$.

On est donc dans le cas (i). On constate que les courbes elliptiques sur $\mathbb{Q}$ de conducteur $2^8$ sont à multiplications complexes par l'anneau d'entiers de $K$, où $K$ est le corps $\mathbb{Q}(i)$ ou $\mathbb{Q}(\sqrt{-2})$. On déduit de là que l'image de $\varrho_p^{E_1}$ est contenue dans le normalisateur d'un sous-groupe de Cartan $C$ de $\mathrm{Aut}(E_1[p])$.

(i.1) Supposons que $C$ soit déployé. Dans ce cas, $p$ est décomposé dans $K$ et on a $p \geq 11$. Si $p$ est distinct de 13, on doit avoir $N_{E_1} = 2^8$ (cf. [13, th. 1]), ce qui entraîne $(a,b,c) = (1,1,1)$. Si $p = 13$, on a la même conclusion (cf. [11, p. 89, deuxième alinéa de la preuve de la prop. 4.2]).

(i.2) Supposons que $C$ soit non déployé. L'image de $\varrho_p^{E_1}$ est alors le normalisateur de $C$ (cf. [21, prop. 12]). D'après le théorème 8.1 de [11], l'invariant modulaire de $E_1$ doit appartenir à $\mathbb{Z}[1/p]$. Cela entraîne $ab = \pm 1$ puis $(a, b, c) = (1, 1, 1)$, ou bien que $p$ divise $ab$ ; cette dernière possibilité ne peut se produire, comme on le vérifie en utilisant les mêmes arguments que ceux qui se trouvent dans l'alinéa (2) de la preuve du théorème 1.

Cela termine la démonstration du théorème 2.

**Appendice.** On se propose ici de fournir quelques indications sur la méthode décrite par N. Bruin dans [5] qui permet de démontrer les résultats, signalés dans l'introduction, à propos des ensembles $S_0(\beta, 5)$ et $S_1(0, 5)$.

L'assertion concernant $S_0(3, 5)$ peut se déduire directement du lemme 4.8.3 et des propositions 4.8.17 et 4.8.18 de [5] (signalons que dans l'énoncé de la prop. 4.8.18, on a en fait $X(P) = -1$). De même, celle concernant $S_1(0, 5)$ résulte du lemme 4.8.2 et des propositions 4.8.14, 4.8.15 et 4.8.16 de [5].

Indiquons la démarche suivie pour la détermination de l'ensemble $S_0(1, 5)$. On considère un élément $(a, b, c)$ de $S_0(1, 5)$. On a

$$a^5 + 2b^5 = c^2.$$

Choisissons une racine $\alpha$ dans $\mathbb{C}$ du polynôme $X^5 - 2$ et notons $K$ le corps $\mathbb{Q}(\alpha)$. Posons

$$Q = X^4 + \alpha X^3 + \alpha^2 X^2 + \alpha^3 X + \alpha^4.$$

Alors $X^5 - 2 = (X - \alpha)Q$. On a le résultat suivant :

Proposition. *Soient $C_1$ et $C_2$ les quartiques définies sur $K$ d'équations*

$$C_1 : \quad y^2 = Q(x) \quad \text{et} \quad C_2 : \quad (\alpha - 1)y^2 = Q(x).$$

*Alors, il existe $z \in K$ tel que*

$$\left(-\frac{a}{b}, z\right) \in C_1(K) \cup C_2(K).$$

*Démonstration.* Notons $\widetilde{Q}$ le polynôme homogène associé à $Q$. On a l'égalité

$$(a + \alpha b)\widetilde{Q}(a, -b) = c^2.$$

L'anneau des entiers $O_K$ de $K$ est principal (cf. [2]). Soit $\pi$ un élément irréductible de $O_K$ dont l'exposant dans la décomposition de $a + \alpha b$ en produit d'éléments irréductibles de $O_K$ est impair. On vérifie que $\pi$ divise 2 ou 5, puis que $\pi$ est associé à $\alpha$ ou $\alpha^2 + 1$. Par ailleurs, les entiers

$$u_1 = \alpha - 1 \quad \text{et} \quad u_2 = \alpha^3 + \alpha + 1$$

forment une base du groupe des unités de $O_K$ modulo $\{\pm 1\}$ (cf. [2]). On déduit de là l'existence d'entiers $n_i$ égaux à 0 ou 1 tels que l'on ait

$$a + \alpha b \equiv \pm u_1^{n_1} u_2^{n_2} \alpha^{n_3} (\alpha^2 + 1)^{n_4} \bmod K^{*2}.$$

Puisque la norme de $K$ sur $\mathbb{Q}$ de $a + b\alpha$ est un carré dans $\mathbb{Q}$, il en résulte que

$$a + \alpha b \equiv u_1^{n_1} u_2^{n_2} \bmod K^{*2}.$$

Soient $\mathfrak{P}_2$ l'idéal de $O_K$ au-dessus de 2 et $K_{\mathfrak{P}_2}$ le complété de $K$ en $\mathfrak{P}_2$. Les entiers $a$ et $b$ étant premiers entre eux, $a$ est impair et $a + b\alpha$ est une unité de $K_{\mathfrak{P}_2}$. Sa classe modulo les carrés de $K_{\mathfrak{P}_2}$ ne dépend donc que des classes de $a$ et $b$ modulo 8. En utilisant le fait que

$$\frac{a + b\alpha}{u_1^{n_1} u_2^{n_2}} \in K_{\mathfrak{P}_2}^{*2},$$

on constate alors que l'on doit avoir $n_2 = 0$, ce qui entraîne la proposition.

Les quartiques $C_1$ et $C_2$ représentent deux courbes elliptiques sur $K$ et une 2-descente montre que les groupes $C_1(K)$ et $C_2(K)$ sont de rang 2. D'après la proposition, on est amené à déterminer les points d'abscisse dans $\mathbb{Q}$ de $C_1(K)$ et de $C_2(K)$. On peut utiliser pour cela les méthodes de type Chabauty qui se trouvent dans [5]. Les détails des arguments qui interviennent sont trop longs pour être présentés ici. Signalons simplement que l'on peut déterminer ces points à l'aide du logiciel de calculs ALGAE qui a été écrit par N. Bruin (cf. [6]). On constate alors que si $x \in \mathbb{Q}$ est l'abscisse d'un point de $C_1(K)$, on a $x \in \{0, 3/4, 1\}$. De même, si $x \in \mathbb{Q}$ est l'abscisse d'un point de $C_2(K)$, on a $x = 1$ ou $x = -3$. On obtient ainsi que $S_0(1,5) = \{(-1,1,1)\}$.

Les mêmes arguments que ceux indiqués ci-dessus permettent de déterminer les ensembles $S_0(2,5)$ et $S_0(4,5)$.

## Références


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

[2] C. Batut, D. Bernardi, K. Belabas, H. Cohen and M. Olivier, *User's guide to PARI-GP* (*version 2.0.12*), Lab A2X, Univ. de Bordeaux I, Bordeaux, 1998.

[3] M. Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, preprint, Mai 2002.

[4] B. J. Birch and W. Kuyk (eds.), *Modular Functions of One Variable IV* (*Antwerp, 1972*), Lecture Notes in Math. 476, Springer, 1975.

[5] N. Bruin, *Chabauty methods and covering techniques applied to generalised Fermat equations*, PhD thesis, Leiden Univ., 1999.

[6] —, *ALGAE package and documentation*, 2001, http://www.cecm.sfu.ca/~bruin/#Software

[7] Y. Bugeaud, *On the diophantine equation* $x^2 - 2^m = \pm y^n$, Proc. Amer. Math. Soc. 125 (1997), 3203–3208.
[8] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 2nd ed., 1997.
[9] H. Darmon, *The equations* $x^n + y^n = z^2$ *and* $x^n + y^n = z^3$, Internat. Math. Res. Notices 1993, no. 10, 263–274.
[10] —, *Serre's conjectures*, in: Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), CMS Conf. Proc. 17, Amer. Math. Soc., 1995, 135–153.
[11] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. 490 (1997), 81–100.
[12] F. Diamond, *On deformation rings and Hecke rings*, Ann. of Math. 144 (1996), 137–166.
[13] E. Halberstadt et A. Kraus, *Sur les modules de torsion des courbes elliptiques*, Math. Ann. 310 (1998), 47–54.
[14] A. Kraus, *Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique*, Dissertationes Math. 364 (1997).
[15] —, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. 49 (1997), 1139–1161.
[16] G. Ligozat, *Courbes modulaires de genre* 1, Bull. Soc. Math. France. Mém. 43 (1975).
[17] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129–162.
[18] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3, J. Number Theory 44 (1993), 119–152.
[19] B. Poonen, *Some diophantine equations of the form* $x^n + y^n = z^m$, Acta Arith. 86 (1998), 193–205.
[20] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. 100 (1990), 431–476.
[21] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, ibid. 15 (1972), 259–331.
[22] —, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179–230.
[23] —, *Travaux de Wiles* (*et Taylor*, ...), *partie I*, dans : Séminaire Bourbaki 1994/95, Astérisque 237 (1996), 319–332.
[24] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in [4], 33–52.
[25] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. 141 (1995), 443–551.

114 rue Saint Denis
93100 Montreuil, France
E-mail: ivorra@math.jussieu.fr

*Reçu le 15.6.2001*
*et révisé le 19.7.2002* (4053)