Formes homogènes de degré 3 et puissances p-ièmes

Nicolas Billerey

Université Paris 6, Projet théorie des nombres, UMR 7586*,*
Case 247*, 4, place Jussieu, Institut de Mathématiques,*
75252 *PARIS, FRANCE*

Résumé

In this paper, we are interested in diophantine equations of type $F(x, y) = dz^p$ where F is a separable homogeneous form of degree ≥ 3 with integer coefficients, d a fixed integer ≥ 1 and p a prime number ≥ 7. As a consequence of the *abc* conjecture, if p is sufficiently large and (a, b, c) is a non trivial proper solution of the above equation, we have $c = \pm 1$. In the case where F has degree 3, we associate to (a, b, c) an elliptic curve defined over $\mathbb{Q}$ called the Frey curve or Hellegouarch-Frey curve. This allows us to deduce our conjecture from another one about elliptic curves attributed to G. Frey and B. Mazur (which is itself a consequence of the *abc* conjecture). We then applied our construction to the study of an explicit form. We give some results about the set of non trivial proper solutions of the equation considered for several values of d.

Key words: Forms of degree higher than two ; Elliptic Curves ; Modular Representations.

1 Introduction

On se propose de faire quelques remarques sur la conjecture suivante.

Conjecture 1.1 (A) *Soient $F \in \mathbb{Z}[X, Y]$ une forme homogène séparable de degré ≥ 3 et d un entier ≥ 1. Il existe une constante $C_{d,F} > 0$ ne dépendant*

Email address: billerey@math.jussieu.fr (Nicolas Billerey).
URL: http ://www.institut.math.jussieu.fr/∼billerey/ (Nicolas Billerey).

que de d et F telle que si p est un nombre premier $> C_{d,F}$ et (a,b,c) un triplet d'entiers non nuls premiers entre eux vérifiant l'égalité

$$F(a,b) = dc^p,$$

alors on a $c = \pm 1$.

Les seuls résultats déjà connus sur cette conjecture concernent certains cas particuliers d'équations de Fermat généralisées où d est un entier convenablement choisi et où $F(x,y)$ est l'une des formes suivantes (cf. [21,13,9,5,23]) :

$$x^3+y^3, \quad x^4+y^4, \quad x^4-y^4, \quad x^5+y^5 \quad \text{et} \quad x^6+y^6.$$

Les équations $F(x,y) = \pm d$ d'inconnues x, y dans $\mathbb{Z}$ sont appelées équations de Thue. Elles ont été particulièrement étudiées. On sait par exemple qu'elles n'ont qu'un nombre fini de solutions (cf. par exemple [15, p.363]). Par ailleurs, si $p \geq 5$ est fixé, un théorème de [11] affirme qu'il n'existe qu'un nombre fini de triplets d'entiers non nuls (a,b,c) premiers entre eux tels que $F(a,b) = dc^p$. La conjecture (A) entraîne donc que l'ensemble des triplets (a,b,c) d'entiers non nuls premiers entre eux pour lesquels il existe un nombre premier $p \geq 5$ tel que $F(a,b) = dc^p$, est fini.

On rappelle dans l'Appendice A que la conjecture (A) est une conséquence de la conjecture *abc*.

Dans cet article, on s'intéresse plus spécifiquement aux équations diophantiennes de la forme

$$F(x,y) = dz^p, \tag{1}$$

où F est une forme homogène séparable de degré 3 à coefficients entiers relatifs, p un nombre premier ≥ 7 et d un entier ≥ 1.

Le cas particulier de l'équation (1)

$$x^3+y^3 = z^p, \tag{2}$$

a été étudié par H. Darmon et A. Granville ([11]) et A. Kraus ([21]). Leur approche repose sur l'étude modulaire de la représentation galoisienne des points de p-torsion d'une certaine courbe elliptique, appelée parfois courbe de Frey ou courbe de Hellegouarch-Frey, associée à une hypothétique solution de l'équation (2).

Conformément à la terminologie utilisée dans [11], on dira qu'un triplet d'entiers $(a,b,c) \in \mathbb{Z}^3$ est solution de l'équation (1) si $F(a,b) = dc^p$, qu'elle est propre si a, b et c sont premiers entre eux et qu'elle est non triviale si abc est non nul.

Dans la partie 2, on généralise la construction de la courbe de Frey associée à l'équation (2) dans [11] à toutes les formes homogènes séparables de degré 3

$$F(x,y) = t_0x^3 + t_1x^2y + t_2xy^2 + t_3y^3,$$

avec t_0, t_1, t_2 et t_3 entiers relatifs. Si (a,b,c) est une solution propre et non triviale de (1), la courbe E que l'on construit a pour équation

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$\begin{cases} a_2 = t_1a - t_2b, \\ a_4 = t_0t_2a^2 + (3t_0t_3 - t_1t_2)ab + t_1t_3b^2, \\ a_6 = t_0^2t_3a^3 - t_0(t_2^2 - 2t_1t_3)a^2b + t_3(t_1^2 - 2t_0t_2)ab^2 - t_0t_3^2b^3. \end{cases}$$

On démontre au théorème 2.3 que si p est assez grand et $c \neq \pm 1$, alors E est une courbe de Frey au sens de la définition 2.2.

Cette construction offre l'avantage de relier le problème diophantien soulevé par l'équation (1) à des résultats ou conjectures classiques de théorie des nombres ou, plus spécifiquement, de la théorie des courbes elliptiques. Tel est le cas, par exemple, de la conjecture suivante, attribuée à G. Frey et B. Mazur (cf. [10] et [22]) :

Conjecture 1.2 (Frey-Mazur) *Soit A une courbe elliptique définie sur $\mathbb{Q}$. On désigne par $\mathcal{F}_A$ l'ensemble des nombres premiers ℓ pour lesquels il existe une courbe elliptique $A^{(\ell)}$ définie sur $\mathbb{Q}$, non isogène à A sur $\mathbb{Q}$, telle que les modules galoisiens des points de ℓ-torsion de A et A' soient isomorphes. Alors, l'ensemble $\mathcal{F}_A$ est fini.*

Cette conjecture n'a actuellement été démontrée pour aucune courbe elliptique. Si A est une courbe elliptique définie sur $\mathbb{Q}$, on sait que 2, 3 et 5 sont dans $\mathcal{F}_A$.

En utilisant la construction de E, on montre (proposition 2.9) que la conjecture ci-dessus implique la conjecture (A) pour les formes homogènes de degré 3.

On donne par ailleurs dans l'Appendice B une démonstration, due à Kraus, du fait que la conjecture *abc* implique (via une forme faible de la conjecture de Szpiro) la conjecture de Frey-Mazur. On a donc en résumé le diagramme

d'implications suivant.

$$\begin{array}{ccc} \text{Conjecture de Frey-Mazur} & \Longleftarrow\!\!\!= & \text{Conjecture } abc \\ \Downarrow & & \Downarrow \\ \text{Conjecture } (A) \text{ pour } \deg(F)=3 & & \text{Conjecture } (A) \end{array}$$

Si F une forme homogène séparable de degré ≥ 3 à coefficients entiers relatifs, on pose $f(x) = F(x,1)$. Lorsque $d = 1$ et $y = 1$, l'équation (1) s'écrit

$$f(x) = z^p. \tag{3}$$

En 1920, Nagell a démontré que pour le polynôme

$$f(x) = x^3 + x^2 + x + 1, \tag{4}$$

l'équation (3) n'admettait pas de solution non triviale ($xz \neq 0$) pour $p \geq 3$ et seulement $(x,z) = (7,20)$ lorsque $p = 2$ ([27, p.73]). Outre le cas particulier de l'équation de Catalan, $x^3 \pm z^p = 1$, on trouvera d'autres exemples de résolution de telles équations dans [3] et [6].

Suivant l'exemple de Nagell, nous illustrons dans la partie 3 la construction de la courbe de Frey précédente avec l'étude de l'équation (1) lorsque F est la forme homogène de degré 3 suivante

$$F(x,y) = x^3 + x^2y + xy^2 + y^3. \tag{5}$$

Si (a,b,c) appartient à l'ensemble $S_p(d)$ des solutions propres et non triviales de l'équation (1) où F est la forme ci-dessus et d un entier ≥ 1, on lui associe la courbe E d'équation

$$E : y^2 = x^3 + (a-b)x^2 + (a+b)^2x + a^3 + a^2b - ab^2 - b^3.$$

Pour certains entiers d libres de puissances troisièmes, on obtient plusieurs résultats sur $S_p(d)$. À titre d'exemple, on montre par des arguments de nature modulaire (théorème 3.2) que si $d = 2$, 6, 10 ou 22, alors $S_p(d)$ est vide pour $p \geq 7$. De même, si ℓ est un nombre premier vérifiant certaines conditions explicites, alors $S_p(2\ell)$ est vide lorsque p est suffisamment grand. Tel est le cas, par exemple, lorsque $\ell = 19, 43, 59, 61, 67, 83$ (théorème 3.3).

Bien que notre construction ne permette pas de retrouver le résultat de Nagell (correspondant au cas où $d = 1$ et $y = 1$), on explique dans la partie 4 comment la théorie modulaire permet d'aborder, voire de résoudre complètement, certaines équations diophantiennes, certes plus artificielles mais néanmoins non triviales, de la forme (1) ou (3) lorsque le polynôme considéré est de degré ≥ 3.

Remerciements. Je remercie M. Hindry et A. Kraus pour les conversations que j'ai eues avec eux pendant la préparation de ce travail.

2 La courbe elliptique E

On considère dans cette partie une forme homogène séparable de degré 3 à coefficients entiers relatifs

$$F(x,y) = t_0x^3 + t_1x^2y + t_2xy^2 + t_3y^3.$$

Posons $f(x) = F(x,1)$. Le polynôme F étant séparable, il en va de même pour f.

On considère un nombre premier $p \geq 7$, un entier $d \geq 1$ et (a,b,c) une solution propre et non triviale de l'équation (1).

2.1 Équation de la courbe E

On commence par supposer $t_0 \neq 0$, i.e. $\deg(f) = 3$. Soit $K = \mathbb{Q}(\alpha,\beta,\gamma)$ l'extension de $\mathbb{Q}$ dans $\mathbb{C}$ engendrée par les racines α, β, γ du polynôme f. On a alors la factorisation suivante :

$$F(x,y) = t_0(x-\alpha y)(x-\beta y)(x-\gamma y).$$

On associe à (a,b,c) une courbe elliptique $E/\mathbb{Q}$ comme suit. Posons :

$$\begin{cases} A = t_0(\beta-\gamma)(a-\alpha b), \\ B = t_0(\gamma-\alpha)(a-\beta b), \\ C = t_0(\alpha-\beta)(a-\gamma b). \end{cases}$$

Par construction, on a

$$A + B + C = 0.$$

Soit $\mathcal{E}$ la cubique d'équation :

$$\mathcal{E} : Y^2 = X(X-A)(X+B). \tag{6}$$

Son disciminant est

$$\Delta(\mathcal{E}) = 16(AB)^2(A+B)^2 = 16\mathfrak{D}(f)F(a,b)^2,$$

où $\mathfrak{D}(f)$ est le discriminant du polynôme f. L'entier c étant non nul et le polynôme f séparable, on a $\Delta(\mathcal{E}) \neq 0$. L'équation (6) définit donc une courbe elliptique sur K.

Considérons les trois éléments u_1, u_2 et u_3 de K définis par

$$\begin{cases} u_1 = t_0(\alpha a + \gamma\beta b), \\ u_2 = t_0(\beta a + \gamma\alpha b), \\ u_3 = t_0(\gamma a + \beta\alpha b). \end{cases}$$

Ils vérifient les égalités : $A = u_2 - u_3$, $B = u_3 - u_1$ et $C = u_1 - u_2$. Le changement de variables

$$x = X + u_3, \quad y = Y, \tag{7}$$

transforme alors l'équation (6) en l'équation :

$$E : y^2 = (x - u_1)(x - u_2)(x - u_3).$$

Cette courbe E a pour équation :

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \tag{8}$$

avec

$$\begin{cases} a_2 = t_1a - t_2b, \\ a_4 = t_0t_2a^2 + (3t_0t_3 - t_1t_2)ab + t_1t_3b^2, \\ a_6 = t_0^2t_3a^3 - t_0(t_2^2 - 2t_1t_3)a^2b + t_3(t_1^2 - 2t_0t_2)ab^2 - t_0t_3^2b^3. \end{cases}$$

La courbe elliptique E est donc définie sur $\mathbb{Q}$ et le changement de variables (7) fournit un isomorphisme défini sur K de $\mathcal{E}$ sur E. De plus, les invariants standard $c_4(E)$ et $\Delta(E)$ de (8) sont inchangés par rapport à ceux de $\mathcal{E}$ (cf. [38]). On les note respectivement c_4 et Δ. On a :

$$\begin{cases} c_4 = 16\Big((t_1^2 - 3t_0t_2)a^2 + (t_1t_2 - 9t_0t_3)ab + (t_2^2 - 3t_1t_3)b^2\Big), \\ \Delta = 16\mathfrak{D}(f)F(a,b)^2 \\ \qquad \text{où } \mathfrak{D}(f) = -27t_0^2t_3^2 + (18t_1t_2t_3 - 4t_2^3)t_0 - 4t_3t_1^3 + t_1^2t_2^2. \end{cases} \tag{9}$$

Supposons $t_0 = 0$. Dans ce cas, on associe à (a, b, c) la courbe ellipitique $E/\mathbb{Q}$ d'équation

$$E : y^2 = x^3 + (t_1a - t_2b)x^2 + t_1(t_3b - t_2a)bx + t_1^2t_3ab^2.$$

Il s'agit de la courbe d'équation (8) avec $t_0 = 0$.

Remarque 2.1 *Supposons qu'il existe $x_0 \in \mathbb{Q}$ racine du polynôme f. Alors, E a un point d'ordre 2 rationnel sur $\mathbb{Q}$. Si $x_0 = 0$, tel est le cas du point $(t_2 b, 0)$, sinon tel est le cas de $(t_0 x_0 a - \frac{t_3}{x_0} b, 0)$.*

2.2 La courbe de Frey E

On rappelle que p est un nombre premier ≥ 7 et que (a, b, c) est une solution propre et non triviale de l'équation (1). Notons $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ et $\mathrm{G}_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ le groupe de Galois absolu de $\mathbb{Q}$. Soit A une courbe elliptique définie sur $\mathbb{Q}$ et $A[p]$ le sous-groupe de $A(\overline{\mathbb{Q}})$ constitué des points de p-torsion de A. C'est un $\mathbb{F}_p$-espace vectoriel de dimension 2 sur lequel le groupe $\mathrm{G}_{\mathbb{Q}}$ opère continûment. Par le choix d'une base de $A[p]$ sur $\mathbb{F}_p$, on en déduit un homomorphisme de groupes

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

On associe à cette représentation un poids k qui est un entier ≥ 2 et un conducteur $N(\rho_p^A)$ qui est un entier ≥ 1, premier à p, qui divise le conducteur N_A de A (cf. [32, §1]). Désignons par Δ_A le discriminant minimal de A. Si ℓ est un nombre premier, notons v_ℓ la valuation ℓ-adique de $\mathbb{Q}$.

Définition 2.2 *Soit $A/\mathbb{Q}$ une courbe elliptique définie sur $\mathbb{Q}$. On désigne par S_A l'ensemble des nombres premiers de mauvaise réduction de A. Soient S un sous-ensemble de S_A et p un nombre premier. On dira que A est une courbe de Frey associée au couple (p, S) si les trois conditions suivantes sont satisfaites.*

(1) La représentation ρ_p^A est irréductible.

(2) L'ensemble S est strictement inclus dans S_A.

(3) Pour tout nombre premier $\ell \in S_A \setminus S$, la courbe A a réduction multiplicative en ℓ et $v_\ell(\Delta_A) \equiv 0 \pmod{p}$.

Avec la définition ci-dessus, on a le résultat suivant.

Théorème 2.3 *Il existe une constante $\alpha(d, F) \geq 0$ ne dépendant que de d et F telle que si $c \neq \pm 1$ et $p > \alpha(d, F)$, alors la courbe E est une courbe de Frey associée au couple (p, S) où S est l'ensemble des diviseurs premiers de $2d\mathfrak{D}(f)$ de mauvaise réduction.*

Démontrons à présent cet énoncé.

2.2.1 Résultats préliminaires

On a la relation suivante :

$$U(a,b)F(a,b) + V(a,b)c_4 = -16\mathfrak{D}(f)b^4, \tag{10}$$

où

$$\begin{cases} U(a,b) = 16\Big(3t_0(3t_0t_2 - t_1^2)a + (t_1^3 - 6t_0t_1t_2 + 27t_0^2t_3)b\Big) \\ V(a,b) = 3t_0^2a^2 + 2t_0t_1ab + (4t_0t_2 - t_1^2)b^2. \end{cases}$$

On en déduit le lemme suivant.

Lemme 2.4 *Soit ℓ un nombre premier divisant Δ et ne divisant pas $2d\mathfrak{D}(f)$. L'équation (8) est minimale en ℓ et la courbe E a réduction multiplicative en ℓ. De plus, $v_\ell(\Delta_E)$ est multiple de p.*

Démonstration : Soit ℓ un nombre premier impair ne divisant pas $d\mathfrak{D}(f)$ et divisant $\Delta = 2^4\mathfrak{D}(f)d^2c^{2p}$. Nécessairement, ℓ divise l'entier c. Supposons par l'absurde que ℓ divise le coefficient c_4. D'après la relation (10), l'entier ℓ divise alors également $16\mathfrak{D}(f)b^4$. Or ℓ ne divise pas $2\mathfrak{D}(f)$, donc ℓ divise b. De l'expression de $F(a,b)$, on en déduit que ℓ divise t_0a^3. Si ℓ ne divise pas a, alors ℓ divise t_0 et d'après l'expression du coefficient c_4 de la courbe E ci-dessus, il vient que ℓ divise également t_1. Mais alors ℓ divise $\mathfrak{D}(f)$ d'après l'expression (9) ci-dessus. C'est une contradiction. Donc ℓ divise a. Comme ℓ divise aussi b et c, c'est contraire au fait que (a,b,c) soit une solution propre de (1). On en déduit que ℓ ne divise pas c_4.

La congruence $v_\ell(\Delta_E) \equiv 0 \pmod{p}$ résulte de l'égalité $v_\ell(\Delta) = v_\ell(\Delta_E)$ et de l'expression (9) du coefficient Δ.

Lemme 2.5 *Pour p assez grand, la représentation ρ_p^E est irréductible. Si E a un point d'ordre 2 rationnel sur $\mathbb{Q}$, c'est le cas pour $p \geq 11$. Si l'invariant modulaire j de E est différent de -15^3 et 255^3, la représentation ρ_7^E est irréductible.*

Démonstration : La représentation ρ_p^E est irréductible dès que $p > 163$ d'après [26].

Supposons que E a un point d'ordre 2 rationnel sur $\mathbb{Q}$ (c'est par exemple le cas si f est réductible sur $\mathbb{Q}$ d'après la remarque 2.1). Si ρ_p^E était réductible, le groupe $E(\overline{\mathbb{Q}})$ possèdrait un sous-groupe d'ordre $2p$ stable par $\mathrm{G}_{\mathbb{Q}}$, de sorte que la courbe modulaire $Y_0(2p)$ aurait un point rationnel sur $\mathbb{Q}$. Or, si $p \geq 11$, B. Mazur et M. Kenku ont démontré que l'ensemble $Y_0(2p)(\mathbb{Q})$ est vide (cf. [17]). D'où le résultat dans ce cas.

Le cas $p = 7$ se traite en remarquant que la courbe modulaire $Y_0(14)$ est la courbe elliptique notée 14A1 dans les tables de [8] et qu'elle possède exactement deux points rationnels sur $\mathbb{Q}$ qui correspondent aux deux classes de $\overline{\mathbb{Q}}$-isomorphisme des courbes elliptiques d'invariants $j = -15^3$ et 255^3 ([25, p.45]). D'où le lemme.

Lemme 2.6 *Si p ne divise pas $d\mathfrak{D}(f)$, alors on a $k = 2$.*

DÉMONSTRATION : On suppose que p ne divise pas $d\mathfrak{D}(f)$. Alors, d'après le lemme 2.4, l'équation (8) est minimale en p, la courbe E a réduction semi-stable en p et l'exposant de p dans le discriminant minimal de E est multiple de p. D'où $k = 2$ ([32, prop. 5]).

Le lemme suivant servira à plusieurs reprises (pour un résultat plus précis, voir [36, V.§4]).

Lemme 2.7 *Soit S' un ensemble fini de nombres premiers. Il n'existe qu'un nombre fini de triplets d'entiers (u, v, m) vérifiant les trois conditions suivantes :*

(1) on a $F(u, v) = m$,

(2) les entiers u et v sont premiers entre eux,

(3) l'entier m a tous ses diviseurs premiers dans S'.

DÉMONSTRATION : Posons $S' = \{p_1, \ldots, p_r\}$. Soit $n \in \mathbb{Z} \setminus \{0\}$. L'ensemble

$$\left\{ (x, y) \in \mathbb{Z}\left[\frac{1}{S'}\right]^2 \;\middle|\; F(x, y) = n \right\}$$

est fini ([15, p.363]).

On en déduit que si $\mathcal{N} = \{\pm p_1^{\alpha_1} \cdots p_r^{\alpha_r},\ \text{avec } 0 \leq \alpha_i \leq 2\}$, alors l'ensemble

$$\mathcal{F} = \left\{ (x, y) \in \mathbb{Z}\left[\frac{1}{S'}\right]^2 \;\middle|\; F(x, y) = n,\ \text{avec } n \in \mathcal{N} \right\}$$

est encore fini.

Soit (u, v, m) un triplet d'entiers vérifiant les trois conditions du lemme. Il existe un unique entier $Z > 0$ ayant tous ses diviseurs premiers dans S' tel que $m = Z^3 n$ avec $n \in \mathcal{N}$. On a alors

$$F\left(\frac{u}{Z}, \frac{v}{Z}\right) = n.$$

En particulier, il existe r et s tels que

$$\left(\frac{u}{Z}, \frac{v}{Z}\right) = (r, s) \in \mathcal{F}.$$

Les entiers u et v étant premiers entre eux, l'entier Z est le plus petit dénominateur commun > 0 de r et s. On en déduit qu'il n'existe qu'un nombre fini de valeurs possibles pour u et v et, par conséquent, pour m. Cela démontre le lemme.

Notations. Soit S' un ensemble fini non vide de nombres premiers. On désigne par $\mathcal{F}_{F,S'}$ l'ensemble (fini) des triplets (u, v, m) satisfaisant aux trois conditions du lemme 2.7. On pose alors

$$N_{F,S'} = \begin{cases} \max\{|m|, (u, v, m) \in \mathcal{F}_{F,S'}\} \text{ si } \mathcal{F}_{F,S'} \neq \emptyset \\ 1 \qquad\qquad\qquad\qquad \text{sinon.} \end{cases} \tag{11}$$

L'entier $N_{F,S'}$ ne dépend que de F et S'.

Lemme 2.8 *Il existe une constante $\beta(d, F) \geq 0$ ne dépendant que de d et F telle que si $p > \beta(d, F)$, alors l'une des deux conditions suivantes est réalisée :*

(1) on a $c = \pm 1$,

(2) il existe un nombre premier ne divisant pas $2d\mathfrak{D}(f)$ en lequel E a mauvaise réduction.

Démonstration : Supposons la seconde condition non réalisée. Alors, d'après le lemme 2.4, l'entier c a tous ses diviseurs premiers dans l'ensemble S' des diviseurs premiers de $2d\mathfrak{D}(f)$. Par ailleurs, si $\mathrm{pgcd}(a, b)$ désigne le pgcd de a et b, alors $(\mathrm{pgcd}(a, b))^3$ divise d. Posons

$$a' = \frac{a}{\mathrm{pgcd}(a, b)}, \quad b' = \frac{b}{\mathrm{pgcd}(a, b)} \quad \text{et} \quad d' = \frac{d}{(\mathrm{pgcd}(a, b))^3}.$$

Le triplet $(a', b', d'c^p)$ vérifie les trois conditions du lemme 2.7, i.e. appartient à l'ensemble fini $\mathcal{F}_{F,S'}$. Posons (avec les notations précédentes)

$$\beta(d, F) = \frac{\log N_{F,S'}}{\log 2} \geq 0.$$

L'ensemble S' ne dépendant que de F et d, il en va de même pour $\beta(d, F)$. Si l'on a $p > \beta(d, F)$, alors $d'2^p > N_{F,S'}$. On a donc $c = \pm 1$. Cela démontre le lemme 2.8.

2.2.2 Fin de la démonstration du théorème 2.3

Notons S l'ensemble des diviseurs premiers de $2d\mathfrak{D}(f)$ en lesquels la courbe E a mauvaise réduction. D'après le lemme 2.5, il existe une constante $\gamma(d,F) \geq 5$ telle que si $p > \gamma(d,F)$, alors ρ_p^E est irréductible. Posons, avec les notations du lemme 2.8, $\alpha(d,F) = \max(\beta(d,F), \gamma(d,F))$. Si $c \neq \pm 1$ et $p > \alpha(d,F)$, alors $p > \beta(d,F)$ et, d'après le lemme 2.8, il existe un nombre premier de mauvaise réduction qui ne soit pas dans S, i.e. $S_E \setminus S \neq \emptyset$. Par ailleurs, d'après le lemme 2.4, pour tout nombre premier $\ell \in S_E \setminus S$, E a réduction multiplicative en ℓ et $v_\ell(\Delta_E) \equiv 0 \pmod{p}$. D'où le théorème.

2.3 Lien avec la conjecture de Frey - Mazur

Notation. Soit A une courbe elliptique définie sur $\mathbb{Q}$. On pose, avec les notations de la conjecture de Frey-Mazur,

$$\nu_A = \max\{\ell \mid \ell \in \mathcal{F}_A\}.$$

D'après cette conjecture, $\nu_A \in \mathbb{N}$.

Proposition 2.9 *La conjecture de Frey-Mazur implique la conjecture (A) pour les formes de degré* 3.

DÉMONSTRATION : D'après les lemmes 2.5 et 2.6, on peut sans restriction supposer la représentation ρ_p^E irréductible et de poids 2. Le conducteur $N(\rho_p^E)$ est majoré par une constante M indépendante du quadruplet (a,b,c,p). En effet, si ℓ est un diviseur premier de $N(\rho_p^E)$, alors, d'après le lemme 2.4 et [19, p. 28], ℓ divise $2d\mathfrak{D}(f)$. De plus, on a $v_2(N(\rho_p^E)) \leq 8$, $v_3(N(\rho_p^E)) \leq 5$ et si $\ell \geq 5$, $v_\ell(N(\rho_p^E)) \leq 2$ (cf. [29]). On peut donc, par exemple, choisir $M = (2d\mathfrak{D}(f))^8$.

Par ailleurs, d'après le théorème 3 de [20], il existe une constante $\eta_{d,F}$ ne dépendant que de d et F telle que si $p > \eta_{d,F}$, alors il existe une courbe elliptique A définie sur $\mathbb{Q}$ de conducteur $N_A = N(\rho_p^E)$ telle que les représentations ρ_p^E et ρ_p^A soient isomorphes.

Supposons l'inégalité suivante vérifiée

$$p > \nu_{d,F} = \max\{\eta_{d,F}, \nu_{A'} \mid A' \text{ courbe elliptique sur } \mathbb{Q} \text{ telle que } N_{A'} \leq M\}.$$

L'entier M ne dépendant que de d et F, il en va de même pour $\nu_{d,F}$. Considérons alors ℓ un nombre premier divisant c et ne divisant pas $2d\mathfrak{D}(f)N_A$. En particulier, ℓ divise Δ sans diviser $2d\mathfrak{D}(f)$, donc, d'après le lemme 2.4, la courbe E a mauvaise réduction multiplicative en ℓ. De plus, comme $p > \nu_{d,F} \geq \nu_A$, les courbes E et A sont $\mathbb{Q}$-isogènes d'après la conjecture de Frey-Mazur et on

a

$$1 = v_\ell(N_E) = v_\ell(N_A) = 0, \quad \text{car } \ell \text{ ne divise pas } N_A.$$

C'est une contradiction. On en déduit que c a tous ses diviseurs premiers inclus dans l'ensemble S' des diviseurs premiers de $2d\mathfrak{D}(f)\prod N_{A'}$ où le produit porte sur l'ensemble fini (cf. [35, IX §6]) des classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques A' définies sur $\mathbb{Q}$ de conducteur $\leq M$.

Si $\mathrm{pgcd}(a,b)$ désigne le pgcd de a et b, alors $(\mathrm{pgcd}(a,b))^3$ divise d. Posons

$$a' = \frac{a}{\mathrm{pgcd}(a,b)}, \quad b' = \frac{b}{\mathrm{pgcd}(a,b)} \quad \text{et} \quad d' = \frac{d}{(\mathrm{pgcd}(a,b))^3}.$$

Le triplet $(a', b', d'c^p)$ vérifie les trois conditions du lemme 2.7, i.e. appartient à l'ensemble fini $\mathcal{F}_{F,S'}$. Posons (avec les notations (11))

$$C_{d,F} = \frac{\log N_{F,S'}}{\log 2} \geq 0.$$

L'ensemble S' ne dépendant que de F et d, il en va de même pour $C_{d,F}$. Et, si $p > C_{d,F}$, alors $d'2^p > N_{F,S'}$. On a donc $c = \pm 1$. C'est l'énoncé de la conjecture (A) .

3 Étude d'un exemple

À titre d'exemple, on applique, dans cette partie, la construction précédente au cas particulier de la forme homogène

$$F(x,y) = x^3 + x^2y + xy^2 + y^3.$$

Soient p un nombre premier ≥ 7 et d un entier ≥ 1. Rappelons que $S_p(d)$ désigne l'ensemble des solutions propres et non triviales de l'équation

$$F(x,y) = x^3 + x^2y + xy^2 + y^3 = dz^p. \tag{12}$$

Dans toute cette partie, on fait l'hypothèse suivante :

l'entier d libre de puissance troisième.

Sous cette hypothèse, si (a,b,c) appartient à $S_p(d)$, alors les entiers a, b et c sont premiers entre eux deux-à-deux.

En utilisant la courbe E d'équation (8) associée un élément de $S_p(d)$, et la méthode modulaire (dont le principe est résumé au début du paragraphe 3.3), on démontre plusieurs résulats sur l'équation (12).

Le premier concerne le cas $d = 1$.

Théorème 3.1 *Soit (a, b, c) un élément de $S_p(1)$. Alors, l'entier c est impair.*

Pour certaines valeurs de l'entier d, on a un résultat complet.

Théorème 3.2 *Les ensembles $S_p(2)$, $S_p(6)$, $S_p(10)$ et $S_p(22)$ sont vides.*

Soit ℓ est un nombre premier ≥ 13. On souhaite montrer, comme au théorème précédent pour $\ell = 3, 5$ et 11, la vacuité de l'ensemble $S_p(2\ell)$ (au-moins lorsque p est grand). Cela sera le cas si ℓ vérifie certaines conditions. Plus précisément, on désigne par g la fonction définie sur $\mathbb{N}^*$ par

$$g(n) = \begin{cases} \frac{50}{13} \cdot \frac{\log(n)}{\log(2)} & \text{si } n < 2^9, \\ 18 + 2\frac{\log n}{\log 2} & \text{si } 2^9 \leq n < 2^{362} \\ \frac{50}{13} \cdot \frac{\log(n)}{\log(2)} & \text{si } n \geq 2^{362}. \end{cases}$$

On dira que ℓ satisfait à la propriété (P) si pour tout entier k vérifiant l'inégalité

$$2 \leq k < g(\ell),$$

aucun des entiers $\ell - 1$, $\ell - 2^k$, $\ell + 2^k$ et $2^k - \ell$ n'est un carré.

On a alors le résultat suivant.

Théorème 3.3 *On suppose que ℓ vérifie la propriété (P). Il existe une constante $\kappa(\ell)$ ne dépendant que de ℓ telle que si $p > \kappa(\ell)$, alors l'ensemble $S_p(2\ell)$ est vide.*

Remarque 3.4 *On peut par exemple prendre $\kappa(\ell) = \left(4\sqrt{\ell + 1} + 1\right)^{4(\ell-1)}$. L'amélioration de cette borne est, dans la pratique, limitée par la connaissance des newform (au sens de [1]) de poids 2 et de niveau 64ℓ. Par exemple, pour $\ell = 11$, on a $\kappa(11) \approx 7 \cdot 10^{46}$, alors que $S_p(22)$ est vide pour $p \geq 7$ d'après le théorème 3.2. Les nombres premiers $13 \leq \ell \leq 200$ satisfaisant à la condition (P) sont*

$$\ell = 19, 43, 59, 61, 67, 83, 107, 109, 131, 139, 149, 157, 163, 167, 179, 181 \text{ et } 191.$$

La suite de la partie 3 est consacrée à la démonstration des théorèmes 3.1, 3.2 et 3.3.

Soit (a, b, c) un élément de $S_p(d)$. À un tel triplet on associe la courbe elliptique $E/\mathbb{Q}$ définie par l'équation (8) avec $t_0 = t_1 = t_2 = t_3 = 1$:

$$y^2 = x^3 + (a-b)x^2 + (a+b)^2x + a^3 + a^2b - ab^2 - b^3. \tag{13}$$

La courbe E possède un unique point d'ordre 2 rationnel sur $\mathbb{Q}$, à savoir $(b-a, 0)$.

On a $\mathfrak{D}(f) = -16$ et les invariants standard (c_4, c_6, Δ) associés à E sont les suivants (cf. (9) et [38]) :

$$\begin{cases} c_4 = -32(a^2 + 4ab + b^2), \\ c_6 = -128(5a^3 + 3a^2b - 3ab^2 - 5b^3), \\ \Delta = -2^8 F(a,b)^2 = -2^8 c^{2p} d^2. \end{cases} \tag{14}$$

Rappelons que N_E désigne le conducteur de E et Δ_E son discrimant minimal. Posons

$$r = \prod_{\ell \mid cd, \ell \neq 2} \ell.$$

Lemme 3.5 *La courbe E est semi-stable en dehors de 2. Elle a réduction additive en 2. L'équation (13) est globalement minimale.*

(1) Supposons d impair. Alors, $ab \not\equiv 1 \pmod 4$ et on a

$$N_E = \begin{cases} 2^6 r \text{ si } ab \equiv -1 \pmod 4, \\ 2^7 r \text{ si } ab \text{ est pair.} \end{cases}$$

L'invariant modulaire j de E est entier en 2 si et seulement si ab est pair.

(2) Supposons $v_2(d) = 1$. Alors on a

$$ab \equiv -1 \pmod 4 \quad \text{et} \quad N_E = 2^6 r.$$

L'invariant modulaire j de E n'est pas entier en 2.

(3) Supposons $v_2(d) = 2$. Alors ab est impair et on a

$$N_E = \begin{cases} 2^5 r \text{ si } ab \equiv 1 \pmod 4, \\ 2^6 r \text{ si } ab \equiv -1 \pmod 4. \end{cases}$$

L'invariant modulaire j de E est entier en 2 si et seulement si $ab \equiv 1 \pmod 4$.

De plus, si ℓ est un nombre premier impair, alors p divise $v_\ell(\Delta_E)$ si et seulement si ℓ ne divise pas d.

DÉMONSTRATION : Soit ℓ un nombre premier impair. Supposons tout d'abord que l'entier ℓ divise Δ. D'après l'expression (14) ci-dessus, l'entier ℓ divise alors

$$F(a,b) = (a+b)(a^2+b^2) = dc^p. \tag{15}$$

Remarquons que ℓ ne divise pas ab. Dans le cas contraire, l'entier a, par exemple, serait divisible par ℓ. Cela entrainerait que ℓ divise b (car ℓ divise $F(a,b)$) ce qui est contraire au fait que les entiers a et b sont premiers entre eux.

On en déduit que ℓ ne divise pas c_4. En effet, on a

$$c_4 \equiv \begin{cases} -2^6 ab \pmod{\ell} \text{ si } \ell \text{ divise } a+b, \\ -2^7 ab \pmod{\ell} \text{ si } \ell \text{ divise } a^2+b^2. \end{cases}$$

L'équation (13) est donc minimale en ℓ et la courbe E a mauvaise réduction de type multiplicatif en ℓ. On a $v_\ell(\Delta) = v_\ell(\Delta_E)$.

D'autre part, si ℓ ne divise pas Δ, la courbe E a bonne réduction en ℓ et l'équation (13) est minimale en ℓ.

Par ailleurs, on a dans les deux cas,

$$v_\ell(\Delta_E) = v_\ell(\Delta) \equiv 2v_\ell(d) \pmod{p}.$$

En particulier, p divise $v_\ell(\Delta_E)$ si et seulement si ℓ ne divise pas d.

Étudions à présent la minimalité de (13) et le type de réduction de E en 2.

(1) Supposons ab impair. Alors,

$$F(a,b) \equiv 2(a+b) \pmod{8} \quad \text{et} \quad v_2(c_4) = 6.$$

(a) Si $ab \equiv 1 \pmod 4$, alors $v_2(F(a,b)) = 2$ donc nécessairement $v_2(d) = 2$ et c est impair. On vérifie que l'on a

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (6, \geq 9, 12). \tag{16}$$

D'après le tableau II de [29], l'équation (13) est minimale en 2 et on est dans le cas I_ν^* avec $\nu = 2$ ou $\nu = 3$. Avec l'algorithme de Tate ([38, p.50]) on trouve $\nu = 3$ et on a $v_2(N_E) = 5$. De plus, l'invariant j est entier en 2 dans ce cas.

(b) Si $ab \equiv -1 \pmod 4$, alors $v_2(F(a,b)) \geq 3$, donc c est pair. De plus,

$$v_2(\Delta) = 8 + 2v_2(d) + 2pv_2(c) \geq 22.$$

Par ailleurs, on a

$$-\frac{c_6}{128} \equiv 5a + 3b - 3a - 5b \equiv 4a \pmod 8.$$

On en déduit

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (6, 9, \geq 22).$$

D'après [29], l'équation (13) est minimale en 2 et on a $v_2(N_E) = 6$. L'invariant j n'est pas entier en 2.

(2) Supposons ab pair. La solution (a, b, c) étant propre, a est pair et b impair (ou a est impair et b pair). On en déduit que c et d sont nécessairement impairs. D'où

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (5, 7, 8). \tag{17}$$

D'après [29], l'équation (13) est minimale en 2 et on a $v_2(N_E) = 7$. L'invariant j de E est entier en 2.

D'où le résultat.

3.2 La représentation ρ_p^E

Lemme 3.6 *La représentation ρ_p^E est (absolument) irréductible.*

DÉMONSTRATION : La courbe E a un point d'ordre 2 rationnel sur $\mathbb{Q}$, donc d'après le lemme 2.5, la représentation ρ_p^E est irréductible pour $p \geq 11$. Posons $t = a/b$. Alors, l'égalité $j = -15^3$ ou 255^3 (où j est l'invariant modulaire de E) conduit à

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

Or ces équations n'ont pas de solution rationnelle comme on le vérifie facilement. Cela démontre l'irréductibilité de ρ_7^E et le lemme.

Lemme 3.7 *On a $k = 2$ si p ne divise pas d et $k = p + 1$ sinon.*

DÉMONSTRATION : Supposons que p ne divise pas d. Alors d'après les lemmes 2.6 et 3.5, on a $k = 2$.

Supposons que p divise d. D'après le lemme 3.5, la courbe E a alors réduction de type multiplicatif en p et p ne divise pas $v_p(\Delta_E)$. Cela conduit à $k = p + 1$, d'où le résultat.

Posons

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

Lemme 3.8 *(1) On suppose que d est impair. Alors, $ab \not\equiv 1 \pmod 4$ et on a*

$$N(\rho_p^E) = \begin{cases} 2^6 r' \text{ si } ab \equiv -1 \pmod 4, \\ 2^7 r' \text{ si } ab \text{ est pair.} \end{cases}$$

(2) On suppose que $v_2(d) = 1$. Alors on a

$$ab \equiv -1 \pmod 4 \quad et \quad N(\rho_p^E) = 2^6 r'.$$

(3) On suppose que $v_2(d) = 2$. Alors ab est impair et on a

$$N(\rho_p^E) = \begin{cases} 2^5 r' \text{ si } ab \equiv 1 \pmod 4, \\ 2^6 r' \text{ si } ab \equiv -1 \pmod 4. \end{cases}$$

DÉMONSTRATION : Soit $\ell \neq p$ un nombre premier impair de mauvaise réduction. D'après le lemme 3.5, ℓ divise cd, l'équation (13) est minimale en ℓ et E a mauvaise réduction de type multiplicatif en ℓ.

Supposons que ℓ ne divise pas d. Alors, $v_\ell(\Delta_E)$ est multiple de p (*loc. cit.*). On en déduit que $v_\ell(N(\rho_p^E)) = 0$ ([19, p.28]).

Supposons que ℓ divise d. Alors, $v_\ell(\Delta_E)$ n'est pas multiple de p (lemme 3.5) et on a $v_\ell(N(\rho_p^E)) = 1$ ([19, p.28]).

D'après le lemme 3.5, la courbe E a donc réduction additive en 2 et on a $v_2(N(\rho_p^E)) = v_2(N_E)$ (*loc. cit.*). D'où le lemme.

3.3 Démonstrations des théorèmes 3.1, 3.2 et 3.3

On suppose dans tout ce paragraphe qu'il existe $(a, b, c) \in S_p(d)$ où p est un nombre premier ≥ 7 et d l'un des entiers considérés dans les énoncés des théorèmes 3.1, 3.2 et 3.3.

Notations et rappels. Soit $n \in \mathbb{N}^*$. On désigne par $\mathcal{S}_2^+(n)$ l'espace des newform (au sens de [1]) de poids 2 pour le sous-groupe $\Gamma_0(n)$ de $\mathrm{SL}_2(\mathbb{Z})$. On dit que $f \in \mathcal{S}_2^+(n)$ est normalisée si son développement de Fourier à l'infini s'écrit

$$f = q + \sum_{m \geq 2} a_m(f) q^m, \quad \text{avec } q = e^{2i\pi\tau}.$$

Il y a exactement $\dim_{\mathbb{C}}(\mathcal{S}_2^+(n))$ formes normalisées dans $\mathcal{S}_2^+(n)$. Pour une telle forme, notons K_f le corps de rationalité des coefficients $a_m(f)$, $m \geq 2$ et $\mathrm{N}_{K_f/\mathbb{Q}}$ la norme de l'extension $K_f/\mathbb{Q}$.

Si $A/\mathbb{Q}$ est une courbe elliptique, on note

$$L_A(s) = \sum_{m \geq 0} a_m(A) m^{-s}$$

sa fonction L de Hasse-Weil.

Rappelons le résultat bien connu suivant (cf. par exemple [33]).

Proposition 3.9 *Il existe $f \in \mathcal{S}_k^+(N(\rho_p^E))$ normalisée telle que pour tout nombre premier ℓ, les conditions suivantes soient réalisées.*
(1) Si ℓ divise N_E et ne divise pas $pN(\rho_p^E)$, alors

$$p \text{ divise } \mathrm{N}_{K_f/\mathbb{Q}}(a_\ell(f) \pm (\ell + 1)).$$

(2) Si ℓ ne divise pas pN_E, alors il existe un entier $r \leq \sqrt{l}$ tel que

$$p \text{ divise } \mathrm{N}_{K_f/\mathbb{Q}}(a_\ell(f) \pm 2r).$$

Pour l'assertion (2), on utilise le fait que, comme E a un point d'ordre 2 rationnel sur $\mathbb{Q}$, le coefficient $a_\ell(E)$ est pair. On a de plus $|a_\ell(E)| \leq 2\sqrt{\ell}$ d'après les bornes de Weil.

Si f, vérifiant les conditions de la proposition 3.9, a ses coefficients $a_m(f)$ dans $\mathbb{Z}$, alors elle correspond à une courbe elliptique E_f de conducteur $N(\rho_p^E)$ définie sur $\mathbb{Q}$ et les représentations ρ_p^E et $\rho_p^{E_f}$ sont isomorphes.

Soit $\mathbb{Q}(E[p])/\mathbb{Q}$ l'extension de $\mathbb{Q}$ engendrée par les coordonnées des points de p-torsion de E. C'est une extension galoisienne de $\mathbb{Q}$. Soit e son indice de ramification en 2.

Lemme 3.10 *Supposons $ab \equiv -1 \pmod 4$. On a $e = 2p$.*

Démonstration : Supposons $ab \equiv -1 \pmod 4$. D'après lemme 3.5, l'invariant modulaire j de E n'est pas entier en 2. De plus, on a

$$v_2(j) = 18 - (8 + 2v_2(d) + 2pv_2(c)) \equiv 10 - 2v_2(d) \not\equiv 0 \pmod p$$

car $v_2(d) = 0$ ou 1 par hypothèse. On en déduit $e = 2p$ ([7, cor. 1]).

3.3.1 Démonstration du théorème 3.1

Supposons $d = 1$. D'après le lemme 3.8, on a

$$N(\rho_p^E) = \begin{cases} 2^6 \text{ si } ab \equiv -1 \pmod 4, \\ 2^7 \text{ si } ab \text{ est pair.} \end{cases}$$

Supposons $ab \equiv -1 \pmod 4$. L'espace $\mathcal{S}_2^+(64)$ n'est constitué que d'une seule classe de $\mathbb{Q}$-isogénie de courbe elliptique de conducteur 64. Par ailleurs, la courbe E a potentiellement réduction multiplicative en 2 et son défaut de semi-stabilité en 2 est d'ordre $2p$ (lemme 3.10). Or, les courbes de conducteur 64 ont réduction additive en 2 et leur invariant modulaire est entier. Si A est une telle courbe, l'indice de ramification en 2 de l'extension $\mathbb{Q}(A[p])/\mathbb{Q}$ est 8 (cf. [8] et [18]). Les représentations ρ_p^E et ρ_p^A ne sont donc pas isomorphes. On en déduit que ab est pair. D'où le théorème 3.1.

3.3.2 Démonstration du théorème 3.2

Supposons que $d \in \{2, 6, 10, 22\}$. D'après le lemme 3.8, on a $ab \equiv -1 \pmod 4$ et

$$N(\rho_p^E) = \begin{cases} 2^6 & \text{si } d = 2, \\ 2^6 \cdot 3 & \text{si } d = 6, \\ 2^6 \cdot 5 & \text{si } d = 10, \\ 2^6 \cdot 11 & \text{si } d = 22 \text{ et } p \neq 11, \\ 2^6 & \text{si } d = 22 \text{ et } p = 11. \end{cases}$$

De plus, d'après le lemme 3.10, on a $e = 2p$.

3.3.2.1 Supposons $d = 2$. On a alors $N(\rho_p^E) = 64$. On montre, avec le même argument qu'au paragraphe 3.3.1, que l'ensemble $S_p(2)$ est vide.

3.3.2.2 Supposons $d = 6$. L'espace $\mathcal{S}_2^+(192)$ est de dimension 4 et engendré par quatre classes de $\mathbb{Q}$-isogénie de courbes elliptiques définies sur $\mathbb{Q}$ (cf. [37]). Toutes ont réduction additive en 2 et un invariant modulaire entier en 2. Leur défaut de semi-stabilité en 2 est d'ordre 8 ou 24 (cf. [8] et [18]). En particulier, il est différent de $2p$. On en déduit que l'ensemble $S_p(6)$ est vide.

3.3.2.3 Supposons $d = 10$. L'espace $\mathcal{S}_2^+(320)$ est engendré par six classes de $\mathbb{Q}$-isogénie de courbes elliptiques de conducteur 320 et deux formes modulaires f_1 et f_2 dont les coefficients de Fourier sont conjugués sur $\mathbb{Q}(\sqrt{2})$ (cf. [37]). La forme $f = f_1$ ou f_2 est à coefficients dans l'anneau d'entiers du corps K_f engendré sur $\mathbb{Q}$ par une racine α du polynôme $X^2 - 8$ (*loc. cit.*). Avec les notations de la proposition 3.9, on a pour $\ell = 3$, le tableau suivant.

$a_3(f)$	$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) \pm 4)$	$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f))$	$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) \pm 2)$
α	8	-8	-4

La forme f ne vérifie donc pas les conditions de la proposition 3.9. On en déduit que ρ_p^E est isomorphe à la représentation ρ_p^A d'une courbe elliptique $A/\mathbb{Q}$ de conducteur 320. C'est absurde car elles ont toutes réduction additive en 2 et un invariant modulaire entier en 2 (leur défaut de semi-stabilité en 2 divise 24 d'après [31, p.386], en particulier il est différent de $2p$). L'ensemble $S_p(10)$ est donc vide.

3.3.2.4 Supposons $d = 22$ et $p \neq 11$. L'espace $\mathcal{S}_2^+(704)$ est constitué de douze classes de $\mathbb{Q}$-isogénie de courbes elliptiques de conducteur 704 et de huit formes modulaires. Chacune de ces huit formes est conjuguée par l'action de $\mathrm{G}_\mathbb{Q}$ à l'une des quatre formes notées 704M1, 704N1, 704O1 et 704P1 dans [37]. Avec les notations de la proposition 3.9, on a le tableau suivant pour $\ell = 3$.

Newform f	704M1	704N1	704O1	704P1
Polynôme P_f tel que $K_f = \mathbb{Q}(\alpha)$ et $P_f(\alpha) = 0$	$X^2 + X - 4$	$X^2 - X - 4$	$X^2 + X - 4$	$X^2 - X - 4$
$a_3(f)$	α	α	α	α
$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) + 4)$	8	16	8	16
$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) - 4)$	16	8	16	8
$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f))$	-4	-4	-4	-4
$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) + 2)$	-2	2	-2	2
$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) - 2)$	2	-2	2	-2

Aucune de ces formes ne vérifiant les conditions de la proposition 3.9, on en déduit que ρ_p^E est isomorphe à la représentation ρ_p^A d'une courbe elliptique $A/\mathbb{Q}$ de conducteur 704. C'est absurde car elles ont toutes réduction additive en 2 et un invariant modulaire entier en 2. L'ensemble $S_p(22)$ est donc vide dans ce cas.

3.3.2.5 Supposons $d = 22$ et $p = 11$. La représentation ρ_{11}^E est irréductible, de poids 12 (lemme 3.7) et de conducteur 64. Je remercie le referee de m'avoir signalé qu'il existe alors, d'après [30, (2.2)] et [12, lem. 2.1], $f \in \mathcal{S}_2^+(12 \cdot 64)$ normalisée telle pour tout nombre premier $\ell \neq 2, 11$, les conditions suivantes sont réalisées :

(1) Si ℓ divise N_E, alors 11 divise $\mathrm{N}_{K_f/\mathbb{Q}}(a_\ell(f) \pm (\ell + 1))$.

(2) Il existe un entier $r \leq \sqrt{l}$ tel que 11 divise $\mathrm{N}_{K_f/\mathbb{Q}}(a_\ell(f) \pm 2r)$.

Le tableau précédent montre alors que ces conditions ne sont pas vérifiées pour $\ell = 3$ et f l'une des formes conjuguée par l'action de $\mathrm{G}_{\mathbb{Q}}$ à celles notées 704M1, 704N1, 704O1 et 704P1 dans [37]. Par ailleurs, on a vu que ρ_{11}^E n'est pas isomorphe à la représentation ρ_{11}^A d'une courbe elliptique $A/\mathbb{Q}$ de conducteur 704. On en déduit que l'ensemble $S_{11}(22)$ est vide. D'où le théorème 3.2.

Cela démontre le théorème 3.2.

3.3.3 Démonstration du théorème 3.3

Supposons $d = 2\ell$, où ℓ est un nombre premier ≥ 13 satisfaisant à la propriété (P). La représentation ρ_p^E est alors irréductible pour $p \geq 7$ et de poids 2 dès que $p \neq \ell$ (lemmes 3.6 et 3.7). On a alors $ab \equiv -1 \pmod 4$ et $N(\rho_p^E) = 2^6\ell$.

D'après [20, th.3], il existe une constante $\kappa(\ell) > \ell$ ne dépendant que de ℓ vérifiant la condition suivante : si $p > \kappa(\ell)$, alors il existe une courbe elliptique E' définie sur $\mathbb{Q}$, de conducteur $N(\rho_p^E) = 2^6\ell$, telle que les représentations ρ_p^E et $\rho_p^{E'}$ soient isomorphes.

Quitte à augmenter $\kappa(\ell)$, on peut de plus supposer que E' a un point d'ordre 2 rationnel sur $\mathbb{Q}$ (cf. démonstration du th. 4 de [20] et [34, IV-6]).

Lorsqu'il n'existe pas de courbe elliptique sur $\mathbb{Q}$ de conducteur 64ℓ ayant aumoins un point d'ordre 2 rationnel sur $\mathbb{Q}$, on a une contradiction. Or c'est précisément le cas lorsque ℓ vérifie la propriété (P) d'après un théorème de W. Ivorra (cf. [16]). D'après [20], on peut prendre $\kappa(\ell) = \left(4\sqrt{\ell+1}+1\right)^{4(\ell-1)}$. On en déduit le théorème 3.3.

Remarque 3.11 *Pour caractériser l'existence de courbe elliptique sur $\mathbb{Q}$ ayant un point d'ordre deux rationnel sur $\mathbb{Q}$ et un conducteur 64ℓ, Ivorra ([16]) utilise les bornes données par Beukers (corollaires 1 et 2 de [4]) sur les solutions de l'équation de Ramanujan-Nagell. Ces bornes ont depuis été améliorées par Bauer et Bennett ([2]). Notre définition de la fonction g prend en compte ces améliorations (lorsque $2^9 \leq n < 2^{362}$ on a adapté la démonstration du corollaire 2 de [4] aux nouvelles bornes).*

4 Remarques en degré ≥ 3

4.1 Courbe de Frey en degré 6

Soit F un polynôme homogène de degré 6 séparable à coefficients entiers. Sous certaines conditions portant sur F, on peut, comme à la partie 2, construire une courbe elliptique ayant de bonnes propriétés de réduction, associée à l'équation (1).

Par exemple, pour $F(x,y) = \Phi_9(x,y) = x^6 + x^3y^3 + y^6$, on obtient la courbe elliptique suivante :

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$\begin{cases} a_2 = 3ab, \\ a_4 = -3(a^4 - a^3b + 2a^2b^2 - ab^3 + b^4), \\ a_6 = a^6 - 9a^5b + 9a^4b^2 - 19a^3b^3 + 9a^2b^4 - 9ab^5 + b^6. \end{cases}$$

Son discriminant est $\Delta = 2^4 \cdot 3^4 \cdot \Phi_9(a,b)^2$. Elle est semi-stable en dehors de 2 et 3. Une telle courbe devrait permettre d'obtenir des résultats analogues à ceux de la partie 3 pour la forme $F = \Phi_9$.

4.2 Détermination des solutions entières de certaines équations superelliptiques

Dans les parties 2 et 3, on a associé une courbe de Frey à une équation diophantienne donnée. On illustre ici sur un exemple la possibilité de montrer la vacuité de l'ensemble des solutions d'une équation en partant de la donnée d'une courbe elliptique bien choisie.

Soit t une indéterminée. On considère la courbe $E/\mathbb{Q}[t]$ d'équation :

$$E : y^2 + txy = x^3 + (1+t)x.$$

Ses coefficients $\Delta(t)$ et $c_4(t)$ sont les éléments suivants de $\mathbb{Q}[t]$:

$$\Delta(t) = t^6 + 2t^5 + t^4 - 64t^3 - 192t^2 - 192t - 64,$$

$$c_4(t) = t^4 - 48t - 48.$$

De plus, si R désigne leur résultant, on a :

$$R = 2^{16}.$$

Autrement dit, la courbe E est semi-stable en dehors de 2. On spécialise en t entier. Si t est divisible par 4, la valuation en 2 de $\Delta(t)$ est 6. De même, si $v_2(t) = 1$, alors $v_2(\Delta(t)) = 4$. Enfin, si t est impair, $\Delta(t)$ est pair et $c_4(t)$ impair.

Par ailleurs, $(0, 0)$ est un point d'ordre 2 de E rationnel sur $\mathbb{Q}$. La représentation ρ_p^E est donc irréductible pour $p \geq 11$ (lemme 2.5). De plus, l'invariant modulaire j de E est différent de -15^3 et 255^3. On en déduit que ρ_7^E est également irréductible (*loc. cit.*).

On suppose à présent qu'il existe un entier c tel que t vérifie l'équation superelliptique :

$$\Delta(t) = c^p,$$

où p est un nombre premier ≥ 7. D'après les remarques ci-dessus, t est impair. Dans ce cas, la courbe E est semi-stable et la représentation ρ_p^E est de poids 2 et de conducteur 1. C'est absurde. Cela contredit l'existence de c.

A La conjecture *abc* implique la conjecture (A)

Dans [24], M. Langevin montre que la conjecture *abc* est équivalente à la conjecture suivante.

Conjecture A.1 *Soient $F \in \mathbb{Z}[X, Y]$ une forme homogène séparable de degré ≥ 3 et ε un réel > 0. Il existe une constante $C_{\varepsilon,F} > 0$ ne dépendant que de ε et F telle que pour tout couple (a, b) d'entiers non nuls premiers entre eux, on a :*

$$\mathrm{rad}(F(a, b)) \geq C_{\varepsilon,F} \max(|a|, |b|)^{\deg(F)-2-\varepsilon},$$

où $\mathrm{rad}(n)$, $n \in \mathbb{N}^*$, *désigne le produit de tous les nombres premiers divisant n.*

Déduisons la conjecture (A) de cet énoncé.

Proposition A.2 *La conjecture abc implique la conjecture (A).*

Démonstration : Soient F une forme homogène séparable de degré ≥ 3 à coefficients entiers relatifs et d un entier ≥ 1. On considère (a, b, c) une solution propre et non triviale de (1). Posons

$$a' = \frac{a}{\mathrm{pgcd}(a, b)} \quad \text{et} \quad b' = \frac{b}{\mathrm{pgcd}(a, b)},$$

où $\mathrm{pgcd}(a,b)$ désigne le pgcd de a et b. Les entiers a, b et c étant premiers entre eux, on en déduit que $(\mathrm{pgcd}(a,b))^{\deg(F)}$ divise d. On a alors

$$F(a',b') = d'c^p, \quad \text{où } d' = \frac{d}{(\mathrm{pgcd}(a,b))^{\deg(F)}}. \tag{A.1}$$

Les entiers a' et b' étant premiers entre eux, on déduit de la conjecture ci-dessus que pour tout $\varepsilon > 0$, il existe une constante $C_{\varepsilon,F} > 0$ ne dépendant que de ε et F telle que

$$\mathrm{rad}(F(a',b')) \geq C_{\varepsilon,F} \max(|a'|,|b'|)^{\deg(F)-2-\varepsilon}. \tag{A.2}$$

Or, d'après (A.1), on a $\mathrm{rad}(F(a',b')) \leq |d'c|$. Par ailleurs, il existe une constante M_F ne dépendant que de F telle que

$$\max(|a'|,|b'|)^{\deg(F)} \geq M_F |d'c^p|.$$

On déduit alors de (A.2) l'inégalité suivante

$$|d'c| \geq C_{\varepsilon,F} \left(M_F |d'c^p|\right)^{\alpha}, \quad \text{où } \alpha = 1 - \frac{2+\varepsilon}{\deg(F)}.$$

Supposons $\varepsilon < 1$. On a alors $0 < \alpha < 1$ et

$$|c|^{\alpha p - 1} \leq \frac{|d'|^{1-\alpha}}{C_{\varepsilon,F} M_F^{\alpha}}.$$

Pour p suffisamment grand, cela implique $c = \pm 1$. C'est le résultat voulu.

B La conjecture *abc* implique la conjecture de Frey-Mazur

La conjecture de Szpiro (forme faible) affirme l'existence de constantes absolues α et β telles que pour toute courbe elliptique A définie sur $\mathbb{Q}$, on ait

$$|\Delta_A| < \alpha N_A^{\beta}, \tag{B.1}$$

où Δ_A désigne le discriminant minimal de A et N_A son conducteur. Cet énoncé est une conséquence de la conjecture *abc* (cf. [28]). Nous allons montrer qu'il implique la conjecture de Frey-Mazur.

Proposition B.1 *La conjecture abc implique la conjecture de Frey-Mazur.*

Ce résultat m'a été communiqué par A. Kraus. Il figure, sous forme de notes non publiées, dans les Comptes - Rendus du Séminaire de Théorie des Nombres de Caen (exposé XVIII, année 1989 - 1990).

DÉMONSTRATION : Rappelons le résultat suivant.

Lemme B.2 *Soient A et A' deux courbes elliptiques définies sur $\mathbb{Q}$ telles que pour une infinité de nombres premiers p, les modules galoisiens des points de p-torsion de A et A' soient isomorphes. Alors, les courbes A et A' sont isogènes.*

DÉMONSTRATION (lemme B.2) : Notons S la réunion des places de mauvaise réduction de A et A'. Si en un nombre premier p les modules galoisiens des points de p-torsion de A et A' sont isomorphes, on a

$$a_\ell(A) \equiv a_\ell(A') \pmod{p} \quad \text{pour } \ell \notin S \cup \{p\} \text{ (cf. [31, 5.2])}.$$

Par hypothèse, ces congruences sont satisfaites pour une infinité de nombres premiers p. On en déduit les égalités

$$a_\ell(A) = a_\ell(A') \quad \text{pour } \ell \notin S.$$

D'après un théorème de G. Faltings, cela implique que les courbes A et A' sont isogènes ([14, §5, cor. 2]). D'où le lemme.

Soit A une courbe elliptique définie sur $\mathbb{Q}$. Si ℓ est un nombre premier, on rappelle que v_ℓ désigne la valuation ℓ-adique de $\mathbb{Q}$. Considérons un nombre premier $p \in \mathcal{F}_A$, c'est-à-dire pour lequel il existe une courbe elliptique $A^{(p)}$ définie sur $\mathbb{Q}$ telle que les représentations ρ_p^A et $\rho_p^{A^{(p)}}$ soient isomorphes. D'après [19, p.28], il existe une constante $c(A) > 7$ ne dépendant que de A telle que si $p > c(A)$ alors

$$N\left(\rho_p^A\right) = N_A. \tag{B.2}$$

Les représentations ρ_p^A et $\rho_p^{A^{(p)}}$ étant isomorphes, on a, en particulier,

$$N\left(\rho_p^A\right) = N\left(\rho_p^{A^{(p)}}\right). \tag{B.3}$$

On en déduit que N_A divise $N_{A^{(p)}}$. On écrit

$$N_{A^{(p)}} = N_A \cdot u_p. \tag{B.4}$$

Montrons alors que u_p^p divise le discriminant minimal $\Delta_{A^{(p)}}$ de $A^{(p)}$.

On considère pour cela un nombre premier $\ell \neq p$. Alors

$$v_\ell\left(N\left(\rho_p^{A^{(p)}}\right)\right) = v_\ell\left(N_{A^{(p)}}\right)$$

sauf si $A^{(p)}$ a en ℓ réduction multiplicative et p divise $v_\ell(\Delta_{A^{(p)}})$ ([19, p.28]). Autrement dit, si ℓ divise u_p, alors, d'après les égalités (B.2) et (B.3) et la remarque ci-dessus, $A^{(p)}$ a en ℓ réduction multiplicative et p divise $v_\ell(\Delta_{A^{(p)}})$. En particulier, $v_\ell(u_p) = 1$.

L'entier $N\left(\rho_p^A\right)$ est, par définition, premier à p. D'après l'égalité (B.2), la courbe A a donc bonne réduction en p et le poids de ρ_p^A est 2 (cf. [32]). On en déduit que la représentation $\rho_p^{A^{(p)}}$ est également de poids 2 et que l'on est dans l'un des cas suivants :

(1) la courbe $A^{(p)}$ a bonne réduction en p ;

(2) la courbe $A^{(p)}$ a mauvaise réduction multiplicative en p et l'exposant de p dans $\Delta_{A^{(p)}}$ est multiple de p ;

(3) la courbe $A^{(p)}$ a mauvaise réduction additive en p.

Or d'après [19, p.6], si $A^{(p)}$ a mauvaise réduction additive en p et si $\rho_p^{A^{(p)}}$ est de poids 2, alors, $p \leq 7$. C'est absurde car on a supposé $p > c(A) > 7$. Le cas (3) ne peut donc pas se produire.

On en déduit donc, comme annoncé, que u_p^p divise $\Delta_{A^{(p)}}$. On applique à présent l'inégalité (B.1) à la courbe $A^{(p)}$. On a :

$$|\Delta_{A^{(p)}}| < \alpha N_{A^{(p)}}^{\beta}.$$

Or d'après l'égalité (B.4) et le fait que u_p^p divise $\Delta_{A^{(p)}}$, on a

$$|u_p|^{p-\beta} < \alpha N_A^{\beta}.$$

Il existe donc une constante $p(A)$ ne dépendant que de A telle que si $p > p(A)$, alors $u_p = 1$. On en déduit

$$N_{A^{(p)}} = N_A.$$

Or, à $\mathbb{Q}$-isomorphisme près, il n'y a qu'un nombre fini de courbes elliptiques de conducteur donné. Le lemme B.2 entraîne alors le résultat.

Références

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

[2] M. Bauer, M. A. Bennett, Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation, Ramanujan J. 6 (2) (2002) 209–270.

[3] M. A. Bennett, V. Vatsal, S. Yazdani, Ternary Diophantine equations of signature $(p, p, 3)$, Compos. Math. 140 (6) (2004) 1399–1416.

[4] F. Beukers, On the generalized Ramanujan-Nagell equation. I, Acta Arith. 38 (4) (1980/81) 389–410.

[5] N. Billerey, Équations de Fermat de type $(5, 5, p)$, Bull. Austral. Math. Soc.À paraître.

[6] Y. Bugeaud, G. Hanrot, M. Mignotte, Sur l'équation diophantienne $(x^n-1)/(x-1) = y^q$. III, Proc. London Math. Soc. (3) 84 (1) (2002) 59–78.

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

[8] J. E. Cremona, Algorithms for modular elliptic curves, 2nd ed., Cambridge University Press, Cambridge, 1997.

[9] H. Darmon, The equation $x^4 - y^4 = z^p$, C. R. Math. Rep. Acad. Sci. Canada 15 (6) (1993) 286–290.

[10] H. Darmon, Serre's conjectures, in : Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), vol. 17 of CMS Conf. Proc., Amer. Math. Soc., Providence, RI, 1995, pp. 135–153.

[11] H. Darmon, A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. 27 (6) (1995) 513–543.

[12] F. Diamond, The refined conjecture of Serre, in : Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 22–37.

[13] J. S. Ellenberg, Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$, Amer. J. Math. 126 (4) (2004) 763–787.

[14] G. Faltings, Finiteness theorems for abelian varieties over number fields, in : Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 9–27.

[15] M. Hindry, J. H. Silverman, Diophantine geometry, vol. 201 of Graduate Texts in Mathematics, Springer-Verlag, New York, 2000, an introduction.

[16] W. Ivorra, Courbes elliptiques sur $\mathbf{Q}$, ayant un point d'ordre 2 rationnel sur $\mathbf{Q}$, de conducteur $2^N p$, Dissertationes Math. (Rozprawy Mat.) 429 (2004) 55.

[17] M. A. Kenku, On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class, J. Number Theory 15 (2) (1982) 199–202.

[18] A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, Manuscripta Math. 69 (4) (1990) 353–385.

[19] A. Kraus, Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique, Dissertationes Math. (Rozprawy Mat.) 364 (1997) 39.

[20] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, Canad. J. Math. 49 (6) (1997) 1139–1161.

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

[22] A. Kraus, On the equation $x^p + y^q = z^r$: a survey, Ramanujan J. 3 (3) (1999) 315–333.

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

[24] M. Langevin, Imbrications entre le théorème de Mason, la descente de Belyi et les différentes formes de la conjecture (abc), J. Théor. Nombres Bordeaux 11 (1) (1999) 91–109, les XXèmes Journées Arithmétiques (Limoges, 1997).

[25] G. Ligozat, Courbes modulaires de genre 1, Société Mathématique de France, Paris, 1975, bull. Soc. Math. France, Mém. 43, Supplément au Bull. Soc. Math. France Tome 103, no. 3.

[26] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math. 44 (2) (1978) 129–162.

[27] T. Nagell, Collected papers of Trygve Nagell. Vol. 1, vol. 121 of Queen's Papers in Pure and Applied Mathematics, Queen's University, Kingston, ON, 2002, edited by Paulo Ribenboim and with a short biography of Nagell by J. W. S. Cassels [reprinted from Acta Arith. **55** (1990), no. 2, 109–112].

[28] J. Oesterlé, Nouvelles approches du "théorème" de Fermat, Astérisque (161-162) (1988) Exp. No. 694, 4, 165–186 (1989), séminaire Bourbaki, Vol. 1987/88.

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

[30] K. A. Ribet, Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, in : Motives (Seattle, WA, 1991), vol. 55 of Proc. Sympos. Pure Math., Amer. Math. Soc., Providence, RI, 1994, pp. 639–676.

[31] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (4) (1972) 259–331.

[32] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. 54 (1) (1987) 179–230.

[33] J.-P. Serre, Travaux de Wiles (et Taylor, ...). I, Astérisque (237) (1996) Exp. No. 803, 5, 319–332, séminaire Bourbaki, Vol. 1994/95.

[34] J.-P. Serre, Abelian l-adic representations and elliptic curves, vol. 7 of Research Notes in Mathematics, A K Peters Ltd., Wellesley, MA, 1998, with the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[35] J. H. Silverman, The arithmetic of elliptic curves, vol. 106 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1992, corrected reprint of the 1986 original.

[36] V. G. Sprindžuk, Classical Diophantine equations, vol. 1559 of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1993.

[37] W. Stein, The Modular Forms Database,
`http ://modular.math.washington.edu/Tables`.

[38] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, in : Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 33–52. Lecture Notes in Math., Vol. 476.